applied system innovation

MDPI

Article

Leveraging Self-Sovereign Identity for Certifying Extra-Curricular Competencies and Skills in University Programs

Pablo López-Márquez [1], Jessica Zaqueros-Martinez [2], Bruno Ramos-Cruz [2], Francisco José Quesada-Real [2,*] and Mercedes Rodriguez-Garcia [1]

[1] School of Engineering, University of Cádiz, 11519 Puerto Real, Spain; pablo.lopezmarquez@alum.uca.es (P.L.-M.); mercedes.rodriguez@uca.es (M.R.-G.)
[2] Higher Polytechnic School, University of Jaén, 23071 Jaén, Spain; zaqueros@ujaen.es (J.Z.-M.); brcruz@ujaen.es (B.R.-C.)
* Correspondence: fqreal@ujaen.es

Abstract

Traditional academic degrees often fail to capture the full range of competencies students acquire throughout their university education, particularly those developed through laboratory activities, internships, volunteering, and other extra-curricular experiences. This limitation hinders students' ability to differentiate themselves in increasingly competitive labor markets and complicates employers' identification of candidates with balanced technical and transversal competencies. To address this challenge, this paper presents a design-oriented research study proposing a Self-Sovereign Identity (SSI)-based framework for the decentralized issuance and verification of academic micro-credentials. The proposed approach combines a structured methodology for generating micro-credentials with a decentralized architecture supported by a prototype implementation based on SSI technologies. The framework enables universities, lecturers, and other trusted entities to issue verifiable and tamper-resistant credentials that students can securely manage, control, and share through SSI wallets. Unlike existing approaches, which typically focus either on secure credential infrastructures or on the pedagogical value of micro-credentials, the proposed framework integrates both technological and educational perspectives while explicitly supporting the certification of extra-curricular and soft skills. The system supports the creation of granular and portable competency profiles while enhancing transparency, authenticity, interoperability, and trust in credential management. Furthermore, the paper discusses key challenges associated with large-scale adoption, including trust management, governance, scalability, interoperability, and issuer credibility. The results suggest that SSI-based micro-credentialing represents a promising approach for improving the recognition of both technical and transversal competencies, contributing to better alignment between higher education outcomes and evolving labor market demands.

Keywords: micro-credentials; higher education; self-sovereign identity; educational technology

Check for updates

Academic Editor: Abdelkader Sbihi

Received: 30 September 2024
Revised: 2 May 2026
Accepted: 25 May 2026
Published: 30 May 2026

Copyright: © 2026 by the authors. Published by MDPI on behalf of the International Institute of Knowledge Innovation and Invention. 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.

1. Introduction

Higher education has traditionally focused on certifying academic achievements through standardized degrees awarded upon completion of studies. These degrees formally recognize the knowledge and competencies students acquire during their academic journey [1]. However, in today's competitive job market, a degree alone often fails to capture the full range of skills and experiences that students develop, particularly those

acquired through extra-curricular activities and the cultivation of soft skills, which are essential for shaping well-rounded professionals [2].

Recent evidence highlights a persistent and widening gap between higher education outcomes and labor market expectations. For instance, recent employability reports indicate that only 30–41% of graduates secure employment aligned with their field of study, while approximately 48% report feeling unprepared for entry-level roles [3]. Furthermore, employer surveys reveal substantial discrepancies between graduates' self-perceived competencies and employers' expectations, with differences reaching up to 25–30% in key skills such as communication, leadership, and problem-solving [4]. Complementary studies also show that employers consistently identify deficiencies in essential competencies, including communication, critical thinking, and adaptability [5,6]. These findings underscore a structural mismatch between traditional academic certification and the skills required in modern workplaces.

In this context, the certification of both academic knowledge and practical experience has become increasingly important, as it validates technical competencies while also highlighting the development of soft skills, which are highly valued by employers [7]. Traditional degrees provide only a general indication of academic achievement and fail to differentiate individual competencies, as all graduates within a program receive the same diploma regardless of their specific experiences and skillsets [8].

This limitation is particularly evident in skills acquired outside the classroom. Students frequently engage in extra-curricular activities such as specialist courses, conference presentations, internships, Erasmus mobility programs, and volunteer work, which are critical for developing competencies not captured by traditional academic transcripts. For instance, Quesada-Real et al. [9] report that students develop skills such as teamwork, problem-solving, and adaptability during their studies; however, these competencies are rarely formally certified.

This disconnect between traditional certification methods and the need to recognize a broader spectrum of competencies exposes significant limitations in current academic credentialing systems. In addition, conventional paper-based certificates are vulnerable to issues such as forgery and inefficient verification processes, which can undermine their credibility [10].

To address these challenges, blockchain technology has been increasingly adopted in the academic sector to enhance transparency, security, and trust in the issuance of educational credentials. Prior works have explored blockchain-based solutions for certificate management and verification, highlighting their potential to improve authenticity and reduce fraud [11–15]. Building upon these developments, SSI [16] has emerged as a promising paradigm for decentralized identity and credential management [16]. SSI enables individuals to own, control, and share their credentials without relying on centralized authorities, facilitating the issuance of verifiable, tamper-proof digital credentials.

Recent studies have explored the use of SSI in educational contexts [17–22]. However, the existing literature remains fragmented. On the one hand, technical approaches focus on secure and interoperable infrastructures for credential management, emphasizing aspects such as decentralization, scalability, and trust. On the other hand, educational studies highlight the importance of micro-credentials for employability and skills recognition but lack robust technological frameworks for their secure and verifiable implementation. Moreover, most existing solutions are primarily oriented toward formal academic achievements, with limited attention to the certification of extra-curricular competencies and soft skills.

Despite these advances, there remains a lack of comprehensive frameworks that integrate technological infrastructures with pedagogical needs while providing structured methodologies for generating micro-credentials. In particular, current approaches do

not adequately address how diverse skills acquired throughout a student's academic journey—especially transversal and extra-curricular competencies—can be systematically captured, validated, and issued as verifiable credentials.

To bridge this gap, this paper adopts a design-oriented research approach and proposes a novel SSI-based framework for certifying extra-curricular competencies and skills in higher education. Unlike prior work, which typically addresses either the technological infrastructure for secure credentialing or the pedagogical value of micro-credentials, our approach integrates both perspectives through a structured framework that enables the granular and verifiable certification of technical and transversal competencies.

The main contributions of this work are threefold:

- A structured methodology for generating micro-credentials, including well-defined use cases, certification criteria, and proficiency levels for both technical and soft skills.
- A decentralized SSI-based architecture that enables multiple actors (e.g., universities, lecturers, and external organizations) to issue and verify tamper-proof and privacy-preserving credentials.
- A functional prototype implemented using SSI technologies, demonstrating the feasibility of the proposed approach in a realistic academic scenario.

By explicitly addressing the certification of extra-curricular activities and soft skills, the proposed framework enables the creation of personalized, verifiable competency portfolios that extend beyond traditional academic credentials. This contributes to bridging the gap between higher education outcomes and labor market expectations, providing a more comprehensive and trustworthy representation of student capabilities.

The remainder of the paper is structured as follows: Section 2 provides the background on skills in education, micro-credentials, and SSI. Section 3 presents the proposed SSI-based academic certification framework, including the methodology for generating micro-credentials and the system architecture and implementation. Section 4 offers an illustrative example of the system's practical application. Section 5 examines the strengths, limitations and ethical implications of the proposal. Section 6 compares our approach with related works. Finally, Section 7 concludes the paper and outlines directions for future work.

2. Background

This section introduces the differences in competencies and skills in education as well as the essential concepts of micro-credentials and SSI, which form the foundation of our approach to enhancing skill certification in higher education.

2.1. Competencies and Skills in Education

The terms *skills* and *competencies* are often used interchangeably in both academic and labor market contexts; however, they denote conceptually distinct and hierarchically related constructs. In educational theory, *competence* is defined as the ability to mobilize and integrate knowledge, skills, and attitudes to effectively address tasks and challenges within a specific context [23]. Competence-based learning (CBL) builds on this perspective by emphasizing the development and assessment of such integrated capabilities, rather than the isolated acquisition of theoretical knowledge [24]. This approach prioritizes performance in authentic or real-world situations, thereby reducing the gap between academic learning and professional practice [25].

In contrast, a *skill* refers to a specific learned ability that enables the execution of a task with a defined level of proficiency. Skills are typically observable, measurable, and context-dependent. Crucially, they function as the operational components of competence: while skills describe the ability to perform discrete actions, competence reflects the effective orchestration of multiple skills, combined with knowledge and attitudes, in complex and

dynamic environments [26]. Therefore, competence can be understood as an emergent, higher-level construct derived from the coordinated application of multiple skills in context.

In higher education, preparing graduates for contemporary labor markets requires the development of both discrete skills and broader competencies. These capabilities are commonly categorized into two complementary dimensions: technical (*hard*) skills and transversal (*soft*) skills. This distinction reflects the dual nature of professional performance, where domain-specific expertise must be complemented by the ability to operate effectively in socially and organizationally complex environments [27].

Hard skills refer to discipline-specific knowledge and operational abilities that enable individuals to perform specialized tasks within a given field. They are typically acquired through formal education and reinforced through structured practice. Examples include programming, data analysis, engineering design, and laboratory experimentation. Due to their procedural and well-defined nature, hard skills can be assessed through standardized evaluation mechanisms, such as examinations, projects, and certifications. Their importance is particularly pronounced in technical domains, where precision, methodological rigor, and up-to-date expertise are essential for effective performance.

Soft skills, by contrast, encompass a set of transferable capabilities that shape how individuals interact, think, and adapt across contexts. These include communication, teamwork, problem-solving, leadership, and adaptability. Unlike hard skills, they are not discipline-specific but influence behavior in diverse professional environments. Soft skills are typically developed through experiential learning processes, such as collaborative work, problem-based learning, internships, and participation in extracurricular activities. Although more difficult to measure, their relevance has been consistently highlighted, given their critical role in employability, innovation, and long-term career success [28,29].

The relationship between hard and soft skills is not merely additive but integrative: effective competence in real-world settings requires the simultaneous application of both dimensions. For example, solving an engineering problem demands not only technical expertise but also communication, collaboration, and decision-making capabilities. Consequently, contemporary higher education increasingly adopts holistic learning models that promote the integrated development of skills as a pathway toward competence acquisition, aligning graduate profiles with evolving labor market demands.

In this context, the micro-credentialing framework proposed in this paper operationalizes this conceptual distinction by enabling the granular certification of individual skills—both technical and transversal—while supporting their aggregation into broader competency profiles. This approach provides a more accurate, transparent, and verifiable representation of student capabilities, bridging the gap between theoretical competence models and their practical recognition in digital credentialing systems.

2.2. Micro-Credentials

Micro-credentials are digital certifications that recognize specific skills, competencies, or knowledge acquired through various educational and professional experiences [30]. Unlike traditional degrees, which cover a broad range of learning over an extended period, micro-credentials focus on discrete, measurable achievements [31]. They can be awarded for activities such as short courses, workshops, or demonstrating proficiency in specific tools or skill sets. As digital entities, micro-credentials are easily shareable and verifiable via online platforms [32–34].

The primary purpose of micro-credentials is to offer a flexible and granular approach to recognizing learning and skill development. In higher education, they help bridge the gap between formal education and the evolving demands of the workforce [35,36]. As industries and technologies evolve, professionals increasingly need to acquire targeted

skills in shorter timeframes, and micro-credentials provide a mechanism to certify these competencies without the time and financial commitment required for full degree programs.

Micro-credentials are used across multiple contexts, including higher education [37–39], professional development [40–42], and workforce training [43–45]. In universities, they are often integrated into degree programs to complement traditional curricula with targeted skill development. For instance, the European Commission has promoted micro-credentials through a common framework aimed at ensuring standardization, quality, and cross-border recognition across higher education institutions [46]. In parallel, initiatives such as the Digital Credentials Consortium led by the Massachusetts Institute of Technology (MIT) have developed interoperable infrastructures for issuing and verifying digital credentials, facilitating their adoption in academic ecosystems [47]. Similarly, universities such as the University of Melbourne have implemented institution-wide digital credentialing strategies to support lifelong learning and flexible education pathways [48].

The benefits of micro-credentials in higher education are significant [36]. They enable flexible and personalized learning pathways, allowing students to build competency-based portfolios aligned with career objectives. Furthermore, they enhance employability by providing verifiable evidence of skills directly relevant to industry needs, while their digital nature facilitates easy sharing across professional platforms.

However, implementing micro-credentials in higher education presents several challenges [49]. Ensuring quality, consistency, and recognition remains critical, as the rapid expansion of micro-credential offerings may lead to fragmentation and variability in their perceived value. Integrating micro-credentials into existing curricula requires careful design to ensure alignment with learning outcomes and institutional strategies. In addition, institutions must address technical challenges related to issuing, managing, and verifying credentials through secure and scalable infrastructures.

Despite these challenges, existing initiatives demonstrate that they can be effectively addressed through coordinated efforts. The European approach emphasizes policy-level standardization and interoperability [46], while technical consortia such as the Digital Credentials Consortium provide practical infrastructures and governance models for trusted credential exchange [47]. These examples highlight that successful implementation requires the combination of technological solutions, institutional alignment, and shared standards.

Overall, while challenges remain, current implementations show that micro-credentials can be successfully integrated into higher education systems when supported by robust frameworks, interoperable technologies, and institutional collaboration.

2.3. Self-Sovereign Identity

SSI is an emerging paradigm for decentralized identity management that enables individuals to create, own, and control their digital identities without reliance on centralized authorities [16]. In contrast to traditional identity management systems—where identity data is stored and managed by third-party providers—SSI shifts control to the individual, enhancing privacy, security, and user autonomy.

From a technical perspective, SSI is grounded in a set of standards and protocols that enable secure, interoperable, and verifiable identity interactions. The SSI ecosystem is typically described through a trust model involving three main actors: issuer, holder, and verifier (see Figure 1). The issuer generates digitally signed credentials, the holder stores and manages these credentials in a secure digital wallet, and the verifier validates them without requiring direct interaction with the issuer. These interactions are conducted through secure peer-to-peer (P2P) communication channels, ensuring confidentiality and integrity [50].

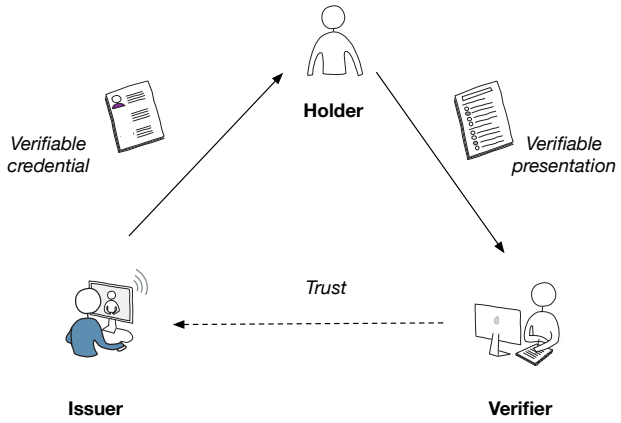

Figure 1. Trust triangle (adapted from [16]).

At the core of SSI are three key technological components, aligned with W3C standards: Decentralized Identifiers (DIDs) [51], Verifiable Credentials (VCs), and Verifiable Data Registries (VDRs) [52].

- *DIDs* are globally unique identifiers that are created and controlled by the user, without dependence on a central authority. Each DID resolves to a DID Document containing cryptographic material (e.g., public keys), service endpoints, and authentication methods. These elements enable secure identification, authentication, and key management in a decentralized environment.
- *VCs* are tamper-evident, cryptographically signed digital credentials that encode claims about an entity (e.g., a student's competencies or achievements). VCs follow a standardized data model and can be selectively disclosed by the holder through *verifiable presentations*, allowing fine-grained control over what information is shared. Cryptographic techniques such as digital signatures and zero-knowledge proofs ensure authenticity, integrity, and privacy.
- *VDRs* provide a decentralized infrastructure—often implemented using Distributed Ledger Technologies (DLTs)—to anchor DIDs and public keys. Rather than storing personal data, these registries maintain cryptographic proofs and metadata, enabling trust verification without exposing sensitive information. Their immutability ensures that identity-related data cannot be altered or tampered with.

Within the context of the proposed framework, SSI serves as the foundational layer for secure and decentralized micro-credential management. Educational institutions and authorized entities act as issuers, generating verifiable credentials that certify both technical and soft skills. Students act as holders, storing these credentials in digital wallets and controlling their disclosure. Employers or external organizations act as verifiers, validating credentials through cryptographic verification using public keys retrieved from the VDR.

This architecture eliminates the need for centralized verification processes and enables real-time, trustless validation of credentials. Furthermore, the use of verifiable presentations allows students to aggregate and selectively disclose multiple micro-credentials, supporting the creation of personalized and context-aware competency profiles.

The application of SSI in education addresses key limitations of traditional credentialing systems, including susceptibility to forgery, lack of interoperability, and limited user control [18–20]. By providing a decentralized and standards-based approach, SSI enables secure, portable, and verifiable academic credentials that can be shared across institutional and geographical boundaries.

However, the adoption of SSI also introduces technical and organizational challenges. These include the need for interoperable standards, scalable trust frameworks, and integra-

tion with existing academic systems. In addition, ensuring usability and user acceptance of digital wallets and decentralized identity mechanisms remains a critical factor for real-world deployment.

Despite these challenges, SSI represents a key enabling technology for next-generation digital credentialing systems. By combining cryptographic security, decentralized infrastructure, and user-centric identity management, it provides the technological foundation for more transparent, flexible, and trustworthy education ecosystems.

3. SSI-Based Academic Certification Framework

In this section, we present the use of micro-credentials in the academic environment, the proposed methodology for generating them, and the architecture and implementation of the SSI-based micro-credentialing system.

3.1. Micro-Credentials in the Academic Environment

In the current educational landscape, there is an increasing emphasis on equipping students with a comprehensive skill set. While traditional hard skills, such as technical expertise and subject-specific knowledge, remain essential, the growing importance of soft skills—such as leadership, communication, and teamwork—is becoming increasingly valuable. To effectively address this requirement, we propose to deploy our SSI-based micro-credentialing architecture in educational institutions. The system will be able to recognize and validate a wide range of student accomplishments, encompassing both technical and interpersonal skills. This dual recognition system ensures that students graduate with a comprehensive and nuanced portfolio of micro-credentials that reflects their full range of abilities. By implementing this micro-credentialing system, educational institutions can significantly enhance students' resumes, providing them with a more well-rounded acknowledgment of their capabilities. Now, students' resumes can offer a clear and detailed picture of their competencies to employers, educational institutions, and professional networks. The integration of SSI technology further optimizes this process, enabling students to securely store, manage, and share their micro-credentials with complete autonomy. The control of these micro-credentials resides entirely with the student, rather than the issuing institution, ensuring both privacy and flexibility.

Both the university (or its schools, faculties or departments) and its individual professors collaborate to issue micro-credentials that acknowledge the diverse skill sets students acquire throughout their academic journey. University-issued micro-credentials provide recognition of core competencies, both in technical and interpersonal skills, while professor-issued micro-credentials offer detailed insights into specialized hard skills directly related to their courses and areas of expertise and soft skills demonstrated in practical settings. Granular recognition of student capabilities empowers them to present a well-rounded portfolio that accurately reflects their abilities and potential. Students hold their micro-credentials in SSI wallets on their smartphones or personal computers, giving them full control to manage and share their credentials as needed. These wallets consolidate micro-credentials issued by both the university and individual professors. The SSI wallet generates a globally unique DID for the student, enabling the secure linking of micro-credentials without disclosing personal information. Students can demonstrate their skills by sharing their micro-credentials with employers (e.g., when applying for a job), educational institutions (e.g., when applying to a competitive graduate program), or on professional networks (e.g., when displaying their achievements). These recipients can easily verify the credentials' authenticity and integrity through the digital signatures of the issuers and holders.

3.2. Methodology for Generating Micro-Credentials

This subsection describes the proposed methodology for generating SSI-based micro-credentials aimed at certifying skills and competencies in higher education environments. The methodology is designed to provide a structured, transparent, and reproducible process for the definition, assessment, issuance, and verification of micro-credentials. In contrast to existing approaches that mainly focus on technological infrastructures, the proposed methodology also incorporates pedagogical and assessment-related aspects, facilitating its integration into real academic workflows.

The methodology is organized into four sequential stages: (i) identification of certification scenarios, (ii) definition of competency levels, (iii) specification of certifiable competencies and skills, and (iv) credential issuance and management. Together, these stages define a complete lifecycle for SSI-based academic micro-credentials.

3.2.1. Identification of Certification Scenarios

The first stage consists of identifying the academic and extracurricular scenarios in which micro-credentials can be generated. This stage defines the contexts in which students demonstrate measurable achievements that can be formally recognized through SSI-based credentials.

The primary certification scenarios considered in this work are the following:

- *Achievement of specific competencies within a course:* Micro-credentials are issued when students demonstrate proficiency in well-defined learning outcomes associated with a subject. For example, in a programming course (e.g., Python), students may obtain a credential after successfully demonstrating mastery of concepts such as syntax, control structures, or data types.
- *Completion of courses or academic modules:* Micro-credentials can certify the successful completion of subjects or specialized training modules. For instance, students completing a Robotics course may receive a credential recognizing the acquisition of integrated technical competencies.
- *Demonstration of practical or technical skills:* Students who successfully complete laboratory activities, capstone projects, or performance-based assessments may obtain credentials associated with practical competencies. Examples include programming challenges, cybersecurity exercises, or the operation of industrial robots.
- *Demonstration of transversal competencies:* The framework also supports the certification of soft skills, including communication, teamwork, leadership, adaptability, and community engagement. These competencies may be evaluated through presentations, collaborative activities, mentoring tasks, volunteering, or participation in student organizations.

This stage is essential to ensure that the generated micro-credentials are aligned with institutional educational objectives and labor market demands.

3.2.2. Definition of Competency Levels

Once the certification scenarios have been identified, the second stage defines the competency levels associated with the issued credentials. The objective is to provide a consistent mechanism for differentiating the degree of achievement demonstrated by students.

The proposed methodology defines two certification levels:

- *Excellent*: Represents exceptional performance significantly exceeding the expected learning outcomes or evaluation criteria.
- *Proficient*: Represents advanced performance that is clearly above average expectations.

The decision to restrict the model to these two levels is intentional and motivated by both pedagogical and operational considerations. From a pedagogical perspective, limiting the number of levels preserves the exclusivity and signaling value of the credentials by focusing on high-quality achievements. From an operational perspective, it reduces the administrative burden associated with defining, evaluating, and maintaining multiple granular certification levels.

3.2.3. Specification of Certifiable Competencies and Skills

The third stage defines the set of competencies and skills that can be certified within the framework. These competencies include both technical and transversal dimensions aligned with current educational objectives and labor market requirements.

Table 1 summarizes the initial set of competencies and skills considered in this work. The proposed framework is initially tailored to engineering education, which explains the inclusion of competencies such as programming and technical proficiency. Nevertheless, the framework is flexible and the set of certifiable competencies can be adapted to the specific requirements of different institutions or academic disciplines.

The selected competencies reflect a holistic view of student development by combining analytical, technical, interpersonal, and ethical dimensions. This flexibility enables institutions to adapt the framework to different educational contexts while maintaining a consistent certification methodology.

Table 1. Key competencies and skills considered for certification.

Competencies/Skills	Description
Problem-Solving	Ability to analyze complex problems and develop effective solutions
Teamwork	Capacity to work collaboratively with others to achieve common goals
Communication	Proficiency in conveying ideas clearly, both verbally and in writing
Leadership	Ability to guide teams and take responsibility for outcomes
Adaptability	Flexibility in responding to new challenges and environments
Technical Proficiency	Expertise in engineering tools, software, and methodologies
Project Management	Skills in planning and executing projects within constraints
Critical Thinking	Ability to evaluate information and make sound decisions
Innovation	Creativity in developing new ideas or solutions
Time Management	Efficient organization and prioritization of tasks
Ethical Judgment	Ability to make responsible and ethical decisions
Data Analysis	Competence in interpreting and analyzing data
Programming Skills	Proficiency in relevant programming languages
Attention to Detail	Precision in executing tasks accurately
Sustainability Awareness	Understanding of sustainable practices
Community Engagement	Participation in socially responsible activities

3.2.4. Credential Issuance and Management

The final stage defines the workflow for issuing, storing, and verifying SSI-based micro-credentials. This workflow follows the principles of the SSI paradigm and ensures the integrity, authenticity, and portability of credentials.

The credential lifecycle consists of the following steps:

1. *Assessment:* Students are evaluated through examinations, projects, laboratory activities, coursework, or observational assessments designed to measure specific competencies and skills.
2. *Verification:* Assessment results are validated by authorized academic staff, such as lecturers or program coordinators. This process may include reviewing submissions, applying evaluation rubrics, and validating compliance with certification criteria.
3. *Credential generation and issuance:* Once verification is completed, the institution or instructor generates a micro-credential encoded as a W3C Verifiable Credential. The credential is digitally signed using the issuer's cryptographic keys to guarantee authenticity and integrity.
4. *Storage and management:* Issued credentials are delivered to the student's SSI wallet, where they remain under the student's control. The wallet enables secure storage and management of credentials.
5. *Sharing and verification:* Students can selectively share their credentials with external entities, such as employers or educational institutions. Credential verification is performed through cryptographic validation mechanisms without requiring direct interaction with the issuer.

Overall, the proposed methodology defines a systematic and scalable process for generating SSI-based micro-credentials. By combining pedagogical criteria with secure decentralized technologies, the framework supports transparent, verifiable, and interoperable credentialing processes aligned with both educational practices and SSI principles.

3.3. Architecture

The architecture is designed to facilitate the issuance and verification of micro-credentials for both hard (technical) and soft (interpersonal) skills. Micro-credentials are issued by organizations or individual professionals to individuals who have demonstrated specific competencies. The system allows individuals to share their micro-credentials with other entities, effectively showcasing their skills. By leveraging the core components of the SSI system described in Section 2.3—blockchain technology, DIDs, and verifiable credentials—our architecture ensures privacy, security, and integrity throughout the lifecycle of micro-credentials. The result is a decentralized, user-centric system that empowers individuals to control and manage their micro-credentials autonomously.

Figure 2 depicts the essential components of the SSI-based micro-credentialing architecture, with *Entity A* acting as the *issuer*, *Entity B* as the *verifier*, and the *holder* represented by an *individual*. All participants use SSI wallets on their personal devices—smartphones or personal computers—to securely issue, store, share, and verify micro-credentials while safeguarding privacy. Specifically, an *SSI wallet* is a secure digital application that provides the following capabilities: (1) identity management, (2) micro-credential management, and (3) the creation of secure P2P communication channels for exchanging micro-credentials. The SSI wallet manages the owner's identity by generating and handling DIDs—globally unique, decentralized identifiers representing participants' digital identities within the system. Unlike traditional identifiers (e.g., usernames or email addresses), DIDs are self-generated and controlled by users' SSI wallets. The SSI wallets also securely store the private keys associated with the public keys linked to these DIDs, ensuring that only the wallet owner can authenticate their identity or digitally sign. Additionally, the SSI wallet acts as a personal hub where individuals can store their micro-credentials and prepare them for sharing with different entities. SSI wallets establish encrypted P2P communication channels between users within the architecture, enabling the secure off-Ledger exchange of micro-credentials without exposing sensitive data to third parties.

Our architecture leverages blockchain technology to provide a decentralized, immutable, and publicly accessible ledger—*SSI Ledger*—which removes the need for a central authority in verifying micro-credentials. The SSI Ledger acts as a *Decentralized Public Key Infrastructure* (DPKI), where public keys linked to users' DIDs are stored in tamper-proof DID Documents (DDOs). These public keys are essential for validating the digital signatures embedded in micro-credentials and their verifiable presentations, ensuring their authenticity and integrity. The immutable nature of the SSI Ledger is vital for maintaining trust within the architecture, as it guarantees that DIDs and their corresponding DDOs remain unaltered once written.

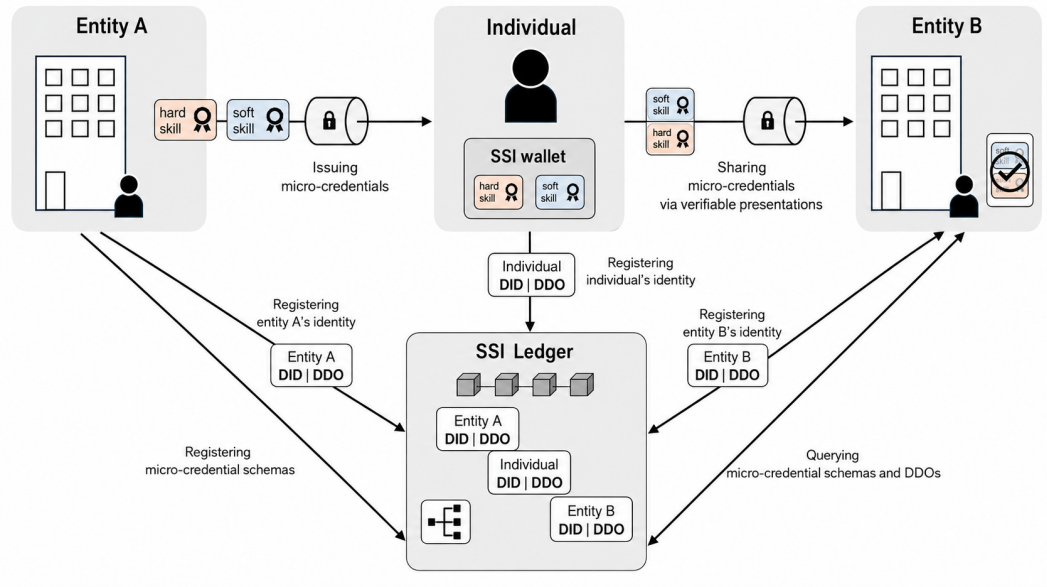

Figure 2. SSI-based micro-credentialing architecture.

To ensure interoperability among different participants within the architecture, micro-credentials conform to a data schema that defines their structure and content. This schema, which is publicly accessible and stored on the SSI Ledger by the issuer, can be consulted by any participant to interpret the micro-credentials and ensure consistency across the system. The schema includes key fields, such as the specific skill and the issuing entity. To protect user privacy, micro-credentials themselves are stored off-Ledger within the SSI wallets of their respective owners, ensuring that sensitive information remains secure and under the control of the individual.

Below we detail the data flow within the SSI-based micro-credentialing architecture.

- *Identity creation:* The holder sets up an SSI wallet, which generates a globally unique DID along with its corresponding pair of cryptographic keys (public and private). This DID functions as the holder's digital identity within the system. The holder's DID, along with a DDO containing the public key, is registered on the SSI Ledger, ensuring a secure association between the DID and the public key. This setup enables verifiers to use the holder's public key for reliable verification of the holder's credential presentations. Issuers and verifiers also create their own SSI wallets following a similar process.
- *Skill acquisition and micro-credential issuance:* The holder acquires hard and soft skills through educational programs or professional experiences. Entities where the skills are acquired create micro-credentials to recognize these achievements, adhering to a predefined schema. These micro-credentials are then issued off-Ledger via a secure P2P channel to the holder's SSI wallet, where they are securely stored. The holder can

organize, manage, and prepare these micro-credentials as verifiable presentations for sharing when needed.

- *Micro-credential sharing and verification:* The holder can share their micro-credentials with multiple verifiers as needed (e.g., when applying for an educational program or job), maintaining control over their digital identity and personal data. To demonstrate competencies to verifying entities, the holder selects the relevant micro-credentials and compiles them into a verifiable presentation. This presentation is signed by the holder and shared off-Ledger with the verifier via a secure P2P communication channel established between the holder and verifier's SSI wallets. The verifier ensures the authenticity and integrity of the verifiable presentation by validating its digital signatures. First, it verifies the signatures of the micro-credentials contained in the verifiable presentation using the issuers' public keys. Next, it verifies the signature of the verifiable presentation itself using the holder's public key. These public keys are retrieved from the corresponding DDOs registered on the SSI Ledger.

3.4. Implementation

A prototype implementation of the proposed SSI-based micro-credentialing architecture has been developed and made publicly available in a GitHub repository [53]. This prototype is implemented in Python 3.12 using the SSI frameworks Hyperledger Ursa [54], Indy [55], and Aries [56]. Hyperledger Indy forms the foundation for the decentralized identity ledger, facilitating the creation, storage, and management of DIDs and verifiable micro-credentials. Hyperledger Ursa enhances the system's security by providing cryptographic libraries for secure management of keys and digital signatures, ensuring that all network interactions are cryptographically secure and privacy-preserving. Hyperledger Aries acts as the communication layer, enabling secure, P2P messaging between agents of SSI wallets that manage identities and micro-credentials on behalf of users. Aries also supports the creation of verifiable presentations, essential for sharing micro-credentials in a privacy-respecting manner. To simulate and test our prototype, we employed VON-Network [57], a development environment that emulates a production-level blockchain network. VON-Network facilitates the deployment of test networks that mimic real-world scenarios, allowing us to experiment with and fine-tune the SSI components.

The prototype architecture comprises three agents: the holder, the issuer, and the verifier, each executing specific actions associated with their respective roles. Once the prototype is set up, these agents can be initiated using the command terminal. The process begins with the creation of micro-credential schemas and the establishment of a connection between the issuer and holder agents. The issuer then generates and issues a micro-credential to the holder. After receiving the micro-credential, the holder connects with the verifier agent to create a verifiable presentation of their micro-credentials and shares it with the verifier. The verifier can then validate the micro-credentials, ensuring they are legitimate and were indeed issued by the issuer.

4. Illustrative Example

This section presents a realistic implementation scenario to illustrate how the proposed SSI-based micro-credentialing framework operates within a university environment. The example is structured as an end-to-end workflow, covering identity creation, skill acquisition, credential issuance, and external verification. Figure 3 summarizes the data flow.

We consider Alice, a third-year computer engineering student enrolled at a university that has adopted the proposed framework. The system is integrated with the university's Learning Management System (LMS) and administrative platforms, enabling the seamless generation and management of micro-credentials.

This workflow aligns with the architecture described in Section 3, where the roles of issuer, holder, and verifier, as well as the interactions between SSI wallets and the SSI Ledger, are formally defined.

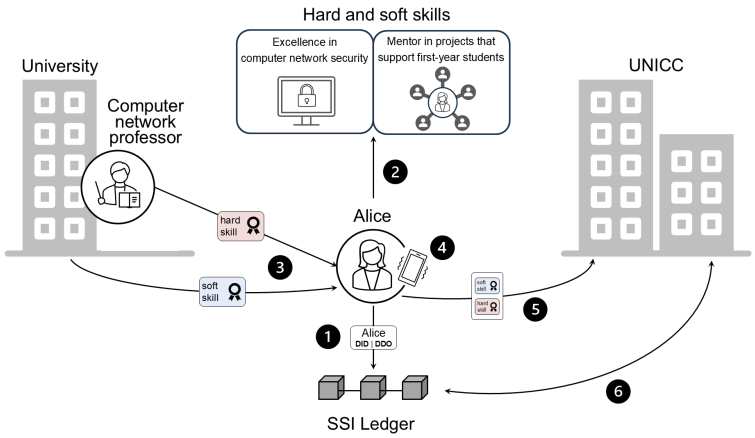

Figure 3. Dataflow of the SSI-based micro-credentialing process.

Step 1: System Initialization and Identity Setup.

At the beginning of her studies, Alice creates her self-sovereign identity using the university's SSI wallet application as part of the standard enrollment process. The wallet generates a DID and its corresponding DDO, which is anchored on the SSI Ledger. In parallel, the university and its authorized staff (e.g., lecturers, program coordinators) are registered as trusted issuers within the system, each associated with their own DIDs. This step establishes the trust framework required for subsequent credential issuance and verification.

Step 2: Skill Acquisition and Assessment.

During the semester, Alice participates in both formal and informal learning activities. In the *Computer Networks* course, her competencies are assessed through structured evaluation methods, including exams, laboratory exercises, and project-based assignments, mapped to specific learning outcomes such as *network security*.

In parallel, Alice engages in a university mentoring program, where her leadership and communication skills are evaluated using predefined rubrics that combine supervisor feedback, peer assessment, and participation indicators. These evaluation processes are managed through the LMS, ensuring traceability and consistency.

Step 3: Credential Generation and Issuance.

Once Alice meets the predefined evaluation criteria, micro-credentials are generated automatically or semi-automatically through the institutional system. The course instructor issues a credential for "*Proficient Computer Network Security*", while the extracurricular program coordinator issues a credential for "*Excellence in Leadership and Communication*". Each credential follows a standardized schema and includes metadata such as skill description, proficiency level, issuer identity, and issuance date. The credentials are cryptographically signed using the issuer's private key and transmitted securely to Alice's SSI wallet via a peer-to-peer channel.

Step 4: Credential Management and Composition.

Alice stores the received micro-credentials in her SSI wallet, where she can organize them into structured portfolios (e.g., technical skills, soft skills, extracurricular achievements). The wallet enables Alice to compose verifiable presentations by selectively com-

bining credentials depending on the intended use case, supporting flexible and context-aware disclosure.

Step 5: Credential Sharing.

When applying for the *Cybersecurity Awareness Leadership Program* fellowship at the *United Nations International Computing Centre* (UNICC), Alice generates a tailored verifiable presentation containing both credentials. The sharing process follows a request–response protocol, where the verifier specifies required attributes and Alice provides only the relevant credentials. Communication is established through a secure peer-to-peer channel between the respective SSI wallets.

Step 6: Credential Verification.

The UNICC verifies the authenticity and integrity of the credentials by validating their digital signatures. This involves retrieving the public keys associated with the university and instructor DIDs from the SSI Ledger and checking the cryptographic proofs embedded in the credentials and the presentation. The process is fully automated and does not require direct interaction with the issuing entities, significantly reducing verification time and administrative overhead.

This scenario demonstrates how the proposed framework can be seamlessly integrated into existing university processes, from assessment to credential issuance and external validation. It highlights the feasibility of automating credential generation, ensuring trust through cryptographic verification, and enabling students to actively manage and present their competencies. Ultimately, the framework supports a more transparent, flexible, and efficient ecosystem for recognizing skills, bridging the gap between academic achievement and labor market requirements.

5. Discussion

This section examines the implications of adopting SSI-based micro-credentialing in higher education. Specifically, we discuss the main advantages of the proposed approach, the technical and organizational challenges associated with its implementation, the ethical considerations derived from decentralized credential management, and the broader impact of this paradigm on future academic credentialing systems.

5.1. Benefits of SSI-Based Credentialing

The application of SSI to academic micro-credentialing promotes a transition from traditional degree-centric models toward more flexible, learner-centered, and competency-oriented credentialing systems. In particular, SSI enables the issuance of granular and personalized credentials capable of recognizing both technical and transversal competencies that are typically not reflected in conventional academic transcripts [36,49].

By leveraging decentralized identity infrastructures and cryptographic verification mechanisms, SSI-based credentials become tamper-resistant, portable, and independently verifiable without requiring direct interaction with issuing institutions. This improves transparency, authenticity, and trust in credentialing processes while reducing dependency on centralized authorities [17,18].

From the learner's perspective, SSI facilitates the creation of comprehensive competency portfolios that reflect skills acquired across formal, informal, and extra-curricular learning experiences. Such competency-based representations are increasingly relevant in labor markets characterized by rapid technological evolution and growing demand for hybrid skill profiles [5,6]. Furthermore, formally recognizing these competencies may positively influence student engagement and motivation by providing visible and verifiable evidence of their achievements.

5.2. Implementation Challenges

Despite its potential benefits, the implementation of SSI-based micro-credentialing introduces several technical, organizational, and governance-related challenges.

One of the primary challenges concerns scalability and trust management. In decentralized ecosystems, the value and credibility of credentials depend heavily on the reputation and reliability of credential issuers. Consequently, robust governance mechanisms are required to support issuer accreditation, trust establishment, monitoring, and potential revocation processes [21,22].

Interoperability with existing university infrastructures also represents a significant barrier. Many higher education institutions continue to rely on legacy information systems that were not designed to support decentralized identity models or verifiable credential standards. As a result, integrating SSI technologies into institutional workflows may require substantial technical adaptation and resource investment. In addition, the absence of universally adopted deployment standards for SSI in educational contexts further complicates interoperability and large-scale adoption [17].

Organizational and cultural resistance may also hinder adoption. Transitioning from institution-controlled credentialing models toward user-controlled identity management constitutes a substantial paradigm shift. Universities may express concerns regarding governance, regulatory compliance, accountability, operational complexity, and long-term sustainability. These barriers are consistent with broader digital transformation challenges reported in higher education, where institutional inertia and limited technical expertise often delay technological innovation [49].

5.3. Ethical Implications

The adoption of SSI for academic credentialing also raises important ethical considerations that must be carefully addressed to ensure responsible, fair, and inclusive deployment.

First, although SSI strengthens user autonomy and control over credentials, it simultaneously transfers part of the responsibility for identity and credential management to individuals. This may exacerbate inequalities associated with digital literacy, access to secure technologies, or technological awareness, potentially contributing to new forms of digital exclusion [58].

Second, privacy and data protection remain critical concerns. While SSI architectures support privacy-preserving mechanisms such as selective disclosure, the aggregation of multiple micro-credentials may still reveal sensitive information regarding students' academic trajectories, performance patterns, or personal profiles. Consequently, compliance with regulatory frameworks such as the General Data Protection Regulation (GDPR) [59] is essential, particularly regarding principles such as data minimization, informed consent, and purpose limitation.

Finally, the assessment and certification of transversal competencies and soft skills introduce risks related to subjectivity, inconsistency, and bias. Unlike technical competencies, soft skills are often context-dependent and more difficult to evaluate objectively. Without clearly defined assessment criteria and transparent evaluation mechanisms, credentialing processes may unintentionally reproduce biases or inconsistencies across evaluators and institutions.

Addressing these ethical challenges requires integrating principles such as privacy-by-design, transparency, fairness, inclusivity, and accountability into both the technological architecture and the governance frameworks surrounding SSI-based credentialing systems.

5.4. Implications and Outlook

The adoption of SSI-based micro-credentialing may significantly reshape how competencies are recognized, validated, and communicated within higher education ecosystems.

By enabling flexible, transparent, and learner-centered credentialing models, SSI contributes to narrowing the gap between academic outcomes and labor market expectations.

However, realizing this potential requires coordinated efforts across technological, institutional, and regulatory dimensions. Future developments should prioritize interoperability through standardization initiatives, the establishment of robust trust frameworks, and alignment with emerging policy and regulatory initiatives at both European and international levels.

6. Related Works

The application of blockchain and SSI in education has gained significant attention, particularly in digital credentialing. Existing contributions can be broadly grouped into four research streams: (i) blockchain-based certification systems, (ii) SSI-based identity and credential management, (iii) interoperable credential infrastructures, and (iv) micro-credential frameworks focused on employability and soft skills.

Early work leverages blockchain to enhance the security and integrity of academic credentials, addressing issues such as forgery, verification efficiency, and trusted record management. Grech et al. [17] highlight the gap between the conceptual potential of blockchain/SSI and their real-world adoption, while Faizan [21] emphasizes their role in improving transparency and trust in academic record management.

A second line of research focuses on SSI adoption in education. Herbke and Yildiz [19] propose the ELMO2EDS framework to transform traditional credentials into SSI-compliant formats, prioritizing privacy and user control. Queiruga-Dios et al. [18] analyze SSI integration within universities, showing its potential to streamline credential issuance and verification. Similarly, Al et al. [20] introduce Hei-bct, a blockchain-based SSI framework for secure academic record sharing.

Recent work has addressed scalability and architectural challenges. Wilczynski and Budzik propose *Skillchain*, a service-oriented blockchain platform incorporating governance-aware smart contracts and Proof-of-Authority consensus to support scalable micro-credential management [60]. While this approach advances infrastructure design and interoperability, it focuses primarily on technical aspects and does not address pedagogical integration or the certification of transversal skills.

A third research stream examines large-scale interoperability infrastructures. Kiiskila [22] explores the European Blockchain Services Infrastructure (EBSI), highlighting its role in enabling cross-border credential recognition. However, these initiatives largely focus on formal qualifications rather than fine-grained skill certification.

Finally, recent studies emphasize the role of micro-credentials in employability and soft skills development. Bruguera et al. [61] show that micro-credentials are perceived as effective tools to bridge the soft skills gap, although challenges remain in their design and adoption. Similarly, Lago Ávila et al. [62] highlight their role in certifying transversal competencies and enhancing student differentiation in competitive job markets. Epaphras [63] further positions micro-credentials as a mechanism to bridge the gap between higher education and industry needs. However, these works lack robust technological frameworks for secure and verifiable credential management.

Despite these advances, three key limitations remain. First, technical solutions primarily focus on secure credential infrastructures, with limited attention to extra-curricular competencies and soft skills. Second, educational studies emphasize employability but lack integration with secure, decentralized technologies. Third, there is a lack of structured methodologies for generating, validating, and issuing micro-credentials within higher education.

To address these limitations, this work integrates SSI-based credential management with a structured methodology for issuing micro-credentials that capture both technical and transversal skills. This approach bridges the gap between technological infrastructures and educational needs, enabling a more granular, flexible, and verifiable representation of student competencies.

Table 2 provides a comparative overview of existing approaches and our proposal, highlighting key differences in terms of technological foundations (SSI/blockchain), scope of certification (formal vs. extra-curricular), consideration of soft skills, and the presence of a structured methodology for micro-credential generation.

Table 2. Comparison with related works.

Work	SSI/Blockchain	Formal Credentials	Extra-Curricular	Soft Skills	Methodology
Grech et al. [17]	✓	✓	✗	✗	✗
Herbke et al. [19]	✓	✓	✗	✗	✗
Queiruga et al. [18]	✓	✓	✗	✗	✗
Al et al. [20]	✓	✓	✗	✗	✗
Faizan [21]	✓	✓	✗	✗	✗
Kiiskila [22]	✓	✓	✗	✗	✗
Wilczynski et al. [60]	✓	✓	✗	✗	✓
Bruguera et al. [61]	✗	✗	✓	✓	✗
Lago et al. [62]	✗	✗	✓	✓	✗
Epaphras [63]	✗	✗	✓	✓	✗
This work	✓	✓	✓	✓	✓

7. Conclusions

This paper has presented an SSI-based framework for certifying extra-curricular competencies in higher education, addressing several limitations associated with traditional degree-centric credentialing models. By enabling verifiable, tamper-resistant, and portable micro-credentials, the proposed approach supports a more granular, flexible, and learner-centered representation of student capabilities, encompassing both technical and transversal competencies. The framework demonstrates the potential of SSI technologies to enhance transparency, trust, and interoperability in academic credentialing while supporting the recognition of skills acquired through formal and extra-curricular learning experiences. At the same time, the study highlights that large-scale adoption depends on addressing important challenges related to scalability, interoperability, governance, and trust management. In particular, establishing reliable trust frameworks and ensuring the credibility of credential issuers remain critical requirements for sustainable deployment of SSI-based credentialing ecosystems.

Future work will focus on validating and extending the proposed framework in real educational environments. In particular, pilot implementations in university settings will be conducted to evaluate usability, institutional adoption, and integration with existing academic infrastructures and workflows. Future developments will also prioritize interoperability through alignment with initiatives such as the European Blockchain Services Infrastructure (EBSI) and emerging international standards for digital credentials and SSI ecosystems, facilitating cross-border recognition and portability of competencies. Additionally, empirical studies will analyze the impact of SSI-based micro-credentials on employability, competency recognition, and student differentiation in labor market contexts.

Further technical extensions may include the integration of Internet of Things (IoT)-based mechanisms for automated competency validation [64], as well as aggregation mechanisms capable of composing higher-level certifications from multiple micro-credentials.

Author Contributions: Conceptualization, J.Z.-M., B.R.-C., F.J.Q.-R. and M.R.-G.; methodology, J.Z.-M., B.R.-C., F.J.Q.-R. and M.R.-G.; software, P.L.-M.; validation, P.L.-M., J.Z.-M., B.R.-C., F.J.Q.-R. and M.R.-G.; investigation, P.L.-M., J.Z.-M., B.R.-C., F.J.Q.-R. and M.R.-G.; writing—original draft preparation, P.L.-M., F.J.Q.-R. and M.R.-G.; writing—review, P.L.-M., J.Z.-M., B.R.-C., F.J.Q.-R. and M.R.-G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by grant PID2023-148867OB-I00 funded by MICIU/AEI/10.13039/501100011033 and ERDF/EU.

Data Availability Statement: Dataset available on request from the author.

Acknowledgments: During the preparation of this manuscript, the authors used ChatGPT 4o for the purposes of proofreading. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

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

Abbreviations

The following abbreviations are used in this manuscript:

CBL	Competence-based Learning
DDO	Decentralized Identifier Document
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DPKI	Decentralized Public Key Infrastructure
EBSI	European Blockchain Services Infrastructure
GDPR	General Data Protection Regulation
IoT	Internet of Things
LMS	Learning Management System
MIT	Massachusetts Institute of Technology
P2P	Peer-to-peer
SSI	Self-sovereign Identity
STEM	Science, Technology, Engineering, and Mathematics
UNICC	United Nations International Computing Center
VC	Verifiable Credential
VDR	Verifiable Data Registry

References

1. Altbach, P.G.; Reisberg, L.; Rumbley, L.E. *Global Perspectives on Higher Education*; Johns Hopkins University Press: Baltimore, MD, USA, 2016.
2. Higgins, J.; Barrie, S. *Higher Education and Skills for the Future(s) of Work*; Springer: Berlin/Heidelberg, Germany, 2016.
3. Cengage Group. 2025 Graduate Employability Report. 2025. Available online: https://www.cengagegroup.com/news/press-releases/2025/cengage-group-2025-employability-report/ (accessed on 1 May 2026).
4. National Association of Colleges and Employers (NACE). The Gap in Perceptions of New Grads' Competency Proficiency and Resources to Shrink It. 2024. Available online: https://naceweb.org/career-readiness/competencies/the-gap-in-perceptions-of-new-grads-competency-proficiency-and-resources-to-shrink-it (accessed on 1 May 2026).
5. Tushar, H.; Sooraksa, N. Global employability skills in the 21st century workplace: A semi-systematic literature review. *Heliyon* **2023**, *9*, e21023. [CrossRef]
6. Phusavat, K.; Ongkunaruk, P.; Anussornnitisarn, P. Gaining insights into the employability of university graduates: Implications from the students' inputs. *Stud. High. Educ.* **2025**, 1–19. [CrossRef]
7. Heckman, J.J.; Kautz, T. Hard Evidence on Soft Skills. *Labour Econ.* **2018**, *29*, 91–93.

8. Brown, P.; Lauder, H.; Cheung, S.Y. Degrees of Difference: Understanding the Value of Higher Education Credentials in the Workforce. *J. Educ. Work.* **2020**, *33*, 1–14.
9. Quesada-Real, F.J.; Perez-Peña, F.; Morgado-Estévez, A.; Ruiz-Lendínez, J.J. Applying active learning by contextualizing robotic applications to historical heritage. *Comput. Appl. Eng. Educ.* **2024**, *32*, e22687. [CrossRef]
10. Tomlinson, M. Forms of graduate capital and their relationship to graduate employability. *Educ. Train.* **2017**, *59*, 338–352. [CrossRef]
11. Holotescu, C. Understanding blockchain opportunities and challenges. In *Proceedings of the Conference Proceedings of »eLearning and Software for Education« (eLSE)*; Carol I National Defence University Publishing House: Bucharest, Romania, 2018; Volume 14, pp. 275–283.
12. Kanan, T.; Obaidat, A.T.; Al-Lahham, M. SmartCert blockchain imperative for educational certificates. In *Proceedings of the 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*; IEEE: New York, NY, USA, 2019; pp. 629–633.
13. Capece, G.; Levialdi Ghiron, N.; Pasquale, F. Blockchain technology: Redefining trust for digital certificates. *Sustainability* **2020**, *12*, 8952. [CrossRef]
14. Saleh, O.S.; Ghazali, O.; Rana, M.E. Blockchain based framework for educational certificates verification. *J. Crit. Rev.* **2020**, *7*, 79–84. [CrossRef]
15. Bhaskar, P.; Tiwari, C.K.; Joshi, A. Blockchain in education management: Present and future applications. *Interact. Technol. Smart Educ.* **2021**, *18*, 1–17. [CrossRef]
16. Preukschat, A.; Reed, D. *Self-Sovereign Identity*; Manning Publications: Shelter Island, NY, USA, 2021.
17. Grech, A.; Sood, I.; Ariño, L. Blockchain, self-sovereign identity and digital credentials: Promise versus praxis in education. *Front. Blockchain* **2021**, *4*, 616779. [CrossRef]
18. Queiruga-Dios, A.; Bullón Pérez, J.J.; Hernández Encinas, L. Self-sovereign identity in university context. In *Proceedings of the 2022 31st Conference of Open Innovations Association (FRUCT)*; IEEE: New York, NY, USA, 2022; pp. 259–264.
19. Herbke, P.; Yildiz, H. ELMO2EDS: Transforming educational credentials into self-sovereign identity paradigm. In *Proceedings of the 2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET)*; IEEE: New York, NY, USA, 2022; pp. 1–7.
20. Al Mansoori, S.; Maheshwari, P. Hei-bct: A framework to implement blockchain-based self-sovereign identity solution in higher education institutions. In *Proceedings of the 2022 8th International Conference on Information Technology Trends (ITT)*; IEEE: New York, NY, USA, 2022; pp. 6–10.
21. Faizan, M.; Riaz, N.; Saif, U. Transforming university records management: A comprehensive review of blockchain and self-sovereign identity applications. *Int. J. Sci. Res. Arch.* **2024**, *11*, 984–996. [CrossRef]
22. Kiiskilä, P.; Hylli, O.; Pirkkalainen, H. How can European blockchain services infrastructure be used for managing educational digital credentials? In *Proceedings of the 14th Scandinavian Conference on Information Systems (SCIS)*; Association for Information Systems: Atlanta, GA, USA, 2023.
23. Mulder, M.; Weigel, T.; Collins, K. The concept of competence in the development of vocational education and training in selected EU member states: A critical analysis. *J. Vocat. Educ. Train.* **2007**, *59*, 67–88. [CrossRef]
24. Koenen, A.; Dochy, F.; Berghmans, I. A phenomenographic analysis of the implementation of competence-based education in higher education. *Teach. Teach. Educ.* **2015**, *50*, 1–12. [CrossRef]
25. Van Merriënboer, J.; Kirschner, P.A. *Ten Steps to Complex Learning: A Systematic Approach to Four-Component Instructional Design*; Routledge: Oxfordshire, UK, 2017.
26. Mulder, M. Competence-based education and training. *J. Agric. Educ. Ext.* **2012**, *18*, 305–314. [CrossRef]
27. OECD. *OECD Skills Outlook 2019: Thriving in a Digital World*; OECD Publishing: Paris, France, 2019. [CrossRef]
28. World Economic Forum. The Future of Jobs Report. 2023. Available online: https://www.weforum.org/reports/the-future-of-jobs-report-2023 (accessed on 1 May 2026).
29. Anderson, M. The Growing Demand for Soft Skills in the Workplace. *Bus. Educ. Q.* **2021**, *20*, 67–79.
30. Gauthier, T. The value of microcredentials: The employer's perspective. *J. Competency-Based Educ.* **2020**, *5*, e01209. [CrossRef]
31. Lemoine, P.A.; Richardson, M.D. Micro-credentials, nano degrees, and digital badges: New credentials for global higher education. *Int. J. Technol. Educ. Mark. (IJTEM)* **2015**, *5*, 36–49. [CrossRef]
32. Halavais, A. *Microcredentials on the Open Web*; AOIR Selected Papers of Internet Research: Mexico City, Mexico, 2013.
33. Pickard, L.; Shah, D.; De Simone, J.J. Mapping microcredentials across MOOC platforms. In *Proceedings of the 2018 Learning with MOOCS (LWMOOCS)*; IEEE: New York, NY, USA, 2018; pp. 17–21.
34. van de Laar, M.; West, R.E.; Cosma, P.; Katwal, D.; Mancigotti, C. The value of educational microcredentials in open access online education: A doctoral education case. *Open Learn. J. Open Distance e-Learn.* **2024**, *39*, 373–386. [CrossRef]
35. Selvaratnam, R.M.; Sankey, M.D. An integrative literature review of the implementation of micro-credentials in higher education: Implications for practice in Australasia. *J. Teach. Learn. Grad. Employab.* **2021**, *12*, 1–17. [CrossRef]

36. Ahsan, K.; Akbar, S.; Kam, B.; Abdulrahman, M.D. Implementation of micro-credentials in higher education: A systematic literature review. *Educ. Inf. Technol.* **2023**, *28*, 13505–13540. [CrossRef]
37. Ahmat, N.H.C.; Bashir, M.A.A.; Razali, A.R.; Kasolang, S. Micro-credentials in higher education institutions: Challenges and opportunities. *Asian J. Univ. Educ.* **2021**, *17*, 281–290. [CrossRef]
38. Rottmann, A.K.; Duggan, M.H. Micro-credentials in higher education. In *Handbook of Research on Innovations in Non-Traditional Educational Practices*; IGI Global: Hershey, PA, USA, 2021; pp. 223–236.
39. Thi Ngoc Ha, N.; Spittle, M.; Watt, A.; Van Dyke, N. A systematic literature review of micro-credentials in higher education: A non-zero-sum game. *High. Educ. Res. Dev.* **2023**, *42*, 1527–1548. [CrossRef]
40. Berry, B. Micro-credentials: The badges of professional growth. *Educ. Dig.* **2017**, *82*, 21.
41. Bartz, D.E.; Kritsonis, W.A. Micro-credentialing and the individualized professional development approach to learning for teachers. *Natl. Forum Teach. Educ. J.* **2019**, *29*, 1–11.
42. Hunt, T.; Carter, R.; Zhang, L.; Yang, S. Micro-credentials: The potential of personalized professional development. *Dev. Learn. Organ. Int. J.* **2020**, *34*, 33–35. [CrossRef]
43. Cosby, A.; McDonald, N.; Lovric, K. Designing a skills training pathway for the agricultural workforce from the employer perspective: Skills micro-credentials from seasonal worker to supervisor. *J. Agric. Educ. Ext.* **2024**, *30*, 535–552. [CrossRef]
44. Griffith, B.; Beauchamp, S.; Bates, R. Growing Oklahoma's Workforce Readiness Through Micro-Credentials. In *Career Ready Education Through Experiential Learning*; IGI Global: Hershey, PA, USA, 2021; pp. 1–18.
45. McGreal, R.; Olcott, D., Jr. *Micro-Credentials Landscape Report: Transforming Workforce Futures: Strategic Perspectives and Practices for University Micro-Credentials*; Technical Report; Athabasca University: Athabasca, AB, Canada, 2021.
46. European Commission. Council Recommendation on a European Approach to Micro-Credentials for Lifelong Learning and Employability. 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022H0627(01) (accessed on 1 May 2026).
47. Digital Credentials Consortium. *Building the Digital Credential Infrastructure for the Future*; Massachusetts Institute of Technology (MIT): Cambridge, MA, USA, 2020. Available online: https://digitalcredentials.mit.edu (accessed on 1 May 2026).
48. Lang, J.; Giglietta, K. Implementing continuing professional education micro-credentials in a university context. In *Handbook of Research on Credential Innovations for Inclusive Pathways to Professions*; IGI Global Scientific Publishing: Palmdale, PA, USA, 2022; pp. 45–64.
49. Varadarajan, S.; Koh, J.H.L.; Daniel, B.K. A systematic review of the opportunities and challenges of micro-credentials for multiple stakeholders: Learners, employers, higher education institutions and government. *Int. J. Educ. Technol. High. Educ.* **2023**, *20*, 13. [CrossRef] [PubMed]
50. Ford, B.; Srisuresh, P.; Kegel, D. Peer-to-peer communication across network address translators. In *Proceedings of the USENIX Annual Technical Conference, General Track*; USENIX Association: Berkeley, CA, USA, 2005; pp. 179–192.
51. Sporny, M.; Longley, D.; Sabadello, M.; Reed, D.; Steele, O.; Allen, C. *Decentralized Identifiers (DIDs) v1. 0*; Technical Report; World Wide Web Consortium (W3C): Cambridge, MA, USA, 2022.
52. Sporny, M.; Longley, D.; Chadwick, D.; Herman, I. Verifiable Credentials Data Model v2.0. W3C Recommendation REC-vc-Data-Model-2.0-20250515, World Wide Web Consortium (W3C), 2025. Available online: https://www.w3.org/TR/vc-data-model-2.0/ (accessed on 1 May 2026).
53. Márquez, P.L. Micro-Credentials SSI Prototype. 2026. Available online: https://github.com/Darthpab/micro-credentials/tree/main (accessed on 1 May 2026).
54. Hyperledger Foundation. Hyperledger Ursa. 2026. Available online: https://github.com/hyperledger/ursa (accessed on 1 May 2026).
55. Hyperledger Foundation. Hyperledger Indy. 2026. Available online: https://github.com/hyperledger/indy (accessed on 1 May 2026).
56. Hyperledger Foundation. Hyperledger Aries. 2026. Available online: https://github.com/hyperledger/aries (accessed on 1 May 2026).
57. Government of British Columbia. VON Network: A Portable Development-Level Indy Node Network. GitHub Repository. Part of the Verifiable Organizations Network (VON) Project. 2026. Available online: https://github.com/bcgov/von-network (accessed on 1 May 2026).
58. Unesco. *Recommendation on the Ethics of Artificial Intelligence*; United Nations Educational, Scientific and Cultural Organization: Paris, France, 2022.
59. GDPR. General Data Protection Regulation (EU) 2016/679, 2016. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 1 May 2026).
60. Wilczynski, A.; Budzik, K. Skillchain: A Service-Oriented Blockchain Platform for Secure and Scalable Microcredential Management. *IEEE Trans. Serv. Comput.* **2026**, 1–14. [CrossRef]

61. Bruguera, C.; Pagés, C.; Peters, M.; Fitó, A. Micro-credentials and soft skills in online education: The employers' perspective. *Distance Educ.* **2025**, *46*, 56–76. [CrossRef]
62. Lago Ávila, M.J.; Bartolomé Muñoz de Luna, A.; Martín Gómez, S. Soft Skills, Mentoring and Micro-Credentials: Strategies for the New Role of 21st Century Professors. *Multidiscip. J. Sch. Educ.* **2024**, *13*, 373–398. [CrossRef]
63. Epaphras, N. Bridging the Skills Gap: A Case for Micro-Credentials in Academic Programs in Institutions of Higher Learning. *Creat. Educ.* **2025**, *16*, 748–769. [CrossRef]
64. Moya, F.; Quesada, F.J.; Martínez, L.; Estrella, F.J. CertifIoT: An IoT and DLT-Based Solution for Enhancing Trust and Transparency in Data Certification. In *Proceedings of the International Conference on Ubiquitous Computing and Ambient Intelligence*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 127–138.

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.