Secure Course Completion Credentialing Using Hyperledger Fabric

Stefan Gogić[1], Nemanja Zdravković[1,*], Emilija Kisić[1] and Ponnusamy Vijayakumar[2]

[1]Faculty of Information Technology, Belgrade Metropolitan University, Tadeuša Košćuška 63, 11000 Belgrade, Serbia
[2]SRM IST, ECE Department, Kattankulathur, Chennai, India

Abstract

In this paper, we present a blokchain solution, based on Hyperledger Fabric, for issuing and validating documents from Higher Education Institutions (HEIs), such as diplomas and diploma supplements. By utilizing Hyperledger Fabric, the most popular distributed ledger technology for private blockchains, we propose a lightweight and secure credentialing three layer blockchain system – the smart contract layer, the blockchain layer itself, and the network layer. With a minimal needed number of functionalities such as issuance and verification, our lightweight system can be deployed on a trustful environment, e. g. faculties from the same university, or a consortium of universities. With such an environment, we eliminate the need for a computationally complex consensus mechanism for adding blocks to the ledger, while retaining easy implementation with the HEIs information system and/or learning management system. Based on previous research and prototyping, our model acts as an additional security layer on top of and HEI's information system and utilizes blockchain's immutable property to keep student's records secure.

Keywords

blockchain, credentialing, distributed ledger, Hyperledger

1. Introduction

Blockchain technologies (BCTs) and distributed ledger technologies (DLTs) have surpassed their initial use in cryprocurrencies, and are already being used in a plethora of fields – from supply chain managements and healthcare, to predictive maintenance systems and public sector [1, 2, 3, 4, 5]. With the rise of Ethereum and its smart contracts written in Solidity, presenting code which can be directly run on the chain itself, paired with a robust consensus mechanism, a secure and immutable record keeping solution in a trustless environment without the need of third-party stakeholder has risen, identifying BCTs/DLTs as disruptive technologies [6].

Credentialing solutions for Higher Education Institutions (HEIs) based on blockchain and similar technologies are still few. As of writing this paper, only a small number of papers have been published [7, 8, 9] compared to other blockchain-based use cases. For instance, one of the main conclusions found in one of the earliest studies on the topic of blockchain in education state that BCTs (and later DLTs) should allow users to be able to automatically verify the validity of certificates in a direct manner, without contacting the HEI that originally issued the documents [7]. Indeed, the authors of [8] state that BCT/DLT-based systems promise a permanent authentication and storage solution for the alternative credentials market. This continuously growing market consists of various kinds of microcredentials, nanodegrees, MOOCs/SPOCs, certificates and/or badges from various types of training and pre-qualification programs. The authors also emphasize scalability issues, most noticeably if the BCT/DLT use the computationally complex Proof-of-Work (PoW) consensus mechanism, as does Bitcoin and many other cryptocurrency networks. The PoW approach will likely remove the need for educational organizations to validate credentials, and other lightweight approaches are needed.

Since the initial hype of using BCT/DLT for various use cases including ones in education, the authors of [9] conducted a literature review of solutions based on public blockchains, highlighting the need for a standardized approach built on a public blockchain to promote faster adoption and acceptance. This recent study states that full functioning and active prototypes are still low in numbers; however, one of the conclusions was that the blockchain application should run on a stable, secure, and trustworthy network.

Indeed, in a trustless environment where actors are not known, public BCTs with robust consensus mechanisms such as Biction are imperative [10, 11, 12]. However, mechanisms such as PoW or various variations of Proof of Stake (PoS) are computationally complex and require powerful, often dedicated computers equipped with a

BISEC'23: 14th International Conference on Business Information Security, November 24, 2023, Niš, Serbia

*Corresponding author.
stefan.gogic.6354@metropolitan.ac.rs (S. Gogić); nemanja.zdravkovic@metropolitan.ac.rs (N. Zdravković); emilija.kisic@metropolitan.ac.rs (E. Kisić); vijayakp@srmist.edu.in (P. Vijayakumar)
0000-0002-2631-6308 (N. Zdravković); 0000-0003-3059-2353 (E. Kisić); 0000-0002-3929-8495 (P. Vijayakumar)

powerful central processing unit (CPU) and/or graphic processing unit (GPU). Conversely, in a more specific environment, i. e. where the nodes in the blockchain network are known (and trusted) parties, a blockchain-based solution with less complex consensus mechanism can be implemented, retaining security with the added benefit of not needing a powerful CPU/GPU to handle blockchain transactions. Usually, this approach is called a distributed ledger technology (DLT).

The authors' main motivation is to utilize a trustful environment and propose a lightweight framework for document credentialing, tailored specifically to HEIs and the issuance and validation of student diplomas and diploma supplements.

Based on literature, commercially (un)available solutions and our own previous attempts, we have identified the following research questions:

- *RQ1*: Is it possible to design a lightweight framework for the specific needs of HEIs to incorporate document issuance and validation in a secure manner, without relying on complex solutions?
- *RQ2*: Can the flexibility of Hyperledger Fabric be used as a basis for incorporating a BCT/DLT-based addition to an existing HEI information system (IS)?

The rest of the paper is organized as follows. Section 2 gives a brief introduction on blockchain technolgies, focusing on Hyperledger Fabric. Afterwards, Section 3 gives presented the proposed system, developed at Belgrade Metropolitan University's (BMU's) Blockchain Technology Laboratory. Finally, Section 4 gives a conclusion, with current limitations and further research ideas.

2. Blockchain and Hyperledger overview

In this Section, we firstly provide a briew overview of the building blocks of a general blockchain system. Afterwards, we focus on the Hyperledger DLT solution, of which Hyperledger Fabric is used to develop the credentialing system.

2.1. Brief blockchain overview

In general, BCTs impose a fundamental change to manner various types of data are processed, and can improve existing data security solutions. A blockchain can be viewed as a shared, append-only distributed ledger, in which all events are stored in linked blocks [13]. These events are often referred as transactions. A copy of the ledger is therefore kept by all nodes which form the blockchain network. Due to the fact that all member nodes have a copy of the ledger, all network nodes are updated in real time, simultaneously. Furher, a block can be viewed as a data structure consisting of the follwing:

1. a header which connects the new block to the previous one.
2. a list of transactions;

Each transaction, besides the data, contains a header with a timestamp, paired with an unique cryptographic signature, thus enablig the ledger to be resistant to modifications. This chain of blocks that is formed and continuously updated can be traced back all the way to the first block, named the genesis block.

The combination of peer-to-peer networking, public-key cryptography, and distributed consensus is what secures blockchain transactions. Conversely to a centralized system, no single entity i.e. node should be able to control the process of adding a block to the chain. As the blockchain is a distributed system, each new block addition is managed by all nodes who share equal rights. This mechanism is utilized in order to overcome security issues, and is achieved through the process known as distributed consensus. This process can be viewed as an agreement among the nodes in the network how to validate each block yet to be added to the chain. Depending on the consensus mechanism, nodes can either compete for correct transaction validation (PoW), be chosen randomly (PoS and its variations), or apply a different algorithm altogether. The algorithms used can vary in computational complexity.

Finally, it is important to note that blockahins are a class of technology; the term refers to different forms of distributed databases with variations in their technical and governance arrangements and complexity.

2.2. Hyperledger and its use cases

Hyperledger is the leading open source community focused on developing various stable frameworks, tools and libraries for enterprise-grade distributed ledger deployments [14]. This community aims to advance BCT/DLT technologies by identifying and more importantly realizing a cross-industry open standard platform for DLTs. The aim of the open standard is to transform the approach to business transactions on a global level [14]. Hyperledger has a modular approach to hosting projects similar to the approach of the Linux Foundation, as shown in Fig. 1. All Hyperledger projects are open source, they are easy to obtain [15]. All Hyperledger projects, with the exception of Hyperledger Indy, are used for general purpose blockchain-based applications and solutions, whereas Hyperledger Indy focuses on decentralized identity [16].

One of the key differences between the various BCTs/DLTs systems is the utilized consensus mechanism. Due

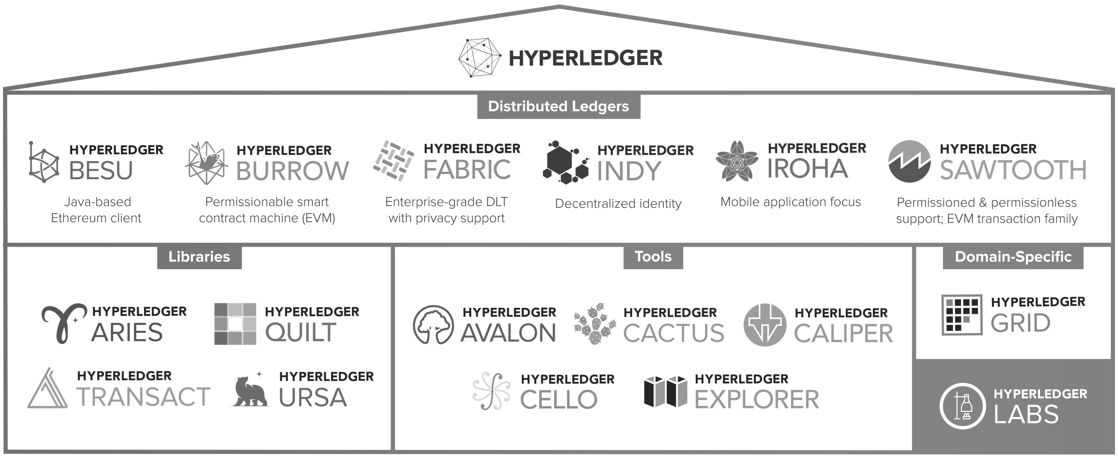


Figure 1: The Hyperledger Project umbrella [15].

to the variety of blockchain usage requirements, Hyperledger provides several different consensus mechanisms [17]. For instance, Fabric uses the Apache Kafka platform [18] as the main Crash Fault Tolerance (CFT) protocol on the network which is permissioned i.e. private, and it is voting-based. Hyperledger Indy utilized a consensus based on Redundant Byzantine Fault Tolerance (RBFT), a protocol inspired by Plenum Byzantine Fault Tolerance (Plenum). Hyperledger Iroha used a variant of the BFT algorithm called Sumeragi, which tolerates more than one Byzantine faulty network nodes. Hyperledger Sawtooth facilitates the so-called pluggable consensus for both lottery and voting algorithms. By default, Hyperledger Sawtooth uses a lottery-based, Nakamoto consensus algorithm called Proof of elapsed time (PoET). Hyperledger Burrow comes with Byzantine Fault-Tolerant Tendermint protocol with a greater transaction rate, whereas Buru implements various consensus algorithms that are involved in transaction validation, block validation, and block production, i.e. mining in the PoW mechanism, while Hyperledger Sawtooth has the most support for smart contract languages [16].

The core Hyperledger-based use cases include banking, healthcare, supply chain management, financial services, information technology, government, and media and entertainment. Indeed, the Hyperledger Foundation promotes a range of business DLTs, including many libraries and tools that provide support for the creation, maintenance, deployment, providing cryptographic work, etc [15].

For the proposed system, the authors have opted to use Hyperledger Fabric, as it is the Hyperledger project with most testing, working real-world applications community, and documentation. The details of Hyperledger Fabric are listed in Table 1.

Table 1
Hyperledger Fabric features

Advantages	Enterprise backing Relative maturity Private channels Modular architecture Smart contracts
Consensus mechanism	Kafka RAFT Solo
Smart contract technology	Chaincode
Smart contract type	Installed
Smart contract language	Go Java Javascript Solidity
State storage	CoudhBD leveldb

3. System model

BMU's ongoing internal R&D includes implementing blockchain in education and e-learning. BMU's Blockchain Technology Laboratory (BCT Lab) is investigating which blockchain technology is most suitable for applying in education, with emphasis on data protection. BMU's BCT Lab is collaborating with ISUM (Information System of University Metropolitan) and BMU's e-Learning center. During a four month testing developing and period, a working prototype for credentialing was developed. The proposed model is comprised of three layers, stacked on top of the zeroth layer, which is the HEI's IS:

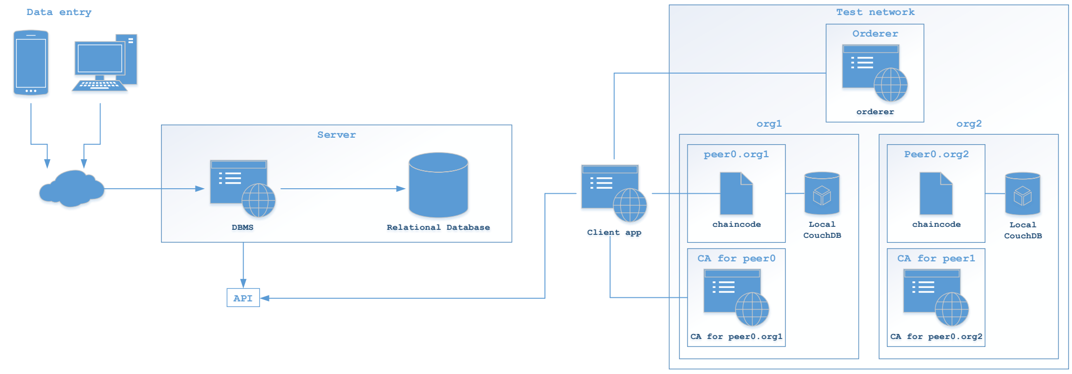


Figure 2: Proposed system consisting of a data entry system and the test blockchain network, communicating over an API.

1. the smart contract layer;
2. the blockchain layer itself;
3. the network layer.

The smart contract layer runs the chaincode to add the data to a block. It is present on every node, denoted as a peer. The blockchain layer consists of the peer itself, a Certification Authority (CA) for that peer, and a local NoSQL database - CouchDB. The network layer consists of the test network with two peers, denoted with `org1` and `org2`.

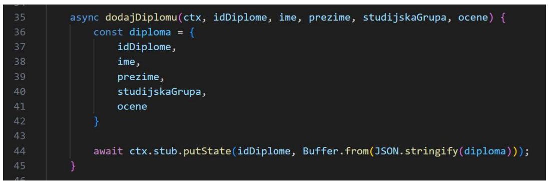
The system was developed in two stages – Stage 1 consists of using an isolated GIT branch of the HEIs to add a functionality to export diploma supplemental materials as an API to the blockchain network. Stage 2 comprised of developing a lightweight blockchain application, based on Hyperledger Fabric, to connect the the API and add the data to a block. The architecture of the two-stage system is shown in Fig. 2.

The main parameter which Hyperledger Fabric uses is the transaction context `ctx`. It holds the needed information for transaction logic "per transaction" or "per contract". IT enables to access the `stub` which allows various blockchain operations such as state returns, adding a new item to the block, or getting all blocks (in our case diploma supplements).

To add a diploma supplement, it is needed to connect toe the peer node using a gateway, and to get the chaincode from the network.

To write the transaction i.e. diploma object, an asynchronous `promise` function will get all the necessary parameters for add a new diploma supplement, as shown in Fig. 3. It will create a new object with those parameters which will be later added to teh blockchain using `stub` API operations.

The data which is added to the blockchain has the following structure:



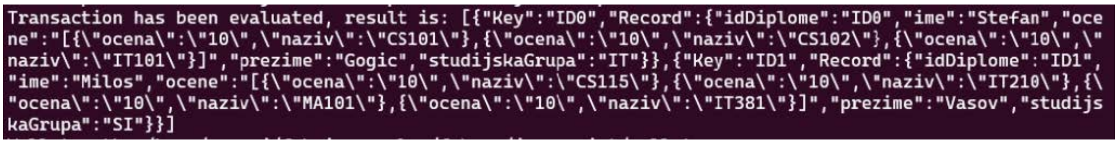
```
    async dodajDiplomu(ctx, idDiplome, ime, prezime, studijskaGrupa, ocene) {
        const diploma = {
            idDiplome,
            ime,
            prezime,
            studijskaGrupa,
            ocene
        }

        await ctx.stub.putState(idDiplome, Buffer.from(JSON.stringify(diploma)));
    }
```

Figure 3: Asynchronous `promise` function.

```
const diplomas =
[
    {
      "name": "Firstname",
      "surname": "Surname",
      "studygroup": "StudyGroup",
      "grades":
          [
              {
                  "grade": "GradeValue",
                  "course": "CourseCode",
              },
              ...
          ]
    }
 ...
]
```

When data is added, a message can be viewed in the console terminal to confirm a successful transaction, as shown in Fig. 4. In our testbed, and endpoint was not deployed from the IS's side; therefore we have manually added the data in the same format as the HEI's IS would provide.



```
Transaction has been evaluated, result is: [{"Key":"ID0","Record":{"idDiplome":"ID0","ime":"Stefan","oce
ne":"[{\"ocena\":\"10\",\"naziv\":\"CS101\"},{\"ocena\":\"10\",\"naziv\":\"CS102\"},{\"ocena\":\"10\",\"
naziv\":\"IT101\"}]","prezime":"Gogic","studijskaGrupa":"IT"}},{"Key":"ID1","Record":{"idDiplome":"ID1",
"ime":"Milos","ocene":"[{\"ocena\":\"10\",\"naziv\":\"CS115\"},{\"ocena\":\"10\",\"naziv\":\"IT210\"},{\
"ocena\":\"10\",\"naziv\":\"MA101\"},{\"ocena\":\"10\",\"naziv\":\"IT381\"}]","prezime":"Vasov","studijs
kaGrupa":"SI"}}]
```

Figure 4: Transaction successfully added.

4. Conclusion

In this paper, we have used Hyperledger Fabric to develop a lightweight blockchain network for credentialing HEI's diplomas and diploma supplements. Currently, our system only addresses the issuance use-case, while validation use-case remains open. As prototyping was conducted in an isolated environment, several open issues still remain. Firstly, should the blockchain remain private, or be public (where anyone can be a part of the network)? As the target group of the system are first and foremost HEIs, the authors, as was discussed in other literature as well, opt for a private blockchain solution, where the HEIs comprise the network. Still, there exists a possibility to add the learners as nodes as well.

Using Hyperledger Fabric, data such as diplomas and supplements can be issued and verified reliably. Blockchain can help learning platforms to add an additional layer to their credentialing process. We have presented a blockchain-based credentialing system can be easily deployable and connected to a learning platform. Within our proposed system, upon generating the certificate file for the diploma and/or supplement, the HEI's IS will make a transaction to the blockchain. This entry will also have the certificate information, alongside metadata required for the transaction header. This information will be encrypted, and can be accessed only by the IS, the student, and an authorized third party.

This new issuance transaction is sent to the blockchain, where the other nodes in the network will verify it and add it to the blockchain using a simpler consensus mechanism. Each node will have a local copy of the blockchain on a NoSQL database like CouchDB. For certificate validation, upon receiving the access link, the student or an authorized third party can verify the digital credential by accessing the blockchain through a query. If a match is found on the blockchain, the certificate file is validated and a corresponding message appears.

The innate immutability property of BCT/DLT does not allow fraudulent or modified certificate files to be deemed as verified. Any tampering to the certificate file will result in a vastly different hashed value of the file, ensuring impossible verification.

Acknowledgment

This paper was supported by the Blockchain Technology Laboratory at Belgrade Metropolitan University, Belgrade, Serbia.

References

[1] B. K. Mohanta, S. S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in: 2018 9th international conference on computing, communication and networking technologies (ICCCNT), IEEE, 2018, pp. 1–4.

[2] K. Zīle, R. Strazdiņa, Blockchain use cases and their feasibility, Applied Computer Systems 23 (2018) 12–20.

[3] P. Zhang, D. C. Schmidt, J. White, G. Lenz, Blockchain technology use cases in healthcare, in: Advances in computers, volume 111, Elsevier, 2018, pp. 1–41.

[4] M. Alabadi, A. Habbal, Next-generation predictive maintenance: leveraging blockchain and dynamic deep learning in a domain-independent system, PeerJ Computer Science 9 (2023) e1712.

[5] V. Milicevic, N. Zdravkovic, J. Jovic, On the selection of suitable blockchain technologies for supply chain management, International Journal for Quality Research (2023).

[6] N. Zdravković, J. Jović, M. Damnjanović, Secure credentialing in e-learning using blockchain, in: Proceedings of the 11th Conference on eLearning (eLearning-2020), 2020, pp. 39–42.

[7] A. Grech, A. F. Camilleri, Blockchain in education, Luxembourg: Publications Office of the European Union, 2017.

[8] M. Jirgensons, J. Kapenieks, Blockchain and the future of digital learning credential assessment and management, Journal of teacher education for sustainability 20 (2018) 145–156.

[9] G. Caldarelli, J. Ellul, Trusted academic transcripts on the blockchain: A systematic literature review, Applied Sciences 11 (2021) 1842.

[10] P. Ocheja, B. Flanagan, H. Ueda, H. Ogata, Managing lifelong learning records through blockchain, Research and Practice in Technology Enhanced Learning 14 (2019) 1–19.

[11] F. R. Vidal, F. Gouveia, C. Soares, Revocation mechanisms for academic certificates stored on a blockchain, in: 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), IEEE, 2020, pp. 1–6.

[12] F. Vidal, F. Gouveia, C. Soares, Analysis of blockchain technology for higher education, in: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, 2019, pp. 28–33.

[13] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends, in: 2017 IEEE international congress on big data (BigData congress), IEEE, 2017, pp. 557–564.

[14] C. Cachin, et al., Architecture of the hyperledger blockchain fabric, in: Workshop on distributed cryptocurrencies and consensus ledgers, volume 310, Chicago, IL, 2016.

[15] The Hyperledger Foundation, https://www.hyperledger.org, 2023.

[16] V. Milićević, J. Jović, N. Zdravković, An overview of hyperledger blockchain technologies and their uses, in: Proceedings of the 11th International Conference on Information Society and Technology (ICIST 2021), 2021, pp. 62–65.

[17] J. Moubarak, E. Filiol, M. Chamoun, Comparative analysis of blockchain technologies and tor network: Two faces of the same reality?, in: 2017 1st Cyber Security in Networking Conference (CSNet), IEEE, 2017, pp. 1–9.

[18] B. R. Hiraman, et al., A study of apache kafka in big data stream processing, in: 2018 International Conference on Information, Communication, Engineering and Technology (ICICET), IEEE, 2018, pp. 1–3.