International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:14, No:9, 2020

Leveraging Hyperledger Iroha for the Issuance and Verification of Higher-Education Certificates

Vasiliki Vlachou, Christos Kontzinos, Ourania Markaki, Panagiotis Kokkinakos, Vagelis Karakolis, John Psarras

***Abstract*—**Higher Education is resisting the pull of technology, especially as this concerns the issuance and verification of degrees and certificates. It is widely known that education certificates are largely produced in paper form making them vulnerable to damage while holders of such certificates are dependent on the universities and other issuing organisations. QualiChain is an EU Horizon 2020 (H2020) research project aiming to transform and revolutionise the domain of public education and its ties with the job market by leveraging blockchain, analytics and decision support to develop a platform for the verification and sharing of education certificates. Blockchain plays an integral part in the QualiChain solution in providing a trustworthy environment to store, share and manage such accreditations. Under the context of this paper, three prominent blockchain platforms (Ethereum, Hyperledger Fabric, Hyperledger Iroha) were considered as a means of experimentation for creating a system with the basic functionalities that will be needed for trustworthy degree verification. The methodology and respective system developed and presented in this paper used Hyperledger Iroha and proved that this specific platform can be used to easily develop decentralize applications. Future papers will attempt to further experiment with other blockchain platforms and assess which has the best potential.

***Keywords*—**Blockchain, degree verification, higher education certificates, Hyperledger Iroha.

I. Introduction

WHILE digitization nowadays has impacted many facets of professional development, the same cannot be said for higher education, the main mission of which is to prepare students and aspiring job seekers to enter the workforce. The main challenge currently faced by higher education pertains to the effective training of future job seekers, a training that must be dynamic and consider advances in technology and the job market to accordingly shape a higher education curriculum [1]. In addition, such training can stem from many sources, both formal (e.g., university courses, degrees, official seminars etc.) and informal (e.g., open courses, personal research, and reading etc.) [2], which means that students end up having an educational portfolio of fragmented information and qualifications, most of which cannot be verified, leading to great uncertainty from the side of employers regarding the actual skill level of any given student or prospective job seeker [1]. Moreover, even formal sources of training, such as a university degree, are still largely published on paper form [1], [3], making it harder to validate them and contrast them with real knowledge, especially given the significant rise of degree fraud [4]. All the above lead to the conclusion that management in higher education and certification of education documents require revolutionary new tools [1] and approaches.

Now, most higher education institutions keep student data in proprietary formats, with access to them being granted only to select IT professionals within the school for safety and privacy reasons. Students are usually granted some form of external access to their data without the ability and tools to analyse them, manage them and effectively share them with external parties. This fact can create significant challenges for students who wish to continue their studies in another institution or prove their qualifications to a prospective employer, since such proofs are usually published in paper form, making them prone to damage and loss while at the same time keeping the student dependent on the university administration for the publishing and validation of an education document or degree [5]. It is considered that a solution to these challenges could be the establishment of digital certificates from universities and other education institutions as the new norm, since they can be easier to manage, store and share with interested parties. There are several vital points with regards to this new paradigm, including standardization of data, storage location, and most importantly the safety of a student's personal data, the latter being also enforced in the EU by the General Data Protection Regulation (GDPR).

While the aforementioned challenges are hard to tackle, the rise of innovative technologies that could provide novel solutions and positively impact the way that educational documents are managed, stored and shared must be considered. One such technology is blockchain, also known as distributed ledger technology. Blockchain is a decentralised technology, which refers to the processes of data verification, storage, maintenance, and transmission, which follow a distributed approach. Trust between the nodes of a blockchain is achieved via consensus algorithms that verify transactions and perform changes in the network only upon receiving the agreement of the network's majority, instead of centralised organisations, which is the case in traditional databases [4]. In a higher education setting, this means that a blockchain system empowers the users (i.e., the students), by allowing them to keep a decentralised copy of their data that they can manage and share as they like. Data safety in the system is ensured via cryptographic algorithms within the system that ensure no data tampering, as any attempt to change even a small bit of

Vasiliki Vlachou, Christos Kontzinos, Ourania Markaki, Panagiotis Kokkinakos, Vagelis Karakolis, and John Psarras are with the Decision Support Systems Lab of the National Technical University of Athens, Athens, Greece (e-mail: svlachou@epu.ntua.gr, ckon@epu.ntua.gr, omarkaki@epu.ntua.gr, pkokkinakos@epu.ntua.gr, vkarakolis@epu.ntua.gr, john@epu.ntua.gr).

information requires system consensus which is achieved in various ways depending on the respective blockchain platform. A blockchain-powered system in higher education can enhance reliability (no single point of failure), efficiency (all data are automatically run through set procedures called smart contracts), security, and trust (trust is achieved by the entire system and not a centralised entity).

At this point, it should be mentioned that this paper is written under the context of the EU research project, QualiChain that aims to leverage blockchain to develop a distributed platform that will allow students to manage and share their academic and employment qualifications in a decentralised manner while also providing the means for the trustworthy verification of such credentials. QualiChain will also experiment with smart badge endorsements to award students with verifiable micro-accreditations to enhance everyday student life. To showcase and validate the impact of the platform, QualiChain includes in its consortium a number of universities that will pilot the platform to assess its capability in verifying degrees in a decentralised and trustworthy manner. However, in developing such a system, the first aspect that needs to be considered is the specific blockchain framework (e.g., Ethereum, Hyperledger etc.) that will be employed to develop the solution. Different frameworks provide different capabilities and as such need to be in turn assessed to select the most suitable one to develop an effective education blockchain. This paper is the first in a series of experiments that aim to assess the various blockchain frameworks, select the most suitable ones and in turn use them to develop initial versions of a blockchain that is responsible for the management and sharing of university degrees and other qualifications. Specifically, under the context of this paper the Hyperledger Iroha framework was analysed and used to develop a blockchain system.

Section I introduces the scope of the present paper by presenting the current situation in Higher Education and explaining how blockchain can lead to more effective and secure solutions. Section II presents approaches and platforms found in the research bibliography relevant to blockchain in education and discusses the impact of the GDPR in the development of such approaches. Section III discusses the platform and approach that was used for the solution developed. Section IV describes the system that was developed and the usage scenarios in which it can be implemented and finally, Section V concludes the document and presents the next steps of the current research work.

II. Background

A. Blockchain Approaches in Education

While blockchain is a relatively new technology, mainly implemented in the field of cryptocurrencies, its inherent properties can be applied in multiple other domains as well. There is a growing interest among the research community for the development of blockchain systems for higher education, aiming to provide an alternative and secure solution for student data management and degree verification. Lizcano and Lara [1] proposed a blockchain model that allows higher education institutions to modify their curricula based on the professional profiles of their students that are validated by prospective employers, also advocating a decentralised model of confidence for transactions based on an academic cryptocurrency. In addition, the MIT Media Lab [6] produced Blockcerts, that stored digital certificates of qualifications in a blockchain after the latter had been validated by a respective authority or institution. The proposed digital certification model had great institutional support and acceptance, to the extent that other Universities have now adopted it. The Edublock of the Institute for the Future (IFTF) [7] is a platform that provides students with a kind of digital currency to quantify teaching hours as transactions and be able to store them in Blockchain. In this case, the approach is the opposite of Blockcerts', since what is stored is not qualifications, but hours spent in face-to-face or remote classes. Meanwhile, the Edgecoin project [8] seeks to establish a specific Cryptocurrency, based on Bitcoin, to regulate the market of goods and services related to the educational field, such as enrolments in online courses, micro-contracts between training institutions, and digital transactions of economic assets for the acquisition of books, support services or regulated studies. Rooksby and Dimitrov [9] have implemented a blockchain system based on Ethereum for use by a university to store student grades and to provide a cryptocurrency. Finally, concerning the EU, the UK Open University project Openblockchain [10] aims to promote blockchain-based digital portfolios as a new paradigm for storing verified academic and employment qualifications in the form of smart badges that can be shared seamlessly, thus improving mobility in higher education and the labour market. In addition, the European Commission (EC) launched in 2018 the EU Blockchain Observatory and Forum [11], [12] with the objective to promote blockchain research in Europe and organise current national and European blockchain initiatives to create an ecosystem of research, knowledge and technical components. The EU Blockchain Observatory led to the development of a European blockchain partnership, consisting of 22 member-states [13] with the explicit purpose to coordinate current efforts and promote wider-scale blockchain applications that can be implemented in a pan-European scale.

B. Impact of GDPR in Blockchain Solutions

The General Data Protection Regulation (EU) 2016/679 (GDPR) is an EU regulation, established in 2016 for the protection of EU citizens regarding the processing of their personal data [14]. The GDPR appoints both obligations and higher requirements on the service providers that are responsible for the management and processing of personal data in order to return control of those data to their owners. The GDPR provides data owners with certain basic rights concerning their data, such as the right to deny processing of data and the right to data deletion, among others. However, the right to data deletion is opposite to blockchain's fundamental principle of immutability, i.e., once a piece of data is stored inside the blockchain, it can never be deleted. As such, the

research community is trying to figure out new approaches to implement blockchain as this concerns the storing and managing of personal data. Most solutions follow the Privacy by Design approach, which considers all security mechanisms right from the beginning of implementation ensuring that the developed product or application follows all legal and ethical requirements regarding data privacy [15]. However, the main way, in which developers of blockchain systems are trying to comply with the GDPR is by using the blockchain ledger for storing of the transaction hash while keeping any personal and transaction data off chain. In such a system, the transaction hash stored inside the blockchain contains (cryptographically) information about the location of the transaction data. Owners of the data can provide access to them by sharing with other users of the system their private or public key (depending on the case) that can be used to decipher the location of the data. This approach is being followed by various researchers in the development of GDPR-compliant blockchain solutions, not only in the field of education but in any domain in which blockchain is required to work with personal data [16]-[18]. The solution developed under the context of this paper also follows this approach, as the blockchain is mainly used for verifying transactions and cryptographically storing information about the off-chain location of the actual data. If users of the system require their data to be deleted from it, then the off-chain copy is deleted and all that is left in the blockchain is a cryptographic signature that points to a null location.

III. Methodology

This section aims to provide a deep understanding of not only the framework used for the development of the blockchain-based application, but also the blockchain's architecture and security model. The certificate issuance and verification workflows are also presented.

A. Current Blockchain Frameworks

This section includes a comparative analysis of three blockchain frameworks that were considered for the development of a university blockchain solution, namely Ethereum, Hyperledger Fabric and Hyperledger Iroha. Ethereum [19] is a blockchain platform that lets anyone create and use decentralized applications that are based on blockchain technology. Ethereum is neither controlled nor owned by any central authority - it is an open-source project built and maintained by many people around the world. Unlike other protocols, Ethereum was designed to be adaptable and flexible. New applications can be easily implemented on the Ethereum platform, and it is safe for anyone to use them. Hyperledger Fabric [20], [21] is a permissioned distributed ledger technology platform, designed mainly for use in enterprise contexts. Hyperledger Fabric is an open-source project established under the Linux Foundation. A diverse set of developers and scientists from multiple organizations contribute to the continuous improvement and maintenance of the platform. The architecture of Fabric is highly modular and configurable, enabling innovation and versatility, so that the platform can adjust to the needs of each use case. Hyperledger Iroha [22] is a platform that can be used for the development of trusted, secure and fast blockchain-based applications. It is an open-source project that includes a variety of mobile and desktop libraries, which contain predefined commands and queries. Hyperledger Iroha can introduce great advantages to applications that indicatively (yet not exhaustively) concern the issuance of certificates and the management of digital assets. Table I summarises and compares the key features of the aforementioned frameworks.

TABLE I
Comparative Analysis of Ethereum, Hyperledger Fabric and Hyperledger Iroha

	Ethereum	Hyperledger Fabric	Hyperledger Iroha
Smart contracts	✔	✔	—
Predefined commands & queries	—	—	✔
Network	Permission-less	Permissioned	Permissioned
Consensus algorithm	Proof of Work (PoW) / Proof of Stake (PoS)	Network starters can choose a consensus mechanism that best fits the needs of each use case	Yet Another Consensus (YAC)
Native currency	Ether	No, but it can be developed with smart contracts	No, but it can be created using assets
Programming languages	Programming languages modelled on existing languages	General-purpose programming languages, e.g., Java and Go	Java, Javascript, Python and Swift
Permissions	Through smart contracts	Channels and Private Data	Permissions and Roles
Use cases	Mainly applications that automate direct interaction between peers or facilitate coordinated group action across a network, e.g., the coordination of peer-to-peer marketplaces and the automation of complex financial contracts	Enterprise applications, e.g., finance and supply chain logistics	Mainly applications concerning digital data management, e.g., medical and educational certificates and transfer of assets

All frameworks can be used for the implementation of an application concerning the issuance and verification of educational certificates. However, this paper examines the use of Hyperledger Iroha for the following reasons:

1) It can be effectively used mainly for digital data management
2) It is possible to give access to the network only to authorized educational institutions, students and employers, since Iroha has a robust permission system
3) Students can grant potential employers' access to their certificates through predefined commands
4) It is the easiest one to set up in a real-life scenario.

B. Blockchain Block

This section describes the structure of the transactions and the blockchain blocks. For the proposed blockchain to comply

with the GDPR, certificates will be stored outside of the blockchain, e.g., in institution's private servers, clouds, and peer-to-peer networks. It will be up to the institutions and the students to decide not only where to cryptographically store the certificates, but also who will have access to them. The hashes of the certificates will be stored on the blockchain. Thus, anyone with access to a certificate will be able to verify its authenticity and immutability by leveraging the blockchain.

The block and transaction structure will conform to the Hyperledger Iroha blockchain structure [22]. The security and storage of transaction information will be ensured by using Merkle Trees.

Each block contains the following:

- Block's hash
- Block's payload, which includes:
  - Height of block
  - Timestamp (unix time in milliseconds) of creation
  - Hash of the previous block to create the chain of blocks
  - Array of transactions that have been successfully committed to the ledger
  - Signatures of peers that voted for the block during the consensus round.

Each transaction contains the following:

- Hash of transaction
- Transaction's Payload, which stores the following:
  - Time (unix time in milliseconds) of creation
  - Commands included in the transaction. The hash of a certificate can be found in the commands section of the respective transaction.
  - Account ID of transaction creator
  - Quorum field, which indicates the required number of signatures
  - Transaction's signatures that include the ed25519 public key and the signature.

C. System Security

1) Hash Functions

This section discusses how hash functions can be used for the verification of certificates issued through the application. Given a certificate, a user should be able to determine, in a trustworthy manner, when it was published, by whom, and whether or not it has been tampered since its issuance. The verification of the authenticity and immutability of the certificates will be implemented via use of hashes stored on the blockchain. Blockchain architecture guarantees the immutability of the data stored in the blockchain. Thus, the blockchain-backed certificate hashes provide an integrity guarantee for the off-chain certificates.

Some of the most well-known and widely used hash functions include SHA-1, SHA-256, SHA-3, and MD5. SHA-256 hash function will be used for the computation of the certificate hashes and is currently being used in blockchains that require hash functions of great security, such as the Bitcoin blockchain. SHA-256 is more secure than MD5 and SHA-1, while it has higher performance than the SHA-3 functions [23]. SHA-256 produces a 32-bytes long hash, which can be stored both on the description field of a transfer transaction and on the details of an Iroha account.

2) Key Management

This section examines the application's key management implementation. The main idea of Public-key Cryptography [24] or Asymmetric Cryptography is that both the sender and the recipient of a message own a different pair of public-private keys instead of sharing a secret key, as in the case of Symmetric Key Cryptography. Blockchain's security model is based on Public-key Cryptography. Both users' identities and transaction identifiers are created and authenticated using public key certificates. Therefore, secure encryption key management needs to be implemented to ensure the security of the system. The key management must follow the instructions of the Hyperledger Iroha platform, since the solution developed under the context of this publication concerns the development of a blockchain-backed issuance and verification model based on this framework.

First, the default key pairs used for the installation of Iroha need to be replaced by new pairs of keys generated in a secure way. The private key should be known only to its owner, who is responsible for its maintenance and recovery, and thus, it should be stored locally, e.g., on the owner's digital wallet of choice. On the other hand, the public key may be disseminated widely. Hence, besides being locally stored, it may also be stored on a server to be accessible to other users and nodes of the network.

3) Authentication & Authorisation

This section includes a short comparison of permissioned and permissionless blockchains and presents the advantages of permissioned blockchain networks as far as this paper's blockchain solution is concerned.

A permissionless blockchain allows everyone to become part of the network and contribute to its maintenance by validating transactions and creating new blocks. Permissioned blockchains act as closed ecosystems, where permission is required to join the network and perform certain actions. Each blockchain network has its own set of advantages and disadvantages and thus, its benefits can be better leveraged for the implementation of certain use cases.

Hyperledger Iroha is a permissioned blockchain system. Therefore, the network of the developed application will also be permissioned. This provides an additional level of security, since only authorized educational institutions will be able to issue a certificate using the implemented blockchain. As a result, the creation of virtual educational institutions for the issuance of fake certificates will be impossible.

4) Consensus Algorithms

This section includes an analysis of three consensus algorithms that were considered for the blockchain-backed application, namely Proof of Work, Proof of Stake and Yet Another Consensus. Consensus algorithms in blockchain systems guarantee that all non-faulty peers of the network perform the same state machine updates in the same order and thus, reach a common agreement about the current state of the distributed ledger.

Proof of Work (PoW) [25] involves solving a complex computational problem that is very difficult to solve, yet trivial to verify the answer to. PoW, as used by Satoshi Nakamoto in Bitcoin blockchain [26], involves computing a value that when hashed with a given hash function, results in the hash beginning with a predefined number of zero bits. However, the proposed method is too resource-intensive (expensive specialized hardware, electricity) to be practical for many applications. PoW is also vulnerable to 51% attack by a group of miners that control more than 50% of the network's computing power, while its probabilistic nature causes a lack of transaction finality. Proof of Stake (PoS) is an ecological alternative to the PoW consensus mechanism. In this algorithm, the probability to create a new block and receive the reward is commensurate with a user's stake in the system. However, since this mechanism gives the decision-making power to users who hold stake in the system, PoS is vulnerable to attack by users who hold more than 50% of a network's cryptocurrency and thus, new kinds of centralization risks are introduced. Yet Another Consensus (YAC) [27] is a practical decentralized byzantine fault-tolerant consensus algorithm that solves the problems of inefficient message passing and of the existence of strong leaders. In a blockchain that concerns the issuance and validation of educational certificates, the system should be independent from strong leaders. As shown by [27] this mechanism achieves low latency, high transaction throughput, and great scalability, while it requires the supermajority (> 2/3) of peer votes to create a new block. This algorithm is used to provide Byzantine fault tolerant consensus to the Hyperledger Iroha platform and hence, is the one used in the solution proposed.

D. Degree Issuance & Verification Workflow

This section presents the procedure that needs to be followed for the issuance and validation of an educational certificate.

In order to issue an educational certificate through blockchain, the institution needs to sign the hash of the content of the digital certificate using its private key and append that signature to the certificate, which is then passed to the application. Next, the SHA-256 digest of the final certificate is computed. This hash can be used to verify that the certificate has not been altered since issuance. Finally, the institution stores the hash within a blockchain transaction.

The verification of a certificate requires the holder of the certificate to disclose both the certificate itself and the location of its hash on the blockchain. The validator needs to compute the SHA-256 hash of the certificate and compare it with the hash stored on the blockchain. The validator can also confirm that a given certificate was indeed issued by the named university by decrypting the signature using the institution's public key and comparing the decrypted signature with the hash of the rest of the certificate content.

IV. System Implementation

At this point, both the framework that will be used for the development of the university blockchain solution and the blockchain's architecture and security model have been discussed in detail. This section concerns the implementation and simulation of the blockchain-backed application. In order to install and configure Hyperledger Iroha, the instructions of the Iroha documentation need to be followed [22]. The configuration of the Iroha network requires to clone and modify, according to the needs of each application, the Iroha repository [28].

A. Application Functionality

This application will assist stakeholders to perform tasks related to the issuance and validation of certificates. More specifically:

- Educational institutions will be able to issue academic certificates whose authenticity can be verified through the blockchain.
- Students will be able to grant to prospective employers access to certificates' blockchain-backed integrity guarantee.
- Employers will be able to verify certificates' authenticity and immutability.

For the application to be fully functional, additional functionality has been developed. For instance, each user will be able to manage their account and get information about their past transactions, while employers will also be able to verify that a given certificate was indeed issued by the named university. Moreover, the administrators of the application will be responsible for the proper operation of the system by indicatively, yet not exhaustively, creating new accounts and assets. However, the additional functionality will not be further discussed, since this paper aims at evaluating the system as far as the main functionality is concerned.

B. Application Implementation

1) Core Concepts

This section discusses how some of the core concepts of Hyperledger Iroha [22] are leveraged for the implementation of the solution.

According to the system's functionality, each user account can represent a university, a student, an employer, or an administrator.

In Hyperledger Iroha, educational certificates can be represented by assets. Different types of certificates will correspond to different assets named after the respective certificate, e.g., bachelor and master.

Hyperledger Iroha uses a role-based access control system to limit the actions of users. For a user to be able to perform a specific set of commands, they need to have already been granted permission to do so. For instance, an institution cannot issue a certificate unless they have permission to transfer assets and set the details of the respective student account. Most permissions cannot be granted to an account directly; hence, each user will be granted roles that hold the set of necessary permissions.

Domains allow the grouping of accounts and assets. Four domains will be created for the representation of the account groups. Another domain will be used for the certificates to be

registered as assets.

2) Genesis Block

This section describes the genesis block of the blockchain-backed application. Genesis block implements the core concepts presented in the previous sub-section. More specifically, the Iroha repository [28] is modified for the genesis block to create:

- the default roles of each user group.
- the domains "uni", "stud"," empl", "bc" and "cert" that respectively concern educational institutions, students, employers, administrators, and certificates.
- assets for the representation of bachelors, masters, and Ph.Ds. since these are the main certificates issued by educational institutions. However, both the administrators and the universities will be able to create new assets if necessary.
- an administrator account.
- network peers, namely nodes that participate in the consensus process.

3) Functionality

This section presents the most important actions that can be performed by the stakeholders. The issuance and verification of certificates rely on the ability to transfer assets, set the details of another account (in order to inform them about the issuance transaction hash), and search transactions by their hash. Both students and employers can grant other accounts the permission to set their details, so that they can receive the hash of the transaction concerning the issuance of a specific certificate. They can also revoke from other accounts the permission to set their account details upon the receipt of the hash.

Educational institutions will be able to issue new certificates and give students access to their integrity guarantee. To do so, the institution needs to:

- transfer one asset corresponding to the type of the certificate to the student. This asset indicates that the student has completed their studies.
- add the URI and the hash of the certificate to the student account details. The certificate's URI is stored in the account details to facilitate the demonstration of the platform. In the real-time scenario, the URI will not be stored on the blockchain. Both the holder of each certificate and the respective educational institution will be responsible for the certificate's storage. However, information about the off-chain location of the actual certificates could be cryptographically stored on the blockchain. Thus, the prospective employers will not be able to find out the location of a certificate through the blockchain without having the necessary information (e.g., a key) to do so.
- add the hash of the certificate's issuance transaction, that is the transaction that includes the two aforementioned actions, to the student account details.

All these actions are executed by only one function.

Every user will be able to get the details of their account set by another user. As a result, the students and the employers will be able to get the transaction hash set by universities and students respectively.

Students will be able to give prospective employers the necessary information so that they can verify the authenticity of a certificate. More specifically, through the related to this functionality command, the following actions are executed:

- the student adds the hash of the certificate's issuance transaction, initiated by the respective educational institution, to the prospective employer's account details.
- the student retrieves information about the certificate, e.g., its hash and URI.

Students, universities, and employees have the permission to request a transaction if they know its hash. Thus, they can retrieve a certificate's issuance transaction in order to check its validity.

Employers will be able to compute through the application the hash of a certificate stored in PDF format in order to compare it with the hash stored on the blockchain.

C. Use Cases

1) Certificate Issuance

In this use case a university, named *university*, was created that would like to award a bachelor's degree to a student named *student*. The issuance process requires the execution of the following actions shown in Fig. 1 and 2 that are explained below.

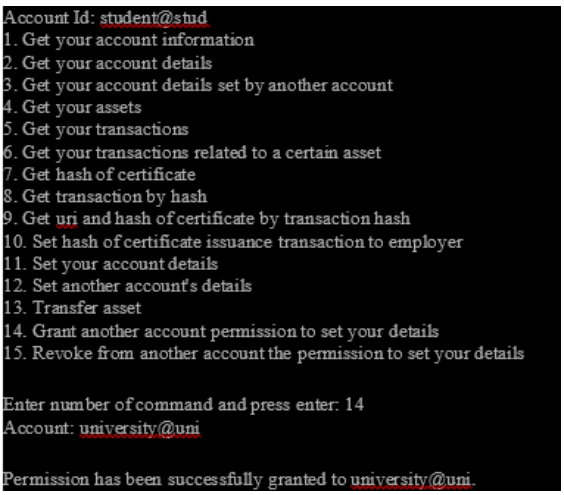

Fig. 1 Student grants university permission to set their account details

- *Student* needs to apply for the certificate by granting *university* permission to set their account details. To do so, *student* needs to log in to their account, select the command "14. Grant another account permission to set your details" and insert *university's* account id. This process is illustrated in Fig. 1. After issuance of the certificate, *student* can revoke from *university* the permission to set their account details by executing the command "15. Revoke from another account the

permission to set your details".

– *University* needs to issue the certificate. To do so, *university* should log in to its account, select the command "7. Issue certificate", and type *student's* account id, the type of the certificate, i.e. bachelor, and the certificate's URI, as shown in Fig. 2.

2) Certificate Validation

In this case a student, named *student*, was created that would like to grant a prospective employer, named *employer*, access to the integrity guarantee of their bachelor's degree, so that *employer* can validate the certificate. The following actions need to be performed:

– *Employer* needs to grant *student* permission to set their account details. To do so, *employer* needs to log in to their account, select the command "9. Grant another account permission to set your details" and insert *student's* account id. After validation *employer* should revoke from *student* the permission to set their account details by executing the command "10. Revoke from another account the permission to set your details".

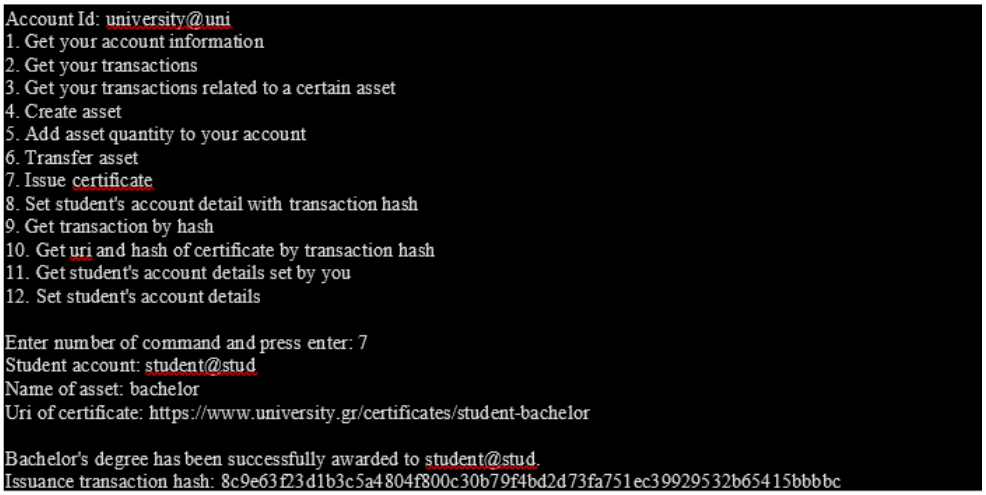

Fig. 2 University awards a bachelor's degree to student

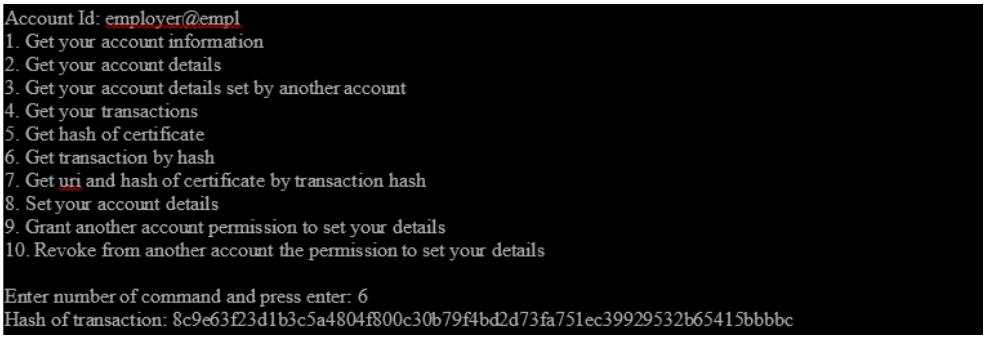

Fig. 3 Employer asks for the transaction hash of a certificate

– *Student* needs to give *employer* access to the certificate's issuance transaction so that *employer* can validate the certificate. To do so, *student* should log in to their account and get the certificate's issuance transaction hash, which is stored in their account details, by executing the command "3. Get your account details set by another account" and typing *university's* account id. Then, *student* should select the command "10. Set hash of certificate issuance transaction to employer" and insert the transaction hash, *employer's* account id, and the name of the detail they want to set, e.g., *student* bachelor. This process is shown in Fig. 4.

– *Employer* needs to check the validity of the certificate. To do so, *employer should* get the certificate's issuance transaction hash, which is stored in their account details, by executing the command "3. Get your account details set by another account" and typing *student's* account id. *Employer* should then retrieve the transaction by selecting the command "6. Get transaction by hash" and inserting the hash retrieved during the previous step. Finally, *employer* can use the command "5. Get hash of certificate" to compute the certificate's hash and compare it with the hash stored on the blockchain.

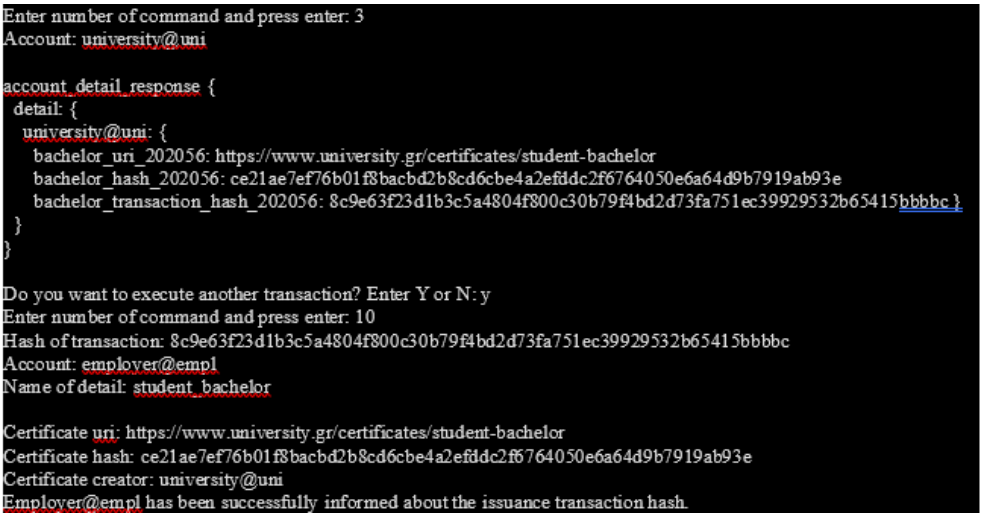

Fig. 4 Student gets their account details and gives employer access to the certificate's issuance transaction

V. Conclusions

This paper, which analyses and uses the Hyperledger Iroha framework, is the first in a series of experiments that aim to study existing blockchain frameworks and develop an initial version of a blockchain-backed application for the management of educational certificates. The development of such an application not only confirms that blockchain can contribute to the alleviation of the education sector's challenging problems, but also demonstrates the fact that secure and trustworthy systems based on Hyperledger Iroha can be easily implemented.

As far as this paper is concerned, future work includes the further development of the application so that it can be used in real-life scenarios. For instance, fully functional wallets should be integrated into the platform. Additional future steps include the following: the implementation of similar applications based on Ethereum and Hyperledger Fabric frameworks, the study of other existing blockchain frameworks that could be used for the education sector's digitisation, and the semantification of blockchain data in order to link them with Linked Data.

Acknowledgment

This work has been co-funded by the European Union's Horizon 2020 research and innovation programme under the QualiChain project, Grant Agreement No 822404.

References

[1] Lizcano, D., Lara, J.A., White, B. et al. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. J Comput High Educ, 2020, 32, pp. 109–134.

[2] Bartolomé, A. R., Bellver, C., Castañeda, L., & Adell, J. Blockchain in education: Introduction and review of the state of the art. EDUTEC, Revista Electrónica de Tecnología Educativa (Electronic Journal of Educational Technology), 2017, 61, pp. 1–14.

[3] Gräther, Wolfgang, et al. "Blockchain for education: lifelong learning passport." Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET), 2018.

[4] G. Chen, B. Xu, M. Lu, and N.-S. Chen, ''Exploring blockchain technology and its potential applications for education,'' Smart Learn. Environ., 2018, vol. 5, no. 1, pp. 1.

[5] M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in IEEE Access, 2018, vol. 6, pp. 5112-5127.

[6] MIT, blockcerts, (Online). Available at: https://www.blockcerts.org/. Accessed in April 2020.

[7] Learningisearning, learningisearning2026 (Online). Available at: http://www.learningisearning2026.org/. Accessed in April 2020.

[8] EdgeCoin Project (Online). Available at: http://www.edgecoin.io/. Accessed in April 2020.

[9] Rooksby, John, and Kristiyan Dimitrov. "Trustless education? A blockchain system for university grades." New Value Transactions: Understanding and Designing for Distributed Autonomous Organisations, Workshop at DIS. 2017.

[10] Openblockchain. Researching the potential of blockchains. Knowledge Media Institute, The Open University, UK, 2018. Retrieved from http://blockchain.open.ac.uk. Accessed in April 2020.

[11] Grech, A., & Camilleri, A. Blockchain in education. Joint Research Centre Science for Policy Report, European Commission, Brussels, 2017. Retrieved from http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108255/jrc108255_blockchain_in_education%281%29.pdf#page=66. Accessed in April 2020.

[12] EC. (2018a). European Commission launches the EU Blockchain Observatory and Forum. European Commission, Brussels. Retrieved from https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-eu-blockchain-observatory-and-forum. Accessed in April 2020.

[13] EC. (2018b). European countries join blockchain Partnership. European Commission, Brussels. Retrieved from https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership. Accessed in April 2020.

[14] EC. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. European Commission, Brussels. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed in April 2020.

[15] TechGDPR: GDPR's Right to be Forgotten in Blockchain: it's not black and white. Retrieved from https://techgdpr.com/blog/gdpr-right-to-be-forgotten-blockchain/. Accessed in February 2020.

[16] Truong, Nguyen Binh, et al. "GDPR-compliant personal data management: A blockchain-based solution." arXiv preprint arXiv:1904.03038, 2019.

[17] Mahindrakar, Abhishek, and Karuna Pande Joshi. "Automating GDPR Compliance using Policy Integrated Blockchain." 6th IEEE International Conference on Big Data Security on Cloud (BigDataSecurity 2020), 2020.

[18] Onik, Md Mehedi Hassan, et al. "Privacy-aware blockchain for personal

data sharing and tracking." Open Computer Science, 2019, Vol. 9.1, pp. 80-91.
[19] Ethereum Homestead. Ethereum Homestead Documentation. Retrieved from https://ethereum-homestead.readthedocs.io/en/latest/index.html. Accessed in February 2020.
[20] Hyperledger Fabric. A blockchain platform for the enterprise. Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-2.0/index.html. Accessed in February 2020.
[21] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich et al., Hyperledger fabric: A distributed operating system for permissioned blockchains., 2018.pp. 1-15
[22] Hyperledger Iroha. Hyperledger Iroha Documentation. Retrieved from https://iroha.readthedocs.io/en/master/index.html. Accessed in April 2020.
[23] Dahal, Ram Krishna, Jagdish Bhatta, and Tanka Nath Dhamala. "Performance Analysis of SHA-2 and SHA-3 finalists." International Journal on Cryptography and Information Security (IJCIS), 2013, 3.3, pp. 720-730.
[24] W. Diffie and M. E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory, November 1976, IT–22(6), pp. 644–654.
[25] C. Dwork and M. Naor, “Pricing via processing or combatting junk mail,” in Advances in Cryptology - CRYPTO ’92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, Proceedings, 1992, pp. 139–147.
[26] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. Retrieved from: https://bitcoin.org/bitcoin.pdf. Accessed in February 2020.
[27] Muratov, Fedor, et al. "YAC: BFT consensus algorithm for blockchain." arXiv preprint arXiv:1809.00554, 2018.
[28] Hyperledger Iroha. Hyperledger iroha Github Repository. Retrieved from https://github.com/hyperledger/iroha. Accessed in April 2020.