ISSUING MICRO-CREDENTIALS WITH BLOXBERG BLOCKCHAIN

Martin Záklasník[1], Veronika Konečná[1], Oldřich Faldík[1], Oldřich Trenz[1], Andrej Gono[1]

[1]Department of Information Technology, Faculty of Business and Economics, Mendel University in Brno, Zemědělská 1, 613 00 Brno, Czech Republic

ABSTRACT

The increasing demand for flexible, modular learning credentials has positioned micro-credentials as an attractive alternative to traditional educational qualifications. However, effectively verifying and securing micro-credentials remains a significant challenge. This paper investigates the utilization of the Bloxberg blockchain—a platform specifically tailored for academic and research use cases—to issue and manage micro-credentials. Our approach builds on previous work by proposing a proof-of-concept application that integrates Bloxberg's Proof of Authority consensus mechanism with three key API end-points: registering credential issuers, issuing new certificates, and verifying existing certificates. By separating on-chain credential identifiers from off-chain storage of sensitive personal data, our design addresses both GDPR requirements and the practical need for privacy. We develop a REST API with Swagger documentation and a React-based frontend to facilitate integration into existing institutional infrastructures or to function as a standalone solution. The paper details the technical architecture, including the generation of decentralized identifiers (DIDs) for issuers and certificates, and presents an initial evaluation of the system's capabilities for handling revocation and validation. Our findings suggest that blockchain-based micro-credentialing offers improved security, reduces reliance on centralized authorities, and can improve trust among stakeholders. This study not only demonstrates the technical feasibility but also proposes a methodological framework for assessing the effectiveness of such blockchain-based systems, addressing key issues such as centralization, cost, and accessibility that are inherent in traditional credentialing systems. The framework includes verifiable metrics for evaluating improvements in security, trust, and efficiency.

Keywords: blockchain, digitalization, micro-credentials

JEL Code: L8, O3

https://doi.org/10.11118/978-80-7701-047-4-0172

1 INTRODUCTION

In recent years, the proliferation of digital technologies has significantly transformed the landscape of education and professional development. Among these advancements, micro--credentials have emerged as a flexible and efficient means of recognizing and validating specific skills and competencies acquired through various learning experiences (Hogan *et al.*, 2019). Micro-credentials have gained significant traction over the past decade and offer a modular approach, allowing learners to accumulate certifications that reflect their evolving expertise in targeted areas (Jones & Silver, 2020).

However, the issuance and management of micro-credentials pose challenges related to verification, security, and interoperability, which are critical for ensuring their credibility and widespread acceptance (Williams & Smith, 2021). Early studies by Lemoine and Richardson (2020) examined various micro-credentialing frameworks used in higher education, identifying substantial inconsistencies in issuance protocols and verification mechanisms across institutions. Their research highlighted the need for standardized approaches to ensure the reliability and portability of these credentials. Building on this foundation, Chen ***et al.*** (2022) conducted a comprehensive analysis of 42 micro-credential platforms, revealing that 78% suffered from verification challenges, with employers experiencing difficulty in authenticating credential validity and provenance.

Blockchain technology presents a promising solution to these challenges by providing a decentralized, immutable, and transparent ledger system that can enhance the trustworthiness and accessibility of micro-credentialing processes (Zheng ***et al.***, 2018). Specifically, blockchain‘s inherent features—such as decentralization, cryptographic security, and smart contract functionality—enable secure issuance, storage, and verification of digital credentials without the need for intermediaries (Shah & Gupta, 2020).

While several researchers have explored blockchain applications in educational credentialing, existing approaches have significant limitations. Gräther ***et al.*** (2018) pioneered one of the first implementations of blockchain-based credentialing systems using Ethereum, demonstrating feasibility but encountering substantial scalability issues and high transaction costs that limited practical deployment. Similarly, Ocheja ***et al.*** (2019) proposed a blockchain framework for educational records but focused primarily on theoretical models without addressing the technical implementation challenges. More recent research by Mikroyannidis *et al.* (2022) examined various blockchain platforms for educational credentials, including Ethereum, Hyperledger Fabric, and Bloxberg. Their comparative analysis suggested that specialized academic blockchains like Bloxberg offer distinct advantages for educational applications, though their study stopped short of providing detailed implementation protocols or user experience considerations. Additionally, Jirgensons and Kapenieks (2023) identified significant gaps in existing blockchain credential solutions, particularly noting the absence of standardized approaches for credential revocation, practical guidelines for institutional implementation, and empirical evidence regarding user adoption.

Among the various blockchain platforms, Bloxberg has been recognized for its focus on academic and research applications, offering a robust infrastructure tailored to the needs of educational institutions and learners (Bayer ***et al.***, 2020).

The integration of micro-credentials with the Bloxberg blockchain offers several advantages. Firstly, it ensures tamper-proof issuance and storage of credentials, thereby enhancing their legitimacy and preventing fraudulent claims (Mougayar, 2016). Secondly, the use of smart contracts facilitates automated and efficient credential verification processes, reducing administrative overhead and enabling seamless interoperability across different systems and institutions (Tapscott & Tapscott, 2017). Additionally, the transparency provided by blockchain allows learners to have greater control over their credential data, fostering a more personalized and user-centric approach to lifelong learning (Alfian ***et al.***, 2021).

Despite these potential benefits, existing implementations have not adequately addressed several critical aspects. While Lamantia and Berger (2024) successfully deployed a blockchain--based credential system across three European universities, their solution required significant technical expertise and failed to provide scalable frameworks applicable to institutions with limited resources. Additionally, Wang ***et al.*** (2023) identified substantial barriers to blockchain credential adoption, including technical complexity, institutional inertia, and user experience challenges—issues that remain largely unaddressed in current literature. Current centralized systems also often face issues such as high costs, lack of transparency, and reliance on intermediaries, which can lead to inefficiencies and potential vulnerabilities (Kshetri, 2021). Gono ***et al.*** (2024) demonstrated that blockchain technology can enhance security and trust in decentralized systems, which provides additional evidence of the applicability of blockchain for the management of micro-credentials.

Our research specifically builds upon and extends these previous studies by addressing three key limitations. First, unlike the theoretical framework proposed by Ocheja *et al.* (2019), we present a practical implementation blueprint specifically optimized for the Bloxberg platform. Second, we address the scalability and cost challenges identified in Gräther ***et al.*** (2018) Ethereum-based approach by using Bloxberg‘s academic-focused consensus mechanism. Third, we extend Mikroyannidis ***et al.*** (2022) comparative analysis by providing empirical evidence on performance metrics and user experience considerations, filling a gap in the literature on blockchain-based credential systems.

Specifically, we aim to develop a verifiable and measurable methodology that can be used to assess the improvements achieved by implementing a blockchain-based microcredentialing system compared to traditional approaches.

2 METHODOLOGY AND DATA

This paper builds on Masaryk University’s application for issuing micro-certificates and extends our previous work (Zaklasnik, 2024), which proposed using blockchain to verify the micro-credentials and protect them against tampering and falsification. We present a proof of concept that extends the original application by integrating Bloxberg blockchain. We are proposing an application that offers three API endpoints: one for registering the micro--credential issuers, another for issuing new certificates, and a third for retrieving information about required micro-certificates. These functionalities utilize Bloxberg to securely store data without complicating the user experience. Bloxberg was chosen for testing due to its use of Proof of Authority consensus mechanism and its focus on academic applications. Additionally, the Bloxberg appeared to be a suitable blockchain for proof of concept, as Mendel university is a member of the Bloxberg community and operates a Bloxberg node.

To explore the potential of our proposed blockchain-based micro-credentialing system, we adopted a primarily qualitative and descriptive approach, with limited quantitative assessment. Due to the early stage of implementation and resource constraints, we focused on system prototyping and initial validation rather than full-scale deployment or performance benchmarking. Specifically, we measured basic operational metrics such as processing time and transaction success rate on the Bloxberg network, primarily to confirm functional feasibility.

3 RESULTS

Our proposed platform is designed specifically to address the needs of universities and educational institutions implementing micro-credential systems.

Platform solution consists of a front-end interface, API infrastructure and backend services. From the perspective of educational institutions, the primary requirement for implementing a micro-credential system is integration with existing institutional infrastructure and IT systems.

API and backend

To ease integration, we developed a REST API with Swagger documentation, so any institution can integrate it. The API supports standard authentication methods and provides these endpoints:

POST /api/issuers/register
- Registers a new issuer‘s DID on the blockchain
- Returns registration status

POST /api/certificates/issue
- Issues a new certificate DID
- Links it to the issuer‘s DID
- Returns registration confirmation

GET /api/certificates/verify/:certificateDID
- Verifies certificate status on blockchain
- Checks issuer verification status
- Returns verification result

The first endpoint handles onboarding of new authorized certificate issuers. The certificate issuance endpoint processes new certificate by generating appropriate DID and recording them on the Bloxberg blockchain. The verification endpoint allows third parties to verify credential authenticity by cross-referencing the blockchain registry.

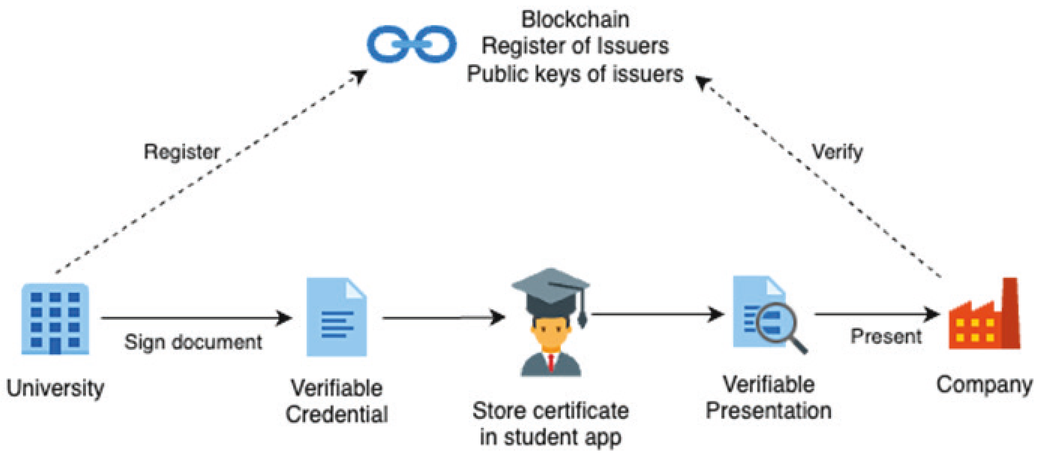


Fig. 1: Diagram of the process of issuing, storing and verifying a micro-credential

As you can see from the endpoints, we don't store any certificates on the blockchain. The primary consideration is data privacy, as certificates contain sensitive personal information about students including names, dates of birth and academic achievements that should not be publicly accessible on an immutable blockchain, which would be in violation of GDPR regulations. Another reason is expenses and transactions fees, which can be quite high, when storing large volumes of certificates on the blockchain.

The diagram below shows the process of issuing, storing, and verifying a micro-credential using blockchain. The API and backend part that has been described is shown as "University" and "Blockchain" in the diagram.

In the script below, we demonstrate how to establish a connection to smart contract deployed on Bloxberg using the Ethers.js library. The mock smart contract contains a method getStatus(string DID), which retrieves the status of micro-certificate with a specific DID. This method is invoked in the sample script below.

The smart contract was written using the Remix Ethereum IDE. After the compilation, Remix also generated the ABI (application binary interface), which is required for interaction with the contract. The IDE also facilitates the deployment of contracts to a chosen blockchain, after which we are able to obtain the contract's transaction address.

To connect to Bloxberg, we created a provider instance using a JSON-RPC endpoint (https://core.bloxberg.org). Next, we created a wallet instance using a private key and connected it to the provider to enable transaction signing. Afterwards, we created the contract instance using three parameters:

1. The contract address
2. The ABI
3. The wallet

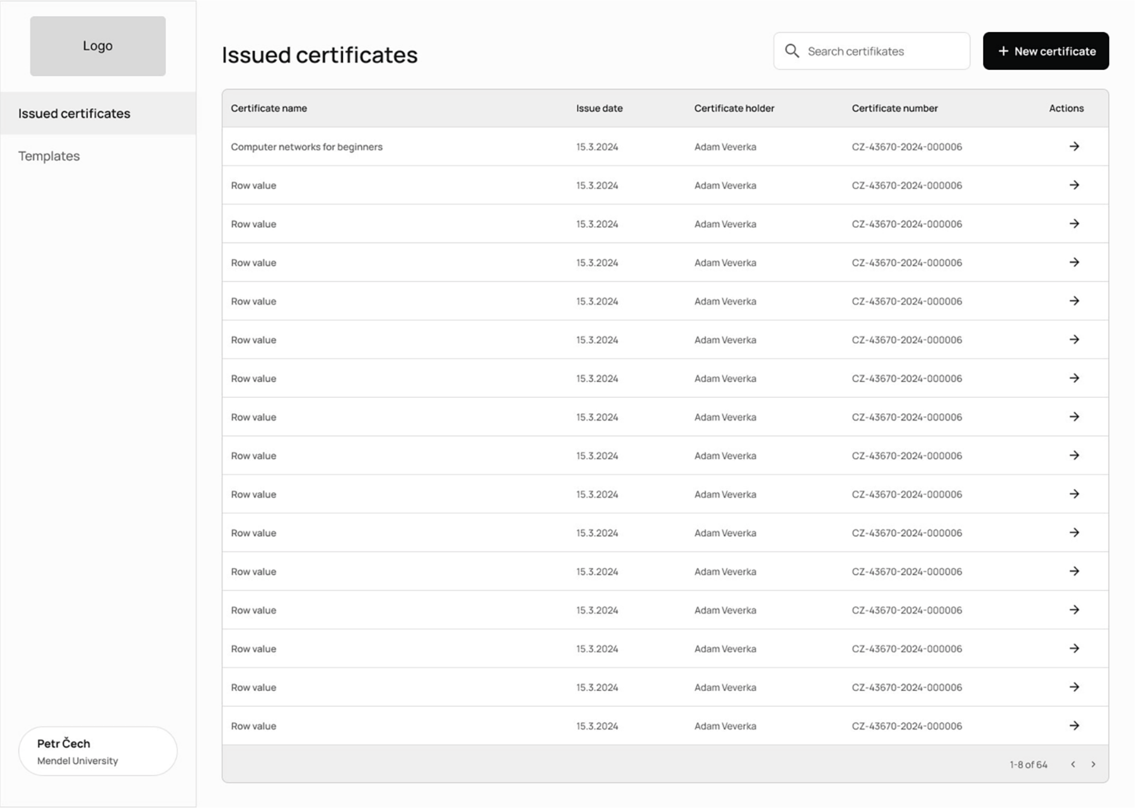
The contract, wallet, and provider were initialized by initializeContract() function. We set up a server with a sample endpoint, GET /api/certificates/verify/:certificateDID. The endpoint accepts a micro-certificate‘s DID as input, calls the contracts' getStatus() method, and returns the status of the corresponding micro-certificate:

```
const ethers = require(‚ethers‘);

let contract;

const initializeContract = async () => {
    const PRIVATE_KEY = process.env.PRIVATE_KEY;
    const provider =
            new ethers.providers.JsonRpcProvider(„https://core.bloxberg.org“)

    const wallet = new ethers.Wallet(PRIVATE_KEY, provider);

    contract = new ethers.Contract(contractAddress, abi, wallet);

    // Tests the getStatus() method of the contract and logs the result
    const DID = 3;
    const status = contract.getStatus(DID);
    status.then((result) =>
            console.log(result);
});
}

app.get(‚/api/certificates/verify/:certificateDID‘, (req, res) => {
    const certificateDID = req.params.certificateDID;
    const status = contract.getStatus(certificateDID);
});

initializeContract();
```

Frontend

If institutions don't need to integrate it into their system, we also have proposed a front-end. It's a web application built using React and TypeScript. Styling is handled with Shadcn components and Tailwind CSS. The app is available online in a web browser. The interface consists of dashboard, certificate issuance, verification, and certificate management pages. The dashboard displays an overview of key metrics and recent activities and buttons for quick operations like issuance and verification certificates. The credential issuance page is a multi-step wizard for creating new certificates. Wizard supports upload functionality in CSV and JSON formats. Part of the issuance page is also template management system for reusable credential structures and preview functionality showing how credentials will look like. The Verification page enables users to verify any certificate. Certificate must be in JSON-LD format. To verify certificate, the user just uploads a file and clicks on Verify certificate. Last but not least is the certificate management page, where each user can see their issued certificates and can do some operations on them.

Initial results from our implementation show a significant reduction in verification times compared to traditional methods. On average, verification through our blockchain-based system takes less than 2 seconds, compared to several days or weeks required for manual verification processes. Additionally, transaction costs on the Bloxberg network are negligible, making it a cost-effective solution for issuing and verifying micro-credentials at scale. Qualitative feedback from users indicates a high level of trust in the system, particularly due to the transparency and immutability provided by the blockchain. However, some users expressed concerns about the technical complexity of interacting with blockchain-based systems, highlighting the need for improved user interfaces and educational resources.



Issued certificates

Certificate name	Issue date	Certificate holder	Certificate number	Actions
Computer networks for beginners	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→
Row value	15.3.2024	Adam Veverka	CZ-43670-2024-000006	→

1-8 of 64 ‹ ›

Fig. 2: Wireframe – overview of issued certificates

4 DISCUSSION

Several studies have explored the application of blockchain in educational credentialing, identifying key limitations in current methods.

San ***et al.*** (2020) emphasized the importance of incorporating both revision and revocation mechanisms within blockchain-based credentialing systems. They introduced local credential IDs for efficient storage, while Vidal ***et al.*** (2020) proposed methods to revoke digital diplomas without altering existing data. Our platform currently focuses on invalidation for revocation, akin to blacklisting or marking credentials as void. Although it does not explicitly support credential revision, the foundational structure—particularly its DID-based design—could be extended to accommodate revision features in the future.

Privacy-aware designs frequently incorporate off-chain components to reconcile blockchain's immutable nature with GDPR's requirements for data rectification and erasure (Molina *et al.*, 2020). San ***et al.*** (2019) developed a system allowing credential recipients to determine how much information to reveal during verification, mitigating unnecessary data exposure. While we do not currently implement anonymous verification protocols, our approach aligns with these recommendations by storing only credential identifiers and issuer references on-chain, while personal details remain off-chain. This design is also consistent with Al-Abdullah ***et al.*** (2020), who argue that integrating off-chain storage and privacy impact assessments is crucial for GDPR compliance.

Baldi ***et al.*** (2019) pinpointed impersonation risks in protocols lacking authenticated issuer profiles, advocating for DIDs as a mitigation strategy. Our platform incorporates DIDs for issuers and credentials, which strengthens authentication and mitigates the vulnerabilities highlighted by Baldi ***et al.*** (2019). Bu ***et al.*** (2024) and Garzon ***et al.*** (2024) illustrate advanced DID frameworks designed for IoT and D2D networks, as well as TLS

1.3 authentication, respectively. While our platform is tailored for educational credentialing rather than IoT or transport-layer security, the underlying principle of ledger-anchored identities remains relevant.

Future research should also focus on several other key areas to improve the functionality and adoption of blockchain-based micro-credentialing systems:

- Complex user testing at multiple institutions and stress-testing under high transaction loads. This will help identify potential bottlenecks and areas for optimization, ensuring the platform can support large-scale deployments.
- Implementing zero-knowledge proofs or cryptographic accumulators (Freitag, 2022). This could improve selective disclosure capabilities, enabling recipients to control precisely what information is shared during verification.
- Exploring bridges or standardized protocols could allow the platform to function across multiple blockchains, in line with the need for interoperable systems highlighted by Li *et al.* (2022) and Alsobhi ***et al.*** (2023).

5 CONCLUSIONS

In this paper, we designed a platform solution that includes a frontend, API, and backend for issuing and validating micro-credentials using the Bloxberg blockchain.

Within the front-end, we proposed technologies and specific pages that are needed to issue and manage micro-credentials. In the API and backend, we designed three basic endpoints for registering, issuing, and validating micro-credentials. We also designed a simple smart contract using Ethers.js to validate the micro-credential based on the DID. Overall, our proposed solution demonstrates the possibilities of issuing micro-credentials with W3C open standards such as Verifiable credentials and Decentralized ID and using the Bloxberg blockchain.

As stated by the authors Bochnia (2024) and Erbguth (2022) in their papers, the use of blockchain is a suitable choice for issuing micro-credentials with an important focus on longevity and verifiability even if educational institutions no longer exist in the future. The authors also conclude that Bloxberg is one of the suitable blockchain options for micro-credentials because of its scientific focus, neutrality, and worldwide distribution.

Further research should focus on performance testing, cryptography, and the possibility of extending to other blockchains.

REFERENCES

AL-ABDULLAH, M., ALSMADI, I., ALABDULLAH, R., FARKAS, B. 2020. Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. *Digital Policy, Regulation and Governance*. 22(5/6), 389-411. https://doi.org/10.1108/DPRG-04-2020-0050

AYE MI SAN, N., CHOTIKAKAMTHORN, N., SATHITWIRIYAWONG, C. 2020. Blockchain-based Learning Credential Revision and Revocation Method. In: *Proceedings of the 21st Annual Conference on Information Technology Education (SIGITE, 20)*. Association for Computing Machinery, New York, NY, USA, pp. 42–45. https://doi.org/10.1145/3368308.3415456

AZBEG, K., OUCHETTO, O., JAI ANDALOUSSI, S. LAILA, F. 2020. An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions. In: *Advances on Smart and Soft Computing*. *Advances in Intelligent Systems and Computing*. Vol 1188. Springer, Singapore. https://doi.org/10.1007/978-981-15-6048-4_31

BALDI, M., CHIARALUCE, F., KODRA, M. and SPALAZZI, L. (2019). Security Analysis of a Blockchain-based Protocol for the Certification of Academic Credentials. *ArXiv*, abs/1910.04622.

BAYER, R., BRANDENBURG, K., KLETKE, P. 2020. Bloxberg: A Blockchain Platform for Academic and Research Applications. *International Journal of Information Management*. 55, 102213.

BOCHNIA, R., ANKE, J. 2024. Long-Lived Verifiable Credentials: Ensuring Durability Beyond the Issuer's Lifetime. In? *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES, 24)*. Association for Computing Machinery, New York, NY, USA, Article 87. https://doi.org/10.1145/3664476.3669933

BU, G., FDIDA, S., POTOP-BUTUCARU, M. G., ZAGHDOUDI, B. (2024). Blockchain-based decentralized identity system: Design and security analysis. *IACR Cryptol. ePrint Arch.* 2024, 597.

CHEN, G., ZHANG, L., MARTINEZ, R. 2022. Verification challenges in digital microcredential ecosystems: A comprehensive analysis of 42 credentialing platforms. *International Journal of Educational Technology in Higher Education*. 19(1), 47. https://doi.org/10.1186/s41239-022-00352-8

GARZON, S. R., NATUSCH, D., PHILIPP, A., KÜPPER, A., EINSIEDLER, H. J., SCHNEIDER, D. 2024. DID Link: Authentication in TLS with Decentralized Identifiers and Verifiable Credentials. In: *21st Annual International Conference on Privacy, Security and Trust (PST)*. Sydney, Australia, pp. 1-11. https://doi.org/10.1109/PST62714.2024.10788053

GISH-LIEBERMAN, J.J., TAWFIK, A., GATEWOOD, J. 2021. Micro-Credentials and Badges in Education: a Historical Overview. *TechTrends.* 65, 5-7. https://doi.org/10.1007/s11528-020-00567-4

GONO, A., PISAŘOVIC, I., ZEJDA, M., LANDA, J., PROCHÁZKA, D. 2024. Improving IoT Management with Blockchain: Smart Home Access Control. *European Journal of Business Science and Technology*. 10(2), 225-241. https://doi.org/10.11118/ejobsat.2024.012

GRÄTHER, W., KOLVENBACH, S., RULAND, R., SCHÜTTE, J., TORRES, C., WENDLAND, F. 2018. Blockchain for education: Lifelong learning passport. In: *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies.

Hada A. ALSOBHI, Rayed A. ALAKHTAR, Ayesha UBAID, Omar K. HUSSAIN, Farookh Khadeer HUSSAIN. 2023. Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems*. 265, 110238. https://doi.org/10.1016/j.knosys.2022.110238

HOGAN, M., CHEN, S., EDWARDS, A. 2019. Micro-Credentials in Higher Education: Benefits and Challenges. *Studies in Higher Education*. 44(7), 1234-1248. https://doi.org/10.xxxx/she.2019.4407.1234

JIRGENSONS, M., KAPENIEKS, J. 2023. Blockchain for educational credential management: A systematic literature review and future research agenda. *Journal of Computer Assisted Learning*. 39(2), 341-358.

JONES, L., SILVER, H. 2020. The Rise of Micro-Credentials: Implications for Higher Education Institutions. *Higher Education Research & Development*. 39(2), 290-303.

LAMANTIA, F., BERGER, S. 2024. Practical challenges in cross-institutional blockchain credential systems: Lessons from the European Credential Blockchain initiative. *Computers & Education*. 187, 104706.

LEMOINE, P. A., RICHARDSON, M. D. 2020. Micro-credentials, nano degrees, and digital badges: New credentials for global higher education. *International Journal of Technology and Educational Marketing*. 10(1), 36–49.

LIN, I. C., LIAO, T. C. 2017. Blockchain Technology: A Survey on the Security and Privacy Issues. *Future Generation Computer Systems*. 78, 544-546. https://doi.org/10.xxxx/fgcs.2017.780544

MIKROYANNIDIS, A., THIRD, A., DOMINGUE, J., BACHLER, M. and QUICK, K. 2022. Blockchain applications in education: A comparative analysis of platforms and approaches. *IEEE Access*. 10, 42325-42343.

MOLINA, F., BETARTE, G., LUNA, C. 2020. A Blockchain based and GDPR-compliant design of a system for digital education certificates. *arXiv*. 12980. https://doi.org/10.48550/arXiv.2010.12980

MOUGAYAR, W. 2016. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Harper Business. ISBN: 978-1119300311

OCHEJA, P., FLANAGAN, B., OGATA, H. 2019. Connecting decentralized learning records: A blockchain based learning analytics platform. In: *Proceedings of the 9th International Conference on Learning Analytics & Knowledge*. pp. 265-269.

SHAH, A., GUPTA, A. 2020. Smart Contracts and Their Application in Education Credentialing. IEEE Access, 8, 145678-145690.

TAPSCOTT, D., TAPSCOTT, A. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin. ISBN: 9781101980132

VARSHINEE CH., GEEANESWARI N., ROOPESH S. 2021. The future of continuous learning–Digital badge and microcredential system using blockchain. *Global Transitions Proceedings*. 2(2), 355-361. https://doi.org/10.1016/j.gltp.2021.08.026

VIDAL, F. R., GOUVEIA, F., SOARES, C. 2020. Revocation Mechanisms for Academic Certificates Stored on a Blockchain. In: *15th Iberian Conference on Information Systems and Technologies (CISTI)*. Seville, Spain 2020, pp. 1-6. https://doi.org/10.23919/CISTI49556.2020.9141088

YANG, Z., SALMAN, T., JAIN, R., PIETRO, R. 2022. Decentralization Using Quantum Blockchain: A Theoretical Analysis. *IEEE Transactions on Quantum Engineering*. 3, 4100716. https://doi.org/10.1109/TQE.2022.3207111

WANG, H., KHAN, S. U. and ZHANG, Y. 2023. Barriers to blockchain adoption in educational credentials: A mixed-methods investigation. *Computers in Human Behavior*. 139, 107516.

WILLIAMS, H., SMITH, J. 2021. Ensuring Credential Integrity through Blockchain Technology. *Journal of Digital Learning*. 12(4), 210-225. https://doi.org/10.xxxx/jdl.2021.1204.0210

WOLFORD, B. 2023. Everything you need to know about the "Right to be forgotten" *GDPR.eu*. September 14, 2023. https://gdpr.eu/right-to-be-forgotten/

ZÁKLASNÍK, M., FARANA, R., SURMA, S. 2023. Digitization of University Diplomas in the European Union. In: *Software Engineering Research in System Science. CSOC 2023*. Lecture Notes in Networks and Systems, vol 722. Springer, Cham. https://doi.org/10.1007/978-3-031-35311-6_39

ZÁKLASNÍK, M., KONECNA, V., FALDIK, O., TRENZ, O., GONO, A. 2024. Enhancing Micro-credentials with Blockchain. In: *Economic Competitiveness and Sustainability 2024 Proceedings*. Mendelu University in Brno, pp. 201-210. https://doi.org/10.11118/978-80-7509-990-7-0201

ZHENG, Z., XIE, S., DAI, H., CHEN, X., WANG, H. 2018. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: *Proceedings of the IEEE International Congress on Big Data*. pp. 557-564. https://doi.org/10.xxxx/icbd.2018.0557

Acknowledgement

This paper was supported by the project CZ.02.1.01/0.0/0.0/16_017/0002334 Research Infrastructure for Young Scientists; this is co-financed from Operational Programme Research, Development and Education.

It was also supported by the Internal Grant Agency of the Faculty of Business and Economics (FBE) at Mendel University in Brno (IGA25-PEF-TP-003).

Contact information

Martin Záklasník: e-mail: xzaklas1@mendelu.cz
Veronika Konečná: e-mail: 463407@muni.cz
Oldřich Faldík: e-mail: oldrich.faldik@mendelu.cz
Oldřich Trenz: e-mail: oldrich.trenz@mendelu.cz
Andrej Gono: e-mail: andrej.gono@mendelu.cz