A Permissioned Blockchain-Based System for Verification of Academic Records

Ahmed Badr, Laura Rafferty, Qusay H. Mahmoud, Khalid Elgazzar, Patrick C. K. Hung
Ontario Tech University
Oshawa, Ontario, Canada
{Ahmed.Badr,laura.rafferty,qusay.mahmoud,khalid.elgazzar,patrick.hung}@uoit.ca

***Abstract*—While academic institutions maintain records such as transcripts and certificates, they are often requested to share these records with other institutions at the request of students for credit transfer, or prerequisites for acceptance into new academic programs. While the transfer of academic records is a regular daily activity for the institutions, there is often significant overhead involved as the process of transfer and verification is extremely manual. The need for an automated end-to-end solution for the transfer and verification of academic records between institutions is on the edge to reduce wait times for students to transfer their records, as well as to provide a reliable verification method to avoid academic fraud. This paper presents a permissioned blockchain-based system to allow institutions to securely and dependably transfer and verify academic records at the student request. Permissioned blockchains, such as Hyperledger, provide a more scalable and cost-effective and private solution for enterprise applications. Our solution is comprised of a web interface for enrolling and requesting the transfer, with a backend using Hyperledger Fabric and Hyperledger Composer to retain the hash of the records on the blockchain for verification.**

Keywords—Blockchain, Hyperledger Fabric, Academic Record Verification

I. Introduction

Despite largely subscribing to the modern practice of maintaining electronic records, most academic institutions continue to rely on manual processes for transferring academic records such as transcripts and certificates between institutions and to potential employers. The typical transfer of a student's transcript from their home institution to another can take a few days to over a month with processing and delivery times using the widely adopted paper method. In addition to the significant wait times and opportunity for physical damage or loss of the records in transit, there are also risks of counterfeit credentials by fraudulent parties. The physical mailing of paper records also comes with high costs associated with the processing times, manual work effort, postal fees, and transit. E-mail based solutions, PDF record transfers, secure drop sites are becoming increasingly common. For credential verification, online degree and credential verification services such as York University's *YU Verify Online* [1] and University of Texas [2] are also being adopted to allow third parties to verify that individuals have obtained academic credentials without having to go through a manual request process. Third-party services such as the National Student Clearinghouse [3] provide verification of student enrolment, certifications, degrees, graduation dates as well as an electronic transcript exchange for registered institutions mainly in the United States but also many other countries including Canada. In Ontario, the Ontario College Application Service (OCAS) and Ontario Universities' Application Centre (OUAC) utilize shared systems for automated electronic transfers of transcripts between academic institutions within the province. OCAS uses an Electronic Transcript Management System (eTMS) which provides a semi-automated system for high schools to transfer transcripts to postsecondary institutions on behalf of students. OCAS and OUAC both use standard XML formats for academic records established by the Postsecondary Electronic Standards Council (PESC) [4], which have been widely adopted by academic institutions within Canada and the United States, as well as some others in Australia, Ireland, and the Netherlands.

While these solutions provide a more modern approach to the transfer of academic records, there are still limitations in terms of widespread adoption, auditability, and scalability. Academic institutions could benefit from blockchain technologies to provide a decentralized and immutable ledger to confirm the integrity of academic records [5] [6]. There have been several recent works, further described in Section II. These works go beyond traditional methods and have begun to implement solutions utilizing blockchain technologies. Such solutions provide an immutable record of academic records and transactions which support verification by third parties without the significant manual overhead and associated costs. A successful solution for electronic records exchange must support the following capabilities:

1. *Completeness*: End-to-end system to allow students and academic institutions to easily request, upload, transfer, and validate records. It must provide automation and be easy to use as well as open to recipients who may be outside of the network.
2. *Security and Privacy*: The system must provide a secure and reliable way to transfer, store, and verify the integrity of academic records. It must limit the distribution of confidential data to only the intended recipient, as well as limit the amount of data stored on the blockchain.
3. *Scalability*: It must be able to support the growing number of universities, students, and records, handle modifications and additions to records and support records in different formats, scales, etc. while remaining usable and stable.

978-1-7281-1542-9/19/$31.00 ©2019 IEEE

A. Blockchain for Record Storage

Traditional storage of records within a database demonstrates some limitations in terms of auditing and verification by external parties. While blockchain provides an immutable, distributed ledger, it can be extended to provide verifiable artifacts of records, while peer nodes maintain a copy of the ledger and validate through consensus protocols. When adapting a blockchain-based solution for practical applications, there are several challenges that need to be considered. Blockchain applications include possible overhead and long processing times if expensive consensus protocols are required. Further, due to the immutability of the blockchain, there must be considerations to what data is stored on it for the privacy of users. This inspires the approach of "off-chain" record storage, using a combination of on and off-chain methodologies to include only what is required on the blockchain itself, such as a hash of the record, in order to save space and overhead and to preserve the privacy of the student's data.

B. Permissioned Blockchain

Public permissionless blockchains, such as Bitcoin and Ethereum, operate on public, open, anonymous networks. Due to the openness of these networks, participants are considered untrusted and thorough Byzantine fault-tolerant consensus (i.e. Proof of Work) is required in order to account for potential faults or malicious nodes. Further, due to the excessive computations required to reach consensus, the participants require economic incentive for participation, which is offered in the form of block reward. These procedures can become costly in terms of resources, time, and finances, which often counteracts the potential value provided by the blockchain application to make it infeasible for practical use. These limitations motivated the direction of permissioned blockchain networks such as Hyperledger. Permissioned blockchain networks operate on private, segregated networks where participants are identifiable and therefore more trusted due to their identifiability. For this reason, less expensive consensus protocols can be used, providing better performance with higher transaction throughput performance, lower latency of transaction confirmation, and lower costs. Further, the network can be segregated to allow for nodes to only have access to and verify transactions that they are permissioned for. This is ideal for maintaining the confidentiality and privacy of sensitive data within the network. For these reasons, permissioned blockchain networks are more appealing for the cost, performance and confidentiality requirements of practical enterprise applications.

Hyperledger Fabric [7] is a blockchain platform for private and permissioned business networks, providing a foundation for transactional applications across business networks using smart contracts and maintaining an immutable ledger. Hyperledger Composer is a framework for the development of applications built on top of Hyperledger Fabric, allowing for the development of applications from the business level and using REST APIs. This allows the developers to model files to describe assets, participants, and transactions in a business network, as well as create access control rules to limit the data available to each participant according to only what is required for their specific function. For our system, we chose to use Hyperledger as a permissioned blockchain, with a hybrid of on- and off-chain record storage, where only a hash of the record is stored on the blockchain rather than the entire record. This allows us to utilize the immutability of the blockchain for recording and verifying the integrity of records while preserving the privacy of users and limiting the resources saved in the blockchain. While the blockchain component provides the ledger of transactions and record data, we also provide a web application component for users to interface with to perform tasks through an intuitive interface.

The goal of our proposed system is to address the limitations of existing solutions by providing a secure, verifiable, and tamper-proof method for verification of academic records between institutions using blockchain technologies. To this end, the rest of this paper is organized as follows. Section II discusses the related work. Our proposed solution is presented in Section III. In Section IV, we evaluate how the solution performs at scale based on benchmarking of our experiments. Finally, Section V draws concluding remarks and highlights future directions.

II. Related Work

There have been several notable solutions in recent years to provide a solution for transfer and validation of academic records using blockchain technologies. Digital signatures can provide authentication and integrity of documents, while blockchain solutions provide additional capabilities through an immutable, distributed ledger. Several solutions offer a method to simply verify the existence of a document stored securely and permanently within the blockchain. Proof of Existence blockchain notary service [8] allows users to record a SHA256 hash of a document to a Bitcoin transaction, creating proof of the existence of the document at the time of the transaction which can be verified by anyone by viewing the public blockchain ledger. A patent [9] submitted by the Sony Corporation, among other applications, identifies a system for using blockchain to store academic records, with smart contracts to transfer credentials. When a student sends an academic credential to a recipient institution, a reference to the blockchain address can be included so it can be verified. The University of Nicosia [10] has a solution which reduces the number of blockchain transactions by first creating a hash of all student certificates for a course, then creating a document with a listing of all certificate hashes. This listing is then hashed and then recorded in the transaction to be viewed and verified by the recipient. This solution is also effective for recording credentials for an independent course but has not been scaled to accommodate entire academic institutions with a large number of courses, students, and transcripts.

The MIT Digital Certificates Project [11] provides a system for registering digital certificates to the Bitcoin blockchain, which can then be shared and verified. This has been adopted by some organizations for issuing certificates for attending training sessions, or proof of employment. Limitations with using the Bitcoin blockchain include long transaction times, and the solution may not be scalable to a large number of requests that would be required for adoption to large academic institutions.

Other solutions using permissioned blockchains include CredenceLedger [12], which operates on a permissioned blockchain using multichain streams. It also records hashes of the records within the blockchain, with a mobile application front end interface for students to manage their credentials. The

Greek Research and Technology Network (GRNET) in collaboration with blockchain research and development company IOHK, have implemented an application for verification of student diplomas using Enterprise Cardano, combined with a web application front end [13]. [14] use an Ethereum private blockchain to implement a personal data store (PDS) for users to manage their personal data such as health records and academic records. The Blockchain for Education platform [15] uses smart contracts based on the Ethereum blockchain for certificate management and identity management. Hashes of certificates are stored on the blockchain while the full document is stored in the BSCW document management system. The identities of the accreditation authorities and certification authorities are also registered on the blockchain, with profiles of certification authorities stored within the Inter-Planetary File System (IPFS). TrueRec is also an Ethereum-based application developed by SAP [16], which allows users and potential employers to manage and verify professional and academic qualifications within a mobile application. The user requests the issuing institution to send the credentials, which are then stored as hashes in the user's digital wallet, which can then be verified by other institutions.

III. PROPOSED SOLUTION

This section presents our proposed end-to-end solution for transmission and verification of academic records. We will begin with an overview of assumptions, followed by a description of the system architecture and implementation, then a discussion on scalability as well as some challenges and solutions identified throughout the development process.

A. Assumptions and Scope

We have made the below assumptions in the initial development of our system, which have limited the scope of the initial proof of concept implementation.

1. The system is limited to the request and transfer of transcripts and academic records "as is". This assumes that the home institution attests to the accuracy and integrity of the record provided to the system. Conversion of grading schemes, course equivalencies, or translations is out of scope.
2. Full registration and validation of Universities and students into the system is out of scope. This process would be defined upon implementation. Universities will be responsible for validating the enrolment of students, but this is outside of the current scope.
3. Payment system integration for student requests is out of current scope, however, this can be easily extended.
4. Academic records are valid indefinitely unless given an expiry by the issuing institution.

B. Architecture

The system consists of two main components, the blockchain application layer, and the web application layer as illustrated in Fig. 1. The web application layer provides an interactive interface for users while interacting with the Hyperledger Fabric network through APIs.

The Blockchain Application Layer is comprised of the Hyperledger Composer model file, script file, ACL file, and query file, which make up the Business Network Archive to be implemented in Hyperledger Fabric. Our model file defines the University and Student participants, as well as the Transcript asset. The script file defines the function `sendTranscript()`, which is initiates the transaction to change ownership of the student's transcript from the home institution to the recipient institution.

The Web Application provides an interface for Students and Academic Institutions to perform functions such as requesting a transcript to be sent, uploading and hashing a transcript, and verifying a transcript. Users can perform functions through the web application by interfacing with the Hyperledger REST APIs to perform the functions. A database of the students, universities, transcripts, and transcript requests is used by the web application and corresponds to the contents of the Hyperledger ledger.

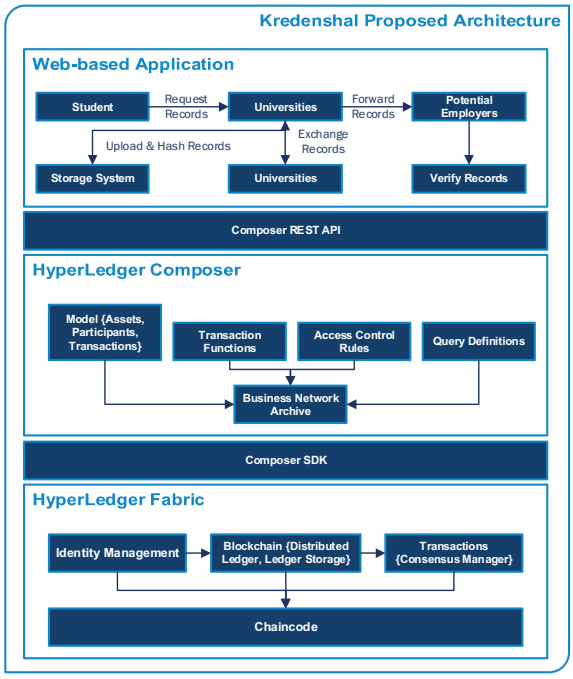

Fig. 1. System Architecture

C. Implementation

As discussed in the previous section, we implemented our system with a web application hosted on Google Cloud, with Hyperledger Composer and Hyperledger Fabric. This section will elaborate on the implementation details.

1) Business Network Archive

The Hyperledger Composer business network archive provides a description of the participants, assets, transactions, as well as the access control rules for the system. Network participants are defined for the Students and Universities. The transcript asset is also defined, which records the hash of the file, as well as a download link, timestamp, and optional expiry date:

```
participant Student identified by id
participant University identified by id
```

The function SendTranscript() is defined for the transaction to transfer ownership to the recipient university, which adds the recipient to the array of recipient universities:

2) Transcript Request and Transfer Process

The process for a transcript request would follow the below steps, where the participants are the Student, his/her Home University, and the Recipient University which will be receiving the transcript.

- The Student logs into the web application and submits the request for their transcript to be sent to a specified recipient institution.
- The Home University receives the request and uploads the transcript through the web interface.
- The transcript is stored on the web server, and a hash of the transcript is calculated
- The `sendTranscript()` function is invoked, then initiates the transaction to transfers ownership of the transcript to the recipient university and records the hash of the transcript within the transaction.
- The recipient university is now able to access the transcript through the web application and verify the file through the hash saved on the blockchain. Transcript file can be compared to the hash.

3) Validation Process

Once the recipient university receives the transcript, they can validate the integrity of the file by comparing it to the hash stored within Hyperledger. This protects from the possibility of forged credentials and is resilient to possible faults such as listed below:

- *The student did not attend the university claimed*: A student requests a transcript from. If the student did not attend the university claimed, they will not complete the transcript request for the student.
- *Student attempts to modify transcript*: A student receives their transcript and modifies it before sending to the recipient institution. The transcript will no longer match the hash stored in the blockchain, therefore the recipient institution will recognize that it has been modified.
- *Recipient University attempts to access credentials of a student without request*: ACL will restrict the access to any credential or transaction that a participant has not been authorized to access.
- University attempts to view academic record transactions from other universities
- *Host university database has an outage, is lost, or has been the target of ransomware*: original transcript may be lost or unavailable, however, the hash of the transcript will still be recorded in the blockchain and any copies of the transcript can still be verified.
- *The web application is compromised:* if the web application is compromised or observes an outage, the Hyperledger blockchain will still remain available for verification of records that have already been sent.

4) Access Control

The ACL file provides granular access control to provide permissions to participants to only be able to view resources and transactions that are required for their job functions. Since we are dealing with permissioned ledger each participant in the system is assigned certain permissions which allow specific actions to be done by the participant. For example, for each participant of type "Student", the following permissions are granted for that participant through ACL rules:

- *R1a_StudentsSeeUpdateThemselvesOnly*: this rule gives permission to the student to Read/Update his own data only.
- *R1b_StudentsSeeTheirTranscripts*: this rule gives permission to the student to view only transcripts issued or requested by his/herself.

D. Scalabiliy

While the system has a requirement for scalability to be able to accommodate increasing numbers of universities, students, and academic records, we have introduced several components to support the additional load. Through the use of permissioned blockchain, we are able to accommodate larger amounts of participants and transactions without causing extreme resource utilization on the nodes. Further, the web application component allows participants to perform transactions on the system without being directly part of the Hyperledger network, and therefore there is no requirement for each participant to run any client on their system.

TABLE 1 illustrates a comparison between popular public and permissioned blockchain networks according to the average transaction time to identify how they may scale to large applications. Public blockchains such as Bitcoin have a known scalability problem, with a relatively low limit on the amount of transactions the network can process at a time and high costs per transaction. This severely limits the ability to scale to large enterprise applications. Some solutions have been developed to increase the scalability of blockchains such as Bitcoin Lightning Network to create channels between participants, and Ethereum Sharding, which has potential to increase the transaction threshold of Ethereum dramatically [17]. Permissioned blockchains such as Multichain and Hyperledger in their default states maintain smaller chains, and lower transaction times, and are able to scale to accommodate more transactions. Factors that contribute to transaction speed include block size and network latency.

TABLE 1. BLOCKCHAIN TRANSACTIONS PER SECOND COMPARISON

	Type	Transactions/s
Bitcoin	Public	3.3 - 7
Ethereum	Public	15-25
Multichain	Private	500-1000
Cardano	Public	5-7
Hyperledger	Permissioned	2500

E. Challenges and Solutions

Our system has been designed to provide ease of use and scalability, using a permissioned blockchain to allow for faster processing times, web application to provide a usable interface for users. All transcripts are signed, hashed and stored in the blockchain. Access control lists provide permissioned access based on requirements of the users. Data retention and privacy can introduce concerns for users.

IV. EXPERIMENTAL EVALUATION AND RESULTS

We evaluate our system performance using Apache JMeter to assess average response time. The experiments are conducted

with 2 vCPUs with 3.6GB RAM. During the experiments, 95% of the CPU utilization was used and approximately 30% of the memory. We generated HTTPs requests using Apache JMeter, where the load is sent using 500 threads (users) with a round-up period of 250 seconds. Fig. 2 shows the overall system behavior (most notably in terms of response time) for a total of 32251 requests generated in 559 seconds. The system was able to successfully handle requests with an average throughput of 21.7 requests/second. The system response time increases as more requests come in to the system with no observed drop outs. However, as the system reaches capacity, we observe a high number of request rejection with an overall steady throughput.

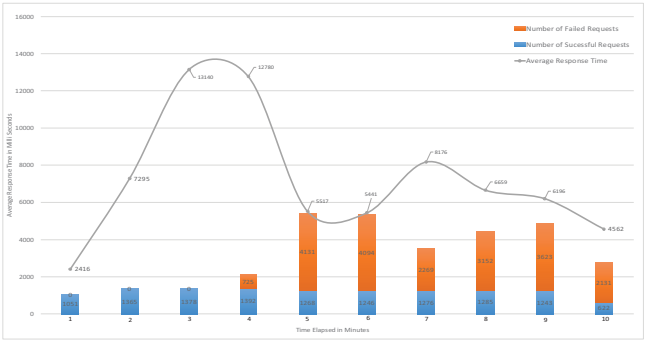

Fig. 2. Average Response Time

In comparison to related systems identified in Section II, TABLE 2 shows how our system is able to provide more flexibility for support of any file times or formats of academic records, including both transcripts and certificates. It also provides an automated solution, with and is more scalable to accommodate the potential load of many institutions and users.

TABLE 2. COMPARISON OF SYSTEMS

	Blockchain	Record	Automated	Immutable	Scalable
Traditional Mail	N/A	Any	No	No	No
PDF Signed eTranscripts	N/A	Transcript	Maybe	No	Maybe
University of Nicosia	Bitcoin	Certificate	No	Yes	No
MIT BlockCerts	Bitcoin	Any	No	Yes	No
CredenceLedger	Multichain	Certificate	Yes	Yes	Maybe
Our Solution	Hyperledger	Any	Yes	Yes	Yes

V. CONCLUSION AND FUTURE WORK

This paper presents a solution to the challenge of transferring and proposes a system to verify academic records between academic institutions. Using Hyperledger as a private permissioned blockchain introduces higher performance, cost-effectiveness, and privacy compared to public blockchain solutions. The system is also open and can be extended to any record type according to the specific requirements of individual institutions. While our system provides an easy to use and secure solution, widespread adoption by different institutions is essential to reach the required mass momentum. While this is currently directed towards academic institutions, it can be easily extended to include organizations wishing to validate credentials of prospective job applicants. The system could also be adapted to leverage and enhance existing solutions, such as to act as a broker between networks (i.e. interprovincial and international).

Further works to improve our system would include additional automation to fully eliminate manual efforts and fully integrate with academic institutions information systems for minimal user interaction requirements. This would include the functionality to allow academic institutions to upload transcripts in bulk.

REFERENCES

[1] York Unversity, "YU Verify - Degree Verification," [Online]. Available: https://registrar.yorku.ca/graduation/yuverify. [Accessed 2 December 2018].

[2] The University of Texas, "Verifying Degrees and Dates of Attendance," [Online]. Available: https://registrar.utexas.edu/students/degrees/verify. [Accessed 2 December 2018].

[3] National Student Clearinghouse, "National Student Clearinghouse Verification Services," [Online]. Available: http://nscverifications.org/welcome-to-verification-services/. [Accessed 2 December 2018].

[4] Postsecondary Electronic Standards Council, "PESC Approved Standards," [Online]. Available: http://www.pesc.org/pesc-approved-standards.html. [Accessed 2 December 2018].

[5] 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, pp. 145-156, 2018.

[6] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," in *11th European Conference on Technology Enhanced Learning*, Lyon, France, 2016.

[7] E. Androulaki, A. Barger, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the 13th EuroSys Conference*, Porto, Portugal, 2018.

[8] PoEx Co., Ltd, "poex.io," [Online]. Available: https://poex.io/prove. [Accessed 2 December 2018].

[9] Z. Zhang, "Electronic Apparatus, Method for Electronic Apparatus and Information Processing System". Tokyo, Japan Patent US20170346637A1, 30 November 2017.

[10] University of Nicosia, "Academic Certificates on the Blockchain," [Online]. Available: https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/. [Accessed: 25 November 2018].

[11] MIT Media Lab Learning Initiative and Learning Machine, "Digital Certificates Project," [Online]. Available: http://certificates.media.mit.edu/. [Accessed 25 November 2018].

[12] R. Arenas and P. Fernandez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials," in *IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Stuttgart, Germany, 2018.

[13] A. Castor, "Cardano Blockchain's First Use Case: Proof of University Diplomas in Greece," 2 January 2018. [Online]. Available: https://bitcoinmagazine.com/articles/cardano-blockchains-first-use-case-proof-university-diplomas-greece/. [Accessed: 2 December 2018].

[14] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han and P. Sarda, "Blockchain as a Notarization Service for Data Sharing with Personal Data Store," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2018.

[15] S. Kolvenbach, R. Ruland, W. Gräther and W. Prinz, "Blockchain 4 Education," in *Proceedings of 16th European Conference on Computer-Supported Cooperative Work-Panels, Posters and Demos*, 2018.

[16] SAP, "Meet TrueRec by SAP: Trusted Digital Credentials Powered by Blockchain," 24 July 2017. [Online]. Available: https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/. [Accessed: 2 Dec 2018].

[17] A. Chauhan, O. P. Malviya, M. Verma and T. S. Mor, "Blockchain and Scalability," in *IEEE International Conference on Software Quality, Reliability and Security Companion*, 2018.