International Journal of Advanced Technology and Engineering Exploration, Vol 11(119)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2024.111100329

Review Article

Tackling counterfeit certificate problems with blockchain technology: a review

Robiah Binti Arifin[1*], Wan Aezwani Wan Abu Bakar[2], Mustafa Bin Man[3] and Bishwajeet Pandey Kumar[4]
Infostructure and Network Management Centre, Universiti Sultan Zainal Abidin, 21030 Kuala Nerus, Terengganu, Malaysia[1]
Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, 22200 Besut Campus, Besut, Terengganu, Malaysia[2]
Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu, 21030 Kuala Nerus, Terengganu, Malaysia[3]
Department of Intelligent System and Cyber Security, Astana IT University, Astana, Kazakhstan[4]

Received: 20-March-2024; Revised: 22-September-2024; Accepted: 27-September-2024

Abstract
Counterfeit (fake) certificate problems have become a global issue, with many countries struggling to detect and prevent them. Addressing these challenges is crucial to maintaining quality standards in the education sector and providing assurance to employers about the legitimacy of qualifications held by prospective employees. The adoption of advanced technologies such as blockchain, Ethereum, Hyperledger, and smart contracts (SCs) shows promise in tackling these challenges. Blockchain, in particular, has emerged as a leading solution across various fields, with numerous applications proposed to combat the issue of fake certificates. A simplified analysis on the application and implementation of blockchain technologies, including Ethereum, SC, and consensus mechanisms, was reviewed in this paper to mitigate these problems using various tools, methods, and blockchain platforms. It covers diverse applications, ranging from counterfeit certificate prevention in education to implementations in manufacturing and engineering, utilizing different blockchain technologies. Additionally, several open-source tools that support the development of the Ethereum blockchain environment were discussed in the paper. The findings highlight significant contributions to enhancing the integrity of certificates using the Ethereum blockchain. The paper also explores the use of tools such as Remix, an integrated development environment (IDE), MetaMask, and Ganache, which facilitate development in a testing environment. However, it was discovered that these tools are not suitable for production purposes.

Keywords
Fake certificate, Blockchain, Ethereum, Smart contracts, Consensus mechanisms.

1.Introduction
According to Malaysia Higher Education Ministry statistics, the total of intake, enrolment and graduation students increased year by year [1]. An increment of graduation students every year affects job opportunities because graduation students compete with each other to find and catch the job opportunities. The main criteria for employers to choose the employees is based on their certificate. Authenticity of certificate is an important and easy way for employers to select and hire the employees. Unfortunately, numerous cases forging the certificate were traced because lack of mechanism to validate the certificate.

The persistence of fake certificate problems remains a pressing issue within the education sector, particularly in higher education. Numerous instances of counterfeit certificates have been detected globally. For example, in the United State of America, approximately 2,000,000 forged certificates were uncovered [2]. Similarly, the United Kingdom reported a total of 270 cases [3], and in Singapore, 660 individuals were found to have used fake certificates, as reported by the Ministry of Manpower

*Author for correspondence

[4]. Additionally, the Vietnamese ministry of education (MoE) and Training identified more than 10,000 fake certificates [5].

The issue of fake certificates has been increasing year by year, becoming a worldwide problem. These issues negatively impact the education domain, particularly in terms of the quality and credibility of academic qualifications. It is essential to address these issues to ensure that the quality and credibility of academic qualifications are recognized without dispute.

To address these challenges associated with forged certificates, blockchain technology offers a promising solution. Blockchain, introduced by Satoshi Nakamoto in 2008, operates on a decentralized distributed database model [6]. It combines cryptography and an open distributed ledger system, initially designed for digital currency applications [6].

However, implementation of blockchain able to overcome the fake certificate issues, but the challenges of implementation blockchain is about the performance of transaction data into the blockchain. Transaction speed is one of the important criteria in blockchain performance because it affected the numbering of throughput.

Regarding the widely discussed issue of counterfeit certificates, the objective of this paper is to explore methods implemented in previous studies. The preferred reporting items for systematic reviews and meta-analyses (PRISMA) method is used to search, select, and analyze papers based on inclusion and exclusion criteria. This paper reviews the proposed applications and solutions to address these issues. Finally, these methods, proposed applications, and solutions are analyzed.

The remainder of the paper is organized as follows: related work is discussed in Section 2, recent methods and tools are explored in Section 3, discussion and analysis are presented in Section 4, and conclusions are provided in Section 5.

2.Related work

To overcome the counterfeit certificate issues, a few methods that implemented by previous researches including blockchain, Ethereum and consensus algorithm discussed in this paper. These methods currently trending to overcome the counterfeit certificate issues. Regarding these methods, this section firstly discussed about the blockchain technology then proceed with the blockchain types focused on Ethereum. Additionally, this section also discusses the consensus algorithms that support the security aspect of blockchain technology.

2.1Blockchain technology

Blockchain is a technology that implements the data storage in block data structure [7]. Blockchain allows only write and read transactions [8], and data is processed through cryptographic procedures [9]. The implementation of consensus algorithms ensures the security and integrity of blockchain characteristics. The consensus algorithm interacts among the nodes [10]. Consensus roles make sure every transaction data should get an agreement. The agreement is needed by each node to commit the transaction to ensure the transaction process runs smoothly and secured. The consensus algorithm procedure supports the integrity and security of data on the blockchain.

The other characteristics of blockchain are immutability, reliability, efficiency, and trustworthiness. The characteristics of blockchain highlight this technology to grow very fast. Blockchain technology has expanded rapidly. The objective of improvement of blockchain is to increase the ability of blockchain. The improvement of blockchain consists of four phases, each phase proposed with new features. *Table 1* shows the features that were proposed on each phase [11].

Table 1 Phase of the blockchain evolution

Phase	Blockchain environment
1.0 (Bitcoin)	Implement only in crypto currency application
2.0 (Ethereum)	Implement smart contract (SC) and consensus
3.0 (Bitcoin, Ethereum, Hyperledger, etc.)	Support backend coding, decentralized applications (dApps)
4.0 (Bitcoin, Ethereum, Hyperledger, etc.)	

The blockchain is typically categorized into three types: public, consortium, and private [12]. Private blockchains are commonly developed by industries or organizations and are generally considered less secure than public blockchains. However, their security level largely depends on the measures implemented by the developer. Deploying a private blockchain is usually more cost-effective than a public one because it does not require as much expenditure on energy, time, and resources for achieving consensus.

Public blockchains, on the other hand, are accessible to all participants. Every participant has the ability to read, write, and audit the blockchain. They are deemed more secure than private blockchains due to their complex rules and intricate consensus algorithms, which serve to safeguard against malicious entities.

The consortium blockchain is a combination of both private blockchain and public blockchain. The public blockchain is popular and widely used because of its security and performance [13]. Bitcoin and Ethereum are types of public blockchain that are mostly applied [14] on various domains.

2.2Ethereum

Ethereum is an open-source platform to develop decentralized distributed data and its popular and widely used [14]. It was introduced by Buterin [15] in his white paper in 2013. Ethereum aimed to address the limitation of bitcoin [16]. Bitcoin and Ethereum are similar because they are public blockchain.

However, Bitcoin implemented the distributed ledger concept and Ethereum implemented the distributed data storage concept. Recent efforts in 5 years back (as illustrated in *Table 2*) discover and segregate the used of Ethereum technology on their research ranging in various domain from education to application in management, voting, health, insurance, oil and gas application, supply chain as well as human resource. These domain and issues are selected because of its ability to overcome through blockchain technology.

Table 2 Ethereum implementation on various domain

Authors & Year	Domain	Issues
Jeong and Choi [17] (2019)	Human resources	Performance assessment for hiring
Serranito et al. [18] (2020)	Education	Qualification verifications issues
Gaikwad et al. [19] (2021)	Education	Fake certificate issues
Malsa et al. [20] (2021)	Education	Certificate verification
Badlani et al. [21] (2022)	Management	Fake document academic
Lee et al. [22] (2022)	Vote	Voting fairness issue
Chondrogiannis et al. [23] (2022)	Insurance	Insurance individual and contact record
Ahmad et al. [24] (2022)	Oil and Gas	Managing oil and gas supply chain
Jaya et al. [25] (2023)	Health	Validation and of drug record
Ahamed and Vignesh [26] (2023)	Supply chain	Food supply chain management
Rustemi et al. [27] (2023)	Education	Academic Certificate and verification
Tang et al. [28] (2024)	Data security	Fraud detection

The advantages of Ethereum include its support for SC [29]. Distributed data storage means everyone is allowed to run their own application and blockchain on their own server. The SC is proposed by Nick Szabo in the early 1990s to support the Ethereum blockchain. It is developed and stored in the Ethereum blockchain and considered as the important part in Ethereum to run the instruction and command [30]. The SC is a high-level programming language to execute the instruction and validate the data on a specific address in blockchain. To write the SC, solidity is one of the programming languages that can support it. It is similar to the Java script programming language. Other programming languages that support SC are Mutan, Python, Viper and Chaincode.

2.3Consensus

Consensus is an algorithm to get agreement among the nodes before any transaction is agreed to commit [31]. In blockchain technology consensus is an important part to execute the blockchain to ensure the data is consistent and integrity [20]. The consensus also is one of security platforms in blockchain transactions. Any transaction process must get an agreement among the nodes through the consensus algorithm [32, 18]. There are diverse types of consensuses such as proof-of-work (PoW), proof-of-stake (PoS), Byzantine fault tolerant (BFT), and proof-of-authority (PoA). Each type possesses their own advantage and is suitable to implement based on the situation and environment. The selection of the consensus variant based on the blockchain type and blockchain client. Different consensuses possess its own procedure and policies [33, 22]. It also consists of its own characteristics and as illustrated in *Table 3* [34, 23].

Table 3 List of consensuses

Consensus	Speciality
PoS	More spike in blockchain
PoW	Able to solve a mathematical puzzle

Consensus	Speciality
Proof of Luck	Implemented the random selection
Proof of elapsed time	Able to set up the scheduling while the timeout
Proof of space	Implemented in bigger size of hard disk environment

3.Recent method and tools

In contemporary times, numerous industry sectors are vigorously adopting blockchain technology across various facets of their operations, spanning education, healthcare, transportation, supply chain management, and beyond. This segment explores into the integration of blockchain within the realm of higher education, aimed at mitigating the challenges associated with counterfeit certificates. Also discussed the methods that implemented to solve the fake certificate issues including tools that able to support implementation of blockchain.

3.1Fake certificate issues in higher education

The first case of fake certificate issues was traced in 1883 at Wooton [1]. It was traced because the certificate was issued by an undefined university. After that, various countries detected fake certificate issues. It has increased year by year and become a big issue in the higher education domain [35]. The main factor causing the fake certificate issues giant is difficulties of manual certificate verification. Certificate validation is a big issue among employers. The extra cost and time needed to verify the employee certificates [36].

The fake certificate issues can be defeated through a framework based on blockchain technology [37]. The framework includes a few features such as security, transparency and reduced cost. Embedded blockchain technology is able to support the verification process to avoid academic certificates frauds [38].

3.2Blockchain implementation

According to recent reviews, blockchain technology presents a promising solution to combat counterfeit certificates and ensure validation. The utilization of Ethereum blockchain alongside SC has been identified as effective in addressing this issue. The potential of blockchain technology and SC extends to facilitating the verification process of higher education certificates [39].

In contemporary times, numerous applications built on blockchain technology have been suggested to address the problem of counterfeit certificates. This study explores into the challenges surrounding certificate verification [40]. To tackle these challenges, the research suggests implementing a digital certificate system rooted in Ethereum and SC The proposed system aims to combat counterfeit certificates and minimize management expenses. However, blockchain-based certificates are not generated automatically; rather, they require a request from the student or candidate. Subsequently, authorized individuals review these requests and determine their approval. One drawback is that if a student fails to request a blockchain-based certificate, the verification issues may not be fully resolved.

The weaknesses in tracing fake certificate methods contribute significantly to the prevalence of fake certificate issues. In addressing this challenge, a digital certificate system was introduced [8]. These systems leverage the Ethereum blockchain and solidity SC. Their functionalities encompass both the issuance and verification of certificates. However, to initiate the issuance of a digital certificate, a request from the student is required. The generation of digital certificates is contingent upon student requests. In cases where students do not request certificate generation via the blockchain, manual certificate verification procedures are implemented.

There is currently no established standard mechanism for certificate verification, leading to a rise in forged certificate problems that pose significant challenges [31]. To address this issue, a web-based application was created to facilitate the generation and validation of certificates using the Ethereum blockchain and SC. However, limitations exist within these applications, as they restrict modifier values to less than or equal to four and are tailored only for specific courses in generating and validating certificates. Ideally, such applications should allow for the adjustment of modifier values and comparison with any relevant courses, enabling automated verification through SC.

The initiative outlined in [41] introduced an application developed on the Hyperledger Fabric Blockchain, named VECefblock. This application operates on the amazon elastic compute cloud (Amazon EC2 Cloud), ensuring continuous execution. It targets authentication certificates to combat counterfeit certificate problems in Vietnam. The proposed application encompasses both certificate generation and verification for all students, with a particular emphasis on data privacy and transaction throughput. However, it lacks consideration for data validation and changes. Data

alterations may occur due to errors in input by lecturers or administrators.

Certificate access permission related in certificate verification process [42] examines the topic of certificate access permissions. It explores the integration of Hyperledger Fabric and internet of things (IoT) to enhance the effectiveness of certificate access permissions. These applications utilize digital signatures and hash keys, which are stored alongside the digital certificate, aiming to uphold the validity of issued certificates. However, the paper lacks detailed explanation on how the proposed model generates and verifies certificates.

To avoid the leaking of the academic records [43], new application is proposed. The application applied Ethereum as a blockchain platform and the Proof of Authority as a consensus algorithm. These applications allow others education institute to join the consortium. The proposed model did not highlight how the data for each education institute will keep privacy.

Similarly, [44] introduced a system called MOETVBC, designed to address counterfeit certificate concerns in Saudi Arabia. This application leverages Hyperledger as its blockchain platform to create a secure, expedient, and transparent solution. Its primary focus lies in streamlining the certificate verification process. However, one limitation pertains to data sourcing. The data resources rely solely on the MoE rather than directly from educational institutions. Consequently, verification processes may experience delays if the MoE encounters challenges in collecting data from these organizations.

The work presented in [45] introduces a theoretical model aimed at tackling the problem of counterfeit certificates. This model encompasses both the issuance and verification of certificates through blockchain technology. Overall, the proposed model appears comprehensive in addressing counterfeit certificate concerns. Utilizing blockchain ensures the security and reliability of verification statuses. However, verification responses may not be immediate, as the verification process extends across email platforms, necessitating additional time.

Recognizing the imperative for higher education to address counterfeit certificate issues, a Higher Education Certificate model was proposed [46]. This model delves into aspects such as certificate issuance, verification, data transactions, and data privacy. Nonetheless, a limitation arises from certificates being issued only upon student request, thereby hindering verification via blockchain processing.

Regarding the implementation of blockchain to address counterfeit certificate issues, *Table 4* summarizes previous research that applied blockchain technology to overcome these challenges.

Table 4 Methods and solution for counterfeit certificate issues

Author	Year	Solution	Method
Nguyen et al. [41]	2020	Certificate verification	Hyperledger
Saleh et al. [14]	2020	Certificate verification	Hyperledger
Toyoda et al. [47]	2020	Digital certificate and verification	Ethereum, SC & consensus algorithm
Gaikwad et al. [19]	2021	Certificate verification	Ethereum & SC
Ayub et al. [48]	2021	Certificate verification	Hyperledger
Guerreiro et al. [38]	2022	Certificate verification and integration	Ethereum & SC
Badlani et al. [21]	2022	Certificate verification	Ethereum
Leka, et al. [49]	2022	Digital certificate and verification	Ethereum & SC
Ghani et al. [50]	2022	Digital certificate and verification	Hyperledger & SC
Kistaubayev et al. [51]	2022	Certificate verification and student information	Ethereum

Based on *Table 4*, 6 out of *10* previous studies addressing counterfeit certificate issues proposed using the Ethereum blockchain for creating digital certificates and verification. Ethereum is popular because it implements distributed data storage, allowing users to run their own applications and blockchain [52]. It can also store data with an unlimited block size [53]. The remaining 4 studies

suggested implementing Hyperledger for this purpose.

3.3Tools

Numerous tools are available to aid in blockchain development, including Remix integrated development environment (IDE), MetaMask, Ganache, and others. Each tool possesses its unique functionality; for instance, Ganache is utilized to generate a development blockchain. Meanwhile, Remix IDE and MetaMask are employed to facilitate the blockchain development process. The Truffle IDE, MetaMask, Infura application programmer's interface (API), SC, and the Ropsten Network were utilized to aid in configuring the proposed applications [54]. Furthermore, Truffle and Web3 supported the Rinkeby test network for data transaction storage [55]. These tools were implemented to bolster the proposed application's integration of blockchain technology, as illustrated in *Table 5*.

Table 5 Supported tools for Blockchain implementation

Authors/Year	Tools	Implementation
Malsa et al. [20] (2021)	Remix IDE and MetaMask	Testing the send transaction into blockchain and generate private key
Gaikwad et al. [19] (2021)	Rinkeby	Testing blockchain network
Hawashin et al. [56] (2021)	Remix IDE	Create and compile SC
Shawon et al. [13] (2021)	Remix IDE and MetaMask	Writing SC and generate private key
Ahmad et al. [24] (2022)	Web3	Generate the private key
Ahamed and Vignesh [26] (2023)	Ganache and Truffle	Create Ethereum blockchain used testnet and migrate blockchain and SC
Leka et al. [49] (2022)	Ganache and Rinkeby	Generate Ethereum and testing blockchain network

Table 5 indicates the advantages of implementing these tools are their ease of use and configuration. However, the disadvantage is that they are only suitable for use in a development environment. Implementing them in a production environment poses a high risk.

3.4Digital certificate and verification issues

The implementation of blockchain technology has become a trending solution to address counterfeit certificate issues. Various methods, including Bitcoin, Ethereum, Hyperledger, SC, and consensus algorithms, are currently being used to tackle these challenges. These methods are integrated into proposed systems to generate and verify digital certificates. While most proposed systems using blockchain methods have successfully addressed counterfeit issues, the performance of accessing and verifying digital certificates still requires further attention.

Table 6 demonstrates that blockchain implementation is capable of addressing counterfeit certificate issues. However, starting in 2023, performance issues related to the steps involved in digital certificate generation, viewing, and verification have been revisited for further discussion.

Table 6 Performance issues in blockchain technology

Authors	Year	Case study
Rustemi et al. [27]	2023	Certificate verification
Wang et al. [57]	2023	Educational data
Aini et al. [58]	2023	Certificate verification
Fang et al. [59]	2024	Credential verification
Feng et al. [60]	2024	Certificate authentication
Liu et al. [61]	2024	Certificate verification
Mai et al. [62]	2024	Certificate verification
Al and Morato [63]	2023	Certificate verification

4.Discussion and analysis

The review analysis was conducted using the PRISMA method, which is an evidence-based approach for systematic reviews to identify relevant resources [64]. *Figure 1* depicts a block diagram illustrating the process of analysis based on previous studies. A total of 160 articles and 5 sources from websites were sought, but only 115 articles and 1 website source were successfully retrieved (*Figure 1*). The search was conducted using keywords such as "blockchain," "certificate issues," and "Ethereum." Of these, only 61 articles were included and used in this paper, while 54 were excluded.

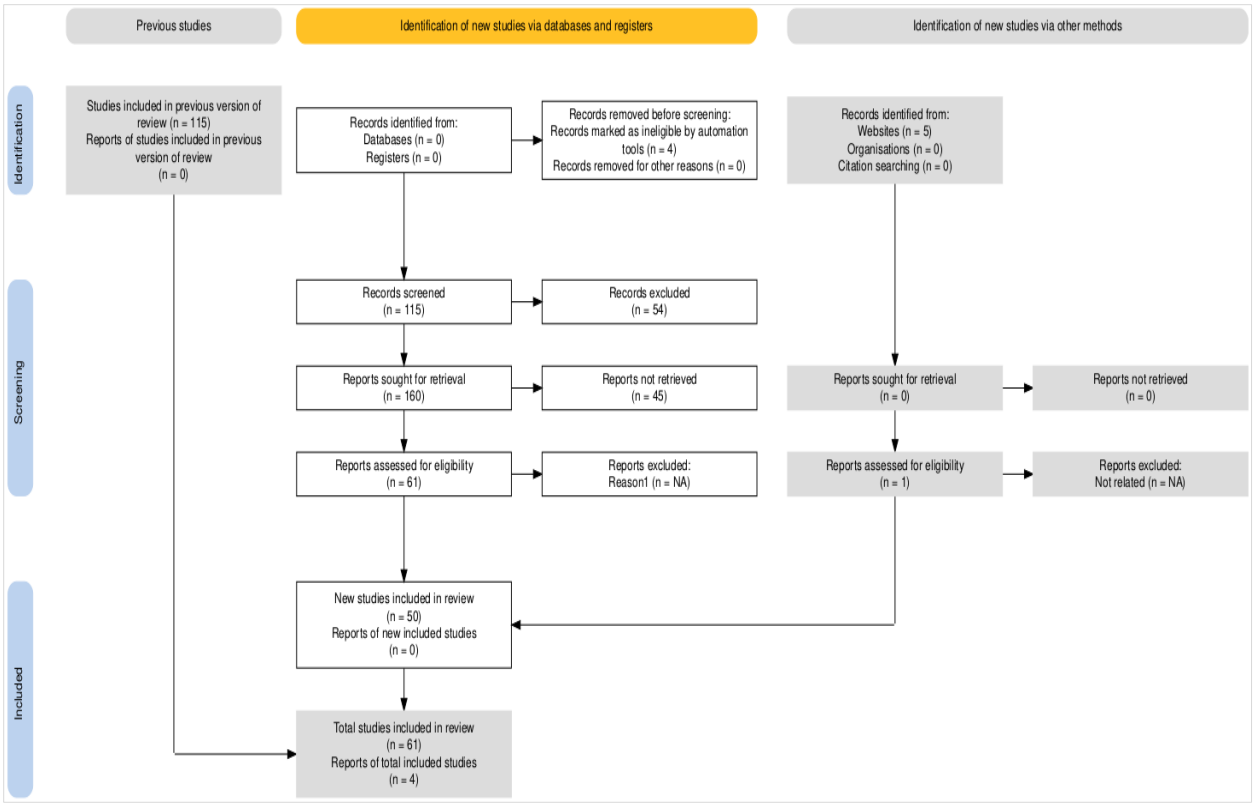


Figure 1 Analysis based on PRISMA

The 61 articles included in this review were sourced from various publications, including Journals (45), Proceedings (13), Books (1), Magazines (1), and Website articles (1), as shown in *Figure 2*.

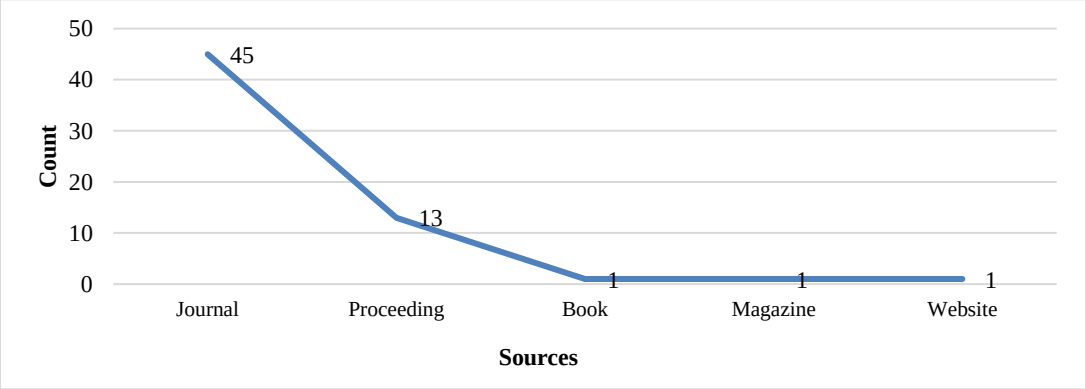


Figure 2 Sources of articles included in the review

All the articles focused on blockchain technology, and analyses were conducted from various angles and perspectives, drawing from previous research. Additionally, *Table 7* shows the distribution of the reviewed papers based on the year and type of article, including journals, proceedings, books, magazines, and websites.

Table 7 Distribution of articles reviewed by year and type

Year	Journal	Proceeding	Book	Magazine	Websites
2024	5	2	0	0	0
2023	8	1	0	0	0
2022	7	3	0	0	0
2021	8	4	0	1	1
2020	6	3	0	0	0
2019	6	0	0	0	0
2018	1	0	1	0	0

The articles reviewed were also analyzed based on their publication sources, as shown in *Figure 3*. Nine different types of publishers were considered for the review and analysis (*Figure 4*): IEEE (24), Education Journal (3), ACM (5), Applied Science (8), Frontiers (2), Electronic Journal (4), Science & Technology Journal (5), Science Computer (2), and other publishers (8). Meanwhile, out of the 61 articles related to the discussion, a dataset was developed and these issues were analyzed, covering the implementation of blockchain in various domains, fake certificate issues, and development tools that support blockchain implementation to address counterfeit problems.

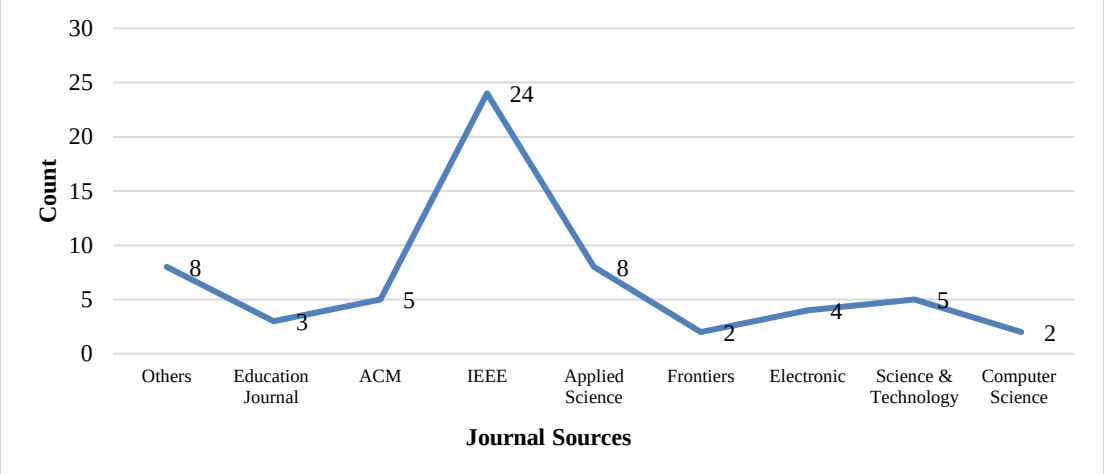
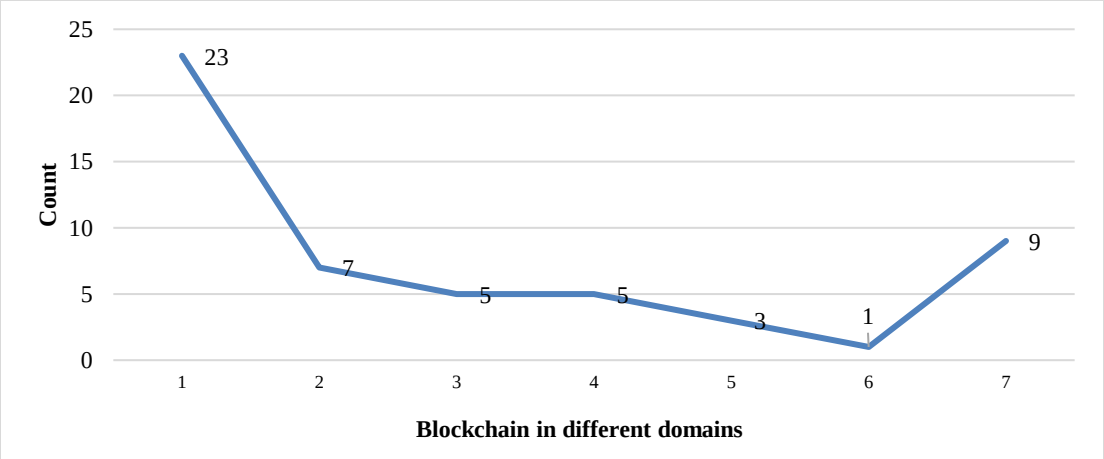


Figure 3 Number of articles according to the publication sources

4.1Blockchain in various domain

Blockchain's implementation merely seen across various domain, but education domain is the most popular discussed among the researchers with the total of 50 efforts from 2018 to 2024 as depicted in *Figure 1*. According to *Figure 4*, the education sector dominates the discussion on blockchain-related issues, with 23 studies addressing this area, whereas only 7 studies focus on the management sector. Additionally, 9 issues are related to other sectors, with 5 pertaining to the health domain. The oil and gas, insurance, and supply chain sectors each have 5, 3, and 1 issue discussed, respectively, in both insurance and supply chain domains. *Figure 5* explores and highlights the prevalence of fake certificate issues specifically within the education sector during the period from 2018 to 2024.



1: Education, 2: Management, 3: Health: 4: Oil and Gas, 5: Insurance, 6: Supply chain and 7: Others

Figure 4 Implementation of blockchain in different domains

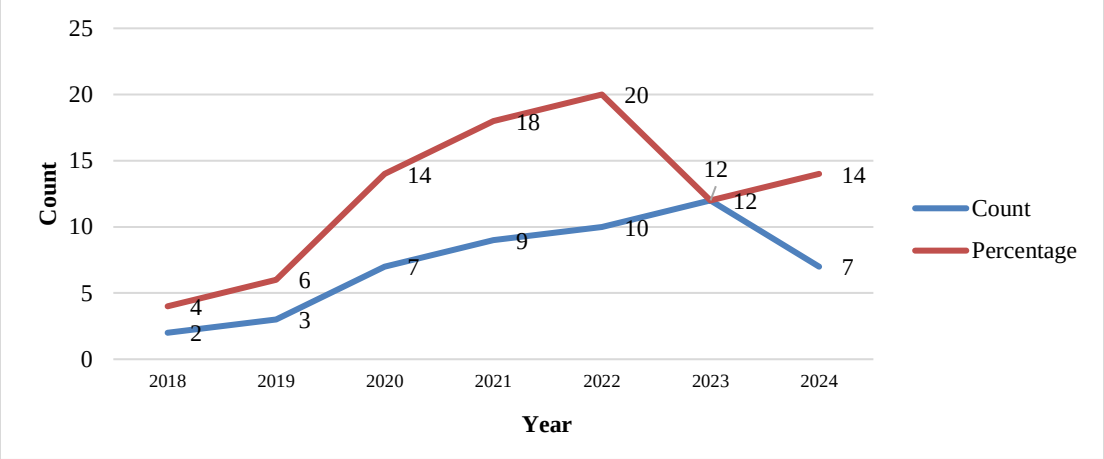


Figure 5 Blockchain discussion year wise in education domain

As shown in *Figure 5*, discussions regarding counterfeit certificates in the education domain began in 2018, accounting for 2 articles (4% of the total). These discussions have steadily increased each year, rising to 3 articles (6%) in 2019, 7 articles (14%) in 2020, and 9 articles (18%) in 2021. In 2022, the number of discussions reached 10 articles (20%), followed by 12 articles (24%) in 2023, and 7 articles (14%) by June 2024. The increasing percentage of discussions on this topic highlights its growing relevance and the urgent need for resolution.

4.2Fake certificate issues

Numerous researchers have engaged in discussions regarding counterfeit certificate concerns, proposing various methods and applications to address them through blockchain technology. *Figure 6* illustrates the statistics pertaining to counterfeit certificate issues and the solutions proposed by previous studies considering different aspect.

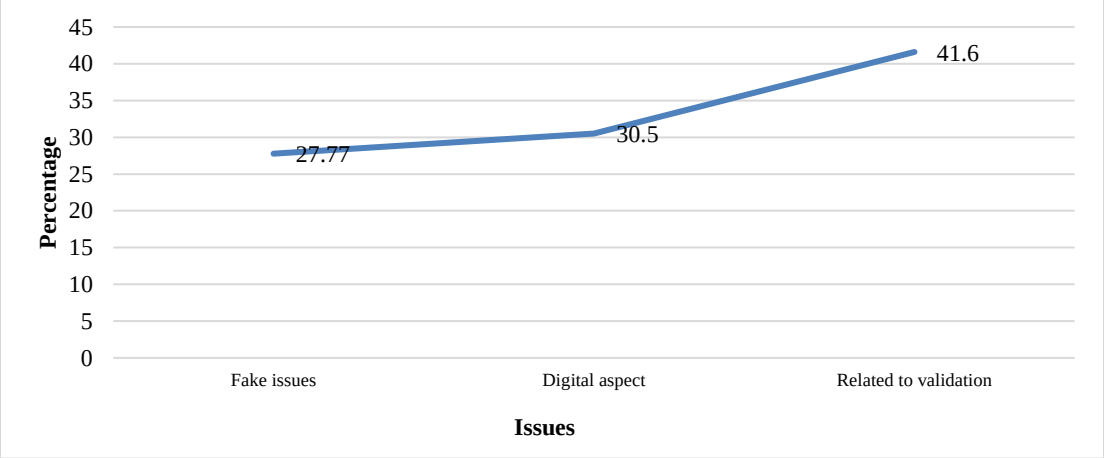


Figure 6 Issues and proposed method to overcome fake certificate issues

Figure 6 reveals around 27.77% of researchers have addressed the issue of counterfeit certificates. To tackle this challenge, 30.5% have advocated for digital certificates using blockchain, while 41.6% have suggested certificate validation based on blockchain technology. However, these proposals lack detailed explanations regarding crucial aspects such as data transaction, validation, privacy, and throughput. Addressing these criteria is essential for the implementation of blockchain-based applications, as outlined in *Table 8*.

The criteria mentioned in *Table 8* are important aspects to address counterfeit issues. However, they are not all-inclusive in the blockchain process, as shown in *Table 9*.

Table 8 Key criteria for discussion

Criteria	Description
Data validation	How and who have authorities to validate the data before it able to commit into the blockchain. Data validation process is important task because data that sored in blockchain impossible to update.
Data privacy	It becomes an issue if the application was share with other organization or education institute. Supposed each organization able to handle their own data and keep it privacy.
Data transaction	The process of data transaction includes write and read data from blockchain is important to ensure the performance of proposed application.
Data throughput	Throughput is a successful numbering transaction per second. The increase of throughput related with the application performance.

Table 9 List of criteria

Criteria	Blockchain
Data validation	Exclusion
Data privacy	Exclusion
Data transaction	Inclusion
Data throughput	Inclusion

Table 9 shows that data validation and data privacy are not inherently included in the blockchain engine; they depend on the application setup. On the other hand, data transaction and data throughput are criteria embedded in the blockchain engine. However, the performance of data transactions and data throughput depends on several factors, including the consensus algorithm, data size, network, number of nodes, and other variables.

4.3Development tools

Meanwhile in terms of tools, most researchers discussed about the tools such as Remix IDE, Truffle, Ganache and MetaMask. These tools able to support development application using blockchain environment only. The detail prescription on how to implement the application using blockchain technology in production environment is yet to disclose further since those tools are embedded in the in-house development of the Ethereum blockchain applications.

4.4Limitations

The main challenge in completing this study was finding and reviewing relevant papers. Most papers did not discuss or provide detailed methods for addressing counterfeit issues. They merely stated that blockchain can address these issues without explaining the proposed methods in detail.

Additionally, most papers did not discuss the tools needed to support blockchain development in a production environment. They only mentioned open-source tools like Ganache, MetaMask, and Web3, without detailing the specific functions of each tool. Therefore, additional research on these open-source methods was required.

A complete list of abbreviations is listed in *Appendix I.*

5.Conclusion

Utilizing blockchain technology for the generation and validation of digital certificates provides an effective solution to address counterfeit certificate issues. The inherent characteristics of blockchain, such as transparency and immutability, instill trust and make it well-suited for tackling these challenges. In this study, various blockchain platforms used for generating and validating academic certificates are examined. Many researchers have proposed prototypes and theoretical approaches to mitigate these issues; however, these methods often do not cover the entire certification process, including data integration and ensuring the validity of information committed to the blockchain. Additionally, tools that facilitate blockchain implementation, such as Remix IDE, Truffle, Ganache, and MetaMask, are analyzed. It is concluded that developing blockchain-based applications requires the support of open-source tools. However, these tools may not always be suitable for production environments. In light of the limitations of open-source tools and the shortcomings of previous systems, the MongoDB, Angular, Ionic, Node.js, smart contract, truffle, ethereum blockchain, and python (MAINSTEP) model (MongoDB, Angular, Ionic, Node.js, SCs, Truffle, Ethereum Blockchain, and Python) can be proposed for blockchain-based application development to combat counterfeit certificate issues. These methods enable the utilization of blockchain, Ethereum, SC, and consensus mechanisms in production environments. Additionally, concerns regarding data validation, privacy, transaction processing, and throughput are addressed to ensure the efficacy of the developed applications.

Acknowledgment
We would like to extend our sincere gratitude to the Center of Research and Innovation Management (CREIM) at UniSZA for their invaluable financial support toward this publication. This work was partially supported by grant code UniSZA/2024/PSU-TDP/03, titled Study on Strengthening International Research Collaboration – Center for Research and Innovation Management, UniSZA. We also express our heartfelt appreciation to the UMT team members. Additionally, we used ChatGPT to assist with language refinement.

Conflicts of interest
The authors have no conflicts of interest to declare.

Data availability
None.

Author's contribution statement
Robiah Arifin: Conceptualized, wrote, and edited the manuscript, conducted the study, and analyzed the results. **Wan Aezwani Wan Abu Bakar**: Conceptualized and revised the paper, supervised the conducted study, checked the study results and proofread the final corrected version. **Mustafa Bin Man**: Conceptualized and idea initiation. **Bishwajeet Pandey Kumar**: Conceptualized, Editing. Proofreading and network linkages.

References
[1] https://www.mohe.gov.my. Accessed 20 January 2024.
[2] Grolleau G, Lakhal T, Mzoughi N. An introduction to the economics of fake degrees. Journal of Economic Issues. 2008; 42(3):673-93.
[3] Garwe EC. Qualification, award and recognition fraud in higher education in Zimbabwe. Journal of Studies in Education. 2015; 5(2):119-35.
[4] https://www.straitstimes.com/global. Accessed 20 January 2024.
[5] Dinh TT, Wang J, Chen G, Liu R, Ooi BC, Tan KL. Blockbench: a framework for analyzing private blockchains. In proceedings of the international conference on management of data 2017 (pp. 1085-100). ACM.
[6] Nakamoto S. A peer-to-peer electronic cash system. Bitcoin. 2008; 4(2):1-24.
[7] Monrat AA, Schelén O, Andersson K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access. 2019; 7:117134-51.
[8] Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate. In international conference on applied system invention 2018 (pp. 1046-51). IEEE.
[9] Fernandez-carames TM, Fraga-lamas P. Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access. 2020; 8:21091-116.
[10] Mingxiao D, Xiaofeng M, Zhe Z, Xiangwei W, Qijun C. A review on consensus algorithm of blockchain. In international conference on systems, man, and cybernetics 2017 (pp. 2567-72). IEEE.
[11] Delgado-von-eitzen C, Anido-rifón L, Fernández-iglesias MJ. Blockchain applications in education: a systematic literature review. Applied Sciences. 2021; 11(24):11811.
[12] Wang J, Wu P, Wang X, Shou W. The outlook of blockchain technology for construction engineering management. Frontiers of Engineering Management. 2017; 4(1):67-75.
[13] Shawon SK, Ahammad H, Shetu SZ, Rahman M, Hossain SA. DIUcerts DApp: a blockchain-based solution for verification of educational certificates. In 12th international conference on computing communication and networking technologies 2021 (pp. 1-10). IEEE.
[14] Saleh OS, Ghazali O, Rana ME. Blockchain based framework for educational certificates verification. Journal of Critical Reviews. 2020; 7(3):79-84.
[15] Buterin V. A next-generation SC and decentralized application platform. White Paper. 2014; 3(37):2-1.
[16] Vujičić D, Jagodić D, Ranđić S. Blockchain technology, bitcoin, and ethereum: a brief overview. In 17th international symposium infoteh-jahorina (infoteh) 2018 (pp. 1-6). IEEE.
[17] Jeong WY, Choi M. Design of recruitment management platform using digital certificate on blockchain. Journal of Information Processing Systems. 2019; 15(3):707-16.
[18] Serranito D, Vasconcelos A, Guerreiro S, Correia M. Blockchain ecosystem for verifiable qualifications. In 2nd conference on blockchain research & applications for innovative networks and services 2020 (pp. 192-9). IEEE.
[19] Gaikwad H, D'souza N, Gupta R, Tripathy AK. A blockchain-based verification system for academic certificates. In international conference on system, computation, automation and networking 2021 (pp. 1-6). IEEE.
[20] Malsa N, Vyas V, Gautam J, Ghosh A, Shaw RN. CERTbchain: a step by step approach towards building a blockchain based distributed appliaction for certificate verification system. In 6th international conference on computing, communication and automation 2021 (pp. 800-6). IEEE.
[21] Badlani S, Aditya T, Maniar S, Devadkar K. Educrypto: transforming education using blockchain. In 6th international conference on intelligent computing and control systems 2022 (pp. 829-36). IEEE.
[22] Lee CH, Neo HF, Teo CC. Secure e-voting system based on blockchain technology. Journal of System and Management Sciences. 2022; 12(5):121-38.
[23] Chondrogiannis E, Andronikou V, Karanastasis E, Litke A, Varvarigou T. Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health

insurance organizations. Blockchain: Research and Applications. 2022; 3(2):100049.
[24] Ahmad RW, Salah K, Jayaraman R, Yaqoob I, Omar M. Blockchain in oil and gas industry: applications, challenges, and future trends. Technology in Society. 2022; 68:101941.
[25] Jaya RM, Rakkhitta VD, Sembiring P, Edbert IS, Suhartono D. Blockchain applications in drug data records. Procedia Computer Science. 2023; 216:739-48.
[26] Ahamed NN, Vignesh R. A build and deploy ethereum smart contract for food supply chain management in truffle-ganache framework. In 9th international conference on advanced computing and communication systems 2023 (pp. 36-40). IEEE.
[27] Rustemi A, Dalipi F, Atanasovski V, Risteski A. A systematic literature review on blockchain-based systems for academic certificate verification. IEEE Access. 2023; 11:64679-96.
[28] Tang M, Ye M, Chen W, Zhou D. BiLSTM4DPS: an attention-based BiLSTM approach for detecting phishing scams in Ethereum. Expert Systems with Applications. 2024; 256:124941.
[29] Guo H, Yu X. A survey on blockchain technology and its security. Blockchain: Research and Applications. 2022; 3(2):100067.
[30] Haveri P, Rashmi UB, Narayan DG, Nagaratna K, Shivaraj K. Edublock: securing educational documents using blockchain technology. In international conference on computing, communication and networking technologies 2020 (pp. 1-7). IEEE.
[31] Rajeswari TR, Shareef SK, Khan S, Venkatesh N, Ali A, Devi VS. Generating and validating certificates using blockchain. In 6th international conference on communication and electronics systems 2021 (pp. 1048-52). IEEE.
[32] Rane M, Singh S, Singh R, Amarsinh V. Integrity and authenticity of academic documents using blockchain approach. In ITM web of conferences 2020 (pp. 1-5). EDP Sciences.
[33] Kaur M, Khan MZ, Gupta S, Noorwali A, Chakraborty C, Pani SK. MBCP: Performance analysis of large scale mainstream blockchain consensus protocols. IEEE Access. 2021; 9:80931-44.
[34] Pahlajani S, Kshirsagar A, Pachghare V. Survey on private blockchain consensus algorithms. In 1st international conference on innovations in information and communication technology 2019 (pp. 1-6). IEEE.
[35] Abbas AA. Cloud-based framework for issuing and verifying academic certificates. International Journal of Advanced Trends in Computer Science and Engineering. 2019; 8(6):2743-9.
[36] Caldarelli G, Ellul J. Trusted academic transcripts on the blockchain: a systematic literature review. Applied Sciences. 2021; 11(4):1-22.
[37] He B, Feng T. Encryption scheme of verifiable search based on blockchain in cloud environment. Cryptography. 2023; 7(2):1-17.
[38] Guerreiro S, Ferreira JF, Fonseca T, Correia M. Integrating an academic management system with blockchain: a case study. Blockchain: Research and Applications. 2022; 3(4):100099.
[39] SS ML, Shettar MA. Block chain based framework for document verification. In 2nd international conference on artificial intelligence and signal processing 2022 (pp. 1-5). IEEE.
[40] Badhe V, Nhavale P, Todkar S, Shinde P, Kolhar K. Digital certificate system for verification of educational certificates using blockchain. International Journal of Scientific Research in Science and Technology. 2020; 7(5):45-50.
[41] Nguyen BM, Dao TC, Do BL. Towards a blockchain-based certificate authentication system in Vietnam. Peer Journal Computer Science. 2020; 6:1-27.
[42] Goud BM, Lilaramani D, Swain M. Generation and authentication of digital certificates using ethereum based decentralized mechanism for mitigating data fraud on RISC-V. In international conference on computational performance evaluation 2021(pp. 905-9). IEEE.
[43] Daraghmi EY, Daraghmi YA, Yuan SM. UniChain: a design of blockchain-based system for electronic academic records access and permissions management. Applied Sciences. 2019; 9(22):1-27.
[44] Alangari S, Alshahrani SM, Khan NA, Alghamdi AA, Almalki J, Al SW. Developing a blockchain-based digitally secured model for the educational sector in Saudi Arabia toward digital transformation. Peer Journal Computer Science. 2022; 8:1-22.
[45] Ghazali O, Saleh OS. A graduation certificate verification model via utilization of the blockchain technology. Journal of Telecommunication, Electronic and Computer Engineering. 2018; 10(3-2):29-34.
[46] Ali MA, Bhaya WS. Higher education's certificates model based on blockchain technology. In journal of physics: conference series 2021 (pp. 1-10). IOP Publishing.
[47] Toyoda K, Machi K, Ohtake Y, Zhang AN. Function-level bottleneck analysis of private proof-of-authority Ethereum blockchain. IEEE Access. 2020; 8:141611-21.
[48] Ayub KA, Laghari AA, Shaikh AA, Bourouis S, Mamlouk AM, Alshazly H. Educational blockchain: a secure degree attestation and verification traceability architecture for higher education commission. Applied Sciences. 2021; 11(22):10917.
[49] Leka E, Kordha E, Hamzallari K. Towards an IPFS-blockchain based authentication/management system of academic certification in western Balkans. In 45th jubilee international convention on information, communication and electronic technology 2022 (pp. 1448-53). IEEE.
[50] Ghani RF, Salman AA, Khudhair AB, Aljobouri L. Blockchain-based student certificate management and system sharing using hyperledger fabric platform. Periodicals of Engineering and Natural Sciences. 2022; 10(2):207-18.
[51] Kistaubayev Y, Mutanov G, Mansurova M, Saxenbayeva Z, Shakan Y. Ethereum-based information system for digital higher education

registry and verification of student achievement documents. Future Internet. 2022; 15(1):1-19.
[52] Dos SAAW, Coutinho EF, Bezerra CI. Performance evaluation of data transactions in blockchain. IEEE Latin America Transactions. 2021; 20(3):409-16.
[53] Dhulavvagol PM, Bhajantri VH, Totad SG. Blockchain ethereum clients performance analysis considering E-voting application. Procedia Computer Science. 2020; 167:2506-15.
[54] Appasani B, Mishra SK, Jha AV, Mishra SK, Enescu FM, Sorlei IS, et al. Blockchain-enabled smart grid applications: architecture, challenges, and solutions. Sustainability. 2022; 14(14):1-33.
[55] Islam MM, Merlec MM, In HP. A comparative analysis of proof-of-authority consensus algorithms: aura vs clique. In international conference on services computing 2022 (pp. 327-32). IEEE.
[56] Hawashin D, Mahboobeh DA, Salah K, Jayaraman R, Yaqoob I, Debe M, et al. Blockchain-based management of blood donation. IEEE Access. 2021; 9:163016-32.
[57] Wang Y, Cong X, Zi L, Xiang Q. Blockchain for credibility in educational development: key technology, application potential, and performance evaluation. Security and Communication Networks. 2023; 2023(1):5614241.
[58] Aini Q, Harahap EP, Santoso NP, Sari SN, Sunarya PA. Blockchain based certificate verification system management. APTISI Transactions on Management. 2023; 7(3):191-200.
[59] Fang J, Feng T, Guo X, Ma R, Lu Y. Blockchain-cloud privacy-enhanced distributed industrial data trading based on verifiable credentials. Journal of Cloud Computing. 2024; 13(1):30.
[60] Feng X, Wang L, Bai X, Yang P. Distributed identity management mechanism based on improved block-chain certificateless encryption algorithm. Physical Communication. 2024; 65:102341.
[61] Liu H, Ming Y, Wang C, Zhao Y, Zhang S, Lu R. Blockchain-assisted verifiable certificate-based searchable encryption against untrusted cloud server for industrial internet of things. Future Generation Computer Systems. 2024; 153:97-112.
[62] Mai CK, Iqbal MS, Rohith A, Suchetan TCK, Shinde PC. Applicant credentials tracker for employment using blockchain technology. International Journal of Intelligent Systems and Applications in Engineering. 2024; 12(3s):320-7.
[63] Al SB, Morato J. The use of blockchain technology in the educational field in Bahrain. In international congress on blockchain and applications 2023 (pp. 527-35). Cham: Springer Nature Switzerland.
[64] Haddaway NR, Page MJ, Pritchard CC, Mcguinness LA. PRISMA2020: an R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and open Synthesis. Campbell Systematic Reviews. 2022; 18(2): e1230.

Robiah Binti Arifin is currently a PhD-level postgraduate student at Universiti Sultan Zainal Abidin (UniSZA). She has nearly 20 years of experience in software development and has contributed to UniSZA for almost 6 years, focusing on Decentralized Applications (DApps) using the Ethereum blockchain. She is currently leading the development of Big Data infrastructure at UniSZA.
Email: robiah@unisza.edu.my

Wan Aezwani Wan Abu Bakar obtained her Ph.D. in Computer Science from Universiti Malaysia Terengganu (UMT) in November 2016, specializing in association rules in frequent itemset mining. She earned her Master of Science in Computer Science from Universiti Teknologi Malaysia in 2000, focusing on fingerprint image segmentation, after completing her bachelor's degree in the same field from Universiti Putra Malaysia in 1998. Since January 1, 2018, she has been a member of the Faculty of Informatics & Computing at UniSZA, Besut Campus. Dr. Wan Aezwani has overseen three DPU grants totalling 45.5K and one FRGS grant of 70K. Her research is concentrated on developing water-based sensors for Intelligent Mosquito Home Systems in combating dengue, creating predictive models for heart disease and breast cancer in machine learning, and innovative educational tools. She has spearheaded significant research endeavors and a prolific publication record, contributing significantly to advancements in her field.
Email: wanaezwani@unisza.edu.my

Mustafa Bin Man is the Associate Professor of the Faculty of Ocean Engineering Technology and Informatics (FTKKI) and a Deputy Director at Research Management Innovation Centre (RMIC), UMT. He started his PhD studies in July 2009 and finished his studies at UTM in Computer Science in 2012. He received Computer Science Diploma, Degree, and Masters Degree from UPM. In 2012, he was awarded a “MIMOS Prestigious Awards” for his PhD by MIMOS Berhad. His research is focused on developing multiple types of databases integration models and in Augmented Reality (AR), Android Based, and IT related across domain platforms. He is the leader of the UMT matching grant collaborator.
Email: mustafaman@umt.edu.my

Bishwajeet Pandey Kumar is a Professor at Department of Intelligent System and Cyber Security, Astana IT University Kazakhstan. He is a senior member of IEEE, USA since 2019. He got the Professor of the Year-2023 award at Lords Cricket Ground by London Organization of Skills Development (LOSD), UK. He is also a visiting professor at Eurasian National University, Astana, Kazakhstan (QS World Rank 355) and UCSI University, Kuala Lumpur, Malaysia (QS World Rank 300). He is a research Fellow at University of Sultan Zainul Abdin (UniSZA), Malaysia. He was the Research Head of the School of Computer Science and Engineering at Jain University, Bangalore, India. He holds a Ph.D. in Computer Science and Engineering from Gran Sasso Science Institute, Italy. He completed Masters from the Indian Institute of Information Technology (IIIT), Gwalior, India. With over 15 years of experience, he has worked as a Research Consultant and Associate Visiting Professor. He has also held positions as an Assistant Professor at various universities e.g. Chitkara University, Chandigarh University, and Birla Institute of Applied Science, Bhimtal India. Dr. Pandey has visited 47 countries and attended 101 conferences, receiving best paper awards in multiple countries. He has authored over 200 papers and published ten books. With interests in Green Computing, High-Performance Computing, Cyber-Physical Systems, Machine Learning, and Cyber Security, he has several Indian patents and serves on the board of directors for student-founded startups. He has 3100+ citations (Google Scholar) and 27 H-index (Google Scholar), 18 H-Index(Scopus). He has generated revenue of 20 million INR in his start-up Gyancity Research Consultancy Pvt Ltd since 2018.
Email: bk.pandey@astanait.edu.kz

Appendix I

S. No.	Abbreviation	Description
1	AI	Artificial Intelligence
2	Amazon EC2 Cloud	Amazon Elastic Compute Cloud
3	API	Application Programmer's Interface
4	BFT	Byzantine Fault Tolerant
5	dApps	Decentralized Application
6	IDE	Integrated Development Environment
7	IoT	Internet of Things
8	MAINSTEP	MongoDB, Angular, Ionic, Node.js, SC, Truffle, Ethereum Blockchain, and Python
9	MetaMask	MetaMask is a cryptocurrency wallet made specifically for tokens on the Ethereum blockchain
10	MoE	Ministry of Education
11	PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
12	PoA	Proof-of-Authority
13	PoS	Proof-of-Stake
14	PoW	Proof-of-Work
15	SC	Smart Contract