Leveraging Blockchain technology in the Education Sector

Devaki Kulkarni[a], Ruchika Pande[b], Akhil Shaji[c], Shweta Patil[d], Radhika Kulkarni[e]

[a,b,c,d,e] Pune Institute of Computer Technology, Pune, Maharashtra, India
[a]disk1269@gmail.com, [b]ruchikapande99@gmail.com, [c]akhilshaji2610@gmail.com, [d]shweta30patil1999@gmail.com, [e]radhikavikaskulkarni@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: The act of maintaining educational records both online and on paper have become a norm. With the enforcement of lockdowns due to the Covid-19 pandemic, the education sector attempted to move their entire operations online. However with this move, various operations such as Verification of Documents, Approval of LORs have become harder to deal with in a legitimate manner. In this paper, we have compared various existing methods to deal with the problem at hand and proposed our system for the same.

Keywords: Blockchain, Education, Smart Contracts, Document Verification, File, Assignment, IPFS

1. Introduction

In general, educational institutions such as schools and colleges etc. are tasked with the tiresome paperwork in areas such as : (1) documentation of student achievements, (2) approval of official documents, (3) student performance assessment. Certificates are exceptionally regarded as they serve as a marker of the human capital. Here, the human capital means the knowledge, the skills that are possessed by a person through education. Academic qualifications not only reflect the knowledge, skills and expertise of any person but also the person's dedication, abilities and reliability. Due to the importance of these certificates, people often lie about their achievements.

In the current system, the verification of such files is manual and information is brought and confirmation is done from a centralized server. It requires a lot of endeavors to keep a centralised server and at the time of verification, the server may get inaccessible. In this way, depending on a centralized server for documents such as certificates, marksheets, etc doesn't ensure accessibility and uprightness. The existing combination of pen and paper based and online storage based systems makes the data vulnerable to hacking, equipment failures and natural disasters, data redundancy etc.

Further, errors caused due to human negligence add to the problem at hand. Blockchain fixes the problem of identifying the authenticity of the documents. Information on when and by whom the records are added is completely open. Certificates that are stored on the Blockchain will allow learners to get fast and convenient access to their records and share this information with the recruiting employers. Blockchain systems prevent the dispersal of patent resources across the Internet. It further allows learners to get access to study materials and share their projects and ideas. Application of various methodologies studied can be used to build a robust all-inclusive portal which facilitates easy operability for all the entities involved in educational institutions.

To reduce the education sector's load pertaining to documentation, Blockchain can be leveraged to transform activities and protocols involved in the daily operability of the institutions into reliable software. Blockchain domain has seen promising research in various other domains such as cryptocurrency, finance, insurance, copyright protection etc. Blockchain provides an immutable, tamper-proof mechanism for efficient handling of student records. This ensures documents and their various versions are recorded to avoid data inconsistency. Furthermore, Blockchain coupled with business level logic, brings Smart Contracts to the fore.

Smart Contracts are computer protocols which operate to enforce a physical routine or a set of activities. It consists of software that is created for the sole purpose of auditing and enforcing a said protocol within a private network. It eliminates the need for a human entity or a third party to verify the validity of the activity. For example, if a student wishes to get approval of concerned authorities for a document, Smart Contracts ensure the document is approved by the authentic authority within a particular time frame and in a particular manner. This saves the student time spent in physically approaching all authorities. It also prevents fraudulent approvals, thereby guaranteeing the legitimacy of the document. Such a software also benefits educators in a way that they can assign and evaluate assignments effectively. One such platform to write and deploy contracts on a blockchain is Solidity.

This paper aims to explore the various ways to upload and verify educational documents on a decentralised system.

2. Background

Blockchain

Figuratively and logically, the Blockchain technology corresponds to a chain of blocks, known as nodes [1]. The basic idea behind the utility of blockchain is to perform tamper proof operations. This is very well facilitated by various security mechanisms adopted by Blockchain such as Public-Private key encryption, hashing algorithms such as the SHA-256 used by ethereum, mining and consensus algorithms such as proof of work and proof of concept.

Blockchain today finds its place among the front line of various cutting edge technologies and security protocols thanks to its tamper-less capabilities.

IPFS

IPFS is the abbreviation for **InterPlanetary File System**, IPFS holds its key principles in the fields of distributed file storage on a decentralized network, providing tamper-proof authentication and transfer of files. IPFS holds immense value for storage and authentication of data over a blockchain based content sharing and storing platform. Each content is stored in forms of hashes and addresses, which are held secured and tamper proof. Furthermore, every copy of the file that's retrieved is further verified with the requested hash to provide further authentication and authorization is carried out using public keys sets of the author[2].

Hashing

Hashing is one of the finest and oldest encryption techniques used, it forms the backbone of blockchain and IPFS, hash functions are essentially mathematical functions which generate fixed length output to a particular input, for the same given input the output never varies, which makes hashing a key ingredient in authorization and verification algorithms.

SHA-256 is the hashing algorithm which is widely followed in the realm of cyber-security, SHA-256 being more stable than SHA-512 makes it a better algorithm of choice when it comes to complex mining and consensus algorithms on the Blockchain[3].

3. Related Work

In recent times, the rise in the data breaches has escalated suspicion on mediators. Blockchain technology has become an effective solution in addressing this issue. In this, the transaction of any commodity is verified by miners who are real participants of the system [4]. Due to decentralised and tamper-proof nature of Blockchain, it is applied in different fields like healthcare, banking services, supply-chain management etc.

Several schemes have been proposed in the field of digital copyright. In [5], the researchers propose a system which tracks the records of the file by adopting non-repudiation of blockchain. In the field of healthcare, a proposed system solves the problem of data breach of health records. In a system, the author presents a blockchain and IoT based system for diabetic patients. It monitors the patient remotely and warns about the potentially threatening situations. In the power energy field, the researchers suggest a blockchain based solution to strengthen the protection of energy data against cyber-attacks [6-7]. Blockchain technology can also be applied in transport and supply chain management [8].

Research has been carried out in using blockchain technology in the education field and some organizations have begun to apply this technology.

Hongzhi Li, Dezhi Han proposes a system in which the blockchain is used for security and safety of data storage whereas smart contracts are used to keep track of the process of file sharing and file storage. Basically, to store the original documents, off-chain storage servers are used. The documents are first encrypted and then stored on the servers. The hash of the documents are put on the blockchain. The off-chain data is secured by checking the hash information of the records on the blockchain periodically.

Guiyan Wang et al. [9] presents a system which combines three types of blockchains for educational purposes. The private data of the students get stored on the private blockchain which is deployed by each institution. The important documents of the students which are required by the recruiters are uploaded on the consortium blockchain. To guarantee safety, the commitment of all the information in the consortium blockchain ought to be focused on the public blockchain intermittently.

Ujjal Marjit and Prabhakar Kumar [10] propose an Ethereum blockchain based framework to reduce the problem of single point of failure in Open Education Resources (OER) systems. IPFS is used for storing the hypermedia. Smart contracts interact with the stakeholders of the open education resource system.

The research community in the Blockchain domain has focused on various aspects like access control, trusted system, privacy safeguarding systems, data breach tracker etc. Considering these various aspects we propose the Blockchain based educational system Edublocks. Below we have summarized research studies that have used blockchain and discuss their relationship with our work.

Access control : The research work in [11] describes the use of blockchain as a role based authentication system. The health record system proposed in [12] implements access control for health records across different hospitals with the help of public blockchain. The proposed Edublocks system provides access control for various functions of the system like verifying the documents, viewing the documents etc .

Trusted system : The lawful part of utilizing blockchain as an authentic source is additionally expanded by common consent as mentioned in [13]. These works portray utilizing information put on the public blockchain as an unquestionable proof in a courtroom. Namecoin framework [14] utilizes blockchain innovation as a trusted source for the Domain Name System (DNS). The current work uses blockchain as a trusted source thereby eliminating the third party for document verification.

Privacy safeguarding systems : For key management services, the DESCENT system [15] utilizes blockchain along with the smart contracts. It elaborates the idea of sharing the secret keys in the public environment. For the protection of sensitive data, secret sharing techniques are further explained in [16]. In comparison to these techniques, the presented Edublocks system uses encryption techniques to preserve the privacy of the information that is stored on the blockchain.

Data breach tracker : Utilizing the blockchain as a data breach tracker was first described by the Project Provenance [17]. Bitcoin is used as a data provenance framework for research scenarios and is additionally explored in [18]. The study proposes a system which comes up with a data provenance framework that uses blockchain. The user events are recorded and put up on the blockchain transactions. An external entity called auditor verifies these transactions. Transaction receipts are generated using Tieron API. After the data is logged on the blockchain, the system verifies the changes. The proposed Edublocks system follows the similar process to track the data breach.

The work presented in this aims to make use of the blockchain technology to attain breakthroughs in the education system which provides unmediated document verification and its secure storage, an interface for the recruiter for certificate verification and a decentralized platform for assignment submissions and correction, offering incentive based rewards for students for mining.

4. Proposed Methodology

Blockchain has been the flag-bearer when it comes to matters to authentication and retaining integrity of intellectual property rights, leveraging this into something as grass-root as the educational system further reassures organized community well-being in the long run.

The proposed project architecture aims at facilitating a decentralized alternative to carry out two major functionalities:

(a) Decentralized-Documentation authorization for Students, and a direct portal for verification for third-party institutions.

(b) A Decentralized assignment submissions and authorization portal with plagiarism checker.

Each student and faculty would be provided with login credentials which are heavily encrypted, to avoid any malpractice over the network. Initial verification of documents is to be carried out by the Educational Institution, after which a copy of the documents is stored using IPFS, the hash of the file is furthermore put up on the distributed ledger to further concur to transparency and immutability. Figure 1 depicts a system architecture of the proposed Edublocks system:

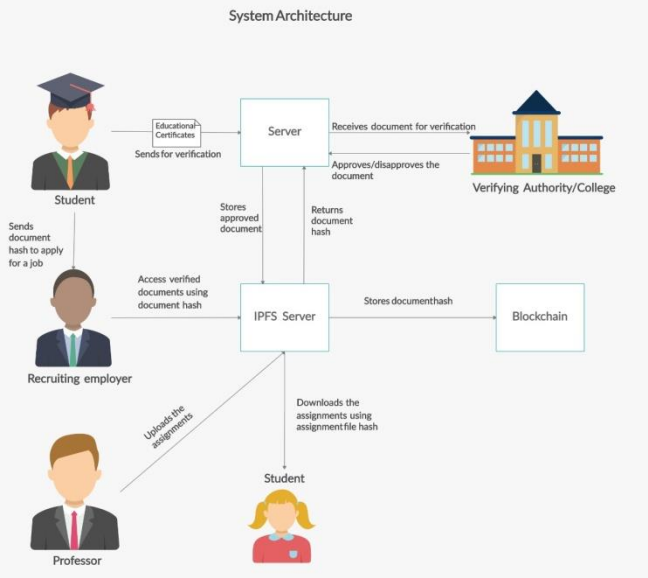

Figure 1 : Edublocks System Architecture

Whenever a third-party such as a company coming over campus wishes to verify credentials of the candidate, all they need to do is demand the hash, and the submitted files by the candidate are directly verified from the IPFS and the previously calculated cryptographic hash function.

Another eminent functionality offered by the system is verification and authentication of genuine LORs and Research internships offered by the campus. The system also aims at acting as a decentralized-tamperproof interface for assignment submission.

The dynamic aspect of the system is shown in Figure 2 with the help of an activity diagram:

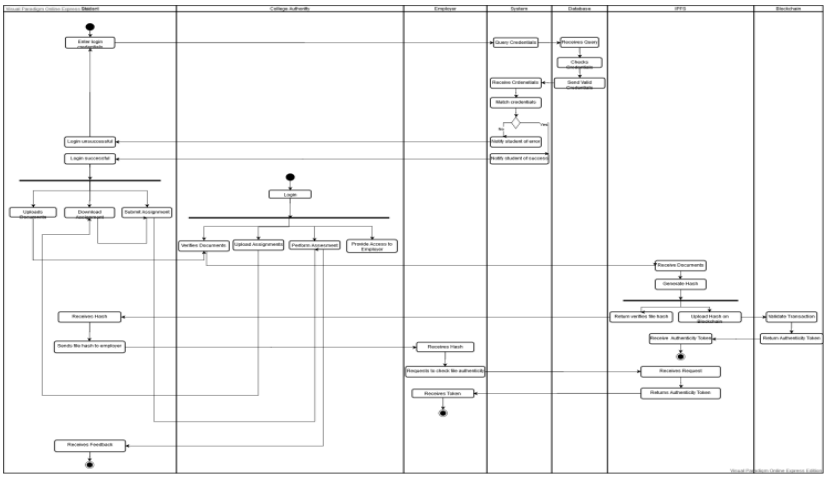

Figure 2 : Activity Diagram

The scope of the proposed system is to give a simple and attractive application to minimize the risks involved with carrying documents, physically everywhere to verify the documents. In this application, the student uploads the document that needs to be verified. The college authority verifies this document and uploads the file on the IPFS. IPFS then converts this file into small encrypted blocks and creates a hash out of it. Now this document can stay on a distributed network and can be retrieved by using the assigned Public Private Key (PPK) combination. Additional functionality of the system is that it provides a decentralized interface for assignment upload and submission to prevent problems such as single point of failure that are present in the centralized system. Thus, we aim to build a system which works in a decentralized fashion to offer more systematic and efficient way of operations in educational institutions. The entire Blockchain and its associated ledger is to be implemented on a private chain, such as Hyperledger Fabric to ensure there is no flaw in the consensus and incentivisation algorithms, where in which majority of students would tend to manipulate majority of consensus, hence leading to a tampered chain of blocks.

5. Conclusion

With the recent out-burst in scams relating to the educational industry and fake-certificates being easily available at one's perusal, the situation calls for a thorough introspection into the current working of educational institutes and hiring practises throughout institutions world-wide. A tamper-proof system is the need of the hour, and Blockchain could be the flag-bearer in that common direction.

Getting the whole system decentralized would further instantiate trust and integrity corresponding to educational institutions, hence catering to a more socially-aware and legitimate social sphere. In the future work, we plan to further focus on new application use cases like institutional purchase record keeping, financial record keeping, dead-stock management etc using blockchain in education.

References

1. B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain A Beginner's Guide to Building Blockchain Solutions*. Berkeley, CA: Apress, 2018.
2. "Hashing", Docs.ipfs.io, 2021. [Online]. Available: https://docs.ipfs.io/guides/concepts/hashes/. [Accessed: 10- Feb- 2021].
3. I. Giechaskiel, C. Cremers and K. Rasmussen, "When the Crypto in Cryptocurrencies Breaks: Bitcoin Security under Broken Primitives", IEEE Security & Privacy, vol. 16, no. 4, pp. 46-56, 2018. Available: 10.1109/msp.2018.3111253.
4. W. Liang, Y. Fan, K. Li, D. Zhang and J. Gaudiot, "Secure Data Storage and Recovery in Industrial Blockchain Network Environments", *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6543-6552, 2020. Available: 10.1109/tii.2020.2966069.
5. B. Zhao et al., "Y-DWMS: A Digital Watermark Management System Based on Smart Contracts", Sensors, vol. 19, no. 14, p. 3091, 2019. Available: 10.3390/s19143091.
6. C. Pop et al., "Blockchain-Based Scalable and Tamper-Evident Solution for Registering Energy Data", *Sensors*, vol. 19, no. 14, p. 3033, 2019. Available: 10.3390/s19143033.
7. G. Liang, S. Weller, F. Luo, J. Zhao and Z. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks", *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162-3173, 2019. Available: 10.1109/tsg.2018.2819663.
8. M. Kim et al., "A Secure Charging System for Electric Vehicles Based on Blockchain", *Sensors*, vol. 19, no. 13, p. 3028, 2019. Available: 10.3390/s19133028.
9. G. Wang, H. Zhang, B. Xiao, Y.-C. Chung, and W. Cai, "EduBloud: A Blockchain-based Education Cloud," *2019 Computing, Communications and IoT Applications (ComComAp)*, 2019.
10. U. Marjit and P. Kumar, "Towards a Decentralized and Distributed Framework for Open Educational Resources based on IPFS and Blockchain," *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 2020.
11. "The Bitcoin Network as a Platform for Trans-Organizational ..." [Online]. Available: https://www.researchgate.net/publication/317060932_The_Bitcoin_Network_as_Platform_for_Trans-Organizational_Attribute_Authentication. [Accessed: 11-Feb-2021].
12. A. Ekblaw and A. Azaria, "MedRec: Medical Data Management on the Blockchain · Viral Communications," *Viral Communications*, 11-Apr-2016. [Online]. Available: https://viral.media.mit.edu/pub/medrec. [Accessed: 11-Feb-2021].
13. D. Bollier , "Reinventing Law for the Commons memo." [Online]. Available: https://www.boell.de/sites/default/files/reinventing_law_for_the_commons_memo.pdf. [Accessed: 11-Feb-2021].
14. V. Durham., "Namecoin", Namecoin.org, 2010. [Online]. Available: https://www.namecoin.org/. [Accessed: 11- Feb- 2021].

15. P. Linder, "DECENT- A Practical Alternative to Government Backdoors," 2016. [Online]. Available: https://eprint.iacr.org/2016/245.pdf. [Accessed: 11-Feb-2021].

16. P. Laud, A. Pankova, and R. Jagomägis, "Preprocessing Based Verification of Multiparty Protocols with Honest Majority," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 23–76, 2017.

17. "Blockchain: the solution for supply chain transparency," *Provenance*, 21-Nov-2015. [Online]. Available: https://www.provenance.org/whitepaper. [Accessed: 11-Feb-2021].

18. "Better with bitcoin," The Economist, 2016. [Online]. Available: https://www.economist.com/science-and-technology/2016/05/21/better-with-bitcoin. [Accessed: 11-Feb-2021].