Healthcare Information Exchange Using Blockchain and Machine Learning

Basant Kumar(✉), Istafa Albusaidi, and Maram Halloush

Modern College of Business and Science, Bowsher/Muscat, Muscat, Sultanate of Oman
{basant,20199619,20189293}@mcbs.edu.om

Abstract. In several industries, including healthcare, new technologies like blockchain and machine learning are being leveraged to generate innovative solutions. A blockchain network is used in the healthcare system, coupled with machine learning, to store and distribute patient data among hospitals, diagnostic labs, pharmaceutical companies, and clinicians. Applications based on Blockchain, and Machine Learning can precisely identify grave errors, including ones that could be fatal in the healthcare and medical industries. The efficiency, security, and transparency of sharing medical data can therefore be improved. Utilizing these two technologies allows medical institutions to gain knowledge and enhance patient data analysis. In this document, blockchain and Machine Learning were studied and their benefits to the process of the Healthcare Information Exchange Process. The benefits and characteristics of both the technologies and how they help with the process are discussed in a simple way. Blockchain works. Blockchain facilitates decentralized data protection in the healthcare industry and prevents specific risks while Decision-making, patient outcomes, and healthcare professional automation are all aided by Machine Learning in the interchange of healthcare information.

Keywords: Blockchain · Nodes · Machine Learning · Healthcare Information Exchange · Chatbots

1 Introduction

Blockchain (BL) and machine learning (ML) technologies have advantages in the healthcare industry, making them implementable. These advantages include documenting and sharing medical information, forecasting disease risk, classifying images from magnetic resonance imaging (MRI) scans, and more. Modern tasks were previously carried out by medical professionals and personnel, but since the appearance of these advancements, tasks are now carried out by various computers. In fact, ML is a type of AI in which computers are allowed to train using specialized methods. Machine intelligence is similarly trained to accumulate segregated data to eventually enable the system to conduct picture detection, categorization, and recognition. Learners evolve through specific methods and instruction.

Therefore, the more data there is, the more accurate the results will be as a result, ML techniques are important approaches to be used in the proposed strategy. Blockchain

N. Bacanin and H. Shaker (Eds.): ICIITB 2022, ACSR 104, pp. 55–69, 2023.
https://doi.org/10.2991/978-94-6463-110-4_6

can be thought of as a record that exists within a system and preserves certain sources of evidence on each end. In other words, a blockchain is an electronic method of data storage that cannot be altered, hacked, or scammed [1]. Blockchain is therefore used to securely store specific types of data, while machine learning is used for other purposes. As a result, blockchain and machine learning are both separate methodologies.

There are a lot of healthcare institutions nowadays, and most of these facilities, use healthcare information exchange. However, there are still some few problems faced by the incoming and long-term care patients and the workers who work in the healthcare facility such as the doctors, pharmacists, labs, and specialists. This project is designed to understand healthcare information exchange and how it can be used with the blockchain and the machine learning technology, and how it's going to help the healthcare care information exchange process.

2 Background

In this section, three topics will be discussed, Healthcare Information Exchange (HIE), Blockchain(BC) and Machine Learning (ML):

2.1 Healthcare Information Exchange

Healthcare information exchange (HIE) amongst health providers has recently been shown to be very beneficial to the medical/healthcare sector [2].

Identification and Purpose

The electronic interchange of healthcare-related data between medical institutions, health information organizations—companies that oversee and regulate the distribution of this data—and governmental organizations in accordance with national standards is known as health information exchange (HIE) [3].

The purpose of HIE is to increase the budget, superiority, security, and competence of patient care, HIE works to facilitate appropriate and secure access to and retrieval of a patient's health information. The term "HIE" can refer to both the act of exchanging information between two or more healthcare organizations or providers and the entity in charge of doing so [4].

Key Forms of HIE

By enabling appropriate access to and secure electronic sharing of a patient's critical medical information, the electronic health information exchange (HIE) helps to increase the efficiency, effectiveness, safety, and affordability of patient care [5].

Currently, there are three main forms of HIE:

1. **Directed Exchange**
   Providers utilize directed exchange to transfer patient data quickly and securely to other healthcare professionals, such as laboratory tests and results, patient referrals, or discharge summaries. It is frequently compared to sending a protected email because this information is transmitted securely, reliably, and encrypted over the internet between medical experts. Coordinated care is made possible by this type of information interchange, which benefits both patients and clinicians [5].

2. **Query-based exchange**
   Providers search and locate available clinical sources on a patient via query-based exchange. When dispensing unanticipated care, this kind of trade is frequently employed. For instance:

   Emergency room doctors may modify treatment plans to prevent adverse medication reactions or redundant testing if they have access to patient information via query-based exchange, such as medications, recent radiology images, and problem lists [5].
3. **Consumer-mediated exchange**
   Patients may manage their health care online in a manner akin to how they could manage their money through online banking thanks to consumer-mediated exchange, which gives them access to their health information. Patients who have access to their own health information can take an active role in the coordination of their care by giving their health information to other professionals, recognizing and fixing inaccurate or lacking health information, recognizing and fixing inaccurate billing information tracking and keeping an eye on their personal well-being [5].

Consumer-Mediated Exchange

Patients can manage their health care online in a manner akin to how they might manage their finances through online banking thanks to consumer-mediated exchange, which gives them access to their health information [5].

Flaws of the HIE Process

Usually, most of the medical information are either stored in papers, or old hardware, despite the availability of secured electronic data transfer. It is done through text messages or when the patients carry their records from a one appointment to the other when that specific medical information is transmitted from one clinic to the other or from one doctor to the other. While provider-patient communication cannot be replaced by electronic health information exchange, it can significantly increase the completeness of the patient's records, which can have a significant impact on care. This is because past medical history, current medications, and other information are jointly reviewed during visits [5].

Importance of HIE

As technology advances and alternatives for exchanging health information grow, health information exchange plays a significant role in the healthcare system by enhancing interoperability. Health information sharing is becoming more popular internationally as healthcare professionals see its advantages for patient care [6].

2.2 Blockchain

Identification
Blockchain can be identifies in simple words as a public ledger, where all devoted transactions are stored in a chain of blocks. The more blocks added to the chain, the longer it grows and expands [7]. NIST identifies blockchain as a distributed digital ledger that is impenetrable to tampering and tamper-evident, typically without a central authority [8].

Types of Blockchain

1. **Private**
   A permissioned or private blockchain is a decentralized platform or system that permits the exchange of private data among a particular group of users or within a company. Entry to a private blockchain is controlled entirely and limited to a select set of individuals who share the same affiliation or field. Additionally, private blockchain regulates who may take part in the consensus process. A private blockchain nonetheless enjoys the advantages of other blockchain characteristics like visibility, public ledger of all transactions, and consensus despite being constrained and managed by a central authority.
2. **Public**
   A public or censorable blockchain is an open source, decentralized network that allows anybody to join and participate in mining. Every participating node has ability to write, read, validate, and mine blocks without any restrictions. In most cases, a group of transactions are combined into a new block, and players fight to find the best nonce (through the mining process) to profit from it. Bitcoin and Ethereum have the most well-known public blockchains.
3. **Consortium**
   A hybrid (consortium) blockchain is a combination of a private and public blockchain in which several organizations manage the consensus and block validation decisions, as well as who has access to the blockchain.

Method of Work and Security
A predetermined set of nodes share and validate ledgers in a private blockchain. Nodes that want to join the system must initiate or be validated by the system. The owner of an authorized note has the ultimate authority to regulate access in systems where all notes are fully trusted [9].

There are three conditions must be met by every and any information system, especially when it's related to healthcare affiliations, to provide security: confidentiality, integrity, and availability. Due to blockchain's decentralized nature, even if one or more nodes are compromised, the overall system functionality may be ensured. Securing a user's private key is part of maintaining confidentiality in blockchain because doing so is necessary to undermine the system or pass off as someone else.

When transmitting information, the integrity and security are ensured using the public and private keys. Each user has a distinct private key, which ensures that they are the rightful owners of any information. The user signs the data with his private key to prove

his legitimacy to the network. The public key is derived from the private key based on a specific algorithm that the system uses. The public keys are spread over the network because they are irreversible (a private key cannot be obtained from public keys). To access the data, other users must use their public keys.

To guarantee the security and integrity of information exchange, public and private keys are used. Each user has a special private key that ensures their ownership of certain pieces of information. To demonstrate his authority to the entire network, the user signs the data with his private key. Based on a certain algorithm that the system employs, the public key is produced from the private key. Since the public keys are irreversible, they are dispersed throughout the network. Public keys are required for other users to access the data.

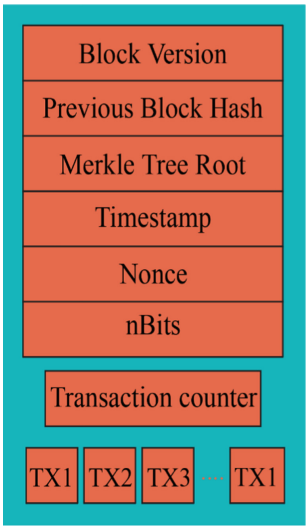
For instance, CONIKS [10], developed a key management system to handle encryption keys and free users. In this system, two-step verification is used. The receiver's public key is validated first, and then the key is examined to make sure it hasn't been changed over time. Blockchain makes it impossible for unauthorized parties to tamper with the data, ensuring integrity. A blockchain-based integrity IoT framework was suggested in [11] to do away with the need for third parties to be trusted. Because of its distributed system architecture approach, blockchain achieves availability in the most straightforward method.

Since all transactions must be confirmed and validated by a group or community of miners, blockchain security mechanisms prevent hacking through distributed consensus, protecting the security of management systems and the centralized data storage.

A blockchain network is additionally watched over by every node, and since every node keeps a copy of the blockchain, hostile nodes (users) are unable to add modified blocks into the public ledger. As a result, even if numerous ledgers are compromised, the blockchain will not be affected because third-party blockchain copies are thought to constitute a reliable backup [12]. Blockchain technology has the power to protect the network from some dangerous behaviors. Some of them, meanwhile, could harm the blockchain network [13].

A Single Block's Architecture

In the Fig on the left, the block structure is displayed. Each block has a timestamp, nBits, nonce, parent block hash, Merkle tree root hash, and block version. The necessary validation criteria are shown in block versions. To create a chain, the parent hash block represents the hash of the previous block. It uses a 256-bit hash. The time in seconds since 1970 is represented by a timestamp, and the current hashing target, or nBits, is a requirement for the block to be valid [14].



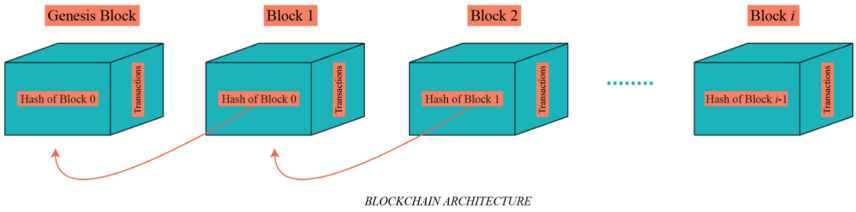
The header hash must be less than or equal to nBits, an unsigned integer, for that header to be a legitimate component of the blockchain. An invalidating hash for the block is produced by a nonce, a 4-byte random value. The block hash begins with zeros and gradually increases in number over time to make it harder to decipher [15]. Therefore, to ensure that the block is authentic, miners continuously compute and guess the nonce that will result in the precise hash (including the number of zeros at the beginning). In other words, when the nonce is plugged into the hashing process, the miners must produce an output that satisfies certain criteria. Until an adequate output value is discovered, miners utilize brute force to guess the proper value algorithm. This calculation is required because any alteration to the input data results in a completely different output. Therefore, these calculations must produce an exact result that corresponds to a distinct input.

Blockchain's Architecture

Blockchain can be visualized as a traditional public ledger, as seen in the Figs. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 [16] [17] Where a complete list of transaction (Tx) records is recorded on a series of blocks (hashed timestamps) [16, 18].

Each block has a reference to the parent block, which is the block that came before it. A hash value, which is a single, distinctive value for each block that renders the block valid, is used to represent this reference. The genesis block is the very first block on the blockchain, and since it lacks a parent block, its hash value is a simple zero.

The uncle block, which is produced when two blocks are mined simultaneously, is another word that the Ethereum blockchain has suggested. When this occurs, one block is regarded as the official block and is linked to the chain, while the other block is left out and is referred to as an uncle block. In contrast to Bitcoin, which ignores the entire block, the hashes of uncle blocks are also retained in the Ethereum blockchain [19]:



BLOCKCHAIN ARCHITECTURE

Blockchain's Benefits to the HIE Process

Since blockchain technology can be expanded to become a standard for stakeholders, it enables the safe sharing of Electronic Health Records (EHRs) [20]. Many benefits come from using blockchain for EHR, like protecting patient privacy [20] and raising the standard of healthcare [21]. The use of blockchain has been driven by the demand for patient-centric services and the necessity to link various systems [22].

Patients have complete ownership over their medical records because to blockchain. Due to its extreme case-sensitivity, patient information must be handled with great care when being transmitted and stored. Denial of Service (DoS), mining attacks, storage assaults, and dropping attacks are among the malicious attacks that are most likely to target it [23]. Because it includes a variety of access control measures, blockchain offers a safe and resistant platform for the healthcare industry against errors and attacks [24].

2.3 Machine Learning

Definition of Machine Learning (ML)

Machine learning (ML) is the study of computer algorithms for learning from experience. ML is a subfield of artificial intelligence (AI) that creates computer systems capable of doing tasks that need human intellect [25]. While healthcare information exchange is essential for carefully translating and disseminating information to help and educate patients and the public, ML has been shown to be relevant in healthcare due to its capabilities for complicated dialogue management and conversational flexibility [26]. In this subject overview, we will discuss how the use of ML/AI in healthcare communication might assist people. Chatbots for information, health education, cancer therapy, and medical imaging are examples of this.

Use of Machine Learning in HIE

Chatbots and its Identification

A chatbot is a type of computer system that allows humans to engage with computers using natural human language. AliMe, DeepProbe, SuperAgent, MILABOT, and RubyStar are some examples of current chatbot systems. ("[Solved] Machine Learning in Healthcare Communication Need review of ...") A chatbot may identify user input in a variety of formats and access data to offer a pre-set acknowledgement [27].

Chatbot for Patient Care

Healthcare chatbots have significant potential in medical communication since they improve communication between clinic-patient and doctor-patient. It can assist meet

the high demand for health services through remote testing, prescription follow-up monitoring, or phone consultations.

Emergency Response
In an emergency, a few minutes might be the difference between life and death. In many circumstances, faster health care and accessible systems can save many lives. A semi-automated end-to-end emergency paramedical response system bot can be accessed.

Chatbots Jobs
A chatbot may do quick and simple health surveys, set up personalized health-related reminders, connect with healthcare teams, arrange appointments, and access and analyze health data. Chatbots can respond quickly or instantly to patients' healthcare-related concerns while looking for symptoms or trends in illness prediction. One example is the Internet-based Doc-Bot, which can be accessed through cell phone or Messenger. The bot may be programmed to respond to certain health situations, populations, or activities.

3 Research Methodology

For the research, data was collected from primary and secondary resources. The primary source of data was from a survey, a survey of 16 questions was conducted and sent to different people from different age groups, careers, and specializations. The survey helped in coming up with solutions that can be solved especially here in the sultanate. It made us realize that there is very little awareness about Blockchain in the Sultanate of Oman. The secondary source of data was retrieved from online journals, articles such as research gate, google scholar, IEEE, Springer, and other reliable websites. Results will be shown and discussed in the next section.

4 Results and Discussions

Below are the results we have gathered from the survey we did to gain more knowledge on how people view Blockchain and Machine Learning. And followed by analysis of each question and how the respondents responded.

Survey Results
And in Fig. 2 shows us that 67% of the respondents agree with the fact that sharing records using blockchain is private and user friendly while 13% of them just agreed, and 10% of them were neutral about it and 10% disagreed and no one strongly disagreed.

Survey Conclusion
The survey result brough the conclusion that not many people are aware of what blockchain is, and how many people used machine learning application without knowing what it is. To solve this solution, certain organizations should raise more awareness about blockchain and machine learning and how it can ease the process of HIE. This can be done by conducting seminars and conferences for schools and universities. Also, to introduce blockchain and machine learning as a course for Information Security or Cybersecurity students in case it could be implemented in the Sultanate.

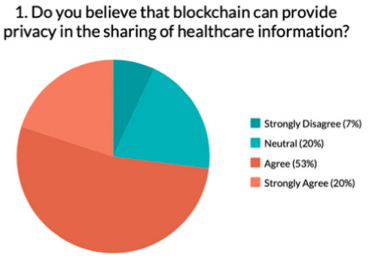


Fig. 1. 20% of the respondents strongly agree that blockchain can provide privacy in sharing healthcare information, while 53% agreed, 20% were neutral and 7% strongly disagreed.

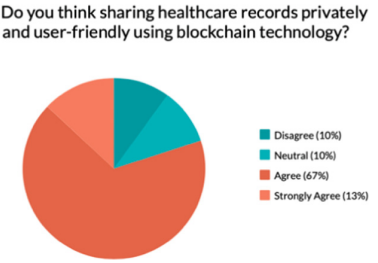


Fig. 2. 67% of the respondents agree with the fact that sharing records using blockchain is private and user friendly while 13% of them just agreed, and 10% of them were neutral about it and 10% disagreed and no one strongly disagreed.

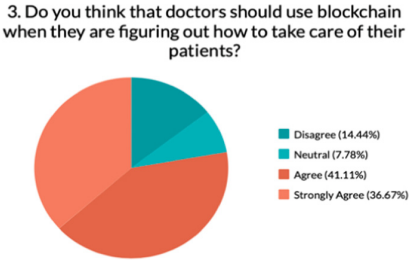


Fig. 3. 14.44% of the respondents disagreed to not use blockchain while taking care of their patient, while 41.11% agree, and 36.67% strongly agreed to using blockchain and 7.78% of the respondents were neutral about it.

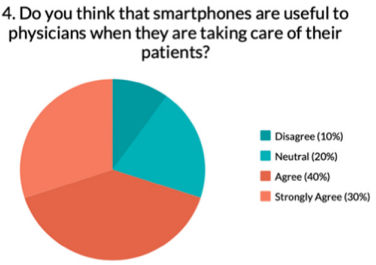


Fig. 4. 40% of the respondents agreed that using smartphones is useful when physicians take care of their patients, while 30% strongly agreed, and on the other hand, 20% were neutral and 10% disagreed.

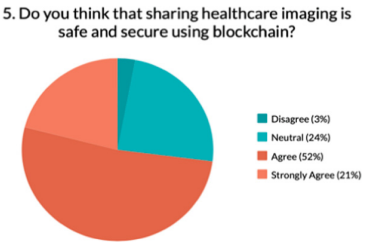


Fig. 5. 52% of the respondents agreed that sharing data from imaging is safe while using blockchain while 21% just agreed. Instead, 24% were neutral and only 3% disagreed.

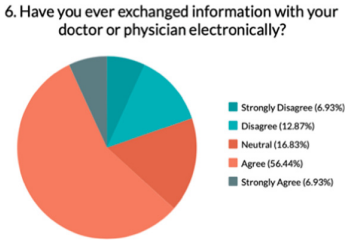


Fig. 6. That 56.445 of the respondents agreed on exchanging information with their doctors, and 6.93% of them have exchanged information with their doctors while 16.83% of them never have done that since they were neutral. While 12.87% of them disagree with this idea and 6.93% of them never shared their data before

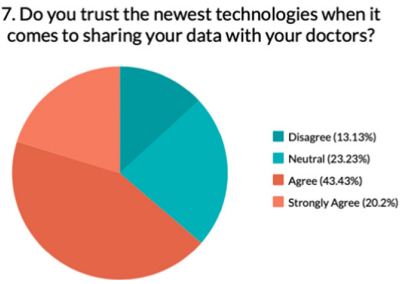


Fig. 7. 20.2% of the respondents strongly agreed with trusting the new technologies, and 43.43% agreed to it, and 23.23% of them were neutral about it. Whereas 13.1% of them disagreed.

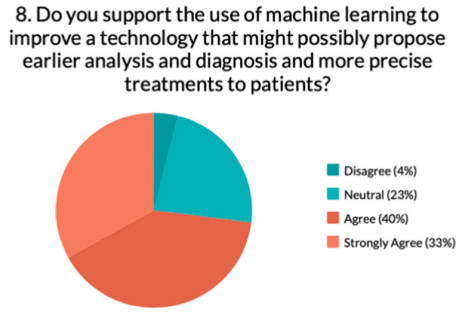


Fig. 8. 40% of the respondents agreed to the use of machine learning to improve certain technologies that can save someone's life with early diagnosis, and 33% strongly agreed with it. While 23% of them were neutral about it and only 4% of them disagreed as they think there are better ways to diagnose patients.

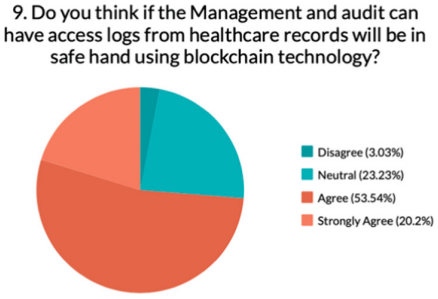


Fig. 9. 53.54% of the respondents agreed that is safe for auditors and management officers to have access to the health care records and logs of the patients if blockchain technology was used while 20.2% strongly agreed to that. Meanwhile, 3.03% disagreed and 23.23% were neutral about it.

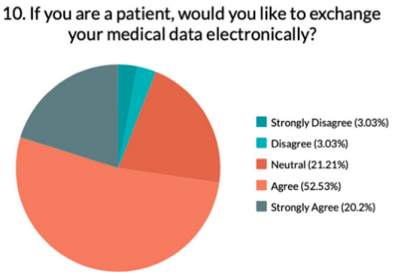


Fig. 10. 52.32% of the respondents agreed to sharing and exchanging their medical data with their physicians and doctors, and 20.2% strongly agreed to that. While 21.21% were neutral about it as they never shared their information's with any of the healthcare's facilities. While 3.03% disagreed and 3.03% strongly disagreed as they never shared and don't think it's a good idea.

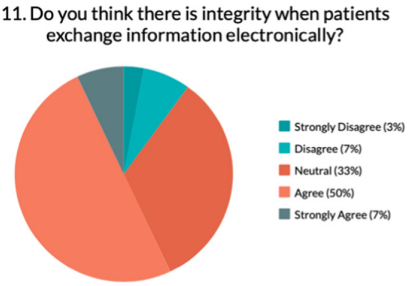


Fig. 11. 50% of the respondents agreed and believe that there is integrity when patients share their information with their doctors electronically, while 7% of them strongly agreed to that. On the other hand, 33% of them were neutral, but 7% of them disagreed and 3% of them strongly disagreed.

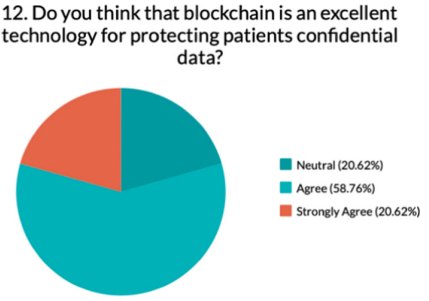


Fig. 12. 58.76% of the respondents agreed anything that Blockchain is an excellent method to protect patient confidential data, and 20.62% of them strongly agreed to that. While 20.62% of them were neutral about it. Luckily no one disagreed or strongly disagreed

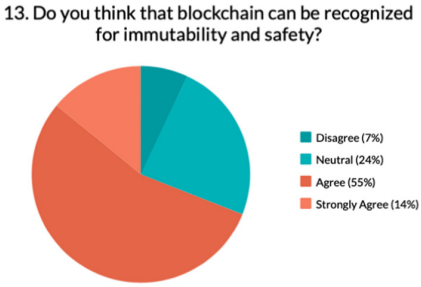


Fig. 13. 55% of the respondents agreed to that Blockchain can be emerging brilliant safe for use with patience, and 14% of them strongly agrees with that. While on the other hand, 24% of them were neutral and 7% of them disagreed

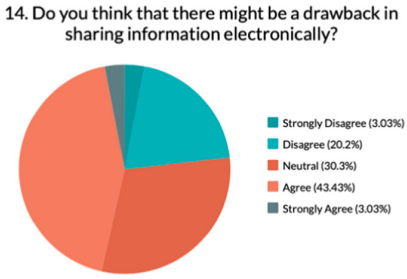


Fig. 14. 43.43% of the respondents agree and think that they might be a drawback it comes to patients and sharing their information electronically, and 3.03% of them strongly agreed and 30.3% of them where neutral about it. Meanwhile, 20.2% of them disagreed and 3.03% of them strongly disagreed and think that there won't be any drawbacks

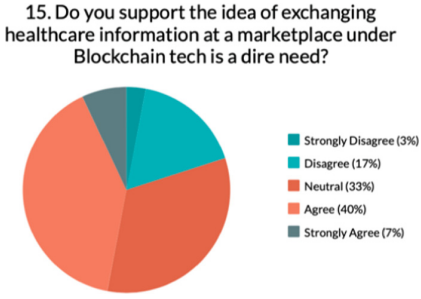


Fig. 15. 40% of the respondents who took this survey agreed to supporting the idea of exchanging healthcare information at the marketplace while using Blockchain is a dire need, while 7% of them strongly agreed to that. And while this is a present of them were neutral as they think it won't be a day you need, and 17% of them disagreed, and 3% of them strongly disagreed

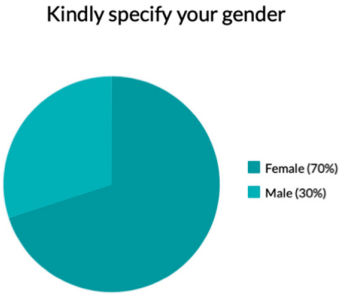


Fig. 16. 70% of the thirty respondents were females and the other 30% were male.

References

1. Jain S, Doriya R. Security framework to healthcare robots for secure sharing of healthcare data from cloud. International Journal of Information Technology 14(5), 2429-2439 (2022).
2. B. E. Dixon and C. M. Cusack, "Measuring the value of health information exchange," in Health Information Exchange. CONFERENCE 2016, pp. 231–248, Elsevier (2016).
3. Researchgate, https://www.researchgate.net/profile/Shan-Jiang-, last accessed 2022.
4. Techtarget, https://www.techtarget.com/searchhealthit/definition/Health-information-exchange-HIE What is Health Information Exchange (HIE)?, last accessed 2022/10/21.
5. Healthit, https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/what-hie, last accessed 2022/10/07
6. Mobisoftinfotech.com, https://mobisoftinfotech.com/resources/blog/health-information-exchange-benefits-and-challenges/, last accessed 2022/10/07,
7. Allquantor.at, https://allquantor.at/blockchainbib/pdf/zheng2018blockchain.pdf, last accessed 2022/10/07.
8. NISTIR 8202, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf, last accessed 2022/10/10.
9. Bitcoin.org, https://bitcoin.org/bitcoin.pdf, last accessed 2022/10/10.
10. Princeton.edu, https://coniks.cs.princeton.edu, last accessed 2022/10/11
11. Liu, B.; Yu, X.L.; Chen, S.; Xu, X.; Zhu, L.: "Blockchain Based Data Integrity Service Framework for IoT Data." pp. 468–475. Honolulu, HI, USA (2022).
12. Xu, J.J,: "Are blockchains immune to all malicious attacks?". Journal 2(25), 25-27 (2022).
13. Cai, Y.; Zhu, D. Fraud detections for online businesses: a perspective from blockchain technology.
14. Bitcoin.org, https://bitcoin.org/en/glossary/, last accessed 2022/10/12.
15. Norberhuis, S.D. MultiChain: A Cybercurrency for Cooperation. Master's Thesis, Delft University of Technology, Delft, The Netherlands, (2022).
16. Sultan, K.; Ruhi, U.; Lakhani, R,: "Conceptualizing Blockchains: Characteristics and Applications. In Proceedings of the 11th IADIS International Conference on Information Systems" 2018, pp. 49–57 Lisbon, Portugal, 14–16 April (2022).
17. Zubaydi H, Chhong Y, Ko K, Hanshi S, Karuppayahh S. A Review on the Role of Blockchain Technology in the Healthcare Domain. (2022).
18. Chuen, D.L.K. (Ed.) Handbook Of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data; Academic Press: Cambridge, MA, USA, (2015).
19. Blockchainlab.com, http://blockchainlab.com/pdf/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, last accessed 2022.

20. 21. Esposito, C.; Santis, A.D.; Tortora, G.; Chang, H.; Choo, K.K.R.: "Blockchain: A anacea for Healthcare Cloud-BasedDataSecurityandPrivacy?" IEEECloudComput, Journal 5, pp 31–37 (2019).
21. Omar, A.A.; Rahman, M.S.; Kiyomoto, A.B.: "MediBchain A Blockchain Based Privacy Preserving Platform for Healthcare Data. In Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage", pp 28–29. Guangzhou, China, (2017).
22. Karame, G.O.; Roeschlin, M.; Gervais, A.; Capkun, S.; Androulaki, E.; C˘apkun, S.: "MisbehaviorinBitcoin: A Study of Double-Spending and Accountability". Journal 18(2), (2018).
23. 25. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R.: "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT". Sensors 19, 326 (2020).
24. Karame, G.O.; Roeschlin, M.; Gervais, A.; Capkun, S.; Androulaki, E.; C˘apkun, S.MisbehaviorinBitcoin: A Study of Double-Spending and Accountability. ACM Trans. Inf. Syst. Secur.18, 2 (2018).
25. Kubicki, Grzegorz, Kiełbasa, Tomasz, Wiche, Jarosław, http://bitp.cnbop.pl/wp-content/uploads/2017/05/BITP_Vol_45_Issue_1_2017_pp.142-153.pdf, vol. 45, pp142–153. Bezpieczeństwo i Technika Pożarnicza (2017).
26. IEEE 18th International Conference on Magnet Technology Exhibitors List. IEEE Transactions on Applied Superconductivity. 14(2):p, 145 (2006).
27. Lukman, A.S.; Ameedeen, M.A. "Modern Chatbot Systems: A Technical Review." ("Machine Learning Enabled Health Care Chat Bot - Academia.edu") In Proceedings of the Future Technologies Conference (FTC) 2018; Arai, K., Bhatia, R., Kapoor, S., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 1012–1023 (2018).