STUDENTS' DOCUMENT VERIFICATION PORTAL

A PROJECT REPORT

for

INFORMATION SECURITY MANAGEMENT

(CSE3502)

in

B. Tech (Information Technology)

by

KSHITIJ DHYANI (Slot: F1)

(18BIT0131)

SUBHRA PALADHI (Slot:F1)

(18BIT0191)

JAHNAVI MISHRA (Slot:F1)

(18BIT0243)

Winter semester, 2021

Under the Guidance of

Prof. SUMAIYA THASEEN I

Associate Professor Grade 1, SITE

PROBLEM STATEMENT:

Idea:

Colleges are very intensive when it comes to placements, but every time a student is placed, the employing company asks for document verification from the college. The college then finds the details and manually communicates the information to the employing company. This has many loopholes. Essentially there is no guarantee of integrity and authenticity of the data provided, and the manual labor involved proves to be very slow in nature. Moreover, the data is open to manipulation by the providing authorities and is vulnerable to hacking. The security of this data is essentially very weak, in contrast to how important it can prove to be in students' life and professional career. We propose a blockchain-powered storage ledger, which stores the documents of the students inside a blockchain, this ensures that the data is tamper-proof and is 100% authentic. Moreover, to eliminate the manual labor our proposed technology provides a web interface, which includes many features such as one -tap retrieval of all information of the required students, student searching based on skill keywords, additionally, we provide protected transcripts of the students as well as graphical visualization of the student details for better understanding, using graphs and maps. Our proposed technology solves all present challenges in the industry and provides a prudent alternative for faster and more reliable data exchange between the employer and the college.

Scope:

This model can be used to create a blockchain-based datastore to store and manage various documents of students. When a student joins the college, at that time all the required documents will be verified and uploaded to the blockchain. After that, whenever a company wants to hire a student and need the document, it can be directly shared. This will make sharing of the student details and documents very easy and at the same time guarantee that the documents are correct.

➢ Novelty:

A major concern for the recruiters is the authenticity of the academic records and the documents submitted by the students at the time of placements. With the advancements in technologies, generating fake documents has become very easy. Also the alteration in records is no big deal nowadays. Usually the methods used for the verification of academic records by the universities are more tedious, time consuming. Either it is done manually which is not at all feasible when the number of students is high and is also error prone or techniques like QR code generation and scanning, hashing techniques, watermarking techniques are used for the verification. All these are time consuming when the number of students is very large. But in our proposed model we are using blockchain based techniques. So all the documents of the students will be uploaded at one place and forgery is also not possible and is not at all feasible. So in this way the authenticity and integrity of the records will be maintained and can be accessed by the recruiter during the time of need.

Literature Survey:

1. On Automatic Authenticity Verification of Printed Security Documents: [1]

This paper provides the first attempt to engage the machine in testing the authenticity and integrity of the document. A certain category of security documents is considered for the current test. Bank cheques, several types of tickets like lottery tickets, plane tickets, etc. Criminal attempts to produce a counterfeit version of these texts are on the rise. This study aims to develop a standard framework for verifying the authenticity of such security documents. The proposed method begins by computerizing the security features in the text images and then the concept of authentication is compared to the redefined location in the feature space. Bank audits are considered a research guide. Support Vector Machines (SVMs) are used to verify the authenticity of these cheques. Offline kernel functions are used to perform this test. The results show that polynomial kernel based SVM provides approximately 99.5% accuracy of seemingly accurate bias testing. This powerfully approves the effectiveness of the projected authentication method for secure paper documents.

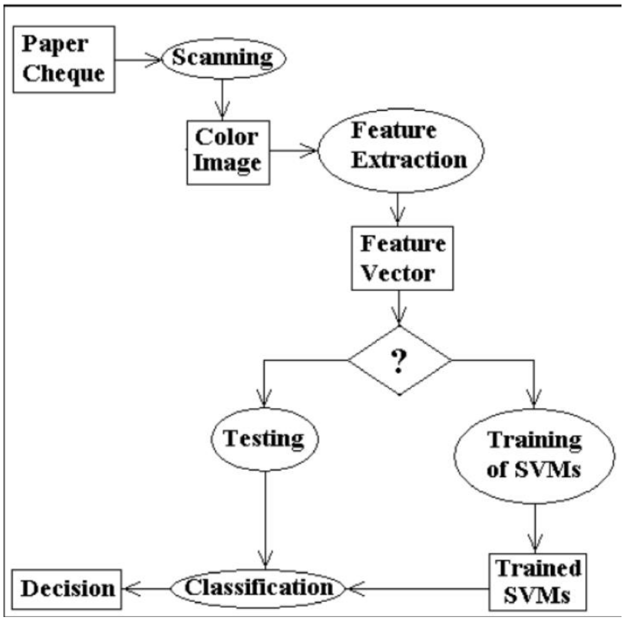

Fig 1: Proposed authentication system [1]

The proposed methodology is as follows. Bank cheques are scanned as color images and then features are extracted from both genuine and fraud bank cheques. Support vector machines (SVM) are used for designing classification element. A set of characterized samples is used to train the SVMs. Next another set of samples is used to authenticate the classification accuracy. The proposed framework is a feasible and a low cost and effective solution.

2. Automated Batch Certificate Generation and Verification System [2]

In this paper a client server based certification generation and verification model is proposed to decrease the processing time of the generation of certificate and to minize the efforts in verifying the authenticity and integrity of the certificates manually.

This model allows the user to define the template of the certificate and certificate format without any prior knowledge of XML just by using few buttons from the system GUI, verifying the certificates and generating multiple certificates simultaneously.

- The four elements of the model are as follows:

1. Template Creation
2. Certificate Generation
3. Certificate Verification
4. Upload module

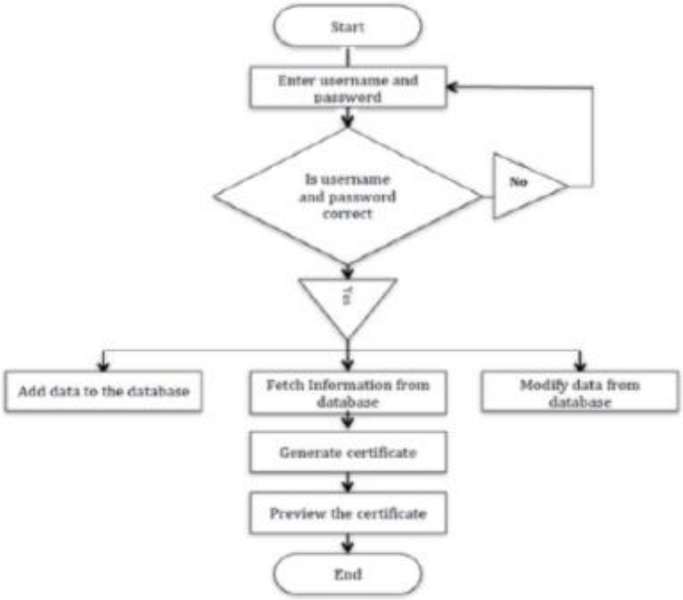
Start
Enter username and password
Is username and password correct
No
Yes
Add data to the database
Fetch Information from database
Modify data from database
Generate certificate
Preview the certificate
End

Fig 2: System Flowchart [2]

This model can be widely used by institutions at low cost and it is feasible. Also generation of multiple certificates of desired template and their verification happens using a single model. So it is less time consuming as it is automated.

3. An Online Verification System of Students and Graduates Documents and Certificates: A Developed Strategy That Prevents Fraud Qualifications [3]

Verification of the student records and academic documents like certificates,degree and all is still a difficult task for universities all around the world. The traditional ways include mails or verification in person. But this is still a very tedious and not so feasible method. Also a very crucial step of recruitment procedure is to go through resumes and Letter of recommendation and other qualifications of the apllicants and make sure that all of them are genuine and authentic.

Hence in this work a model has been proposed to standardize the whole procedure.
A unified e- portal is designed to make a whole procedure smooth and effort less and more convenient for both the students as well as the universities and recruiters.

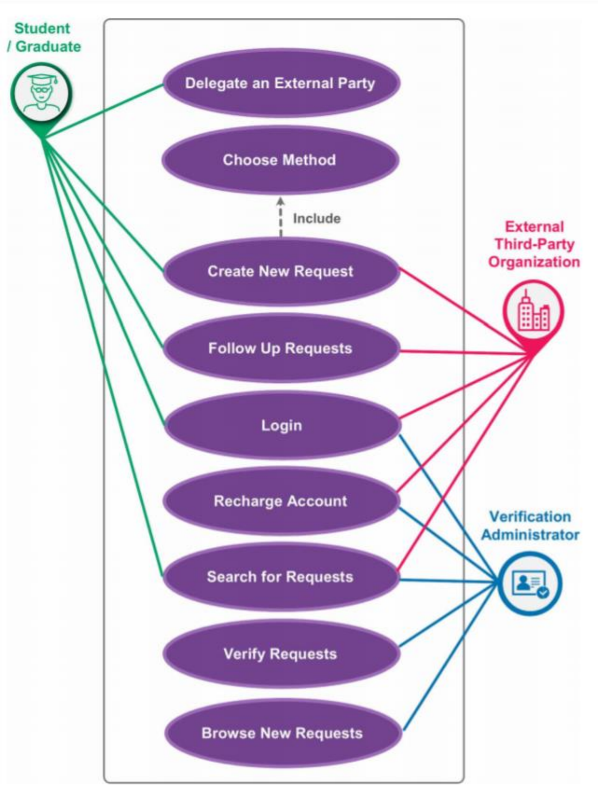

Fig 3: UML usecase diagram of the model proposed [3]

The implementation of the proposed model is done in various stages.
They are as follows:
The traditional and current practices of document verification are discussed with the stakeholders to have an idea of the pros and cons of each practice and to come to a conclusion with the best solution.

The system interfaces are designed and programmed using Active Server Page (ASPx) and HTML5.Work is done on graphics and new software interfaces. Usecase models are made to have an idea of the needs of all the parties

The model is designed from both the perspectives. The perspective and needs of the students are kept in mind, perpective of external parties is also taken care of.

Then the administration and monitoring of the system is taken care of.
The results of this study indicated the crucial development of higher educational institutions in the Gulf and Arab States which illustrates the positive feedback and hence calls for constant improvements and updations.

4. A Generic Certificate Verification System for Nigerian Universities [4]

The certificates that are issued to the students by the universities are very crucial for them as it acts as a proof of learning and also a recognition granted to students for their achievements. But with the advancements in technology, fake certificates can be easily made using photoshop and various printing techniques. Certificates of various institutions can be forged easily and the detection of this forgery becomes very difficult.

Hence to address these issues a model has been proposed in this paper. It is called Certificate Verification System for Institutions (CVSI) which is designed using a top down design approach and an iterative SDLC model.
PHP and javascript are used for making the front end design of the model. In the existing system, MySQL database is used but the proposed model has some improvements and hence MongoDb with is a NoSQL database is used for storing certificates due to its better flexibility and durability.
Coming to the proposed method for certificate verification, the university gives a secret number to each graduate with the certificate to maintain confidentiality. Three parties should be involved in this verification process.

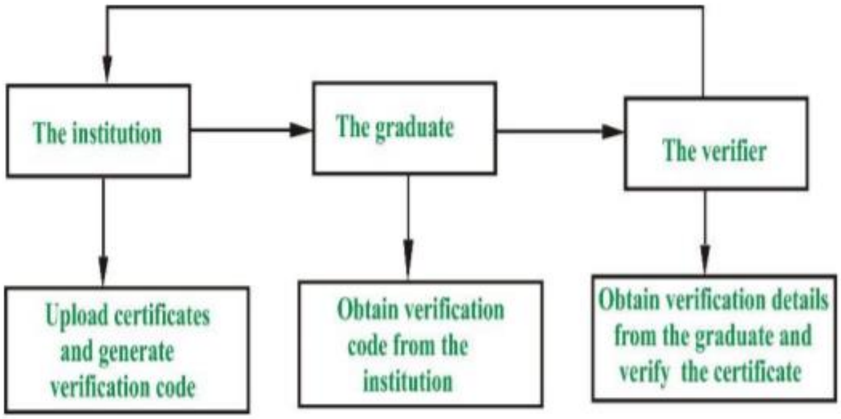
The institution
The graduate
The verifier
Upload certificates and generate verification code
Obtain verification code from the institution
Obtain verification details from the graduate and verify the certificate

Fig 4: Proposed method for certificate verification [4]

All the components of the system algorithm (such as different subprogram/modules designed separately) are integrated to become a single program and then test run.

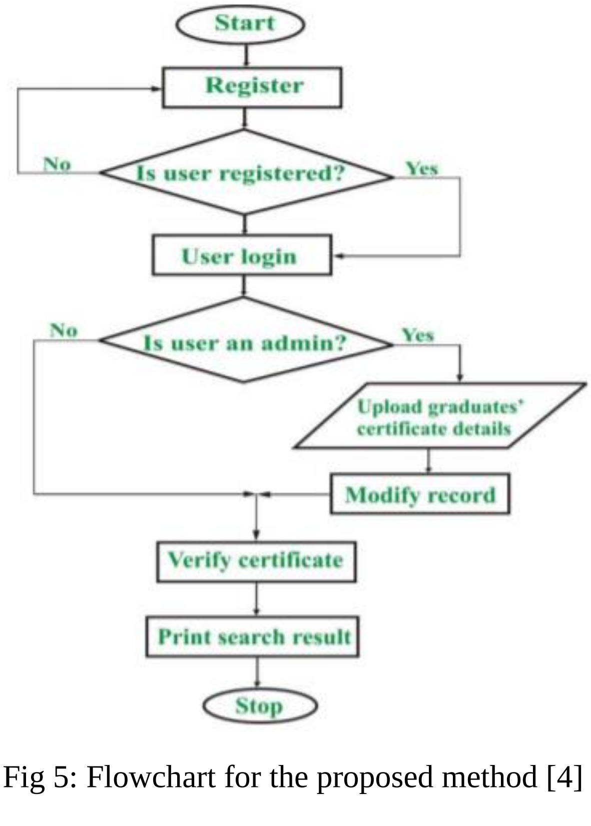

Fig 5: Flowchart for the proposed method [4]

This method is more affordable and feasible as compared to traditional methods like manual verification, verification using QR code, watermarking and biometrics which are very cost consuming and hence less convenient for students as well as universities.

5. An Authentic and Secure Printed Document from Forgery Attack by Combining Perceptual Hash and Optical Character Recognition:[5]

The employment of printed documents is still frequently used. Among them are certificates, forms, diplomas and important letters. This has the possibility to be subjugated by negligent parties by faking documents or forgery attacks.
In this paper, a new scheme is proposed to detect forgery attacks to maintain the authenticity and integrity of the documents. In this scheme, the physical document verification process is done through the combination of OCR (Optical Character Recognition) and QR Code methods. The hash value is then signed to produce a digital signature from the document creator. Through the mechanism of hash values, signatures and QR Codes, physical documents are authentic and safe from forgery attacks text modification.

This method involves two stages: The process of creating documents and the verification of the physical document.

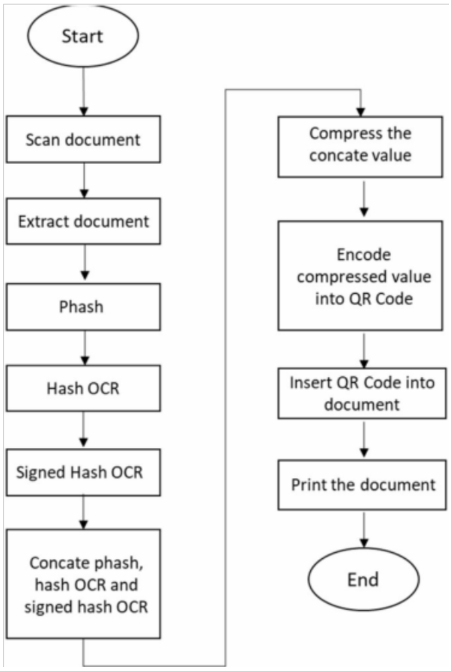
Start
Scan document
Extract document
Phash
Hash OCR
Signed Hash OCR
Concate phash, hash OCR and signed hash OCR
Compress the concate value
Encode compressed value into QR Code
Insert QR Code into document
Print the document
End

Fig 6 : Creation of the document [5]

In the document verification stage, perceptual hashes are used to extract all parts of the document. The textual part that is present in the document's scanned images is extracted using OCR and hash is generated using SHA-256. The hash value and sign value are encoded into a QR code and then put in the document. Then the QR code reader will read the QR code given in the document and test its authenticity and integrity.

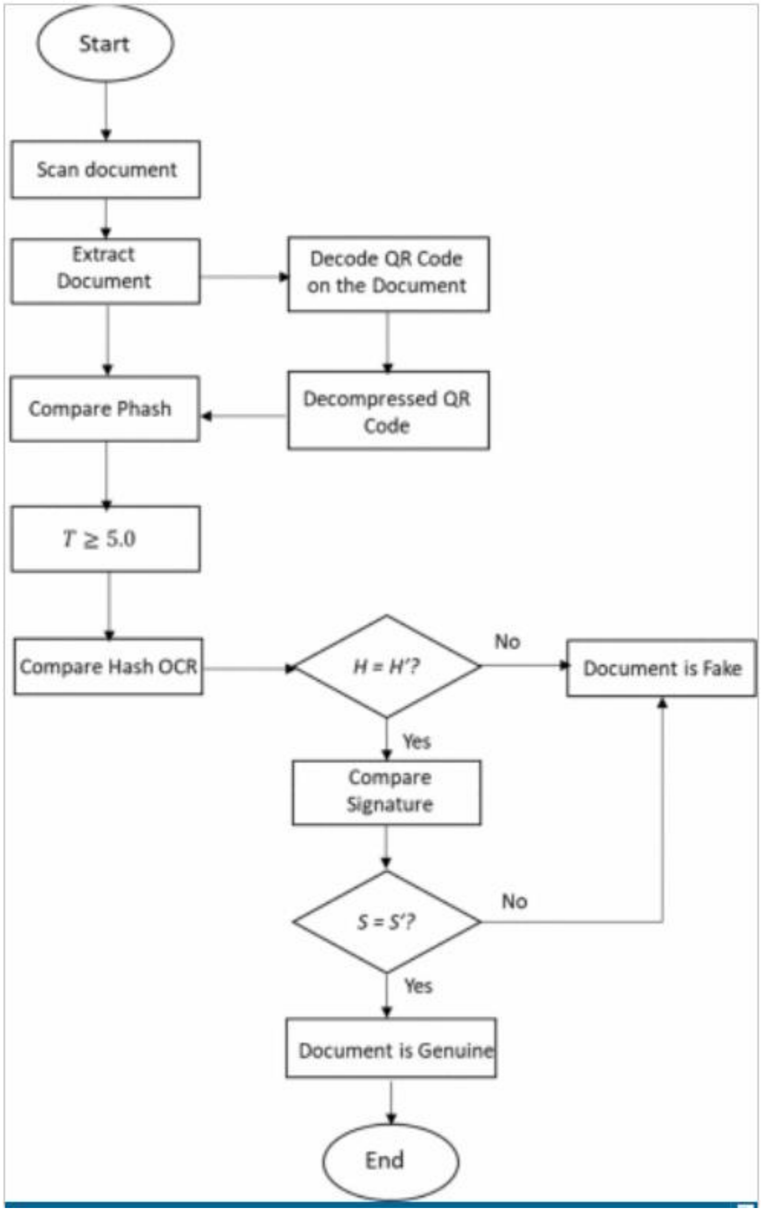

Fig 7: Flowchart for the document verification phase [5]

The combined usage of OCR and perceptual hash proves to be an effective method but comparatively cost consuming and can not be afforded.

6. Bitcoin: A Peer-to-Peer Electronic Cash System [6]

In this paper, the author Satoshi Nakamoto writes about bitcoin which was the first blockchain. Blockchain is a peer-to-peer system that does not require a central authority through which the operations(transactions) on the blockchain need to be verified or approved from. A trust-based system has a central authority that verifies the transactions which is a bottleneck in the whole system. If the central authority is breached or gets corrupted or goes down then the whole system goes bust. Blockchain is based on cryptographic proof instead of trust.

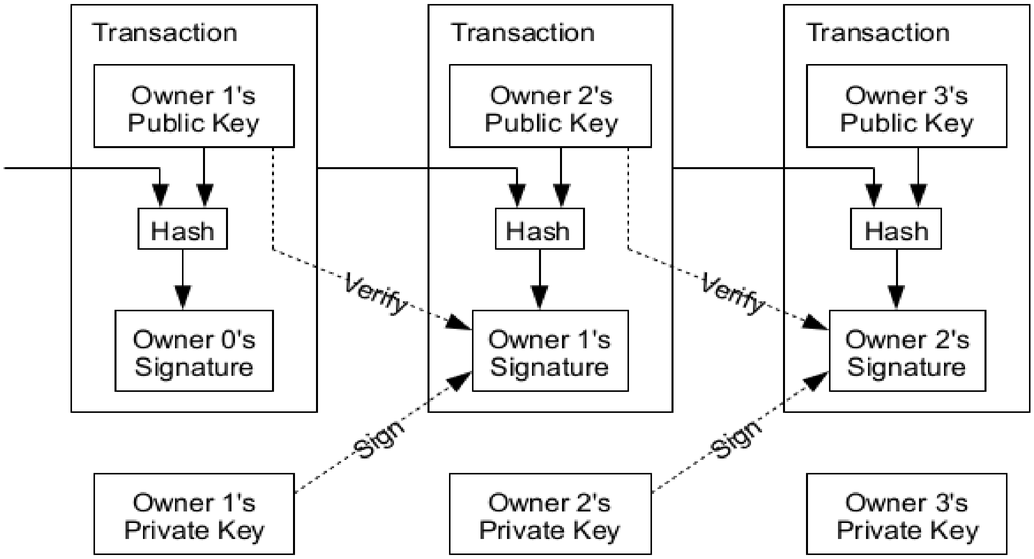

Fig 8: Structure of blocks in a blockchain [6]

Each block has its own unique hash, the hash of the previous block, sender's and receiver's encrypted identifier. If something is changed in the block's data then the hash value is also changed.

For a transaction to be confirmed, each transaction is publicly announced. The majority of the nodes in the blockchain network need to agree to the transaction. A distributed timestamp server is required for this process. It is implemented using the proof of work concept. To get the proof of work, a hash needs to be calculated with the required number of zeros. A nonce is used which is incremented until the required hash is generated. The proof-of-work calculation is a one-CPU-one vote system. To change one block on the chain, the attacker has to calculate the hash for that block and all the block after that and surpass the original chain. For this, the attacker has to get control of at least 51% of the total processing power(CPUs) on the network which makes it almost impossible.

Nodes consider the longest chain to be the correct chain and works on it. If two nodes broadcast different versions of the next block simultaneously. The nodes consider the block they receive first as the correct branch and saves the other one in case it becomes longer. When the next block is created and it gets added to one of the chains, that chain becomes longer and all the nodes that shift to this chain. If a node fails to receive a block, it requests it when it receives the next block.

7. On Immutability of Blockchains [7]

Immutability is essential in a blockchain as it provides a guarantee that the information in the chain is valid and every transaction that ever occurred has been recorded which increases the transparency of the system. To obtain immutability blockchain depends on a computationally hard problem. To change 1 block in the chain, the work for that block and for all the blocks in the chain after that need to computed and this chain needs to outpace the original chain.

This work proposes a single party protocol. It can be used for permissioned blockchains. Permissioned blockchain can be used at places where traditional institutions like Governments were used to mediate between entities that were mutually mistrusting. For such a situation, a blockchain will work as it is a trusted immutable and secure ledger. As such a network will be comparatively small, proof-of-work doesn’t provide the required level of security as it will require a comparatively small number of systems to go rouge and rewrite the original chain. For permissioned blockchains, proof-of-sequential-work is required. In this, each node in the network maintains its own proof-of-sequential-work chain. The personal chains are connected to the ledger chain by adding Merkle pointers to the block. Personal chains will have the Merkle root and the ledger chain has the Merkle path to the proof-of-sequential-work, the pointer to the ledger block and the signature.

8. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends [8]

Smart contracts are computer protocols that verify and enforce a contract between multiple parties on a blockchain. Ethereum was the first blockchain to implement complex smart contracts. Ethereum has Ethereum virtual machine(EVM) to create runtime for executing smart contracts. It can be used to create decentralized applications(dApps).

Smart contracts are made up of "If-Then" statements which acts are trigger conditions. A transaction can trigger a contract and gets stored in the blockchain if it is a valid transaction according to the contract.

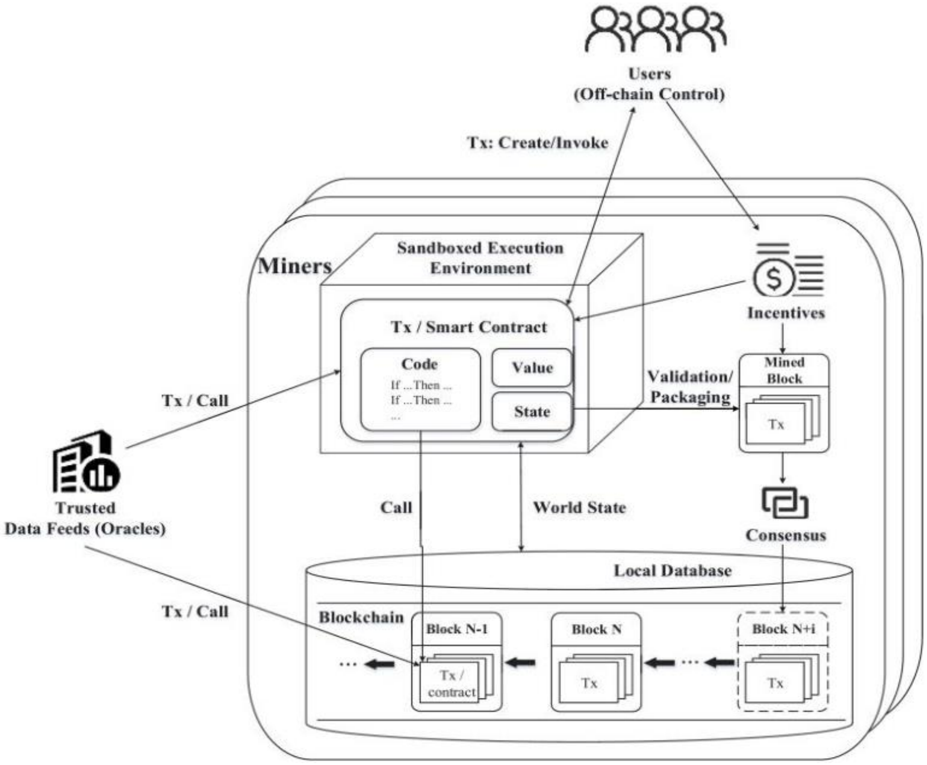

Fig 9: Operational mechanisms of smart contracts [8]

Smart contracts have application in finance, E-Government, organizational management, energy distribution etc. Smart contracts are decentralized, verifiable, enforceable and can be executed between distrusting parties without the requirement of a trusted authority.

9. Blockchain versus Database: A Critical Analysis [9]

Blockchain has the potential for wide usage due to its distributed data storage and immutable behaviour. In this work, the authors have analysed how blockchain is being implemented effectively in various use cases.

a. Everledger have used blockchain in the diamond supply chain to maintain an audit trail to increase transparency. Blockchain can be used in such a place as all transactions in the chain are verified by all the nodes and the transactions are immutable.

b. International money transactions in the current system take 2-3 business days. Bank of Canada is working on a blockchain-based distributed ledger using crypto-currency which will enable instantaneous payment settlements.

c. Researchers from MIT have proposed a blockchain-based system to bring down administrative work in hospitals. It will also enable sharing of medical history between the different doctor in a private way and let the patient will have control of their private data.

In this work, the author suggested that smart homes are not a good scenario for using blockchain as it is already in a private network. Whereas supply chain management or home-based renewable energy generation and distribution management system is a good place to apply blockchain.

10. Do you need a Blockchain? [10]

In this work, the authors take a look at permissioned and permissionless blockchain and compare and evaluated some uses cases in this work and analyzed to find out what type of blockchain is suitable for them. Here are some of the use cases that have been analyzed in this work.

A. **Decentralized autonomous organizations:** Such a company is run through a set of smart contracts with no central authority. For every decision voting takes place. In some situation, a permissioned blockchain can be used in some situation but for most situation, a permissionless blockchain is suitable. However, the contracts and their code should be written carefully otherwise there is a threat of “DAO hack” which might result in huge losses.

B. **Proof of ownership of Intellectual property:** The creator of a digital object can prove the ownership of their property by using a public permissionless blockchain as a time stamping it to the digital ledger with their identity. Non-fungible token(NFT) is built over this concept.

C. **E-Voting:** An E-Voting system should be both private and publicly verifiable at the same time. For such a situation a public permissioned blockchain is suitable. For such a situation a trusted party is required which decides who is permitted on the blockchain. Choosing such a trusted party is the biggest challenge to an E-Voting system.

11. Application of Blockchain Technology in Online Education [11]

Due to the plethora of varied certifications plaguing the market, there is a lack of a single vastly recognized and unified certification system and grading. Using blockchain, we can develop a single distributed database of grades and certificates, this will increase the confidence in the grades and reduce ambiguities that are afloat in the educational industry regarding course credibility. This unified grading will also enable us to predict a learning trajectory for the students and cultivate the unique interests of each individual.

12. Blockchain for Education: Lifelong Learning Passport [12]

As people move towards a more digital era, digital footprints and digital certifications gain more importance, amongst employers and industrial experts. Additionally, more and more people are starting to upload educational content on the internet, and learning skills has become much easier in recent years. Many new educational hubs such as Udemy, Coursera have emerged, which offer online courses in varied skills. These virtual certifications can easily be recorded in a tamper-proof blockchain, which could ensure permanent and verifiable storage of these data. This paper brings forth a very comprehensive platform that offers very profound features ranging from management of your certifications, management of certification authorities, various intelligent services for certifiers, employers, learners, and other interested parties. The information on the platform powered by tamper-free blockchain can act as a passport, as in a completely trustable representation of the technical skills of an individual.

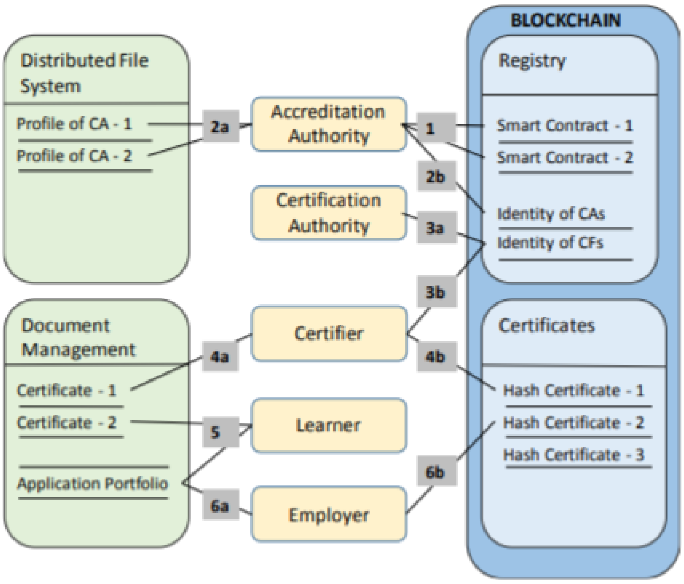

Fig 10: Architecture of the proposed platform. [12]

13. EDUCTX: A Blockchain-Based Higher Education Credit Platform [13]

Every educational institute follows a globally accepted curriculum. This curriculum is generally broken down into a credit system. These credits represent the profile of the student and a blockchain-powered platform can offer a unified viewpoint for students to be judged. Every time we go for higher education the other institute always checks these credits and grade points, so with a unified viewpoint, It will be easier for every institute to grade and judge fairly. This will eliminate the need for LORs, SOPs, which are used to determine the authenticity of the student. The whole process of higher education requires a very complex combination of too many things, which is still not sufficient to rightly determine the worth of the student, due to various loopholes and manipulation by the students. EduCTX offers a blockchain platform that is inspired by the concept of the European Credit Transfer and Accumulation System which basically aims to form single merit for judgment for all students/employees.

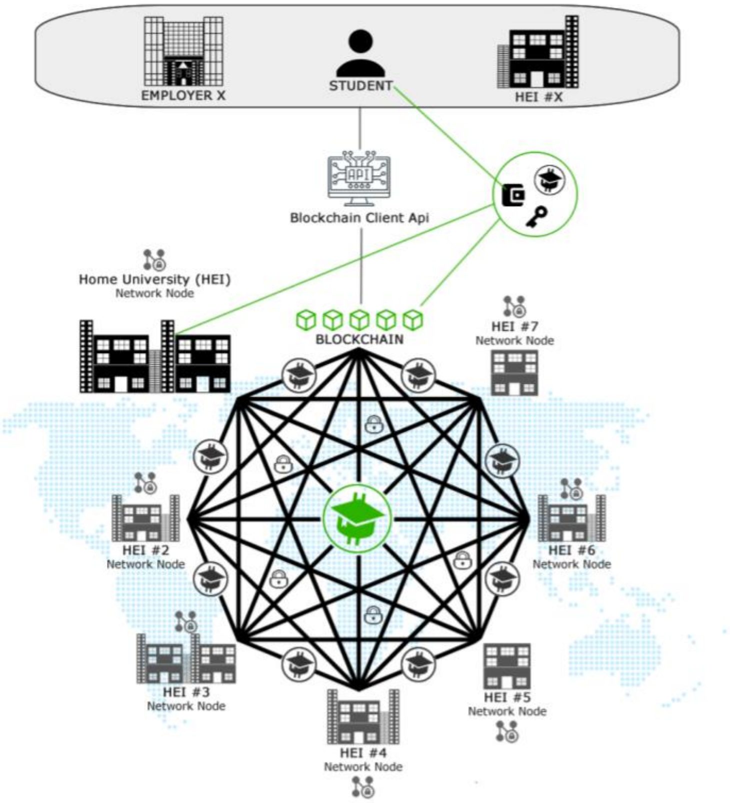

Fig 11: A globally accepted blockchain-powered credit system for uniform and standard grading and judgment [13]

14. Blockchain-Based Applications in Education: A Systematic Review [14]

This paper provides a detailed insight into how the technology of blockchain has changed the education industry in recent years. It dives deeper into the various sectors inside the educational industry where the concept of blockchain is being most heavily used. This primarily includes certification management which covered around 41% of all the innovations, around 29%

discussed storage of student details, whereas around 6% focused on how blockchain can improve the present collaborative learning environments. Lastly around another 6% focused on credit transfer applications. Essentially the paper showed in a very detailed manner, that blockchain has vastly increased the security, integrity, and reliability of the educational sectors. It also covered aspects such as which geological locations have been the most active with blockchain technologies in the educational sector and also showed how over the years blockchain has been gaining popularity in a very exponential manner.

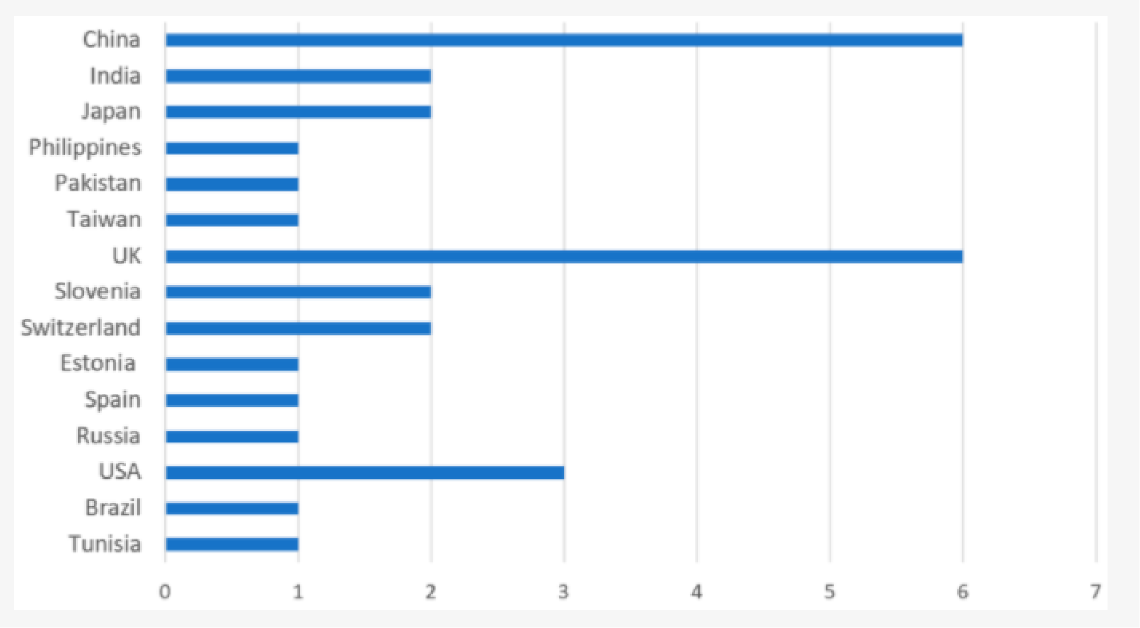

Fig 12: A statistical view of the degree of adoption of blockchain technology, across various countries. [14]

15. Exploring blockchain technology and its potential applications for education [15]

This paper explores all the potential verticals where blockchain could be utilized in the educational sector. It starts off by discussing application opportunities and goes on sketches the future of blockchain in education, it concludes by discussing the limitations of blockchain in education. The research articles talk about the use of blockchain for preventing degree fraud by providing blockchain ID to each degree being used and hence maintain a blockchain ledger to ensure authenticity. The research article further puts forward an interesting analogy of creating a network of students and teachers, where students are rewarded for working in defined behavior, similar to how miners are rewarded in a blockchain network. Ideas of how blockchain promotes fair evaluation are also discussed in the article. The paper also takes into account the limitations such as the immutability of a blockchain to cause problems, when students/teachers wish to correct something in the ledger. Additionally, it's quite difficult to implement a very complex education structure in a blockchain, but as the technology matures we can expect more advanced applications to surface on the market.

➢ Platform:

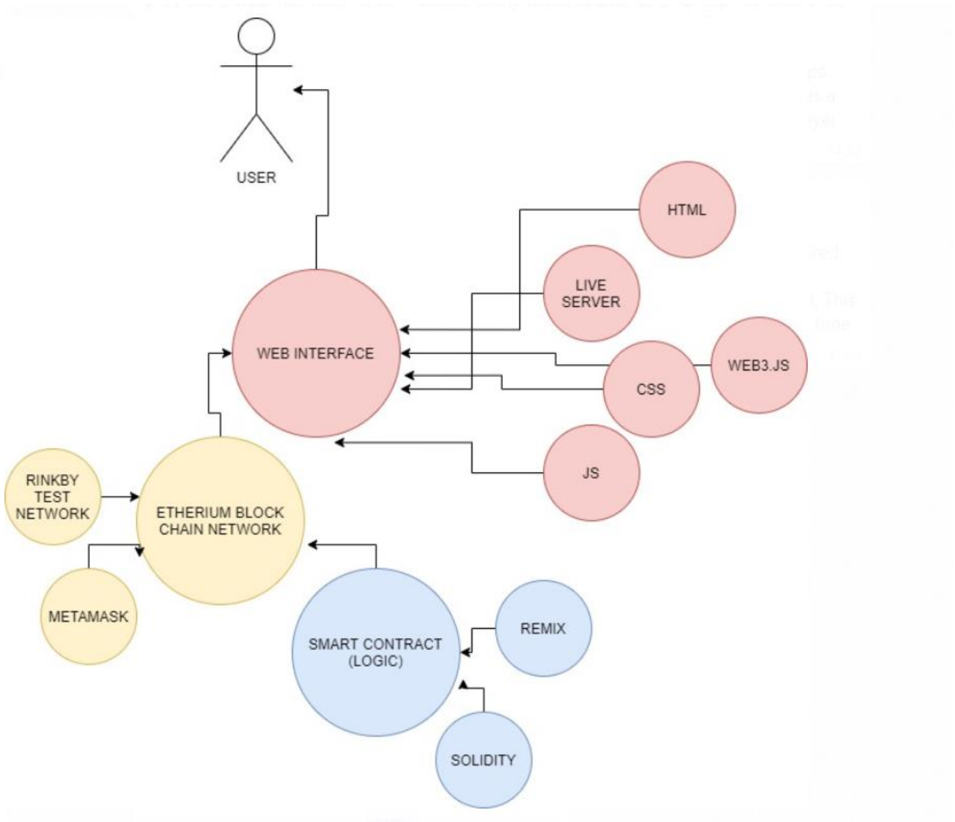

Fig 13: Platforms used

Blockchain is still a developing technology, and hence there is no one-for-all platform, we had to use a variety of different platforms for different things. Essentially there are 3 main components of the project.

Namely 1) the actual blockchain, 2) the smart contract (the logic behind the blockchain), and 3) the web interface for users. For our project, we have used the ethereum blockchain which is hosted on the rinkby test network, further we use meta mask as our wallet to perform transactions in the Ethereum network. The logic of the blockchain is written in the solidity programming language, and we have used REMIX as an Integrated Development Environment. Lastly, the web interface is developed using HTML, CSS, and JS for the designing and WEB3.JS for connecting it to the blockchain.

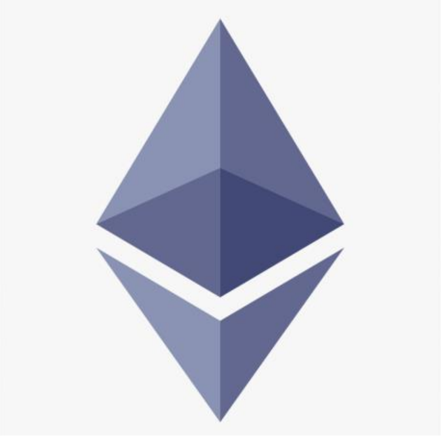

Fig 14 : Ethereum

Fig 15: Metamask

Fig 16 : Remix Fig 17: Web3.JS

REFERENCES:

[1] Garain, U., & Halder, B. (2008, December). On automatic authenticity verification of printed security documents. In *2008 Sixth Indian Conference on Computer Vision, Graphics & Image Processing* (pp. 706-713). IEEE.

[2] Yusuf, A. D., Boukar, M. M., & Shamiluulu, S. (2017, November). Automated batch certificate generation and verification system. In *2017 13th International Conference on Electronics, Computer and Computation (ICECCO)* (pp. 1-5). IEEE.

[3] Brdesee, H. S. (2019). An Online Verification System of Students and Graduates Documents and Certificates: A Developed Strategy That Prevents Fraud Qualifications. *International Journal of Smart Education and Urban Society (IJSEUS)*, *10*(2), 1-18.

[4] Obilikwu, P., Usman, K., & Kwaghtyo, K. D. (2019). A Generic Certificate Verification System for Nigerian Universities.

[5] Putro, P. A. W., & Luthfi, M. (2019, October). An authentic and secure printed document from forgery attack by combining perceptual hash and optical character recognition. In *2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)* (pp. 157-162). IEEE.

[6] Nakamoto, S. (2019). *Bitcoin: A peer-to-peer electronic cash system*. Manubot.

[7] Landerreche, E., & Stevens, M. (2018). On immutability of blockchains. In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET).

[8] Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277.

[9] Chowdhury, M. J. M., Colman, A., Kabir, M. A., Han, J., & Sarda, P. (2018, August). Blockchain versus database: a critical analysis. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1348-1353). IEEE.

[10] Wüst, K., & Gervais, A. (2018, June). Do you need a blockchain?. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE.

[11] Sun, H., Wang, X., & Wang, X. (2018). Application of Blockchain Technology in Online Education. *International Journal of Emerging Technologies in Learning*, *13*(10).

[12] Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). Blockchain for education: lifelong learning passport. In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. European Society for Socially Embedded Technologies (EUSSET).

[13] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE access*, *6*, 5112-5127.

[14] Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. *Applied Sciences*, *9*(12), 2400.

[15] Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, *5*(1), 1-10.