A Blockchain application for Verification of Academic Information

[1]V. Sairadhesh, [2]B. Uday Kumar, [3]H. Sairam, [4]CH. NEpholarsingh
Guide: Ms. Femimol R

Dept of computer science and Engineering
Bharath Institute of Higher Education and Research

Abstract- **Blockchain technologies are awakening in recent years the interest of different actors in various sectors and, among them, the education field, which is studying the application of these technologies to improve information traceability, accountability, and integrity, while guaranteeing its privacy, transparency, robustness, trustworthiness, and authenticity. Different interesting proposals and projects were launched and are currently being developed. Nevertheless, there are still issues not adequately addressed, such as scalability, privacy, and compliance with international regulations such as the General Data Protection Regulation in Europe. This paper analyzes the application of blockchain technologies and related challenges to issue and verify educational data and proposes an innovative solution to tackle them. The proposed model supports the issuance, storage, and verification of different types of academic information, both formal and informal, and complies with applicable regulations, protecting the privacy of users' personal data. This proposal also addresses the scalability challenges and paves the way for a global academic certification system.**

Objective:
This research proposes a novel and innovative solution to issue, store, recover, share, and verify heterogeneous and unrestricted types of academic information using blockchain. The system also contemplates that if for any reason, the academic institution disappears, under certain conditions, the issued academic accreditations could still be verified and even recovered by the holder

APPLICATION
This evaluation record is based totally on diverse stressed out and wi-fi applications used to alert humans to animal assaults.
A trap camera is an image sensor that is widely used for biodiversity monitoring, species reputation and tracking natural lifestyles.

INTRODUCTION:
The process of issuing and registering academic data is presently a process carried out within each educational institution's proprietary systems and largely isolated from other organizations' record-keeping procedures. This situation impacts directly the verification of students' educational data since, in many cases, the authentication of a transcript or certificate can only be performed manually, which is very costly in resources and time Moreover, if a presently active institution discontinues its educational activities and disappears, all its educational data will probably vanish and the traceability between alumni and their original completed studies will be lost, which, in turn, prevents the verification of such studies by a third party. A trustful blockchain-based system can be a solution for these issues since it can tamperproof registered er academic information to be easily verified by third parties.

LITERATURE SURVEY
Blockchain-Based solution for COVID-19 Digital Medicsl Passports and immunity certificates COVID-19 has emerged as a highly contagious disease which has caused a devastating impact across the world with a very large number of infections and deaths. Timely and accurate testing is paramount to an effective response to this pandemic as it helps identify infections and therefore mitigate (isolate/cure) them. In this paper, we investigate this challenge and contribute by presenting a blockchain-based solution that incorporates self-sovereign identity, re-encryption proxies, and decentralized storage, such as the interplanetary file systems (IPFS). Our solution implements digital medical passports (DMP) and immunity certificates for COVID-19 test-takers. We present smart contracts based on the Ethereum blockchain written and tested successfully to maintain a digital medical identity for test-takers that help in a prompt trusted response directly by the relevant medical authorities. We reduce the response time of the medical facilities, alleviate the spread of false information by using immutable trusted blockchain, and curb the spread of the disease through DMP. We present a detailed description of the system design, development, and evaluation (cost and security analysis) for the proposed solution. Since our code leverages the use of the on-chain events, the cost of our design is almost negligible.
Verfication and validation of Certificate Using Blockchain
According to the Indian Ministry of Education statistics, document verification is a complex domain that involves various challenging and tedious processes to authenticate. Due to the lack of an effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed.In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillful generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. In order to solve the problem of counterfeiting certificates,the digital certificate system based on blockchain technology would be proposed. By the modifiable

property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate a in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile, calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. In this research, the authors have identified the security themes required for document verification in the blockchain.This research also identifies the gaps and loopholes in the current blockchain-based educational certificate verification. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries.

Blockchain Based Framework For Educational certificates Verification

Document verification is a complex domain that involves various challenging and tedious processes to authenticate. Moreover various types of documents for instance banking documents, government documents, transaction documents, educational certificates etc. might involve customized verification and authentication practices. The content for each type vary significantly, hence requires to be dealt in a distinct manner. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skilfully generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, credibility of both the document holder and the issuing authority is jeopardized. Blockchain technology has recently emerged as a potential mean for authenticating the document verification process and a significant tool to combat document fraud and misuse. This research aimed to enhance the document verification process using blockchain technology. In this research, authors have identified the security themes required for document verification in the blockchain. This research also identifies the gaps and loopholes in the current blockchain based educational certificate verification solutions. At the end, a blockchain based framework for verifying educational certificates focusing on themes including authentication, authorization, confidentiality, privacy and ownership is proposed using the Hyperledger Fabric Framework.

EXISTING SYSTEM:

The process of issuing and registering academic data is presently a process carried out within each educational institution's proprietary systems the authentication of a transcript or certificate can only be performed manually , which is very costly in resources and time.

This has to be done by using the centralized approach by using the databases. In this existing system academic verification is done manually which is a lot of time and cost consuming and less trustworthy

DIS-ADAVANTAGES

By the centralized system attacks easily can be done and tampering of certificates also very easy . Some to name like,

(1) "degree mills" that generate fake qualifications that are sold to customers
(2) fabricated documents that are generated by inexistent academic institutions
(3) modified documents that alter authentic documents with false dates ,courses , specializations.
(4) "in-house"-produced certificates, which are fake academic records created by a real institution and printed and sealed.

PROPOSED SYSTEM

- This proposed model proposes innovative solutions to issue, store, recover, and verify heterogeneous types of academic information using blockchain, a technology whose characteristics of resistance to unauthorized modifications and traceability of the operations carried out make it perfect to achieve the pursued objectives.
- Before, Blockchain there used to be many problems related to data Integrity, scalability, availability and security. Blockchain has solved those problems efficiently.
- Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum, and its own programming language, called Solidity. As a blockchain network, Ethereum is a decentralized public ledger for verifying and recording transactions.
- In the proposed Architecture for Certificate verification, there are three stakeholders Students, University, and Company. In the proposed framework we use ganache for the local Ethereum test network. To connect with every stakeholder must have a Metamask (provider) account Each stakeholder has to register to the network with the Metamask account respective to their position as a university, company, or student. For Students to register, each student will be provided with a unique ID through a unique ID student has to register to the respective university.
- Every University will issue certificates to the students in the university with the unique certificate id by the student Meta mask wallet address. This Certificate will be pushed to the network with the parameters certificate id, accessed by, IPFS value, Merklee hash value, etc..,
- And, Each student has an option to request the certificate of their university, then the university will give access certificate to the respective student or rejects the certificate e. If access is given, the student has access to download the certificate from the blockchain(IPFS).
- Every Company has an option to post the job with the unique job id, job type, salary, location, etc..,.This information will be pushed to the network using the provider and saves the all the information and creates new variables like who is applied for job, who is not yet verified.
- Every student has option to apply for all the jobs posted by different companies , every student has to apply for a job using a certificate and its certificate id.By applying to a particular job, the sstudent'saddress will be added to the applied list in job's smart

contract. Then this will update the applied persons on the company side , thecompany has an option to verify the ccertificates, which uses ipfs values Merklee hash values to check.

.

DISCUSSION

The proposed framework is designed with the *privacy by design* principle in mind to protect personal data and to comply with the European GDPR, one of the most restrictive regulations insofar privacy is concerned. By using this system, data subject's consent must be explicitly granted and registered as the holder transmits to the institution *E* their blockchain account to be associated with the issued academic information. After the educational data were issued by the institution, the holder of the data has the possibility to allow and later withdraw access to all or only certain data items to any third party just by adding or removing their account (*T*'s) in a smart contract. Everything is trustfully and tamperproof recorded.

CONCLUSION AND FUTURE WORK

None of the initiatives analyzed in which blockchain is presently applied in the world of education complies with the GDPR, registers any type of academic information, or conveniently addresses the scalability problem in case the system is massively adopted and the volume of transactions increases exponentially, which, in turn, limits their global applicability. These challenges are individually addressed by this innovative contribution. The proposed solution allows, on the one hand, to reliably store and make verified by a third party any type of academic record without compromising the privacy of personal data and complying with the requirements of the GDPR. On the other hand, the system layout, based on a set of blockchains, enhances the performance and scalability of the system. Future work already under development is focused on (i) technically prototyping an operational scheme based on this model utilizing currently existing technology, (ii) developing a proof-of-concept implementation system, (iii) validating it with real users, and (iv) measuring and evaluating the outcomes (i.e., among others, average response time and throughput of the system even changing the number of academic information to be recorded, distribution of the submitted queries and transactions).

REFERENCES:

1. Saleh, O.S.; Ghazali, O.; Rana, M.E. Blockchain-based framework for educational certificates verification. J. Crit. Rev. 2020, 7, 79–84. [CrossRef]
2. Muzammil, M. Corrupt schools, corrupt universities: What can be done? Comp. A J. Comp. Int. Educ. 2010, 40, 385–387. [CrossRef]
3. Creating Pathways to Careers in IT. Available online: https://services.google.com/fh/files/misc/it_cert_impactreport_booklet_rgb_digital_version.pdf. (accessed on 16 March 2021).
4. Lyons, T.; Courcelles, L.; Timsit, K. Blockchain, and the GDPR; The European Union Blockchain Observatory and Forum, European Commission: Brussels, Belgium, 2018.
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://www.bitcoin.org/bitcoin.pdf. (accessed on 17 January 2021).
6. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019, 100, 143–174. [CrossRef].
7. Mirabelli, G.; Solina, V. Blockchain and agricultural supply chains traceability: Research trends and future challenges. Procedia Manuf. 2020, 42, 414–421. [CrossRef].
8. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Appl. Sci. 2019, 9, 1736. [CrossRef]
9. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Sicily, Italy, 18–20 June 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2018; pp. 49–56. [CrossRef].