International Conference on Recent Trends in Data Science and its Applications
DOI: rp-9788770040723.134

EduChain:A Blockchain Based Identity Verification Model for Educational Institutions

ShriyaVenkatramani and Shravan Suresh
Department of Data Science and Business Systems
SRM IST
SRM Nagar, Kattankulathur, 603203, Tamil Nadu, India.
{sv3569 & ss8244}@srmist.edu.in

Dr. Paul T Sheeba
Department of Data Science and Business Systems
SRM IST
SRM Nagar, Kattankulathur, 603203, Tamil Nadu, India
pault@srmist.edu.in

***Abstract*—When it comes to cyber security, educational institutions are often undervalued. Since educational institutions typically have a huge population, the procedure for issuing and verifying identity documents must be secure, dependable, and efficient. The process may require students to make multiple trips to the issuing authorities' offices. This is just a waste of time for all the parties involved. Inadequate methods for verifying students' identities have contributed to a rise in the number of cases of digital identity theft. This paper proposes a blockchain-based identity verification model for educational institutions, as well as explores the possibility of designing such a model for Government Institutions. Third parties can validate the user's data without wasting time or money due to the immutable and decentralised ledger. For uploading files that we wish to store on the block so that a user can view and interact with them directly, our goal is to develop a front-end website with HTML, CSS, and JS. All of the student identities would be stored in an IPFS calledweb3.storage.Blockchain-based identity management system shave the potential to significantly improve user control over their own data, as well as transparency, accountability, and dependability. They can also speed up administrative processes.**

Index Terms—IPFS, Blockchain, Document Verification, SHA256,AsymmetricEncryption

I. INTRODUCTION

Asuccessfulsocietyrequiresitscitizenstobeidentifieduniquely. It is a collection of statements about an individualthat are used to distinguish them. The person's name, date ofbirth,country,andnationalidentityaretypicallyincludedhere. Thesedatasetsaregeneratedandmaintainedbycentralized organizations(governmentservers).

Educationalinstitutionsoperateinasimilarmanner.Allrelevantdocumentsarekeptinacentralrepository,andacentralauthorityprovideseveryone theiruniqueidentity.

Ateducationalinstitutions,alargequantityofpersonallyidentifiable information about students is stored. All of thisinformation, which is maintained in a Central Repository, ismanaged by the administrators of the institution. There is agood chance that the data was accidentally edited or tamperedwith. If this central repository is compromised, all sensitiveinformationaboutindividualsmightbeaccessiblebyunauthorisedpersons.Thisisconcerningsinceitopensthedoor to identity theft, security theft, and other forms of crimes,making it necessary to use strong security measures. In therecent times according to Lagzian, M.(2018) [1] identity theftshave increased significantly in the academic world. Another cause for concern is that students have no idea about who hasaccess to their data and what is being done with their data.Essentially, users' personal data is being used without theirconsent. This makes it essential to include transparency in themodel.

A. BlockchainTechnology:

"SatoshiNakamoto"introducedtheblockchainconcept in his [2] 2008 white paper, describing it as atrust less technology and claimed that bitcoin was thefirstopen-sourceapplicationofblockchaintechnology. Through cryptography, peer reviews, anddecentralised transactions, Blockchain ensures trust,security,anddataintegrity,henceeliminatingtheneed for middlemen. A Blockchain is a distributed,transparent, and immutable ledger that improves trustandproducesasystemthatisquick,safe,andreliable. Blockchain has gained popularity in a lot ofsectorslikefinance,healthcare,etcintherecentyears.[3]

Blockchainisacombinationofthreecoretechnologies:cryptographickeys,apeer-to-peernetwork, and a digital ledger. There are two types ofcryptographickeys:privatekeysandpublickeys.Eachindividualornodehasbothofthesekeys,which are used to generate a digital signature. Thisdigitalsignatureisauniqueandsecuredigitalidentificationreference,anditisthemostcriticalcomponentofblockchaintechnology.

B. Inter-PlanetaryFileSystem(IPFS)

IPFS (Inter Planetary File System) [4] is a peer-to-peer,content-addressed,version-controlledfilesystem.HTTPisthecurrentdefaultmethodforexchanging data across the Internet, howeverit failsin several instances. Large files cannot be sent viaHTTP,dataisnotpermanentonHTTP,HTTPisprimarily a Client-Server protocol, resulting in lowlatency and making it challenging to build a peer-to-peer connection. Also, real-time video streaming overHTTP is hard. All of these limitations are overcomewith IPFS. Data is requested using the hash that isreturned when data is uploaded to an IPFS network.The network allows for the distribution and copyingof data, which makes the data permanent. It searchesfor the nearest copy of the requested data when youmakearequest,whichcausesahighlatencyandpreventscongestion.Datacentralizationisnotpossiblesincethedataiscompletely distributed.

RELATED WORK

TABLE I

Year	Title	**Author(s)**	*Inference*
2018	A Comprehensive Integration of National	KumaresanMudliar;Harshal Parekh;PrasenjitBhavathankar	The proposed model [5] is to create a secure, transparent digital national identity system

Year	Title	**Author(s)**	*Inference*
	Identity with Blockchain Technology		using barcode or QR code scanning. There may be trust and adoption issues if the system fails to meet expectations, as it will be used by both government officials and citizens. To ensure successful adoption and compliance with legal requirements, thorough testing is necessary.
2018	Blockchain-based Identity Management with Mobile Device	ZhiminGao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, Weidong Shi	BlockID [6] provides a framework that embeds government issued ID into a digital certificate, which is further bound with a smart- phone through biometric-based user authentication. This ensures the security of the system by providing binding and confidentiality/integrity, and preliminary implementation of BlockID on the phone hasdemonstrated its feasibility.
2019	Blockchain Based Identity Verification Model	Gunit Malik, KshitijParasrampuria, SaiPrasanth Reddy, Dr. Seema Shah	The paper [7] discusses a blockchain-based solution for verifying the authenticity of the government issued identification documents using an HTML/CSS interface, file handling/database system, and Hyperledger Fabric platform. Downsides of the solution include high costs, proof of work consensus mechanism, and difficulty in maintaining security and privacy. Off- chain databases and cloud storage or a hybrid system, can help mitigate some of these risks.
2019	Blockchain-Based Identity Verification System	Arshad Jamal, RababAlayham Abbas Helmi, Mariam-Aisha Fatima	A Blockchain-based Identity Verification System is proposed [8] to store personal records on the blockchain.Individuals can control access to their data in the system. The system has three types of consumers: user, authority, and third-party requesters. The system should be designed to allow for multiple requests to be made at a time. Data should be stored on the blockchain for improved security andtamper-proofing.
2019	Self-Sovereign Dynamic Digital Identities based on Blockchain Technology	Himani Gulati, Chin- Tser Huang	The paper [9] introduces a self-sovereign digital identity system based on blockchain technology. The system allows individuals to maintain and control their own identity information. The identity information can include biometrics and any other variable information. The design does not address privacy concerns of users when it comes to sharing their personal data. It is important to only share necessary data and allow users to havecontrol over their data.
2020	Zero-Chain: A Blockchain-Based Identity for Digital City Operating System	Kwame OmonoAsamoah , Hu Xia , SandroAmofa, Obiri Isaac Amankona, KechengLuo, Qi Xia JianbinGao , Xiaojiang Du and Mohsen Guizani	The authors of the paper [10] are attempting to create a secure system for digital city management, specifically focused on the secure identification of individual residents. Their system will store user attributes and securely transmit them to other system components for verification, ultimately creating a digital identity for the applying resident. The set of transactions leading to the ID creation will be stored in the blockchain, ensuring security and providing a basis for the development of a digital infrastructure for smart city management.
2021	BIdM: A Blockchain-Enabled Cross-Domain Identity Management System	Ruibiao Chen, FangxingShu, Shuokang Huang, Lei Huang, Huafang Liu, Jin Liu, Kai Lei	The paper [11] proposes a decentralized identity management system and cross-domain authenticationsystem to solve the problem of single point of failure in authentication centres. Limitations of the model include scalability issues and difficulty in ensuring trust and privacy. To overcome these limitations, the model should be designed to be more scalable and use cryptography to ensure trust and privacy.The model should also be designed with the minimum disclosure principle in mind, to only disclose necessary identity information during

DOI: rp-9788770040723.134

Year	Title	**Author(s)**	*Inference*
			authentication.

II. PROPOSED ARCHITECTURE

EduChain is a model for identity verification using IPFS andblockchaininaneducationalorganisationthathasthepotential to increase efficiency, security, and transparency intheverificationprocess.Firstly,themodelinvolvesthreeparties: the student, the admin, and the requestor. The studentregisters on the portal and is assigned a unique ID (API key)thattheycanusetologintothesystem.Theythenuploadtheir documents on the IPFS, which generates a unique hashforeachdocument.Thishashservesasproofofthedocument's authenticity and is used to verify the documentlateron.Theadminplaysacrucialroleintheverificationprocess. They can view all the files uploaded by the studentand verify them by checking the contents of each document.Once verified, the admin pushes the student's API key to theblockchain,whichservesasapermanentrecordofthestudent'sverifiedidentity.Thisensuresthatthestudent'sidentity information cannot be tampered with or altered in anyway. The requestor can then request access to the student'sinformation onthe portal.However, beforegranting access,theadminfirstobtainsthestudent'spermission.Oncethestudent grants permission, the admin provides the requestorwiththepublickeyoftheblockcontainingthestudent's verified identity information. This public key can be used bytherequestor to accessthestudent'sinformation.

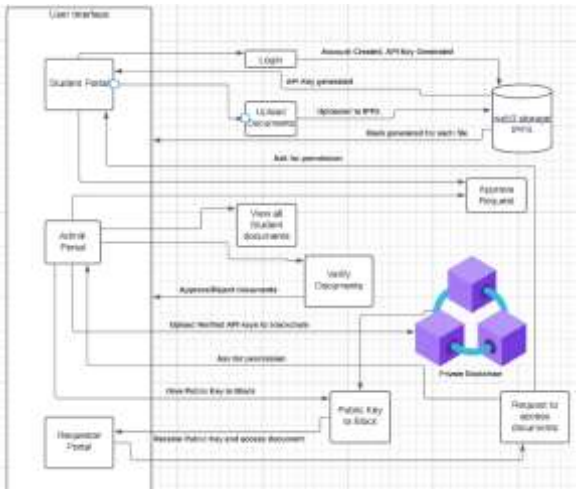

Fig.1.ArchitectureDiagram

III. METHODOLOGY

Theproposedmodelhas 3 maincomponents:TheUI,theIPFSandthe Blockchain.

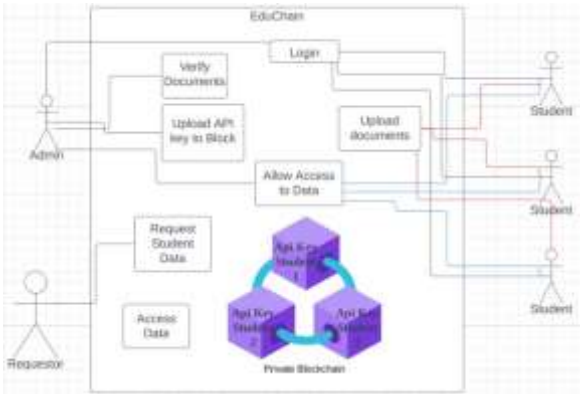

Fig. 2.UseCaseDiagram

TheUserInterface:TodesignasimpleyetappealingUIthatwillserveastheEduChainportal,weusedHTML,CSS,andJS. The student, the administrator, and the requestor are thethreemainpersonasforEduChain.

A. Thestudentportal:Thestudentwouldregisterthemselves and make a new login for themselves onthe student portal. The student would then receive anAPIkeyfortheirID.Theywouldbeuniquelyidentified by this. This API key can be used by thestudent to log into IPFS. The student can then uploadtheirdocumentstotheportalandwaitforadminverification. Each uploaded document would have adistinct hash that would be used to identify it. Thestudent may preview any uploaded documents in theimagegallerycarousel.Oncetheirpaperworkdocuments have been approved, their API key will beuploadedtotheblockchain,giving themaccesstotheirdocuments.Requestorsmaysubmitrequests,which students may approve or reject, after which therequestormay see therequested documents.

B. Theadminportal:Everystudentislistedonthisadmin portal. Each student who has registered on theportalisvisibletotheadministrator.Allofthestudent's uploaded documents are visible when theyclickonaspecificstudent.Theadmin verifies thedocumentsandthenapproves them.Fordemonstrative purposes, we have established correctfilenamingasthecriterionforacceptance(FILENAME in all capitals eg: AADHAR). Criteriacanbeestablishedbasedonwhattheuniversityrequires.Oncethepapershavebeenverified,theadministrator will upload the student's API key to theblock. All requests submitted by the requestor can beviewed by the admin, who can then accept or rejectthem. The admin provides the public key to the blocktherequestor needsafterreceivingapproval.

C. The requestor: The requestor submits the request toaccess the student data. Once the request has beenapproved by the student and the administrator, theyare given access to the public key of the block wherethe student's API keyis uploaded. They can accessthe student's uploaded documents using this API keyand use themasnecessary.

The requestor functionality provides an added layer of securityand control for students over who can view their documents,ensuringthatonlythosewhohavebeenapprovedbythestudentcanaccessthem.Italsomakesitpossibleforrequestorstoaccesstherequireddocumentsquicklyandeasily,withouthavingtogothroughthestretched-out andpotentiallyriskyprocedureofaskingdocumentsfromthestudent directly. All the parties are equally involved in sharingandaccessingpersonal studentdata.

IPFS: In our proposed system, IPFS will be used as the storageplatform for all the documents uploaded by the

DOI: rp-9788770040723.134

students. EachdocumentuploadedbythestudentwillbestoredontheIPFS network and will be associated with a unique hash. This hashwill be used to retrieve the document from the IPFS network.Web3.storage is a cloud storage solution built on top of theIPFS network. It provides developers with an easy-to-use andreliable way to store and retrieve files on the IPFS network,withouthavingtomanagetheunderlyinginfrastructure themselves. It is easily scalable and very reliable and it waseasy to integrate it to our website using the API it provides forintegration. The service is designed to ensure that files arestoredsecurelyandcanbeaccessedquicklyandeasily.Additionally,thecostofstoringandsharingdocumentsisquitelow.

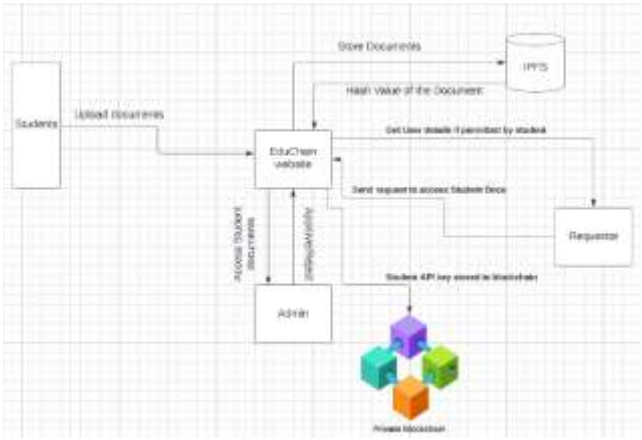

Fig. 3.SystemDesign

Blockchain: In an educational setting, verifying the identity ofstudentsiscrucialformaintainingacademicintegrityandpreventing fraud [12]. By using a blockchain architecture thatincludesastudent'sAPIkey,wecanensurethatonlyauthorized people have access to personal student data.Theuseofa blockchainarchitectureprovidestransparencyandaccountability. Because the blockchain is decentralized anddistributedacrossmultiplenodes,itistransparentandauditable by anyone with access to the network. This meansthat administrators can monitor and verify the usage of thestudent's API key, ensuring that it is being used for authorizedpurposesonly.

In a simple blockchain architecture, each block would containa student's API key. To achieve this, we would first define thestructure of a block, including its components and properties.We will be using JavaScript to develop this private Blockchainrepresentation.ByusingJavaScript,wecancreateablockchain that is accessible and easy to integrate intotheexistingsystem,whilestillprovidingthesecurityandimmutability thatblockchain technologyoffers.

Typically, a basic block is made up of a hash, a body, and aheader. The header includes information about the block, likeitsindex,timestamp,andhashoftheblockprecedingitinthechain. The body contains the actual data to be stored in theblock,whichinourcasewouldbethestudent'sAPIkey.Finally, the hash is a unique identifier for the block that isgenerated by running the block's header and body through acryptographichash function.

WecreateaJavaScriptobjectthatrepresentstheblock'sstructure and has attributes header, body, and hash in order toaddanewblocktoourblockchain.Theblock'sindex,timestamp,andthehashoftheprecedingblockinthechainare all included in the header properties. The body propertywouldcontainthestudent'sAPIkey.Finally,thehashpropertywouldbegeneratedbyrunningtheblock'sheaderand body through a hash function. In our case we would beusing SHA-256algorithm forhashing.

SHA-256[13] is a one-way hash function that is impossible toreverse, making it difficult for attackers to tamper with theblockchainorcreatefakeblocks.Itisfastandefficient,generating a unique hash value for any input data quickly. It isa widely used hash function that has been extensively testedand reviewed by the cryptography community. Using SHA-256 in this model ensures that the blockchain is compatiblewithexistingplatforms,makingiteasiertointegrateanduse.

IV. Conclusion And Future Enhancements

Document verification is a crucial aspect of various fields,includingbanking,healthcare,legal,educationandmany more. Blockchain technology is well-suited to address issuesrelated to document verification and identity authentication.Onceinformationisaddedtotheblockchain,itcannotbechanged.Thispropertymakesitidealforensuringtheintegrityandauthenticityofdocuments.Inconclusion, theproposed EduChain system provides a secure and transparentplatform for storing and sharing educational documents. ByusingIPFSforstorageandablockchainarchitectureforauthentication and authorization, the system ensures that onlyauthorized individuals canaccess a student's personal data.The system provides a simple and appealing user interface forstudents, administrators, and requestors, making it easy to useand integrate into existing systems. Additionally, the use of adistributed blockchainarchitecture ensures transparency andaccountability, making it difficult for attackers to tamper withthe informationstoredinthe blockchain.

The EduChain model can be integrated with other educationalsystems to provide seamless access to educational credentialsand documents. APIs can be created to integrate with LMS orSIS,andthemodelcanbeexpandedtoothereducationalinstitutions. This will provide a universal platform for studentsto store and share their academic credentials and documents,makingtheentireprocessmoreefficientandtransparent.Integrationswithsmartcontracts[14]canbedoneinthefuture to automate the verification and authentication processof academic documents. This will ensure that the documentsareverifiedautomatically,eliminatingtheneedformanualverification by administrators. The EduChain model can alsobe integrated with AI and Machine Learning algorithms toprovide advanced analytics and insights [15] into academicdocuments. This will help institutions to identify trends

andpatternsinacademicperformance,allowingthemtomakemoreinformeddecisionsaboutstudentprogressandachievement.

Overall, the EduChain model has the potential to revolutionizethe way academic credentials and documents are stored andshared, providing a more efficient and transparent system thatis accessible to all. As technology continues to evolve, therewill be opportunities to enhance and expand the EduChainmodel to provide evengreatervalue to students, educators,and institutions.

REFERENCES

[1] Dadkhah, Mehdi,Mehraeen, Mohammad andBorchardt, Glenn,"Identity Theft in the Academic World Leads to Junk Science," Science andEngineeringEthics, 2018,24.10.1007/s11948-016-9867-x.

[2] S. Nakamoto,Bitcoin: A Peer-to-Peer Electronic Cash System, 2008,https://bitcoin.org/bitcoin.pdf

[3] Z.Zheng,S.Xie,H.Dai,X.ChenandH.Wang,"AnOverview ofBlockchainTechnology:Architecture,Consensus, and FutureTrends," 2017IEEEInternationalCongressonBigData(BigDataCongress),Honolulu,HI,USA,pp.557-564,2017,doi:10.1109/BigDataCongress.2017.85.

[4] Benet,Juan,(2014)."IPFS-ContentAddressed,Versioned,P2PFileSystem," 2017.

[5] K.Mudliar,H.ParekhandP.Bhavathankar,"Acomprehensiveintegration ofnationalidentitywithblockchaintechnology,"2018International Conference on Communication information and ComputingTechnology(ICCICT),Mumbai,India,pp.1-6,2018,doi:10.1109/ICCICT.2018.8325891.

[6] ZhiminGao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen,andWeidongShi.,"Blockchain-basedIdentity ManagementwithMobile Device,". In Proceedings of the 1st Workshop on Cryptocurrenciesand Blockchains for Distributed Systems (CryBlock'18). Association forComputingMachinery,NewYork,NY,USA,pp. 66–70,2018,https://doi.org/10.1145/3211933.3211945.

[7] G. Malik, K. Parasrampuria, S. P. Reddy and S. Shah, "Blockchain BasedIdentity Verification Model," 2019 International Conference on VisionTowardsEmergingTrendsinCommunicationandNetworking(ViTECoN),Vellore,India,pp.1-6,2019,doi:10.1109/ViTECoN.2019.8899569.

[8] Jamal, Arshad,Helmi, Rabab,Syahirah, Ampuanand Fatima, Mariam-Aisha,"Blockchain-Based Identity Verification System,"pp. 253-257, 2019,10.1109/ICSEngT.2019.8906403.

[9] H. Gulati and C. T. Huang, "Self-Sovereign Dynamic Digital Identitiesbased on Blockchain Technology," 2019 SoutheastCon, Huntsville, AL,USA,pp.1-6,2019,doi:10.1109/SoutheastCon42311.2019.9020518.

[10] Dhanabalan, S. S., Sitharthan, R., Madurakavi, K., Thirumurugan, A., Rajesh, M., Avaninathan, S. R., & Carrasco, M. F. (2022). Flexible compact system for wearable health monitoring applications.Computers and Electrical Engineering, 102, 108130.

[11] R.Chen etal.,"BIdM:ABlockchain-EnabledCross-DomainIdentityManagement System," in Journal of Communications and InformationNetworks,vol.6,no.1,pp.44-58,March2021,doi:10.23919/JCIN.2021.9387704.

[12] F.M.Enescu,N.Bizon andV. M.Ionescu,"Blockchain technologyprotects diplomas against fraud," 2021 13th International Conference onElectronics,ComputersandArtificialIntelligence(ECAI),Pitesti,Romania,pp.1-6,2021,doi:10.1109/ECAI52376.2021.9515107.

[13] Pazhani. A, A. J., Gunasekaran, P., Shanmuganathan, V., Lim, S., Madasamy, K., Manoharan, R., &Verma, A. (2022).Peer–Peer Communication Using Novel Slice Handover Algorithm for 5G Wireless Networks.Journal of Sensor and Actuator Networks, 11(4), 82.

[14] A. Abuhashim and C. C. Tan, "Smart Contract Designs on BlockchainApplications," 2020IEEESymposiumonComputersandCommunications(ISCC),Rennes,France,pp.1-4,2020,doi:10.1109/ISCC50000.2020.9219622.

[15] I.H. Sarker, "Machine Learning: Algorithms, Real-World Applications andResearchDirections,"SNCOMPUT.SCI., vol.2,p. 160,2021,https://doi.org/10.1007/s42979-021-00592-x