

Doqfy: Digital Document Verification using Blockchain and IPFS

Devika Sawant

Information Technology Department
RMD Sinhgad School of Engineering
Pune, India
devikasawant31@gmail.com

Prathamesh Apsingekar

Information Technology Department
RMD Sinhgad School of Engineering
Pune, India
meshpratham.ap25@gmail.com

Vaishnavi More

Information Technology Department
RMD Sinhgad School of Engineering
Pune, India
vaishnaviamore03@gmail.com

Ashutosh Mahadik

Information Technology Department
RMD Sinhgad School of Engineering
Pune, India
mahadiknashutosh@gmail.com

Abstract—Every year, millions of students enroll in Indian higher education institutions, generating numerous certificates such as marksheets, certificates, appreciation cards, and diplomas throughout their academic journey. For admissions or job applications, students are required to submit these documents to institutes or companies. However, manually tracking and validating the authenticity of these certificates becomes a tedious task. In the era of AI tools and smart editing technologies, the risk of modifying scores on scorecards or forging someone else's documents has increased. Manual document verification is not only time-consuming but also incurs paper costs and poses challenges to managing old records. There is a pressing need to address this issue and streamline the document verification process, ensuring confidentiality, reliability, and data availability. This paper suggests creating a verification system based on blockchain technology aimed at preserving data integrity. The system involves three key entities: the student, the university, and the company. The student initiates the verification process by uploading the document, and the university validates it by uploading the original document they possess. If the hash values match, the document is considered verified, and a QR code is embedded for easy sharing and verification status checks by companies. The advantages of such a system include reduced risk for students of losing or damaging certificates and simplified certificate validation procedures. This blockchain-based approach enhances the security, efficiency, and integrity of the document verification process.

Index Terms—blockchain, manual verification, QR code, confidentiality, reliability, data availability

I. INTRODUCTION

In India, the basic cycle of education involves students being promoted to higher classes each year. After completing higher secondary education, students seek admission to junior college. For undergraduate education, there is yet another transition to a different college, and some may pursue postgraduate studies or opt for job placements.

However, a significant challenge arises as students need to present all their certificates at each stage for validation. This manual verification process becomes tedious for validators,

requiring them to meticulously check each document detail against the original copies they maintain. Moreover, this process involves record-keeping and incurs paper costs.

Another concern is the counterfeiting of documents, which is prevalent at a mass level. In India, obtaining a white-collar job without academic credentials is nearly impossible, leading some students with lower scores to resort to illegal means. Various methods are employed, including:

- 1) Degree Mills: Where fake degrees are generated and sold to clients.
- 2) Modified Documents: Involving alterations to original documents, such as changes in name or scores.
- 3) In-House Produced: Involving the creation of fake documents with the assistance of corrupt officials within institutions.

Even if the documents are genuine, the traditional verification process demands the submission of documents to the company, leading to a waste of time for the student, the university, and the company.

To address these challenges and mitigate the issues, blockchain technology emerges as a viable solution. Blockchain ensures data integrity since the information stored in it cannot be altered. With this technology, data validation occurs only when a consensus is reached. Every transaction within the blockchain is interconnected within a chain, guaranteeing that all participants possess the most recent ledger version. The concept of a distributed ledger involves duplicating and storing transactional data across multiple nodes. Because blockchain operates as a peer-to-peer network, there's no reliance on third-party providers for transaction validation.

This approach to record-keeping ensures resistance to tampering, with each peer retaining a complete ledger copy. The incorporation of new transactions necessitates consensus from the majority of peers or compliance with predetermined rules. This transformative approach not only addresses document

verification challenges but also revolutionizes the process. By implementing blockchain in the education system, the need for physical document submission is eliminated. Instead of conventional approaches, academic certificates and accomplishments find secure storage on the blockchain, presenting a decentralized and transparent method for institutions and businesses to authenticate their validity. This not only amplifies security and operational efficiency but also mitigates the hazards associated with manual document management, ensuring a dependable and efficient verification process for all stakeholders engaged.

II. LITERATURE SURVEY

To address issues in the current document verification process, the paper proposes a system that automatically generates and verifies certificates, leveraging decentralized document storage and record-keeping in an immutable distributed ledger such as the Ethereum blockchain given in [1]. This also enhances understanding of blockchain, transactions, and data storage in interconnected blocks. If data in any block changes, its hash is altered, indicating tampering.

Broadly, the system involves three primary stakeholders: students, universities, and companies as found in [2]. This paper introduces a significant role, the owner, responsible for verifying and granting permissions to universities and companies to eliminate fake registrations.

The encryption algorithm used for data is AES, as proposed in [3], which also eliminates reliance on centralized systems for file storage by incorporating decentralized storage, IPFS. However, a drawback is identified: using the 'document hash' as a key, publicly available on the chain, poses challenges in future larger implementations.

The platform SkillCheck, outlined in [4], awards crypto tokens to evaluators, relying entirely on blockchain and employing technologies like Ganache, Truffle, and the Metamask wallet for transactions, simplifying testing. The system efficiently manages a large number of students with minimal teaching staff.

A potential cost concern arises if documents are converted into binary and stored on the blockchain compared to the current centralized system. Paper [5] proposes an alternative, suggesting storing documents in a decentralized manner using IPFS, enhancing data resilience and accessibility by breaking files into smaller chunks distributed across a node network. Each file is referenced using content-based addressing, reducing dependence on servers compared to traditional storage systems.

By combining the insights from all these references, a system can be built that utilizes decentralized storage (IPFS) and the Ethereum blockchain for the verification of document

identity, as detailed in [6].

This paper addresses the problems and drawbacks identified in the previously proposed methodologies

III. PROPOSED METHODOLOGY

A. Modules

- 1) Blockchain: is like a steady digital ledger, forming the heart of the project. It creates a reliable space where all actions are visible and impossible to change.
- 2) Ethereum: is a decentralized blockchain platform enabling smart contracts and decentralized applications (DApps). Smart contracts are self-executing contracts with encoded terms, facilitating trustless and automated transactions on the Ethereum network. Solidity is Ethereum's programming language for creating smart contracts, defining their logic and behavior.
- 3) IPFS: (InterPlanetary File System) is a peer-to-peer protocol designed for decentralized file storage and sharing. It operates on a distributed network, utilizing content-based addressing to locate files efficiently.
- 4) Ganache: is a local blockchain development environment that allows developers to test and deploy Ethereum smart contracts on a personal blockchain. It provides a user-friendly interface for simulating various blockchain scenarios and interactions.
- 5) Truffle: streamlines the compilation, linking, deployment, and binary management of Solidity smart contracts.
- 6) MetaMask: is a popular cryptocurrency wallet and browser extension that enables users to interact with decentralized applications (DApps) on the Ethereum blockchain.
- 7) Ethers.js: is a JavaScript library for Ethereum development, facilitating smart contract interactions and wallet management. It simplifies blockchain transactions, making it popular among developers for building decentralized applications (DApps) with ease and efficiency.
- 8) React: is employed for building the frontend, offering users a seamless experience with features like smooth page switches, fast loading and added features for extra security, compiling and storing HTML pages in the backend without revealing details to users.
- 9) Node.js: is a server-side JavaScript runtime environment that facilitates the execution of JavaScript code outside the browser, enabling efficient and scalable web application development. It is recognized for its non-blocking, event-driven architecture, enhancing the responsiveness of applications.
- 10) MongoDB: is a versatile NoSQL database, storing data in a flexible, document-oriented format. It is favored for its scalability and efficiency in handling diverse data types.

B. Project Description

To address existing flaws in current verification methods, this system introduces an automatic certificate verification

process, complemented by QR codes for seamless sharing and validation. This ensures authenticated, reliable, and unalterable data. The following sections provide an in-depth explanation of the system design and functionality

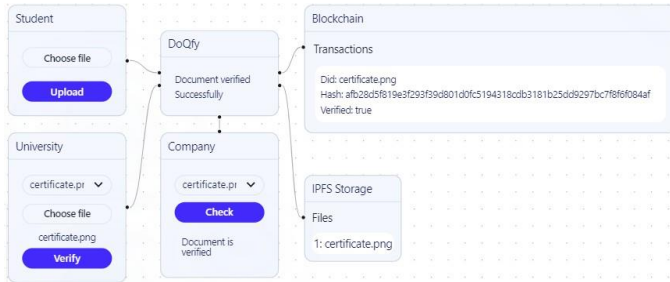


Fig. 1. User Interaction

1) Working: This approach streamlines the verification of document authenticity, guaranteeing both integrity and originality through the utilization of technologies like blockchain and IPFS. The Fig. 1 illustrates how users engage with smart contracts, involving the following participants:

- a) Student: The student initiates the process by selecting their university from a list and uploading the document they wish to verify. Upon completion, the student receives a documentId for reference.
- b) University: The university acts as a Certificate Verifying Authority
 - For former students who are not part of the new system: University officials handle the verification process by selecting the document submitted by the student and uploading the original digital copy they possess. The system verifies the data by matching both documents, ensuring authenticity, and updates the status to verified if data matches.
 - For new students: the university simplifies the process by directly generating verified documents before handing them to students. This eliminates the need for students to undergo additional verification steps.

After verification, an email is sent to the student, including the documentId, hash, and a QR code embedded in the document for easy reference and validation.
- c) Company: Companies, as end-users, play a crucial role in the system. They can access only those documents for which students or universities have granted permission for viewing.
 - They can scan the QR code of the document to obtain details about the document’s originality, integrity, and authenticity.
 - During the hiring process, companies can also upload documents provided by the student to verify their authenticity and check the verification status
- d) Owner: The owner manages the registration of universities and companies to prevent the inclusion of fake entities by verifying their legal government documents.

C. System Design

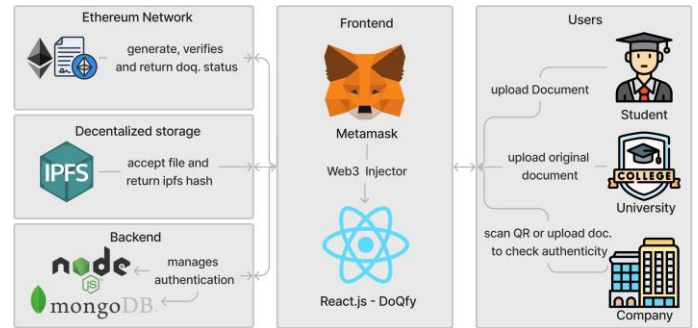


Fig. 2. System Design

Users start by signing up and logging into the website "Do- qfy.". Ethers.js seamlessly connects the site with Metamask and the smart contract, ensuring a smooth integration between the user’s account, their Metamask wallet, and the underlying blockchain-based smart contract functionality.

First student select the university and upload the document that document is send to ipfs through node.js and ipfs return the ipfs hash or cid which is unique for each document then this hash ,student address ,selected university address and documentId generated by system is send to ethereum smart contract function uploadDocument which creates a mapping of document with documentId and stores this information in blockchain.

Second university get request for verification of document then they select the document which they want to verify then upload the original copy of document that they have and click on verify , then again document is send to ipfs, it return the ipfs hash , then this hash and documentId is send to smart contract function verifydocument which checks the hash of student uploaded document and original university document hash if they both match then verification status is updated to true.

Third Company can upload the document uploaded by student and check its authenticity by using the same above process or give unique documentId to check verification status of document, then this id is send to smart contract function checkstatus which returns the document verification status true or false depending upon verified or not.

IV. IMPLEMENTATION DETAILS

The implementation involves key components such as the Ethereum blockchain, IPFS for document storage, smart contract development using Solidity, and interaction with the Ethereum network using tools like Truffle and ethers.js.

A. Smart Contract

A smart contract named DoQfy is deployed on the Ethereum blockchain. The contract contains a struct named Document to represent document details, including owner address, university address, IPFS hash, and verification status. Documents are stored in a mapping named documentsById with unique

document IDs. Events, such as LogPrint, are emitted to signify successful transactions.

```
//SPDX-License-Identifier: MIT
pragma solidity ^0.8.1;
contract DoQfy {
    struct Document {
        address owner;
        address universityAddress;
        string ipfsHash;
        bool verified;
    }
    mapping(string => Document) private
    documentsById;
    event LogPrint(string message);

    function uploadDocument(string memory
    uniqueId, string memory ipfsHash,
    address universityAddress) public {
        Document memory document =
        Document({
            owner: msg.sender,
            universityAddress:
            universityAddress,
            ipfsHash: ipfsHash,
            verified: false
        });
        documentsById[uniqueId]=document;
        emit LogPrint("Document uploaded
        successfully");
    }

    function verifyDocument(string memory
    uniqueId, string memory ipfsHash)
    public{
        Document storage document =
        documentsById[uniqueId];
        require(keccak256(abi.encodePacked
        (document.ipfsHash)) == keccak256
        (abi.encodePacked(ipfsHash)),
        "Fake document");
        document.verified = true;
        emit LogPrint("Document verified
        successfully");
    }

    function checkStatus(string memory
    uniqueId)
    public view returns (bool) {
        Document storage document =
        documentsById[uniqueId];
        return document.verified;
    }
}
```

B. IPFS Integration

The IPFS client is utilized to pin documents on the IPFS network. Files are added to IPFS, and the resulting CID (Content Identifier) or hash is returned.

```
const ipfs = create({
    host: "localhost",
    protocol: "http",
    port: 5001,
});

const result = await ipfs.add(file, {
    pin: true,
});
return result.cid.toString();
```

C. Ethers.js and Contract Interaction

Leveraging the Ethers.js library enables communication with the Ethereum blockchain. A signer is acquired through MetaMask or equivalent providers. The instantiation of the DoQfy smart contract involves supplying the contract address and Application Binary Interface (ABI).

```
const userSigner = new ethers.providers.Web3Provider
(window.ethereum).getSigner();
const smartContract = new ethers.Contract(
    contractAddress, contractAbi, userSigner);
const userAccounts = await window.ethereum.request({
    method: 'eth_requestAccounts' });
const transaction1 = await contract.uploadDocument(
    uniqueId, ipfsHash, universityAddress, { from:
    userAccounts[0] }); await transaction1.wait();
const transaction2 = await contract.verifyDocument(
    uniqueId, ipfsHash, { from: userAccounts[0] });
await transaction2.wait();
const transaction3 = await contract.checkStatus(
    uniqueId, { from: userAccounts[0] }); return
transaction3;
```

D. User Authentication

User registration and login are securely managed using MongoDB and Node.js, providing a robust backend for the DoQfy platform.

This implementation guarantees a secure and scalable document verification system by integrating blockchain and IPFS technologies effectively.

V. RESULTS AND DISCUSSIONS

Following are some of the implementation results:

A. Registration

Users begin by selecting their role and registering using their email and password. Additionally, the Metamask account address is automatically fetched and set during registration

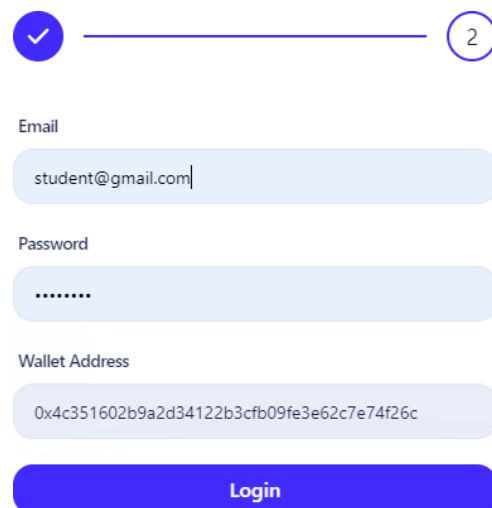


Fig. 3. Registration Page

B. Owner

The owner is responsible for verifying university and company registrations. After successful verification, universities or companies can commence their respective operations.

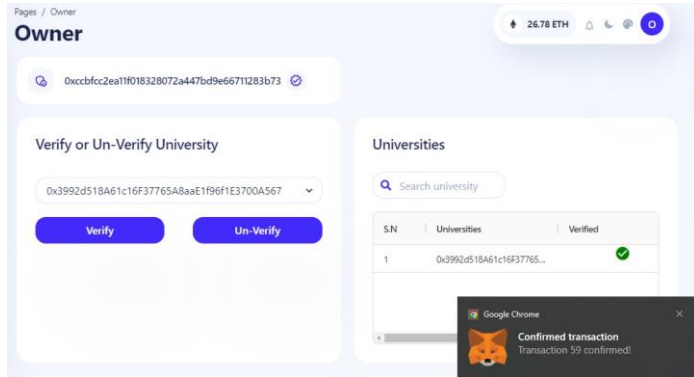


Fig. 4. Owner Page

E. Company

Companies have two options: they can either scan the QR code or upload the document submitted by the student to check the authenticity and verification status of the document.

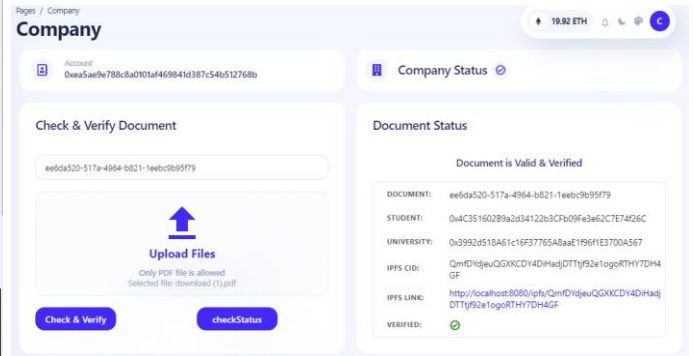


Fig. 7. Company Page

C. Student

Students choose their university, upload the document, and confirm the Metamask transaction from their account. The document is then sent to the university for verification.

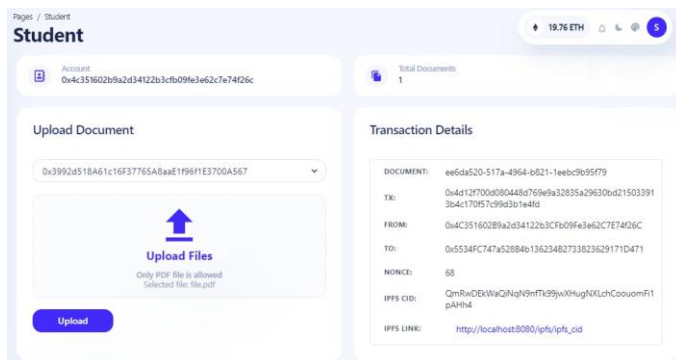


Fig. 5. Student Page

F. Form

The form is a verified document with a QR code embedded on it.

FORM - 3
[rule 4 (1)]

AFFIDAVIT OF CLAIMANT/ PARENT(S)
(Rule 4, Order 18 of the Code of Civil Procedure, 1908)


I, son / daughter of
Shri/Smt. aged years,
occupation residing at village/
Town Tahsil
District State here by Solemnly
affirm as under-

2. I hereby give the genealogy tree of my family and relatives, which is as under: -

3. Other relevant submissions to be made or any essential explanation to be made, in support of Caste /Tribe claim, including the sociology, anthropological and ethnological (anthropological moorings and ethnology kinship), genetical traits, of the Caste/Tribes, if any;

To the best of my knowledge and belief the information given in application FORM - 1 and in this affidavit is based on facts and is correct.

Place: _____
Date: _____
Signature.....
(Name of the applicant/claimant)



8910cd76-84b5-4aa3-8835-3d40e9fbf791

Fig. 8. Form Page

D. University

Universities select the document for verification, upload the original copy, and click "verify." If both documents match, the verification status is set to true.

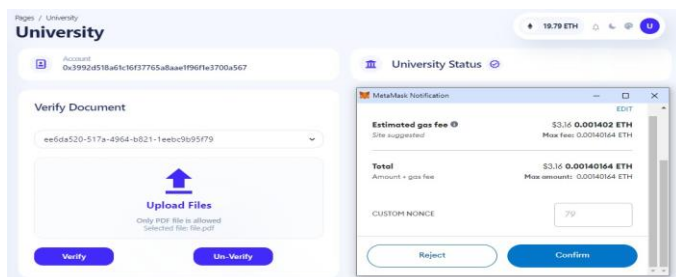


Fig. 6. University Page

G. Gas Usage Metrics

In the Ethereum ecosystem, gas fees are a critical aspect of executing transactions and interacting with smart contracts. Computational effort on the Ethereum network is measured in units referred to as Gas. When users initiate transactions or engage with smart contracts, they must pay a corresponding gas fee, denominated in Ether (ETH), to compensate network miners. This fee varies based on the complexity of the operation and network demand.

TABLE I
UPLOADDOCUMENT GAS COST

Gas Used	Gas Cost	Gas Fee
270035	20 Gwei	0.005401 Eth

In the Ethereum smart contracts context, gas functions as a unit representing the computational resources essential for executing operations. For the 'uploadDocument' function, the gas used is 270,035 units, reflecting the computational effort involved in executing this particular smart contract function. The gas price, set at 20 Gwei (20,000,000,000 wei, a smaller denomination of Ether), determines the cost per unit of gas. The gas limit, also set at 270,035 units, represents the maximum amount of gas allowed for the function. In this case, the gas fee for executing 'uploadDocument' is calculated by multiplying the gas used (270,035) by the gas price (20 Gwei), resulting in a fee of 0.005401 ETH.

TABLE II
VERIFYDOCUMENT GAS COST

Gas Used	Gas Cost	Gas Fee
70082	20 Gwei	0.001402 Eth

Similarly, for the 'verifyDocument' function, the gas used is 70,082 units, reflecting the computational resources expended during execution. The gas price remains at 20 Gwei, and the gas limit is 70,082 units. Consequently, the gas fee for 'verifyDocument' is calculated as the multiplication of the gas (70,082) and the price of gas (20 Gwei), resulting in a fee of 0.001402 ETH. These gas parameters, including gas used, gas price, and gas limit, collectively determine the cost and resource allocation associated with executing specific functions on the Ethereum blockchain

VI. CONCLUSION

The primary advantage of Blockchain lies in its capability to generate immutable records. This feature ensures a transparent and secure system. The system automates certificate generation, reducing manual work for verification. This not only minimizes the risk of students losing certificates but also enhances data security. Hash values of certificates find their storage in the blockchain, while the primary documents are maintained within the InterPlanetary File System (IPFS), ensuring data preservation and transparency.

Traditional document verification for employment is both costly and time-consuming, often relying on third parties. The paper illustrates how blockchain technology eliminates these challenges. Implementing such a system can significantly reduce fraud related to work history, offering a more reliable solution for companies.

ACKNOWLEDGMENT

Academic knowledge is translated into practical solutions with the system "Doqfy: Digital Document Verification Using Blockchain and IPFS." Grateful for the opportunity, we extend our heartfelt thanks to our guide, Ms. Suvarna Potdukhe, whose unwavering motivation and guidance propelled us. Special thanks to Ms. Shweta kale (HOD) for her crucial support in making this paper a reality. Lastly, the paper acknowledges and appreciates the authors of the references and literature that contributed to the project.

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 (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigData-Congress.2017.85.
- [2] J. -C. Cheng, N. -Y. Lee, C. Chi and Y. -H. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.
- [3] A. Singh, S. Chauhan and A. K. Goel, "Blockchain Based Verification of Educational and Professional Certificates," 2023 2nd International Conference on Computational Systems and Communication (ICCS), Thiruvananthapuram, India, 2023, pp. 1-7, doi: 10.1109/ICCS56913.2023.10143008.
- [4] J. Gupta and S. Nath, "SkillCheck: An Incentive-based Certification System using Blockchains," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169457.
- [5] E. Nyalety, R. M. Parizi, Q. Zhang and K. -K. R. Choo, "Block-IPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 18-25, doi: 10.1109/Blockchain.2019.00012.
- [6] G. Malik, K. Parasrampur, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTE-CoN.2019.8899569.
- [7] A. K. Shrivastava, C. Vashisth, A. Rajak and A. K. Tripathi, "A Decentralized Way to Store and Authenticate Educational Documents on Private Blockchain," 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/ICICT46931.2019.8977633.
- [8] M. Z. Chowdhury and Asaduzzaman, "A Blockchain-Based Decentralized Document Authentication System for Multiple Organizations," 2022 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Naya Raipur, India, 2022, pp. 269-274, doi: 10.1109/WIECON-ECE57977.2022.10151411.
- [9] S. Halder, H. A. Kumar, S. Lavu and R. S R, "Digital Degree Issuing and Verification Using Blockchain," 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), Bengaluru, India, 2022, pp. 1-4, doi: 10.1109/CCIP57447.2022.10058644.
- [10] P. Haveri, U. B. Rashmi, D. G. Narayan, K. Nagaratna and K. Shivaraj, "EduBlock: Securing Educational Documents using Blockchain Technology," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225265.