DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

Healthcare Based Block Chain Survey In IOT

Ghazwh Ganem jumaa[1], Atheer Raheem Muhsin[2], Rasha M. Mohsin[3],Abeer Tariq Maolood [4]

[1,2,3,4]Computer Science Department ,University of Technology, Baghdad, Iraq

[1]110072@uotechnology.edu.iq, [2]110079@uotechnology.edu.iq,

[3]rasha.m.mohsin@uotechnology.edu.iq, [4]abeer.t.maolood@uotechnology.edu.iq

Abstract- *Because block chain technology can improve distributed systems' security, dependability, and resilience, it has been gaining popularity. Research based on this technique has helped a number of fields, including data analysis, finance, remote sensing, and healthcare. The primary characteristics that make block chain technology appealing include distributed ledgers, decentralization, privacy, transparency, and data immutability. However, because there is a chance of a privacy breach, medical records that hold private patient information make this system extremely complex. The purpose of this project is to investigate block chain applications in the healthcare sector. We also include articles that touch on other topics, like the Internet of Things, information management, medicine supply chain tracking, and privacy and security issues. Lastly, we aim to investigate block chain concepts in the medical field by evaluating their advantages and disadvantages and providing direction to other studies in the field. We also provide a summary of the Block chain's techniques.*

Index Terms*—IoT, Block Chain, Healthcare, Smart Contract, Etherum.*

I. INTRODUCTION

Block chain is a public, decentralized digital ledger that keeps track of transactions across numerous computers, preventing any record from being changed in the past without changing any subsequent blocks. Blockchain creates a lengthy chain by being validated and connected to the previous "block." Blockchain is the name of the record, after all. Because every transaction is publicly published and verified, blockchain offers a high degree of accountability.

No one can change any of the data that is entered into the Blockchain. It proves that the information is true and unaltered. Blockchain improves stability and demonstrates its vulnerability to hacking by storing data on networks rather than a central database. Blockchain provides an excellent platform for creating and competing with conventional businesses for innovative and cutting-edge business models [1–3].

Blockchain makes it easier for marketers to keep track of medical product usage. Blockchain technology will be used by the pharmaceutical and health industries to eradicate fake drugs, allowing for the tracking of all of these drugs. It aids in identifying the source of deception. Blockchain can ensure that patient records are kept private; once a medical history is created, it can be stored on the blockchain and cannot be altered. All of the hospital's commodity hardware is connected to this decentralized network. Researchers are able to calculate estimates for treatments, medications, and cures for a variety of diseases and conditions utilizing the resources that these gadgets save [4,5].

A distributed ledger network called blockchain adds entries and never removes or changes them without unanimous consent. The value of a Blockchain hash is determined by a cryptographic hash that links each data block with freshly updated information block records. Data is available and accountable to all network users thanks to the distributed Block chain ledger architecture, which guarantees that data is not handled in any centralized location. By preventing a single attack, this decentralized method fortifies and secures the system.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

By doubling the quantity of medical practice and monitoring, it makes it easier to manage health data and patient care while saving time and money for both patients and practitioners. By storing medical records on a block chain, the patient will be able to monitor the movement of their data [6].

II. INTERNET OF THINGS AND BLOCK CHAIN

Using IoT and smart devices led to the prevalence of ubiquitous computing. Presently, there were over twenty billion IoT devices and smart phones. The devices of IoT are vital in the majority of conditions via IoT based sensor networks providing remote monitoring, where as smart devices are providing a remote realtime video feed to the individuals. In addition, the applications of IoT, including diagnostic reporting, body sensing and healthcare, monitoring and industrial automation, assets tracking, surveillance and security, telemedicine and telemedicine consultation, telemetry, and so on, are making massive advances [7]. One of the reasons that IoT is very wide spread is due to its capability in sharing information between devices, support for heterogeneity, and simplicity of accessibility. Yet, such properties are inducing a few obstacles, particularly associated with trust, privacy, and security [8]. Because of the lack of audit mechanism or verification, the challenges related totrust, privacy, and security were complex and critical in IoT, particularly in the sensitive information domain, including healthcare, economics, military communication, and engineering [9]. Since the block chain is providing an approach for information exchange between a group of undependable entities, its inherent characteristics, including fraud protection, authentication, data integrity, and so on. are solving the requirements related to trust, privacy, and security in IoT [10].

III. ARCHITECTURE OF BLOCK CHAIN

Initially, a bitcoin has been generated with the technology of block chain for keeping away from double spending, yet presently, the block chain is used for other reasons. IoT in this study is an example. Generally, the term “block chain” is utilized for mentioning data structures occasionally to systems or networks. In addition, the block chain can be defined as a list of ordered blocks [11], in which each one of the blocks consists of transactions. Also, each one of the block chain blocks is associated with the preceding block, consisting of a hash from the previous block, as can be seen in *Fig 1*. Thus, the transaction history on block chains might not be erased or altered without totally altering the block chain contents. This is why block chains are considered to be sage against hackers[12].

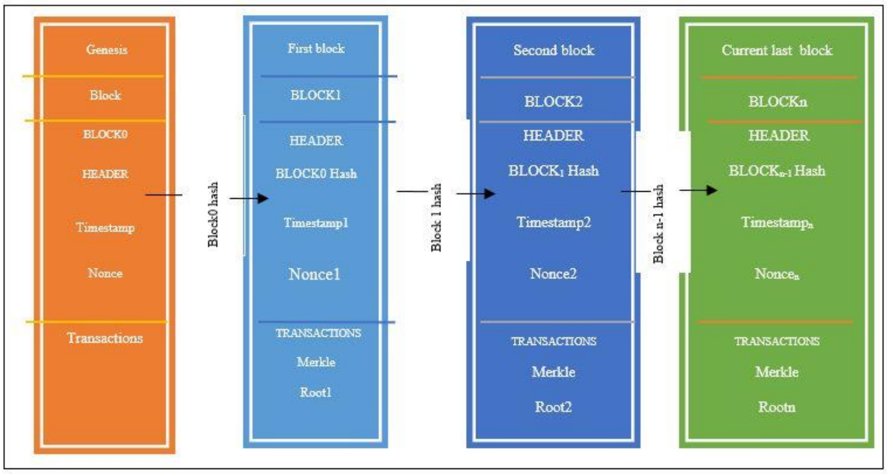

FIG. 1. A BLOCK CHAIN LIST.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

Block chains have many properties:

A. Persistency. Transactions on the block chain might be validated quickly, while invalid transactions won't be identified via miners. Therefore, there is no possibility for erasing transactions which already occurred [13].

B. Auditability. Each block chain transaction indicates a previous one. Thus, all transactions will be simply tracked and verified [14].

C. Decentralization. Third forces on the block chain aren't needed for verifying transactions. The consensus algorithm is the one utilized for maintaining the consistency of data on block chain networks [15].

D. Anonymity. In block chain networks, each one of the users is interacted by means of a generated address. Thus, the user's real identity isn't shown in the interaction[16].

E. Data structure. Transactions have been formatted into blocks which were connected with the use of a crypto graphic hashing algorithm that takes as its input prior entry data. The output includes a secure data chain where a block won't be changed with no invalidation of the hash [17].

F. Distributed. Each network's node includes a full data copy since the genesis block (first block in the chain), removing any single point of failure.

G. Security. The block chain's data integrity is ensured via the cryptographic hash functions. Also, authenticity is guaranteed via using private keys. Altering the block might lead to changes in its hash function,which might render the block in consistent with all subsequently chained blocks; this might be identified via other system nodes and the changes will bedis allowed [18].

H. Consensus. Nodes are algorithmically validating new entries; entries which have been validated via most of the nodes were included in the block chain.

I. Transparency with privacy. Transactions are not just visible to everyone, yet they were considered to be traceable throughout the chain; all ledger transactions might be viewed via all participants. Even though all participants have full copies related to the database transactions, no user identity is visible [19].

J. Time stamps. Time stamping is ensuring that the transaction order is complete and precise.

K. Software updates by consensus. Updates to the block chain software were accepted via verification by consensus.

L. Disinter mediation. Block chains are eliminating the requirement for intermediaries, decreasing the costs of overhead, and mitigate single point of failure vulnerability.

M. Turing Complete. Computability was unbounded, provided one has the needed resources; one might write contracts for nearly all computational problems [20]

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

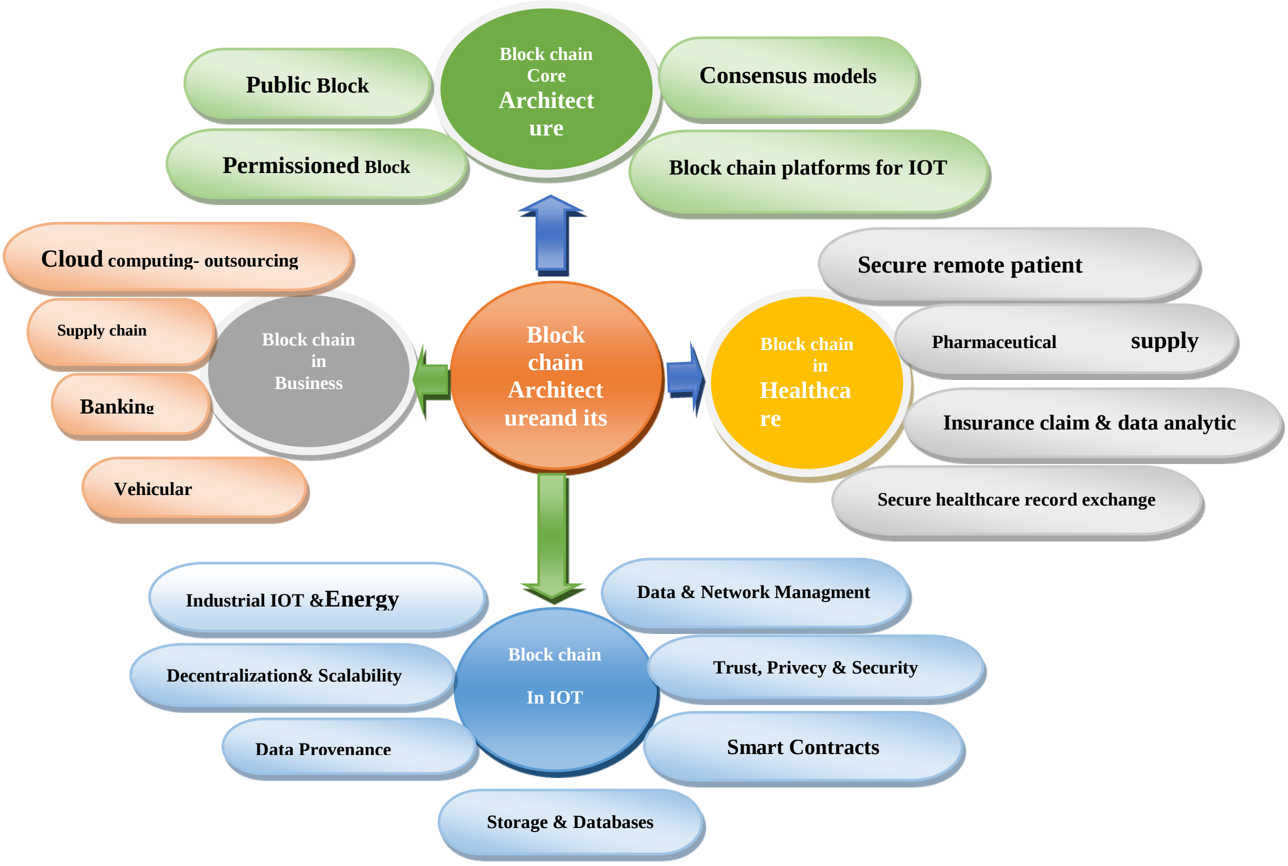
Public Block
Block chain Core Architecture
Consensus models
Permissioned Block
Block chain platforms for IOT
Cloud computing- outsourcing
Supply chain
Block chain in Business
Banking
Vehicular
Block chain Architectureand its
Block chain in Healthcare
Secure remote patient
Pharmaceutical supply
Insurance claim & data analytic
Secure healthcare record exchange
Industrial IOT &Energy
Data & Network Managment
Decentralization& Scalability
Block chain In IOT
Trust, Privecy & Security
Data Provenance
Smart Contracts
Storage & Databases

FIG. 2. SHOWS A BLOCK CHAIN ARCHITECTURE AND ITS APPLICATIONS PRESENTED IN THIS ARTICLE.

IV. SECURITY OF BLOCK CHAIN

The major criteria defining the security policy of an organization asa set of security rules, guide lines, or procedures forced (or assumed to be forced) in the future and/or currently via hypothetical or actual organization in the operational environment [4]. In addition, the policies of access control were developed from trivial matrices to very complicated representation indicated in advanced and sophisticated languages. It is verified that such complexity and expansions are requiring robust automatic approaches for understanding and managing them [5]. With regard to conventional access control models, the policies of access control were specified as a set of rules which are stored in the server or, at best, distributed on many network nodes. In IoT, there is a necessity for having a distributed policy which goes with IoT’s decentralized aspect, and thus (and for many other reasons indicated later), the block chain is used in this work as a base for the suggested framework; also, there is a necessity for having a dynamic policy which considers the context where the smart devices are, yet also that might be enhanced with time, such enhancement clearly doesn’t, and can’t, be controlled via human beings assuming the massive and heterogeneous amount of data generated via IoT. Thus, this study is using AI algorithms, particularly the ones related to machine learning, for ensuring the task.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

V. SMART CONTRACT

In the year 1997, Szabo [20] provided the smart contract concept as a way for digitally formalizing and securing the relations across the network. Also, the smart contract isde_nedas an application which runs on the block chain network as well as executed via all the participants in the network [21]. In addition, the smart contracts were specified as computer codes governing the block chain transactions and the conditionsrelated to mutually agreed contracts [22]. Lately, a lot of block chain based projects conducted smart contracts, including hyperledger and Ethereum platform. They are allowing transactions and truste dagreements to be rendered among distinct, anonymous entities without a requirement for an external enforcement mechanism or central authority. Furthermore, the platform of Ethereum allows creating smart contracts suiting the required system's requirements. With regard to using smart contracts in the systems of EMRs, they allow developing dynamic and scalable conditions, rules, and terms for securely sharing and exchanging medical records.

VI. ETHERUM

Ethereum can be defined as one of the block chain platforms developed via Vitalik Buterin,as well as discussing a few Bitcoin restrictions. The major advantage of Ethereum is that it is supporting full Turing completeness, indicating that Ethereum is keeping up with all computing types. Furthermore, Ethereum is specified as a transaction based state machine. The major Ethereum significant elements are as follows:

A. **Currency.** For doing the computations in the network in a data transmission form, "Ether" or ETH was utilized as intrinsic currency on Ethereum.

B. **Transaction.** In Ethereum, a transaction is indicating a signed data package that is storing messages which are going to be sent from EOA. Also, account creation and message call were the two transaction types in Ethereum. Furthermore the transaction includes the message recipient, the signature of the sender, the number of Ether as well as the data to be sent, also the number of Starts (Gas limit) and Gas price.

C. **Technology used.** Ethereum applies many technologies involving data storage, web technology, and client/node implementation.

D. **Account.** Each one of the Ethereum accounts has a 20-bytes address and includes 4 parts, particularly non cecounter, storage, either balance, and contract code. Contract Account and Externally Owned Account (EOA) were the two account types in Ethereum. Also, EOA was controlled via the private key, while the contract account was controlled via contract code. Only EOA activates the Contract Account.

E. **Consensus algorithm.** There are three consensus algorithm types in Ethereum, particularly Proof of Work (PoW), Stake (PoS), and Proof of Authority (PoA).[23-24].

VII. MATHEMATICAL MODELING FOR BLOCKCHAIN TECHNOLOGY [25]

1- Consensus Mechanisms

A-Proof of Work (PoW):

- Block generation times can be examined using probability distributions or queuing theory.
- Simulate the amount of work needed to solve cryptographic riddles.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

B-Proof of Stake (PoS):

- Using Markov models to model staking pool state transitions
- Examine validators' incentives using game theory.

C- Byzantine Fault Tolerance (BFT):

- Graph theory and decision trees as mathematical models for the Byzantine generals' dilemma

2- Cryptographic Models

A-Hash Functions:

- The outputs of hash functions (uniformity and collision resistance) are statistically analyzed.

B-Elliptic Curve Cryptography:

- Using number theory to model encryption and secure key creation.

C-.Zero-Knowledge Proofs:

- Formalizing zero-knowledge protocols using algebraic structures.

3- Economic and Game Theory Models

A-Tokenomics:

- Use differential equations to create models for inflation and deflation as well as token supply.

***B-Auction Models*:**

- Examine blockchain-based resource allocation using auction theory (e.g., Ethereum gas fee auctions).

C-Incentive Mechanisms:

- Game-theoretic models to assess how participants behave in transaction validation, staking, and mining

4. Network and Security Models

A-Blockchain Network Propagation:

- Simulate transaction propagation using stochastic models and graph theory.

B-Attack Models:

- Use Markov chains and probability models to examine vulnerabilities such as a 51% attack.

C-Network Scalability:

Queueing theory for analyzing transaction processing speeds

5. Data Storage and Optimization

***A-Merkle Trees*:**

- Model Merkle tree structures using combinatorics and graph algorithms.

B-Sharding:

- Optimization algorithms for data distribution in blockchain networks.

C-Compression Models:

- Use information theory to optimize storage for distributed ledgers.

VIII. DIFFERENT BETWEEN BLOCKCHAIN WITH AND WITHOUT IOT [26]

A-Data Source and Input

- **Without IoT**:
  - Data is typically input manually or comes from other digital systems.
  - Usually, data is entered by hand or is obtained from other electronic systems.
  - Uses pre-existing software programs or human involvement to feed data.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

    - Restricted to conventional use cases such as supply chain monitoring, smart contracts, or cryptocurrency.
- **With IoT**:
    - IoT devices, including sensors, RFID tags, and connected gadgets, automatically generate data.
    - Dynamic and autonomous operations are made possible by continuous and real-time data input from the physical world.
    - Makes it possible for uses like automated supply chains, smart cities, and connected cars.

B-Trust and Data Authenticity

- **Without IoT**:
    - Although blockchain guarantees participant confidence, the validity of data is dependent on the dependability of data sources.
    - Input that is not independently validated may include errors or be tampered with.
- **With IoT**:
    - By feeding data straight to the blockchain, IoT devices lessen the possibility of data entry point manipulation.
    - By combining the immutability of blockchain technology with the IoT's capacity to collect sensor-based, real-world data, trust is increased.

C-Automation and Smart Contracts

- **Without IoT**:
    - The blockchain system's digital triggers are the only sources of automation.
    - Smart contracts depend on predetermined digital criteria, which frequently call for outside validation.
- **With IoT**:
    - Real-world events, like temperature thresholds and location changes, can be detected by IoT sensors, and smart contracts may respond to them.
    - Enables autonomous decision-making in fields like industrial automation and logistics.

D-Scalability and Data Volume

- **Without IoT**:
    - Because transactions are restricted to inputs from users or applications, the volume of data is manageable.
    - Scalability in terms of network traffic and storage is easier to maintain.
- **With IoT**:
    - The amount of transactions on the blockchain can be greatly increased by high-frequency data from IoT devices.
    - To manage the massive data influx, technologies like Layer 2 scaling or off-chain storage are needed.

E-Security and Privacy

- **Without IoT**:
    - Security is concerned with safeguarding nodes and keys as well as maintaining the integrity of the blockchain.
    - User identity and transaction metadata are at the center of privacy concerns.
- **With IoT**:
    - IoT devices have the potential to create vulnerabilities like sensor spoofing or hacking.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

  - To protect the blockchain network and IoT devices, further security layers are required.
  - Device identity protection and IoT data streams are now included in the privacy challenges.

F-Applications

- **Without IoT**:
  - Cryptocurrencies (e.g., Bitcoin, Ethereum).
  - Decentralized finance (DeFi).
  - Digital identity management.
- **With IoT**:
  - Energy management and smart grids.
  - Industrial IoT and predictive maintenance.
  - Autonomous vehicles and smart transportation.
  - Medical monitoring and linked equipment.

TABLE I. SUMMARAY TABLE

Feature	**Blockchain Only**	**Blockchain with IoT**
Data Input	Manual or digital systems	Automated from IoT devices
Automation	Digital triggers only	Real-world event-driven triggers
Data Volume	Moderate	High
Security	Blockchain-specific threats	IoT and blockchain vulnerabilities
Applications	Cryptocurrencies, DeFi	Smart cities, logistics, healthcare

IX. LITERATURE SURVEY

TABLE II. SUMMARIZE METHODS OF BLOCK CHAIN

Ref.	Concept	Type of Security	Goal of Study	Conclusion
27	Transfer security data in the block chain network	RSA Cryptosystem	Deployed across organizations that rely on high security communicating media files viz., images, audio, video, and documents making the communication at most secure	Any type of file can be transferred by converting it into a text file using Base64 encoding. The raw text encoding was encrypted using RSA due to its benefits provided inters of the co-factoring needed to break it.
28	Block chain to a health application network	Smart contracts	modified block chain models adequate for the devices of IOT	The solutions are making the IOT transactions and application data further secure as well as anonymous across the block chain based network.
29	Information security as well as a solution via using a block chain in data security.	Hash value	Improve the security of cloud computing	Cloud computing is vital to store information, while the information is simply accessible any time and from any place.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

30	Data securely with a Customized technology of block chain.	Designing a generic hierarchical IOT and monitoring topology Block chain For safely storing the data of IOUT.	Ensure that the data which is transmitted over hierarchical sensor networks were private and secure with no high computational costs are still a challenge	Performance analysis as well as mitigation related to security Attacks analysis shows the simplicity of architecture for monitoring IOUT data.
31	Electronic Health Record	Hash value	Developed for sharing information with other healthcare organizations and providers	Promoting the development regarding larger healthcare ecosystems, including new and old innovations
32	Such systems include healthcare, industrial, also others	new light weight Proof of Block & Trade (POBT) consensus algorithm	Smart and effective business processes were based on the networks of IOT,	Reducing the computational time needed via peers as well as allowing high rates of the transaction for resource constrained IOT devices
33	block chain for ensuring the distributed aspect suggested in IOT	Access control in the context of IOT via suggesting a fully distributed and dynamic security policy.	Coming with a centralized architecture, without transmitting the access control management from the central entity to the network nodes	Providing an optimized, dynamic, and self-adjusted security policy.
34	Block chain approach for proposing a decentralized privacy preserving as well as secure Machine learning system,	Pseudo identity for protecting real identity	Designing a decentralized Stochastic Gradient Descent (SGD) algorithm for learning general Predictive model over the block chain.	Developing an extended differential privacy system which is providing strong privacy protection
35	Allow the peers in the block chain network to directly trading as data consumers and data creators.	Smart contract and an encryption algorithm were utilized for controlling the access right of the users	Using a decentralization feature related to block chain for removing centralized platform	CP-ABE algorithm for solving the data security problems and and access control in conventional data- Distribution systems.
36	quantum signature systems	smart contracts	Improving the security performance related to block chain smart contracts against quantum attacks	It is more adequate for the decentralized distributed business applications
37	Novel incentive mechanism leveraging the degree of health providers in terms of their attempts to maintain Medical records as well as to create new blocks.	smart contracts	Improving the present systems as it is providing secure, interoperable, and efficient medical records via patients, healthcare providers,	Including throughput, response time, and communication overhead, the results are indicating the effectiveness of the proposal to handle a Large data-set at low latency.
38	Enhances the individual’s access to quality as well as inexpensive healthcare services	Protocols	Reducing medical errors, improving the safety of patients, and optimizing the healthcare processes.	Integrating multiagent as well as RFID technologies into IOT platform for health-care.
39	Describing the way that a block chain Technology might be utilized in Public Health	Data sharing	Providing interoperability between many partners	Security and privacy for the sensitive data as well as the effect of

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

	Surveillance via decentralized sharing related to genomic data.		sharing the data, yet were worried About their privacy.	decentralization in organizational infrastructures for eliminating inadequacies for Sharing data.
40	Describing a novel system, Model Chain, for adapting the technology of block chain for privacy-preserving machine learning	Hash function	Designing a novel proof-of-information algorithm for determining the order related to the online learning process.	The technology of block chain solves the Privacy preserving healthcare predictive modeling tasks and increasing interoperability
41	Nvestigating the potential of applying BCN in Contract Management, Supply Chain Management, and Electronic Document Management (EDM).	Conceptual Framework	A detailed framework for employing BCN in supply chain management. However, the framework is not validated by smart contracts deployment.	To overcome the issues of collaborative information sharing among project participants, data reliability, transparency, and information traceability
42	Developing Private/Public blockchain networks for construction supply chain management.	Proof-of-concept	Developed a prototype for the construction supply chain process. However, it focuses on financial management rather than information exchange.	The primary reason behind their study was to explore the feasibility and the benefits of using this technology in the construction environment. Even though this study introduced workable prototypes in material information management, the solutions focused primarily on the financial transactions between the supplier and the end user.

X. CONCLUSIONS

In order to assess healthcare utilizing this new technology and to provide a starting point for developing future applications in this area, the given study made reference to a set of evaluation metrics from a technical and domain standpoint. The primary characteristics of blockchain technology security, dependability, and transparency—make it essential for multi-domain systems like finance, data analytics, and healthcare. Blockchain has enormous potential to track pharmaceuticals in supply chains, improve patient record management, and increase the confidentiality and privacy of medical data. Notwithstanding blockchain's benefits, handling private medical data is difficult because of the possibility of privacy violations.

Future suggestions for expanding blockchain's application in healthcare:

1. Create more effective procedures to safeguard private patient information.
2. Ensuring data sharing without disclosing private information by utilizing sophisticated encryption methods and processes like Zero-Knowledge Proofs.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

REFERENCES

[1] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: a comprehensive review and directions for future research, Appl. Sci. 9 (9) (2019) 1736.

[2] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila, Blockchain utilization in healthcare: key requirements and challenges, in: In2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom), IEEE, 2018 Sep 17, pp. 1–7**.**

[3] G. Moona, M. Jewariya, R. Sharma, Relevance of dimensional metrology in manufacturing industries, MAPAN 34 (2019) 97–104, https://doi.org/10.1007/ s12647-018-0291-3.

[4] M.H. Kassab, J. DeFranco, T. Malas, Giuseppe Destefanis Laplante, V.V. Neto, Exploring research in Blockchain for healthcare and a roadmap for the future, IEEE Trans. Emerg. Top. Comput. (2019), 1-1.

[5] B. Shen, J. Guo, Y. Yang, MedChain: efficient healthcare data sharing via Blockchain, Appl. Sci. 9 (6) (2019) 1207.

[6] U. Chelladurai, S. Pandian, A novel blockchain based electronic health record automation system for healthcare, J. Ambient Intell. Humanized Comput. (2021).

[7] S. Ge, S. M. Chun, H. S. Kim, and J. T. Park, "Design and implementation of interoperable IOT healthcare system based on international standards," in Proc. 13th IEEE, Annual Consumer Communications & Networking Conference, 2016.

[8] K. R. Darshan and K. R. Anandakumar, "A comprehensive review on usage of internet of things (IOT) in healthcare system," in Proc. International Conference on Emerging Research in Electronics, Computer Science and Technology, 2015.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for fine grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89–98, November2006.

[10] M. Mettler, "Block chain technology in health-care: The revolution starts here," in e-Health Networking, Applications and Services (Health com), 2016 IEEE 18th International Conference on. IEEE, 2016, pp. 1–3.

[11] K.; Devetsikiotis, M. Block chains and Smart Contracts for the Internet of Things. IEEE Access2016, 4, 2292–2303.

[12] Qu, C.; Tao, M.; Yuan, R. A Hyper graph -Based Block chain Model and Application in Internet of things-Enabled Smart Homes. Sensors 2018, 18, 2784.

[13] A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Block chain and IOT Integration: A Systematic Survey. Sensors 2018, 18, 2575.

[14] Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Block chain with Novel Privacy Risk Control. J. Med. Syst. 2016, 40, 218.

[15] Zhu, X.; Badr, Y. Identity Management Systems for the Internet of Things: A Survey towards Block chain Solutions. Sensors 2018, 18, 4215.

[16] D. A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Block chain for IOT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (Per Com Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.

[17] M. M. Block chain technology in health-care: The revolution starts here. In Proceedings of the 2016IEEE 18th International Conference on e-Health Networking, Applications and Services (Health com),Munich, Germany, 14–17 September 2016.

[18] M. Conoscenti, A. Vetro, and J. C. De Martin, "Block chain for the internet of things: A systematic literature review," in Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of. IEEE, 2016, pp. 1–6.

[19] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Block chain technology innovations," in Proc. IEEE Technology &Engineering Management Conference (TEMSCON), June 2017.

[20] J. Gao, K. O. Asamoah, E. B. Sifah, A. Smahi, Q. Xia, H. Xia, X. Zhang,and G. Dong, "Grid Monitoring: Secured sovereign block chain based monitoring on smart grid," IEEE Access, vol. 6, pp. 9917–9925, 2018.

[21] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Block chain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks," IEEE Trans. Smart Grid, pp. 1–1, 2018.

[22] N. Zhumabe kuly Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Block chain and Anonymous Messaging Streams," IEEE Trans. Dependable Secur.Comput., pp. 1–1, 2016.

[23] N. Kshetri, "Block chain's roles in strengthening cyber security and protecting privacy," Telecommunications Policy, vol. 41, no. 10, pp.1027–1038, Nov. 2017.

[24] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of block chain for the internet of things," IEEE Access, pp. 1–23, May2018.

Received 13/September/2024; Accepted 27/November/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.7

[25] M. Basheer, F. Elghaish, T. Brooks, F. P.Rahimian, C. Park,Blockchain-baseddecentralised material management system for construction projects, Journal of Building Engineering Volume 82, 1 April 2024, 108263.

[26] D. Sheng, L. Ding, B. Zhong, P.E.D. Love, H. Luo, J. Chen Construction quality information management with blockchains Autom. ConStruct., 120 (2020), 10.1016/j.autcon.2020.

[27] A. Panarello, N.Tapas,.; Merlino, G.; Longo, F.; Puliafito, A. Block chain and IoT Integration: A Systematic Survey. Sensors 2018, 18, 2575.

[28] A. Dhar D. GautamSrivastava , S Dhar, and Rajani Singh , A Decentralized Privacy-Preserving Health care Block chain for IOT, Received: 12 December 2018; Accepted: 10 January 2019; Published: 15 January 2019.

[29] A. Dorri; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Block chain for IOT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.

[30] M. Mettler Block chain technology in health-care: The revolution starts here. In Proceedings of the 2016IEEE 18th International Conference on e-Health Networking, Applications and Services (Health com),Munich, Germany, 14–17 September 2016.

[31] M .Mohan, B.J.Nirmal , R.Sophie Angela , R.Nivetha Angel, A.Joseph Praveen, Securing patient Health Record in Block chain With Abe Access Control, Volume 02 Issue 06 June 2020.

[32] SujitBiswas, Member, IEEE, Kashif Sharif, Member, IEEE, Fan Li, Member, IEEE, PoBT: A Light Weight Consensus Algorithm for Scalable IOT Business Block chain, final publication. Citation information: DOI 10.1109/JIOT.2019.2958077, IEEE Internet of Things Journal.

[33] A OUTCHAKOUCHT, Hamza ES-SAMAALI, Jean Philippe LEROY, Dynamic Access Control Policy based on Block chain and Machine Learning for the Internet of Things, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No.7, 2017.

[34] X. Chen_, JinlongJi_, C. Luoy, W. iaoz and P. Li_, When Machine Learning Meets Block chain: A Decentralized, Privacy-preserving and Secure Design, 2018 IEEE International Conference on Big Data (Big Data).

[35] H. Bowen, Li Yi, Fang Li1, D Xinhua, Chen Ping, Block chain-based Access Control Data Distribution System, 2019 IEEE 5th International Conference on Computer and Communications.

[36] Z, Jing Qu, P Liu, And J. Yu, A Block chain Smart Contract Based on Light-Weighted Quantum Blind Signature, date of current version October 4, 2019.

[37] E.Yasser Daraghmi, Y. –Awwad Daraghmi, And S. -Ming Yuan, Med Chain: A Design of Block chain-Based System for Medical Records Access and Permissions Management, Digital Object Identifier 10.1109/ACCESS.2019.2952942.

[38] C. Elena Turcua, Cornel Octavian Turcua, Internet of Things as Key Enabler for Sustainable Health care Delivery, the 2nd International Conference on Integrated Information, 2013.

[39] J. Luis BellodCisneros, F. Møller Aarestrup, Public Health Surveillance using Decentralized Techn9logies, Block chain in Healthcare ISSN 2573-8240.

[40] T. Ting Kuo, L. Ohno-Machado, and Model Chain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Block chain Networks, 2018.

[41] M. Kiu, K.W. Lai, F.C. Chia, P.F. Wong Blockchain Integration into Electronic Document Management (EDM) System in Construction Common Data Environment, Smart and Sustainable Built Environment Ahead-Of-Print (Ahead-of-print) (2022), 10.1108/SASBE-12-2021-0231.

[42] R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G. Amarasinghe, S. Che Public and private blockchain in construction business process and information integration Autom. ConStruct. 118 (2020) Article 103276.

Received 13/September/2024; Accepted 27/November/2024