

Article

Qualitative Analysis of a Blockchain-Based System Adoption for Academic Credentials Verification That Complies with the GDPR: GAVIN Project

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

atlanTTic, University of Vigo, 36310 Vigo, Spain; christian.voneitzen@det.uvigo.es (C.D.-v.-E.); manolo@uvigo.es (M.J.F.-I.); maria.ruiz@det.uvigo.es (M.R.-M.)

* Correspondence: lanido@det.uvigo.es

Abstract

This article presents a qualitative analysis of GAVIN, a Blockchain-based system for educational information management that is fully compliant with the General Data Protection Regulation (GDPR). This system was designed to address the challenges of academic credential verification and recovery in a context where academic certificate issuance and verification is highly fragmented, with institutions operating isolated systems that hinder efficient verification and facilitate the proliferation of fraudulent documents. The GAVIN model introduces a multi-blockchain architecture aimed at recognition of formal, non-formal, and informal learning, guaranteeing compliance with GDPR. After completing the design and development of a functional prototype, this study discusses its qualitative evaluation by means of a validation workshop with diverse stakeholders from the education sector, using pre- and post-workshop questionnaires grounded in the Technology Acceptance Model (TAM). Results indicate a strong perceived usefulness and significant potential to improve current credentialing processes. However, concerns were raised regarding implementation feasibility, associated costs, the need for official standardization, and the importance of establishing robust governance and sustainable business models. This study offers valuable insights into the challenges and opportunities of blockchain adoption in education, providing guidance for future development and policy-making.

Keywords: blockchain; GDPR; TAM; academic certifications; general data protection regulation; technology acceptance model



Academic Editor: Gianluca Lax

Received: 16 October 2025

Revised: 4 November 2025

Accepted: 7 November 2025

Published: 11 November 2025

Citation: Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J.; Ruiz-Molina, M. Qualitative Analysis of a Blockchain-Based System Adoption for Academic Credentials Verification That Complies with the GDPR: GAVIN Project. *Appl. Sci.* **2025**, *15*, 11958. <https://doi.org/10.3390/app152211958>

Copyright: © 2025 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

Currently, academic data is issued and stored within the isolated systems of individual educational institutions, with little to no interoperability among them. This fragmentation directly impacts the verification process, as authenticating records or certificates often requires manual procedures resulting in significant resource and time costs.

As global competition intensifies, the demand for verifiable proof of academic and professional qualifications has inadvertently fueled the spread of counterfeit educational credentials. These fraudulent documents come from various sources, including “degree factories” [1] that generate fake certificates for sale, documents created by nonexistent academic institutions [2], alterations of authentic documents with false dates or courses, certificates produced by dishonest employees of real institutions [2], and inaccurate translations of authentic documents used to meet requirements in other countries.

The inherent fragmentation of the current system, characterized by isolated institutional systems, the absence of universal standards, and reliance on manual verification, is the main cause of the prevalence of fraud and verification challenges. In this context, the problem extends beyond the existence of fake certificates; it stems from a fundamental lack of interoperability and robust trust mechanisms within the traditional academic qualifications ecosystem. Rather than introducing uncontrolled decentralization, the proposed solution aims to establish a controlled and verifiable decentralized system where trust is distributed and secured through cryptographic means, thereby reducing reliance on centralized, and often unreliable, authorities.

Moreover, universally accepted standards to represent academic information are nonexistent. A critical aspect, usually ignored, is the lack of traceability and verifiability in the case that an institution ceases its educational activities and disappears. This affects all forms of education, including formal, non-formal and informal, which are increasingly relevant in modern professional environments, as evidenced by major companies like Google [3], Amazon (https://aws.amazon.com/es/certification/?nc1=h_ls, accessed on 20 September 2025) and Microsoft (<https://learn.microsoft.com/en-us/credentials/>, accessed on 20 September 2025) which issue certificates for online courses.

The GAVIN project introduces an innovative solution that leverages blockchain technology to issue, store, retrieve, share, and verify academic information. It supports a flexible format that accommodates all types of certificates, ensures scalability, and complies with the GDPR [4]. The system is designed to harness key blockchain features such as immutability and traceability without requiring educational institutions to alter their existing information systems.

A core design principle of GAVIN is to return control of academic data to its rightful owners, allowing individuals to selectively share all or part of their credentials with third parties. Uniquely, GAVIN also addresses the critical challenge of data verification and recovery in cases where the issuing institution ceases to exist. The model is explicitly designed to meet the stringent requirements of the GDPR [5] while also tackling the scalability limitations typically associated with blockchain technologies.

The primary objective of this study is to qualitatively validate the GAVIN model as a technological solution for issuing and verifying academic certifications, ensuring its scalability, perceived usefulness, and compliance with the GDPR. To achieve this, the following hypotheses are proposed, inspired by the Technology Acceptance Model (TAM) for validating technological systems:

H1 (Perceived Usefulness): Participants from the education sector will perceive the GAVIN model as useful for improving the processes of issuing, verifying, and recovering academic certifications.

H2 (Security and Trust): Users will consider the GAVIN model to offer a more secure and trustworthy system compared to current procedures.

H3 (Feasibility): Participants will regard the implementation of the GAVIN model in their institutions as feasible within a medium-term timeframe (2 to 5 years), recognizing its adaptability to diverse educational environments.

H4 (Privacy Protection): Participants will positively evaluate the model's GDPR compliance as a key differentiating factor, given that data is handled in full compliance with one of the most rigorous data protection frameworks worldwide.

In summary, the main contributions of this work are threefold, namely (1) the design and development of a multi-blockchain architecture aimed at the issuance, verification, and retrieval of academic credentials through mechanisms that ensure strict GDPR compliance; (2) the functional validation of the proposed system through its implementation in the GAVIN project; and (3) the evaluation of user acceptance based on a qualitative methodology grounded in the Technology Acceptance Model (TAM).

The remainder of this article is organized as follows: Section 2 reviews related work; Section 3 outlines the blockchain technological context, the legal framework, and the impact of fraud within the global educational ecosystem; Section 4 presents the proposed model and its architecture; Section 5 details the validation process and the procedures applied; Section 6 reports the results; Section 7 discusses the scope and implications of the findings; and Section 8 concludes the paper.

2. Related Work

The educational sector is actively exploring blockchain technology and its applications to effectively protect academic information since 2013 [6]. Despite the growing number of blockchain-based initiatives in education, most remain in the early stages of practical development, and only a few have reached a level of maturity that allows practical adoption by academic institutions and related stakeholders.

An exhaustive analysis of the scientific literature reveals that the most frequent category for blockchain usage in education is the issuing and verification of academic certificates [7–33]. Illustrative examples include the introduction of Bitcoin to register academic certificates by the University of Nicosia in 2014 [6]. Another notable example is Blockcerts, from the MIT Media Lab [34], an open-source platform built on the Bitcoin and Ethereum blockchains for issuing and verifying academic diplomas. Both projects primarily record a hash digest of academic certificates on the blockchain, not the complete data.

EduCTX [35] represents a different approach focused on the issuance of tokens as credits to acquire learning competences, inspired by the European Credit Transfer System (ECTS). This research also indicates a predominant focus on the notarization and verification of academic certificates and records, with very little effort dedicated to more complex academic information, such as learning stories, learning content, or assessment data.

Sambasiva Rao et al. [36] investigated the use of distributed ledger technologies for issuing and verifying academic certificates, describing the fundamental operational flow and discussing the associated challenges. Their study mentions Layer 2 blockchains and Lightning Networks as potential solutions to scalability issues. However, regarding GDPR compliance, they only propose the use of protected sandboxes for experimentation with personal data, without presenting any real-world application or product.

Sudha et al. [37] address the challenge of storing certificate data on-chain by opting to store a SHA-256 hash of the data. Similarly, Al Sakib et al. [38] use hashing techniques to record data on-chain. Singh et al. [39] emphasize the need for systems to combat academic fraud and propose a solution that stores hashed certificate data on the blockchain, while using a peer-to-peer network to store the actual content. Although this approach may appear closer to GDPR compliance, it is still not acceptable because hashed data is not considered anonymous under GDPR provisions, since to be deemed as anonymous, data cannot be derived solely from the original data [40]. Moreover, fully decentralized public blockchain solutions are inherently non-compliant with GDPR, as all nodes have access to the stored content, potentially leading to privacy breaches.

Anandapadmanaban et al. [41] introduce the use of NFTs on the Ethereum public blockchain to issue certificates under the EduChain initiative. However, this approach

also fails to meet GDPR requirements. Stefan-Robert and Butincu [42] propose a model with on-chain access control and revocation mechanisms, similar to the GAVIN model. Their system uses peer-to-peer networks to store original certificate data, which is not GDPR-compliant, as discussed above. While their paper includes the development of smart contracts, it does not present a working prototype or any user feedback through surveys.

Most of the reviewed articles present theoretical models without practical implementation or testing. Exceptions include papers [38,41], which describe and showcase developed prototypes of their proposed solutions. However, none of these works include user testing or feedback from real users interacting with the systems. Additionally, studies published prior to 2021 [29] do not address GDPR compliance, nor do they explore strategies for meeting its requirements.

On the other hand, several studies used surveys to explore the adoption of blockchain in the academic sector. For instance, ref. [43] applies the Technology Acceptance Model (TAM) [44] to evaluate the factors influencing individuals' willingness to integrate blockchain into educational settings, organizing questions according to TAM's core dimensions. Awaji et al. [45] focus on the use of blockchain by verifiers and stakeholders to validate academic information, emphasizing the need for a unified solution regardless of the origin of the data. In [46], the authors assess the acceptance of a blockchain-based model for issuing and validating certificates, using hypotheses related to trust, privacy, social influence, efficiency, and cost. Similarly, ref. [47] investigates the feasibility of implementing blockchain technologies in higher education institutions through qualitative surveys and interviews with professors. Mohammad and Vargas [48] present a qualitative evaluation of the challenges reported by participants regarding blockchain adoption in education, based on survey responses. However, none of these studies include user testing of a specific model designed for direct interaction, nor do they assess the usability and functionality of such systems from the end-user perspective.

We can conclude that most blockchain research in education is focused on the issuing and verification of academic certificates. Previous research also shows that compliance with data and privacy regulations, which is instrumental in any open system managing academic certificates, is a challenge that is still unsolved. Existing literature also emphasizes the importance of addressing educational information beyond certification in a scenario where there are no universally accepted standards for representing academic information [34,49,50].

With the exception of Kuvshinov et al. [51], nearly all the analyzed initiatives rely on a single blockchain, an approach that simplifies design but inherently constrains performance and scalability. Wahab et al. [52] proposed Tangle as their technological foundation, a fast blockchain that currently does not offer full support for smart contracts. Academic information is stored using a combination of off-chain and on-chain systems using diverse approaches.

With the exception of the works by Molina et al. [53], Daraghmi et al. [54] and Lam and Dongol [49], none of the investigated initiatives comprehensively addresses GDPR compliance. However, the two later proposals address GDPR compliance only partially. Only a limited number of initiatives implement data encryption to protect the information.

3. Context

To understand the relevance and scope of the GAVIN project, the technological, legal, and systemic context in which it operates is briefly discussed below. This section outlines the foundational concepts of blockchain and smart contracts, the regulatory framework established by the GDPR, and the broader challenges posed by fraud and fragmentation in the global education ecosystem. Together, these elements provide the backdrop for

the development and evaluation of a secure, scalable, and privacy-compliant solution for academic credential verification.

3.1. Blockchain and Smart Contracts

A blockchain, originally proposed by Nakamoto as the ledger for Bitcoin [55], can be understood as a distributed and decentralized database replicated across the nodes of a peer-to-peer network. Data is structured into blocks that store records and are securely linked through cryptographic methods to form a digital ledger. Each block contains transactions and additional data, along with a reference to the hash of the preceding block, thus preserving the integrity and continuity of the chain. This design allows any user to verify a transaction once it has been recorded. Thanks to cryptography, the records become immutable and trustworthy without the need for a central authority.

Several types of blockchain coexist, each with its specific characteristics:

- Public blockchains are open and fully decentralized, meaning anyone can submit transactions, run a node on the network, or participate in block creation. Their main strength lies in transparency and data integrity assurance, although they face limitations in scalability and validation speed. Information confidentiality is virtually nonexistent, as all data is exposed to network nodes. While encrypted data can be stored, the immutable nature of the blockchain poses future risks if encryption algorithms become obsolete. Public blockchains are suitable for scenarios where transparency and decentralization are essential, such as cryptocurrencies. Examples include Bitcoin and Ethereum [56].
- Private blockchains are managed by a single organization and are typically referred to as permissioned blockchains, as access is granted by the implementing entity. A prominent example includes solutions developed under the Hyperledger framework by the Linux Foundation [57,58]. Since participants in these networks are identified, consensus mechanisms are less demanding, resulting in faster block creation and improved scalability. Their main advantage is privacy, as only authorized nodes can access the data. This type of blockchain is particularly appealing to businesses and financial institutions that require control, confidentiality, and immutable record-keeping.
- Consortium or federated blockchains are jointly managed by multiple organizations, each operating its own nodes. Although participation requires permission, some information can be shared publicly. This places them between public and private blockchains, combining advantages and limitations from both models.

At this point it is important to highlight the concept of smart contracts, introduced by Nick Szabo [59]. These are pieces of code that run automatically when triggered by a user or another smart contract, performing predefined functions as specified in their logic. Once deployed on a blockchain, smart contracts benefit from immutability, resistance to tampering, and autonomous execution without human intervention. Ethereum [60] stands out as one of the most prominent platforms for implementing such contracts, due to its robust support for decentralized applications.

3.2. The General Data Protection Regulation (GDPR)

The General Data Protection Regulation [4] is a regulation of the European Parliament that governs the protection of individuals with regard to the processing of personal data and the free movement of such data within the European Union. This legal framework covers both clearly identifiable data (e.g., name, address, or date of birth) and any other element that, alone or in combination, can be used to identify an individual. Given the severity of financial penalties for non-compliance, any project involving personal information must

be designed according to the principle of ‘privacy, security, and legality by design’, as established in Art. 25(1) of the regulation, through the implementation of appropriate technical and organizational measures.

The GDPR stands as a key framework ensuring that data processing is conducted lawfully, transparently, and with full accountability, in accordance with Article 5. Its scope applies to data controllers and processors operating within the EU, as well as entities abroad processing EU residents’ data in the context of offering goods or services. Compliance with the regulation not only mitigates legal and financial risks but also strengthens the operational integrity of systems by ensuring mechanisms for control, data minimization, informed consent, and traceability of operations.

3.3. Impact of Fraud in the Global Education Ecosystem

The growing number of fake certificates and fraudulent academic information in an increasingly interconnected society represents a real and growing threat to the integrity of the education systems and even the labour market [61]. Beyond the problem of fraud, the absence of a globally accessible platform for academic information constrains the ability to gain a comprehensive understanding of the most demanded fields of study and to compare how students in different countries obtain their qualifications. This represents a missed opportunity to extract valuable educational insights and inform policy development.

The shortcomings of the current system go beyond security concerns, making it difficult to verify diverse types of educational credentials within a unified framework. The problem is both about ensuring the security and integrity of academic records and also about enabling global verification of educational data. A comprehensive solution, such as the GAVIN proposal, must address both defensive aspects (e.g., fraud prevention, data integrity) and proactive capabilities such as unified verification tools, transforming a security challenge into an opportunity for systemic improvement and innovation in the education sector.

4. The GAVIN Project

The current landscape of blockchain applications in education reveals several critical limitations. Most existing solutions struggle to fully comply with the GDPR, fail to comprehensively record diverse types of academic data, and do not adequately address scalability, which in turn is an essential factor for widespread adoption. These shortcomings significantly restrict their practical applicability.

A major gap in the educational ecosystem is the absence of universally accepted standards and centralized yet trustworthy systems for managing academic records. Blockchain technology has the potential to fill this void, but only if it effectively resolves key challenges related to privacy and scalability.

The literature consistently highlights that many blockchain-based educational solutions fall short in terms of GDPR compliance and scalability. These are not minor technical issues, but they are fundamental barriers to real-world adoption, often overlooked in existing implementations. GAVIN’s core purpose is not merely to introduce another blockchain solution, but to offer one that, through its architectural design, directly addresses these critical and frequently neglected challenges. This strategic focus positions GAVIN as a more mature, practical, and legally robust alternative for deployment in complex educational environments.

GAVIN also incorporates mechanisms for data recovery to prevent information loss, similar to other initiatives. However, it goes a step further by guaranteeing data persistence even if the issuing academic institution ceases to operate, thereby reinforcing its GDPR compliance and distinguishing it as a unique solution. Another key feature of the GAVIN

framework is its ability to selectively share specific portions of a holder's educational data. It also supports a wide range of academic information formats, offering flexibility in registry structures.

A direct comparison with other existing solutions [62] demonstrates that GAVIN is fully GDPR-compliant, with this compliance being a strategic advantage validated by experts [5]. The widespread lack of GDPR adherence among current solutions underscores a significant regulatory and design challenge, which, incidentally, GAVIN successfully overcomes. While this achievement requires a more complex architecture, such as off-chain storage of personal data, it results in a legally stronger and more reliable system. GDPR compliance is thus a central innovation and a key differentiator for the GAVIN project, making it a viable and trustworthy solution for real-world implementation.

4.1. Architecture and Key Components

GAVIN enables the issuance, storage, verification, and retrieval of academic data spanning formal and informal learning settings. It supports several application scenarios, including the issuing of certificates and the integrated management of academic information, the registry of learning paths, the tracking of competency values, and recording academic credits of any kind, with a fully variable and flexible number of fields.

The key elements of the proposed design and its dynamics are depicted in Figure 1, which provides a general overview of the architecture of the system.

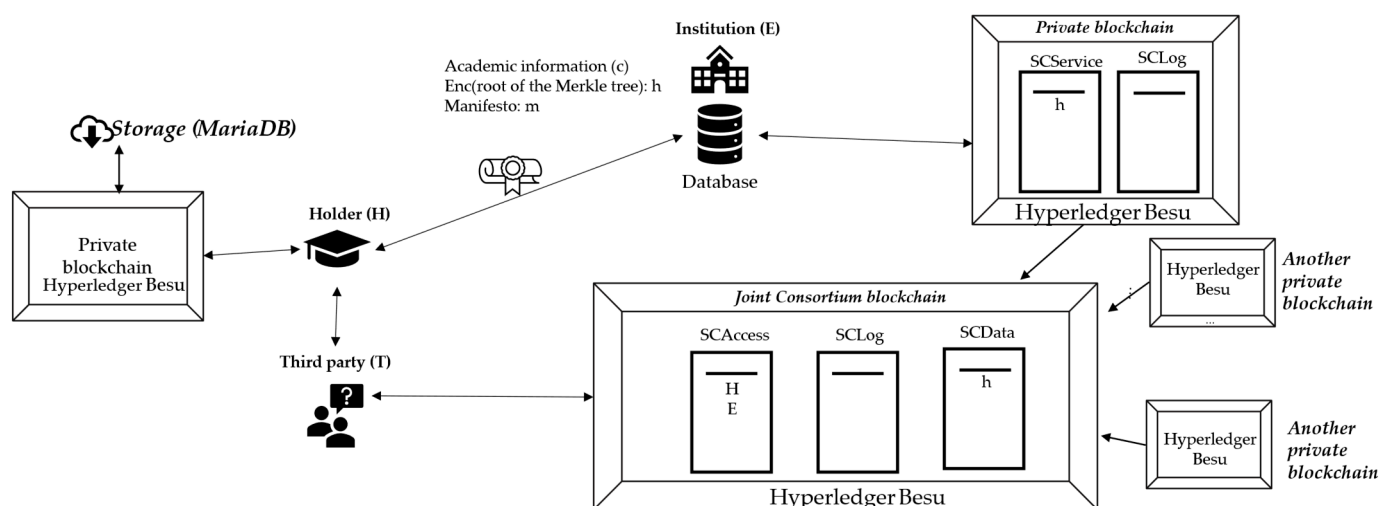


Figure 1. System architecture overview and technologies involved.

4.2. GAVIN's Privacy by Design

The GAVIN model is designed under the "Privacy by Design" principle (Art. 25) as a key requirement. It complies with Art. 6, Section 1 of the GDPR and other related articles, ensuring that data subjects retain control over access to their own personal information. This includes the ability to selectively share their data according to their preferences, to receive notifications when their information is processed, and to request and retrieve their personal records (Art. 20). Moreover, the system supports the critical functionality of granting and revoking permissions to specific third parties (Art. 7, Section 3). Technically, the "right to erasure" (i.e., the "right to be forgotten" in Art. 17) is explicitly considered in GAVIN's core design.

To be compliant with the GDPR, personal academic data is stored in the databases of the educational institutions and not directly on the blockchain. This design choice directly addresses the fundamental conflict between blockchain's immutability and GDPR

requirements, as hash digests of personal data are explicitly deemed as not valid as an anonymization technique from the point of view of the GDPR [63,64].

GAVIN's strong focus on GDPR compliance drives a key architectural decision: storing sensitive personal data off-chain within institutional databases. This choice is not merely about improving efficiency or storage capacity but a legal necessity. Blockchain's inherent immutability conflicts with the GDPR's "right to erasure", making off-chain storage a foundational requirement. Combined with encryption and key management, this approach reflects an [63,64] innovative response to strict regulatory demands, as it demonstrates how legal constraints can inspire new architectural models in blockchain design, resulting in systems that are both more robust and legally compliant.

4.3. GAVIN's Multi-Blockchain Architecture

To tackle scalability and performance challenges, GAVIN adopts a multi-blockchain architecture. Its core consists of a consortium blockchain composed of prominent national and international organizations connected to the education sector. This main chain is linked to an open-ended number of private blockchains, each operated by regional or local academic institutions. These private blockchains function independently and are self-managed, periodically transmitting selected transactions to the consortium blockchain.

This distributed model efficiently handles the complex process of issuing academic credentials, aligning with modern scalability strategies. It is particularly well-suited to the globally fragmented landscape of educational document issuers.

Note that GAVIN's multi-blockchain design is not a generic technical fix addressing scalability, but a deliberate response to the decentralized and autonomous nature of global education. By respecting institutional independence and avoiding the need for a centralized, monolithic infrastructure, GAVIN offers a solution that integrates seamlessly into legacy educational structures. Besides enhancing scalability, this architectural alignment with real-world educational ecosystems makes GAVIN more adaptable, less disruptive, and more likely to be accepted by diverse institutions.

4.4. Academic Information Workflow in GAVIN

The process, depicted in Figure 2, is initiated with an academic institution (E) issuing a certificate containing both sensitive elements (for example, name, title) and non-sensitive information (for example, academic information type, course's name). A Merkle Tree is generated from the certificate and registered in the private database of the issuing institution (idp). Subsequently, a transaction is submitted to a private blockchain containing a reference to the internal database record (idp), the location of the database server's access point (se), the encrypted root of the Merkle Tree (h), a validity indicator, and a list of authorized accounts (aa).

In GAVIN's architecture, each branch of the Merkle Tree represents a distinct data element, structured according to the issuing institution's data model. These nodes contain not only academic information but also flexible metadata, such as certificate validity, expiration dates, and other relevant attributes.

To enhance security, each data element within the tree is associated with a unique, non-trivial secret key. A keyed message authentication code (KMAC), based on SHA3 [65], is then computed for each element. This process ensures that the final Merkle Tree root encapsulates both the academic data and its corresponding authentication codes. The issuing entity (E) shares the secret key with the data holder (H), adding an additional layer of anonymization.

KMAC plays a critical role in guaranteeing data integrity and authenticity, as only those with the correct secret key may generate valid authentication codes. Its resistance to

preimage and length-extension attacks makes it particularly suitable for environments like GAVIN, where sensitive information must be shared selectively. This method is recognized as a secure approach to data anonymization [5,64].

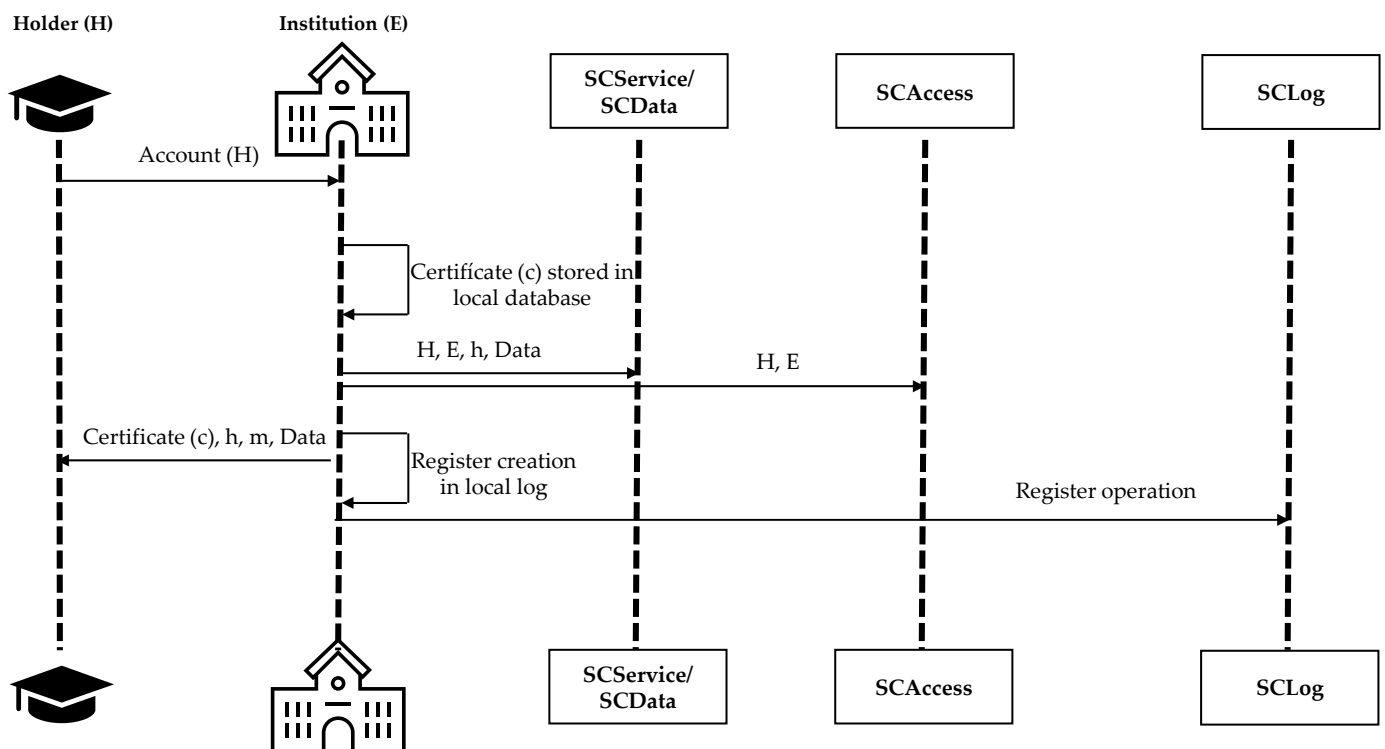


Figure 2. Issuance of academic information.

In a nutshell, each item in the Merkle Tree combines academic data with a unique key provided by the issuer to the holder, ensuring that shared information remains anonymized and protected. This structure allows for granular control over data disclosure: third parties can verify only the specific elements required, without accessing the full dataset, supporting secure, selective sharing.

Optionally, non-sensitive public data (pd) (“Data”) can be added to the transaction in the blockchain for the sake of global data analysis as described in the model [61]. The full certification (c), its encrypted Merkle Tree (h) and its manifesto (m) are transmitted in a secure way to the holder. All the operations are registered in a local log, which is hashed and sent to the blockchain SCLog to guarantee traceability. SCService provides the only authorized access point to the institution’s database. Periodically, the private blockchain transmits the registered information (h, idp, se, valid) to the smart contract SCData, on the main consortium blockchain, and the authorized accounts (aa) to SCAccess.

4.4.1. Verification of Academic Information

Three different cases are considered for the certificate verification by a third party (T):

- **Case 1: Holder-initiated verification.** In this scenario, the holder (H) shares the complete certificate (c) directly with a third party (T) and simultaneously grants access permission by adding T’s account to the SCAccess smart contract (aa). T then requests the encrypted Merkle Tree root (h) from SCData, which verifies T’s authorization through SCAccess and records the access attempt in SCLog. If access is approved, SCData returns the validity status and h. T decrypts h using the issuing institution’s public key and compares it with the Merkle Tree root embedded in the received

certificate (c) to confirm its authenticity and ensure that it was not revoked. The process is represented in Figure 3.

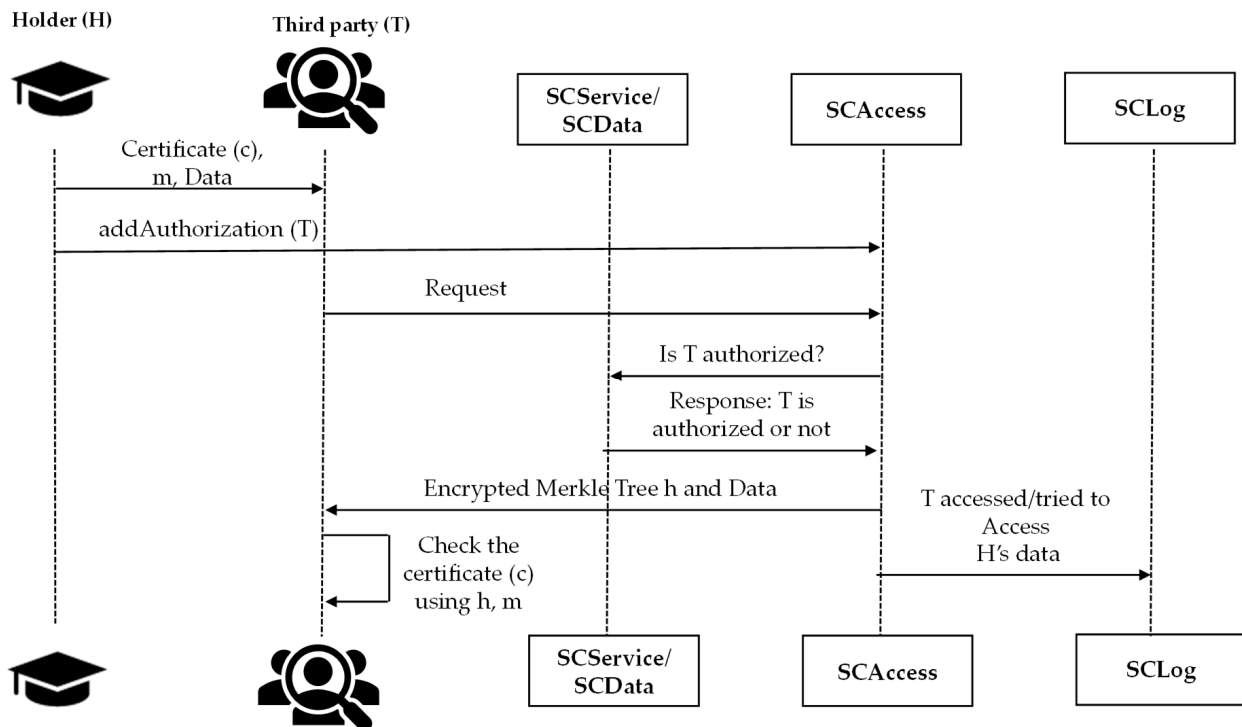


Figure 3. Case 1: Holder sends the certificate to a third party and allows for its verification.

- Case 2: Partial disclosure by the holder. In this case, the holder (H) chooses to share only a subset of the information contained in the certificate (c) with a third party (T), thereby protecting the privacy of non-essential data. To do so, H transmits only the selected information, the corresponding Merkle Tree paths, and the manifesto (m) through a secure channel. As in Case 1, H adds T's account to SCAccess (aa), specifying that this is a partial-access use case. When T requests the encrypted Merkle Tree root (h) from SCSData, the system checks the permissions in SCAccess and logs the request in SCLog. Once authorized, T retrieves the validity status and h, decrypts h using the issuer's public key, and verifies the integrity of the shared information by comparing the obtained root with the calculated Merkle Tree paths. Figure 4 describes the sequence diagram for this use case.
- Case 3: Institution-mediated verification. In this third scenario, the holder (H) authorizes the third party (T) to obtain the complete certificate (c) directly from the issuing institution (E). To enable this, H adds T's address to SCAccess (aa) and identifies the operation as a direct-access use case. T then requests from SCSData the internal database reference (idp) and the location of the institution's database server (se). After SCSData verifies the authorization through SCAccess, it provides these details to T. T uses them to request the certificate (c) from SCSData, which again validates the authorization and securely transmits the data. Both SCSData and SCSData record all access attempts and completed operations in SCLog. If necessary, T may subsequently verify the authenticity and validity of (c) following the procedure described in Case 1. This use case is outlined in Figure 5.

Non-sensitive public data stored on the consortium blockchain, such as the type, title, or category of academic credentials, may be anonymously analyzed to derive educational statistics and learning trends.

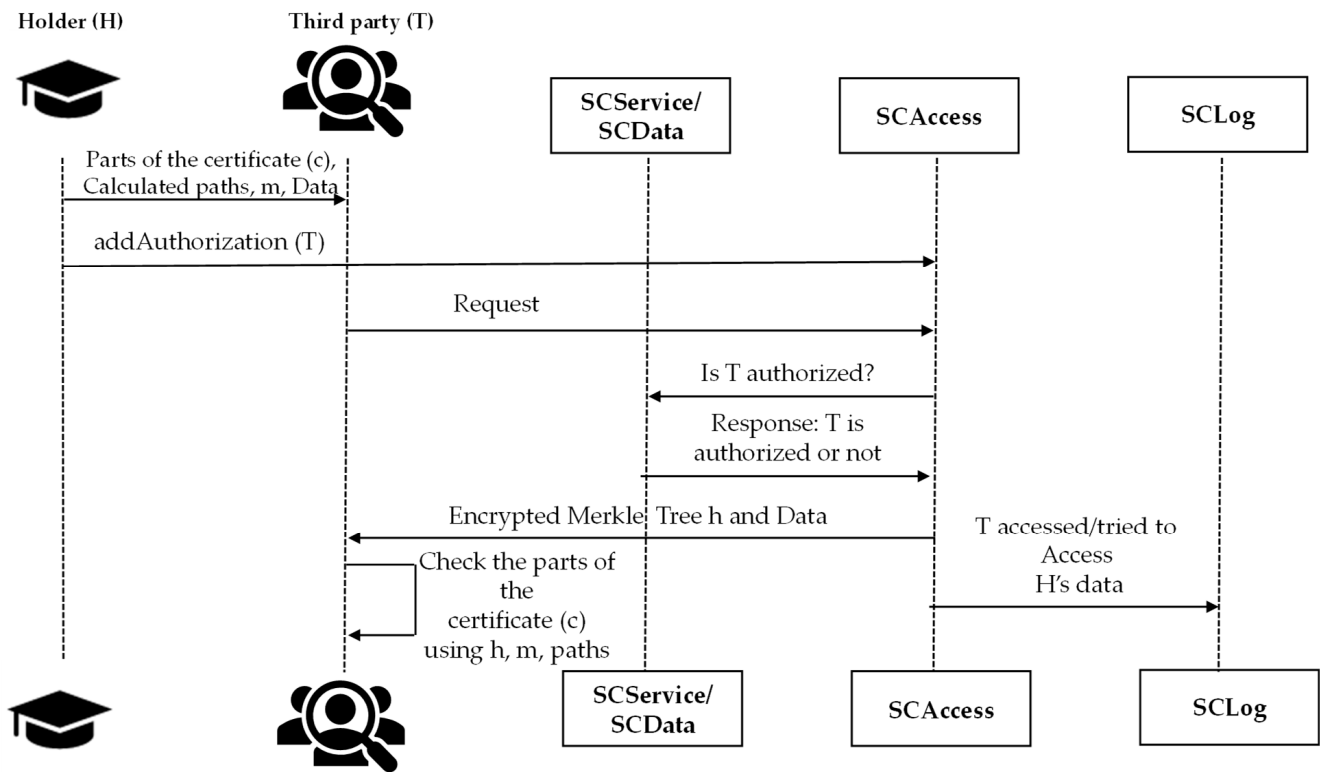


Figure 4. Case 2: The holder only wants to share the academic information partially.

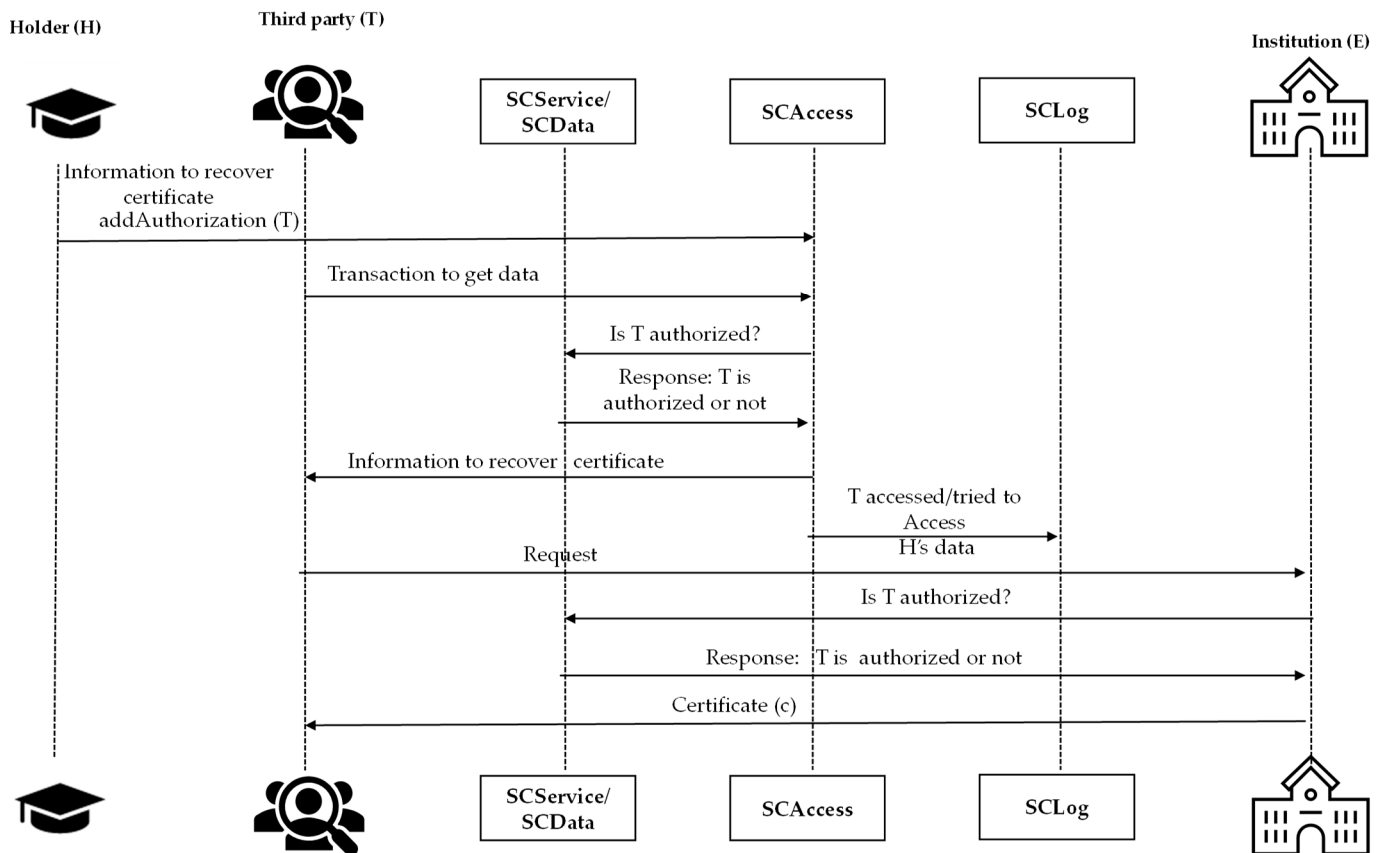


Figure 5. Case 3: The holder allows a third party to receive the certificate directly from the academic institution.

4.4.2. Modification of Academic Information

If either the academic institution (E) or the holder (H) needs to modify specific academic information (e.g., to correct a typographical error or inaccurate data) the issuing institution updates the information in its internal database, generates a new certificate (c'), and submits the corresponding new encrypted Merkle Tree root (h') to the SCSmart contract on the relevant blockchain. This process automatically generates a new transaction identifier (ID').

The institution then transmits the updated certificate (c') and, if necessary, a new manifesto (m') to the holder. As a result, any subsequent verification of the previous version of the certificate under Case 1 or Case 2 will indicate that a modification has occurred.

All modifications carried out in the institution's private database are recorded in SCLog to ensure full traceability. From that point onward, the same verification, modification, or deletion procedures described for new academic information apply to the updated data.

The overall sequence of this operation is illustrated in Figure 6.

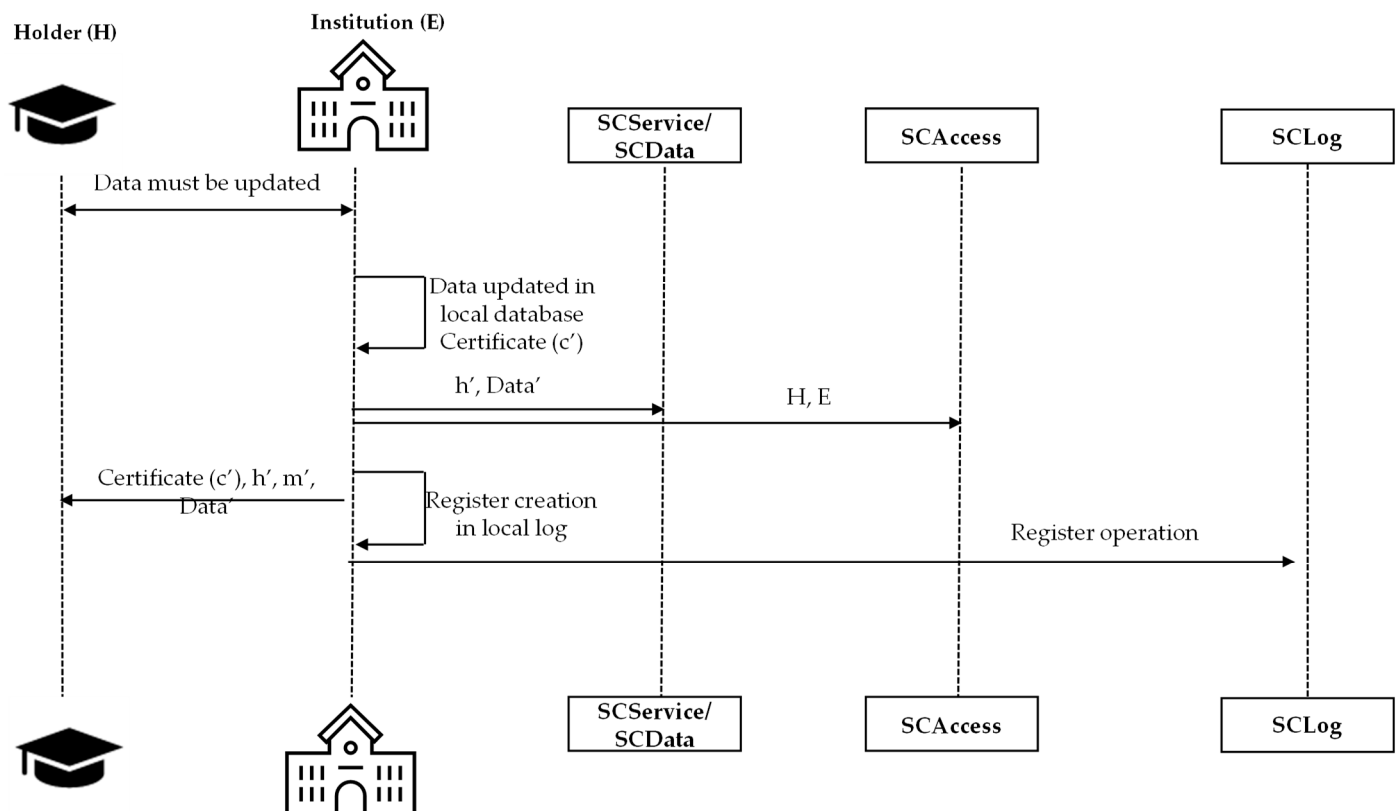


Figure 6. Modification of Academic Information.

4.4.3. Revocation/Deletion of Academic Information

Provided that such deletion is legally permissible, if the issuing institution (E) or the holder (H) decides to delete academic information, the institution must first remove the academic data from its internal database. It then updates the blockchain by marking the associated records in SCSmart and, subsequently, in SCData as invalid.

During this process, the linked data fields (i.e., idp , se , h) are reset to zero, and all accounts related to that record in SCAccess are deleted. Consequently, only non-personal information from past transactions, such as historical references to idp , se or h , remain stored on the blockchain.

Following the revocation, any attempt to verify the deleted academic data will return an error, confirming that the record is no longer valid or accessible.

The complete sequence of this procedure is illustrated in Figure 7.

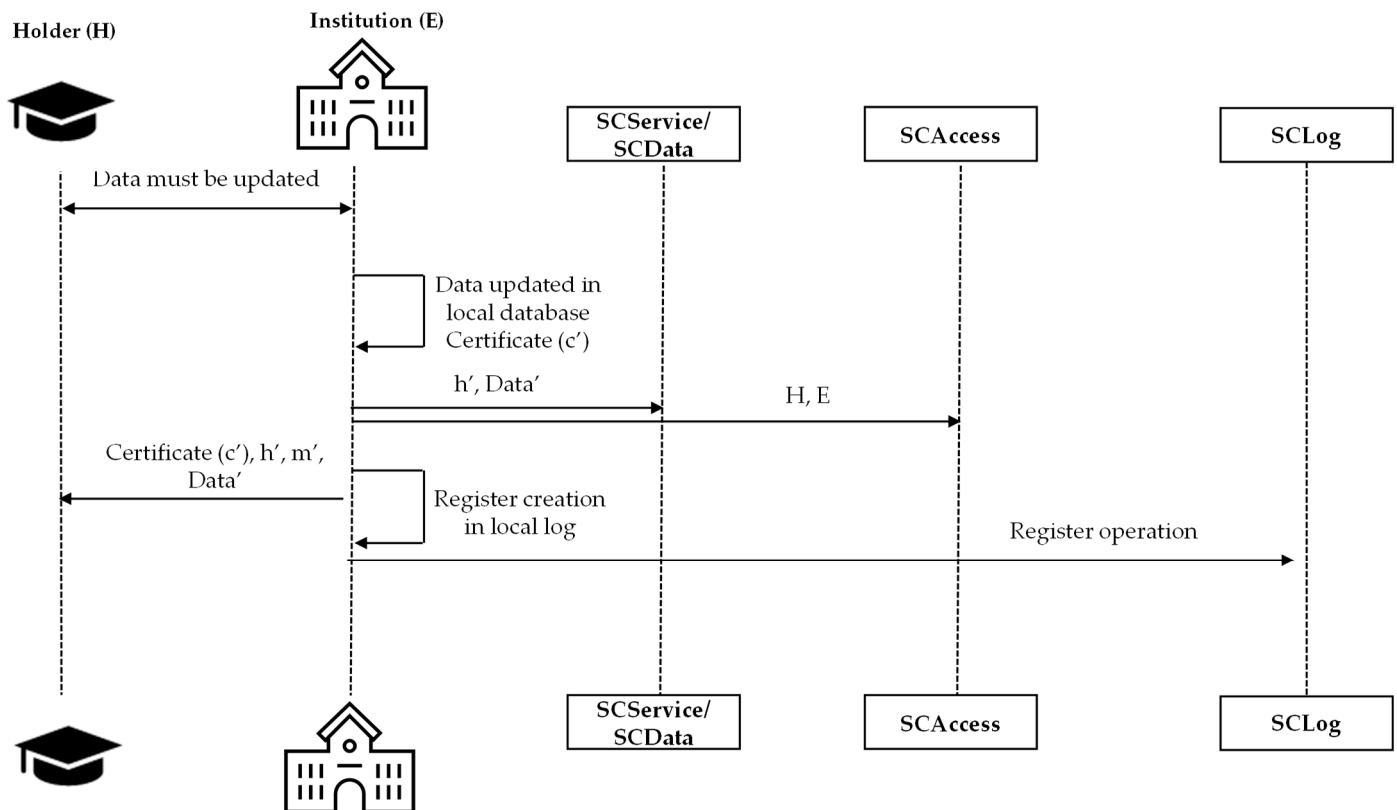


Figure 7. Revocation/Deletion of Academic Information.

4.4.4. Verification or Retrieval of Academic Information in Case of Institution Discontinuation

A persistent challenge for systems that store academic data off-chain in compliance with the GDPR is the inability to recover such information if the issuing institution ceases operations. This situation arises frequently in the contexts of non-formal and informal education, where organizations issuing credentials are often private companies or training entities that may later discontinue their activities.

In the proposed GAVIN model, if the holder (H) still possesses their certificate and the linked data, and the system remains functional except for the decommissioned issuer (E), verification can proceed normally under the procedures described in Cases 1 and 2. The authenticity of the certificate can thus be confirmed without depending on the institution's continued existence.

However, if the holder no longer retains the academic certificate and the issuing institution is no longer operational, meaning that its databases and servers are inaccessible, direct recovery of the information (Case 3) becomes impossible. To address this critical limitation, GAVIN introduces a dedicated recovery mechanism designed for situations in which an institution is expected to terminate its educational activities.

Before ceasing operations, the institution (E) must export the affected educational data, in its final encrypted form as stored in its databases, to a distributed storage infrastructure based on MariaDB. The encryption keys are shared with each data owner in accordance with GAVIN's cryptographic model. Access to this distributed storage is controlled through a private blockchain that acts as an authorization layer. The sequence of this publication process is shown in Figure 8.

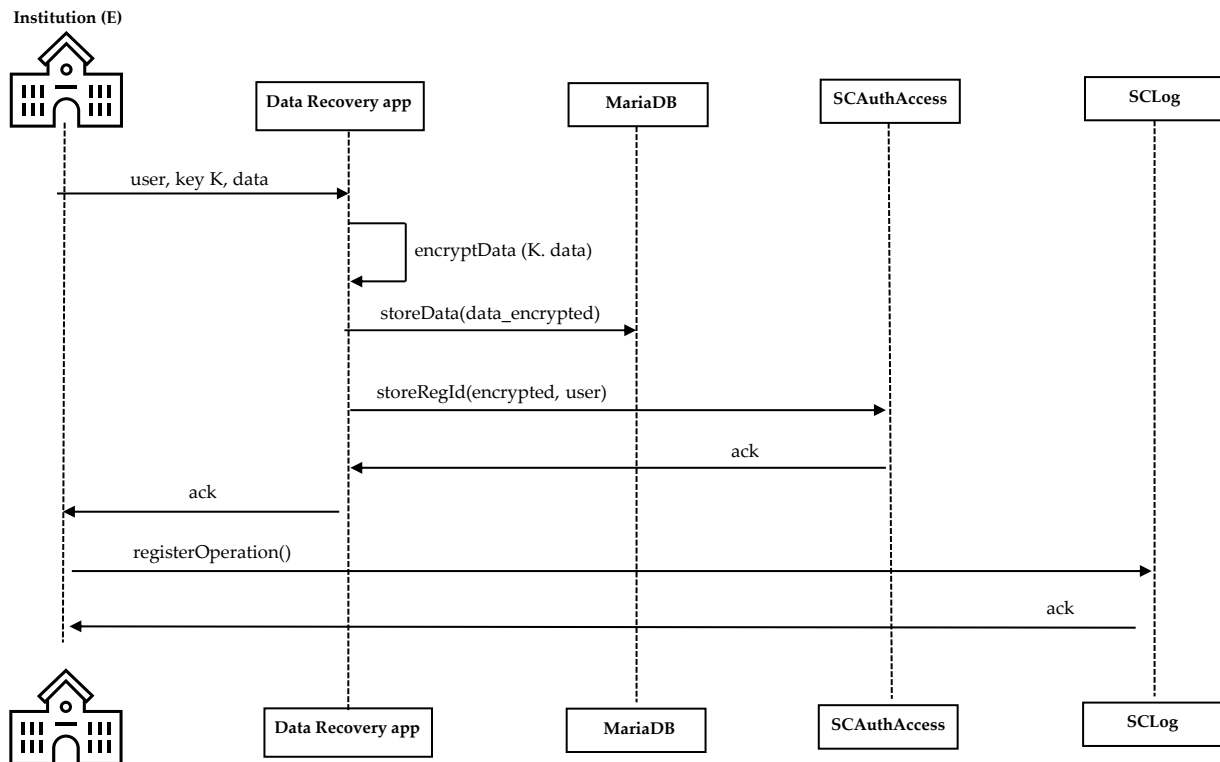


Figure 8. Storage of the academic information.

If a holder (H) wishes to retrieve their certificate after the institution's discontinuation, the private blockchain recognizes the holder as the legitimate data subject. Since H retains the encryption key previously shared with the institution (E), they can decrypt and recover their academic information directly from the distributed storage system. The retrieval process is depicted in Figure 9.

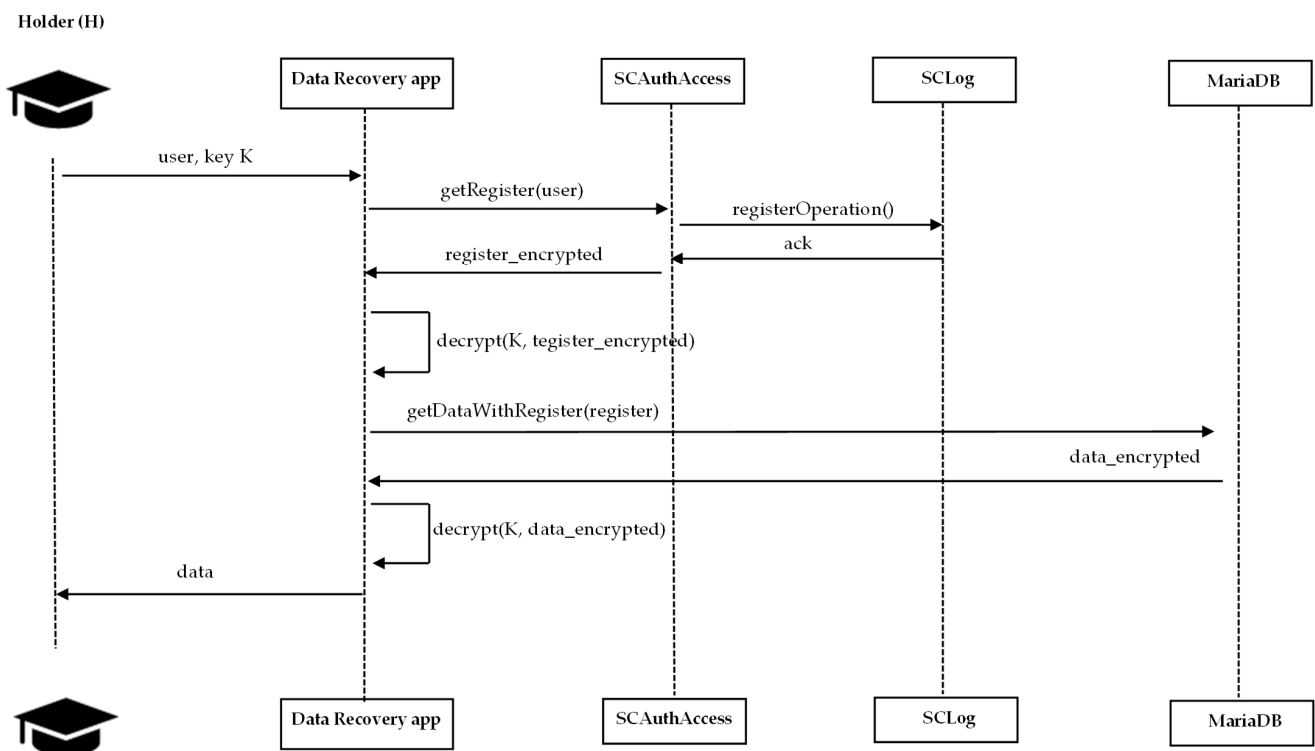


Figure 9. Retrieval of academic information.

Importantly, if the holder deletes their personal decryption key, the corresponding encrypted information becomes permanently inaccessible. Because the data remains stored in an encrypted form within a controlled private environment, its irreversibility through key deletion satisfies the GDPR's "right to erasure."

The distributed storage network must provide sufficient capacity and scalability to handle these records, though it is not intended to archive all academic data indefinitely, but only the encrypted records belonging to institutions that have permanently ceased operations.

4.5. GDPR Compliance

The proposed model has been conceived to meet the highest security and privacy standards, ensuring integrity, confidentiality, authentication, controlled access, availability, non-repudiation, and full conformity with the GDPR [5].

Because blockchain data is inherently immutable, any record stored on-chain cannot be altered after creation. This property guarantees data integrity. However, to preserve privacy and comply with the GDPR, only non-personal information is registered on the blockchain, while personal academic data is maintained securely off-chain within institutional databases.

In cases where an issuing institution ceases to operate, its encrypted academic records can be transferred to a distributed database protected by a blockchain-based access control mechanism. Since this information remains encrypted and can only be decrypted using the key jointly held by the data owner and the former institution, confidentiality is preserved.

Beyond security, the model also reinforces privacy through anonymization strategies. Holders can use distinct blockchain accounts for each certificate, preventing the correlation of multiple credentials with a single identity. All communications between entities in the system must occur over secure channels, and each participating node and institutional access point must implement robust protection measures. Likewise, private keys must be carefully managed to prevent unauthorized access.

Only third parties explicitly authorized by the data owner can access on-chain information used for validation or retrieval purposes. Every interaction is permanently recorded on the blockchain, creating an auditable log that guarantees accountability and transparency. Trust in the system is further reinforced by restricting participation in both private blockchains and the main consortium blockchain to recognized academic or institutional entities. If any participant acts inappropriately, their credentials can be revoked, invalidating all associated academic data.

Availability is inherently supported by the distributed nature of the blockchain network, which ensures that information remains accessible as long as any node remains active. Non-repudiation is also achieved, as all operations require participants to digitally sign transactions using their private keys, which are subsequently stored in immutable form on the blockchain.

Through this combination of architectural and procedural safeguards, the proposed model achieves GDPR compliance not as an isolated requirement but as an integral design principle, balancing transparency, privacy, and legal accountability within a secure, verifiable educational data ecosystem.

4.6. Proof-of-Concept Implementation

As depicted in Figure 1, the viability of the proposed model is demonstrated through the implementation of a proof-of-concept (<https://github.com/gavin-research/GavinProject>, accessed on 1 November 2025) using Hyperledger Besu [66], an advanced Ethereum client that facilitates confining a permissioned and privacy-enabled Ethereum

network using the privacy group feature [67,68], to create the private and consortium blockchains, which are connected, as represented in Figure 10, using an Inter-Blockchain Communication protocol (IBC YUI [69], developed by the Cosmos project [70]) that was specifically adapted for GAVIN [71].

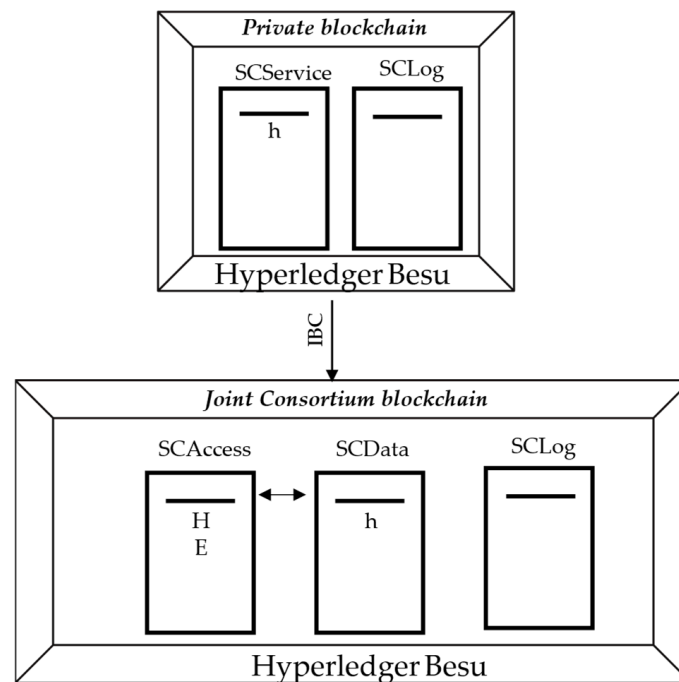


Figure 10. Interconnection between the private and consortium blockchains using IBC.

4.6.1. Holders and Third Parties

Both holders and third parties have a blockchain account in the system, which will be stored in a Metamask (<https://www.metamask.io>, accessed on 1 November 2025) wallet and allow them to consume the services provided in the web developed for GAVIN. The model assumes that holders and third-party users already possess consortium blockchain accounts. Their creation process is beyond this work's scope, as it relies on Hyperledger Besu's standard account generation procedure.

4.6.2. Education Institutions

Each participating educational institution is connected to one of the private blockchains built on Hyperledger Besu and holds at least one account with the necessary permissions to issue academic data.

The process of recovering a holder's account, generating a shared encryption key, issuing and encrypting academic information, storing it in the institution's internal database, and securely transferring the resulting data to the holder lies outside the scope of this implementation. Note that these operations depend on the specific configuration of each institution and are handled through secure data exchanges between the institution and the individual student.

This proof-of-concept focuses instead on the blockchain-related mechanisms. It assumes that each institution operates its own information system capable of interacting with the private blockchain via a secure API.

Because GAVIN employs a flexible data model, institutions can integrate without having to redesign their internal infrastructures, but only minor adaptations may be required to connect their local servers to the blockchain through the provided API, which must be appropriately secured.

A schematic representation of this integration is shown in Figure 11, where academic institutions communicate through an API to transmit verified data to their corresponding private blockchain.

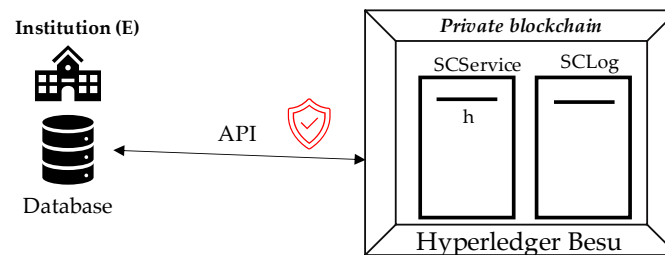


Figure 11. Academic institutions connect via an API to send data to the private blockchain.

4.6.3. Private Blockchains

In this initial proof-of-concept, each private blockchain is implemented using Hyperledger Besu. However, the proposed architecture is not limited to this framework, as any blockchain platform that supports account-level access control rather than node-level control, and is able to interoperate with the main consortium blockchain, may also be adopted, provided that it complies with the communication and data exchange mechanisms defined by the model.

Each private blockchain periodically transmits verified transactions and operational data to the consortium blockchain, ensuring coherence across the system. Communication between academic institutions and their corresponding private chains is carried out through a secure API, as outlined in the model.

The participating institutions within a private blockchain, as well as their assigned roles and permissions, are determined through an offline governance process. Each blockchain is provisioned with the computational and storage capacity required to manage the volume of data generated by its affiliated organizations.

Institutions are grouped into private blockchains according to relevant criteria such as geographic region, academic network, or institutional type. For instance, national public universities might share a single private blockchain, whereas university federations or consortiums could operate their own.

The management and maintenance of each private chain are the collective responsibility of the institutions that participate in it, ensuring decentralized control while maintaining regulatory and operational consistency.

4.6.4. Consortium Blockchain

The consortium blockchain functions as the system's central coordination layer, integrating information from all participating private blockchains. In the proof-of-concept implementation, it is also deployed using Hyperledger Besu, though the model remains platform-agnostic and compatible with any technology supporting Ethereum-compatible smart contracts and secure cross-chain communication.

This blockchain stores only non-personal metadata such as references to academic records, validation indicators, and information needed to trace data provenance. Personal or sensitive information is never recorded on this chain, in full compliance with GDPR principles.

The consortium blockchain operates under the shared governance of participating academic institutions and authorized educational authorities. Each authorized participant holds one or more validator nodes, which are responsible for confirming transactions and maintaining network integrity. Consensus is achieved through the IBFT (Istanbul Byzantine

Fault Tolerance) mechanism, ensuring both fault tolerance and high transaction throughput, as required by the model.

To facilitate interoperability, each private blockchain communicates periodically with the consortium layer, submitting verified records and updates through dedicated smart contracts (cf. Figure 1).

These smart contracts serve as the interface between private and consortium blockchains, enabling synchronization, verification, and decentralized auditability across the entire system. In the current proof-of-concept, the consortium blockchain acts as the public anchor of trust, ensuring transparency and providing an immutable record of all verification-related transactions while preserving the privacy of the underlying academic data [72].

4.6.5. Data Persistence for Discontinued Institutions

As outlined in Section 4.4.4, GAVIN provides a mechanism to preserve academic records if an issuing institution is discontinued. In such cases, the institution's encrypted academic records can be transferred to a distributed storage system based on MariaDB [73], with access control managed by a smart contract deployed on the consortium blockchain responsible for data verification.

To separate use cases and maintain modularity, this process is implemented using an additional blockchain built on Hyperledger Besu. The data transfer is carried out via an API protected by a Blockchain Application Firewall [74], allowing an authorized system operator to upload the institution's records to the MariaDB system. The smart contract then ensures that only the rightful data owner can access and decrypt the information. This enables continued use and sharing of the academic data, as described in use cases 1 and 2.

5. GAVIN Validation

To validate the Proof-of-Concept of the GAVIN project, a workshop was organized to gather feedback from potential end users. The workshop was organized to include people from various areas related to education, grouped into specific roles to ensure a wide range of opinions. The invited profiles included:

- Academic Administration Staff (AAS): Issuers of the credentials, responsible for managing student data and issuing them the certifications.
- Students and Job Seekers: Users of the system to whom academic information is issued, owners of their own data, equivalent to the role of "holders".
- IT Managers: Technical profile that provides an informed opinion on the technological choices and architecture of GAVIN's Proof-of-Concept.
- Human Resources and Recruiters: Verifiers of the academic certifications in the enterprises.
- Academic Decision-makers: Individuals responsible for managing and defining academic courses, whose opinion is essential for the integration of GAVIN into current academic environments.

A total of 91 people were invited, 75 confirmed their attendance, 73 completed the pre-workshop questionnaire, and 60 completed the post-workshop questionnaire.

5.1. Workshop Design

The preparation for the workshop included the draft of an introductory document, a formal invitation, and a presentation of the Proof-of-Concept and demonstration videos for each of the use cases discussed above.

5.1.1. Instruments

Two questionnaires were designed, one to be completed before and the other after the workshop, to facilitate the collection of ideas and opinions, allowing for a comparison of perceptions. The questionnaires were created using Microsoft Forms and made in three languages: Spanish, Galician, and English. To evaluate users' perceptions of the technology, the TAM [75] method was followed, which considers perceived usefulness, perceived ease of use, and perceived enjoyment.

5.1.2. Procedure

The workshop was structured with an introduction to the GAVIN project and its technologies, a technical demonstration, and a question-and-answer session. A video of the use cases was shown instead of a live demonstration to avoid potential technical errors during the workshop. Of the 91 people contacted, 75 confirmed their attendance, 73 responded to the pre-workshop questionnaire, and 60 responded to the post-workshop questionnaire.

5.1.3. Data Analysis

Responses were analysed quantitatively and qualitatively:

- Quantitative analysis: Arithmetic means and standard deviations were calculated for each question and role.
- Comparative analysis: Pre- and post-workshop responses were compared to assess changes in perception.
- Qualitative analysis: Open-ended responses were categorized to identify recurring themes, concerns, and suggestions.

The analysis focused on validating the hypotheses related to usefulness, trust, scalability, and GDPR compliance.

6. Validation Results

This section discusses the outcomes of the validation workshop, that is, the analysis of the responses obtained from the pre- and post-workshop questionnaires.

6.1. Pre-Workshop Questionnaire

The pre-workshop questionnaire, completed by 73 participants, probed initial expectations and familiarity with relevant aspects of the project. The distribution of roles was balanced, with a lower participation of the profile "Student/Seeking for a job".

In terms of familiarity with academic certification verification systems, there was an equal split between those who were familiar with them and those who were not, with the majority of those being familiar occasional users. Satisfaction with current verification systems was low, with an average of 2.80 out of 5 for all roles, indicating widespread dissatisfaction. The frequency of fraud issues, verification difficulties, or incomplete verification was perceived as moderately frequent, with an average of 2.63 out of 5, which proves the need for a solution.

General knowledge about blockchain technology, which is fundamental to the model, was low, with an average score of 2.37 out of 5, indicating a superficial understanding on the part of most respondents. In contrast, knowledge about the limitations of the General Data Protection Regulation was slightly higher, with an average score of 2.93, showing a higher level of understanding in comparison with the technical side.

A very positive result was the perception of the usefulness of a system to verify the authenticity of academic certificates, with an average of 4.57 out of 5, indicating strong agreement with the need for a system like that. Similarly, most respondents felt that such

a system would improve their institutions' current procedures for issuing and verifying certifications, with an average of 4.17. However, conviction about the feasibility of implementing such a system in their own institutions was lower, although still in the majority, with an average of 3.91.

The most frequently expressed expectation in the open questions was “To learn more about the model/technologies/system developed”, demonstrating clear curiosity about the developed model of GAVIN. Some respondents mentioned micro-credentials, SIGMA—a cloud-based academic management system widely used in Spanish universities (<https://www.sigmaaie.org/en/solutions/sigma-academic>, accessed on 20 September 2025), and Europass (<https://europass.europa.eu/en>, accessed on 20 September 2025), indicating their knowledge of current systems related to the issuance of academic certifications.

The analysis by roles in the pre-workshop questionnaire revealed a variety of perceptions. IT managers showed slightly higher satisfaction with current systems (3.00), while students/seeking a job were the least satisfied (2.50). In terms of the frequency of fraud, Academic Administration Staff (AAS) perceived fewer problems (2.25) than HR/Recruiters (2.80). Knowledge of blockchain was low across all roles, with Academic Administration Staff (AAS) reporting the lowest level (1.86). Knowledge of the GDPR was highest among HR/Recruiters (3.20). The perceived usefulness of the system was consistently high across all roles (above 4.50), with Academic decision-makers being the most convinced (4.73). The improvement of current procedures was also highly valued, although IT Managers showed less conviction (3.89). Finally, the feasibility of implementation in the institution itself showed less confidence among Students/Seeking for a job (3.43) and IT Managers (3.67).

Table 1 presents the questions from the pre-questionnaire.

Table 1. Questions included in the pre-questionnaire.

ID	Question
Q1	Are you satisfied with the current systems for verifying academic certifications at your institution?
Q2	How frequent are issues of fraud, difficulties in verifying academic certifications, or even incomplete verification in your professional environment?
Q3	What level of knowledge do you have about blockchain technology?
Q4	Are you aware of the limitations imposed by the General Data Protection Regulation (GDPR) on the processing of personal credentials?
Q5	From my point of view, a system to verify that the information included in academic certificates is truthful could be useful.
Q6	From my perspective, a system designed to issue and verify academic certifications could improve the current procedures available at my institution.
Q7	I consider it feasible for my institution to use a system to issue and verify academic information, depending on the type of organization.

The results of these questions are presented in Table 2. In addition to the mean score for each item, the standard deviation is shown as an error bar to provide a quantitative measure of the variability and consensus among respondents.

Table 2. Results of the Pre-Workshop Questionnaire (mean scores and standard deviation).

Role	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Academic Administration Staff	2.67 ± 0.779	2.25 ± 1.289	1.86 ± 1.100	3.07 ± 1.328	4.57 ± 0.646	4.31 ± 0.751	4.25 ± 1.055
Student/Seeking for a job	2.50 ± 0.535	2.38 ± 0.916	2.56 ± 1.014	2.78 ± 1.202	4.67 ± 0.500	4.11 ± 0.928	3.43 ± 1.512
IT Managers	3.00 ± 1.000	2.67 ± 1.033	2.56 ± 1.014	2.67 ± 1.118	4.56 ± 0.727	3.89 ± 1.453	3.67 ± 1.500
Human Resources and Recruiters	2.89 ± 0.601	2.8 ± 0.9189	2.10 ± 1.197	3.20 ± 0.919	4.60 ± 0.516	4.20 ± 0.789	4.00 ± 0.817
Academic decision-makers	2.86 ± 1.027	2.53 ± 1.246	2.25 ± 1.000	2.71 ± 1.359	4.73 ± 0.458	4.35 ± 0.862	4.00 ± 1.033
All roles	2.80 ± 0.853	2.63 ± 1.134	2.37 ± 1.137	2.93 ± 1.248	4.57 ± 0.604	4.17 ± 0.907	3.91 ± 1.128

6.2. Post-Workshop Questionnaire

After the workshop, 60 of the 75 attendees responded to the post-workshop questionnaire, revealing a general optimism. Most participants were optimistic about the model's ability to reduce academic fraud and facilitate verification without direct contact with the issuing institution, with an average score of 4.77 out of 5. Similarly, the vast majority believed that implementing the model would speed up the academic certification verification process, with an average score of 4.60.

Respondents also perceived the system as more reliable and secure than current procedures, with an average score of 4.65. These positive results were maintained when evaluating whether the use cases presented (issuance, full/partial verification, recovery in case of institutional disappearance) reflected real-life situations and were clearly applicable, with an average score of 4.48. The perception that the implementation of the model would bring modernization to their institutions was also high, with an average of 4.73.

In addition, the general perception was that the model is fairly easy to adapt to existing systems, with an average of 4.22, a satisfactory result given that the Proof-of-Concept yet showed some manual operations to be automatized in a final product. Regarding implementation in their own institutions, a large proportion wanted to see it within the next two years, and a smaller group was positive about the next five years. Attendees had considerable confidence in the system's ability to adapt to real cases, with an average of 4.35.

The perceived usefulness of an academic certificate verification system remained high, even improving slightly in comparison with the pre-workshop questionnaire (4.74 post-workshop vs. 4.57 pre-workshop), with an increase in responses with a value of "5". The perception that the system would improve the current procedures also became more positive (4.65 post-workshop vs. 4.17 pre-workshop), suggesting that the workshop succeeded in demonstrating the applicability of the use cases despite the technological complexity. However, the opinion on the feasibility of their institutions using a system such as the one presented remained virtually unchanged (3.89 post-workshop vs. 3.91 pre-workshop), which could be due to the known difficulties of integrating digital certification systems in the academic field.

In the open questions, the most interesting aspects of the workshop were the practicality of the system and its use cases, as well as the consideration of academic data privacy and security. The usefulness of partial verification and the flexibility of the model for non-formal certifications were also highlighted. Suggested improvements focused on the usability and automation of the product, something that must be implemented for a final product, and the need for a business and marketing model.

The main barriers and costs identified for implementation included the potentially high cost, the lack of systems to overall issue digital certificates (due to the education field still being largely paper based), the need for training to use the model, clarification of who bears the costs of using and maintaining the blockchains, the lack of a formal standardization, and the need for global adoption for effectiveness. Additional comments pointed to long-term implementation due to the limitations of physical formats (such as The Diploma Supplement (<https://europass.europa.eu/en/learn-europe/diploma-supplement>, accessed on 26 August 2025), the security of user wallets, and technical complexity, especially in key management and student responsibility for their own data and accounts.

The analysis by roles in the post-workshop questionnaire revealed that students were the most optimistic, especially regarding the implementation of the system, although ironically, they were the least convinced that the system would improve verification procedures. HR/recruiters were the most pessimistic about short-term implementation and the second least convinced about process improvement. IT Managers and Academic decision-

makers were the most reluctant about the ease of implementation and coexistence with the current systems, attributing this to the complexity of integrating modern technologies, such as blockchain, in a system that is still very traditional, and the need to define maintenance responsibilities.

Table 3 lists the questions of the post-questionnaire.

Table 3. Questions included in the post-questionnaire.

ID	Question
Q1	I believe this system would help reduce academic fraud and make it possible to verify certificates without direct contact with the issuing institution.
Q2	I believe this system would help save time and resources compared to the current processes for verifying academic certifications.
Q3	I believe this system would allow for safer and more reliable verification compared to the current processes for verifying academic certifications.
Q4	The use cases presented in the workshop reflect real-life situations and are clearly applicable.
Q5	This type of solution can help modernize the management of academic certifications.
Q6	I believe this solution could coexist without major difficulty with current systems.
Q7	I would like to see this type of technology implemented in my environment within the next 2 years.
Q8	I would like to see this type of technology implemented in my environment within the next 5 years.
Q9	I trust in the system's ability to adapt to real cases.
Q10	From my point of view, a system to verify that the information included in academic certificates is truthful could be useful.
Q11	From my perspective, a system designed to issue and verify academic certifications could improve the current procedures available.
Q12	I consider it feasible for my institution to use a system to issue and/or verify academic certifications, depending on the type of organization.

In addition to the mean score reported for each item in Table 4, the corresponding standard deviation is presented as an error bar. This approach provides an objective representation of the variability in the responses and helps to assess the degree of consensus among the participants.

Table 4. Results of the Post-Workshop Questionnaire (mean scores and standard deviation).

Role	Q1	Q2	Q3	Q4	Q5	Q6
Academic Administration Staff	4.58 ± 0.515	4.58 ± 0.515	4.42 ± 0.515	4.58 ± 0.515	4.92 ± 0.289	4.55 ± 0.688
Student/Seeking for a job	4.88 ± 0.354	5.00 ± 0.000	5.00 ± 0.000	5.00 ± 0.000	5.00 ± 0.000	4.38 ± 0.744
IT Managers	4.80 ± 0.447	4.20 ± 0.837	4.40 ± 0.894	4.00 ± 1.000	4.20 ± 1.095	3.80 ± 0.837
Human Resources and Recruiters	4.75 ± 0.500	4.50 ± 0.577	4.75 ± 0.500	4.75 ± 0.500	4.75 ± 0.500	4.50 ± 0.577
Academic decision-makers	4.86 ± 0.354	4.50 ± 0.535	4.63 ± 0.518	4.50 ± 0.535	4.75 ± 0.463	3.86 ± 0.690
All roles	4.77 ± 0.465	4.60 ± 0.588	4.65 ± 0.547	4.48 ± 0.701	4.73 ± 0.548	4.22 ± 0.750
Role	Q7	Q8	Q9	Q10	Q11	Q12
Academic Administration Staff	4.45 ± 0.688	4.83 ± 0.389	4.42 ± 0.515	4.75 ± 0.452	4.67 ± 0.492	3.67 ± 1.155
Student/Seeking for a job	4.63 ± 0.744	5.00 ± 0.000	4.75 ± 0.463	5.00 ± 0.000	4.80 ± 0.354	3.86 ± 1.069
IT Managers	3.50 ± 0.577	4.25 ± 0.957	3.80 ± 0.837	4.20 ± 0.837	4.20 ± 0.447	3.75 ± 1.500
Human Resources and Recruiters	5.00 ± 0.000	4.75 ± 0.500	4.25 ± 0.957	5.00 ± 0.000	5.00 ± 0.000	4.50 ± 1.000
Academic decision-makers	4.25 ± 0.707	4.63 ± 0.744	4.50 ± 0.535	4.88 ± 0.354	4.88 ± 0.354	4.17 ± 0.983
All roles	4.40 ± 0.842	4.68 ± 0.631	4.35 ± 0.799	4.74 ± 0.579	4.65 ± 0.577	3.89 ± 1.076

6.3. Perception Evolution (Pre-Workshop vs. Post-Workshop)

The methodology of the workshop, which included questionnaires before and after the presentation of GAVIN's Proof-of-Concept, allowed us to observe changes in the perception of the participants. This section describes the evolution of participants' perceptions, comparing the results of the pre-workshop and post-workshop questionnaires for the common questions, and analysing the open responses in greater detail.

Three key questions in both questionnaires were analysed in order to compare the evolution of technological acceptance, namely perceived utility (i.e., question 5 pre-workshop and 10 post-workshop), improvement on current methods (question 6 pre-workshop and 11 post-workshop) and implementation feasibility (question 7 pre-workshop and 12 post-workshop).

With respect to perceived utility, before the workshop, participants rated this aspect with an average score of 4.57. Following the demonstration of the Proof-of-Concept and the detailed explanation of the GAVIN model, the average increased to 4.74. This improvement, marked by a higher frequency of maximum Likert scores ("5" instead of "4"), suggests that the practical presentation helped reinforce participants' belief in the usefulness of a system for verifying academic certificates. Despite the inherent complexity of blockchain technology, the inclusion of real-world use cases and the emphasis on data privacy and security resonated positively with the audience.

The second key indicator analyzed was the perceived improvement over current methods for issuing and verifying academic certifications. Before the workshop, this aspect received an average score of 4.17. After the presentation and demonstration of the GAVIN model, the score rose significantly to 4.65. This nearly half-point increase reflects the workshop's success in clearly communicating the advantages of the proposed system. Despite the potential complexity of the underlying technology, participants recognized how GAVIN's use cases could substantially enhance existing procedures. The ability to reduce fraud and accelerate verification without requiring direct contact with the issuing institution was identified as a major contributor to this improved perception.

The third key indicator examined was the perceived feasibility of implementing the GAVIN model. Before the workshop, this aspect received an average score of 3.91, which remained nearly unchanged at 3.89 after the session. This result suggests that while participants clearly recognized the benefits of the system, they also acknowledged the significant challenges involved in integrating digital certificate solutions within academic institutions. These concerns reflect broader issues such as technological readiness, institutional infrastructure, and the complexity of transitioning to electronic systems for credential issuance and verification.

To contextualize the qualitative feedback gathered during the workshop, three open-ended questions were analyzed to better understand participants' perceptions of the GAVIN model. These questions focused on (1) the most interesting aspects of the workshop, (2) suggested improvements to the system and its presentation, and (3) perceived barriers and costs associated with implementation. The responses provide valuable insights into both the strengths of the model and the challenges that must be addressed to ensure its successful adoption in real-world educational environments.

Participants consistently highlighted the practicality of the GAVIN system and the relevance of its use cases as the most compelling aspects of the workshop. The model's strong emphasis on privacy and security in handling academic data was also frequently mentioned, reflecting a growing concern for data protection in educational technologies. Attendees appreciated the system's ability to perform partial verification of academic certifications, allowing for selective data sharing. Additionally, the flexibility of the model to accommodate non-formal and informal learning credentials was seen as a valuable feature, aligning with the evolving nature of education and lifelong learning.

While the workshop was positively received, several participants suggested enhancements to the Proof-of-Concept, particularly in terms of usability and automation. The current version included manual steps and a limited interface, which some found restrictive. As a result, there was strong interest in organizing a follow-up workshop once a finalized product is available. Another recurring suggestion was the development of a clear

business model and marketing strategy to support broader adoption. Many participants noted that more detailed feedback could be provided once the system is fully operational and ready for real-world use by end-users.

Finally, despite the enthusiasm for the GAVIN model, participants identified several barriers to implementation. The most common concern was the potentially high cost of deploying and maintaining the system, especially in institutions that still rely heavily on paper-based processes. The lack of standardized digital infrastructure and the need for user training were also seen as significant challenges. Questions around who would bear the costs of blockchain maintenance and system operation added to the uncertainty. Furthermore, the absence of formal standardization and the need for global adoption were highlighted as critical factors for achieving full effectiveness. Additional concerns included the long-term transition from physical formats like the Diploma Supplement, the importance of securing users' wallets to prevent key loss or theft, and the technical complexity of key management and user responsibility for personal data.

Table 5 summarizes the average scores before and after the workshop, along with the absolute and percentage changes.

Table 5. Comparative evolution of participants' perceptions before and after the workshop.

Question	Pre-Workshop Average	Post-Workshop Average	Difference	% Change (vs. Pre)
Perceived Utility	4.57	4.74	+0.17	+3.72%
Improvement on Current Methods	4.17	4.65	+0.48	+11.51%
Feasibility of Implementation	3.91	3.89	−0.02	−0.51%

6.4. Perceptions According to Participants' Role

The role analysis in the post-workshop questionnaire revealed that students were the most optimistic, especially regarding the implementation of the system, although ironically, they were the least convinced that the system would improve verification procedures. Nonetheless, it is highlightable that they also think a tool to verify their academic information is useful, with a unanimity of 5 points out of 5. This shows that they care about the verification of their hard-earned skills, although they may not be familiar with the technical specifications. But they think that a verification process must exist, so they do not have to compete in the market with people who fake their own certifications to get a job or enter a certain university.

The fact that they are the least convinced that GAVIN will improve the verification procedures makes sense due to them not being familiar with the verification process, a task performed by the third parties receiving the students' certifications. Nonetheless, given how the model offers solutions to all roles involved in certificate issuing and verification, students can see the value in having all their academic data stored in the same place, making it easier for them to present it to third parties all at once. Not only that, but they also see great value in the privacy preservation of their information, being allowed to share only partial information with said third parties.

The role of HR/recruiters was the most pessimistic about implementation in the short term and the second least convinced of process improvement. This is due to the difficulties in implementing any kind of digital certificate system within the educational sector. Both the need for standardization at a large enough scale and the differences between all the academic entities' systems make the implementation a challenge.

On the other hand, they were the group that would like to see this system fully implemented as soon as possible, preferably in 2 years, due to all the issues regarding

fake certificates that the model solves. This makes sense due to current models, as they explained, are too diversified depending on the academic certification origin and type, which sometimes can be even manually made and therefore slow.

At the same time, it is also highlightable that HR/recruiters are the second role, after the student's role, to believe that the GAVIN model is more secure and trustworthy than the current verification systems. They also consider that the showcased use cases in the workshop are a good reflection of the reality and real use cases executed daily. This indicates that the model accomplishes successfully all the required functionalities that its potential users need and execute, and not only that, but it also does it in a better way than current models and technologies used in the academic field.

IT managers and academic decision-makers were the most reticent about the ease of implementation and coexistence with current systems, attributing it to the complexity of integrating modern technologies such as blockchain and the need to define maintenance responsibilities. They were concerned about the difficulties of implementing digital models in the education field, given how current important and widely established certifications, like the European Diploma Supplement, are still mainly issued only in traditional media, meaning on paper. The lack of integration of digital models and initiatives by the authorities in the education field, regardless of technology, level of complexity or even provided solutions, makes it more difficult for roles familiar with these procedures to believe in the easy implementation of a model like GAVIN.

On the other hand, AAS is the most optimistic role when thinking of integrating this model within the already existing infrastructures.

They are also the second role to want this technology to be implemented in the next 5 years. This mirrors the necessity from other roles, too, of having a trustworthy system to verify certifications to fix the problem. Nonetheless, they think in the long term (5 years vs. 2 years) because of the same reason behind the reply to this other question. On "I consider it feasible for my institution to use a system to issue and/or verify academic certifications, depending on the type of organization", they are the role that changed their mind the most regarding the question about going from a 4.25 in the question before the workshop to a 3.67 after it. This question is about the feasibility of the GAVIN model being adopted by the education entities they work in, and due to similar concerns, other roles, like HR/recruiters, have shown that they are aware of the difficulties to integrate any kind of digital model into their system, with a likely added difficulty due to the usage of innovative technologies such as blockchain.

We can deduce that, in general lines, all the roles see in the model of GAVIN a complete solution for their necessities that also solves the current issues of the verification systems in the educational field. But, at the same time, they also admit that the multiple bureaucratic processes, and already-established traditional systems in the education field, mean an added difficulty for any digital verification system to be implemented in it.

The results confirm the initial hypotheses. Perceived utility (H1) received an average score of 4.74 out of 5, while perceived security (H2) scored 4.65. Implementation feasibility (H3) was rated at 4.40 for the next two years and 4.68 for the next five years. Furthermore, GDPR compliance (H4) was frequently highlighted as a positive aspect in open-ended responses, reflecting a strong interest in personal data protection.

7. Discussion

The primary objective of the survey was to evaluate user acceptance, perceived usefulness, and ease of use of the proposed system in accordance with the established Technology Acceptance Model (TAM) framework. Given that the study followed a descriptive and exploratory approach, the analysis was intentionally limited to summary statistics such as

means, standard deviations, and response distributions, sufficient to capture participants' perceptions and identify general trends. The purpose of this phase was not to test causal hypotheses or predictive relationships but to provide an initial, empirically grounded assessment of user attitudes toward the system. Consequently, the use of more complex statistical techniques was deemed unnecessary and beyond the intended scope of this work, which focuses on validating the model's practical feasibility and user acceptance rather than on performing inferential or multivariate analysis.

As a general remark, end users expressed a positive attitude toward technologies like the one proposed by GAVIN. However, due to existing challenges in integrating digital certificate systems within the academic sector, their optimism about actual implementation is somewhat tempered. This concern is especially noticeable among IT managers and academic decision-makers, likely because they are directly involved in the setup and training required for new technologies.

Despite the need for broad institutional acceptance, users acknowledged that GAVIN effectively addresses several current issues related to certificate issuance and verification. They appreciated the platform's flexibility in supporting any data model, regardless of structure, which facilitates integration with existing systems. Notably, users found the verification process intuitive and valued the ability to check multiple certifications in one place. They also highlighted the system's strength in detecting fraudulent certificates, thanks to its blockchain foundation.

Some participants felt that the Proof-of-Concept was still somewhat difficult to use, but this was attributed to its early-stage development. As a consequence, it was concluded that it would be beneficial to repeat the workshop with a finalized version of the product, for example, eliminating manual steps and allowing users to interact directly with a polished interface.

In summary, it was confirmed that workshop results validate the proposed hypotheses. Participants recognized GAVIN's usefulness, security, scalability, and regulatory compliance, reinforcing its potential as a technological solution for the educational ecosystem.

8. Conclusions

The outcomes of the validation workshop reflect a broad positive reception of GAVIN across various stakeholders within the education sector. Participants widely acknowledged the system's potential to reduce academic fraud, streamline verification processes and enhance the security and reliability of credentials. Particularly appreciated were GAVIN's adaptability to different learning formats (i.e., formal, informal, and non-formal) and its strong emphasis on GDPR compliance and data privacy. The multi-blockchain architecture and scalability-oriented design were also recognized as relevant strengths, addressing key limitations found in existing solutions.

Nonetheless, despite the positive perception of GAVIN's utility and innovation, the study also highlights significant challenges in transitioning toward real-world deployment. Concerns were raised about the high implementation costs, the lack of standardized digital infrastructure in many institutions, and the need for comprehensive end-user training. Additionally, the absence of a clear business model and marketing strategy, along with uncertainty around blockchain maintenance responsibilities and associated costs, were identified as critical barriers to widespread adoption. The technical complexity of blockchain was also seen as a potential obstacle, particularly in the management of keys and credentials, and the responsibility placed on data holders.

The persistence of these concerns, even after the Proof-of-Concept demonstration, suggests that the challenges are not purely technical but also organizational, financial, and regulatory. The still-limited integration of digital certificates in many institutions

remains a fundamental barrier for solutions like GAVIN's. To unlock its full potential and enable global adoption, greater standardization and coordinated efforts from educational authorities will be required, possibly at an international level.

The qualitative analysis of user feedback, especially the differences observed across roles, with students showing more enthusiasm and HR/IT professionals expressing greater caution, offers valuable insights for future development. To gather more precise and actionable feedback, it would be beneficial to conduct additional workshops using a finalized and fully functional version of the platform. This would allow for deeper user interaction, increased automation, and a more direct comparison with existing systems in educational institutions, ultimately helping refine GAVIN's design and implementation strategy.

The qualitative methodology employed, including pre- and post-workshop questionnaires based on the Technology Acceptance Model (TAM), was demonstrated to be highly effective in capturing user perceptions and validating the proposed hypotheses. The structured approach and diversity of participant roles provided a solid foundation for analysis and reinforced the relevance of the GAVIN model within real educational contexts.

As a continuation of this project, the GAVIN architecture offers a promising outlook for large-scale deployment across national and international academic networks, enabling secure and GDPR-compliant verification of academic information among diverse institutions. Future research will focus on optimizing the balance between privacy protection and the strengthening of data authority and authenticity. This will involve the exploration and development of new mechanisms for traceability, decentralized validation, and institutional accreditation.

In addition, ongoing work will address interoperability [76] and regulatory compliance within the European context, particularly in relation to the eIDAS Regulation [77] (eIDAS 2) on electronic identification and trust services, with the ultimate goal of establishing a pan-European digital ecosystem that supports the cross-border verification of academic credentials.

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. and M.R.-M.; validation, C.D.-v.-E., L.A.-R., M.J.F.-I. and M.R.-M.; formal analysis, C.D.-v.-E., L.A.-R., M.J.F.-I. and M.R.-M.; investigation, C.D.-v.-E. and M.R.-M.; data curation, C.D.-v.-E., L.A.-R., M.J.F.-I. and M.R.-M.; writing—original draft preparation, C.D.-v.-E., M.J.F.-I. and M.R.-M.; writing—review and editing, C.D.-v.-E., L.A.-R., M.J.F.-I. and M.R.-M.; 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 MICIU/AEI/10.13039/501100011033 and by the European Union NextGenerationEU/PRTR. Funding for open access charge: Universidade de Vigo/CISUG.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article; further inquiries can be directed to the corresponding author.

Acknowledgments: We would like to thank the member of the GAVIN team at atlantTic, Pablo Molina-Martínez, for his insightful comments.

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. Google. Creating Pathways to Careers in IT. 2019. Available online: https://services.google.com/fh/files/misc/it_cert_impactreport_booklet_rgb_digital_version.pdf (accessed on 28 December 2021).
4. Voigt, P.; Von dem Bussche, A. *The EU General Data Protection Regulation (GDPR)*; Springer: Cham, Switzerland, 2017. [CrossRef]
5. Gómez-Vieites, A.; Delgado-von-Eitzen, C.; Estévez-García, D. GDPR-Compliant Academic Certification via Blockchain: Legal and Technical Validation of the GAVIN Project. *Appl. Sci.* **2025**, *15*, 9191. [CrossRef]
6. Grech, A.; Camilleri, A.F. *Blockchain in Education*; Publications Office of the European Union: Luxembourg, 2017. [CrossRef]
7. Alammary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-Based Applications in Education: A Systematic Review. *Appl. Sci.* **2019**, *9*, 2400. [CrossRef]
8. Bhaskar, P.; Tiwari, C.K.; Joshi, A. Blockchain in Education Management: Present and Future Applications. *Interact. Technol. Smart Educ.* **2020**, ahead-of-print. [CrossRef]
9. 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]
10. Raimundo, R.; Rosário, A. Blockchain System in the Higher Education. *Eur. J. Investig. Health Psychol. Educ.* **2021**, *11*, 276–293. [CrossRef] [PubMed]
11. 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 International Publishing: Cham, Switzerland, 2022; pp. 553–571. [CrossRef]
12. Talat, M.; Riaz, S.; Farooq, M.S. Effect of Blockchain on Education: A Systemic Literature Review. *VEAST Trans. Softw. Eng.* **2022**, *10*, 116–124. [CrossRef]
13. 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, Switzerland, 2019; Volume 11432, pp. 191–202. [CrossRef]
14. Chinnasamy, P.; Ramani, D.R.; Ayyasamy, R.K.; Jebamani, B.J.A.; Dhanasekaran, S.; Praveena, V. Applications of Blockchain Technology in Modern Education System—Systematic Review. In Proceedings of the 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 23–25 January 2023; pp. 1–4. [CrossRef]
15. Hu, D.; Pongpatcharattrontep, D.; Timsard, S.; Khamaksorn, A. Blockchain Applications in Higher Education: A Systematic Literature Review. In Proceedings of the 2023 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), Phuket, Thailand, 22–25 March 2023; pp. 188–193. [CrossRef]
16. Rustemi, A.; Dalipi, F.; Atanasovski, V.; Risteski, A. A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification. *IEEE Access* **2023**, *11*, 64679–64696. [CrossRef]
17. Al-Tawara, F.; Qasaimeh, M.; Jarad, D.; Al-Qassas, R.S. Utilizing the Blockchain Technology for Higher Education in the Era of Pandemics: A Systematic Review. In Proceedings of the 2023 14th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 21–23 November 2023; pp. 1–6. [CrossRef]
18. Molopa, S.T.; Cronje, J. Research on Blockchain Adoption in Higher Education: A Systematic Review and Conceptual Model. In *Advances in Information and Communication*; Arai, K., Ed.; Springer Nature: Cham, Switzerland, 2024; pp. 110–130.
19. Caldarelli, G.; Ellul, J. Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review. *Appl. Sci.* **2021**, *11*, 1842. [CrossRef]
20. Vaezinejad, S.; Chen, Y.; Kouhizadeh, M.; Ozpolat, K. Blockchain Technology for Higher Education and Recruitment: A Systematic Literature Review. *Eurasian J. Bus. Econ.* **2024**, *17*, 1–27. [CrossRef]
21. Wang, X.; Younas, M.; Jiang, Y.; Imran, M.; Almusharraf, N. Transforming Education Through Blockchain: A Systematic Review of Applications, Projects, and Challenges. *IEEE Access* **2025**, *13*, 13264–13284. [CrossRef]
22. Silaghi, D.L.; Popescu, D.E. A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions. *Computers* **2025**, *14*, 141. [CrossRef]
23. Jain, R.; Seth, N.; Sood, K.; Grima, S. Mapping the Research on Blockchain in Education: A Systematic Review and Bibliometric Analysis. In *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management*; Sood, K., Balusamy, B., Grima, S., Eds.; Contemporary Studies in Economic and Financial Analysis; Emerald Publishing Limited: Leeds, UK, 2023; Volume 111C, pp. 53–66. [CrossRef]
24. de Alwis, A.; Shrestha, A.; Sarker, T. Exploring Governance for Accreditation in the Education Sector using Blockchain Technology: A Systematic Literature Review. *Discov. Educ.* **2025**, *4*, 57. [CrossRef]

25. Ayare, A.A.; Jadhav, V.A.; Banatwala, M.K.; Changlere, S.V.; Mote, A.; Joshi, P. A Systematic Review on Blockchain-Based Framework for Storing Educational Records Using InterPlanetary File System. *Cureus J. Comput. Sci.* **2025**, *2*. [\[CrossRef\]](#)
26. Choudhary, A.; Chawla, M.; Tiwari, N. Analyzing Functional, Technical and Bibliometric Trends of Blockchain Applications in Education: A Systematic Review. *Multimed. Tools Appl.* **2025**, *84*, 4003–4048. [\[CrossRef\]](#)
27. Castro, R.Q.; Au-Yong-Oliveira, M. Blockchain and Higher Education Diplomas. *Eur. J. Investig. Health Psychol. Educ.* **2021**, *11*, 154–167. [\[CrossRef\]](#) [\[PubMed\]](#)
28. 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. [\[CrossRef\]](#)
29. Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Blockchain Applications in Education: A Systematic Literature Review. *Appl. Sci.* **2021**, *11*, 11811. [\[CrossRef\]](#)
30. Hameed, B.; Murad, M.; Noman, A.; Javed, M.; Ramzan, M.; Ashfaq, F.; Usman, H.; Yousaf, M. A Review of Blockchain based Educational Projects. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [\[CrossRef\]](#)
31. 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. [\[CrossRef\]](#)
32. Loukil, F.; Abed, M.; Boukadi, K. Blockchain adoption in education: A systematic literature review. *Educ. Inf. Technol.* **2021**, *26*, 5779–5797. [\[CrossRef\]](#)
33. 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. [\[CrossRef\]](#)
34. 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. [\[CrossRef\]](#)
35. Turkanović, M.; Hölbl, M.; Košič, K.; Heričko, M.; Kamišalić, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access* **2018**, *6*, 5112–5127. [\[CrossRef\]](#)
36. Rao, A.S.; Bhargav, K.V.S.; Rastogi, R.; Basha, S.K.J.; Shaik, N. Blockchain Technology in Educational Credentials. In Proceedings of the 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM), Dehradun, India, 22–23 November 2024; pp. 1–7. [\[CrossRef\]](#)
37. Sudha, K.; Ali, A.; Mohammed, N.Q.; Dawood, I.I.; Goud, K.S.; Reddy, B.D.; Reddy, B.S.; Singla, B. Educational Certificate Verification System using Block-chain Technology. In Proceedings of the 2024 International Conference on Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA), Manipal, India, 20–21 December 2024; pp. 1–6. [\[CrossRef\]](#)
38. Al Sakib, S.; Rakib, M.; Hossain, M.M.; Islam, M.S.; Khan, B.R.; Reza, M.S. Blockchain Based Certificate Verification for Employee Hiring & Admission System. In Proceedings of the 2023 26th International Conference on Computer and Information Technology (ICCIT), Cox’s Bazar, Bangladesh, 13–15 December 2023; pp. 1–6. [\[CrossRef\]](#)
39. Singh, A.; Chauhan, S.P.S.; Goel, A.K. Blockchain Based Verification of Educational and Professional Certificates. In Proceedings of the 2023 2nd International Conference on Computational Systems and Communication (ICCSC), Thiruvananthapuram, India, 3–4 March 2023; pp. 1–7. [\[CrossRef\]](#)
40. 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 2025).
41. Anandapadmanaban, B.; Umesh, A.V.; Anilkumar, A.; Das, A.K.; Joseph, R.B. EduChain: A Blockchain-Based System for Efficient and Secure Certificate Verification. In Proceedings of the 2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST), Kochi, India, 3–5 April 2025; Volume 1, pp. 1–6. [\[CrossRef\]](#)
42. Stefan-Robert, C.; Butincu, C.N. Decentralized Blockchain-based Platform for Managing and Issuing Academic Certificates. In Proceedings of the ICSTCC 2024–28th International Conference on System Theory, Control and Computing, Sinaia, Romania, 10–12 October 2024; pp. 570–575. [\[CrossRef\]](#)
43. Ullah, N.; Al-Rahmi, W.M.; Alzahrani, A.I.; Alfarraj, O.; Alblehai, F.M. Blockchain Technology Adoption in Smart Learning Environments. *Sustainability* **2021**, *13*, 1801. [\[CrossRef\]](#)
44. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q.* **1989**, *13*, 319–340. Available online: <http://www.jstor.org/stable/249008> (accessed on 5 September 2025). [\[CrossRef\]](#)
45. Awaji, B.; Solaiman, E.; Marshall, L. Investigating the Requirements for Building a Blockchain-Based Achievement Record System. In Proceedings of the 5th International Conference on Information and Education Innovations, ICIEI’20, London, UK, 26–28 July 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 56–60. [\[CrossRef\]](#)
46. Alshahrani, M.; Beloff, N.; White, M. Towards a Blockchain-based Smart Certification System for Higher Education: An Empirical Study. *Int. J. Com. Dig. Sys.* **2016**. [\[CrossRef\]](#)
47. Ramos, C.R.D.S.; Queiroz, M.M. Blockchain in Education: The Influence of Trust on Adoption and Implementation. *RAUSP Manag. J.* **2022**, *57*, 316–331. [\[CrossRef\]](#)

48. Mohammad, A.; Vargas, S. Barriers Affecting Higher Education Institutions' Adoption of Blockchain Technology: A Qualitative Study. *Informatics* **2022**, *9*, 64. [CrossRef]
49. Lam, T.Y.; Dongol, B. A blockchain-enabled e-learning platform. *Interact. Learn. Environ.* **2020**, *30*, 1229–1251. [CrossRef]
50. Ocheja, P.; Flanagan, B.; Ueda, H.; Ogata, H. Managing lifelong learning records through blockchain. *Res. Pract. Technol. Enhanc. Learn.* **2019**, *14*, 4. [CrossRef]
51. Kuvshinov, K.; Nikiforov, I.; Mostovoy, J.; Mukhutdinov, D. Disciplina: Blockchain for Education. 2018. Available online: <https://web.archive.org/web/20250114133407/https://www.disciplina.io/yellowpaper.pdf> (accessed on 14 January 2025).
52. Wahab, A.; Barlas, M.; Mahmood, W. Zenith Certifier: A Framework to Authenticate Academic Verifications Using Tangle. *J. Softw. Syst. Dev.* **2018**, *13*. Available online: <https://ibimapublishing.com/wp-content/uploads/articles/JSSD/2018/370695/370695.pdf> (accessed on 20 September 2025).
53. 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*, 3:1–3:23. [CrossRef]
54. 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]
55. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 14 October 2025).
56. Wu, X.; Zou, Z.; Song, D. Ethereum Tools and Frameworks. In *Learn Ethereum: Build Your Own Decentralized Applications with Ethereum and Smart Contracts*; Packt: Birmingham, UK, 2019; pp. 294–335.
57. Hyperledger. Whitepaper Introduction Hyperledger. 2018. Available online: <https://www.hyperledger.org/learn/white-papers> (accessed on 2 April 2025).
58. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–15. [CrossRef]
59. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday* **1997**, *2*. [CrossRef]
60. Antonopoulos, A.M.; Wood, G. *Mastering Ethereum. Building Smart Contracts and DApps*, 1st ed.; O'Reilly Media: Sebastopol, CA, USA, 2019; pp. 297–318.
61. 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]
62. 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. [CrossRef]
63. Lyons, T.; Courcelas, L.; Timsit, K. Blockchain and the GDPR. The European Union Blockchain Observatory and Forum. 2018. Available online: https://blockchain-observatory.ec.europa.eu/document/download/b3a919ed-0045-46f8-89de-f23ca140e037_en?filename=20181016_report_gdpr.pdf (accessed on 14 April 2025).
64. Agencia Española de Protección de Datos; European Data Protection Supervisor. 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 8 July 2025).
65. Krawczyk, H.; Bellare, M.; Canetti, R. HMAC: Keyed-Hashing for Message Authentication; RFC 2104. 1997. Available online: <https://datatracker.ietf.org/doc/html/rfc2104> (accessed on 14 April 2025).
66. Delgado-von-Eitzen, C.; Fernández-Iglesias, M.J.; Anido-Rifón, L. A GDPR-Compliant Blockchain Architecture for the Verification of Educational Credentials: Design, Implementation, and Evaluation. *Implement. Eval.* **2025**, Preprint. [CrossRef]
67. Hyperledger. Hyperledger Besu Documentation. 2025. Available online: <https://lf-hyperledger.atlassian.net/wiki/spaces/BESU/pages/22154225/Documentation> (accessed on 5 April 2025).
68. Fan, C.; Lin, C.; Khazaei, H.; Musilek, P. Performance Analysis of Hyperledger Besu in Private Blockchain. In Proceedings of the 2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Newark, CA, USA, 15–18 August 2022; pp. 64–73. [CrossRef]
69. Datachain. Hyperledger Labs YUI. 2025. Available online: <https://www.datachain.jp/yui> (accessed on 16 April 2025).
70. Kwon, J.; Buchman, E. Cosmos Whitepaper. A Network of Distributed Ledger. 2019. Available online: <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md> (accessed on 16 April 2025).
71. Delgado-von-Eitzen, C.; Anido-Rifón, L.; Ruiz-Molina, M.; Fernández-Iglesias, M.J. Bridging the Gap: Achieving Seamless Interoperability Between Ethereum-Based Blockchains Using Inter-Blockchain Communication Protocols. *Softw. Pract. Exp.* **2025**, *55*, 1749–1772. [CrossRef]
72. Delgado-von-Eitzen, C.; Fernández-Iglesias, M.J.; Anido-Rifón, L.; Llamas-Nistal, M. Ethereum Blockchain Interconnectivity for Dynamic and Privacy-Preserving Access Control. *IEEE Access* **2025**, *13*, 112918–112931. [CrossRef]
73. Kenler, E.; Razzoli, F. *MariaDB Essentials*; Packt Publishing Ltd.: Mumbai, India, 2015.

74. Delgado-von-Eitzen, C.; Iglesias, M.J.F.; Rifón, L.E.A.; Mikic-Fonte, F.A. Blockchain Beyond Immutability: Application Firewalls on Ethereum-Based Platforms. *Comput. Stand. Interfaces* **2026**, *95*, 104038. [[CrossRef](#)]
75. Davis, F.D. Technology Acceptance Model: TAM. *Al-Suqri MN Al-Aufi AS Inf. Seek. Behav. Technol. Adopt.* **1989**, *205*, 5.
76. Anido-Rifón, L. Standardization of a Blockchain-Based Interoperability Platform for Academic Credentials. 2025. Available online: <https://blockstand.eu/blockstand/uploads/2025/05/Anido-Blockstand-report2-v1.pdf> (accessed on 11 August 2025).
77. Anido-Rifón, L. A Proposal for a Blockchain-based Academic Certification System that Complies with the GDPR. 2025. Available online: <https://blockstand.eu/blockstand/uploads/2025/05/Anido-Blockstand-report1-v1.4.pdf> (accessed on 11 August 2025).

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.