A Lightweight Permissioned Distributed Ledger for Credentialing in Higher Education Institutions

Nemanja Zdravković[1], Nikola Dimitrijević[1], Dušan Simjanović[1], and Vijayakumar Ponnusamy[2]

[1] *Belgrade Metropolitan University, Tadeuša Košćuška 63, Belgrade, Serbia*
[2] *SRM Institute for Science and Technology, SRM Nagar, Kattankulathur - 603 203 Chengalpattu District, Tamil Nadu, India*

Abstract

Blockchain and similar distributed ledger technologies are often referred as the next disruptor in Information-Communication Technologies. The security properties blockchain technologies offer have surpassed the initial use-cases in cryptocurrencies, and a variety of blockchain-based solutions are appearing daily in healthcare, financial technology, supply chain management, and education. In this paper, we examine a permissioned blockchain, i.e., a distributed ledger solution for students' credentialing during their studies at a Higher Education Institution. Utilizing the Hyperledger platform, which allowed us to use a lightweight consensus mechanism, we aim to incorporate the model within an existing faculty- or university-level information system. With the innate properties of immutability and transparency, the presented model provides authorized users with a secure proof of student credentials which can be verified at any time.

Keywords

blockchain, distributed ledger, e-learning, student credentialing

1. Introduction

Even before the recent COVID-19 pandemic, online education portals such as edX, Coursera, and Udacity were getting a large influx of new learners, and Massive Online Open Courses (MOOCs) have gained a notable significance in the contemporary educational scenario [1]. Learning portals can be focused for professionals, such as LinkedIn Learning, or for a wider audience with various levels of prior knowledge, such as Skill Share and Udemy. These portals meant for learners often with no previous background required, cannot compete in quality compared to an accredited online curriculum offered by a Higher Education Institutions (HEIs). These policies are also mirrored in pricing options – some portals offer free courses or course snippets with paid certification after course completion, while others offer different subscription levels. However, most often these types of learning portals charge per course. Alongside MOOCs, a growing number of HEIs are offering their new and current students the option of online enrollment, or offer blended learning as a combination of face-to-face and online studies [2, 3]. In addition, HEIs may offer complete or truncated versions of their curriculum on other portals, delivering an equal or similar education content in terms of quality [4, 5].

The aim of this paper is to present a system for credentialing the certificates gained from HEIs and similar learning platforms by applying blockchain technology (BCT). Blockchains are append-only ledgers to which data can be added but changed or removed only in extraordinary circumstances. This feature guarantees the integrity of the data. BCT addresses interoperability issues by creating an

Proceedings 13th International Conference on eLearning (eLearning-2022), September 29–30, 2022, Belgrade, Serbia
EMAIL: nemanja.zdravkovic@metropolitan.ac.rs (A. 1); nikola.dimitrijevic@metropolitan.ac.rs (A. 2); dusan.simjanovic@metropolitan.ac.rs (A. 3); vijayakp@srmist.edu.in (A. 4)
ORCID: 0000-0002-2631-6308 (A. 1); 0000-0002-6595-9277 (A. 2); 0000-0002-1709-0765 (A. 3); 0000-0002-3929-8495 (A. 4)


overarching mechanism to link disparate personal records, such as badges and certificates from various learning platforms.

The rest of the paper is organized as follows. Section 2 presents our motivation behind applying blockchain to HEI credentialing. Section 3 gives a brief overview of blockchain fundamentals, followed by the proposed system model, where we use the lightweight Hyperledger distributed ledger. Finally, in Section 4, we draw conclusions, highlighting the areas for future research and platform development.

2. Motivation

Blockchain is often referred as one of the next disruptive technology [6]. The security properties that these classes of technologies offer, especially transparency, immutability and innate use of public key cryptography, made blockchain surpass the initial and most widely known use-case in cryptocurrencies and financial tech [7, 8]. Indeed, today exists a plethora of blockchain-based solutions in areas such as education, supply chain management, healthcare, and the public sector. [9 – 13] In addition, a very large number of start-ups in blockchain development and blockchain-as-a-service (BaaS) are emerging, while in the scientific community, journal special issues and conference tracks on blockchain may be found more and more.

However, regarding blockchain-based solutions for education, especially in credentialing, there exist only a relatively small number of papers published compared to other blockchain-based applications [14 – 16]. The authors of [14] state that their BCTs platform promises permanent authentication as well as storage for the so-called credentials market, that is made up of various kinds of micro-credentials. These micro-credentials include nanodegrees, MOOCs, and certificates and/or badges from various types of training programs. Their platform gives users direct control and, more importantly, management over their credentials. They highlight potential issues such as scalability, especially when the blockchain uses the computationally complex consensus mechanism proof-of-work (PoW), the same mechanism as Bitcoin. Paper [15] points out that blockchain-based solutions in education allow learners and as well as teaching staff to automatically verify the validity of certificates directly, without the contacting the organization that originally issued those credentials. This approach aims to remove the need for educational organizations to constantly validate credentials. The authors of [16] give an abstract model for secure credential in e-Learning to both HEI and MOOC platforms. In this paper, we mostly build upon the concepts found in [16], expanding to a more lightweight model, applying private blockchain technologies such as Hyperledger, and the use of lightweight cryptography often accompanied with Internet of Things (IoT) applications.

3. Lightweight blockchain-based system for credentialing

In this Section, we firstly give a brief overview of BCTs, highlighting the use of private BTCs for our model. Afterwards, we present the proposed model, expanding our previous model in [16]. Our new model is more focused on building a network of known peers, allowing the use of a more lightweight, but still secure credentialing network. Finally, we present two use-cases for the transactions in the network.

3.1. Blockchain fundamentals

Blockchain technologies impose a significant paradigm shift in the methods of data processing, especially when dealing with personal data. A blockchain network can be viewed as a data structure, which is shared among nodes comprising the network. The data structure is append-only, and all events, which are termed transactions, are stored in linked blocks [17]. Each transaction, besides the data itself, contains a unique cryptographic signature, ID and timestamp and a hash value of the previous block, which makes the blocks in the chain resistant to alterations. All blocks therefore form a chain, and can trace back to the first block, called the genesis block. As the blockchain is a distributed network, and all nodes in the network are updated with the current version of the blockchain in real time. A blockchain

relies on distributed peer-to-peer networking, public-key cryptography algorithms, and distributed consensus, which is the mechanism allowing new blocks to be added to the blockchain.

The combination of these three core concepts is what secures the blockchain and its transactions. In a centralized system, there exists a single entity which is able to control the process of adding a block to the chain; however, in blockchain, each block is managed by all nodes, which share the same level of permissions. Table 1 highlights the benefits of implementing a blockchain-based solution over a traditional centralized solution [18]. With decentralization, security issues can be resolved through the process known as distributed consensus. This process establishes a formal agreement between the participating nodes in the blockchain to validate a data block before it can be added to the chain. Depending on the consensus algorithm, nodes can e.g. compete among themselves for correct transaction validation, or be chosen to validate randomly. These algorithms can vary in complexity and power consumption.

Table 1
Comparison between using a traditional centralized platform and a blockchain platform [18]

Aspects	Centralized platform	Blockchain-based platform
Data Handling	Supports create, read, update, and delete operations.	Only read and write options are available
Authority	Controlled by the administrator	Decentralized even in private blockchains
Integrity	Data can be altered	Data are immutable and auditable
Privacy	High chances of malicious cyberattacks	Data are stored using cryptography technology
Transparency	Databases are not transparent	Data are stored in a distributed network
Quality Assurance	Administrators are needed to authenticate data	Data can be tracked and traced to the origin.
Fault tolerance	High risk of single point of failure	Distributed ledger is highly fault-tolerant.
Cost	Easy to implement and maintain.	Uncertainty in the operating and maintenance costs.
Performance	Fast, with great scalability	Slow; scalability is a challenge.

It is important to note that blockchains are a group of technology; the term refers to different forms of distributed databases with variations in their technical and governance arrangements and complexity. Custom-made, private blockchains developed for a specific purpose are often referred to as distributed ledger technologies (DLTs).

As far as the author's knowledge, implementing BCT in education is still a novel topic, and in existing literature, there exist different approaches as to which data should, and more importantly, which data should not be kept on the DLT [19 – 23].

3.2. System model

In this paper, we present an improved model for credentialing from [16], which is primarily aimed at a network of HEIs, such as different Faculties which belong to the same university, or for different Universities. We identify three main parts of our model, as shown in Figure 1. The first part is the authorized user, who can access the DTL using an online platform that connects to the DTL network. The user may or may not be a student from the HEI that he/she is requesting a certification validation; however, the user must be authorized. An individual node is the faculty or university which issues the Diploma/Certificate of their students. The third and most important part is the DLT network running

Hyperledger, which can be accessed by the user, and by the node as well. Whereas in [16] the network can run independently of the platform, here we empathize that all nodes that the network is comprised of are known, i.e. we are using private blockchains or DLTs. By having known nodes, the model has significant improvements. Firstly, all nodes are therefore by default trusted parties. Secondly, by making the network private, a node cannot be added easily; usually, adding a node to a private network requires an invitation. Finally, private DLTs such as Hyperledger allow the use of lightweight consensus mechanisms, making block addition less computationally complex and hence less power consuming.

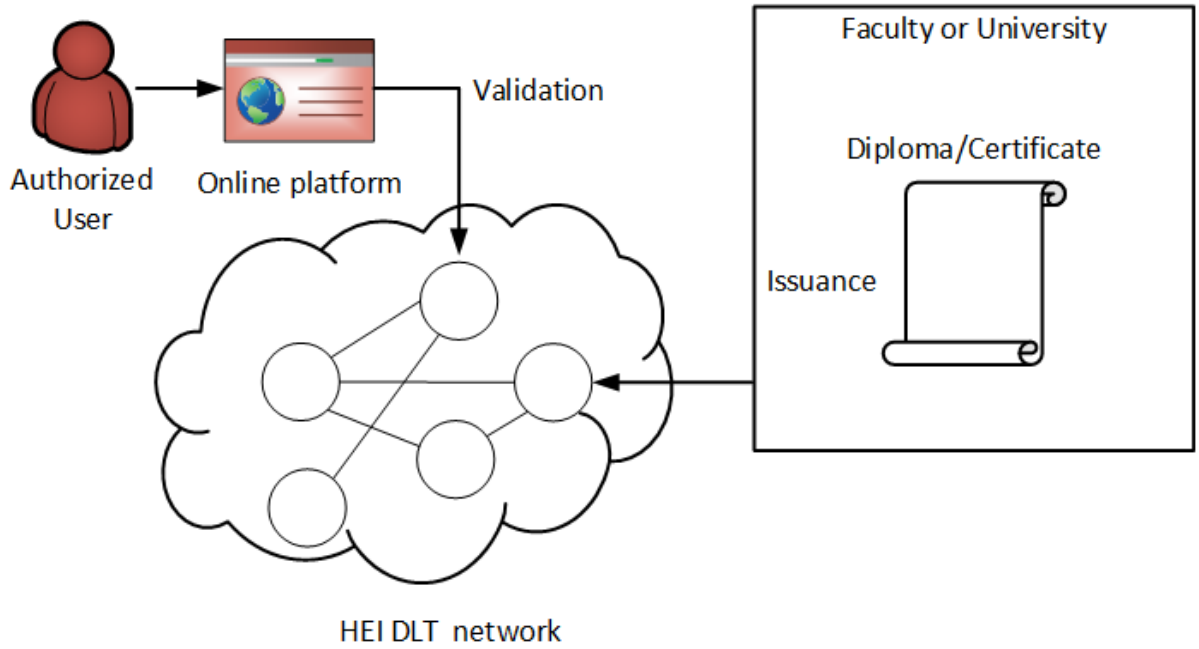

Figure 1: DLT-based credentialing model.

3.3. Network transactions

Two network transaction exist in our model – certificate issuance and validation. Every node in the network should firstly be able to issue a digital document representing a diploma and/or certificate. When a student of the HEI which as a part of the network is awarded the document, a DLT issuance transaction is triggered. It is assumed that the HEI will have its information system (IS) which keeps all documents as well, and it is the IS itself which is connected to the DLT network through an Application programming interface (API). This transaction will contain the same information as would the digital document itself, alongside the metadata required for the transaction header. Furthermore, each issuance transaction can be a single block, as there is no high frequency of issuing these types of documents and therefore no need for a so-called transaction pool. This information will be encrypted, and can be accessed only by the HEI, the student which the document belongs, and an authorized third party upon explicit request. Other nodes in the network will verify it and add it to the blockchain using a lightweight consensus mechanism. Platforms such as Hyperledger Fabric Lightweight or Hyperledger Minifabric can be used for the validation process, or an altogether new mechanism, such as Proof-of-Block-and-Trade (PoBT), primarily suggested for IoT applications [24].

The other type of transaction is certificate validation. This type of transaction can be triggered by a node of the network as well, or through a proxy, an authorized user. Upon requesting access for validation, the authorized user is given an access link, from which the user can verify the document by

accessing the DTL through a web application. For example, let say a potential employed wants to verity a digital document that the student has provided for a job application. Rather than contacting the HEI that issued the document, the potential employer will be given with a verification link. Upon registering, this user can access the DTL network for document validation only through the issuing HEI.

When the certificate file is uploaded, its metadata and hashed values are indexed and compared to previously validated entries in the blockchain. This represents the validation transaction, triggered from the HEI providing the verification link. If a match is found on the blockchain, the certificate file is validated and a corresponding message appears on the web interface. If not, a negative message appears instead. The sequential diagram for both transactions is shown in Figure 2.

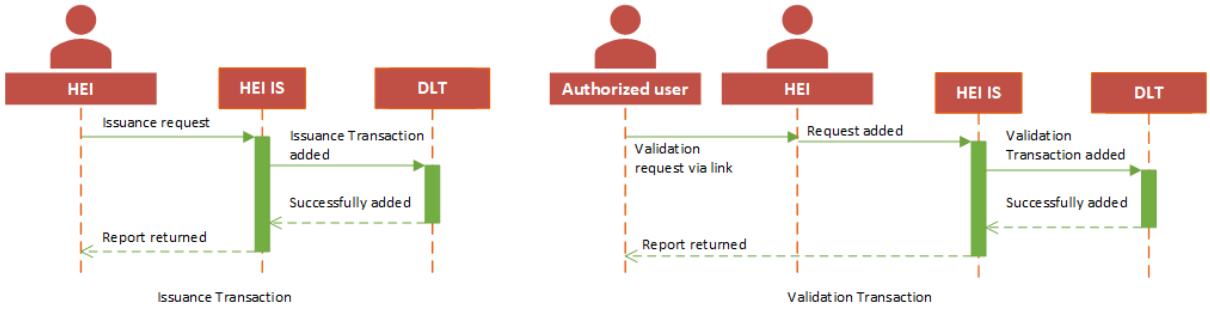

Figure 2: Sequential diagrams for both types of transactions.

The innate security properties of of DLTs, as a subset of BCTs, especially the immutability property, makes modified or fraudulent digital documents practically impossible to pass verification. Any tampering to the digital document file will result in a vastly different hashed value of the file, hence only valid documents can be correctly verified.

4. Conclusion

Using private blockchain, i.e. DLTs, sensitive data such as digital certificates from HEIs can be issued and verified reliably, without the need for complex computational power and electrical power consumption. Blockchain and distributed ledgers can aid HEIs such as Faculties and Universities by adding an additional layer to their credentialing process, with little maintenance cost but with added security. In this paper, we have presented a DLT-based system for issuance and validation that can be easily deployable and connected to a HEI's IS. With this layer, issuance and validation could become a seamless process as there are only two types of transactions that need to be implements in the network. Adding blockchain-based solutions to HEIs such as the one presented in this paper therefore presents a step towards more secure studying, from the perspective of the student, and from the education institution as well.

This model has its limitations. Namely, it is required that a HEI has an IS which can be expanded by adding the DLT layer. As of writing this paper, the model has not yet been developed; however, future work includes developing a standalone prototype paired with a mock HEI IS for testing, and later for implementation on a live system.

Acknowledgements

This paper was supported in part by the Blockchain Technology Laboratory at Belgrade Metropolitan University, Belgrade, Serbia, and in part by the Ministry of Education, Science and Technological Development, Republic of Serbia (Project III44006).

5. References

[1] S. K. Ch and S. Popuri, Impact of online education: A study on online learning platforms and edX, in: Proc. IEEE MITE, (2013): 366-370.

[2] K. L. Smart and J. J. Cappel, Students' Perceptions of Online Learning: A Comparative Study, Journal of Information Technology Education: Research, vol. 5, no. 1, (2006): 201-219.

[3] J. Davis, Traditional vs. Online learning: It's not an either/or proposition, Employment Relations Today, vol. 27, no. 1, (2000): 47-60.

[4] L. Yuan, S. J. Powell, and B. Olivier. “Beyond MOOCs: Sustainable online learning in institutions, Cetis whitepaper, 2014.
[5] D. Jansen, J. Rosewell K. Kear, Quality Frameworks for MOOCs, in: Open Education: from OERs to MOOCs, M. Jemni K. M. Kinshuk, Eds., Springer, 2017.
[6] J. Mattila, The blockchain phenomenon–the disruptive potential of distributed consensus architectures, ETLA working papers, no. 38, 2016.
[7] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009.
[8] S. Underwood, Blockchain beyond bitcoin, Commun. ACM, vol. 59, no. 11, (2016): 15–17.
[9] M. Mettler, Blockchain technology in healthcare: The revolution starts here, Healthcom, (2016): 1-3.
[10] V. Grković, J. Jović, N. Zdravković, M. Trajanović, D. Domazet, and V. Ponnusamy, Usage of Blockchain Technology for Sensitive Data Protection – Medical Records Use Case, in: Proc. ICIST 2020, (2020): 216 – 221.
[11] C. W. Cai, Disruption of financial intermediation by FinTech: a review on crowdfunding and blockchain, Accounting & Finance, vol. 58, no. 4, (2018): 965-992.
[12] S. Saberi, M. Kouhizadeh, J. Sarkis and L. Shen, Blockchain technology and its relationships to sustainable supply chain management, International Journal of Production Research, vol. 57, no. 7, (2019) 2117-2135.
[13] G. Chen, B. Xu, M. Lu, and N. S. Chen, Exploring blockchain technology and its potential applications for education, Smart Learning Environments, vol. 5, no. 1, (2018): 1.
[14] M. Jirgensons, and J. Kapenieks, Blockchain and the future of digital learning credential assessment and management, Journal of Teacher Education for Sustainability, vol. 20, no.1, (2018): 145-156.
[15] A. Grech, and A. F. Camilleri. Blockchain in education, A. Inamorato dos Santos, Ed, EUR 28778, European Union, 2017.
[16] N. Zdravković, J. Jović, M. Damnjanović, Secure Credentialing in e-Learning using Blockchain, in: Proc. of the 11th International Conference on e-Learning, pp. (2020): 39-43.
[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: Proc. IEEE BigData congress, (2017): 557-564.
[18] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, MEDREC: Using blockchain for medical data access and permission management, in: Proc. of the 2nd International IEEE OBD Conference, (2016): 25–30.
[19] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, EduCTX: A Blockchain-Based Higher Education Credit Platform, IEEE Access, vol. 6, (2018): 5112-5127.
[20] S. Kolvenbach, R. Ruland, W. Gräther, and W. Prinz, Blockchain 4 education, in: Proc. of 16th European Conference on Computer-Supported Cooperative WorkPanels, Posters and Demos, 2018.
[21] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres, and F. Wendland, Blockchain for education: lifelong learning passport, in: Proc. of 1st ERCIM Blockchain Workshop, 2018.
[22] H. Sun, X. Wang, and X. Wang, Application of blockchain technology in online education, International Journal of Emerging Technologies in Learning, vol. 13, no. 10, pp. (2018): 252-259.
[23] A. Kamišalić, M. Turkanović, S. Mrdović, and M. Heričko, A preliminary review of blockchain-based solutions in higher education, in: Proc. International workshop on learning technology for education in cloud, (2019) 114-124.
[24] S. Biswas, K. Sharif, F. L., S. Maharjan, S. P. Mohanty, and Y. Wang, PoBT: A lightweight consensus algorithm for scalable IoT business blockchain. IEEE Internet of Things Journal 7, no. 3 (2019): 2343-2355.