IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

Marksheet Verification System using Blockchain

Kiran H S[1], Bhat Divya Subrahmanya[2], Usha J[3]

Student, Master of Computer Applications, RV College of Engineering, Bengaluru, India[1,2]

Professor, Master of Computer Applications, RV College of Engineering, Bengaluru, India[3]

Abstract: Faking of mark sheets, forging the mark sheets have become a major problem in today's times in terms of gaining employment opportunities. India is moving towards digitization but this leads to easy forging or tampering of the online documents like the mark sheets. A mark sheet in the PDF format can easily be tampered and this leads to a fear among the institutions to provide soft copies of the mark sheets instead of hard copies. Blockchain is the new trend currently in the digital market. But apart from proving its importance in just the domain of finance it can also be used in the other domains. One among them is the verification of documents, mainly the marksheets for the employment domain, using their hash values. Blockchain provides the facility of adding up data items without giving the provision for editing them which proves the major security aspect of any database.

Keywords: Blockchain, metamask, ethereum, transaction, ganache, smart contracts, solidity.

I.INTRODUCTİON

Blockchain is a technology which is trending due to its storage and security capabilities. It is a type of distributed database system where in the database can be said to be distributed in a decentralized network (peer-to-peer network). It is the main reason for the existence of cryptocurrency. But apart from the financial domain, it can also be used for other purposes like the education system and employment domain. Educational institutions provide students with various certificates which are then verified by employers or higher educational institutions. In order to gain the career opportunities, candidates sometimes also resolve to forging the certificates. Everything in today's times is going digital but taking the academic documents like the mark sheets to an online platform is considered to be very difficult as it is very easy to tamper them and create such certificates at low cost. For solving this issue, Blockchain technology can be taken into consideration for the storage of the soft copies of the mark sheets. This also helps in easy verification of the mark sheets as required by the employers.

Here the concept of comparison of the hash values are used. The hash value of any document is always unique. Any changes made in the document results in the change in hash value. It can be assumed that instead of blockchain any database can be put to use to store the mark sheets into it along with the roll no., and hash value of the mark sheet. But anyone with the required privileges can access the database and hackers can easily edit such databases. The hash value of a tampered mark sheet can be provided into the database and in such cases if only the mark sheets are compared then one can say that the process of verification of the mark sheet has gone wrong. It will be legitimate only if even the mark sheets are also compared. For such processes human intervention is required.

In blockchain, each block has its own hash address and also the data in the block once added cannot be changed at all. Any changes made in the block will result in the creation of a new block instead of having the already existing block to be changed. Any internal persons in the examination and results section of any university will then be not able to make any changes to the document. Hence this system focuses mainly on just the storage of mark sheets' hash values rather

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

than storing the mark sheet itself.

II.RELATED WORKS

Nora Naik, et. al. in [9] proposed a system consisting of two sections - one for issuing the ceritficate and the other for verifying it. Here the use of SHA256 algorithm is observed which calculates the hash value of the mark sheet and stores the same in the blockchain. The marks of the student is first entered on the website that generates the student mark sheet. The mark sheet is then hashed and stored in the blockchain after hashing it with the private key and the mark sheet along with the institute public key is sent to the student. For verification purpose, the mark sheet PDF is uploaded on the website and using the roll no. of the student the hash value of the mark sheet is retrieved and compared to the calculated hash value of the mark sheet. This system can be enhanced with the use of smart contracts.

Hamdi A. Ahmed and Jong-Wook Jang in [10] worked on a system to authenticate higher educational certificate using QR code tags. A certificate template for a particular institution is selected predefined by the verification system. The information of the student will be entered and a unique string hash to recognize whether the certificate is generated by the system or not is created. The digest value contains the hash string and private key for institutions. To sign the hash value, the private key of the institution is used. This signature is encoded with the institution alias and fed into QR code generator. The QR code from the certificate is scanned and the hash values are compared. The system can be improved in terms of security and must provide the functionality of authentication of the user.

Harshal Pandit, et. al. in their paper [11] titled “Secured E-Documents and Sharing using Encrypted QR-Code”, proposed a system where a user will enroll himself/herself at a data center where his/her documents will be uploaded on the database. The user will receive a user-ID and password after the documents are verified manually. When a third party user requests for documents, then using the user credentials, the user logs in and selects the documents to be sent. A QR code is generated which is shared with the third party and on scanning the code, the third party can access the documents. Hence, it can be said that the document verification takes place only once in a manual way.

Maykin Warasart and Pramote Kuacharoen in [12], proposed a system to authenticate paper-based documents using digital signature and QR code. Before providing the document to the user, a message is composed after which the hash value of the message is generated. This value is then encoded with the private key of the sender resulting in a digital signature. The message and signature are combined together to be stored in the QR code and fed into the QR code generator which prints them on the paper before sending it to the receiver. The authenticity can be checked by scanning the document where the hash value of the message is computed. The message is validated by using Optical Character Recognition (OCR) that computes the hash value of the message and compares it with the hash value obtained from QR code. İf they are identical, the printed message is authentic otherwise it is necessary to keep a human review. Hence this process is semi-automatic.

Patrick Obilikwu, Karim Usman, Kenneth Dekera Kwaghtyo in [13] proposed a model for a generic certificate verification system for Nigerian Universities where the verification is done in a manual manner. The mark sheets are stored in a NoSQL database. The use of NoSQL provides the advantages of being flexible and scalable. This model implements the use of top-down approach along with the iterative methods to perform continuous testing of the system.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

But the verification is done manually.

Osman Ghazali, Omar Saleh in [14] worked on using cloud for the purpose of certificate verification. The main issues addressed by this model are security, validity and confidentiality. For the purpose of security, the process of cryptography is embedded. The system produces a Transaction Authorization Code (TAC) which is then sent by the graduate to his employer along with the certificate. The TAC remains valid only for a specific duration of time. The validity of the marksheet is verified using the serial number provided on the certificate and the TAC value. The confidentiality of the mark sheet is taken care of by the secret key provided to the graduate.

Rishabh Garg, in his paper [15] investigated the feasibility, benefits, challenges and risks of blockchain in the field of education and employment. This study explores the use of blockchain for issuing and validating academic credentials. The method implements the use of private key, IPFS server, cryptography, biometric hash and a secret phrase to validate the student's credential. The study discusses the use of decentralized platform so that anyone can verify anyone's academic credentials but the certificate owner is the only one who can share his data at his will.

Trong Thua Huynh, Dang-Khoa Pham in [16] have used the consensus mechanism of Proof of Stake (PoS) for the purpose of block mining. This is done to save energy consumption and time to solve hash values as in case of Proof of Work (PoW) in order to improve the performance of transaction verification in digital issuing and validating system. The system will be improved in terms of security and transparency using the Casper version 2 protocol along with the use of smart contracts as future enhancements.

Omar S. Saleh, Osman Ghazali, Qusay Al maatouk in their study [17] discussed about the document verification like its aim, its workflow and the types of the documents. Various ways of verifying the documents include the watermarked QR code, RFIDs, QR code and 2D barcode. The verification process varies in three concepts – tools used, scope and procedure of verification. However, each of the techniques in this study are backed by some flaws in terms of providing a seamless unified certification verification.

T. Rama Reddy, et. al. in [18] proposed a system for securing and verifying graduate credentials using blockchain. When a certificate is added into a block, a unique ID with the Aadhar card number as a primary key is returned. The verification is done using the transaction ID and the Aadhar card number. Future works for this proposal includes the application of CryptCloud+, storage of employment and experience data and also the tracking of such data apart from the storage of just student marks information. İt can be also used to provide integrity to other types of documents that require time stamps.

The studies show that issues exist during verification of the authenticity of digital mark sheets. The physical hard copies of the mark sheets come with various water marks that help in proving authenticity. But in the case of digital mark sheets, it is very easy to edit documents. For digital document verification, hashes are the only way in which one can identify the authenticity of such mark sheets. When blockchain is used, it becomes difficult for anyone to change the data which is already stored in the blockchain. Thus, blockchain, help educational institutions to move towards issuing digital mark sheets that can be easily shared.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

III.PROPOSED METHODOLOGY

The proposed system focuses on the uploading of data of mark sheet along with the roll no. of the student into the blockchain and verification of the same by a recruiter. The verification of the mark sheets is based on the comparison of the hash values. The platform to use blockchain over the application is Ganache which provides us with the network over which we need to build our blockchain for testing purposes along with some dummy gas amount in some virtual accounts. The MetaMask interface is connected with the application in order to connect blockchain to the application. The whole system is divided into three modules namely- upload, search and verify.

Upload: The univeristy providing the mark sheets can upload the mark sheet along with the USN (University Seat Number) of the student in the application. The hash value of the mark sheet is calculated. İn order to process the transaction, a small amount of gas fees will be paid by the university through MetaMask after which the block containing the USN and hash value of the mark sheet will be mined into the blockchain.

Search: The USN and hash values of the mark sheets are stored in the form of mapping structures with key-value pairs. Here the USN of the student acts as the key and the hash value acts as the value for this structure. Using the USN of the student, the hash value of his/her respective mark sheet can be searched and retrieved.

Verify: For the verification module, the hash value of the mark sheet uploaded is calculated. The hash value stored for the particular USN will be retrieved back. This retrieved hash value and the calculated hash value will then be compared. Verification will be successful only if both the hash values will be same.

Diagrammatically the process can be represented as shown in fig. 1:

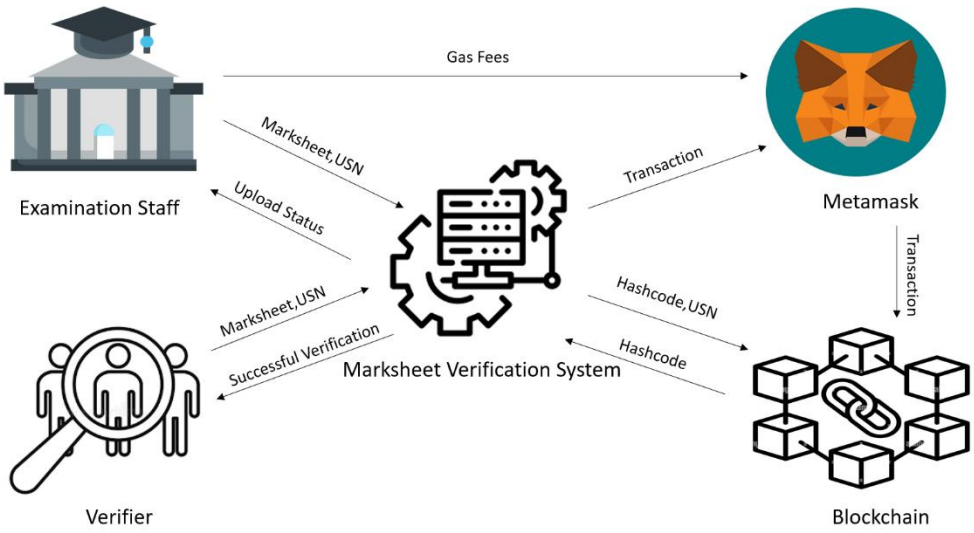

Fig. 1 Architecture of the proposed system

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

Flow of data in the application is as shown in the fig. 2:

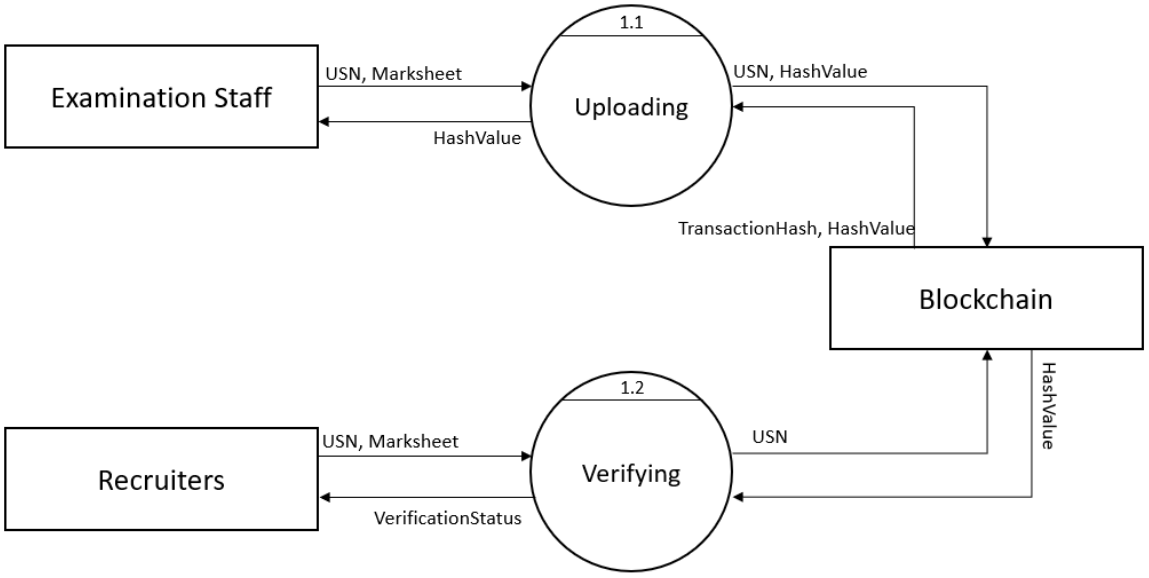

Fig. 2 Data Flow Diagram

Module Description

1. Upload Module

This module uploads the hash value of the mark sheets issued by the universities and it is mapped to the USN of the student

- Input: Mark sheet, USN
- Process: Hash value with USN of student is mined into blockchain
- Output: Upload status

2. Verify Module

This module verifies the authenticity of the mark sheets for the recruiting staff

- Input: Mark sheet, USN
- Process: Hash value of the mark sheet is calculated and the hash value mapped with the particular USN is retrieved. The comparison of the calculated hash value and the retrieved value takes place and the appropriate output is displayed
- Output: Verification status

3. Search Module

This module searches the document's hash value through the blocks.

- Input: USN
- Process: USN entered is compared with the USNs present in the blockchain and hash value mapped with that USN is retrieved.
- Output: Hash value

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

IV.OUTCOME

The examination staff can enter the USN of the student and upload the mark sheet of the student.

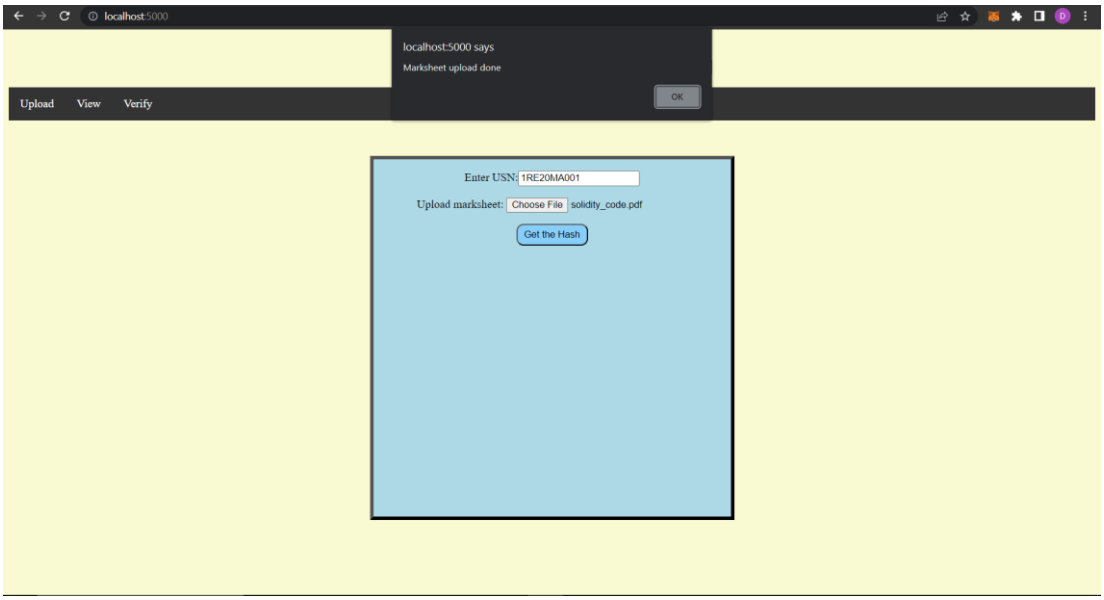

Fig. 3 Successful uploading of the mark sheet

Once the gas fees is paid, a message to acknowledge the uploading of the mark sheet is printed as shown in fig. 3.

If the user just needs the hash value of the candidate without uploading the file, then it can be done by entering the USN of the candidate and clicking on 'Get the Hash' button.

Fig. 4 Output for retrieving the hash

The fig. 4 shows the hash value obtained from the blockchain for the particular USN.

In the search module, when the USN of the student is entered and 'Get the Hash' button is clicked, the hash value mapped with that USN can be found as shown in fig. 5.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

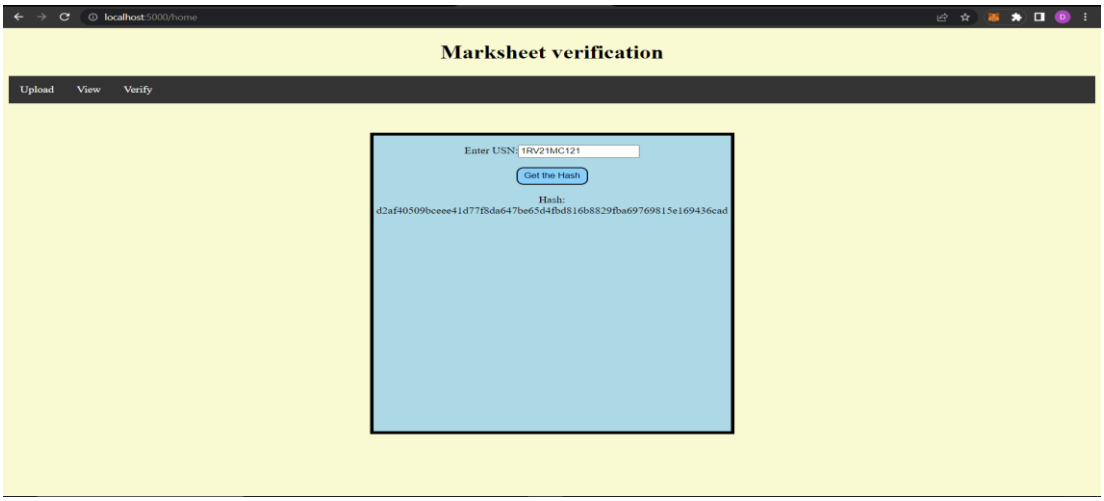

Fig. 5 Output for View page

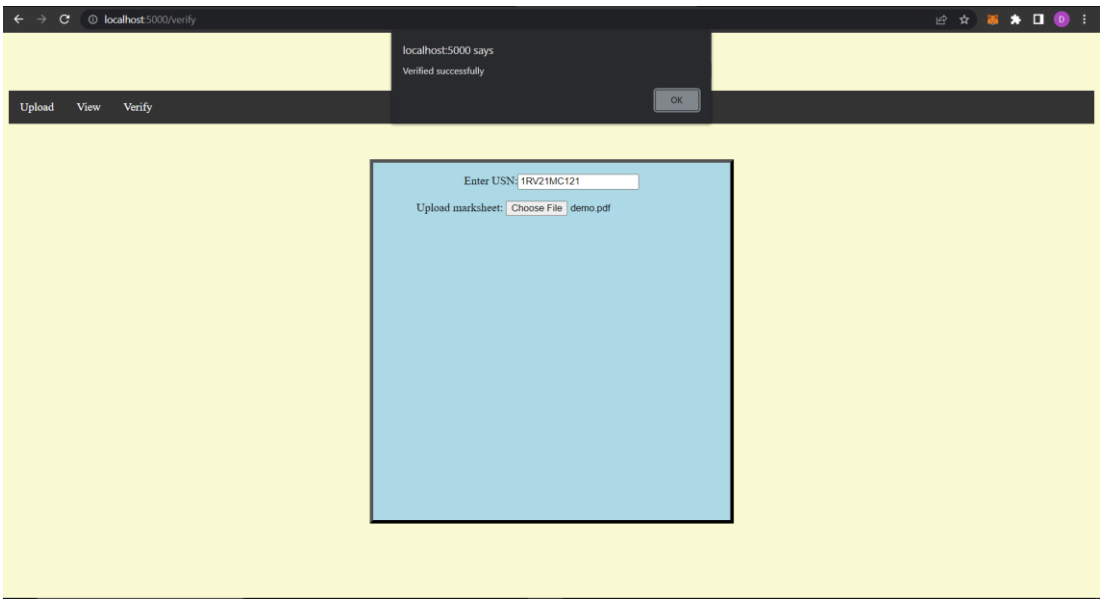

Fig. 6 Message to display genuine mark sheet

If the hash value of the file uploaded and that mapped with the USN in the blockchain are the same, then the message indicating that both of them are equal is printed on the screen using the alert box as 'Verified successfully' as shown in fig. 6.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

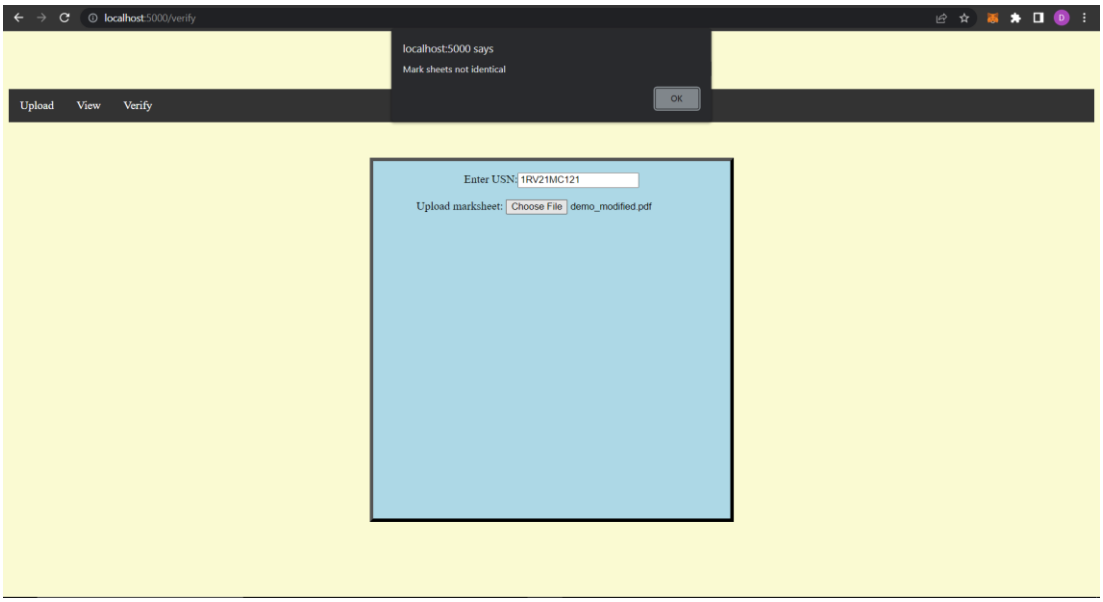

Fig. 7 Message to display modified mark sheet

If both of them are not equal, then a message to indicate that they are not equal is printed on the screen with the alert box as 'Mark sheets not identical' as shown in fig. 7.

V.CONCLUSİON

'Mark Sheet Verification System using Blockchain' is mainly for the universities and the recruiters for the purpose of providing the facility of issuing digital mark cards rather than having the burden of printing the hardcopies. It makes use of the effective storage system of blockchain to securely store the mark sheet details and uses the concept of hash value to maintain the integrity of the mark sheet. Any change in mark sheet content can easily be verified with the help of the hash values. Also, the values stored in the block of blockchain cannot be changed by any means. This adds to another feature of the system to prevent the modification of the mark sheet in blockchain. It takes in minimum amount of input in order to verify the identity of the person and hence provides the output without much of complexity.

VI.FUTURE SCOPE

In order to improve the security of the system more by introducing authentication of the users into the web portal can also be considered as the step to enhance the proposed work more. Also, the website can indulge in the creation of websites by providing the universities the freedom to create their mark sheet template and update the same into the storage system and the student. This can be improved by providing the examination and results section staff to even provide softcopies of the mark sheets to the student.

REFERENCES

[1] Cornelius C. Agbo, Qusay H. Mahmoud, J. Mikael Eklund, "Blockchain Technology in Healthcare: A Systematic Review", MDPI Healthcare 7(2):56, 4 April 2019.

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

[3] O'Reilly: Chapter 7. The Blockchain. [Online].. Available: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html.

[4] Ethereum: What is Ethereum? [Online].. Available: https://ethereum.org/en/what-is-ethereum/.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Vol. 10, Issue 3, March 2023

DOI: 10.17148/IARJSET.2023.10313

[5] Linda Orenes-Lerma: Ledger Academy: How does Blockchain transaction work?, updated October 25 2022, [Online].. Available: https://www.ledger.com/academy/how-does-a-blockchain-transaction-work.

[6] Stan Schroeder, Crypto wallet MetaMask now lets you swap tokens on your phone. [Online].. Available: https://in.mashable.com/tech/21000/crypto-wallet-metamask-now-lets-you-swap-tokens-on-your-phone, 2021-06-26.

[7] Himanshi, "Solidity:A Programming Language for Smart Contracts". [Online].. Available: https://www.naukri.com/learning/articles/solidity-programming-language/,Jul 1,2022

[8] IBM: Smart contracts defined. [Online].. Available: https://www.ibm.com/in-en/topics/smart-contracts.

[9] Nora Naik, Dattaram Naik, Rohit Naik, Ashvedhpednekar, Shaunakvalawalker, Vinayak Sinai Bhandiye, "Marksheet verification using Blockchain", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), pp.37-46, Volume. 9, Dec 2019.

[10] Hamdi A. Ahmed, Jong-Wook Jang, "Higher Educational Certifcate Authentication System using QR Code Tag", International Journal of Applied Engineering Research, ISSN 0973-4562, pp. 9728-9734, Volume. 12, Number. 20, 2017.

[11] Harshal Pandit, Shailendra Nipane, Suraj Jadhav, Sunita Naik, "Secured E-Documents and Sharing using Encrypted QR-Code", International Journal of Computer Applications, IJCA Proceedings on National Conference on Role of Engineers in National Building, Number. 1, 2016.

[12] Maykin Warasart, Pramote Kuacharoen, "Paper-based Document Authentication using Digital Signature and QR Code", 4th International Conference on Computer Engineering and Technology (ICCET 2012).

[13] Patrick Obilikwu, Karim Usman, Kenneth Dekera Kwaghtyo, "A Generic Ceritificate Verification System for Nigerian Universities", International Journal of Computer Science and Mobile Computing, Volume. 8, Issue. 10, pg. 137-148, October 2019.

[14] Osman Ghazali, Omar S Saleh, "Cloud Based Graduation Ceritificate Verification Model", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume. 5, Issue. 2, February 2017.

[15] Rishabh Garg, "Blockchain Ecosystem for Education & Employment Verifcation", 13th International Conference on Network & Communication Security, Toronto, Canada, 25-26 September 2021.

[16] Trong Thua Huynh, Dang-Khoa Pham, "Eunicert: Ethereum Based Digital Certificate Verification System", International Journal of Network Security & its Applications (IJNSA), Volume. 11, Number. 5, September 2019.

[17] Omar S. Saleh, Osman Ghazali, Qusay Al maatouk, "Graduation Certificate Verification Model: A Preliminary Study", International Journal of Advanced Computer Science and Applications, Volume. 10, Number. 7, 2019.

[18] T. Rama Reddy, P. V. G. D. Prasad Reddy, Rayudu Srinivas, Ch. V. Raghavendran, R. V. S. Lalitha, B. Annapurna, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain", EURASIP Journal on Information Security, Article Number. 7, 2021.

