Implementation and Analysis of Blockchain Based DApp for Secure Sharing of Students' Credentials

Raaj Anand Mishra*, Anshuman Kalla†, Nimer Amol Singh¶, Madhusanka Liyanage‡§
*†¶School of Computing and Information Technology, Manipal University Jaipur, India
‡School of Computer Science, University College Dublin, Ireland
§Centre for Wireless Communications, University of Oulu, Finland
{raaj.169103057*, nimer.169104006¶}@muj.manipal.edu, †anshuman.kalla@jaipur.manipal.edu, ‡madhusanka@ucd.ie

***Abstract*—The paper aims to resolve security issues revolving around the sharing of students' credentials by leveraging the blockchain technology. It proposes a novel blockchain-based architecture followed by its implementation as a decentralized application (DApp). Further, the cost & the performance analysis are carried out based on the experiments conducted.**

***Index Terms*—Blockchain, Smart Contracts, DApp, Ethereum**

I. Introduction

Transcripts, diploma & degree certificates, internship & training certificates, migration & transfer certificates, character certificate, letter of recommendation, etc. are the set of essential credentials that stay with an individual for his/her lifetime. Issuing and sharing of these credentials is an integral process of our education ecosystem and plays a vital role during the recruitment drives of companies. To enhance security of the issued credentials, educational institutes make use of numerous methods like assigning unique identification number, putting uniquely distinguishable hologram, affixing student's passport-sized photograph, printing the details of the students like date of birth, place of birth, parents' name, registration/enrollment number, etc. Moreover, at the time of recruitment process, companies also need to verify the credentials that it receives directly from the applicants. Indeed, many times, companies contact the parent institution to endorse the credentials it has received from applicants. Such kind of process is tedious, costly and time-consuming.

Some of the recent papers that have presented the benefits and the challenges of using blockchain technology in education are [1], [2], [3], [4] and [5]. However, there is still a need to design a working prototype of student-credential sharing platform which can offer services for all the stakeholders in the education ecosystem.

The paper modestly claims three-fold contribution:

- A novel yet pragmatic blockchain-based architecture is proposed for secure sharing of students' credentials among various stakeholders.
- A prototype of the proposed architecture is developed as a Decentralized Application (DApp) using Ethereum.
- Performance analysis in terms of execution & transaction cost of the developed smart contracts and the execution time of important operations are carried out.

The demo and implementation details of the prototype can be found here[1].

II. The Proposed Architecture

An architecture comprising of five major stakeholders, blockchain infrastructure and file (or cloud) storage is depicted in figure 1. Decentralized application along with the smart contracts govern the interactions between multiple stakeholders.

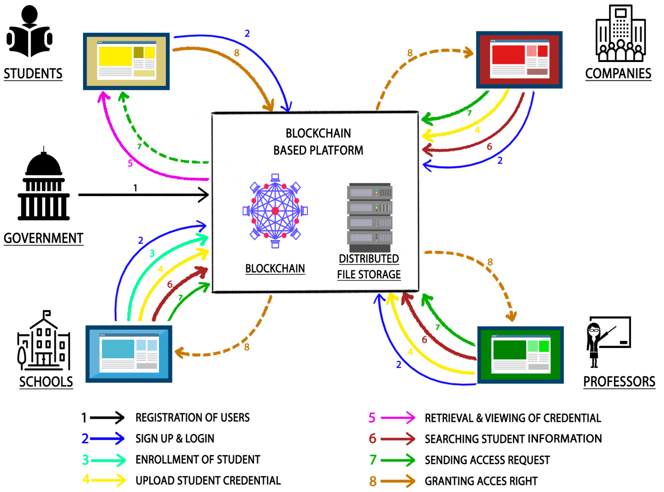

Fig. 1: Proposed Architecture for sharing students' credentials

Next, we discuss the roles of various stakeholders. *Government* body creates unique identities for all the stakeholders. Based on these identities, accounts are created for all the other stakeholders. *Schools* have a list of enrolled students for whom it has to issue and share the credentials. On the contrary, when a student seeks admission to a new school, this school may need to view the applicant's credentials already issued by the previous school(s). *Students* want to view their academic credentials. Further, students need a way to provide access to their credentials to the intended school at the time of admission or the company at the time of recruitment. *Companies*, during recruitment, demand access to the applicant's credentials. Alternatively, a company would issue certificates to students on completion of training or internship. Like companies, *Professors* need to view the applicant's credentials for recruitment of positions like Ph.D., PostDoc, etc. Alternatively, professors may have to furnish a letter of recommendation or internship certificate to their students.

The core functionalities of the proposed architecture are (i) *Registration of User:* assigns a unique ID to every user. The way to create unique IDs is discretion of the government

[1] https://sites.google.com/view/blockchain-project/home

body, (ii) *Sign-up and Login of User:* allows users to undergo one-time sign-up process which would ease future logins, (iii) *Enrollment of Student:* happens at the time of admission, (iv) *Uploading of Credential:* by school or company or professor, (v) *Retrieval and Viewing of Credential:* enables students to retrieve their credentials, (vi) *Searching Student Information:* facilitates stakeholders to search student's information (Students can decide which of their information will be visible to stakeholders), (vii) *Sending Access Request:* allows schools, professors and companies to send access request to students to view their credentials and (viii) *Granting Access Right:* empowers students to approve the received access requests.

III. Implementation

To develop a prototype of the proposed architecture we make use of Ethereum, MetaMask, Web3.js, Next.js and IPFS. For the first-level implementation, three different types of stakeholders are considered; school, student and company. Each stakeholder has different set of functionalities (and restrictions) which are offered (and imposed) using different dashboards of the DApp. *School dashboard* has two options; (i) to add students to the list of enrolled students and (ii) to upload credentials for already enrolled students. When a credential is uploaded on IPFS, a hash value is returned. This hash value along with the metadata of the credential is pushed to the Ethereum such that only intended student can view it. *Student dashboard* offers three options; (i) to view the uploaded credentials, (ii) to view the access requests sent by the companies and (iii) to grant access after viewing those access requests. *Company dashboard* has three options; (i) to view the list of schools and the students enrolled under a selected school, (ii) to send an access request, (iii) to view the credentials once the students grants access. The DApp consists of front-end which at the back-end runs on a decentralized platform i.e. the Ethereum. Seven different smart contracts are designed and their details are available on the same web-page where demo is available.

IV. Experiment Results and Discussion

The developed DApp is analyzed by running different experiments over Rinkeby (Ethereum's) test network. Table I shows the costs for various smart contracts and table II shows the transaction cost for some important functions.

TABLE I: Deployment Cost of Smart Contracts

Contract Name	Execution Cost (Gas)	Transaction Cost (Gas)
User	671302	939570
File	812244	1115776
Student	1014987	1387779
School	1680974	2269274
Request	919555	1272975
ShareFiles	556281	790677
Company	894342	1232750

In general, reading data from blockchain takes negligible time. However, when a user writes data, transactions are validated, blocks are mined and appended to the existing blockchain. The average time for a transaction/request to get processed on the Rinkeby Test Network is 15 s according to their official website. To compute the average and the variations in the execution time for uploading a credential, 100 upload requests were sent back-to-back. Figure 2 shows the results with 95% confidence interval. The average turns out to be 16.00337 s. The difference between the observed average time and the official average time is 1.00337 s. The additional delay is due to the time required for execution of smart contracts on the Ethereum and communication delay.

TABLE II: Cost of some of the important functions

Transaction	Cost (Gwei)	Cost (Ether**)	Cost (USD***)
Enrolling a student	72240	0.00007224	0.016
Uploading a credential*	158513	0.000158513	0.036
Company retrieving a credential*	158499	0.000158499	0.036
Student sharing a credential*	24831	0.000024831	0.006

* depends on title and description length. We used 20 letters for both
** 1 ether = 10^9 gwei, *** 1 ether=$ 227.17 on 20.07.2019

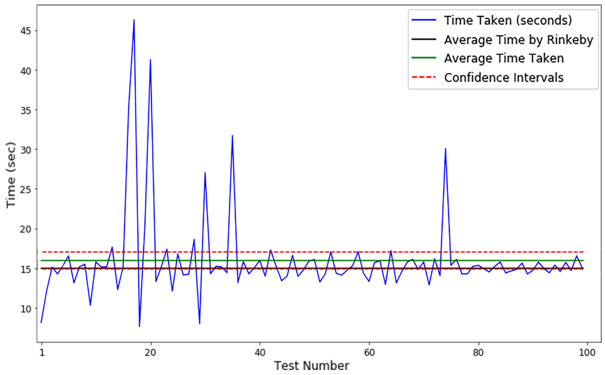

Fig. 2: Execution time for credential upload requests

V. Conclusions

The paper presents a simple and pragmatic blockchain-based architecture for secure sharing student's credentials. Further, a DApp is developed and its performance is analyzed in terms of costs and execution time. In future, we intent to extend the work by including privacy along with security.

Acknowledgement

This work is supported by Academy of Finland and European Union in RESPONSE 5G (Grant No: 789658) and 6Genesis Flagship (grant no. 318927) project.

References

[1] X. Tao, "The application and challenges of blockchain technology in educational practice," *Modern Educational Technology*, vol. 1, p. 019, 2017.

[2] T. Nguyen, "Gradubique: An academic transcript database using blockchain architecture," 2018.

[3] J. Hope, "Give students ownership of credentials with blockchain technology," *The Successful Registrar*, vol. 19, no. 1, pp. 1–7, 2019.

[4] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.

[5] J. Rooksby and K. Dimitrov, "Trustless education? A blockchain system for university grades," in *New Value Transactions: Understanding and Designing for Distributed Autonomous Organisations, Workshop at DIS*, 2017.