Adapting Blockchain for Secure and Efficient Identity Management in Oman's e-Government

Asma Hamed salem AlBadi[1], Aisha Salim Rashid AlShibli[2], Dhiya Hamed Ali AlSaqri[3] Arwa Khalfan AlSariri[4]

[1]Assistant Lecturer, University of Technology and Applied Sciences Suhar
asma.albadi@utas.edu.om
[2]Lecturer, University of Technology and Applied Sciences Suhar aisha.alshibli@utas.edu.om
[3]Assistant Lecturer, University of Technology and Applied Sciences Suhar
dhiya.alsaqri@utas.edu.om
[4] Assistant Lecturer, University of Technology and Applied Sciences Suhar
Arwa.alsariri@utas.edu.om

Abstract: This research paper examines the potential application of blockchain technology in e-government identity management, with a specific focus on the case of Oman. Traditional centralized identity systems in e-government face various challenges, such as security vulnerabilities and limited compatibility among government agencies. By utilizing the decentralized and unalterable characteristics of blockchain, Oman can enhance the security, privacy, efficiency, and transparency of identity management in e-government. The advantages include improved security and privacy, streamlined processes, data sharing and interoperability, transparency, cost reduction, and empowerment of citizens. The paper presents examples of blockchain-based identity management systems implemented in different sectors and countries, along with research studies in the field. Additionally, a survey was conducted to assess awareness and willingness to adopt blockchain-based identity management in Oman's e-government. The findings emphasize the importance of considering technical requirements, legal frameworks, interoperability standards, and user acceptance for successful implementation. Overall, blockchain technology offers promising solutions to strengthen identity management in e-government and establish a trustworthy digital environment for citizens and businesses.

Keywords: Blockchain, identity management, e-government

1. INTRODUCTION

Blockchain technology is one of the modern technologies that are being applied in all aspects of life in countries, whether it is health or administrative aspects. Currently, countries are striving to study the possibility of applying blockchain not just in the security system-based of countries, but to be applied as advanced technology that enhances the overall security mechanism , such as using it as identity authentication. In general, researchers began studying in this field in the year 2008 on Stuart Haber's previous work to be at the beginning as a notebook for Bitcoin crypto-currency transactions. When it comes to an innovative technology to develop reality, whether it is in the information security sector or in the programming sector or other sectors, many studies often appear that base their study on a newly discovered technology or a technology developed from another technology discovered a long time ago or through the integration of more than one technology with each other in order to study the ability of this technology to work effectively under various circumstances, including different environments and the different main objective behind applying the application.

The previous research history about the blockchain technology has been summarized in the following table.

Table 1. history about the blockchain technology

Researcher's Name	Year of conducted study	Range of the study	Results
Miau and Yang [1]	2018	Research papers and articles from 2008 to 2017.	Found that 801 articles categorized to 3 stages of blockchain study: • 2008-2013, the study was about the Bitcoin and crypto currencies. • 2014-2015 rapid growth in the number of studies on Bitcoin theory. • Since 2016 till many researchers have studied blockchain with smart contracts.
Yli-Huumo, et.al [2]	2016	41 research paper	Found that the research papers focus on verity of aspects, which shown in the following points: • Bitcoin system with 60% out of 80%. • blockchain applications + Bitcoin system with 20% out of 80% • The proposed solution on improving and enhancing the limitation of using the blockchain technology -for security and privacy perspectives- lacked from concrete and accurate evaluation.
da Silva Momo, et.al [3]	2019	Research papers from an international database called Crunchbase	Inside the Crunchbase, a repository with 100 thousand records was created to save models of different companies from over the world that built their models based on blockchain technology. The results showed that 801 companies created the models for different perspectives in business, agriculture, and education, such as: • Cryptocurrencies purchase and sale. • Services and applications for promotion, future and smart contracts, credit and financial services, food tracking, and transporting. • Run courses that use blockchain. • Application in health care. For example, tests, checking diabetes, and the science of life.

In terms of the business sector, different firms that used this technology were examined in order to evaluate and survey the usage of blockchain in this direction as well as get out the percentage of these evaluations. The chart below shows the technology used in financial and technology sectors in 6 firms each. Furthermore, it is used in health care, retailing and transportation sectors in 2 firms each as well. Beside, 1 firm used it in motor vehicles, telecommunications, and beverage tobacco and food sectors [4]

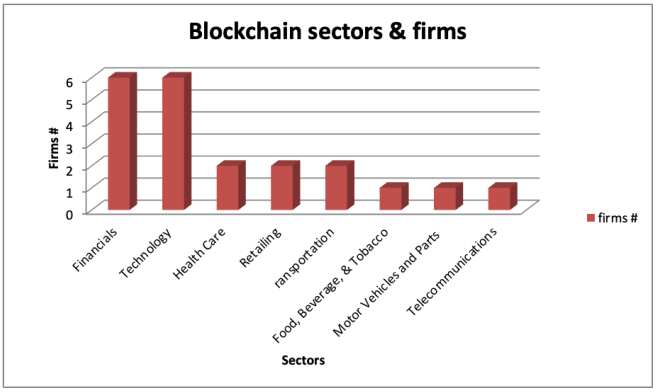

Fig. 1. Blockchain sectors and firms

Case, C. J., King, D. L., & Case, J. A. (2020), further categorized the firms that used blockchain technology based on the industry. The below chart illustrates blockchain firms by industry, which are 5 firms in banking, 2 in software, and 2 in mail, package, and freight delivery. Also, there are some firms in different industries that vary from PCs to telecommunications [4].

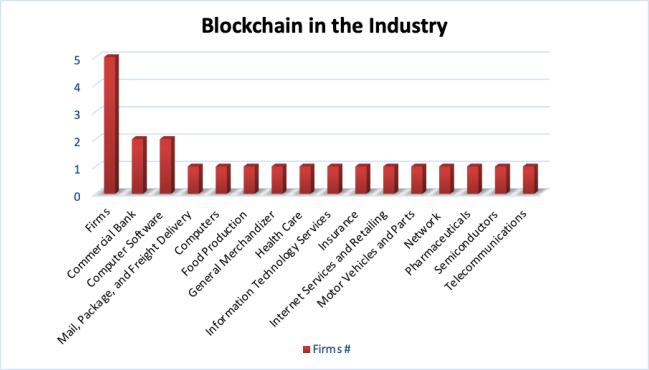

Fig. 2. Blockchain in the industry

All studies have shown the development & evolution of the blockchain from Bitcoin to a high-quality and diverse technology used at all levels. Work in this field is still ongoing and other uses are being discovered, all of which are in the interest of governments, institutions, and companies that use them in a variety of ways. In this paper, we examine the ability to use blockchain technology as identity authentication, where work in this field has already begun to be implemented in many countries. The literature summarizes some of the research that was done based on using blockchain technology as identity authentication with an explanation of the purpose of using it.

2. Literature Review and Analysis of Related Work

J.S. Hammudoglu and his team created a new mobile authentication system based entirely on local processing. They developed an open source solution on Android to scout the ability of smartphones to obtain, operate and recognize fingerprints using compact hardware only. The architecture that they developed is completely standalone design, which does not require any connection to the cloud or server or any further permission to login to the hardware reader using fingerprint. The architecture consists of three levels. First, acquiring a fingerprint by using the camera of the smartphone. Second, process the pipeline to gain accurate features. Third, match the features of the fingerprint with other fingerprints that are stored locally. The results show that the accuracy of all fingerprints were matched with 55% overall and 67% of accuracy matching thumb fingerprints. In short, the system provides identity -self-sovereign- solution and consolidates un-permission Blockchain key attestation and identification [5].

Gilda, S. proposed an identity system based on a blockchain idea for user's authorization and authentication using two policies, which are access control based on the attribute and privacy preserving policy. Lastly, the control will return back to the user based on the user's identity. The technology is using a special blockchain that is going to keep track of all the data about users and store them in a private manner such as data and events access and user's authorization request. By this way, the user's data will surely have integrity. Therefore, the mechanism is very useful in terms of checking the identity of users, which will facilitate the work and make it done in a fast and proper way. Such a mechanism might be used in electricity bills, passports and driving licenses. Cryptographic method is used to provide privacy to user's data as well as transaction's auditability. In short, the mechanism is working well with 72.3% of accuracy [6]. Chang Soo Sung and Joo Yeon Park, studied and adapted identity management system based on blockchain technology to be used in general sector. Through studying and understanding the circumstances and the benefits of using it in general services by reviewing research papers and trying to find out the design and architecture of their systems in order to be implemented in the Korean environment. They found that the identity management systems based on Blockchain improve and enhance user's data control in terms of reliability, accountability and transparency as well as reducing the cost and the time during delivering the services to the public, which shall increase the efficiency of the system. With a view to implement such a system in the government sector, difficulties must be resolved first, such as in a realistic process, which is really time consuming. [7]

Blockchain-based, Radio Frequency Identification (RFID) for protocol's transfer was proposed as a tag ownership by Yong Gana, Yuan Zhuangb and Lei He. The technologies were used in implementing RFID for different purposes. The first one was applying a hash function to make a guarantee that all messages are safe. The second technology was using the blockchain to double the security on the messages without any participation of third

parties such as TTP because the used blockchain is decentralized. A pseudonym confirms the identity of tags and it's not published to the reader or any untrusted existence. As a final step, GNY logic was analyzed. In short, RFID ensures the privacy of the identity messages tags forward and backward [8].

Smart city system based on blockchain mechanism had fulfilled by Carmen ROTUNĂ and her team. Their idea is to analyze how the blockchain will act based on a given service in order to contribute to developing an infrastructure of smart cities, which will be the backbone to implement the model of smart city ecosystem based on self-identity that is used as an authentication system in transportation. Moreover, it summarized the fields where this technology can be used, which is illustrated in Figure 1. The result showed that blockchain is a sufficient technology for performing high security mechanisms in transportation and communication systems of any developing city, which improve the performance and the quality of the smart city's applications [9].

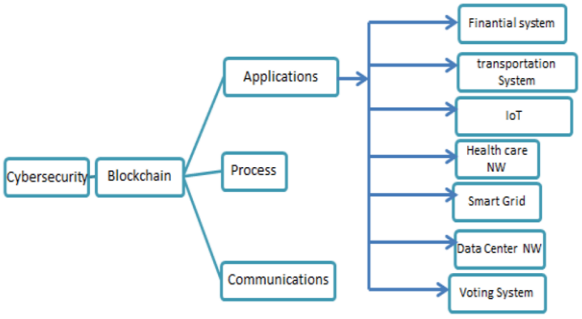

Fig. 3. Blockchain technology fields

Fatemeh Mohammadipanah and Hedieh Sajedi proposed a potential approach for securing and developing microbial databases based on the blockchain concepts. The contribution of the blockchain concepts in developing microbial databases are mentioned in Figure 2. This approach used the consensus algorithm as an essential layer of the proposed system, which was performed using Proof of Work (PoW). This technique calculates the value of a block with the number of zeros based on updating the random number. In short, the blockchain concepts helped to develop the database [10].

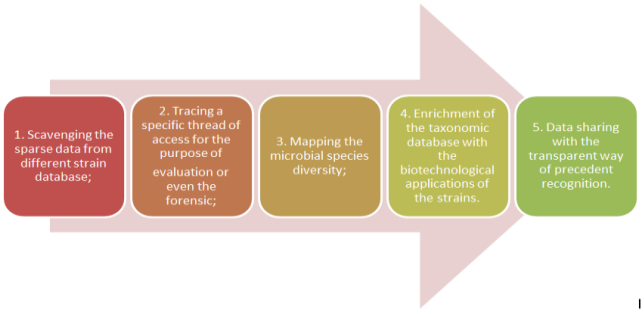

Fig. 4. The contribution of the blockchain concepts in developing microbial databases

Finally, Some countries that used blockchain as identity authentication are summarized in the following table. They are just examples and not exhaustive.

Table 2. List of countries that used blockchain

Country	Year	Subject
Estonia	2017	The Digital Republic Secured by Blockchain [11]
Turkey	2019 - 2020	• Towards a Blockchain-based digital identity verification, record attestation and record sharing system [12] • Blockchain-based electronic voting system for elections in Turkey [13] • A blockchain based land registration system proposal for Turkey [14]
Thailand	2017-2022	• Blockchain Ecosystem to Raise Thailand's Telecommunication Sector to a Smart Society According to Thailand 4.0 Policy [14] • How Blockchain and smart contracts impact business in Thailand [15] • A practical national digital ID framework on the blockchain (NIDBC) [16]

3. E-Government and Identity Management in Oman

Currently, identity management in Oman's e-Government relies on centralized systems, which can be vulnerable to security breaches and lack interoperability. To overcome these challenges, innovative solutions are needed to improve identity management and enhance the e-Government experience.

Blockchain technology offers a promising solution. By utilizing the decentralized and immutable nature of blockchain, Oman can enhance the security, privacy, efficiency, and transparency of identity management. With blockchain-based identity management, identity records can be securely stored and shared, verification processes can be streamlined, and trust and accountability can be enhanced. However, implementing blockchain-based identity management requires careful consideration of technical requirements, legal frameworks, interoperability standards, and user acceptance. By leveraging blockchain technology, Oman can improve its e-Government services, protect citizen data, and create a more efficient and trustworthy digital environment.

4. Potential benefits and advantages for Oman's e-government

Blockchain technology offers numerous benefits for e-government identity management in Oman:

1. Enhanced Security: The decentralized and unalterable nature of blockchain ensures the security and integrity of identity information, reducing the risk of fraud or data breaches.
2. Improved Privacy: Blockchain-based identity management empowers individuals to control the sharing of their personal data, enhancing privacy and minimizing unnecessary information collection.
3. Efficient Processes: Automation enabled by blockchain streamlines identity verification, authentication, and document validation, leading to faster and more efficient e-government services.
4. Interoperability and Data Sharing: Blockchain facilitates secure data sharing among government agencies, promoting seamless integration and reducing administrative redundancies.
5. Transparency and Accountability: The transparent nature of blockchain enhances accountability and trust by providing an auditable trail of identity management activities.
6. Reduced Costs: By eliminating intermediaries and manual verification processes, blockchain-based systems can lower operational expenses and mitigate identity fraud-related costs.
7. Empowering Citizens: Blockchain-based identity management empowers individuals to manage their digital identities autonomously, resulting in increased convenience, trust, and autonomy when accessing e-government services.

5. Research Methods

A study was conducted to investigate how blockchain technology can be adapted to apply to identity management in the e-government of Oman. The research design employed for this study was a quantitative approach using a survey questionnaire to collect data from the target population. This section provides an overview of the research design, data collection methods, data analysis techniques, ethical considerations, and limitations of the study.

The primary data collection method utilized was a structured survey questionnaire. The questionnaire was developed based on an extensive review of existing literature and research on identity management and blockchain technology in e-government contexts. The questions were designed to assess participants' awareness, perceptions, and willingness to adapt to blockchain-based identity management in Oman's e-government.

The target population for this study consisted of individuals who have experience with Oman's e-government services. A convenience sampling technique was employed to select participants from various age groups, occupations, and educational backgrounds to ensure diversity in the sample. The survey was distributed electronically using online platforms, and participants were given a defined timeframe to complete the questionnaire.

6. RESULTS AND DISCUSSION

VI.1. Question 1

Data for question one were descriptive through statistics As described in Table3. The respondents' level of education ranged between diploma, Bachelor, Masters and Doctoral. The highest percentage was for Master holders which is 43.43% then 34.34% for Bachelor holders, 11.11% for Diploma holders and 10.10% for Doctoral holders.

Table 3.Respondents' level of education

Answer Choices	Responses
Diploma	11.11%
Bachelor	34.34%
Masters	43.43%
Doctoral	10.10%
Other	1.01%

VI.2. Question 2

In the survey conducted for this research, participants were asked about their specialization, and the majority of respondents indicated backgrounds in computer science with specializations in security, networking, AI, software development, and a smaller portion represented business management. This diverse range of specializations among the participants provides valuable insights into the perspectives of both technical experts and business professionals regarding the adaptation of identity management based on blockchain technology in Oman's e-government.

VI.3. Question 3

In the survey conducted for this research, participants were asked about the organization they belong to, and the responses varied across different public and private sector organizations in Oman.

VI.4. Question 4

Data for question one were descriptive through statistics As described in Table4. The respondents' age ranged between 18 and 64. The highest percentage was for ages between 25-34 which is 37.37% then 33.33%for the range 35-44, 15.15% for the range 18-24, 12.12% for the range 45-54 and 2.02% for the range 55-64 .

Table 4. Respondents' age

Answer Choices	Responses
18-24	15.15%
25-34	37.37%
35-44	33.33%
45-54	12.12%
55-64	2.02%

VI.5. Question 5

The survey results indicate that a significant portion of respondents feel they have control over their confidential information when interacting with online services, with 27.55% strongly agreeing and 48.98% agreeing. However, a considerable number (19.39%) still express disagreement or strong disagreement. Similarly, while there is some agreement (20.20% strongly agree, 48.48% agree) that saving credit card details on business websites eases online transactions, a notable percentage (18.18% disagree, 13.13% strongly disagree) holds a contrary view. The safety of using credit card details on online services is met with mixed opinions, as 37.76% agree, but 48.98% disagree. When it comes to saving passwords on websites, a significant majority (65.65%) expresses disagreement, indicating a preference for entering passwords each time. Sharing passwords and private information with friends is widely discouraged, with 73.74% strongly disagreeing. Overall, there is recognition (weighted average: 2.27) of considering potential consequences when sharing personal information, and a consensus (66.67% strongly agree) on the importance of setting privacy settings.

VI.6. Question 6

In the survey, respondents were asked about the type of authentication they currently utilize. The results indicate that 44% of respondents reported using a centralized authentication system with their own authentication server. 50% of respondents indicated using a single sign-on approach with a trusted third-party authentication provider. A small percentage of respondents (5.21%) provided other responses, indicating the use of alternative authentication methods or preferences for example two-factor authentication. These findings highlight the diverse range of authentication practices currently in use, showcasing the importance of considering various approaches when implementing blockchain-based identity management in Oman's e-government.

VI.7. Question 7

The survey showed that 74.23% of respondents are satisfied with the current authentication system, while 25.77% expressed dissatisfaction. This shows that while the majority of users are happy with the system, a sizable minority are not. Further analysis is needed to understand the reasons behind satisfaction or dissatisfaction and to identify opportunities for improvement or potential adoption of blockchain-based authentication systems based on user preferences.

VI.8. Question 8

According to the survey, a significant majority of 80.81% of the respondents are open to transitioning to a better authentication system, while 19.19% did not express a preference for a change. These results emphasize the strong desire among most participants to adopt an advanced authentication system and benefit from its potential advantages. The findings underscore the significance of exploring alternatives, such as blockchain-based authentication systems, which have the potential to enhance security and provide improved user experiences.

VI.9. Question 9

The survey revealed that a majority of respondents (58.51%) did not experience any technical difficulties. However, a significant percentage faced issues such as authentication system downtime (17.02%), breaches of confidential information (14.89%), unauthorized data fetching (8.51%), and data corruption, modification, or fabrication

(14.89%). A small portion (1.06%) provided other responses. These findings emphasize the importance of addressing technical challenges in authentication systems, including enhancing system reliability, security measures, and data integrity safeguards**.**

VI.10. Question 10

The survey findings indicate that individuals have taken various actions to deal with technical problems. A notable percentage (37.04%) utilized hardware or software controls, while 28.40% implemented new authentication policies. Furthermore, 44.44% reported the issues to higher authorities seeking resolution. These results highlight a proactive attitude towards overcoming challenges, involving the implementation of stricter controls, policy enhancements, and effective communication. These measures aim to tackle technical difficulties and improve the overall effectiveness of authentication systems.

VI.11. Question 11

The survey revealed that slightly over half (52.04%) of the respondents are aware of blockchain-based authentication systems, while 47.96% are not. This indicates a reasonable level of familiarity among the surveyed population. These findings serve as a starting point for further examination and comparison of perceptions and opinions about these authentication systems among those who are aware of them.

VI.12. Question 12

33.33% of respondents believe organizations in Oman are acquainted with blockchain-based authentication systems, while 66.67% believe they are not. These findings indicate that a considerable majority perceive a lack of familiarity among organizations in Oman regarding this technology. This suggests a potential gap in awareness or adoption of blockchain-based authentication systems in the surveyed context, emphasizing the importance of investigating the factors that influence knowledge and adoption of this technology among organizations in Oman.

VI.13. Question 13

This question focused on evaluating the adaptation with blockchain-based authentication systems in oman organizations. The responses provided valuable insights from participants with different backgrounds and ages. A majority of respondents (91.86%) expressed that Oman organizations can adapt with blockchain-based authentication systems. While (8.14%) of respondents did not agree on that.

VI.14. Question 14

One of the survey's aims was to measure the willingness of individuals to shift to blockchain-based authentication systems. 88.24% of respondents showed their interest to shift to such systems. On the other hand, only 11.76% responses did not show their interest.

VI.15. Question 15

The survey aims to improve the authentication process of organizations in Oman through blockchain-based authentication. Participants were asked whether this shifting would enhance the authentication process. 47.06% Agreed upon that while 49.41% were not sure about it.

VI.16. Question 16

The survey participants were asked about their willingness of shifting to touch-less technology, regardless of the price. And surprisingly 84.62% were happy to shift to such technology and only 15.38% of them showed that shifting to touchless technology is undesirable.

VI.17. Question 17

One of the measures that the survey focused on was the confident of participants while using the leap motion device. Table 5 below shows their response to this question:

Based on their responses we clearly can see how confident they were when using leap motion.

VI.18. Question 18

The survey participants were asked about the organization's willingness of shifting to blockchain-based authentication systems , regardless of the cost. And surprisingly 46.34% were happy to shift to such technology and 53.66% of them showed that shifting to blockchain-based authentication systems is undesirable.

VI.19. Question 19

The survey also focused on measuring the effectiveness of blockchain-based authentication systems in overcoming the technical and security issues . 36.14% of responses show how effective blockchain-based authentication is. On the other hand 63.86% of responses showed uncertainty.

7. Conclusion

In this research study, we examined how Oman's e-government can adapt identity management based on blockchain technology. In order to evaluate the potential benefits and challenges of implementing blockchain-based identity management in Oman, an extensive literature review, an analysis of existing case studies, and data collection from a survey questionnaire have been conducted.

Oman's e-government could benefit significantly from blockchain technology, according to the findings of this study. By leveraging blockchain technology, digital identities can be managed more efficiently, effectively, and transparently, improving security, privacy, efficiency, and transparency. Additionally, the results of the survey indicate that participants are ready to embrace technological advancements and are willing to adapt to blockchain-based identity management systems.

8. ACKNOWLEDGMENTS

We would like to express our sincere gratitude to all those who have supported and contributed to this research. Their assistance and valuable input have been crucial in the successful completion of this study.

REFERENCES

[1] Miau, S., & Yang, J. M. (2018). Bibliometrics-based evaluation of the Blockchain research trend: 2008–March 2017. Technology Analysis & Strategic Management, 30(9), 1029-1045.

[2] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

[3] Momo, F. D. S., Schiavi, G. S., Behr, A., & Lucena, P. (2019). Business models and blockchain: What can change?. Revista de Administração Contemporânea, 23, 228-248.

[4] Case, C. J., King, D. L., & Case, J. A. (2020). Blockchain: an empirical review of fortune 500 website postings and usage. Journal of Business and Behavioral Sciences, 32(2), 42-52.

[5] Hammudoglu, J. S., Sparreboom, J., Rauhamaa, J. I., Faber, J. K., Guerchi, L. C., Samiotis, I. P., ... & Pouwelse, J. A. (2017). Portable trust: biometric-based authentication and blockchain storage for self-sovereign identity systems. arXiv preprint arXiv:1706.03744.

[6] Gilda, S., Jain, T., & Dhalla, A. (2023). None Shall Pass: A blockchain-based federated identity management system. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2022 (pp. 329-352). Singapore: Springer Nature Singapore.

[7] Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. Journal of Enterprise Information Management, 34(5), 1481-1505.

[8] Gan, Y., Zhuang, Y., & He, L. (2019). RFID tag ownership transfer protocol using blockchain. International Journal of Performability Engineering, 15(9), 2544.

[9] Rotună, C., GHEORGHIȚĂ, A., Zamfiroiu, A., & SMADA ANAGRAMA, D. (2019). Smart City Ecosystem Using Blockchain Technology. Informatica Economica, 23(4).

[10] Mohammadipanah, F., & Sajedi, H. (2021). Potential of blockchain approach on development and security of microbial databases. Biological Procedures Online, 23(1), 1-8.

[11] Heller, N. (2017). Estonia, the digital republic. The New Yorker, 18.

[12] Aydar, M., Ayvaz, S., & Cetin, S. C. (2019). Towards a Blockchain based digital identity verification, record attestation and record sharing system. arXiv preprint arXiv:1906.09791.

[13] Bulut, R., Kantarcı, A., Keskin, S., & Bahtiyar, Ş. (2019, September). Blockchain-based electronic voting system for elections in Turkey. In 2019 4th International Conference on Computer Science and Engineering (UBMK) (pp. 183-188). IEEE.

[14] Mendi, A. F., Sakaklı, K. K., & Çabuk, A. (2020, October). A blockchain based land registration system proposal for Turkey. In 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-6). IEEE.

[15] Surakratanasakul, B., Kreesuradej, W., Ariya, A., Junsantor, P., & Busaba, B. (2022). Blockchain Ecosystem to Raise Thailand's Telecommunication Sector to a Smart Society According to Thailand 4.0 Policy. NBTC Journal, 6(6), 199-231.

[16] Voehlert, M. E. (2017). How blockchain and smart contracts impact business in Thailand. Unpublished Doctoral dissertation). Thammasat University.

[17] Chalaemwongwan, N., & Kurutach, W. (2018, July). A practical national digital ID framework on blockchain (NIDBC). In 2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) (pp. 497-500). IEEE.

DOI: https://doi.org/10.15379/ijmst.v10i4.2245