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.


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 authenti-
cate them if necessary [4], [5], [6]. There are problems with
the way that academic certifications are now issued and veri-
fi ed 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 au-
thenticity 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 re-
quired 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 ap-
ply 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. Universi-
ties, 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, in-
cluding 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, en-
ryption, 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 decen-
tralization, immutability, transparency, autonomy, protection,
and confidentiality. The blockchain’s most notable and critical
feature is decentralization, which means that blockchain tech-
nology 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 up-
date the ledger, and together they make up the blockchain.
Therefore, it is no longer necessary for the blockchain to de-
pend 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 comple-
tion 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, at-
taining a given excellence standard, or learning a certain quan-
tity 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, 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.

3.3 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>
<thead>
<tr>
<th>Criteria for exclusion</th>
<th>Criteria for inclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-English studies</td>
<td>The whole text can be found online.</td>
</tr>
<tr>
<td>Book reviews, white papers, and editorial comments</td>
<td>Journal and Conference studies published before 2018 up to the date we performed this review (the last five years)</td>
</tr>
</tbody>
</table>

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 process. The data shows a clear trend of increasing interest in academic certificate verification using blockchain technology.
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, 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

Table 2. Extracted Data from Items Are Displayed.

<table>
<thead>
<tr>
<th>Item of Data</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The paper’s title</td>
</tr>
<tr>
<td>Year</td>
<td>The year of publishing</td>
</tr>
<tr>
<td>Author(s)</td>
<td>The name of the author(s)</td>
</tr>
<tr>
<td>Country</td>
<td>The home country of the researcher(s)</td>
</tr>
<tr>
<td>Type</td>
<td>Journal / Conference</td>
</tr>
</tbody>
</table>

Figure 1. Review Process Diagram.

Figure 2. The Selected Papers’ Publishing Year.

Figure 3. The Included Papers’ Geographic Distribution.
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].

Security:

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 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 (DSL) 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].

Figure 4. The Articles Distribution by Publication Venues.
### Table 3. The Explanation of Related Studies.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saleh et al [2]</td>
<td>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.</td>
</tr>
<tr>
<td>Leka and Selimi [4]</td>
<td>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.</td>
</tr>
<tr>
<td>Ghazali [20]</td>
<td>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.</td>
</tr>
<tr>
<td>Serranito et al [22]</td>
<td>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.</td>
</tr>
<tr>
<td>Billah et al [23]</td>
<td>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.</td>
</tr>
<tr>
<td>Alam et al [24]</td>
<td>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.</td>
</tr>
<tr>
<td>Liu et al [25]</td>
<td>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.</td>
</tr>
<tr>
<td>Farouk et al [26]</td>
<td>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.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Reference</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ali and Bhaya [27]</td>
<td>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.</td>
</tr>
<tr>
<td>Dalal et al [28]</td>
<td>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.</td>
</tr>
<tr>
<td>Maulani et al [29]</td>
<td>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.</td>
</tr>
<tr>
<td>Take and Rokade [30]</td>
<td>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.</td>
</tr>
<tr>
<td>Lamkoti et al [31]</td>
<td>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.</td>
</tr>
<tr>
<td>Rama Reddy et al Li et al [32]</td>
<td>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.</td>
</tr>
<tr>
<td>Li et al [33]</td>
<td>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.</td>
</tr>
<tr>
<td>Ghani et al [34]</td>
<td>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.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Reference</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarganachari et al [35]</td>
<td>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.</td>
</tr>
<tr>
<td>Delgado-Von-eitzen et al [36]</td>
<td>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.</td>
</tr>
<tr>
<td>Vidal et al [37]</td>
<td>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.</td>
</tr>
<tr>
<td>Hargude et al [38]</td>
<td>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.</td>
</tr>
</tbody>
</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
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 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.

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

<table>
<thead>
<tr>
<th>Refs</th>
<th>Publishing Year</th>
<th>Country</th>
<th>Publication Venues</th>
<th>Decentralize</th>
<th>Immutability</th>
<th>Traceability</th>
<th>Transparency</th>
<th>Security</th>
<th>Efficiency</th>
<th>Confidentiality</th>
<th>Censorships Resistant</th>
<th>Trust</th>
<th>Smart contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>[22]</td>
<td>2020</td>
<td>Portugal</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[23]</td>
<td>2021</td>
<td>Bangladesh</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[26]</td>
<td>2020</td>
<td>Portugal</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[27]</td>
<td>2021</td>
<td>Malaysia</td>
<td>Journal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[28]</td>
<td>2020</td>
<td>Portugal</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[29]</td>
<td>2021</td>
<td>Portugal</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[30]</td>
<td>2021</td>
<td>Portugal</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[31]</td>
<td>2021</td>
<td>Portugal</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[32]</td>
<td>2021</td>
<td>Portugal</td>
<td>Conference</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[33]</td>
<td>2019</td>
<td>Malaysia</td>
<td>Journal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[34]</td>
<td>2021</td>
<td>India</td>
<td>Journal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[35]</td>
<td>2021</td>
<td>India</td>
<td>Journal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[36]</td>
<td>2021</td>
<td>India</td>
<td>Journal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[37]</td>
<td>2021</td>
<td>India</td>
<td>Journal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>[38]</td>
<td>2021</td>
<td>India</td>
<td>Journal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

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


مراجعة : عملية التحقق من الشهادات الأكاديمية باستخدام تقنية البلوكين

عبد الكريم صابر كريم ، احمد جلال شاكر
قسم علوم الحاسوب، كلية علوم الحاسوب وتكنولوجيا المعلومات، جامعة كركوك، كركوك، العراق.

الباحث المسؤول: stcha010@uokirkuk.edu.iq

المخلاصة

كان للتقدم السريع الذي تشهده تقنية البلوكين تأثير على مجموعة متنوعة من المجالات، بما في ذلك المالي، وأنظمة الرعاية الصحية، وأنظمة سلسلة الإمداد. وسبب عناصرها الفريدة، مثل اللامركزية والخبارية بالثقة والأمن، استخدمت هذه التقنية مؤخرًا 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 أفكار جديدة. وكثيراً ما يكون ذلك مثابة نقطة انطلاق كيية لاختيار المرشحين خلال عملية التوظيف. وسبب الافتقار إلى آلة فحالة للكشف عن الشهادات الأكاديمية عرضة للغش والتزوير والتقليد. ولكلفة هذا الاجتهاد، نفذت المؤسسات التعليمية أساليب غالباً ما تستخدم قيم ثقية ثالث بالتحقق من شرعية الشهادات الأكاديمية. وأجرت مراجعة للدراسات المرجعية لهذا الغرض. وتم اختيار العديد من قواعد البيانات والورقات التي ركزت على أدوات التشفير في التحقق من الشهادات الأكاديمية التي قدمت إجابات هامة بدلاً من مجرد الإجابة على بيانات عامة عن الموضوع. وبحث هذه الورقة في فوائد تقنية البلوكين والتحديات التي تواجهها في التحقق من شرعية الشهادات الأكاديمية. وفي النتائج التي تم الحصول عليها، أشير إلى أنه على الرغم من أن تقنية البلوكين في مجال التحقق من الدرجة الأكاديمية لا تزال محاولة جديًا، فإن هذا المجال يطوي على كثير من الأمل بالنسبة لعملية التحقق من الشهادات الأكاديمية. وأخيرًا، وتجنب الوثائق المزورة، تركز ورقة المراجعة هذه على الأوراق المتعلقة بنظام أصلية الشهادات الأكاديمية (ACAS) باستخدام تقنية البلوكين.

الكلمات الدالة: بلوكين; الشهادة الأكاديمية; العقد الذكي; اللامركزية; التحقق.

التمويل: لا يوجد.

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

إقرارات:

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

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