IJIRMET ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024

Digital Document Management in Cloud Environments

[1] Dr. D. Anitha, M.E, [2]Dhanasri A, [3]Dharshini C, [4]Divya K V

[1]Head of the Department, Department of Information Technology Muthayammal Engineering College (Autonomous) Rasipuram - 637 408, Tamil Nadu, India.assvanitha@gmail.com

[2]Department of Information Technology Muthayammal Engineering College (Autonomous) Rasipuram - 637 408, Tamil Nadu, India. dhanasriit2024@gmail.com

[3]Department of Information Technology Muthayammal Engineering College (Autonomous) Rasipuram - 637 408, Tamil Nadu, India. dharshinichelladurai2003@gmail.com

[4]Department of Information Technology Muthayammal Engineering College (Autonomous) Rasipuram - 637 408, Tamil Nadu, India. divyadazzy06@gmail.com.

Abstract: ***Education and the ways in which people study and engage with educational institutions are evolving in the era of digital revolution. Additionally, there is a huge demand for increasing human knowledge due to the growth of social life. Nowadays, a growing number of people—from lifelong learners to doctorate candidates—use internet resources to advance their education and skill sets. Blockchain-based diploma learning, featuring student digital signature verification and verifiable certificate sharing, has the potential to revolutionize the education sector. This project proposes the implementation of a blockchain-based system to revolutionize diploma registration and verification, aiming to mitigate issues associated with counterfeit certificates and uncertified institutes. The system operates on a decentralized blockchain network, employing smart contracts to streamline the registration, verification, and approval processes. Institutes register on the blockchain, receiving unique identifiers, and issue digital certificates to students with individualized digital signatures for authenticity. By leveraging blockchain technology, this approach ensures the integrity and authenticity of academic credentials. The immutable nature of blockchain records makes it nearly impossible for certificates to be altered or falsified, fostering trust and transparency among employers, educational institutions, and other stakeholders. Moreover, students benefit from the convenience and accessibility of digital diplomas and certificates, reducing the risk of loss or damage. They also gain greater control over who can access their academic records, allowing for secure sharing with potential employers and other relevant parties. Furthermore, the streamlined verification process reduces the time and cost associated with background checks.***

Index Terms—Education System, Diploma Institutes, Blockchain Technology, Document Verification, Digital Signature, Certificate Sharing.

I. INTRODUCTION

In the midst of the digital revolution that is reshaping the landscape of education, the demand for innovative solutions to enhance the authenticity and accessibility of academic credentials has never been more pressing. This project introduces a groundbreaking initiative – a blockchain-based diploma registration and verification system designed to revolutionize the way educational institutions manage and authenticate academic records. As the digital era transforms how individuals engage with educational content, the rise of counterfeit certificates and uncertified institutes poses significant challenges. This project proposes a decentralized blockchain network that leverages smart contracts to streamline the traditionally cumbersome processes of diploma registration, verification, and approval. Educational institutes register on the blockchain, each receiving a unique identifier to establish their credibility. The issuance of digital certificates to students incorporates individualized digital signatures, ensuring the authenticity of academic credentials. The immutable nature of blockchain records renders certificates virtually tamper-proof, fostering trust among employers, educational institutions, and other stakeholders. Students benefit from the convenience and accessibility of digital diplomas, reducing the risk of loss or damage. Moreover, they gain greater control over who can access their academic records, allowing for secure sharing with potential employers. The streamlined verification process not only enhances efficiency but also significantly reduces the time and cost associated with background checks. This initiative stands at the forefront of the evolving education landscape, offering a secure, transparent, and technologically advanced solution to combat fraud, empower students, and contribute to the broader paradigm shift towards a more efficient and trustworthy education credential ecosystem.

BLOCKCHAIN TECHNOLOGY

P2P networks are expanded upon by blockchain, which offers a universal data set that all actors may rely on, notwithstanding the possibility that they do not know or trust one another. Every network node stores encrypted and unchangeable copies of data, forming a shared and reliable ledger of transactions. Native network tokens are used as financial incentives to strengthen the network's resilience against attacks and collusion.

For the Internet, blockchain and related technologies offer a universal and transparent layer of accounting and governance. Every network user has instantaneous access to the same data. All actors may see the details of transactions occurring over the network and can determine where they came from. Blockchain can alternatively be thought of as a public, transparent, international governance system or a distributed accounting system. A transaction is recorded permanently on the blockchain when it is approved by the network through majority consensus. If not, the transaction is declined and doesn't proceed. The only transactions regarded as legitimate and final are those that have been added to the blockchain.

By using machine consensus, a Blockchain system allows peer-to-peer (P2P) value transactions without the need for an intermediary. It functions over the Internet on a network of computers that are all running the protocol and have an identical copy of the transaction ledger. The blockchain is a shared, public database of transactions that keeps track of every transaction made from the first block, known as the genesis block, to the present day.

Given that a national authority in the nation will be in charge of the blockchain, this research employs consortium blockchain. The main building block of the blockchain is a block. A block is made up of a header and a body, with the transactions being written to the system located in the block body. The block's header comprises details about the block, such as its prior hash, nonce value, difficulty, and time stamp for both the transactions and the block. The block's length varies, but it was estimated to be between one and eight megabytes in size. The block to be placed is uniquely identified by its header.

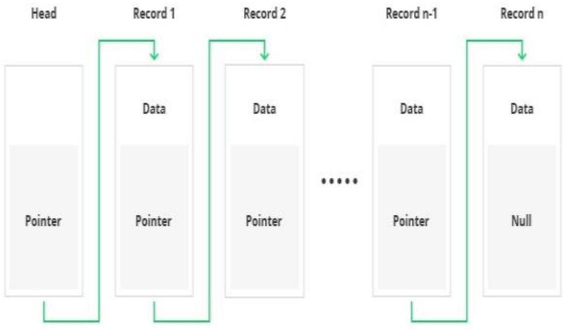

Fig.1 Data Storage in Blockchain Model

II. RELATED WORK

Tang, et.al,…[1] suggested a solution that was made possible by Blockchain by using a few fundamental data structures and cryptographic primitives. The diploma issuer and users should run the smart contract to store hash values of their public key certificates on the platform, and also update these values when the signing keys have been revoked. As a remark, these entities should store their public key certificates locally. To interact with the Blockchain platform, every user should obtain a wallet which should allow him/her to securely store relevant data and execute smart contracts. Similarly, the diploma issuer should also obtain a wallet. At the same time, the issuer should maintain a local database to store data from all its users. When the users want to present some attributes of his diploma to a diploma verifier, they should present the corresponding salt values for these attributes as well. They should also supply the required values for pertinent internal and leaf nodes so that the diploma verifier may calculate the value of the attribute hash tree's root node. Finally, should provide the two signatures in his diploma. The public key certificates of the diploma issuer and users should be certified by respective authorities which act as the root of trust. Determining these authorities is outside the purview of this work and will be made once the suggested method is put into practice. Assume, of course, that all entities are in possession of the trustworthy signature verification keys that have been provided by the authorities. The holder of the diploma must faithfully perform its duties. For instance, it must appropriately handle its key pair, updating it upon revocation and promptly posting the new public key certificate's hash value to the Blockchain. It must adhere to the process for creating diplomas and maintaining data on Blockchain.

Wang, et.al,…[2] implemented PFPoFL, which is resistant to spoofing and Sybil attacks, enables effective artificial intelligence (AI) task outsourcing, federated mining, model evaluation, and reward distribution in a fully decentralized way. It makes use of new transaction kinds, a unique block structure, and credit-based rewards. In addition, PF-PoFL provides miners with a user-level differential privacy method to stop implicit privacy leaks during FL model training. Three different types of blockchain nodes are involved in PFPoFL: (i) requesters, who generate FL jobs; (ii) model trainers, which are made up of miners and curators and train FL models in a pool; and (iii) validators, who are chosen from miners and are in charge of grading the models and suggesting new blocks.To be more precise, requesters post their FL tasks and incentives directly to the blockchain, and a community of validator’s works together to keep an organized queue of incomplete jobs. Through the use of the federation formation game, a group of miners with different training data sizes, non-IID degrees, and network delays dynamically build a stable pooled structure for an incomplete task. The associated curator then oversees a competition between pools to train the FL model, with the winner pool receiving the task reward through a consensus approach. The transaction costs are divided equally among the validators. Credit-based incentives are another feature of PF-PoFL that encourages miners to participate honestly and boosts consensus efficiency. Moreover, each pool's miners will receive strict privacy protection thanks to a user-level privacy-preserving model training method.It also describes an optimized pool formulation technique based on the federation formation game, where miners in heterogeneous FL tasks can self-organize into a disjoint Nash-stable split despite having different properties (e.g., non-IID degree, network delay, and training samples). The suggested PF-PoFL method has been proven to be efficient and effective by simulation results.

Wang, et.al,…[3] developed a safe PCP sharing scheme (BBC) for PCP sharing networks that is based on the energy blockchain. An energy blockchain-based architecture is first developed for PCP sharing networks to offer energy sharing services for EVs and PCPs using distributed ledgers and cryptocurrencies. Next, create a safe PCP sharing method based on reputation to increase consensus efficiency while using smaller signature sizes. Furthermore, based on ratings, behaviours, and fading, a distributed reputation method is built to evaluate the reliability of consensus nodes in blockchain. With the suggested method, EVs and PCPs can cooperatively and decentralized exchange energy ledgers and transactions. Here, as well, create a reputation-based secure PCP sharing method with smaller signature sizes to enhance blockchain security and consensus effectiveness.Each consensus node's PoW difficulty can be changed according on its reputation value. In addition, a distributed reputation system is used to evaluate consensus nodes, or local aggregators (LAGs), according to ratings and actions recorded in the blockchain. In order to simulate the energy interactions between EVs and PCPs, create a cooperative coalition-matching game here as well. The many-to-one matching game is used to choose the best candidate to link for both EVs and PCP coalitions, while the coalition game is used to examine the coalition formation process among PCPs. Next, a joint coalition matching game model that takes into account users' cooperation, competition, social characteristics, and practical limits was given for optimal energy scheduling in PCPSNs.Results from the suggested simulations and actual implementation showed the usefulness of the suggested scheme in compared to other current methods, especially in terms of increased consensus security, improved participant QoE, and increased RE efficiency.

Saleh, et.al,…[4] introduced 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. It may be noted from the previous section that in some solution cases reviews indicate certain themes of security are addressed and other themes are not addressed. However, it was observed that all the solutions provide inadequate security in terms of addressing all the five themes discussed in research. Therefore, it is found that in the reviewed solution cases the certificate is open to vulnerability and data security is inadequate. Hence, from the online solution reviews, the gaps found in the existing certificate verification solutions are authentication, authorization, confidentiality, privacy, and ownership. Because of that, this research aimed to close the mentioned gaps by proposing a blockchain based framework for the academic certificates verification focusing on authentication, authorization, confidentiality, privacy, and ownership themes. The proposed framework is build based on Hyperledger Fabric framework due its benefits. There are various blockchain platforms available; however the top three dominant blockchain platforms include Bitcoin, Ethereum and Hyperledger. Ethereum and Bitcoin are permission less blockchains, where anyone can join the network as well as write and read transactions. On the other hand, Hyperledger is a permissioned blockchain, where only predefined participants can join a network, view and make transactions. Based on the requirements of educational certificates in the blockchain, Hyperledger would be the most suitable platform in proposed approach due to its inherent privacy and role based access mechanism for accessing the documents.

Castro, et.al,…[5] presented an integrative literature review, summarizing articles read, along with the main concepts and contributions. A major Portuguese university employs one of the authors, who until recently served as a committee member on a doctoral programme requiring applicants to submit a Hague apostille certification upon application (a type of authenticity certificate that certifies a public document was issued by an authorized institution, thereby eliminating the need for such documents to be legalized abroad). Notably, a sizable portion of overseas applicants were not aware of this, neglected to submit it, and as a result, were not approved for the PhD programme. Furthermore, this was a huge disappointment because, in a few cases, arrangements for study and travel abroad had been formed. The Hague apostille would not be required with a different, decentralized, "watertight" (meaning that intermediary information providers would not be permitted to tamper with the automatically attached information) blockchain approach, saving time, money, and even a great deal of "heartbreak". Blockchain is viewed as a possible way to enhance the procedure, offer more efficiency, transparency, and decentralization, which will ultimately reduce diploma fraud. Additionally, a global (transnational) certificate validation environment can be constructed using it. Its unchangeability can increase trustworthiness and lower the chance of information loss.

III. BACKGROUND OF THE WORK

Since the early stages of blockchain technology development coincided with the emergence of cryptocurrencies, particularly Bitcoin as a cryptocurrency, the majority of people are familiar with the birth of blockchain technology as Bitcoin. The use of consensus techniques, smart contracts, and hash value generation in chain blocks enable the application of blockchain to intelligent devices. Blockchain technology can also improve the quality of remote learning by expediting the accreditation process, increasing transparency, and enabling simpler access for authorized individuals. Additionally, this technology can be used to enhance the current shortcomings of the certificate verification systems in place and issue digital degree certificates that cannot be changed.Blockchain technology has the ability to completely transform education by bringing more accessible and cost-effective learning options and changing the relationship between schools and their students. The administration of student tuition payments is a labor-intensive process involving many parties, including parents, students, scholarship foundations, private lenders, state agencies, and the often massive bureaucracy of university finance departments. Users may expedite this process with the aid of blockchain technology, cutting down on expenses and ultimately lowering the cost of schooling. In the meantime, the technology has already been used for pay-as-you-go classes that use smart contracts and accept cryptocurrencies as payment in open learning models.

IV. BLOCKCHAIN BASED DIPLOMA VERIFICATION AND CERTIFICATES SHARING

The proposed system is the implementation of blockchain system for the generation, verification, and revocation of diplomas. Every service that has been executed before in the blockchain system has certain hash values that are stored in the blockchain network. The respective institution can only generate the diploma in electronic form and digitally sign it after confirming that the student who made the request has all of the unique hash values created at the beginning. Prospective students submit their certificates with digital signatures, initiating a transparent verification process by the institutes. Successful verifications trigger smart contracts for approval, updating the blockchain with immutable records of diplomas. The system also facilitates the secure storage and distribution of verified certificates, ensuring their tamper-proof nature. The blockchain's transparency and traceability enhance the overall credibility of educational credentials, while a user-friendly interface ensures accessibility for both institutes and students. This innovative solution has the potential to significantly reduce instances of fraudulent certifications, providing a reliable and secure foundation for academic qualifications in the digital age. The same process is also used for verification of the diploma as well as revocation, which in fact represents the deletion and regeneration of the diploma from the beginning. It also provides digital certificate sharing process through blockchain network.

The decentralized blockchain infrastructure forms the backbone of a novel system that promises to transform the way educational credentials are registered, verified, and approved. Institutes wishing to participate in this system undergo a seamless registration process on the blockchain, each receiving a unique identifier. Prospective students enrolling in diploma programs submit their certificates, accompanied by their own digital signatures, initiating a verification process facilitated by the institutes. The verification process, executed on the blockchain, rigorously examines the submitted documents, checking the legitimacy of the certificates and confirming the eligibility of the students. Upon successful verification, institutes use smart contracts to approve the student's request, updating the blockchain with transparent and immutable records of approved diplomas. After approval, institutes upload the certificates to the blockchain, the immutability of the blockchain guarantees the perpetual trustworthiness of the academic records stored within the system.

Fig.2 Proposed Framework

Framework Creation

The blockchain system for the generation, verification, and revocation of diplomas would include the following actors: students, higher education institutions, and the blockchain network. Communication between students and institutions for higher education is done through the proposed application. Institutes interested in participating in the system register on the blockchain by providing necessary details and credentials. Each registered institute is assigned a unique identifier on the blockchain.

Request for Diploma

Students can request the creation of a diploma once they have completed their studies and met all of their obligations to the higher education institution. All process is done through the application part of the blockchain system. Students interested in joining a diploma program submit their certificates along with a digital signature to the blockchain platform. The digital signature helps in verifying the authenticity of the submitted documents. Student’s request is the attachment of the student’s digital signature, in addition to other data that accurately identifies the student.

Request Approval

The respective institution can only generate the diploma in electronic form. Institution digitally signs it after confirming that the student who made the request has all of the unique hash values created at the beginning. The same process is also used for verification of the diploma as well as revocation, which in fact represents the deletion and regeneration of the diploma from the beginning. Institutes review the submitted documents through the blockchain platform. The institute's verification process involves validating the digital signature, checking the authenticity of the certificate, and confirming the student's eligibility. Once the verification is successful, the institute approves the student's request on the blockchain using a smart contract. The approval status is updated on the blockchain, ensuring transparency and traceability.

Digital Certificate Sharing

Students and educational institutions can trust the authenticity of the certificates as they can verify them on the blockchain. Students can easily access their digital diplomas and certificates from anywhere, reducing the risk of loss or damage. After approval, the institute uploads the student's certificates to the blockchain. Certificates are stored in a secure and tamper-proof manner, providing a reliable source of verified credentials. All transactions, including registrations, verifications, and approvals, are recorded on the blockchain. The immutability of the blockchain ensures that the record of diplomas and certifications remains trustworthy over time.

METHODOLOGY

Blockchain Technology

Blockchain is an open, trusted, shared ledger of transactions that is not controlled by any one person but is accessible to all. It is a distributed database that keeps an ever-expanding list of transaction data records safe from alteration and tampering via cryptography. There exist three distinct varieties of blockchain technology: consortium, private, and public. Public blockchains like as Bitcoin and Ethereum, allow anybody, anywhere, to join and receive relief whenever they choose. These intricate mathematical functions serve as evidence for this. The company's internal public ledger is called the private blockchain, and access to it is only authorized by the blockchain's owner. Because there are fewer nodes in the private blockchain than in the public one, block creation and mining speed are significantly faster. However, the consortium blockchain is used by a company or set of companies, and membership standards are used to more effectively manage blockchain transactions in place of a consensus.

Hashing

The process of hashing converts an arbitrary, variable-sized input into an output with a fixed size. Various functions are available for doing hashing at different levels. The MD5 algorithm yields a hash value that is 128 nit, or 32 symbols long, and is commonly used for hashing. The series' most recent algorithm is MD5, however earlier iterations included Md2, Md3, and Md4. Although the technique was intended to be used as a cryptographic hashing algorithm, it has certain vulnerabilities because of issues that limit the number of unique hashes that it can produce. Another cryptographic hash algorithm is the Secure Hashing Algorithm (SHA), which produces a 160-bit hash value made up of 40 hexadecimal characters. The algorithm's use has decreased since it was unable to withstand collusion attacks. SHA 3 and SHA 256 are two of the new algorithms that have been proposed during this time. The US National Security Agency created the SHA 2 family of algorithms. New hash algorithms SHA 256 and SHA 512 are considered secure elsewhere and do not have collusion issues, at least not yet.

Each block in a blockchain is made up of the headers listed below.
Previous Hash: The previous block can be found using this hash address.
Transaction Details: Information about each and every transaction that must take place.
Nonce: An arbitrary integer assigned by cryptography to distinguish the hash address of a block.
Hash Address of the Block:

A hashing algorithm is used to send the previously mentioned data, including the nonce, transaction details, and previous hash. This produces an output that is known as the distinct "hash address" and has a length of 64 characters (256 bits). It is called the hash of the block as a result. Many people worldwide attempt to use computational procedures to determine the appropriate hash value to satisfy a predefined criterion. When the predefined condition is satisfied, the transaction is finished. To put it another way, a proof of work challenge is a mathematical puzzle that blockchain miners try to solve. The first person to figure it out wins a prize.

Mining

"Mining" is the term used in Blockchain technology to describe the process of adding transactional data to the current digital/public ledger. Although the phrase is linked to Bitcoin, it can also apply to other Blockchain-based technologies. By creating a block transaction's difficult-to-forge hash, mining ensures the security of the entire Blockchain without requiring a centralized mechanism.

Block and Hash Generation
1. A block with details on the transactions those are currently underway.
Every piece of data produces a hash.
3. A hash is a combination of letters and integers.
4. The order in which transactions occur is recorded.
5. The hash is dependent on both the current transaction and the hash of the prior transaction.
6. Any modification to a transaction, no matter how tiny, results in a fresh hash.
7. The nodes examine the hash to ensure that a transaction has not been altered.
8. A transaction is recorded in a block once it has received approval from the majority of nodes.
9. The Blockchain is made up of all the blocks that refer to each other.
10. Because a blockchain is distributed over numerous computers, each of which has a copy of the blockchain, it is effective.

V. CONCLUSION

In conclusion, this blockchain-based diploma registration and verification project represents a groundbreaking advancement in ensuring the integrity and authenticity of academic credentials. By leveraging the decentralized, transparent, and immutable nature of blockchain technology, the initiative introduces a robust framework for institutes to register, verify, and approve diplomas securely. The incorporation of digital signatures ensures the legitimacy of certificates, mitigating the pervasive issue of fake diplomas and uncertified institutions. The transparent and traceable nature of the blockchain not only enhances the credibility of academic records but also provides a reliable mechanism for authorized entities to verify credentials efficiently.

REFERENCES

[1] Kwan-Loo, Kevin B., José C. Ortíz-Bayliss, Santiago E. Conant-Pablos, Hugo Terashima-Marín, and P. Rad. "Detection of violent behavior using neural networks and pose estimation." IEEE Access 10 (2022): 86339-86352.
[2] Adil, Muhammad, SaqibMamoon, Ali Zakir, Muhammad ArslanManzoor, and ZhichaoLian. "Multi scale-adaptive super-resolution person re-identification using GAN." Ieee Access 8 (2020): 177351-177362.
[3] Alansari, Mohamad, Oussama Abdul Hay, SajidJaved, AbdulhaidShoufan, YahyaZweiri, and NaoufelWerghi. "GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations." IEEE Access (2023).
[4] Deng, Jiankang, JiaGuo, EvangelosVerveras, Irene Kotsia, and StefanosZafeiriou. "Retinaface: Single-shot multi-level face localisation in the wild." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 5203-5212. 2020.
[5] Deng, Jiankang, JiaGuo, NiannanXue, and StefanosZafeiriou. "Arcface: Additive angular margin loss for deep face recognition." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 4690-4699. 2019.
[6] Zhu, Yanjia, HongxiangCai, Shuhan Zhang, Chenhao Wang, and YichaoXiong. "Tinaface: Strong but simple baseline for face detection." arXiv preprint arXiv:2011.13183 (2020).
[7] Feng, Yao, Fan Wu, Xiaohu Shao, Yanfeng Wang, and Xi Zhou. "Joint 3d face reconstruction and dense alignment with position map regression network." In Proceedings of the European conference on computer vision (ECCV), pp. 534-551. 2018.

[8] Ferrari, Claudio, Stefano Berretti, and Alberrto Del Bimbo. "Extended youtube faces: a dataset for heterogeneous open-set face identification." In 2018 24th International Conference on Pattern Recognition (ICPR), pp. 3408-3413.IEEE, 2018.
[9] Lin, Yiming, Shiyang Cheng, JieShen, and MajaPantic. "Mobiface: A novel dataset for mobile face tracking in the wild." In 2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019), pp. 1-8.IEEE, 2019.
[10] Wang, Hao, Yitong Wang, Zheng Zhou, Xing Ji, Dihong Gong, Jingchao Zhou, Zhifeng Li, and Wei Liu. "Cosface: Large margin cosine loss for deep face recognition." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5265-5274. 2018.