BLOCKCHAIN BASED CERTIFICATE VALIDATION

Mrs. G. Jyothi , Assistant Professor, Department of Information Technology,
Vignan's Institute of information Technology(A),Visakhapatnam-530049
Ms. Sravani Kundrapu, MCA Student, Department of Master Of Computer Applications,
Vignan's Institute of information Technology(A),Visakhapatnam-530049

ABSTRACT:
As we move towards a more digital world, important documents like academic diplomas from educational institutions and the SSLC and HSC are also being converted to digital representations. But while institutions and organizations deal with laborious procedures for validating and verifying certificates, students frequently struggle to keep track of their actual degree certificates. In order to improve security and expedite validation processes, our project attempts to address this problem by implementing a blockchain-based certificate storage system. First, paper certificates are converted to digital formats, and each certificate is assigned a unique hash code that is produced by a chaotic algorithm. After that, the blockchain securely stores these digital certificates.These certificates can be verified and validated with the help of a mobile application, which makes use of blockchain technology to provide a more effective and safe validation process.

Keywords:
Blockchain Technology, Distributed Ledger, Smart contracts, Consensus Mechanisms, Cryptographic Hashing, Digital Signatures Decentralized Trust Model, Peer-to-Peer Network, Data Integrity, Security Measures.

INTRODUCTION :

Ensuring the legitimacy and dependability of certificates is crucial in today's digital age for a number of reasons, including identity verification, professional accreditation, and education. Conventional certification techniques are susceptible to hazards including single points of failure, manipulation, and fraud since they frequently depend on centralized authorities.

Blockchain technology has emerged as a potential answer to these problems. Blockchain, which was initially created for cryptocurrencies like Bitcoin, has matured into a decentralized, impenetrable architecture with uses outside of finance. Blockchain functions as a distributed ledger in essence, safely logging transactions and connecting them in blocks over a computer network. The integrity and immutability of the transaction history are guaranteed by the distinct cryptographic hash that is contained in each block and is created from the data of the block before it. Using blockchain technology in certificate validation seeks to improve security and confidence in the verification process. Using the immutability, transparency, and consensus mechanisms of blockchain technology, the goal is to create a reliable document certification system. Cryptographic hashing algorithms and smart contracts—self-executing contracts with terms encoded into code—transform data into distinct character strings that allow stakeholders to independently confirm the authenticity and integrity of certificates without the need for middlemen.The ultimate goal of implementing blockchain-based certificate validation is to lower the risks of fraud, counterfeiting, and dependence on centralized bodies by giving people and organizations more confidence in the legitimacy of certificates.

LITERATURE SURVEY

The project's main goals are to construct a validation system and an immutable certificate generation. We have cited a few previously published publications and the contributions of other experts in this subject in support of this. Blockchain technology, a cutting-edge storage system, and digital certificate validations were the major topics of our literature review.

Our first paper was presented by Zibin Zheng , Shaoan Xie, Hong-Ning Dai. An Overview of Blockchain Technology[1],the title of our paper offers an extensive exploration of blockchain, elucidating key concepts including "smart contracts." Within the blockchain, data hashes are stored in preceding blocks, forming a continuous chain of nodes. Any alteration to the data results in a change in its hash, which no longer corresponds with the previous block's hash, serving as an indicator of tampering.

Decentralization stands out as a disruptive attribute of blockchain technology. Transactions occur within applications installed on individuals' devices, eliminating the need for central institutions or servers. Verification, accounting, storage, maintenance, and data transmission within the blockchain rely on a distributed system. This approach not only conserves resources and streamlines transactions but also mitigates the potential for control by centralized entities. Blockchain technology employs a timestamped structure to store data, introducing a time element that enhances verification and traceability.

The second paper was titled as smart contract and Ethereum[2], presented by Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen. Smart contracts are coded instructions designed to enforce predefined rules, facilitating the Transfer of digital assets within the blockchain. These contracts are invoked by external applications to execute various transactions. In blockchain-based asset transactions governed by smart contracts, the code autonomously triggers to finalize the specific transaction between involved parties. This code constitutes the smart contract itself. Utilizing Ethereum as the platform, developers have the capability to craft their own blockchain applications. Ethereum is a decentralized open-source blockchain that incorporates smart contract capabilities. It serves as a prime illustration of blockchain technology and operates as a cryptocurrency system, widely recognized as the second most valuable digital currency after bitcoin.

The third paper was titled as "blockipfs (Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability)[3]" which shed light on integrating IPFS with Blockchain. It compared traditional IPFS with Blockchain-enabled IPFS, showing that blockipfs outperformed in various categories like upload, read, and download transactions.

The Final Paper proposed a model for identity verification based on blockchain [4]. Like the second and third papers, their system comprised an Issuing Authority responsible for document generation, utilization of a hashing algorithm, and storage of its value. To enhance security, they opted for asymmetric encryption instead of public hash keys utilized in other systems.

CONCLUSION

This study uses blockchain technology to address the problem of certificate forging. Data security is crucial, and blockchain's unquestionable structure improves security and reduces the possibility of certificate fabrication. With the help of our application, users can quickly verify and authenticate certificates, guaranteeing the confidentiality and correctness of their information. This technology also makes managing digital certificates easier, making it a more user-friendly option than conventional paper-based certification processes.

REFERENCES:-

[1] Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen ,An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE 6th International Congress on Big Data, 2017.

[2] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.

[3] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

[4] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology", International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-5S3, February 2019.

[5] Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim-Kwang Raymond Choo, “BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability”, IEEE International Conference on Blockchain, 2019.

[6] Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah, “Blockchain Based Identity Verification Model”, International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019.

[7] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

[8] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain.

[9] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi “Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[10] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, “ Certificate Verification System using Blockchain” Computer Engineering Department, Mumbai University.

[11]M. Warasart and P. Kuacharoen, “Paper-based Document Authentication using Digital Signature and QR Code,” no. Iccet, 2012.

[12] S.Sunitha kumari, D.Saveetha “Blockchain and Smart Contract for Digital Document Verification” Department of Information Technology- SRM Institute of Science and Technology.

[13] Omars Saleh, osman ghazali, muhammad ehsan rana, “Blockchain based framework for educational certificates verification” Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia, Kedah, Malaysia.