Kirkuk University Journal-Scientific Studies Vol. 18, Iss. 1, p 62-75, 2023. doi:10.32894/kujss.2023.135876.1072

Review: Verification Process of Academic Certificates Using Blockchain Technology

Abdulkareem Saber Kareem*, Ahmed Chalak Shakir

Department of Computer Science, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq.
*Corresponding author : stcha010@uokirkuk.edu.iq.

Article Information

Article Type:
Review Article

Keywords:
Blockchain; Academic certificate; Smart contract; Decentralization; Verification.

History:
Received: 12 September 2022.
Accepted: 29 January 2022.
Published: 31 March 2023.

Citation: Abdulkareem Saber Kareem, Ahmed Chalak Shakir, Review: Verification Process of Academic Certificates Using Blockchain Technology, Kirkuk University Journal-Scientific Studies, 18(1), 62-75, 2023, https://doi.org/10.32894/kujss.2023.135876.1072

Abstract

The rapid advances in Blockchain technology have impacted various areas, including financial, healthcare, and supply chain systems. Due to its unique characteristics, such as decentralization, trustworthiness, and security, this technology has recently been used in education, particularly in the verification of academic certificates. A certificate from an academic institution is a crucial document that could give someone access to new prospects. It frequently serves as a great starting point for choosing candidates during the recruitment process. Due to the lack of an effective anti-forging mechanism, academic certificates are vulnerable to fraud, forgery, and imitation. To combat this trend, educational institutions have implemented methods that often entail a third party verifying the legitimacy of academic certificates. A review of reference studies was conducted for this purpose. Many databases and papers that focused on blockchain in academic certificate verification and made important contributions rather than just making general statements about the topic were chosen. This paper investigates the benefits and challenges of blockchain technology in academic certificate verification. In the results obtained, it has been suggested that while blockchain technology in academic degree verification is still a new field, it holds a lot of promise for the academic certificate verification process as a whole. Finally, to avoid fake documents, this review paper focuses on papers related to the Academic Certificate Authenticity System (ACAS) using blockchain technology.

1. Introduction:

Educational certificates are crucial credentials for students and graduates, provided by educational institutions. Proof of learning and eligibility to pursue further education and employment Because of developments in information technology and the availability of low- and high-cost equipment, fraudulent access to vital papers such as identification cards, certificates, and passports is conceivable. Traditional document verification is expensive, and the time-consuming human involvement procedure may lead to academic credential fraud [1]. Academic certifications are highly prized since they serve as an indicator of the bearer's human capital. Human capital can be defined as knowledge, talents, capabilities, and aptitudes acquired via education. Academic credentials are particularly significant in the workplace since they ensure not only the holders' knowledge, competence, and skills but also their abilities, reliability, and devotion. According to the bearers, there is a link between higher educational attainment, greater career chances, and financial stability. Academic qualifications are considered authentic when they are given by a university that is legally allowed to award such diplomas [2]. Students who have fulfilled all of the criteria for graduation get certificates from their institutions. Because an electronic document cannot effectively replace a physical certificate, most graduation certificates are paper-based documents [3]. The issues today with academic certificates in the form of paper-based documents are supported by corruption and the potential to easily fake and disseminate these certificates in

huge quantities, all of which make it impossible to authenticate them if necessary [4], [5], [6]. There are problems with the way that academic certifications are now issued and verified that revolve around the concept of trust. When fraudulent certificates are issued in the name of educational institutions, their reputation and brand are harmed. The validity and authenticity of academic certificates that potential candidates give to employers cannot be quickly and affordably verified. Due to this loophole, numerous instances of wrongdoing by unscrupulous parties have occurred [7]. The processes required to verify the authenticity of such certificates in the context of today's paper-based academic credentials are notoriously time-consuming and expensive, requiring a sizable workforce and expertise. Many authors have proposed the use of blockchain technology to accelerate academic credential issuance and verification to address this issue and improve the onerous and time-consuming administrative procedures surrounding certificates [8], [9]. The goal of this research is to add to the existing body of literature on the application of blockchain technology in academic certificate verification. Using a thorough review of the literature, we intend to apply technology to improve academic certificate management (issuance and verification). Finally, it explores the benefits and challenges of using such technology. By examining how blockchain technology is being applied to academic certificate verification, this study adds something new and timely to the academic certificate verification process literature. Universities, employers, students, and researchers who are interested in learning more about this cutting-edge technology and how it might have a significant impact on the academic certificate verification process are its main target audience.

2. Background:

2.1 Blockchain Technology:

Blockchain technology is a relatively new technology that has grabbed the curiosity of a wide range of stakeholders. Because of its popularity, Bitcoin was first associated with cryptocurrency exchanges [10]. Blockchain-based designs have been proposed for a wide range of applications, including sensor networks, the Internet of Things, smart cities, healthcare, education, and others [11]. A blockchain system is similar to a distributed registry, which acts as a shared database, synchronizing and validating all of its copies [12]. The term "blockchain" refers to the conceptual design of an electronic payment method relying on P2P networking, encryption, timestamp technology, and many other technologies. Blockchain technology is a decentralized database with five layers: data; network; consensus; incentive; contact; and application. Blockchain technology is characterized by decentralization, immutability, transparency, autonomy, protection, and confidentiality. The blockchain's most notable and critical feature is decentralization, which means that blockchain technology does not require the usage of any trusted third-party organizations and that each node in the network stores all of the network's transaction data [13]. The blockchain uses cryptography, a sort of mathematics, to prevent records from being forged or hacked [14]. Cryptographic algorithms are used to safeguard information and information systems and to protect the confidentiality of sensitive data in cyberspace [15]. The term "blockchain" refers to a collection of blocks, each of which holds information about the past, present, and future of the system. Each block plays a key role in linking with the previous and following blocks as soon as it enters the system to become a member of the chain. The fundamental purpose of each block is to record, validate, and distribute transactions to other blocks. This means that deleting or changing a block in the chain would have an impact on the next block in the chain [16]. Six essential components make up a blockchain [17], as follows:

* **Decentralized:** Each node may record, store, and update the ledger, and together they make up the blockchain. Therefore, it is no longer necessary for the blockchain to depend on a single centralized node like a master node.

* **Transparent:** Each node sees the data from the block that was spread across the other linked nodes and recorded by each node, resulting in transparency between the nodes.

* **Open Source:** The bulk of blockchain systems are open to the public; transactions can be reviewed by anybody, and anyone can use blockchain technologies to create any program they want.

* **Autonomy:** The concept is to trust one person with the entire system, and no one can intervene because every node on the blockchain system can transfer or update data safely thanks to the consensus foundation.

* **Immutable:** All records are permanently saved and can't be updated unless someone manages to concurrently control more than 51% of the total number of nodes.

* **Anonymity:** Blockchain technologies have resolved the issue of node-to-node trust, allowing for anonymous data transmission or even transactions with the knowledge of the recipient's blockchain address.

2.2 Academic Certificates:

An academic certificate is a record that attests to the completion of a particular education program and/or provides proof that learning objectives were met. Academic certificates can be used for several things, including recognizing a student's successful completion of a particular learning experience, attaining a given excellence standard, or learning a certain quantity in a particular subject [18]. These documents are utilized

in three different procedures, such as issuing, sharing, and verifying [19]. An academic certificate is often a paper-based document because an electronic certificate cannot be used in place of a physical one [3]. Academic certifications are highly prized since they represent the holders' human capital. Human capital refers to the knowledge, abilities, skills, and competencies gained via education. Academic certificates are very important in job settings since they serve as a guarantee of the holders' abilities, reliability, and dedication, in addition to their knowledge, expertise, and other skills [20].

3. Methodology:

The guidelines established by Okoli and Schabram [21] were used to conduct this review. The subsections that follow clarify how these approaches were implemented in this review. This review was undertaken to gain an understanding of the range of research on academic certificate verification systems, to address review issues by understanding what is known about the topic, and to offer a theoretical framework for further investigation.

3.1 Research Question Formulation:

The following research questions were developed based on the goal of this study.

1. What Blockchain Elements Are Addressed in the Blockchain Application in Academic Certificate Verification?
2. What are the benefits of blockchain technology in academic certificate-verifying systems?
3. What challenges exist in implementing blockchain technology in systems that validate academic certificates?

3.2 Search Strategy:

Significant scientific databases like IEEE Xplore, Springer, Google Scholar, the ACM Digital Library, Elsevier ScienceDirect, and the Web of Sciences are used in this work. As for keywords, blockchain and smart contracts, as well as academic certificate verification, are employed. 201 papers were shown as search results until August 2022. A total of 20 related publications were chosen as the most related research based on the main contributions of these papers. It does not evaluate research articles that are only focused on blockchain finance and blockchain law. However, it analyzes all the papers and finds two obvious key points. On one hand, because the total number of publications is still limited, the topic of blockchain in the sphere of academic certificate verification is new. On the other hand, academic certificate verification research contributions have grown year after year, indicating that this study issue is both necessary and promising. A taxonomy for the problem of academic certificate verification is proposed in this work.

3.3 Inclusion and Exclusion of Articles:

This stage comprises choosing acceptable publications to aid in addressing the research questions. To accomplish this, a set of inclusion and exclusion criteria, as shown in Table 1, have been developed:

Table 1. Inclusion and Exclusion Criteria for Related Publications.

Criteria for exclusion	Criteria for inclusion
Non-English studies	The whole text can be found online.
Book reviews, white papers, and editorial comments	Journal and Conference
studies published before 2018	Studies published from 2018 up to the date we performed this review (the last five years)

By filtering studies based on title and abstract, it is possible to reject duplicate articles and articles related to the application of blockchain technology, which is not used in the field of academic certification management. However, some articles were rejected because the full text could not be accessed. The search selection process resulted in this review. 181 papers out of 201 were excluded, and 20 relevant publications were investigated.

3.4 Data Extraction:

Data extraction was used on studies after they were selected. The suitable data was picked from the shortlisted main studies focusing on blockchain-based academic certificate management initiatives and fundamental characteristics, followed by identified projects at this level. After that, the data was analyzed. The academic certificate programs were covered by 20 primary studies: [2], [4], [20], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], and [38].

3.5 Data Analysis:

Information was extracted from the included studies using an extraction form. The form was created specifically for this evaluation and was tested across all work. The five items on the form are listed in Table 1.

Data analysis was done after the data from the papers had been extracted. Four key themes that were already defined and derived from the study questions were used to examine the retrieved data. The themes covered elements, benefits, and challenges.

4. Result:

Fig.1 displays the number of studies that were found, screened, and either accepted or rejected at each stage of the selection

Table 2. Extracted Data from Items Are Displayed.

Item of Data	Definition
Title	The paper's title
Year	The year of publishing
Author(s)	The name of the author(s)
Country	The home country of the researcher(s)
Type	Journal / Conference

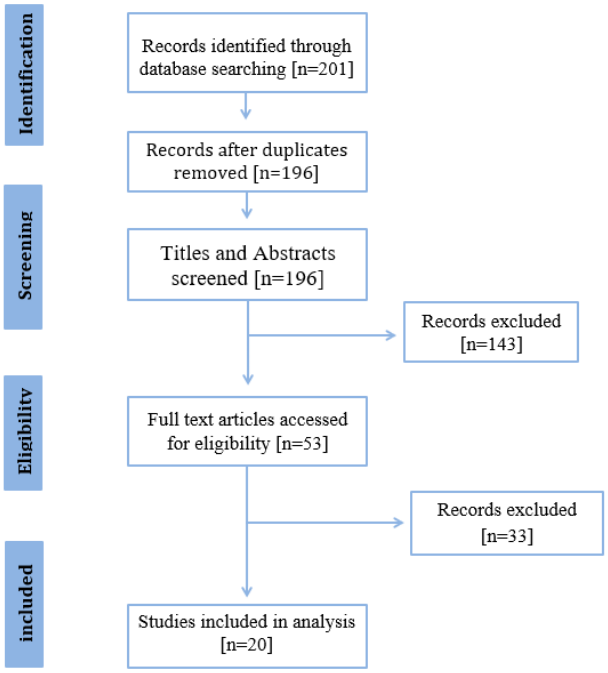

Figure 1. Review Process Diagram.

process. Five of the 201 articles that were extracted in total from the nine chosen electronic databases were eliminated due to duplication. Then, 143 were disqualified when their titles and abstracts were scrutinized. At this point, 53 articles had been examined for the full-text review, and 33 had been deleted after the full-text versions had been read as they lacked sufficient information for the review. Twenty publications were ultimately selected for this review and included in the data extraction procedure.

4.1 Year of Publication as well as Geographic Distribution:

Some ground-breaking papers have been published to examine the adoption of blockchain for academic certificate verification. Twenty research publications promoting blockchain integration with academic degrees have been published. One of the 20 scientific publications was published in 2018, another in 2019, and the final nine were published in 2021. 2022,

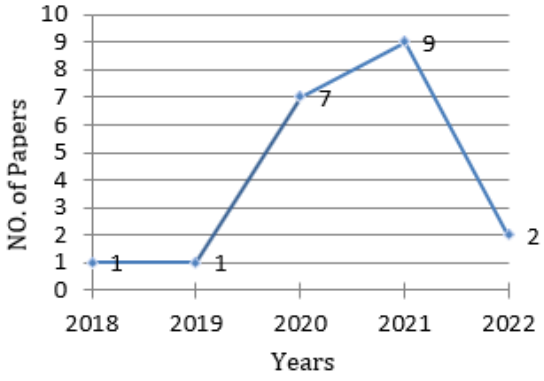

Figure 2. The Selected Papers' Publishing Year.

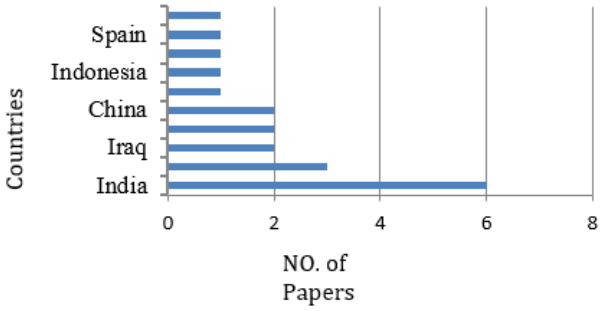

Figure 3. The Included Papers' Geographic Distribution.

however, indicates a decline with two items, given that the data collection occurred around May 2022. This suggests that efforts to apply blockchain technology to the area of examining academic credentials are just beginning. Fig 2 illustrates the distribution of articles by year of publication.

Figure 3 demonstrates that publications came from India (30%, n = 6), Malaysia (15%, n = 3), Iraq (10%, n = 2), Portugal (10%, n = 2), China (10%, n = 2), and the rest of the countries, for each of which only one paper was published. It appears from the table that India (6) contributed the most, followed by Malaysia (3), Iraq (4), and China (2). Finally, North Macedonia, Indonesia, Bangladesh, Spain, and KSA each produced one.

4.2 The Venues for Publication:

Fig.4 illustrates the distribution of publications by venues. The bulk (16) were published in journal publications, with four being conference proceedings.

4.3 Summary Explanation of Studies:

A synopsis of each publication is provided in this section, along with any blockchain technology used by the author or authors. An explanation of each publication is presented in

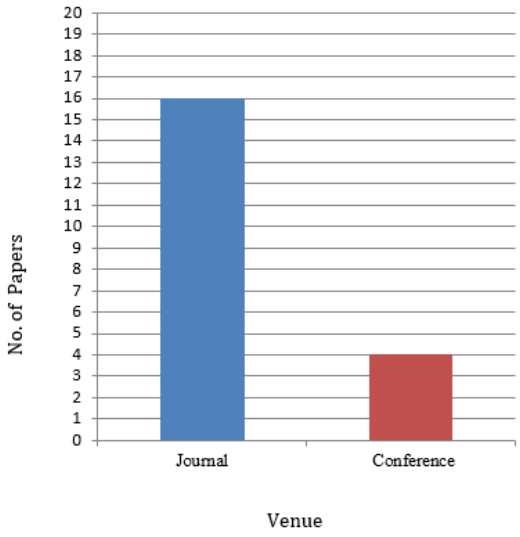

Figure 4. The Articles Distribution by Publication Venues.

Table 3.

4.4 The challenges we face in using blockchain technology for academic certification verification:

Challenges determine the characteristics of blockchain adoption, such as privacy, immutability, immaturity, security, and data unavailability.

Privacy:

It is difficult but essential to ensure privacy while ensuring security on the blockchain, especially when a learner's academic certificates are at risk [39]. three of the articles chosen for this review [39], [40], and [36] addressed privacy concerns in the academic certificate verification system setting. Nowadays, many educational institutions follow stringent privacy regulations that are required by law. Students have faith in the people who handle their data. But if all of this data is recorded in a public ledger, it will no longer be seen as private. Public blockchains are ineffective for keeping this data in this case, even when encrypted [40]. As a result, a private blockchain or consortium may be advantageous, where students would only have limited access and all of their personal information would be kept private, as it should be [36]. Despite this, there are several laws for protecting personal information in different nations that should be taken into account. The European General Data Protection Regulation (GDPR) [39], for instance, places considerable restrictions on the preservation of personal data in unaltered storage systems like blockchains [41].

Immutability:

A crucial aspect of blockchain technology is immutability, which refers to the inability to change the data recorded in the blocks [41]. According to two publications [37], [20], the immutability property would have two disadvantages when used with the academic certificate verification process. It eliminates the option for some students to amend their academic certificates for justifiable reasons. In addition, certificates stored on the blockchain cannot be deleted in the event of certificate revocation [37], [20].

Immaturity:

Another challenge is caused by how young blockchain technology is. According to one publication [22], there are some immaturity issues with blockchain. Ensuring decentralization is the main architectural difficulty in software engineering. By operating over a vast number of nodes without any central oversight, a permissionless blockchain like Ethereum offers a high level of decentralization (except for new software versions that, however, can be installed by the participants in their nodes) [22].

Security:

According to four publications [25], [29], [32], and [40], security is still a difficult problem, even though blockchain is renowned for its security and the community's efforts to make the platform reliable and safe [29]. Due to the usage of distributed ledger technology (DSLT) by several academic institutions around the globe, security must be prioritized, and blockchain security and vulnerabilities must be taken into account. The application of blockchain in education: GDPR-compliant and scalable certification and verification of academic information addressed several blockchain security vulnerabilities that might have an impact on the academic certificate verification process [39].

Table 3. The Explanation of Related Studies.

Reference	Explanation
Saleh et al [2]	They suggested the Hyperledger Fabric Framework as a blockchain-based framework for certifying educational certificates with a focus on authentication, authorization, confidentiality, privacy, and ownership.
Leka and Selimi [4]	They suggested a system that uses blockchain to distribute academic certifications and covers all the key elements of blockchain, including traceability, provenance, certification, and authentication. It provides value and speeds up the process of providing certificates in educational institutions.
Ghazali [20]	To improve the verification process, a blockchain-based paradigm for diploma verification was put forth in this study. The suggested paradigm offers several advantages to customers, recipients, and issuing bodies. The benefit of the suggested paradigm is that the blockchain itself hosts all the data needed to authenticate and validate the certificate. The suggested methodology will be put into practice and used in a few different educational institutions for future work. It will be upgraded to use smart contracts in the future.
Serranito et al [22]	They make use of blockchain technology and smart contracts to establish a decentralized verification solution for higher education credentials, such as university diplomas. The five main parts of the solution are used to implement it: the HEI client, the consortium app, the recruiting app, the consortium smart contract, and the HEI smart contract.
Billah et al [23]	Based on the technology used in this study, they created a blockchain certificate system. The system's application is run by the EVM and was created on the Ethereum platform.
Alam et al [24]	This study would provide a thorough examination of blockchain security, privacy, and trust. It investigates the challenges and further applications of blockchain technology in the field of education. Finally, it suggests a blockchain-based framework for the dependable and safe maintenance of student records.
Liu et al [25]	They propose a system that suggests a secure control technique for blockchains' digital certificate-based data access. The suggested solution creates a safe authentication mechanism for privacy data in blockchains without confirming the encrypted identity signature of the third-party participant by fusing blockchain and digital certificate technology. The fair contract signing of multiple signers via blockchain is supported by the high-efficiency network forwarding mechanism suggested in this work.
Farouk et al [26]	In this study, the authors built a website using blockchain technology integrated as a class data storage feature and user-owned digital certificates. Users can select which class to take on the website page that will be built, which is an online classroom. Users who enrol in a class are required to finish several assignments and exams in that class to receive a digital certificate. Users first need to have an Ethereum account or wallet to enrol in a class.

Continued on next page

Reference	Explanation
Ali and Bhaya [27]	The authors of this study introduced a blockchain-based architecture that intends to offer certificates that are simple to apply for, distribute, and verify with a third party. To decrease certificate forgery, the mechanism of the suggested model suggests permanent, distributed hash records of students' credentials in higher education. Also, they discussed the advantages, features, opportunities, and difficulties associated with using this paradigm in higher education.
Dalal et al [28]	In this study, the authors used blockchain technology in the educational space to propose the use of biometrics to verify student identities and academic credentials. A security layer was added to the database using blockchain technology. The blockchain was implemented using the Ethereum platform.
Maulani et al [29]	This study explains how digital certificates using blockchain technology are secure. Blockchain technology's security feature for spotting false certificates is currently well-known and pervasive. The availability of blockchain technology is a technology that can be practical, can offer a solution to present issues, and is also very beneficial for community activities.
Take and Rokade [30]	The authors' goal for this project is to create a system for the dynamic and secure creation of electronic certificates using smart contracts in a blockchain context. An example of a distributed, open-source blockchain platform with a proprietary mining technique and a smart contract The suggested method generates dynamic QR codes and individual certificates for each student's document.
Lamkoti et al [31]	In this study, with the help of distributed technologies such as Ethereum smart contracts and IPFS, their proposed approach makes it easy to verify the authenticity of a document as well as its integrity and authenticity.
Rama Reddy et al Li et al [32]	Their proposed system is a blockchain consortium consisting of universities, the institutions they belong to, independent colleges, and corporations. Universities usually add students' degrees first, after which companies or other validators can verify the credentials with the student's Aadhar number or certificate transaction ID.
Li et al [33]	Using a combination of public and private blockchains, the authors of this paper propose a blockchain system for e-learning assessment and certification. This system includes four distinct smart contract schemes for the implementation of e-learning assessment and credit exchange; digital certificate issuance and secure storage; digital certificate verification; and e-learning voucher allocation, respectively.
Ghani et al [34]	The authors of this paper have suggested and put into practice an electronic system for distributing certificates. The Hyperledger private blockchain was used to develop the system. In just a few seconds, hundreds of transactions can be uploaded to the blockchain. The certifications were secured and managed by the proposed system using hashing and smart contracts.

Continued on next page

Reference	Explanation
Sarganachari et al [35]	The authors suggested a system that uses blockchain technology to digitize both the production and verification of degree certificates. The authors take advantage of the Hyperledger fabric, a modular blockchain platform that serves as a base for creating blockchain-based goods, solutions, and applications using plug-and-play components, to create digital scores and mark cards.
Delgado-Von-eitzen et al [36]	In this study, the authors investigate problems associated with the use of blockchain technology to create and verify educational data and suggest a creative way to address them. Their proposed model complies with current laws, protects the privacy of users' data, and supports the issuance, storage, and verification of various types of academic materials, both formal and informal.
Vidal et al [37]	They suggest a higher education application that issues academic certifications using the blockchain and includes a way to withdraw any digital diplomas that may have been created inadvertently.
Hargude et al [38]	The authors of this study have identified the security topics needed for blockchain document verification. This study also identifies the weaknesses and openings in the current blockchain-based system for verifying educational certificates. The system will also generate a linked QR code and an inquiry string code. Through mobile phone scanning or website searches, it will enable the demand unit to confirm the legitimacy of the paper certificate.
End of Table	

Data Unavailability:

The unavailability of data is a further issue mentioned in three articles [39], [20], and [31]. Data management in the hands of users runs the risk of making the data unavailable and having an impact on the applications that depend on it. Additionally, the ownership rights of student data are ambiguous [30] because of the distributed ledger and the decentralized nature of the blockchain. Currently, data handling is the responsibility of the academic institution's administration division. However, the blockchain minimizes the duties of the management department because all data is stored there. Then, fresh problems appear: who is the owner of the digital data? Who has the right to utilize it? Who has access to the findings of the data analysis? [31].

5. Discussion:

In this section, answers to research questions are systematically presented, and what can be learned from the literature about blockchain in academic certificate verification is discussed.

5.1 Addressed Elements by Blockchain:

Instead of being stored by a central authority, blockchain-based academic certification studies are completely decentralized. Data from academic certificate initiatives will be stored on a decentralized blockchain network, ensuring system transparency and independence. Because a blockchain is an open source of data, the data must be preserved in a trustworthy and correct manner. In addition, the project's decentralized management system would allow institutions or employers to validate original certificates with a single click, rather than having to go through the time-consuming and technical process of confirming each certification individually. Another requirement typically addressed in academic certification verification case studies is immutability, which entails the ability to disable the ability and make modifications to initial or earlier data. This feature is supported by cryptographic security in distributed ledgers and is the most expensive part of blockchains since it requires technology such as databases, distribution, and hashing to ensure that the data does not change. Several blockchain elements are especially addressed in academic certificate verification, according to the full analysis. For example, traceability (the ability to monitor certificates) is addressed in 19 of the 20 case studies examined. Traceability, when combined with transparency, improves certificate visibility while also ensuring certificate security, aiding in certificate verification. Stakeholders can efficiently track transactions by accessing data records with time stamps. As evidenced by 53 studies, transparency, on the other hand, allows stakeholders to monitor and access data across the supply chain. Transparency allows validating and auditing distributed ledger elements by allowing access to activity history. Academic certificate verification case studies also address security, efficiency, and confidentiality as blockchain benefits. Cyber security refers to cyber security procedures that prevent unauthorized parties from gaining access to data, either intentionally or unintentionally. In academic degree verification processes, the great level of difficulty in modifying data on blockchains is critical. Efficiency refers to the elimination of needless costs, bureaucracy, and intermediaries. Academic credential verification processes are made more efficient by faster data handling, simpler accessibility, and the removal of geographical limits. On the other hand, confidentiality relates to the protection of users' personal information and data, as well as some aspects of their transactions. In academic certificate verification processes, this feature is difficult to balance with transparency and traceability, but with blockchains, stakeholders may prefer a private, permissioned blockchain alternative to limit the monitoring and control operations in the blockchain. Censorship The term "resistant" refers to data that has not been altered or rewritten. Every transaction, however, is visible to everyone. However, given its anonymity features, SGE can filter the transaction. Finally, trust is the result of all of the aforementioned characteristics of blockchain applications in academic certificate verification. The capacity of blockchain to remove untrustworthy parties while allowing information exchange, immutability, visibility, and automation establishes confidence. Stakeholder trust in traditional academic degree verification processes is built through transactions, whereas trust in blockchain-based academic degree verification processes is built through blockchain distributed ledger accounting. Blockchains can fundamentally enhance transactions between parties in an environment where trust is low. Blockchain-based "smart contracts" are computer protocols designed to make contracts easier to create, verify, and enforce. As a result, the blockchain enables the execution of a conditional contract without the involvement of a third party. These smart contracts can be tracked in the blockchain ledger just like transactions, and they cannot be undone. A smart contract may be thought of as any generic computation that is being done on the blockchain and can be any type of software in its current form, which is used by platforms like Ethereum and Hyperledger. The benefits it offered for cryptocurrencies were its capabilities for repeatability and contracted execution. However, some research has revealed that some smart contracts, like Ethereum, have ambiguities in their contract language that could lead to flaws and, as a result, raise security issues [42].

5.2 Benefits of Blockchain Technology:

Blockchain technology is an intriguing new field of developing technology with a lot of potential for the academic certificate verification system. The benefits of blockchain technology in academic certificate-verifying systems range from data management to data verification without jeopardizing authenticity. The blockchain data is accessible and verifiable around

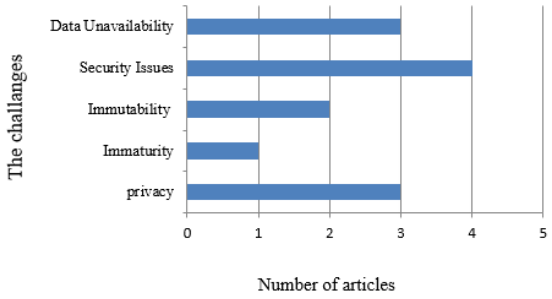

Figure 5. Challenges in Adopting Blockchain Technology.

the clock, with complete openness. Blockchain technology is commonly utilized for the issue and verification of educational certificates such as degrees, transcripts, and students' skills, achievements, and professional abilities that can be confirmed by employers all over the world [43]. The certification procedure is streamlined thanks to blockchain technology, and employers will spend less time verifying academic findings. It serves the education industry by offering a secure platform for sharing student data, increasing confidence, lowering costs, and increasing transparency. Blockchain technology retains a complete record of the transaction in data blocks that are sequentially ordered by timestamps. The cryptographic algorithm avoids data tampering and fraud by preventing the deletion of old and new data blocks [44]. It creates a virtual infrastructure for document storage and handles students' credentials and achievement records for the rest of their lives, minimizing administrative expenses and bureaucratic procedures for universities [45].

In a variety of fields, blockchain technology is critical for addressing scalability issues, privacy concerns, and reliability issues [46]. High security, better control over data access, trust, low cost, identity verification, effective data administration, interactivity, system interoperability, accountability, and transparency are advantages of blockchain technology for an academic certificate-verifying system. Blockchain technology will permanently and safely end the paper-based system for universities [43].

5.3 Challenges in Adopting Blockchain Technology:

Reviewing published literature describing the challenges of utilizing blockchain technology for the authentication of academic certificates was one goal of this study. These issues have been broken down into five categories: privacy, immaturity, immutability, security, and data unavailability (Fig 5 illustrates).

Firstly, this analysis revealed that while academics have concentrated on privacy-preserving methods, few articles have taken into account the significance of adhering to data protection legislation like the CCPA and GDPR. Furthermore, educational institutions can improve their chances of deploying blockchain systems that abide by data protection rules in addition to using the right privacy-preserving technologies. For instance, they might try to determine whether a blockchain is necessary to achieve a certain academic, commercial, or social goal, or they might adopt permissioned blockchains with more onerous usage guidelines.

Secondly, one of the obstacles to blockchain adoption in certificate verification is immaturity. This analysis revealed that one of the articles under consideration stated that blockchain still has certain immaturity issues from various perspectives, such as the poor usability of blockchain-based apps and solutions. Usability was not the primary concern of the chosen article, which gave greater attention to other concerns like security and privacy. Therefore, new user-friendly interfaces that better match user needs should be implemented to increase the use of blockchain, and administrative personnel, academics, and students should all receive training on how to use the technology. Thirdly, a crucial aspect of blockchain technology is the impossibility of changing the data stored in the blocks, which constitutes blockchain's immutability. However, according to four of the articles under evaluation, immutability is a major obstacle to the use of blockchain technology for academic certificate verification systems. For example, if a diploma is revoked, the certificates stored on the blockchain cannot be changed. Because of this, immutability can limit the use of blockchain for sensitive student data, such as in admissions, certificate or degree verification, and exams or assessments that call for the power to revoke. In this sense, a framework's capacity to scale and function efficiently is impacted by the need for ongoing system improvements. Therefore, more investigation is required into the compromise between adaptability and resource conservation. Fourthly, despite being a safe technology, blockchain is nevertheless vulnerable to security breaches. Four of the articles under evaluation addressed various blockchain security vulnerabilities that might have an impact on the academic certificate verification process. However, a thorough examination of these attacks is necessary. Researchers should categorize attacks more specifically and conduct more analyses and simulations of potential attacks. This will strengthen reliability and offer a safe foundation for the use of blockchain technology in the future. Finally, for transparent and decentralized data storage, blockchain technology is the ideal solution. It also permits open data access, and its immutability strengthens it. However, as stated in the two articles, because distributed ledger technology does not function as a pure database, there are some issues with blockchain data availability. Performance and bandwidth issues arise when requesting data from a blockchain. The main reason for this is that, unlike other conventional databases, blockchains lack an initial query language. The distributed nature of blockchain also presents a challenge in this situation.

Table 4. Lists the Most Frequent Blockchain Features Found in These Studies.

				Features Are Used in These Studies.									
Refs.	Publishing Year	Country	Publication Venues	Decentralize	Immutability	Traceability	Transparency	Security	Efficiency	Confidentiality	Censorships Resistant	Trust	Smart contract
[2]	2020	Malaysia	Journal	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗
[4]	2020	N.Macedonia	Journal	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
[20]	2018	Malaysia	Journal	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓
[22]	2020	Portugal	Conference	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
[23]	2021	Bangladesh	Conference	✓	✓	✓	✗	✓	✗	✗	✓	✓	✓
[24]	2021	KSA	Journal	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗
[25]	2020	China	Journal	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗
[26]	2022	Indonesia	Journal	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗
[27]	2021	Iraq	Journal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[28]	2020	India	Journal	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
[29]	2021	Malaysia	Journal	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗
[30]	2021	India	Journal	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓
[31]	2021	India	Journal	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓
[32]	2021	India	Journal	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗
[33]	2019	China	Conference	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗
[4]	2022	Iraq	Journal	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓
[35]	2020	India	Journal	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓
[36]	2021	Spain	Journal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[37]	2020	Portugal	Conference	✓	✓	✗	✗	✓	✗	✗	✗	✓	✓
[38]	2021	India	Journal	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗
		Total		20	20	19	14	19	10	9	18	16	12

6. Conclusions:

Blockchain technology delivers decentralized, secure, dependable, and transparent systems and provides a distributed ledger that is encrypted. In this paper, the contributions of blockchain to the Academic Certificate Authentication System (ACAS) are described. The blockchain elements also identify and discuss what is relevant to the academic certificate verification application. This review reviews 20 studies and discusses the potential advantages and difficulties they can bring to the system. The paper contributes to the existing body of knowledge by highlighting the current development, benefits, challenges, and application of blockchain technology in the Academic Certificate Authenticity System (ACAS). Concerning the current developments, there has been an increasing trend in the number of publications and citations in the field. In addition, India has the most publications, followed by Malaysia, Iraq, Portugal, and China. The study also concludes that the use of blockchain for credential administration is still in its infancy. However, scalability, security, and cost remain the main barriers and need attention from professionals in the field. In conclusion, our contribution is a thorough analysis of previous research on the use of blockchain in academic certificate verification, together with a discussion of the major difficulties. These revelations will help scholars comprehend the primary research areas and find new research avenues. The suggested framework will be put into practice in the academic certificate verification system and adopted by a few academic institutions to guide future work.

Funding: None.

Data Availability Statement: All of the data supporting the findings of the presented study are available from corresponding author on request.

Declarations:

Conflict of interest: The authors declare that they have no conflict of interest.

Ethical approval: The manuscript has not been published or submitted to another journal, nor is it under review.

References

[1] Smartcert blockchain imperative for educational certificates. 2019, doi:10.1109/JEEIT.2019.8717505.

[2] O. S. Saleh, O. Ghazali, and M. E. Rana. Blockchain based framework for educational certificates verification. *Journal of Critical Reviews*, 7(3): 79–84, 2020,doi:10.31838/jcr.07.03.13.

[3] M. Warasart and P. Kuacharoen. Paper-based document authentication using digital signature and qr code. *4th International Conference on Communication Engineering and Computer Science*, 40: 94–98, 2012, doi:10.1007/s00397-008-0296-x.

[4] E. Leka and B. Selimi. Bcert-a decentralized academic certificate system distribution using blockchain technology. *International Journal on Information Technologies and Security*, 12(4): 103–118, 2020, 10.24237/djps.1402.403B.

[5] J. Hallak and M. Poisson. *Corrupt Schools, Corrupt Universities: What Can be Done?* UNESCO Publishing, 1st edition, 2007, doi:10.1007/s00397-006-0148-5.

[6] R. H. Sayed. Potential of blockchain technology to solve fake diploma problem. *University of JyväskyläDepartment of Computer Science and Information Systems*, 2-65, 2019.

[7] F. Rhodes. Blockchain certificates: a prototype implementation for digitising educational certificates. *Journal of Chemical Physics*, 55,(393): 298–305, 1971, doi:10.2307/3615019.

[8] A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar, and P. C. K. Hung. A permissioned blockchain-based system for verification of academic records. 10^{th} *IFIP International Conference on New Technologies, Mobility and Security*, 1–5, 2019, doi:10.1109/NTMS.2019.8763831.

[9] A. Ghaffar and M. Hussain. Bceap – a blockchain embedded academic paradigm to augment legacy education through application. *International Conference Proceedings Series*, 2019, doi:10.1145/3341325.3342036.

[10] N. T. Courtois, K. T. Gradon, and K. Schmeh. Crypto currency regulation and law enforcement perspectives. *arxiv,* `http://arxiv.org/abs/2109.01047`, 38, 2021.

[11] W. S. Melo, A. Bessani, N. Neves, A. O. Santin, and L. F. R. C. Carmo. Using blockchains to implement distributed measuring systems. *IEEE Transactions on Instrumentation and Measurement*, 68(5): 1503–1514, 2011, doi:10.1109/TIM.2019.2898013.

[12] A. K. Shrestha, J. Vassileva, and R. Deters. A blockchain platform for user data sharing ensuring user control and incentives. *Front. Blockchain*, 3: 1–22, 2020, doi:10.3389/fbloc.2020.497985.

[13] M. Li, L. Zeng, L. Zhao, R. Yang, D. An, and H. Fan. Blockchain-watermarking for compressive sensed images. *IEEE Access*, 9: 56457–56467, 2021, doi:10.1109/ACCESS.2021.3072196.

[14] K. Munim I. Islam and S. J. Oishwee. Blockchain-watermarking for compressive sensed images. *IEEE Access*, 8: 68333–68341, 2020, doi:10.1109/ACCESS.2020.2985647.

[15] A. Ahmad. A new security method for the internet of things based on ciphering and deciphering algorithms. *Kirkuk University Journal-Scientific Studies*, 13(3): 154–174, 2018, doi:10.32894/kujss.2018.13.3.12.

[16] A. Khatoon. A blockchain-based smart contract system for healthcare management. *Electron*, 9(1): 154–174, 2020, doi:10.3390/electronics9010094.

[17] I. C. Lin and T. C. Liao. A survey of blockchain security issues and challenges. *International Journal of Network Security*, 19(5): 653–659, 2017, doi:10.6633/IJNS.201709.

[18] D. T. Serranito. *A Blockchain-based Platform for Sharing and Verifying Education Certificates*. techno lisboa, 2020.

[19] A.Grech and A. F. Camilleri. Blockchain in education, 2017.

[20] O. Ghazali. A graduation certificate verification model via utilization of the blockchain technology. *Journal of Telecommunication, Electronic and Computer Engineering*, 10(3), 2018.

[21] C. Okoli and K. Schabram. Working papers on information systems a guide to conducting a systematic literature review of information systems research. *Social Science Research Network*, 10(2010), 2020, doi:10.2139/ssrn.1954824.

[22] D. Serranito, A. Vasconcelos, S. Guerreiro, and M. Correia. Blockchain ecosystem for verifiable qualifications. 2^{ed} *Conference on Blockchain Research Applications for Innovative Networks and Services*, 192–199, 2020, doi:10.1109/BRAINS49436.2020.9223305.

[23] S. N. Billah, R. Pollobe, F. Hossain, N. M. Abir, A. Z. Zarin, and M. F. Mridha. Blockchain-based architecture for certificate authentication. *Social Science Research Network*, 10, 2021, doi:10.2139/ssrn.3842788.

[24] S. Alam, H. Abdullah, Y. Ayoub, R. Abdulhaq, A. Alshaikh, and A. Hayawi. A blockchain-based framework for secure educational credentials. *Turkish Journal of Computer and Mathematics Education*, 12(10): 5157–5167, 2021.

[25] B. Liu, L. Xiao, J. Long, M. Tang, and O. Hosam. Secure digital certificate-based data access control scheme in blockchain. *IEEE Access*, 8: 91751–91760, 2020, doi:10.1109/ACCESS.2020.2993921.

[26] S. A. Faaroek, A. Saulina Panjaitan, Z. Fauziah, and N. Septiani. Design and build academic website with digital certificate storage using blockchain technology. *IAIC Transactions on Sustainable Digital Innovation*, 3(2): 175–184, 2022, doi:10.34306/itsdi.v3i2.562.

[27] M. A. Ali and W. S. Bhaya. Higher education's certificates model based on blockchain technology. *Journal of Physics: Conference Series - IOPsciencen*, 1879(2), 2021, doi:10.1088/1742-6596/1879/2/022091.

[28] J. Dalal, M. Chaturvedi, H. Gandre, and S. Thombare. Verification of identity and educational certificates of students using biometric and blockchain. *Social Science Research Network Electron Journal*, 5, 2021, doi:10.2139/ssrn.3564638.

[29] G. Maulani, E. Ayu Nabila, and W. Yestina Sari. University raharja 1,4,5 university sangga buana 2 university utara malaysia 3. *Asosiasi Perguruan Tinggi Swasta Indonesia APTISI PUSAT*, 1: 136–150, 2021.

[30] S. N. Take and P. M. D. Rokade. Customized e-certification generation using blockchain technology for distributed framework. *International Journal of Computer Trends and Technology*, 4: 442–446, 2021.

[31] R. S. Lamkoti, D. Maji, A. Bharati Gondhalekar, and H. Shetty. Certificate verification using blockchain and generation of transcript. *International Journal of Computer Trends and Technology*, 10(3): 539–544, 2021.

[32] T. Rama Reddy, P. V. G. D. Prasad Reddy, R. Srinivas, C. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna. Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. *EURASIP Journal on Information Security*, 2021(1), 2021, doi:10.1186/s13635-021-00122-5.

[33] C. Li, J. Guo, G. Zhang, Y. Wang, Y. Sun, and R. Bie. A blockchain system for e-learning assessment and certification. *IEEE International Conference on Smart Internet of Things*, 212–219.

[34] R. F. Ghani, A. A. Salman, A. B. Khudhair, and L. Aljobouri. Blockchain-based student certificate management and system sharing using hyperledger fabric platform. *Periodicals of Engineering and Natural Sciences*, 10(2):207–218, 2022, doi:10.21533/pen.v10i2.2839.

[35] N. Sarganachari, A. Anjum, and S. IL Christa. Digital degrees and markcards using blockchain technology. *International Journal of Innovative Research in Science, Engineering and Technology*, 9(2):14038–14046, 2020.

[36] C. Delgado-Von-Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias. Application of blockchain in education: Gdpr-compliant and scalable certification and verification of academic information. *Applied Sciences*, 11(10):4537, 2021, doi:10.3390/app11104537.

[37] F. R. Vidal, F. Gouveia, and C. Soares. Revocation mechanisms for academic certificates stored on a blockchain. *Institute of Electrical and Electronics Engineers*, 24–27, 2020, doi:10.23919/CISTI49556.2020.9141088.

[38] R. Hargude, G. Ashutosh, A. Nawale, S. Adsure, and S. Engineer. Verification and validation of certificate using blockchain. *International Journal of Creative Reseacrh Thoughts*, 9(6): 714–718, 2021.

[39] F. Molina, G. Betarte, and C. Luna. A blockchain based and gdpr-compliant design of a system for digital education certificates. *arxiv,* `http://arxiv.org/abs/2010.12980`, 2020.

[40] M. Baldi, F. Chiaraluce, M. Kodra, and L. Spalazzi. Security analysis of a blockchain-based protocol for the certification of academic credentials. *CEUR Workshop Proceedings*, 2580:1–12, 2020.

[41] G. Capece, N. L. Ghiron, and F. Pasquale. Blockchain technology: Redefining trust for digital certificates. *MDPI*, 12(21): 1–12, 2020, doi:10.3390/su12218952.

[42] H. A. M. Deenmahomed, M. M. Didier, and R. K. Sungkur. The future of university education: Examination, transcript, and certificate system using blockchain. *Computer Applications in Engineering Education*, 29(5): 1234–1256, 2021, doi:10.1002/cae.22381.

[43] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani. Blockchain-based applications in education: A systematic review. *Applied Sciences*, 9(12): 2400, 2019.

[44] H. Sun, X. Wang, and X. Wang. Application of blockchain technology in online education. *International Journal of Emerging Technologies in Learning*, 13(10): 252–259, 2018, doi:10.3991/ijet.v13i10.9455.

[45] M. Jirgensons and J. Kapenieks. Blockchain and the future of digital learning credential assessment and management. *Journal of Teacher Education for Sustainability - Sciendo*, 20(1): 145–156, 2018, doi:10.2478/jtes-2018-0009.

[46] H. Malviya. How blockchain will defend iot. *Social Science Research Network*, 12, 2016, doi:10.2139/ssrn.2883711.

مراجعة : عملية التحقق من الشهادات الاكاديمية باستخدام تقنية بلوكجين

* عبدالكريم صابر كريم ، احمد جالاك شاكر

قسم علوم الحاسوب، كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة كركوك، كركوك، العراق.

* **الباحث المسؤول:** *stcha*010@*uokirkuk.edu.iq*

الخلاصة

كان للتقدم السريع الذي شهدته تقنية البلوكجين تأثير على مجموعة متنوعة من المجالات، بما في ذلك المالية، وأنظمة الرعاية الصحية، وأنظمة سلاسل الإمداد. وبسبب خصائصها الفريدة، مثل اللامركزية والجدارة بالثقة والأمن، استخدمت هذه التقنية مؤخرا في التعليم ، ولا سيما في التحقق من الشهادات الأكاديمية. فالشهادة التي تقدمها مؤسسة أكاديمية هي وثيقة حاسمة يمكن أن تتيح لأي شخص إمكانية الوصول إلى آفاق جديدة. وكثيراً ما يكون ذلك بمثابة نقطة انطلاق كبيرة لاختيار المرشحين خلال عملية التوظيف. وبسبب الافتقار إلى آلية فعالة لمكافحة التزوير فإن الشهادات الأكاديمية عرضة للغش والتزوير والتقليد. ولمكافحة هذا الاتجاه، نفذت المؤسسات التعليمية أساليب غالبا ما تستلزم قيام طرف ثالث بالتحقق من شرعية الشهادات الأكاديمية. وأجرء مراجعة للدراسات المرجعية لهذا الغرض. وتم اختبار العديد من قواعد البيانات والورقات التي ركزت على سد الثغرات في التحقق من الشهادات الأكاديمية التي قدمت إسهامات هامة بدلا من مجرد الإدلاء ببيانات عامة عن الموضوع. وتبحث هذه الورقة في فوائد تقنية البلوكجين والتحديات التي تواجهها في التحقق من الشهادات الأكاديمية. وفي النتائج التي تم الحصول عليها، أشير إلى أنه على الرغم من أن تقنية البلوكجين في مجال التحقق من الدرجة الأكاديمية لا تزال مجالا جديداً، فإن هذا المجال يطوى على كثير من الأمل بالنسبة لعملية التحقق من الشهادات الأكاديمية . وأخيراً، ولتجنب الوثائق المزورة، تركز ورقة المراجعة هذه على الأوراق المتعلقة بنظام أصالة الشهادات الأكاديمية (*ACAS*) باستخدام تقنية البلوكجين.

الكلمات الدالة: بلوكجين؛ الشهادة الأكاديمية؛ العقد الذكي؛ اللامركزية؛ التحقق.

التمويل: لايوجد.

بيان توفر البيانات: جميع البيانات الداعمة لنتائج الدراسة المقدمة يمكن طلبها من المؤلف المسؤول.

اقرارات:

تضارب المصالح: يقر المؤلفون أنه ليس لديهم تضارب في المصالح.

الموافقة الأخلاقية: لم يتم نشر المخطوطة أو تقديمها لمجلة أخرى، كما أنها ليست قيد المراجعة.