Distributed fabric Blockchain-based Academic Certificates

NAVANEETHA KIRSHNAN M, Head of the Department,
Department of Computer Science and Engineering
KRISHNAGANESH SR, Student of Computer Science and Engineering
MARK ANTONY D. A, Student of Computer Science and Engineering
St. Joseph College of Engineering, Sriperumbudur, Chennai.

Abstract:

Block chain innovation (BT) affirms the benefits of belief in the power, cooperation, organization, evidence identification, legitimacy, and transparency. These are strong long-term recommendations on how to verify the authenticity of education certificates because the paper-based certificate is free of fraud and is vulnerable to fraud. This book review began with a collection of peer-reviewed peer-to-peer reviews and a flamboyant framework of articles from various other channels to analyse the latest methods, strategies, and recent command patterns used in block chain development in document validation. from various sectors such as banks, medical records, education system, etc. This paper proposes digital block chain certification based on a system that uses a system to verify identity and time, student space is stored as blocks using block chain technology. Distributed public records with proven and unchanged evidence that preserves the status of the document, creating security for digital assets. This clearly meant that this technology is needed to keep digital assets secure and that anyone can access them without losing data and keep them at a low cost.

KEYWORDS – Block chain, a block chain platform, solutions, and applications for certificate authentications, Challenge.

Introduction:

The internet of the future is blockchain technology. First The blockchain is Bitcoin introduced by Satoshi Nakamoto; Bitcoin came into existence in 2009. Now Bitcoin became very popular. Bitcoin is a plentiful popular digital currency used in peer networks in blockchain cases.

Blockchain technology has its capabilities Distributed, Distributed, Secure and Fast, Clear, and unchangeable. These are more beneficial than the available technology. A linked list such as a data structure that records data and its activities with peers to see the network in public. Each movement of the data is protected by the hashing SHA-256 algorithm and everything a summary of the activity will be collected and stored as blocks of data. Then the blocks are combined with the previous hash value block etc. also protected from tamper penetration.

All this the operation of the blockchain will produce a secure and unchangeable record of transactions that take place across the board P2P network. The huge benefits of the blockchain are empowering many writers' study systems. Can save student information as to qualifications certificates and provider history and address student data on the network. The cryptography feature in blockchain technology keeps data secure with proof of interference which will prevent the attacker from reaching and committing fraud certificates from the blockchain. No one can access and fix its certificates other than those with access rights. So this powerful feature of Blockchain suggests the use of this blockchain technology to ensure quality certificates and student details are not protected. Blockchain establishes a set of compatibility with the same functionality methods using the standard book, smart contract, and cross-chain technology. The method consolidates the data into a stream formed by time, space, and instantaneous multidimensional overlap by editing to be done it is recording, traceable, fragmented, priced, and marketable technical barriers.

Objectives:

- Fake education certificates have been a long-standing issue in the education community. Not until the Massachusetts Institute of Technology Media Lab released its Block-certs project, a process used primarily by combining the hash value of local files in a blockchain but there are still many problems, making the effective method of protection a reality certification and dignity certificates appear
- a series of cryptographic solutions are proposed to solve the above problems, which include, using a multi-sign system to improve certification validation; hard work on a secure withdrawal method to improve the credibility of withdrawal of certificates; to establishing an ID that is a secure organization to verify ownership of the issuing entity

Literature Survey:

A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme. **Author:** Abba Garba; Zhong Chen; Zhi Guan; Gautam Srivastava. Our approach depends upon DNS/DNSSEC infrastructure which requires complex requirements for deployment as well as the adoption rate has been low.

Techniques of Securing Educational Document using Blockchain and IPFS based System. **Author:** Rutuja D. Sanjekar; Balaji M. Patil.

Even if some attacker tries to manipulate the information present in the blockchain the hash value of the block gets changed.

System Design:

Verification Application:

Verification applications are responsible for checking the authenticity and integrity of pre-issued certificates. It covers mainly two components: a web-based application as well client-based application. Verification apps download activities and receive verification details with blockchain API, and then the system verifies authentication of verification details compared to receipt check details.

The main component functions can be described as follows:

- Upload the PDF files / Scan the QR code
- Calculate the hash value for the PDF file
- The client makes a request with the blockchain
- The interaction with blockchain API
- The logic of the verification
- Authentication management: the issuing address.
- The verification of hash value on the certificate (to avoid tampering)
- The verification to confirm if the hash value is in the Merkle tree

Issuing Application

The issuing applications are responsible for the main business logic, which includes the certificates, applying, reviewing, turning over, and issuing.

It merged the hash of the certificate in a Merkle tree and send the Merkle root to the blockchain by APIs.

The main component functions can be described as follows: Login function

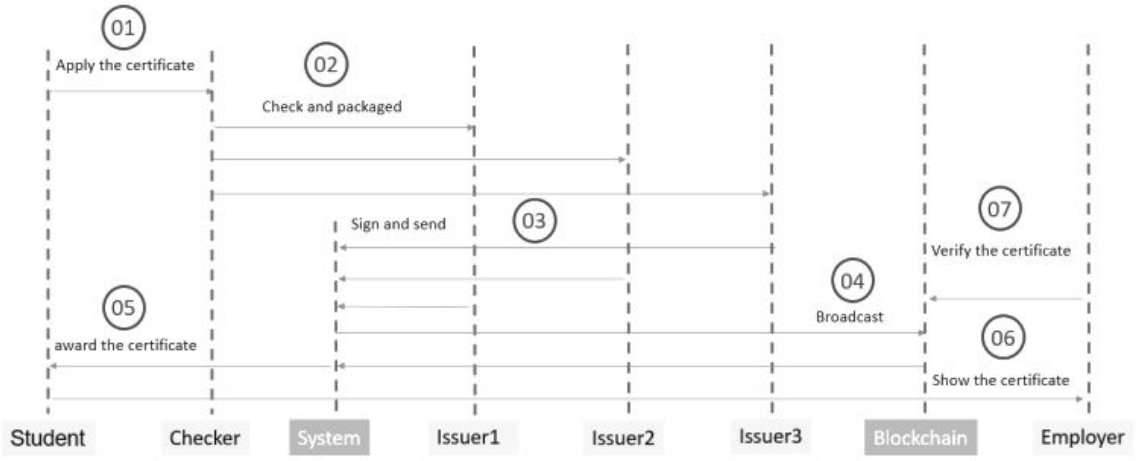
- The security of login
- Reset the forgotten password(option) Privilege control

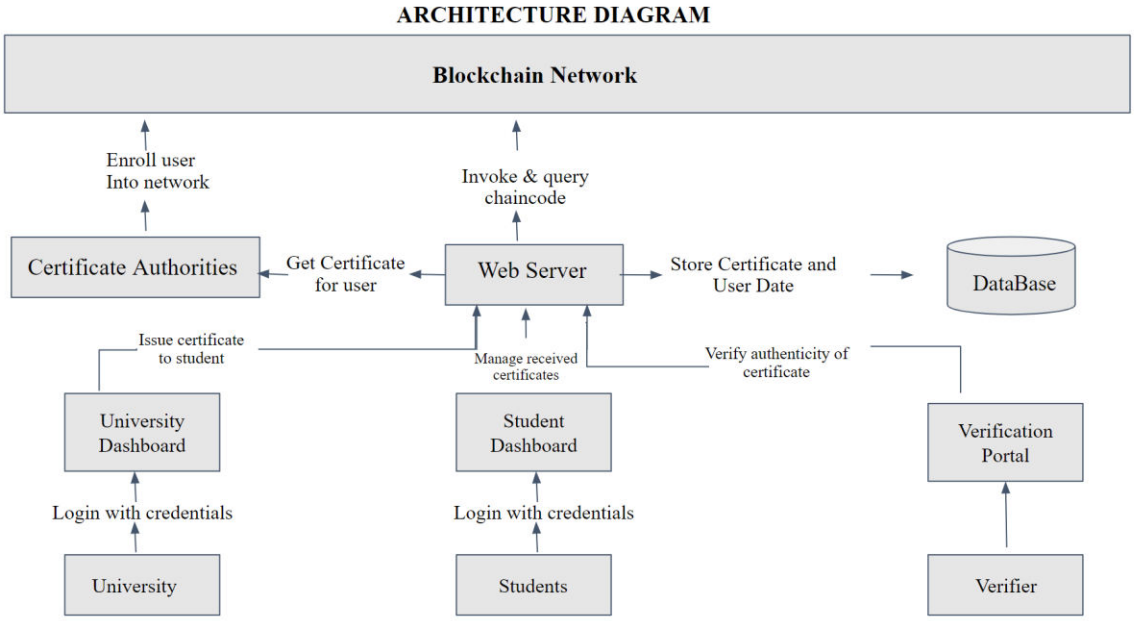
o User role with different privileges o Different pages when changing to different user roles The approval process (student->>checker->>supervisor->>administration staff->>head of school) Multi-signature function Auditing the certificate

o View the published certificate o View the signed certificate o View the certificate ready to sign Revoking the certificate o For one certificate

o For batch certificates Switch different environments (runtime environment/testing environment) Administration page to manage the data, the privilege, and more. Cold storage for the keys (will release in the next version)

Work Flow Diagram





So the complete workflow can able to get the maximum accuracy level of values for the prediction project.

Implementation:

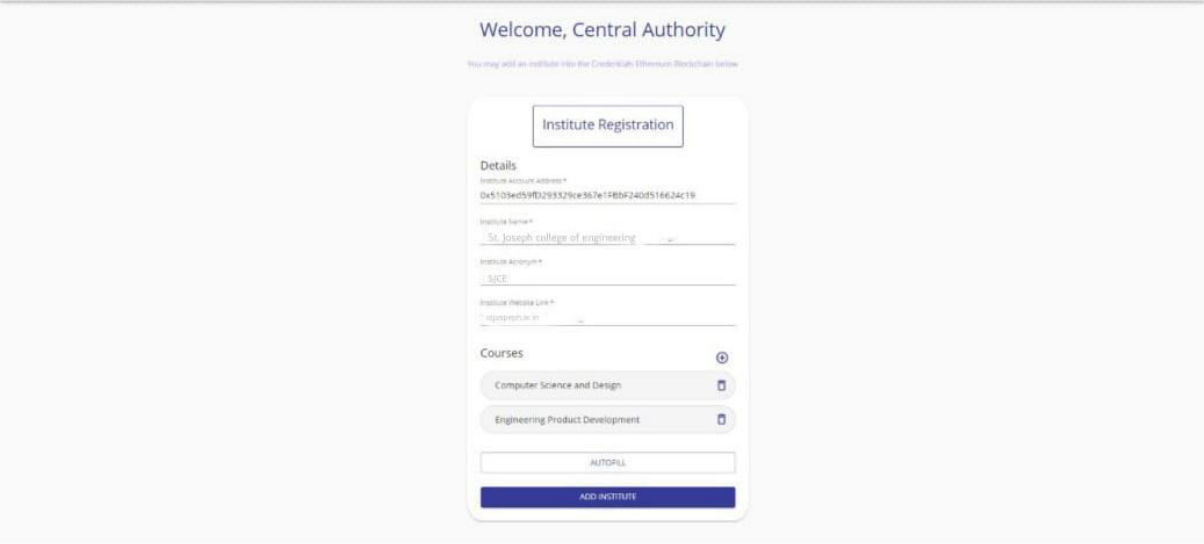
Certification.sol

```
pragma solidity ^0.5.0;
pragma experimental ABIEncoderV2;

import "./Institution.sol";

contract Certification {
    // State Variables
    address public owner;
    Institution public institution;

    // Mappings
    mapping(bytes32 => Certificate) private certificates;

    // Events
    event certificateGenerated(bytes32 _certificateId);
    event certificateRevoked(bytes32 _certificateId);

    constructor(Institution _institution) public {
        owner = msg.sender;
        institution = _institution;
    }

    struct Certificate {
        // Individual Info
        string candidate_name;
        string course_name;
        string creation_date;

        // Institute Info
        string institute_name;
        string institute_acronym;
        string institute_link;

        // Revocation status
        bool revoked;
    }
```

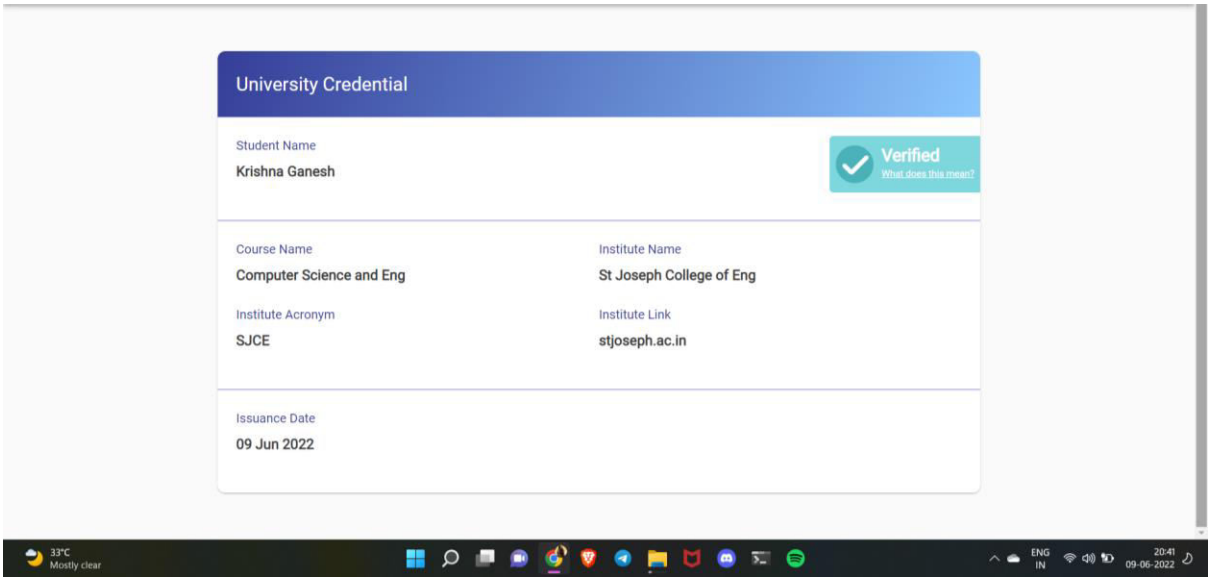
```
    function stringToBytes32(string memory source) private pure returns (bytes32 result) {
        bytes memory tempEmptyStringTest = bytes(source);
        if (tempEmptyStringTest.length == 0) {
            return 0x0;
        }
        assembly {
                result := mload(add(source, 32))
        }
    }

    function generateCertificate(
        string memory _id,
        string memory _candidate_name,
        uint256 _course_index,
        string memory _creation_date) public {
        require(institution.checkInstitutePermission(msg.sender) == true, "Institute account does
not exist");
        bytes32 byte_id = stringToBytes32(_id);
        // require(certificates[byte_id].creation_date == 0, "Certificate with given id already
exists");
        bytes memory tempEmptyStringNameTest = bytes(
            certificates[byte_id].creation_date
        );
        require(
            tempEmptyStringNameTest.length == 0,
            "Certificate with given id already exists"
        );
        (string memory _institute_name, string memory _institute_acronym, string memory
_institute_link, Institution.Course[] memory _institute_courses) =
institution.getInstituteData(msg.sender);
        require(_course_index >= 0 && _course_index < _institute_courses.length, "Invalid
Course index");
        string memory _course_name = _institute_courses[_course_index].course_name;
        bool revocation_status = false;
        certificates[byte_id] = Certificate(_candidate_name, _course_name, _creation_date,
_institute_name, _institute_acronym, _institute_link, revocation_status);
        emit certificateGenerated(byte_id);
    }

    function getData(string memory _id) public view returns(string memory, string memory,
string memory, string memory, string memory, string memory, bool) {
        bytes32 byte_id = stringToBytes32(_id);
        Certificate memory temp = certificates[byte_id];
        // require(certificates[byte_id].creation_date != 0, "Certificate id does not exist!");
```

```
        bytes memory tempEmptyStringNameTest = bytes(
            certificates[byte_id].creation_date
        );
        require(
            tempEmptyStringNameTest.length != 0,
            "Certificate id does not exist"
        );
        return (temp.candidate_name, temp.course_name, temp.creation_date,
temp.institute_name, temp.institute_acronym, temp.institute_link, temp.revoked);
    }

    function revokeCertificate(string memory _id) public {
        require(institution.checkInstitutePermission(msg.sender) == true, "Institute account does
not exist");
        bytes32 byte_id = stringToBytes32(_id);
        bytes memory tempEmptyStringNameTest = bytes(
            certificates[byte_id].creation_date
        );
        require(
            tempEmptyStringNameTest.length != 0,
            "Certificate id does not exist"
        );
        certificates[byte_id].revoked = true;
        emit certificateRevoked(byte_id);
    }
}
```

Certification validation with verifer



To use the front-end application running at http://localhost:3000/, connect to the Localhost Network in metamask.



Conclusion:

Blockchain is one of the most popular and newly developed technologies which can be used sparingly in various fields such as health care, insurance, banks, electronic voting, supply chain management, and certificate verification and digital identity etc. Blockchain is considered a secure, stable technology on networks that are shared publicly and with peers. Blockchain allows you to keep track of the amount of data you have to pay in the construction of a complex network. Most of the papers show the implementation of blockchain technology in an Ethereum blockchain-based education program with coins. This clearly shows the requirement for private blockchain Fabric Hyperledger without a coin to

use the education system to ensure quality certificates. It is a complete source of additional research using this in education. Blockchain is also used to extract large amounts of data internally in education systems, banks, health care systems, provision chain management, and much more applications with security confidence and ease in an open-source book to researchers and analysts

.

Dr.M.Navaneethakrishnan M.E., PhD is a Head of the Department in the Department of Computer Science and Engineering at St. Joseph College of Engineering, Sriperumbudur, Chennai, Tamil Nadu. He has completed his Ph.D, in Cyber Security - Computer Science and Engineering in 2017 from Manonmaniam Sundaranar University (MSU) Tirunelveli, Tamilnadu. He has done his M.E, CSE in Anna University Chennai in the year 2008. Dr.M.Navaneethakrishnan has 15 years of teaching experience and has 58 publications in International Journals and Conferences. His research interests include network security, Computer Networks, data science and Machine Learning. He is an active member of ISTE, CSI, IEANG and IEI

Mr.S.R.KRISHNAGANESH B.E.,Student of Computer Science and Engineering at St.Joseph College of Engineering,Sriperumbudur,Chennai,TamilNadu.I had attended many International Conference, Workshops, Hackathons and Seminars in the area of Blockchain.

Mr.D.A.MARK ANTONY B.E.,Student of Computer Science and Engineering at St.Joseph College of Engineering,Sriperumbudur,Chennai,TamilNadu.I had attended many International Conference, Workshops, Hackathons and Seminars in the area of Blockchain.