Proceedings of the Pakistan Academy of Sciences: A Physical and Computational Sciences 60(3): 1-13 (2023)

ISSN (Print): 2518-4245; ISSN (Online): 2518-4253
https://doi.org/10.53560/PPASA(60-3)816

Pakistan Academy of Sciences

Review Article

Blockchain in Healthcare: A Comprehensive Survey of Implementations and a Secure Model Proposal

Mehak Maqbool Memon[1], Manzoor Ahmed Hashmani[1*], Filmann Taput Simpao[2], Anthony Cinco Sales[3], Neil Quinones Santillan[4], and Dodo Khan[1]

[1]Department of Computer and Information Sciences, Universiti Teknologi Petronas, Malaysia
[2]College of Engineering, University of Southeastern Philippines, Philippines
[3]Department of Science and Technology, Regional Office No. XI, Philippines
[4]MS3 Agriventures Corp, Philippines

Abstract: Blockchain's core attributes, including decentralization, transparency, and immutability, have positioned it as a pioneering technology in the realm of financial technology (fintech) and have rendered it highly applicable across diverse industries. The current enterprise ecosystem has faced setbacks primarily due to a lack of trust in the existing infrastructure. This issue can be traced back to the centralized management of healthcare data, making it vulnerable to tampering and fraudulent activities, resulting in financial losses. The existing enterprise ecosystem failed due to the lack of trust in the currently in-place infrastructure. This problem can be attributed to the centralized healthcare data management, which is prone to tampering and fraudulent activities leading to capital loss. The present study relates to a comprehensive survey conducted in timespan from 2018 to 2022 on the implementation of blockchain technology in the healthcare industry, identifying and discussing the key challenges facing the healthcare industry, such as fraud, and scams against healthcare data. It is found that there is an enormous inclination towards the decentralization of patient-centric data. However, a rapid decline is reported due to the privacy and security concerns of the confidential and sensitive data. Moreover, it is noticed that most of the implementations utilized either Ethereum or Hyperledger. Based on the survey's findings, the study proposed a blockchain-based healthcare framework that can address the identified challenges by providing a secure and transparent platform for collecting, storing, and sharing patient health data while prioritizing security and privacy.

Keywords: Blockchain in Healthcare, Healthcare Scams, Blockchain Solution, eHealthcare, Blockchain Architectures, Hyperledger, Enterprise Ecosystem, Ethereum, Transparency, Survey.

1. INTRODUCTION

Blockchain (BC), with its core features including decentralization, transparency, and immutability, has emerged as a leader in financial technology (fintech). These features are applicable to various industries desiring transparent and trackable practices. The enterprise blockchain provides a decentralised platform to involve stakeholders to increase gain margins. Some of the known enterprise blockchains include digital identity systems for theft reduction by providing greater ownership of the data [1], sustainable solutions for companies suffering from siloed infrastructures with multiple touchpoints [1, 2], healthcare & insurance requiring efficient data management to protect sensitive data by streamlining transparent data verification practices and distributions [3], entertainment and sports industry prone to piracy of the digital content may be benefitted by managing authentic digital distributions and fan engagement with enhanced loyalty programs and incentives [4], and real estate and supply chain involving global agencies to efficiently monitor and track the digital asset management [2, 5]. The existing enterprise ecosystem failed due to the lack of trust in the currently in-place infrastructure. A similar problem can be attributed to the centralised healthcare data management. Healthcare big data is growing rapidly, including information of patients,

Received: April 2023; Accepted: September 2023
*Corresponding author: Manzoor Ahmed Hashmani <manzoor.hashmani@utp.edu.my>

hospitals, and insurance agencies, with the medical insurance system functioning based on the data transmitted by the hospitals (including physicians and pharmacies). The insurance claims are borne by the agency based on the logs generated against the patient's health in the form of medical treatments, medicines and equipment used. Since the entire workflow is centralized and all involved use their centralized independent silos, it is easier to tamper with the data [3-9]. This form of tampering leads to easier ways of fraudulent scams against medical insurance. As per the 2020 report of the United States Sentencing Commission, losses related to healthcare scams have exponentially increased in the US over the years [4, 10]. The capital loss witnessed over the period from 2016 to 2020. Care Anti-Fraud Association (NHCAA), claims tens of billions of dollars of fraudulent scams per year. one source of fraud is from the patients themselves by identity swapping or identity theft, wherein one person's insurance is used by another person. Finally, the prescriptions are also forged and illegally used to claim the increased amount of money [5, 11]. The traditional data-sharing methods were deemed as the major cause of the scams due to centralized data stores and single-point-of-failure, which results in poor data security and privacy strategies. The second major problem is unconnected data in which a patient's information can be easily changed, leaving behind no trace leading to another security-related problem. Moreover, in healthcare scenarios, insurance claims are essentially dependent on third-party administrators. As such, sharing this information with third-party administrators over a network means exposing sensitive data to cyber-attacks [6]. Considering the current healthcare ecosystem and associated data-driven attacks. A decentralized solution such as blockchain has the potential to bring medical big data onto the decentralized ledger, where a single change is transparent to all the individuals/ organizations involved. The data on the blockchain is secure due to the usage of cryptography, where only known users can have access to the actual information. This study makes a significant contribution in two ways. Firstly, it conducted a comprehensive survey on the implementation of blockchain technology in the healthcare industry. The survey explored various aspects such as fraud, scams, and data storage techniques related to healthcare. By examining these issues, the study identified the key challenges facing the healthcare industry regarding implementing blockchain technology and the major frameworks to be implemented. Secondly, based on the findings from the survey, the study proposed a blockchain-based healthcare framework that can address the identified challenges. The proposed framework consists of different components. By integrating these components, the proposed framework aims to provide a secure and transparent platform for collecting, storing, and sharing patient health data while prioritizing security and privacy.

2. SURVEY METHODOLOGY AND CRITICAL ANALYSIS ON HEALTHCARE IMPLEMENTATIONS

The current healthcare ecosystem is susceptible to scams and fraud due to centralized regulatory entities. This centralized scenario deviates the entire healthcare insurance ecosystem from the goal of health policies to uphold the applicant's/ patient's health. Over the period of the last decade, blockchain-based solutions have been revolutionizing different domains such as supply chain, education, healthcare and so on [7, 15, 22-24]. This revolution is in terms of the minimization of single-entity dependence and ownership of data to maintain the integrity of patients.

This section critically analyzes healthcare-related blockchain-based research reported in a timespan from 2018 to 2022. At the time of compilation of this research, the main 3 (Google Scholar, IEEE, Science Direct) repositories have been queried with 3 different search queries. The search queries included the following phrases: "medical fraud detection blockchain decentralization"; "healthcare blockchain system"; and "healthcare blockchain system smart contracts". The search resulted in the retrieval of 39 indexed research articles. Figure 1 shows the blockchain-based healthcare research solution trend. In the year 2020, most of the blockchain-based solutions have been reported due to the readily available implementation resources and the hype in the domain of blockchain solutions, whereas a rapid decline was seen in the following years. One of the major reasons for this decline is the usage of architectural platforms which leads to lesser trust of stakeholders in the technology due to the shift towards public networks.

Drilling down further into the details of these researches uncovered the fact that most of the decentralized healthcare researches used Ethereum-based platforms, which raises concerns about private patient data handling as it is inherently a public blockchain network. Figure 2 shows the division of development platforms reported in the 39 Combine these paragraphs.

Figure 2 shows over 40 % of the blockchain-based healthcare solution are backed by Ethereum-based architectures which inherits features of public blockchain architecture. Whereas 28 % research focuses merely on the conceptualization of use case under consideration. Hyperledger-based implementations dominate only 17 percent of the overall research which inherits the features of the consortium blockchain solution. Finally, 5 and 10 percent represent other platforms and articles without platform specifics respectively.

The comprehensive critical analysis of these 39 blockchain-based healthcare research articles is further presented in Table 1 which shows detailed analysis of conducted research. It is seen

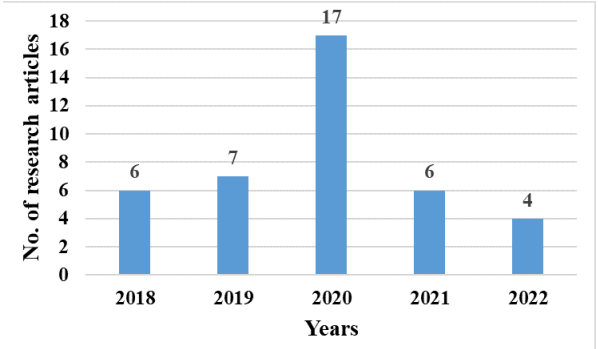

Fig. 1. Distribution of research articles in healthcare blockchain system (2018-2022)

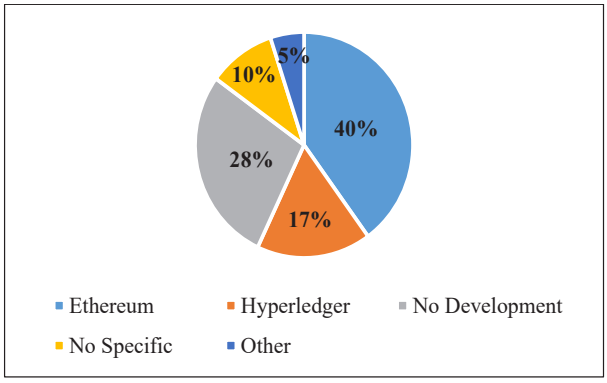

Fig. 2. Blockchain based Development Platforms for Healthcare

that there is immense inclination towards the decentralization of patient-centric data. However, most of the articles have provided the conceptual module for the healthcare sector. As stated earlier, a rapid decline in the blockchain-based studies in healthcare was witnessed leading the researchers to believe that it is due to the privacy concerns of the confidential and sensitive hospital data which otherwise is inaccessible to irrelevant identities. Most of the reported developed use cases are based on public blockchain networks which can be easily accessed by any registered node. Moreover, registration of new nodes is comparatively easy in public blockchains. Additionally, if encryption mechanisms are implemented on top of public blockchain network, it increases the computational resources. Eventually, stakeholders may lose interest in blockchain technology due to association of sensitive patient data to be handled. The private blockchain systems are still governed by a singular entity, meaning hospitals and third-party insurance companies should create their own separate ledgers which serves the purpose of traceability within respective organizations only. Whereas the consortium-based blockchains (such as Hyperledger) seem to be a promising solution as the development ecosystem is designed in such a way that all the involved entities are brought onto a single ledger and new registration of nodes is still controlled by the authorized nodes. Section 4 further discusses the details of public and consortium-based architectures of blockchain to compare the offered features with respect to the healthcare data and how they can help in reduction of healthcare scams.

3. APPLICABILITY OF BLOCKCHAIN DEVELOPMENT PLATFORMS

The most popular blockchain development platforms are Ethereum and Hyperledger. Both networks belong to different architectural schemes based on the accessibility. As mentioned earlier, Ethereum is a public blockchain while Hyperledger is a consortium blockchain. This section compares the features of both platforms with respect to enterprise business use as in the case of healthcare. Both the blockchain platforms are open source. In converting existing healthcare management systems, it is imperative to identify the correct representative platform for the implementation.

Table 1. The comprehensive critical analysis Blockchain based healthcare research.

S. No.	Title	Survey/ Use case	Year	Comments
1	Identifying fraud in medical insurance based on blockchain and deep learning [8]	Use case	2022	• Bidirectional Encoder Representations from Transformers (BERT-LE) model. • Based on consortium Blockchain • Two real datasets from two 3A hospitals • Participants: Hospital, regulatory agency, Medical insurance center, patient • Practical Byzantine Fault Tolerance (PBFT) consensus • No clear specification which blockchain architecture/ framework is used (Hyperledger/quorum etc) • Uses Machine Learning (ML) along with decentralization.
2	A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges [9]	Survey	2022	• Reports 12 Ethereum, 6 Hyperledger, 6 others (4 without smart contract) research articles. • Future research might consider incorporating more technological characteristics to improve feasibility evaluation and narrow the gap between ideas and implementations, propelling healthcare technology.
3	Blockchain Framework for Cognitive Sensor Network Using Non-Cooperative Game Theory [10]	Use case	2022	• Ethereum-based private blockchain for medical sensory data tracing and tracking. • Keeps track of patient's illness and treatments. • Proposes a merger module based on Blockchain (BC), ML and IoT to bring in Internet of Medical Things (IOMT) scenario working. • EEG blood pressure data of patient and other details of patient and hospital are saved in the decentralized ledger. • Focuses fraud detection in medicare. • Federated Learning Aware Blockchain Enabled IoMT is proposed. • Does not mention which blockchain is used.
4	Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations [11]	Use case	2022	• Ethereum-based implementation for maintaining health insurance data. • With additional layer of security as the blockchain used is implicitly public.
5	Healthcare Insurance Frauds: Taxonomy and Blockchain-Based Detection Framework (Block-HI) [12]	Use case	2021	• Just a plan for blockchain implementation in medicare fraud detections. • Considers up to 12 different ways of threat in medicare to be resolved by decentralization. • Good for conceptualization.
6	Health Insurance Claim Using Blockchain [13]	Use case	2021	• Medical health report keeping via decentralization. • Implements blockchain but does not provide any information of architecture. • Provides good conceptualization.
7	Decentralized Healthcare Management System Using Blockchain to Secure Sensitive Medical Data for Users [14]	Use case	2021	• Proposes SADS (stringent authentication and decentralized storage). • Correlates the implementation with the usage for fraud detection but originally implanted for record keeping. • Uses hash function of SHA-256. • No clear mentions of blockchain architecture used.

8	HealthBlock: A secure blockchain-based healthcare data management system [15]	Use case	2021	• Detailed study with all the conceptualization diagrams. • Closely consider the aspect of privacy and security. • Hyperledger based implementation is used.
9	A Blockchain and Artificial Intelligence-Based, Patient-Centric Healthcare System for Combating the COVID-19 Pandemic: Opportunities and Applications [16]	Survey	2021	• Detailed survey for the applicability of BC in healthcare along with integration of AI. • Proposes a conceptualization module to create decentralized medicare solution. • Proposes usage of Ethereum-based blockchain which nullifies the privacy and secrecy of patient in its original form.
10	Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions [17]	Survey	2021	• Discusses the storage issues of Medicare BC solutions. • Detailed study focusing Ethereum perspective. • Presents existing decentralized medical health data keeping solutions.
11	Implementing healthcare services on a large scale: Challenges and remedies based on blockchain technology [18]	Use case	2020	• Proposes AarogyaChain. • Uses Hyperledger. • Identifies speed throughput for transactions. • three tiers: the tier-I comprises of patients and physicians, the tier-II includes healthcare organizations, and the tier-III is the government. • Three probs speed, security, and decentralization requirements together
12	Application of Blockchain and IoT towards Pharmaceutical Industry [19]	Use case	2020	• General blockchain study. • Discusses challenges for use case no information for blockchain architecture.
13	Blockchain technology applications to postmarket surveillance of medical devices [20]	Use case (Plan only)	2020	• Focuses post market surveillance issue of the medical devices and emphasizes on the usage of blockchain technology. • Gives out 10-year long term switch plan to convert the centralized mechanism to decentralized. • No mention of recommendation for usage of type of blockchain architecture.
14	Health Care Insurance Fraud Detection Using Blockchain [21]	Use case	2020	• Uses tendermint having BFT consensus but the core is built on public blockchain, Ethereum-based. • Focuses the problem of fraud detection and in medical insurances. • Good research article for the core blockchain project implementations.
15	Blockchain solutions for healthcare [22]	Survey	2020	• Discusses the evolution of blockchain and relevance with healthcare. • Sheds light on the challenges and future directions of research.
16	Combating Health Care Fraud and Abuse: Conceptualization and Prototyping Study of a Blockchain Antifraud Framework [23]	Use case	2020	• Keeps track of fraud and theft in medical insurances. • Describes every aspect of implementation from front to backend of Decentralized Application (DApp) development. • Ethereum-based implementation with restricted permissions using Health Insurance Portability and Accountability Act (HIPAA) business associate agreement.

17	Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals [24]	Use case	2020	• Manages patient's sensory data on decentralized ledger. • In current state no mechanism for fraud detection. • Hyperledger Fabric based framework. • Mentions details of the development top-to-down.
18	A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things [25]	Use case	2020	• Patient's UAV (unmanned vehicular data) is stored in decentralized ledger to keep the track of activity performed. • Proposed BHealth system is based on Ethereum, which is public blockchain, this raises issues related to privacy and security of patient.
19	GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare [26]	Use case	2020	• Patients record maintenance meeting the aspect of privacy and confidentiality. • Consortium-based implementation. • Implicit privacy handling by implemented BC architecture. • Added intelligence by using convolutional neural networks. • More information for DApp implementation is required.
20	S2HS- A blockchain based approach for smart healthcare system [27]	Use case	2020	• Maintenance of electronic medical records on decentralized ledger. • Detailed analysis of blockchain technology growth. • Just the conceptualization, analysis of blockchain research w.r.t healthcare dept.
21	Blockchain-based electronic healthcare record system for healthcare 4.0 applications [28]	Use case	2020	• Hyperledger based implementation. • Detailed analysis of transaction time and cost for performance.
22	A Blockchain-Based Smart Contract System for Healthcare Management [29]	Use case	2020	• Detailed in terms of more participant and use cases (pharmacy, physicians, consultants, patients, and insurance agency roles) have been addressed. • Uses Ethereum-based implementation and uses Delegated PoS (Proof-of-Stake) Consensus.
23	Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare [30]	Use case	2020	• Proposes a sensory data keeping engine to track patient's health. • Implements BC network from scratch in MATLAB networking simulator. • Does not discuss privacy concerns. • Focuses identification and comparison of packet delivery ratio, energy consumed and latency.
24	Use of Blockchain Technology to Curb Novel Coronavirus Disease (COVID-19) Transmission [31]	Use case	2020	• Implements Ethereum-based blockchain. • Proposes the data management and sharing of covid patients to help stop the spreading of virus. • This use case works well with public blockchain.
25	A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain Technology [32]	Use case	2020	• Ethereum-based blockchain is used. • The specific smart contract used are mocha and chai. • Privacy concerns remains unresolved.

26	SHealth: A Blockchain-Based Health System with Smart Contracts Capabilities [33]	Use case	2020	• PBFT is used for consensus. • The blockchain is implemented from scratch, however, it is compatible with Hyperledger.
27	Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey [34]	Survey	2020	• Detailed survey with conceptual diagrams for each category of BC architecture and its relevance with distributed medicare data. • Compare and contrast discussions of private, public and consortium blockchain architectures can be extended w.r.t security.
28	A Blockchain-Based System for Anti-Fraud of Healthcare Insurance [35]	Use case	2019	• Anti-fraud service application architecture based on blockchain with cross-cloud platform. • Future work discusses implementation of Hyperledger.
29	Secure and Scalable mHealth Data Management Using Blockchain Combined With Client Hashchain: System Design and Validation [36]	Use case	2019	• Uses Hyperledger Fabric v1.0 for implementation combined with client hashchain of extra security layer. • Provides mobile based health decentralised solution (mhealth). • Tackles medical health record keeping only.
30	Fraud Detection in Medical Insurance Claim with Privacy Preserving Data Publishing in TLS-N Using Blockchain [37]	Use case	2019	• Focused research of decentralized solution for insurance related thefts. • Ethereum-based smart contract implementation. • Incorporating TLS-N in communication. • The core bc remains public.
31	Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology [38]	Use case	2019	• Hyperledger with PBFT consensus algorithm-based implementation is used. • Considers security and privacy aspects of patient and hospital data. • No real data implementation so far. • No mentions of fraud detection.
32	A Secure Healthcare System Design Framework using Blockchain Technology [39]	Use case	2019	• Presents the conceptualization framework with role of different entities and amalgamation of IoT. • Discusses privacy concerns of patient but w.r.t blockchain implementation does not mention any concern.
33	Blockchain in healthcare applications: Research challenges and opportunities [40]	Use case	2019	• Discusses different theoretical aspects of blockchain networks. • Mentions privacy, consensus mechanisms but does not mention the suitable platform for development. • Compares the existing medicare data BC networks.
34	Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives [41]	Survey	2019	• Discusses opportunities for medicare to be handled on distributed ledger. • Mentions all the possibilities & challenges of integration with AI & ML. • Can be further extended w.r.t to development platforms.
35	Geospatial blockchain: promises, challenges, and scenarios in health and healthcare[42]	Survey	2018	• Discusses possibilities of decentralization for different domains including pharmaceutical, medicine, supply chain, clinical trials, and smart cities. • Focuses on the identification of bc search interest in all the mentioned domains.

36	Privacy-friendly platform for healthcare data in cloud based on blockchain environment [43]	Use case	2018	• Ethereum-based patient record keeping. • The research is inclined towards the applicability in terms of time consumed for retrieval (speed) and cost involved. • Such sensitive data should be kept secure – Major flaw.
37	Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring [44]	Use case	2018	• Covers the aspect of patient's health monitoring via decentralization. • Private blockchain based on Ethereum. • Quotes "Hyperledger is more user friendly with a UI and customer support." • Implements private Ethereum blockchain. • The use case focuses transparent information sharing between physician and the patient. • Uses extra layer of encryption as privacy mechanism.
38	A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract [45]	Use case	2018	• IoT based blockchain solution for patient's health monitoring. • Implements Ethereum-based BC • As counter mechanism for privacy of patient in public BC sets patient's identity to anonymous but his/her medical history remains on public blockchain. • Presence of data raises concerns related to hacking of the authorized nodes or fishing with random identity numbers to identify the actual one remains unresolved.
39	Blockchain and Smart Contracts in a Decentralized Health Infrastructure [46]	Use case	2018	• Assigns medical cards to the patients and connect all the involved parties (physicians, patients, insurance agencies) over single platform. • Provides the concept of BC in medicare scenario does not mention development concerns.

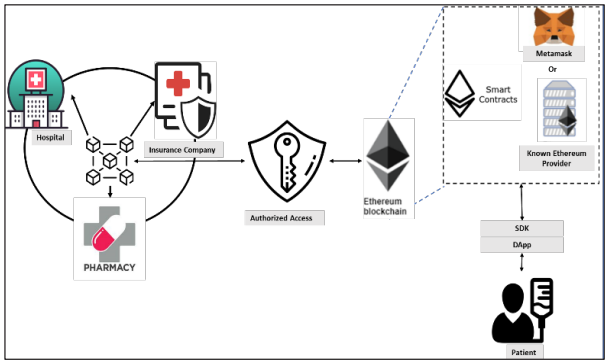

Fig 3. Implementation schema of Ethereum [14]

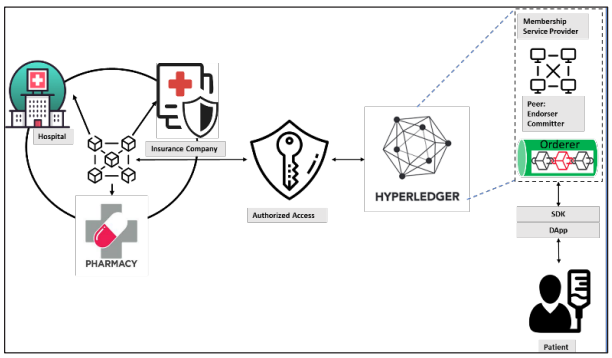

Fig 4. Implementation schema of Hyperledger [27]

3.1 Ethereum

In operating the system on Ethereum's EVM (Ethereum Virtual Machine), 'gas' is required to get the access of public network. For every transaction, Combine these paragraphs.

Implying that if the threatening entity has gas, it can easily get the access of network. Figure 3 shows the Ethereum-based implementation schema for healthcare data management. All the entities are connected over the Ethereum blockchain. A patient registers via the DApp interface, which is connected to the EVM. In getting the EVM imprint, either metamask or known providers are requested. Finally, all the existing nodes are connected via predefined smart contracts.

3.2 Hyperledger

Hyperledger is one of the consortiums blockchain architectures. It is based on the modular approach

for enterprise blockchain solutions. The consensus is based on different components including peers, MSP (Membership Service Provider), and orderer. All the peers are nominated by administrators of each organization thus no unauthorized entities can trespass the distributed ledger. The key feature of Hyperledger is freedom of selection for consensus. The consensus is divided into three steps: endorsement, ordering, and validation. Figure 4 shows the Hyperledger-based implementation schema for healthcare data management. Table 2 compares the features of Ethereum and Hyperledger. The supporting languages of Ethereum development are Go and Solidity whereas Hyperledger support several programming languages with rich functionalities and already known to the research community. Both platforms support their respective consensus. However, the consensus supported by Hyperledger is transactional level, implying tracking of every single change to be logged.

After a detailed comparative discussion of the known existing blockchain architectures and the platforms, the final argument to be addressed is the selection of a platform for enterprise data management infrastructure. Considering the requirements and workflows involved in enterprise's business logic (healthcare), specifically for insurance claims and scam tracking, the idea is to provide access only to authorized users that are also predefined/nominated peers. This ensures the decentralization of data among the organizations without affecting privacy of patient. Both the feature decentralization along with the implicit privacy feature is offered by Hyperledger.

4. PROPOSED BLOCKCHAIN BASED HEALTHCARE MODEL

The proposed blockchain-based healthcare model is designed to provide a secure and transparent framework for collecting, storing, and sharing patient health data. It aims to improve the security and privacy of patient data by utilizing blockchain technology to provide a decentralized and tamper-proof platform for storing and sharing patient health data with other entities such as insurance claims, pharmacies, prescription etc. This ensures that patient health data is secure and protected from unauthorized access, while also providing transparency in the use and sharing of the data. This model addresses the frauds, scams in the healthcare eco system (hospitals, insurances and patients). The Figure 5 illustrated Blockchain based health

Table 2. Public versus consortium Blockchain development platform

Platform	Ethereum	Hyperledger
• Type	• Permission less, public, or private (limited permissions)	• Consortium
• Database Compatibility	• Ethereum's Rust client Parity uses RocksDB Ethereum's Go, C++ and Python clients all use LevelDB • BigchainDB	• Compatible with CouchDB
• Supporting languages	• Go, Solidity	• JavaScript, Java, Go, Python, and Node.js
• Host Platform	• Ethereum developers	• IBM
• Operating System	• Linux, macOS, Windows	• Linux foundation(base) Linux, Windows
• Consensus	• Mining based on Proof of Work (PoW) • Ledger level • PoA (Aura) • PoS (Casper)	• Multiple approaches (PBFT, CFT-Kafka, Raft) • Transaction-level
• Currency	• Ether • Tokens via smart contracts	• None (Currency and tokens via chaincode)
• Smart contracts	• Smart contract code (e.g., Solidity)	• Smart contract development in JavaScript, Java, Go, and Node.js

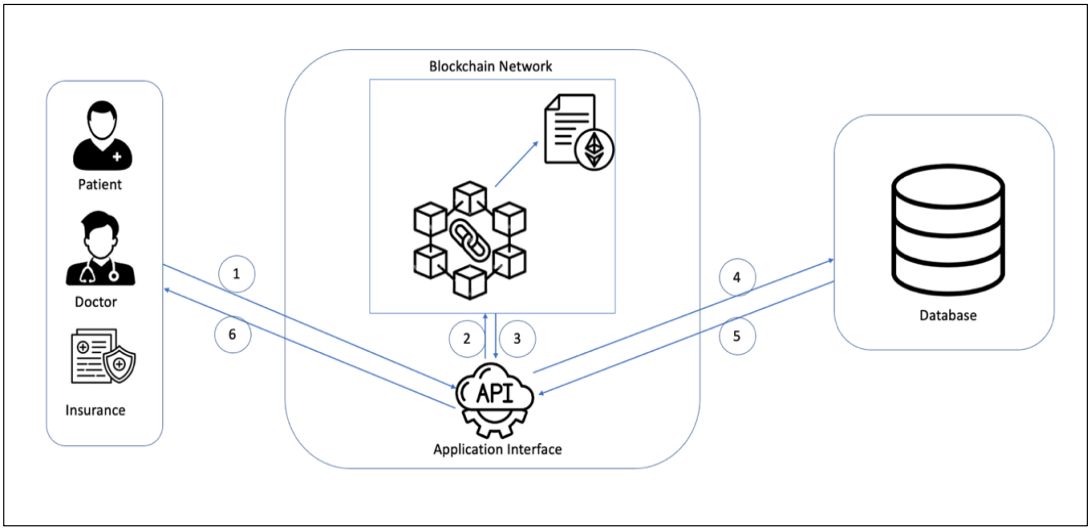

Fig. 5. Proposed healthcare model

model which is consists of six components that work together to ensure the privacy and security of patient health data while enabling healthcare providers and patients to access and utilize the data to improve healthcare outcomes [47]. Moreover, Figure 6 shows the flow of data from its origin (patient) to Blockchain and electronic health record (EHR). Initially data generates from patient's wearable or medical device, and it will be forwarded to Blockchain via API and eventually EHR in very transparent way. It also be query back to patient or healthcare provider with the same path. Any temper on data has to get a consensus from other stakeholders.

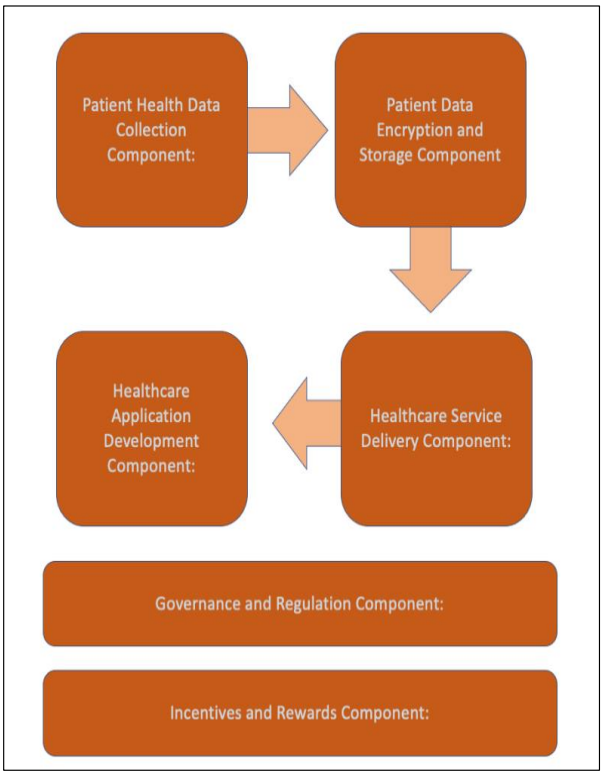

Fig 6. Flow of data in the proposed model

The model consists of six components:

- Patient Health Data Collection Component: This component is responsible for collecting patient health data from various sources, including medical devices and healthcare providers, wearables etc.
- Patient Data Encryption and Storage Component: This component receives and stores the encrypted patient health data on the blockchain. The blockchain ensures that the data is decentralized and tamper-proof, providing a secure and transparent platform for sharing patient health data.
- Healthcare Service Delivery Component: This component provides healthcare services to healthcare providers, patients, and other stakeholders based on the patient health data stored on the blockchain. These services may include telemedicine, remote monitoring, and personalized medicine.
- Healthcare Application Development Component: This component provides healthcare applications that enable healthcare providers to access and interact with the patient health data stored on the blockchain. These applications may include mobile apps, web portals, and electronic health records (EHRs).

- Governance and Regulation Component: This component provides oversight and governance of the framework, ensuring that the patient health data is accessed, used, and shared in a secure and transparent manner. This includes regulatory compliance, data privacy, and security standards.
- Incentives and Rewards Component: This component provides incentives for stakeholders to participate in the framework, encouraging the sharing of health data and use of the services provided. These incentives may include tokens, rewards, and discounts.

Overall, the proposed blockchain-based layered healthcare model is designed to prioritize security and privacy, with a focus on regulatory compliance and transparency. It aims to provide a secure and transparent platform for collecting, storing, and sharing patient health data while enabling healthcare providers and patients to access and utilize the data to improve healthcare outcomes. The model is designed to prioritize security and privacy, with a focus on regulatory compliance and transparency.

5. CONCLUSIONS

The present survey shows that the decentralized, transparent, and immutable features of Blockchain have made it a leading technology in fintech and applicable to various industries. However, the lack of trust in the existing enterprise ecosystem has led to problems, such as centralized healthcare data management being prone to tampering and fraudulent activities, causing capital loss. To address these challenges, a comprehensive survey was conducted and a blockchain-based healthcare framework was proposed that provides a secure and transparent platform for collecting, storing, and sharing patient health data while prioritizing security and privacy. This framework has the potential to revolutionize the healthcare industry and bring about a new era of trust and transparency in data management.

6. ACKNOWLEDGEMENT

This research work is a part of an ongoing research project jointly funded and facilitated by the Universiti Teknologi PETRONAS, Malaysia, University of Southeastern Philippines, Philippines, Department of Science and Technology, Philippines, and MS3 Agri-ventures Corporation, Philippines (Grant Number: 015ME0-307). Authors also acknowledge support, guidance, and advise of Prof. Dr. Mohd Shahir Liew and Assoc. Prof. Dr. Mohd Fadzil Hassan in the completion of this work.

7. CONFLICT OF INTEREST

The authors declare no conflict of interest.

8. REFERENCES

1. D. Khan, L.T. Jung, and M.A. Hashmani. Systematic literature review of challenges in blockchain scalability. *Applied Sciences* 11(20): 9372 (2021).
2. D. Khan, M.M. Memon, M.A. Hashmani, F.T. Simpao, A.C. Sales, and N.Q. Santillan. A Critical Review on Blockchain Frameworks for Dapp. *International Journal of Technology Management and Information System* 5(1): 1-10 (2023).
3. D. Khan, L.T. Jung, M.A. Hashmani, and M.K. Cheong. Blockchain Enabled Diabetic Patients' Data Sharing and Real Time Monitoring. *In CS & IT Conference Proceedings* 12(6): (2022).
4. D. Khan, L.T. Jung, M.A. Hashmani, and A. Waqas. A critical review of blockchain consensus model. *3rd international conference on computing, mathematics and engineering technologies (iCoMET):* 1-6 (2020).
5. D. Khan, L.T. Jung, and M.A. Hashmani. Proof-of-Review: A Review based Consensus Protocol for Blockchain Application. *International Journal of Advanced Computer Science and Applications* 12(3): 290-300 (2021).
6. K.C. Moke, T.J. Low, and D. Khan. IoT blockchain data veracity with data loss tolerance. *Applied Sciences* 11(21): 9978 (2021).
7. D. Khan, L.T. Jung, M.A. Hashmani, and M.K. Cheong. Empirical performance analysis of hyperledger LTS for small and medium enterprises. *Sensors* 22(3): 915 (2022).
8. G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. Rodrigues. Identifying fraud in medical insurance based on blockchain and deep learning. *Future Generation Computer Systems* 130: 140-154 (2021).
9. M.S. Rahman, M.A. Islam, M.A. Uddin, and G. Stea. A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges. *Internet of Things* 19(8): 100551 (2022).
10. S. Surekha, and M.Z.U. Rahman. Blockchain framework for Cognitive Sensor Network using

Non-Cooperative Game Theory. *IEEE Access* 10: 60114-60127 (2022).
11. E. Chondrogiannis, V. Andronikou, E. Karanastasis, A. Litke, T. Varvarigou. Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain: Research and Applications* 3(2): 100049 (2022).
12. L. Ismail and S.J.I.p. Zeadally. Healthcare insurance frauds: Taxonomy and blockchain-based detection framework (Block-HI). *IT professional* 23(4): 36-43 (2021).
13. J. Kuckreja, P. Nigde, and P. Patil. Health Insurance Claim using Blockchain. *International Research Journal of Engineering and Technology (IRJET)* 8(5): 2406-2409 (2021).
14. N. Deepa, T. Devi, N. Gayathri, and S.R. Kumar. Decentralized Healthcare Management System Using Blockchain to Secure Sensitive Medical Data for Users. *Blockchain Security in Cloud Computing* 265-282 (2022).
15. B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M.J.C.N. Abid. HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks* (200): 108500 (2021).
16. M.Y. Jabarulla, and H.N. Lee. A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic. *Opportunities and applications In Healthcare* 9(8): 1019 (2021).
17. S. Kumar, A.K. Bharti, and R. Amin. Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Security and Privacy* 4(5): 162 (2021).
18. P. Pandey, and R. Litoriya. Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. *Health Policy and Technology* 9(1): 69-78 (2020).
19. A. Premkumar, and C. Srimathi. Application of blockchain and IoT towards pharmaceutical industry. *In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*: 729-733 (2020)
20. J. Pane, K.M. Verhamme, L. Shrum, I. Rebollo, and M.C.J.M. Sturkenboom. Blockchain technology applications to postmarket surveillance of medical devices. *Expert Review of Medical Devices* 17(10): 1123-1132 (2020).
21. G. Saldamli, V. Reddy, K.S. Bojja, M.K. Gururaja, Y. Doddaveerappa, and L. Tawalbeh. Health care insurance fraud detection using blockchain. *Seventh International Conference on Software Defined Systems*: 145-152 (2020).
22. P. Zhang, and M.N.K. Boulos. Blockchain solutions for healthcare. In Book: Precision Medicine for Investigators, practitioners and providers. *Academic Press:* 519-524: (2020).
23. T.K. Mackey, K. Miyachi, D. Fung, S. Qian, and J. Short. Combating health care fraud and abuse: Conceptualization and prototyping study of a blockchain antifraud framework. *Journal of medical Internet research* 22(9): e18623 (2020).
24. F. Jamil, S. Ahmad, N. Iqbal, and D.H. Kim. Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors* 20(8): 2195 (2020).
25. A.I. Abhi, and S.Y. Shin. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. *Computers & Electrical Engineering* 84: 106627 (2020).
26. Z. Wang, N. Luo, and P. Zhou. GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare. *Journal of Parallel and Distributed Computing* 142: 1-12 (2020).
27. G. Tripathi, M.A. Ahad, and S. Paiva. S2HS-A blockchain based approach for smart healthcare system. *Healthcare* 8(1): 100391 (2020).
28. S. Tanwar, K. Parekh, and R. Evans. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications* 50: 102407 (2020).
29. A.J.E. Khatoon. A blockchain-based smart contract system for healthcare management. *Electronics* 9(1): 94 (2020).
30. A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B.G. Kim. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics* 9(10): 1609 (2020).
31. A. Khatoon. Use of blockchain technology to curb novel coronavirus disease (COVID-19) transmission. *Available at SSRN* 3584226: (2020).
32. R.M.A. Latif, K. Hussain, N.Z. Jhanjhi, A. Nayyar, and O. Rizwan. A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimedia tools and applications*: 1-24 (2020).
33. M. Zghaibeh, U. Farooq, N.U. Hasan, and I. Baig. Shealth: A blockchain-based health system with smart contracts capabilities. *IEEE Access* 8: 70030-70043 (2020).
34. S. Shi, D. He, L. Li, N. Kumar, M.K. Khan, and K.R. Choo. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security* 97: 101966 (2020).
35. W. Liu, Q. Yu, Z. Li, Z. Li, Y. Su, and J. Zhou. A blockchain-based system for anti-fraud of healthcare insurance. *IEEE 5th International Conference on Computer and Communications (ICCC)*: pp. 1264-1268 (2019).

36. T. Motohashi, T. Hirano, K. Okumura, M. Kashiyama, D. Ichikawa, and T. Ueno. Secure and scalable mhealth data management using blockchain combined with client hashchain: system design and validation. *Journal of medical Internet research* 21(5): e13385 (2019).
37. T. Mohan and K. Praveen. Fraud detection in medical insurance claim with privacy preserving data publishing in TLS-N using blockchain. *International Conference on Advances in Computing and Data Sciences*: pp. 211-220 (2019).
38. M. Usman and U. Qamar. Secure electronic medical records storage and sharing using blockchain technology. *Procedia Computer Science* 174: 321-327 (2020).
39. S. Chakraborty, S. Aich, and H.C. Kim. A secure healthcare system design framework using blockchain technology. *21st International Conference on Advanced Communication Technology (ICACT)*: pp. 260-264 (2019).
40. T. McGhin, K.R. Choo, C.Z. Liu, D. He. Blockchain in healthcare applications: Research challenges and opportunities. *Journal of network and computer applications* 135: 62-75 (2019).
41. A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography* 3(1): 3 (2019).
42. M.N.K. Boulos, J.T. Wilson, and K.A. Clauson. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. *International journal of health geographics* 17: (2018).
43. A. Al Omar, M.Z.A. Bhuiyan, A. Basu, S. Kiyomoto, and S. Rahman. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future generation computer systems* 95: 511-521 (2019).
44. K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, and T. Hayajneh. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems* 42: 1-7 (2018).
45. H. Pham, T. Tran, and Y. Nakashima. A secure remote healthcare system for hospital using blockchain smart contract. *IEEE globecom workshops* (GC Wkshps): pp. 1-6 (2018).
46. S.P. Novikov, O. Kazakov, N. Kulagina, and N. Azarenko. Blockchain and smart contracts in a decentralized health infrastructure. *IEEE International Conference -- Quality Management, Transport and Information Security, Information Technologies* (IT&QM&IS): pp. 697-703 (2018).
47. D. Khan, T.J. Low, and V.T.B. Dang. Challenges and Application of Blockchain in Healthcare Systems. *International Conference on Digital Transformation and Intelligence (ICDI)*: pp. 15-20 (2022).