applied sciences

MDPI

*Article*

# NFTs for the Issuance and Validation of Academic Information That Complies with the GDPR

**Christian Delgado-von-Eitzen, Luis Anido-Rifón * and Manuel J. Fernández-Iglesias**

atlanTTic, University of Vigo, 36310 Vigo, Spain; christiandve@uvigo.es (C.D.-v.-E.); manolo@uvigo.es (M.J.F.-I.)
* Correspondence: lanido@det.uvigo.es

**Abstract:** The issuance and verification of academic certificates face significant challenges in the digital era. The proliferation of counterfeit credentials and the lack of a reliable, universally accepted system for issuing and validating them pose critical issues in the educational domain. Certificates, traditionally issued by centralized educational institutions using their proprietary systems, pose challenges for straightforward verification, generating uncertainty about the credibility of academic achievements. In addition to diplomas issued by academic entities, it is now necessary in virtually all professional fields to stay updated and obtain accreditation for certain skills or experiences, which is a determining factor in securing or enhancing employment. Yet, there is no platform available to consistently demonstrate these capabilities and experiences. This article introduces a novel model for issuing and verifying academic information using non-fungible tokens (NFTs) supported by blockchain technologies, focused on compliance with the General Data Protection Regulation (GDPR). It describes a model that grants control to the data subject, enabling the management of information access while adhering to key GDPR principles. Simultaneously, it remains compatible with existing systems within organizations, and is flexible in certifying various types of academic information. The implications of this model are discussed, emphasizing the importance of addressing privacy in blockchain-based applications.

**Keywords:** blockchain; education; General Data Protection Regulation; GDPR; non-fungible token; NFT; Soulbound token; SBT; academic information; lifelong learning; formal learning; informal learning

check for updates

**Citation:** Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. NFTs for the Issuance and Validation of Academic Information That Complies with the GDPR. *Appl. Sci.* **2024**, *14*, 706. https://doi.org/10.3390/app14020706

Academic Editor: David Megías

Received: 12 December 2023
Revised: 10 January 2024
Accepted: 12 January 2024
Published: 14 January 2024

**Correction Statement:** This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.

**Copyright:** © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

In the digital age, the issuing and verifying academic certificates face notable challenges. The widespread presence of counterfeit accreditations and the lack of a universally trusted system for issuing and verifying them create crucial issues within the educational domain. Certificates are traditionally issued by designated educational institutions through their proprietary information systems. Consequently, their confirmation or the validation of their information by external stakeholders is not easily or directly achievable. This could be due to various factors such as a lack of transparency, complex procedures, or limited access to the necessary data or validation methods, making it difficult to confirm the accuracy or validity of the information contained within the system, which in turn leads to doubts about the authenticity of academic accomplishments.

The absence of mechanisms to verify academic credentials fosters the emergence of degree mills [1] that sell false accreditations; the circulation of diplomas issued by non-existent academic institutions; unauthorized alterations to otherwise valid accreditations regarding course names, the syllabus, or duration, and the creation of false diplomas within academic institutions by dishonest employees [2]. Additionally, inaccurate translations of academic transcripts or diplomas in resumes may occur when applying for jobs in regions speaking a different language.

Beyond diplomas issued by academic bodies, maintaining up-to-date skills and accrediting specific competencies or experience has become imperative in almost every profession,

serving as a pivotal factor in securing or enhancing employment. However, at this time there are no dependable or trustworthy platforms where individuals can effectively showcase skills or abilities acquired outside of formal education or training, and therefore it is challenging to demonstrate these skills in a way that others can easily recognize or verify. While platforms like LinkedIn might seem to offer this feature, professionals often tend to exaggerate or falsify their skills to secure better job positions. The existence of a platform enabling not only information display but also easy verification, while adhering to data protection regulations, would significantly benefit qualified professionals, providing them with better opportunities.

The implementation of blockchain technology has been considered a promising solution to revolutionize the issuance and verification of academic information since 2013 [3]. However, its application to the educational domain is constrained by personal data protection requirements and compliance with regulations such as the General Data Protection Regulation (GDPR) in Europe [4], as discussed below.

The GDPR establishes fundamental principles to safeguard personal data within the European Union and for its citizens, encompassing the data present in academic certificates. Integrating blockchain technology in education poses challenges in complying with GDPR principles, as its design emphasizes data immutability and transparency. This poses a conflict with the GDPR's requirements [5] for data modification or deletion, such as the right to the erasure or rectification of inaccurate information. Ensuring the privacy of sensitive data, such as personal information in academic records, while maintaining the integrity of information on the blockchain, is a critical aspect when implementing this technology to support the issuance of educational certificates.

This research proposes an innovative solution, feasible with current technology, for issuing, storing, and verifying various types of academic information using a blockchain. The objective is to ensure compatibility with the information systems currently available, since expecting entities to upgrade their platforms to adapt to a new system, even if it is universally accepted, is unrealistic. Furthermore, the solution must be flexible enough to register any type of academic information (i.e., support both formal and informal learning), without being confined to specific formats.

A key and distinctive aspect of the proposed solution is its adherence to the constraints imposed by the GDPR in its design, a feature overlooked in practically all alternatives for recording academic information using a blockchain.

The main concepts of blockchains, smart contracts, NFTs, and the General Data Protection Regulation (GDPR) are introduced below, together with their relationship with the education sector. Then, Section 3 presents the innovative model proposed, while Section 4 discusses its implications and benefits. Finally, Section 5 offers some concluding remarks.

## 2. Preliminaries

### 2.1. Blockchain and Education

Blockchain, the technology behind Bitcoin [6], introduced in 2008, serves as a distributed and decentralized database capable of securely recording transactions in an immutable manner. Transactions within a blockchain are stored in blocks, each cryptographically linked to the preceding one, rendering the information nearly impossible to alter once registered in the blockchain. Simultaneously, it remains easily verifiable. Operating as a decentralized system, there are no central actors, and all processes are executed by nodes or devices comprising the peer-to-peer network in which blocks of information are shared.

Actual block contents vary depending on the type of blockchain. They might solely represent economic transactions, as in Bitcoin, or register state changes in variables on platforms like Ethereum [7], enabling the execution of smart contracts [8]. These smart contracts operate autonomously based on their programming within the blockchain, reading information from one or multiple block transactions, and even modifying and storing data in a new block as a new transaction. Due to its foundations, blockchain holds the potential to establish verifiable and transparent records of information, such as academic data.

There exist various types of blockchains, ranging from public blockchains like Bitcoin and Ethereum to private ones, like those based on the Hyperledger framework [9] and consortium blockchains. Public blockchains operate openly without permission (i.e., they are known as permissionless blockchains), allowing anyone to join, read, send, and add information. This transparency might be suitable for ensuring transparency in academic certificate issuance. However, the lack of trust among network members in public blockchains necessitates stricter security mechanisms, which can hinder transaction speed and volume compared to other blockchain types.

Conversely, access to information in private blockchains requires permission, issued by the institution that created, deployed, and maintains the blockchain (i.e., they are known as permissioned blockchains). While offering increased trust among network teams, the security mechanisms need not be as stringent, enabling higher transaction speeds and volumes compared to public blockchains. Hyperledger is presently the most popular framework to create such blockchains.

Consortium blockchains combine elements of both public and private blockchains. They require permission to join but may be configured to allow any user to access stored information, depending on the group of institutions maintaining the blockchain.

Initially, private and consortium blockchains might seem preferable in educational settings, where greater data privacy management and control are necessary. However, this is not always the case [5,10], due to other data protection aspects outlined in the General Data Protection Regulation (GDPR), one of the world's strictest data protection legislations.

While blockchain in education could revolutionize certificate issuance and management by creating immutable and accessible records for validating academic achievements, its adoption must be carefully considered with respect to personal data protection and compliance with regulations like the GDPR. Existing research on blockchain's educational applications [11–30] commonly highlights certificate issuance and validation as the most frequent use case [12,27], with other applications also present [28,31]. However, these proposals do not predominantly focus on solutions compliant with the GDPR in their entirety—except for [32,33], written by the authors of this article, and [32–34], in particular, outlines a detailed model compatible in design with the GDPR and its requirements, considering the resultant system's scalability and additional functionalities, such as support for learning analytics [35,36] or scenarios in case the academic institution ceases to exist [32,35,37–41].

### 2.2. Smart Contracts, NFTs, and Their Role in Education

As previously indicated, certain blockchains enable the execution of smart contracts, which are self-executing programs that automate agreements and could be used for the issuance and verification of academic certificates. These smart contracts could handle the issuance, updating, and verification of academic information in an automated and secure manner, facilitating interaction among academic institutions, students, and third parties.

Blockchain technology, in conjunction with smart contracts, allows the creation of tokens representing specific assets from the physical or digital realms. There are three distinctive token categories:

- Fungible tokens (based on the ERC20 standard [42]) are interchangeable with each other and lack uniqueness. Each fungible token is indistinguishable from another and can be entirely interchangeable without transferring ownership. Common examples include cryptocurrencies like Bitcoin (BTC, ₿) or Ether (ETH, Ξ), Ethereum's cryptocurrency, where each unit is identical and indistinguishable from others.
- Non-fungible tokens (commonly known as NFTs, based on the ERC721 standard [43]) are unique and indivisible, with distinctive characteristics making each one unique and not interchangeable on an equal basis with another token. NFTs are used to represent unique digital assets such as digital artworks, collectibles, or the ownership of virtual goods [44,45]. Each non-fungible token possesses specific attributes differentiating it from similar tokens, thus its value is derived from its singularity and authenticity.

- Semi-fungible tokens (based on the ERC1155 standard [46]) share some characteristics with both fungible and non-fungible tokens. While they are interchangeable in terms of value, they have unique properties and can hold different values within a general category. For instance, tokens representing different editions of a collectible card could be considered semi-fungible. Each card is exchangeable for another of the same type, but unique editions might have varying values.

Within academia, extensive research has been conducted on these token categories, exploring their usefulness and applications across different fields [42,44]. Specifically, several studies examined the introduction of NFTs into education [47]. These studies delve into how NFTs could revolutionize the issuance and verification of academic certificates by providing a unique and unalterable digital means to represent educational accomplishments. Different approaches were considered, such as storing hash data [48] through the creation of a blockchain-based school management system, named the "Ethernal Digital Certificate" [49], using the InterPlanetary File System (IPFS) [50], a hypermedia protocol, and a distributed peer-to-peer resilient file system to tamperproof store and share information that can handle bigger file sizes; employing Decentralized identifiers (DIDs) [51] within NFTs [52] for information storage; or storing information directly on the blockchain [53]. None of these research initiatives, however, specifically addresses compliance with the GDPR.

Moreover, NFTs, initially employed to represent unique digital assets like artworks [54], evolved into dynamic NFTs (dNFTs) capable of reflecting changes in the associated data. This adaptive and updatable information capacity could be crucial in academic information issuance, where data may require periodic modifications to remain updated and accurate in specific circumstances.

### *2.3. General Data Protection Regulation (GDPR)*

The General Data Protection Regulation (GDPR) [4] is a regulation of the European Parliament (EU), 2016/679, concerning the protection of individuals regarding the processing of their personal data and the free movement of such information. This regulation applies not only to personal information like names, surnames, etc., but also to any other information that, in combination with other means, could be used to identify a person. Infringements of the GDPR may result in significant fines. As a consequence, projects that require the management of personal data are conceived according to the principle "privacy, secure, and legal by design", that is, in determining the means for data processing and during the processing itself, it is necessary to implement appropriate technical and organizational measures (General Data Protection Regulation, Article 25, paragraph 1).

Article 5 of the GDPR establishes the fundamentals and principles regarding data processing with which the proposed model must comply:

1. Lawfulness, fairness, and transparency: personal data will be processed lawfully, fairly, and transparently concerning the data subject (GDPR, art. 5.1.a).
2. Purpose limitation: Personal data will be collected for specified, explicit, and legitimate purposes and not processed in a manner incompatible with those purposes. Subsequent processing for archiving purposes in the public interest, scientific or historical research, or statistical purposes, according to Article 89.1, is not considered incompatible with those initial purposes (GDPR, art. 5.1.b).
3. Data minimization: personal data will be adequate, relevant, and limited to what is necessary for the purposes they are processed (GDPR, art. 5.1.c).
4. Accuracy: personal data will be accurate and, when necessary, kept up to date. All reasonable measures will be taken to ensure that inaccurate personal data, considering the purposes for which they are processed, are erased or rectified without delay (GDPR, art. 5.1.d).
5. Storage limitation: Personal data will be stored in a way that allows for the identifying of data subjects for the necessary processing purposes. Personal data can be stored for longer periods, subject to implementing the appropriate technical and organizational

measures required by the regulation, to safeguard the rights and freedoms of the data subject (GDPR, art. 5.1.e).

6. Integrity and confidentiality: personal data will be processed securely, ensuring the appropriate security of personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage, using suitable technical or organizational measures (GDPR, art. 5.1.f).
7. Accountability: the data controller will be responsible and able to demonstrate compliance with paragraph 1 (GDPR, art. 5.2).
8. Data modification (GDPR, art. 16): the data subject has the right to rectify personal data without undue delay by the data controller if they are inaccurate or incomplete.
9. Right to erasure: the user can request the deletion of inaccurately or unlawfully processed data as specified in the GDPR (GDPR, art. 17).
10. Article 20 refers to data portability, granting individuals control over their personal data, allowing them to request and receive their provided data from a controller in a structured, commonly used, machine-readable format (GDPR, art. 20).
11. Article 22 of the GDPR refers to the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning them or significantly affects them (GDPR, art. 22). If a profile generated based on personal information has legal consequences, its management is entirely prohibited, a situation that is highly probable when storing academic information that might help create a profile.
12. Article 45 addresses data transfer to countries outside the European Union, which should be considered. Personal information can only be transferred to a destination country if it is deemed to have a data protection standard equivalent to that of the GDPR (GDPR, art. 45).

## 3. Proposed Model

As discussed above, the issuance of academic certificates within the educational sector is continually evolving to guarantee authenticity and information readiness. Additionally, the present-day job market requires people to keep track of educational achievements not originating from an academic institution, such as informally acquired skill sets or professional experience.

The innovative model proposed is based on issuing NFTs supported by blockchain technology to represent academic information uniquely and dynamically, ensuring compatibility with the GDPR requirements at the same time.

The core concept behind this model is a reformulation of the model proposed in [32] to use NFTs. Note that the technology for interconnecting different blockchains to create a universal platform based on this framework is still under research and in its infancy stage [55–59], the challenge being to achieve the model's privacy and scalability objectives at a global scale.

Thus, the proposal in this paper is a revision of our seminal model so that it can be realized with presently available technology (cf. Figure 1). In this proposal, academic institutions, or anyone wishing to issue an accreditation of some specific educational achievement to an individual with a known blockchain address (i.e., a wallet address), would issue an NFT to that individual, signed with the private key of the issuer, thus emitting academic information as an NFT.

However, generating a record containing personal information (e.g., names, surnames, etc.) and storing it directly in a blockchain or decentralized storage (e.g., IPFS, Swarm, or an equivalent storage model), does not comply with the GDPR [5]. Even if the NFTs were configured as dynamic, allowing the issuer to modify their attributes (e.g., to comply with the data subject's right to modify data), previous blockchain transactions would retain the original data in an immutable way. Additionally, erasing this information is impossible, breaching the right to be forgotten. The GDPR directly prohibits storing data in a permanent storage medium like a blockchain, even if encrypted. For instance,

using a public blockchain like Ethereum and encrypting data with a robust algorithm would permanently store the encrypted information in the blockchain. This poses a risk, as advancements in computing power or algorithm vulnerabilities could expose this personal information in the future. Some projects like Blockcerts [3] store a hash resume of the academic information. However, the GDPR considers the hashed summary an invalid pseudonymization technique [5].

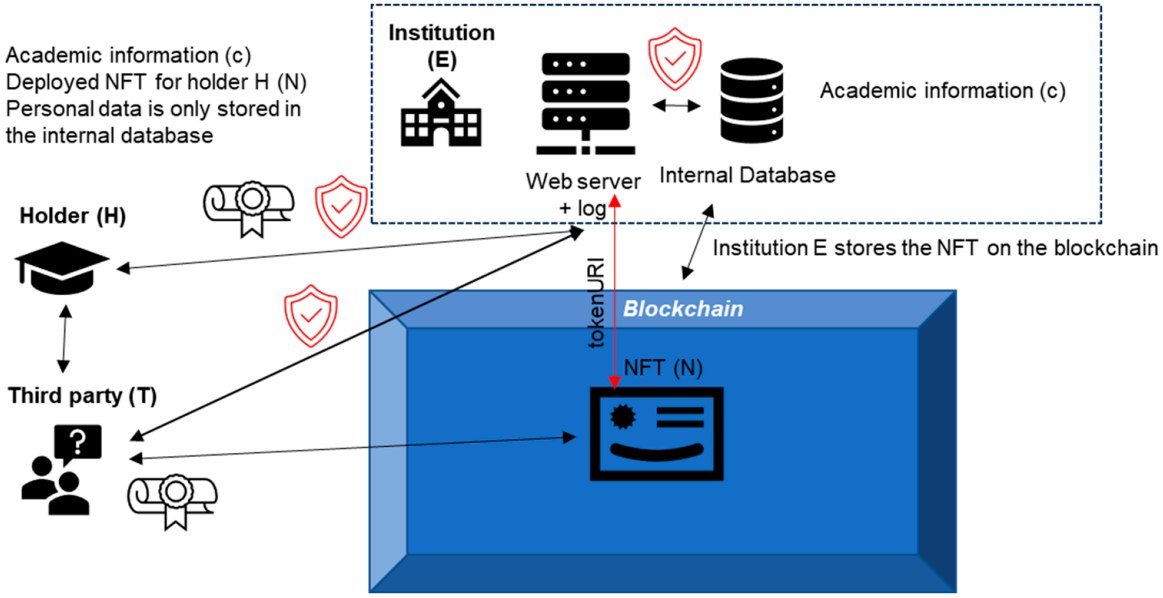



**Figure 1.** Proposed model (overview).

For these reasons, in this model, a distinction is made between information considered public and private data. Examples of public information items are the issuer's address, a recognized institution whose authority can be demonstrated, the recipient's address (for enhanced privacy, individuals can be allowed to generate a new address for each received academic piece of information), the institution name, issuance date, certificate validity, etc. On the other hand, attributes such as names, surnames, grades, and study completion dates, or in the case of professional experience, employers' remarks, photographs, or contact details, are considered private personal information. Note that this model is open-ended and not confined to a fixed set of fields, allowing for its adaptation to various content types.

Table 1 summarizes some of the main initiatives related to blockchain and education extracted from the academic literature, which were also compared with the initial proposed model [32] from the perspective of where data are stored and compliance with the GDPR. The table also includes those that use NFTs for academic information.

**Table 1.** Comparison of other related initiatives to the proposed model on to how information is stored and processed in relation to the GDPR.

| Initiative | Scalability Nr. of Blockchains | Storage | Regenerate Data | Verification | Right to Erasure | Data Modification | Grant/Remove Permissions | Data Portability | Data Access Accountability |
|---|---|---|---|---|---|---|---|---|---|
| Arenas and Fernández [60] | 1 bc multichain | Off. + hash | ✓ | ✓ | - | - | - | - | ✗ |
| Arndt and Guercio [61] | 1 bc | Off./On. | ✗ | ✓ | - | - | ✗ | ✗ | ✗ |
| Badyal and Chowdhary [62] | 1 bc | On. | ✗ | ✓ | - | - | ✗ | ✗ | ✗ |
| Bandar et al. [36] | 1 bc | Off. + hash + digital id | - | ✓ | - | - | - | - | - |
| Blockcerts [63] | 1 blockchain Bitcoin/Eth | Off. + hash | ✗ | ✓ | - | ✗ | ✗ | - | ✗ |
| Bore et al. [64] | 1 bc HL Fabric | Off. + hash + pointer | - | ✓ | - | - | - | - | - |
| Cheng et al. [65] | 1 blockchain Ethereum | Off. + hash + cert. id | ✓ | ✓ | - | - | - | - | - |
| Cheng et al. [66] | 1 bc (HLF) | Off. | ✗ | ✓ | - | - | - | - | - |
| Daraghmi et al. [67] | 1 bc Eth | Off./hash | - | ✓ | - | - | ✓ | - | ✓ |
| Ghazali and Saleh [68] | 1 bc | Off./hash | - | ✓ | - | - | - | - | ✗ |
| Gresch et al. [69] | 1 bc Eth | File + hash | ✗ | ✓ | - | - | - | - | - |
| Han et al. [70] | 1 bc Eth | Off. + pointer to data + hash | ✓ | ✓ | - | - | - | - | - |
| Jeong and Choi [71] | 1 bc Bitcoin/Eth | Off. | ✗ | ✓ | - | - | - | - | - |
| KARATAŞ [72] | 1 bc Eth | On. | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Kuvshinov et al. [73] | Several private bcs and 1 public | On. in a private bc + hash | ✗ | ✓ | - | - | - | - | ✗ |
| Lam and Dongol [74] | 1 bc HL | On + access control | ✓ | ✓ | - | ✓ | - | - | ✗ |
| Li and Han [38] | 1 bc Eth | Off. | ✓ | ✓ | - | - | - | - | ✗ |
| Li et al. [41] | 1 bc | Off. + OBE codes | ✗ | ✓ | - | - | - | - | ✗ |
| Lizcano et al. [35] | 1 bc Eth | Off. + some data on | ✓ | ✓ | - | - | - | - | ✗ |
| Nicosia [3] | 1 bc Bitcoin | Off. + hash | ✗ | ✗ | - | - | - | - | - |
| Nikolić et al. [49] | 1 bc | On + NFT + IPFS | - | ✓ | - | - | - | - | ✗ |
| Ocheja et al. [75] | 1 bc Eth | Off. + hash + pointer | - | ✓ | - | - | - | - | ✗ |
| Palma et al. [39] | 1 bc Eth | On. | ✓ | ✓ | ✗ | - | - | - | ✗ |
| Pfeiffer et al. [53] | 1 bc | On. + NFT | ✓ | ✓ | ✗ | - | ✗ | - | ✗ |
| Prinz et al. [76] | 1 bc Eth | Off. | - | ✓ | - | - | - | - | ✗ |
| Rooksby and Dimitrov [77] | 1 bc Eth | On. | - | ✓ | - | - | - | - | - |
| Saleh et al. [1] | 1 bc HL | Off. + hash | - | ✓ | - | - | - | - | - |
| Srivastava et al. [40] | 1 bc ARK | On. (token) | ✓ | ✓ | - | - | - | - | - |
| Sun et al. [78] | 1 bc | On. + hash | - | ✓ | - | - | - | - | - |
| Tahit et al. [52] | 1 bc Alg | On. + NFT + IPFS + DID | ✓ | ✓ | - | - | ✓ | - | ✗ |

**Table 1.** *Cont.*

| Initiative | Scalability Nr. of Blockchains | Storage | Regenerate Data | Verification | Right to Erasure | Data Modification | Grant/Remove Permissions | Data Portability | Data Access Accountability |
|---|---|---|---|---|---|---|---|---|---|
| Turkanović et al. [37] | 1 bc ARK | On. (token) | ✓ | ✓ | - | - | - | - | ✗ |
| Wahab et al. [79] | 1 bc tangle | Off. + hash | ✗ | ✓ | - | - | - | - | ✗ |
| Xu et al. [80] | 1 bc | On. | - | ✓ | - | - | - | - | ✗ |
| Zhao et al. [48] | 1 bc | Off. + NFT + hash | ✗ | ✓ | - | ✗ | ✗ | - | ✗ |
| Delgado-von-Eitzen et al. (base model) [32] | 1 consortium and *n* private bcs | Off. + hash + pointer to data | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| This design | 1 bc | Off. + NFT with pointer to data | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Legend: BC = blockchain; Off. = off-chain; On. = on-chain; NFT = non-fungible token: Eth = Ethereum; HLF = Hyperledger Fabric; Alg = Algorand; ARK = ARK blockchain; DID = Decentralized identifiers; IPFS = InterPlanetary File System; ✓= Adequately addressed; ✗ = Not addressed; - = No information provided.

### *3.1. Issuance of the Academic Information*

To protect personal information, the approach followed in this model is to dynamically generate a unique token identifier (tokenURI) each time access is requested, either by a centralized or decentralized server with non-persistent storage, avoiding blockchain storage. A tokenURI is a standardized way to provide metadata and information about a specific token, the educational NFT in our case. It is used to link to the academic certification data represented by the NFT.

Figure 2 outlines the academic information's issuance process. With this model, first, the user holding the academic information (H) informs the institution (E) of their account (H). Subsequently, the NFT with a tokenURI containing the (full) academic information is generated, as outlined in the model. The data (c) remains stored in the institution's local database, and upon deploying the NFT, it adds the authorized accounts of H and E, as indicated. These operations are recorded in the web server's log. As an optional element, to further enhance system reliability at regular intervals, for example, every 24 h, a hash summary of the log records can be registered on a blockchain. This way, any unauthorized alterations could potentially be detected.

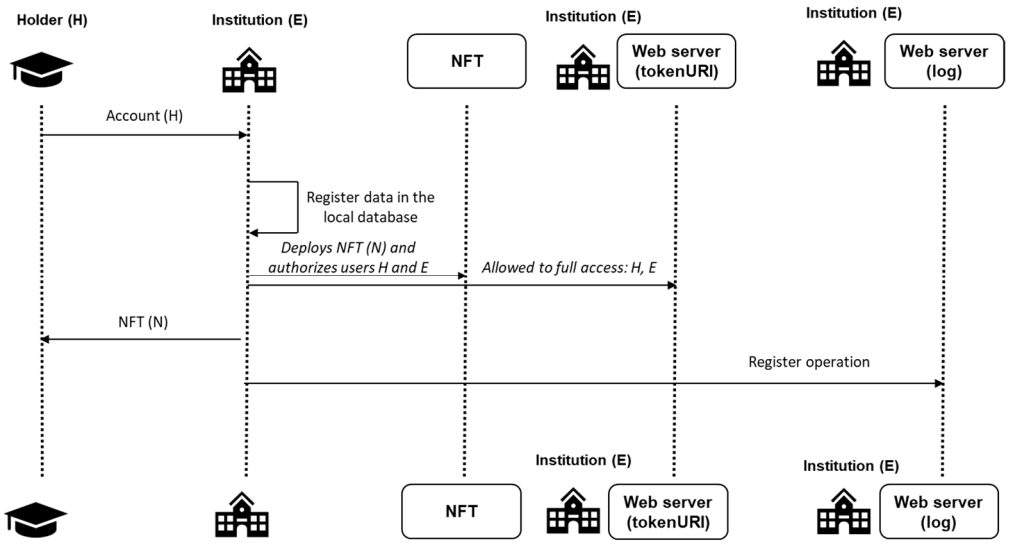



**Figure 2.** Issuance of the academic information.

The data owner will configure access permissions for their academic information.

### *3.2. Access to the Academic Information by a Third Party*

When a third party (with the address T) seeks access to specific academic details of the user, they request these details, through the platform, of the data holder (H). The data holder will grant authorization to T to access either all or certain parts of the data according to their wishes and interests. This permission information will be recorded at institution E associated with that specific NFT (N). H provides T with the address of N after granting permissions through the platform or other channels, and T requests access to N's data. The data stored on the blockchain, such as the issuance date and time of the NFT, its creator, etc., pose no issue. However, the tokenURI queried will depend on T's authorization. The system verifies T's credentials and retrives the information of NFT N, providing either all the data or only specific parts as desired by the data holder H, generating a specific tokenURI that T can verify.

The process discussed above is summarized in Figure 3. If the educational certificate owner (H) wants to revoke access to one or more third parties, they must notify these parties and inform the institution's server, withdrawing access permissions. From that point on, even if the third party retains the NFT address, they cannot access the personal

information. If they stored any copies in other formats off-chain, these should be destroyed to comply with the GDPR, as the data owner has exercised their right to revoke access.

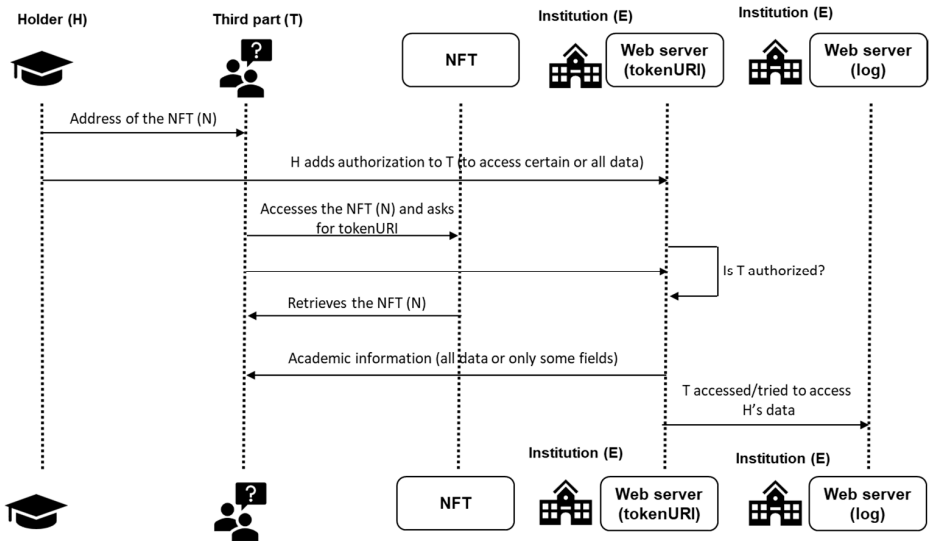



**Figure 3.** A third party wants to access the NFT.

The model assumes that the server dynamically generating the tokenURI content, with access control, also maintains an access log. This log allows the NFT owner to review how many times, when, and by whom their academic information has been accessed.

Although technically feasible, the hash value of the dynamic tokenURI content is not stored. A hashed summary of all personal data is considered inadequate for anonymization. This aspect will be further discussed in the subsequent section.

### *3.3. Modification and Deletion of Academic Information*

This model also allows changes in the academic information under the issuer's control. If the dynamically linked content associated with the tokenURI parameter changes without modifying anything in the blockchain, the academic information could become more comprehensive or updated in case of errors, which is always guaranteed by transactions signed by the issuing entity and stored in the blockchain.

Of course, the deletion of information is also addressed, representing a specific case of data modification wherein the information is erased from the local database of the institution (cf. Figure 4). Consequently, no information will be generated in the tokenURI, and the NFT is invalidated (i.e., marked as invalid).

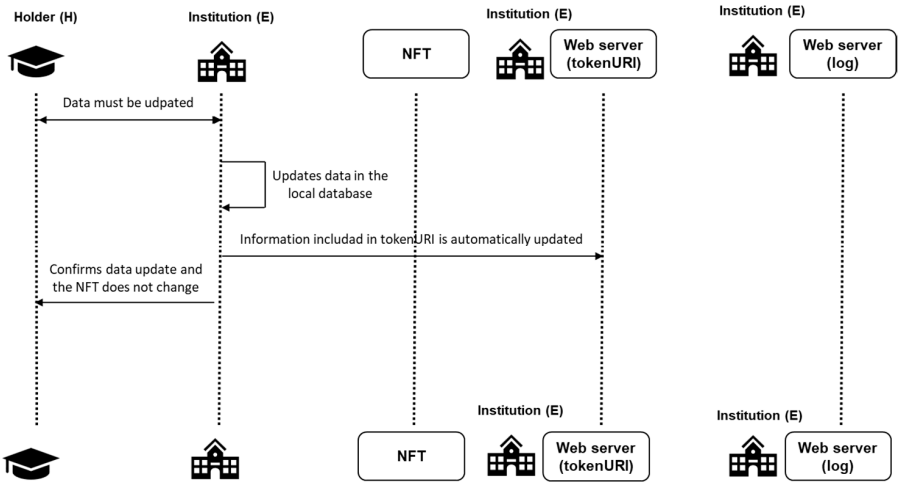



**Figure 4.** Modification of the academic information.

### 3.4. Building a Minimum Viable Product

To demonstrate the feasibility of the proposed model with current technology, an MVP (Minimum Viable Product) was developed using Ethereum and a web server, following the model outlined in Figure 1. In this case, the blockchain is an Ethereum-based blockchain, and the rest of the elements are the same as in that model.

Firstly, an Ethereum smart contract was developed using Solidity, employing the ERC721 standard [43] and OpenZeppelin's (https://www.openzeppelin.com/, accessed on 1 December 2023) secure libraries supporting NFTs. OpenZeppelin is an open-source framework used to build secure smart contracts that provides a complete suite of security products and audit services to build, manage, and verify all aspects of software development and operations for decentralized apps (dApps).

Certain functions were disabled within the smart contract to prevent the transfer of ownership of the NFT to another account, as this asset is not intended to potentially change ownership. Additionally, the burn function was restricted solely to the issuer of the NFT.

Upon deploying the smart contract supporting NFTs, an initial token (0) was created and assigned to the holder of the academic information, identified by their Ethereum public address. The tokenURI was configured to refer to a web address of the form https://www.server.com/data.php?id=xyz (accessed on 11 January 2024).

Whenever these dynamic metadata [81] are requested, a centralized server maintained by the institution E will verify whether the accessing account is authorized. This control mechanism also logs access details, including the date and time.

The dynamically generated metadata file of the token includes attributes such as the institution's name, the internal database registration number where the information is stored, the modification date and time in the internal database, name, surname, national ID number of the individual, completed course name, credits, final grade, validation status or revocation, course credits, course completion date, and course subjects.

In this MVP, additional information, such as the internal database record identifier and the date/time of the last modification in the issuer's database, was included for increased transparency. This allows users accessing the information to know if the registration number has changed or if there have been modifications in the database.

Metadata generation was programmed using a PHP-based script where different metadata are generated based on the input parameter "id". Access control is managed via a cookie; individuals granted permission by the data owner and possessing this cookie can access the complete certificate information or parts of it. Otherwise, access is denied. The user type determines whether all attributes or only a portion of them are generated, simulating the behavior seen when data owners grant access to specific parts of their academic information.

The smart contract was deployed on Ethereum's Görli testnet (Sepolia is another option) using Remix and Metamask for testing, demonstrating the expected functionality of an MVP to verify the feasibility of this NFT-based model.

A logging system on the web server records who logs in to access the information and when, allowing the academic information holder to monitor who accesses their data and manage permission grants or revocations.

## 4. Discussion

The model proposed in this publication was designed not only for ease of the issuance and verification of academic information using NFTs, a widely used type of token, but it was also designed according to the "privacy by design" principle to protect personal data and thus comply with the GDPR, one of the world's most stringent data protection regulations, as previously mentioned. Nevertheless, when employing this system, it is crucial to obtain the explicit consent of the individuals involved and register it in accordance with GDPR's guidelines.

Once an institution has issued some academic record, the data owner possesses a mechanism to grant or revoke access to the metadata of the token containing their personal

information. This individualized control aligns with the requirement that data subjects have control over their data. By revoking authorization for a certain person or institution, notifications are sent, ensuring that they are aware not only of the denial of access to the information but also of their obligation to comply with regulations by destroying any retained data.

If we analyze the requirements outlined in the GDPR, we find that the proposed model fulfills them, as summarized in Table 2.

**Table 2.** Compliance with requirements.

| Requirement | Fulfilled? | Explanation |
| --- | --- | --- |
| Principle of lawfulness, fairness, and transparency. Personal data shall be processed lawfully, fairly, and transparently in relation to the data subject. (GDPR, Art. 5.1.a) | Yes | Explicit consent from the data subject is obtained, as requested by the institution and third parties seeking access to the data. |
| The principle of purpose limitation (GDPR, art. 5.1.b) | Yes | The issuing institution and authorized third parties must only use them for specific purposes. |
| Principle of data minimization (GDPR, art. 5.1.c) | Yes | The model is entirely flexible regarding the set of fields used, ensuring that they are only the minimum necessary for the intended purpose. Moreover, the data subject can select which fields third parties may access when interacting with the NFT. |
| The principle of accuracy (GDPR, art. 5.1.d) | Yes | The personal data are accurate, and in case of any inaccuracy, the issuing institution can easily remove or rectify them, as they are stored within their databases. |
| The principle of storage limitation (GDPR, art. 5.1.e) | Yes | The institution issuing personal academic information has the flexibility to delete it, when necessary, thanks to the proposed model. |
| The principle of integrity and confidentiality (RGPD, art. 5.1.f) | Yes | The issuing institution is responsible for safeguarding the data's integrity and confidentiality. The proposed model based on NFTs does not compromise this requirement. |
| Accountability principle (GDPR, art. 5.2) | Yes | Access logs are maintained by the institution that holds the data, which can be reviewed by the data subject, as outlined in the model. |
| Data modification (GDPR, Art. 16) | Yes | The model allows for easy data modification, ensuring that third parties accessing the information always see the updated, accurate, complete, and correct version. |
| The user has the capacity to exercise the right to be forgotten (RGPD, art. 17). | Yes | If the academic information needs to be deleted, it is a matter of removing it from the issuing entity's internal centralized databases, ensuring no personal data remains on the blockchain. |
| Data portability (GDPR, art. 20) | Yes | The model enables data to be moved from one place to another by either requesting it from the institution or downloading it in a JavaScript object notation (JSON) format from the NFT. |
| The right not to be subject to a decision based solely on automated processing (GDPR, Article 22) | Yes | Even if automated tools are employed to detect the academic information issued under the model, they cannot access personal data without proper authorization. |
| Control of data transfer to countries outside the European Union (GDPR, Art. 45) | Yes | The model does not prevent this control, which remains in the hands of the entity responsible for data processing, as no personal data are stored in the blockchain. |

The model was designed to "implement appropriate technical and organizational measures at the time of determining the means for processing as well as at the time of the actual processing" (GDPR, Article 25, paragraph 1).

Public, private, or consortium blockchain?

The proposed solution utilized a public blockchain (i.e., an Ethereum testnet); however, it could also be deployed on a private or consortium blockchain based on Ethereum or Hyperledger technology, to cite just two examples. The rationale behind leveraging a public blockchain was twofold. First, to demonstrate the feasibility of the solution without the need to deploy a proprietary infrastructure, and second, to underscore that, thanks to the model employed, it is feasible to use a blockchain where all registered information is public and visible to all users without affecting the protection of personal data and compliance with the GDPR.

Indeed, deploying this model on a private or consortium blockchain could potentially enhance the solution's scalability. Given scenarios where thousands of academic records need to be issued promptly [32], permissioned blockchains such as those based on the HyperLedger framework offer better information-recording capabilities, and can withhold up to 20,000 transactions per second [82]. However, considering the focus of this research, centered on using an NFT to record academic information compliant with the GDPR, the outcome remains the same. Even within a permissioned blockchain with limited access, personal data cannot be stored permanently, in line with the stipulations for data protection.

Using a private or consortium blockchain indeed improves costs and scalability, but at the expense of greater centralization, which could potentially pose a risk to the trust in the stored information. However, it is believed that a private or consortium initiative set up to support these educational certification services would be primarily interested in avoiding the risk of manipulations to ensure its trustworthiness.

Is it possible to further decentralize the solution?

According to the model description, its operation, and its advantages, it can be argued that the model relies on a centralized system since personal information is stored on a centralized entity. Additionally, it is worth considering whether further decentralization is feasible.

Regarding the first point, the system does utilize a blockchain to instill confidence that the academic information accessible to third parties was issued by a specific institution, as the transaction is signed by them and contains personal data stored on a central server. In essence, a key aspect of managing personal information, namely guaranteeing confidence and trust, is decentralized. Moreover, due to the proliferation of tools for querying NFTs, the process of verifying data is straightforward, successfully fulfilling the initial goal of verifying the authenticity of academic information.

Addressing the second issue—could it be further decentralized? The answer is affirmative. During the design of this model, an alternative, slightly more decentralized approach was considered, but discarded for reasons elucidated in the following paragraphs.

One method to reduce dependence on the data stored in the centralized server of the issuing institution would be a model like the one introduced in this paper, but additionally incorporating some form of digest of the personal information into the NFT stored on the blockchain. In this case, it would be a dynamic NFT, as one of its fields would correspond to a hash summary of the dynamically generated personal data.

Hence, if a third party wanted to validate specific information provided by the data holder, they would only need to compute the hash summary of the data and compare it with what is stored in the NFT. However, as highlighted above, this approach is not valid from a data protection perspective, since a hash summary is not a sufficiently secure anonymization technique [5].

Nonetheless, it could be possible to combine encryption with a hash summary with data salt, and store this in the blockchain within the NFT [5,10,43,82]. In this scenario, it could be considered that academic information is securely anonymized in this manner, provided the recommendations in [83,84] are followed, despite being per-manently stored

on the blockchain. However, in the development and in the final proposed model, this part was omitted for several reasons:

1. The primary advantage of adding this information is that it increases the degree of decentralization of the solution. Even if the institution issuing the academic information disappears and the tokenURI is empty, it is possible to verify that the data sent by the data holder, along with the salt and key, match the information stored in the NFT available on the blockchain. However, this comes at the expense of the data holder sharing more information (i.e., personal data for verification, salt, and an encryption key).
2. If the recommendations provided by data protection authorities are not strictly followed, personal data could not only be exposed but also permanently stored on the blockchain.
3. Once authorization is granted to a third party to access the data, and the actual data, salt, and encryption key are shared, even if permission is later revoked, if this third party does not destroy or leak the information, data privacy may be compromised. As mentioned, the hash summary with encrypted salt is stored on the blockchain and accessible to anyone if a public blockchain is used.

For these reasons and because, in general, the model does not significantly improve with this addition or better align with the requirements of "privacy, security, and legal by design," a slightly more centralized yet more secure and private approach was chosen, always ensuring that the transactions for issuing NFTs are generated by accredited institutions.

It should also be noted that if the tokenURI is allowed to be updated with the NFT, in case there is a problem with the Internet domain used (server.com in the example), it could be updated so that the NFT continues to function as it should.

Another interesting point for discussion is the issue of burn permissions and who can destroy the NFT and who cannot. In the MVP provided, only the institution issuing the NFT was allowed to destroy it, but provisions could be made for the data holder to have this option as well. From the perspective of data privacy, this poses no significant impact. However, to prevent the unauthorized or even malicious issuance of NFTs to accounts by an organization and render these actions futile, allowing the data holder the burn option would be desirable. Nevertheless, in the case of official academic certifications, for instance, and always within the legal framework of each country, it might not be feasible for a certificate holder to destroy it. This should be reflected when programming the smart contracts that support NFTs.

Another aspect worth analyzing is whether the term NFT is truly fitting for this information. By nullifying the transfer function, as explained, to prevent the holder from transferring ownership of the academic information and leaving the burn function as a choice for the institution, it could be argued that instead of an NFT with value in the market, it is actually a Soulbound token or SBT [85], a unique and non-transferable type of NFT that represents an individual or entity on the blockchain. In this document, the term NFT is used, but, due to its characteristics, it could be accurately classified as an SBT.

## 5. Conclusions

While there are numerous initiatives aimed at applying blockchains in the realm of education, very few (virtually none except [32–34]) consider an aspect as crucial as compliance with data protection regulations such as the GDPR. Furthermore, among these initiatives, there are currently no operational applications or even MVPs; many are still under development while the necessary blockchain technology matures.

Therefore, this research not only proposes the design of an innovative solution following the model described in [32] to issue, store, and easily verify various types of academic information using a blockchain, but it also aims for deployment and use with existing blockchain technology. This goal is achievable while maintaining compatibility with the information systems available in organizations today and ensuring alignment with the GDPR.

As demonstrated in Section 3, the proposed model employs established blockchain technologies such as smart contracts, NFTs, and web technologies for token metadata generation, along with an access control and logging system. These technologies are mature and easily integrable with practically any information system utilized, often without requiring significant financial investment.

The proposed model is also entirely flexible when it comes to registering any type of official and unofficial, formal, or even informally acquired, competences and skills. It does not mandate a specific data storage model; instead, it is defined in JSON format by the issuing organization based on its requirements. Consequently, this flexibility could create job opportunities for individuals who may demonstrate their skills, experience, or knowledge through accreditations issued by various organizations, the value of which will inherently increase with public recognition.

The proposal fulfills its objectives of GDPR compliance and feasibility using existing blockchain technologies, albeit at the expense of a certain degree of centralization and a lack of scalability in the case of a high volume of transactions. For instance, using Ethereum, as in the developed MVP, the current performance stands at approximately 15 transactions per second. The centralization, as explained in the discussion section, arises from our inability to store personal data in a permanent storage medium like the blockchain. GDPR compliance is considered a fundamental goal of this publication, and, as such, certain decentralized elements have been sacrificed while still leveraging the potential of the blockchain. An NFT is generated using this technology, ensuring the authenticity and integrity of the deployed data. The discussion section presents alternative approaches, but also explains why this compromise is considered the best solution. Scalability remains an aspect to address from a technical perspective, and is more reliant on blockchain solutions from a technological viewpoint than on the applications, such as in this case. Nonetheless, there is always the option, as indicated in the discussion section, to utilize more scalable and faster private blockchains.

However, the most significant contribution lies in the model's compliance with the GDPR. Data owners always retain control, determining precisely what aspects of their academic information to share (whether all or specific parts) and with whom. This control extends to monitoring data access and the ability to revoke permissions at any time, as elucidated in this article.

**Author Contributions:** Conceptualization, C.D.-v.-E., L.A.-R. and M.J.F.-I.; methodology, C.D.-v.-E.; software, C.D.-v.-E.; validation, C.D.-v.-E., L.A.-R. and M.J.F.-I.; formal analysis, C.D.-v.-E., L.A.-R. and M.J.F.-I.; investigation, C.D.-v.-E.; data curation, C.D.-v.-E., L.A.-R. and M.J.F.-I.; writing—original draft preparation, C.D.-v.-E. and M.J.F.-I.; writing—review and editing, C.D.-v.-E., L.A.-R. and M.J.F.-I.; supervision, C.D.-v.-E., L.A.-R. and M.J.F.-I. All authors have read and agreed to the published version of the manuscript.

**Funding:** Grant TED2021-130828B-I00 funded by MCIN/AEI/10.13039/501100011033 and European Union NextGenerationEU/PRTR.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data presented in this study are available upon request from the corresponding author. As the development is an initial minimum viable prototype (MVP), the data is not published and it is only accessible upon request. Please note that all the information required to replicate the MVP is already included in the article.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Saleh, O.S.; Ghazali, O.; Rana, M.E. Blockchain based framework for educational certificates verification. *J. Crit. Rev.* **2020**, *7*, 79–84. [CrossRef]
2. Muzammil, M. Corrupt schools, corrupt universities: What can be done? *Comp. A J. Comp. Int. Educ.* **2010**, *40*, 385–387. [CrossRef]

3. Grech, A.; Camilleri, A.F. *Blockchain in Education*; Publications Office of the European Union: Luxembourg, 2017.
4. von dem Bussche, A.; Voigt, P. *The EU General Data Protection Regulation (GDPR)*; Springer: Cham, Switherland, 2017; ISBN 978-3-319-57959-7.
5. Lyons, T.; Courcelas, L.; Timsit, K. *Blockchain and the GDPR*; European Parliamentary Research Service: Brussels, Belgium, 2018.
6. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2018. Available online: https://www.bitcoin.org/bitcoin.pdf (accessed on 1 December 2023).
7. Swan, M. *Blockchain: Blueprint for a New Economy*, 1st ed.; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015; ISBN 1491920491.
8. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday* **1997**, *2*. [CrossRef]
9. HYPERLEDGER. Whitepaper Introduction Hyperledger. July 2018. Available online: https://www.hyperledger.org/learn/white-papers (accessed on 14 October 2023).
10. Lyons, T.; Courcelas, L. *Blockchain and Cyber Security*; The European Union Blockchain Observatory and Forum: Brussels, Belgium, 2020.
11. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-Based Applications in Education: A Systematic Review. *Appl. Sci.* **2019**, *9*, 2400. [CrossRef]
12. Yumna, H.; Khan, M.M.; Ikram, M.; Ilyas, S. Use of Blockchain in Education: A Systematic Literature Review. In *Intelligent Information and Database Systems*; Nguyen, N.T., Gaol, F.L., Hong, T.-P., Trawiński, B., Eds.; Springer: Cham, Switherland, 2019; Volume 11432, pp. 191–202.
13. Castro, R.Q.; Au-Yong-Oliveira, M. Blockchain and Higher Education Diplomas. *Eur. J. Investig. Heal. Psychol. Educ.* **2021**, *11*, 154–167. [CrossRef] [PubMed]
14. Dash, M.K.; Panda, G.; Kumar, A.; Luthra, S. Applications of blockchain in government education sector: A comprehensive review and future research potentials. *J. Glob. Oper. Strateg. Sourc.* **2022**, *15*, 449–472. [CrossRef]
15. Reis-Marques, C.; Figueiredo, R.; de Castro Neto, M. Applications of Blockchain Technology to Higher Education Arena: A Bibliometric Analysis. *Eur. J. Investig. Health Psychol. Educ.* **2021**, *11*, 1406–1421. [CrossRef]
16. RushabhBalpande; Patil, K. Usability of Blockchain Technology in Higher Education: A systematic review identifying the current issues in the education system. *J. Phys. Conf. Ser.* **2021**, *1964*, 42017. [CrossRef]
17. Aulia, V.; Yazid, S. Review of Blockchain Application in Education Data Management. In Proceedings of the 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Cameron Highlands, Malaysia, 15–17 June 2021; pp. 95–101.
18. Razia, B.; Awwad, B. *A Comprehensive Review of Blockchain Technology and Its Related Aspects in Higher Education BT—Technologies, Artificial Intelligence and the Future of Learning Post-COVID-19: The Crucial Role of International Accreditation*; Hamdan, A., Hassanien, A.E., Mescon, T., Alareeni, B., Eds.; Springer: Cham, Switherland, 2022; pp. 553–571, ISBN 978-3-030-93921-2.
19. Sunny, F.A.; Hajek, P.; Munk, M.; Abedin, M.Z.; Satu, M.S.; Efat, M.I.A.; Islam, M.J. A Systematic Review of Blockchain Applications. *IEEE Access* **2022**, *10*, 59155–59177. [CrossRef]
20. Talat, M.; Riaz, S.; Farooq, M.S. Effect of Blockchain on Education: A Systemic Literature Review. *VFAST Trans. Softw. Eng.* **2022**, *10*, 116–124.
21. Ocheja, P.; Agbo, F.J.; Oyelere, S.S.; Flanagan, B.; Ogata, H. Blockchain in Education: A Systematic Review and Practical Case Studies. *IEEE Access* **2022**, *10*, 99525–99540. [CrossRef]
22. Kabashi, F.; Snopce, H.; Aliu, A.; Luma, A.; Shkurti, L. A Systematic Literature Review of Blockchain for Higher Education. In Proceedings of the 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), Manama, Bahrain, 8–9 March 2023; pp. 1–6.
23. Malibari, N.A. A Survey on Blockchain-based Applications in Education. In Proceedings of the 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 12–14 March 2020; pp. 266–270.
24. Bhaskar, P.; Tiwari, C.K.; Joshi, A. Blockchain in education management: Present and future applications. *Interact. Technol. Smart Educ.* **2020**, ahead-of-print. [CrossRef]
25. Caldarelli, G.; Ellul, J. Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review. *Appl. Sci.* **2021**, *11*, 1842. [CrossRef]
26. Raimundo, R.; Rosário, A. Blockchain System in the Higher Education. *Eur. J. Investig. Health Psychol. Educ.* **2021**, *11*, 276–293. [CrossRef] [PubMed]
27. Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Blockchain applications in education: A systematic literature review. *Appl. Sci.* **2021**, *11*, 11811. [CrossRef]
28. Hameed, B.; Khan, M.M.; Noman, A.; Ahmad, M.J.; Talib, M.R.; Ashfaq, F.; Usman, H.; Yousaf, M. A Review of Blockchain based Educational Projects. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 101065. [CrossRef]
29. Loukil, F.; Abed, M.; Boukadi, K. Blockchain adoption in education: A systematic literature review. *Educ. Inf. Technol.* **2021**, *26*, 5779–5797. [CrossRef]
30. Awaji, B.; Solaiman, E.; Albshri, A. Blockchain-Based Applications in Higher Education: A Systematic Mapping Study. In Proceedings of the 5th International Conference on Information and Education Innovations; Association for Computing Machinery: New York, NY, USA, 2020; pp. 96–104.

31. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, Fog and edge computing enabled smart campuses and universities. *Appl. Sci.* **2019**, *9*, 4479. [CrossRef]
32. Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information. *Appl. Sci.* **2021**, *11*, 4537. [CrossRef]
33. Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Blockchain for the Scalable Issuance and Verification of Private Academic Information. In Proceedings of the 2021 International Conference on Advanced Learning Technologies (ICALT), Tartu, Estonia, 12–15 July 2021; pp. 436–438.
34. Molina, F.; Betarte, G.; Luna, C. A Blockchain based and GDPR-compliant design of a system for digital education certificates. *Clei Electron. J.* **2023**, *26*, 23. [CrossRef]
35. Lizcano, D.; Lara, J.A.; White, B.; Aljawarneh, S. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *J. Comput. High. Educ.* **2019**, *32*, 109–134. [CrossRef]
36. Bandara, I.; Ioras, F.; Arraiza, M.P. The Emerging Trend of Blockchain for Validating Degree Apprenticeship Certification in Cybersecurity Education. In Proceedings of the 12th International Technology, Education and Development Conference, Valencia, Spain, 5–7 March 2018; pp. 7677–7683. [CrossRef]
37. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
38. Li, H.; Han, D. EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme. *IEEE Access* **2019**, *7*, 179273–179289. [CrossRef]
39. Palma, L.M.; Vigil, M.A.G.; Pereira, F.L.; Martina, J.E. Blockchain and smart contracts for higher education registry in Brazil. *Int. J. Netw. Manag.* **2019**, *29*, e2061. [CrossRef]
40. Srivastava, A.; Bhattacharya, P.; Singh, A.; Mathur, A.; Prakash, O.; Pradhan, R. A Distributed Credit Transfer Educational Framework based on Blockchain. In Proceedings of the 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), Allahabad, India, 21–23 September 2018; pp. 54–59.
41. Li, T.; Duan, B.; Liu, D.; Fu, Z. Design of outcome-based education blockchain. *Int. J. Perform. Eng.* **2018**, *14*, 2403–2413. [CrossRef]
42. Vogelsteller, F.; Buterin, V. ERC-20: Token Standard. Ethereum Improvement Proposals. 2015. Available online: https://eips.ethereum.org/EIPS/eip-20 (accessed on 14 October 2023).
43. Entriken, W.; Shirley, D.; Evans, J.; Sachs, N. ERC-721: Non-Fungible Token Standard. Ethereum Improvement Proposals. 2018. Available online: https://eips.ethereum.org/EIPS/eip-721 (accessed on 14 October 2023).
44. Wang, Q.; Li, R.; Wang, Q.; Chen, S. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. *arXiv* **2021**, arXiv:2105.07447.
45. Bao, H.; Roubaud, D. Non-Fungible Token: A Systematic Review and Research Agenda. *J. Risk Financ. Manag.* **2022**, *15*, 215. [CrossRef]
46. Radomski, W.; Cooke, A.; Castonguay, P.; Therien, J.; Binet, E.; Sandford, R. ERC-1155: Multi Token Standard. Ethereum Improvement Proposals. 2018. Available online: https://eips.ethereum.org/EIPS/eip-1155 (accessed on 14 October 2023).
47. Wu, C.-H.; Liu, C.-Y. Educational Applications of Non-Fungible Token (NFT). *Sustainability* **2023**, *15*, 7. [CrossRef]
48. Zhao, X.; Si, Y.-W. NFTCert: NFT-Based Certificates with Online Payment Gateway. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; pp. 538–543.
49. Nikolić, S.; Matić, S.; Čapko, D.; Vukmirović, S.; Nedić, N. Development of a Blockchain-Based Application for Digital Certificates in Education. In Proceedings of the 2022 30th Telecommunications Forum (TELFOR), Belgrade, Serbia, 15–16 November 2022; pp. 1–4.
50. Marjit, U.; Kumar, P. Towards a Decentralized and Distributed Framework for Open Educational Resources based on IPFS and Blockchain. In Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 13–14 March 2020; pp. 1–6. [CrossRef]
51. Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M.; Holt, J. Decentralized identifiers (dids) v1.0. *Draft Community Gr. Rep.* 2022. Available online: https://www.w3.org/TR/did-core/ (accessed on 14 October 2023).
52. Tahlil, T.; Gomasta, S.S.; Ali, A.B.M.S. AlgoCert: Adopt Non-transferable NFT for the Issuance and Verification of Educational Certificates using Algorand Blockchain. In Proceedings of the 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), Gold Coast, Australia, 18–20 December 2022; pp. 1–8.
53. Pfeiffer, A.; Denk, N.; Serada, A.; Dingli, A. Digital identities, nfts and ai in the education sector: Showcasing a demonstrator. In Proceedings of the 16th International Technology, Education and Development Conference, Valencia, Spain, 7–8 March 2022; pp. 6867–6876.
54. Chalmers, D.; Fisch, C.; Matthews, R.; Quinn, W.; Recker, J. Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs? *J. Bus. Ventur. Insights* **2022**, *17*, e00309. [CrossRef]
55. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Comput. Surv.* **2021**, *54*, 168. [CrossRef]
56. Wang, G.; Wang, Q.; Chen, S. Exploring Blockchains Interoperability: A Systematic Survey. *ACM Comput. Surv.* **2023**, *55*, 290. [CrossRef]

57. Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. *Towards Blockchain Interoperability*; Springer: Cham, Switherland, 2019; pp. 3–10.
58. Monika; Bhatia, R. Interoperability Solutions for Blockchain. In Proceedings of the 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 9–10 October 2020; pp. 381–385.
59. Lafourcade, P.; Lombard-Platet, M. About blockchain interoperability. *Inf. Process. Lett.* **2020**, *161*, 105976. [CrossRef]
60. Arenas, R.; Fernandez, P. CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. In Proceedings of the IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17–20 June 2018; pp. 1–6.
61. Arndt, T.; Guercio, A. Blockchain-based transcripts for mobile higher-education. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 84–89. [CrossRef]
62. Badyal, S.; Chowdhary, A. Alumnichain: Blockchain based records verification service. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 4296–4299. [CrossRef]
63. Baldi, M.; Chiaraluce, F.; Kodra, M.; Spalazzi, L. Security analysis of a blockchain-based protocol for the certification of academic credentials. *arXiv* **2019**, arXiv:1910.04622.
64. Bore, N.; Karumba, S.; Mutahi, J.; Darnell, S.S.; Wayua, C.; Weldemariam, K. Towards Blockchain-enabled school information hub. In Proceedings of the Ninth International Conference on Information and Communication Technologies and Development—ICTD '17, Lahore, Pakistan, 16–19 November 2017; pp. 1–4.
65. Cheng, J.-C.; Lee, N.-Y.; Chi, C.; Chen, Y.-H. Blockchain and Smart Contract for Digital Certificate. In Proceedings of the IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 13–17 April 2018; pp. 1046–1051.
66. Cheng, H.; Lu, J.; Xiang, Z.; Song, B. *A Permissioned Blockchain-Based Platform for Education Certificate Verification*; Zheng, Z., Dai, H.-N., Fu, X., Chen, B., Eds.; Springer: Singapore, 2020; Volume 3, pp. 456–471.
67. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. UniChain: A Design of Blockchain-Based System for Electronic Academic Records Access and Permissions Management. *Appl. Sci.* **2019**, *9*, 4966. [CrossRef]
68. Ghazal, O.; Saleh, O.S. A graduation certificate verification model via utilization of the blockchain technology. *J. Telecommun. Electron. Comput. Eng.* **2018**, *10*, 29–34.
69. Gresch, J.; Rodrigues, B.; Scheid, E.; Kanhere, S.S.; Stiller, B. The proposal of a blockchain-based architecture for transparent certificate handling. In *Proceedings of the Lecture Notes in Business Information Processing*; Abramowicz, W., Paschke, A., Eds.; Springer Verlag: Cham, Switherland, 2019; Volume 339, pp. 185–196.
70. Han, M.; Li, Z.; He, J.; Wu, D.; Xie, Y.; Baba, A. A Novel Blockchain-based Education Records Verification Solution. In Proceedings of the 19th Annual SIG Conference on Information Technology Education, Fort Lauderdale, FL, USA, 3–6 October 2018; pp. 178–183. [CrossRef]
71. Jeong, W.-Y.; Choi, M. Design of recruitment management platform using digital certificate on blockchain. *J. Inf. Process. Syst.* **2019**, *15*, 707–716. [CrossRef]
72. KARATAŞ, E. Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System. *Int. J. Inform. Technol.* **2018**, *11*, 399–406. [CrossRef]
73. Kuvshinov, K.; Nikiforov, I.; Mostovoy, J.; Mukhutdinov, D. Disciplina: Blockchain for Education. 2018. Available online: https://www.disciplina.io/yellowpaper.pdf (accessed on 21 February 2021).
74. Lam, T.Y.; Dongol, B. A blockchain-enabled e-learning platform. *Interact. Learn. Environ.* **2020**, *30*, 1229–1251. [CrossRef]
75. Ocheja, P.; Flanagan, B.; Ueda, H.; Ogata, H. Managing lifelong learning records through blockchain. *Res. Pract. Technol. Enhanc. Learn.* **2019**, *14*, 4. [CrossRef]
76. Prinz, W.; Kolvenbach, S.; Ruland, R. Blockchain for Education: Lifelong Learning Passport. *ERCIM News* **2020**, *120*, 15–16.
77. Rooksby, J.; Dimitrov, K. Trustless education? A blockchain system for university grades. *Ubiquity J. Pervasive Media* **2020**, *6*, 83–88. [CrossRef]
78. Sun, H.; Wang, X.; Wang, X. Application of blockchain technology in online education. *Int. J. Emerg. Technol. Learn.* **2018**, *13*, 252–259. [CrossRef]
79. Wahab, A.; Barlas, M.; Mahmood, W. Zenith Certifier: A Framework to Authenticate Academic Verifications Using Tangle. *J. Softw. Syst. Dev.* **2018**, *2018*, 13.
80. Xu, Y.; Zhao, S.; Kong, L.; Zheng, Y.; Zhang, S.; Li, Q. ECBC: A High Performance Educational Certificate Blockchain with Efficient Query. In *Proceedings of the Theoretical Aspects of Computing—ICTAC 2017*; Van Hung, D., Kapur, D., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switherland, 2017; Volume 10580, pp. 288–304.
81. Non-Fungible Token Standard 721. Available online: https://github.com/ethereum/ercs/blob/master/ERCS/erc-721.md (accessed on 1 December 2023).
82. Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. FastFabric: Scaling hyperledger fabric to 20,000 transactions per second. *Int. J. Netw. Manag.* **2020**, *30*, e2099. [CrossRef]
83. Agencia Española de Protección de Datos (AEPD); European Data Protection Supervisor (EDPS). Introduction to the Hash Function as a Personal Data Pseudonymisation Technique. 2019. Available online: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en (accessed on 14 October 2023).

84. CNIL. Blockchain and the Gdpr: Solutions for a Responsible Use of The Blockchain in the Context of Personal Data. 2018. Available online: https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (accessed on 14 October 2023).
85. Cai, B. ERC-5484: Consensual Soulbound Tokens. Available online: https://eips.ethereum.org/EIPS/eip-5484 (accessed on 14 October 2023).

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.