COPY RIGHT

Paper Authors

Vaishnav Koka, G. Praveen Babu

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

BLOCKCHAIN MODEL TO TRACK & VERIFY CERTIFICATES

1 Vaishnav Koka, Mtech in Software Engineering (SE) SIT, JNTUH

2 G. Praveen Babu, Associate Professor of CSE, SCHOOL OF IT, JNTUH

ABSTRACT: In 2018-19, there were over 26.3 million understudies signed up for advanced education in India, and every year, there are near 9 million alumni. A student produces a number of certificates over their whole academic career, whether they are in high school, college, or even a postgraduate programme. These certificates might include results, diplomas, or transcripts. Students must provide these certifications to universities or employers in order to be admitted. It becomes tedious to track these certificates and manually verify their legitimacy. The lack of a suitable anti-forge mechanism results in a situation where it is discovered that the diploma is forged. Everything should be digitalized with the standards of Secrecy, Unwavering quality, and Accessibility to make the information safer and safe. With the use of a technology called Blockchain, all of these are possible. Our system will, in essence, work as follows: a Certificate Issuer will produce certificates, and before sending them to a student, a panel inside that organisation will validate them. Each declaration will have a unique hash key that might be utilized by any business through the entryway to check the testament's validness. A method like this has the advantage of reducing the possibility of a student losing or destroying a certificate and making certificate validation simple.

Keywords: Blockchain, digital certificates, and the creation and verification of certificates

1. INTRODUCTION

Today, possibilities to present new plans of action in generally united commercial centers are made conceivable by blockchain innovation. One of the most troublesome regions where results might be gotten in the medium and long terms is the use of blockchain in the instructive area. One of the areas where blockchain can offer a quick and dependable response is the speedy, solid, and reasonable confirmation of true records, like college degrees. This is made conceivable by the use of generally acknowledged digital forms of money. Consolidated cryptocurrencies like Bitcoin, Ethereum, or Swarm provide a reliable

public blockchain that may be used for additional purposes like a verification tool across many marketplaces. To make an effective plan of action on top of this, picking a suitable public blockchain regarding openness, flexibility, and reasonableness is fundamental.

In India, the crucial configuration of an understudy's schooling is to sign up for kindergarten, then, at that point, move to an alternate school for essential, center, and secondary school courses. Subsequent to moving on from secondary school, understudies should now apply for

admission to junior school. Additionally, there is a second college switch for graduation. This is the fundamental academic year cycle for students. Some students choose to continue their further education after this. The issue with this cycle is that a student must provide all of his certifications for validation at each level. The certificate might be lost or damaged as a result of this. Additionally, the validator finds authenticating each certificate to be laborious. With such a large population, our nation virtually always sees 26.3 million graduates each year. Keeping track of and validating such a large number of records is exceedingly difficult. As a result, tampering and the creation of bogus or duplicate certificates become an unwelcome scenario. There are several covert organisations doing this swindle behind everyone's back in our nation. Up till today, technology has advanced significantly. It will take a lot of focus to distinguish between a fake and an authentic certificate, which will waste valuable time. Blockchain is a technology that has the potential to eliminate this drawback. Why use Blockchain then? because under actual circumstances, data on a blockchain cannot be modified. Even if data is altered, it just takes a moment for us to be informed of the change. A node or piece of data in a blockchain is only confirmed when many parties agree with it. As a result, the system would be authenticated and reliable at all times.
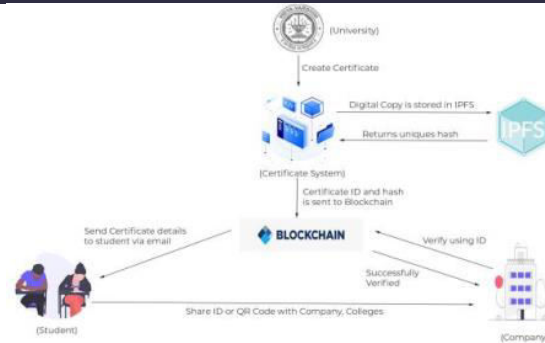

Fig.1: Inter Planetary File System (IPFS) a protocol and peer-to-peer network for storing and sharing data in a distributed file system

2. RELATED WORK

An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends [1]:

As per Zibin Zheng, Shaoan Xie, and others, Blockchain, the innovation that supports Bitcoin, has as of late drawn a ton of interest. Blockchain capabilities as an unchangeable record that empowers decentralized exchange handling. Various enterprises, including monetary administrations, notoriety the board, and the Internet of Things (IoT), are seeing the development of blockchain-based applications. Blockchain innovation actually faces a few snags, including versatility and security issues, which should be settled. This paper gives an exhaustive prologue to blockchain innovation. In the first place, we give a concise prologue to blockchain engineering prior to differentiating a few normal agreement procedures applied across different blockchains. Additionally

momentarily tended to are innovative hardships and ongoing progressions. We additionally frame potential blockchain improvements later on.

Blockchain and Smart Contract for Digital Certificate [2]:

Narn-Yih Lee, Jiin-Chiou, and others, The blockchain-based computerized testament framework would be proposed as an answer for the issue of declaration imitation. The blockchain's changelessness took into consideration the making of advanced authentications with against fake and certainty. In this framework, giving advanced declarations is finished in the way recorded underneath. Make an electronic duplicate of the paper declaration alongside any important information and enter it into the data set first. Meanwhile, decide the electronic record's hash esteem. The hash worth ought to then be added to the block in the chain framework. To be connected to the paper endorsement, the framework will produce a connected QR-code and a request string code. Through cell phone examining or online hunts, it will empower the interest unit to affirm the authenticity of the paper testament. The arrangement not just builds the authenticity of assorted paper-based authentications, yet in addition radically brings down the risk of testament misfortune because of the unchangeable qualities of the blockchain.

BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability [4]:

A circulated record framework called the Interplanetary File System (IPFS) expects to decentralize the web and make it speedier and more compelling. It utilizes notable advancements like BitTorrent and Git to assemble a data sharing multitude of processing units. IPFS has had critical progressions and reception from both confidential people and business substances since its send off in 2016. Clients can share documents and data all around the world on the grounds that to its scattered organization. Enormous documents that might require a great deal of data transmission to transfer or download over the Web work well with IPFS. This appropriated document framework has acquired fame rapidly to some extent on the grounds that IPFS is worked to run on top of numerous conventions including FTP and HTTP. In any case, there are fundamental security and access control gives that should be tended to, for example, the powerlessness to follow how records are gotten to. To consolidate IPFS with blockchain innovation, this article proposes a clever technique (BlockIPFS) that leaves an unmistakable review trail. Utilizing blockchain as a help, BlockIPFS empowers us to expand the information's unwavering quality, initiation security, and give an immediate way to follow back every type of effort associated with a particular record.

3. PROPOSED SYSTEM

Blockchain innovation offers various likely advantages for far and wide advanced education, learning, and development, including the quick and secure confirmation and check of understudy accreditations.

Moreover, they could allow producing to evidence adaptations to be inspected and guarantee the classification and honesty of their imprint confirmations. Moreover, the changelessness, availability, or serious level of safety essential for keeping up with the information records cause no extra expenses.
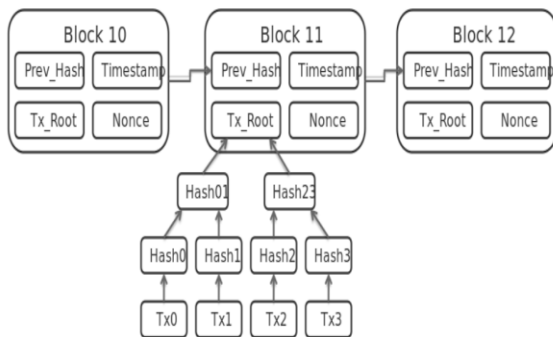

Fig.2: Structure of transactions and data blocks linked in a blockchain

FUNCTIONALITIES:

1) Blockchain: Blockchain, which served as the basis for the whole project, is best understood as an immutable database. It offers a reliable setting where what has been done is clear and unchangeable.

2) Ethereum: Decentralized and open-source, Ethereum is a Blockchain that supports brilliant agreements. Ethereum is the most ordinarily utilized and most expensive digital currency after bitcoin, and it is additionally the best exhibit of blockchain innovation.

3) SmartContract: At the point when a client makes a move, shrewd agreements is a piece of code that sudden spikes in demand for a Blockchain. A shrewd agreement might

be written in different dialects, including undeniable level dialects like Strength that are basically the same as Typescript and low-level dialects like C++ and Java.

4. CERTIFICATION AND VERIFICATION OF DEGREES BASED IN BLOCKCHAIN/BLOCKCERTS

The strategy starts once an understudy procures their certification and cases their title, subsequently the association — in this model, the college or advanced education foundation — will remind the understudies to request that they have their new titles recorded on the Blockchain. Whenever we have gotten every one of the reactions from the understudies, we can gather a rundown utilizing the cert-devices to create the supposed bunch of testaments, which contains the information that will be all stepped in the resulting stage utilizing the cert-backer. The cert-guarantor is utilitarian, yet for this wide outline, we will just zero in on the cycle that changes over a bunch of unsigned endorsements into a group of marked blockchain declarations. To finish this stage and pay for the blockchain exchange that will incorporate all of the data relating to our Testaments, you should likewise have some digital currencies like Bitcoin or Ethereum in your wallet. The last significant part, cert-verifier-js, isn't utilized in the issue cycle yet is still exceptionally vital for note since it controls the whole interaction in switch, doing every one of the fundamental stages to confirm that the declaration is marked and associated with

International Journal for Innovative Engineering and Management Research
A Peer Reviewed Open Access International Journal
www.ijiemr.org

the claimer, for this situation the graduated understudy.

(i)   Student's usage

From the outlook of the understudy, the system will be easier in light of the fact that the association handles an enormous part of the declaration giving cycle. The cycle for getting an understudy keen on having their certification put away on a blockchain is very direct. The college will email the understudy when the title-giving methodology has started to catch their wallet data and connection the authentication to their wallet. The understudy wallet will have a public key and a confidential key, very much like each and every wallet on the blockchain. The pass expression that creates the confidential key and fills in as a wallet will be the understudy's liability to store in a protected vault. On the off chance that the understudy loses the pass expression data, they will be expected to build another wallet and recover the title issue. Also, the framework will just require the public key to make the title, which will act as the understudy's particular, unmistakable character. To make things more clear, the understudy will be responsible for making their own ID on the blockchain and will just give the framework the number that extraordinarily distinguishes it. At the point when the title is at last just held by the understudy, no extra information will be saved in the framework or blockchain, which expands the cycle's security.

5. BLOCKCHAIN TECHNOLOGY FEATURES

Blockchain [1] is a state of the art innovation that makes the way for new sorts of dispersed programming models. With these models, parts can come to settlements on their common states for decentralized and value-based information sharing across a tremendous organization of untrusted members without depending on a focal joining point that ought to be relied upon by all framework parts. The blockchain information structure, which accumulates and stores data pretty much all exchanges that have at any point occurred inside the blockchain network, is a period stepped rundown of blocks. To keep away from control and adjustment, the blockchain offers a permanent information store that main licenses adding exchanges and disallows changing or eradicating any recently recorded exchanges. Digital forms of money, which have been a critical peculiarity over the course of the past year because of their likely utilization of the innovation, are the most notable Blockchain use. The biggest and generally critical of them is Bitcoin [6], and along with later ones like Ethereum, they are presently driving the digital money market with more than 1.600 different currencies4, and their market cap, which was near a trillion bucks last year however is currently north of 300 billion, is the biggest of every one of them.

6. MODULES

As many fake certificates are utilized to acquire occupations and there is no ongoing innovation to identify such phony endorsements, in this venture we are utilizing Blockchain innovation to store scholastic authentications to keep away from declaration fake. To forestall such fraud we are utilizing Blockchain based testament check.

1)   Admin or AICTE Module: After entering the credentials "admin" and "admin," the administrator can access the system by following the steps below.

a)   Add Verification Officials: Using this module, the administrator can add multiple verifier officials, including SSC, Intermediate, PHD, and PG verifiers.

b)   Upload Verified Certificates to Blockchain: Using this module, the administrator will upload verified certificates to Blockchain. For each certificate image, a single hash code will be generated and saved in the blockchain memory. Blockchain compares the test certificate's hash code to the stored hash code each time we upload a test certificate; in the event that a match is found, the endorsement is confirmed, and the proprietor's data is recovered and shown; Otherwise, the certificate authentication fails.

c)   Search Verified Certificates: The administrator will upload a test certificate to this module. The program will then use the certificate to create a hash code and compare it to pictures on the Blockchain; The certificate will be recognized if a match is found.

2)   Verify Officials Login: Officials will log into the program using the admin user's username and password to upload and view certificates.
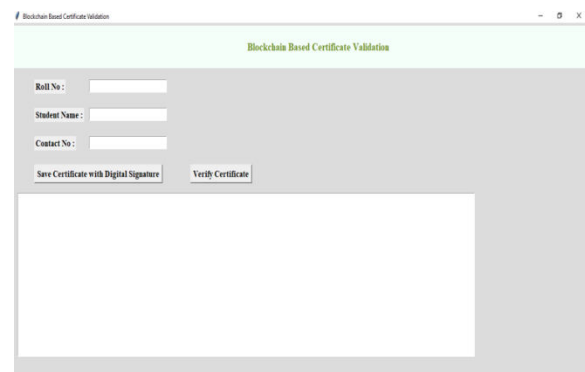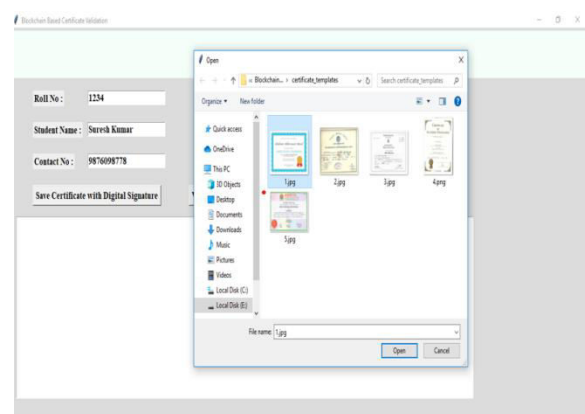
7.   EXPERIMENTAL RESULST

Fig.3: Home screen
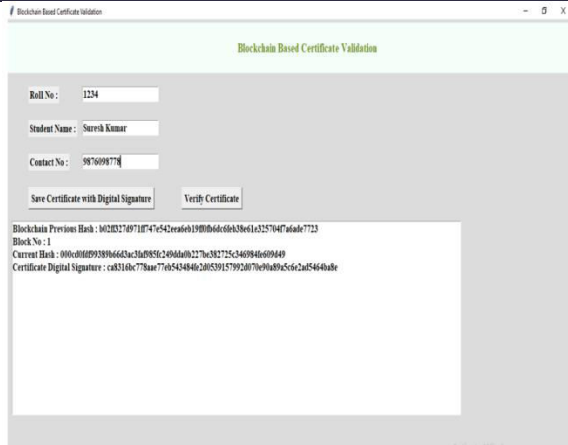

Fig.4: Save certificate with digital signature
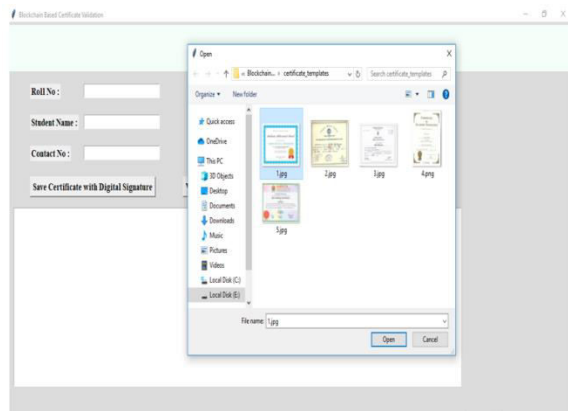
Fig.5: Blockchain generated hash
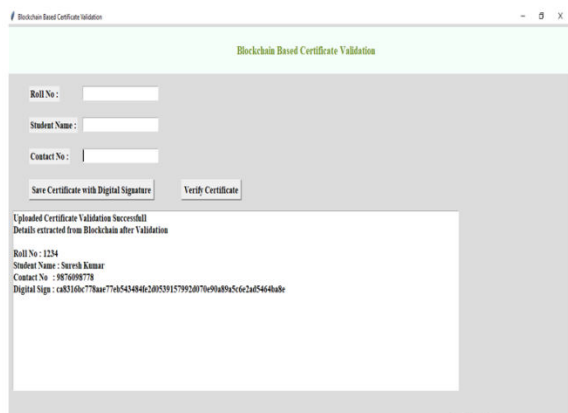

Fig.6: View certificate

Fig.7: Verification of certificate screen

8. CONCLUSION

One of the key characteristics of Blockchain is the creation of immutable ledgers. We can create a system where each step of the process is clear and unchangeable with the help of this behavior. The process of creating certificates is made easier by our system, which also reduces the amount of manual labor required for their verification. Additionally, there is a comparably minimal chance of credential loss for students. We reduce the amount of data that has been altered by utilising an extra hashing technique. The blockchain is used to store the certificate's hash.

9. FUTURE SCOPE

This thesis looked at a variety of counterfeit-reduction strategies. To reduce reliance on outside factors, these modifications were taken into account and their effect on reducing counterfeits was evaluated. It was not possible to implement all of the requested improvements due to time restrictions and the fact that various other system upgrades were also necessary. The next stages include finalising these implementations for the suggested system and maybe launching pilots. The idea and implementation for minimising fake goods in the supply chain for humanitarian aid are presently being explored.

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, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," Proceedings of IEEE International Conference on Applied System Innovation 2018.

[3] 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.

[4] 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.

[5] 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.

[6] Shi, N.; Tan, L.; Li, W.; Qi, X.; Yu, K. A blockchain-empowered AAA scheme in the large-scale HetNet. Digit. Commun. Netw. 2020, 7, 308–316. [CrossRef]

[7]. Capece, G.; Levialdi Ghiron, N.; Pasquale, F. Blockchain Technology: Redefining Trust for Digital Certificates. Sustainability 2020, 12, 8952. [CrossRef]

[8]. Turkanovi´c, M.; Hölbl, M.; Košiˇc, K.; Heriˇcko, M.; Kamišali´c, A. EduCTX: A blockchain-based higher education credit platform. IEEE Access 2018, 6, 5112–5127. [CrossRef]

[9]. Feng, W.; Li, Y.; Yang, X.; Yan, Z.; Chen, L. Blockchain-based data transmission control for Tactical Data Link. Digit. Commun. Netw. 2020, 7, 285–294. [CrossRef]

[10]. Lutfiani, N.; Aini, Q.; Ali, M.I.; Wijayanti, L.; Nabila, E.A. Transformation of Blockchain and Opportunities for Education 4.0. Int. J. Educ. Learn. 2021, 3.

[11]. Aamir, M.; Qureshi, R.; Khan, F.A.; Huzaifa, M. Blockchain Based Academic Records Verification in Smart Cities. Wirel. Pers. Commun. 2020, 113, 1397–1406. [CrossRef]

[12]. Song, J.; Zhang, P.; Alkubati, M.; Bao, Y.; Yu, G. Research advances on blockchain-as-a-service: Architectures, applications and challenges. Digit. Commun. Netw. 2021. [CrossRef]

[13]. Graf, M.; Küsters, R.; Rausch, D. Accountability in a Permissioned Blockchain: Formal Analysis of Hyperledger Fabric. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P), Genoa, Italy, 7–11 September 2020; pp. 236–255.

[14]. Peng, L.; Feng, W.; Yan, Z.; Li, Y.; Zhou, X.; Shimizu, S. Privacy preservation in permissionless blockchain: A survey. Digit. Commun. Netw. 2020, 7, 295–307. [CrossRef]

[15]. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sustain. Energy Rev. 2019, 100, 143–174.