Computer Communications 154 (2020) 223–235

Contents lists available at ScienceDirect

Computer Communications

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

Review

Blockchain platform for industrial healthcare: Vision and future opportunities

Ahmed Farouk [a,b,*], Amal Alahmadi [a], Shohini Ghose [a], Atefeh Mashatan [b]

[a] Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada
[b] School of Information Technology Management, Ryerson University, Toronto, Canada

ARTICLE INFO

Keywords:
Blockchain
Internet of Things
Industrial healthcare
Internet of Healthcare Things

ABSTRACT

Medical data has become an essential element for industrial healthcare. The growth in medical data is accompanied by the need to process it in a secure manner. As the infrastructure of this industry consists of connected devices and software applications that communicate with other IT systems, the industrial healthcare market will be greatly impacted by the use of blockchain and the Internet of Things (IoT). These technologies will improve processing efficiency, the creation of business opportunities, requirement regulation, information security, and transparency. While sharing electronic health records can assist in improving diagnosis accuracy, privacy and security preservation are imperative. In the network of IoT devices, that exchange involves sensitive medical data; patient monitoring has to be totally secured against privacy risks and attacks. Delays in treatment progress and emergency treatments could also result in medical data security and confidentiality violations.

Applying blockchain technology to the healthcare industry could improve information security management; healthcare data could be analyzed and communicated while preserving the privacy and security of the data. Here we critically look at how these two key technologies (blockchain and IoT) – especially blockchain – will impact the healthcare industry.

Contents

* Corresponding author at: Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada.
E-mail address: afarouk@wlu.ca (A. Farouk).

https://doi.org/10.1016/j.comcom.2020.02.058
Received 17 December 2019; Received in revised form 9 February 2020; Accepted 21 February 2020
Available online 27 February 2020

1. Introduction

Experts describe the Internet of Things as "Things" or smart devices (e.g., sensors, surveillance, drones, etc.) that have the capabilities of sensing, collecting, processing, and exchanging information with other interlinked devices [1]. These operations are done either locally or remotely through cloud-based systems. Industrial companies are increasingly adopting IoT technologies, and their industrial application has been named the Industrial Internet of Things (IIoT). IIoT enables convenience, an on-demand network of accessing a wide range of manufacturing resources, efficient service provision, and minimum management effort [2]. However, the cost of sensors and actuators is too high for some companies to adopt the platform, preventing the development of an IoT ecosystem [3].

Blockchain technology can be applied to the information sharing component of IoT. It provides a secure method for sharing vital information captured by IoT devices [4]. With this fact in mind, a platform called the Blockchain Platform for Industrial Internet of Things (BPIIoT) was created by a team of researchers focusing on decentralization and peer-to-peer exchanges on the platform. This platform would be an improvement on the current Cloud-Based Manufacturing (CBM) platform, as the BPIIoT enables legacy shop floor equipment to be integrated into a cloud environment, in turn, removing the financial barrier preventing the fostering of an industry wide ecosystem. This ecosystem could support transactions between the users across the manufacturing industry, e.g., logistics, healthcare, agriculture, energy, industry, supply chains [5,6].

Many healthcare organizations are already using the Internet of Healthcare Things (IoHT), from monitoring newborns to tracking inventory, and maintaining assets [7]. There are two distinct categories of use cases — one for clinical services and the other for support operations. In clinical settings, IoHT improves patient-centric activities with remote patient monitoring (RPM). This extends to clinical trials where IoHT closely tracks vital signs and any other indicators important to the study, such as blood-sugar levels and weight trends.

IoHT benefits support operations by enabling improved utilization of mobile medical assets, which will additionally reduce overall operational costs. This improvement is facilitated by equipment-centric sensors and data-collection capabilities that can reduce costs and give the staff real-time information about the usage rates and location of digital X-ray equipment, ventilators, and other movable resources. This allows equipment to be assigned more effectively and to be more quickly located when needed, saving care workers valuable time. Also, IoHT sensory inputs can show technicians the real-time performance status of expensive machines such as magnetic resonance imaging (MRI) equipment.

Healthcare decision-makers are also evaluating the combination of IoHT and augmented-reality (AR) technology to create digital twins of the technology [8]. Interactive and highly visual AR interfaces may digitally recreate sophisticated hospital equipment to give technicians and clinicians realistic, hands-on training opportunities.

One concern in implementing IoHT is the security and reliability of the servers used to connect the IoT devices and exchange critical medical data [9]. There is an obvious solution: a blockchain which is able to fully protect the process through decentralization and encryption [10]. Blockchain, is gaining attention because of its ability to generate and securely distribute permanent, unalterable records of transactions. Blockchain creates sequences of transactions, known as blocks, and records them in an ongoing chain of events that can be shared among members of a network. Because the blocks are protected using advanced cryptographic technology, the records are virtually impossible to change [11].

Research by the management consulting firm, Deloitte, determined that 35% of executives at health and life sciences companies are planning to implement blockchain within the next 12 months [12]. Blockchain has broad implications for the healthcare industry, including the ability to simplify and improve security and accuracy for cumbersome, inefficient processes [13]. Examples include streamlining claims adjudication, faster medical insurance enrollment and augmenting B2B activity across the healthcare value chain. Other blockchain opportunities include faster and more-efficient credentialing of employees.

The patient centric mechanisms of the healthcare industry make it suitable for blockchain and IoHT technologies [14]. The combination of the two technologies enables the secure, unalterable transmission of medical data. It will allow medical products to be traced through the supply chain, including medical devices and pharmaceutical products. Such traceability provides a valuable forensic trail if quality issues arise after the delivery of an item. Additionally, this traceability can enable organizations to expedite recalls by quickly determining the location of inventory across the supply chain.

We will discuss the unique features of blockchain and explore the prospective benefits and future directions of blockchain for the healthcare sector. The paper is organized as follows. Section 2 discusses blockchain technology and architecture, Section 3 introduces healthcare applications of blockchain, Section 4 discusses the future directions of blockchain for the healthcare sector and Section 5 is the paper's conclusion.

2. Blockchain technology and architecture

Blockchain technology provides the means for safe and secure transactions without having to trust a third party. This concept in blockchain is known as "trustlessness" — as long as each participant in a transaction can trust in the accuracy and integrity of the ledger, there is no additional requirement for trust between the parties [15]. Blockchain provides an immutable digital ledger that is widely distributed and peer-validated. It does not require currency to function appropriately and most enterprise-level blockchain applications require no particular currency, coin, or token. Blockchain can also be used as an event tracking system where announcements mark the occurrence of significant events, and those events can be made actionable through the use of smart contracts/chaincode; software programmed to respond to certain types of these events [16].

Guiding principles to design a Blockchain application should be a series of yes/no questions that you, your team, and your organization must agree on before starting solution design. The answers will define the default or assumed view or behavior of the solution. This does not mean your solution cannot or will not do the opposite, just that if doing the opposite is needed, it requires justification. Some examples of questions to build guiding principles include [17]:

- Do you need to store states? In other words, if no data to be stored, no need for blockchain.
- Are there multiple writers? In other words, if only one writer required, no need for blockchain.

2.1. History of blockchain

Satoshi Nakamoto described blockchain as the underlying technology in Bitcoin [18] which is the world's first and largest blockchain. Although blockchain started with Bitcoin, it has gained a lot of attention outside the realm of cryptocurrencies as well.

Bitcoin is a cryptocurrency that allows its users to stay highly anonymous through the use of public-key cryptography and cryptographic hashing. Using public-key cryptography, users store their bitcoin in a digital wallet [19]. This wallet contains the account's private key which is used to sign all transactions from that account. Any transactions presented by that account will be verified by the network using the corresponding public key for the account [20]. While common, anonymity is not a requirement of a blockchain platform [21]. Many platforms, especially those aimed at business and enterprise use, replace anonymity with identity to allow solutions architects and administrators the ability to define and enforce permissions and role-based access. In many

business scenarios, the anonymity and full-transparency that define public platforms are wholly undesirable, but some sort of permanent append-only ledger is still required.

For now, think of blockchain as the following simple process (See Fig. 1):

(1) An announcement is made before multiple witnesses (nodes, miners, validators, etc.).
(2) Each participant documents the details of the announcement in their own personal copy of the ledger.
(3) Announcements are grouped together in "blocks". Each participant regularly attempts to compare their current block with the current block of all the other participants on the network.
(4) If there is a version of the current block which the majority of participants have in common, this version is considered to be the truth. Any participant that does not have the same data as the majority will discard their copy, obtain a copy from another participant, and move on.

Significant Blockchain Dates (See Fig. 2):

There are several big companies and governments exploring blockchain technology, e.g., American Express, Microsoft. Here, we will summarize the most important events which represent breakthroughs in either the development of blockchain architecture or the industrial applications.

2009 — First Bitcoin Block Created [18,22].
2010 — Satoshi Disappears in December — Date of last public post.
2012 — Estonian Blockchain Technology — e-Estonia
2015 — Ethereum and Hyperledger both go live [23].
2018 — Demand for blockchain increases, 14 Open Jobs for every blockchain developer.
2019 — Walmart requires produce suppliers to be using a blockchain solution [24].
2021 — Dubai hosts all government operations and record-keeping operations on blockchain as part of the Smart Dubai 2021 initiative [25].

2.2. Blockchain components

Blockchain technology consists of several different components that work together. By combining these components, blockchain technology is able to offer certain promises to its users.

- *Ledger*
  At its most basic level, blockchain is an immutable record or digital ledger just like a traditional ledger (See Fig. 3). The ledger is often used to track and manage asset ownership. However, blockchain can be a simple record keeping device for all kinds of data — whether that data relates to asset ownership or not. Although blockchain is often described as a new and cutting-edge technology, the truth is blockchain is nothing more than a creative amalgamation of many old concepts, techniques, and methodologies. These components include ledgers, cryptography, group consensus, immutability and more. At the core of blockchain is a ledger — a record-keeping infrastructure which allows the keepers of a ledger to tell a story. This story usually revolves around the ownership and history of ownership of assets, although ledgers can be used to record just about any type of data imaginable [26].
- *Cryptography*
  Another core component of blockchain technology is cryptography — the study of how to communicate information in a confidential or authentic manner. In blockchain technology, we use cryptography to protect anonymity, to provide ledger immutability, and to validate claims that people make against assets tracked and managed on the blockchain. To chain blocks together today, all data in a block is run through a particular function called a "cryptographic hash". Cryptographic hashes create a unique output or identifier for a specific input. Therefore, the hash of each block will always be unique based upon the inputs. Attempting to change the data in a block will result in a hash or ID that no longer matches the original value recorded on the next block in the chain. To link or chain blocks of data together the header of the current block contains the hash of the last (validated) block. Changing the data on any block in a blockchain will result in a completely different hash, and the new hash will not match the hash in the next block header thus breaking the blockchain and invalidating all blocks linked to where the change was made. This makes blockchain technology tamper resistant and makes it highly censorship-resistant [27].
- *Peer-to-Peer Network*
  Blockchain makes extensive use of existing computer networking technology, specifically peer-to-peer network architectures. The same technology that serves as the backbone of our modern internet also underlies blockchain. Using peer-to-peer (P2P) network architecture increases redundancy and fault tolerance by removing single points of failure commonly found in typical client/server network architectures [18].
- *Assets*
  Finally, assets are a vital component of any blockchain solution. Assets are merely the items that we are keeping records about, the items that 'matter' in the context of a given solution or use case. Assets can be defined as anything that requires a record of ownership. This can be monetary, non-monetary, or just information, like health records, tickets to an event, an auto title, or a patent. Blockchain started as a record keeping system to record the transfer of digital "tokens" or "coins" such as Bitcoin and other cryptocurrencies. These coins and tokens required a way to keep a record of ownership. Out of the need to create a record of digital ownership, blockchain was born. In many ways blockchain seeks to supplement the internet of information we know today with the internet of the value we are designing for the future [28].
- *Merkle Trees*
  Blockchain uses Merkle trees for fast and efficient validation of data. Merkle trees summarize the entire set of data in a block by creating a root hash of that data. The root hash is found by repeatedly hashing pairs of child nodes of data until only one node is left. The last remaining child node is known as the Merkle root [29] (See Fig. 4).
- *Consensus Algorithms*
  Consensus is a way to ensure the nodes on the network verify the transactions and agree with their order and existence on the ledger. In the case of applications like a cryptocurrency, this process is critical to prevent double spending or other invalid data being written to the underlying ledger, which is a database of all the transactions. With consensus, there are different solutions that fit different situations. When deciding to use a specific consensus mechanism, one takes on an opportunity cost (e.g., security, speed, etc.). The main difference between consensus mechanisms is the way in which they delegate and reward the verification of transactions. Proof-of-work (PoW) and proof-of-stake (PoS) are the most common ones. There are other consensus mechanisms, especially in private and permissioned scenarios, for example in Hyperledger, where we do not need computationally intensive consensus mechanisms. There are more efficient alternatives for consensus if blockchain is not public. Here, we will summarize consensus algorithms.

  PoW
  Bitcoin implemented Byzantine Fault Tolerance through a validation system called PoW. Byzantine Fault Tolerance means that two nodes can communicate safely across a network, knowing that they are displaying the same data even if some peers crash

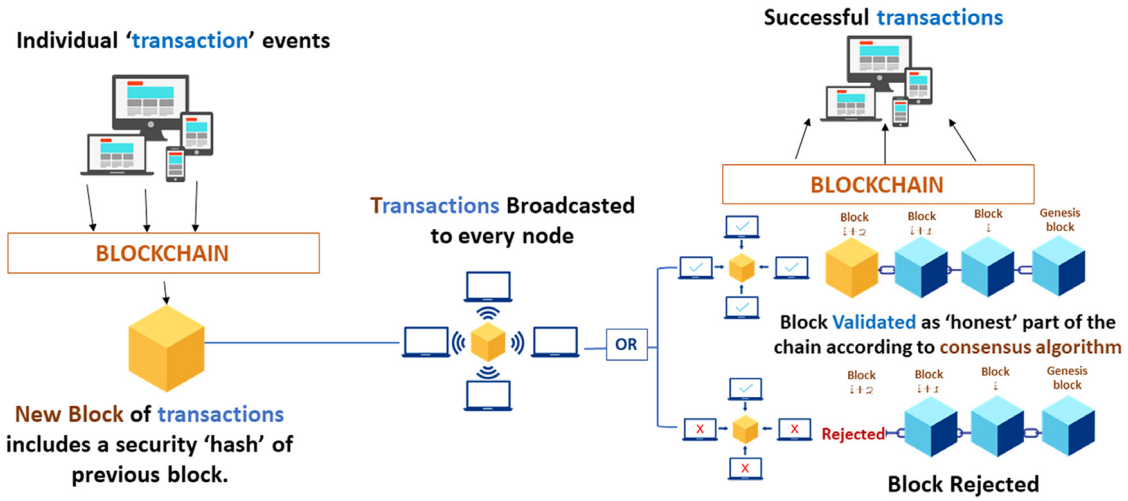

Fig. 1. The process of blockchain.

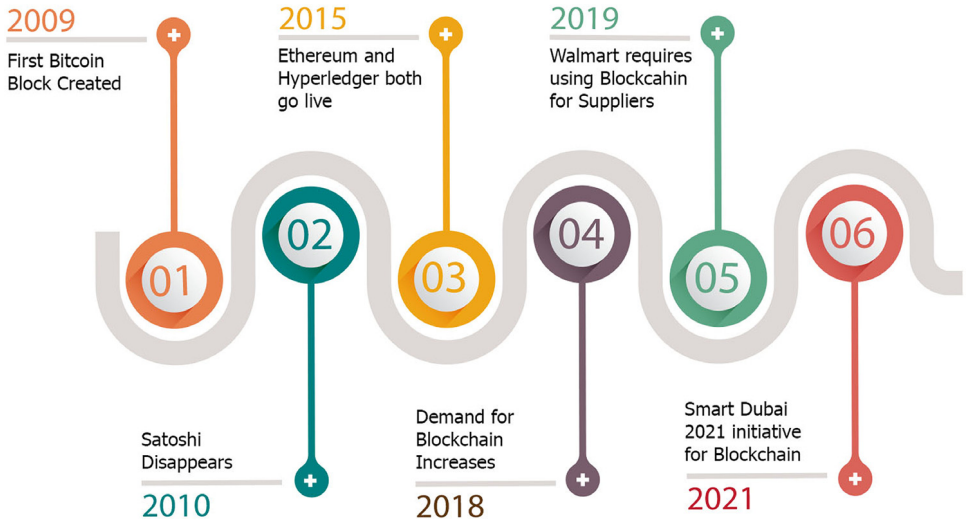

Fig. 2. Significant blockchain dates.

or attack the network maliciously [29]. The Byzantine Generals Problem is solvable if a certain percentage of the network is honest; at most 33% of the generals/network nodes can be traitors/malicious. Therefore, blockchain consensus algorithms are designed to be Byzantine Fault Tolerant — as long as 67% of users are benign, the network will reach consensus.

In PoW consensus, when a block is validated, each node competes to solve a guessing game problem to validate the block of data. This problem is non-computational and random guesses are most efficient. Nodes are called miners, and each miner attempts to guess a piece of data called the "nonce" to succeed in validating a block. All block data plus the current guess (nonce) are run through a cryptographic hash — if the resulting output matches the current level of "difficulty" (usually expressed as a fixed number of leading zeros) the miner has guessed the right answer [29].

This difficulty is adjusted by the network to keep the average block mining time consistent with the schedule defined by the platform. A nonce is the random data that is combined with the block data which will produce a hash output matching the current difficulty level of the blockchain. Any miner who thinks they have the correct answer will share it with all other miners. Miners will confirm the answer is correct by using the nonce with their block data to try to get a result that matches the difficulty setting. If 51% or more of the miners agree with the proposed nonce, the transactions on the winner's block are considered to be correct, and the miner with the correct answer will be rewarded (reward is given in platform tokens). If the majority of miners do not agree with the nonce, no reward is given and the work performed is a sunk cost as validation did not occur [30].

Any nodes that do not have the correct block data will reconcile by copying the validated block from neighboring nodes. PoW consensus creates a game theory incentive for each node to behave accurately and honestly; any dishonest participants will incur real-world costs in guessing the nonce for a zero percent chance of being rewarded with a payout. When transactions are broadcast to the blockchain network, it takes time for these transactions to be confirmed. This is because transactions are verified by groups. When a transaction is initiated, it is sent to a pool with other unconfirmed transactions.

Nodes group these transactions and then select blocks to be added to the chain. Each block is chained by including data from the previous block, and the number of blocks in the chain is the block height. If two blocks were to be added to the chain at the same time the chain with the greater block height is selected to be the primary chain. The height of a block refers to the number of

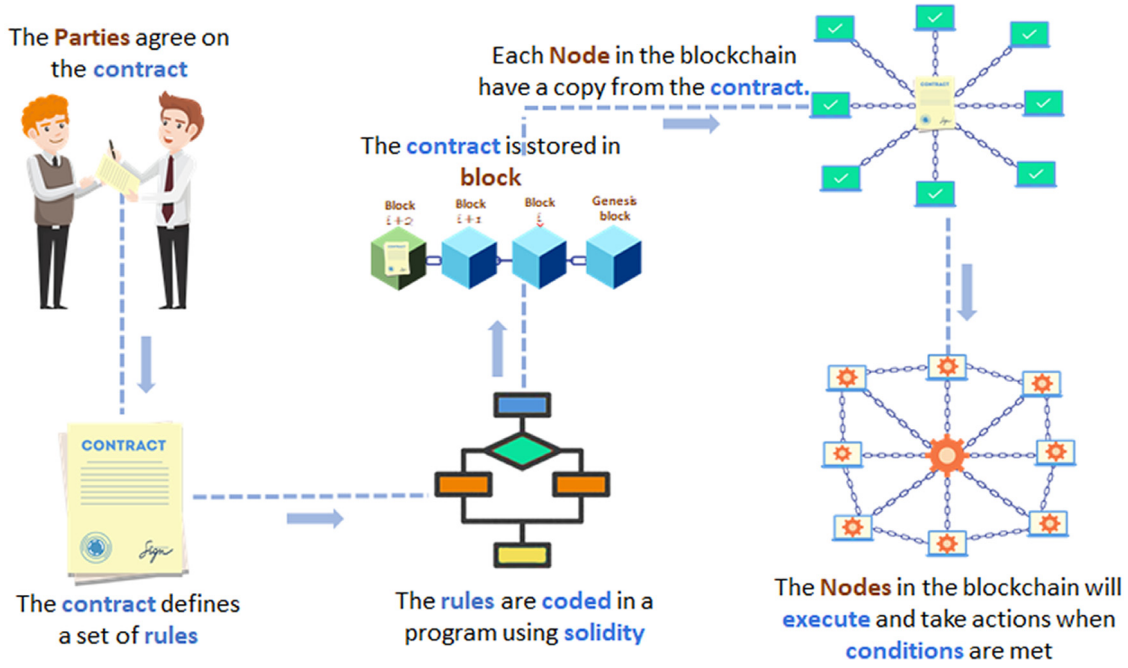

Fig. 3. Smart contract operation.

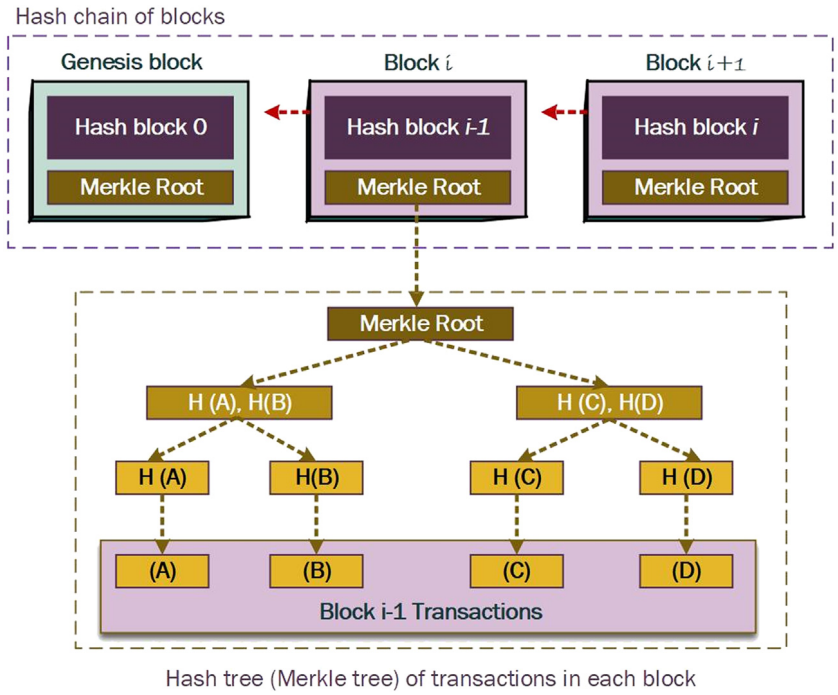

Fig. 4. Merkle tree.

blocks on the chain after the one in question. Block height is an indicator of the security of the data on the block; changing data in any block requires an attacker to change every subsequent block. The more of those blocks an attacker must alter, the more difficult it becomes to pull off an attack [30].

PoS

PoS is a newer Blockchain consensus system that has been proposed as an alternative to PoW consensus to overcome the scalability and cost concerns in PoW. PoS removes the guessing game from the validation of blocks so mining no longer requires powerful and specialized hardware. This vastly reduces the energy consumption of the network as well. PoS consensus uses a system where "validator" nodes each give or pay a stake in order to validate transactions. When it is time for group consensus, all who wish to participate lock up funds in a stake. A random node is selected and the hash of that node's block data is shown to all other participants. All other nodes wager on the validity of the block transactions. If the majority agree with the proposed block, the random node is rewarded as are all who wagered on that node.

If the majority disagree, the random node loses their stake, gets no reward, and a new node is randomly selected to share their block

data. The game theory incentive towards honesty and accuracy is maintained, only the mechanics of how it is enforced are changed. The key difference with this consensus is that no computing is ever performed during consensus, only wagering. Any kind of device can wager, regardless of computing power. Etheruem is using PoS as a consensus algorithm to verify the transactions of the blockchain.

Proof of Activity
This is a hybrid of PoW and PoS. Empty template blocks are mined (PoW) then filled with transactions which are validated via PoS.

Proof of Burn
Coins are "burned" by sending them to an address where they cannot be retrieved. The more coins burned, the better the chances of being selected to mine the next block.

Proof of Capacity
Hard drive space is staked to participate. The most space 'staked', the better the odds of being selected to mine the next block. The consensus algorithm here generates large datasets called 'plots' which consume storage.

Proof of Elapsed Time
This was created by Intel to run on their trusted execution environment. It is similar to PoW but far more energy efficient. The concern is this requires trust in Intel and can be viewed as a central authority.

Proof of Authority (PoA)
This uses a set of "authorities" which are nodes that are explicitly allowed to create new blocks and secure the Blockchain. This is a replacement for PoW but only for Private Blockchains. Nodes have to earn the right to become a validator/authority.

2.3. Types of blockchain

A blockchain solution can be measured and evaluated against the following three metrics:

- ***Public vs. Private***
  Who can write data to the blockchain? Public blockchains allow for large audiences or the public itself to add data to the ledger. Bitcoin is an example of a public blockchain network — there are no rules or permissions around who can trade Bitcoin. Anyone can buy, sell, or send Bitcoin to anyone else. A blockchain solution used to track how charitable donations are used by a non-profit would be an example of a private solution. In such a solution, only designated officers of the non-profit organization should be allowed to share metrics detailing how donations are allocated and spent [31].
- ***Permissioned vs. Permissionless***
  Permissionless platforms are solutions which are open, and in which the public have little need for permission or role-based access. These platforms do not have a native ability to track and manage identity and to subsequently define and enforce permissions based on that identity. This does NOT mean that you cannot build a permissioned solution on a permissionless platform, it merely means if you choose to do so, you are responsible for designing and implementing a method to track and manage identity and draw permissions against that identity. When developing a solution, a great way to determine what type of blockchain is needed is to determine if all participants are considered equal or should some have abilities or permissions that others do not. Answering this will help guide the decision to use either a permissioned or permission-less blockchain technology [31]. An example of a permissioned blockchain is an enterprise blockchain solution whereby only authorized employees have access. Digital currency, which can be exchanged and traded by all, is an example of a permission-less Blockchain.

2.4. Benefits and drawbacks of blockchain technology

Benefits of blockchain

Blockchain technology provides shared infrastructure between organizations in a business network. Since internal line of business (LOB) systems are the single source of truth for any question about an organization, what is the only source of truth for processes that span multiple organizations in a business network?. Blockchain is more secure compared to the traditional database since if the data is hacked, changed, or corrupted, we lose what the truth was. Blockchain has a high degree of security and an extensive permission set to verify and control who can access data in what circumstances. It also improves quality assurance services by tracking the origins of all supply chain components to mitigate the cost and control any damaged elements. An example is, food origin and/or safety recall using a smart contract as a replacement for middlemen operators [32,33].

Blockchain is redundant and highly fault-tolerant; if a single node were to lose track of the ledger, it would remain somewhere else on the network. To better understand fault tolerance, we can think of a group message. Everyone in the group message has a copy of the conversation; if someone wanted to delete something in the group chat, they would need to remove it on everyone's phone. Fault tolerance is especially useful when many people are participating. Another important advantage is tokenization, which opens new business possibilities and creates trade-able tokens backed by real-world value. Tokenization represents fractional asset ownership and digitization, for example, owning 1 car in 1 city, or owning 100 cars in 100 cities. Blockchain ensures consistent business processes across different organizations and automates the business process by employing a smart contract. Finally, blockchain removes intermediaries, which reduces cost and increases the efficiency of business operations. It allows the organizations to operate faster and reacts to changes in the business landscape much quicker than they could otherwise [32,33].

Drawbacks of Blockchain

Blockchain is no different from any other technology — the benefits it provides come at a cost. There are drawbacks to the blockchain that must be adequately considered to determine if blockchain is the right choice for an overall solutions architecture. Blockchain technology is extremely inefficient since it is very new technology (it is constantly changing and evolving, and there are a limited number of people trained in that area, and if available, at a high cost). Suitable use cases, best practices, and recommended patterns are still being developed [32,33].

Another serious drawback is the scalability of blockchain compared to conventional technology. The number of transactions blockchain is capable of processing is lower than that of Visa and other technologies. For blockchain to become competitive in terms of performance, it is necessary to increase the capacity by several orders of magnitude. Also, it can be tricky (even impossible) to get a complete "God Mode" view of the solution and its data; many platforms and toolsets are still pre-production releases, and may not be ready for heavy applications development [32,33].

Another important consideration for developing blockchain technology is energy consumption. The first consensus algorithm to mine bitcoin is PoW which consumes an estimated 7.67 gigawatts of electricity per year. This is similar to the energy used by countries such as Ireland (3.1 gigawatts) and Austria (8.2 gigawatts) [35]. Recently, many ways have been proposed to reduce the consumption of blockchain energy and the associated carbon footprint. These include (1) transferring from the PoW validation to PoS or PoA (i.e., the current estimated annual electricity consumption of Bitcoin is 72.78 TWH compared to 7.1 TWH for Ethereum, which is nearly 90% less) [36], (2) building blockchains that work differently from the ones that use so much energy and (3) focusing on sustainable ways to mine bitcoin (solar or wind energy).

Blockchain technology is affected by some vulnerabilities and attacks such as 51% attack and denial of service attack. A 51% attack is

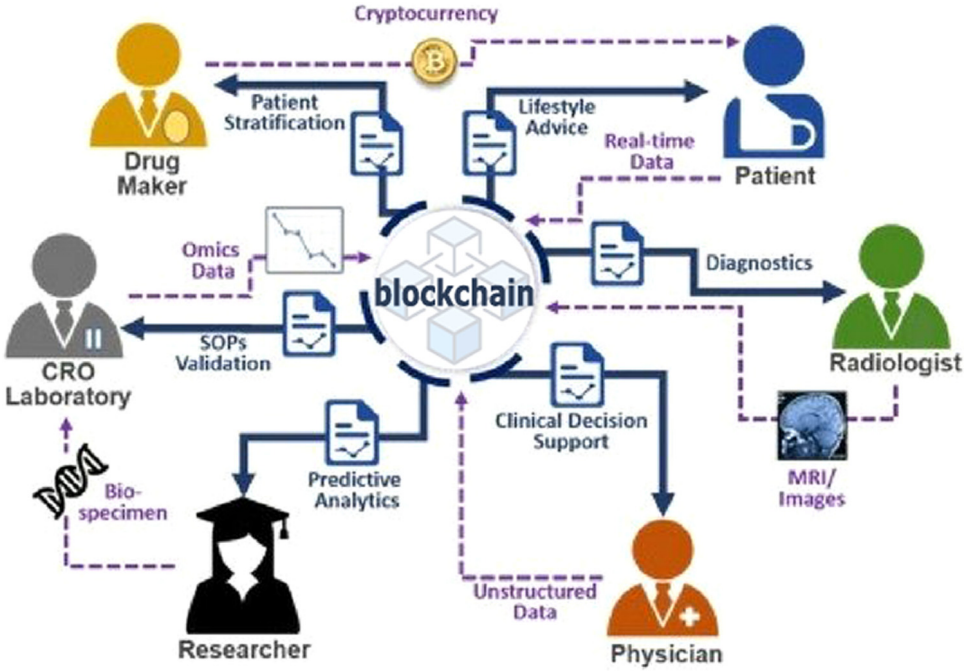

Fig. 5. Blockchain as platform for healthcare.

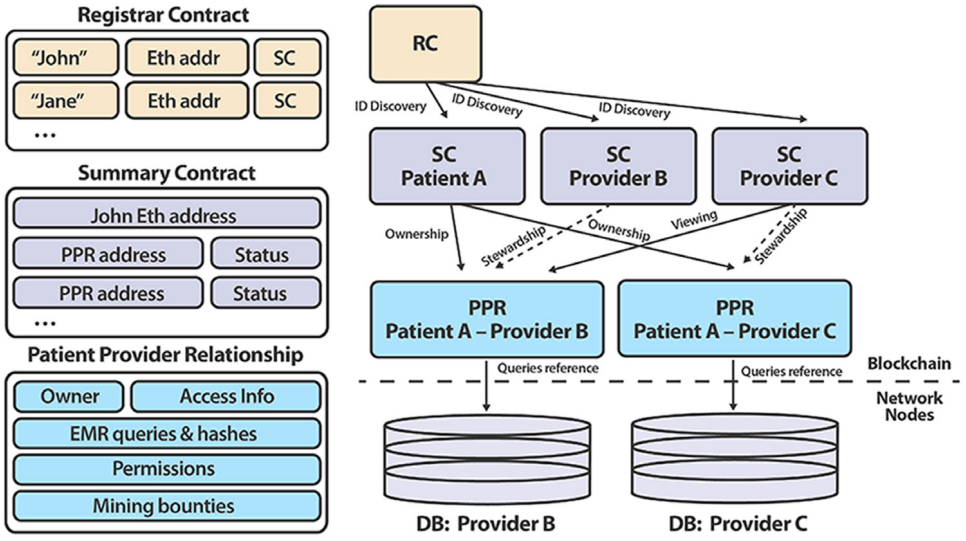

Fig. 6. Blockchain as structure for electronic medical records [34].

one of the most straightforward possible attacks against the blockchain since it takes advantage of the legitimate function of the consensus algorithm. In a Proof of Work blockchain, the state of the blockchain is determined by majority vote since, in the event of a divergent blockchain, the branch with the higher amount of work behind it wins. If an attacker controls 51% of a PoW blockchain's computational resources, they control the blockchain. Performing a 51% attack requires an attacker to purchase, rent, or steal enough computational resources to have more than the rest of a blockchain network put together. Once they control the blockchain, they can perform double-spend attacks. In a Denial of Service "DoS" attack, an attacker attempts to degrade a service's operations or make it completely non-functional. In traditional, centralized networks, DoS attacks targets the network's bottlenecks or single points of failure. Blockchains are designed to be decentralized and have no single points of failure, but DoS attacks can still be effective against them. The details of a DoS attack depend on the blockchain technology and where bottlenecks and single points of failure arise in its operations.

3. Blockchain technology in healthcare

Various blockchain architectures can improve the services provided for the healthcare system. Fig. 5 represents a blockchain combined with IoT technologies that enables the healthcare facilities to have efficient and accurate record management, which is critical. The entire process with the various components from the time of collecting real-time data of patients using IoT until providing a suitable drug that ensures the satisfaction of the patient is described. In [34], the blockchain is utilized as a structure to manage the electronic medical records of the patients (see Fig. 6). The structure is divided into three categories of contracts, which are Registrar Contract (RC), Patient–Provider Relationship Contract (PPR), and Summary Contract (SC). RC is used to transform

the identification of participants to their associated Ethereum address identity, and PPR is generated between two nodes in the system for storing and managing the medical records of patients. SC is responsible for retrieving the history of medical records for patients and indicating all the participant's previous and existing activities with other nodes in the system. A unique framework to maintain the exchange of health information that combines the health organizations, institutions and patients is illustrated in [37]. Furthermore, the structure involves universal, and\secure network infrastructure, provable identification and authentication of every participant, compatible representation of authorization to access electronic health information, and numerous other benefits (see Fig. 7).

There are many start-up companies that use blockchain for various healthcare solutions including managing patients' identity, supporting patient-centric healthcare, recording and tracking personalized medicine, building policies where patients could share their perspective on medical records and information with different stakeholders securely, and so on. A list of these companies is provided in Table 1. Also, there are mentoring and IoHT mechanisms for the healthcare industry in blockchain as shown in Tables 2, 3. Table 2 discusses the various solutions provided by blockchain technology for healthcare industry and what are the concepts employed to achieve these solutions. Also, it mentions the weak points of these solutions, and therefore identifies what should be improved for better healthcare services. This table thus provides guidelines for healthcare organizers to tailor the best blockchain solutions for their needs. Table 3 discusses different mechanisms for Internet of Medical Things "IoMT" for Healthcare Industry in the Blockchain and their disadvantages. We discuss below some examples of healthcare facilities and how blockchain functions benefit them.

3.1. A new intelligent healthcare system for the patient

In every organization or facility, there has to be a database that stores the numerous different data sets for the facility and its stakeholders. These databases are usually decentralized, meaning they contain a number of other databases working together. Decentralized databases are advantageous in information management, especially in the healthcare industry [3,38]. For a healthcare facility, for instance, where various types of specific information are input by a large number of users, the database can become ambiguous and complex. Blockchain technology could create a solution for cases where you find predestined fields of information like elderly care or chronic diseases. Significant challenges that occur include: wastage of time, resources, media disruptions, the sizable amount of health records, changes in communication criteria, conflicting IT interfaces, and incompatibility of information processes of the various stakeholders (physicians, practitioners, medical specialists, therapists, health centers, and research labs, etc.).

The Gem is a famous American start-up company that has been heavily involved in this field since it launched the Gem Health Network. It provides a platform/ecosystem that accommodates businesses, users, and experts in the healthcare industry [39]. In return, this has enabled users to get personalized and improved patient-centered care, while allowing the parties to interact efficiently. Blockchain technology, through the shared network created by Gem, solves most of these operational problems and unlocks wasted resources and related potential applications in healthcare [14]. The network provides its users the opportunity to be able to access the latest treatment information, while reducing instances of inaccurate or outdated information. The Gem Health Network also provides transparency to all of the stakeholders and enables the tracking of patients and the medical experts' interactions. In the past [38], a patient's medical treatment was visible only to the patient and healthcare practitioners, making the data confidential to those parties. Using blockchain technology, patient data will be available to the entire medical facility and stakeholders; a great benefit for future medical operations. Estonia and

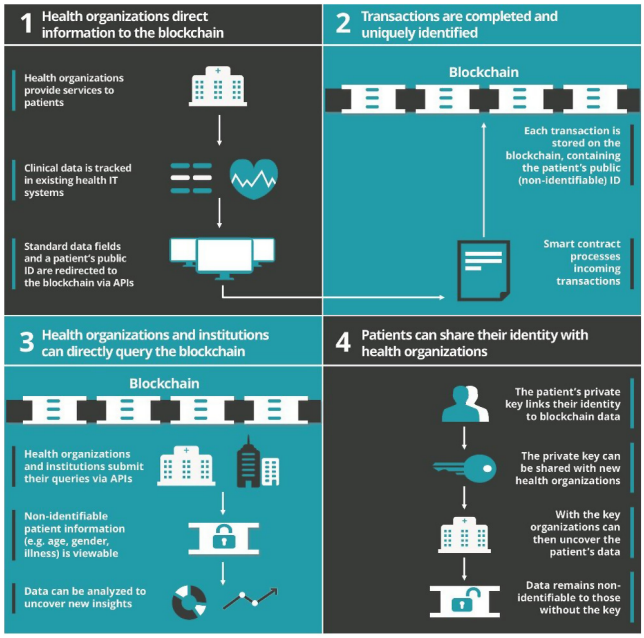

Fig. 7. Healthcare blockchain framework [37].

healthcare blockchain provider, Guardtime, proved that a full healthcare infrastructure could be under a blockchain, demonstrating that the incorporation of blockchain technologies and IoT is genuinely beneficial.

3.2. Enhancing the privacy of patients data

Stored information and patient-generated health data, is highly valuable [2]. Technological innovations in the healthcare industry have led to the development of wearable devices, including smartwatches, fitness bands, trackers and in-built body chips that monitor patient data. These wearable devices have contributed to an increase in the flow of data generated by patients. Blockchain technology offers solutions to the challenges that come with the increase in healthcare data [38].

Swiss digital health start-up Healthbank provides blockchain solutions, providing the following capabilities to its users and facilities:

- the sharing and handling of healthcare data and patient transactions;
- the retrieval of private patients' information including heart rate, sleep patterns, blood pressure, eating, consumed medicines, health history, and lifestyle habits;
- data saving and availability of data for medical research; and
- the storing and managing of facilities' data in a secure location.

Even with all of these capabilities, Healthbank still offers users sovereignty of their information; users are able to save their data and to make it available to medical researches. Individual medical data stored at Healthbank has proven to be of great significance to patients and donors. In addition, blockchain allows medical data accessible to researchers to be followed during the research, which could be of monetary value to the patient and a source of side income if they choose to share their data for research. Healthbank has contributed significantly to the health sector and medical research, assisting in the digitization of digital business and digital health initiatives.

Table 1
Summarized list of start-up companies involved in blockchain healthcare solutions.

Company name	Country based	Blockchain healthcare solutions
PokitDok	United States	• Patients' identity and claims management, plus real-time benefits verification (for treatment or pharmacy) [40].
Patientory	United States	• Access management for patients' healthcare information and connecting the patient's specific care team with the community to understand more about the patient's condition [41].
Guardtime	Estonia	• Security and scalability of various enterprise solutions. One of the most current implementations of Guardtime's blockchain is the E-government of Estonia [42].
Chronicled	United States	• The creation of a supply chain for the healthcare system with built-in trust, automation, and privacy [43].
Gem	United States	• Support for patient-centric healthcare and personalized medicine [14].
Nebula Genomics	United States	• Assurance of end-to-end security of the transmission of genomes [44].
Doc.AI	United States	• Healthcare data collection and management: the collection of health data of patients is encrypted by blockchain technology, After which, it can be embedded in machine learning algorithms to predict the health condition and required treatment of the patients [45].
Iryo	Slovenia	• The unification of health records from multiple sources [46].
Coral Health	United States	• Build policies where patients could securely and efficiently share their medical records and personal perspectives with different stakeholders. The proposed platform expedites a more general application of personalized medicine [47].
Medicalchain	Switzerland	• Securely save medical records and share them with various medical stakeholders. Records will only be shared only if access is permitted by patients. Medicalchain also provides telemedicine on its architecture: it enables patients to interact with their doctors by online conversations, and distributes their health report [48].
EncrypGen	United States	• Assist people in exchanging the data held in their DNA, reliably and securely, for cryptocurrency tokens [49].
Blockpharma	France	• Enhance the traceability of drugs, improving competition drug copying [50].
BurstIQ, Inc.	United States	• The capabilities of big data are unlocked using AI for data processing and blockchain for data protection [50].
Shivom	United States	• Provide clients with the means to participate in the Genomic information market by supporting the maintenance of data in spite of the time and place [51].
Bodyo	United Arab Emirates	• Measuring blood sugar, blood pressure, height, weight, muscle, fat mass, and many other factors with a health pod [52].
Exochain	United States	• Individuals are enabled to control how clinical trial researchers may interact with their medical data. This can potentially lead to increased quantity and quality of patients recruited for clinical trials, while at the same time giving individuals precision control over their medical information [53].
Novartis	Switzerland	• Using blockchain and IoTs, false medicines are recognized and temperatures are tracked with real-time perceptibility for every stakeholder in the process of a supply chain. This ensures that drugs are securely distributed [54].
Curisium	United States of America	• Secure computation technologies allow payers, providers, and life science companies to engage in patient-centric value-based contracts [55].
Healthcombix	United States of America	• Confidential human data asset management, disease prediction, and decentralized payment networks create robust new healthcare ecosystems [50].
SimplyVital Health	United States of America	• Obtain an understanding of what occurs to patients while they move out of the hospital [47].
Blockchain Health Co.	United States of America	• Honest communication linking the patients and medical research; patients can distribute their data directly to researchers [56].
Akiri	United States of America	• Creating trust by supporting protection, credentials, authentication, agreement, and identification in an architecture where the medical data will never be stored [46].

3.3. Enhancing drug credibility in the pharmaceutical industry

In addition to the discussed benefits of blockchain technology in healthcare operations involving patient data, blockchain technology adds value to the development and production of medical drugs [38, 68]. It can be used to closely monitor the processes involved in the research, development, production, sales, and availability of drugs.

In the world at large, the World Health Organization noted that at least ten percent of the drugs were counterfeit compared to thirty percent seen in developing countries. Counterfeit drugs usually contain the right active ingredient but lack the required percentage in terms of dosage, or they are poorly produced, which make them dangerous for human consumption [68]. Counterfeit drugs exist for cardiovascular disorders, cancer, contraceptives, and other prescription drugs, as well as lifestyle drugs (i.e.: supplements, stimulants, and weight reduction, etc.). To combat the production and distribution of counterfeit drugs, the Counterfeit Medicines Project, in partnership with Cisco, IBM, and Block, was created with the aim of ensuring that all drugs were marked with a timestamp indicating the day of production and origin which would be visible to the patients and healthcare facilities [68]. The project uses blockchain technology to achieve safety control: drug origins and ingredients would be detected early enough to sniff out any counterfeit drugs in the market.

4. Future directions of blockchain technology in the healthcare industry

4.1. Blockchain and the Internet of Things

IoT is the extended power of the internet beyond our current computers and smartphones to connect billions of smart objects. These devices include everything from smart healthcare wearables, to vehicles, smart homes, and sensors of all types that are revolutionizing the industry at all levels. As 95% of new technologies will depend on IoT, the estimated number of connected devices will increase to 50 billion by 2020, and it will become a part of our daily life [69]. Every single device and sensor in the IoT environment signifies a possible risk. IoT applications have been proposed in a wide variety of domains in healthcare to provide real time verifiable audits of operational data collected via medical devices. A medical device is a type of apparatus, appliance, software, material, and/or other article, which can be used alone or in combination with other devices specifically for diagnostic and/or therapeutic purposes [70].

Furthermore, many medical devices rely on machine-to-machine communication with limited or zero human intervention. This results in: (1) automated tasks, commands, and the distribution of information; (2) the interconnection and communication between medical devices; and (3) predictive maintenance of medical devices and intelligent

Table 2
Comparison of methods and tractability of some Blockchain mechanisms in the Healthcare industry.

Ref.	Solutions	Methods	Disadvantages
[57]	Traceability of consent in clinical trials	Proof of concept with time stamp	• Unsure whether the person signed the consent is the right one or not. • Patient concerns over the security of their data causing trepidation over joining the trial.
[58]	Tracking, securing, and management of clinical trials	Permissioned Ethereum, blockchain	• Lack of network scalability.
[59]	Monitoring and management of clinical data in multisite trials	Permissioned Hyperledger Fabric, blockchain	• The cost of network setup is high
[60]	Monitoring and detecting falsified, spurious and counterfeit drugs	Ethereum and Hyperledger Fabric, and Delegated PoS(DPoS) and practical Byzantine fault tolerance (PBFT)	• Simulated results differ from actual results. • It requires implementation plans and policies.
[61]	Inspection and tracking the data flow of drugs to prevent counterfeit drugs.	Consortium PoW	• Further analysis and tests for the regulations and system are required. • Consultation with key investors to perform a cost–benefit evaluation.
[62]	Analyze, trace, manage and verify medical data for clinical trial and precision medicine	General blockchain platform	• Lack of consistency
[63]	Track and deliver drugs in a secure way by combining patient information, drug dose, doctor information and prescription.	Smart contract with Permissioned Hyperledger Fabric, blockchain	• Scalability challenges: response time and system latency increases with the number users.

Table 3
Comparison of some IoMT mechanisms for Healthcare industry in the Blockchain.

Ref.	Solutions	Methods	Disadvantages
[64]	Management, monitoring and secure analysis of real-time medical data collected by sensors.	Consortium-managed blockchain, and the Ethereum Platform	• Insecure data transmission: information between the patient's sensor device and the blockchain nodes can be transmitted over public channels. • Management of keys will become a problem if the number of medical sensors increases. • Verification of real-time medical data can be delayed.
[65]	Securing, sharing, analyzing, and storage dyslexia data captured by multimedia IoT for mobile patients.	Permissioned Ethereum and Hyperledger private Blockchain.	• The recognition rate of dyslexic patterns has to increase. • Delay in uploading test components.
[66]	Ensuring security, storage, transparency and automation of structural health information	The proposed structure of blockchain is private and consortium-led, and Verification of PoW, and contain smart contracts for autonomous decision making.	• Delay for monitoring real-time data can cause security risks.
[67]	Developing a tamper-resistant mobile health platform for cognitive behavioral therapy.	Private Hyperledger Fabric, blockchain	• Vulnerable to attack (outdated codes and consensus algorithm)

manufacturing. There are also challenges associated with maintaining the growth of the IoT environment including: (1) transparency — IoT applications acting on behalf of users need transparency to allow users to verify the information; (2) trust — IoT applications require a level of trust adding financial overhead and risks that can subvert a centralized application; (3) longevity -long-lived IoT devices may outlive the infrastructure that supports them, exposing vulnerabilities or causing them to fail. The infrastructure lacks longevity primarily due to frequent technology changes and scalability. Blockchain can be integrated with IoT to solve these issues since blockchain can:

- chart the progression of wearables and medical devices, and the data they generate;
- keep devices safe for patients by providing a chain of custody and an immutable forensic trial;
- keep the generated data secure;
- empower patients by allowing them to know the status of their medical devices before they are received and that the data recorded is accessible only to whomever they give permission;
- remove a single point of failure and bottleneck of IoT architecture by moving towards a distributed IoT architecture rather than a centralized one;
- improve the security of IoT in healthcare organizations by employing blockchain architecture to perform identity authentication; and
- recognize medicines and track temperatures with real-time perceptibility for every stakeholder in the process of a supply chain, ensuring authentic, safe distribution of drugs.

4.2. Blockchain and quantum

Standard cryptographic functions are used to achieve security in blockchain technology. These functions are mostly computationally

secure which means breaking them needs substantial computing resources, which are not commonly available. The advent of the quantum computer enabling the decryption of data protected by traditional encryption algorithms will affect these technologies since a quantum computer can break the computational security of these functions. Compared to classical computing, quantum computers can harness unusual quantum properties such as superposition and quantum entanglement to efficiently process information [71–73]. Therefore, it is anticipated that applying quantum technologies in the smart environment will enable abilities and achievements that are, as yet, unrivaled by their classical equivalents. These improvements include computing speed, guaranteed security, and minimal storage requirements [74–76].

Quantum computing poses a significant threat to current cryptographic building blocks [77]. Current estimates predict quantum computing will be powerful enough to break commonly used security standards within the next few decades [78,79]. As such, it is essential for new devices and technologies to prepare for the world of quantum computing and the cyber-attacks that will subsequently be developed. A future implementation of blockchain technology must also be prepared for quantum computing, as any vulnerability could lead to tampering with the ledger and could undermine the entire system. Lastly, current public key cryptography infrastructure must change to become quantum-resistant, otherwise legacy infrastructure will be vulnerable. Recently demonstrated quantum-blockchain systems are based on information-theoretic secure authentication with the key being generated from quantum key distribution systems. But such a setup requires a pairwise connection between all the users [80]. Another way for ensuring quantum security is to use quantum secure direct communication for N users with authentication or quantum digital signatures. In these schemes, it is important to understand the limitations on the quantum network topology and number of dishonest (faulty) nodes on the network. After the authentication/signature processes is completed, one can use the standard family of broadcast protocols and find an optimal way for creating quantum-secured distributed information systems.

Innovations built on the principles of quantum mechanics hold the potential to affect health care on nearly every level, from diagnosis and treatment to data storage and transmission. The principles of quantum blockchain technology will improve the security of medical data and prevent the data from being leaked. Furthermore, we can more quickly sequence DNA and solve other big data problems in health care using techniques such as laser microscopy that is built on the principles of quantum mechanics and using quantum computers. This opens up the possibility of personalized medicine based on individuals' unique genetic makeup

4.3. Blockchain and artificial intelligence

Recent advances in deep learning based on artificial neural networks have enabled unprecedented improvements in various tasks, e.g., speech recognition [81], image recognition [82], drug discovery [83] and gene analysis for cancer research [84,85]. To achieve even higher accuracy, a massive amount of data must be fed to deep learning models, which would require excessively high computational overhead. This problem can be solved by employing distributed deep learning techniques which have been investigated extensively in recent years.

In order to generate good models in machine learning, a large amount of data is required. Broad data increases the overall throughput which helps make a more generalized conclusion, and produces a more efficient and reliable system. Incorporating blockchain databases in machine learning could lead to safer data, and better machine learning models. One of the critical tasks is to combine deep learning and blockchain in the healthcare ecosystem: the enhanced availability of data and current progress in artificial intelligence can lead to the unique possibilities in healthcare but also significant challenges for patients, developers, providers, and regulators. New deep learning and substitution learning methods are adapting and analyzing all data about patients. An example is the converting of standard facial images and videos into robust sources of data for predictive analytics. A blockchain-enabled decentralized individual medical records ecosystem could facilitate innovative strategies for drug development, biomarker improvement, and secure healthcare. A marketplace employing blockchain and deep learning techniques to safely distribute data may solve the challenges faced by regulators and pass the power for protecting private data including medical reports back to the people. Recently, the Joint Research Centre from the European Commission demonstrated the potential to improve healthcare services in Africa through the use of artificial intelligence and blockchain technology called "CareAi" [86].

4.4. Blockchain testing

Blockchain applications for the healthcare industry represent one of the areas of blockchain functionality testing. The purpose of testing is to ensure that the developed business network fits the desired requirements of the organization and prevents the various types of bugs. These bugs can be in the form of (1) business logic — something is not right according to business requirements, (2) security — the code is vulnerable to some security exploits, (3) regression — some code updates caused existing features to break, (4) performance — the code is slow, or some actions execute extra functions, (5) accessibility — the code does not meet specifications for accessibility (Americans with Disabilities Act), (6) UI bugs — user interface does not meet the design specification and (7) integration — two or more components do not work together as expected

The testing procedure is divided into three main processes. First, is integration testing which depends on the developer platform to integrate the current system with the blockchain. It is evident that the primary obligation is to guarantee compatibility and accurate communication. Second, is the testing of node functionality which is important since the peer-to-peer architecture is distributed through a network of nodes employing a particular protocol for authentication. Every node must be individually checked and tested for its perspective function. Third, is the testing of the performance of the blockchain which should be tested for all aspects related to the network latency. The network latency depends on the size of the block, the number of participating nodes, the expected size of the transaction and the access time of the queries. Performance testing should identify needed controls for using a cloud environment like auto-scaling for chaotic circumstances. Finally, the security of blockchain needs to be tested against possible attacks. This checks the integrity of the network by ensuring all transmitted transactions are encrypted, and the access control lists (ACL) are performed correctly. ACL are a sequence of rules providing a set of permissions to participating nodes of the blockchain (i.e.: policies allowing patients to securely share their medical records with different stakeholders).

The proposed platform expedites a more general application of personalized medicine. Medical data could be shared with the following steps: (1) the patient's private key links their identity to blockchain data; (2) the private key can be shared with new health organizations; and (3) with the key, organizations can then unlock the patient's data.

4.5. Blockchain, Big Data management and analytics

Blockchain is one of the current promising solutions for dealing with a large volume of medical data, and its efficiency has been proved in various areas of medical research. Big data in the healthcare industry is essential as it is used in the prediction of diseases, inhibition of comorbidities, death, and medical expenses. In many countries, medical data is compiled in a large database where the generated information could be adopted for the treatment and management of diseases. But,

there are several difficulties in implementing big data in healthcare, particularly with respect to privacy, protection, standards, governance, the combination of data, data adaptation, data analysis, incorporation of technology, etc. It is necessary that these difficulties are addressed before big data can be implemented successfully in healthcare. Overcoming these difficulties, and improving the processing performance of medical big data could be achieved by deploying blockchain technology in healthcare organizations. Blockchain can secure, manage and analyze medical big data by:

- storing the medical records of patients and making sure it was not corrupted or changed accidentally or by any malicious participants;
- analyzing medical big data by tracking the performed transactions over the blockchain network.
- managing access to patients' health information and connecting patients' specific healthcare team with the medical community;
- ensuring reliable and secure end-to-end security of genome data; and
- the collection and management of healthcare data, encrypted by blockchain technology, which can be used in machine learning algorithms to predict health conditions and treatment.

5. Conclusion

Deploying blockchain technology in the healthcare industry and research has its advantages and disadvantages. It will improve the security, management, and analysis of healthcare big data. Since healthcare data is sensitive and requires real-time processing, especially in emergencies, we have to choose the type of consensus algorithm, the working platform, and type of blockchain carefully. Another concern is to make sure that the right access to blockchain is developed correctly to avoid the leakage of patient personal information. Furthermore, healthcare executives planning IoHT and blockchain implementations should consider two supplemental technologies that can speed up adoption and time to value. The first is the use of AI, which aggregates and then extracts insights by recognizing patterns and correlations across large volumes of data. Hybrid clouds are the second key to a strong IoHT and blockchain foundation. These new hybrid cloud-at-customer models provide highly scalable public-cloud applications and services while keeping clinical data behind enterprise firewalls to conform organizational and regulatory requirements.

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.

References

[1] Partha Pratim Ray, Mithun Mukherjee, Lei Shu, Internet of Things for disaster management: State-of-the-art and prospects, IEEE Access 5 (2017) 18818–18835.

[2] M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, A systematic review of the use of blockchain in healthcare, Symmetry 10 (10) (2018) 470.

[3] Y. Lu, Blockchain and the related issues: a review of current research topics, J. Manag. Anal. 5 (4) (2018) 231–255.

[4] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the Internet of Things, IEEE Access 4 (2016) 2292–2303.

[5] D. Liu, A. Alahmadi, J. Ni, X. Lin, X. Shen, Anonymous reputation system for iiot-enabled retail marketing atop pos blockchain, IEEE Trans. Ind. Inf. 15 (6) (2019) 3527–3537.

[6] A. Ali, S. Latif, J. Qadir, S. Kanhere, J. Singh, J. Crowcroft, Blockchain and the future of the internet: A comprehensive review, 2019, arXiv preprint arXiv:1904.00733.

[7] S.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.S. Kwak, The Internet of Things for health care: a comprehensive survey, IEEE Access 3 (2015) 678–708.

[8] M. Kranz, Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry, John Wiley & Sons, 2016.

[9] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[10] G. Zyskind, O. Nathan, Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180–184.

[11] W. Mougayar, The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology, John Wiley & Sons, 2016.

[12] Y. Chen, S. Ding, Z. Xu, H. Zheng, S. Yang, Blockchain-based medical records secure storage and medical service framework, J. Med. Syst. 43 (1) (2019) 5.

[13] T. McGhin, K.K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: Research challenges and opportunities, J. Netw. Comput. Appl. (2019).

[14] M. Mettler, Blockchain technology in healthcare: The revolution starts here, in: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services, Healthcom, IEEE, 2016, pp. 1–3.

[15] Z. Zheng, S. Xie, H.N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.

[16] L.S. Sankar, M. Sindhu, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS, IEEE, 2017, pp. 1–5.

[17] K. Wüst, A. Gervais, Do you need a blockchain? in: 2018 Crypto Valley Conference on Blockchain Technology, CVCBT, IEEE, 2018, pp. 45–54.

[18] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2019, Manubot.

[19] R. Böhme, N. Christin, B. Edelman, T. Moore, Bitcoin: Economics, technology, and governance, J. Econ. Perspect. 29 (2) (2015) 213–238.

[20] T.T. Motohashi, T. Hirano, K. Okumura, M. Kashiyama, D. Ichikawa, T. Ueno, Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation, J. Med. Internet Res. 21 (5) (2019) e13385.

[21] G. Zyskind, O. Nathan, Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180–184.

[22] S. Nakamoto, Bitcoin Open Source Implementation of P2P Currency, P2P foundation, 2009, p. 18.

[23] G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, 15, Ethereum project yellow paper, 2014, pp. 1–32.

[24] J. Al-Jaroodi, N. Mohamed, Blockchain in industries: A survey, IEEE Access 7 (2019) 36500–36515.

[25] A.B. Bishr, Dubai: A city powered by blockchain, Innov. Technol. Gov. Glob. 12 (3–4) (2019) 4–8.

[26] M. Pilkington, Blockchain technology: principles and applications, in: Research Handbook on Digital Transformations, Edward Elgar Publishing, 2016.

[27] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data, BigData Congress, IEEE, 2017, pp. 557–564.

[28] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc, 2015.

[29] I.C. Lin, T.C. Liao, A survey of blockchain security issues and challenges, IJ Netw. Secur. 19 (5) (2017) 653–659.

[30] C. Cachin, M. Vukolić, Blockchain consensus protocols in the wild, 2017, arXiv preprint arXiv:1707.01873.

[31] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, P. Rimba, et al., A taxonomy of blockchain-based systems for architecture design, in: 2017 IEEE International Conference on Software Architecture, ICSA, IEEE, 2017, pp. 243–252.

[32] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, V. Santamaria, To blockchain or not to blockchain: That is the question, IT Prof. 20 (2) (2018) 62–74.

[33] M. Niranjanamurthy, B.N. Nithya, S. Jagannatha, Analysis of blockchain technology: pros, cons and SWOT, Cluster Comput. 22 (6) (2019) 14743–14757.

[34] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data, in: Proceedings of IEEE open & big data conference, vol. 13, 2016, p. 13.

[35] A. De Vries, Bitcoin's growing energy problem, Joule 2 (5) (2018) 801–805.

[36] Digiconomist, Ethereum energy consumption index (beta), 2019, [Online]. Available: https://digiconomist.net/ethereum-energy-consumption. (Accessed Dec. 2, 2019).

[37] R. Krawiec, D. Housman, M. White, M. Filipova, F. Quarre, D. Barr, L. Tsai, et al., Blockchain: Opportunities for health care, in: Proc. NIST Workshop Blockchain Healthcare, 2016, pp. 1–16.

[38] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. 40 (10) (2016) 218.

[39] M. Liu, F.R. Yu, Y. Teng, V.C. Leung, M. Song, Performance optimization for Blockchain-enabled industrial Internet of Things (IIOT) systems: A deep reinforcement learning approach, IEEE Trans. Ind. Inf. 15 (6) (2019) 3559–3570.

[40] T. Dunlevy, T.C. Tanner Jr., D. Gosnell, T.D. Whitmire IV, U.S. Patent Application No. 14/884, 703, 2017.

[41] C. McFarlane, M. Beer, J. Brown, N. Prendergast, Patientory: A Healthcare Peer-to-Peer EMR Storage Network V1, Entrust Inc., Addison, TX, USA, 2017.

[42] A. Buldas, A. Kroonmaa, R. Laanoja, Keyless signatures' infrastructure: How to build global distributed hash-trees, in: Nordic Conference on Secure IT Systems, Springer, Berlin, Heidelberg, 2013, pp. 313–320.

[43] K.A. Clauson, E.A. Breeden, C. Davidson, T.K. Mackey, Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare, 2018, Blockchain in healthcare today.
[44] H.I. Ozercan, A.M. Ileri, E. Ayday, C. Alkan, Realizing the potential of blockchain technologies in genomics, Genome Res. 28 (9) (2018) 1255–1263.
[45] F. Corea, The convergence of AI and blockchain, in: Applied Artificial Intelligence: Where AI Can Be Used in Business, Springer, Cham, 2019, pp. 19–26.
[46] G.J. Katuwal, S. Pandey, M. Hennessey, B. Lamichhane, Applications of blockchain in healthcare: current landscape & challenges, 2018, arXiv preprint arXiv:1812.02776.
[47] C. Monteil, Blockchain and health, in: Digital Medicine, Springer, Cham, 2019, pp. 41–47.
[48] S. Armstrong, Bitcoin technology could take a bite out of NHS data problem, BMJ 361 (2018) k1996.
[49] M. Shabani, Blockchain-based platforms for genomic data sharing: a decentralized approach in response to the governance problems? J. Am. Med. Inform. Assoc. 26 (1) (2019) 76–80.
[50] K. Yaeger, M. Martini, J. Rasouli, A. Costa, Emerging blockchain technology solutions for modern healthcare infrastructure, J. Sci. Innov. Med. 2 (1) (2019).
[51] S. Namasudra, G.C. Deka, R. Bali, Applications and future trends of DNA computing, Adv. DNA Comput. Crypt. 18 (2018) 1–192.
[52] Bodyo, [Online] Available: https://bodyo.com/. (Accessed Dec. 1, 2019).
[53] Exochain, [Online]. Available: https://exochain.com/. (Accessed Dec. 1, 2019).
[54] M. Scorringe, More than medicine: Pharmaceutical industry collaborations with the UK NHS, in: Sustainable Entrepreneurship, Springer, Cham, 2019, pp. 111–137.
[55] Curisium, [Online]. Available: https://www.curisium.com/. (Accessed Dec. 1, 2019).
[56] A.L. Duca, C. Bacciu, A. Marchetti, How distributed ledgers can transform healthcare applications, Blockchain Eng. 25 (2016).
[57] M. Benchoufi, R. Porcher, P. Ravaud, Blockchain protocols in clinical trials: transparency and traceability of consent, F1000Research 6 (2017).
[58] T. Nugent, D. Upton, M. Cimpoesu, Improving data transparency in clinical trials using blockchain smart contracts, F1000Research 5 (2016).
[59] O. Choudhury, N. Fairoza, I. Sylla, A. Das, A blockchain framework for managing and monitoring data in multi-site clinical trials, 2019, arXiv preprint arXiv:1902.03975.
[60] P. Sylim, F. Liu, A. Marcelo, P. Fontelo, Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention, JMIR Res. Protoc. 7 (9) (2018) e10163.
[61] J.H. Tseng, Y.C. Liao, B. Chong, S.W. Liao, Governance on the drug supply chain via gcoin blockchain, Int. J. Environ. Res. Public Health 15 (6) (2018) 1055.
[62] Z. Shae, J.J. Tsai, On the design of a blockchain platform for clinical trial and precision medicine, in: 2017 IEEE 37th International Conference on Distributed Computing Systems, ICDCS, IEEE, 2017, pp. 1972–1980.
[63] Z. Shae, J.J. Tsai, On the design of a blockchain platform for clinical trial and precision medicine, in: 2017 IEEE 37th International Conference on Distributed Computing Systems, ICDCS, IEEE, 2017, pp. 1972–1980.
[64] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (7) (2018) 130.
[65] M.A. Rahman, E. Hassanain, M.M. Rashid, S.J. Barnes, M.S. Hossain, Spatial blockchain-based secure mass screening framework for children with dyslexia, IEEE Access 6 (2018) 61876–61885.
[66] B.W. Jo, R.M.A. Khan, Y.S. Lee, Hybrid blockchain and internet-of-things network for underground structure health monitoring, Sensors 18 (12) (2018) 4268.
[67] D. Ichikawa, M. Kashiyama, T. Ueno, Tamper-resistant mobile health using blockchain technology, JMIR mHealth uHealth 5 (7) (2017) e111.
[68] P. Zhang, D.C. Schmidt, J. White, G. Lenz, Blockchain technology use cases in healthcare, in: Advances in computers, vol. 111, Elsevier, 2018, pp. 1–41.
[69] G. Davis, 2020: Life with 50 billion connected devices, in: 2018 IEEE International Conference on Consumer Electronics, ICCE, IEEE, 2018, p. 1.
[70] J.P. Davim (Ed.), The Design and Manufacture of Medical Devices, Elsevier, 2012.
[71] A.F. Metwaly, M.Z. Rashad, F.A. Omara, A.A. Megahed, Architecture of multicast centralized key management scheme using quantum key distribution and classical symmetric encryption, Eur. Phys. J. Spec. Top. 223 (8) (2014) 1711–1728.
[72] A. Farouk, M. Zakaria, A. Megahed, F.A. Omara, A generalized architecture of quantum secure direct communication for N disjointed users with authentication, Sci. Rep. 5 (1) (2015) 1–17.
[73] M. Naseri, M.A. Raji, M.R. Hantehzadeh, A. Farouk, A. Boochani, S. Solaymani, A scheme for secure quantum communication network with authentication using GHZ-like states and cluster states controlled teleportation, Quantum Inf. Process. 14 (11) (2015) 4279–4295.
[74] N.R. Zhou, J.F. Li, Z.B. Yu, L.H. Gong, A. Farouk, New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states, Quantum Inf. Process. 16 (1) (2017) 4.
[75] A. Farouk, J. Batle, M. Elhoseny, M. Naseri, M. Lone, A. Fedorov, M. Abdel-Aty, et al., Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states, Front. Phys. 13 (2) (2018) 130306.
[76] H. Abulkasim, A. Farouk, H. Alsuqaih, W. Hamdan, S. Hamad, S. Ghose, Improving the security of quantum key agreement protocols with single photon in both polarization and spatial-mode degrees of freedom, Quantum Inf. Process. 17 (11) (2018) 316.
[77] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134.
[78] M. Mosca, Cybersecurity in an era with quantum computers: will we be ready? IEEE Secur. Priv. 16 (5) (2018) 38–41.
[79] B. Bauer, D. Wecker, A.J. Millis, M.B. Hastings, M. Troyer, Hybrid quantum–classical approach to correlated materials, Phys. Rev. X 6 (3) (2016) 031045.
[80] E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.K. Fedorov, et al., Quantum-secured blockchain, Quantum Sci. Technol. 3 (3) (2018) 035004.
[81] R. Miikkulainen, J. Liang, E. Meyerson, A. Rawal, D. Fink, O. Francon, B. Hodjat, et al., Evolving deep neural networks, in: Artificial Intelligence in the Age of Neural Networks and Brain Computing, Academic Press, 2019, pp. 293–312.
[82] A. Elola, E. Aramendi, U. Irusta, A. Picón, E. Alonso, P. Owens, A. Idris, Deep neural networks for ECG-based pulse detection during out-of-hospital cardiac arrest, Entropy 21 (3) (2019) 305.
[83] N. Stephenson, E. Shane, J. Chase, J. Rowland, D. Ries, N. Justice, R. Cao, et al., Survey of machine learning techniques in drug discovery, Curr. Drug Metab. 20 (3) (2019) 185–193.
[84] K.K. Wong, R. Rostomily, S.T. Wong, Prognostic gene discovery in glioblastoma patients using deep learning, Cancers 11 (1) (2019) 53.
[85] O. Klein, F. Kanter, H. Kulbe, P. Jank, C. Denkert, G. Nebrich, S. Darb-Esfahani, et al., MALDI-imaging for classification of epithelial ovarian cancer histotypes from a tissue microarray using machine learning methods, Proteom. Clin. Appl. 13 (1) (2019) 170018.
[86] A. Duricic, CareAI: A solution for African healthcare? 2018, [Online] Available: https://mastersofmedia.hum.uva.nl/blog/2018/09/23/careai-a-solution-for-african-healthcare/. (Accessed Dec. 1, 2019).