electronics

MDPI

Review

Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends

Zhang Wenhua [1], Faizan Qamar [1], Taj-Aldeen Naser Abdali [2], Rosilah Hassan [1,*], Syed Talib Abbas Jafri [3] and Quang Ngoc Nguyen [4,*]

[1] Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi 43600, Malaysia
[2] Department of Computer Engineering, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Maysan 10011, Iraq
[3] Department of Electronic Engineering, NED University of Engineering & Technology, Karachi 75270, Pakistan
[4] Faculty of Science and Engineering, Waseda University, Shinjuku-ku, Tokyo 169–0051, Japan
* Correspondence: rosilah@ukm.edu.my (R.H.); quang.nguyen@fuji.waseda.jp (Q.N.N.)

Abstract: Blockchain technology provides a data structure with inherent security properties that include cryptography, decentralization, and consensus, which ensure trust in transactions. It covers widely applicable usages, such as in intelligent manufacturing, finance, the Internet of things (IoT), medicine and health, and many different areas, especially in medical health data security and privacy protection areas. Its natural attributes, such as contracts and consensus mechanisms, have leading-edge advantages in protecting data confidentiality, integrity, and availability. The security issues are gradually revealed with in-depth research and vigorous development. Unlike traditional paper storage methods, modern medical records are stored electronically. Blockchain technology provided a decentralized solution to the trust-less issues between distrusting parties without third-party guarantees, but the "trust-less" security through technology was easily misunderstood and hindered the security differences between public and private blockchains appropriately. The mentioned advantages and disadvantages motivated us to provide an advancement and comprehensive study regarding the applicability of blockchain technology. This paper focuses on the healthcare security issues in blockchain and sorts out the security risks in six layers of blockchain technology by comparing and analyzing existing security measures. It also explores and defines the different security attacks and challenges when applying blockchain technology, which promotes theoretical research and robust security protocol development in the current and future distributed work environment.

Keywords: blockchain; security; privacy; healthcare; six-layer; parallel security

Citation: Wenhua, Z.; Qamar, F.; Abdali, T.-A.N.; Hassan, R.; Jafri, S.T.A.; Nguyen, Q.N. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics* **2023**, *12*, 546. https://doi.org/10.3390/electronics12030546

Academic Editors: Chunjie Yang, Qing-Guo Wang, Ping Zhou, Zhaohui Jiang and Zhuoyun Nie

Received: 28 November 2022
Revised: 3 January 2023
Accepted: 5 January 2023
Published: 20 January 2023

1. Introduction

As the distributed ledger that documents bitcoin transactions, blockchain was initially introduced in 2008, and then the genesis block mined by Nakamoto in 2009 verified the concept of blockchain [1]. The framework concept included the E-cash system based on a peer-to-peer (P2P) network, encryption, timestamp, and blockchain technology [2]. It is a successful application where peers can share values using transactions without the need for a central authority to safeguard consumer privacy and avoid identity fraud [3].

Blockchain technology has been implemented in numerous fields as part of the infrastructure of some businesses that require transparency, integrity, and dependability [4] since its inception, from the initial cryptocurrency to the current blockchain-based application for industry 5.0 [5–7]. However, with the massive application of blockchain technology and the continuous development of new technologies, blockchain technology's challenges and threats are constantly escalating. In Ethereum, a smart contract is a piece of code deployed to the network so everyone can access it [8]. The implementation of blockchain technology in the healthcare sector may encompass all aspects of hospital systems, such as

process, supervision, statistics, finance, auditing, and archival materials, as well as provide valuable technical assistance for re-establishing the structure of hospital informatization and workflow. Technological improvements in blockchain from 1.0 to 5.0 [9–13] make it more suitable and stable for industrial applications and business requirements:

- *Blockchain 1.0:* the programmable currency represented by bitcoin led the new digital payment system. The decentralized, key-based digital currency transaction model makes it the origin of blockchain technology.
- *Blockchain 2.0:* based on the programmable society, blockchain-based applications are widely used in social fields such as finance, P2P transactions, information creditable registration, ownership and copyright confirmation, and intelligent management.
- *Blockchain 3.0:* it makes blockchain more widely applied to decentralized applications (DApps), and through decentralization, non-tampering, and trusted sharing, improves operational efficiency and the trust level of the society.
- *Blockchain 4.0:* an extension of the last generation to make the DApps more feasible for real-time business scenarios that apply in Industrial Revolution (IR) 4.0, which regulates within the network through the consensus protocol [14,15].
- *Blockchain 5.0:* this generation is considered an upcoming generation of blockchain because it reduces the traditional blockchain limitations [16] and the virtual connections for increased processing speed and security [17].

Blockchain 1.0, 2.0, 3.0, 4.0, and 5.0 are not progressive evolutions but are in different application stages. From 1.0 to 5.0, they are all parallel scopes of development playing their due roles in various fields. Figure 1 depicts the scope of technical improvement in blockchain, while Figure 2 shows the comparison between traditional and blockchain transparency networks.

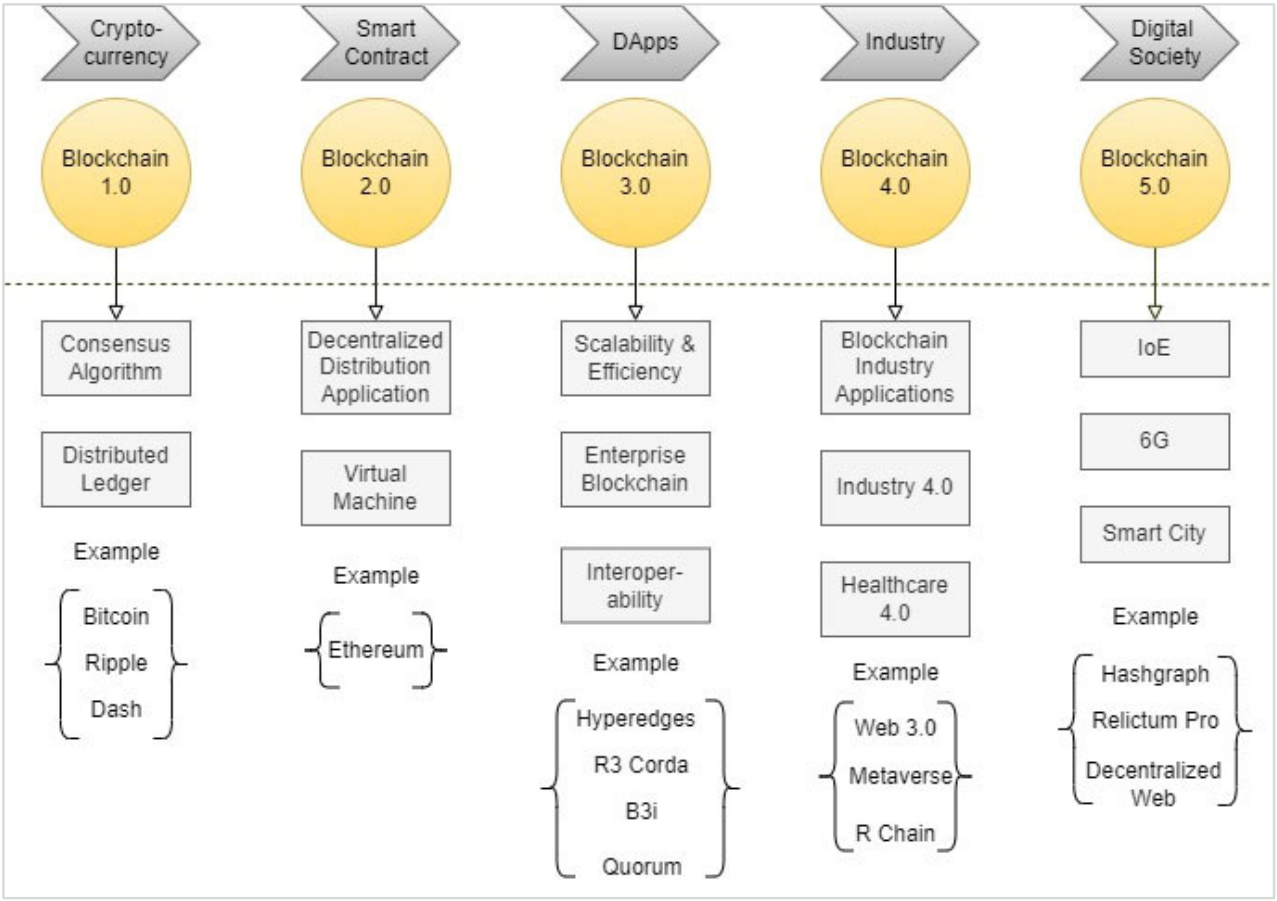
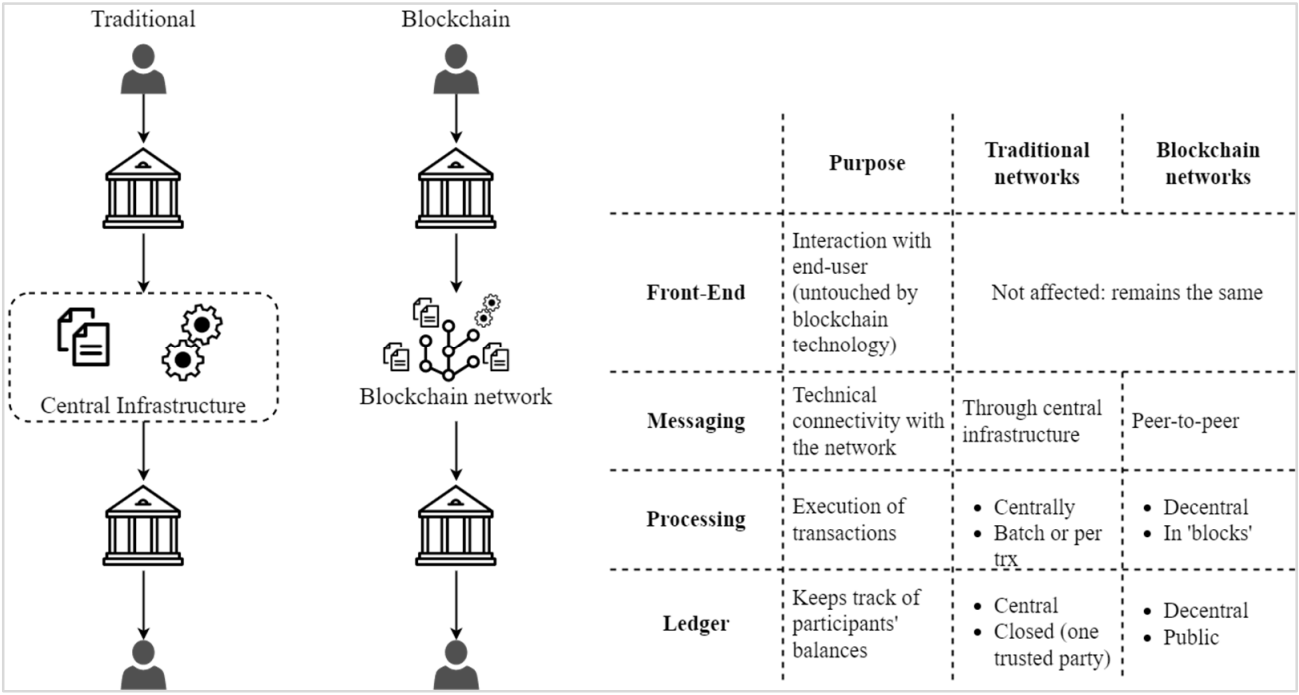


Figure 1. The scope of technical improvement in blockchain.



	Purpose	Traditional networks	Blockchain networks
Front-End	Interaction with end-user (untouched by blockchain technology)	Not affected: remains the same	
Messaging	Technical connectivity with the network	Through central infrastructure	Peer-to-peer
Processing	Execution of transactions	• Centrally • Batch or per trx	• Decentral • In 'blocks'
Ledger	Keeps track of participants' balances	• Central • Closed (one trusted party)	• Decentral • Public

Figure 2. The transparency network comparison between traditional and blockchain.

Since the release of blockchain 2.0, the technology has been decoupled from currency transactions, and its potential for other financial and inter-organizational interactions has been investigated, referring to applications beyond currency transactions. With increased digitalization, blockchain 3.0 gives additionally distributed storage capacity and scalability without reducing security and aids in the integration of data from various sources without compromising privacy. Transparency is provided without disclosing ownership, interoperability is ensured without introducing unnecessary complexity, and a source of authentication is established. Blockchain technology's flexibility and multifaceted capabilities provide enormous possibilities for healthcare innovation, integration, and sustainability.

1.1. The Concept and Features of Blockchain

Firstly, from a technical perspective, blockchain is not a new technology but consists of a series of existing technologies:

- Peer-*to*-peer network immutable distributed ledger: ensures that the single node ledger is structurally immutable through the data structure of blockchain.
- Security technology such as encryption: cryptography and hash algorithms guarantee the security and privacy of transactions.
- Consensus algorithms: a pure mathematical mechanism for collective verification of blockchain to establish a trusting relationship between all parties and uses technology to ensure that the consensus results.
- Smart contract: A new concept of the contract was introduced by Nick Szabo in 1994, who called this new contract "smart" because it includes a set of agreements by which contract participants can enforce these commitments. Smart contracts guarantee trusted business deals without third-party involvement, and the main purpose of smart contracts is to provide a security method and reduce transaction costs with other contracts. Therefore, smart contracts ensure that all the transactions between the nodes are credible and reliable [18].

Secondly, in principle view, blockchain is a distributed-shared ledger technology, which establishes a decentralized, machine-trusted, and collectively distributed shared

ledger system and uses a perfect mathematical solution to develop a mechanism for the trust and consensus of all parties involved.

Blockchain features:

- *Sharing and openness:* the system is open to all participants, who have the right to know and equally enjoy blockchain information.
- *The consensus:* through the voting of particular nodes to complete the verification and confirm transactions in a fraction of the time. If several nodes can reach a consensus without the related interests for a transaction, it considers the network's consensus.
- *Fair competition:* the operations of all nodes are calculated by algorithms, and algorithms determine the accounting rights.
- Authenticity and integrity: each record is recorded truthfully and completely under supervision.
- *Safe and reliable:* data encryption and cryptography mechanisms prevent the data from being tampered with and forged; the complex checksum sharing mechanism ensures integrity, availability, and confidentiality. Multiple attackers are detected through an encryption standard (digital signature) in which every node has its key, and the packet transmission is performed when the key is in a valid state [19].

1.2. Limitations and Challenges of Blockchain Security

Health information is collected with a variety of medical data sources and complicated data forms. Data sharing allows EHR interaction across multiple healthcare platforms, but it also compromises patient privacy. Blockchain technology has several technical obstacles affecting its large-scale and widespread in the healthcare sector [20–24]:

- Limited transaction performance and scalability: blockchain's limited transaction processing capacity and the slow time for transactions to form blocks.

The expansion solutions are as follows:

1. *Sharding:* the idea of sharding is to divide the overall state of the blockchain into different blocks and process them in parallel.
2. *Off-chain:* high throughput of transactions can be achieved by moving the computation and verification process to a separate protocol off-chain; blockchain is used as an agreement layer to manage the sum of a sequence of transactions.
3. *DAGs (directed acyclic graph):* a graph organization consisting of vertices and edges (vertices are purposes within the graph, and edges are methods from one point to a different graph). A DAG guarantees that there are not any cycles that allow acquiring the grouping of nodes along with the topological sequence.

- Limited privacy protection: blockchain can be tamper-proof and decentralized, but precisely because the user's ledger is transparent to participating organizations, that is, any organization can access the same data. Unmasked users' private data on the chain will amplify the risk of user privacy leakage. Currently, in public chain systems such as Bitcoin, all transaction information is public (including transaction amounts). This means it does not meet some regulatory privacy requirements, such as General Data Protection Regulation (GDPR) [25]. There is a need for the following related security technologies to make further breakthroughs:

1. *Homomorphic encryption:* HE encrypts the transaction data and protects it with the public key. The transactions are ciphertext operations, and the final ledger is encrypted and stored. The obtained ledger records cannot be decrypted even if the node was compromised. The process of HE is shown in Figure 3.
2. *Zero-knowledge proof:* ZKP verification can be made without any useful information provided by the verifier and without revealing the proven message to the verifier during the proof process.
3. *Trusted execution environment:* the security zone of the principal processor that ensures the code and information loaded inside are secured classification and respectability.

4. *Storage constraints:* the blockchain database is stored indefinitely that only can be added but cannot be changed. Consequently, data storage adds a major expense for the circulated network, and each full node must store ever-increasing data endlessly. Thus, storage is an immense obstacle for any real-world application based on a blockchain.

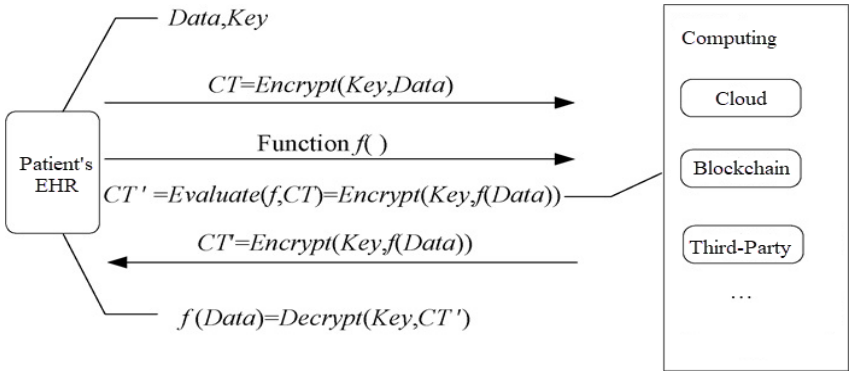


Figure 3. The progress of homomeric encryption.

At present, the storage solutions of the public chains are as follows:

- *Swarm:* an Ethereum P2P sharing protocol that allows users to store application code and data in the swarm nodes under the main chain, and then users can access the blockchain to exchange the data.
- *The Storj network:* files and data are sharded, encrypted, and distributed to multiple nodes so that each node can only store a small part of the data.
- *The IPFS:* an optional peer-to-peer hypermedia protocol that provides a high-throughput block storage model based on content-addressable hyperlinks. Essentially, it allows files to be stored permanently and distributed while providing historical versions of files, thus removing duplicate files.
- *Decent:* a distributed content-sharing platform that allows users to upload and digitally monetize the sharing of their work (videos, music, e-books, EHR, etc.) without relying on a centralized third party for sharing.
- *Alliance chain:* the data can be archived in the alliance chain. Blockchain operating system only retains recent data, preserving historical data through archiving.

Table 1 shows the advantage and limitations of blockchain technology [26–28].

Table 1. The advantages and limitations of blockchain technology.

Advantages	Limitations
Reduce cost and increase efficiency.	Cost-effectiveness has yet to be proven.
Secure, accessible, and real-time.	Insecure with data leaking issue.
Network transactions database.	Regulatory issues and technical challenges.
Better security against "pushing".	Risk for potential compromise of data set.
Easy communication in the more extensive network.	Smaller networks pose the same concern.

Blockchain technology is applied in the health sector to address security threats, as homomeric encryption is a hot method to secure EHR privacy and security. The comparison of the implementation of blockchain technology and HE is shown in Table 2.

Table 2. The comparison of the implementation of blockchain technology and homomorphic encryption.

Ref.	Application Domain	Implemented Algorithm	Summary
[29]	Healthcare medical claims in blockchain	Paillier encryption scheme	The insurance company sends the request to the hospital to verify the integrity of the patient's EHR.
[30]	Property digital copyright Protection	Large prime number (LPN) algorithm	Blockchain-based auction to protect the property's digital copyright in an effective and practical way.
[31]	Genomics, Health, National security, Education	HE, Fully homomorphic encryption (FHE)	The paper presents a list of potential applications for HE in various domains to determine the importance of data privacy and security.
[32]	Biomedical sensitive data sharing in the public cloud	El Gamal, Discrete Logarithms	The proposed solution brings a new simple model to minimize the risk of sharing medical data in the public cloud, the limitation of this model is that it needs to run online.
[33]	Personal health data collection and storage	BGV scheme, Leveled homomorphic using modulus switching (RLWE)	The author proposed a system that applied HE to secure personal health data collection, storage, and transmission in the cloud.
[34]	Healthcare medicine side effect query system	Smart and Vercauteren, SIMD Style FHE	A time-efficient privacy-preserving query system model and implementation in a real-world medicine side effect query system. Higher communication cost with or without threads, but still practical.
[35]	Medical data collection	Fan and Vercauteren, Lattice based leveled homomorphic (RLWE)	HE applied in clinical research to help patients and doctors accelerate learning from real-world data.

1.3. Motivation and Contribution

The nature of cryptography determines that it has high requirements for the hardware equipment and software tools when processing data and computing plans; it is impossible to have fixed standard computing hardware (such as CPU or GPU) to achieve a satisfactory level. In addition, during the operation of large-scale equipment, especially for encryption/decryption calculations, the noise and heat generated by hardware equipment also pose a huge challenge to calculation speed and memory management.

The academic community has conducted extensive research on the architecture, privacy, and network security of blockchain technology, but not been much in-depth research on the implementations of blockchain technology in the medical industry. This article starts with the fundamental theory of blockchain and progresses to the security architecture, conducting in-depth research and analysis on the challenges and future trends of

blockchain healthcare development and combining potential medical advancement with current cryptography encryption technology. It will also provide a practical reference for the development of blockchain technology in the healthcare industry, provide comprehensive theoretical research and strong security protocol development, and promote the implementation and development of blockchain technology in the medical field.

From the above introduction, we have an overview of the blockchain concept, how it works, its limitations, and its challenges. The remaining part of the paper is structured as follows: Section 2 presents the literature review works. Section 3 dissects the security issues in six layers of blockchain technology. Section 4 provides a comparative study on blockchain-based healthcare implementation and data management. Section 5 explores future research on blockchain security, and in the last section, the full conclusion for this work has been shown.

2. Literature Review

With the widespread circulation of bitcoin and the vigorous development of decentralized platforms in finance or non-financial applications, blockchain has set off a global research boom. Blockchain simplifies EHR sharing between end-user and healthcare infrastructure without disrupting communication. These facilities are provided through trust lines and interoperability certification using distributed ledger technology. Modern Healthcare Apps focus on the privacy of users and the security of shared information to prevent anonymous and unauthorized access by illegal users. Thus, trust, authentication, and privacy are the main requirements for sharing EHRs among different users [36]. Mechanism loopholes, attack methods, and security measures are crucial to the security threat issues at all levels of the blockchain. While it provides security guarantees for a trustless environment, it also faces various challenges in security and privacy [37]. Many countries and originations have turned their research direction focus on the security of blockchain [38,39]. This article focuses on the security issues in blockchain technology and the applications in the healthcare field sorting out the security risks at the technical levels based on six-layers architectures to compare and analyze the existing security measures to develop a stronger secure protocol in the blockchain environment. The conceptual framework of parallel security provides useful security technical, theoretical support, and reference for research on blockchain security. A framework based on a parallel healthcare system is proposed to model and represent the patient's condition, diagnosis, and treatment process, for achieving accurate prediction and guidance of disease diagnosis and treatment through parallel execution [40].

2.1. Research and Significance of Blockchain Security

Since the inception of blockchain technology, there have been five generations of technological developments, and the range of applications has grown dramatically [41]. It is important to investigate and research the security issues associated with blockchain technology.

- Studying the security of blockchain helps to accelerate innovation development. Blockchain involves many aspects, such as the basic cryptographic scheme, distributed consistency, economic incentives, and network security.
- Studying the security of blockchain helps to accelerate technology promotion. Incomplete theoretical security analysis, lack of code evaluation, and frequent security incidents limit the development of blockchain. The study of safe and efficient solutions can be applied to more healthcare scenarios, and gradually widened application examples will also better test the security of blockchain in practice.
- Researching blockchain security helps to realize a trustworthy programmable society. The programmability and automatic execution show smart contracts' intelligent features; studying blockchain's security will help improve the security level and design principle of smart contracts, simplify the development process, and enhance interoperation. Secure blockchain architecture and self-executing smart contracts can technically enforce contracts, reduce default risk, and build a trusty programmable society.

Studying the security of blockchain helps to achieve controllable supervision. The immutability and anonymity of blockchain create challenges to achieving regulation. The supervision mechanism can prevent and detect illegal behaviors in the system and is a security repair method after the system is attacked. Analysis of existing blockchain vulnerabilities, potential attacks, and privacy protection mechanisms is beneficial to formulate network monitoring strategies and design more efficient and secure supervision mechanisms.

2.2. Security Objectives on Blockchain

According to the network system's security requirements, the basic security goal of blockchain system construction is to use cryptography network security and other technical means to protect all levels of blockchain security systems [42]. Security objectives such as consensus security, smart contract security, privacy protection, and content security are closely related to data security [43].

Quantum technology derived from digital and networked assets will provide faster, more advanced blockchain solutions, as well as chances to boost blockchain security and performance [44–46]. Kashyap discusses a way to implement blockchain and quantum cryptography in a quantum cryptosystem [47]. The security and development of network technology are intertwined and synchronized, and the security vulnerabilities and privacy risks in the IoT system can be well addressed by blockchain technology [48]. IoT applications in the healthcare field shorten the communication limitations between doctors and patients as they can be diagnosed remotely in emergency scenarios through intelligent devices and sensors. Blockchain technology is mainly applied in healthcare as it decentralizes immutability, security, privacy, and transparency [49]. Systems of healthcare, IoT, and blockchain are interdependent and share reliable resources. In the technical integration process, [50] conducted a new paradigm investigation on the security risks and challenges. In Monrat's work [51], he provided a comparative study of the different consensus mechanisms and discussed the challenges.

2.2.1. Consensus Security

The security of the data inside the blockchain will be verified by a single entity with rights to the full blockchain network relying on distributed nodes to ensure security. All nodes in the blockchain network performing security for their own blocks causes mistrust of the blocks that are not maintained by individual nodes. In order to prove the authenticity of the verified blocks by different nodes, various methods have been developed to ensure the authenticity of the blocks. The first method of proof of work [52–54] indicates that every node cannot either verify large amounts of blocks or if they are trustworthy; therefore, a one-on-one vote is not used, and only nodes that control a wide array of scarce resources such as computational power or cryptocurrency are selected to create a block that can be authenticated over the blockchain network. If an honest node receives two blocks, then it will only accept the block having the longest chain, thus verifying the integrity of the blocks on the network. The same algorithm also works if the node has the most stakes or resources available, e.g., cryptocurrency as proof of stakes [55–57]. These two methods can also be integrated to check both work and stakes simultaneously, creating a hybrid consensus [58,59].

2.2.2. Smart Contracts

Blockchain 2.0, as referred to, sometimes enables a complete programming language to create smart contracts applications on the blockchain [60]. The security of smart contracts is an important factor as it includes financial settings attracting various hacking attempts and leaving the blockchain network prone to network attacks. Due to the nature of smart contracts, they are triggered in the blockchain network to each node when predefined conditions are met. It is designed to ensure the parties included in any transactions gets their fare-share or contract amount after the conditions are met. They are self-triggered and cannot be stopped. There are, though, several drawbacks that include exploiting

smart contracts to perform undesired operations on the targeted machine without the knowledge of the user, including blockchain withholding attacks [61,62], pool attacks [63], and inconspicuous traps [64].

2.2.3. Privacy and Content Protection

One of the key features of the block is the privacy of the user's identity interacting with the network and hiding transactions that are of someone else. However, this is hard to obtain as the blockchain network is an open system, so each node can verify the integrity of the blocks. The anonymous nature is kept in the blockchain to protect the privacy of the users, which can be broken in several ways [65]. The de-anonymization can be obtained by several attacks, some common to network attacks, others more focused on blockchain. A simple network scan or analysis can leak some information regarding the incoming blocks and their originator [66]. Address clustering can be used to bifurcate the originators of the first block, which are often miners, by finding blocks having no origin-destination pair [67,68], though it is not easy but can be accomplished. One attempt to de-anonymize user information was carried out in [69] using transaction fingerprinting, where the hour of the day, time of the hour, coin flow, and input/output balance are used to track down almost 40% of the bitcoin users. Various types of mixing services [70,71] can be used to protect the user and transaction information. Other than that, online anonymity using a VPN and the Tor network can be used to protect user identification over the blockchain network.

2.3. Parallel Security of Blockchain

Blockchain's parallel security theory uses parallel intelligence and ACP (artificial systems + computational experiments + parallel execution) method [72,73] to realize security decision-making [74]. Parallel security theory constructs artificial blockchain systems by formally describing fundamental elements' static characteristics and dynamic behaviors, such as consensus algorithms, node states, network environments, and security-related incentive mechanisms. Figure 4 shows the concept of parallel security [75], using the artificial system (A) method to model the actual blockchain system to reflect the operating state of the actual system. Method calculation experiments (C) to differentiate artificial attack experiments, analysis, and evaluation are carried out in the artificial system to grasp the evolution law and countermeasures of the corresponding actual blockchain system under various attacks. Additionally, to form a perfect "scenario-response" knowledge base using the parallel execution (P) method, with parallel execution and artificial systems co-evolving with real systems under the same attack, training and learning, experiment and education, management, and control of the actual blockchain system are realized.

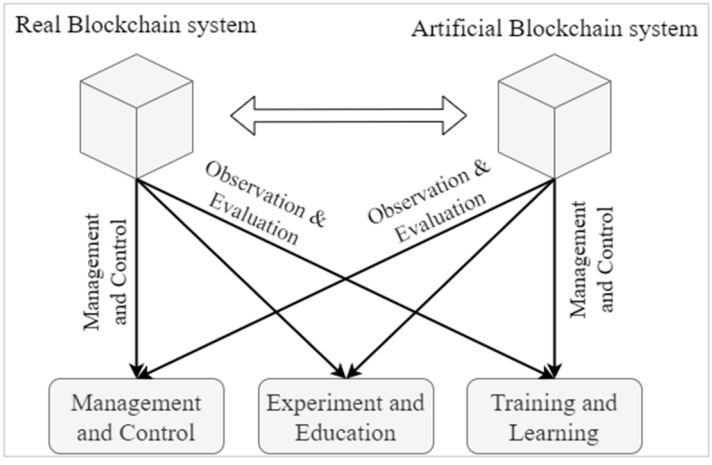


Figure 4. A framework of parallel security on the blockchain.

The parallel security system can optimize the security decision-making of blockchain, accurately and efficiently solving the security threats encountered by the system in the actual operation [76]. However, parallel security is more of a guiding security attack and defense. Its implementation still needs to gradually solve the general modeling, attack simulation, computational experimentation, blockchain intelligent analysis, bidirectional guidance, and the co-evolution of the artificial and the real system.

3. Security Issues of Blockchain Technology

Blockchain has a wide range of applications in the healthcare sector that help healthcare researchers discover the genetic code by facilitating the secure transfer of the patient's medical records, managing the drug supply chain, and facilitating the secure transfer of patient medical data. The descriptions highlight cryptography, immutability, and decentralization, which seem secure [77] due to cryptographic security and the assurance that hardly modify data without the knowledge of other participants [78]. Cryptographic algorithms are essential to realizing the data security system [79]. This does not mean that the blockchain is immune to cyber-attacks and securities fraud. As a multidisciplinary composite new technology, with in-depth research and frequent security incidents, the security flaws of blockchain at all levels are gradually exposed.

Electronic health records (EHRs) are currently stored digitally, and blockchain-based healthcare systems are centralized on a small scale [80]. To continue making blockchain technology an accomplishment, multiple fund providers, healthcare researchers, and health ministries will need to collaborate for the transformation of the healthcare sector, as it will significantly help end users. There are several major blockchain security challenges and preventions [81]:

51% attacks: Miners' primary responsibility is to confirm the transaction request and package data, allowing them to explore the next block even further. A 51% attack is arguably the highest risk in the blockchain industry, as it involves the possibility of modifying the entire blockchain, which is more likely to occur early in the blockchain when there are very few miners on the chain. To increase the hash rate, improve the mining pool monitoring, and avoid using proof-of-work (PoW) consensus procedures to prevent 51% attacks.

Sybil attacks: In a Sybil attack, hackers create fake network nodes and flood the target network with an overwhelming number of false identities, crashing the system and disrupting the chain's transactions. To avoid Sybil attacks, use appropriate consensus algorithms, monitor the behavior of other nodes, and stare for nodes that are only forwarding blocks from one user.

Phishing attacks: Phishing attacks on blockchain systems are getting to be more common, causing genuine issues. In a phishing attack, the hacker's objective is to obtain the user's accreditations. They have the capacity to send legitimate-looking emails to the proprietor of the wallet key. While the user enters login data through a joined false hyperlink, get the qualifications and other data. Improve the security of your browser and device by installing malicious link detection software or reliable anti-malware software, keeping systems and software up to date. Do not click on unknown links, and when using an electronic wallet or other important information, avoid turning on Wi-Fi for online banking transactions to prevent phishing attacks.

Routing attacks: Routing attacks are blockchain technology's next significant security and privacy risk. Hackers can leverage an account's anonymity to intercept data sent to internet service providers. The danger is that these assaults will commonly expose confidential information or assets without the user's awareness. To minimize routing attacks, users ought to ensure secure routing methods must be implemented (with certificates), encrypt user data, use strong passwords and change them regularly, and self-educate about the risks that information security poses.

Private key security attacks: Blockchain technology is based on public-key cryptography; improper implementation or handling of public-key cryptography can result in serious blockchain security issues. An attacker may be able to obtain your private key from the

public key if your blockchain's key signing is poorly implemented. Controlling your private key entails owning all of your data in a blockchain.

Blockchain endpoint vulnerabilities: The vulnerability of blockchain endpoints is another major issue in blockchain security. To obtain the user's password, hackers might track user behavior and target devices. This is one of the most well-known blockchain security flaws. To avoid endpoint vulnerabilities, do not save blockchain keys as text files in the devices, and regularly inspect the system, noting the time, location, and device access.

This section will reinterpret based on the six-layer architecture [82]. Each layer can be subdivided into two parts: the basic module and the security module, as shown in Figure 5. The basic module is the basic component used to realize the main functions of this layer, whereas the security module is a security component used to ensure the security of each layer and provide safe and stable technical support for the upper layer.

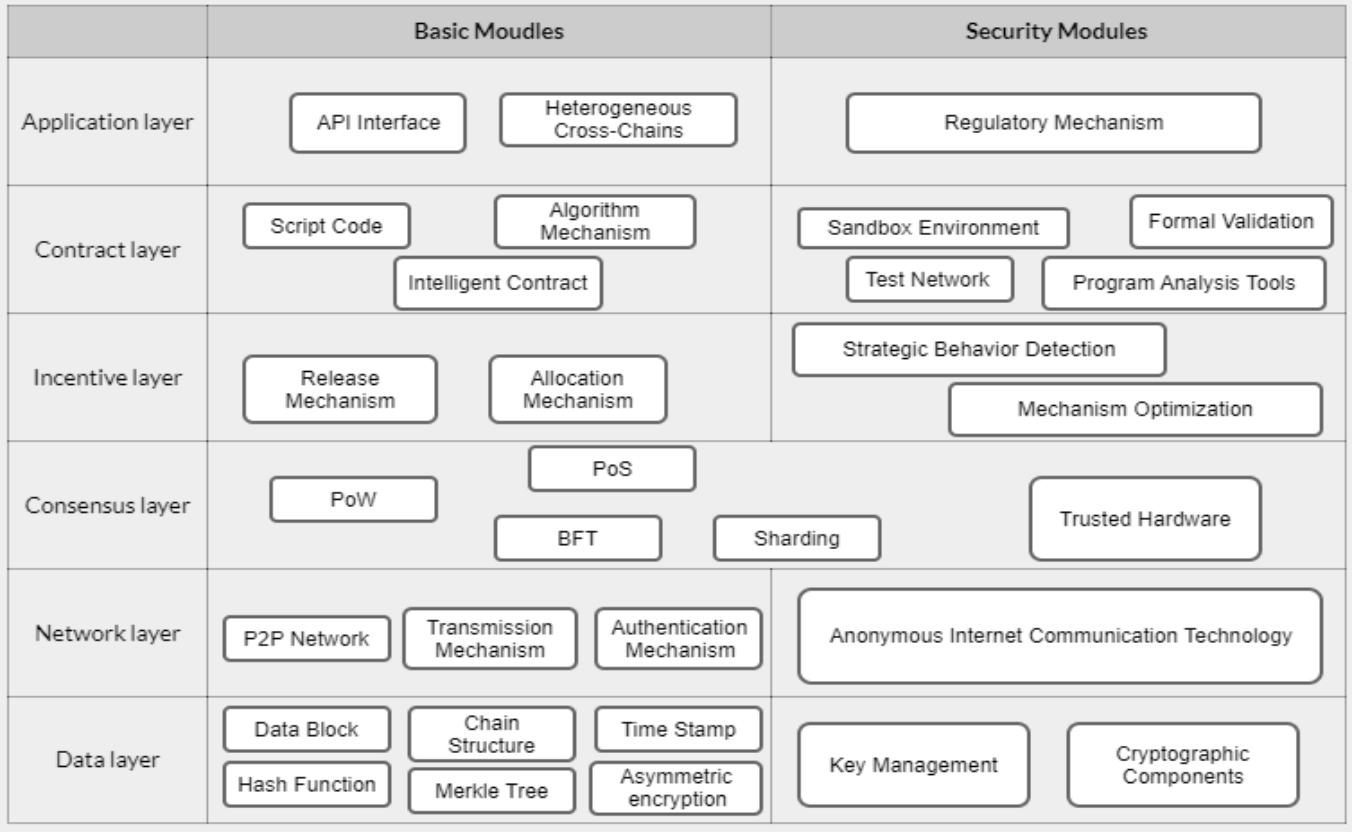


Figure 5. The blockchain system architecture.

3.1. Data Layer

The security module included in the data layer, such as other cryptographic components, is the basis for realizing other five-layer functions. The data layer is facing the following security issues:

- *Quantum computing:* The blockchain data layer's transactions and data blocks involve various cryptographic components [83]. In order to meet higher privacy protection requirements, some blockchains are required privacy protection technologies such as ring signatures and zero-knowledge proofs, but those will affect the security of the data layer [84].
- *Improper key management:* Blockchain-based applications, especially in the financial field, are easily the targets of greedy attackers, relevant digital asset transactions, and healthcare involved in personal details.
- *Leaks and lost keys*: Due to improper use and storage, it has brought immense losses to users; therefore, a reasonable key management mechanism is required. Password-

protected secret sharing (PPSS) is an online threshold wallet scheme [85], and it is the mainstream research direction for blockchain to realize secure key management in the future.

- *Closely related transactions:* Most blockchain-based digital platforms use digital pseudonyms, but this method only provides weak identity anonymity; the correlation between transactions and transaction amounts is disclosed on the blockchain. Once an address is exposed, all public key addresses of the user may be inferred. Through the transaction cluster analysis and transaction graph analysis [86], the user's real identity can also be inferred from the statistical characteristics of the transaction.
- *Code Vulnerability:* Some of the cryptographic components may also have flaws and loopholes in the process of compiling. The transaction malleability attack [87] is an attack against data layer code vulnerabilities, which exploits the malleability of transactions using digital signatures during the compilation process, often used to attack bitcoin trading platforms.

Firstly, the attacker will request a withdrawal from the trading platform. Then, the platform will create a transaction for the attacker. After that, the attacker regenerates the TXID identifier based on the changed transaction to forge a new transaction and broadcasts it to the network. Once the attack is successful, the attacker will get double the bitcoin [88]. Some studies try to deal with the malleability attack of the transaction by modifying the structure of TXID [89].

3.2. Network Layer

The network layer includes a variety of network technologies, and the core function is to ensure the legal joining and effective communication of blockchain nodes. The security issues of the technology itself will inevitably bring security risks to the blockchain network layer:

- *P2P network security vulnerabilities:* The P2P network [90,91] provides a distributed and self-organizing connection mode for nodes in a peer-to-peer network environment, lacking mechanisms such as identity authentication, data verification, and network security management. The P2P network adopts it impossible to use firewalls, intrusion detection, and other technologies for targeted protection due to unequal working modes. The nodes in the network are more vulnerable to attack.
- *Node's network topology:* The node's network topology can create the convenience for attackers to find the attack targets and carry out attacks. Attackers can monitor the network topology by actively injecting packets or passively monitoring the data packets transmitted between routes. The eclipse attack [92] is a typical attack method in which attackers use the topology relationship between nodes to achieve network isolation. The solar eclipse attack can be used as the basis for other attacks [93]: the attacker implements the solar eclipse attack on the node with a computing power advantage, realizes the separation of computing power, affects the distribution of mining rewards, and further reduces the difficulty of attacks such as (self-mining) and double payment [94].
- *Privacy protection issues*: The privacy protection at the data layer cannot avoid the correlation between transaction and user IP address during network transmission; attackers can use the method to monitor and track the IP address destroying privacy protection. The network layer provides the mixing service for anonymous payment in the field of digital currency [95]. Mixing service refers to mixing and outputting multiple unrelated inputs to make sure the outsider cannot correlate the transaction to ensure the flow of digital currency cannot be distinguished to achieve anonymity payment [96].

Centralized mixer and decentralized mixer are two types of mixing services:

- *Centralized mixer:* Performed by a third-party server, the user sends the transaction token, and after multiple transactions are mixed, it will finally send to the recipient.

This method destroys blockchain's decentralization characteristics, hidden dangers such as third-party backdoors to steal tokens and the single point of failure.

The TumbleBit protocol is an off-chain currency mixing protocol, which also requires the participation of a third party but cannot know the transaction details besides only providing services [97].

- *Decentralized mixer*: Generates a new transaction by spontaneously mixing multiple transactions and redistributes the tokens according to the original transaction, thereby realizing anonymous payment.

CoinJoin [98] is a protocol-independent anonymous cryptocurrency mixing technology. Users need to entrust a third party to construct a transaction that mixes multiple inputs, but the CoinJoin technology is not completely anonymous; the third party which provides the service can know the flow of mixed currency transactions.

3.3. Consensus Layer

The consensus layer is to ensure the node sharing with the same valid view and communication mode provided by the blockchain network, committed to designing a more secure, more efficient, and low-energy cost consensus mechanism. An efficient consensus mechanism could help improve the performance of the blockchain system, provide a strong security guarantee, support application scenarios with complex functions, and promote the expansion and extension of blockchain technology.

However, the consensus mechanism still has some limitations, such as incomplete proofs of security, unreliable security assumptions, poor scalability, unstable consistency, and difficulty in initialization and reconstruction:

- *Incomplete proof of security:* Consensus mechanisms need to consider various variables when modeling security, but new consensus mechanisms keep emerging, and some frameworks cannot fully security certify new mechanisms. Kiayias proposed a security model and proof method in synchronous networks [99]. Most of the provable security research on the consensus mechanism focuses on the PoW, which often only considers a single variable. The complex network environment also challenges the security analysis of the consensus mechanism.
- *Unreliable security assumptions:* The security evaluation of modern cryptosystems relies on computational complexity theory, but some security assumptions are easily broken in practical applications. As an example of Bitcoin using PoW, according to the mining pool computing power reach, 56.5% will easily break the security assumption of PoW, preventing the verification and recording of transactions and destroying the activity of the consensus mechanism.
- *Inconsistent consistency:* Consistency is a high property to measure the security of the consensus mechanism, but it is difficult to ensure stable consistency in practical applications. Even proof of elapsed time (PoET) [100] and proof of luck (PoL) [101] utilize trusted hardware to provide randomness to ensure that the consistency of the consensus mechanism is not affected by network conditions.
- *Poor scalability:* Scalability is an important attribute of consensus mechanism research and an indispensable part of blockchain usability [102]. The blocks will increase with the generations, but the number of transactions contained in a block is limited. The Elastico protocol is the first consensus mechanism based on the idea of sharding on blockchain [103]. The legal digital currency framework RSCoin scheme proposed by the Bank of England [104] also uses sharding technology in the permission-obtained blockchain to improve the scalability of blockchain. It seems that the sharding technology theoretically solves the problem of poor scalability, but it introduces the problem of cross-chain transactions, which requires strong security assumptions, and reduces the security of blockchain.

- *Consistency unstable:* The initialization of blockchain is the premise to confirm the stability and reliability of the consensus mechanism, directly related to whether the execution process of the subsequent consensus mechanism is safe and reliable.

There are two ways to initialize blockchain nowadays; one is to rely on a third party to generate the genesis block. This goes against the original intention of the decentralized design of blockchain and cannot be applied to the permission-less blockchain solution in the P2P network, nor to ensure the randomness and security of the genesis block generated by the third party, which may affect the generation of subsequent blocks. Another one is obtained from an existing natural transition; a mature blockchain that relies on a mature PoW-based blockchain to transition to generate a genesis block, increases the complexity of initialization. The insecurity of PoW will directly affect the security of the genesis block and the generation of subsequent blocks:

- *Difficult initialization and reconstruction:* The consensus mechanism endows blockchain with immutability and improves its credibility, but it also increases the difficulty of reconstruction. Once the security is breached, the blockchain cannot be effectively restored to the previous state before the attack without trusted third-party control.

A hard fork [105,106] is the only feasible way to reconstruct blockchain at present. However, there are still many limitations in hard-fork reconstruction, and the hard-fork process will cause both parties to lose interest in these legal transactions.

3.4. Incentive Layer

In the permission-less blockchain, the incentive and consensus layers are interdependent to maintain the security and stability of the blockchain system jointly. The consensus mechanism design will affect the selection of incentive entities and the incentive distribution strategy; correspondingly, the incentive mechanism design is also related to the security of the consensus mechanism and the stability of the blockchain. The nodes that participate in transaction verification and block generation to obtain higher rewards may adopt strategies that are not conducive to maintenance to improve their profits and even pose security threats [107]. Therefore, the incentive layer needs strategic behavior detection and dynamic reward mechanism optimization:

- *The selfish mining attack:* In the ideal condition, the node obtains mining rewards that are proportional to the computing power in the PoW blockchain, but in the actual mining process, some nodes will obtain more than their rewards, which means a selfish mining attack [108]. The selfish mining attack is an attack against PoW proposed by Eyal in 2013, which is not easy to detect and prevent. In theory, PoW-based permission-less blockchain systems may be attacked by selfish mining. It poses a serious threat to the system's security and the incentive mechanism's fairness.
- *Block withholding:* The mining pool reduces the cost of node mining so that every node can participate and get rewards. Some mining pools will use the target mining pool's reward distribution strategy to implement block-withholding attacks to obtain higher rewards. By entrusting some miners to join the target mining pool to contribute to the invalid workload, share the rewards of the target mining pool, chase the entire mining pool, and obtain higher rewards.
- *Unsustainable problem:* The incentive mechanism of digital currencies such as bitcoin includes block rewards and transaction fees, but the main income of miner nodes gradually decreases due to the limit of blocks. With the reduction of block rewards, these blockchains will inevitably rely entirely on transaction fee-driven and face unsustainable problems. Carlsten studied the stability of blockchain in the extreme case of relying on transaction fees to motivate nodes [109] and points out that only relying on transaction fee rewards is difficult to avoid the tragedy of the commons, resulting in many blockchain forks, affecting the security and efficiency of the blockchain. However, the inflation will be with the continuous token issuance, and block rewards will not be attractive over time.

3.5. Contract Layer

The smart contract is a computer program that can be automatically executed according to pre-set contract terms between buyer and seller, including code and data set to deploy, the core of the contract layer. Ethereum is the earliest open-source smart contract development platform [110] because it is open-source and involves the transaction of digital currency; once the code loopholes are exploited, irreversible losses will be caused:

- *Exploited code:* Ethereum uses the scripting language to smart code contracts, and it is difficult to avoid loopholes. According to the smart contract survey [111–113], attacks on Ethereum smart contracts [114] areas: transaction-ordering (TOD) attacks, time-stamp dependency attacks, DAO attacks, stack size limit attacks, immutable bugs attacks, gas-less send attacks, re-entrancy attacks, and the short address attack.
- *External data source call problem:* Blockchain technology is designed to ensure secure payments without the supervision of a trusted third party, but smart contracts need to access external data through trusted technology to establish a relationship with the outside. The TLSNotary and Towncrier schemes [115,116] use the Hypertext Transfer Protocol Secure (HTTPS) protocol to access external data, but they cannot guarantee the consistency and authenticity of the data accessed by different nodes nor avoid the data provider website maliciously changed data or attack to cause a single point of failure. The Auger scheme [117] requires specific users to return results at a specific time by setting a penalty mechanism, but it does not provide users with an interface to access the system at will, which limits its usability.
- *Formal verification is not perfect:* The security problems exposed by the EVM provided by Ethereum endanger the execution of smart contracts and users' digital assets; thus, formal verification and program analysis tools are required to analyze the smart contract code and execution process. However, since most of the existing tools are for the detection and verification of known vulnerabilities, a future study needs existing anti-patterns and program analysis for dynamic detection.
- *Privacy protection issues:* Ethereum and Hyperledger are open-source platforms. Smart contracts involve many users, and the execution of transactions also requires users to provide transaction information. Like the data layer, cryptography provides technical support for improving the privacy-preserving properties of smart contracts. Some applications with high confidentiality requirements and complex functions pose challenges to designing and writing smart contracts. Cryptography also has limitations in practical applications.

3.6. Application Layer

Blockchain has been widely applied in finance, supply chain, energy, and other fields [118,119]. The application layer needs to reflect the business functions in different scenarios, and the architecture design also will be some slight differences. The application layer directly interacts with users and needs to have a certain commonality in the design of architecture. Generally, the application layer includes an API interface, cross-chain heterogeneity, and supervision technology:

- *Difficulty in cross-chain operation:* With many heterogeneous blockchain applications, it is imperative to connect them with cross-chain technology to build an interconnected, interoperable, and trustworthy application network. Decentralized blockchain, unlike traditional systems, achieves interoperability through central nodes. How to realize the connection between decentralized blockchain platforms is the biggest challenge faced by cross-chain technology. Blockchain developers have successively used technologies such as a notarization mechanism, sidechain or relay network, hashed time-locked contract (HTLC), and distributed private key control to achieve heterogeneous blockchain interconnection.
- *Lack of regulatory technology:* Security incidents similar to darknet transactions, ransomware, and theft of digital assets in Bitcoin and Ethereum have sparked wide debate in the community about the lack of oversight of blockchain platforms. Supervision

technology consists of reporting, tracking, and accountability of illegal acts to ensure the security of the content of the blockchain platform. However, the decentralization, invariability, and obscurity of blockchain make it more delicate to set up a supervision medium. As the most mature blockchain platform operation with the highest demand rate, Bitcoin has naturally come to the forefront of supervisory technology exploration [120]. Since the network's data monitoring and analysis schemes generally use a "one-size-fits-all" monitoring technology approach, risking the abduction of honest users who typically use Bitcoin for legal transactions; thus, supervision technology on Bitcoin is inevitably not applicable to other blockchain mining platforms.

- *Other attacks:* The code vulnerabilities in the development process of the application layer, especially in the application scenario where the third-party platform is involved, it is more prone to the risk of unauthorized vulnerability. In addition, in a multi-party blockchain application, an attacker can control the application software or hardware within the scope of personal authority, implement a MATE attack (man-at-the-end attack) [121], violate the application layer protocol regulations or Industry norms, maliciously leak or tampering with user information, destroying the confidentiality and integrity of data.

Predicated on the above of these factors, while blockchain has a number of security flaws, cyber security professionals can do a lot to mitigate these issues, which will help to design more robust security protocols in a distributed environment. IT experts with well-honed analytical and technical skills will be well-positioned to deploy blockchain in the most secure manner. Logically, understanding every detail that affects blockchain security is critical as well.

4. Blockchain-Based Healthcare

Blockchain adoption in the health industry requires not only overcoming technological challenges but also developing a solid foundation in terms of hardware and network infrastructure [122]. Fortunately, in today's ICT construction, big manufacturers will provide customized products and services or professional equipment, reducing the difficulties of the facility significantly. Blockchain networks have a wide range applied to healthcare systems corresponding to security and privacy to protect patients' medical data from unauthorized access [123]. However, due to the lack of expert design of security protocols, healthcare systems face many security threats, such as interoperability [124], authenticity, data sharing, medical data transmission, and mobile health deliberation [125]. Moreover, due to the large number of developed hardware devices, the main concern for blockchain in healthcare is implementation and data management.

4.1. Implementation of Blockchain-Based Healthcare

Health and medical data refer to patient treatment records collected throughout the process of personal health prevention and patient care. The system is a sharing system that integrates medical records with computing technologies [126]. The system consists of three modules: data collection, data security, and data service. The data collection module is used to obtain patient health information, the security module is used to establish a protection mechanism for the health service, and the service module is used to meet patients' requests for medical records [127].

According to the above technical solution, the data service module includes a data analysis module, a historical case module, a health guidance module, and a patient evaluation module. The data analysis module is used to compare the collected medical and health data of patients with the data in the blockchain of medical institutions analysis [128]. A historical case module is used to store the past recovery of patients. The health guidance module provides a platform for medical institutions to provide rehabilitation guidance to patients, and the patient evaluation module provides a platform for patients to evaluate medical institutions.

A type of operating technique for a blockchain-based medical data-sharing system includes the following steps:

Step 1: During the patient's recuperation, the medical data-sharing system is used to collect digital records.

Step 2: Securely upload and safeguard the EHR to the health sector blockchain.

Step 3: Compare the newly established EHR to the data stored on the blockchain, perform data analysis, and upload the outcomes.

Step 4: Establish the patient evaluation platform and integrate it directly into the healthcare blockchain.

4.2. Data Management in Blockchain-Based Healthcare

Blockchain technology is among the most recent advancements in information technology, allowing network participants to record transactions and instantly share them with other blockchain users [129]. Blockchain was utilized in several research studies to overcome the inadequacies of current Electronic Health Records (EHR) systems [130].

In addition, by preserving the hash of cloud data on the blockchain, they were able to solve security and privacy concerns about medical records [131]. However, the systems are susceptible to a single point of failure in these tasks because of the cloud server. Furthermore, the technique does not address the issue of patient privacy when medical records are maintained in a centralized cloud database. Many research studies [132–134] propose using blockchain to store medical data in a distributed ledger to overcome the issue of a single point of failure.

In this field, four main categories were proposed as solutions to the security issues of patient data: Firstly, data encryption and decryption techniques [135–137]. Secondly, a new digital signature scheme [138]. Thirdly, the secure data communication method [139]. Fourthly is the key generator mechanism [140] using blockchain technology.

Two important aspects of privacy-preserving systems are controllability and traceability. Therefore, [141] proposed a blockchain-based strategy to allow patients easily own, control, and share their personal data while maintaining their privacy. Secure multiparty computing (MPC) and indicator-centric schema (ICS) are also included in this application-based approach, while Ref. [142] provided a case study that concluded with a demonstration of the enormous benefits of combining the IoT and blockchain. IoT devices are utilized as collectors of the patient's private health data in their work [143], and the patient's real-time data might be preserved in the blockchain. They also discuss blockchain's controllability and traceability features. Their research also looked at the scalability of the blockchain in the context of big data.

The studies [144–146] discussed consent management in eHealth contexts and advocated blockchain as the safest and most trustworthy way to handle healthcare data. Access to personal data has become a worry in this digital age, with security and privacy issues to contend with due to hacker motivations and privacy violations. This is achievable in the eHealth field, where patient health information management systems must adhere to several regulations while staying accessible to officially authorized healthcare practitioners. Most people have heard about blockchain in the payment industry because of its most well-known use, bitcoin. The smart-contract-based healthcare management system has demonstrated how decentralization principles can be applied in the medical ecosystem for large-scale data management. It is also useful to streamline complex medical procedures and an innovative approach to medical record handling using blockchain technology, providing flexibility, interoperability, and accessibility.

4.3. Future Trends of Blockchain-Based Healthcare

Blockchain will have a significant technical impact on humanity's world, and the value, the potential of blockchain healthcare still scratched the surface [147]. Blockchain healthcare will not only revolutionize technology and transform sectors, but it will also upend human society's present order, legal recognition, and value systems [148]. With

the progressive maturation of blockchain technology, it is expected that the following development trends will materialize.

4.3.1. Zero-Knowledge Proof

The blockchain is, by definition, extremely transparent. Any node in the bitcoin system may read and download all of the data recorded in the ledger, and the blockchain incorporates zero-knowledge proof technology to provide consumers and organizations with privacy [149]. The data are utilized to execute the smart contract, and the exact substance of the data is not shared.

4.3.2. Artificial Intelligence

Blockchain can be applied to artificial intelligence to develop a decentralized market and collaborative platform for various AI components like data, algorithms, and computing power [150]. This might open the door for a completely new phase of AI and creative design. Blockchain in healthcare will improve decision-reliability, clarity, and transparency. Artificial intelligence will serve as the foundation for anti-counterfeiting and privacy protection because all blockchain data is accessible to the public.

4.3.3. Internet of Things

Healthcare blockchain technology has the potential to add an extra level of transparency and security to IoT data while also facilitating IoT efficiency, scalability, and standardization in the future [151]. Patients will be able to control who has access to the data collected by blockchain-enabled IoT devices used in healthcare, which will increase the security of the devices against hackers and provide an accurate record of who has viewed the data [152]. Depending on the particular conditions tracked by IoT sensors, blockchain-based solutions supported by smart contracts might automate payments in supply chains.

5. Future Research Focuses on Blockchain Healthcare Security

The security is different between public and private blockchains according to blockchain type, and the difference is another highlight of blockchain security explained properly. Public blockchain networks are accessible and allow any user to join while maintaining participant anonymity; private blockchain needs tighter regulatory and compliance controls [153]. Blockchain can be used to store encoded personal health records that only certain parties have permission to access. To protect patient information, healthcare requires additional requirements, such as interoperability and data transfer. The process of sharing data with other sources is called interoperability. Distributed ledgers provide secure and confidential healthcare management with the participation of healthcare recipients, healthcare providers, insurers, and regulators [154].

Traditionally, personal health record data was stored and maintained on paper; with the advent of cloud developments, the records were shifted to a centralized storage facility. The new era of healthcare, also as known as Health 5.0, necessitates the remote and real-time collection of large users' health data via various sensors and smart wearable devices [155] used for remote health monitoring [156]. These data are produced in large quantities and must be monitored, transmitted, and handled securely. Some patients are afraid to share their private health information with a distributed network, and some hospitals are also hesitant to share specific medication details with insurance companies. Aside from diagnosis and treatment, blockchain technology can help solve a variety of security issues in the healthcare industry [157], as shown in Table 3.

Blockchain has a wide range of applications and functions in healthcare. By facilitating the secure transfer of patient medical records, managing the drug supply chain, and facilitating the safe transfer of patient medical records, blockchain technology assists healthcare researchers in discovering genetic codes [158]. Figure 6 displays the characteristics and key facilitators of the blockchain across a variety of healthcare spheres and associated

fields. Blockchain technology's fully digitalized elements and its use in healthcare-related applications are major reasons for its adoption.

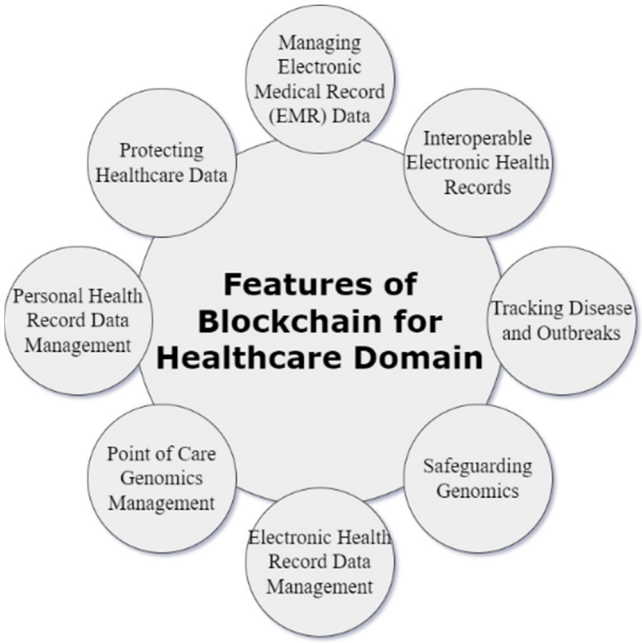


Figure 6. Blockchain features for the healthcare domain.

Table 3. Issues addressed in the healthcare sector by blockchain-based approach [159,160].

Issues Addressed	Blockchain-Based Healthcare Approach	Advantages	Limitations
Security attacks, data privacy	Medical records and data management	To reduce the various attacks on the healthcare system	High bandwidth and high computing power
Security attacks	Patient Monitoring/ERH	Integration with IoT addresses security concerns	Mining incentives and some specific blockchain attacks are not a concern
Data leakage	Drug traceability	Data authentication and privacy, increasing system flexibility	Drug traceability scene complex
Patients' data real-time monitoring security	Real-time patient monitoring/ERH	Systematic protection of data and use of patient data in a more relevant form	Time delay while verifying blocks
Access control, data tampering	Medical records and data management	Ensure the patients' data is legal, transparency of records, and the security of data	Transaction time lacking
Data security	Medical records and data management	An Interoperable Trust Model for Healthcare IoT	Unable to recognize symptom patterns from wearables
Data management	Medical records and data management	Paper works on the security issues	It cannot the security aspects/attacks of IoT
Patients' data monitoring and management	Real-time patient monitoring/ERH and data management	Medical devices read patient vital signs and share them with authorized doctors and hospitals in a secure blockchain network	Lack of communication between the server and devices

The invention of blockchain lies in the consummation of distributed agreements, and smart contracts running on it can also realize rich business functions. Security blights in all situations are demanded in further exploration and disquisition in terms of agreement medium, sequestration protection, supervision medium, and cross-chain technology.

There are four major security considerations to consider while opting for or designing a blockchain security solution. A security solution is regarded to be effective for blockchain if it addresses all four key security concerns:

- *Confidentiality:* The basic idea behind using a blockchain-based system is to enable trusted users better to share information or important content. In this case, the confidentiality of the information we are exchanging is critical.
- *Integrity:* Another critical security concern associated with confidentiality is data integrity. Maintaining data integrity means the data should not be changed in any way. The data sent and received by the sender should be the original messages. If a third party intervenes in the middle and modifies some of the information, its integrity is compromised. The proper security protocol is required to ensure the content's integrity.
- *Non-repudiation:* Non-repudiation means the inability to deny or take accountability for a transaction. When some node denies sending or receiving information to or from another node, this unaccountability issue becomes a significant security concern, which is unlikely to occur in a peer-to-peer network. Non-repudiation should also be addressed in the security procedures. It is accomplished by providing a transaction proofing method in which both the sender and receiver have proof of the transaction.
- *Authentication:* Blockchain is a widespread network with lots of users as participants. In such a case, users may forge their identities in order to commit fraud. To prevent this from happening, proper user authentication is required. Cryptographic techniques such as digital signatures ensure that no user can impersonate another person. Within a blockchain network, only authentic and authorized nodes can transact.

5.1. Breaking "Impossible Trinity"

Although research on consensus mechanisms has achieved some results, it still faces the problems of decentralization, security, and scalability [161]. PoW is the earliest consensus mechanism applied to a blockchain, which has always had low efficiency and high energy consumption problems. How to break the "impossible trinity" deadlock and consider decentralization, security and scalability is an important problem to be solved in the development of the blockchain consensus mechanism.

5.2. Privacy Protection and Controllable Supervision

Privacy protection and regulatory mechanisms are both directions that need to be focused on in future blockchain security [162]. In architecture design, privacy protection relies on cryptographic technologies such as zero-knowledge proof, homomorphic encryption, mixing service technology, the Tor network, and other anonymous network communication technologies to achieve protection of transaction data, user identity, smart contracts, and user behavior information [163].

The future development of blockchain privacy protection will rely on a highly secure and efficient cryptographic scheme and focus on user identities, transaction information, contract codes, and other aspects of privacy protection. In the future, the design of the regulatory blockchain requires institutional innovation and the use of regulatory technology to "govern the chain with the chain", and in addition to regulation, the blockchain-based application needs to be strengthened.

5.3. Blockchain Interconnection

In the process of realizing blockchain interconnection, numerous security problems will also come to the focal points of future exploration [164]. To diversify the data and support more functions, blockchain applications inevitably need to connect to external data

sources to achieve interconnection with the digital world; the decentralization of blockchain was opposed to the centralized operation when interconnecting with the external data source [165]. Numerous miscellaneous blockchain platforms bear effective cross-chain technology to achieve connection.

The secure connection between blockchain and the external data source will help to speed up the consummation of the decentralized IoT operation system, which is anticipated to liberate the serious problem of centralized cargo in the physical world and reduce the operating model of the organization. The connection between blockchain and external data sources should not only exploit the advantages of blockchain to solve the problems of information security, large-scale warehouse, and effectiveness in society but also balance the conflict between the decentralized blockchain and centralized blockchain.

5.4. System-Level Security Architecture

Blockchain development establishes a system-wide security system, improves the security of the entire blockchain, promotes the standardization of blockchain security, and provides guidelines for design, management, and use for the development of blockchain [166]. The construction will focus on security objectives such as data security, consent security, privacy protection, smart contract security, and content security, focusing on physical storage, keys management, network transmission security, functional applications and blockchain confidential data, controllable supervision along with other aspects technical specifications and protective measures.

6. Conclusions

The advancement of medical care is moving into a new era with the development of Health 5.0. Blockchain, as a technological solution, possesses decentralization, secure sharing, non-tampering, and high privacy, which provides a breakthrough for the existing bottleneck of EHR security and privacy development new perspective. Protecting patient medical records from cyberattacks and maintaining privacy with authenticated access is one of the most important challenges facing the healthcare industry. Blockchain security is the foundation of healthcare development, the future development of blockchain security will mainly lie in technology application, application deepening, and supervision systems. Blockchain has natural advantages in managing data security issues, but its own limitations have reduced the healthcare field's involvement in blockchain technology. Homomorphic encryption is a promising solution to the problems of blockchain latency and data privacy. Only authorized parties can encrypt and access particular data during interactions, protecting the security of sensitive patient records. The next study will focus on how to enhance efficiency while preserving data privacy and security, minimize the number of smart contracts, and ensure safe interaction in malevolent mode.

Author Contributions: Conceptualization, Z.W. and F.Q.; Methodology, Z.W., T.-A.N.A. and S.T.A.J.; Visualization, T.-A.N.A. and R.H.; Writing—original draft preparation, Z.W. and F.Q.; Writing—review and editing, Z.W., F.Q., S.T.A.J. and Q.N.N.; Funding acquisition, R.H. All authors have read and agreed to the published version of the manuscript.

Funding: This paper is supported under Universiti Kebangsaan Malaysia Fundamental Research Grant Scheme (FRGS) Code # FRGS/1/2022/ICT11/UKM/02/1. It is also supported by Universiti Kebangsaan Malaysia Dana Impak Perdana 2022.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge the support provided by the Network and Communication Technology (NCT) Research Groups, FTSM, UKM in providing facilities throughout this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of Industry and Blockchain Era: Monitoring Price Hike and Corruption using BIoT for Smart Government and Industry 4.0. *IEEE Trans. Ind. Inform.* **2022**, *18*, 9153–9161. [CrossRef]
2. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* **2008**, 21260.
3. Hassen, A.; Abdulhussein, A.A.; Darwish, S.M.; Othman, Z.; Tiun, S.; Lotfy, Y. Towards a secure signature scheme based on multimodal biometric technology: Application for IOT Blockchain network. *Symmetry* **2020**, *12*, 1699. [CrossRef]
4. Jafar, U.; Aziz, M.A.; Shukur, Z.; Hussain, H.A. A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors* **2022**, *22*, 7585. [CrossRef] [PubMed]
5. Khan, S.N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E. Bani-HaniBlockchain smart contracts: Applications, challenges, and future trends. *Peer Peer Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef]
6. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
7. Rupa, C.; Midhunchakkaravarthy, D.; Hasan, M.K.; Alhumyani, H.; Saeed, R.A. Industry 5.0: Ethereum blockchain technology based DApp smart contract. *Math. Biosci. Eng.* **2021**, *18*, 7010–7027. [CrossRef] [PubMed]
8. Jafar, U.; Ab Aziz, M.J.; Shukur, Z. Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors* **2021**, *21*, 5874. [CrossRef]
9. Khan, G.; Zahid, A.; Hussain, M.; Farooq, M.; Riaz, U.; Alam, T.M. A journey of web and blockchain towards the Industry 4.0: An overview. In Proceedings of the 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 1–2 November 2019; IEEE: New York, NY, USA, 2019; pp. 1–7.
10. Mukherjee, P.; Pradhan, C. Blockchain 1.0 to blockchain 4.0—The evolutionary transformation of blockchain technology. In *Blockchain Technology: Applications and Challenges*; Springer: Cham, Switzerland, 2021; pp. 29–49.
11. Aggarwal, S.; Kumar, N.; Alhussein, M.; Muhammad, G. Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead. *IEEE Network* **2021**, *35*, 20–29. [CrossRef]
12. Choi, T.-M.; Siqin, T. Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transp. Res. Part E Logist. Transp. Rev.* **2022**, *160*, 102653. [CrossRef]
13. Kazmi, S.H.A.; Masood, A.; Nisar, K. Design and analysis of multi efficiency motors based high endurance multi rotor with central thrust. In Proceedings of the 2021 IEEE 15th International Conference on Application of Information and Communication Technologies (AICT), Baku, Azerbaijan, 13–15 October 2021; IEEE: New York, NY, USA, 2021; pp. 1–4.
14. Moke, K.C.; Low, T.J.; Khan, D. IoT Blockchain Data Veracity with Data Loss Tolerance. *Appl. Sci.* **2021**, *11*, 9978. [CrossRef]
15. Jameel, F.; Javaid, U.; Khan, W.; Aman, M.; Pervaiz, H.; Jäntti, R. Reinforcement Learning in Blockchain-Enabled IIoT Networks: A Survey of Recent Advances and Open Challenges. *Sustainability* **2020**, *12*, 5161. [CrossRef]
16. Hoxha, L. Hashgraph the Future of Decentralized Technology and the End of Blockchain. *Eur. J. Eng. Form. Sci.* **2018**, *2*, 86–89.
17. Tanwar, S. Blockchain Revolution from 1.0 to 5.0: Technological Perspective. In *Blockchain Technology*; Springer: Singapore, 2022; pp. 43–61.
18. Kairaldeen, A.R.; Abdullah, N.F.; Abu-Samah, A.; Nordin, R. Data Integrity Time Optimization of a Blockchain IoT Smart Home Network Using Different Consensus and Hash Algorithms. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 4401809. [CrossRef]
19. Talukdar, I.; Hassan, R.; Hossen, S.; Ahmad, K.; Qamar, F.; Ahmed, A.S. Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 6693316. [CrossRef]
20. Barman, N.; Deepak, G.; Martini, M.G. Blockchain for video streaming: Opportunities, challenges, and open issues. *Computer* **2020**, *53*, 45–56. [CrossRef]
21. Qureshi, A.; Jiménez, D.M. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. *Appl. Sci.* **2020**, *11*, 1. [CrossRef]
22. Halpin, H.; Piekarska, M. Introduction to security and privacy on the blockchain. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017; IEEE: New York, NY, USA, 2017; pp. 1–3.
23. Shevkar, R. Performance-Based Analysis of Blockchain Scalability Metric. *Tehnički glasnik* **2021**, *15*, 133–142.
24. Lange, T. Post-quantum Cryptography. *Nature* **2017**, *549*, 188–194.
25. Shafiq, M.M. Framework for Social Media Regulations in Pakistan. *J. Mass Commun. Dep. Dep. Mass Commun. Karachi U.* **2022**, *26*.
26. Sarmah, S.S. Understanding blockchain technology. *Comput. Sci. Eng.* **2018**, *8*, 23–29.
27. Golosova, J.; Romanovs, A. The advantages and disadvantages of the blockchain technology. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 8–10 November 2018; IEEE: New York, NY, USA, 2018; pp. 1–6.
28. Mechkaroska, D.; Dimitrova, V.; Popovska-Mitrovikj, A. Analysis of the possibilities for improvement of blockchain technology. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; IEEE: New York, NY, USA, 2018; pp. 1–4.

29. Xu, W.; Wu, L.; Yan, Y. Privacy-preserving scheme of electronic health records based on blockchain and homomorphic encryption. *J. Comput. Res. Dev.* **2018**, *55*, 2233–2243.
30. Sun, W.; Fang, H.; Zheng, S.; Qian, Q. Blockchain and homomorphic encryption for digital copyright protection. In Proceedings of the 2020 IEEE Intl Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Exeter, UK, 17–19 December 2020; IEEE: New York, NY, USA, 2020; pp. 754–761.
31. Archer, D.; Chen, L.; Cheon, J.H.; Gilad-Bachrach, R.; Hallman, R.A.; Huang, Z.; Jiang, X.; Kumaresan, R.; Malin, B.A.; Sofia, H.; et al. Applications of homomorphic encryption. In *Crypto Standardization Workshop, Microsoft Research*; Sn: Redmond, WA, USA, 2017; Volume 14.
32. Raisaro, J.L.; Klann, J.G.; Wagholikar, K.B.; Estiri, H.; Hubaux, J.-P.; Murphy, S.N. Feasibility of Homomorphic Encryption for Sharing I2B2 Aggregate-Level Data in the Cloud. *AMIA Jt. Summits Transl. Sci. Proc.* **2018**, *2017*, 176–185.
33. Bocu, R.; Costache, C. A homomorphic encryption-based system for securely managing personal health metrics data. *IBM J. Res. Dev.* **2018**, *62*, 1:1–1:10. [CrossRef]
34. Jiang, Y.; Noguchi, T.; Kanno, N.; Yasumura, Y.; Suzuki, T.; Ishimaki, Y.; Yamana, H. A privacy-preserving query system using fully homomorphic encryption with real-world implementation for medicine-side effect search. In Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services, Munich, Germany, 2–4 December 2019; pp. 63–72.
35. Paddock, S.; Abedtash, H.; Zummo, J.; Thomas, S. Proof-of-concept study: Homomorphically encrypted data can support real-time learning in personalized cancer medicine. *BMC Med. Inform. Decis. Mak.* **2019**, *19*, 1–10. [CrossRef]
36. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2018**, *25*, 1398–1411. [CrossRef]
37. Heilman, E.; Kendler, A.; Zohar, A.; Goldberg, S. Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), Baltimore, MD, USA, 12–14 August 2015; pp. 129–144.
38. Hon, W.K.; Palfreyman, J.; Tegart, M. *Distributed Ledger Technology & Cybersecurity*; European Union Agency for Network and Information Securit (ENISA): Athens, Greece, 2016.
39. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
40. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.-Y. Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [CrossRef]
41. Singh, S.; Hosen, A.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
42. Garay, J.; Kiayias, A.; Leonardos, N. The bitcoin backbone protocol: Analysis and applications. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, 30 May–3 June 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 281–310.
43. Jafri, N.; Yusof, M.M. Managing Data Security Risk in Model Software As A Service (SAAS). *Asia-Pac. J. Inf. Technol. Multimed.* **2018**, *7*, 99–117. [CrossRef]
44. Ikeda, K. Security and privacy of blockchain and quantum computation. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 199–228.
45. Fedorov, A.K.; Kiktenko, E.O.; Lvovsky, A.I. Quantum computers put blockchain security at risk. *Nature* **2018**, *563*, 465–467. [CrossRef] [PubMed]
46. Fernandez-Carames, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
47. Kashyap, S.; Bhushan, B.; Kumar, A.; Nand, P. Quantum blockchain approach for security enhancement in cyberworld. In *Multimedia Technologies in the Internet of Things Environment*; Springer: Singapore, 2022; Volume 3, pp. 1–22.
48. Hussain, H.A.; Mansor, Z.; Shukur, Z. Comprehensive Survey and Research Directions on Blockchain Iot Access Control. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 2021. [CrossRef]
49. Bhushan, B.; Sinha, P.; Sagayam, K.; Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Comput. Electr. Eng.* **2021**, *90*, 106897. [CrossRef]
50. Gilboy, M.B.; Heinerichs, S.; Pazzaglia, G. Enhancing Student Engagement Using the Flipped Classroom. *J. Nutr. Educ. Behav.* **2014**, *47*, 109–114. [CrossRef] [PubMed]
51. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
52. Tromp, J. Cuckoo cycle: A memory bound graph-theoretic proof-of-work. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 49–62.
53. Miller, A.; Kosba, A.; Katz, J.; Shi, E. Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 680–691.
54. Eyal, I.; Gencer, A.; Sirer, E.; van Renesse, R. {Bitcoin-NG}: A scalable blockchain protocol. In Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), Santa Clara, CA, USA, 17–18 March 2016; pp. 45–59.
55. Wiki, N. Whitepaper: Nxt. 2018. Available online: https://nxtwiki.org (accessed on 27 November 2022).

56. Bentov, I.; Gabizon, A.; Mizrahi, A. Cryptocurrencies without proof of work. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 142–157.
57. Russell, A.; Zuckerman, D. Perfect information leader election in log* n+ O (1) rounds. *J. Comput. Syst. Sci.* **2001**, *63*, 612–626. [CrossRef]
58. Duong, T.; Fan, L.; Katz, J.; Thai, P.; Zhou, H.-S. 2-hop blockchain: Combining proof-of-work and proof-of-stake securely. In Proceedings of the European Symposium on Research in Computer Security, Guildford, UK, 14–18 September 2020; Springer: Cham, Switzerland, 2020; pp. 697–712.
59. Duong, T.; Chepurnoy, A.; Fan, L.; Zhou, H.-S. Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Incheon, Republic of Korea, 4 June 2018; pp. 1–13.
60. Wang, Z.; Jin, H.; Dai, W.; Choo, K.-K.R.; Zou, D. Ethereum smart contract security research: Survey and future research opportunities. *Front. Comput. Sci.* **2020**, *15*, 1–18. [CrossRef]
61. Kwon, Y.; Kim, D.; Son, Y.; Vasserman, E.; Kim, Y. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 195–209.
62. Eyal, I. The miner's dilemma. In *2015 IEEE Symposium on Security and Privacy*; IEEE: New York, NY, USA, 2015; pp. 89–103.
63. Velner, Y.; Teutsch, J.; Luu, L. Smart contracts make bitcoin mining pools vulnerable. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017; Springer: Cham, Switzerland, 2017; pp. 298–316.
64. Torres, C.F.; Steichen, M. The art of the scam: Demystifying honeypots in ethereum smart contracts. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 1591–1607.
65. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in blockchain system. *J. Netw. Comput. Appl.* **2018**, *126*, 45–58. [CrossRef]
66. Koshy, P.; Koshy, D.; McDaniel, P. An analysis of anonymity in bitcoin using p2p network traffic. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 469–485.
67. Liao, K.; Zhao, Z.; Doupé, A.; Ahn, G.-J. Behind closed doors: Measurement and analysis of CryptoLocker ransoms in Bitcoin. In Proceedings of the 2016 APWG Symposium on Electronic Crime Research (eCrime), Toronto, ON, Canada, 1–3 June 2016; IEEE: New York, NY, USA, 2016; pp. 1–13.
68. Spagnuolo, M.; Maggi, F.; Zanero, S. Bitiodine: Extracting intelligence from the bitcoin network. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 457–468.
69. Reid, F.; Harrigan, M. An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks*; Springer: New York, NY, USA, 2013; pp. 197–223.
70. Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.M.; Savage, S. A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Internet Measurement Conference, Barcelona, Spain, 23–25 October 2013; pp. 127–140.
71. Maxwell, G. CoinSwap: Transaction graph disjoint trustless trading. CoinSwap: Transactiongraphdisjointtrustlesstrading (October 2013). 2013. Available online: https://bitcointalk.org/index.php?topic=321228.msg3440187#msg3440187 (accessed on 27 November 2022).
72. Feiyue, W. Computational Experiments for Behavior Analysis and Decision Evaluation of Complex System. *J. Syst. Simul.* **2004**, *16*, 893–897.
73. Fei-Yue, W. Artificial societies, computational experiments, and parallel systems: A discussion on computational theory of complex social-economic systems. *Complex Syst. Complex. Sci.* **2004**, *1*, 25–35.
74. Utchel, D.M. The Parallel Security Apparatus: Examining the Cases of Baathist Iraq, Syria, and Iran. Ph.D. Dissertation, University of Nevada, Las Vegas, NV, USA, 2019.
75. Gong, X.; Liu, X.; Jing, S.; Xiong, G.; Zhou, J. Parallel-education-blockchain driven smart education: Challenges and issues. In Proceedings of the 2018 Chinese Automation Congress (CAC), Xi'an, China, 30 November–2 December 2018; IEEE: New York, NY, USA, 2018; pp. 2390–2395.
76. Guo, H.; Yu, X. A survey on blockchain technology and its security. *Blockchain Res. Appl.* **2022**, *3*, 100067. [CrossRef]
77. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; IEEE: New York, NY, USA, 2015; pp. 180–184.
78. Hassan, R.; Ahmed, A.; Osman, N.E. Enhancing security for IPv6 neighbor discovery protocol using cryptography. *Am. J. Appl. Sci.* **2014**, *11*, 1472–1479. [CrossRef]
79. Aruna, M.G.; Hasan, M.K.; Islam, S.; Mohan, K.G.; Sharan, P.; Hassan, R. Cloud to cloud data migration using self sovereign identity for 5G and beyond. *Clust. Comput.* **2021**, *25*, 2317–2331. [CrossRef]
80. Bhattacharya, S.; Singh, A.; Hossain, M. Strengthening public health surveillance through blockchain technology. *AIMS Public Health* **2019**, *6*, 326–333. [CrossRef]
81. MIslam, R.; Rahman, M.; Mahmud, M.; Rahman, M.; Mohamad, M.H.S. A Review on blockchain security issues and challenges. In Proceedings of the 2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, 7 August 2021; IEEE: New York, NY, USA, 2021; pp. 227–232.

82. Sullivan, C. Blockchain-based identity: The advantages and disadvantages. In *Blockchain and the Public Sector*; Springer: Cham, Switzerland, 2021; pp. 197–218.
83. Mavroeidis, V.; Vishi, K.; Zych, M.; Jøsang, A. The impact of quantum computing on present cryptography. *arXiv* **2018**, arXiv:1804.00200. [CrossRef]
84. Chen, L.; Jordan, S.; Liu, Y.K.; Moody, D.; Peralta, R.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016.
85. Jarecki, S.; Kiayias, A.; Krawczyk, H.; Xu, J. Highly-efficient and composable password-protected secret sharing (or: How to protect your bitcoin wallet online). In Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbruecken, Germany, 21–24 March 2016; IEEE: New York, NY, USA, 2016; pp. 276–291.
86. Fleder, M.; Kester, M.; Pillai, S. Bitcoin transaction graph analysis. *arXiv* **2015**, arXiv:1502.01657.
87. Decker, C.; Wattenhofer, R. Bitcoin transaction malleability and MtGox. In *European Symposium on Research in Computer Security*; Springer: Cham, Switzerland, 2014; pp. 313–326.
88. Karame, G.O.; Androulaki, E.; Roeschlin, M.; Gervais, A.; Čapkun, S. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2015**, *18*, 1–32. [CrossRef]
89. Rajput, U.; Abbas, F.; Oh, H. A solution towards eliminating transaction malleability in bitcoin. *J. Inf. Process. Syst.* **2018**, *14*, 837–850.
90. Washbourne, L. A survey of P2P Network security. *arXiv* **2015**, arXiv:1504.01358.
91. Li, J. A Survey of Peer-to-Peer Network Security Issues. *Retrieved Novemb.* **2007**, *29*, 2010.
92. Buterin, V. A Next-Generation Smart Contract and Decentralized Application Platform. 2018. Available online: https://github.com/ethereum/wiki/wiki/White-Paper (accessed on 5 October 2018).
93. Nayak, K.; Kumar, S.; Miller, A.; Shi, E. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbruecken, Germany, 21–24 March 2016; IEEE: New York, NY, USA, 2016; pp. 305–320.
94. Ahmed, M.M.; Hasan, M.K.; Shafiq, M.; Qays, O.; Gadekallu, T.R.; Nebhen, J.; Islam, S. A peer-to-peer blockchain based interconnected power system. *Energy Rep.* **2021**, *7*, 7890–7905. [CrossRef]
95. Prado-Romero, M.A.; Doerr, C.; Gago-Alonso, A. Discovering bitcoin mixing using anomaly detection. In *Iberoamerican Congress on Pattern Recognition*; Springer: Cham, Switzerland, 2017; pp. 534–541.
96. Bonneau, J.; Narayanan, A.; Miller, A.; Clark, J.; Kroll, J.; Felten, E.W. Mixcoin: Anonymity for bitcoin with accountable mixes. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 486–504.
97. Heilman, E.; Alshenibr, L.; Baldimtsi, F.; Scafuro, A.; Goldberg, S. Tumblebit: An untrusted bitcoin-compatible anonymous payment hub. In *Cryptology ePrint Archive*; International Association for Cryptologic Research: Lyon, France, 2016.
98. Maurer, F.K.; Neudecker, T.; Florian, M. Anonymous CoinJoin transactions with arbitrary values. In Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS, Sydney, NSW, Australia, 1–4 August 2017; IEEE: New York, NY, USA, 2017; pp. 522–529.
99. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; Springer: New York, NY, USA, 2017; pp. 357–388.
100. Chatzigiannakis, I.; Spirakis, P. The Dynamics and stability of probabilistic population processes. In *International Symposium on Stabilization, Safety, and Security of Distributed Systems*; Springer: Cham, Switzerland, 2017; pp. 33–45.
101. Milutinovic, M.; He, W.; Wu, H.; Kanwal, M. Proof of luck: An efficient blockchain consensus protocol. In Proceedings of the 1st Workshop on System Software for Trusted Execution—Middleware'16: 17th International Middleware Conference, Trento, Italy, 12–16 December 2016; pp. 1–6.
102. Shuai, Z.; Yong, Y.; Xiao-Chun, N.; Fei-Yue, W. Scaling blockchain towards bitcoin: Key technologies, constraints and related issues. *Acta Autom. Sin.* **2019**, *45*, 1015–1030.
103. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 17–30.
104. Han, X.; Yuan, Y.; Wang, F.-Y. A blockchain-based framework for central bank digital currency. In Proceedings of the 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Zhengzhou, China, 6–8 November 2016; IEEE: New York, NY, USA, 2019; pp. 263–268.
105. Schär, F. Blockchain forks: A formal classification framework and persistency analysis. *Singap. Econ. Rev.* **2020**, *101712*, 1–11. [CrossRef]
106. Yiu, C. An Overview of Forks and Coordination in Blockchain Development. *arXiv* **2021**, arXiv:2102.10006.
107. Kazmi, S.H.A.; Qamar, F.; Hassan, R.; Nisar, K.; Chowdhry, B.S. Survey on Joint Paradigm of 5G and SDN Emerging Mobile Technologies: Architecture, Security, Challenges and Research Directions. *Wirel. Pers. Commun.* **2023**, 1. [CrossRef]
108. Sapirshtein, A.; Sompolinsky, Y.; Zohar, A. Optimal selfish mining strategies in bitcoin. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 515–532.

109. Carlsten, M.; Kalodner, H.; Weinberg, S.; Narayanan, A. On the instability of bitcoin without the block reward. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 154–167.
110. Lamport, L. The part-time parliament. In *Concurrency: The Works of Leslie Lamport*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 277–317.
111. Ellul, J.; Galea, J.; Ganado, M.; Mccarthy, S.; Pace, G.J. Regulating blockchain, DLT and smart contracts: A technology regulator's perspective. In *ERA Forum*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 21, pp. 209–220.
112. Jiang, B.; Liu, Y.; Chan, W. Contractfuzzer: Fuzzing smart contracts for vulnerability detection. In Proceedings of the 2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE), Montpellier, France, 3–7 September 2018; IEEE: New York, NY, USA, 2018; pp. 259–269.
113. Badruddoja, S.; Dantu, R.; He, Y.; Upadhayay, K.; Thompson, M. Making smart contracts smarter. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, NSW, Australia, 3–6 May 2021; IEEE: New York, NY, USA, 2021; pp. 1–3.
114. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on ethereum smart contracts (sok). In Proceedings of the International Conference on Principles of Security and Trust, Uppsala, Sweden, 24–25 April 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 164–186.
115. Ladleif, J.; Weber, I.; Weske, M. External data monitoring using oracles in blockchain-based process execution. In Proceedings of the International Conference on Business Process Management, Rome, Italy, 6–10 September 2020; Springer: Cham, Switzerland, 2020; pp. 67–81.
116. Zhang, F.; Cecchetti, E.; Croman, K.; Juels, A.; Shi, E. Town crier: An authenticated data feed for smart contracts. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 270–282.
117. Peterson, J.; Krug, J.; Zoltu, M.; Williams, A.; Alexander, S. Augur: A decentralized oracle and prediction market platform. *arXiv* **2015**, arXiv:1501.01042.
118. Yong, Z.T.Y.; Ao-Ying, Z.; Chao, D.Y.; Fei-Yue, W. Blockchain technology: From data intelligence to knowledge automation. *Acta Autom. Sin.* **2017**, *43*, 1485–1490.
119. Yuan, Y.; Wang, F.-Y. Parallel blockchain: Concept, methods and issues. *Acta Autom. Sin.* **2017**, *43*, 1703–1712.
120. Vukolić, M. Rethinking permissioned blockchains. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, United Arab Emirates, 2–6 April 2017. [CrossRef]
121. Collberg, C.; Davidson, J.; Giacobazzi, R.; Gu, Y.X.; Herzberg, A.; Wang, F.-Y. Toward Digital Asset Protection. *IEEE Intell. Syst.* **2011**, *26*, 8–13. [CrossRef]
122. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* **2022**, *34*, 11475–11490. [CrossRef]
123. Odeh, A.; Keshta, I.; Abu Al-Haija, Q. Analysis of Blockchain in the Healthcare Sector: Application and Issues. *Symmetry* **2022**, *14*, 1760. [CrossRef]
124. Tandon, A.; Dhir, A.; Islam, A.; Mäntymäki, M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput. Ind.* **2020**, *122*, 103290. [CrossRef]
125. Sarkar, A.; Maitra, T.; Maitra, T.; Neogy, S. Blockchain in healthcare system: Security issues, attacks and challenges. In *Blockchain Technology: Applications and Challenges*; Springer: Cham, Switzerland, 2021; pp. 113–133.
126. Chelladurai, U.; Pandian, S. A novel blockchain based electronic health record automation system for healthcare. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *13*, 693–703. [CrossRef]
127. Fatima, N.; Agarwal, P.; Sohail, S.S. Security and privacy issues of blockchain technology in health care—A review. In *ICT Analysis Applications*; Springer: Singapore, 2022; pp. 193–201.
128. Hasan, H.R.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Omar, M.; Ellahham, S. Blockchain-Enabled Telehealth Ser-vices Using Smart Contracts. *IEEE Access* **2021**, *9*, 151944–151959. [CrossRef]
129. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. *Int. J. Healthc. Manag.* **2022**, *15*, 70–83. [CrossRef]
130. Saravanan, M.; Shubha, R.; Marks, A.; Iyer, V. SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; IEEE: New York, NY, USA, 2017; pp. 1–6.
131. Meri, A.; Hasan, M.; Safie, N. Success factors affecting the healthcare professionals to utilize cloud computing services. *Asia-Pac. J. Inf. Technol. Multimed.* **2017**, *6*, 31–42.
132. 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.* **2018**, *42*, 130. [CrossRef]
133. Abdali, T.-A.N.; Hassan, R.; Aman, A.M.; Nguyen, Q.N. Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues. *IEEE Access* **2021**, *9*, 75961–75980. [CrossRef]
134. Khalil, A.M.U.; Lai, D.T.C.; King, O.S. Cluster analysis for identifying obesity subgroups in health and nutitional status survey data. *Asia-Pac. J. Inf. Technol. Multimed. (APJITM)* **2021**, *10*, 146–169.
135. Badr, S.; Gomaa, I.; Abd-Elrahman, E. Multi-tier blockchain framework for IoT-EHRs systems. *Procedia Comput. Sci.* **2018**, *141*, 159–166. [CrossRef]

136. Zhang, X.; Poslad, S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; IEEE: New York, NY, USA, 2018; pp. 1–6.
137. Wang, H.; Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *J. Med. Syst.* **2018**, *42*, 152. [CrossRef] [PubMed]
138. 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* **2018**, *6*, 11676–11686. [CrossRef]
139. Brogan, J.; Baskaran, I.; Ramachandran, N. Authenticating health activity data using distributed ledger technologies. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 257–266. [CrossRef] [PubMed]
140. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.S.; de Albuquerque, V.H.C. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. *Cogn. Syst. Res.* **2018**, *52*, 1–11. [CrossRef]
141. 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.* **2016**, *40*, 218. [CrossRef]
142. Simić, M.; Sladić, G.; Milosavljević, B. A case study IoT and blockchain powered healthcare. In Proceedings of the 8th PSU-UNS International Conference on Engineering and Technology (ICET-2017), Novi Sad, Serbia, 8–10 June 2017; University of Novi Sad Press: Novi Sad, Serbia, 2017; pp. 1–4.
143. Ghazal, T.M.; Hasan, M.K.; Alshurideh, M.T.; Alzoubi, H.M.; Ahmad, M.; Akbar, S.S.; Al Kurdi, B.; Akour, I.A. IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare—A Review. *Future Internet* **2021**, *13*, 218. [CrossRef]
144. Genestier, P.; Zouarhi, S.; Limeux, P.; Excoffier, D.; Prola, A.; Sandon, S.; Temerson, J.-M. Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges. *J. Int. Soc. Telemed. Ehealth* **2017**, *5*, GKR-e24.
145. Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* **2020**, *9*, 94. [CrossRef]
146. Pham, H.L.; Tran, T.; Nakashima, Y. A secure remote healthcare system for hospital using blockchain smart contract. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; IEEE: New York, NY, USA, 2018; pp. 1–6.
147. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* **2019**, *7*, 56. [CrossRef]
148. Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access* **2021**, *9*, 37397–37409. [CrossRef]
149. 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* **2022**, *22*, 7716. [CrossRef]
150. Vyas, S.; Shabaz, M.; Pandit, P.; Parvathy, L.R.; Ofori, I. Integration of Artificial Intelligence and Blockchain Technology in Healthcare and Agriculture. *J. Food Qual.* **2022**, *2022*, 4228448. [CrossRef]
151. Li, D.; Deng, L.; Cai, Z.; Souri, A. Blockchain as a service models in the Internet of Things management: Systematic review. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4139. [CrossRef]
152. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R.; Jolfaei, A.; Islam, A.N. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *J. Parallel Distrib. Comput.* **2023**, *172*, 69–83. [CrossRef]
153. Abu-Elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-Alrazaq, A. The benefits and threats of blockchain technology in healthcare: A scoping review. *Int. J. Med. Inform.* **2020**, *142*, 104246. [CrossRef]
154. Zheng, X.; Zhu, Y.; Si, X. A survey on challenges and progresses in blockchain technologies: A performance and security perspective. *Appl. Sci.* **2019**, *9*, 4731. [CrossRef]
155. Ratta, P.; Kaur, A.; Sharma, S.; Shabaz, M.; Dhiman, G. Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *J. Food Qual.* **2021**, *2021*, 7608296. [CrossRef]
156. Naresh, V.S.; Pericherla, S.S.; Murty, P.S.R.; Sivaranjani, R. Internet of Things in Healthcare: Architecture, Applications, Challenges, and Solutions. *Comput. Syst. Sci. Eng.* **2020**, *35*, 411–421. [CrossRef]
157. Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security aspects of blockchain technology intended for industrial applications. *Electronics* **2021**, *10*, 951. [CrossRef]
158. Kamruzzaman, M.M.; Yan, B.; Sarker MN, I.; Alruwaili, O.; Wu, M.; Alrashdi, I. Blockchain and Fog Computing in IoT-Driven Healthcare Services for Smart Cities. *J. Healthc. Eng.* **2022**, *2022*, 9957888. [CrossRef] [PubMed]
159. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [CrossRef]
160. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and smart healthcare security: A survey. *Procedia Comput. Sci.* **2020**, *175*, 615–620. [CrossRef]
161. Lin, S.Y.; Zhang, L.; Li, J.; Ji, L.L.; Sun, Y. A survey of application research based on blockchain smart contract. *Wirel. Netw.* **2022**, *28*, 635–690. [CrossRef]
162. Liu, J.; Zhao, J.; Huang, H.; Xu, G. A novel logistics data privacy protection method based on blockchain. *Multimed. Tools Appl.* **2022**, *81*, 23867–23887. [CrossRef]
163. Ramzan, S.; Aqdus, A.; Ravi, V.; Koundal, D.; Amin, R.; Al Ghamdi, M.A. Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Trans. Eng. Manag.* **2022**, *1*, 1–17. [CrossRef]

164. UmaMaheswaran, S.K.; Prasad, G.; Omarov, B.; Abdul-Zahra, D.S.; Vashistha, P.; Pant, B.; Kaliyaperumal, K. Major Challenges and Future Approaches in the Employment of Blockchain and Machine Learning Techniques in the Health and Medicine. *Secur. Commun. Netw.* **2022**, *2022*, 5944919. [CrossRef]
165. Mecozzi, R.; Perrone, G.; Anelli, D.; Saitto, N.; Paggi, E.; Mancini, D. Blockchain-related identity and access management challenges: (de) centralized digital identities regulation. In Proceedings of the 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 22–25 August 2022; IEEE: New York, NY, USA, 2022; pp. 443–448.
166. Khalil, A.I.; Rahman, M.S. Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis. *Appl. Sci.* **2022**, *12*, 11039.