IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Online Document Verification Using Blockchain

[1]Abhijeet Gupta, [2]Chetan Khobragade, [3]Mrudul Gaidhane, [4]Chetan Pawar
[123]Student, [4]Assistant Professor
[1]Electronics and Telecommunication Department,
[1]Pune Institute of Computer Technology, Pune, India

Abstract: The rise of digitalization has resulted in an increase in online transactions, necessitating the need for secure and dependable methods of document verification. Traditional document verification methods frequently involve manual and time-consuming processes that are vulnerable to fraud and error. Blockchain technology, which provides a secure, transparent, and tamper-proof platform for validation, has emerged as a potential solution to this problem in recent years. The use of blockchain for online document verification entails the use of a distributed ledger system that records and validates the authenticity of documents in a decentralized manner. The procedure entails creating a digital fingerprint of the document, which is then stored on the blockchain. The blockchain creates a secure and immutable record of the document, preventing it from being altered or tampered with. The increased security provided by blockchain is one of the primary advantages of using it for online document verification. Because the blockchain is decentralized, there is no single point of failure, making it more resistant to hacking and other types of cyber-attacks. Furthermore, the use of cryptography ensures that the documents are encrypted, which increases their security.

***Index Terms* - Document Verification, De-Centralized System, Ethereum-Based Blockchain Network.**

I. Introduction

Online document verification has become an integral part of many companies and organizations in the modern digital age. From banking firms to healthcare professionals, there is a huge market for reliable and safe methods of checking the legitimacy of digital records. Traditional methods of document verification, on the other hand, are frequently afflicted by problems such as fraud, error, and ineffectiveness. As a consequence, blockchain technology has emerged as a potential remedy for this issue. Blockchain is a distributed ledger and public blockchain system that allows for safe and open transaction capturing and affirmation. Its differentiating characteristics, such as irreversibility, clarity, and decentralization, make it a perfect forum for online document verification. It is now feasible to establish an encrypted and tamper-proof record of documents using blockchain, ensuring their integrity and genuineness. The application of the blockchain for online document verification does have the potential to completely convert how we authenticate and verify documents online. When compared to conventional approaches, it can provide a more effective and cost-effective solution while also increasing security and decreasing the likelihood of fraud and error. As a result, it is not surprising that many companies and institutions are continuing to investigate the use of blockchain for validation, and adaptation is expected to increase over the next few years.

II. Literature Review

The authors proposed a document verification system that uses blockchain technology to ensure the authenticity and integrity of online documents in "An online document verification system using blockchain technology" [1]. The proposed system makes use of a distributed ledger to store hashed documents and digital signatures. The authors also built a system prototype and tested its performance. The authors proposed a blockchain-based system for verifying academic certificates in "A blockchain-based online document verification system for academic certificates" [2]. To ensure the authenticity of academic certificates, the system employs a combination of hash functions and digital signatures. The authors also conducted experiments to assess the system's performance. In "A blockchain-based approach for online document verification" [3], the authors proposed a blockchain-based approach for verifying online documents. The proposed system employs a distributed ledger that stores the hash of the documents and their digital signatures. The authors also evaluated the performance of the system through experiments. The authors proposed a blockchain-based system for verifying online documents for government and business applications in "Blockchain-Based Online Document Verification System for Government and Business Applications" [4]. The system makes use of a distributed ledger to store the hash of the documents as well as their digital signatures. The authors also conducted experiments to assess the system's performance. The authors proposed a document verification system that uses smart contracts and blockchain technology to ensure the authenticity and integrity of online documents in "An Online Document Verification System Using Smart Contracts and Blockchain Technology" [5]. The proposed system makes use of a distributed ledger to store the hashes of the documents as well as their digital signatures. The authors also built a system prototype and tested its performance.

III. Proposed Methodology

3.1 Actors

The intricate system entails three integral components or organizations, namely the originator of the document, the authorizing institution, and affiliated parties, such as a corporation, capable of authenticating the disseminated online document. In the process, the organization furnishes the document to a user, who subsequently permits users to upload it onto a server. Moreover, the verifier, in this instance, the corporation, assumes the responsibility of verifying both the document and the user, thereby ensuring their credibility and authenticity.

3.2 Process – Interaction between actors

The system's actors have clearly defined roles.

- User - The user, being the rightful proprietor of the document, is endowed with the authority to liaise with the verifier on its behalf, thereby facilitating the process of authentication and validation.
- Organization - The organization oversees releasing the document.
- Verifier: Upon examining the document, the verifier possesses the discernment to ascertain its authenticity and subsequently implement the suitable course of action.

Only a select group of validated and sanctioned organizations are granted the privilege to access the chain. These organizations, possessing the requisite authorization, are empowered to transmit the relevant documents and user identification information to a smart contract. Within this mechanism, the verifiers can autonomously authenticate the document at hand, leveraging the public key stipulated by the said organization.

3.3 Registration of the Document

Prior to publishing any papers onto the system, it is a prerequisite that the business serving as the document's issuer undergoes the verification process. Upon successful verification, a public-private key pair is created for this organization, whereby the organization is entrusted with the public key, while the client application designated for the organization stores the private key thus generated. Through the amalgamation of an asymmetric public key cryptography approach, the public-private key pair is fortified.In the event that a user enters into any transaction with the organization, leading to the generation and issuance of a document, the organization undertakes the creation of a digital facsimile of the certificate in the form of a portable document format (PDF).Comprehensively encapsulating the information pertaining to both the issuance of the user and the corresponding company, the certificate assumes a pivotal role in the documentation process. To simplify the process, for the purpose of illustration, let us consider that a document is merely linked to a user id and an organization id. Upon receipt of the aforementioned parameters, the client application, utilizing the private key of the organization, conducts a signature check, prior to proceeding with the transaction. In the event that the signature is established as genuine, a transaction is initiated, aimed at appending the hash onto the Blockchain, leading to the generation of a unique transaction ID. In conjunction with this activity, a compacted digital duplicate of the document, along with the transaction ID, is also furnished to the user, which is preserved by the user in tandem with the digital copy. It is incumbent upon the user to consistently apprise the verifier of this information, whenever transmitting the document.

3.4 Verification of the Document

Upon receipt of the parameters Hi and Ui, the client application located at the verifier end triggers the invocation of a function embedded within the smart contract. In accordance with the process, the verifier transmits the base64-encoded string of the digital document to this function. Subsequently, a comparative analysis is conducted, whereby the hash value Hi obtained from the Blockchain is juxtaposed against the SHA-256 hash generated from the copy of the document. In the event of a match between the aforementioned hashes, the document copy relayed to the verifier is deemed to be legitimate and unaltered. It is important to note that this technique has the capability of detecting even the slightest modification in a digital file, down to a single pixel.

IV. System Architecture

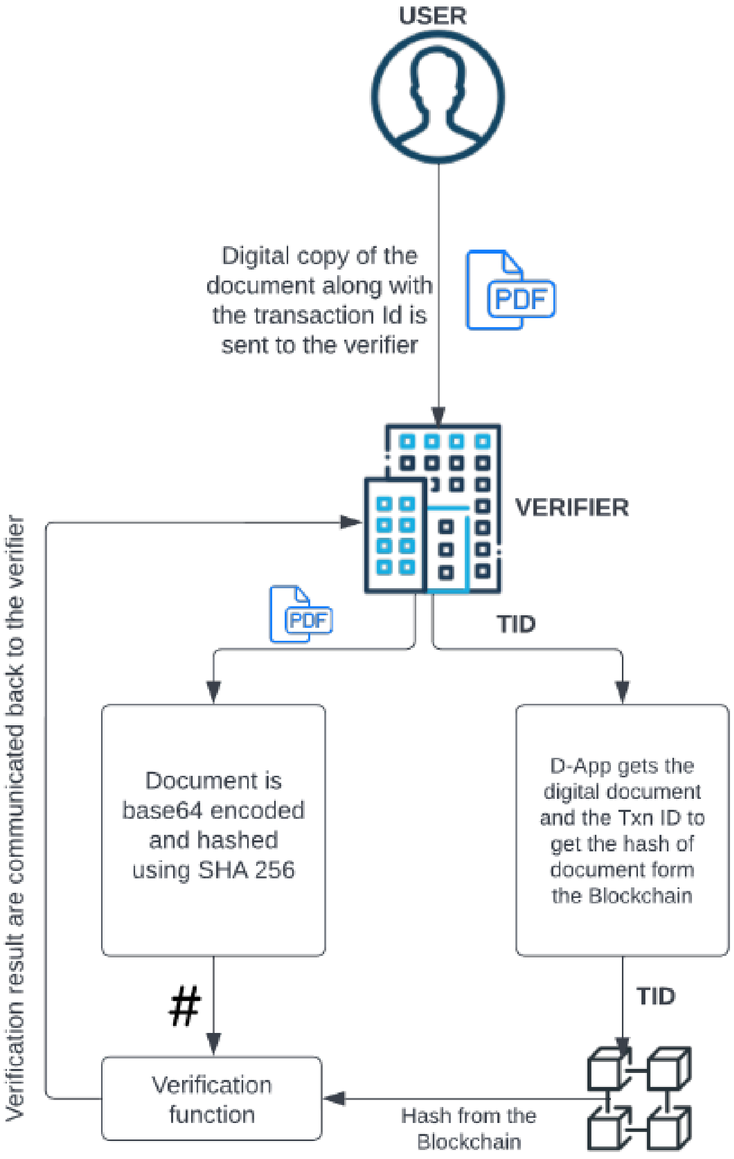
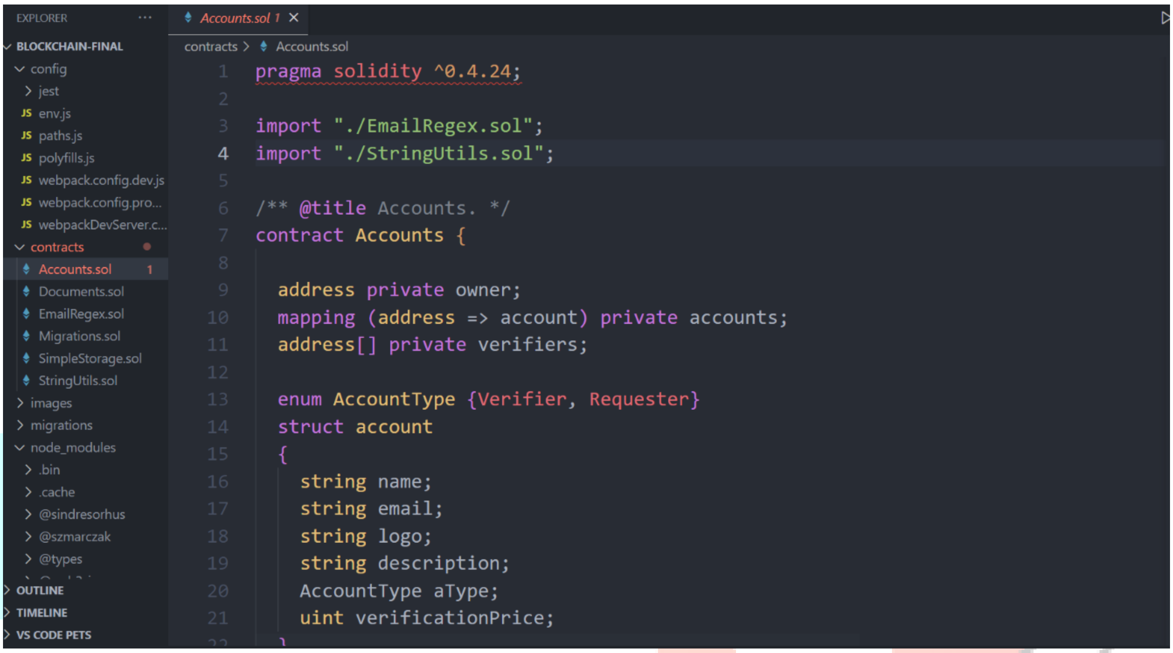

USER
Digital copy of the document along with the transaction Id is sent to the verifier
PDF
VERIFIER
PDF
TID
Document is base64 encoded and hashed using SHA 256
D-App gets the digital document and the Txn ID to get the hash of document form the Blockchain
#
TID
Verification function
Hash from the Blockchain
Verification result are communicated back to the verifier

Fig 1 System Architecture Diagram

Fig. 1 illustrates the comprehensive system architecture devised for the verification of online documents, premised upon the blockchain technology. The architecture embodies all five suggested methodologies, namely the User Interface, Web Application, Smart Contract, Blockchain Network, and Document Storage. User Interface: The User Interface, serving as the gateway for the user, is manifested as a web portal where users can submit their documents, while also verifying the legitimacy of documents that have already been posted. The construction of the web site, necessitates the utilization of JavaScript, CSS, and HTML.

Web application: The Web Application is tasked with receiving and processing user requests received via the User Interface. To this end, it is developed utilizing a server-side programming language like Python or Node.js, and processes HTTP requests utilizing a web framework such as Flask or Express.js.

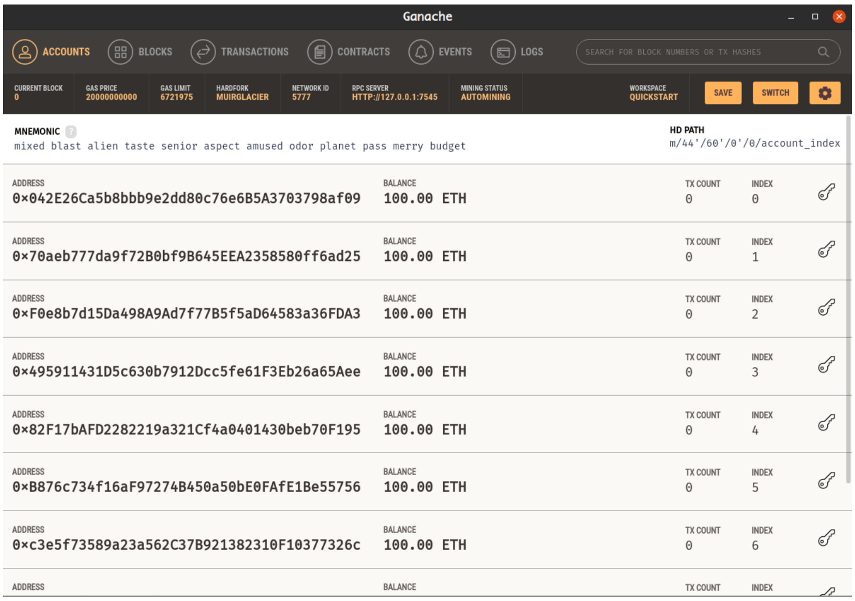
Smart Contract: The Smart Contract, constituting a vital component of the system, facilitates the storage and retrieval of document hashes through the execution of a program code that runs on the blockchain. Creation of the Smart Contract requires the use of a blockchain development platform such as Ethereum, while programming languages such as Solidity are utilized for its development.



```
pragma solidity ^0.4.24;

import "./EmailRegex.sol";
import "./StringUtils.sol";

/** @title Accounts. */
contract Accounts {

  address private owner;
  mapping (address => account) private accounts;
  address[] private verifiers;

  enum AccountType {Verifier, Requester}
  struct account
  {
    string name;
    string email;
    string logo;
    string description;
    AccountType aType;
    uint verificationPrice;
  }
```

Fig 2 Demonstration of Smart Contracts

Blockchain Network: The blockchain network constitutes a distributed and decentralized arrangement of nodes, which are responsible for storing document hashes and executing smart contract code. This network configuration is constructed using a blockchain platform that is tailored to fulfill this purpose, with choices such as Ethereum or Hyperledger Fabric being considered for the development of such a network. The network is composed of several nodes, each of which contributes to the distributed ledger that forms the foundation of the system's robust and immutable data storage mechanism. Through this distributed architecture, the system can ensure that the documents and their corresponding hashes are distributed across the network, thereby enhancing their security and resistance to tampering. Additionally, the decentralized nature of the blockchain network eliminates the need for a central authority or intermediary to oversee and administer transactions, thus promoting trust and transparency among the network participants.



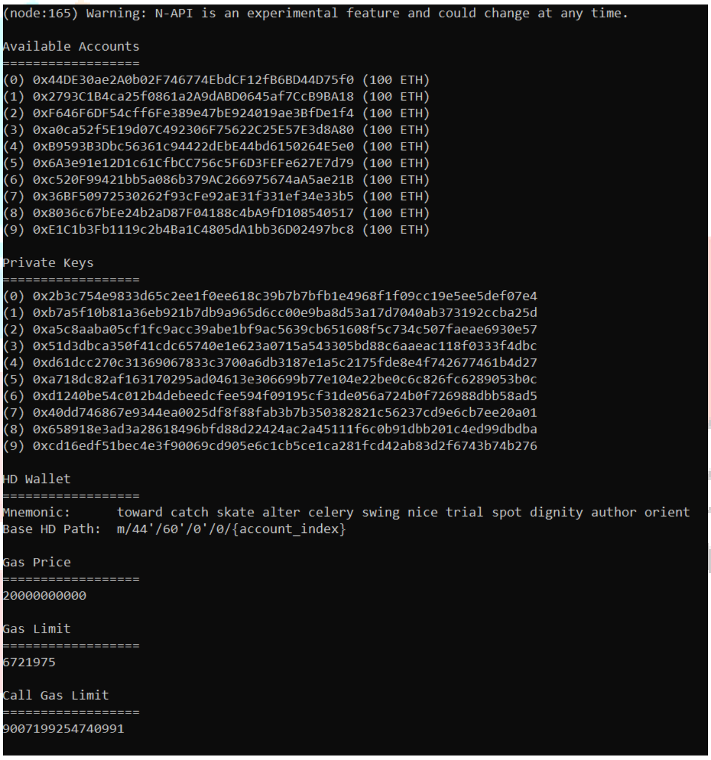
CURRENT BLOCK 0 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE QUICKSTART

MNEMONIC
mixed blast alien taste senior aspect amused odor planet pass merry budget

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×042E26Ca5b8bbb9e2dd80c76e6B5A3703798af09	100.00 ETH	0	0
0×70aeb777da9f72B0bf9B645EEA2358580ff6ad25	100.00 ETH	0	1
0×F0e8b7d15Da498A9Ad7f77B5f5aD64583a36FDA3	100.00 ETH	0	2
0×495911431D5c630b7912Dcc5fe61F3Eb26a65Aee	100.00 ETH	0	3
0×82F17bAFD2282219a321Cf4a0401430beb70F195	100.00 ETH	0	4
0×B876c734f16aF97274B450a50bE0FAfE1Be55756	100.00 ETH	0	5
0×c3e5f73589a23a562C37B921382310F10377326c	100.00 ETH	0	6

Fig 3 Ganache for Test Development



```
(node:165) Warning: N-API is an experimental feature and could change at any time.

Available Accounts
==================
(0) 0x44DE30ae2A0b02F746774EbdCF12fB6BD44D75f0 (100 ETH)
(1) 0x2793C1B4ca25f0861a2A9dABD0645af7CcB9BA18 (100 ETH)
(2) 0xF646F6DF54cff6Fe389e47bE924019ae3BfDe1f4 (100 ETH)
(3) 0xa0ca52f5E19d07C492306F75622C25E57E3d8A80 (100 ETH)
(4) 0xB9593B3Dbc56361c94422dEbE44bd6150264E5e0 (100 ETH)
(5) 0x6A3e91e12D1c61CfbCC756c5F6D3FEFe627E7d79 (100 ETH)
(6) 0xc520F99421bb5a086b379AC266975674aA5ae21B (100 ETH)
(7) 0x36BF50972530262f93cFe92aE31f331ef34e33b5 (100 ETH)
(8) 0x8036c67bEe24b2aD87F04188c4bA9fD108540517 (100 ETH)
(9) 0xE1C1b3Fb1119c2b4Ba1C4805dA1bb36D02497bc8 (100 ETH)

Private Keys
==================
(0) 0x2b3c754e9833d65c2ee1f0ee618c39b7b7bfb1e4968f1f09cc19e5ee5def07e4
(1) 0xb7a5f10b81a36eb921b7db9a965d6cc00e9ba8d53a17d7040ab373192ccba25d
(2) 0xa5c8aaba05cf1fc9acc39abe1bf9ac5639cb651608f5c734c507faeae6930e57
(3) 0x51d3dbca350f41cdc65740e1e623a0715a543305bd88c6aaeac118f0333f4dbc
(4) 0xd61dcc270c31369067833c3700a6db3187e1a5c2175fde8e4f742677461b4d27
(5) 0xa718dc82af163170295ad04613e306699b77e104e22be0c6c826fc6289053b0c
(6) 0xd1240be54c012b4debeedcfee594f09195cf31de056a724b0f726988dbb58ad5
(7) 0x40dd746867e9344ea0025df8f88fab3b7b350382821c56237cd9e6cb7ee20a01
(8) 0x658918e3ad3a28618496bfd88d22424ac2a45111f6c0b91dbb201c4ed99dbdba
(9) 0xcd16edf51bec4e3f90069cd905e6c1cb5ce1ca281fcd42ab83d2f6743b74b276

HD Wallet
==================
Mnemonic:      toward catch skate alter celery swing nice trial spot dignity author orient
Base HD Path:  m/44'/60'/0'/0/{account_index}

Gas Price
==================
20000000000

Gas Limit
==================
6721975

Call Gas Limit
==================
9007199254740991
```

Fig 4 Ganache CLI for generating test accounts along with private keys

Document Storage: In order to ensure the reliability and security of the document files, it is recommended to employ a robust and trustworthy storage solution such as Amazon S3 or Google Cloud Storage. These storage systems provide a high level of data protection and integrity, coupled with an array of advanced features that enable the system to efficiently manage and store large volumes of data. Such storage systems leverage cutting-edge encryption and security protocols to safeguard the documents against unauthorized access and tampering, while also offering redundancy and durability guarantees to ensure that the data remains accessible and recoverable even in the event of hardware failures or other catastrophic events. The use of such storage solutions is thus crucial to the success and viability of the blockchain-based document verification system, as it provides a secure and reliable repository for the documents themselves, thereby reinforcing the system's overall security posture and enhancing user confidence in the authenticity and validity of the documents.

V. CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The longstanding problem of counterfeit and altered documents within institutional structures has been exacerbated by issues such as poor communication between document issuers and verifiers, and the absence of a standardized method for record-keeping. However, in recent times, the employment of blockchain technology has emerged as a potential solution to these concerns.

Through the replacement of traditional hard-copy documents with their digital counterparts, the system endeavours to streamline and optimize the verification process for electronic documentation, enhance fraud detection capabilities, and maximize cost-effectiveness. Given the inherent transparency of the system's publishing and verification protocols, coupled with its ability to authenticate and validate provided information, blockchain-based technology is able to effectively curtail the creation of fraudulent electronic documentation.

Blockchain technology, an innovation that was originally introduced for Bitcoin and subsequently adopted by many other cryptocurrencies, has the potential to revolutionize nearly every aspect of our existence, including but not limited to, finance, supply chain management, identity verification, and voting systems. Despite its widespread adoption and increased popularity, the blockchain sector is still in its infancy, offering ample opportunities for novel and innovative applications of this technology, particularly in the realm of creating a system of collective trust among its users.

5.2 Future Scope

Blockchain technology holds immense potential for the future of online document verification, owing to its decentralized, immutable, and tamper-proof nature, which eliminates the requirement for a central authority and enables multiple parties to access the same information. The wide range of potential applications of blockchain technology in online document verification includes but is not limited to:

Identity Verification: Identity documents like passports, licences, and national ID cards can be safely stored and verified using blockchain technology. These documents can be authenticated using blockchain in real-time and without the need for a centralised authority.

Educational Certificates: Academic credentials are easily verifiable by employers and educational institutions worldwide because to the ability of educational institutions to issue and preserve them on blockchain.

Medical Records: Blockchain technology allows for the secure and open sharing of medical records by healthcare providers. This will assist in lowering errors and enhancing patient outcomes.

Legal Documents: A blockchain-based record of ownership and transaction history can be created by storing legal documents including contracts, deeds, and patents.

Financial Documents: Financial firms can utilise blockchain to track and verify documents like investment contracts, insurance policies, and loan agreements.

In general, blockchain-based online document verification has the potential to greatly reduce fraud and raise transparency across a range of businesses. We can anticipate seeing more cutting-edge uses for blockchain in document verification as the technology develops.

VI. Acknowledgment

The application of knowledge gained through academic years is nourished when practical implementation takes place. During the execution of this project, we have implemented various theories and implemented principles studied in theory over the course of our education along with exploring various new-technologies, latest innovations in relation to our study topic. We are filled with gratitude for the opportunity to implement the same for this opportunity to publish our paper titled, "**Online Document Verification Using Blockchain**" which is a part of our BE-Project. It would have been an impossible task without the guidance of our guide **Mr. Chetan C. Pawar** and his constant motivation for the same, for which we are filled with gratitude. We would also like to express our gratitude to all the lab asst and dept staff for their continuous guidance. Finally, we are acknowledging all the authors of the references and other literatures referred to in this project.

References

[1] S. T. Ahmed and M. S. Hossain, "An online document verification system using blockchain technology," 2018 IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, 2018, pp. 720-723.

[2] F. C. C. De Souza, F. V. Dos Santos, R. A. L. Righi and A. S. Kofuji, "A blockchain-based online document verification system for academic certificates," 2018 IEEE International Conference on Information Reuse and Integration (IRI), Salt Lake City, UT, 2018, pp. 528-534.

[3] S. H. Kim, S. H. Kim and M. Y. Chung, "A blockchain-based approach for online document verification," 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2018, pp. 1489-1491.

[4] B. C. Lee, J. W. Kim and J. H. Kim, "Blockchain-Based Online Document Verification System for Government and Business Applications," in IEEE Access, vol. 6, pp. 15593-15599, 2018.

[5] S. Roy and A. Jain, "An Online Document Verification System using Smart Contracts and Blockchain Technology," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0206-0211.

[6] S. A. Sultana and S. T. Ahmed, "A Blockchain-Based Secure Online Document Verification System," 2020 IEEE 12th International Conference on Electrical and Computer Engineering (ICECE), Dhaka, Bangladesh, 2020, pp. 71-74.

[7] F. Ahmad, N. Naseer, and A. Zaman, "Secure Online Document Verification using Blockchain," 2020 IEEE 6th International Conference on Computer and Communications (ICCC), Chengdu, China, 2020, pp. 214-219.

[8] H. A. Alshahrani and S. A. Alshebeili, "A Blockchain-based Online Document Verification System for E-Learning," 2021 IEEE International Conference on Computer and Information Technology (CIT), Riyadh, Saudi Arabia, 2021, pp. 1-4.

[9] B. K. Das and D. N. Kundu, "Online Document Verification System using Blockchain Technology," 2021 International Conference on Computational Intelligence and Data Science (ICCIDS), Kolkata, India, 2021, pp. 1-6.