Blockchain in Healthcare: A Beginner's Guide and Its Role in Orthopaedic Surgery

Jyoti Khandelwal[1[0000-0002-3027-258X]] and Seema Sharma[2[0009-0004-2798-3059]]

[1] University of Engineering & Management, Jaipur, India
[1]jyoti.khandelwal19@gmail.com
[2]drseemasharma196@gmail.com

Abstract. Blockchain can potentially transform several areas in the healthcare industry, where patient privacy and data security are critical. These areas include orthopaedic registries, medical imaging, research data, patient data management, and the integration of Internet of Things (IoT) devices. At the moment, decentralized architecture is becoming more popular in place of centralized processing, storage, and computing. Distributed ledger technology is one of the key innovations that has made this change possible. This is among the factors contributing to blockchain's increasing popularity in the business and medical world. An extensive analysis of blockchain technology and its significance in the field of orthopedic surgery is given in this paper. In orthopaedic surgery, blockchain is crucial for improving supply chain transparency, implant traceability, and safe patient data management. It also describes the security protocols that are implemented within the blockchain and the use of different token standards, all of which have come together to create a very effective technology that can develop on its own.

Keywords: Blockchain, Decentralized, Medical, Orthopaedic, Protocol.

1 Introduction

Blockchain is a transformative technology that has enabled a wide range of applications across various domains, including financial services, the Internet of Things (IoT), and more. Furthermore, more precise diagnosis and treatment recommendations may be made possible by combining blockchain technology with artificial intelligence (AI), machine learning, and deep learning. Large datasets saved on the blockchain can be used to train AI systems, which will improve automated clinical decision-making. All things considered, blockchain technology may improve orthopaedics' data security, interoperability, and teamwork. Although there are obstacles to overcome, like adoption barriers and the desire to share data, blockchain is a promising invention for the sector because of its advantages.

The block could be considered as a public ledger which stores the digital record of a transaction. The blocks formed are then chained to the other blocks in a chronological manner such that every new block that is added to this chain contains a copy of the last

transaction that happened in the previous block forming a chain-link hence the name “Blockchain" [1].

Since Bitcoin was created in 2008, blockchain technology has grown in prominence. It provides a safe, decentralized approach to data management and security. This paper examines the uses of blockchain technology in orthopaedics and emphasises its advantages. Furthermore, more precise diagnosis and treatment recommendations may be made possible by combining blockchain technology with artificial intelligence (AI), machine learning, and deep learning. Large datasets saved on the blockchain can be used to train AI systems, which will improve automated clinical decision-making. All things considered, blockchain technology may improve orthopedics’ data security, interoperability, and teamwork. Although there are obstacles to overcome, like adoption barriers and the desire to share data, blockchain is a promising invention for the sector because of its advantages.

Ethereum is one such Blockchain. It is a public blockchain platform that allows anyone to create applications without the requirement for expensive blockchain development. Ethereum introduces smart contracts (SCs), which can be written using Solidity [2]. The application of the Merkle Trees method for Blockchain technologies is a major contribution of this research. Smart contracts based on Blockchain Ethereum Technology are used to do this [3].

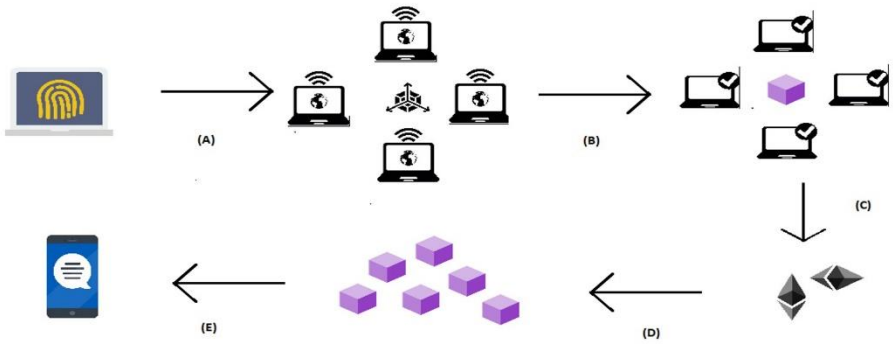

Fig. 1 Workflow of Blockchain.

The workflow steps depicted in Fig. 1 are as follows: (A) The transaction requested is broadcast to a P2P network consisting of computers known as nodes; (B) The transaction is verified by participants of blockchain; (C) The verified transaction is then combined with other transactions to create a new block of data; (D) The new block is then added to the blockchain; (E) The transaction is now complete.

2 Fundamentals of Blockchain

2.1 Hashing

Hashing is a component of Blockchain that provides a cryptographic signature, which is a unique fixed length string that is used to identify a piece of data. They're made by

putting the information into a "Hash Function." Every piece of unique data we enter in the "Data" section will be processed by the Hash function, which will produce a unique hash that will be used to identify the data in the relevant column. The length of the generated hash remains constant regardless of the data provided.

2.2 Blocks

A block is an extended type of hashing that is identical to a hash except that the data is divided into three parts: a block number, a nonce, and the data. The notion is that a block is "signed" if the hash formed with the block number, nonce, and data all start with four 0s. The first block, commonly known as the genesis block, has a previous hash of 0s, while subsequent blocks carry the preceding block's hash. All of this is taken into account when generating the current cell's hash. As a result, any change in any earlier block will render the entire chain of nodes invalid or unsigned.

2.3 Tokens

A token in blockchain is a digital asset that represents value, ownership, or utility within a blockchain ecosystem. Let's say a bad actor in the network tries to alter the data, or fork the network. So, if he wants to update the specifics of a transaction, the information will be verified by the other peers in the network, and the details with the most votes will be chosen as the primary ledger.

2.4 Smart contracts

Smart contracts are computational programs that run when specific conditions are met and are stored on a blockchain. They're typically used to streamline the execution of a contract so that all parties may be confident of the outcome right away, without any need for middlemen or wasted time. They can also automate a workflow, commencing the next phase whenever certain conditions are met.

3 Implementations of Blockchain

3.1 Bitcoin

Bitcoins are represented as a balance in a bitcoin account. A Bitcoin address, generated from the public key through a one-way cryptographic function, serves as a public identifier for a Bitcoin account. Users can send bitcoins to this address using its publicly available information. To spend the bitcoins from the account, access to the corresponding private key is required.

3.2 Ethereum

Ethereum is a blockchain platform that includes a Turing complete programming language. It includes an abstract layer that lets users design their own ownership, transac-

tion types, and state transition algorithms. Smart contracts, which are a set of cryptographic rules which are only executed if certain conditions are satisfied, are used to do this. The Ethereum Network is made up of accounts and state transitions, each of which has a 20-byte address. The world state is a mapping between addresses and account statuses. Ethereum supports two types of accounts: externally managed (controlled by private keys) and contract accounts (controlled by their contract code). An Ethereum account consists of four fields: nonce, ether balance, contract code hash, and storage root.

3.3 AAVE Protocol

Within the Ethereum network, the AAVE protocol is used. AAVE, a decentralized non-custodial liquidity market protocol, allows users to participate as depositors or borrowers. Depositors earn a passive income by supplying liquidity to the market, while borrowers might borrow with overcollateralization (indefinitely) or under collateralization (temporarily). Because the protocol is open source, it may be used by any third-party service or application, which improves your offering.

3.4 Consensus Protocols

Under a centralized structure, the entire system is controlled by a single entity. Since everyone in the network must decide what is best for the network collectively, a decentralized structure is very different. Consensus ensures that an agreement is reached that benefits the entire network, while majority rule controls voting in a decentralized network [4]. The blockchain consensus algorithms must therefore be appropriate for the requirements of its particular application. This section's subsections will cover a number of consensus methods and how the blockchain uses them.

Proof of Work (PoW). Proof of Work (PoW) is a technique for obtaining consensus in a blockchain network and has been the foundational consensus model of several cryptocurrencies. Here the network mining nodes must demonstrate the work they've done and submitted which then qualifies them to add new transactions and blocks to the blockchain as part of the PoW consensus method [5].

It provides security to the network by having a goal to make the chain longer. Because it has had the greatest computational labor done, the longest chain is the most plausible as the valid one. This is due to the fact that a fraudulent miner would have to solve the block nonce sooner than everyone else. To beat everyone else, one needs over 51% of the network's mining power to continuously create malicious but valid blocks. To complete this amount of "work," one will need a lot of processing power. And if this energy capacity is put into earning coin rewards it can even outweigh the benefits that one gets from an attack [6].

As shown in Fig. 2, Sybil attacks in a blockchain operate as follows: (A) The intruder begins to create its very own private blockchain branch; (B) When the false chain has grown large enough, the intruder broadcasts it to the whole network; (C) Since its blocks had lower conformations, the real chain was abandoned.

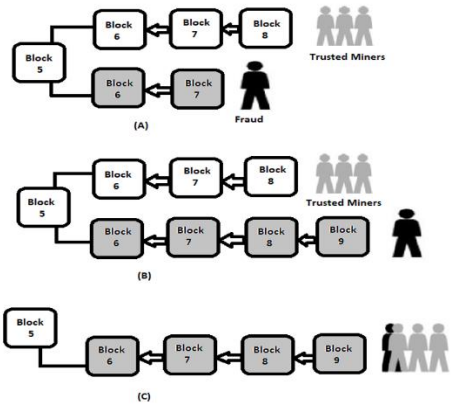

Fig. 2: Sybil attacks in a Blockchain.

Proof of Stake (PoS). Proof of Stake (PoS) is a less energy-intensive version of Proof of Work (PoW). In PoS, the node that generates the next block is chosen depending on how much "staked" they have in relation to other nodes. Random allocation and staking age along the wealth of the node are two aspects of the technique [7].

4 Token Standards

The various tokens present in the ethereum network Table 1 represents the characteristics of these tokens.

Table 1. Represents the characteristics of different tokens.

Technical Specifications	ERC-20	ERC-721	ERC-1155
Ease of Use	Each transaction necessitates a single operation.	Each transaction necessitates a single operation.	Multiple operations can be performed in a single transaction.
Supported tokens	Supports fungible tokens.	Supports non-fungible tokens.	Supports fungible as well as Non-fungible tokens.
Smart Contracts	One common smart contract is required.	Each token must have its own smart contract.	For infinite tokens, a single smart contract is required.

Token Transfer	You can send one or two tokens at a time.	Allows for a single token transfer at a time.	Allows for the transfer of a large number of tokens in one go.
Storage	It necessitates additional storage on the chain.	It may be stored off or on a chain.	It may be stored off or on a chain.

5 Application of Blockchain Technology in Orthopedic Surgery

Blockchain enhances security and transparency via smart contracts and encryption, allowing for real-time patient access, monitoring, and control of medical data. As it enables shared, up-to-date patient data in multiple locations, a decentralized system improves resource management and allows secure, verifiable sharing of expanded and reliable health information [8]. In addition to empowering medical research by providing a steady flow of anonymized, tamper-proof datasets suitable for clinical enquiries, it facilitates Eliza-style telemedicine, rehabilitation and secure data sharing as well [9].

5.1 The Orthopedic Registration and Blockchain

Since Sweden launched the first national orthopaedic registry for total knee arthroplasty (TKA) in 1975, global registries have collected data on implants, surgical methods, and failures, with records maintained by operating surgeons [10]. Current Web 2.0 systems face issues like data tampering, high costs, and lack of ownership. Blockchain technology offers a secure, decentralized, and immutable solution, enabling patient-controlled access via keys and automating processes through smart contracts, improving data sharing, and transparency, and reducing administrative burdens [11]. However, integrating Blockchain into orthopedics faces technological, regulatory, financial, and practical challenges that must be addressed for effective implementation [12].

5.2 Blockchain and Medical Imaging

Centralized storage system often leads to missing copies and costly repeat exams, nonetheless medical imaging is crucial for disease detection. This enables the decentralized, timestamped, secure and encrypted storage of MIRs that can only be accessed by smart contracts authorized by the patient. This reduces redundancy, eases data sharing, and improves accuracy, efficiency and privacy while saving money. Yet hurdles to acceptance are slow tech adoption and an all-in overhaul on treatment of sensitive data, which would be able to improve diagnoses and automate clinical tasks for patients and clinicians [13].

5.3 Blockchain, Research Data & Clinical Perspectives

The use of blockchain technology allows for decentralization and encryption, which greatly enhances the protection of patient data and can streamline the process of improved standards of healthcare and research participation [14]. This not only allows patients to participate in studies, for which they might earn governance tokens, but it also helps wearables, imaging, and scoring scale data to be used as an integrated unit that improves research, reduces bias and increases validity [15]. Smart contracts allow part of the data to be shared globally to enable multi-center studies as well as to increase databases. In orthopedics, this can mean tracking implants from manufacture to implantation all the way down to recording outcomes and assisting with decisions from the data, which leads to better future designs. It also validates legal interactions, such as consent for surgeries and payments, and authenticates training materials for medical personnel. Such traditional form of (centralized) data storing can be replaced using virtual data storage (blockchain) revolutionizing health data management, research, and patient care combined with AI and any other technology. Below are useful examples and prospective case studies which can illustrate how these concepts might be implemented in practice:

Secure Patient Data Sharing. Imagine a blockchain-based platform that allows individuals to securely share their orthopaedic health data with researchers or pharmaceutical companies who are developing new therapies. Each patient who provides data gets governance tokens as reward. These tokens can either be spent on premium services on the site or to vote on possible future directions of research. By giving patients control over their data, this approach not only enables them but also motivates them to contribute to medical research.

Improved Clinical Trials. One example of this is that a blockchain technology could potentially simplify patient recruitment for clinical trials. Researchers can quickly find potential volunteers who match the criteria of the study by allowing individuals to register their health profiles on a blockchain. Patients agree to join the network and are rewarded with governance tokens, which may be redeemed for exclusive medical insights or health services. This system enhances trust in clinical research and ensures transparency in the selection of participants.

Improved Transparency and Data Integrity In Studies. A research organization uses a blockchain to record all of the data associated with a multi-year study on the efficacy of a novel orthopaedic surgery method. To ensure the integrity of the research data, every data entry is time-stamped and unchangeable. Governance tokens are given to patients who provide their post-operative results to the study, encouraging a feeling of involvement and ownership in the investigation. This method encourages responsibility and transparency in medical research while also protecting the data.

Platforms for Decentralized Health Data. A decentralized marketplace where individuals can securely sell their de-identified health data to researchers or pharmaceutical companies. Blockchain technology ensures that each transaction is secure and that patients retain control over who can access their data. Patients are rewarded with governance tokens for every transaction and will be able to cash out of or use tokens for other services within the ecosystem. This marketplace allows data providers (the patients) to retain strict control over who accesses their health data while benefiting directly from them and democratizing access to important health data.

Patient-Driven Research Initiatives. Blockchain technology is deployed by a rare orthopedic disease patient advocacy group to set up a research fund in a way that aligns research with patient values. Patients donate data and are rewarded with governance tokens that allow them to vote on what research gets funded. The model promotes data sharing while having the research priorities set by those who will be most affected by the outcomes.

5.4 Internet of Things: Blockchain and the Internet of Medical Things in Orthopaedics

The Internet of Things (IoT) and its healthcare component called the Internet of Medical Things (IoMT) interrelate the virtual aspects with the physical to improve the quality of life and services [16].Connected wearable IoT devices, such as sensors attached to the body, track patients by monitoring a range of parameters and store the data securely within blockchain systems. Fitted on the wrist or chest — or integrated into prosthetics and external fixators — such devices provide the real-time status of recovery, deformities and rehabilitation. Data sharing is made seamless by communication protocols such as RFID, NFC, Bluetooth, and 5G. A great example is IoT: In orthopedics for instance, brings data health visualization from the operation table to normal day life, whereas blockchain ensures the data integrity. IoT, as well as blockchain, can unanimously be deemed as the decentralization and innovative method in the arena of healthcare, which generally improves the scope of patient care, personalized treatment and clinical outcomes through better integration of data as well as real time monitoring.

5.5 Technical Challenges

Blockchain technology faces scalability challenges, especially with proof-of-work (PoW) systems, limiting its ability to handle high transaction volumes needed for orthopedic registers. Interoperability issues arise when multiple healthcare providers use different blockchain systems, complicating data integration. While blockchain enhances security, its immutability raises privacy concerns, making it difficult to update or delete data, potentially conflicting with regulations allowing patients to modify or remove their information.

Regulatory and Compliance Issues. Compliance with data protection regulations such as the General Data Protection Regulation (GDPR) in the EU may be challenging. There is a fundamental clash between the immutable and decentralized nature of blockchain technology, and laws mandating that data must be editable or delectable. The absence of uniformity among blockchain technologies can challenge the regulatory compliance. Regulatory bodies may find it challenging to set guidelines that consider the diversity of blockchain use cases.

Financial Impediments. The deployment of Blockchain technology involves significant up-front investment – system integration, training, and infrastructure requirements. For many health care providers — and particularly small clinics or hospitals — the cost may be prohibitive. Ongoing Maintenance Cost– This is the amount for regular updates, maintenance, and implementation of security measures in a blockchain system. The need for specialist personnel to implement and manage blockchain networks drives the price even higher.

Realistic Considerations. The Benefits of Blockchain Must Be Clearly Explained Yet a shortage of qualified workers makes hiring or training new employees costly and time-consuming. In addition, orthopaedic records contain complex information such as images and reports, which the blockchain may not adequately accommodate at this time.

6 Conclusion

This paper explores the fundamentals of blockchain, including tokens, protocols, and its application in orthopedic surgery. Blockchain ensures secure data management, transparency, and efficiency, with token standards (ERC-20) enabling transactions and consensus protocols (PoW, PoS) enhancing security. In orthopedic surgery, blockchain improves patient data security, implant tracking, and supply chain management, ensuring trust, efficiency, and better surgical outcomes. As the technology advances, its role in healthcare transformation will continue to grow.

References

1. Ravani, A., Edupuganti, S., Pugh, J., Sushama, S.: Blockchain merging of Business and Technology. Applications of Blockchain Technology, 174–191 (2023).
2. Khan, U., An, Z. Y., Imran, A.: A Blockchain Ethereum technology-enabled digital content: Development of trading and Sharing Economy Data. IEEE Access, 8, 217045–217056 (2020).
3. Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., Leung, V. C.: Decentralized applications: The blockchain-empowered software system. IEEE Access, 6, 53019–53033 (2018).
4. Kaur, S., Chaturvedi, S., Sharma, A., Kar, J.: A research survey on applications of consensus protocols in Blockchain. Security and Communication Networks, 2021, 1–22 (2021).

5. Gemeliarana, I. G., Sari, R. F.: Evaluation of proof of work (POW) Blockchains Security Network on Selfish Mining. 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), (2018).
6. Jesus, E. F., Chicarino, V. R., de Albuquerque, C. V., Rocha, A. A.: A survey of how to use blockchain to secure internet of things and the stalker attack. Security and Communication Networks, 2018, 1–27 (2018).
7. Irresberger, F.: Coin concentration of proof-of-stake blockchains. SSRN Electronic Journal. (2018).
8. Papathanasiou, J., Petrov, I., Kashilska, Y., Kostov, K., Dzhafer, N.: Is telerehabilitation a top priority for the Bulgarian healthcare system in the post covid-19 ERA? Health Policy and Technology, 11(4), 100664 (2022).
9. Tan, T. L., Salam, I., Singh, M.: Blockchain-based healthcare management system with two-side verifiability. PLOS ONE, 17(4) (2022).
10. Delaunay, C.: Registries in orthopaedics. Orthopaedics & Traumatology: Surgery & Research, 101(1) (2015).
11. Thomson, C., Beale, R.: Is Blockchain Ready for Orthopaedics? A systematic review. Journal of Clinical Orthopaedics and Trauma, 23, 101615 (2021).
12. Porsdam Mann, S., Savulescu, J., Ravaud, P., Benchoufi, M.: Blockchain, consent and prosent for Medical Research. Journal of Medical Ethics, 47(4), 244–250 (2020).
13. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., Choo, K.-K. R.: Applications of blockchain in ensuring the security and privacy of Electronic Health Record Systems: A survey. Computers & Security, 97, 101966 (2020).
14. Kumar, R., Arjunaditya, Singh, D., Srinivasan, K., Hu, Y.-C.: AI-powered blockchain technology for Public Health: A Contemporary Review, open challenges, and future research directions. Healthcare, 11(1), 81(2022).
15. Meschini, C., Cauteruccio, M., Oliva, M. S., Sircana, G., Vitiello, R., Rovere, G., Muratori, F., Maccauro, G., Ziranu, A.: Hip and knee replacement in patients with ochronosis: Clinical experience and literature review. Orthopedic Reviews, (2020).
16. Sadoughi, F., Behmanesh, A., Sayfouri, N.: Internet of things in medicine: A systematic mapping study. Journal of Biomedical Informatics, 103, 103383 (2020).