Background Verification of Marks Cards

Ashika Jayachandran[1], Yamuna N[2], Afreentaj[3], Lavanya M[4], Bhoomika P[5]
[1,2,3,4]*Dept of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur - 572105*
[5]*Guide, Dept of Computer Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur - 572105*

***Abstract*— Traditional methods of background verification are often plagued by inefficiencies, fraud, and data tampering risks. By leveraging the decentralized and immutable nature of block chain technology, this study aims to enhance the security, transparency, and reliability of the verification process. The proposed system ensures that credentials issued on Mark's Card are permanently recorded on a block chain, making them easily verifiable by third parties while protecting the privacy of individuals. This approach not only reduces the likelihood of credential fraud but also streamlines the verification process, providing a faster and more trustworthy means of confirming qualifications and identities. The paper discusses the design and implementation of the block chain system, evaluates its performance, and analyzes its potential impact on the broader landscape of digital credentialing and background verification. Initial results demonstrate significant improvements in data integrity, verification speed, and overall trustworthiness, highlighting the promise of block chain technology in revolutionizing credential verification processes.**

Keywords—Mark's card, Third party, Privacy, verification.

I. INTRODUCTION

In today's increasingly digital world, the verification of identity and credentials is a critical component of various processes, from academic admissions and employment to financial transactions and access control. Traditional background verification methods, however, are often fraught with challenges such as inefficiencies, high costs, susceptibility to fraud, and data tampering. These issues not only undermine the trust in verified information but also lead to significant delays and administrative burdens.

Mark's Card is a digital credentialing tool designed to simplify and secure the process of identity and qualification verification. Despite its advantages over paper-based credentials, the current system still relies on centralized databases, which are vulnerable to hacking, data breaches, and unauthorized modifications. To address these vulnerabilities and further enhance the security and efficiency of Mark's Card, this paper proposes the integration of block chain technology into the background verification process. Block chain technology, with its decentralized, transparent, and immutable ledger, offers a promising solution to the aforementioned challenges. By recording credential information on a block chain, we can ensure that once data is entered, it cannot be altered or deleted, thereby significantly reducing the risk of fraud and enhancing data integrity. Additionally, the decentralized nature of block chain eliminates the need for a central authority, distributing trust across the network and providing a more resilient verification system.

II LITERATURE SURVEY

Here are summaries of papers on background verification of marks card including details of the year, authors, title, and a brief introduction to their work:

Nora Naik, et. al. in [9] proposed a system consisting of two sections - one for issuing the certificate and the other for verifying it. Here theuseofSHA256 algorithm is observed which calculates the hash value of the mark sheet and stores the same in the block chain. 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 block chain 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.

May kin 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. If 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 K waghtyo 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 No SQL database. The use of No SQL 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. 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 mark sheet 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 block chain in the field of education and employment. This study explores the use of block chain 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.

The main objective of the Mark's Card system using block chain for background verification is to create a secure, efficient, and transparent verification process. To provide a highly secure environment for storing and managing background verification data, leveraging block chain's inherent immutability and encryption features to prevent fraud and unauthorized alterations.

III. METHODOLOGY

Apache Cassandra is a free and open-source, distributed, wide-column store, No SQL database

management system designed to handle large amounts of data across many commodity servers, providing high availability with no single point of failure. Cassandra offers support for clusters spanning multiple data centers, with asynchronous master less replication allowing low latency operations for all clients. Cassandra was designed to implement a combination of Amazon's Dynamo distributed storage and replication techniques combined with Google's Big table data and storage engine model.

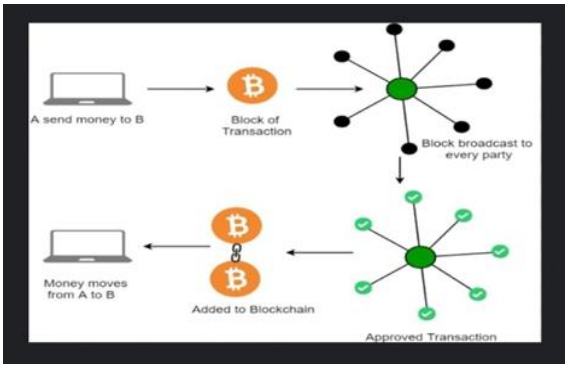
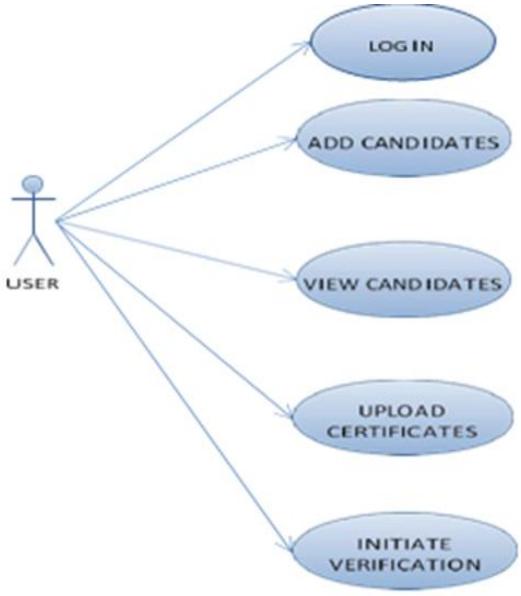


Figure 1: Bock chain transaction

Every node in the cluster has the same role. There is no single point of failure. Data is distributed across the cluster (so each node contains different data), but there is no master as every node can service any request.



Our system can perform various operations like

1. User Login:

- User inputs their username and password.
- Upon successful verification, the user is logged into the system.

2. Add Candidates and View Candidates:

- User' Add Candidates' section and 'View Candidates' section.
- System saves the candidate details to the database and click on individual candidates to view more detailed information.

3.Upload Certificates:

- User selects a candidate from the 'View Candidates 'list.
- User uploads relevant certificates/documents for the selected candidate.
- Systemsavestheuploadedcertificates/documentstothe candidate'sprofile.

4.Initiate Verification

- User selects a candidate and their uploaded certificates.
- System processes verification request, and updates candidate's profile with verification.

IV RESULTS AND DISCUSSIONS

The Agribot is purely non-convectional and reduces human effort. It saves time for farmers and water for irrigation. The result shows accuracy in seed sowing and watering the crop. The estimated time for basic activities is observed is less as traditional farming. The prototype of the project is shown in figures 4 and 5. The setup contains a seed drum for seeding, ploughing rods for ploughing the soil and a tank to supply water to the field.

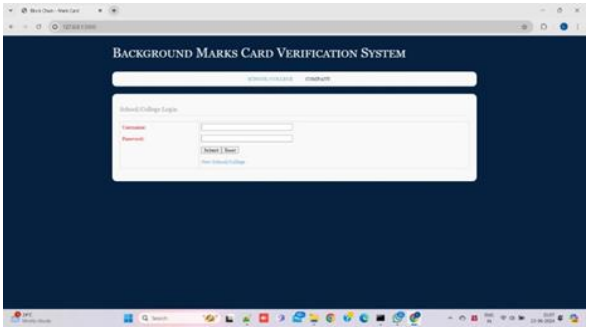


Figure 1: User interface

Application Overview: The image shows the login page of a web application called "Background Marks Card Verification System. “This system is to be designed for verifying academic credentials.

User Interface: The page provides a login form for schools and colleges, requiring a username and

password. There is also a link for new schools or colleges to register.

Navigation: The top menu includes two options: "School/College" and "Company," indicating that the system might support different types of users for verifying marks or credentials.

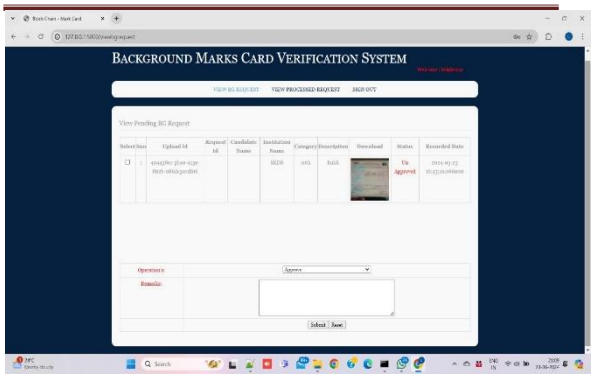


Figure 2: View BG Request

Dashboard View: The image displays the "Background Marks Card Verification System" dashboard for viewing pending background (BG) requests. The user is logged in as "brightway."

Pending Request Details: The table lists details of pending verification requests, including Upload ID, Request ID, Candidate Name, Institution Name, Category, Description, Download link, Status (Unapproved), and Recorded Date.

Actions: Below the table, there's an operation section where the user can approve or disapprove the request, add remarks, and submit the decision. The navigation bar allows viewing BG requests, processed requests, and signing out.

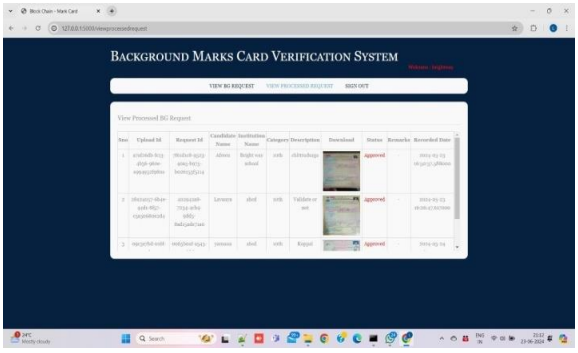


Figure 3: View Processed Request

Processed Requests Overview: The image shows the "Background Marks Card Verification System" page for viewing processed background (BG) requests. The user "brightway" is logged in.

Request Details: The table lists details of processed verification requests, including Upload ID, Request ID, Candidate Name, Institution Name, Category, Description, Download link, Status (Approved), Remarks, and Recorded Date.

Navigation: The top navigation bar allows the user to switch between viewing BG requests, processed requests, and signing out. This page specifically shows approved requests with downloadable documents for each entry.

V CONCLUSSIONS

'Back Ground Verification Of Marks Card' 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 block chain 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 block chain cannot be changed by any means. This adds to another feature of the system to prevent the modification of the mark sheet in block chain. 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.

REFERENCES

[1]. M. Warasartand P. Kuacharoen, "Paper-based Document Authenticating using Digital Signature and QR Code," no. Iccet, 2012.

[2]. Z.Chen, "Anti- Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique."

[3]. Oliver,Miquel;Moreno,Joan;Prieto,Gerson;Benitez,David(2018):"UsingBlockchain as a tool for tracking and verification of official degrees: business model",29th European Regional Conference of the ITS

[4]. Juliana Nazare, Kim Hamilton Duffy, J. Philipp Schmidt "Digital Certificate Project" MIT Media Labs, 2015

[5]. Stephen Thompson "The Preservation of Digital Signatures on the Block chain" University of British Columbia iSchool Student Journal ,vol.3 (Spring 2017).

[6]. Osman Ghazali and Omar S. Saleh, “A Graduation Certificate Verification Model via Utilization of the Block chain Technology”, e-ISSN: 2289-8131 vol. 10 no. 3-2.Chen, Huang, C.H., P.J., Lin, Y.J.,

[7]. X. Technologies, “Block chain imperative for educational certificates, ”X an bell Technologies, 2017

[8]. MIT Media Lab Learning Initiative and Learning Machine, “Digital Certificates Projects.[Online]. Available: http://certificates.media.mid.edu/.

[9]. R. Arenas and P. Fernadez, “Credence Ledger: A Permissioned Block chain for Verifiable Academic Credentials.”In IEEE international conference on Engineering, Technology and Innovation (ICE/ITMC). Stuttgart, Germany 2018.

[10]. Ahmed Badr, Laura Rafferty, Quassy H. Mahmoud, Khalid Elgazzar, Patrick C.K. Hung “A Permissioned Blockchain-Based System for Verification of Academic Records” in IEEE 2019.

[11]. Yang, Jiachen, Jingfei Ni, Yang Li, Jiabao Wen, and Desheng Chen. "The intelligent path planning system of agricultural robot via reinforcement learning." Sensors 22, no. 12 (2022): 4316.