WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Decentralized System for Verification of Educational Certificates Using Block Chain

R. Suchitra[1], G. Sampath Kumar[2], G. Indra Prasad[3], A. Jaswanth[4], A. Vasu.[5]

[1]Associate Professor, [2,3,4,5]Student -8th Semester
Department of Computer Science & Engineering, Lendi Institute of Engineering & Technology, Vizianagaram, India.
[1]suchitra1243@gmail.com, [2]sampath1gsk@gmail.com, [3]Indraprasadnarwal143@gmail.com, [4]jassucherry225@gmail.com,
[5]asapu.Vasu2001@gmail.com

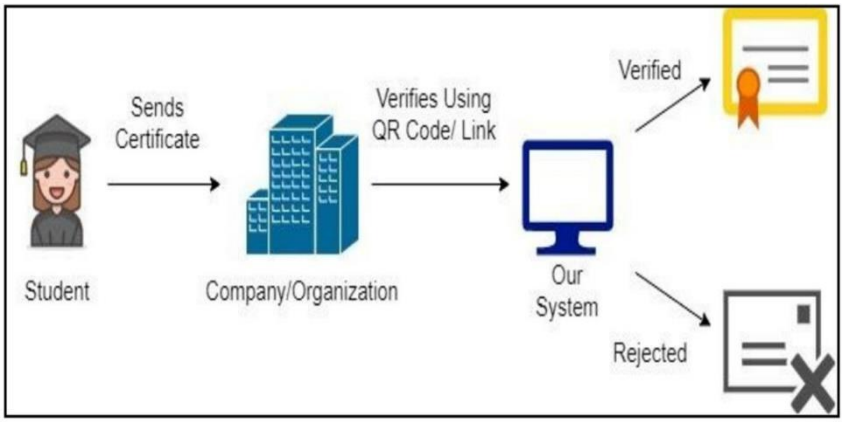
ABSTRACT-

Educational certificate verification is the process of checking and verifying the certificate legitimacy of graduate students. Millions of students complete their education each year and go on to do higher studies or a corporate job. In this case student credentials are verified through a lengthy document verification process. This results in significant overhead as documents are transferred between institutions for verification. The current certification system provides traditional certificates and electronic certificate to the candidates. That's why certificates can be tampered with and lost at any time. Moreover, Traditional paper certificates and electronic certificates have difficulties in preservation and management, not to mention other problems concerning inconvenient verification, poor reliability, anti-counterfeiting, and anti- tampering. This issue can be addressed by creating Digital Certificates or E-Certificates. Digital certificates can be generated using the block chain technology with QR-code embedded on each certificate. To address the verification problem, the verifier would have to just scan the QR- code and validate it. This concept will help educational institutions and other service sectors like healthcare, bank to verify certificates of a particular individual in very less time, effortlessly and in a cost-effective manner. This project is based on block chain technology and smart contract, in which a set of block chain certificate system aiming at providing block chain certificate services for college students.

KEY WORDS: - *Block chain, Academic Record Verification, QR code, Digital Certificates, Decentralized Application, Ethereum.*

1. INTRODUCTION

The traditional education systems are no standard for the necessity of including the most advanced technology to enhance their entire consistency. Currently, the educational sector provides traditional certificates to the student after completion of a degree. That means the copies need to deal with in person; they aren't tamper-resistant and can be lost anytime. In this case, Block Chain brings us a massive opportunity with a trustable interaction among students, universities, and employers in the educational certificate verification process. Block Chain technology provides the ground of a decentralized system environment where all data is immutable, and once it is verified, data cannot be altered. It also removes the involvement of third-party from a system. This decentralized technology is assumed to remodel industry, merchandising, and education infrastructure and contribute to expeditious development and prosperity internationally. A decentralized Block Chain system uses consensus algorithms and cryptography techniques to records all the transactions and their details in multiple locations simultaneously. It also records the changes in the transaction and data transaction flow and provides a transparent, immutable record of all data. However, this decentralization, immutability, traceability features of Block Chain ensures that the data is truthful, accurate, secured, and safe. The below figure shows how Block Chain can be used in the educational certificate issues and verification process.



2. LITERATURE SURVEY

Research has been in progress to identify the fake documents and certificates, both paper and digital form. The following are some of the methods proposed to curtail fake documents.

MV Ramana Murthy [1] presented a method to detect fake paper-based documents with ECC based digital signatures and cryptography.

Xiaojing Gu [2] designed an attribute dependency-based detection method, called SSLight, in which some attribute dependencies are observed that are rarely present in legitimate samples.

Dr. A. M. Kahonge [3] proposed a mechanism that uses the web and database programming, XML data sharing along with message passing via a very simple web service to share academic records between employers and the educational institutions.

Zheng Dong [4] presented a scheme for detecting forged certificates from trusted CAs developed from a large and timely collection of certificates. In this method, classification is done automatically by building machine-learning models using deep neural networks (DNN). Kajal P. Chavan [5] proposed a system where the digital data, which is encrypted in the marks memo as a QR code, can only be retrieved back and decrypted by authorized users only using their web-application, which is hosted in their website. But all these are centralized applications and can be easily tampered. The following are various applications proposed based on Block Chain technology.

Ming L [6] proposed a Block Chain-based decentralized framework for crowdsourcing named CrowdBC, in which a requester's task can be solved by a group of workers without depending on any intermediate third party, users' privacy can be guaranteed and also the required transaction fee is low.

Haibo Yi [7] proposed an e-voting scheme, which is Block Chain-based and meets the essential requirements of the e-voting procedure. All votes are linked using hash values in a Block Chain.

Yi Chen [8] designed a storage scheme to store and manage personal medical data using Block Chain and cloud storage.

Ali Dorr [9] proposed a Block Chain-based framework to protect the privacy of users and to improve the security of the vehicular ecosystem.

Xiao Yue [10] proposed an application, healthcare data gateway, whose architecture is based on Block Chain to enable patient to control and share their medical reports seamlessly and securely without violating the privacy, which also provides a new way to improve the efficacy of healthcare systems while keeping patient data private.

Daniel Kraft [11] stated mining as a Poisson process with time-dependent intensity and used this model to derive predictions about block times for various hash-rate scenarios.

Tomaso Aste [12] published a paper that provides basic concepts of Block Chain and also presented the challenges, the future opportunities, and the foreseeable impact of Block Chain and distributed ledger technologies in the industry and society.

3. METHODOLOGY

3.1Algorithm Description: RSA

RSA is a public-key encryption algorithm widely used for securing sensitive data over the internet. It was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977.

The RSA algorithm uses two keys - a public key and a private key. The public key is used to encrypt the data, while the private key is used to decrypt it. The security of the RSA algorithm is based on the fact that it is difficult to factorize the product of two large prime numbers.

The RSA algorithm works as follows

- Choose two large prime numbers, p and q.
- Calculate n = p * q.
- Calculate the totient of n, $\varphi(n) = (p-1) * (q-1)$.
- Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
- Calculate d, the modular multiplicative inverse of e modulo $\varphi(n)$. This means that
- $(d * e) \% \varphi(n)=1$.
- The public key is (n, e) and the private key is (n, d). To encrypt a message m using the public key (n, e), the sender does the following:
- Convert the message m to an integer representation M.

- Calculate C = M^e mod n, which is the encrypted message. • Send the encrypted message C to the receiver. To decrypt the encrypted message C using the private key (n, d), the receiver does the following:
- Calculate M = C^d mod n, which is the decrypted message.
- Convert the integer representation M back to the original message m.

The RSA algorithm is widely used for secure communication and digital signatures. However, it is computationally intensive and can be vulnerable to attacks such as side- channel attacks and factorization attacks.

3.2 Solidity

Dapps otherwise referred to as Decentralized Applications are applications built on the open source, peer-to-peer network of Ethereum Block Chain which uses smart contracts and front- end user interfaces to create decentralized platforms. Developing a Dapp, like any other app, requires programming and executing code on the system. Solidity programming stands apart from the other programming languages and is the programming language of choice in Ethereum.

Solidity is a brand-new programming language developed by Ethereum, the second- largestcrypto currency market by capitalization.Solidity is a relatively new language that is rapidly growing. Solidity is currently the core language on Ethereum and other private Block Chains operating on competing platforms, such as Monax and its Hyperledger Burrow Block Chain which uses Tender mint for consensus.

SWIFT has created a proof of concept that runs on Burrow and uses Solidity Solidity is a statically typed programming language designed for developing smart contracts that run on the Ethereum Virtual Machine (EVM) or compatible virtual machines.

3.3 ETHEREUM:

Ethereum is a Block Chain platform with its own crypto currency, called Ether (ETH) or Ethereum, and its own programming language, called Solidity. As a Block Chain network, Ethereum is a decentralized public ledger for verifying and recording transactions. Its crypto currency is now second only to Bit coin in market value. It is the fuel that runs the network. It is used to pay for the computational resources and the transaction fees for any transaction executed on the Ethereum network. Like Bit coins, ether is a peer-to-peer currency. Apart from being used to pay for transactions, ether is also used to buy gas, which is used to pay for the computation of any transaction made on the Ethereum network.

4. EXPERIMENT

4.1 Smart Contracts:

Smart contracts were first proposed by Nick Szabo in the early 1990s. He explained that a smart contract enabled computers to execute transaction clauses. As Block Chain has become popular, smart contracts have received increased attention. Smart contracts are the main feature of Ethereum, a Block Chain platform founded in 2015. A smart contract is “a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of Block Chain”. Smart contracts can be created using the Ethereum Block Chain. Developers are able, according to their needs, to specify any instruction in smart contracts; develop various types of applications, including those that interact with other contracts; store data; and transfer Ethers. Additionally, smart contracts that are deployed in Block Chains are copied to each node to prevent contract tampering. With related operations executed by computers and services provided by Ethereum, human error can be reduced to avoid disputes regarding such contracts. Smart contracts are mostly used in voting system and crypto currency applications.

4.2 MetaMask

MetaMask is an extension for accessing Ethereum enabled distributed applications or Dapps in your browser. The extension injects the Ethereum web3 API into every websites JavaScript context so that Dapps can read from the Block Chain.

4.3 Ganache:

Ganache is used for testing Solidity contracts on a personal Ethereum Block Chain. It by default provides an easy setup for spinning up a network with around ten users with each having 100 eths on their account. These accounts can be used to mimic the transactions between the users.

4.4 System Design :-

Design is the process of defining concepts such as architecture, modules and components, the differences between these components, and the information passing through the system. It aims to meet the specific needs and requirements of the business or organization by creating a consistent and efficient process. System Design mainly focuses on defining the architecture, components, modules, interfaces and information of the system to meet specific requirements. Design can be seen as the application of technology to production. System Design means a systematic approach to system design.

It can be a bottom-up or top-down approach, but in both cases, the process is systematic, taking into account all the changes that need to be made in the system, from the architecture to the required hardware and software to information. and how it is transmitted and exchanged system-wide. It then overlaps with systems design, systems analysis, systems engineering, and systems architecture.

Use case Diagram: -

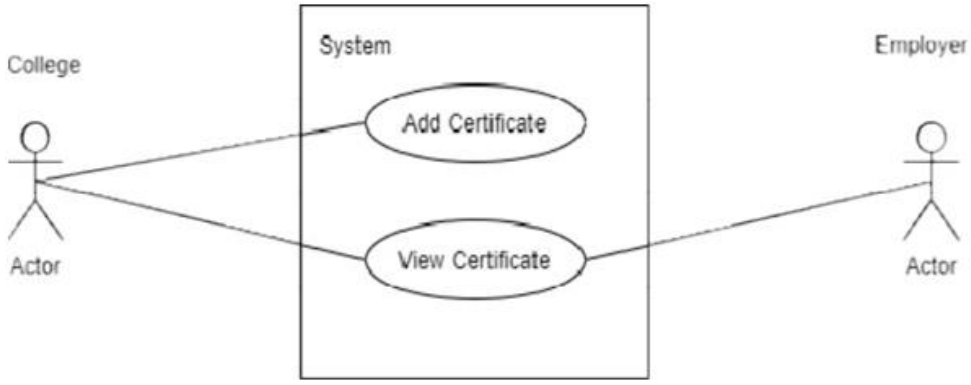


Fig 4: Use case Diagram

EXPERIMENT RESULTS:-

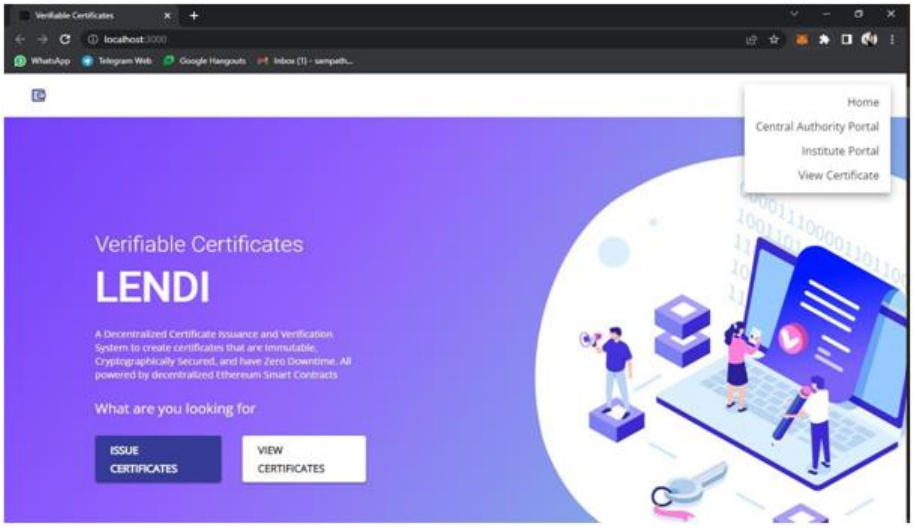


Fig 4.1 Fig Home screen

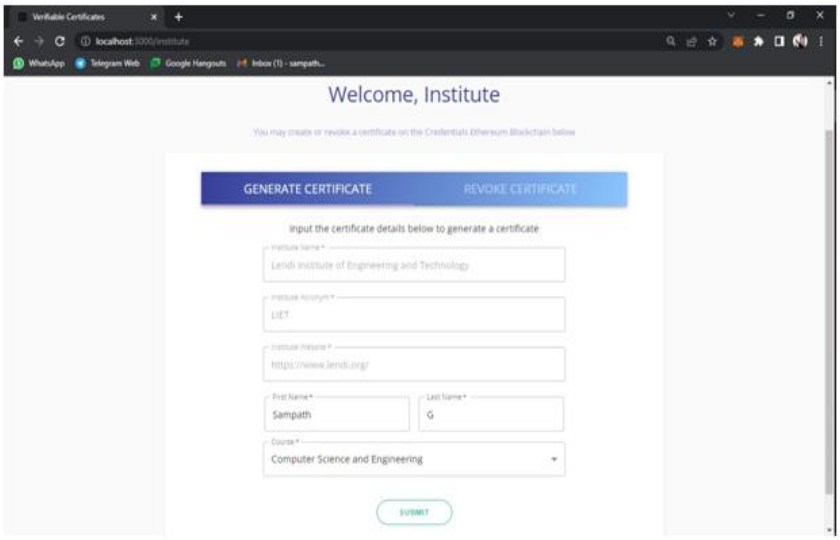


Fig 4.2 Generating Certificate

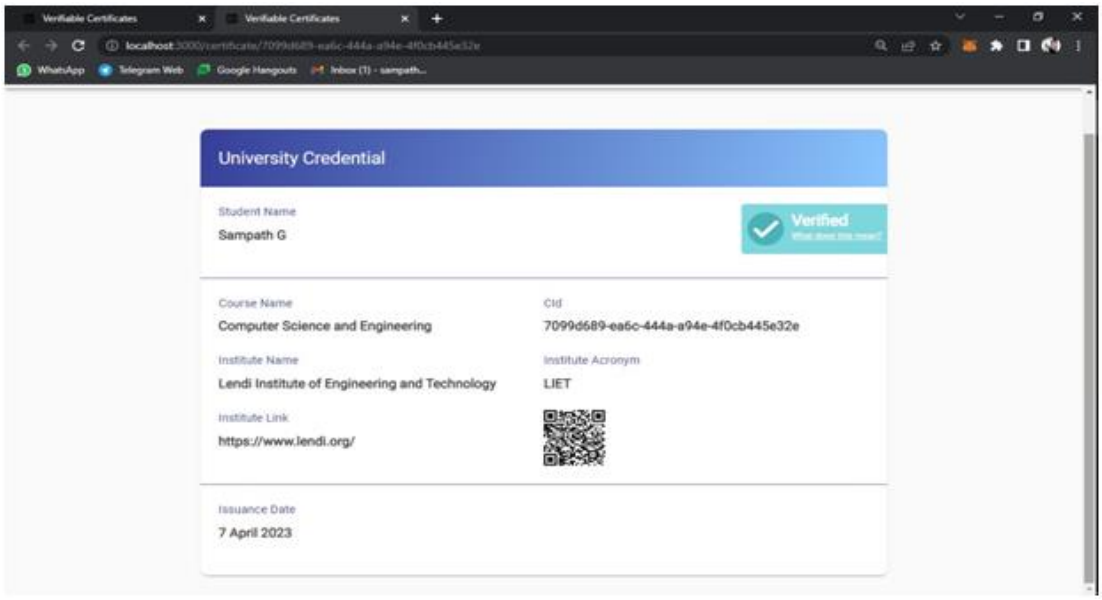


Fig 4.3 Certificate Displayed

5. CONCLUSION:

Public Block Chain technology provides a secure, reliable, and cost-effective solution to the problem of certificate validation. It ensures that the certificates are secure and reliable, and that any attempts to tamper with them are quickly detected and rejected. It also helps to reduce the cost of validation, as the Block Chain system is distributed and requires no central authority.

The use of public Block Chain technology also helps to reduce the risk of fraud. By ensuring that the certificates are securely stored and validated, it helps to protect against any attempts to forge or alter the certificates. This helps to ensure the integrity of the educational system

6. References:

1. S.G.K. Murthy, M.V.R. Murthy, A.C. Sarma, Elliptic curve based signature method to control fake paper based certificates; Proceedings of the World Congress on Engineering and Computer Science 2011 Vol I WCECS 2011, October 19-21, 2011, San Francisco, USA, ISBN: 978-988-18210-9-6 ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)
2. X. Gu, X. Gu, On the detection of fake certificates via attribute correlation. Entropy 17, 3806–3837 (2015). https://doi.org/10.3390/e17063806
3. J.M. Muthoni, A.M. Kahonge, E-verification – a case of academic testimonials (2015) UoN Digital Repository Home (http://erepository.uonbi.ac.ke)
4. K.P. Chavan, R.R. Kamble, P.P. Meshram, K.K. Doke, QR code based digitized marksheet system. Int. J. Eng. Res. Adv. Technol. ISSN 02(03), 24546135 (2016)
5. D. Zheng, K. Kane, L.J. Camp, Detection of rogue certificates from trusted certificate authorities using deep neural networks, ACM Transactions on Privacy and Security, 19(2), 1–31 (2016) https://doi.org/10.1145/2975591
6. M. Li et al. CrowdBC: A Block Chain-Based Decentralized Framework for Crowdsourcing. IEEE Trans Parall Distrib Syst, 30(6), 1251-1266 (2019) https://doi.org/10.1109/TPDS.2018.2881735.
7. Yi, H. Securing e-voting based on Block Chain in P2P network. J Wireless Com Network 2019, 137 (2019). https://doi.org/10.1186/s13638-019-1473-6