Privacy Preserving Electronic Health Record with Consortium Blockchain

Adri Gautama
Doctoral Program of Information System, School of Postgraduate Studies,
Diponegoro University
Semarang, Indonesia
agautama@students.undip.ac.id

Adian Fatchur Rochim
Department of Computer Engineering
Diponegoro University
Semarang, Indonesia
adian@ce.undip.ac.id

Luhur Bayuaji
Computer Science
Budi Luhur University
Jakarta, Indonesia
luhur.bayuaji@budiluhur.ac.id

***Abstract*— Every patient has health record, it was written as statement of patient's conditions, treatments, and medications, and nowadays it is become digitalized, it can be copied and shared easily, but the nature of EHR is private, not for public, private between patients and healthcare provider. Privacy preserving can be done by implementing Blockchain network for storing EHR, only authorized users or nodes can access and write data to the network. New block in blockchain created as per consensus among nodes, every node can join a blockchain network if it is public, to meet a consensus required resources intensive cryptographic challenge, in private blockchain, only selected can join and involved in the network or specific transaction. In healthcare, data privacy is the main concerned, need a secure, scalable, and efficient blockchain hence implementing consortium blockchain is perfect match for EHR where multiple healthcare provider can operate in a single platform to conduct transaction or sharing EHR among members. This study analyzes 15 articles derived from IEEE Explore, Science Direct and Scopus by implementing screening with keyword Consortium Blockchain and EHR and proposing new blockchain model accommodating solution for challenges on access, storage, sharing, privacy, and performance.**

Keywords — e-health, EHR, Privacy, Consortium Blockchain.

I. Introduction

When human as an individual and social being can live their life effectively, then they are in a condition where structurally, functionally, and emotionally can be called in a healthy [1]. To have a healthy condition, humans have to implement a good lifestyle, eating healthy food, good rest, and periodic exercise. This will create a good immune system to fight disease and infection, but human has susceptibility to bacteria, virus, disease, and toxin, it can make human sick. When we sick, we seek care from medical institutions, doctors and nurses will try to provide necessary care to get us back to a healthy condition. Doctors will make observations, monitoring, testing, resulting in a medical record about patient, about the symptoms, conditions, and treatments.

With the rapid growth of Information Technology (IT), and proven fact of increasing efficiency, this traditional record of medical record, now accessible online, become Electronic Health Record (EHR) which reduces the storage cost, and allow managing medical data of the patient with addition of implementing safety and privacy [2]. Record about patient is private, not for public, so the record must be secured, can be identified on who can create and modify it, cannot be tampered, and can be shared (under specific condition). It is all can be done by implementing Blockchain distributed ledger technology.

This study will focus on implementation of consortium blockchain in solving challenges in EHR, it is organized as follows: first section about introduction on blockchain and EHR, second section explain about how we did the literature review, third section on research result, extracting data and finally last section on conclusion and future work.

A. Blockchain

Blockchain was first introduce as a technology behind bitcoin [3], a payment based on cryptographic proof, no need for intermediary party, direct transaction between two parties and non-reverse. Blockchain began as the technology that underpins bitcoin, first digital currency without middleman with intention to avoid double spending and allow online payments without going via a financial institution, transaction will be timestamped by the network, it will be hashed and formed a chain related to previous chain, it's a very strong chain, to change or modify it, one must redo the consensus process [3]. Blockchain now has expand not only to be implemented in cryptocurrency but has a wide implementation on all aspects that required a secured transaction, data confidentiality, integrity, sharing and privacy preservation [4].

Figure 1, blockchain is chain of blocks, blocks which are connected sequentially, with each having a hash, the timestamped hash of recent valid transactions, and the preceding block's hash. began with the genesis block (first block). Additional block added once participating nodes has reach a consensus and all participating nodes updating their blockchain, information is not stored in one central service, it is distributed, hence blockchain becomes more difficult to tamper.

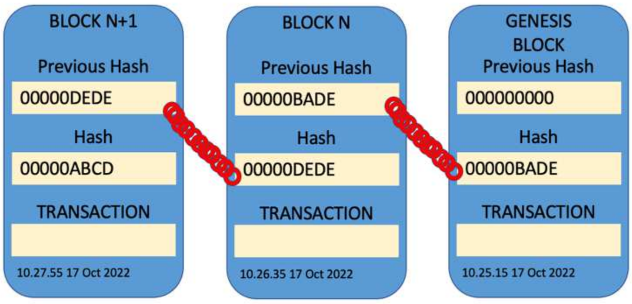

Fig 1. Block of Blockchain

1) Consensus

All participants node needs to have an agreement on present state of the data, adding new blocks need to be verified by all participating node before they can be added to the chain, these two conditions defined consensus algorithms. Different kind of consensus algorithms has their advantages and disadvantages with their various mechanism with the same destination, ability to verify transaction and maintain the block security.

2) Blockchain Platform

A blockchain platform consist of all the software and hardware require to deploy the distributed ledger. On these studies, we have identified two most used blockchain platform, Ethereum and Hyperledger.

a) Ethereum

Ethereum was created to overcome limitation of bitcoin scripting language and enable designers to create customized consensus-based systems that leverage from the scaling, standards, functionality, simplicity of implementation, and compatibility provided by such several models at the same time. With an integrated Turing-complete programming language, anybody may design smart contracts and decentralized apps with full customization with their own preferences on format and algorithm of transition [5]. Ethereum has similarity with bitcoin.

b) Hyperledger

It was all started in 2015, when different companies have one common interest in blockchain has comes up with an agreement that they can achieve more by working together instead of working individually. Hyperledger served as a greenhouse, brings together all users, developers, and vendors with same purpose: learning, developing, and using enterprise blockchains [7]. Hyperledger Fabric, an open source blockchain for business with advanced privacy control, only data want to shared will be shared among permissioned (known) participants. Smart contract is used to document the process automatically, loaded with self-executing code, transaction is trackable and irreversible, creating trust between organizations, saving time, reduce cost and risks [8].

3) Blockchain Type

Based on its nature, permission given, authorization, new block creation, selection of validator or how to join the network, we can classify blockchain type into following three: public, private and consortium blockchain [9], [10].

Private blockchain is not open, it is a closed systems only selected participants can join hence creating improved security, authorization, permissions, and accessibility. It is running with authorized nodes, no one from outside of the private network able to access information and transaction, making it fully controlled by one organization [11].

Public blockchain is open, any node can become member, all members can do all the things [12], each node could take part in the consensus process, all transactions are available to the public and saved in a vast number of participants, making tampering practically difficult.

Private blockchain is centralized (managed by a single party), whereas consortium blockchain, is federated, has feature from private and public. To meet a consensus, public blockchain is permissionless but private and consortium blockchain are permissioned as not every node can join and contribute in the consensus mechanism [11].

Consortium blockchain is built by numerous organizations and is somewhat decentralized because only small number of nodes will take the responsibility to determine consensus. Members are not granted to a single entity, it is granted to a group of nodes, offering significant degree of control, faster processing and makes it more efficient and secure.

It is a hybrid, combine private and public blockchain features and has advantages [13]:

- Nodes and users can join if they have the required permissions.
- Easy to manage and enforce policies as it is governed by consensus protocol.
- Low resources on consensus algorithm
- Provide confidentiality
- High throughput with the implementation of authorized validator nodes.
- Fault tolerance.
- Enterprise level blockchain

B. EHR

When a patient visiting a healthcare institution to get treatment, the institutions need information detail about the patient or profiling, this profile will be recorded along with symptoms, laboratory, treatment, and medicine (medical record). It was written on paper, with the increase usage of computer, the medical record then become electronic medical record (EMR), still same record, but store at a specific computer and owned by the institution, not for shared outside the institution. When patient running a medical consultation in hospital A, patient will have EMR at hospital A, then patient might go to hospital B, then patient will also have EMR at hospital B, EHR was created to streamlined record about patient even though located at separated hospital, patient can go to any hospital, by providing authorization, patient can authorize doctor to read patient's EHR, and this EHR can be linked securely over any network [14]. Using blockchain in an EHR can overcome challenges on unauthorized access, integrity, and interoperability, but in the step of creating a block, required high resources like in the mining process, to reduce the computational cost, [15] proposing a lightweight blockchain framework, a mining mechanism rely on leveling of difficulty based on leading zero.

II. Research Method

We search through three major journal databases, IEEE Explore, Scopus and Science Direct, about implementation of consortium blockchain in EHR, on first step, we have 276 articles, with 78 of them were duplicate, which 198 will be screened by abstract on relevance to the study and apparently 183 are not aligned with the focus study on specific type of blockchain implemented in EHR, and finally by following PRISMA, we have 15 articles to be included in this review study as shown in Fig 2. Literature articles with all the summarized proposed solutions are listed in Table 1.

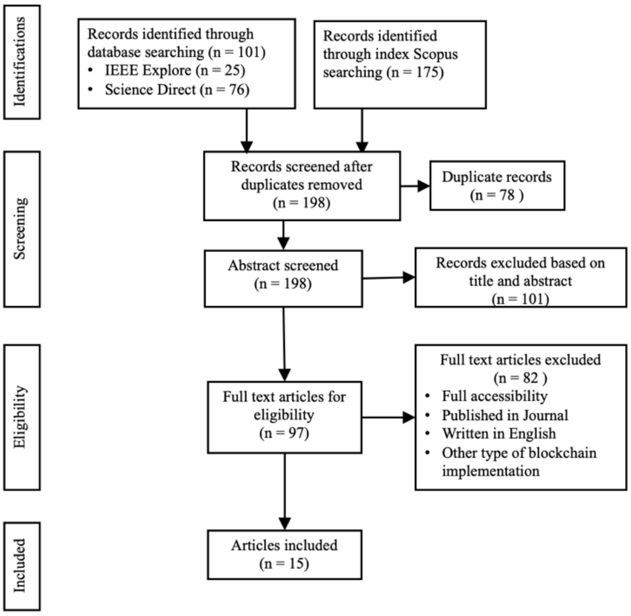
Identifications
Screening
Eligibility
Included
Records identified through database searching (n = 101)
• IEEE Explore (n = 25)
• Science Direct (n = 76)
Records identified through index Scopus searching (n = 175)
Records screened after duplicates removed (n = 198)
Duplicate records (n = 78)
Abstract screened (n = 198)
Records excluded based on title and abstract (n = 101)
Full text articles for eligibility (n = 97)
Full text articles excluded (n = 82)
• Full accessibility
• Published in Journal
• Written in English
• Other type of blockchain implementation
Articles included (n = 15)

Fig 2. Literature Review

There is no favorite journal among the literature in Table 1, but we can identify that these 10 journals are the best option to publish articles related to Blockchain and EHR. Article in the literature identified being published from 2019 to 2022 as show on Fig 3., we managed to identify 3 articles from 2019, 2 articles from 2020, 8 articles from 2021 and 2 articles from 2022.

TABLE 1. Journal name and articles in literature

Journal Name	Articles
Sensors	2
Biomed Res Int	2
Applied Sciences	2
IEEE Access	2
Healthcare Informatics Research	2
Computer Science and Information Systems	1
Informatica	1
Journal of Healthcare Engineering	1
IEEE Transactions on Industrial Informatics	1
Electronics	1

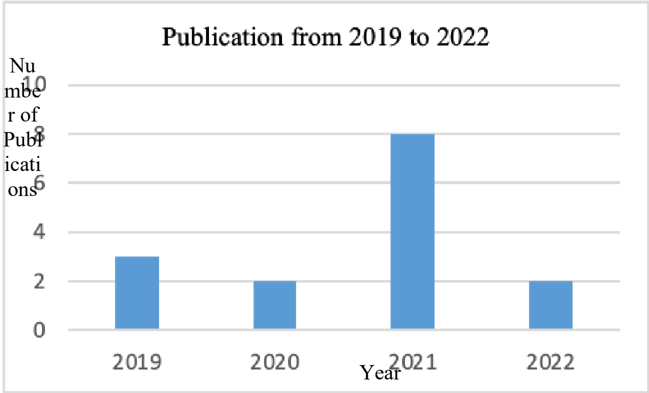

Fig 3. Literature article based on publication year

Sharing electronic medical records (EMR) with patients' authorization, improves control over patients' data by implementing proxy re-encryption algorithm, secure access to blockchain data was realize by using chain code specified to its attributes by blockchain networking scanner executed digitally and automatically. With applying various attribute of role, a separate chain codes will be created to control access, this different level of chain code can be applied using attribute access control. Sharing EMR and secure access achieved by implementing Elliptic Curve Digital Signature Algorithm (ECDSA) mixed with proxy re-encryption combined with attribute access control [16].

Electronic rehabilitation medical record (ERMR) is contributing to rehabilitation treatment to a patient, doctor can effectively assess and analyze patient's and defining next stage of rehab, sharing of ERMR is the main concerned, thus implementing blockchain [17].

Different hospital has different data management and exchange protocol because the lack of no standard data management has created an interoperability issue, blockchain with its capability of decentralized ledger, different level of access and always tracking all transactions, implying the right consensus algorithm will create full control on the network, it is the best solution for this issue [18]. Sharing medical service records between different clinical health provider and maybe in a different country is the main challenge, patient's records by different clinics is not accessible to the doctor in a single location, and difficult to secure widespread data residing in different locations. Every record is globally connected, making it available, especially for patient who travel in different country after validating required authentication on Shibboleth identity management systems [19].

It is difficult to maintain data security sharing in a cloud based EMR, to securely shared EMR, EMR will be store in ciphertext of the original EHR and blockchain will save traceable log information and EHR index by combining cloud storage and consortium blockchain [20]. As an addition to a cloud based EHR, it is used as identity-based signature method with various authority that can withstand a collusion attack [21].

When a patient has multiple EHR hosted by multiple healthcare provider, there are issues on how to access this scattered patient data. It can be solved by developing a system for accessing patient records across EHR, composing a distributed system with consortium blockchain, peer nodes sharing same ledger contain patient's record address in an EHR, each patient will have unique certificate given by local CA, which collaborate in a network channel, and a proxy re-encryption mechanism is used to ensure patient privacy [22].

Medical on Demand (MoD) is providing cloud-based telemedicine services, patient subscribe and unsubscribe to a different MoD service can be happened, dependent on patient's needs which impacted on cost of membership management. To allowed patient to have full ownership of enrolling and leaving anytime and changing their access policies by demand, with no need for unrelated patients to rebuild their private-key in the registration process or update, because an independent update attribute-based encryption (ABE) scheme will be applied with multiple authorities [23].

TABLE 2. Literature Articles – Proposed Solution

Author	Proposed Solution	Access	Sharing	Storage	Privacy	Performance	Supply chain
W. Chen, 2021 [16]	To address the issue of EMR security sharing, a consortium blockchain and proxy re-encryption are being used.	✓	✓				
J. Zhang, 2021 [17]	ERMR sharing system based on blockchain for distributed storage, privacy protection, data security, consistency, traceability, and ownership.		✓				
Z. Dodevski, 2021 [18]	Exchanging information between healthcare institutions and insurance by implementing smart contracts, integration layer and distributed application.		✓				
G. Q. Butt, 2022 [19]	Making medical data available, especially for patients who travel in different countries.		✓				
Q. Qin, 2021 [20]	Proposing a better PBFT mechanism, data encrypted stored in cloud and blockchain stored the index.		✓	✓			
F. Tang, 2019 [21]	With multiple authorities, to implement signature based on identity to overcome attack from N from N 1 authorities.	✓					
D. Tith,2020 [22]	Each patient will have individual certificate given by local CA and to protect their privacy, a proxy re-encryption is implemented.	✓	✓				
R. Guo, 2019 [23]	A blockchain-based multi-authority with independent-update for distributed telemedicine system.	✓					
A. Ali, 2021 [24]	Multiple Certificate of Authority to give policy update flexibility in term or recording or invoking policy.	✓					
P. K. Bharimalla, 2021 [25]	A Blockchain Electronic Healthcare Record (EHR) solution built on Hyperledger fabric that is combined with NLP and Machine Learning to provide useful features for users.	✓					
D. Tith, 2020 [26]	Patient implementing purpose-based consent, to validate doctor's access to patient records				✓		
D. el Majdoubi, 2021 [27]	Framework named SmartMedChain, data stored in IPFS and utilizing smart contracts to realize privacy preserving and accountability of a smart healthcare.		✓	✓	✓		
A. P. Singh, 2021 [28]	Using JavaScript-based smart contracts, to create an architecture of healthcare systems applying decentralized ledger but with patient centric in mind.				✓	✓	
F. Jamil, 2019 [29]	Fake drugs, pharmaceutical supply chain using blockchain.						✓
N. R. Pradhan, 2022 [30]	Multi-hosted testbed and performance evaluation with improved transaction ordering algorithms like as Kafka and RAFT, fault tolerance is achieved.					✓	

Control of accessing the EHR is needed as access to the EHR is only given to authorized entity, by implementing multiple certificates of authority and proposed with implementing smart contracts and access EHR securely [24]. Implementing blockchain to overcome issues of access, storage and transfer and AI/ML with useful features like converting old paper based medical records into EMR or converting handwritten prescriptions into digital text [25].

Patient's consent to access their EHR is critical issue, to better manage patient's consent, and avoiding unintentional usage of EHR, e-consent model was proposed, utilizing purposed based access control scheme. Blockchain is utilized to store information about patient, consents, data access and chain code managing patient consent, doctor who wants to access EHR will be validated by crosschecking doctor's profile with patient's consent that already recorded [26].

Adoption of Internet of Thing (IoT) in medical or known as medical IoT, is a challenge to privacy as data from wearable devices need to be addressed its storage, security, and sharing, applying IPFS can solved storage issue by encrypting the data. Observing execution for any compliances related to patient's privacy can increase accountability of a healthcare system [27].

Utilizing Hyperledger Caliper 0.4.2 as a unified performance analysis and recommending testbed with many hosts to get more accurate broadcast using tools like Tcpdump has resulted in fast performance, reduced latency, and minimal resource consumption inside a blockchain network for accessing, inquiring, and exchanging [30]. Patient centric framework proposing a framework that the main focus is the patient, the interest of the patient like access and sharing preferences, with addition of immutability and performance study on development and implementation using Hyperledger [28].

A secured supply chain management on medicine distributions can prevent counterfeit drugs received by patients. Drug transaction record will be put on blockchain network, creating an ecosystem of healthcare, providing support of accessibility, management, sharing and accountability by using smart contract [29].

III. Discussion

All literature articles can be grouped based on its challenges as follows:

- Access

To have a secured access, a proper identification of who can access is required, authentication without third party authorizing an identification is solved by implementing decentralized identifiers and verifiable credentials [31]. Authentication applied to identified requestor, and

Authorization applied to give level of access or level or permission, both authentication and authorization managed by authentication and authority agency [32].

- Sharing

Patient data can be shared to insurance company, medical provider, or pharmacy. Pharmacy needs patient data to check for allergies, medicine history and patient conditions to determine the dosages. Blockchain and smart contract can be used to manage prescription, interoperable prescription systems that ensure patient control, no information blocking and improves transfer efficiency [33].

- Storage

With the growth of mobile devices, patients can access EHR from anywhere, but data privacy and security are at stakes. Implementing a prototype using Ethereum on mobile app with amazon cloud computing [34] has shown an effective solution and reliable.

- Privacy

The information inside EHR is mostly private information, to maintain its privacy, patient can have full control on the data by creating a patient centric Health Information Exchange (HIE) [35].

- Performance

Blockchain performance can be measured by time needed to create new block of transaction or latency and throughput, another metric to be measured are cost of transaction and traffic in the blockchain platform itself, like memory allocation, delay on the process and CPU process [30].

- Supply Chain

With blockchain, as record cannot be tampered and modified, the same principle can be applied in the field of supply chain, handling medical distributions with the right to maintain record consistency [29].

Based on those challenges, we map the articles into Table 2, 35% are focusing on sharing records and interoperability, challenge about access being discussed by 35% studies and 30 % of studies on storage (10%), privacy (10%) and performance (10%), and the rest talk about supply chain management in medicine distribution.

To overcome challenges that identified from the studies, we proposed a blockchain model that can be used to manage access, sharing, storage, privacy, and performance measurement that can be implemented beyond supply chain in healthcare. Fig 4. Propose the Diponegoro Medical Chain (DMC), starting from first layer, the authorization layer, where central of authority, digital certificate, and unique identification of stakeholder in layer 2 will decided their level of access, authentication, and authorization. Second layer is the stakeholder, in this study, there are 6 entities, patient has full control, or called, patient centric, patient can determine all other entities level of access, what file or transaction the other entity can read or edit, and to protect the data, record will be encrypted, and implementing proxy-encryption to enable sharing the encrypted data but didn’t have decrypt and encrypt the data. Caregivers can have access but limited by patient authorizations and caregivers can update transaction on blockchain, insurance company can verify record to confirmed that all the procedures are aligned with the guideline and can be claimed, the pharmacy need to access prescription and might need to update replacement if the intended medicine is not available, research and government institute may access the record, all through proxy re encryption. Layer 4 is the blockchain network running on consortium blockchain, with Hyperledger fabric as platform and smart contract for defining transactions flow.

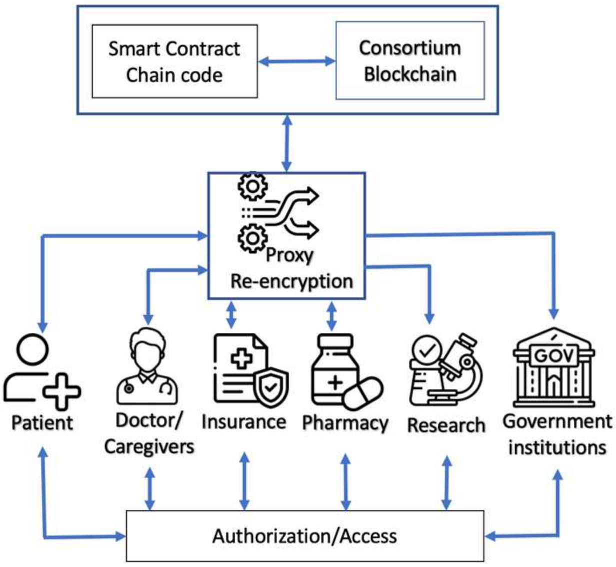

Fig 4. Proposed Model DMC

IV. Conclusion

Implementation of blockchain in healthcare has shown a significant interest, mainly about protecting records and only authorized users can access the records and as awareness of privacy has been increased, sharing the records only to authorized users and advantages of data untampered provided by blockchain has become a strong magnet on studies about implementing blockchain in EHR.

This study reveals that there are more solutions can be identified to solve the challenges on issues of consortium blockchain in healthcare. It can be treated as a main solution to overcome challenges in guarding health records security, but it can also open another implementation to the field, like implementing AI/ML for a recommendation system.

Consortium blockchain has been selected as EHR are mostly hosted by each healthcare provider, patient can share EHR to another healthcare provider disregard of different management, and maybe different policy in different country, with consortium own by healthcare providers, patients can change their information but only provider can add new information. Solutions to all this challenges then proposed in DMC, realizing patient centric, privacy, sharing and chain code.

References

[1] G. McCartney, F. Popham, R. McMaster, and A. Cumbers, “Defining health and health inequalities,” *Public Health*, vol. 172, pp. 22–30, Jul. 2019, doi: 10.1016/J.PUHE.2019.03.023.

[2] S. Niu, L. Chen, J. Wang, and F. Yu, "Electronic Health Record Sharing Scheme with Searchable Attribute-Based Encryption on Blockchain," *IEEE Access*, vol. 8, pp. 7195–7204, 2020, doi: 10.1109/ACCESS.2019.2959044.

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: www.bitcoin.org

[4] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019, doi: 10.1109/ACCESS.2019.2937685.

[5] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform."

[6] M. Sethumadhavan, "On Blockchain Applications: Hyperledger Fabric and Ethereum." [Online]. Available: http://www.ijpam.eu

[7] T. Blummer *et al.*, "An Introduction to Hyperledger," Aug. 2018. https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf (accessed Oct. 24, 2022).

[8] IBM, "What is Hyperledger Fabric." https://www.ibm.com/topics/hyperledger (accessed Oct. 24, 2022).

[9] P. K. Paul, P. S. Aithal, R. Saavedra, and S. Ghosh, "Blockchain Technology and Its Types-A Short Review," 2021. [Online]. Available: https://ssrn.com/abstract=4050933

[10] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, Sep. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[12] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36. Elsevier Ltd, pp. 55–81, Mar. 01, 2019. doi: 10.1016/j.tele.2018.11.006.

[13] M. M. Merlec, M. M. Islam, Y. K. Lee, and H. P. In, "A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme," *Sensors*, vol. 22, no. 3, Feb. 2022, doi: 10.3390/s22031271.

[14] E. P. Ambinder, "Cover Story: Oncology Enters the Information Age What is an Electronic Health Record?" [Online]. Available: www.jopasco.org

[15] V. Mardiansyah and R. F. Sari, "Lightweight Blockchain Framework for Medical Record Data Integrity," *Journal of Applied Science and Engineering (Taiwan)*, vol. 26, no. 1, pp. 91–103, 2022, doi: 10.6180/jase.202301_26(1).0010.

[16] W. Chen, S. Zhu, J. Li, J. Wu, C. L. Chen, and Y. Y. Deng, "Authorized shared electronic medical record system with proxy re-encryption and blockchain technology," *Sensors*, vol. 21, no. 22, Nov. 2021, doi: 10.3390/s21227765.

[17] J. Zhang, Z. Li, R. Tan, and C. Liu, "Design and Application of Electronic Rehabilitation Medical Record (ERMR) Sharing Scheme Based on Blockchain Technology," *Biomed Res Int*, vol. 2021, 2021, doi: 10.1155/2021/3540830.

[18] Z. Dodevski, S. Filiposka, A. Mishev, and V. Trajkovik, "Real time availability and consistency of health-related information across multiple stakeholders: A blockchain based approach," *Computer Science and Information Systems*, vol. 18, no. 3, pp. 927–955, 2021, doi: 10.2298/CSIS200426017D.

[19] G. Q. Butt, T. A. Sayed, R. Riaz, S. S. Rizvi, and A. Paul, "Secure Healthcare Record Sharing Mechanism with Blockchain," *Applied Sciences (Switzerland)*, vol. 12, no. 5, Mar. 2022, doi: 10.3390/app12052307.

[20] Q. Qin, B. Jin, and Y. Liu, "A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain," *Biomed Res Int*, vol. 2021, 2021, doi: 10.1155/2021/6676171.

[21] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019, doi: 10.1109/ACCESS.2019.2904300.

[22] D. Tith *et al.*, "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthc Inform Res*, vol. 26, no. 1, pp. 3–12, Jan. 2020, doi: 10.4258/hir.2020.26.1.3.

[23] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and Efficient Blockchain-Based ABE Scheme with Multi-Authority for Medical on Demand in Telemedicine System," *IEEE Access*, vol. 7, pp. 88012–88025, 2019, doi: 10.1109/ACCESS.2019.2925625.

[24] A. Ali *et al.*, "A novel secure blockchain framework for accessing electronic health records using multiple certificate authority," *Applied Sciences (Switzerland)*, vol. 11, no. 21, Nov. 2021, doi: 10.3390/app11219999.

[25] P. K. Bharimalla, H. Choudhury, S. Parida, D. K. Mallick, and S. R. Dash, "A Blockchain and NLP Based Electronic Health Record System: Indian Subcontinent Context," *Informatica (Slovenia)*, vol. 45, no. 4, pp. 605–616, 2021, doi: 10.31449/INF.V45I4.3503.

[26] D. Tith *et al.*, "Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology," *Healthc Inform Res*, vol. 26, no. 4, pp. 265–273, Oct. 2020, doi: 10.4258/hir.2020.26.4.265.

[27] D. el Majdoubi, H. el Bakkali, and S. Sadki, "SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework," *J Healthc Eng*, vol. 2021, 2021, doi: 10.1155/2021/4145512.

[28] A. P. Singh *et al.*, "A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications," *IEEE Trans Industr Inform*, vol. 17, no. 8, pp. 5779–5789, Aug. 2021, doi: 10.1109/TII.2020.3037889.

[29] F. Jamil, L. Hang, K. H. Kim, and D. H. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electronics (Switzerland)*, vol. 8, no. 5, May 2019, doi: 10.3390/electronics8050505.

[30] N. R. Pradhan *et al.*, "A Novel Blockchain-Based Healthcare System Design and Performance Benchmarking on a Multi-Hosted Testbed," *Sensors*, vol. 22, no. 9, May 2022, doi: 10.3390/s22093449.

[31] T. Manoj, K. Makkithaya, and V. G. Narendra, "A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records," *Cogent Eng*, vol. 9, no. 1, 2022, doi: 10.1080/23311916.2022.2035134.

[32] P. Pandey and R. Litoriya, "Securing and authenticating healthcare records through blockchain technology," *Cryptologia*, vol. 44, no. 4, pp. 341–356, Jul. 2020, doi: 10.1080/01611194.2019.1706060.

[33] A. Taylor, A. Kugler, P. B. Marella, and G. G. Dagher, "VigilRx: A Scalable and Interoperable Prescription Management System Using Blockchain," *IEEE Access*, vol. 10, pp. 25973–25986, 2022, doi: 10.1109/ACCESS.2022.3156015.

[34] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[35] Y. Zhuang, L. R. Sheets, Y. W. Chen, Z. Y. Shae, J. J. P. Tsai, and C. R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J Biomed Health Inform*, vol. 24, no. 8, pp. 2169–2176, Aug. 2020, doi: 10.1109/JBHI.2020.2993072.