# Enabling Trust and Privacy Preserving e-KYC System Using Blockchain

**Viraj Ashok Patil[1], Akshay Kumar Mishra[2], Ketan Kishor Shinde[3], Prof A. A. Patil[4]**

*[1,2,3,4]Department Of Computer Engineering, TSSM's, Padmabhooshan VasantdadaPatil Institute of Technology, Bavdhan-21, Pune, Maharashtra, India.*
*Affiliated To Savitribai Phule Pune University, Pune, India.*

---------------------------------------------------------------------***---------------------------------------------------------------------

**ABSTRACT -** A Blockchain technology guarantees to be highly trending and empowering in financial domain computing programs. The virtual economic system is becoming a fundamental a part of present-day life. in order the use of the digital global increases there are more probabilities of lower is the safety stage. So greater using digitization more the frauds and less the safety. In a few cases of personal information, leakage has brought back into the focus the security troubles with the extraordinary identification sharing mechanisms. A client is predicted to provide his identification for authentication by means of unique agencies. So the KYC process offers with the identity of the user. And in flip, provides the desired security. The KYC strategies which are used by the banks are absolutely dependent on the encryption that's sluggish and it is able to result in the lack of patron info to other their birthday celebration economic establishments. This device can be efficient by means of using Blockchain technology, which has the ability to automate numerous manual approaches and it's also proof against hacks of any type. The immutable blockchain block and its distributed ledger is the best complement to the system of KYC. With the addition of clever contacts, fraud detection may be computerized. For KYC identification info garage, we are able to employ any types of KYC. So, the banks can develop a shared non-public blockchain within the financial institution premise and the equal can be used for verifying the documents. This permits the user to get control in their touchy files and also makes it easier for banks to reap the documents they want for compliance.

***Key Words***: Blockchain, Banking, Digital Certificate, Digital Wallet, Decentralize Identity, Distributed Ledger Technology, Verifiable Credential.

## 1.INTRODUCTION

A Blockchain-based totally protection management device is for offering security to the bank transactions and to implement the KYC manner in an easier and secured manner. Blockchain technology is a brand-new technology which is based totally on mathematical, cryptographic and monetary concepts for preserving a database among diverse contributors without the need of any 0.33 party or central authority. it is a secured distributed database, tamper obvious, in which the validity of a transaction may be demonstrated by means of events in the transaction. Blockchains are normally managed by using a peer-to-peer (P2P) laptop network to be used as a public allotted ledger, wherein nodes together adhere to a consensus set of rules protocol to add and validate new transaction blocks. Al even though blockchain facts are not unalterable, considering the fact that blockchain forks are possible, blockchains can be considered secure via design and exemplify a distributed computing system with high Byzantine fault tolerance. know Your client (KYC) strategies performed through banks on their clients are needless, unmanageable and highly-priced. therefore, a gadget is proposed to automate unskilled obligations and allow sharing of facts related to KYC. Blockchain technology, with its concept of dispensed database, time-stamped ledgers, can correctly assist banks enhance their KYC technique. one of the most important duties of the bank is to make certain facts protection of data of the customers, confidentiality and the country in their account to assure their safety and integrity, inside the method of alternate and processing of records. for that reason, by means of the use of the competencies of innovative facts generation i.e., the Blockchain generation information protection may be performed.

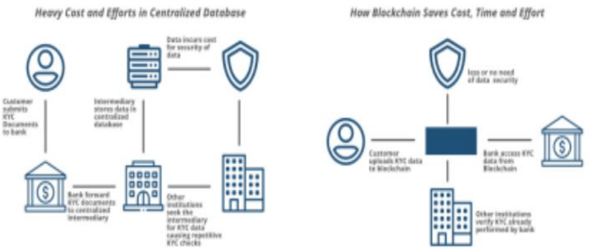

Heavy Cost and Efforts in Centralized Database
Data incurs cost for security of data
Customer submits KYC Documents to bank
Intermediary stores data in centralized database
Bank forward KYC documents to centralized intermediary
Other institutions seek the intermediary for KYC data causing repetitive KYC checks
How Blockchain Saves Cost, Time and Effort
less or no need of data security
Customer uploads KYC data to blockchain
Bank access KYC data from Blockchain
Other institutions verify KYC already performed by bank

**Figure 1**: Blockchain and e-KYC

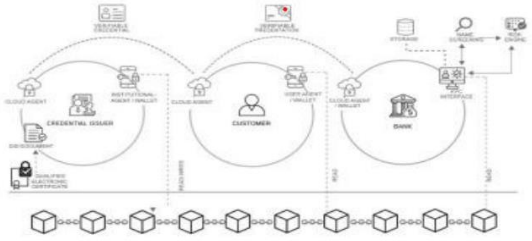


**Figure 2**: Distributed Ledger

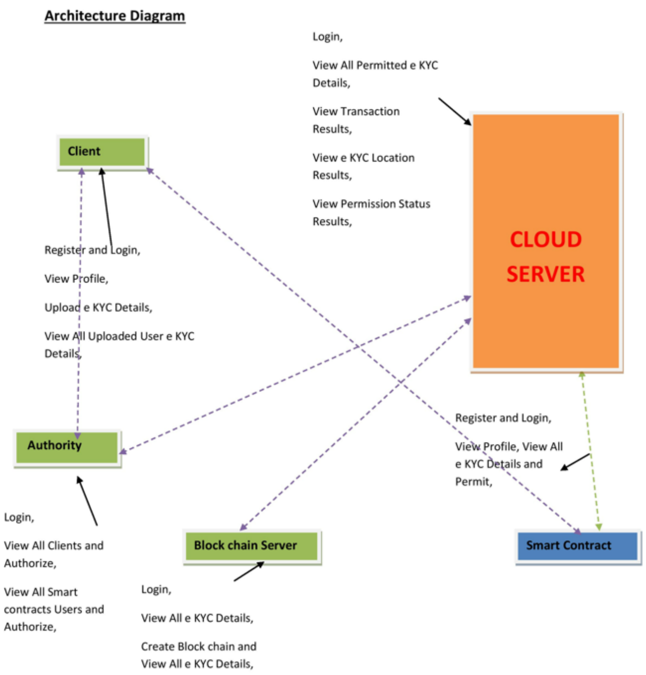
## 2. PROPOSED SYSTEM

In this paper, we aim to address such research gaps by introducing a secure and efficient blockchain-based e- KYC documents registration and verification process with lightweight key cryptographic protocols run in the cloud Interplanetary File System (IPFS). To facilitate the foundational privacy requirement regarding the user's consent collection, we develop a smart contract to generate and enforce the consent to be digitally signed by the customer. The consents will be systematically stored in a blockchain having tamper-proof property which is useful for auditing.

Regarding the data privacy issue, we propose an optimized cryptographic protocol by applying symmetric encryption with public key encryption to encrypt the customers' credential files and employ the ciphertext policy attribute-based encryption (CP-ABE) to encrypt the blockchain transactions. Since CP-ABE provides a one-to-many encryption with fine-grained access control, it allows several FIs to access common encrypted transactional data in the blockchain of the same client based on the access policy defined. Specifically, we devise the policy update algorithm to enable efficient encryption based on a less complicated policy tree structure. Finally, our system allows users to update their e-KYC data with any banks or FIs engaging in the blockchain. The updated e-KYC data is broadcasted in the ledger and the synchronization of the updated data is done by the responsible smart contract.

At the first occurrence of an acronym, spell it out followed by the acronym in parentheses, e.g., charge-coupled diode (CCD).

## 3. SYSTEM ARCHITECTURE


Architecture Diagram
Login,
View All Permitted e KYC Details,
View Transaction Results,
View e KYC Location Results,
View Permission Status Results,
Client
CLOUD SERVER
Register and Login,
View Profile,
Upload e KYC Details,
View All Uploaded User e KYC Details,
Authority
Register and Login,
View Profile, View All e KYC Details and Permit,
Login,
View All Clients and Authorize,
View All Smart contracts Users and Authorize,
Block chain Server
Smart Contract
Login,
View All e KYC Details,
Create Block chain and View All e KYC Details,

The system architecture provides the architecture for the proposed system in the form of different layers. In proposed system, we implement a block chain Based KYC system, in which each customer uploads a data file and encrypts these data with corresponding key. To implement both security preservation and relevant searches, we propose an effective search scheme. In this framework, the server is permitted to viably combine various encrypted records, and safely play out the pursuit without uncovering the user sensitive data, neither information documents nor the questions.

## 4. IMPLEMENTATION

**Authority**: The authority generates the public parameter *PK* and the master private key *MSK* of the system. The authority keeps the *MSK* secret and publishes *PK* available for the subscribers. The authority also generates a secret key generated based on the CP-ABE method and that key is issued to each financial institution (FI).

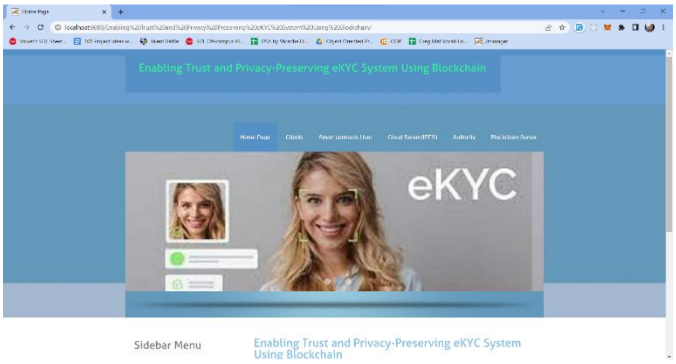
**Clients:** Clients are the customers of financial institutes who join the blockchain-based KYC. Each customer has her own key pair used to encrypt and decrypt her credential data. To allow the credentials to be stored in any FI's database or in the cloud system, the FI must get the consent digitally signed by the client.

**IPFS**: IPFS is a cloud database that stores encrypted documents of KYC bound to each user account. It serves for user's credentials to generate transaction for cryptocurrency. It houses distributed hash table (DHT) keeping the address of the hash value of the clients' credential files which are encrypted in the IPFS storage.

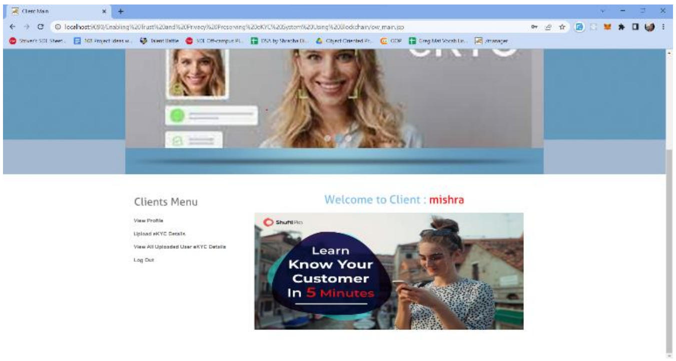
**Blockchain**: Blockchain is used to store the transactions of all KYC related activities. All sensitive transactions of the clients are encrypted. The data on the blockchain is tamperproof based on hash value and cryptography mechanism, which also prevents some illegal activities.

**Smart Contracts**: Smart contracts are used to control and automate all KYC processes. In our system, there are three smart contracts including (1) Register contract is responsible for authenticating users, enrolling new users, and uploading the encrypted credentials to the IPFS, (2) Master contract is responsible for controlling client profiles, keeping hash value of the citizen ID of all clients for interacting with IPFS, and e-consent generation, and (3) Verify contract is responsible for KYC verification.

## HOME PAGE

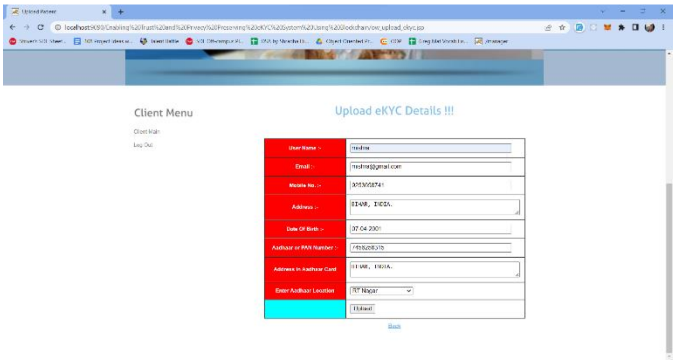

Home Page
localhost:9090/Enabling%20Trust%20and%20Privacy%20Preserving%20eKYC%20System%20Using%20Blockchain/
Enabling Trust and Privacy-Preserving eKYC System Using Blockchain
Home Page
Clients
Smart contracts User
Cloud Server(IPFS)
Authority
Blockchain Server
eKYC
Sidebar Menu
Enabling Trust and Privacy-Preserving eKYC System Using Blockchain

### CLIENT PAGE


Clients Menu
View Profile
Upload eKYC Details
View All Uploaded User eKYC Details
Log Out
ShuftiPro
Learn Know Your Customer In 5 Minutes

Welcome to Client : mishra

### CLIENT DOCUMENTS UPLOAD PAGE

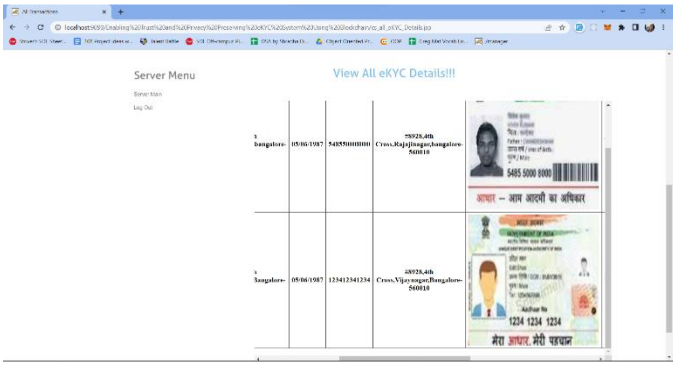


Upload eKYC Details !!!

| | |
|---|---|
| User Name :- | mishra |
| Email :- | mishra@gmail.com |
| Mobile No. :- | 9253668741 |
| Address :- | BIHAR, INDIA. |
| Date Of Birth :- | 07-04-2001 |
| Aadhaar or PAN Number :- | 7458258515 |
| Address In Aadhaar Card | BIHAR, INDIA. |
| Enter Aadhaar Location | RT Nagar |
| | Upload |

Back

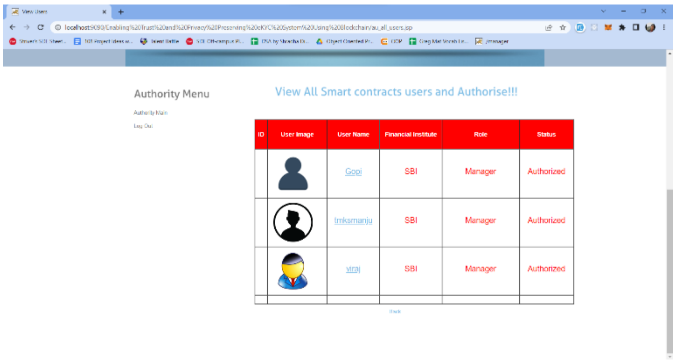
### IPFS PAGE



View All eKYC Details!!!

| | | | | |
|---|---|---|---|---|
| bangalore- | 05/06/1987 | 548550008000 | #8928,4th Cross,Rajajinagar,bangalore-560010 | |
| Bangalore- | 05/06/1987 | 123412341234 | #8928,4th Cross,Vijaynagar,Bangalore-560010 | |

### AUTHORITY PAGE

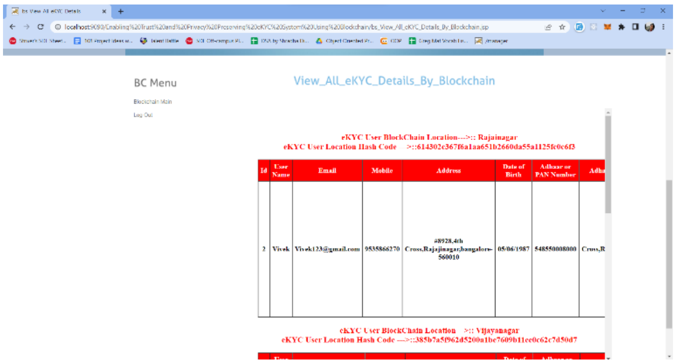


View All Smart contracts users and Authorise!!!

| ID | User Image | User Name | Financial Institute | Role | Status |
|---|---|---|---|---|---|
| | | Gopi | SBI | Manager | Authorized |
| | | tmksmanju | SBI | Manager | Authorized |
| | | viraj | SBI | Manager | Authorized |

Back

### BLOCKCHAIN MAIN PAGE



View_All_eKYC_Details_By_Blockchain

eKYC User BlockChain Location--->:: Rajainagar
eKYC User Location Hash Code --->::614302c367f6a1aa651b2660da55a1125fc0c6f3

| Id | User Name | Email | Mobile | Address | Date of Birth | Adhaar or PAN Number | Adha |
|---|---|---|---|---|---|---|---|
| 2 | Vivek | Vivek123@gmail.com | 9535866270 | #8928,4th Cross,Rajajinagar,bangalore-560010 | 05/06/1987 | 548550008000 | Cross,R |

eKYC User BlockChain Location --->:: Vijayanagar
eKYC User Location Hash Code --->::385b7a5f962d5200a1be7609b11ee0c62c7d50d7

## 5. TESTING METHODOLOGIES

### I) Unit Testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

### II) Integration Testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

### III) System Testing

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

### IV) White-box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

**V) Black-box Testing**

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box. you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

## 6. CONCLUSION

We have presented the privacy-preserving e-KYC approach based on the block chain. Our proposed scheme delivers secure and decentralized authentication and verification of the e-KYC process with the user's consent enforcement feature. In our scheme, the privacy of both customers' identity documents stored in the cloud is guaranteed by the symmetric key and public key encryption while the sensitive transaction data stored in the block chain is encrypted by symmetric key encryption and CP-ABE. Our scheme also allows the KYC data to be updated by the data owner or the customer. In addition, we devised an access policy update algorithm to enable dynamic access authorization. For the evaluation, we performed comparative analysis between our scheme and related works in terms of the computation cost, the communication cost, and performance. The experimental results showed that our scheme outperforms existing schemes in terms of performance, comprehensive KYC compliance features, and the scalable access control mechanism. For future works, we will test a larger sample of data in the real cloud environment and measure the throughput of the system in accommodating high number of e-KYC registration and verification requests. In addition, we will investigate the technique to enable batch verification of e-KYC transactions stored in the block chain with the searchable encryption feature.

## ACKNOWLEDGEMENT

It gives us great pleasure and satisfaction in presenting this preliminary report on "Secured and Privacy Preserving E-Kyc System using Blockchain". We thankful to and fortunate enough to get constant encouragement, support and guidance from all Teaching staffs of [Computer Dept] which helped us in successfully completing our project work. Also, we would like to extend our sincere esteems to all staff in laboratory for their timely support. We have furthermore to thank Computer Department HOD Prof. Ganesh Wayal and Guide Prof. A. A. Patil to encourage us to go ahead and for continuous guidance. We would also like to thank our project team members who showed immense patience and understanding throughout the project. We would like to thank all those, who have directly or indirectly helped us for the completion of the work during this project.

## REFERENCES

[1] Somchart Fugkeaw, ``Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain," in *Proc. IEEE Region Symp. (Tenssymp)*, May. 2022, pp. 49030.

[2] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu, ``Distributed blockchain-based authentication and authorization protocol for smart grid," *Wireless Communication. Mobile Computation.*, vol. 2021, pp. 1_15, Apr. 2021, doi: 10.1155/2021/5560621.

[3] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, ``Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci. Eng. Inf. Tech.*, vol. 8, pp.1735_1745, Sep. 2018.

[4] A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. A. Yousuf, and M. A. Yousuf, ``Secure and transparent KYC for banking system using IPFS and blockchain technology," in *Proc. IEEE Region Symp. (TENSYMP)*, Jun. 2020, pp. 348_351.

[5] M. Pic, G. Mahfoudi, and A. Trabelsi, ``RemoteKYC: Attacks and countermeasures," in *Proc. Eur. Intell. Secur. Informat. Conf. (EISIC)*, Nov. 2019, pp. 126_129.

[6] W. Shbair, M. Steichen, and J. François, ``Blockchain orchestration and experimentation framework: A case study of KYC," in *Proc. 1st IEEE/IFIP Int. Workshop Manag. Managed Blockchain (Man Block)*, Jeju Island, South Korea, Aug. 2018, pp. 23_25.

[7] R. Norvill, M. Steichen, W. M. Shbair, and R. State, ``Demo: Blockchain for the simpli_cation and automation of KYC result sharing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 9_10, doi: 10.1109/BLOC.2019.8751480.

[8] T. Mikula and R. H. Jacobsen, ``Identity and access management with blockchain in electronic healthcare records," in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, Prague, Czech Republic, Aug. 2018, pp. 699_706.

[9] S. Wang, R. Pei, and Y. Zhang, ``EIDM: A ethereum-based cloud user identity management protocol," *IEEE Access*, vol. 7, pp. 115281_115291, 2019, doi: 10.1109/ACCESS.2019.2933989.

[10] N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, ``KYC optimization by blockchain based hyperledger fabric network," in *Proc. 4th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE)*, Mar. 2021, pp. 1294_1299.

[11] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke, and T. Varvarigou, ``Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture, " *Future Internet*, vol. 12, no. 41, pp. 1_13, 2020.

[12] J. Bethencourt, A. Sahai, and B.Waters, ``Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, May 2007, pp. 321_334.

[13] I. Gutierrez-Aguero, S. Anguita, X. Larrucea, A. Gomez-Goiri, and B. Urquizu, ``Burnable pseudo-identity: A non-binding anonymous identity method for ethereum," *IEEE Access*, vol. 9, pp. 108912_108923, 2021.

[14] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jan. 8, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[15] J. P. Moyano and O. Ross, ``KYC optimization using distributed ledger technology," *Bus. Inf. Syst. Eng.*, vol. 59, no. 6, pp. 411_423, Dec. 2017.
[16] A. Chowdhary, S. Agrawal, and B. Rudra, ``Blockchain based framework for Student identity and educational certi_cate veri_cation," in *Proc. 2nd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Aug. 2021,pp. 916_921.