ENHANCING MICRO-CREDENTIALS WITH BLOCKCHAIN

Martin Základsník[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 article addresses the problem of using micro-credentials in the educational process and explores the possibilities of their deployment through blockchain technology. The topic of micro-credentials as the first step in the process of digitalization of the educational process is presented along with the setting of its trustworthiness. A variety of advantages can be associated with micro-credentials, including the confirmation of individual transactions at the level of the educational process.

One of the main problems in the centralized storage of micro-credentials is the risk of unauthorized access and the possibility of leakage of sensitive information. This paper proposes the implementation of blockchain technology as a way to decentralize data storage. This would eliminate the threat of unauthorized access and provide a higher level of data security and integrity.

Challenges associated with a centralized certificate authority such as scalability issues and outages are also discussed. It can be evaluated that blockchain can provide a robust and reliable framework for digitizing certificates in the education sector.

The conclusions of the paper highlight the benefits of decentralization through blockchain and the need to open up the certification network for corporate certificates. Overall, the paper discusses the importance and benefits of using blockchain technology to enhance the security and efficiency of digital certificates in the education sector.

Keywords: blockchain, digitalization, micro-credentials

JEL Code: L8, O3

1 INTRODUCTION

Digitalization is one of the most discussed topics in recent years. Every industry is affected by digitalization in some way. Within the education sector, many certificates or diplomas are being issued, which currently exist mainly in paper form. The disadvantage of paper certificates is that verifying their authenticity can be complicated and they are therefore relatively easy to falsify. Proving a paper certificate is also complicated by the difficulties of certified copies and so on. The solution may be to digitalize these certificates.

https://doi.org/10.11118/978-80-7509-990-7-0201

The first step of digitalization in education is the digitalization of individual successfully completed courses, the micro-credentials. Micro-credentials have several advantages. They provide students with a visual and tangible record of their skills or achievements. By taking inspiration from gaming badges, they can create an element of competition and reward that is typical in a gaming environment. Earning a badge or micro-certificate can be seen as a reward for achieving a specific goal or skill (Gish-Lieberman, 2021). These certificates can also then be used to prove completion of a course without the student completing the entire study programme.

Another key step in the process of digitalization of education is the storage of digital certificates in a central database. While this offers advantages in accessibility and management, it brings with it security challenges. A central database may face the risk of unauthorized access or leakage of sensitive information contained in digital certificates. In addition, if this database is down or unavailable, authentication of certificates can be complicated (Hada, 2023).

One possible solution to these challenges may be the implementation of blockchain technology. Blockchain offers a decentralized way of storing data, which can eliminate the risk of unauthorized access or manipulation of certificates. This would ensure a higher level of security and data integrity. Moreover, due to decentralization, it would be possible to authenticate certificates even in the event of central system failures. Thus, the implementation of blockchain could provide a robust and reliable framework for digitizing certificates in education (Zaklasnik, 2023).

The aim of the article is to outline the possibilities of extending the existing platform (Masaryk University, 2023) for issuing micro-credentials created by Masaryk University and Charles University with the use of blockchain technology. The Masaryk University provides a central verification point and storage place for micro-credentials and Charles University provides a central catalogue of courses for which can be issued micro-credentials issued. This approach has several limitations related to scalability, openness and resiliency. (Charles University, 2024)

Proposed solution will ensure decentralization and higher security of the whole system and the possibility of involving other educational institutions and companies, which will create a unique unified platform in which the user can have all the certificates from all different institutions. The A sub-goal is then to introduce the JSON-LD data format for micro-credentials and the process of issuing and storing micro-credentials data on the blockchain.

2 EXISTING SOLUTIONS

Typically, the existing solutions are possible to integrate with own Learning Management Systems (LMS) and main publishing platforms, meaning they can be easily integrated into university systems. They offer the possibility to share credentials on social platforms such as LinkedIn, Facebook, X and others, as well as manage the public profiles for both issuer and recipient and download the credential in various formats. The solutions often provide data analytic tools for monitoring the issuance of certificates, as well as their performance and impact. They are usually well scalable and being offered to small, as well as enterprise-sized institutions. The blockchain layer is often included in a broader subscription model.

2.1 Credly

Credly enables users to issue, manage and claim digital credentials. To claim a credential on Credly, the recipient must create an account. Issuing digital credentials on Credly is facilitated through the paid dedicated Acclaim platform. The issuance can be one-time manual or automated, using Credly's API integrated into existing systems. In the case of Credly, blockchain is not the underlying platform but rather an extension available as part of the Acclaim subscription. To publish the credential on the blockchain, first, the issuer much enable this possibility and then it must be approved by the receiver as well or the receiver can claim the credential without the blockchain verification (Credly, 2024).

2.2 Sertifier

Sertifier provides digital certificates and badge solutions for startups, small to medium-sized businesses, and enterprises. Their certificate offerings range from product certificates and online courses to employee training. Among their clients are Paypal, Cisco, Coachhub, Johnson & Johnson, and others, with over 8 million credentials issued. Sertifier operates in a hybrid mode, combining traditional storage and blockchain technologies. Two out of three subscription plans include blockchain features, providing enhanced security, authentication, and streamlined verification processes to prevent data tampering. They use the robust blockchain platform Velocity Network™ to ensure the integrity of every credential and enable real-time verification anywhere and anytime. Moreover, the Verified Wallet is necessary for storing credentials.

By digitally signing the credentials, the issuer guarantees their authenticity. The credentials are then issued and stored on the blockchain. The recipient must confirm the credential accuracy, claim it, and add it to their own blockchain-verified portfolio (Sertifier, 2024).

2.3 CredSure

CredSure is credentialing platform utilized by over a million users worldwide. Is uses blockchain for the credential's verification and stores all the credentials on the blockchain. They primarily focus on eliminating the issues connected to paper certificates and offer a platform for the translation of paper docs to digitalized files.

They enable credential collection, data evaluation, or ensuring trust. In the case of CredSure, both issuer and receiver of the credentials need their blockchain wallet where the credentials will be stored.

Users and verifiers can access the credential using unique URL or QR code on the verification page, that displays the issued course or product. CredSure also enables automation of the issuance and sending of credentials and badges, while providing technical support (Credsure, 2024).

2.4 EvidenZ

EvidenZ is a framework for blockchain verification of credentials, primarily focusing on higher education. Currently, 232 institutions across 25 countries are involved. It prioritizes user-friendliness and supports multiple devices and can operate on any blockchain.

For the issuance of every certificate, the essential part of the process is burning a part of the BCDT token. Among others, EvidenZ collaborates with Avalanche, Binance, and uses aleph.im for data storage on a secure and decentralized network. EvidenZ stores only encrypted data on the blockchain, rather than the actual documents or their hash fingerprints. Before issuing the data, it first verifies the identity of data issuers to establish trust. It is also convenient that no registration is needed to claim the credential, and owning a blockchain wallet is not required (although an email confirmation is needed to claim the credential). This is because EvidenZ uses shareable URLs for permanent access to the credential (EvidenZ, 2024).

3 METHODOLOGY AND DATA

The authors Selvaratnam and Sankey (2021) identify a number of disadvantages of paper certificates in the context of micro-credentials. Paper certificates are static, easy to falsify, difficult to share, and lacking in detailed information about the qualifications achieved. In addition, the production of paper certificates has a negative impact on the environment. In contrast, digital micro-credentials offer flexibility, robust security, ease of sharing, detailed information and environmental friendliness. The authors highlight that digital micro-credentials are

better suited to modern trends in education and the labour market and represent a more efficient and modern alternative to paper certificates.

3.1 Current micro-service infrastructure

The current micro-credentials system at Masaryk University integrates several technological components to ensure efficient course management, issuance, and verification of micro-credentials.

The system issues micro-certificates in electronic format (JSON-LD) following European Digital Credentials (EDC) specifications. Each micro-certificate contains essential details about the learner‘s achievements, issuer information, and validity period. If incorrect data is found post-issuance, the certificate can be invalidated, marking it as invalid and disabling its verification links without deleting it from the database.

Issued micro-certificates are accessible to recipients through digital wallets or direct email. They are not stored in a public database, preserving privacy and security. Verification is facilitated by a web-based tool, EDCI Viewer, allowing third parties to upload the micro-certificate file for validation, thus ensuring integrity and authenticity.

The system generates a PDF version of the micro-certificate, including a verification link. This representation meets standard requirements and can be digitally signed by the issuing institution for additional authenticity. Utilizing RESTful API for secure data transfer over HTTPS, the system ensures all API requests are authenticated, allowing only authorized clients to access or modify data.

A central database stores all issued micro-certificates and their metadata, enabling easy retrieval and management. The system supports automated updates and maintenance of certificate validity, including the renewal of electronic seals. There is also web interface, which caters to different user groups, including public verifiers, administrative personnel, and recipients of micro-certificates. This simplifies the processes of certificate issuance, management, and verification.

We aim to achieve three main goals in the extension of Masaryk University‘s existing platform for issuing micro-credentials with blockchain technology:

1. Decentralization and increased security: by using blockchain technology, the platform will move from a centralized model to a decentralized one. This transition increases the overall security of the system because the data is distributed across a network of nodes, making it resistant to tampering and unauthorized changes.
2. Openness and scalability: implementation of the blockchain simplifies the involvement of new entities outside Masaryk University. This allows other educational institutions and companies to join the platform, which supports collaboration and creates a uniform ecosystem for micro-credentials.
3. Standardization: JSON-LD (JavaScript Object Notation for Linked Data) is the W3C standard used for micro-credentials. JSON-LD offers a standardized and machine-readable format that is not dependent on any one platform or system.

This article uses both qualitative and quantitative research approaches. Within the qualitative analysis, it investigates existing literature related to blockchain technology in the context of educational certificates, specifically micro-credentials. The quantitative analysis then examines the technical aspects of blockchain implementation. This includes an analysis of existing blockchain platforms and protocols suitable for issuing and verifying micro-credentials.

Blockchain technology was selected for a decentralized approach of issuing certificates, with emphasis on speed, energy efficiency and security. Proof of Authority (PoA) algorithm was preferred for its speed, proven reliability and wide use in private blockchains.

The feasibility of PoA as a consensus algorithm in blockchain networks have been explored by Joshi (2021), who emphasizes the need for security, reliability, and speed in such

algorithms. Ali, Sahib and Waleed (2019) further discuss the use of PoA in preserving authentication and authorization on the blockchain, highlighting its potential in addressing the challenges of big data size and verification time. Alrubei, Ball and Rigelsford (2021) proposes a novel consensus mechanism, Honesty-based Distributed Proof-of-Authority (HDPoA), which combines PoA and Proof-of-Work (PoW) to enhance security and reduce confirmation time in IoT-blockchain applications. Lastly, Khalil, Aziz and Asif (2021) suggest the use of PoA in the Ethereum blockchain platform for charitable organizations, emphasizing its potential to enhance trust and transparency.

Trusted authority-formed voters were selected as participants in the network, contributing by issuing and verifying certificates. The evaluation of different blockchains led to the preference of Proof of Authority over other algorithms to achieve optimal security and efficiency results. Considering privacy and legal issues, an analysis of challenges related to the right to be forgotten and certificate updates was also considered.

Limitations

This paper only covers the design concept for the platform extension. Full implementation of the proposed solution would require further research and development, including pilot testing.

4 RESULTS

Masaryk University uses JSON-LD format for their micro-credentials platform.

JSON-LD (JSON for Linked Data) provides a standardized format for structuring and representing data (W3C, 2022). Among the advantages is that JSON-LD is human readable. Each micro credential can be used to record all certificate data such as student identity, course completion data, number of credits, etc. This structured data allows for efficient processing across multiple systems and platforms, including integration with a blockchain platform. Below is an example of what a micro-credential looks like in JSON-LD format.

```
{
 “@context”: [
   “https://www.w3.org/2018/credentials/v1”,
   “https://www.w3.org/2018/credentials/examples/v1”
 ],
 “id”: “http://example.edu/credentials/58473”,
 “type”: [“VerifiableCredential”, “AlumniCredential”],
 “issuer”: “https://example.edu/issuers/565049”,
 “issuanceDate”: “2010-01-01T00:00:00Z”,
 “credentialSubject”: {
   “id”: “did:example:ebfeb1f712ebc6f1c276e12ec21”,
   “alumniOf”: {
     “id”: “did:example:c276e12ec21ebfeb1f712ebc6f1”,
     “name”: [{
       “value”: “Example University”,
       “lang”: “en”
     }, {
       “value”: “Exemple d’Université”,
       “lang”: “fr”
     }]
   }
 },
 “proof”: { ... }
}
```

Fig. 1: Verifiable Credentials Data Model v1.1.
Source: W3C, 2022

A decentralized approach provided by blockchain could make the process of issuing certificates faster and not dependent on one central authority, when it comes to certificates that require human input and aren't issued automatically by digital authority.

When choosing a blockchain suitable for this use-case, we identified multiple key requirements. To be proven beneficial over typical centralized databases, it should be fast enough, energy efficient and secure, while allowing decision-making for a selected group of members. This approach prefers private blockchains and specific consensual algorithms. It eliminates, for example, widely spread Proof of Work, that is secure, but slow and energy consuming. It also makes Proof of Stake to be questionable, potentially allowing one party to own more voting power, unless this concern is addressed at the beginning. (Xiao et al., 2020) We also intend to avoid experimental and untested solutions. As a suitable solution now, it seems to be a Proof of Authority consensual algorithm, as it is fast, tested, not too complex for implementation and used widely in private blockchains. The voters are selected, trustworthy authorities, and as motivation could serve their reputation and right to stay in the ecosystem, instead of transaction fees (Azbeg, 2021. Khalil, 2021). The voters would be companies and academic institutions involved in the network, issuing certificates and validating those of theirs, as well as accepting new members into the network. This way, every new incoming authority will gain a voting right and the ecosystem will be naturally scaled-up.

As we try to think about a long-lasting solution, it is worth considering the infrastructure to be quantum resilient, as the academic sector could be prone to possible future quantum attacks. A lot of blockchains aren't easily adjustable and don't implement quantum resistant algorithms at the moment (Yang, 2022).

Although the certificate owners would be able to own the certificate and decide whether to make it private or not, there are still privacy and legal issues in this aspect. A potential challenge is the whole legal framework itself, which isn't well established for blockchain yet. Blockchain nature could challenge some legal requirements, such as the right to be forgotten defined by GDPR, that contradicts with the immutable nature of blockchain (Wolford, 2023). A subsequent issue is the need to update the certificate, for example in case it becomes invalid or was issued wrong. This particular aspect of changing policies should be discussed prior, when setting up the blockchain rules. In this case it should be noted that changes into blockchain transactions are very often hard to implement and could introduce more vulnerabilities.

Another potential issue could be initial investment into the new infrastructure, which should be calculated if it is worth the potential advantages. On the other hand, blockchain eliminates the single point of failure risk. The centralized databases, of course, use replicas and back-ups, that usually stays more storage efficient than blockchain (as every involved party needs to have their own blockchain replica), although the centralized databases also need to be managed, giving space to more failures and security issues. Therefore, the proposed solution of blockchain infrastructure should also address ways to optimize storage efficiency.

The process of creating and distributing micro-credentials in an educational institution involves several steps. The core components of the system include the educational institution, a JSON-LD generator, a cryptographic hashing function, a blockchain network, a QR code generator, and a student application.

The blockchain network uses the Proof of Authority consensus algorithm, chosen for its transaction processing capabilities and minimal energy consumption. Validators in this network are trusted entities, such as academic institutions ensuring data integrity and security. Smart contracts are utilized to automate the issuance, verification, and revocation of credentials on the blockchain.

Each micro-credential is structured in the JSON-LD format, enabling seamless integration with the blockchain. This standardization supports the representation of detailed credential data, including student identity, course completion data, and credit count. Credentials are issued in both digital format for blockchain records and as downloadable PDFs for offline use. Each PDF certificate includes a QR code that links back to the blockchain record for verification purposes.

All credential data are hashed using cryptographic functions (SHA-256) and stored on the blockchain, safeguarding against tampering and unauthorized alterations. Verification of credentials can be performed through decentralized nodes, ensuring availability and reliability even if a central system fails.

Important part of the system are RESTful APIs to connect the blockchain with existing Learning Management Systems (LMS) and the Student Information System (SIS). These APIs facilitate secure data exchanges and real-time updates of credential statuses.

The practical process then starts, when the student completes a course or training for which the student can earn a micro-credential. After successful course completion, students can opt for a digital version of their diploma. If they choose digitization, their consent must be obtained and stored in line with GDPR regulations. With consent, the institution can generate a "Verifiable Credential" (digital diploma adhering to W3C standards) containing relevant information such as course title, student name, completion date and other metadata. The student can then download a micro-credential from the institution via a secure online portal and store it in their digital wallet, which can be a software application on a mobile device (Základsník, 2023).

At the same time, a hash is generated using a cryptographic hash function, such as SHA-256, from the content of the certificate. A hash is a unique and fixed string of characters that represents the entire contents of a micro-credential. This hash is stored on the blockchain, which secures it from manipulation and allows independent verification of the micro-credential.

It is also possible to generate a PDF certificate. This certificate is used for offline presentation and contains all relevant information about the micro-credential, including the QR code. The QR code makes it easy to verify the validity of the certificate by scanning it with a smartphone or other device.

The image below shows the entire flow of generating and storing a micro-credential.

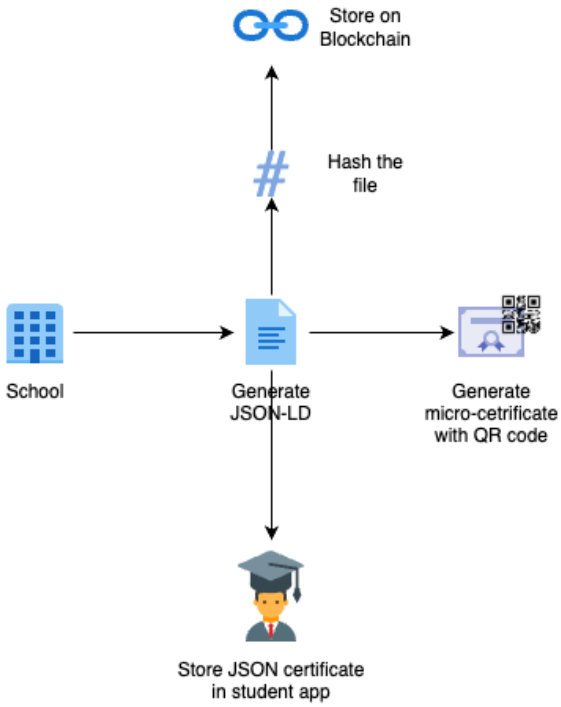

Fig. 2: The process of generating and storing micro--credentials on the blockchain, 2024

5 DISCUSSION AND CONCLUSIONS

Traditional paper certificates in education are prone to falsification and fraud as mentioned by the authors Selvaratnam and Sankey (2021). As well as that, students may find it difficult to prove the legitimacy of the certificates issued in different institutions.

In this paper, we research and propose the implementation of micro-credentials and blockchain for digitizing education. According to experts, the use of Blockchain technology in education is a potential use case (Casey, 2019. Clark, 2016).

Our proposed extension of Masaryk University's existing platform for issuing micro-credentials using blockchain technology offers several advantages over the current centralized system. By decentralizing the platform, we ensure the overall security and integrity of the micro-credentials issuance process, where data is protected from tampering and modification. Compared to similar existing solutions, our proposal does not issue credentials solely in digital form, but rather serves as an extension of paper certificates and both formats are supposed to coexist alongside each other. Additionally, having a private blockchain with a proof of authority algorithm grants involved parties a voting right a decision-making option, which could help our solution to evolve in alignment with academic sector needs

In addition, by implementing blockchain, we enable the involvement of new educational institutions beyond Masaryk University. In this way, we are creating a universal platform and ecosystem where students can have all the certificates they have achieved.

The future work will involve a comprehensive requirement analysis and system design identifying and engaging key stakeholders, including academic institutions, certification authorities, and potential employers.

Next step is setting up the blockchain network that supports the PoA consensus algorithm. The configuration of blockchain nodes for participating institutions will follow, ensuring each node is correctly integrated into the network and capable of issuing and verifying micro-credentials.

Next development will involve finalizing the JSON-LD format for micro-credentials. This format must include all necessary metadata and adhere to W3C standards, ensuring interoperability and ease of use. There will be an intuitive user interface for facilitating the issuance, management, and verification of micro-credentials by both issuers and recipients. Integrating the blockchain system with existing Learning Management Systems (LMS) at participating institutions will be another critical task.

Detailed testing will be conducted to ensure the system works as intended and is secure. Functional testing will verify that all system components operate correctly, while security testing will identify and mitigate potential vulnerabilities. A pilot deployment involving a limited number of courses and students will follow. The system's performance will be evaluated in terms of speed, scalability, and user satisfaction.

Acknowledgements

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.

REFERENCES

ALI, W. A., SAHIB, N. M. and WALEED, J. 2019. Preservation Authentication and Authorization on Blockchain. In: *2019 2nd International Conference on Engineering Technology and its Applications (IICETA)*, pp. 83-88. https://doi.org/10.1109/IICETA.2019.8835346

ALRUBEI, S. M., BALL, E. and RIGELSFORD, J. M. 2021. Securing IoT-Blockchain Applications Through Honesty-Based Distributed Proof of Authority Consensus Algorithm. In: *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1-7. https://doi.org/10.1109/CyberSA52016.2021.9435428

AZBEG, K., OUCHETTO, O., JAI ANDALOUSSI, S. and LAILA, F. 2020. An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions. In: *Advances on Smart and Soft Computing*, pp. 357-369. https://doi.org/10.1007/978-981-15-6048-4_31

BLOCKCERTS. 2024. *Blockchain Credentials*. https://www.blockcerts.org/

CASEY, J. 2019. *My Skills Project* [White Paper]. IFI Charitable Trust. https://myskills.org.uk/wp-content/uploads/2019/03/My-Skills-White-Paper-25-3-19.pdf

CLARK, D. 2016. Ten ways Blockchain could be used in education. *oeb-insights* [online]. https://oeb.global/oeb-insights/10-ways-blockchain-could-be-used-ineducation/

CREDLY. 2024. *Digital Credentials*. https://info.credly.com/

CREDSURE. 2024. Certif-ID International GmbH. *CredSure* [online]. https://credsure.io/

DNV. 2024. Traceable trusted certificates. *www.dnv.com* [online]. https://www.dnv.com/assurance/certificates-in-the-blockchain/

EVIDENZ. 2024. *The ultimate blockchain digital credentialing technology*. https://www.evidenz.io/

GISH-LIEBERMAN, J. J., TAWFIK, A. and 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

ALSOBHI, Hada A., ALAKHTAR, Rayed A., UBAID, Ayesha, HUSSAIN, Omar K., HUSSAIN, Farookh Khadeer 2023. Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems*, 265, ISSN 0950-7051. https://doi.org/10.1016/j.knosys.2022.110238

CHARLES UNIVERSITY. 2024 *Zlepšení prostupnosti vzdělání na úrovni vysokých škol pomocí mikrocertifikátů*. https://cczv.cuni.cz/CCZV-572.html

CHARLES UNIVERSITY. 2023. *Micro-Credentials at Charles University*. https://cczv.cuni.cz/CCZV-572-version1-prirucka___micro_credentials_na_uk_eng.pdf

JOSHI, S. 2021. Feasibility of Proof of Authority as a Consensus Protocol Model. *ArXiv,* abs/2109.02480.

KHALIL, I., AZIZ, O. and ASIF, N. 2021. Blockchain and Its Implementation for Charitable Organizations. In: *2021 International Conference on Innovative Computing (ICIC)*, pp. 1-10.

MASARYK UNIVERSITY. 2023. Mikrocertifikáty ve vzdělávání. MU je zavádí jako jedna z prvních v Evropě. *MUNI* [online]. https://www.em.muni.cz/udalosti/16554-mikrocertifikaty-ve-vzdelavani-mu-je-zavadi-jako-jedna-z-prvnich-v-evrope

SELVARATNAM, Ratna Malar and SANKEY, Michael. 2021. An integrative literature review of the implementation of micro-credentials in higher education: Implications for practice in Australasia. *Journal of Teaching and Learning for Graduate Employability*, 12, 1-17. https://doi.org/10.21153/jtlge2021vol12no1art942

SERTIFIER. 2024. *Sertifier*. https://sertifier.com/

VARSHINEE, C., GEEANESWARI, N. and ROOPESH, S. 2021. The future of continuous learning–Digital badge and microcredential system using blockchain. *Global Transitions Proceedings*, 2, 355-361. ISSN 2666-285X. https://doi.org/10.1016/j.gltp.2021.08.026

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

WORLD WIDE WEB CONSORTIUM–W3C. 2022. *Verifiable Credentials Data Model v1.1*. https://www.w3.org/TR/vc-data-model/

XIAO, Y., ZHANG, N., LOU, W. and HOU, Y. T. 2020. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys & Tutorials*, 22(2), 1432-1465. https://doi.org/10.1109/COMST.2020.2969706

YANG, Z., SALMAN, T., JAIN, R. and 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

ZÁKLASNÍK, M., FARANA, R. and SURMA, S. 2023. Digitization of University Diplomas in the European Union. In: SILHAVY, R. and SILHAVY, P. (Eds.). S*oftware 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

Contact information

Martin Zaklasnik: email: xzaklas1@mendelu.cz
Veronika Konecna: email: 463407@mail.muni.cz
Oldrich Faldik: email: oldrich.faldik@mendelu.cz
Oldrich Trenz: email: oldrich.trenz@mendelu.cz
Andrej Gono: email: xgono@mendelu.cz