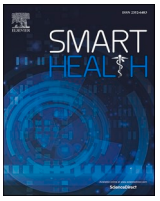
Smart Health 23 (2022) 100223

Contents lists available at ScienceDirect

Smart Health

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



Blockchain technology in the future of healthcare

Quazi Mamun

School of Computing, Mathematics and Engineering, Charles Sturt University, NSW, Australia

ARTICLE INFO

Keywords:
Healthcare
Blockchain
eHR
Use-case

ABSTRACT

The overarching vision of Blockchain technology for the future would be to address many problems affecting the Healthcare industry today with the creation of a shared archive of health-related information for physicians and patients independent of their electronic diagnosis, improving safety and secrecy, investing fewer resources on the medical staff and more money on patient care. It is only the beginning of what is likely that a Blockchain movement has come out of cryptocurrency and has made its path to the medical industry. Within the sense of intelligent health, Blockchain could have distinctive benefits from a context-aware viewpoint, especially where people and society as a whole can profit from effective and customised solutions. In this paper, we discuss numerous use cases of Blockchain in the healthcare industry. The symbiotic relationship between Blockchain and intelligent health is discussed. Additionally, we address many obstacles for integrating Blockchain-based applications in the health sector and several future research prospects.

1. Introduction

Among the horizontal innovations in healthcare, like the Internet, Cloud computing, or image processing, Blockchain is considered the next horizontal innovation (Angraal et al., 2017). In simple terms, a Blockchain is a time-stamped series of permanent data records managed by a cluster of computers that are not owned by an entity. Each block of this information (e.g. block) is secured by cryptographic principles (e.g. chain) and is bound to each other. The reason the Blockchain is valued so much is: (i) a single entity does not own it, thus, distributed (ii) the data is cryptographically secure in the Blockchain (iii) The Blockchain is irreversible, so that no one can alter the details in the Blockchain and (iv) the transparency of Blockchain-data can be monitored at any time. (Ahram et al., 2017).

The question arises, how Blockchain can bring benefits to healthcare. Simply saying, the healthcare industry can significantly benefit from Blockchain technology. Blockchain technology can help healthcare experts and the overall healthcare industry improve performance, patient data transparency (Dagher et al., 2018), tracking and accountability, and reduce costs. In addition, a range of Blockchain products can be tailored to address various healthcare applications. This list includes secure management of electronic health records (EHRs), patient consent management (Benchoufi et al., 2017), drug traceability, data security in clinical trials, incentivisation through micropayments, etc.

In this paper, we discuss various use cases of implementing Blockchain in healthcare with specific examples. We also discuss the possible future adoption of Artificial Intelligence (AI) and Machine Learning (ML) techniques with Blockchain technology for healthcare systems. Finally, we discuss the reluctance of adopting Blockchain technology in health-related services.

E-mail address: qmamun@csu.edu.au.

https://doi.org/10.1016/j.smhl.2021.100223
Received 13 March 2021; Received in revised form 23 August 2021; Accepted 1 November 2021
Available online 16 November 2021

2. Blockchain basics

Before we elaborate on how Blockchain technology works, we shed some light on the problem that blockchain technology was developed to solve. To verify that a document (such as a dollar bill, driver license or a vote in the election) is legit, we look it up with the relevant authority. For example, each dollar bill has a serial number that the bank records; each driver license number is recorded by the motor authority; each voter is registered with an election commission. Whether the authority is a bank, state office, or a person that has the power to issue and validate the information, there is one thing that all of these mechanisms have in common - they are all centralised. These central authorities have a lot of power and may become corrupt intentionally or unintentionally.

Decentralisation reduces the risk for corruption, fraud and manipulation. Blockchain technology is a new and innovative way to implement decentralisation. In a nutshell, Blockchain technology is a solution for the problem of centralisation. It is a system for keeping records by everybody, without any need for a central authority-a decentralised way of maintaining a ledger that is practically impossible to falsify.

A Blockchain is called a blockchain because it is simply a chain of Blocks. Imagine maintaining a shared ledger with many pages of records. Each page begins with a sort of summary of the page before it. If the contents of a page are changed, the next page's summary should be changed too. Thus, the pages are linked or chained together. In technological terms, pages are called blocks. And since each block is linked to the previous block's data, we have a chain of blocks or a blockchain.

Many people think that Satoshi Nakamoto, the mysterious inventor of Bitcoin, created Blockchain technology. Technically he only created the first real-life implementation of it - Bitcoin. In fact, the word Blockchain was never even mentioned in Satoshi's original whitepaper. The closest he came to saying Blockchain is a "chain of blocks".

There are four elements a blockchain needs to have a life of its own.

The first element required to support a blockchain is a peer-to-peer network - A network of computers, also known as equally privileged nodes. It's open to anyone and everyone. This network enables nodes to communicate and share remotely.

The second ingredient is cryptography. Cryptography is the art of secure communication in a hostile environment. It allows a node to verify messages and prove the authenticity of messages, even when malicious players are around.

The third element is a consensus algorithm. It means the participating nodes need to agree on rules on adding a block with the existing Blockchain. There are many types of consensus rules, such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Authority (PoA), Proof of Elapsed Time (PoET) etc. These algorithms state that all participating nodes need to prove something for someone to earn the right to add a block to the existing Blockchain.

Finally, our last element is punishment and reward. This element is derived from game theory, and it makes sure that it will always be in the best interest of all nodes to follow the rules.

However, there is a fifth element that cannot be synthesised-market adoption. There may be a group of five nodes sharing a ledger with a consensus algorithm. However, it does not make it decentralised since not enough participating nodes are a part of the system. Moreover, if there is no adoption, there is no value to the Blockchain technology, and the fourth element of punishment and reward is ineffective. Once it achieves a critical mass in the number of users, a blockchain becomes truly decentralised and, therefore, immutable.

Blockchains can broadly be categorised into two classes-public and private. A public blockchain is open to everybody; it's trans-national and borderless. It's censorship-resistant, and it doesn't require any 3rd party. It's also neutral - there's no such thing as a "good", "bad", "illegal", or "legal" transaction. There's only a "valid" or "invalid" one.

On the other hand, a private blockchain is limited to authorised participants only, and a handful of entities governs it. A significant number of researchers believe that in most private blockchains cases, a blockchain is not really required; sharing spreadsheets between the participants may meet the need.

Sometimes, organisations utilise the best of both worlds by using a hybrid Blockchain, a type of blockchain technology that combines private and public Blockchain elements. It allows organisations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored in the Blockchain and what data will be opened up publicly.

Typically, transactions and records in a hybrid blockchain are not made public but can be verified when needed, such as by allowing access through a smart contract. Confidential information is kept inside the network but is still verifiable. Even though a private entity may own the hybrid Blockchain, it cannot alter transactions. When a user joins a hybrid blockchain, they have full access to the network. The user's identity is protected from other users unless they engage in a transaction. Then, their identity is revealed to the other party.

Federated blockchain or consortium blockchain is a technology where multiple organisations govern the platform instead of only a single organisation. It's not a public platform rather a permissioned platform.

3. Healthcare sector and Blockchain

The healthcare sector comprises publicly traded companies supporting all facets of the healthcare sector. It consists of clinical, preventive, treatment and therapeutic services providers including doctors, nurses, hospitals, and other private, government, and voluntary institutions such as residential, educational, dental, domestic health, medical, surgical, ambulatory, and medical and diagnostic laboratories. It also covers drug and medical equipment suppliers and health insurance companies. Blockchain technology can benefit all sectors of the healthcare system. However, a careful selection of Blockchain types is necessary for effective implementation.

At present, three types of Blockchains are available; public, proprietary and consortium Blockchains. Each type of Blockchain has various features in terms of permissions, access and data sensitivity protection for Blockchains (Reyna, 2018, pp. 173–190). For specific Blockchain styles, the current definition of Blockchain for different applications remains unclear. In the healthcare sector, in particular, that medical information is considered to be confidential and vulnerable.

Public Blockchains such as Bitcoin, Ethereum etc., are very well known to everybody are self-explaining. They are fully open ecosystems in which everybody can participate. There is also an integrated incentive mechanism in the network, which rewards participants for their more in-depth participation. Nevertheless, a decentralised Blockchain will not help the health care industry. First, the blocks in bitcoin and ethereal have a storage problem, as is exceptionally well documented. Bitcoin has a little more than 1 MB/ Block, which is simply not sufficient to perform the kind of transactions and keep data needed by health institutes. Then we have the question of results that was also quite well known. Bitcoin is hardly able to process seven to eight transactions per second. The consensus algorithm used in Bitcoin requires around 10 min to reach the consensus among the miners to add a new block in the Blockchain. In other words, the latency is too much. Big medical institutions have to deal with enormous trading blocks with almost 0 latency every day. Indeed, latency of any kind could potentially endanger life. The consensus algorithm in public Blockchains, such as proof-of-work used in Bitcoin, requires a massive amount of computer power to solve challenging puzzles. As a consequence, spending so much money on consensus algorithms is not practical for these institutes.

Lastly, the openness of public Blockchains is another detriment. Medical organisations may not want to engage in a network that everyone can access and join as clinical institutes treat highly classified and sensitive data and do not want to communicate outside their circles. Thus, public blockchains may not be a practical solution in this regard. However, there is another type of Blockchain that is practical for health institutes and is called private Blockchain [6].

Those who wish to participate in the privately-owned chain must receive permission to join this network. That is why private chains are also called “permitted blockchain.” They can join the private chain. This makes it possible for some people who can participate in consensus to be restricted. The following could provide access to new participants:

- The existing participants involved in the ecosystem.
- A power governed.
- A consortium.

After an organisation enters the Blockchain community, it can play a part in network maintenance. Hyperledger Fabric is an instance of a licenced Blockchain system application from the Linux Foundation’s Hyperledger Project. It was designed to meet these specifications of the business. Private chains are specifically designed for business purposes that provide various benefits, such as fast transfers, anonymity and high security.

In addition, in recent years, the development of health-related IoT devices has increased, with these products having an internet capability that could provide patent monitoring in real-time (Dwivedi et al., 2019). Apple has recently developed and incorporated ECG with its new Apple watch. Apple has, for instance, implemented heart rate monitors into wearable and mobile devices. According to the journal article in the Journal of Medical Systems, “Healthcare Blockchain System Using Smart Contracts for Secure Automated Patient Monitoring” (July 2018)", Blockchain can improve security and automate the provision of health-related notification in remote patient monitoring systems” (Griggs, 2018).

Smart contracts in Blockchains have allowed Blockchains to store data retrieved on request (Li et al., 2019). But smart contracts can be tedious to implement and require specialised support to administer and maintain. Several journal articles provide concept designs for utilising IoT for health-related purposes. These concept designs are primarily based on the use of private Blockchains as they add additional permission-based security. One concept solution was to utilise individual smart contracts for each IoT device and create and administer all these smart contracts.

A dedicated smart contract on public Blockchains with a defined data format may be available for IoT health devices for anyone to use. A smart contract and data format that still provides privacy and security due to the medical information involved. It would mean fewer administration requirements and several smart contracts being added to the Blockchains.

Researchers have been proposing to utilise Blockchain technology in healthcare in different ways. In (Xie et al., 2019), Xie et al. suggested a blockchain-based system for ensuring biopharmaceutical product distribution in this paper. This system employs stochastic simulation to guide the blockchain network, ensuring that biopharmaceutical items are protected from counterfeiting, fraud, theft, and temperature diversion. Despite this, the suggested solution increases the supply chain process’ efficiency, transparency, security, and reliability. Using the Proof of Authority (PoA) technology, the smart contracts for the system were created and defined. The last feature is the ability to monitor data streams in real-time on the blockchain network. According to the results, the system performs well.

Drug delivery information management and tracking system for the pharmaceutical business was proposed by Wigand et al. (Wigand et al., 2011). The drug supply chain has been secured using a variety of technologies, including RFID and electronic product code information service (EPCIS). Collective action theory and transaction cost theory were used to build the research environment. They established a number of guidelines for all parties involved in the medicine distribution procedure. Contraband is a big issue for pharmaceutical companies and health groups. This is a problem that many worldwide health organisations are trying to solve, but the sales of these pharmaceuticals continue to grow.

For the traceability and management of the supply chain, Molina et al. (Molina et al., 2019) recommend a system using blockchain technology, where each participant may track and inspect the medicine delivery at each stage. Based on a case study, the proposed system was developed.

However, one central question to answer is whether blockchain technology is the next big thing for healthcare? There are hypes-Blockchain is the panacea for all systems. Different start-ups may try to use blockchain technology to solve some problems. In most cases, we may ask two questions: First, are they using a public or private blockchain? And second, do they even need a blockchain? If the answer to the first question is a private blockchain, there is nothing very disruptive here. For the second question, we go back to the primary reason for the Blockchain creation, where we mentioned the dangers of centralisation. But these dangers are only meaningful if stake size is vast. For example, the queue to the pharmacy can be managed in a centralised manner, rather than using Blockchain technology.

Blockchain technology is very good at decentralising, but it's also very inefficient, slow and energy-consuming. For example, Bitcoin's network takes 10 min on average to confirm a transaction. It is not the ideal waiting time for buying a cup of coffee at a coffee shop. The only reason to choose Blockchain technology as the solution is if the problem is centralisation. If a system does not need to decentralise something, the system probably does not need to use blockchain technology and are better off with some centralised solution.

In the following section, we discuss some use cases of Blockchain technology, looking forward to the healthcare industry's frontier research and the possible future development direction where this technology will imprint numerous positive effects.

4. Different use cases of Blockchain in healthcare

This section portrays different use cases of Blockchain technology in the healthcare system for realising different benefits in healthcare sectors. The benefits include, but not limited to, decentralisation, improved data security and privacy (Zhang et al., 2018), health data ownership, availability and robustness, transparency and trust, and data verifiability.

4.1. A seamless healthcare system

The fact that organisations have several fragmented health records about patients is one of the biggest health problems nowadays. This problem can be solved by adding Blockchain (Gordon & Catalini, 2018) medical record transactions. A smart contract can be launched to create a smart health ecosystem to give a patient's electronic health record limited access. Doctors will write notes, insert scans and testing tests, all of which are reported as transactions. The pharmacy records the transaction on the Blockchain when it dispenses medication. The patient gives his/her insurer limited access to check treatment and payment payments. Patients reward doctors with clever contracts. Doctors will be able to review medical cases remotely and provide advice or a second opinion. To monitor health insurance patients' progress and fitness, they will receive tokens or lower premiums from health insurers. Patients are also given limited-time access to medical information for medical testing for research institutions. Some tokens may be issued, which patients will use on the Blockchain data from wearable fitness devices to store the electronic health records and transfer value and payments. This Blockchain-based healthcare ecosystem will allow developers to develop smart applications that analyse health data and provide recommendations such as nutrition and fitness routines.

4.2. Electronic health record (EHR)

Over a number of years, the health sector has been affected by centralised systems' development, the regulation of data on health, and the mandate to work with the various EHR service providers to digitise medical data (Nguyen et al., 2019). Most repositories are not interacting with each other, but they are information owned by health workers, pharmaceutical companies and other stakeholders in the health and the health ecosystem. The inability to interoperate between most systems for quantitative health data, both individual (patient) and community (public) levels, illustrates the structural challenges that are often found in the following situations:

- When patients want other healthcare providers to contact or seek medical services
- Where the clinical trial administrators want to confirm their participants ' extensive medical data
- When pharmaceutical companies try to ensure that drugs dispersed on global markets are authentic.

Blockchain technology can help healthcare experts and the overall healthcare industry to improve performance, patient data transparency, tracking, and accountability, as well as reduce costs. In addition, a range of Blockchain products can be tailored to address various healthcare applications, including the following:

- Secure management of electronic health records (EHRs)
- Patient consent management
- Drug traceability
- Data security in clinical trials
- Incentivisation through micropayments

4.3. Counterfeit drugs

Counterfeit drugs are a modern-day problem. It is estimated that every year between 120,000 to a million people die because of them. Moreover, inefficient supply chains mean more expensive drugs. Regulatory requirements mean there are significant reporting burdens on pharmaceuticals. Blockchain technology may help in this regard to develop a solution to these problems (Kumar & Tripathi, 2019). Blockchain with artificial intelligence and advanced data analytics may be used to eliminate fake medicines from the supply chain and bring about greater efficiencies. Manufacturers, warehouse, shipping and logistics companies will be integrated into the hospital or pharmacy. Each packet of medicines can be tracked on the Blockchain. The customer can check whether a medicine is genuine by using the mobile app, which allows significant advantages. Fake drugs do not enter the pharmaceutical supply chain. AI and data analytics make delivery systems more efficient. It will also help to prevent price distortions through the efficient distribution of medicines. Automated regulatory reporting and facilitate automatic payments throughout the supply chain will be allowed.

4.4. Emergency disaster relief

Blockchain allows us to reimagine processes and reveal the true power of collaboration during an emergency disaster relief situation (Aranda et al., 2019). Unclear information from many independent sources like emails or social media can hinder the fast and efficient coordination of help in disaster relief missions (Labonte, 2014). A shared system of record can significantly reduce complexity and streamline interactions between multiple parties. Blockchain allows connecting several independent systems using a decentralised network without having a single party controlling the data systems.

Imagine an emergency disaster relief situation where the United Nations launched an international disaster relief mission just after an earthquake has struck an island. Three organisations A, B, and C, set up camps all over the island-each of them brings specific resources. A helps with drinking water, B brings medical support, and C provides helicopters. The Blockchain acts as a single source of truth and provides transparency over asset needs. Let us assume the B camp has several doctors that need to fly to the other side of the island. They enter a request in interface F, which is then broadcasted to all mission participants via Blockchain. All other participants can instantly see the request and react to the specific offer. Here camp A can provide the helicopters to be on-site as quickly as possible. All camps will agree on a smart contract, the simple open algorithm embedded in the Blockchain, ensuring that everyone sticks to commonly agreed-upon rules. Once an offer matches the request, it automatically provides help without delay, and no other party needs to act on it.

The ability to collaborate directly on a business process across organisations is one of the key elements. Almost all Blockchain use cases have in common. Blockchain guarantees autonomy from intermediaries and ensures transparency and data sovereignty for each party. Everyone covers its costs while all can benefit from the efficiency of the distributed system. This is only one of many cases.

4.5. Pharmaceutical supply chains

In the pharmaceutical industry, safety, stability and safety are among the highest standards. Supply chain management can be monitored safely and transparently with Blockchain, for example. This can reduce delays and human errors significantly. It can also be used at any stage in the supply chain to track prices, labour, and even waste pollution (Bocek et al., 2017). They can also be utilised to verify product authenticity by keeping track of their origin and fighting against the falsified market in drugs, which annually costs $200 billion in losses. Companies like Chronicled, Blockpharma, and Modum are already working towards more efficient Blockchain logistic solutions. Modum, in particular, works in compliance with EU laws that require proof that medicinal products have not been exposed to specific conditions, especially certain temperatures, which may comprise their quality. The solution of Modum was to develop a sensor that records the environmental conditions while physical products move, and it records them permanently on the Blockchain.

4.6. Genomic market

Blockchain networks can be constructed to enable people to safely and securely exchange genomic data in a new emerging market. It is expected that opportunities for personal genome sequencing will create a data market worth billions of dollars (De Cristofaro, 2014). And what is the best technology to deal with data security problems and guarantee data passes without intermediaries from the source to the end-user? It's the Blockchain without any hesitation. Blockchain can be used to enhance genomic data protection, enable customers to procure genomic data effectively, and tackle genomic big data challenges.

4.7. Healthcare payments

The health industry suffers from an inefficient, outdated health care payment process that leads to the thousands of wastes spent due to alleged mistakes and disputes. Uncomplicated agreements between shareholders mean that information is not shared and exchanged. Imagine a world where all parties within a business network have access to the same information, meaning there is always a synchronous version of the truth.

Blockchain is a decentralised, shared ledger, and it allows transactions and asset tracking to record any value. The shared directory enables everyone to monitor and analyse an asset's state in close to real-time to enable end-to-end tracking. (Pouraghily & Wolf, 2019).

Today's major pain point is the pre-authorisation process, which some insurance companies require before deciding to pay for

certain services. Determining a given expense is covered by a member's insurance policy can be a slow process for many reasons, such as the involvement of multiple stakeholders in the variance in the amount covered. Based on the payer-provider relationship, the processes are typically complex, involve several manual steps, and may be due to poor communication and technology. With Blockchain, a single ledger shared among the healthcare stakeholders contains the patient's entitlement and smart contracts, which encode the pre-authorisation conditions. This automates information collection and sharing, allowing for real-time determination of benefits. Some advantages of using Blockchain for pre-authorisation include improving cash flow due to faster transaction settlement, timely patient treatment, accurate payment to the provider, reduced administrative costs, and double record-keeping.

Today, another major issue is dealing with claims submitted for a patient who has either lost coverage or switched insurance companies. In a perfect world, all healthcare providers would validate a patient's current insurance status before an appointment, but that is not always the case. Often, validation is not completed because the process is simply manual and time-consuming, or they trust that the patient will tell them ahead of time. The claims process is initiated when a patient visits a provider after that provider renders services. A claim is submitted to the patient's health insurance. The insurance company then processes that claim and notifies the other parties of its decision. In this scenario, if the claim is rejected due to issues with the patient's insurance status when the patient has no insurance, the healthcare provider must then try to recover the out-of-pocket cost of the service already rendered, which is very difficult to do. In the case of an outdated patient's insurance record, the provider must then update that claim and submit it again. This results in overhead costs and can cause long delays in overall healthcare.

A Blockchain-enabled system provides accountability for all stakeholders in the claim specifications and reimbursement rules. The contracts between the vendors, clients, payers and public regulators have been negotiated and held on the Blockchain via smart contracts. Healthcare providers would know exactly what information is needed before claims are submitted. Providers can easily format claim data to ensure that all data is entered correctly in an accurate format, as required for the Blockchain. This clarity reduces or eliminates claims being returned due to insufficient information, thus saving time and effort for all parties involved. Blockchain plays an increasing position in health care IT and provides any stakeholder in the industry with beneficial disruption and productivity. Health organisations must recognise and test the technologies of Blockchain now to ensure they are ready for tomorrow's shifts.

4.8. Medical staff credentialing

The certification for healthcare professionals can be a time consuming and wasteful endeavour by phone calls, faxes and snail-mail. Because Blockchains can be checked and gradually modified, the software is ideal for credentials. Blockchain authentication technologies and control limits create a safe repository that all members of the chain will use. Each contributor to the data can have access or access to the entire ledger.

Further possible Blockchain use is the credential "smart contract," a contract that involves using Blockchain's software as a living credential database. The premise is that the credential information is constantly being modified in a single database with inputs and updates from those entered in int. In this fashion, it would not be necessary every time there was a need for credentialing information spanning the period from completion of college through the most recent credentialing relevant events to seek the information from the multitude of repositories where it resides. Instead, it would be available immediately, with access to display the practitioner's records directly or through a guide provided to the individual managing the database. This approach would save time and cost significantly as a repetitive process in which delay is inevitably expensive.

4.9. IoT security for remote monitoring

One of the most prominent developments in digital health is using remote surveillance solutions that provide accountability for patients' health across all sensors that measure essential signals for patients. More proactive and preventive treatment is available to practitioners. However, security is a crucial problem in IoT health, both maintaining patient data privacy and safety and not being impaired in creating false information. In emergencies, e.g. when alerting the carer of an older adult to a heart attack or fall, a connected system may be dependent upon. It is also vital that supports are highly resistant to DDoS and/or other attacks that interrupt service.

Blockchain ensures that only authorised parties can gain access to personal data stored as a unique hash function on the Blockchain (any change in the source data will create a different hash function, and a user must have a specific set of cryptographic keys to decode the hash function into the source data).

If patient data is registered as a hash function in the blockchain directory, it is almost impossible to handle them as all saved copies are needed.

The decentralised nature of Blockchain means that IoT devices can communicate directly without a centralised server. This type of communication makes it very difficult to initiate a distributed denial-of-service attack or man in the middle attack.

Although Blockchain could improve IoT safety in healthcare, these use cases are still in the early stages of development, and it is not yet clear if Blockchain would be the right tool to use. For digital health companies to consider how to ensure remote monitoring devices' security, it is worth investigating Blockchain, but only as part of a much more robust end-to-end security strategy.

4.10. Blockchain technology merged with artificial intelligence (AI)

Blockchain and Artificial Intelligence technology can be combined to improve the quality of care in healthcare systems. It will cut costs in the medical industry, and as a result, healthcare will become more accessible and affordable. Blockchain enables encrypted data, which AI requires. As a result of blockchain technology, it will be possible to determine the logic involved in algorithmic decision-making.

In healthcare, Blockchain will assist eliminate repetitive work, rework, and reconciliation. With the help of artificial intelligence (AI), we can direct the work in a predictive healthcare setting and achieve the optimum level of service intensity Patients, clinicians, and caregivers will receive the information in a context-appropriate way.

As an example, consider a case study related to the COVID-19 case. Blockchain plays a strategic role in COVID-19-safe clinical practice. The combination of the potentialities of Blockchain and Artificial Intelligence rapidly identify the diagnosis and treatment specific for COVID-19 patients and contributes to the development of clinical guidelines for possible epidemics (similar to coronavirus) in the future.

The data from clinical laboratories, hospitals, primary care physicians, pediatricians, and other sources are shared while respecting privacy and security with Blockchain. Analysis of data is done by using AI solutions.

Consider, for example, the COVID-19 case study. The COVID-19-safe clinical practice relies on blockchain technology. With the combination of Blockchain and Artificial Intelligence, COVID-19 patients may be quickly diagnosed and treated, which helps build therapeutic recommendations for future outbreaks (similar to coronavirus). A blockchain-based system allows for sharing data from clinical laboratories to hospitals to primary care physicians to pediatrics while maintaining privacy and security. AI solutions are used to analyse data. This paradigm is useful for risk management, stimulates the creation of novel pharmaceuticals, and encourages research into suitable therapies.

5. The reluctance of adopting Blockchain in healthcare

Although invented in 2008 by Satoshi Nakamoto (Nakamoto & Bitcoin, 2008), Blockchain technology is relatively new. It was created to serve as a public transaction ledger for the Bitcoin cryptocurrency. There has been a shortage of rigorous work since 2008, and not enough attention has been on the actual technology behind Bitcoin. This lack of research affects Blockchain technology adoption. There is "no legal framework to support or support smart contracts" (Dell'erba, 2018), making it more difficult for companies to embrace it fully and want to implement it in their businesses.

Early in 2019, Deloitte conducted a Global Blockchain Survey (Deloitte's 2019 global Blockchain Survey) in which 29% of respondents identified a lack of understanding of Blockchain technology as one of the key obstacles to adopting this technology (Griggs, 2018). In fact, research continued surrounding the bitcoin rather than the infrastructure that bitcoin uses. There is insufficient evidence of the true efficacy of Blockchain technology, and 22% of respondents to the Deloitte Global Blockchain Survey agree. The reluctance of adopting Blockchain technology in healthcare may include:

5.1. The cost of mass adoption

Currently, there are no systems that are designed to take advantage of Blockchain technology. When Blockchain is meant to be used for a specific purpose, developers must create their code (or have someone else do it)—building new software costs a great deal of money ranging from $10,000 for basic applications to $800,000 or more for unique software with complex functionality.

5.2. Lack of experts in Blockchain technology

The shortage of experts is affecting adoption in two ways. First, there are not enough people working on innovation to meet demand. Second, exclusivity means that it costs a lot to employ current Blockchain experts. Ideally, the growing interest in Blockchain technology would encourage more people to learn about it.

5.3. People are reluctant to change

The potential of Blockchain to revolutionise issues such as contracts and financial markets makes it less likely for people to adopt the software rapidly. Examples of this can be seen throughout history. The Harvard Business Review refers to TCP/IP as an excellent example of slow adoption. Researchers began using TCP/IP in 1972 because it allowed them to send emails to each other. A handful of companies were involved in TCP/IP in the 1980s, but the technology was not mainstream until the mid-1990s. If it took more than two decades for TCP/IP to reach out to users, then we can't expect everyone to start using Blockchain within a decade of its inception.

5.4. Regulation, law, and politics

One of the main hurdles of reluctance in adopting Blockchain is legislation, law, and policy, with excitement around this technology (Hsueh & Chin, 2017). In 2019, Deloitte conducted a study that asked managers, "What are the barriers to an increase in adoption and scope of Blockchain technology in your company or plan if any?" (Deloitte's 2019 global Blockchain Survey). 30% of respondents claimed that regulatory problems pose the main obstacle to further Blockchain investment.

Perhaps the immature nature of the technology or its associations with bitcoin has made many industries suspicious. Fears that a distributed computerised system is entirely reliant may also arise to prevent the Blockchain from being implemented to solve complex problems such as compliance with DSCSA (Drug Supply Chain Security Act). The implementation of Blockchain asks for confidence in data stores without depending on a reliable broker to authenticate a transaction that prohibits healthcare organisations from storing and transmitting sensitive information in the healthcare industry.

6. Conclusion

The technology of Blockchain is constantly changing rather than going to complete. Several potential problems need to be addressed if biomedical and health care systems want to adopt this technology. Openness and confidentiality is the first challenge. On a blockchain network, everyone can see everything. Some believe the medical data should be kept outside of the chain. However, the Blockchain simply held the hash of the details on the tag. Speed and scalability is the second challenge. When processing the transaction pace, a proof of concept test is projected to be only a few hundredths of the standard method, for example, a credit card. Seeing that the number of health care transactions is immense, a technical breakthrough is required in Blockchain. The last challenge is a 51% attack. Although this is only a theoretical risk, a clear solution should be proposed (Ahram et al., 2017).

Data is both a powerful resource and a limitation when it comes to the healthcare industry's multi-level ecosystem. Several problems are associated with data management, such as excessive paperwork, lengthy delays, and miscommunication. Blockchain has become the go-to option for data-intensive industries, including healthcare, and it is no more a secret.

In terms of health information, blockchain technology can serve as a convergence point even though the healthcare industry has been overburdened with data. Blockchain can give solutions for stakeholders in the field to deal with this "datafied". Because of its immutable and decentralised nature, Blockchain technology can be the answer to reducing costs while optimising procedures.

Healthcare Blockchain ventures may, therefore, need to bear this in mind when constructing their solutions. Akin to building a playground and then hoping rival gangs will use the slides and swings together, platform entrepreneurs might prudently consider gaining buy-in from stakeholders beforehand and then building relationships on-chain one variable at a time.

There are many challenges ahead. The perfect business models for Blockchain are far from being agreed upon. One thing is for certain, though – if you want to compete with the incumbents, collaboration is essential.

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

Deloitte's 2019 global Blockchain Survey. Deloitte Insights. www.deloitte.com/insights/us/en/topics/understanding-blockchain-potential/global-blockchain-survey.html.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (June 2017). Blockchain technology innovations. In *Proceedings of the 2017 IEEE technology & engineering management conference (TEMSCON), Santa Clara, CA, USA* (pp. 137–141), 8–10.

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology applications in health care. *Circulation: Cardiovascular Quality and Outcomes, 10*(9), e003800.

Aranda, D. A., Fernández, L. M. M., & Stantchev, V. (2019). Integration of Internet of Things (IoT) and Blockchain to increase humanitarian aid supply chains performance. In *2019 5th international conference on transportation information and safety (ICTIS), Liverpool, United Kingdom* (pp. 140–145).

Benchoufi, M., Porcher, R., & Ravaud, P. (2017). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000research.com, 6*. https://doi.org/10.12688/f1000research.10531.1

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere - a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM), Lisbon* (pp. 772–777).

Dagher, G. G., Mohler, J., Milojkovic, M., Marella, P. B., & Marella, B. (2018). Privacy-preserving framework for access control and interoperability of electronic health records using Blockchain technology. *Sustainable cities and society, 39*, 283–297.

De Cristofaro, E. (Mar.-Apr. 2014). Genomic privacy and the rise of a new research community. *IEEE security & privacy* (Vol. 12,(2), 80–83.

Dell'erba, Marco (2018). Demystifying technology. Do smart contracts require a new legal framework? Regulatory fragmentation, self-regulation, public regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3228445

W. J. Gordon C. Catalini "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability" Computational and Structural Biotechnology Journal vol. 16 pp. 224-230 2018.

Dwivedi, A. D., Srivastava, G., & Singh, S. D.a. R. (2019). A decentralised privacy-preserving healthcare Blockchain for IoT. *Sensors — Open Access Journal Jan., 19*(2), 326.

Griggs, K. (2018). Healthcare Blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems, 42*(7), 1–7.

Hsueh, C., & Chin, C. (2017). EPoW: Solving blockchain problems economically. In *2017 IEEE SmartWorld, ubiquitous intelligence & computing, advanced & trusted computed, scalable computing & communications, Cloud & big data computing, internet of people and smart city innovation (smart world/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), San Francisco, CA* (pp. 1–8).

Kumar, R., & Tripathi, R. (2019). Traceability of counterfeit medicine supply chain through Blockchain. In *2019 11th international conference on communication systems & networks (COMSNETS), Bengaluru, India* (pp. 568–570).

N. A.M. Labonte "Challenges in humanitarian information management and exchange: Evidence from Haiti" Disasters vol. 38 no. s1 pp. S50-S72 2014.

Li, M., Xia, L., & Seneviratne, O. (2019). Leveraging standards Based ontological concepts in distributed ledgers: A healthcare smart contract example. In *2019 IEEE international conference on decentralised applications and infrastructures (DAPPCON), newark, CA, USA* (pp. 152–157).

Molina, J. C., Delgado, D. T., & Tarazona, G. (2019). Using Blockchain for traceability in the drug supply chain. In *Proceedings of the international conference on knowledge management in organizations, Zamora, Spain, 15–18 July 2019* (pp. 536–548). Berlin, Germany: Springer.

Nakamoto, S., & Bitcoin, S. (2008). *A peer-to-peer electronic cash system*. Available online: accessed on 12 November 2019 www.bitcoin.org.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile Cloud Based E-health systems. In *IEEE access* (Vol. 7, pp. 66792–66806). https://doi.org/10.1109/ACCESS.2019.2917555

Pouraghily, A., & Wolf, T. (2019). A lightweight payment verification protocol for Blockchain transactions on IoT devices. In *2019 international conference on computing, networking and communications (ICNC), Honolulu, HI, USA* (pp. 617–623).

Reyna, A. M. (2018). *On Blockchain and its integration with IoT. Challenges and opportunities*. Future Generation Computer Systems.

Wigand, R. T., Mande, D. M., & Wood, J. D. (11–13 April 2011). Information management and tracking of drugs in supply chains within the pharmaceutical industry. In *Proceedings of the 2011 eighth international conference on information technology: New Generations* (pp. 500–507). NV, USA: Las Vegas.

Xie, W., Wang, B., Ye, Z., Wu, W., You, J., & Zhou, Q. (8–11 December 2019). Simulation-based Blockchain design to secure Biopharmaceutical supply chain. In *Proceedings of the 2019 winter simulation conference (WSC)* (pp. 797–808). MD, USA: National Harbor.

Zhang, P., White, J., Schmidt, D., Lenz, G., & Rosebloom FHIR-Chain, S. (2018). *ApplyingBlockchain to securely and scalably share clinical data*.

Further reading

Guo, R., Shi, H., Zheng, D., Jing, C., Zhuang, C., & Wang, Z. (2019). Flexible and efficient Blockchain-Based ABE scheme with multi-authority for medical on demand in telemedicine system. *IEEE Access, 7*, 88012–88025.