TRUST CENTRIC PRIVACY PRESERVING BLOCKCHAIN BASED DIGITAL CERTIFICATE LOCKER

JAYAPRATHA S1, GOWSALYA A2, RASMI J3, ROSLINA BEGUM R3

Assistant Professor, Department of Computer Science and Engineering,

Sri Bharathi Engineering College for Women, Kaikkurichi, Pudukkottai

Abstract: Millions of students complete their education each year and go on to do higher studies or a corporate job. In this case student credentials are verified through a lengthy document verification process. This results in significant overhead as documents are transferred between institutions for verification. It is a costly, lengthy, and time-consuming procedure as university authorities invest millions of dollars in maintaining the entire process each year. The employer also takes plenty of time to counterfeiting certificates. A fake certificate generated by skilful scammers is always tough to identify and address as the original one. Therefore, there is a crucial need to upgrade the certification and verification process. This project introduced a Block chain based decentralized Student Verification platform that offers an easy way to issue, check, and verify educational certificates. The student's identity and document are both verified by matching the hashes already present in the Block chain. Also, in the proposed method the documents are linked to the student to another layer of verification. The implementation of this proposed platform can be used to issue, receive and verify the student and their certificates.

INTRODUCTION

1.1 Overview
Education verifications are a valuable tool in pre-employment background checks, since they confirm whether or not a candidate has earned the diploma or degree claimed, hence highlighting a candidate's qualifications and possibly revealing information about your candidate's honesty and integrity. An Education Verification search confirms the education degree, training, potential discrepancies before you hire. Sometimes referred to as an Education Background Check or an Education Check, this service is used to confirm educational experience at high schools, universities, colleges. To prevent tampering or reproduction by copier machines, most of the genuine educational institutions if scanned or photocopied, the matter/design would be far different than the original colour. In case of a void feature, the word COPY appears when an attempt is made to copy a degree. This feature will not be seen in the original document. However, if photocopied, the feature appears on duplicate copy.

1.2 Background of the Project
In this modern age, computers have verified the cause of their existence. The advent of computers in our society caused a lot of criticism on the danger it poses on the society. Critics of computer and new techniques express their fear on how computers will displace and replace all human skills thus resulting to mass unemployment. The presence of computer on virtually every field of today's fast life has proved the critic wrong as the invention of computers and new technologies continues to create additional jobs for those who identify themselves with computers and new technologies. This makes computes partner to human beings in any fields of human endeavour. Over the past decades, students' identification and verification has been a major problem in large institutions as documents, certificate and studentship can be forged at a great rate and easy way, using the computer negatively. Forgers fail to know that in this fast-moving world, the computer has equally served as an aid to decision making, verification and authentication.
Decisions are largely based on experience and principle. The value of every degree is the reputation of the institution and the students produced, hence, the greatest obstacle to any academic institution which is dishonesty and forgery has to be balanced with verification and authentication systems and processes.

1.3 Problem Statement
An important step in job recruiting is to go through résumés and job applications and check if they contain incorrect or fraudulent information. In fact, hiring the wrong person can be an expensive torment and may be extremely disruptive. Providentially, verification of the genuineness of a certificate or mark list issued is possible over using a proposed certificate verification system. Thus, most major companies use background checks as part of the standard practice for screening potential employees. Such measure "should be used within every organization that has serious consequences associated with security breaches," and more penetratingly for employees in highly sensitive or trusted

positions. As opposed to a background check, which only looks into a person's past, honesty/integrity tests have been utilized to assist in the hiring process since the middle of the last century. Such assessments are considered hypothetically useful supplements to the standard background check as they help identify and select better workers and accordingly "improve the quality of an organization's overall performance".

1.4 Block chain Technology

Block chain is defined as a ledger of decentralized data that is securely shared. Block chain technology enables a collective group of select participants to share data. With block chain cloud services, transactional data from multiple sources can be easily collected, integrated, and shared. Data is broken up into shared blocks that are chained together with unique identifiers in the form of cryptographic hashes. Block chain provides data integrity with a single source of truth, eliminating data duplication and increasing security..

Decentralized trust:

The key reason that organizations use block chain technology, instead of other data stores, is to provide a guarantee of data integrity without relying on a central authority. This is called decentralized trust through reliable data.

Block chain blocks:

The name block chain comes from the fact that the data is stored in blocks, and each block is connected to the previous block, making up a chainlike structure. With block chain technology, you can only add (append) new blocks to a block chain. You can't modify or delete any block after it gets added to the block chain.

Consensus algorithms:

Algorithms that enforce the rules within a block chain system. Once the participating parties set up rules for the block chain, the consensus algorithm ensures that those rules are followed.

Block chain nodes:

Block chain blocks of data are stored on nodes—the storage units that keep the data in sync or up to date. Any node can quickly determine if any block has changed since it was added. When a new, full node joins the block chain network, it downloads a copy of all the blocks currently on the chain. After the new node synchronizes with the other nodes and has the latest block chain version, it can receive any new blocks, just like other nodes.

There are two main types of block chain nodes:

- Full nodes store a complete copy of the block chain.
- Lightweight nodes only store the most recent blocks, and can request older blocks when users need them.

1.4.1 History of block chain

A protocol similar to block chain was first proposed in a 1982 dissertation by David Chum, an American computer scientist and cryptographer. In 1991, Stuart Haber and W. Scott Sternest worked on furthering the description of a chain of blocks secured through cryptography. From this point on, some individuals began working on developing digital currencies. In 2008, a developer or group of developers working under the pseudonym Satoshi Nanaimo to developed a white paper that established the model for block chain, including the hash method used to timestamp blocks. One year later, in 2009, Satoshi Nanaimo to implement a block chain using the currency Bit coin. To this day, no one knows for sure who Satoshi Nanaimo to really is. Interest in enterprise application of block chain has grown since then as the technology evolved and as block chain-based software and peer-to-peer networks designed for enterprise use came to market .Enterprise leaders started to look more seriously at the technology early on, seeing more and more potential as early as 2014, when block chain , with financial services, life

Education & academia

Education and academia are being disrupted by block chain technology by nature, academic credentials must be universally recognized and verifiable. In both the primary/secondary schooling and university environments, verifying academic credentials remains largely a manual process (heavy on paper documentation and case-by-case checking). Deploying block chain solutions in education could streamline verification procedures, thereby reducing fraudulent claims of unearned educational credits .Sony Global Education, for example, has developed an educational platform in partnership with IBM that uses block chain to secure and share student records. In 2016, Learning Machine collaborated with MIT Media Lab to launch the Blockers toolset, which provides an open infrastructure for academic credentials on the block chain. In 2020, the company was acquired by Hyland Credentials, which provides a block chain-based system for issuing and verifying digital credentials.

3 Modules List
1. Student Verification System Web app
2. Block chain Integration
3. End User Module
4. Provisional Certificate Generator
5. Access Control Policy

4.4 Modules Description
1. Student Verification System Web app
This project designed considering the need of colleges in today's time for end-to-end digitisation. It brings all the stakeholders on a single cloud-based web app platform to provide strong platform-based connectivity for truly digital operations using block chain Technology. Decentralized system with integrated management approach makes is highly relevant for all kinds of colleges and educational organisations.

2. Block chain Integration
This module design and develop a system for dynamic and secure e certificate generation system using smart contracts in a block chain environment.
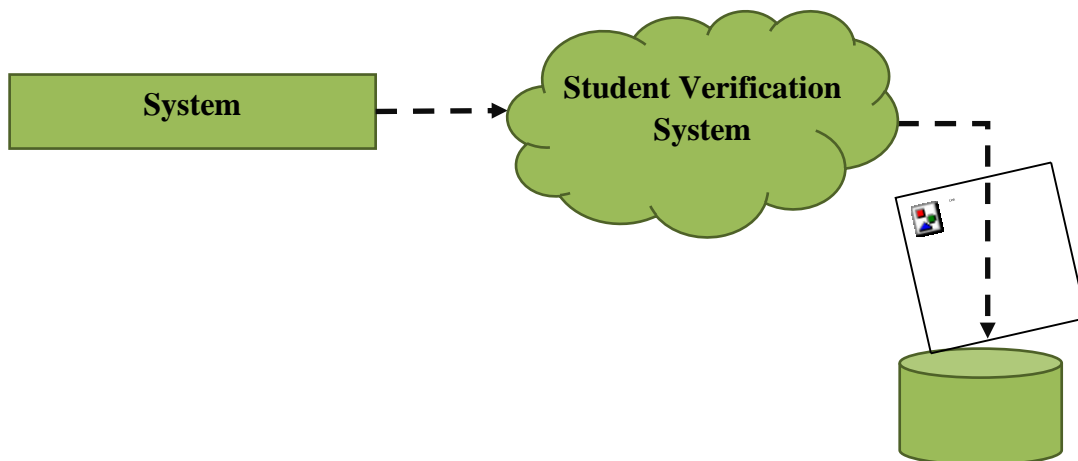

Figure 4.7 block chain integration

Design and integrate own block chain in an open-source environment with a custom mining strategy as well as a smart contract. Finally, validate and explore system performance using a consensus algorithm for proof of validation in show fig 4.7

3. End User Module
3.1 Admin
This module is handled by top management to create role wise user logins to students and staffs accessing Student Verification System. Admin can generate notifications for students and staff; send SMS, emails, reminders time to time.
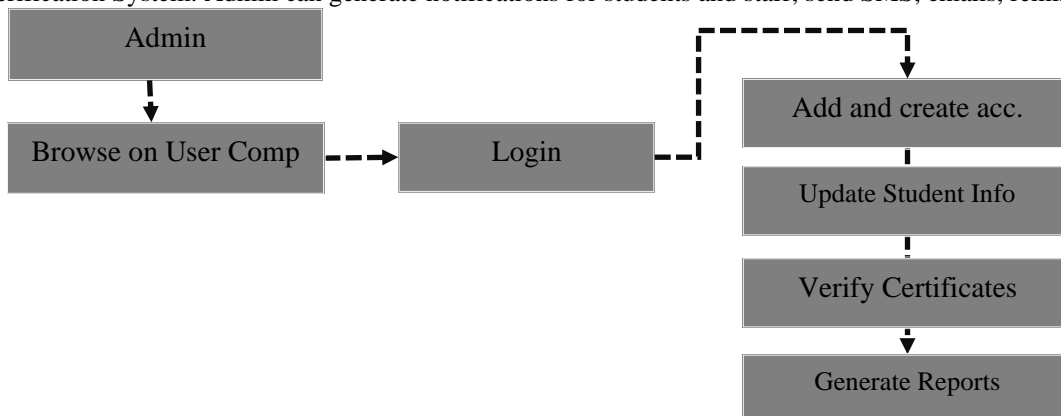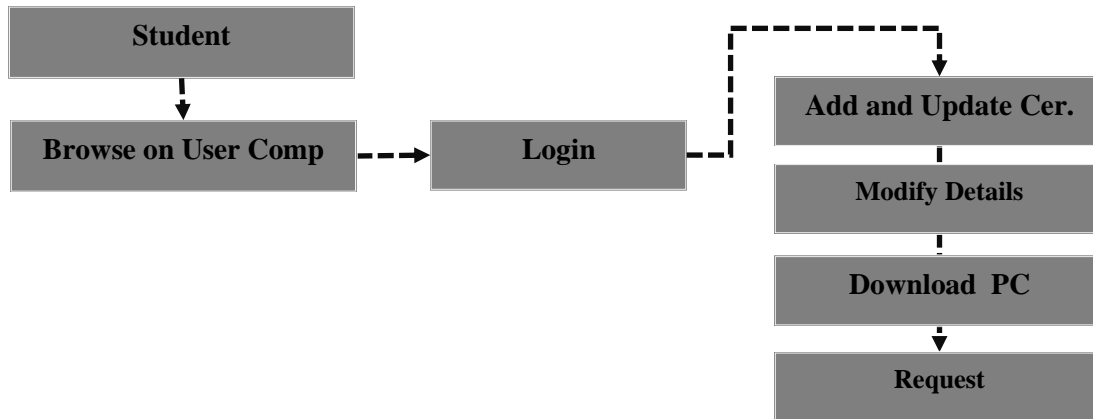

Figure 4.8 admin

Here Admin can add/update/delete student and student education certificates /employee/courses, view course list/student list or many different modules in show fig 4.8

3.2 Student

Here Student can login, view profile, update profile, upload their educational certificates, and download their certificates too.
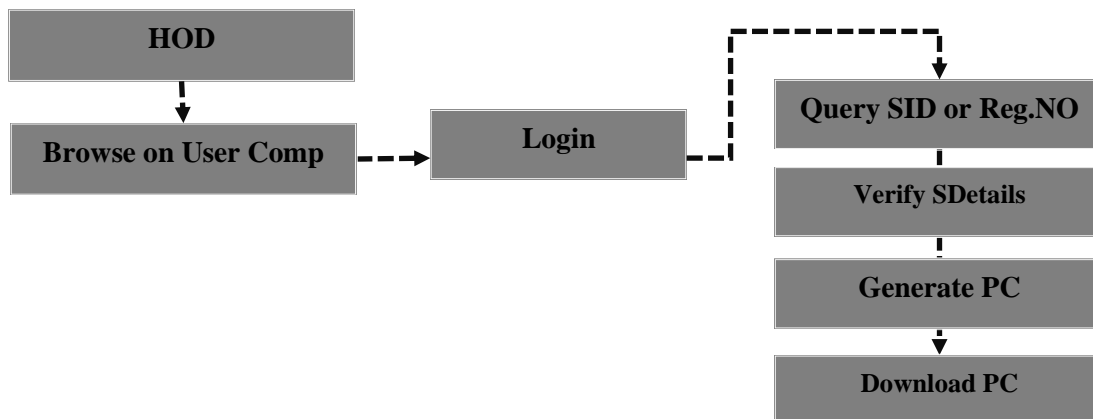

Figure 4.9 students

Student can login, view profile, update profile, upload their educational certificates, and download in show fig 4.9

3.3 Teaching Staff

Faculty/AP/HOD can view profile, here, they will be able to access the information of Students Profile generate and download provisional certificate of the corresponding certificate in show fig 4.10

Figure 4.10 teaching staff

Faculty/AP/HOD can view profile, here, they will be able to access the information of Students Profile generate and download

4. Provisional Certificate Generator

In this module the authorized user verifies the student by searching with registration number or name have entered of a graduate in show fig 4.11
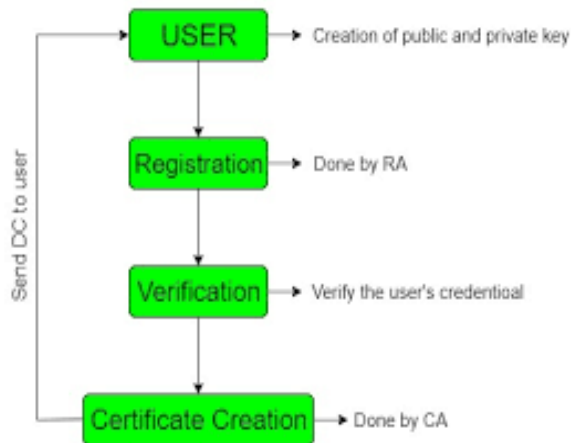
Figure 4.11 certificate generator

after verification the system creates an e-provisional certificate containing a College Emblem and generates a serial number for the Next, the system sends a notification inquiry number to the graduate for future inquires

5. Access   Control Policy

Access control enables you to remotely manage processes, such as adding or revoking user access without requiring any hardware in show fig 4.12
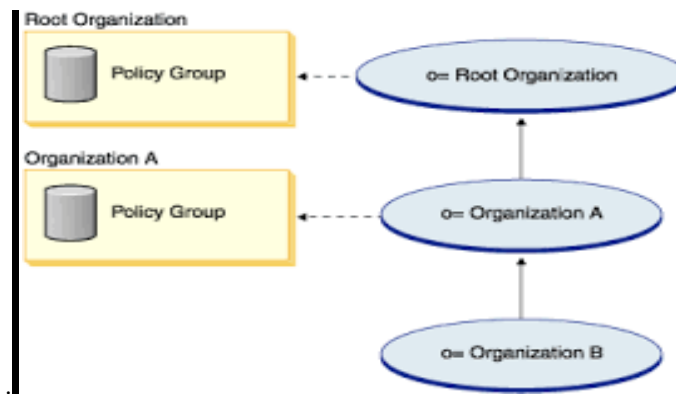

Figure 4.12 control policy

CONCLUSION

The proposed system is a consortium block chain among universities, their affiliated colleges, autonomous colleges, and the companies. Typically, universities first add the students' certificates and subsequently the companies or any other verifier can verify the credentials by using student's registration number or name. The data stored in a block chain will be protected as no one can tamper it or add new transactions to it with a back date. The generated unique ID for each transaction is later used to verify the certificates. This system can be used by all the universities and colleges, in order to provide extra security to the certificates and the students' data. The problem of fake certificates can be eradicated and there will be no question of its validation.

REFERENCES

1. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture Consensus and Future Trends", *2017* IEEE International Congress on Big Data (Big Data Congress), pp. 557-564, 2017.
2. Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, "Blockchain Technology Overview", 2019 National Institute of Standards and Technology Cryptography and Security.
3. A Alammary, S Alhazmi, M Almasri and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review", Applied Sciences, vol. 9, no. 12, pp. 2400, 2019, [online] Available: https://doi.org/10.3390/app9122400.
4. Q. Zheng, Y. Li, P. Chen and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain", 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 704-708, 2018.

5. 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

6. H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme", IEEE Access, vol. 7, pp. 179273-179289, 2019.

7. Emanuel Estrela Bessa and Joberto Martins, "A Blockchain-based Educational Record Repository", 2019 CoRR abs 1904.00315.

8. A. Alkouz, A. HaiYasien, A. Alarabeyyat, K. Samara and M. Al-Saleh, "EPPR: Using Blockchain For Sharing Educational Records" in 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, pp. 234-239, 2019.

9. T. Kanan, A. T. Obaidat and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 629-633, 2019.