SecureExamChain: A Decentralized Approach to Online Assessments

Prof. A. S. Pingle
arati.pingle@pvgcoenashik.org

Vivek Jadhav
vivsurjadhav@gmail.com

Anurag Pawar
pawar.anurag350@gmail.com

Bhaskar Vaidya
bhaskarvaidya.officiall@gmail.com

Sainath Sabale
sainathsabale31@gmail.com

Department of Information Technology
Pune Vidyarthi Griha's College of Engineering & Shrikrushna S. Dhamankar Institute of Management, Nashik

Abstract - In the cutting-edge era, records stands proud as one of the maximum important assets, surpassing other commodities. Users are increasingly willing in the direction of safeguarding their records from outside threats. Blockchain era emerges as a distinguished answer, providing remarkable safety and integrity for information. Initially synonymous with cryptocurrency, blockchain has developed to discover significant use in personal settings within businesses, ensuring records security. The essence of blockchain lies in creating decentralized systems, facilitating stable and green records transmission inside a network. This manner that statistics remains hid from outside entities, with authorized users maintaining extraordinary rights for analyzing and writing facts. Leading international industries which includes Walmart, IBM, and Google are actively embracing blockchain era to assemble Decentralized Applications (DApps). DApps constitute smart structures achieved on a distributed laptop network. Notably, blockchain facilitates the introduction of Smart Contracts, which are automated and secure disbursed ledgers allowing tamper-proof transactions with transparency. Smart contracts utilize hashing, a sturdy mathematical system employing the effective cryptographic algorithm SHA-256, producing a 256-bit signature for input textual content. The Ethereum Blockchain Platform serves as a widely adopted platform for DApps, working as a public community accessible to excited by stable transaction exchanges. Blockchain generation extends its influence throughout numerous sectors, consisting of advertising and marketing, business, education, and deliver chain control. This examine delves into the exam of the Ethereum Blockchain Platform in the academic machine. An application has been developed for the Online Examination System making use of the Ethereum Blockchain Platform, incorporating Smart Contracts, NodeJS for server runtime, and MongoDB because the database system. The blockchain-primarily based device exhibits advanced protection in comparison to cloud-based options. Furthermore, the analysis underscores the heightened trustworthiness of blockchain-based online examinations relative to different systems.

Key Words: Blockchain, NodeJS, SHA-256, Ethereum.

INTRODUCTION

In the cutting-edge generation, the transition of numerous sports to the net has facilitated substantial accessibility to statistics from any place. However, this shift has added new demanding situations, consisting of worries about facts protection, transparency, and trust across the global community. Many academic institutions and impartial organizations, which include the National Testing Agency (NTA), have embraced online exam structures, a fashion increased via the COVID-19 pandemic. The primary obstacles confronted with the aid of such structures are ensuring agree with and protection.

Numerous international marketplace gamers offer solutions inclusive of personal network lockers, passwords, One-Time Passwords (OTPs), and sturdy security measures. The present solutions, often reliant on third-birthday party involvement, gift a key assignment in phrases of data safety. Blockchain era, an emerging paradigm, addresses these challenges by way of beginning a revolution in privatization, ensuring that records stays below the consumer's manipulate with out the need for 1/3-birthday celebration intervention.

In blockchain networks, records blocks are utilized for storing and dealing with statistics. The integrity of the information is maintained thru cryptographic validation of every facts block. Each block is connected with a completely unique cryptographic hash code generated through the effective SHA-256 set of rules. Validators play a essential function within the network, making use of diverse consensus mechanisms to provide a legitimate signature code for every statistics block.

Blockchain is synonymous with decentralized ledgers, which intelligently encapsulate entire datasets generated automatically after assignment completion, often referred to as clever contracts. These smart contracts function evidence of settlement for paintings executed with out reliance on any 0.33-celebration device. Blockchain reveals applications in various domain names, inclusive of commercial enterprise, fitness, supply chain, and schooling systems.

This paper focuses on leveraging blockchain era within the schooling area, specially in accomplishing straightforward examinations. The proposed online examination device the usage of blockchain ensures authentication by requiring candidates to check in and pay the exam charge. Only authenticated users are granted participation rights. Upon login, candidates insert the transaction hash to provoke the exam. Post-exam, all data, along with questions, solutions, transaction info, and timestamps, is securely transmitted to the exam center through a smart agreement at the blockchain community. This smart settlement serves as verifiable evidence for both the consumer and the exam middle.

The rest of the paper is established into four sections. The 2nd segment compares the blockchain-based totally examination system with cloud-primarily based alternatives. The third section presents a review of the technological historical past supporting the blockchain-based examination system. The fourth phase info the device's structure and operation, whilst the very last phase outlines capacity destiny enhancements.

LITURATURE SURVEY

From 2010 onwards, the creation of cloud era revolutionized the education machine, main to the emergence of online publications and examinations. The convenience of getting access to facts from everywhere and at any time made cloud-primarily based systems extensively adopted by using educational corporations, consisting of for authorities examinations. However, this shift added about challenges along with connectivity problems, records security concerns, and the need for sturdy consumer authentication [4,5].

Connectivity troubles caused transaction disasters and hindered easy information change across networks. Data safety became a large fear because of the prevalence of hackers, prompting the use of firewalls and antivirus structures. However, these solutions have been deemed inadequate and high-priced. Additionally, making sure the legitimacy of applicants inside the exam gadget posed a substantial project.

Enter blockchain generation, providing a technique to the demanding situations faced via cloud-primarily based systems. Known for its more desirable safety, transparency, and authentication features, blockchain presents a singular technique to maintaining network integrity. In a blockchain, statistics is based into blocks, every related by way of a completely unique 256-bit hash code [6]. Unlike cloud-based totally systems, there is no want for external additives like Data Centers or firewall extensions. The blockchain community operates as a incredibly stable and licensed environment, minimizing statistics trade and transaction screw ups. In the rare case of a failure, the system halts and eradicates all related statistics.

Blockchain's Decentralized Ledger Application, performing as proof of labor, mechanically facts all relevant data without counting on 0.33-birthday party interventions. This decentralized nature guarantees the reliability, protection, and transparency of the entire examination technique. As cloud-based systems grapple with connectivity, security, and authentication challenges, the integration of blockchain era emerges as a transformative answer, reshaping the panorama of educational tests.

PROPOSED SYSTEM

In this examination system, first candidates register themselves individually and get their blockchain account address. The blockchain account address is a unique address for every participant. This address is of 16-byte code which is generated by applying the SHA 256 algorithm on the registration data. This has code save into the database system of the university portal where the administrator/examination cell identified easily. For the student database, we use the MongoDB database which is easy to run and control. MongoDB is a NoSQL database tool, where there direct data interaction is possible without the need for any query call as well as for the registration and backend services we use Node.JS JavaScript framework, which compatible with GUI and database system. In node.js we write the procedure of all the APIs which are created the endpoints to connect the server of the network and run the application services on the network
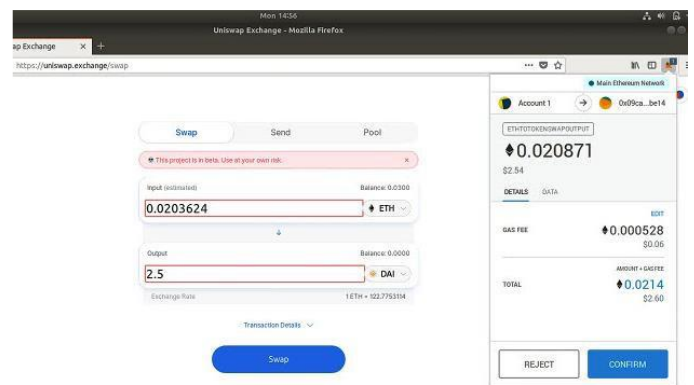

Figure: 1 Proposed System

For the GUI we use the React.JS. It is a JavaScript library that is used to create and build User Interfaces for server-side applications. This is specially used for single-pages applications to handle the view on the web or mobile-based decentralized applications. The special feature of this library is to develop the reusability UI components of the application. For the contracts design and deploy the smart contract we use the solidity contract oriented high-level language which interacts with the application by the Web3.JS Blockchain libraries. This contract invokes all the data into it and generated both end of the system candidate as well as an examination center. The generation of the contract is proof of work on both ends. The transaction fee of the examination is deducted through the Ethereum public token wallet MetaMask. After the transaction, there is a contract is generated which has a hash of transaction present. So, this application has too much secure and transparent.

The Proposed Method

This research proposes a blockchain-based online examination system designed to enhance security, transparency, and student privacy while ensuring a robust and reliable assessment process.

Key Components:

- Student registration and login modules.
- Fee payment integration with MetaMask blockchain wallet.
- Secure question delivery and answer submission using smart contracts.
- Tamper-proof storage of examination data on blockchain

Process Flow:

1. Registration

Students register by providing personal details (name, course, gender, contact information), creating a password, and generating a unique blockchain account address.
Registration data is stored securely in a NoSQL database at the examination center.

2. Login and Fee Payment

Students log in using their registered email and password.
They initiate fee payment via the MetaMask Ethereum blockchain wallet.
Upon successful transaction, a unique transaction hash is generated and verified.

3. Examination

Students access the examination page and begin the test.
Questions are delivered securely through smart contracts, ensuring integrity and confidentiality.
Student answers are encrypted and stored locally.
Upon completion, a smart contract is created, containing student answers, transaction hash, and timestamp.
The smart contract is deployed to the Ethereum blockchain, guaranteeing immutability and transparency.

4. Evaluation and Results

Examiners retrieve student answers from the blockchain using the smart contract. Grading is performed manually or through automated mechanisms within the smart contract.
Results are stored on the blockchain and shared with students, ensuring authenticity and accessibility.
Benefits:Enhanced Security: Blockchain technology prevents unauthorized access, modification, or deletion of examination data.
Transparency: All transactions and actions are recorded on the blockchain, providing an auditable trail for verification and dispute resolution.
Student Privacy: Encryption and secure storage of answers protect student information and prevent unauthorized access.
Decentralization: Elimination of a central authority reduces the risk of data manipulation or corruption.
Immutability: Blockchain records cannot be retroactively altered, ensuring the integrity of examination results.
Future Research Directions:
Integration of Biometric Authentication: Further strengthen student identity verification and prevent cheating.
Exploration of Zero-Knowledge Proofs: Enhance student privacy by concealing sensitive information while maintaining verification capabilities.

Development of Scalability Solutions: Address the potential challenges of handling large-scale examinations on blockchain networks.
Establishment of Standards and Protocols: Ensure interoperability and security across blockchain-based examination systems.
Conclusion:

This proposed method demonstrates a promising approach to leveraging blockchain technology to address security, transparency, and privacy concerns in online examinations. Further research and development are crucial to fully realize its potential and establish blockchain-based examination systems as a secure and reliable alternative for educational assessment.

MOTIVATION

The Blockchain-based online examination systems are motivated by a desire to address several fundamental flaws plaguing traditional methods. These flaws include:
Security: Centralized servers are vulnerable to hacking and data breaches, potentially compromising sensitive student information and exam content. Blockchain's distributed ledger technology creates an immutable record of all transactions, preventing alterations and ensuring data integrity.
Transparency: Traditional systems lack transparency in question selection, exam scoring, and grade allocation, leading to potential bias and distrust. Blockchain enables full transparency, allowing students to verify every step of the process, building trust and fostering a fairer academic environment.
Efficiency: Paper-based and centralized online exams require significant resource allocation for printing, administration, and logistics. Blockchain streamlines the process, automating tasks, reducing costs, and increasing efficiency.
Plagiarism: Traditional systems struggle to effectively detect and prevent cheating. Blockchain can be programmed to identify suspicious patterns and flag potential plagiarism, upholding academic integrity.
Accessibility: Blockchain-based systems can operate independently of centralized authorities, potentially making examinations more accessible for remote students and those in areas with limited infrastructure.
Decentralization: Blockchain removes the reliance on single entities to control and oversee exams, preventing manipulation and promoting a more equitable system.Ultimately, the motivation for blockchain-based online examinations lies in the desire to create a more secure, transparent, efficient, and accessible platform for testing and assessment, fostering a fair and trustworthy environment for both students and institutions.
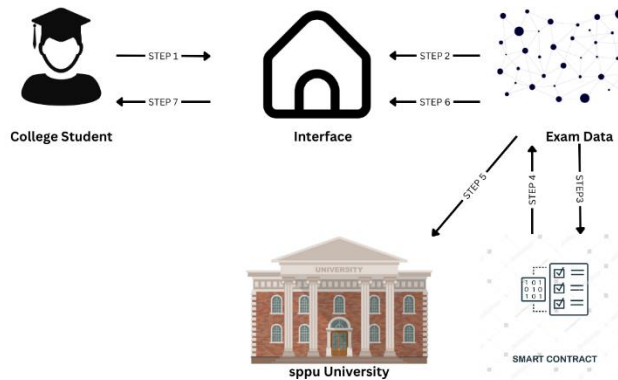
SYSTEM ARCHITECTURE

Fig -1: System Architecture Diagram

CONCLUSION

This research paper is to demonstrates the significant potential of blockchain technology to revolutionize online examinations in the education system. Our proposed system built on the Ethereum platform and utilizing smart contracts offers remarkable advantages over traditional cloud-based approaches. Through enhanced transparency, data security, and tamper-proof record-keeping, blockchain promotes trust and fairness in the assessment process. This study not only successfully implements smart contracts for online examinations but also paves the way for further exploration of decentralized applications in education. Future research can refine existing blockchain-based systems and delve deeper into areas like resource management and improved decision-making for academic institutions. The integration of blockchain technology holds immense promise for shaping a more secure, efficient, and accessible future for online education and examinations.

ACKNOWLEDGEMENT

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System | SatoshiNakamoto Institute," 2008.

[2] M. Walport, "Distributed ledger technology: Beyond block chain," Gov. Off. Sci., pp. 1–88, 2015.

[3] P. Devine, "Blockchain learning: can crypto-currency methods be appropriated to enhance online learning?," ALT Online Winter Conf., 2015.

[4] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," in Proceedings – International Conference on Computer Communications and Networks,ICCCN,2018,doi:10.1109/ICCCN.2018.8487348.

[5] P.Chinnasamy, P.Deepalakshmi, V. Praveena, K.Rajakumari,P.Hamsagayathri, (2019) "Blockchain Technology: A Step Towards Sustainable Development" International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-2S2

[6] R. Beck, J. Stenum Czepluch, N. Lollike, and S. Malone, "Blockchain -The gateway to trust-free cryptographic transactions," in 24th European Conference on Information Systems, ECIS 2016, 2016.

[7] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in Proceedings – 2016 IEEE Symposium on Security and Privacy, SP 2016, 2016, doi: 10.1109/SP.2016.55.

[8] "Node.js." https://nodejs.org/en/ (accessed May 20, 2020).

[9] "Index of /dist/npm/." https://nodejs.org/dist/npm/ (accessed May 20,2020).

[10] Y. Gu, X. Wang, S. Shen, J. Wang, and J. U. Kim, "Analysis of data storage mechanism in NoSQL database MongoDB," in 2015 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW 2015, 2015, doi: 10.1109/ICCE-TW.2015.7217036.

[11] "GitHub - ethereum/mist: [DEPRECATED] Mist. Browse and use Đapps on the Ethereum network." https://github.com/ethereum/mist(accessed Apr. 15, 2020).

[12] V. Buterin, "A next-generation smart contract and Decentralized application platform," Etherum, 2014.

[13] "Welcome to Remix documentation! — Remix, Ethereum-IDE1documentation."https://remix. ide.readthedocs.io/en/latest/ (accessedApr. 15, 2020).

[14] C. Dannen, Introducing Ethereum and Solidity. 2017.

[15] "MetaMask." https://metamask.io/ (accessed Apr. 20, 2020).

[16] B. Carter, "HTML Educational Node.js System (HENS): An Applied System for WEB Development," in Proceedings - 2014 Annual Global Online Conference on Information and Computer Technology, GOCICT 2014, May 2014, pp. 27–31, doi: 10.1109/GOCICT.2014.25.

[17] N. Chandra, A. Jain, V. Kumar, and A. K. Tripathi, "A deep investigation on blockchain network based on platforms and consensus algorithms," Int. J. Adv. Sci. Technol., 2020.

[18] "A Coin Marketplace Implementation on Blockchain Using the Hyperledger Platform," no. September, 2018. Authorized licensed