Internet of Things 25 (2024) 101111

Contents lists available at ScienceDirect

Internet of Things

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

Review article

A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare

Sanjay Kumar Jena [*], Ram Chandra Barik, Rojalina Priyadarshini

Department of Computer Science & Engineering, C.V. Raman Global University, Janla Odisha, 752054, India

ARTICLE INFO

Keywords:
Blockchain
Digital identity
Internet of Things
Internet of Medical Things
Healthcare

ABSTRACT

Digital Identity is a prominent practice across every digital platform for maintaining confidentiality and privacy. The demand for Internet of Things (IoT) and its allied technologies such as Internet of Medical Things (IoMT), the Industrial Internet of Things (IIoT), and the Internet of Video Things (IoVT) is constantly on the rise in both wired and wireless domains. IoT communications emerge as a major challenge for digital identity-based security solutions in the areas of healthcare, transportation, and their allied applications. This paper addresses the different aspects of digital identity for security preservation and maintenance in IoT and blockchain based solutions. It focuses on Confidentiality, Integrity, and Availability (CIA) issues and corresponding digital identity solutions using the duo. The writers perused over 112 publications and shared their findings on cutting-edge technologies related to Digital Identity (DId) in the healthcare industry.

1. Introduction

Any living thing's wealth is their state of health, but for humans, who strive to keep it in any condition, it is especially valuable. God gave life as a gift, and humans have made great strides in science to preserve it. Everybody visits a hospital for treatment of their health, whether they are humans or other animals. Payer demands, stricter regulations, fiercer rivalry, and a worldwide pandemic have all taken a toll on the healthcare business in recent years. This review article discusses the potential of blockchain technology and its implementation in the healthcare sector, including various obstacles encountered [1]. To achieve this, the authors had selected 112 distinct papers to make up the study report on IoT and blockchain with digital identity as a means to acquire healthcare remedies. This three-party involvement is termed as IoTBDId throughout this paper along with the title. There has to be a shift toward a more nuanced approach to digital identity management that takes into account the unique difficulties inherent to the healthcare industry. A genuinely effective identity access management system should streamline and make it easier for Information Technology (IT) personnel to manage the entity, devices, and applications in their healthcare delivery companies while also enhancing security and compliance without creating time-consuming inefficiencies. Otherwise, we can say that the healthcare sector is experiencing a "digital identity crisis".

1.1. Digital identity and its challenges in healthcare

The term "digital identity" refers to the adoption or assertion of an identity in cyberspace by an individual, organization, or electronic device. The digitization of personal data enables its accessibility on the internet, regardless of time or location. Examples

[*] Corresponding author.
E-mail addresses: sanjayjena51@gmail.com (S.K. Jena), ram.chandra@cgu-odisha.ac.in (R.C. Barik), rojalinapriyadarshini@cgu-odisha.ac.in (R. Priyadarshini).

https://doi.org/10.1016/j.iot.2024.101111
Received 18 February 2023; Received in revised form 19 January 2024; Accepted 4 February 2024
Available online 7 February 2024

Table 1
Digital identity and its challenges.

Sl. No.	Challenges faced	References
1	Provided digital identity is not enough to identify the patient during accidental case	[3]
2	Rigorous rules and requirements	
3	Impediments to progress caused by outdated technology	
4	Involvement of contractual and temporary personnel	
5	Manual methods involve seeking for a doctor, bed or appointment	
6	The absence of integrated identity management	[4]

of digital content that individuals commonly share or store online include photographs uploaded to social media platforms, as well as various documents such as certificates, resumes, and other files that are stored in cloud-based storage systems. Additionally, individuals may also access and manage their online banking accounts, which contain sensitive financial information. So, it could not be a blank idea discussion for involving IoTBDId for healthcare; rather, there is the involvement of great experiments that prove the potential of these technologies for demanding applications. They definitely deserve its involvement. The challenges of DId in healthcare are shown in Table 1. Several obstacles appeared, were conquered, and were ready to be defended, but the process still continues. The difficulties encountered by the rescue sectors are outlined in article [2]. According to the article, the most significant issues that the sector is now facing center on the scalability of technology and data access restrictions.

1.2. Scope and contribution

The study's primary objectives, findings, and ramifications would provide readers with a thorough and systematic analysis of referenced articles. The major focus will be on the difficulties, gaps, and forthcoming needs of this sector.

The contributions to the article are as follows:

- It explains the types of IoT environments and infrastructure in a nutshell.
- It explains the blockchain, its types, and its architecture in a nutshell.
- It has also given a systematic study report on digital identity and its various applications, with a focus on healthcare industry.
- It has given the imperative analysis review report by conjugating IoT and blockchain for digital identity solutions in the healthcare industry in state-of-the-art works.

1.3. Organization of paper

The paper is well organized into seven parts, starting with the introduction in the first and the systematic study and analysis report on IoT and blockchain in the second. The third part delivers information about several application areas of digital identity. The fourth part gives a crucial analysis report on the security of IoT, blockchain and digital identity in healthcare. The fifth part concludes the review article with a short and detailed summary report. The sixth and seventh parts were used as references and appendices to the paper.

2. System under study: IoT and blockchain

2.1. IoT in a Nutshell

The IoT is a cutting-edge analytic and automation system that makes use of networking, sensing, big data, and artificial intelligence technology to supply entire systems for a product or service. The goal of this article is to offer a elaborated overview of IoT and potential in its applications in healthcare sector. It undertakes the assessment of fifty publications and provides an output that teaches the fundamental ideas of the IoT required for using IoT in healthcare systems. The IoT generally makes use of established networking protocols and technology. Radio Frequency Identification (RFID), Near Field Communication (NFC), Low Energy Bluetooth, Low Energy Wireless, Low Energy Radio Protocols, Long Term Evolution Advanced (LTE-A), and Wireless Fidelity (Wi-Fi-Direct) are the primary technologies and protocols that make the IoT possible. [5]. While the benefits of the IoT extend to every aspect of daily life and commercial operations, this article will narrow its attention to healthcare. The hardware that is used in IoT systems consists of sensors, devices for a remote dashboard, devices for control, servers, and a device that acts as a router or bridge. These devices are in charge of managing important duties and functions such as system activation, action specifications, security, communication, and detection in order to support certain objectives and activities.

The IoT has applications in every industry and market, as we can observe in Fig. 1. It serves a wide range of user groups, from individuals who want to cut down on their energy usage at home to huge enterprises that want to simplify their business processes. However, the application of this research to medical purposes will be the primary emphasis of this study. The smart bed, smart

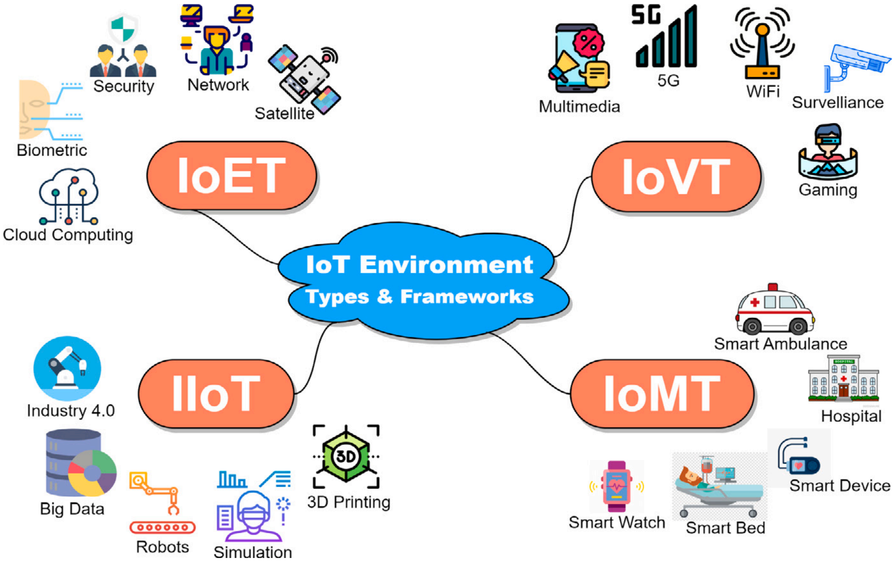


Fig. 1. IoT environment types and frameworks.

chair, smart watch, and smart ambulance vehicle are some of the technologies that are available. These sensors will gather data in real time from several units, and ultimately, they will use IPFS and the blockchain's hash file to transmit all of a patient's data in an encrypted format to the doctor who is been assigned to care for them. In contrast to traditional file sharing systems, which are typically based on a client–server model, wherein files are stored on centralized servers and accessed by clients via protocols like File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), or Server Message Block (SMB), IPFS is a decentralized peer-to-peer and distributed file sharing system. In this part of the article, we will be using IoT devices, which we shall refer to as IoMT devices.

2.1.1. IoT environment types and frameworks

IoVT: IoVT which is short for Internet of Video Things and also Internet of Vulnerable Things [6] is a subset of IoT. IoT has restricted capabilities in its IoVT context [7]. Applications that demand real-time, high-definition video feeds include urban surveillance and healthcare monitoring. Thankfully, 5G wireless networks can provide the infrastructure needed to manage access to a large number of IoVT devices. To further boost system performance, it also facilitates a device-to-device communication mechanism tailored to mobile devices that may experiment with spectrum spatial reuse. Which will motivate authors to design and implement fully or partially decentralized autonomous direct communications among large numbers of IoVT devices [8]. According to the article [9], the current stage is characterized by a dramatic increase in the deployment of large-scale visual sensors, powerful and energy-efficient embedded processing, a meteoric rise in connectivity enabled by 5G technology, swift advances in cloud and edge computing, and the miniaturization of IoVT components. While these advancements are certainly exciting, the Internet of Vulnerable Things has also been the subject of some media coverage. The paper by Mikko Hypponen and Linus Nyman [10] argues that intelligence may also be a weakness. One major factor is the ensuing dearth of expertise in security engineering among these up-and-coming software firms; this is an issue that blockchain can unquestionably address. As can be seen in the next bullet points, IIoT also presents IIoVT, which has a wide range of potential applications in areas like "smart industries" and "intelligent transportation". Thus, it is clear that IoVT is a hybrid setting.

IoET: IoET which is short for Internet of Everything, is a subset of IoT. The IoET is sometimes referred to as the IoE. As time goes by, the Internet's utility and scope only seem to grow. The IoT and IoET are innovative methods of integrating the internet into everyday life. People, Data, Processes, and Physical objects together make up the four cornerstones of IoET. While everything in the IoT consists of stuff. It also increases the life-improving effects of commercial and industrial activities [11]. By introducing connections between the four cornerstones of the IoT, IoET broadens the paradigm. Thus, it includes more connection-based paradigms like Internet of People (IoP), and the Industrial Internet (II) [12].

IIoT: IIoT, which is short for Industrial Internet of Things, is a subset of IoT. As an umbrella term for IoT use in manufacturing, "the IIoT" has recently come into prominence. Practically, it can be said that it is a broader application of Industry 4.0, which looks to place greater emphasis on improving the effectiveness of industrial processes [13]. Cloud-Based manufacturing is a more current on-demand concept that makes use of IoT technology. It makes it possible to have universal, practical, on-demand network access to a shared pool of re-configurable manufacturing resources that can be quickly deployed and released with little administration work or service provider involvement. Therefore, recommending a decentralized, peer-to-peer blockchain-based IIoT platform will serve as a crucial enabler for cloud-based technologies [14]. The emerging idea of Industrial IoT is the push for smart factories in the

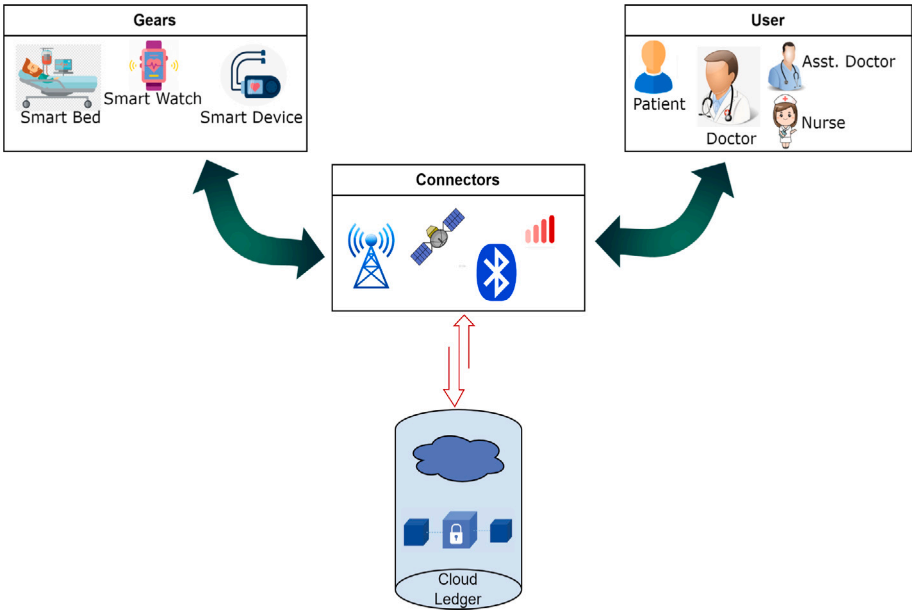


Fig. 2. IoMT framework architecture.

industrial environment. And the most common energy sector is given high priority in the development of IIoT, not only due to the rising demand for energy from consumers, particularly in light of population growth, but also due to the fact that energy management is a crucial component of the industrial sector and the desired low-cost production of goods and services. Other important sectors of critical infrastructure can include water management and transportation [15–18].

IoMT: IoMT stands for Internet of Medical Things and is a subset of IoT. As shown in Fig. 2, the core elements of an IoMT system are the User, Connector, Gears, and Cloud Ledger. The Gears are an interconnected system of sensors and other medical equipment that may act alone or in concert to record the patient's vital statistics. These vital statistics may include vital signs, body temperature, oxygen levels, and electrical activity (ECG, EEG, and muscle activity). The Cloud Ledger may receive this data continuously from the Gear via a network. Processing and cloud storage of the collected data are the responsibilities of the Cloud Ledger. Here the user engages in persistent monitoring of the data that may be accessed and viewed through a mobile device (a smartphone, computer, tablet, etc.) [19,20]. The identification of illnesses and abnormalities in the human body could only be done after a physical examination, for which the majority of the patients had to remain in the hospital for the duration of their therapy. But, this also raises the expense of hospitals while placing pressure on rural and distant healthcare facilities. So, technological advancements over the years have made it feasible to monitor one's health and even diagnose a variety of illnesses via the use of wearable gadgets like smartwatches. Furthermore, technological advancements have shifted the emphasis of the healthcare system from hospitals to individuals receiving treatment. These gears are used as real-time monitoring systems that provide physicians access to real-time data so they may constantly monitor and manage their patients' health [21].

Certainly, we have summarized different IoT extensions, environment types, and frameworks categorizing in according to a consumer, industrial, or manageability focus through many seek broader relevance in Table 2.

2.1.2. IoMT infrastructure, data acquisition, protocols

Robust IoMT infrastructure guarantees that patient data is confidential and securely sent to medical professionals, which may enhance patient care while lowering costs. Medical professionals and experts may now communicate freshly and engagingly. They can use the efficacy of electronic tools to detect life-threatening circumstances, monitor the patient's well-being, and assess the productivity of medical services in line with patient expectations. IoMT has the potential to cause a seismic shift in the global healthcare business in various ways [28]. These can include IoMT at Home, IoMT on body-wearable, IoMT during the transition, and IoMT in the hospital. Integrating the benefits of IoT technology and cloud computing into the medical industry is the goal of IoMT. Additionally, it outlines the protocols for sending data to a blockchain-based healthcare network from a variety of sensors and medical devices that a patient may wear. With the use of various communication protocols like Bluetooth, Zigbee, IEEE 802.11 (Wi-Fi), and others, IoT devices (sensors, actuators, and so on) have been combined with the same physical devices to monitor and share data. In healthcare applications, sensors that are implanted in or worn on the body of the patient are used to gather physiological data from their body, including temperature, pressure rate, electrocardiogram (ECG), electroencephalogram (EEG), and other measurements [29]. Digital identity security is the most pervasive issue now affecting IoMT solutions. According to a warning from the Federal Bureau of Investigation (FBI), modern IoMT devices are very susceptible to weak authentication being

Table 2
IoT environment types and frameworks.

IoT extensions	IoT environments	Frameworks	Ref.
IoE IoNT IoMT IIoT IoVT	Smart Home	Google Nest, Apple Home Kit, Amazon Alexa	[22–27]
	Healthcare	Google Cloud Health API, Android wear, Healthcare Cloud	
	Wearables	Raspberry Pi, Tizen, Audrino, Android wear, Samsung Gear SDK	
	Industry 4.0	OPC UA, Eclipse IoT, Bosch IoT Suite, Siemens MindSphere, PTC ThingWorx, AWS IoT, Microsoft Azure	
	Cloud Computing	AWS IoT, Azure IoT Suite, Google Cloud IoT Core, Oracle IoT	
	Agriculture	Open IoT, FarmBeats, AgSense, Microsoft Azure, SensorUp, IBM Watson	
	Smart Cities	IBM Watson, Honeywell, ThingWorx	
	Vehicles	AUTOSAR, GENIVI Alliance, Android Automotive OS, Apple CarPlay, OpenXC, BlackBerry QNX	
	Multimedia	Node-RED, Microsoft Azure, WebRTC, Kurento, AWS IoT	
	Security	Azure Sphere, IBM Watson, Mbed, RIOT OS, OWASP, Google Cloud IoT Core, Cisco IoT, GE Security	

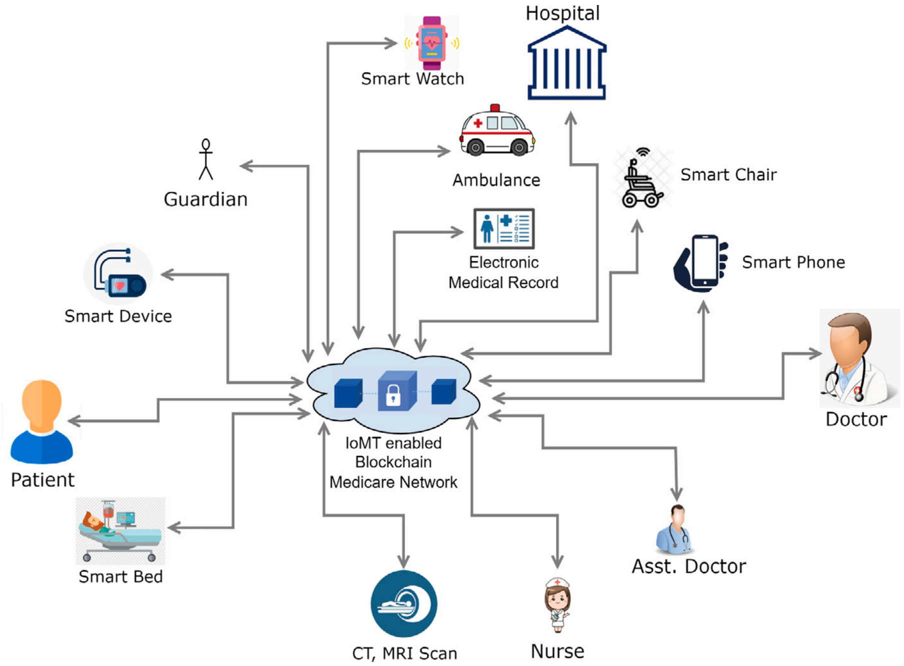


Fig. 3. IoMT infrastructure.

used against them to identify patients. Cybersecurity and anonymity, the pace and scope of usage, product sustainability, and of course costs are a few real challenges that need to be addressed. However, in recent years, it has emerged as a leader in tackling challenges [30].

The infrastructure of an IoMT refers to how the various parts of an IoT healthcare system network are organized and linked together securely, as depicted in Fig. 3.

IoMT on body: Contrarily, on-body wearable medical gadgets linked to remote monitoring or tracking systems constitute "IoMT on body". These gadgets may be utilized away from the house without disrupting regular activities, as shown in Fig. 4. It is to be noted that certain publications may refer to this kind of IoMT on the body or wearable as IoWT [31].

IoMT in home: IoMT at home makes remote monitoring and evaluation of patient data possible. Monitoring life-threatening situations like heart attacks and falls and immediately calling for aid is a great benefit. By identifying problems early on,

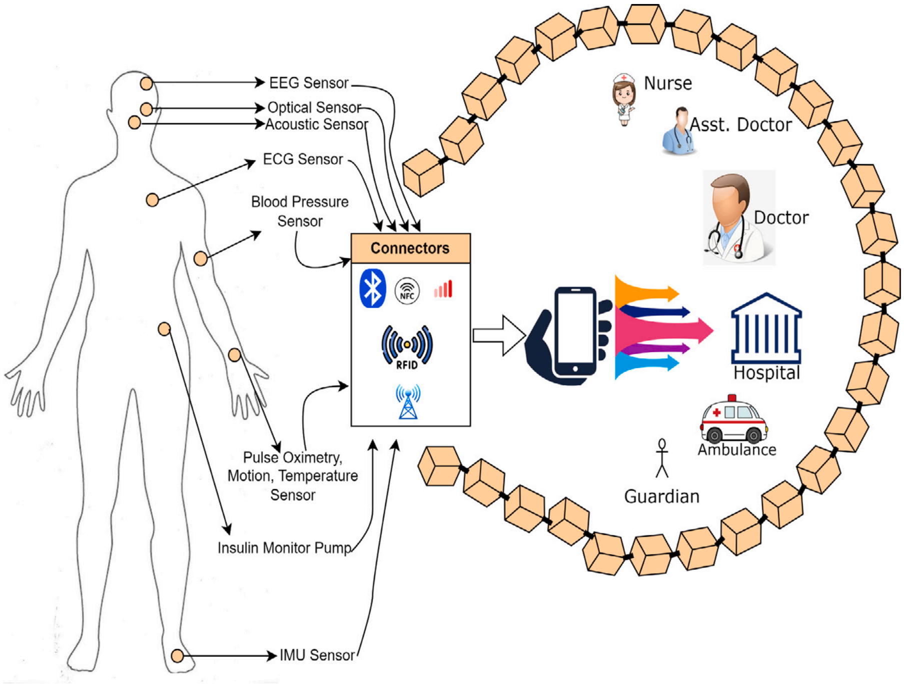


Fig. 4. Communication in blockchain-based IoMT wearable devices.

may decrease hospital readmissions. For continued treatment away from the patient environment, IoMT devices combined with telemedicine may be helpful [32].

IoMT in transport: It is Exactly what it sounds like when people in a certain region utilize IoMT gadgets. Mobility sensors, for instance, are used to monitor patients even while they are being transported in a car. The same emergency response intelligence systems are used by paramedics to monitor patient data outside of the hospital setting [33].

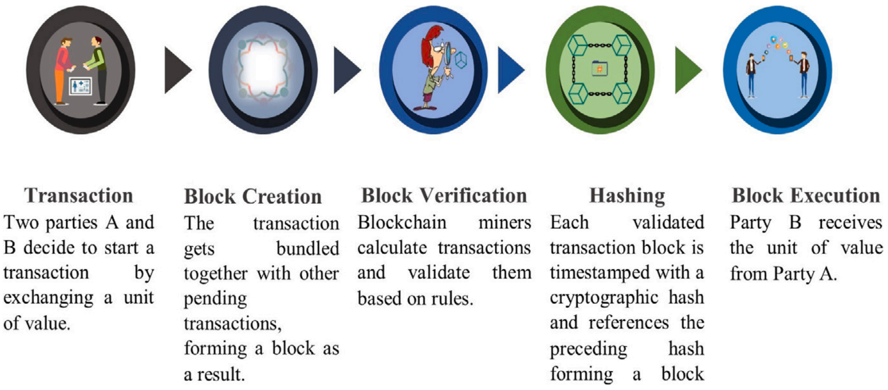
IoMT in hospital: Last but not least, it is essential that hospitals use IoMT to effectively oversee the long-term maintenance of their medical equipment. They must also keep an eye on the patients and medical professionals as they move around the building. As a result, hospitals use sensors and other monitoring technologies to get a bird's-eye view of all these interactions [34].

2.2. Blockchain in a Nutshell

Blockchain is a decentralized, distributed, and public ledger that is used to record transactions across many computers. The most important feature of the blockchain is that Once some data has been recorded in a block, it becomes impossible to change, hack, or tamper with the chain of blocks. This paper assesses thirty publications and provides an output on the usability of decentralized technology in the healthcare sector. With the rise in demand for data, the use of the internet in the current time is very intense, as is the need for security in the wide network chain. Blockchain, a newbie technology with a lot of potentials, is being implemented in many different areas [35]. The application area extends itself from a digital currency to IoT and much more. We have deepened our research area in the digital identity application of blockchain, As identity is the most affected part of the internet. Several comparisons and discussions have been made between the decentralized ledger used by blockchain and the centralized server that is being used today [36,37]. However, blockchain overcomes the challenges of prevalent technologies. For better treatment, the computer-aided diagnosis (CAD) report of the corresponding patients needs to be communicated between hospitals. However, communication of the crucial diagnosis data in wireless platforms opens multiple ways for cyberattacks. Hence, the emergence of a blockchain-driven decentralized model is the essence of the current healthcare domain to restrict cyberattacks. Because the inherent blockchain architecture uses an irreversible hash function to generate unique hash values via SHA-256, SHA-512, MD5, etc. So, to develop a high-end smart hospital the recent blockchain technology must be a safeguard towards their healthcare records. Also, the working steps of blockchain have been displayed in Fig. 5 [38].

2.2.1. Blockchain types

Public blockchain: A public blockchain is known as a permission-less blockchain, anyone and everyone has permission to see the transaction and verify it, as well as participate in the process of reaching a consensus. Since the public blockchain may reach agreements without the need for a single controlling authority, it is seen as decentralized. Every user is responsible for maintaining



Transaction
Two parties A and B decide to start a transaction by exchanging a unit of value.

Block Creation
The transaction gets bundled together with other pending transactions, forming a block as a result.

Block Verification
Blockchain miners calculate transactions and validate them based on rules.

Hashing
Each validated transaction block is timestamped with a cryptographic hash and references the preceding hash forming a block

Block Execution
Party B receives the unit of value from Party A.

Fig. 5. Working steps of blockchain.

Table 3
Different types of blockchain with advantages, disadvantages & applications.

Type of blockchain	Contextual definition	Advantages	Disadvantages	Applications	Ref.
Public Blockchain	It is permissionless and can be accessible by anybody who wishes to join.	Independent Transparent	Security Privacy Anonymity	Cryptocurrency Travel Finance Education	[39,40]
Private Blockchain	It is permissioned and only functions inside an exclusive group of users.	Performance Scalable High speed	Owned by one Costly	healthcare Real estate Cryptocurrency Finance	[41,42]
Hybrid Blockchain	It is a combination of both public and private blockchain.	Independent Performance Scalable High Speed	Owned by one Costly	healthcare Real estate Cryptocurrency	[43,44]
Consortium Blockchain	It is a permissioned blockchain that is administered by a group of companies.	Permissioned Federated High Security	Costly Transparency	Finance Government Supply chain	[45,46]

their copy of the ledger on their local node. The biggest drawback of using a protected public blockchain is that users do not have total privacy and anonymity over their transactions. Anyone can access public blockchains and observe transaction amounts as well as the addresses involved. If the proprietors of the addresses are discovered, the user's anonymity will be compromised [39,40].

Private blockchain: As the name implies, private blockchains are not open to the public. These are only available to people or organizations that are part of a larger group and have collectively agreed to share the ledger among themselves. The only person who has the authority to make modifications to the blockchain is the one who owns it. The fact that private blockchains are exclusively intended for use inside corporate settings is their primary limitation because of the limited scope of their potential uses. They are designed and constructed to pursue certain duties and responsibilities. They are prone to data breaches as well as other types of security concerns [41,42].

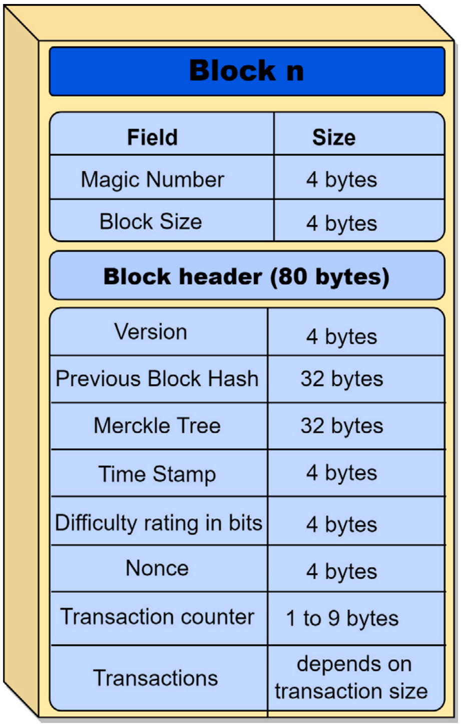
Hybrid blockchain: It is often referred to as a hybrid of public and private blockchains. It incorporates crucial aspects of public as well as private chains in one single system, and by combining the most advantageous features of public and private blockchain protocols, it ensures that all transactions and data remain confidential. When a person gets access to the hybrid blockchain platform, they can participate in all of the platform's activities. He can carry out transactions, inspect transactions, and even add or alter transactions in the same way as it is possible for you to do so. Users, on the other hand, may have peace of mind in the knowledge that their identities will never be disclosed to the general public and will always be protected [43,44].

Consortium blockchain: This blockchain is a permissioned blockchain that is managed by a group of businesses. It is privately held, although not by a single person or organization. For which it is named the federated blockchain. The consortium blockchain, which operates in a manner very similar to that of the hybrid blockchain, combines the most advantageous aspects of public and private blockchains [45,46]. Comparing it to a hybrid one, it is more adaptable and safe. Additionally, it strengthens security and reduces network load.

As a result, we can summarize the various kinds of Blockchains together with their respective benefits and drawbacks in Table 3.

2.2.2. Blockchain architecture security

The most important feature of blockchain is that data remains in an encrypted form, which is resistant to all attacks. In a chain of blocks, the first block is called the genesis block. And three things are to be found inside a block that protect it from attacks: data, a hash of the current block, and a hash of the previous block [47]. There is a block header, a transaction counter, and a transaction in every block. In recording the information, it serves as a distributed system. Fig. 6 provides a concise summary of the blockchain's



Block n

Field	Size
Magic Number	4 bytes
Block Size	4 bytes

Block header (80 bytes)

Version	4 bytes
Previous Block Hash	32 bytes
Merckle Tree	32 bytes
Time Stamp	4 bytes
Difficulty rating in bits	4 bytes
Nonce	4 bytes
Transaction counter	1 to 9 bytes
Transactions	depends on transaction size

Fig. 6. Structure of blockchain.

structure. The next sections provide a more in-depth look at the many building blocks that make up the security of a blockchain network: block hashing, block mining, block algorithms, and block protocols [48].

Block hashing: A hashing function is a one-way pseudo-random mathematical function that accepts an unlimited number of bits as input and produces a finite number of bits as output. It is often termed the digital DNA of the blockchain. Merkle trees now use a hash function as part of their block header. To secure transactions on the blockchain, hash functions play a crucial role. Collision-free, hidden, fixed-size, one-way, and large-change are five of the most significant features of a hash function's mathematical equation used in cryptography. There are many other hashing algorithms out there, but SHA-256 is one of the most popular for usage in block hashing functions with MD5, NTLM, SHA-512, SHA-384, etc. [49,50].

Block mining: Mining on the blockchain is the mechanism through which all Bitcoin and other cryptocurrency transactions are verified. Blockchain miners indulge themselves in mining peer-to-peer encryption using high-end hashing functionality. The miners have a difficult task to solve: finding a solution hash that is a perfect match for the one they are working with. If you already know what mining is in blockchain, you still need to learn why it is so important. Any transaction is only added to the blockchain when mining has authenticated it. As a result, it prevents fraudulent purchases. You are paid for "mining" the blocks, which is another way of saying "authorizing" transactions. There are several mining methods, including CPU mining, GPU mining, ASIC mining, and many more [51,52].

Block protocols: As a collection of guidelines, protocols facilitate the transfer of information between nodes in a network. Because blockchains are used for transactions, protocols are crucial for data sharing and preserving the security of their application networks. Security, Decentralization, Consistency, and Scalability are the four guiding concepts that blockchain technologies seek to solve. The five most widely used blockchain protocols are Hyperledger, Multichain, Ethereum, Quorum, and Corda. Out of these five, hyperledger is a well-known technology that enables businesses to create blockchain-based solutions tailored to their requirements. Many hyperledger initiatives have sprung from an incubation phase and gained notoriety. The hyperledger Besu, Fabric, Indy, Iroha, and Sawtooth blockchains are among them [53].

Block algorithms: Blockchain networks depend on consensus techniques to enable multiple dispersed nodes to come to an agreement with one another. With the help of these techniques, it is possible to ensure dependability in a network with different users or nodes. The ability to resolve this issue, known as the consensus problem, is crucial in distributed computing and multi-agent systems like the blockchain networks used by cryptocurrencies. A general agreement is required to provide transparency, security, and immutability in order to provide knowledge of the real-time status of the distributed ledger since the block network is dispersed and lacks a central authority or central node. This is why the consensus algorithm is an essential component of any guide for developing blockchain applications [54,55]. Table 4 below discusses a few prevalent forms of consensus processes used by different writers in their works.

Table 4
Blockchain algorithms with descriptions.

Name of algorithms	Description	Ref.
PoW	It validates transactions and constructs blockchain blocks.	[56]
PoS	It is the simplest and greenest PoW consensus mechanism for transactions on the blockchain.	[57]
PoC	Blockchains allow nodes to vote on who mines new blocks and verifies transactions by utilizing spare hard disc space.	[58]
PoB	Alternative to Proof-of-Work. Miners "burn" virtual currency tokens to operate the system.	[59]
PoID	Permissionless blockchain may use PoID.	[60]
PoI	It is a shareholder-validator PoS protocol.	[61]
PoA	It is "Proof of Stake" updated. PoS speeds transactions.	[62]
PoA	PoW/PoS hybrid algorithm. Network 51% attacks decline significantly. Higher fault tolerance.	[63]
PoET	Intel developed PoET for PoW cryptography, Nakamoto Style.	[64]
DPoS	Dan Larimer invented DPoS in 2013. DPoS delegates verify blocks.	[65]
LPoS	Waves blockchain leases crypto tokens to a block producing node using LPoS.	[66]
DAG	It is Blockchain 3.0 and can fix several blockchain issues.	[67]
pBFT	It optimizes asynchronous systems that replicates hostile nodes.	[68]
DBFT	As similar to DPoS it enables the delegates in large scale participation through proxy voting.	[69]

Table 5
State of art work on securing digital identity in IoT using blockchain technology.

Ref.	Year of publication	Security model	Analysis
[11]	2015	RFID, Barcode	The paper discussed about cyber attacks on IoT systems in Industry 4.0. Introduction of RFId can be used for tracking industrial products.
[14]	2016	GHOST, Blockchain, Ethereum, Bitcoin, CAP Theorem	The paper introduces Blockchain Platform for IIoT.
[16]	2018	PKC, DNSSEC, IETF, RFC4033, CA	This report reviewed emerging IIoT solutions.
[32]	2018	RFID, Blockchain	The article discusses about IoMT wearable devices important to monitor the health of patients on a daily basis.
[34]	2020	BAKMP-IoMT	Blockchain enabled authentication key in IoMT environment.
[37]	2020	RFID	Supply chain management of pharmaceutical things.

In Table 5, the state-of-the-art work on safeguarding digital identity in the realm of IoT through the utilization of blockchain technology has been beautifully laid out. It consists of a study and analysis of the six chosen references that the writers used in the sections with the security model. Verily, the work were elaborated upon in the preceding passages of Section 2 of this article.

3. System under study: Digital identity

In a nutshell, a user's identity specifies the characteristics with regard to that digital identity [70] which refers to the group of characteristics that may be used to uniquely identify a person or group, such as a name, location, and other contact information [71]. To better understand the concept, we are going to decompose your identity into two categories: the user's physical identity and the corresponding digital identity. This review paper concentrates on what is deemed to be digital identity. But before we get into that, let us have a quick glance at physical identity so that we can briefly go through Digital Identity. Your physical identity is something that identifies you as an individual. It includes everything about you: your physical features, your personality, and your daily behavior. These things differentiate you from others and make your identity unique. Even though two people may be close,

Table 6
Common legal boundaries for digital identity.

Common ethics	Description	Ref.
User Control	It is definitely user friendly in any of its application.	[70–72]
Id Rights	Designed for Human Identity	
Actors of DId	The user, issuer, verifier, decentralized database	
Legal Precision	Identity is crucial for security; hence legislation must be precise.	
Purpose of DId	Trust, Integrity, Security, Privacy and Simplicity are top benefits.	
Authenticity	Reduces danger of data breach	
Availability	The goal is to make data accessible to the authorized user in need.	
Security level	Identity Assurance Level, Authenticator Assurance Level, Federation Assurance Level	
Benchmarks	Digital Signature, eIDAS certification, ISO, Standard on Identity and Credential Assurance, Transport Layer Security, Datagram TLS	
Applications	healthcare, Industries, Education, Banking, Insurance, e-Voting, National Identity etc.	

they are not identical. The conference paper, [72] gives a comprehensive physical analysis report. It examines the relationship between gender, self-esteem, and physical identity with regard to body image. It also evaluates physical identity and self-esteem in connection to gender in a sample of 60 people, divided into two groups of 30 women and 30 men, working under the presumption that physical identity is positively connected to self-esteem. Whereas your digital identity consists of your digital traits and behaviors, as well as aspects of your physical identity and personal data. Hence, both your physical and digital identities must be safeguarded. The common boundaries faced in digital identity can be detailed in tabular form in Table 6.

In today's highly digitized and networked society, the importance of a person's digital identity continues to grow. It is a one-of-a-kind depiction of a person or thing taking part in any online activity. Simply having a user name does not suffice to establish your digital persona. Everything about you that exists in the digital realm contributes to this. Your user account, your digital conduct, your personal information, and even aspects of your physical identity are all part of your digital identity [73]. Whenever you connect to the Internet, there are a set of unique digital identifiers that go along with it. It does not matter if it is a social network account or if you are connecting with someone through any other kind of cyberspace program; you are still giving them access to your identity. As soon as a person joins the realm of cyberspace, it might happen either consciously or unwittingly to them, and you will be sucked into the spider's web with only one touch or click. These features are analogous to those that make up your physical identity. The qualities may simply be identified by the system or website you are using. Your IP address, web browser, and operating system or device type are all pieces of information that may be used to identify you. An advanced form of identity management known as digital identity management is one in which the holder of the identity data really owns their own identity data and has complete control over who may access it without the requirement of any third party to act as in the role to go-between. And so, only a digital identity management system can provide the foundation for safe data exchange across programs. National identity, electronic voting, education, e-commerce, banking, insurance, smart cities, travel, social platforms, healthcare, and many more all benefit from the digital identities that are pictured in Fig. 7. However, the societal dimensions of digital identity must be evaluated.

A 2018 IEEE conference paper, [74] publishes that Self-Sovereign Identification is often hailed as the solution to the issue of digital identity that has plagued us for the past 27 years. The paper follows C. Allen's 10 properties [75] and gives a minimalist prototype for Self-Sovereign Identity. It alludes to a notion that the users of this paradigm are the absolute masters of their own identities. The combination of blockchain's decentralized nature and users' ability to exercise sovereignty over their own data creates a highly secure digital identity. A digital identity management system involves the flow of processes between the issuer, validator, decentralized ledger, and the digital identity bearer. The DId bearer is the one who implies the need for self-sovereignty in its identity. The use of bio-metrics (fingerprints), DNA, signatures, and retina/iris patterns in digital identity also makes it popular and secure, which gives a faith-like feeling in the heart for those who do not even need to understand all about the complexity of the terminologies of secured digital identity [76]. Even though fingerprint-based bio-metrics can be broken into, they are better than passwords at keeping your information safe. You can also use vein patterns, the shape of your face, or even your voice to replace the other vulnerable ones [77].

3.1. Applications of digital identity

3.1.1. National unique identity

Despite the potential importance of digital identification for national identity, there is a dearth of academic literature on the topic. The finest of the papers that may be found online have been culled and presented in this review paper. Case studies and reviews of national digital identities from a wide variety of nations were included in the publications. Out of that, India, Estonia,

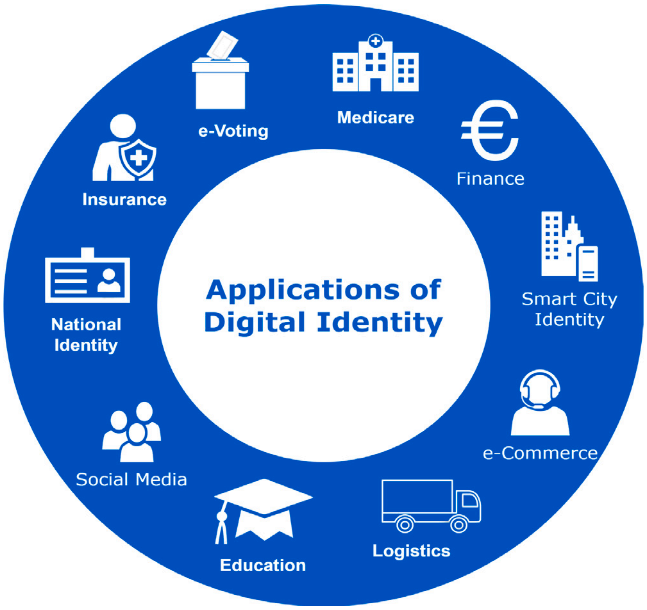


Fig. 7. Applications of digital identity.

Kenya, and Malaysia were the primary points of debate for the authors, which will be expanded upon in the words that follow [78]. Wikipedia reveals that digital identification in the national context may involve a single sign-on and/or the validation of statements by trusted authorities. Many nations have adopted national digital identity cards for their citizens because it has become a matter of nationality, but the majority of developing nations still lag, possibly due to political issues. Nevertheless, it is necessary, and the citizens of the country deserve it to serve as proof of their nationality. In their article "The Emerging Era of Digital Identities: Challenges and Opportunities for the G20", published in August 2022, S. Kanwar, A. Reddy, M. Kedia, and M. Manish described very clearly the case study of the National Integrated Identity Management System (NIIMS), popularly known as Huduma Namba, Kenya's biometric digital identity program that was established in the year 2019. The article includes an overview of digital identification projects across various nations, including India, the US, South Arabia, Brazil, Indonesia, Estonia, the UK, and Italy. It also assessed the influence of those countries, providing us with a clear picture of the nature and purpose of national identity via its implementation and legal framework [79]. Another review article with a case study on Malaysian National Digital Identity (NDI) provides us with a clear image to contribute to our work [80]. The NDI of any nation is a credible and verified mechanism for establishing one's online or cyber identity without supplanting a person's actual physical identity. The primary goal of these efforts is to verify the identities of people utilizing e-government services to gain entry, complete transactions, or use digital signatures, enhancing the integrity, validity, and accessibility of national digital identities that have already been adopted or are in the process of being implemented in any country. Any form of digital identification system that violates human rights will not be tolerated.

The benefits of national identity in the healthcare industry are improved efficiency, security, and patient-centered services such as remote identity verification in telehealth services and patient identification and authentication. It can also be integrated into electronic prescription systems to give patients receiving medication a secure and traceable identity. To guarantee that benefits are paid to the legitimate recipients, the NDI's connection to health insurance data may help stop identity theft and fraud in healthcare insurance claims.

3.1.2. *e-voting*

As we know, voting is the power given to someone who can choose a representative, be it for a nation, an organization, or any group. This has been used since ancient times in many different places but became popular when the term democratic was used in society. This term gives the right to vote a choice of its own. So, voting by the conventional method of balloting is prone to many different errors and difficulties. And the current trend of digitalization also needs voting to change its antique style to a new form that can be shortened to e-voting. It can be expanded to include electronic voting. Hospitals and hospital organizations utilize voting to evaluate public comment, get significant insight into voter behavior, and obtain results for timely reporting [81]. E-voting may be used in a variety of ways thanks to recent technical advances, but a significant change is still needed in this area because people are utilizing comparable developments in other areas of their lives.

The article [82] has put forth a new idea of using blockchain technology for digital voting. It also came up with an experimental model implementation for the proposed approach. But still, it can create some ambiguity in the voters' minds while choosing their representative in this new method. One of the ideas can be to use social media platforms for e-voting, but the point would be how to find a genuine user or duplicate one because many people have multiple fake accounts on this platform. So, a drastic change is

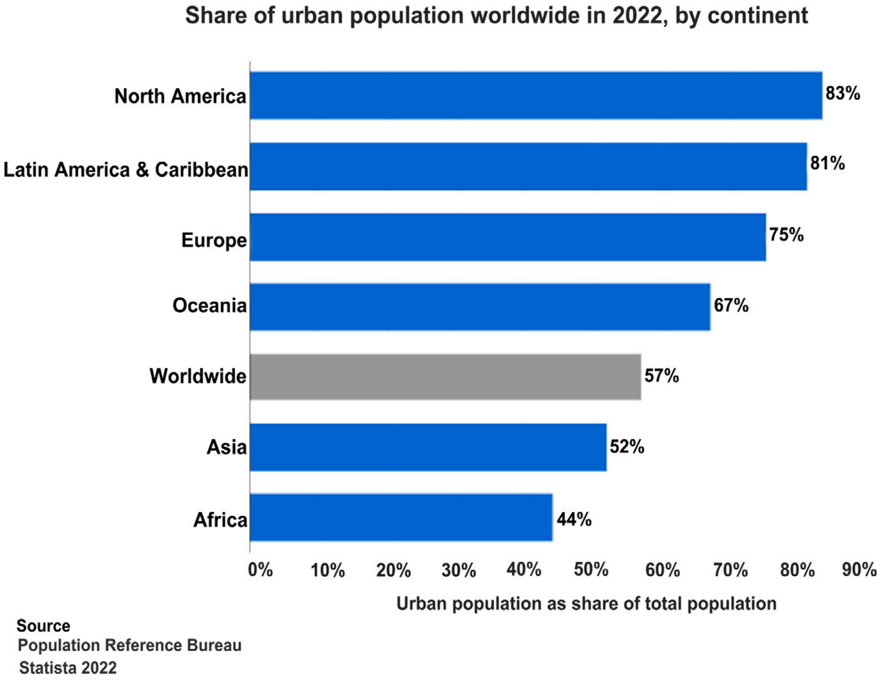


Fig. 8. Worldwide urban population in 2022, continent-wise.
Source: Statista-2022

required with the AI interface for the modification of e-voting, which will also be possible shortly. Yet another journal paper, [83] also gives a detailed study report on the downsides and benefits of e-voting with the implementation of blockchain. But to overcome the risks by converting them into an opportunity instead of adopting a new one should be the only motto. Identity can have a safe utilization, as discussed in the above descriptions, and its applications can also overcome the disadvantages. The article [84] gives a clear model that can be implemented as digital voting by using smart contracts. It describes a step-by-step process with algorithms, from the registration of voters to the casting of votes. The author gives such beautiful writing in its seventeen-page article, which drives a point of attraction.

Thus, it can be concluded that the healthcare sector may develop a really smart hospital with the use of electronic voting. Applications include feedback from patients, online voting for hospital quality of care, and Hospital Association Elections. Thus, votes on hospital boards and advocacy for patient care alternatives are conducted regularly by both bigger hospital groups and individual hospitals.

3.1.3. Smart city

The use of blockchain technology coupled with decentralized digital identities in the context of the creation of smart cities has progressed significantly in recent years, allowing for the provision of a more environmentally friendly infrastructure for the city's inhabitants. Keeping this in mind, the chain of extension of smart cities has risen throughout their growth. As we reported in a case study, many countries have adopted mega projects for transforming their cities into smart cities. Genuinely smart cities took the lead in fulfilling aspects of urban digital life. But still, there is a lot of ambiguity arising in the implementation of technology for the development of smart cities. For this reason, many countries have also started to set up smart city development centers to come up with new ideas in view of the requirement. The IEEE-published conference paper [85] also gives a case study report on smart cities in Estonia that have adopted several innovative approaches to simplify their municipal services. It is anticipated that, without a doubt, this review article will motivate a great number of scholars to have their papers in this field so that a great number of ideas may be produced. Digital Identity is needed to unlock the potential of smart cities, and adding blockchain to it will definitely provide a level of security. The degree of urbanization in the world has increased to a new level, which leads to a demand for smart cities. Fig. 8 source image: Statista [86] is the report that gives the degree of urbanization by continent. The website [87] has released its predictions for the top seven smart cities in the world for the year 2023. At the top of the list is Singapore, which surpassed Seoul, South Korea, which was the first smart city in the world. To get a summary of the forecasts that will lead the city to the top, see Table 7.

Most smart cities focus on infrastructure, transportation, city lighting, and other government functions. Most do not explicitly prioritize health or healthcare beyond improving quality of life. Furthermore, smart cities are inherently urban. However, several significant rural places place a similar emphasis on smart solutions for their citizens, but not on a full scale. Smart cities were created to achieve 360-degree smartness, which would improve the quality of life, economic opportunity, and security for individuals who

Table 7
Smart city ranking of 2023 [87].

Rank	Name of city	Initiation	Singularity excellence
1	Singapore	2017	Introduced contactless payment, public transit, and other smart technologies, supported decarbonization, announced vehicle-free eco-smart city.
2	Helsinki	2017	Recorded and low emission city
3	Zurich	2018	Voted as most walker friendly city
4	Oslo	2019	Aimed for zero emission city
5	Amsterdam	2019	Innovation in renewable energy
6	New York	2020	Recorded most efficient waste management system
7	Seol	2014	Senior citizens' safety initiatives

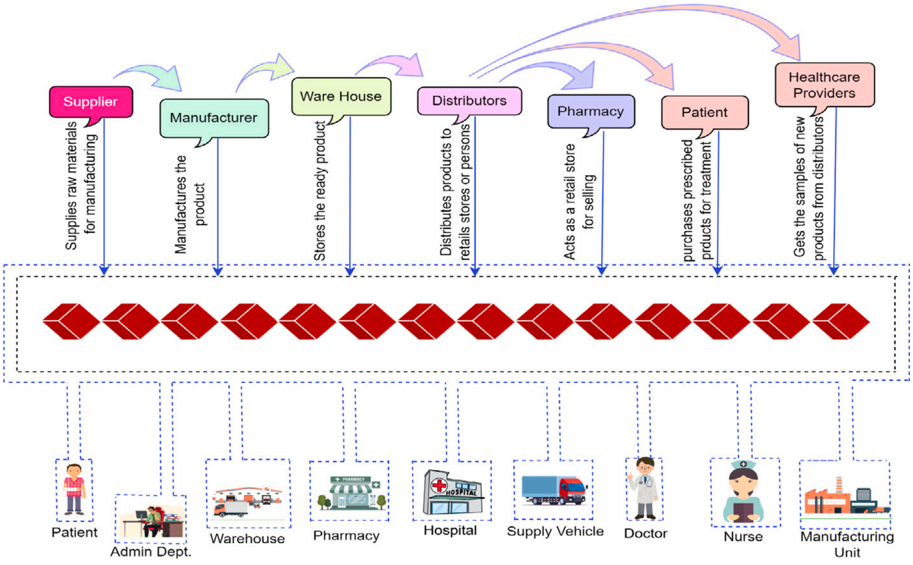

Supplier
Manufacturer
Ware House
Distributors
Pharmacy
Patient
Healthcare Providers
Supplies raw materials for manufacturing
Manufactures the product
Stores the ready product
Distributes products to retails stores or persons
Acts as a retail store for selling
purchases prescribed prducts for treatment
Gets the samples of new products from distributors
Patient
Admin Dept.
Warehouse
Pharmacy
Hospital
Supply Vehicle
Doctor
Nurse
Manufacturing Unit

Fig. 9. Blockchain enabled decentralized supply-chain management.

live in cities and their surroundings. So, with the rising amount of health-related data, as well as the integration of health and human services as part of this trend, citizens may connect with smart services that are expressly tailored to enhance their health. A smart city might be a powerful tool for transforming the healthcare system.

3.1.4. Logistics & supplychain

The application area of digital identity can be included for both logistics and supply chain management systems using a decentralized ledger, where "Logistics" focuses on the physical movement and transportation of goods, while "supply chain management" refers to a larger range of operations that include procurement, production, distribution, and coordination of numerous activities to provide products or services to end users. Whether it is tracking of medicines, transportation, management of assets, or automobile personas, driver identification can be handled safely via blockchain, and devices can be managed and monitored for their entire life cycle. Starting from the manufacturing of the products, it gets enrolled in a unanimous blockchain, and within its lifespan, it includes the transportation, sale, application, and any fraudulent activity or duplication. All different real-time data gets taped inside a ledger of the blockchain, which could be securely accessible by any member of the decentralized network in supply chain management systems, as shown in Fig. 9.

The research article [88] presents a case study report on the use of self-sovereign identities in public transportation. In addition, the work offers a plan of execution as well as a prototype version with reduced quality of a decentralized identity management system for use in the application area. It only provides all of its assessments and graphics for nations that are members of the European Union, which, by law, may be different for any other country. To facilitate uses like aided vehicle driving and safety alerts, the major objective is to equip moving carriers with the ability to transmit data autonomously to the ledger for keeping a record of all the activities [89].

This part of the article concludes by surveying the blockchain supply chain of healthcare products that the aftermath of the COVID-19 outbreak has forced healthcare professionals to rely on technology to regulate their supply chains. Blockchain-based

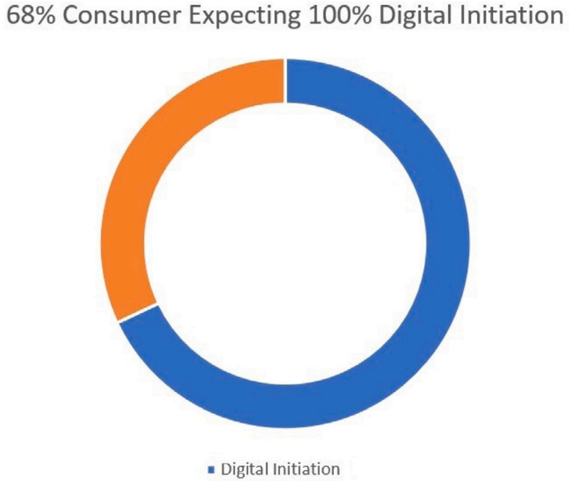


Fig. 10. Percentage of consumers expecting Digitization.
Source: microblink.com

solutions have shown to be extremely beneficial in the healthcare sector by enabling secure data retrieval and storage, resulting in increased data integrity and simplified medical practices. This will be done strategically to increase the efficiency and efficacy of their supply chain operations. In addition, the use of blockchain in the pharmaceutical and medical sectors is predicted to reach $815.65 million by 2026, growing at a CAGR of 22.10% between 2023 and 2030. [90].

3.1.5. Banking and health insurance

It is only the financial institutions that started prioritizing the decentralized ledger for its implementation in their sector. And all the others came after it. These institutions always attempted to make additional applications for improvement in online behavior to provide a secured digital identity for customers in financial transactions. For this reason, only these sectors are emphasized for the research and development of AI and ML. The result is a revolution in finance. Whatever the reason may be, progress is picking up its pace, and here we are with the addition of self-sovereign identification to the distributed ledger. The article [91] discusses the implementation of an open banking system by the financial institution, which allows third-party service providers to access financial data to search for the best offers and enhance the user experience. As a result, questions were raised about identity (digital identity), data sharing, and privacy preservation. This can only be committed by blockchain-based self-sovereignty in the identity. Finance and insurance companies are feeling the effects of technology across the board. Since the outbreak of the pandemic, the global insurance industry has increased with greater urgency.

In spite of the fact that digitization is changing the way in which insurers interact with their covered clients, one thing will not change: the necessity of doing customer verification. In the insurance industry, like in every other facet of the financial sector, there are stringent legislative criteria that must be adhered to for consumer verification. However, the conventional method of user verification might take up a large amount of time; in most circumstances, this period is greater than 20 min. This is just not acceptable in a world where customers anticipate that digital onboarding procedures will take no more than sixty seconds or even less. And it results in a significant loss of user lifetime value for insurers.

It is of the utmost importance that the experience be quick, risk-free, and unbroken. The most successful insurance companies understand this. In the most recent iteration of Signicat‘s Study, titled “The Battle to Onboard 2020: The Effect of COVID-19 and Beyond”, the company conducted a survey that polled 4,000 individuals all around Europe to determine consumer sentiment towards the process of onboarding.

According to the findings of the survey, 68% of customers anticipate having a completely digital onboarding experience, which increased in post-covid. AI, thank goodness, offers a solution to fulfill the requirements set forth by your clients Fig. 10, which has been sourced from microblink depicts the details [92].

3.1.6. e-Commerce

The convergence of healthcare and e-commerce has enabled significant advances in patient care, accessibility, and convenience. Buying and selling of products and services through the internet, together with the related transmission of funds and data, is referred to as e-commerce [93]. Wikipedia reveals that e-commerce makes use of tools like m-commerce, e-fund transfer, supply chain management, online marketing, online inventory management, and automatic data collection systems, and it has become the driving force of the industry. During the covid outbreak, when the whole planet was quarantined and unable to move, it grew rapidly. As a result of COVID-19’s severe vehicular restrictions, the introduction of AI enabled chatbots has become a major game changer to reduce human involvement in the sector [94] aiming to boost efficiency. The widespread use of regional languages has also contributed to the trend’s rising popularity [95]. In healthcare, e-commerce, where drugs medical gadgets and supplements are purchased and sold, product authenticity is critical. The transparency and traceability of blockchain technology also come in handy here. It can be called a rumor that e-commerce is harming any business, but the truth is that it boosts the industry with turbo-powered energy. And also, this can participate in marketing digital identity. So, both digital identity and its application, e-commerce, are interdependent, and so they are inextricably linked.

3.1.7. Social media

Developing a social media network for the healthcare industry necessitates a careful strategy to ensure privacy, security, and compliance with healthcare standards. Social media sites like YouTube, Facebook, Twitter, Instagram, WhatsApp, Telegram, and many others, have been named as the most engaged online platforms in recent years [96]. These platforms participate in reaching the current generation with major technological changes and developments. And also as a major role in spreading socioeconomic, political, cultural, and security issues in the user chain. Since it is an obvious fact that technology cannot advance if it is not employed, So, the social media platform takes the lead role in reaching out to the demanding needs of a generation. As a result, the social media platform has achieved its goal in this modern society and has become the pinnacle of globalization. Facebook in 2004 and YouTube in 2005 emerged as platforms, and now they rule them by connecting people and making a strong human chain. They contain all the daily activity in a timeline that can be tracked whenever required. Still, there is a need to overcome the disabilities of these platforms. Somehow the upcoming metaverse of the applications can be the game changer of the sector. Many challenges are to be overcome for the most anticipated metaverse applications of social media [97].

3.1.8. Education

The use of digital identities in healthcare may have a substantial influence on education by improving learning experiences, assuring secure access to educational resources, and increasing overall efficiency. The education system is on the verge of undergoing a radical digital change. There are many students and teachers who utilize digital technologies for personal purposes outside of school; these tools are often hailed as essential for the classrooms of the 21st century. Schools in today's generation want to use multidimensional educational methods to make the subject interactive so that they can increase the educators learning abilities. In order for educational communities to concentrate on speeding up learning, they need a digital identity platform to guarantee security and streamline operations. A certain review made by [98] describes how a teacher sees herself as a professional, both individually and collectively. The paper also cited research by Beijaard, Verloop, and Vermunt (2000) on Dutch secondary school teachers, which explains that educators value their expertise as subject matter experts, pedagogical experts, and didactic experts. Graduation is not the end of a student's connection to their alma mater. The transition from student to alum to donor is seamless. Because of the critical nature of this issue, the availability of a digital identification platform is of paramount importance. In this sense, a simple student ID card is not sufficient to describe the identity. There can be a lot of vulnerability in it. As technology is developing in parallel, the identity of the student also needs to develop. Learners, healthcare professionals, and educators who use online educational platforms can use digital identification to authenticate themselves securely. Personalized learning paths might be created for healthcare workers based on their positions, expertise, and educational backgrounds. This tailors instructional content to individual requirements, hence improving the learning experience. Simulated learning environments are essential for healthcare education because they allow students and professionals to practice numerous scenarios in a controlled and safe setting. Finally, access to the most recent healthcare research and publications, which are accessible only by authorized persons, contributes to the integrity of academic knowledge. So as the educator's history of education with skill, talent, experience, ability, and deficiency can be on a ledger to keep its identity up to a certain level in the future, Though we can find some social media platforms that have the role of maintaining records of the educators' backgrounds, they are not up to the mark from a security point of view. There can be many vulnerabilities in the form of duplication, back doors, mirrors, and fake information. In light of these trends, it is safe to assume that educational institutions will continue to embrace innovation in their administrative operations, which will be armed with all the cutting-edge tools necessary to be successful and serve the students of the future [99].

3.1.9. Healthcare

IoTBDId will revolutionize healthcare and solve all its deficiencies. The IoT and digital identity play a crucial role in the healthcare sector, enabling improved patient care, efficient operations, and secure access to medical information [100,101]. IoT devices, such as wearable and other connected medical devices, can provide essential information regarding the health conditions of patients. Monitoring patients with IoT devices enables healthcare providers to collect real-time data on vital signs and activity levels, and promotes medical adherence. In addition, IoT-based asset monitoring systems aid healthcare organizations in managing and locating medical supplies, equipment, and devices. Digital Identity solutions enable accurate patient identification and authentication. It gives the patient a sense of self-determination. In addition, it plays a vital function in safeguarding patients' sensitive health information. The implementation of a standard digital identity management solution in a healthcare organization safeguards the transmission of data between diverse IoT devices, electronic health records [102], and other healthcare applications. The implementation of decentralized technology by IoT devices has the potential to alter problems and challenges. Several applications for healthcare involving IoTBDId can be summarized in the following points and tabloid form in Table 8.

Patient identification and authentication: Blockchain-based identity management solutions can give individuals more control over their personal health information. Patients may retain control over their digital identities, giving access to healthcare practitioners and researchers as needed while maintaining privacy and permission. Similarly, IoT devices, such as wearables and linked medical equipment, can provide important information about patients' health. Digital identification solutions aid in effectively identifying and authenticating patients, ensuring that the correct data is connected to the appropriate individual.

Table 8
Applications for healthcare by involving IoTBDId.

Applications	Description	Ref.
Paperless healthcare	IoMT devices will automatically provide the patient health information and treatment specifics to the clinician	[103]
Medical Record Management	IoT devices and secure ledger technologies will handle medical data without paper	[104]
Secured storage of Medical Documents	The entire details of the patient will be there in the secured ledger.	[105]
Secured Data exchange	Patient health information exchange happens in a secured environment	[106]
Telemedicine	Patient can have telemedicine support by remotely contacting to the doctor.	[107]
Self-Sovereign Patient Identity	The patient owns their identities, which would give them control over their own data	[108]
Remote healthcare	Tracking of patient for medication from a remote location made possible.	[109]
Managing Hospital Financial Accounts	The hospital financial management made possible in a secured environment.	[110]
Patient Treatment Tracking	Tracking serious patients from a remote location becomes easier with the use of IoMT devices to determine their development	[111]
Detection of hoaxes	Fake identity detection becomes easier with the implementation of AI and ML	[112]

Secure access to medical records: Digital identity management solutions enable safe access to EHRs and other sensitive medical data. Healthcare providers should use robust authentication and authorization procedures to guarantee that only authorized users can access patient data through IoT-enabled devices. It gives people ownership over their medical data and enables them to safely share their records with healthcare practitioners when required. Blockchain-based EHRs can improve data integrity, speed up access, and reduce the need for duplicate record-keeping.

Remote patient monitoring: Digital identities linked to IoT devices allow for real-time monitoring of patient health. In crises, appropriate healthcare providers can be notified promptly, reducing response times. This is especially useful for people with chronic diseases who need constant monitoring.

Healthcare asset tracking: Healthcare organizations may use IoT-based asset monitoring solutions to manage and identify medical equipment, supplies, and gadgets. Digital identification solutions may be used to identify certain assets with their own digital identities, allowing for more effective monitoring, inventory management, and maintenance.

Privacy and data security: Digital identity management is crucial for preserving patient privacy and securing sensitive healthcare data. Strong authentication, identity federation, and encryption approaches can be used to protect IoT-generated healthcare data from unauthorized access or manipulation. Biometric data, such as fingerprints or retinal scans, are increasingly utilized to identify patients. Biometric data can be more secure when stored and sent via digital identification systems. Furthermore, blockchain may be utilized to provide a decentralized repository for biometric data.

Secure health data exchange: Digital identification systems provide patients with control over their health data. Patients may use their digital identity with many healthcare providers and IoT devices, ensuring that their health information is portable and easily available when needed. Blockchain technology can facilitate safe and decentralized health data sharing between healthcare providers, patients, researchers, and other stakeholders. It protects data integrity, confidentiality, and auditability, lowering the likelihood of data breaches and unauthorized access. Blockchain-based solutions can provide a tamper-proof and transparent record of health-related transactions.

Drug traceability and supply chain management: Ensuring the authenticity and security of medical devices is critical. Blockchain technology can help to develop a transparent and secure supply chain for medical products. This aids in confirming the origin and validity of devices, avoiding the use of counterfeit equipment, assuring authenticity, and increasing patient safety.

Health insurance claim processing: Blockchain technology can help simplify health insurance operations by offering a decentralized and transparent claims management platform. It reduces fraud by confirming the legitimacy of insurance policies and automating claim settlements using smart contracts, resulting in faster and more accurate payment procedures.

Reserach and analytics: Collectively, anonymized IoT data connected to digital IDs may be utilized for research and analytics to uncover health patterns and enhance healthcare services. Proper de-identification procedures are critical for protecting individual privacy.

Table 9
State of Art Work on Securing Digital Identity in healthcare domain using Blockchain.

Ref.	Year of publication	Security model	Technical analysis
[77]	2018	Digital Identity, Biometrics	Finger vein biometrics is discussed.
[100]	2021	Blockchain	Patient data security , Drug traceability, Genomics, avoid expensive error
[103]	2009	EHR, IT, CCHIT	IT-enabled healthcare system is discussed
[105]	2020	Hyperledger AI, IoT, AR, VR	The study discusses using blockchain in healthcare system for automated data collection and verification processes
[106]	2019	HER, Blockchain	The document addresses errors EHR uploads
[107]	2021	IPFS, CA, X.509, PoW	Telemedicine diagnosis and Patients privacy protection scheme
[108]	2020	DLT, Blockchain, Decentralized Id Management	The paper focus on Self-Sovereign Identity of patient.
[109]	2021	Blockchain, Sho Card, PoS	Regarding Covid-19 digital Health ID is considered

AI and ML for decision support: AI and machine learning algorithms may be integrated into healthcare applications to provide decision assistance systems. In the context of healthcare, these technologies can help with risk prediction, fraud detection, and personalized treatment advice.

As the state-of-the art work was presented for Section 2, an analogous assessment of the third segment on eight chosen articles has been put out. Along with the security models that the authors used, this review also provides an outline of the analysis report in Table 9.

4. Security analysis

Blockchain maintains the data in a covert and encrypted manner that ensures confidentiality. It relieves unnecessary paper-based identity management by providing decentralized web-based identity solutions, self-sovereign identity, and simple identity verification. Blockchain safeguards critical IT infrastructure, enabling CIA, especially in IoT environments, and user identity validation.

CIA, which is short for confidentiality, Integrity & Availability, also called as CIA Triad due to the collection of three principles, are considered as the cornerstones of information security. The CIA Triad directs the creation and upkeep of secure systems across a range of industries. Organizations seek to safeguard their data and systems against a range of dangers, such as unauthorized access, data breaches, and service interruptions by upholding these standards. These three fundamental ideas are essential for guaranteeing the security and integrity of patient data especially as the survey article is directed toward healthcare organizations.

IoTBDId analysis report says about strong consent management that guarantees that patients have authority over their digital identities. Patients ought to be allowed to dictate who has access to their medical records and under what circumstances. The function of identity fraud in digital identity management is another secure access restriction, anomaly detection, and real-time monitoring all help to stop fraudulent activity using patient digital identities.

4.1. Imperative security analysis over IoT using digital identity

The usage of Smart IoT devices and applications is thriving day by day, which generates a large amount of data. Significant digital identity analysis on different IoT platforms has been carried out as a review after considering many articles. Especially the digital identity security validation is as follows in Fig. 11.

4.2. Imperative security analysis over blockchain

Blockchain plays a prominent role in creating decentralized user identification due to its ease of use, high efficiency, and low vulnerability when using verifiable credentials. A common digital identity can be framed across different digital and online platforms, depicting the power of blockchain. Mainly the digital identity challenges for blockchain-based solutions, such as in Fig. 12:

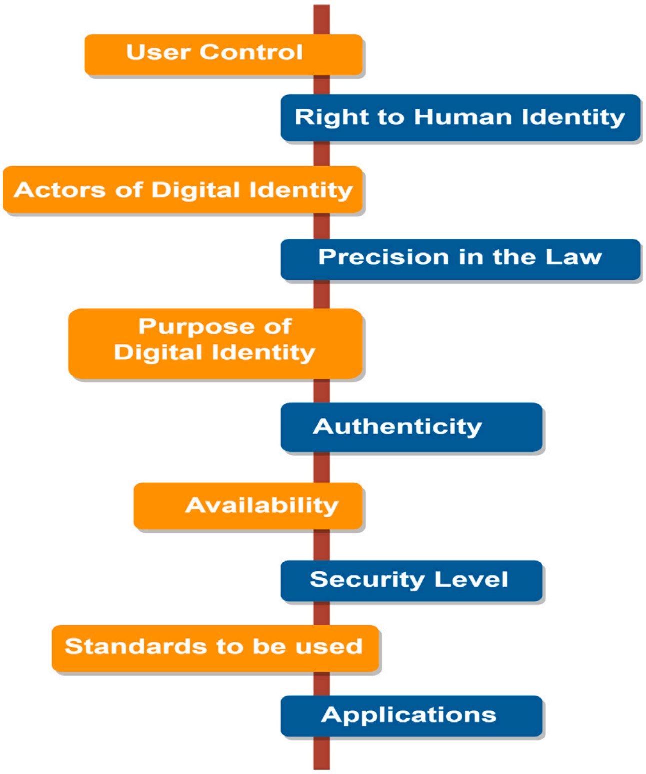


Fig. 11. Digital Identity Security Validators.

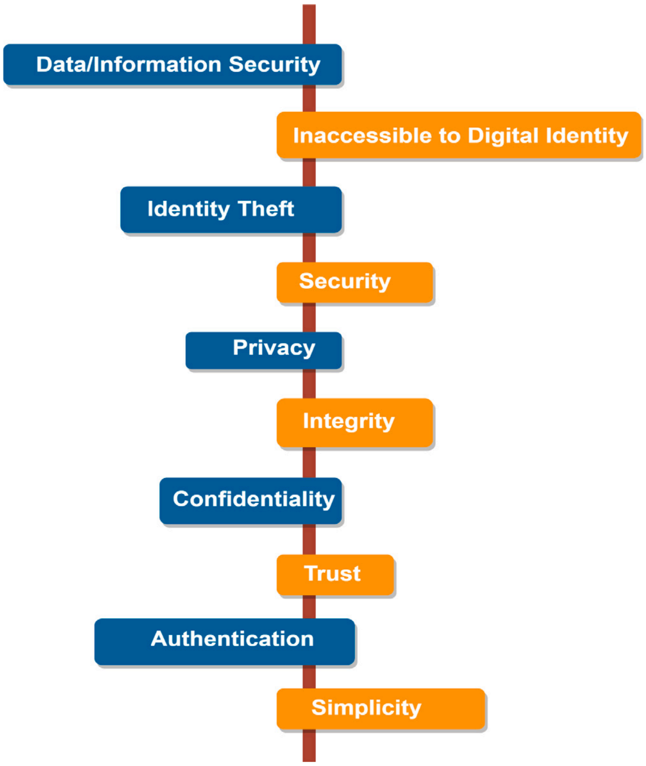


Fig. 12. Digital identity challenges.

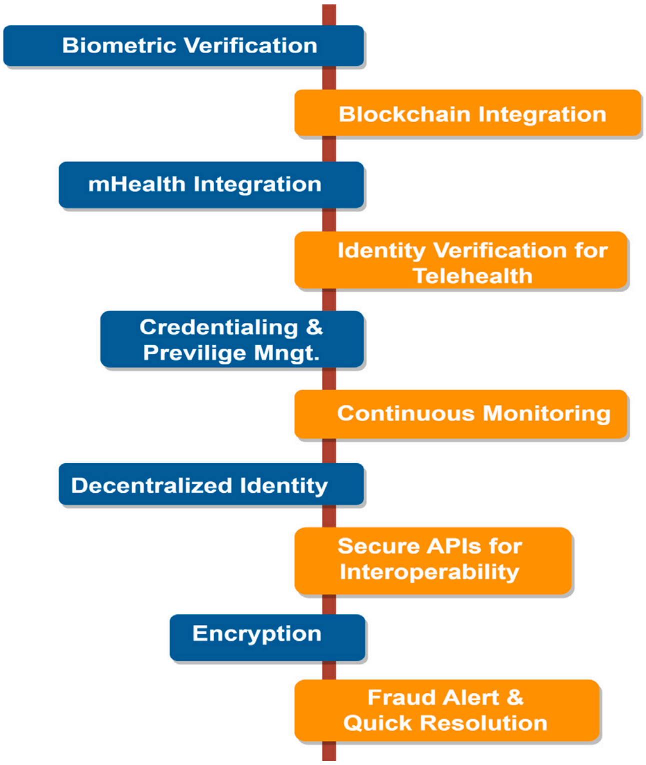

Biometric Verification
Blockchain Integration
mHealth Integration
Identity Verification for Telehealth
Credentialing & Previlige Mngt.
Continuous Monitoring
Decentralized Identity
Secure APIs for Interoperability
Encryption
Fraud Alert & Quick Resolution

Fig. 13. Digital identity solutions for healthcare.

4.3. Imperative security analysis in healthcare using digital identity

This analysis aims to develop a framework that not only addresses the current security challenges but also anticipates future threats. In particular, when it comes to fraud detection, the framework would enable prompt identification and resolution of possible security concerns by facilitating continuous monitoring and real-time analysis of transactions.

Furthermore, the implementation of identity lifecycle management, sometimes referred to as digital identity management, in the healthcare industry emphasizes the significance of managing digital identities from the point of generation to the point of cessation to maintain the relevance and accuracy of the identity information of patients. This improves security while also helping to keep a current trustworthy health information database in blockchain-based smart hospitals that become resilient against failure and data exposure such as in Fig. 13:

5. Conclusion

This paper gives a distinct and rigorous study of digital identity security challenges and solutions on different IoT and blockchain platforms. At first, glimpses of different IoT platforms and their security analysis were pursued, followed by blockchain and types. This survey mainly emphasizes the security aspect of digital identity in the healthcare domain, issues, and solutions using blockchain and are summarized at the end as case studies. Overall, the reader will learn about the problem of digital identity theft in IoT and blockchain.

CRediT authorship contribution statement

Sanjay Kumar Jena: Writing – original draft. **Ram Chandra Barik:** Supervision. **Rojalina Priyadarshini:** Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

I would like to express my gratitude to my primary supervisor, who guided me through this paper. I would also like to thank our madam, Head of the Department of Computer Science and Engineering at C. V. Raman Global University, Bhubaneswar, for her extensive guidance. Thanks are also due to the library staff and research participants who provided invaluable assistance and inspiration, without whom this essay never would have been written. Last but not least, I must give a shout-out to my wonderful parents, spouse, and kids. Their belief in me has kept my spirits and motivation high to make this state-of-the-art review paper.

Appendix

AAL	Authentication Assurance Level
AI	Artificial Intelligence
ASIC	American Standard Code for Information Interchange
CA	Certifying Authority
CPU	Central Processing Unit
DAG	Direct Acyclic Graph
DBFT	Delegated Byzantine Fault Tolerance
DId	Digital Identity
DNSSEC	Domain Name System Security Extension
DPoS	Delegated Proof of Stake
DTLS	Datagram Transport Layer Security
ECG	Electrocardiogram
EEG	Electroencephalogram
eIDAS	Electronic Identification & Authentication Services
FAL	Federation Assurance Level
FPGA	Field programmable Gate Array
GPU	Graphic Process Unit
IAL	Identity Assurance Level
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoET	Internet of Every Things
IoMT	Internet of Medical Things
IoP	Internet of People
IoTBDId	Internet of Things and Blockchain for Digital identity
IoT	Internet of Things
IoVT	Internet of Video Things
IPFS	InterPlanetary File System
ISO	International Organisation for Standards
IT	Information Technology
LPoS	Leased Proof of Stake
LTE	Long Term Evolution
MD5	Message Digest
NFT	Non-Fungible Token
NIIMS	National Integrated Identity Mngt.
NTLM	New Technology LAN Manager
pBFT	Practical Byzantine Fault Tolerance
PKC	Public Key Cryptography
PoA	Proof of Authority
PoA	Proof of Activity
PoB	Proof of Burn
PoC	Proof of Capacity
PoET	Proof of Elapsed Time
PoID	Proof of Identity
PoI	Proof of Importance
PoS	Proof of Stake
PoW	Proof of Work
SHA	Secured Hash Algorithm
TLS	Transport Layer Security
Wi-Fi	Wireless Fidelity
X.509	It is a standard

References

[1] M.A. Engelhardt, Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector, Technol. Innov. Manage. Rev. 7 (10) (2017).

[2] S.G. Alonso, J. Arambarri, M. López-Coronado, I. de la Torre Díez, Proposing new blockchain challenges in ehealth, J. Med. Syst. 43 (3) (2019) 1–7.

[3] J. Lynn, Digital identity in healthcare, 2021.

[4] I. Childress, Healthcare's top five identity and security challenges, 2022.

[5] S. Jain, M. Nehra, R. Kumar, N. Dilbaghi, T. Hu, S. Kumar, A. Kaushik, C.-Z. Li, Internet of medical things (IoMT)-integrated biosensors for point-of-care testing of infectious diseases, Biosens. Bioelectron. 179 (2021) 113074.

[6] P. Anand, Y. Singh, A. Selwal, P.K. Singh, R.A. Felseghi, M.S. Raboaca, Iovt: internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids, Energies 13 (18) (2020) 4813.

[7] A. Sammoud, A. Kumar, M. Bayoumi, T. Elarabi, Real-time streaming challenges in internet of video things (IoVT), in: 2017 IEEE International Symposium on Circuits and Systems, ISCAS, IEEE, 2017, pp. 1–4.

[8] X. Zhang, X. Wei, L. Zhou, Y. Qian, Social-content-aware scalable video streaming in internet of video things, IEEE Internet Things J. 9 (1) (2021) 830–843.

[9] C.W. Chen, Internet of video things: Next-generation IoT with visual sensors, IEEE Internet Things J. 7 (8) (2020) 6676–6685.

[10] H. Mikko, L. Nyman, et al., The internet of (vulnerable) things: On hypponen's law, security engineering, and IoT legislation, Technol. Innov. Manage. Rev. (2017).

[11] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things, in: 2015 52nd ACM/EDAC/IEEE Design Automation Conference, DAC, IEEE, 2015, pp. 1–6.

[12] D.J. Langley, J. van Doorn, I.C. Ng, S. Stieglitz, A. Lazovik, A. Boonstra, The internet of everything: Smart things and their impact on business models, J. Bus. Res. 122 (2021) 853–863.

[13] P.K. Malik, R. Sharma, R. Singh, A. Gehlot, S.C. Satapathy, W.S. Alnumay, D. Pelusi, U. Ghosh, J. Nayak, Industrial internet of things and its applications in industry 4.0: State of the art, Comput. Commun. 166 (2021) 125–139.

[14] A. Bahga, V.K. Madisetti, Blockchain platform for industrial internet of things, J. Softw. Eng. Appl. 9 (10) (2016) 533–546.

[15] D. Serpanos, M. Wolf, Industrial internet of things, in: Internet-of-Things (IoT) Systems, Springer, 2018, pp. 37–54.

[16] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: Challenges, opportunities, and directions, IEEE Trans. Ind. Inform. 14 (11) (2018) 4724–4734.

[17] W.Z. Khan, M. Rehman, H.M. Zangoti, M.K. Afzal, N. Armi, K. Salah, Industrial internet of things: Recent advances, enabling technologies and open challenges, Comput. Electr. Eng. 81 (2020) 106522.

[18] M. Serror, S. Hack, M. Henze, M. Schuba, K. Wehrle, Challenges and opportunities in securing the industrial internet of things, IEEE Trans. Ind. Inform. 17 (5) (2020) 2985–2996.

[19] A.A. Toor, M. Usman, F. Younas, A.C. M. Fong, S.A. Khan, S. Fong, Mining massive E-health data streams for IoMT enabled healthcare systems, Sensors 20 (7) (2020) 2131.

[20] B. Pradhan, S. Bhattacharyya, K. Pal, IoT-based applications in healthcare devices, J. Healthc. Eng. 2021 (2021).

[21] A. Nayyar, V. Puri, N.G. Nguyen, BioSenHealth 1.0: A novel internet of medical things (IoMT)-based patient health monitoring system, in: International Conference on Innovative Computing and Communications, Springer, 2019, pp. 155–164.

[22] S. Cheruvu, A. Kumar, N. Smith, D.M. Wheeler, Demystifying Internet of Things Security: Successful Iot Device/Edge and Platform Security Deployment, Springer Nature, 2020.

[23] M. Ammar, G. Russello, B. Crispo, Internet of things: A survey on the security of IoT frameworks, J. Inf. Secur. Appl. 38 (2018) 8–27.

[24] H. Derhamy, J. Eliasson, J. Delsing, P. Priller, A survey of commercial frameworks for the internet of things, in: 2015 Ieee 20th Conference on Emerging Technologies & Factory Automation, (Etfa), IEEE, 2015, pp. 1–8.

[25] A. Pliatsios, C. Goumopoulos, K. Kotis, A review on iot frameworks supporting multi-level interoperability—the semantic social network of things framework, Int. J. Adv. Internet Technol. 13 (1) (2020) 46–64.

[26] L. Calderoni, A. Magnani, D. Maio, IoT manager: An open-source IoT framework for smart cities, J. Syst. Archit. 98 (2019) 413–423.

[27] S. Ilieva, A. Penchev, D. Petrova-Antonova, Internet of things framework for smart home building, in: Digital Transformation and Global Society: First International Conference, DTGS 2016, St. Petersburg, Russia, June 22-24, 2016, Revised Selected Papers 1, Springer, 2016, pp. 450–462.

[28] B. Newsletter, A detailed guide to the internet of medical things (IoMT), 2023.

[29] C. Dai, X. Liu, H. Xu, L.T. Yang, M.J. Deen, Hybrid deep model for human behavior understanding on industrial internet of video things, IEEE Trans. Ind. Inform. 18 (10) (2021) 7000–7008.

[30] F. Alsubaei, A. Abuhussein, V. Shandilya, S. Shiva, IoMT-SAF: Internet of medical things security assessment framework, Internet Things 8 (2019) 100123.

[31] R.P. Singh, M. Javaid, A. Haleem, R. Vaishya, S. Ali, Internet of medical things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications, J. Clin. Orthopaed. Trauma 11 (4) (2020) 713–717.

[32] F. Qureshi, S. Krishnan, Wearable hardware design for the internet of medical things (IoMT), Sensors 18 (11) (2018) 3812.

[33] I.V. Pustokhina, D.A. Pustokhin, D. Gupta, A. Khanna, K. Shankar, G.N. Nguyen, An effective training scheme for deep neural network in edge computing enabled internet of medical things (IoMT) systems, IEEE Access 8 (2020) 107112–107123.

[34] N. Garg, M. Wazid, A.K. Das, D.P. Singh, J.J. Rodrigues, Y. Park, BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment, IEEE Access 8 (2020) 95956–95977.

[35] Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović, M. Turkanović, Towards the classification of self-sovereign identity properties, IEEE Access 10 (2022) 88306–88329.

[36] M. Takemiya, B. Vanieiev, Sora identity: Secure, digital identity on the blockchain, in: 2018 Ieee 42nd Annual Computer Software and Applications Conference, (Compsac), vol. 2, IEEE, 2018, pp. 582–587.

[37] S.K. Dwivedi, R. Amin, S. Vollala, Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism, J. Inf. Secur. Appl. 54 (2020) 102554.

[38] R. Awati, Consensus algorithm, 2022.

[39] P. Bottoni, C. Di Ciccio, R. Pareschi, D. Tortola, N. Gessa, G. Massa, Blockchain-as-a-service and blockchain-as-a-partner: Implementation options for supply chain optimization, Blockchain: Res. Appl. (2022) 100119.

[40] H. Guo, X. Yu, A survey on blockchain technology and its security, Blockchain: Res. Appl. 3 (2) (2022) 100067.

[41] D. Efanov, P. Roschin, The all-pervasiveness of the blockchain technology, Procedia Comput. Sci. 123 (2018) 116–121.

[42] D. Vujičić, D. Jagodić, S. Ranđić, Blockchain technology, bitcoin, and ethereum: A brief overview, in: 2018 17th International Symposium Infoteh-Jahorina, (Infoteh), IEEE, 2018, pp. 1–6.

[43] S. Mazumdar, S. Ruj, Design of anonymous endorsement system in hyperledger fabric, IEEE Trans. Emerg. Top. Comput. 9 (4) (2019) 1780–1791.

[44] R. Krishnamurthi, T. Shree, A brief analysis of blockchain algorithms and its challenges, Archit. Framew. Dev. Appl. Blockchain Technol. (2019) 69–85.

[45] Y. Zhan, B. Wang, R. Lu, Y. Yu, DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains, Inform. Sci. 559 (2021) 8–21.

[46] C. Yan, C. Zhang, Z. Lu, Z. Wang, Y. Liu, B. Liu, Blockchain abnormal behavior awareness methods: A survey, Cybersecurity 5 (1) (2022) 1–27.

[47] Y. Yang, D. Cooper, J. Collomosse, C.C. Drăgan, M. Manulis, J. Steane, A. Manohar, J. Briggs, H. Jones, W. Moncur, Tapestry: A de-centralized service for trusted interaction online, IEEE Trans. Serv. Comput. 15 (3) (2020) 1385–1398.

[48] O. Delgado-Mohatar, J. Fierrez, R. Tolosana, R. Vera-Rodriguez, Blockchain meets biometrics: Concepts, application to template protection, and trends, 2020, arXiv preprint arXiv:2003.09262.

[49] J.-H. Lee, BIDaaS: Blockchain based ID as a service, IEEE Access 6 (2017) 2274–2278.

[50] S. Kumi, R.K. Lomotey, R. Deters, A blockchain-based platform for data management and sharing, Procedia Comput. Sci. 203 (2022) 95–102.

[51] S. Rani, H. Babbar, S.H.A. Shah, A. Singh, Improvement of energy conservation using blockchain-enabled cognitive wireless networks for smart cities, Sci. Rep. 12 (1) (2022) 1–10.

[52] H. Rasouli, C. Valmohammadi, N. Azad, G. Abbaspour Esfeden, Proposing a digital identity management framework: A mixed-method approach, Concurr. Comput.: Pract. Exper. 33 (17) (2021) e6271.

[53] J.B. Bernabe, J.L. Canovas, J.L. Hernandez-Ramos, R.T. Moreno, A. Skarmeta, Privacy-preserving solutions for blockchain: Review and challenges, IEEE Access 7 (2019) 164908–164940.

[54] T. Li, H. Wang, D. He, J. Yu, Permissioned blockchain-based anonymous and traceable aggregate signature scheme for industrial internet of things, IEEE Internet Things J. 8 (10) (2020) 8387–8398.

[55] A.B. Haque, A.N. Islam, S. Hyrynsalmi, B. Naqvi, K. Smolander, GDPR compliant blockchains–a systematic literature review, IEEE Access 9 (2021) 50593–50606.

[56] S. Xu, X. Chen, Y. He, Evchain: An anonymous blockchain-based system for charging-connected electric vehicles, Tsinghua Sci. Technol. 26 (6) (2021) 845–856.

[57] D. Pennino, M. Pizzonia, A. Vitaletti, M. Zecchini, Efficient certification of endpoint control on blockchain, IEEE Access 9 (2021) 133309–133334.

[58] Š. Čučko, M. Turkanović, Decentralized and self-sovereign identity: Systematic mapping study, IEEE Access 9 (2021) 139009–139027.

[59] L. Stockburger, G. Kokosioulis, A. Mukkamala, R.R. Mukkamala, M. Avital, Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation, Blockchain: Res. Appl. 2 (2) (2021) 100014.

[60] B. Xiao, C. Jin, Z. Li, B. Zhu, X. Li, D. Wang, Proof of importance: A consensus algorithm for importance based on dynamic authorization, in: IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2021, pp. 510–513.

[61] K. Toyoda, K. Machi, Y. Ohtake, A.N. Zhang, Function-level bottleneck analysis of private proof-of-authority ethereum blockchain, IEEE Access 8 (2020) 141611–141621.

[62] I. Bentov, C. Lee, A. Mizrahi, M. Rosenfeld, Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y, ACM SIGMETRICS Perform. Eval. Rev. 42 (3) (2014) 34–37.

[63] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, On security analysis of proof-of-elapsed-time (poet), in: International Symposium on Stabilization, Safety, and Security of Distributed Systems, Springer, 2017, pp. 282–297.

[64] S.M.S. Saad, R.Z.R.M. Radzi, Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos), Int. J. Innov. Comput. 10 (2) (2020).

[65] B. Sriman, S. Ganesh Kumar, P. Shamili, Blockchain technology: Consensus protocol proof of work and proof of stake, in: Intelligent Computing and Applications, Springer, 2021, pp. 395–406.

[66] F.M. Benčić, I.P. Žarko, Distributed ledger technology: Blockchain compared to directed acyclic graph, in: 2018 IEEE 38th International Conference on Distributed Computing Systems, ICDCS, IEEE, 2018, pp. 1569–1570.

[67] X. Hao, L. Yu, L. Zhiqiang, L. Zhen, G. Dawu, Dynamic practical byzantine fault tolerance, in: 2018 IEEE Conference on Communications and Network Security, CNS, IEEE, 2018, pp. 1–8.

[68] I. Görkey, C. El Moussaoui, V. Wijdeveld, E. Sennema, Comparative study of Byzantine fault tolerant consensus algorithms on permissioned blockchains, 2020.

[69] X. Li, Y. Mei, J. Gong, F. Xiang, Z. Sun, A blockchain privacy protection scheme based on ring signature, IEEE Access 8 (2020) 76765–76772.

[70] D. Rountree, Federated Identity Primer, Newnes, 2012.

[71] S. Devi, S. Kotian, M. Kumavat, D. Patel, Digital identity management system using blockchain, 2022, Available at SSRN 4127356.

[72] C. Vasile, Is the body image so important? Physical identity in relation to gender and self esteem, Procedia-Soc. Behav. Sci. 203 (2015) 443–447.

[73] Z. Song, Y. Yu, The digital identity management system model based on blockchain, in: 2022 International Conference on Blockchain Technology and Information Security, ICBCTIS, IEEE, 2022, pp. 131–137.

[74] Q. Stokkink, J. Pouwelse, Deployment of a blockchain-based self-sovereign identity, in: 2018 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1336–1342.

[75] C. Allen, The path to self-sovereign identity, Life Alacrity (2016).

[76] S.K. Jena, R.C. Barik, Decentralized digital identity: A new form of secured identity using blockchain technology, in: International Conference on Information Systems and Management Science, Springer, 2022, pp. 93–102.

[77] S. Daas, M. Boughazi, M. Sedhane, B. Bouledjfane, A review of finger vein biometrics authentication system, in: 2018 International Conference on Applied Smart Systems, ICASS, IEEE, 2018, pp. 1–6.

[78] A. Now, National digital identity programmes: What's next, 2018.

[79] S. Kanwar, A. Reddy, M. Kedia, The Emerging Era of Digital Identities: Challenges and Opportunities for the G20, Asian Development Bank, 2022.

[80] N. Samion, A. Mohamed, Innovation of national digital identity: A review, Int. J. Adv. Trends Comput. Sci. Eng. 9 (1) (2020) 151–159.

[81] K. McCaskey, Hospital associations and the healthy habit of voting, 2021.

[82] K.M. Khan, J. Arshad, M.M. Khan, Secure digital voting system based on blockchain technology, Int. J. Electron. Gov. Res. (IJEGR) 14 (1) (2018) 53–62.

[83] D.D.F. Maesa, P. Mori, Blockchain 3.0 applications survey, J. Parallel Distrib. Comput. 138 (2020) 99–114.

[84] S.T. Alvi, M.N. Uddin, L. Islam, S. Ahamed, DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system, J. King Saud Univ.-Comput. Inf. Sci. 34 (9) (2022) 6855–6871.

[85] R. Rivera, J.G. Robledo, V.M. Larios, J.M. Avalos, How digital identity on blockchain can contribute in a smart city environment, in: 2017 International Smart Cities Conference, (ISC2), IEEE, 2017, pp. 1–4.

[86] statista, Urban population worldwide in 2022, by continent, 2022, https://www.statista.com/statistics/270860/urbanization-by-continent/.

[87] O. Lai, Top 7 smart cities in the world in 2023, Earth. Org (2023).

[88] B.K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology, Internet Things 11 (2020) 100227.

[89] X. Zhang, X. Chen, Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network, IEEE Access 7 (2019) 58241–58254.

[90] What supply chain data will look like in 2025, 2023.

[91] C.-H. Liao, X.-Q. Guan, J.-H. Cheng, S.-M. Yuan, Blockchain-based identity management and access control framework for open banking ecosystem, Future Gener. Comput. Syst. (2022).

[92] Identity verification in the insurance industry, 2022.

[93] A. Alkis, T. Kose, Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from europe, Comput. Hum. Behav. 137 (2022) 107412.

[94] M. Li, R. Wang, Chatbots in e-commerce: The effect of chatbot language style on customers' continuance usage intention and attitude toward brand, J. Retail. Consumer Serv. 71 (2023) 103209.

[95] I.J. Orji, F. Ojadi, U.K. Okwara, The nexus between e-commerce adoption in a health pandemic and firm performance: The role of pandemic response strategies, J. Bus. Res. 145 (2022) 616–635.

[96] W. Zhao, F. Hu, J. Wang, T. Shu, Y. Xu, A systematic literature review on social commerce: Assessing the past and guiding the future, Electron. Commer. Res. Appl. (2022) 101219.

[97] J.K. Adjei, S. Adams, I.K. Mensah, P.E. Tobbin, S. Odei-Appiah, Digital identity management on social media: Exploring the factors that influence personal information disclosure on social media, Sustainability 12 (23) (2020) 9994.

[98] S. Nykvist, M. Mukherjee, Who am i? Developing pre-service teacher identity in a digital world, Procedia-Soc. Behav. Sci. 217 (2016) 851–857.

[99] The-future-of-digital-identity-in-education, 2021.

[100] A. Haleem, M. Javaid, R.P. Singh, R. Suman, S. Rab, Blockchain technology applications in healthcare: An overview, Int. J. Intell. Netw. 2 (2021) 130–139.

[101] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: A blockchain-based privacy preserving scheme for large-scale health data, IEEE Internet Things J. 6 (5) (2019) 8770–8781.

[102] B. Alamri, K. Crowley, I. Richardson, Blockchain-based identity management systems in health IoT: A systematic review, IEEE Access 10 (2022) 59612–59629.

[103] J. Adler M, W. David, Paperless healthcare: Progress and challenges of an IT-enabled healthcare system, Bus. Horiz. 53 (2) (2010) 119–130.

[104] T.-T. Kuo, H.-E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Am. Med. Inform. Assoc. 24 (6) (2017) 1211–1220.

[105] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, J. Inf. Secur. Appl. 50 (2020) 102407.

[106] S. Niu, L. Chen, J. Wang, F. Yu, Electronic health record sharing scheme with searchable attribute-based encryption on blockchain, IEEE Access 8 (2019) 7195–7204.

[107] W. Wang, L. Wang, P. Zhang, S. Xu, K. Fu, L. Song, S. Hu, A privacy protection scheme for telemedicine diagnosis based on double blockchain, J. Inf. Secur. Appl. 61 (2021) 102845.

[108] B. Houtan, A.S. Hafid, D. Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020) 90478–90494.

[109] I.T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, K.N. Qureshi, Health-ID: a blockchain-based decentralized identity management for remote healthcare, in: Healthcare, vol. 9, (6) Multidisciplinary Digital Publishing Institute, 2021, p. 712.

[110] T.A. Syed, A. Alzahrani, S. Jan, M.S. Siddiqui, A. Nadeem, T. Alghamdi, A comparative analysis of blockchain architecture and its applications: Problems and recommendations, IEEE Access 7 (2019) 176838–176869.

[111] W. Zhao, N. Yang, G. Li, K. Zhang, Research on digital identity technology and application based on identification code and trusted account blockchain fusion, in: 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology, AINIT, IEEE, 2021, pp. 405–409.

[112] C.C. Agbo, Q.H. Mahmoud, Comparison of blockchain frameworks for healthcare applications, Internet Technol. Lett. 2 (5) (2019) e122.