A Blockchain Based Authentication for Digital Documents

Naveen Gandhi G [1],Suresh Balaji R [2], Chandralekha P [3],Maheswari M [4] Roselin Mary S [5]

1. Student, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India.
2. Student, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India.
3. Assistant Professor, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India.
4. Assistant Professor, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India.
5. Head of Department, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India.

ABSTRACT

With the rapid boom within the quarter of data technology and smooth access to reasonably-priced and advanced office devices in the marketplace, the faking of crucial files has turn out to be a rely of challenge these days. consequently, the want for verification and authentication practices of various crucial files in the form of banking documents, government documents, transaction documents, instructional certificates etc is likewise increasing. however, various tough and tedious techniques have made document verification very complicated and time-eating which encouraged us to behaviour this studies. in this paper, we gift a decentralized internet utility for virtual record verification using Ethereum blockchain-primarily based era in P2P cloud garage to beautify the verification system by way of making it extra open, obvious, and auditable. The proposed version consists of several strategies together with public/personal key cryptography, online storage security, virtual signatures, hash, peer-to-peer networks and proof of work which has made the verification of any uploaded documents for any business enterprise or authority faster and handy with only a click on. moreover, respective hash values are also assigned to every person document. Our proposed model effectively meets up all of the standards for a digital document verification gadget by assuaging the gaps and difficulties inside the conventional strategies in report verification.

INDEX TERMS : Blockchain, Hashing, Ethereum, Document Verification, Digital Signature, Cryptography

I. INTRODUCTION

The rapid development of facts sharing and changing is driving more and more groups and man or woman users toward the usage of digitized files. furthermore, the bulky and time-consuming use and validation system of traditional physical documents make contributions to motivating humans to apply modern approaches of issuing and validating critical documents. though virtual files are undoubtedly convenient to apply, proving the authenticity of these files is mostly a count of difficulty. due to the technological revolution and ease of get admission to cheap and superior gadget, the forgery of crucial files has grow to be quite easy and made report authentication quite a tedious project. The implication springing up from the hassle of fake documentation is causing severe and alarming impacts and wishes to be urgently considered. therefore, a system to validate the authenticity of essential documents would be substantially beneficial to users for retaining their virtual documents. there may be an open-supply, immutable, and consensus version available known as blockchain to solve this hassle [3].

Blockchain technology is a current invention to enhance the record verification manner and entangle the task of reducing report fraud and misuse [4]. Blockchain without a doubt refers to a dispensed database that chronologically shops multiple blocks chained collectively with each facts % or block storing files in a manner

that makes it impossible to govern these documents [8]. Blockchain is a complicated technology that could play many vast roles within the enterprise to overcome any failure. Blockchain guarantees consider, integrity, consensus, autonomy, and protection [13]. owing to the merely reliable, obvious, and incorruptible technique of storing and validating the transactions, we've got additionally been motivated with the aid of this blockchain era to apply it in our paintings to authenticate essential virtual files.

II. RELATED WORKS

In current years, blockchain has emerge as a completely popular technology in the industry. several surveys and studies had been carried out to enforce blockchain in various sectors. on this element, we are able to describe some of these preceding works available regarding blockchain. Leible et al. discussed the possibilities and advantages of blockchain in open technological know-how structures. They described how can we put in force blockchain in exclusive sectors, and the contribution of blockchain to this point inside the industry, etc . As blockchain is gaining popularity worldwide due to its allotted and decentralized nature, Joshi et al. completed a survey focusing at the fundamental challenges and opportunities in blockchain technology and also its safety and privateness issues are described. The essential idea and structure of blockchain are proven very in brief from the beginning. The authors additionally tried to interpret using blockchain in IoT, protection, security, and scientific sectors. Chen et al. survey discussed unique styles of regions in which blockchain should deliver a higher answer. along with cryptocurrency, healthcare, coverage policy, copyright safety, credit transfer, and so forth . Gilani et al. did a comprehensive survey on blockchain-primarily based identity control and personal statistics garage machine. They discussed a self-sovereign identity (SSI) concept for the customers that's the facts possession manipulate. The survey is all approximately a consumer-centric statistics management gadget doing away with crucial authority the usage of blockchain. A survey on using blockchain in highbrow assets is summarized via Wang et al. Rouhani et al. defined a quick technical review of Ethereum blockchain and clever agreement. Yue et al. proposed a version for records integrity verification the use of the blockchain approach. They described the flaws in a regular cloud-based verification machine that consists of 1/3 party proprietors and made a P2P platform the use of the blockchain based totally Markle tree shape where customers can ensure information integrity. For verification, a random sampling approach is used by the authors. And mathematical assessment of the value and time propagation for this technique is given. Teymourlouei et al. proposed a version for user authentication the use of blockchain that's greater secured than the traditional electronic mail and password based totally authentication machine . The authors described the benefits of the use of private and public keys for file verification.

III. EXISTING SYSTEM

In the present device, identification verification performs an vital role in our each day lives. for instance, get entry to control, bodily protection and global border crossing require us to affirm our get admission to (protection) degree and our identities. to verify who we are through displaying our identification documents containing face pictures, consisting of passports and driver licenses, to human operators. however, this manner is sluggish, hard work extensive and unreliable. As such, an automated machine for matching identity report pics to live face images (selfies) in actual time and with excessive accuracy is required. After verifying a vacationer’s identification by using face contrast, the gate is automatically opened for the tourist to enter. For ID selfie matching, they are comparing a scanned or digital record image.

IV. PROPOSED SYSTEM

we are featuring a certificate machine based on blockchain to triumph over the hassle. statistics are saved in different nodes, and every person who desires to adjust a particular internal datum need to request that other nodes modify it simultaneously. accordingly, the device is quite dependable. We evolved a decentralized utility and designed a certificates system primarily based on Ethereum blockchain. This era became selected because it's far incorruptible, encrypted, and trackable and permits facts synchronization. by way of integrating the functions of blockchain, the system improves the efficiency operations at each level. The gadget saves on paper, cuts control fees, prevents record forgery, and provides correct and dependable facts on digital certificate and compare person live face with demonstrated document face.

ADVANTAGES

Blockchain no longer handiest lets in transparency at transaction level but additionally enhance the availability and integrity of the records. The document garage becomes more scalable due to the storage of hash of the document digitally, occupying less space.

V. SYSTEM DESIGN

person needs to registers into his utility and a request could be despatched to important board server for authentication. until the valuable board server approves the request user can't login into his account. when primary board server approves the request a key may be generated and user can login into his account. After consumer login into his account he needs to add certificate specifically pan card, aadhar card, voter identification, sslc certificate to critical board server. principal board server will review the certificate and accepts or decline the certificates. If imperative board server accepts the accepts the certificates the ones information may be stored in E.C.S and Blockchain. If vital board server declines the certificate it won't be saved in E.C.S. or Block Chain. If consumer needs a certificates he will ship request to primary board server. If central board server located the user info to be real he accepts the request and ahead a request to E.C.S in which all the certificate might be there. E.C.S. responds for the request and certificate could be supplied to the person. If user desires to practice for any certificates he'll send request to vital board server and relevant board server will test the information and ahead the request to E.C.S. E.C.S will generate the QR Code and forwarded to consumer thru primary board server. consumer forwards the QR code to the verifying authority and if all information are correct and face fits with stay face Verifying authority will difficulty the file.

A. MODULES

- User registration and authentication
- User upload certificate
- Get certificate
- QR request and response from verification authority

User registration and authentication:

In this module person wishes to registers into his utility and a request can be dispatched to vital board server for authentication. except the crucial board server approves the request person can not login into his account. while central board server approves the request a key will be generated and user can login into his account.

User upload certificate:

After person login into his account he needs to upload certificate specifically pan card, aadhar card, voter identity, sslc certificate to significant board server. vital board server will assessment the certificates and accepts or decline the certificates. If significant board server accepts the accepts the certificates those information could be stored in E.C.S and Blockchain. If valuable board server declines the certificates it won't be stored in E.C.S. or Block Chain.

Get certificate:

If user wishes a certificates he'll send request to imperative board server. If vital board server found the person information to be authentic he accepts the request and forward a request to E.C.S in which all of the certificates could be there. E.C.S. responds for the request and certificates may be supplied to the user.

QR request and response from verification authority:

If person needs a certificate he's going to ship request to imperative board server. If significant board server determined the person info to be proper he accepts the request and ahead a request to E.C.S where all of the certificates can be there. E.C.S. responds for the request and certificates might be provided to the user.

B. SYSTEM MODEL

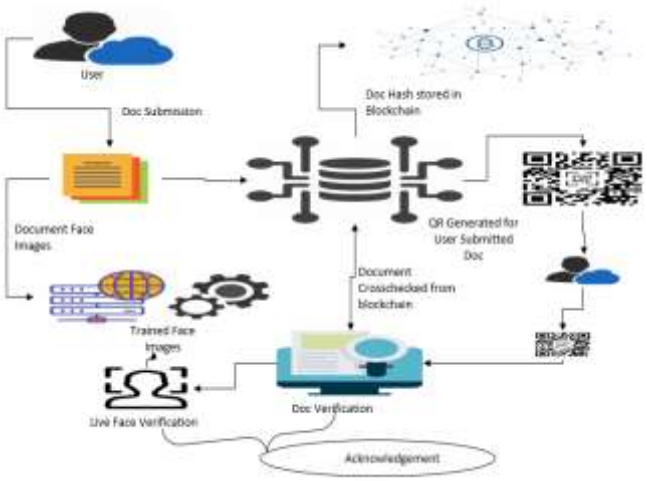

Fig 5.1 System architecture

VI. RESULT AND DISCUSSION

Fig 6.1 admin page

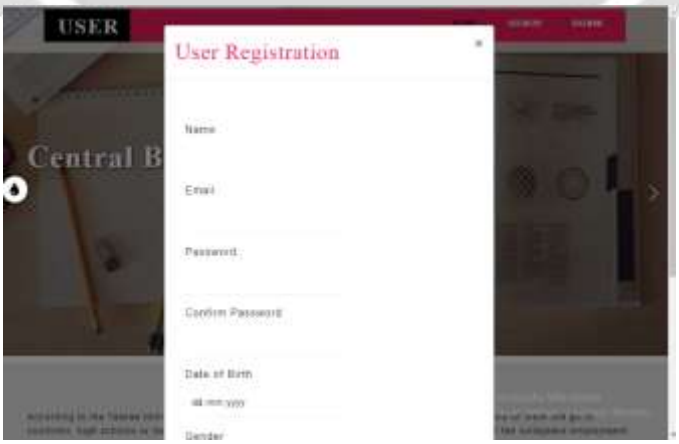

Fig 6.2 user registration

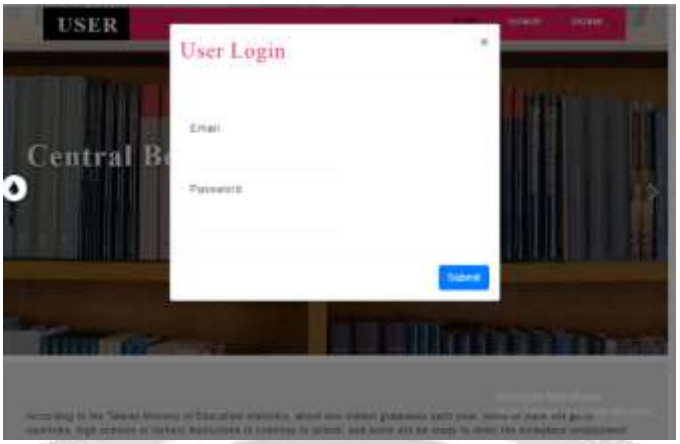

Fig 6.3 user login

Fig 6.4 user identity

Fig 6.5 submitting digital documents

Fig 6.6 QR request for digital documents

Fig 6.7 scan the QR code to decrypt

Fig 6.8 decrypted documents

Fig 6.9 Result

VII CONCLUSION AND FUTURE WORKS

To keep away from file forgery and misuse a higher solution changed into wanted for a long time. therefore, we proposed a model to clear up this global problem. the principle motive of our evolved machine is to create a platform to store and affirm any vital documents like certificates, land/assets/as set facts, scientific facts and many others. We applied the entire machine right into a blockchain network. The collaboration of a few capabilities like cryptographic hash, decentralization and digital signature makes blockchain era immutable .So, there remains no crucial server to very own the statistics instead all the data regarding any transactions is sent to the whole network. Our proposed system stands strongly primarily based on security. hence, any manipulation inside the documents is not possible. The verification end result is usually accurate and efficient. After evaluating our device with the general cloud-based totally statistics garage system and verification manner we located significant development in each protection enhancement and time optimization. And the use of our proposed model statistics corruption and misuse will fairly be decreased. Any organization, business enterprise and group can use this device for better security. Inconclusion, our proposed version ensures integrity and protection for each use case. however, as a brand new and developing technology blockchain has some minor complexities to use in each platform. however nevertheless, blockchain technology outperforms any cutting-edge system software available within the enterprise by using a large margin. despite all of that our future plan with this model is to create a terminal-based file authentication with the support of a couple of file upload and different accessibility to increase usability for higher overall performance.

VIII REFERENCES

[1] S. Leible, S. Schlager, M. Schubotz, and B Gipp, "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science,"
(2019), Front. Blockchain 2:16.doi: 10.3389/fbloc.2019.00016.

[2] A. Prashanth Joshi, M. Han, and Y. Wang, "A Survey on Security and Privacy Issues of Blockchain Technology," (2018), Mathematical Foundations of Computing, Volume 1, Issue 2, pp. 121-147, doi: 10.3934/mfc.2018007.

[3] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A Survey of
Blockchain Applications in Different Domains," (2018), pp. 17-21, doi: https://doi.org/10.1145/3301403.3301407.

[4] K. Gilani, E. Bertin, J. Hatin and N. Crespi, "A Survey on Blockchainbased Identity Management and Decentralized Privacy for Personal Data," 2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), Paris, France, 2020,
pp. 97-101, doi: 10.1109/BRAINS49436.2020.9223312.

[5] J. Wang, S. Wang, G. Junqi, Y. Du, S. Cheng, and X. Li, "A Summary of Research on Blockchain in the Field of Intellectual Property," (2019), Procedia Computer Science, Volume 147, pp. 191-197, doi: https://doi.org/10.1016/j.procs.2019.01.220

[6] S. Rouhani and R. Deters, "Security, Performance, and Applications of Smart Contracts: A Systematic Survey," in IEEE Access, vol. 7, pp. 50759-50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[7] D. Yue, R. Li, Y. Zhang, W. Tian and C. Peng, "Blockchain
Based Data Integrity Verification in P2P Cloud Storage," 2018
IEEE 24th International Conference on Parallel and Distributed
Systems (ICPADS), Singapore, Singapore, 2018, pp. 561-568, doi: 10.1109/PADSW.2018.8644863.

[8] H. Teymourlouei and L. Jackson, "Blockchain: Enhance the Authentication and Verification of the Identity of a User to Prevent Data Breaches and Security Intrusions," (2019).
[9] X. Zhu, "Blockchain-Based Identity Authentication and Intelligent Credit Reporting," (2020), Journal of Physics: Conference Series, volume 1437, 012086, doi: 10.1088/1742-6596/1437/1/012086.

[10] L. M. Arjomandi, G. Khadka, Z. Xiong and N. C. Karmakar, ”Document Verification: A Cloud-Based Computing Pattern Recognition Approach to Chipless RFID,” in IEEE Access, vol. 6, pp. 78007-78015, 2018, doi: 10.1109/ACCESS.2018.2884651.

[11] L. Musarella, F. Buccafurri, G. Lax, and A. Russo, “Ethereum Transaction and Smart Contracts among Secure Identities,” (2019).

[12] C. Lakmal, S. Dangalla, C. Herath, C. Wickramarathna, G. Dias and S. Fernando, ”IDStack — The common protocol for document verification built on digital signatures,” 2017 National Information Technology Conference (NITC), Colombo, 2017, pp. 96-99, doi: 10.1109/NITC.2017.8285654.

[13] M. HamithaNasrin, S. Hemalakshmi, and Prof G. Ramsundar, “A Review on Implementation Techniques of Blockchain enabled Smart Contract for Document Verification,” International Research Journal of Engineering and Technology (IRJET), Volume 6, Issue 2, 81, February
2019.

[14] O. Ghazali, and O. Saleh, “A Graduation Certificate Verification Model via Utilization of the Blockchain Technology,” (2018), Journal of Telecommunication, Electronic and Computer Engineering, 10, pp. 29- 34.

[15] M. Shah and Dr. Priyanka Kumar, “Tamper Proof Birth Certificate using Blockchain Technology”, International Journal of Recent Technology and Engineering (IJRTE), Volume 7, Issue 5S3, pp. 95-98, February 2019.