FMDB *Transactions on Sustainable Techno Learning*

Blockchain's Role in Supporting a Culture of Lifelong Learning

Abeer Amer[1,*], Hisham Sameeh[2]

[1]Department of Information Systems and Computers, Faculty of Business, Alexandria University, Alexandria, Egypt.
[1]Department of Computer Science and Information Systems, Faculty of Management Science, Sadat Academy for Management and Sciences, Alexandria, Egypt.
[2]Department of Computer, Faculty of Business, Alexandria University, Alexandria, Egypt.
abamer.2000@gmail.com[1], hisham.sameeh@gmail.com[2]

Abstract: The demand for continuous skill development has grown significantly, emphasising the necessity of lifelong learning, particularly in the context of e-learning following the COVID-19 pandemic. However, current digital educational systems face several challenges. Academic records are often stored across multiple databases maintained by educational institutions, with restricted access, which prevents learners from managing their own achievements and limits access for job seekers. Additionally, paper-based certificates are susceptible to loss, damage, forgery, and counterfeiting, making authentication a time-consuming and complex process. Studies have shown that a significant percentage of CVs contain inaccurate or misleading information about academic qualifications and employment history. A blockchain-based approach to education provides a secure and transparent system for storing and managing educational credentials, including degrees, diplomas, and training certifications. Blockchain technology ensures tamper-proof data storage, reducing fraud risks and enhancing verification processes. Universities and government entities could oversee this system, allowing learners to share their verified achievements with third parties, such as other educational institutions, recruiters, or employers. This paper presents selected use cases from existing Literature, beginning with a basic blockchain-based educational system and subsequently integrating Smart Badges to support lifelong learning, followed by the implementation of a Self-Sovereign Identity Framework. Finally, the authors propose several research areas for further exploration.

Keywords: E-Learning Systems; Blockchain Technology; Self-Sovereign Identity Framework; Research Areas; Smart Badges; Reducing Fraud Risks; Tamper-Proof Data Storage; Educational System.

Received on: 10/07/2024, **Revised on:** 17/09/2024, **Accepted on:** 12/10/2024, **Published on:** 05/03/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSTL

DOI: https://doi.org/10.69888/FTSTL.2025.000388

Cite as: A. Amer and H. Sameeh, "Blockchain's Role in Supporting a Culture of Lifelong Learning," *FMDB Transactions on Sustainable Techno Learning*., vol. 3, no. 1, pp. 36–46, 2025.

1. Introduction

The need for continuous skill enhancement is growing, making lifelong learning indispensable [1]. Keeping up with emerging trends is essential for maintaining career stability, and since the COVID-19 pandemic, e-learning has gained significant popularity [2]. Verifying the authenticity of diplomas and certificates that validate an individual's skills and accomplishments is often a complex and time-intensive process due to various challenges. Academic records, such as degrees and diplomas, are

[*] Corresponding author.

typically stored as separate data across multiple educational institutions' databases, often with restricted access. Consequently, students and graduates have limited control over their own academic information, while third parties—such as employers or recruiters—are unable to view or contribute to these records. Traditional paper-based certificates pose several drawbacks. For instance, they may lack detailed descriptions of acquired skills due to space constraints. Additionally, as individuals complete more courses, the number of certificates required during job applications increases accordingly. Physical certificates are also susceptible to loss or damage, necessitating the allocation of time and financial resources for replacement. Furthermore, they are vulnerable to forgery and counterfeiting [2].

Studies indicate that a significant portion of CVs contain inaccurate or misleading information regarding academic credentials and employment history [1]. As a result, both individuals and organisations are increasingly seeking a solution that ensures accessibility and verification of graduates' certifications while offering a streamlined approach to managing personal academic records [1]. A blockchain-based approach offers a secure and reliable system for managing educational credentials, including degrees, diplomas, and training certifications, across various educational institutions [6]. This model enables educational providers to store and organise data efficiently while preserving its integrity and security through controlled access permissions. Universities and government bodies could serve as joint administrators of the blockchain network. While only universities should have the authority to create or update student degree records, the ability to share this information should rest solely with the student or graduate, without requiring approval from official entities such as universities or governments. This approach facilitates instant verification of credentials issued at different educational levels, ensuring authenticity.

Furthermore, integrating blockchain technology into education strengthens security by providing tamper-proof certificates [2]. This system mitigates fraudulent activities by ensuring both the integrity of educational data and regulated access for third parties, including universities, recruiters, and employers, regardless of their geographic location. In this paper, we present selected use cases from the Literature, starting with a simple implementation of a blockchain-based solution, then introducing Smart Badges for lifelong learning, and finally the Self-Sovereign Identity Framework.

2. What is Blockchain

Blockchain is a form of Distributed Ledger Technology (DLT) characterised by its immutability, decentralised structure, and replication across a peer-to-peer (P2P) network. The term "blockchain" derives from its structure, where validated transactions are systematically grouped into blocks through a consensus mechanism. Each block is cryptographically linked to its predecessor using a hash digest, ensuring both tamper-evident and tamper-resistant properties. This sequential chaining process continues, forming a linear chain of blocks that strengthens both security and data integrity within the network [6]. Once published, these blocks are appended to all copies of the distributed ledger across network participants, ensuring synchronisation and maintaining an append-only record system. Any conflicts that arise within the network are resolved autonomously through predefined rules, eliminating the need for a centralised authority.

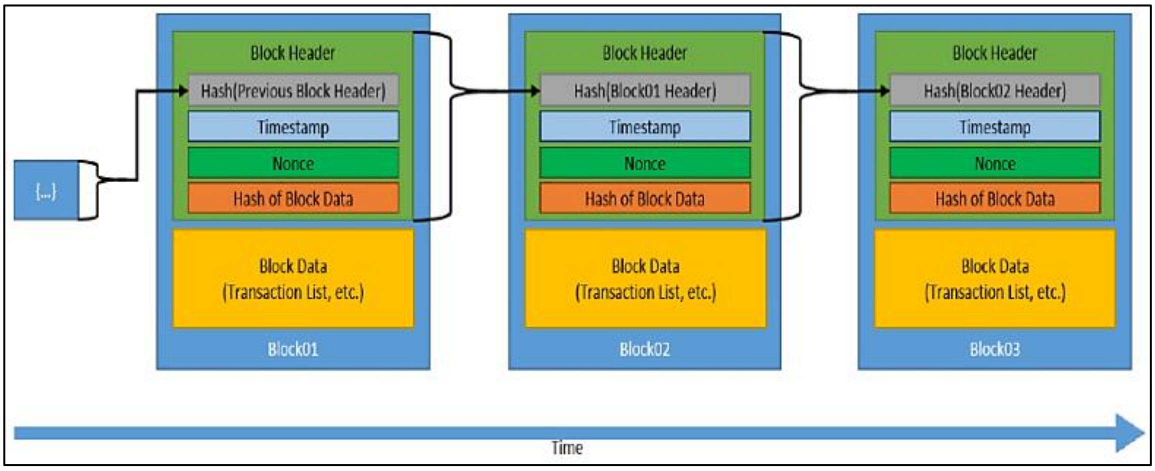


Figure 1: Blockchain general structure

As illustrated in Figure 1, the block structure consists of two primary components: the block header and the block body, with variations in their data depending on the implementation. The commonly used fields include:

- **Block Header:** Contains metadata related to the block, primarily including the previous block hash, the current block hash, and the timestamp marking the time of block creation. Additional information, such as the Merkle tree root, may be included if transactions are hashed using this structure.
- **Block Body:** Holds a list of transactions along with other relevant data. The block hash digest comprises the following elements [3]. The previous block hash, the hash of the current block header, and the hash of the current block data—primarily represented by the Merkle tree root. In the Merkle tree implementation, depicted in Figure 2, all transactions within a block are arranged in a hierarchical structure [4]. Each transaction is hashed and progressively combined until a single root hash emerges, encapsulating the entire dataset [3]. Notably, if any individual transaction is modified, the Merkle tree root will also change [5].

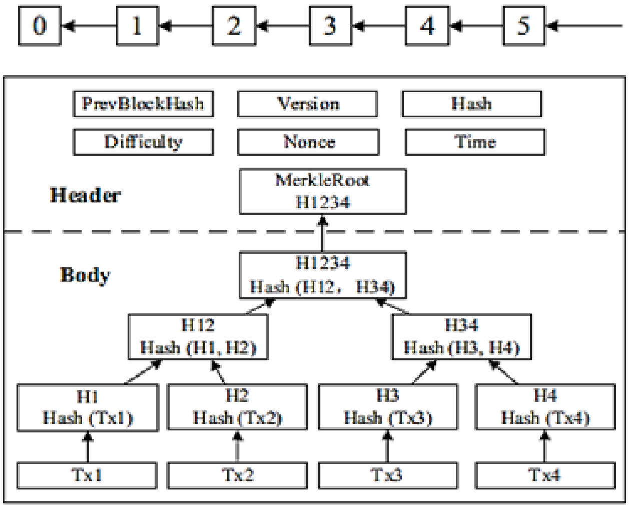


Figure 2: Blockchain general structure showing Merkle tree

A smart contract is the mechanism through which data is entered and processed within a blockchain. Essentially, smart contracts are self-executing programs stored on a blockchain that activate when predefined conditions are met. They facilitate the automated execution of agreements without the need for manual intervention, ensuring that all participants immediately receive verifiable outcomes while eliminating time delays and third-party involvement—ultimately reducing costs. Additionally, smart contracts can automate workflows by initiating subsequent actions once specific conditions are fulfilled [7]. This revised version improves readability and precision while maintaining the original intent. Types of Blockchain Networks are,

- **Public Permissionless Blockchain Networks:** A system is one that anyone can freely join, leave, have an identical copy of the “ledger,” issue transactions, write transactions, read transactions, and participate in transaction validation (consensus) without having to ask for permission, such as Bitcoin [9].
- **Public Permissioned Blockchain Networks:** This type of system is necessary in situations where specific identifiable actors (nodes, users) are granted permissions to write/read and update the system; however, all transactions should be publicly viewable [8].
- **Consortium Blockchains:** An ideal for business when all participant organisations share the responsibilities of maintaining a blockchain [10]. It is permissioned, so only identifiable actors (nodes, users) can utilise the systems [8].
- **Private - Permissioned - Blockchain Networks:** Deployed by one organisation that governs the network, executes the consensus protocol, maintains (writes/updates) the shared ledger, and controls who participates in the network [10]. The network is permissioned by default. Actors (nodes, users) are identified and users’ credentials are assigned by the organisation's administrators [3]; [8].

3. A Few Examples of Blockchain-based Systems in Education from the Literature

In Rauchs et al. [11], an extensive survey on blockchain-based applications is presented, examining their role in academia and the education sector. These applications encompass a range of functions, including online educational platforms that support examination processes, credential management, transcript systems, and academic certification in higher education. Furthermore, they facilitate the secure exchange of student information, improve transparency, and strengthen trust among stakeholders. A key aspect of the survey highlights the integration of artificial intelligence, data analytics, and higher education institutions, emphasising how universities enhance competitiveness by outsourcing course delivery and assessment procedures.

Additionally, the study examines the benefits of blockchain technology—such as immutability and traceability—by comparing it to traditional centralised systems and assessing the distinctive features of blockchain's decentralised framework.

4. Blockchain-based Case Studies in Education

In this section, we present selected use cases from existing research, illustrating the potential applications of blockchain-based solutions in the education sector**.**

4.1. The Romanian Blockchain-based Solution

In Romania, the Ministry of National Education (MEN) oversees the management of the Single National Student Enrolment Registry (RMUR). This digital database records student enrolment from both public and private universities, whether accredited or temporarily licensed. This system operates in accordance with Romanian Education Law No. 1/2011, Article [number]. 201, covering all academic years and study cycles. However, students and graduates do not have direct access to their academic records, and third parties cannot verify the authenticity of a candidate's degrees. Figure 3 illustrates the state of the system before and after the implementation of a blockchain-based solution in Romania.

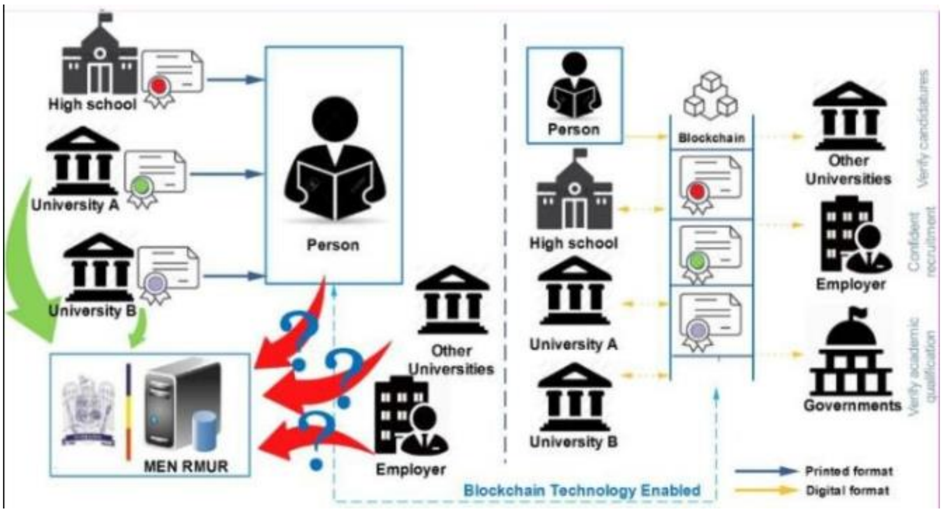


Figure 3: Romanian current state vs. blockchain-based solution

4.2. Ministry of National Education (MEN)

4.2.1. National Student Enrolment Registry (RMUR)

This model enables educational institutions to store and manage data efficiently while ensuring its integrity and security. Universities and government entities could serve as joint custodians of the blockchain network. However, only universities should have the authority to create or modify student degree records, ensuring that academic credentials remain authentic and resistant to counterfeiting. Crucially, students and graduates should have full control over sharing their records without needing approval from official bodies such as universities or governments. Additionally, access to academic data could be granted—with permission—to recruiters and employers. Future developments aim to incorporate Smart Badges [1].

4.2.2. Quali-Chain

This pilot case study examines the Quali-Chain paper, which seeks to enhance lifelong learning by integrating Smart Badges with personalised recommendations [12]. The paper focuses on four key areas to assess the impact of decentralisation: (1) lifelong learning, (2) smart curriculum design, (3) staffing in the public sector, and (4) Human Resources consultancy and competency management services. The primary objectives of the pilot papers, as illustrated in Figure 4, include: (1) ensuring transparent and immutable accreditation, (2) providing personalised recommendations, and (3) facilitating individual professional development.

Supporting Lifelong Learning
Transparent & Immutable Accreditation
Personalised Recommendations
Personal & Professional Progression

Figure 4: The overall goals of the pilot on supporting lifelong learning

- **Transparent and Immutable Accreditation:** Academic degrees and other educational credentials are awarded using Smart Badges, which are securely stored in the learner's e-Portfolio. These badges are based on Open Badges, a certification system that validates skill acquisition and knowledge attainment upon meeting specific criteria, such as completing an online course or other learning activities.
- **Personalised Recommendations:** Learners receive tailored suggestions on what to study next to enhance their education and career trajectory.
- **Personal and Professional Progression:** Recommendations are provided to learners regarding their next career steps, based on the academic qualifications they have obtained.

Quali-Chain stakeholder interactions within the core framework of lifelong learning are illustrated in Figure 5.

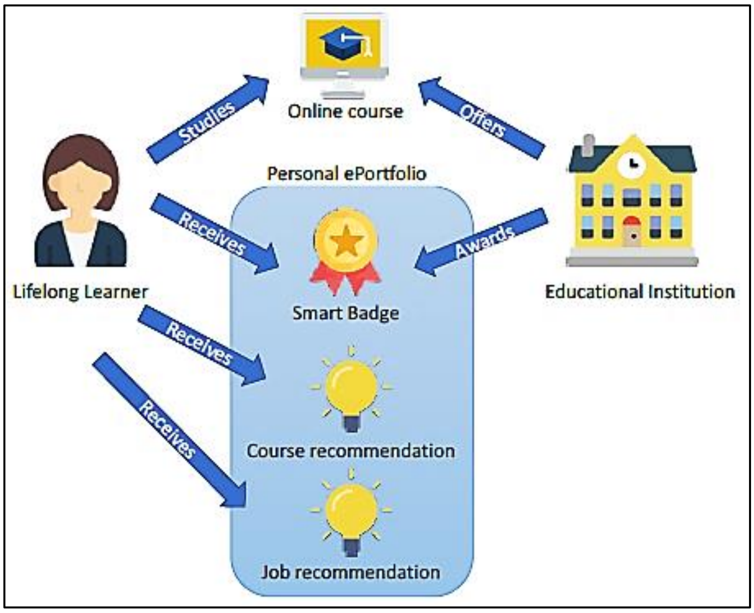


Figure 5: Stakeholder interactions in the main scenario of the lifelong learning pilot

As outlined in Sharma et al. [12], job market data is gathered by harvesting datasets of current job listings and their required skills from a job aggregator developed by the European Data Science Academy (EDSA). These datasets are integrated into Smart Contracts on the Ethereum Blockchain, enabling job-matching based on a learner’s badge-certified skills. In this approach, awarded badges are considered “smart” because they facilitate personalised recommendations for learners, guiding them toward relevant job opportunities. Future research aims to explore the implementation of Self-Sovereign Identity (SSI) for both learners and job seekers [12].

4.2.3. Edu-CTX

Edu-CTX is a web-based credit and grading system designed for higher education, integrating quizzes, digital badges, and micro-credentials to support learners in acquiring targeted skills. This system is modelled after the European Credit Transfer and Accumulation System (ECTS), where students within a distributed peer-to-peer network maintain individual wallets that store tokens upon successful course completion [2]. The structural design of Edu-CTX is illustrated in Figure 6 below:

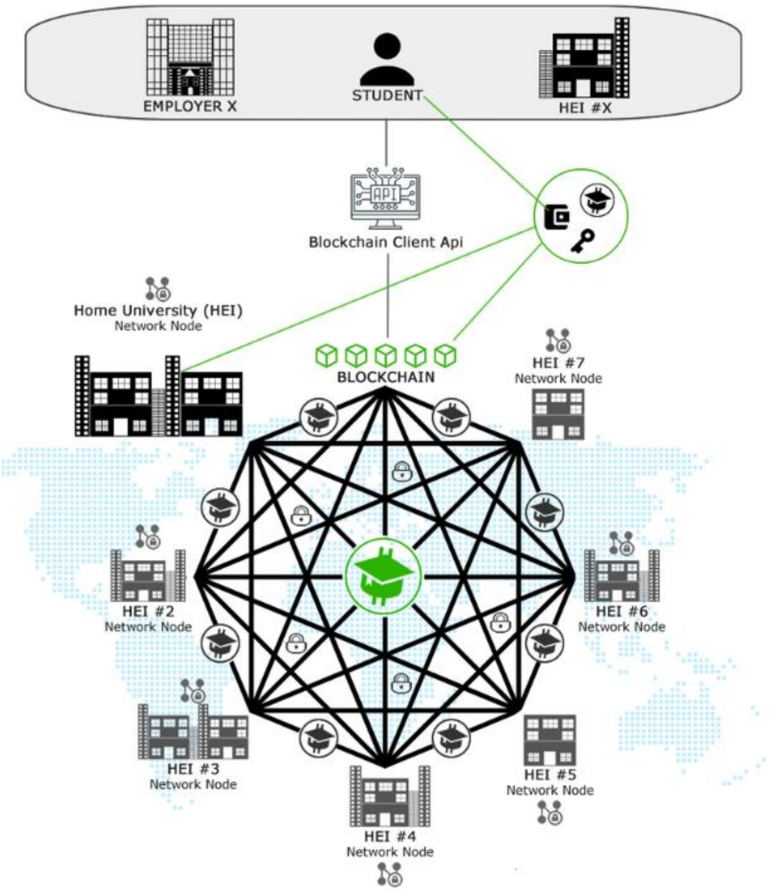
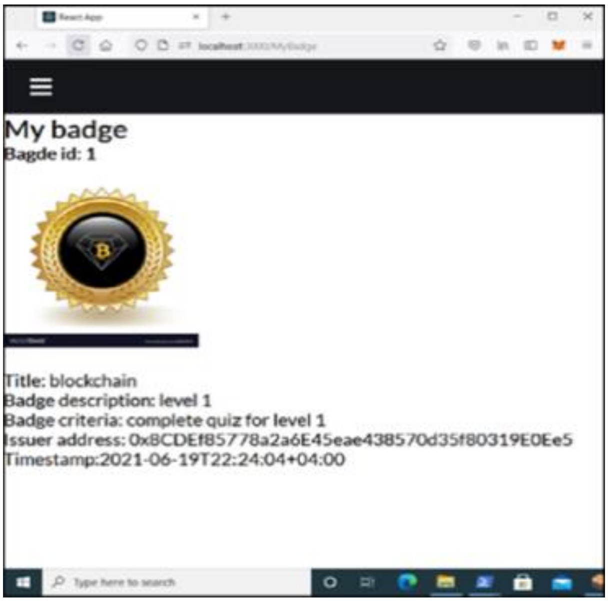


Figure 6: Design structure of Edu-CTX

4.3. A Digital Badge Consists of Three Fundamental Components

- **Signifier:** This is the visual representation of the badge, typically an image that symbolises the achievement. It includes a distinct name, a description, and may also provide guidance on how to earn the badge.
- **Completion Logic:** Defines the criteria required to obtain the badge, which includes:
    - **Trigger:** Specifies the action needed to qualify for the badge.
    - **Pre-requirement:** Outlines any conditions that must be met before activating the trigger.
    - **Conditions:** Details the specific achievements necessary to earn the badge.
    - **Multiplier:** Indicates the number of times the criteria must be fulfilled to receive the badge.
- **Reward:** Represents the benefits or recognition granted upon earning the badge.

Additionally, a digital badge features a clickable hyperlink that grants access to metadata. This metadata contains essential details such as the issuance date, the awarding entity, and other significant information. Metadata can be structured using JavaScript Object Notation for Linked Data (JSON-LD) as illustrated in Figure 7.



My badge

Bagde id: 1

Title: blockchain
Badge description: level 1
Badge criteria: complete quiz for level 1
Issuer address: 0x8CDEf85778a2a6E45eae438570d35f80319E0Ee5
Timestamp:2021-06-19T22:24:04+04:00

Figure 7: Student badge

4.4. The Functionality of Ed-CTX

- **Authentication:** Users, including learners and academic staff, must sign up, log in, and log out using valid credentials. Learners are assigned a certificate wallet for storing their achievements.
- **Course Management:** After successful authentication, academic users can add or update course details.
- **Examination on Blockchain:** Learners complete exams, and upon passing, they receive a course badge as recognition of their achievement (Figure 8).

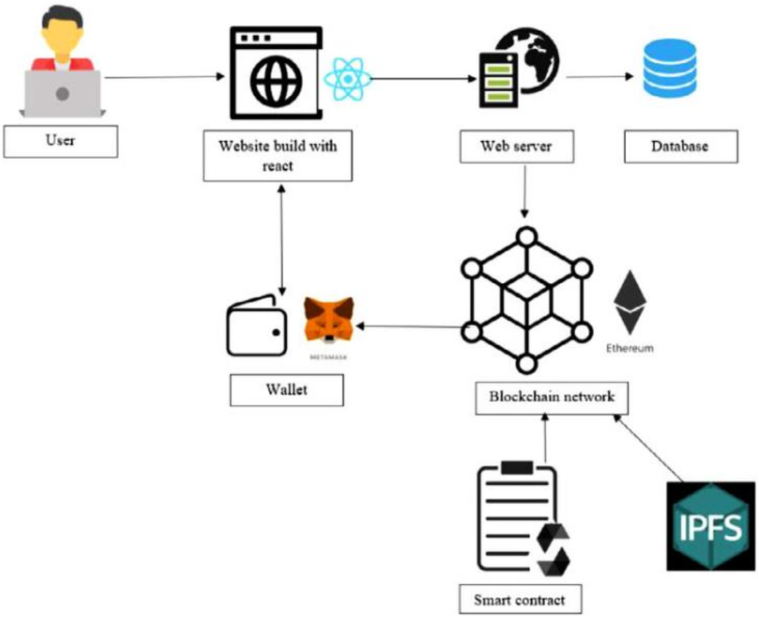


Figure 8: How Edu-TX works

4.5. European Self-Sovereign Identity Framework (ESSIF)

The European Blockchain Partnership (EBP) collaborated with the European Commission (EC) to establish the European Blockchain Services Infrastructure (EBSI), a platform designed to facilitate cross-border services that enable citizens and businesses to manage their identities, educational credentials, and registration documents across the European Union (EU) and beyond. EBSI functions as a public-permissioned blockchain, leveraging a Proof of Authority (PoA) consensus mechanism to ensure efficient and secure validation of transactions. Its APIs provide interoperability with Hyperledger Besu and Hyperledger Fabric. Hyperledger Besu functions as an Ethereum client running on the Ethereum Mainnet, while Hyperledger Fabric serves as a permissioned distributed ledger technology platform. Additionally, EBSI aims to adopt the European Learning Model (ELM) as the standard data framework for managing educational records [13]. EBSI has identified seven key use cases, with two of the most significant ones listed below:

- **European Self-Sovereign Identity:** Enables users to establish and manage their own digital identity across borders, granting them full control over their personal data.
- Diploma Management empowers citizens with digital ownership of their educational credentials, significantly reducing verification costs while enhancing trust in the authenticity of academic documents.

Self-Sovereign Identity (SSI) is a decentralised identity framework that enables digital identification and authentication, allowing individuals, organisations, and even devices to manage their own digital identities with enhanced trust, privacy, and security. Built on blockchain technology, SSI represents the third evolution of Identity Management (IdM), following two earlier models: centralised IdM, where users were required to create accounts with individual service providers (SPs), and federated IdM, where Identity Providers (IdPs) facilitated identity management. In both previous approaches, user identifiers and associated attributes were controlled by SPs or IdPs [15]. SSI operates with three key actors,

- **Identity Holder:** The entity (e.g., a user) requesting and managing their digital identity.
- **Issuer:** The organisation responsible for generating and digitally signing identities, issuing Verifiable Credentials (VCs) that contain various attributes or claims about the identity holder.
- **Verifier:** An entity that requests proof of identity from the holder, using VCs for authentication. Upon successful verification, the verifier grants access to digital services or products [15].

The World Wide Web Consortium (W3C) has established standardised components for SSI,

- **Decentralised Identifiers (DIDs):** Each DID is formatted as a URI and linked to a DID subject (typically an identity holder), along with a DID document containing details such as cryptographic public keys, biometric data, and authentication mechanisms.
- **Verifiable Credentials (VCs) and Verifiable Presentations (VPs):** A VC, sometimes referred to as a Digital Credential (DC), includes information about the issuer, the identity holder, and the claims being verified. The issuer digitally signs this credential to ensure authenticity. VC holders can compile data from multiple VCs issued by different entities and generate a Verifiable Presentation (VP), which can be submitted to a verifier as proof of identity or other required attributes.

A digital wallet is a crucial component in identity management systems. These wallets serve as portable and secure personal repositories, typically available as mobile or cloud-based applications that incorporate both a software interface and an encrypted database. A digital wallet enables users to: (a) Request and store Verifiable Credentials (VCs). (b) Store, manage, and control Decentralised Identifiers (DIDs), private keys, and other sensitive personal data. (c) Distribute Verifiable Presentations (VPs) as needed.

4.6. The ESSIF Framework Adapted to The University Context, As Described in Čučko et al. [14]

- The student has his own legal presentation issued by a Registration Authority as a Legal Entity.
- The uniquely identifiable legal entity is responsible for generating, revoking, and securing Decentralised Identifiers (DIDs) and associated cryptographic keys. Additionally, the DID is recorded on the EBSI Ledger.
- The university, also recognised as a legal entity, provides services and interacts with other parties by verifying data and facilitating digital interactions.
- The students securely store their verifiable identity in a user wallet, which contains all their Verifiable Credentials (VCs) and allows for data collection and sharing.
- Students can present a Verifiable ID or provide an attestation for identification and authentication when required by university staff and faculty.
- The students can also request additional verifiable attestations from the university, adding new VCs to their wallets [14].
- By accumulating multiple VCs, the students can provide a more extensive and credible set of verifiable data for various purposes (Figure 9).

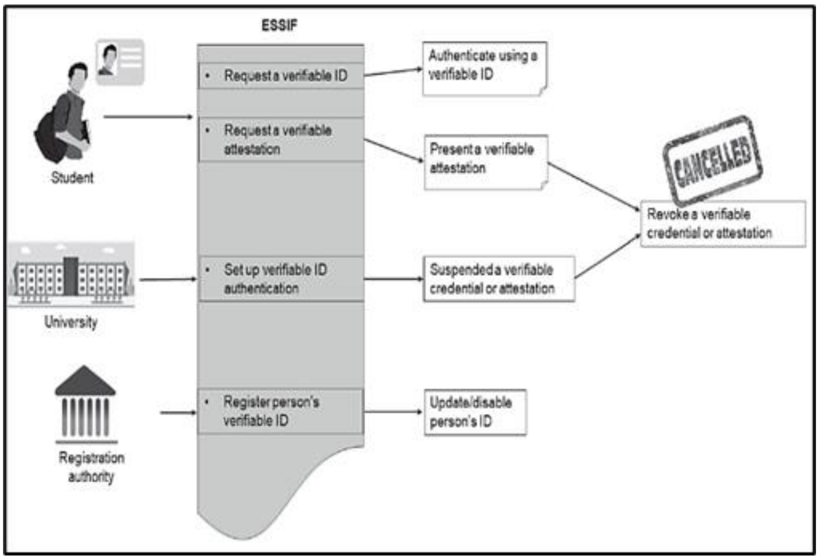

ESSIF
Request a verifiable ID
Request a verifiable attestation
Set up verifiable ID authentication
Register person's verifiable ID
Authenticate using a verifiable ID
Present a verifiable attestation
Suspended a verifiable credential or attestation
Update/disable person's ID
CANCELLED
Revoke a verifiable credential or attestation
Student
University
Registration authority

Figure 9: Scheme of the ESSIF adapted to the university context

The EBSI-based European ESSIF framework is designed primarily to authenticate both natural persons and legal entities, ensuring secure and verifiable digital identities across various sectors. Figure 10 illustrates how ESSIF can be utilised within the EU [16]:

- The student requests credentials from their university.
- The university issues the required credentials to the student.
- An EU agency requests proof of these credentials.
- The student verifies the credentials.

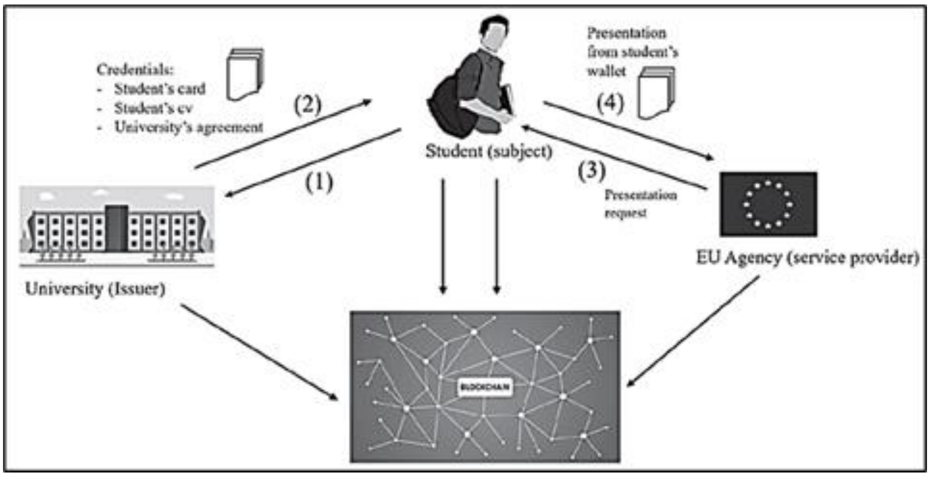


Figure 10: ESSIF can be employed in the EU

5. Discussion and Future Work

Blockchain-based solutions in education are gaining momentum. However, overcoming any native blockchain challenges and achieving the best configuration and/or fine-tuning are outside the scope of this writing. Blockchain solutions offer several advantages over traditional databases, as outlined in Zheng et al. [16].

- **Trust Among Unknown Users:** Blockchain operates on a decentralised model where transactions are verified and validated before being added to the ledger, ensuring trust among participants without requiring prior relationships. Traditional databases rely on administrators who control data access and modifications, limiting trust within the system.

- **Immutability of Data:** Blockchain ensures that all stored data remains unalterable, as each block is cryptographically linked to the previous one via hashing. Any attempt to modify data results in a changed hash, immediately signalling tampering. In contrast, data within conventional databases can be modified by authorised users or exploited by attackers, with no inherent mechanism for detecting or preventing unauthorised changes.
- **Data Redundancy and Recovery in Blockchain:** Blockchain maintains multiple synchronised copies of data across nodes in the network, ensuring that even if a node goes offline, its data remains intact and is recoverable upon rejoining the network. Traditional databases rely on administrators to perform regular backups and implement recovery plans. Without proper backup strategies, a database crash can result in permanent data loss.

As such, in a blockchain-based solution, unlike a database-based one, the digital badge/digital certificate owners will preserve their achievements even if the hosting entity or e-learning platform is shut down or goes out of business. Regarding Digital Badges, actually, there are commercial solutions, for instance, (credly.com, sertifier.com, badgecert.com) that provide services ranging from designing/building, issuing, hosting, publishing, and verifying Badges for free and on a price-based basis for organisations. Self-Sovereign Identity, however, is still in its infancy, with a significant push towards implementing solutions in every aspect of people's lives, including digital wallets. Examples of Self-Sovereign Identity providers, for research and commercial bases are (sovrin.org, microsoft.com, cheqd.io, nuggets. life, okta.com, openwallet.foundation) Importantly, in either case, there are three basic roles: holder, issuer, verifier, and an e-Portfolio for Digital Badge, as well as a digital wallet for SSI, and a digital badge if published on a blockchain. The authors suggest some research points to be considered regarding Badges or Credentials:

- Published papers and patents can be seen as a badge/credential that preserves the author(s)' rights and intellectual property, even if the publisher/journal/conference no longer exists.
- In the case of scholarships, the learner will typically need to complete and pass additional subjects before being eligible to work in the main course, allowing them to demonstrate progress through badges/credentials.
- In cases where universities are equilibrated in terms of working assignments, any required deviations could be assigned as badges/credentials to be achieved.
- For academic staff, the badges/credentials will determine in advance who the candidates are for promotion.

6. Conclusion

In this paper, we provided some use cases for blockchain-based solutions in education, showing the potential of blockchain in lifelong learning. Also, digital badges and Self-Sovereign Identity for digital credentials were presented. In addition, as mentioned in the discussion section, the authors proposed some research points for using smart Badges and Micro credential in future work, which briefly are: a) Issuing them for publications and patents b) For academics, using them for bonus and promotions systems c) To be used as a way of equilibration of degrees between universities d) To be used in scholarships as a way of showing progress and achievements.

Acknowledgement: The authors sincerely thank Alexandria University and Sadat Academy for Management and Sciences for their collaboration and institutional support, which were instrumental in carrying out this research.

Data Availability Statement: All relevant data underlying the findings of this study are available from the corresponding authors upon reasonable request.

Funding Statement: This work was undertaken without financial assistance from public, private, or not-for-profit funding bodies.

Conflicts of Interest Statement: The authors declare that no actual or potential conflicts of interest financial, personal, or professional exist in relation to this study.

Ethics and Consent Statement: Ethical principles were strictly observed in the conduct of this research. Participation was voluntary, informed consent was secured, and the anonymity and confidentiality of all participants were fully protected.

References

1. "What are smart contracts on blockchain?" *IBM*, 1986. Available: https://www.ibm.com/think/topics/smart-contracts [Accessed by 19/10/2023].
2. A. Grech, I. Sood, and L. Ariño, "Blockchain, self-sovereign identity and digital credentials: Promise versus praxis in education," *Frontiers in Blockchain*, vol. 4, no. 3, pp. 1–13, 2021.

3. A. Mikroyannidis, “Blockchain applications in education: A case study in lifelong learning,” *in Proc. 12th Int. Conf. Mobile, Hybrid, and On-line Learning,* Milton Keynes, United Kingdom, 2020.
4. A. Queiruga-Dios, J. José Bullón Pérez and L. Hernández Encinas, “Self-Sovereign Identity in University Context,” *2022 31st Conference of Open Innovations Association (FRUCT),* Helsinki, Finland, 2022.
5. C. Mulligan, J. Scott, S. Warren, and J. Rangaswami, “Blockchain Beyond the Hype a Practical Framework for Business Leaders,” *World Economic Forum,* Geneva, Switzerland, 2018.
6. C. Turcu, C. Turcu, and I. Chiuchisan, “Blockchain and its potential in education,” *arXiv preprint arXiv:1903.09300 [cs.CY]*, 2019. Available: https://arxiv.org/abs/1903.09300 [Accessed by 19/10/2023].
7. D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview, NIST Interagency or Internal Report (NISTIR) 8202 (Draft),” *National Institute of Standards and Technology(NIST),* Gaithersburg, Maryland, United States of America, 2018.
8. J. Grimshaw, “What is blockchain technology?” *Supply Chain Digital, IBM,* 2020. Available: https://supplychain digital.com/technology/ibm-blockchain-what-blockchain-technology [Accessed by 19/10/2023].
9. J. Zhang, S. Zhong, T. Wang, H. C. Chao, and J. Wang, “Blockchain-based systems and applications: a survey,” *Journal of Internet Technology,* vol. 21, no. 1, pp. 1–14, 2020.
10. K. Agrawal, M. Aggarwal, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, “An extensive blockchain based applications survey: Tools, frameworks, opportunities, challenges and solutions,” *IEEE Access*, vol. 10, no. 11, pp. 116858–116906, 2022.
11. M. Rauchs, A. Blandin, K. Bear, and S. B. McKeon, “2nd Global Enterprise Blockchain Benchmarking Study,” *Univ. of Cambridge, Cambridge Centre for Alternative Finance,* 2019. Available: https://papers.ssrn.com/sol3/papers.Cfm? abstract _id=3461765 [Accessed by 19/10/2023].
12. N. Sharma, M. Shamkuwar, S. Kumaresh, I. Singh, and A. Goje, “Introduction to blockchain and distributed systems—fundamental theories and concepts,” in Blockchain for Smart Cities, *Elsevier*, Cambridge, Massachusetts, United States of America, 2021.
13. P. Herbke and H. Yildiz, “ELMO2EDS: Transforming educational credentials into self-sovereign identity paradigm,” *in 2022 20th International Conference on Information Technology Based Higher Education and Training* (ITHET), Antalya, Turkey, 2022.
14. Š. Čučko, Š. Bećirović, A. Kamišalić, S. Mrdović, and M. Turkanović, “Towards the classification of self-sovereign identity properties,” *IEEE Access,* vol. 10, no. 12, pp. 88306–88329, 2022.
15. V. Chukowry, G. Nanuck, and R. K. Sungkur, “The future of continuous learning–Digital badge and microcredential system using blockchain,” *Global Transitions Proceedings,* vol. 2, no. 2, pp. 355–361, 2021.
16. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” *in 2017 IEEE International Congress on Big Data (Big Data Congress),* Honolulu, Hawaii, United States of America, 2017.