RESEARCH ARTICLE OPEN ACCESS

Validating and Enhancing Security of Certificates Using the Ethereum

Dr. U. D.Prasan[1],A. Veda Priya[2],B. Arun Pratap[3],B. Abhiram [4],K. Durga Prasad[5],D. Anil Kumar[6]

[1]Professor&HODofComputerScienceEngineering, Aditya Institute of Technology and Management(AITAM),Tekkali, Andhra Pradesh, India,
[2,3,4,5,6] Students, IV B. Tech CSE, Aditya Institute of Technology and Management (AITAM), Tekkali, Andhra Pradesh, India,

ABSTRACT
Certificates and marks are the key attributes for any Student, over years the verification of these certificates and trackingthe originality of the data provided by students for any kind of admission or Job has been a hectic problem. People and organizations have often taken the help of trusted middle man to check whether the certificates provided by the student are fake or real. This had always been a time taking process and continues to be. Corporate companies do background checks to check whether the given data is true and without any type of misleading data and this makes it tough for them. Also, students face lots of issues trying to preserve their certificates safely as people can access their certificates and falsify their details. To overcome these sets of problems and maintain the security of the certificates we can use Blockchain to issue the certificate with proper verification and can easily be a trusted source for any person or organization. So, we propose the solution of using Blockchain with our project title University Certificate verification using Ethereum and Solidity. This will help the user to store the certificates in a ledger with proper security and can be easily shared with desired person or organization at will with full security guaranteed and these can act as a trusted source.

Keywords – smart contracts, IPFS, Ganache, Certificate Validation, view, Block Chain, Digital Certificate, Ethereum, Hashing

Date of Submission: 18-03-2023 Date of acceptance: 03-04-2023

I. INTRODUCTION

Blockchain is a decentralized digital ledger technology that is used to securely and publicly record transactions. It consists of a series of chronologically connected blocks that contain informational data, like transaction data. Data recorded on the Blockchain cannot be altered or deleted since it is immutable.

One of the core aspects of Blockchain is its decentralized nature. This means that rather than relying on a centralized organization, like a bank or government, to supervise transactions, Blockchain relies on a network of nodes that work together to validate transactions and maintain the integrity of the Blockchain.

Blockchain is the technology behind virtual money like Bitcoin and Ethereum, but it also has a wide range of other potential uses. Decentralized apps, voting systems, supply chain management systems, and other things can all be created with it. Research and development are currently being done on potential applications for the fascinating field of technology known as the blockchain.

1.1 CERTIFICATES IN BLOCKCHAIN

A certificate management system that provides a secure, immutable method of handling certificates can be made using blockchain technology. Here is an overview of how such a system might function:

1. A government creates certificates, which it then uploads to the distributed ledger known as the blockchain.
2. To verify the validity of their certificate at any time, the certificate holder is given a unique code or identification that is linked to their certificate.
3. After a certificate has been confirmed, the Blockchain can be used to check that it was issued by the correct party and that its details haven't been altered.
4.By supplying the special identifier or code, the certificate can be shared with pertinent parties, such as employers or educational institutions. This enables them to swiftly and simply check the certificate's legitimacy.

5.Certificate management is made safe and decentralized via the blockchain, making the system very impervious to fraud and other types of manipulation.
6. The system can be made to be extremely transparent, enabling anyone to inspect the specifics of any certificate kept on the blockchain.

1.1.1 Ethereum

Vitalik Butlerin developed the Blockchain platform Ethereum in 2015. Developers can create decentralized applications (DApps) and smart contracts on this open-source, decentralized platform.

One of Ethereum's distinguishing characteristics is its
support for Turing-complete smart contracts, which enables programmers to create sophisticated applications on the network. This is in contrast to Bitcoin, which only provides limited scripting functionality.

The Ethereum Blockchain makes use of its own digital money, referred to as Ether (ETH), to speed up transactions and reward network nodes. Ether is also used to power apps created on the platform and to cover transaction fees.

A decentralized collection of nodes that validate transactions and carry out smart contracts maintains the Ethereum network. Since there is no single entity in charge of the network, it is immune to censorship and hacking.

Overall, Ethereum has emerged as one of the most widely used block chains enabling programmers to create decentralized applications and smart contracts, and it keeps developing and expanding as new use cases are found.

1.1.2Public smart contracts

Public smart contracts are transparent, publicly available, self-executing programmers that run on a Blockchain network. Without the involvement of middlemen, these contracts are frequently used to automate the trading of digital assets like Cryptocurrency.

The nodes on the Blockchain network carry out public smart contracts, and the code of the contract is available to all users. As a result, the contract's terms are clear and cannot be changed without the network's approval.

Public smart contracts have the advantage of allowing the development of decentralized apps on top of Blockchain networks. Without the involvement of middlemen, these technologies can be utilized to automate difficult procedures like supply chain management.

1.1.3 Private smart contracts

A private Blockchainis a kind of Blockchainnetwork that is intended to be utilized by a select few people or businesses rather than being accessible to the general public. Private blockchains have limited access, and users must be permitted to join, in contrast to public blockchains like Bitcoinor Ethereum, where anybody can participate in the network.

When businesses want to take use of Blockchaintechnology but need to maintain control over who can access and utilize the network, they frequently use private blockchains. This may be helpful for sectors like finance, logistics, and healthcare where it's important to protect sensitive data and adhere to privacy laws.

1.2 PROBLEM STATEMENT:

Certificates play a vital role and these certificates are issued to students in a paper format by the organizations, where everything is centralized and has a minimal amount of proof to be called original. There is no proper decentralized existing system that can easily validate a certificate to be true without any fictitious data in them. The validation of certificates is a very costly and time taking process, which in turn delays various other processes which require certificate validation

1.3 OBJECTIVES:

The objectives of this paperare very clear and open. The main objective of this system is to verify and validate the certificates.

Other objectives of this system are:
1. Obtaining a decentralized system.
2. Securing certificates with unwanted noise in them.
3. Providing trusted sources for the certificates.
4. Access and validation of certificates with ease.
5. Public availability of the certificate in the blockchain.

II.LITERATURE SURVEY

There are many surveys and different applications used in Blockchain certificate management.

Marina, Ninoslav, and Pavel Taskov [1]of title

*Blockchain-based applications for certification management*had considered the factors ensuring security and eliminating fraud, Shortening the time for certificate verification by using the technologies Bitcoin and Ethereum blockchain platform, and encryption algorithms Smart contracts.

Enhancing and streamlining administrative processes is essential. The present certification processes are time-consuming, expensive, and subject to fabrication. By reducing bureaucratic procedures, speeding up certificate verification, and omitting third parties from the process, the implementation of blockchain technology will have a significant impact on certification processes. This programmer provides a transparent, dependable, and robust means to thwart harmful activity, demonstrating the viability of blockchain technology and certification processes.

Jeong, Won-Yong, and Min Choi [2] of the title *The design of Recruitment Management Platform Using Digital Certificateson blockchain*considered the factors of Elimination of inefficiency and social cost problems Difficulties in managing subdivided qualifications using the technologies Hyperledger, JSON-Digital badges, Ethereum, and smart contracts.

The IMS Global Learning Consortium's Open Badges, which are used to earn, issue, and reward badges across many platforms, are compatible with our system's implementation. In contrast to conventional educational systems, the badges are trusted by the IMS standard, the requirements to obtain a badge are confirmed through the network, and the total process is transparent. Also, every certificate awarding event that occurs within our system is documented in a blockchain. One of the things that set our system apart from other systems is this. Once the blockchain has been used to hold the badge award data, it cannot be altered. After that, anyone can use the blockchain to verify the badge's legitimacy.

Maulana, Giandari [3] title *Digital certification Authority with Blockchain cybersecurity in education*considered the Minimize fraud, secure and validate certificates using technologies E-certificate system, Smart contracts. Encryption algorithm.

Blockchain technology's security feature for identifying false certificates is currently quite popular and in use

everywhere. The use of blockchain technology can be convenient, can offer a solution to existing issues, and is also very beneficial for community activities. The electronic certificate system, which verifies the authenticity of the certificate using blockchain technology, is one of the technologies created to carry out the certification process. Blockchain offers several advantages, creates chances for youth, satisfies the skill requirements of business owners, and strengthens relationships between universities and business owners (industrial partners).

Chukowry, Varshinee, GeeaneswariNanuck, and Roopesh Kevin Sungkur [4]of title *The future of continuous learning Digital badge and micro-credential system using blockchain.* Authentication, Course management, Examination of Block, chain Badge Allocation using the technologies Ethereum, React,JS, Sand mart Contracts.

The secret to continuing to be successful and competitive at work is continuous learning. This frequently happens outside of a classroom as well. These days, digital badges and micro certificates are means to identify and honor a learner's accomplishments and specialized abilities. A revolutionary web-based digital badge and micro-credentials system that enables learners to gain the needed abilities is proposed after reviewing the various strategies utilized in existing blockchain-based educational systems.

Ethereum has been used for the Blockchain, and ReactJS has been used to create the front end.

Alam, Tanweer, and Mohamed Benaida.[5] of title*Blockchain and Internet of Things in Higher Education.*This study establishes a connection between blockchain and IoT for the educational system, which employs both technologies. In the proposed study, the IoT and blockchain is combined for the benefit of the educational system. A hyper-distributed public authentic ledger is created using the Blockchain to record the transactions. The study created a fresh opportunity in this field. Several IoT nodes are used to implement and test the framework. This study may serve as a useful framework for enhancing the effectiveness and security of communication in the educational system. This framework is suitable for guaranteeing communication security in the future when large amounts of data are transferred in a heterogeneous environment.We have evaluated the system under many conditions, including memory and processor utilization in the integrated system and how that affects system performance as a whole. We discovered that the suggested framework not only boosts throughput but also establishes direct connections between IoT nodes, increasing system stability. The findings of this study created a new blockchain-based IoT framework for the current educational system. Researchers may expand on this work in the future and use it across the entire kingdom.

III.METHODOLOGY

3.1 PROPOSED SYSTEM:

We propose a decentralized Blockchain-based system that can be used to validate certificates. In this system, every college is entitled to a node in the Blockchain network through which they can push the certificates of the users. In this system, the certificates are denoted with CID, which is a unique identifier for the respective certificate. These certificates are then available publicly to view and validate them.

We use Kaccak 256 algorithm for the encryption of data and we used Smart Contracts to establish authentication and authorization for the system for logging and signing up into the system.

Usage of IPFS software to generate a Unique CID for a certificate using this unique CID to locate the specified certificate in the system to view and validate.

Using this system validation and verification of certificates can be decentralized with added security. This system provides a source of trust as the certificates are pushed into the network with valid authentication and at the same time tampering with them is a herculean task.

3.2 SMART CONTRACTS

Smart contracts are contracts that automatically carry out the conditions of the parties' agreement after being entered into a line of code. These are computer programmers that, when specific requirements are met, automatically carry out a contract's terms without the aid of a third party.

Smart contracts are often carried out using Blockchain technology on a decentralized network of computers, and the outcomes are recorded on a distributed ledger. As all parties can observe the contract's terms and its implementation, this offers a high level of security and transparency.

Following are some essential characteristics and advantages of block chain's smart contracts:

Efficiency: Smart contracts automate many components of a typical contract, eliminating the need for middlemen and hastening and improving the speed and efficiency of contract execution.

Security: Because smart contracts are kept on a decentralized Blockchain network, they are extremely impervious to fraud and tampering.

Transparency: A smart contract is more transparent because all parties can see its conditions, which lowers the possibility of disagreements

Accuracy: Because smart contracts are implemented by the precise terms specified in the code, there is no room for human error.

Savings on time and money: By eliminating the need for middlemen and speeding contract execution, smart contracts may result in time and money savings for all parties involved.

Automation: From straightforward cash transfers to intricate financial instruments, smart contracts can be used to automate a variety of processes.

Overall, smart contracts have the potential to revolutionize the way contracts are executed, by reducing costs, increasing efficiency, and improving security and transparency.

3.2 GANACHE

A personal Block chain emulator called Ganache is employed for testing and development. Developers that create decentralized applications (DApps) on the Ethereum Blockchain frequently use it.

Without having to connect to the main Ethereum network, Ganache enables developers to build a separate Blockchain network that can be used for testing and deploying smart contracts. This is significant because it enables programmers to verify their code's functionality in a secure setting before sending it to the primary network.

Developers can configure their Blockchain networks using Ganache using its user-friendly interface, which also lets them view transaction history and keep track of network activities. Additionally, it offers a selection of tools for testing and debugging smart contracts.

The two versions of Ganache are Ganache CLI and Ganache GUI. Ganache GUI is a graphical user interface that offers a more user-friendly experience, whereas Ganache CLI is a command-line interface tool that can be used to configure and control the Blockchain network.

In conclusion, Ganache is an important tool for Ethereum developers who need to test and debug their smart contracts in a secure setting before releasing them to the live Blockchain network.

3.3 KACCAK 256 ALGORITHM:

keccak256: we use this algorithm to encrypt the data, irrespective of whether the type of data to be encrypted is number or string, the data is converted into bytes32 data type. In this algorithm, the encryption takes place but decryption can't be done, so it is a one-way Cryptographic hash function. This is widely used in Smart Contracts.

3.4 Process:

As discussed above, the system consists of three users and each of them has its own set of flow to do the work. The process in each of the systems is different and unique.

1. **Admin**: An admin creates a node using the Meta Mask wallet and uses the unique Meta Mask id given to the wallet to generate a node along with the college name for which the particular node will be assigned and this process creates the node.

An admin then assigns an institution with the node it has created by entering the Meta Mask id and setting up the password required for the institution which is later on published to the respective institution.

An admin has the access to check the number of

nodes based on the unique Meta Mask Id.
The Authentication and authorization for the admin are done using a smart contract running for the admin for both registration and logging in. This Smart Contract is responsible for all the authentication and error handling during the admin login process.

2. **Institution**: An Institution is a node in our system and it uses the credentials provided by the admin to log into the system. These credentials consist of a unique Meta Mask id and password.
An Institution is responsible for pushing the certificates into the system by entering the Meta Mask and CID or IPFS Hash
A CID is generated by using IPFS software which is supported in Web 3.0, It is a software that stores images and generates a unique id from it known as IPFS Hash or CID.
After entering the Meta Mask id and CID, the certificate is then pushed into the public network of the system, to which users have access.

3. **User**: A User is responsible for validating and viewing the certificates in the network.
A user can view the certificate using the unique roll no and semester details which map it with the unique CID, then the certificate can be viewed with a basic UI template designed in our system.
A user can validate the certificate using the unique CID generated for that certificate and validate certificate and check whether the details are true or not.

3.5 FLOWS OF PROJECT:
The whole system proposed is divided among users with different kinds of access authorization provided to them. In this system, we have 3 different kinds of users who have different roles and work.
The three kinds of users are Admin, Institution, and User.

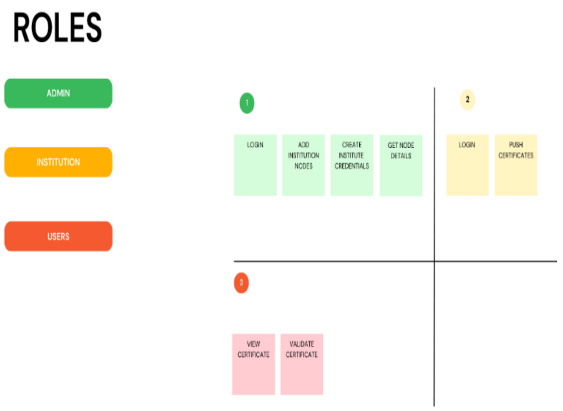


Fig-1: Flow of project

3.3.1. Admin: He is responsible for the creation of nodes in the blockchain system, he also is responsible for creating user credentials for individual institutions with unique MetaMask IDs and passwords. Admin has the access to know the number of Nodes existing in the system.

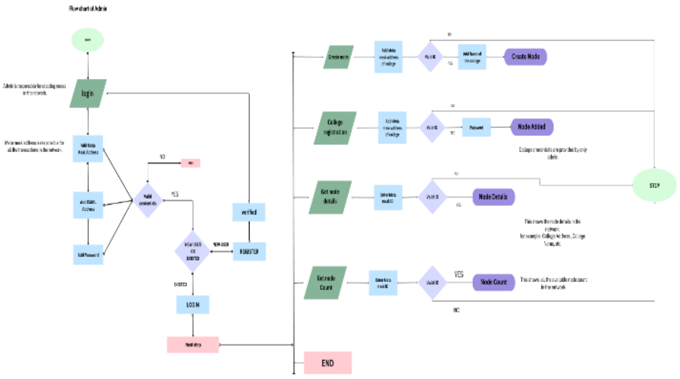


Fig-2: Flow of Admin

3.3.2. Institution: An Institution is a node in our system and it is mainly responsible for pushing the certificates into the blockchain system. It uses the unique credentials provided by the admin.

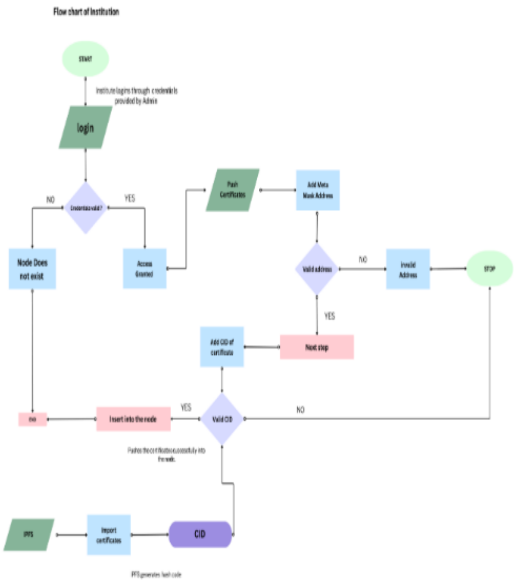


Fig-3: Flow of Institution

3.3.3. User: A User is the backbone of our System. A user has two functionalities which are viewing the certificate and validating the certificate. It is accessible publicly to all users; thus, they can easily view and validate the respective certificates.

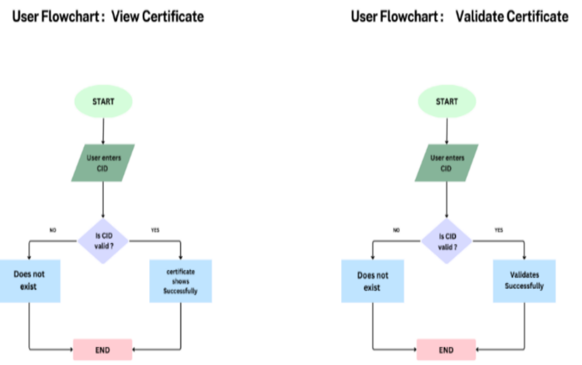
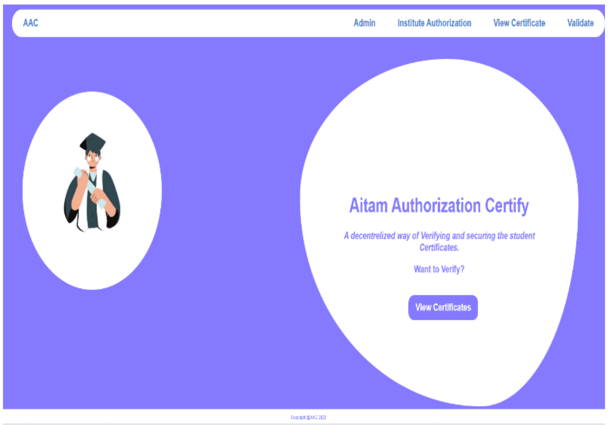


Fig-4: -Flow of User

IV. RESULTS AND DISCUSSION



Aitam Authorization Certify

A decentrelized way of Verifying and securing the student Certificates.

Want to Verify?

Fig-5: Home page

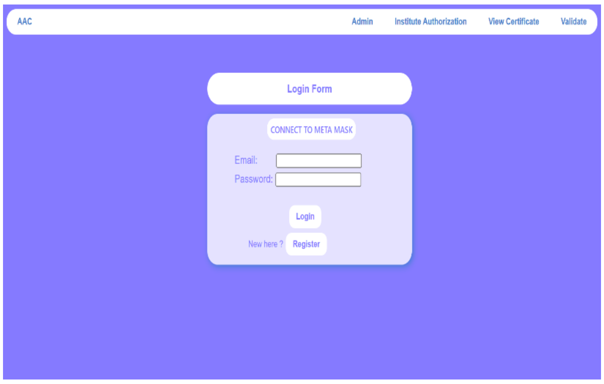
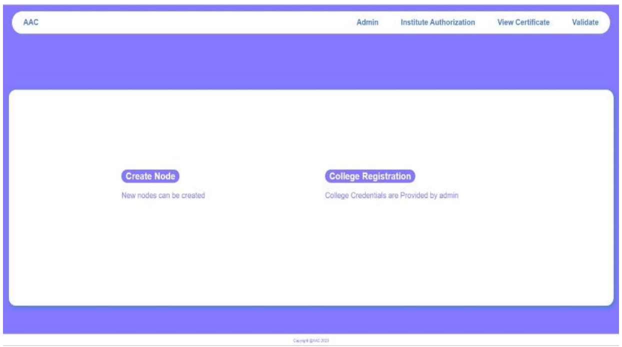


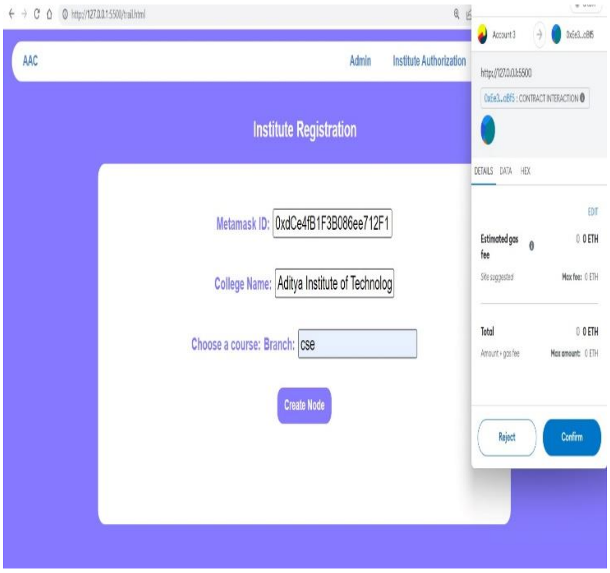
Fig-6: Log in and register into the blockchain by using the MetaMask



New nodes can be created

College Credentials are Provided by admin

Fig-7: we will navigate into the pages that we required like creating new nodes, new college registrations, node count, node details



http://127.0.0.1:5500/trail.html

Institute Registration

Metamask ID: 0xdCe4fB1F3B086ee712F1

College Name: Aditya Institute of Technolog

Choose a course: Branch: cse

http://127.0.0.1:5500

0xEe3...cBf5 : CONTRACT INTERACTION

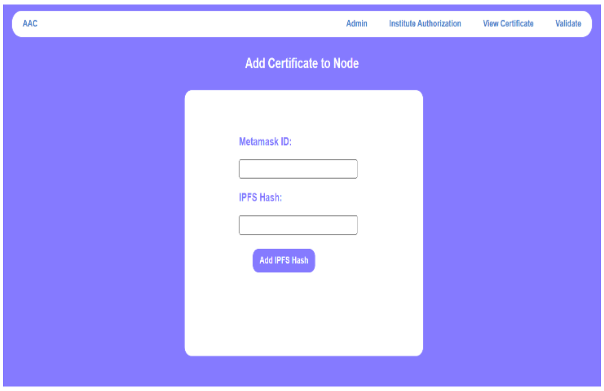
Estimated gas fee 0 0 ETH

Site suggested Max fee: 0 ETH

Total 0 0 ETH

Amount + gas fee Max amount: 0 ETH

Fig: 8: we are adding a college wallet to the blockchain



Add Certificate to Node

Metamask ID:

IPFS Hash:

Fig-9: By using the particular college Id we add the certificates to the node

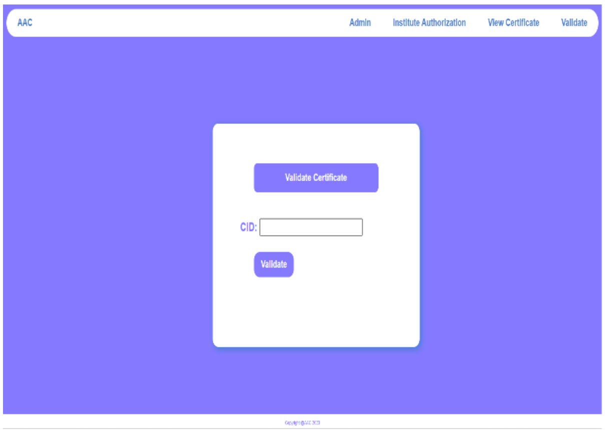


Fig-10: we will validate that the particular certificate present in the Blockchain is not

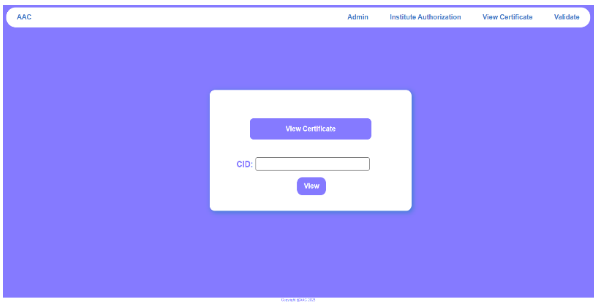
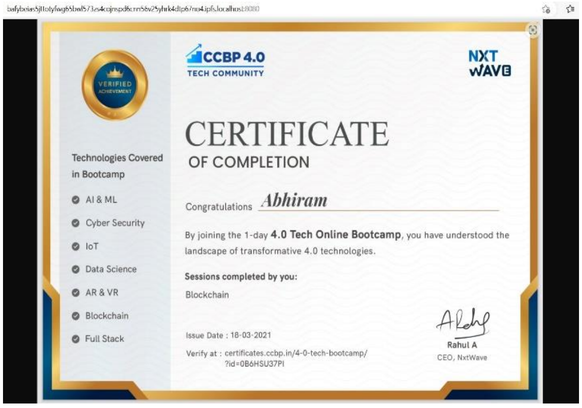


Fig-11: We can view our certificate by using our CID value



bafybeias5jltotyfwg65bwl573zs4cojnspd6cnn56v25yhrk4dtp67no4.ipfs.localhost:8080

CCBP 4.0
TECH COMMUNITY

NXT WAVE

VERIFIED ACHIEVEMENT

CERTIFICATE
OF COMPLETION

Technologies Covered in Bootcamp

- AI & ML
- Cyber Security
- IoT
- Data Science
- AR & VR
- Blockchain
- Full Stack

Congratulations *Abhiram*

By joining the 1-day **4.0 Tech Online Bootcamp**, you have understood the landscape of transformative 4.0 technologies.

Sessions completed by you:
Blockchain

Issue Date : 18-03-2021

Verify at : certificates.ccbp.in/4-0-tech-bootcamp/?id=0B6HSU37PI

Rahul A
CEO, NxtWave

Fig-12: Certificates shown to the user

V.CONCLUSION

To conclude, the blockchain-based system of verifying the certificates and sharing the certificates over a public network is our project which will play a vital role in making the laborious work of checking and verifying certificates at various recruitment, counseling, and interview processes easy and can be done at a very fast pace. Our system is very capable to verify and validate the certificates, which is one of the capable decentralized systems to validate certificates. This is a great system to help people in various fields, such as in Job recruitment, the students can share the certificates in the blockchain with the recruiter and the recruiter need not worry about the details published in the certificates. This system also helps the students to not worry about certificates safety and storage and view the certificates whenever needed. These certificates can easily be shared among different people whenever a need arises and can be viewed.

The limitations of this system are that, the certificates cannot be downloaded and stored but this can be a great addition to the system.

At last, this system can bring a great change to the existing systems and work on the upcoming developments

REFERENCES

[1]. Marina, Ninoslav, and Pavel Taskov. "Blockchain-based application for certification management." Tehnički glasnik 14.4 (2020): 488-492.

[2]. Jeong, Won-Yong, and Min Choi. "Design of recruitment management platform using the digital certificate on the blockchain." Journal of Information Processing Systems 15.3 (2019): 707-716.

[3]. Maulani, Giandari, et al. "Digital Certificate Authority with Blockchain Cybersecurity in Education." Int. J. Cyber IT Serv. Manag 1.1 (2021): 136-150.

[4]. Chukowry, Varshinee, Geeaneswari Nanuck, and Roopesh Kevin Sungkur. "The future of continuous learning–Digital badge and micro-credential system using blockchain." Global Transitions Proceedings 2.2 (2021): 355-361.

[5]. Alam, Tanweer, and Mohamed Benaida. "Blockchain and internet of things in higher education." Tanweer Alam, Mohamed Benaida." Blockchain and Internet of Things in Higher Education." Universal Journal of Educational Research 8 (2020): 2164-2174.