STUDENT-DRIVEN RESEARCH ON BLOCKCHAIN SOLUTIONS FOR MICRO-CREDENTIALING SYSTEMS

Oldřich Faldík[1], Pavel Turčínek[1]

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

ABSTRACT

The rapid advancements in blockchain technology and cryptocurrencies have catalysed a growing demand for professionals equipped to navigate this transformative domain. Mendel University's Blockchain and Cryptocurrencies course addresses this need by integrating theoretical foundations with hands-on project-based learning. The curriculum delves into blockchain architecture, consensus mechanisms, smart contracts, decentralized applications, and economic and regulatory implications. Students engage with diverse blockchain platforms, including Hyperledger Fabric, BigchainDB, Avalanche, Corda, and Polygon Mumbai, to develop real-world solutions for micro-credentialing systems.

The comparative analysis of these platforms reveals distinct trade-offs in scalability, security, privacy, and functionality, offering insights into selecting optimal technologies for specific use cases. Through interdisciplinary projects, students gain practical experience, foster innovation, and prepare for strategic roles in the blockchain industry. This approach highlights the critical interplay between theory and application, equipping students to tackle complex challenges and contribute to blockchain innovation across diverse sectors.

Keywords: blockchain, digitalization, micro-credentials

JEL Code: L8, O3

1 INTRODUCTION

The rapid evolution of blockchain technology and cryptocurrencies has fundamentally transformed industries, driving a demand for professionals equipped with the knowledge and skills to navigate this disruptive landscape. In response to this need, Mendel University in Brno offers a comprehensive course titled Blockchain and Cryptocurrencies. This course combines theoretical insights with practical training to provide students with a deep understanding of blockchain's decentralized systems, the cryptographic principles underpinning cryptocurrencies, and their broader economic, social, and regulatory implications.

https://doi.org/10.11118/978-80-7701-047-4-0060

The curriculum is designed to address the multifaceted nature of blockchain and cryptocurrencies. It begins by exploring the foundational concepts of blockchain as a distributed ledger, including its consensus mechanisms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS), as detailed in Nakamoto's seminal work on Bitcoin (Nakamoto, 2008). Students gain a solid grounding in the mechanics of cryptocurrencies, smart contracts, and decentralized applications (dApps), enabling them to analyze the technical and strategic elements of these innovations. Additionally, the course delves into the economic implications of blockchain, such as its potential to disrupt traditional financial systems and enable decentralized finance (DeFi) (Gudgeon *et al.*, 2020).

A distinctive feature of the course is the emphasis on interdisciplinary learning, equipping students to tackle the broad applicability of blockchain technology across industries. From supply chain transparency (Kshetri, 2018) to healthcare data security (Azaria *et al.*, 2016) and energy trading (Kouhizadeh *et al.*, 2019), blockchain's potential applications are vast. This breadth is reflected in the course content, which encourages students to adopt a systems-oriented approach to addressing complex challenges. Regulatory and ethical considerations are also emphasized, fostering critical thinking about issues such as privacy, governance, and sustainability in blockchain systems.

An essential component of the course is its focus on experiential learning through student-led projects. These projects provide students with hands-on experience in applying blockchain concepts to real-world problems. Guided by teachers, students design and implement blockchain-based solutions.

These projects not only deepen technical competencies but also encourage creative problem solving. For instance, students might create smart contracts for Micro-credentials platform or energy trading platform. Through these endeavours, students engage with cutting-edge platforms such as Ethereum, Hyperledger, and Solana, preparing them for industry roles that require both strategic insight and technical expertise.

The student projects also foster collaboration, as students often work in teams to tackle interdisciplinary challenges (Merbret *et al.*, 2020). Such initiatives encourage peer learning and develop skills in project management, communication, and teamwork. Furthermore, by presenting their projects to peers and industry professionals, students receive valuable feedback, bridging the gap between academia and practice. The impact of such project-based learning aligns with the findings of Anwar *et al.* (2020), who emphasize that real-world applications enhance student engagement and learning outcomes in blockchain education.

2 METHODOLOGY AND DATA

Blockchain technology was selected for a decentralized approach of issuing certificates, with emphasis on speed, energy efficiency and security. Proof of Authority algorithm was preferred for its speed, proven reliability and wide use in private blockchains. 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. The system was designed to support not only certificate issuance but also revocation and renewal, as some certificates are valid only for a limited period. Furthermore, the network had to provide authorized institutions or businesses with access to read and verify valid micro-credentials stored on the blockchain. These requirements were presented to the students as a project assignment. The students formed groups of 3–5 members. Each team chose one of the possible blockchain technologies. They then implemented a certificate management tool using selected technology. Each team then presented and defended their solution.

The research question addressed by the project was whether blockchain technology, specifically various consensus mechanisms, can be effectively used to design a decentralized system for micro-credential management that supports secure issuance, verification, revocation, and renewal. The scientific contribution includes a practical exploration of this approach, insights into implementation challenges, and analysis of legal implications such as the right to be forgotten. Student teams were assessed based on the functionality, security, and usability of their implemented solutions, as well as the clarity of their documentation and final presentations. Evaluation criteria included adherence to project requirements, successful use of blockchain features, and demonstration of certificate management capabilities.

3 RESULTS

3.1 Hyperledger Fabric

Stable development and feature rich. Security features, endorsement policies, handling private data using private collections, generation of user certificates. (Androukali *et al.*, 2018)

Linking chain of certificate changes using composite keys. Chaincode written in Golang, but many possible like Java or TypeScript. Chaincode needs to be approved by peers before deployment.

Advantages:

- Supports private data channels and encrypted sharing of information between specific network participants (e.g., personal identification number can be protected).
- Ability to define complex rules for managing certificates through smart contracts.
- Flexible access control, allowing only authorized institutions to read data.
- Good support for certificate revocation and expiration handling through modifiable smart contracts.
- Strong focus on security and performance.

Disadvantages:

- Higher complexity in configuration and implementation.
- Requires robust infrastructure for network operation.

3.2 BigchainDB

This project implements a decentralized certificate management system built on BigchainDB (McConaghy *et al.*, 2016), a blockchain database that combines the key characteristics of blockchain (decentralization, immutability, and owner-controlled assets) with the advantages of traditional databases (high transaction rate, low latency, and indexing capabilities). The system utilizes a network of four nodes running on Docker containers, each consisting of BigchainDB Server, MongoDB, and Tendermint for consensus.

The implementation leverages FastAPI for the backend REST API and React with Chakra UI for the frontend interface. The system provides comprehensive certificate lifecycle management functionality, including creation, verification, renewal, and revocation of certificates. A notable security feature is the encryption of sensitive personal data (identifiers) using Fernet symmetric encryption, where only the issuing node can decrypt the information. The architecture supports multiple nodes working in a network, with each node maintaining its own cryptographic key pair and the ability to verify certificates issued by other nodes. The system also implements immutable audit trails through blockchain transaction history and provides ledger visualization capabilities, making it suitable for scenarios requiring transparent, tamperproof certificate management such as academic credentials, professional certifications, or digital identity documents.

Advantages:
- High transaction speed.
- Simple data storage and access.

Disadvantages:
- Limited support for smart contracts, making functions like certificate revocation and renewal difficult to implement.
- Insufficient access control and protection for sensitive data.
- Unsuitable for solutions requiring high levels of security and decentralization.

3.3 Avalanche blockchain

The system leverages Avalanche's high-performance (Amores-Sesar *et al.*, 2024), low-latency infrastructure consisting of three chains: **X-Chain:** Handles asset management, **P-Chain:** Handles validator coordination, **C-Chain:** Handles smart contract execution (primary chain).

Advantages:
- High transaction speed and low costs.
- Support for smart contracts, enabling implementation of certificate revocation and renewal.
- Option to create custom subnets with access control and privacy rules.

Disadvantages:
- Sensitive data require encryption and additional protections, increasing complexity.
- Requires knowledge of the Ethereum Virtual Machine (EVM) for smart contract development.

3.4 Corda

Corda (Brown *et al.*, 2016) is a distributed ledger platform designed specifically for enterprise use in the financial sector. Here is an overview of the key concepts that underpin Corda:

States: States represent the current position or status of a ledger and are continuously updated. Each state is an object with a specific value and is uniquely identifiable within the network.

Transactions: Transactions in Corda are proposals to change one or more states. A transaction must be verified and approved by all relevant parties before it can be included in the ledger. Transactions ensure that state changes are valid according to the rules defined in contracts.

Contracts: Contracts in Corda are programs that contain the rules according to which transactions must be executed. Each transaction must comply with the rules defined in the contracts that are relevant to the states changed by the transaction.

Flows: Flows are procedures that enable nodes in the network to coordinate necessary actions to achieve successful execution of a transaction. These flows may include message exchanges, obtaining signatures from consenting parties, and verifying transactions.

Notary: The notary is a special node in the Corda network that prevents double-spending by ensuring that each state can only be used in one transaction at a time. The notary does not judge the content of transactions but verifies their uniqueness and chronological order.

Consortium and private networks: Corda allows the creation of private networks among organizations with similar business interests. These networks can have their own rules and agreements that regulate their interactions.

Compatible privacy: In Corda, transaction data is shared only between parties directly involved in the transaction. This approach ensures that data is kept private and reduces the amount of unnecessary data each node must process.

Advantages:

- Transactions are shared only among involved parties, naturally protecting sensitive information (e.g., social security numbers).
- Support for complex business logic, including certificate revocation and renewal.
- Emphasis on interoperability and integration with existing systems.

Disadvantages:

- Limited decentralization (not a fully decentralized blockchain).
- More complex implementation for less experienced teams.

3.5 Polygon Mumbai

The project utilizes the Polygon Mumbai (Rana *et al.*, 2022) network for efficient and cost-effective blockchain interactions, a Python-based FastAPI backend for seamless communication with the blockchain, and integration with tools like Brownie and Alchemy for contract deployment and testing. This system addresses challenges related to certificate fraud and lifecycle management while showcasing the potential of blockchain technology in sensitive data protection and decentralized governance.

Advantages

- Support for smart contracts through the Ethereum Virtual Machine (EVM).
- Low operational costs and fast transactions.
- Easy implementation of encryption and other safeguards for sensitive data.

Disadvantages

- The public nature of the network makes protecting sensitive data challenging without additional measures.
- As a test network, it is not meant for production, requiring migration to the main network (Polygon Mainnet).

4 DISCUSSION AND CONCLUSIONS

The comparison of Hyperledger Fabric, BigchainDB, Avalanche blockchain, Corda, and Polygon Mumbai for issuing micro-credentials highlights the diverse capabilities and trade-offs inherent in blockchain platforms. Each platform offers unique advantages, reflecting its architectural design, consensus mechanisms, scalability, security, and integration potential, making it suitable for different micro-credentialing use cases.

From an educational perspective, these platforms underscore the multifaceted nature of blockchain technology, reflecting the interdisciplinary focus of the Blockchain and Cryptocurrencies course at Mendel University. By engaging with these cutting-edge platforms, students not only gain technical expertise but also develop a strategic understanding of how blockchain systems can be tailored to solve real-world problems, such as in the domain of credentialing. This aligns with the course's goal of bridging theory and practice, preparing students for innovative roles in the blockchain industry.

In conclusion, the exploration of these platforms for micro-credential issuance demonstrates the importance of selecting the right blockchain based on specific requirements, such as security, scalability, cost, and ecosystem compatibility. These findings enrich the curriculum and provide students with actionable insights into the practical applications of blockchain, fostering a generation of professionals ready to drive blockchain innovation across industries.

REFERENCES

AMORES-SESAR, I., CACHIN, C., SCHNEIDER, P. 2024. An Analysis of Avalanche Consensus. arXiv preprint. *arXiv*:2401.02811. ISSN: 2331-8422. https://arxiv.org/abs/2401.02811

ANDROULAKI, E., BARGE, P., BORTNIKOV, V., MURTHY, C., CACHIN, C., CHANDRA, T., CHAUBEY, P., GETH, K., HENDRICKS, S., LAVENTMAN, G., MANEVICH, Y., YELLICK, J., SETHI, M., SHERER, T., SMITH, A., SORENSEN, B., STATHAKOPOULOS, M., VUKOLIC, M., WAGNER, D. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In: *Proceedings of the Thirteenth EuroSys Conference*. Article 30- ISSN: 0163-5999. https://doi.org/10.1145/3190508.3190538

ANWAR, S., AZIZ, S., KHAN, M. A. 2020. Project-Based Learning in Blockchain Education: Improving Student Engagement and Technical Skills. *Journal of Emerging Technologies in Computing Systems*. 16(3), 57-65. ISSN: 1550-4832

AZARIA, A., EKBLAW, A., VIEIRA, T., LIPPMAN, A. 2016. MedRec: Using Blockchain for Medical Data Access and Permission Management. In: *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, pp. 25-30, ISSN: 2472-6988. https://doi.org/10.1109/OBD.2016.11

BROWN, R. G., CARLYLE, J., GRIGG, I., HEARN, M. 2016. Corda: An Introduction. arXiv preprint *arXiv*:1605.05834. ISSN: 2331-8422. https://arxiv.org/abs/1605.05834

GUDGEON, L., WERNER, S., PEREZ, D., KNOTTENBELT, W. 2020. DeFi Protocols: Risks, Collateral, and the Case for Governance. In: *Proceedings of the International Conference on Decentralized Applications and Infrastructures*. New York: Association for Computing Machinery, pp. 92–112.

KOUHIZADEH, M., SARKIS, J., ZHU, Q. 2019. At the Nexus of Blockchain Technology, the Circular Economy, and Product Deletion. *International Journal of Production Research*. 57(7), 2083-2091. ISSN: 0020-7543. https://doi.org/10.1080/00207543.2018.1542176

KSHETRI, N. 2018. Blockchain's Roles in Meeting Key Supply Chain Management Objectives. *International Journal of Information Management*. 39, 80-89. ISSN: 0268-4012. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

MCCONAGHY, T., MARQUES, R., MÜLLER, A., DE JONGHE, D., MCCONAGHY, T. T., MCMULLEN, G., HENDERSON, R., BELLEMARE, S., GRANZOTTO, A. 2016. BigchainDB: A Scalable Blockchain Database. arXiv preprint, *arXiv*:1605.04984. ISSN: 2331-8422. https://arxiv.org/abs/1605.04984

MERBRET, C., THORP, R., DEVOS, K. 2020. Collaborative Blockchain-Based Learning Environments: Enhancing Engagement and Knowledge Sharing. *Education Technology Research and Development*. 68(4), 987–1002. ISSN: 1042-1629.

NAKAMOTO, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.

RANA, S. K., RANA, A. K., RANA, S. K., SHARMA, V., LILHORE, U. K., KHALAF, O. I., GALLETTA, A. 2022. Decentralized Model to Protect Digital Evidence via Smart Contracts using Layer 2 Polygon Blockchain. *IEEE Access*. 10, 1-12. ISSN: 2169-3536. https://doi.org/10.1109/ACCESS.2023.3302771

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.

Contact information

Oldřich Faldík: e-mail: oldrich.faldik@mendelu.cz
Pavel Turčínek: e-mail: pavel.turcinek@mendelu.cz