International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429)

Securing Healthcare System with the Blockchain Technology

Adriena Lim Ken We'rn[1], Intan Farahama Binti Kamsin[2], Salmiah Binti Amin[3], Nur Khairunnisha Binti Zainal[4]

[1'2'3'4]School of Computing, Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.

[1]adrienalimkw23@gmail.com, [2]intan.farhana@staffmail.apu.edu.my, [3]salmiah@staffmail.apu.edu.my, [4]khairunnisha.zainal@staffmail.apu.edu.my

***Abstract* - In the event of a cyberattack, it might cause care to be disrupted owing to software breakdowns. The inability of healthcare workers to deliver proper care may be hampered by the loss of access to health records. This proposal reviews previous studies and discusses what the current healthcare system looks like, blockchain technology, and other similar systems to understand what can be learned and drawn from. The aim of this research is to implement Blockchain Technology to the healthcare industry in Malaysia to enhance the cybersecurity of the healthcare system, thereby reducing the number of cyber-attacks in the healthcare sector. This study utilizes a quantitative methodology, with respondents chosen using complex probability stratified sampling method to gather data. Aside from that, this proposal describes how surveys and case study evaluations aid in the identification of various system specifications.**

***Index Terms* - Blockchain technology, healthcare, COVID-19, cybersecurity**

1. Introduction

Over the years, cyberattacks such as malware, phishing, man-in-the-middle (MitM), denial-of-service (DOS), or ransomware have caused numerous impacts such as data breaches, system paralyze, etc. One of the most high-profile cyberattacks of the past few years was the Universal Health Services (UHS) attack in 2020, in which a total of 400 hospitals and health facilities in the US and UK were cut off from accessing patient's health records, lead to ambulances being diverted and patient care was delayed. The cyberattack not just wiped-out IT systems, however still disabled the phone systems, and this cyberattack cost a total of 67 million dollars. In addition, in September 2020, one of the victims of the cyberattacks was the Dusseldorf University Hospital, Germany, which was compelled to refuse patients seeking treatment in the emergency room. As a result of delay in receiving treatment, a patient with a endanger life condition died after being transferred to a facility an hour away from the hospital [17]. Since cyberattacks on healthcare sector are still on the rise, appropriate solution needs to be implemented to avoid a gradual increase in cyberattacks. Approximately 83% of the devices used in healthcare sector nowadays run an obsolete and insecure operating system, with the majority of 56% running Windows 7 while the rest 27% including Windows XP or earlier and unsupported Linux version [7]. In contrast, only 11% of operating systems currently run Windows 10, while with the remaining 6% run between Linux and Windows 8. As a result, most systems which are running medical devices are vulnerable to hacking. [7], noted that the end of Windows 7 support as well as the absence of promptly upgrades comes at a time when the amount of stolen medical records is significantly increasing year after year. Thus, this study aims to provide implement Blockchain Technology to the healthcare industry in Malaysia to enhance the cybersecurity of the healthcare system, thereby reducing the number of cyber-attacks in the healthcare sector.

This proposal will consist of several sections: section 2 includes the background to the research topic, reviewing research papers conducted by other industry experts, which will be utilized as the foundation of the project. Section 3, the problem statement, which will further shed a light on, and with section 4 outlining the purpose and objectives of this study. Additionally, in section 5, we will examine what influence and improvement can be brought to the healthcare sector using the findings of this proposal. Section 6, we will talk through the proposed methodology for providing data to this research, and finally, there will be an overview of the proposed system.

2. Research Background / Literature Review

2.1 Blockchain Technology

Blockchain is a distributed public ledger database maintained by a network of authenticated participants or nodes as well as holds unchangeable blocks of data which may be exchanged securely without interposition of a third party. Data is maintained and stored through cryptography signatures as well as consensus algorithms, which are enacted as key enablers of its application. This data preservation capability is a key driver for the use of blockchain in healthcare [15], where large amounts of data are to be exchanged and distributed widely [16]. In

accordance with [28], blockchain can be classified into four structures, which is public, private (or managed), consortium and hybrid. Moreover, blockchain is safeguarded by "proof of work" scheme dictating that this hash should satisfy several difficult-to-attain properties, namely with a specified numeral of leading zeros, a numeral that might raise or reduce relying on how rapidly blocks are constructed [20]. To attain this, participants add on a nonce, which is simply a random number, to the block and attempt to discover the right hash by altering the nonce between attempts to construct a block with a hash that satisfies "proof of work" requirements [4]. Once such a block is generated, it might be sent to the network, which then accepts the block, adds on to the chain of blocks, and then begins producing new blocks of data. As stated by [24] and [4], mining is the procedure of packing data into blocks and executing "proof of work", each block includes a reference to the prior's block hash. Therefore, if there are any modifications in a prior block, the modification will concatenation via the blocks list, giving them brand new and erroneous hashes. As summary, healthcare sector is an ideal candidate for blockchain technology as it can address key problems such as automated claim validation as well as public health management [19]. It allows patients to own data as well as determine who to share it [8], thus addressing current concerns about data ownership and sharing. Simultaneously, it enables relevant institutions to unify, update, securely interchanged, as well as access data records in a seasonable manner using consensus protocols [2]. This is a crucial benefit of blockchain technology for healthcare applications, as current existing practices necessitate data to be stored with a third party [10]. Eventually, it has the potential to bring transparency to the data management processes meanwhile decreasing the likelihood of improper handling or misuse data by hackers. In addition, several researchers also pointed out that one of the key challenges of Blockchain technology is scalability, as stated in [29] and [3] and there are several researches that find the best scaling solutions for blockchain and classify them by level. As researchers concur the validity of utilizing blockchain technology in the cybersecurity sector, it is only fitting that experts apply blockchain technology in the new and current industries worldwide. As Healthcare systems grow more vulnerable to attack in the recent years, experts agree that this technology can and should be applied in the current Healthcare systems to upgrade and sustain security. Upon reflection, best practice is forfeiting electronic health records with a public setting to allow contributes to append and amend on health records.

2.2 **Current Healthcare System**

Healthcare system, in the context of this paragraph, refers to the institutions, people, and resources involved in providing health care to individuals. Current healthcare is being governed by private and public companies, which employ a medium standard of security for the systems deployed in their hospitals and clinics. In the recent years as Covid-19 struck, the healthcare systems worldwide were struck with an overwhelming wave of patients requiring care and treatment, and with the overwhelming requests and demand, some more violent patients resorted to attacking the hospitals to acquire the care they need in malicious ways [12]. These recent attacks made it clear to hospital officials how vulnerable their systems really are [14]. Additionally, to make the process of storing and keeping patient files easier, recent healthcare systems transformed their patient files into digital and converted them to e-files, stored electronically on clouds, online storage, and computer desktops. In the meanwhile, more attacks occur on the current healthcare systems due to the sensitivity of personnel and patient files. This only makes it more dire of a situation that deems an upgrade of the healthcare systems security more necessary.

2.3 **Similar System**

Tangle is the Direct Acyclic Graph Tangle (DAG) consensus algorithm used by Internet of Things Application (IOTA). To send an IOTA transaction, two preceding transactions received must be validated. As more are added to Tangle, the two-for-one, pay-it-forward consensus reinforces the validity of transactions. Since consensus is established by transactions, if somebody can generate one-third from the transactions, they could persuade the remainder of the network that an ineffective transaction is effective [9]. Up till there's sufficient transaction volume which creating one-third from the volume becomes impossible, IOTA sort of like "double-checks" all network transactions on a central node named "the coordinator". Based on IOTA, "the coordinator" works as a training wheel for the system and would be detached once Tangle is large enough [22].

In accordance with [6], Tangle has greater scalability and fluidity, it scalable data unit let the technology to transfer training bits of data as well as process micro-transactions. Hence in this technology, transactions are processed remarkably fast. However, the main drawback of this technology is that it still developing and testing, thus it is less undependable [21].

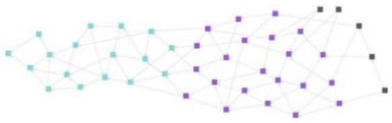

Figure 1: Tangle [21]

Source: ***https://sci-hub.st/10.1109/ICOSST.2018.8632193***

Hashgraph is a consensus approach which provides dissimilar approach to distributed ledger technology. It uses alike information sharing and detection techniques: one of the network participants is required to share all its transaction information with numerous other random selection network nodes [1]. In addition, the following node would be merging the incoming information along with information received from other participants, and any whichever information regarding new transactions will be added. This collection of aggregated information would then be transmitted on to the upcoming randomly chosen node up till all participants are aware of the information produced at the start [25]. However, not just the transaction information itself, but also a timestamp is passed on, as well as information regarding the prior recipients of the information is shared.

In accordance with [25], Hashgraph has only been used in private settings, as a private distributed ledger. If Hashgraph used in a public setting, it might encounter alike challenges as other public distributed ledger systems, mainly in terms of security and manifestation. More crucially, it is a patented technology but not an open source. Therefore, there are still numerous details regarding remain unknown to the crypto developer community, and a decisive verdict on its dependability is unlikely.

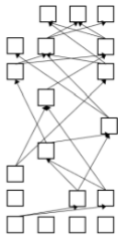

Figure 2.0: Hashgraph [25]

Source:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144241

The table below shows comparison between systems:

Criteria	**Tangle**	**Hashgraph**	**Proposed system**
Architecture	DAG	DAG	Linked List blocks
Applications	Iota	Swirlds	Bitcoin
Copyright	Open source	Patented	Open source
Maturity	Experimental	Experimental	Many implementations
Security	Low	High	High

Table above shows key differences between the proposed system, Tangle and Hashgraph. The architecture used in Tangle and Hashgraph is the same, namely directed acyclic graph (DAG), while the proposed system used linked list blocks. The reason Blockchain is used is because it offers a single transaction layer where healthcare workers can submit as well as share data in a secure manner, through storing a concrete set of standardized data on the chain, along private encrypted links to respectively stored information, for instance; radiographic. Other than that, under applications criteria Tangle uses IOTA, while Hashgraph uses Swirdls and the proposed system uses Bitcoin. According to [1], one of the limitations of IOTA is synchronization problems, while Hashgraph and the proposed system does not have such problems. It is essential to have updated electronic health record in healthcare sector, as this ensures the most accurate representation of health record when is needed. Without regular synchronization, this can bring outdated information when they need it most, and in a healthcare sector, the latest health records can be a life-or-death situation. Unfortunately, healthcare workers don't always have time to update every piece of information in person during their shift hours.

The copyright of Hashgraph is patented compared to Tangle and proposed system which is open source. Since Hashgraph are based on a patented algorithm owned by Swirlds, any new Hashgraph initiative will depend on Swirlds. Moreover, compared to Tangle and Hashgraph, which are still experimental, the maturity of the proposed system is many implementations, therefore, it will be much more reliable. Last but not least, Hashgraph and the proposed system have higher security compared to Tangle. This is because Hashgraph has been shown to be fully asynchronous Byzantine Fault Tolerance (aBFT), which is the gold criterion for distributed systems security, and for the proposed

system, the data cannot be altered or tampered with unless both sides who produced the transaction block.

3. **Problem Statement**

Healthcare organizations are among the most vulnerable to cyber-attacks during the Covid-19 pandemic, with a fivefold rise in cyber-attacks during the pandemic [26]. Since 2016, healthcare organizations have been the target of more cybersecurity assaults than the financial industry, according to [27]. One possible explanation for the increase in cyber-attacks is that the health sector has shifted its focus from systems and practices to their core job of conveying healthcare in arrange to save lives, and attackers are exploiting the COVID-19 pandemic to launch a series of cyberattacks against healthcare organizations [11]. However, attackers could take advantage of anything they can get their hands on e.g., patients electronic health record. In more regrettable case scenarios, ruthless and unethical attackers target healthcare segment to misuse medical resources and restrict access to key care systems, potentially resulting in deaths [13]. As the healthcare industry falls well behind others in terms of cybersecurity. Implementing Blockchain Technology would improve health information security by safeguarding patient data across decentralized peer-to-peer networks and setting the patient at the heart of the system. Due to the Covid-19 epidemic, it is critical to implement the latest cybersecurity technology before it has major consequences on patient wellbeing.

4. **Aim and Objectives**

4.1 **Aim**

The main aim of this research is to implement Blockchain Technology to the healthcare industry in Malaysia to enhance the cybersecurity of the healthcare system, thereby reducing the number of cyber-attacks in the healthcare sector.

4.2 **Objectives**

- To provide an interoperable electronic health record using a secure system and,
- To secure medical supplies and trace the path of pharmaceutical supplies in complete transparency.

5. **Significant of The Research**

The healthcare system has never been more necessary today, mostly since the onset of the 2020 Coronavirus (Covid-19) pandemic. Cyberattacks against the healthcare sector have also surged significantly, putting frontline healthcare workers under constant pressure and demands on their jobs. By deploying this technology, frontline healthcare workers can focus entirely on saving the lives of their patients without concerning about the security of health information as blockchain technology securely encrypt patient data such as medical records. Thus, this can significantly reduce the likelihood of attackers launching a series of cyberattacks and exploiting medical resources during a global disease outbreak.

6. **Methodology**

The research method for the data collection of this research is mainly survey and reviewing case studies. The survey will be carried out to gather quantitative data, which permits respondents to provide more precise and unambiguous answers than qualitative data, which may limit their capability to communicate their answer more precisely. Respondents would also be less perplexed about how to answer the questions. The population surveyed will be at several hospitals in Kuala Lumpur, Malaysia and involve a total amount of 100 respondents. Alternative data collection methods such as interviews would be difficult to obtain due to the large number of respondents involved, due to their irregular working hours and busy schedules of healthcare workers. Therefore, a convenient and quick method is considered necessary. Respondents are selected by applying complex probability stratified sampling method, which means that data will be collected by dividing all the healthcare workers into subgroups by department, which is coronary care unit, nursing administration, and medical records department, and the individuals from these subgroups were randomly selected to form a sample. This sampling method was chosen to lessen the possibility of human bias in the selection of cases to be comprised in the sample [23]. Thus, it is easier for researchers to conduct research, as subgroups are well-defined and non-overlapping. The data gathered from these samples should help us visualize the cybersecurity concerns of most healthcare workers, since no healthcare sector can remain invincible from a cyberattack.

6.1 **Survey**

The survey is to be conducted using online survey tools such as Microsoft Form, Google Form, SurveyMonkey, and the targeted respondents are those who work in

industries that are vulnerable to cyberattacks, such as doctors and nurses. These individuals were chosen as respondents as they are the prospective victims of cyberattacks. Therefore, the questions primarily concern how comfortable respondents are with this type of technology, what actions respondents would take to prevent a cyberattack from occurring, initial security assessment and such.

To analyze and interpret the data collection, diversified techniques could be utilized. Once all the data has been collected, it is time to interpret it. This could be done using statistical analysis, and various software packages can be utilized to perform statistical analysis to accelerate the process. One such software is SPSS, a software that can be used to produce tabular report, charts, graphs of distributions and trends, descriptive statistics like mode, mean, median, frequency, and more intricate statistical analyses like regression models [5]. In addition, statistics assists us in converting quantitative data into helpful information to aid in making decision, and it can be utilized to sum up data, describe patterns, relationships, as well as connections. Therefore, statistics could be either inferable or descriptive. Descriptive statistic aid with data summarization, however inferable statistic significantly differs between groups of data [18].

7. **Overview of The Proposed System**

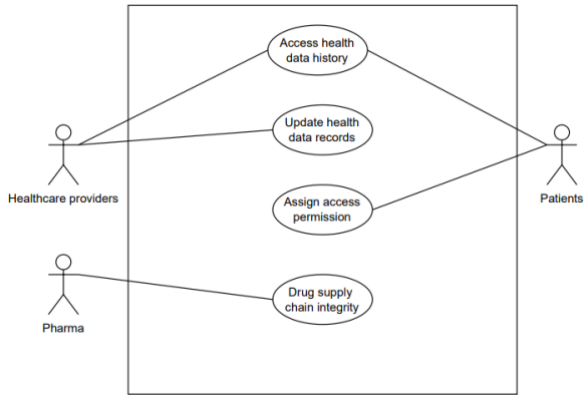

Figure 3.0: Use Case Diagram for roles in Blockchain

Figure 3.0 shows the use case diagram with various roles of participants and their interactions. The roles in the use case diagram are:

1. **Patients**
   This user can control over who has access to their data, thereby reducing the likelihood of data theft. It also guarantees better diagnosis of diseases and provides them with information about their healthcare history.

2. **Healthcare providers**
   This user will be able to access to their patients' health data history and update their health records. Since, Blockchain can allow healthcare providers real-time visibility into the patient's longitudinal record, allowing them to make optimal decisions as well as permitting every participant to integrate the systems without worrying regarding privacy and security concerns.

3. **Pharma**
   This user can access drug supply chain, as this is the relevant section for the user.
   Blockchain technology protects the integrity of the data as this is a key part of supplying patients with their medication. Protecting the integrity of this data is key to the integrity of the whole patient handling process. To enforce the rule of least privilege, pharma has access only to this data to complete their duties and no more information that required.

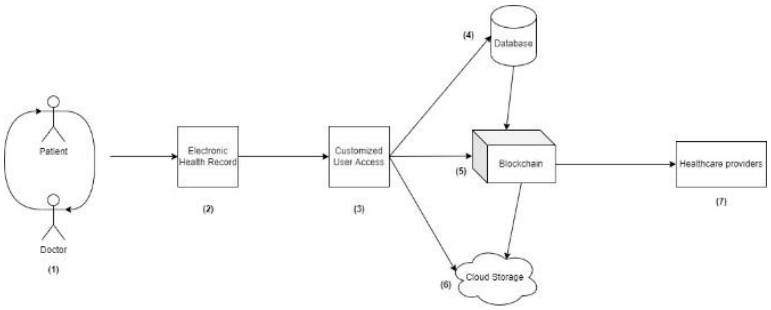

Figure 4.0: Process of healthcare data management in Blockchain

Figure 4.0 depicts the process of healthcare data management in blockchain in 7 steps. In step one, main data is produced with the interplay between a patient and the doctor. This data comprises medical history, present issue, as well as other physiological data. Moving on to step two, an electronic health record (EHR) is created for every patient utilizing the main data gathered in step 1. In addition, other medical details such as those generated from nursing care, medical imaging, as well as medication history are also comprised inside electronic health record. Moreover, in step three, a particular patient who owns the ownership of sensitive electronic health record, as well as customized access control is specified only for the proprietor of the property. Anyone who wish to access such privacy data will have to seek for permission which is forwarded to the electronic health record proprietor, and the

proprietor then determine to whose access will be allowed. In the fourth, fifth and sixth steps, these 3 processes are the heart of the entire process comprising database, blockchain, as well as cloud storage. The database as well as cloud storage store the data in a decentralized way, and blockchain provides high secrecy to guarantee customized genuine user access. Ultimately, in the seventh step, healthcare providers such as hospitals are the end user who seek to obtain access for a secure care delivery that would be authorized by the proprietor. For instance, regardless of where patients are received treatment around the world, patients' health record would be usable and accessible on their mobile phone, as well as verified through distributed ledger like blockchain, which healthcare providers will proceed to add on as time passes.

8. **Conclusion**

In this proposal, we examined how the proposed system theoretically secures the healthcare system, with hacking would be finite by the requirement to attack every user one by one to gain sensitive data. As a result, proposed system can offer an unchangeable audit trail of health data. Future works include enhancing the technology by building secure smart contracts like altering traditional healthcare sectors as well as their business process by automating contractual terms of protocol in an automation way. Additionally, merging blockchain and artificial intelligence (AI) could enhance fuel efficiency in healthcare data analytics. Ultimately, future work should also be considered to improve the scalability of blockchains.

References

[1] Akhtar, Z. (2019). From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild. *IEEE*. https://sci-hub.st/10.1109/UPCON47278.2019.8980029

[2] Alla, S., Soltanisehat, L., Tatar, U., Keskin, O. (2018). Blockchain technology in electronic healthcare systems. *IISE Annual Conf. Expo* 2018 (1), 754–759. https://sci-hub.st/10.1016/j.compind.2020.103290

[3] Andoni, M., Robu. V., Flynn, D., Abram. S., Geach. D., Jenkins. D., McCallum. P. & Peacock. A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Elsevier Ltd*, 100, 143-174. https://www.sciencedirect.com/science/article/pii/S1364032118307184

[4] Adiputra, C.K., Hjort, R. & Sato. H. (2018). A Proposal of Blockchain-based Electronic Voting System. *IEEE. Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4).* https://sci-hub.st/10.1109/WorldS4.2018.8611593

[5] Crossman, A. (2019). *A Review of Software Tools for Quantitative Data Analysis.* ThoughtCo. https://www.thoughtco.com/quantitative-analysis-software-review-3026539#:~:text=SPSS%20is%20the%20most%20popular,any%20type%20of%20data%20file.

[6] Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z. & Peng, M. (2019). When Internet of Things Meets Blockchain: Challenges in Distributed Consensus. *IEEE*. https://sci-hub.st/10.1109/MNET.2019.1900002 -of-healthcare-systems-run-outdated-software

[7] Cohen, J. (2020). *While US Fights COVID-19, 83 Percent of Healthcare Systems Run Outdated Software.* PC. https://sea.pcmag.com/mobile-operating-system/36589/while-us-fights-covid-19-83-percent

[8] Dimitrov, D.V. (2019). Blockchain applications for healthcare data management. *Healthc. Inform.* Res. 25 (1), 51–56. https://e-hir.org/journal/view.php?id=10.4258/hir.2019.25.1.51

[9] Gitbook. (n.d.). *Direct Acyclic Graph Tangle (DAG).* GitBook. https://tokens-economy.gitbook.io/consensus/chain-based-dag/direct-acyclic-graph-tangle-dag#:~:text=Tangle%20is%20the%20DAG%20consensus,previous%20transactions%20you're%20received.&text=This%20is%20directed%2C%20asynchronous%20graph,DAG)%20representing%20each%20individual%20transaction.

[10] Hölbl, M., Kompara, M., Kamisali ˇ c, ´ A., Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry* 10 (10), 470. https://www.mdpi.com/2073-8994/10/10/470

[11] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of medical Internet research*, *23*(4), e21747. https://doi.org/10.2196/21747

[12] Hira, F.A., Khalid, H., Abdul Rasid. S.Z., & Alam, M.M. (2021). A Conceptual Framework to Investigate Health Professionals' Blockchain Technology Adoption Readiness in Malaysia. *Open InternationalJournal ofInformatics(OIJI)*, 9(2). https://www.researchgate.net/profile/Fariha-Hira/publication/357016875_A_Conceptual_Framework_to_Investigate_Health_Professionals'_Blockchain_Technology_Adoption_Readiness_in_Malaysia/links/61b861a9a6251b553ab8963a/A-Conceptual-Framework-to-Investigate-Health-Professionals-Blockchain-Technology-Adoption-Readiness-in-Malaysia.pdf

[13] Jayakumar, P., Brohi. S.N. & Zaman, N. (2020). Top 7 Lessons Learned from Covid-19 Pandemic. *ResearchGate.* https://www.researchgate.net/publication/341254687_Top_7_Lessons_Learned_from_COVID-19_Pandemic

[14] Ismail, H., & Hanafiah, M.M. (2019). Discovering opportunities to meet the challenges of an effective waste electrical and electronic equipment recycling system in Malaysia. *ELSEVIER*, 238. https://www.sciencedirect.com/science/article/abs/pii/S0959652619327970

[15] Kuo, T.T., Gabriel, R.A., Ohno-Machado, L. (2019). Fair compute loads enabled by blockchain: sharing models by alternating client and server roles. *J. Am. Med. Inform. Assoc*, 26 (5), 392–403. http://refhub.elsevier.com/S0166-3615(20)30524-8/sbref0215

[16] Meinert, E., Alturkistani, A., Foley, K.A., Osama, T., Car, J., Majeed, A., Van Velthoven, M., Wells, G., Brindley, D. (2019). Blockchain implementation in health care: protocol for a systematic review. *JMIR Res. Protoc*, 8 (2), e10994. https://www.researchprotocols.org/2019/2/e10994/

[17] Mydin, H.J. (2022). *Future-proofing Malaysia's healthcare system*. TheStar.

https://www.thestar.com.my/lifestyle/health/health-matters/2022/02/05/future-proofing-malaysia039s-healthcare-system

[18] McLeod, S. (2019). *What's the difference between qualitative and quantitative research?* SimplyPsychology. https://www.simplypsychology.org/qualitative-quantitative.html

[19] Mettler, M. (2016). Blockchain technology in healthcare: the revolution starts here. *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1-3. https://ieeexplore.ieee.org/document/7749510

[20] Nakamoto, S. (2008). *A peer-to-peer electronic cash system.* https://bitcoin.org/bitcoin.pdf.Adiputra

[21] Pervez, H., Muneeb, M., Irfan, M.U. & Haq, U. (2018). A Comparative Analysis of DAG-based Blockchain Architectures. *IEEE*. https://sci-hub.st/10.1109/ICOSST.2018.8632193

[22] Ryan, J. (2019). *Blockchain Vs Tangle: Which Is Better?* DZone. https://dzone.com/articles/blockchain-vs-tangle-which-is-better

[23] Sharma, G. (2017). Pros and Cons of different sampling techniques. *International Journal of Applied Research 2017; 3(7): 749-752*. https://d1wqtxts1xzle7.cloudfront.net/58765080/Pros_and_cons_of_sampling-with-cover-page-v2.pdf?Expires=1644587798&Signature=dt11wgU65M0Umfql~EJ2oJkuPgWYxazZ5uhNFzMm~V-YIhqEHr01mlER6jxOn87Fj2EFfCT7VnO6-mqxasYcPQAAl3O2Bl2~W4S1usjv4MMt8iZnJfWS-SSQLyT7a-3PoZxRXSkY-aLftn9NbtOwC0wukeKE9L9Paa8K5j87qRWHn1iWtL9Ogu~2JKR5ug6vB2-s8SeMUyithcWWLd6ieY3ISdWmNDBqkL2kexyW49nB~ThmfjIh-Ju0i~ngZX4nk8pKemzq~ebUkqtxN4-gOf56ZV7GPJzBnUR83oHVN1xYC~j5jLzvrMPExieRRyW8DJoDSN0S9YVxKqHywOk-UQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[24] Sriman B., Ganesh Kumar S. & Shamili P. (2021). Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake. *Intelligent Computing and Applications. Advances in Intelligent Systems and Computing*, vol 1172. https://doi.org/10.1007/978-981-15-5566-4_34

[25] Schueffel, P. (2017). Alternative Distributed Ledger Technologies: Blockchain vs. Tangle vs. Hashgraph - A high-level overview and comparison -. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3144241

[26] World Health Organization. (2020). *WHO reports fivefold increase in cyber-attacks, urges vigilance.* WHO. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[27] Williams, L., Gallant, A., Rasmussen, S., Brown Nicholls, L.A., Cogan, N., Deakin, K., Young, D. & Flowers, P. (2020). *The British Psychological Society*, 25(4), 1039-1054. https://bpspsychub.onlinelibrary.wiley.com/doi/full/10.1111/bjhp.12468

[28] Wegrzyn. K., & Wang, E. (2021). *Types of Blockchain: Public, Private, or Something in Between.* Foley. https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

[29] Zheng, X., Sun, S., Mukkamala, R.R., Vatrapu, R., Ordieres-Meré, J. (2019). Accelerating health data sharing: a solution based on the internet of things and distributed ledger technologies. *J. med. Internet res*, 21 (6), e13583. https://www.jmir.org/2019/6/e13583/