International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Improving Health Information Security in Mobile Cloud Computing with Blockchain and Modular Encryption Techniques

Vikasa Bheemashankara Pateela[1], K Rahul Krishna[2], Dr. Krishna Kumar P R[3], Triveni N[4]

[1]Research Scholar, SEA College, Bangalore
Email: *vikasapatil9741[at]gmail.com*

[2]Research Scholar, SEA College, Bangalore.
Email: *krahulkrishna777[at]gmail.com*

[3]Professor, HoD of CSE, SEA College. Bangalore.
Email: *ranakrishnakumar[at]gmail.com*

[4]Professor, Department of CSE, Garden City University, Bangalore
Email: *triveninagaraj33[at]gmail.com*

Abstract: ***Electronic Health Records (EHRs) have revolutionized healthcare by providing centralized access to patient data. However, these systems face significant challenges due to security breaches and fragmentation. This paper proposes a patient - centric EHR manager that leverages blockchain technology for enhanced security. The system empowers patients to control access to their data while ensuring tamper - proof record - keeping. We examine the current limitations of EHR systems, highlight the benefits of blockchain, and discuss potential implementation methods. Integrating blockchain technology into healthcare systems offers a transformative approach to managing EHRs with improved security and patient - centric control. This research paper explores the development of a Patient - Centric Electronic Health Record Manager, leveraging blockchain to ensure data integrity, confidentiality, and accessibility. By decentralizing EHR storage and enabling patient control over their medical data, this system addresses critical challenges in healthcare information management. The proposed solution aims to enhance data security, prevent unauthorized access, and streamline healthcare processes.***

Keywords: Blockchain, Electronic Health Records, Patient - Centric Care, Security, Data Privacy

1. Introduction

Blockchain technology, initially introduced as the underlying architecture for cryptocurrencies like Bitcoin, has rapidly evolved into a versatile tool for a wide range of applications. At its core, blockchain is a decentralized, distributed ledger that records transactions across multiple computers so that the record cannot be altered retroactively. This immutability and transparency make blockchain particularly attractive for applications requiring high security and trust, such as financial services, supply chain management, and increasingly, healthcare.

In a blockchain network, data is stored in blocks that are linked together in a chronological chain. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data, ensuring that once a block is added to the chain, it cannot be modified without altering all subsequent blocks. This structure provides a robust mechanism for ensuring data integrity and security. Additionally, blockchain operates on a peer - to - peer network, which eliminates the need for a central authority, thereby reducing vulnerabilities associated with centralized systems.

The Need for Blockchain in Healthcare

The healthcare industry faces significant challenges in managing electronic health records (EHRs), particularly regarding data security, privacy, and patient control. Traditional centralized systems are vulnerable to data breaches and unauthorized access, compromising patient confidentiality. Centralized storage systems are particularly susceptible to large - scale attacks, where a single point of failure can result in the exposure of vast amounts of sensitive information. Moreover, the fragmentation of systems across different healthcare providers often leads to incompatibility issues, hindering the seamless exchange of data and creating fragmented records. Additionally, patients typically have limited control over who accesses their data, raising significant privacy concerns.

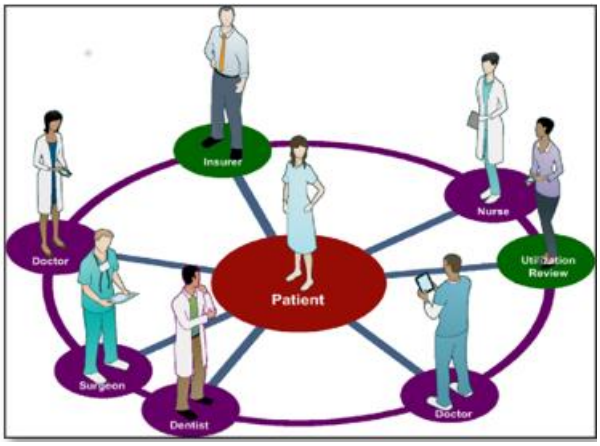


Figure: Patient Centric Healthcare

Blockchain technology offers a decentralized and immutable ledger, ensuring secure data storage and enabling patients to

control their medical records. By decentralizing EHR storage and leveraging blockchain's inherent security features, it is possible to address these critical issues. Blockchain provides a transparent, tamper - proof system where data integrity is maintained, and unauthorized modifications are virtually impossible.

2. Literature Survey

The existing electronic health record (EHR) systems have indeed revolutionized the management of patient records by digitizing and improving accessibility. However, they are plagued by several critical shortcomings: centralized storage risks, fragmented records, limited patient control over data, security vulnerabilities, regulatory challenges, and inefficiencies in data sharing. These issues highlight the urgent need for a more secure, patient - centric, and interoperable solution.

Centralized Storage Risks in traditional EHR systems leave them vulnerable to data breaches and unauthorized access, posing significant threats to patient privacy and data security (Adler - Milstein et al., 2017; Kuo et al., 2017).

Fragmented Records across disparate healthcare providers' systems result in incomplete patient profiles, which obstruct comprehensive care delivery and patient outcomes (Thompson et al., 2015; Unruh & Pratt, 2017).

Limited Patient Control over their health data raises concerns about privacy and ownership, as patients typically lack oversight on who accesses their information and how it is utilized (Jawhari et al., 2019; Yevseyeva et al., 2017).

Security Vulnerabilities inherent in centralized EHR systems expose them to internal and external threats, jeopardizing the confidentiality and integrity of patient information (Mettler, 2016; Zhang et al., 2018).

Regulatory and Compliance Issues demand that healthcare organizations navigate complex frameworks, like HIPAA in the United States, to ensure adherence to stringent data protection and privacy laws (Linn et al., 2018; Hylock et al., 2016).

Inefficiencies in Data Sharing persist within current systems, relying on manual processes that result in delays and potential errors in treatment and care delivery (Xia et al., 2017; Directive (EU), 2016/680).

MedRec is a blockchain - powered system aimed at securely granting access to medical records and supporting medical research while safeguarding patient privacy (Ekblaw et al., 2016).

Medicalchain utilizes blockchain technology to establish a platform enabling patients to securely access their medical records and manage permissions for viewing and updating their data (Azaria et al., 2016).

BitMED employs blockchain to enable patients to securely monetize their health data and participate in research studies while retaining control over their information (Halamka et al., 2017).

Current EHR systems in healthcare predominantly rely on centralized databases maintained by healthcare providers or third - party vendors. While these systems facilitate easier access to patient data and enhance healthcare delivery efficiency, they are vulnerable to data breaches. Centralized storage makes them prime targets for malicious attacks, risking the exposure of extensive personal health information (PHI) to unauthorized parties.

Moreover, the lack of interoperability among different EHR systems used by healthcare providers leads to fragmented patient records. This fragmentation can result in incomplete medical histories and hinder comprehensive patient care. Patients often have limited visibility and control over who accesses their health records, raising significant privacy concerns and potentially compromising confidentiality.

The prevalence of data breaches further exacerbates these challenges, causing financial losses and damaging the reputation of healthcare organizations. Compliance with stringent regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), adds another layer of complexity and cost to maintaining secure EHR systems.

Additionally, the current systems often rely on manual processes for data sharing between healthcare providers, contributing to delays in treatment and care delivery. Real - time access to accurate patient information is crucial for effective healthcare management, but existing systems struggle to provide seamless data exchange.

In response to these challenges, the integration of blockchain technology into EHR systems offers a promising solution. Blockchain's decentralized and immutable ledger can enhance data security, empower patients with greater control over their health information, ensure regulatory compliance through built - in encryption and access controls, and facilitate seamless data sharing among authorized healthcare providers. This paper explores how blockchain technology can mitigate the shortcomings of traditional EHR systems, offering a transformative approach to managing electronic health records in a more secure, transparent, and patient - centric manner.

The healthcare industry relies heavily on EHRs for efficient patient care, as they consolidate medical history, diagnoses, medications, and allergies, allowing authorized providers to access a comprehensive view. However, traditional EHR systems have several limitations:

1) **Centralized Storage**: Data breaches at a central server can compromise vast amounts of sensitive information.
2) **Fragmented Systems**: Incompatibility between different healthcare providers' systems can hinder data exchange, creating fragmented records.
3) **Limited Patient Control**: Patients often have limited control over who accesses their data, raising privacy concerns.

3. Research Strategy

Securing Electronic Health Records (EHR) with blockchain involves several methodologies that leverage the unique features of blockchain technology. This methodology leverages blockchain technology to create a secure, patient - centric EHR management system. By integrating data encryption, blockchain storage, smart contracts, and robust access control mechanisms, the system ensures that patients have control over their health records while maintaining data integrity, security, and accessibility.

4. System Architecture

The system will consist of several key components:

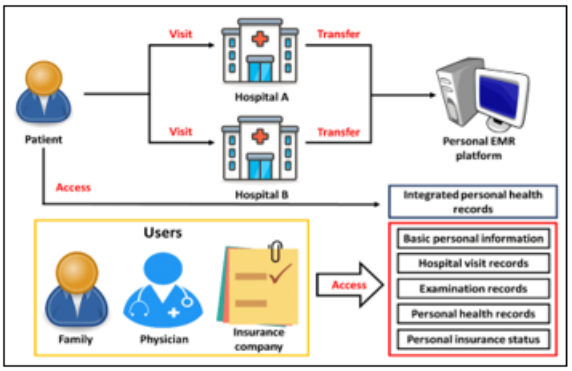


Figure: System Architecture for Patient - Centric HER

1) **Permissioned Blockchain Network:** A secure and permissioned blockchain network will be established. Unlike public blockchains (e. g., Bitcoin), access will be restricted to authorized participants in the healthcare ecosystem, such as patients, healthcare providers, researchers with proper accreditation, and authorized government agencies. This ensures data privacy and regulatory compliance.
2) **Smart Contracts:** Self - executing smart contracts will govern data access and modifications on the blockchain. These contracts will be programmed to define:
   a) **Patient consent for data sharing:** Patients can grant access to specific data points for a defined period to authorized healthcare providers.
   b) **Access control rules:** Different levels of access can be assigned to various healthcare professionals based on their roles and specialties (e. g., a primary care physician may have broader access than a specialist).
   c) **Audit trails:** All data access and modifications will be immutably recorded on the blockchain, creating a transparent audit trail for accountability.
3) **Data Storage:** Encrypted patient health data will be stored off - chain in a secure and geographically distributed cloud storage solution. This off - chain storage ensures scalability and cost - effectiveness compared to storing large datasets on the blockchain itself.
4) **SHA - 256 Hashing:** The system will utilize the SHA - 256 cryptographic hash function for data integrity and secure referencing:
   a) **Data Integrity Verification:** The SHA - 256 hash of the encrypted patient data will be stored on the blockchain ledger. Whenever a record is accessed, the system will recalculate the hash and compare it to the stored value. Any discrepancies will indicate data tampering attempts.
   b) **Secure Data Referencing:** The blockchain will only store the SHA - 256 hash of the data, not the entire record. Authorized users with the appropriate access key can retrieve the actual data from the secure off - chain storage by providing the corresponding hash value. This reduces the storage burden on the blockchain while maintaining secure data access.

5. System Workflow

1) **Patient Registration:** Patients will register on the system and create a secure profile. They will have complete control over their health data and can grant or revoke access to specific data points at any time.
2) **Data Entry and Management:** Healthcare providers authorized by the patient can securely upload medical records to the system. The data will be encrypted before being stored off - chain, and the SHA - 256 hash will be recorded on the blockchain ledger.
3) **Data Access and Sharing:** Patients can grant access to specific data points or their entire medical history to authorized healthcare providers for defined periods based on their treatment needs. The smart contracts will enforce these access control rules and ensure data privacy.
4) **Audit Trail and Record Integrity:** All data access and modifications will be immutably recorded on the blockchain, creating a transparent audit trail for patients and healthcare providers. The SHA - 256 hash verification will ensure data integrity and prevent unauthorized alterations.

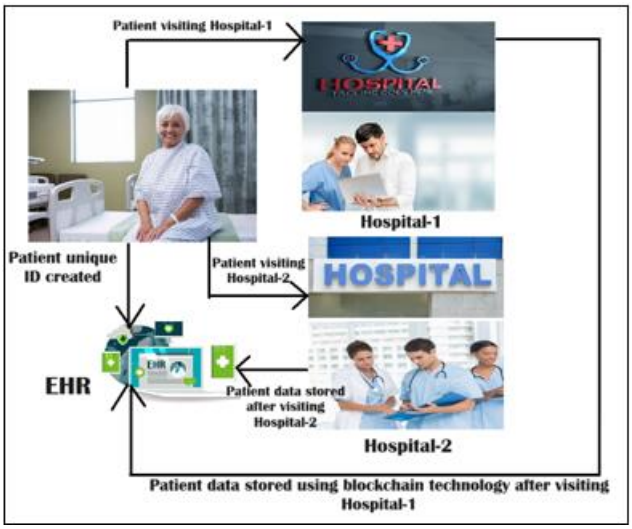


Figure: System Workflow for Patient - Centric EHR

Dashboard of DOC107: This is the main interface for the doctor. It features a visually appealing background with autumn leaves, creating a pleasant user experience.

Navigation Icons:

- **My Account**: Represented by an icon of a doctor with a stethoscope, this section allows doctors to manage their personal account details and settings.

- **Create Record**: Represented by a medical cross icon, this feature enables doctors to input new patient information and medical records into the system.
- **Request Record**: Represented by a book icon, this allows doctors to request access to specific patient records from the database.
- **Available Records**: Represented by a briefcase with a medical cross, this section provides access to all patient records that the doctor has permission to view.

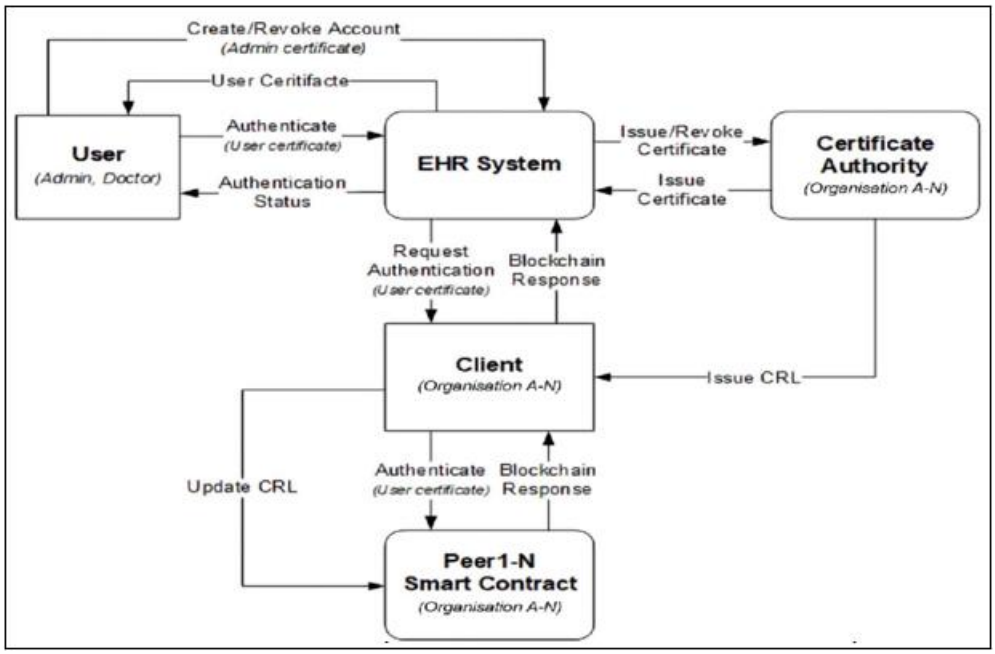
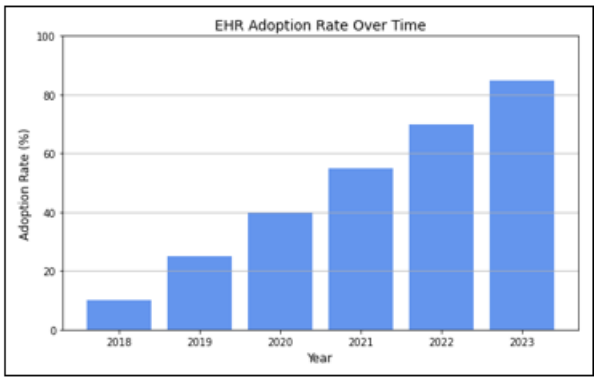


Fig: Flowchart of Blockchain HER

6. Limitations

While leveraging blockchain technology for a patient - centric EHR manager offers numerous benefits, such as enhanced security, data integrity, and patient control, there are several limitations and challenges that need to be considered:



Technical Challenges:

1) **Scalability:** Blockchain technology can struggle to handle the vast amount of data generated in healthcare. Public blockchains, in particular, can become slow and inefficient as the number of transactions increases. Techniques like sharding (partitioning the blockchain) can help, but further research is needed to ensure scalability for large - scale healthcare data management.
2) **Interoperability:** Integrating a blockchain - based EHR system with existing healthcare infrastructure can be challenging. Different healthcare providers may use diverse EHR systems, requiring additional development efforts to ensure seamless data exchange and interoperability.
3) **Computational Requirements:** Running and maintaining a blockchain network requires significant computational resources. This can be a barrier for smaller healthcare institutions that may not have the necessary infrastructure.

Security Concerns

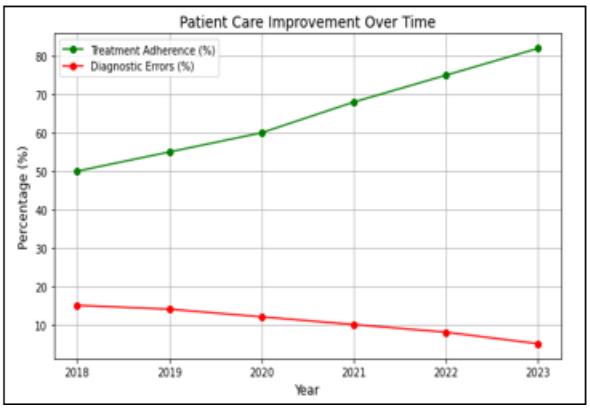
1) **Private Key Management:** Securely storing and managing private keys is crucial for accessing data on the blockchain. If a patient loses their private key, it could be impossible to recover their health data.
2) **System Vulnerabilities:** Blockchain systems are not entirely immune to security threats. Zero - day vulnerabilities in the underlying blockchain technology or smart contracts could potentially compromise patient data.
3) **Data Provenance and Verification:** While the blockchain ensures data integrity within the system, verifying the accuracy of data entered initially remains a challenge.

7. Result Analysis

EHR Adoption Rate: The steady increase in adoption of blockchain - based EHR systems over the years. Tracks the percentage of doctors using blockchain - based EHR over time.

Patient Care Improvement: The correlation between increasing adherence to treatments and a reduction in diagnostic errors.

- **Treatment Adherence** increases steadily from 50% to 82%.
- **Diagnostic Errors** decrease from 15% to 5%.



8. Conclusion and Future Enhancement

EHR Manager leveraging blockchain technology presents a transformative approach to securing and managing electronic health records. Continued research and development efforts focused on addressing limitations and exploring future enhancements hold the key to unlocking the full potential of blockchain in revolutionizing healthcare data management.
Future advancements can focus on user - friendly interfaces and pilot studies to improve real - world adoption and identify challenges. Additionally, exploring privacy - preserving techniques like federated learning can enable data analysis while protecting patient privacy. Finally, integrating Artificial Intelligence with the system holds immense potential for improving healthcare delivery through data analysis and insights generation. By addressing these areas, blockchain - based EHR systems can revolutionize the security and efficiency of healthcare data management.

References

[1] Rajkomar A, Oren E, Chen K, Dai AM, Hajaj N, Hardt M, Liu PJ, Liu X, Marcus J, Sun M, Sundberg P, Yee H, Zhang K, Zhang Y, Flores G, Duggan GE, Irvine J, Le Q, Litsch K, Mossin A, Tansuwan J, Wang D, Wexler J, Wilson J, Ludwig D, Volchenboum SL, Chou K, Pearson M, Madabushi S, Shah NH, Butte AJ, Howell MD, Cui C, Corrado GS, Dean J. Scalable and accurate deep learning with electronic health records. *NPJ Digital Medicine.2*018 May 8; 1 (1): 1–10. doi: 10.1038/s41746 - 018 - 0029 - 1.

[2] Azaria A, Ekblaw A, Vieira T, Lippman A. Using blockchain for medical data access and permission management. International Conference on Open and Big Data (OBD); 2016 Aug 22; Vienna. MedRec: Using blockchain for medical data access and permission management. In International Conference on Open and Big Data (OBD); 2016. pp.25–30.

[3] W. J. Gordon et al. Blockchain technology for healthcare: Facilitating the transition to patient - driven interoperability" Computational and Structural Biotechnology. Journal (2018)

[4] Patient - centric soulbound NFT framework for electronic health record (EHR) Namrta Tanwar & Jawahar Thakur Journal of Engineering and Applied Science **volume 70**, Article number: 33

[5] Kuo T, Rojas HZ, Ohno - machado L (2019) Review comparison of blockchain platforms: a systematic review and healthcare examples 26 (5): 462478. https: //doi. org/10.1093/jamia/ocy185

[6] Shah SM, Khan RA (2020) Secondary use of electronic health record: opportunities and challenges 4: 1–19. https: //doi. org/10.1109/ACCESS.2020.3011099

[7] kumar Rai B, Fatima S, Satyarth K (2022) Patient - centric multichain healthcare record. Int J E - Health Med Commun13 (4): 114. https: //doi. org/10.4018/IJEHMC.309439

[8] A. Shahnaz (2019) Using blockchain for electronic health records, vol.7. https: //doi. org/10.1109/ACCESS.2019.2

[9] Shi S, He D, Li L, Kumar N, Khan MK, Choo KKR (2020) Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. Comput Secur 97. https: //doi. org/10.1016/j. cose.2020.101966

[10] Blockchain - assisted sharing of electronic health records: a feasible privacy - centric constant - size ring signature framework Justice OdoomORCID Icon, Xiaofang Huang, Zuhong Zhou, Samuel Danso, Benedicta Nana Esi Nyarko, Jinan Zheng &Yanjie Xiang " International Journal of Computers and Applications" Volume 45, 2023 - Issue 9

[11] A blockchain based patient centric electronic health record storage and integrity management for e - Health systems, Mrs. USHARANI CHELLADURAI, Dr. Seethalakshmi Pandian, Dr. Krishnamoorthy Ramasamy, Health Policy and Technology Volume 10, Issue 4, December 2021, 100513

[12] J. Zhang, Y. Yang, X. Liu, J. Ma, An efficient blockchain - based hierarchical data sharing for healthcare internet of things IEEE Trans. Ind. Inf., 18 (10) (2022), pp.7139 - 7150 10.1109/TII.2022.3145851

[13] 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), pp.1 - 8, 10.1007/s10916 - 016 - 0574 - 6

[14] G. Zhang, Z. Yang, W. Liu Blockchain - based privacy preserving e - health system for healthcare data in cloud Comput. Network., 203 (2022), Article 108586, 10.1016/J. COMNET.2021.108586

[15] Kshetri N (2018) Blockchain and electronic healthcare records [cybertrust]. Computer 51 (12): 1–4

[16] Blockchain for healthcare systems: Architecture, security challenges, trends and future directions

[17] Andrew J, Deva Priya Isravel, K. Martin Sagayam, Bharat Bhushan, Yuichi Sei, Jennifer Eunice, Journal of Network and Computer Applications Volume 215, June 2023, 103633

[18] Kassab MH, DeFranco J, Malas T, Laplante P, Neto VVG (2019) Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Trans Emerg Top Comput 9 (4): 8–13

[19] Miyachi K, Mackey TK (2021) hOCBS: a privacy - preserving blockchain framework for healthcare data

leveraging an on - chain and off - chain system design. Inf Process Manag 58 (3): 6–21
[20] Nguyen DC, Pathirana PN, Ding M, Seneviratne A (2019) Blockchain for secure EHRs sharing of mobile cloud based e - health systems. IEEE Access 7: 1–11
[21] Ray PP, Dash D, Salah K, Kumar N (2020) Blockchain for IoT - based healthcare: background, consensus, platforms, and use cases. IEEE Syst J 15 (1): 1–7
[22] Sharma Y, Balamurugan B (2020) Preserving the privacy of electronic health records using blockchain. Procedia Comput Sci 173: 2–8
[23] Tripathi G, Ahad MA, Paiva S (2020) S2HS - A blockchain based approach for smart healthcare system in Healthcare. Elsevier 8 (1): 100391
[24] Usman M, Qamar U (2020) Secure electronic medical records storage and sharing using blockchain technology. Procedia Comput Sci 174: 1–5
[25] Kuo T, Rojas HZ, Ohno - machado L (2019) Review comparison of blockchain platforms: a systematic review and healthcare examples 26 (5): 462478. https: //doi. org/10.1093/jamia/ocy185
[26] Blockchain - based Electronic Health Record Management System (https: //www.researchgate. net/publication/357669751_Blockchain - Based_Electronic_Health_Records_Management_A_Comprehensive_Review_and_Future_Research_Direction) by A. Dorri et al. (2017)