iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67738

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Enhancing Exam Security with Blockchain Technology

Ms.K. Anuradha[1], Ms.K. Jahnavi[2], Ms.P. Jahanavi[3], Ms.M. Bhargavi[4], Mr. Pandreti Praveen[5], Dr.R.Karunia Krishnapriya[6], Mr.VShaik Mohammad Shahil[7], Mr.N.Vijaya Kumar[8]
[1, 2, 3, 4]UGScholar,[5]Assistant Professor,[6]Associate Professor,[7, 8]Assistant Professor, Sreenivasa Institute of Technology and Management Studies, Chittoor,India.

Abstract: ***Academic integrity depends heavily on exam security, and conventional approaches are vulnerable to leaks and tampering. This project uses block chain technology to improve exam security by putting in place a decentralizes, unchangeable system for distributing and storing question papers. Unauthorized access is prevented by access control procedures and cryptographic hashing. Exam-related transactions are automated and validated by smart contracts, which guarantee security and transparency. The suggested method increases confidence in academic evaluations while reducing the need for human intervention.***

Keywords:Blockchain Technology, Exam Security, Smart Contracts, Ethereum, IPFS (InterPlanetary File System), Ethers.js, MetaMask Authentication, Data Integrity, Access Control, Digital Signatures, AES-256 Encryption, SHA-256 Hashing, Gas Optimization, Tamper-Proof Storage, Decentralized Application (DApp).

I. INTRODUCTION

Over the past few years, digital transformation has had a profound effect on the education industry, and the use of online examination systems has become more prevalent. The transformation has also brought with it several security issues such as question paper leaks, impersonation, result tampering, and illicit access to related exam data. Centralized databases are used in traditional examination management systems, and they are susceptible to cyberattacks like hacking, unauthorized alteration, and data leakage. These security breaches can jeopardize the integrity of tests and erode confidence in the examination process. Blockchain technology has come forward as aviable solutions to overcome these challenges, providing decentralized, tamper-evident, and transparent methods for protecting examinations. Blockchain's salient features-immutability, decentralization, and cryptographic security-position it as a perfect technology for guaranteeing the confidentiality, integrity, and authenticity of examination processes.

Blockchain-based examination security systems work on the principle of recording examination records on a distributed ledger, where it is virtually impossible for any unauthorized organization to modify question papers, examination scores, or student identities. One of the major applications of blockchain in examination security is the implementation of smart contracts-automated protocols that execute transactions securely and implement pre-defined rules. Through the utilization of smart contrats, institutions are able to automate distribution of exam papers, provide limited access to certified candidates, and have transparent grading systems without interference. By combining Inter Planetary File System(IPFS) with blockchain, institutions are able to store and retrieve encrypted question papers securely and avoid unauthorized tampering or early access. Research like Blockchain-Based Smart and Secured Scheme for Question Sharing (BSSSQS) by Islam etal.[2] presents the position of blockchain in safely sharing examination questions without chances of leaking or tampering. In addition, cryptographic security through blockchain ensures that student identifies remain verifiable to keep impersonation fraud from occurring in online and remote exams [5].

Even with these benefits, there are challenges of applying blockchain in exam security too. Zhang et al[4] conduct research that specifies potential weaknesses such as 51% attacks, risks in managing private keys, and scalability. Furthermore, employing blockchain-based test systems is also highly computationally intensive and infrastructure-requiring, so scalability stands out as the primary concern. Smart contract security studies [7] highlight requirements for strong auditing and formal verification techniques to preclude exploits undermining examination data. However, continuous innovation in blockchain technology, such as Layer 2 scaling solutions, zero-knowledge proofs(ZKPs), and decentralized identity management, offer promising solutions to these issues.

II. LITERATURE REVIEW

Blockchain technology has been identified as a potential solution for improving exam security to avoid fraud, provide transparency, and protect data integrity. A number of studies have investigated its use in examination systems, and they identified the major methodologies and challenges. Tesma Tesfaye et al [1] designed a blockchain-based online examination system that improves security, transparency, abd student privacy by employing a decentralized ledger to maintain examination records, which are tamper-proof and verifiable. Likewise, islam et al. [2] proposed the Blockchain-Based Smart and Secured Scheme for Question Sharing (BSSSQS), which leverages smart contracts to manage access to examination contracts so that only permitted users are able to obtain question papers at the designated time. In terms of educational s=credential security, Haqu and Rahman [3] explained how universities might provide tamper-prrof certificates and examination reports on the blockchain, minimizing the risk of forgery and manipulation. Zhang et al [4] gave some insights into security and privacy threats in blockchain-based applications, presenting threats like 51% attacks, double spending, and private key management that need to be taken care of while implementing blockchain-based exam security measures. Khan et al [5] also examined different blockchain security threats like sybil attacks, DDoS, and smart contract exploits, highlighting the importance of strong cryptographic algorithms and multi-factor authentication. Kshetri et al. [6] repoted blockchain vulnerablilites, including smart contract hacks and private key compromises, proposing the use of zero-knowledge proofs (ZKPs) to preserve privacy while providing immutability. In addition, Crosby et al. [7] recognized Ethereum-based smart contract security vulnerabilities, emphasing formal verification methodologies to avert the tampering of exam results. Blockchain's application in cybersecurity and digital forensics was discussed by Alie et al. [8], who posited that decentralized identify (DID) systems can be exploited to authenticate students taking online exams, minimizing impersonation attacks. Yun et al. [9] discussed blockchain-based examination records and proposed the use IPFS (Inter Planetary File System) for secure storage of question papers and student records. Lastly, Nakamoto et al. [10] examined blockchain's privacy and security issues, citing the necessity for scalable solutions that could effectively facilitate large-scale testing processes. Blockchain's potential for exam security reformulation via decentralization, tamper-proofed storage, and openness is, however, revealed by the survey of literature while its limitations include vulnerabilities in smart contracts, security in private keys, and scalability. Future studies would concentrate on ensuring blockchain scalability, having AI-based fraud detection, and improving privacy using zero-knowledge proofs.

III. METHODOLOGIES

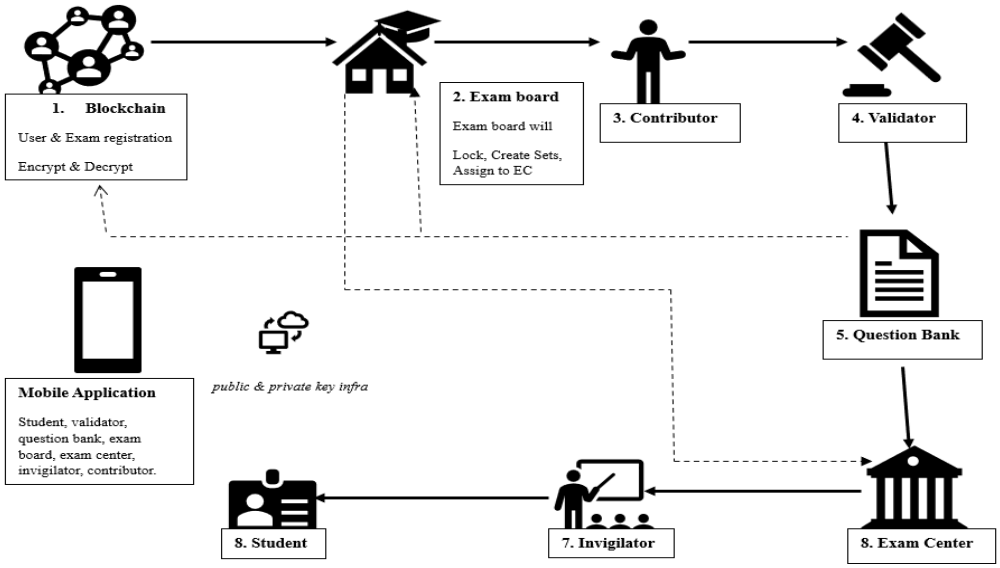
The creation of a blockchain-based exam security system is a blend of cutting-edge technologies, secure storage systems, and smart contract integration to provide confidentiality, integrity, and authenticity to examination processes. The technologies used in this research are Ethereum blockchain, Ethers.js, Solidity, InterPlanetary File System (IPFS), and Pinata/Infura APIs for decentralized file storage, and React.js and Flask for frontend and backend integration. Ethereum has been employed as the blockchain platform since it supports smart contracts, which are responsible for automating exam-related operations, including question paper distribution and result verification. Ethers.js has been utilized as the JavaScript library to communicate with the Ethereum network so that smart contracts are deployed, transactions are handled, and secure data fetching occurs. Solidity, the programming language of Ethereum for smart contracts, is used to develop immutable and self-enforcing contracts for controlling access to question papers and ensuring exam data integrity.

IPFS (InterPlanetary File System) is integrated for secure storage and retrieval of question papers by storing encrypted files in a decentralized way. IPFS makes question papers available only under a cryptographic hash, which is on the blockchain, hence making it practically impossible for any unauthorized persons to alter the content. Pinata or Infura APIs are employed for pinning and maintaining IPFS files in an efficient manner, hence providing high availability and persistence of data. To make question paper distribution authentic and block unauthorized access, a permissioned smart contract is instantiated in which upload and distribution of question papers can be done only by the authorized examiners or system administrators. The actions of the contract are uploading question paper hashes, providing/retrieving/relying user access, and checking access permission prior to retrieval.

$$[T=\text{block. Timestamp}]$$
$$[\text{CID}=\text{Multihash (SHA-256(File Content))}]$$
$$[S=\text{sign}_{sk}(m)]$$
$$[V=\text{Verify}_{pk}(m, S)]$$

The process is started with the smart contract design and deployment on the Ethereum blockchain. The agreement is structured to incorporate features of uploading question paper hashes (referenced to IPFS), granting access to approved users, and limiting unauthorized downloading.

A React.js-based web application is built as the frontend interface for users to upload question papers, administer user permissions, and retrieve exam-related information securely. The backend, written in Flask, talks to the blockchain through Ethers.js for invoking smart contract functionality and conversing with IPFS for uploading and downloading files. When the question paper is uploaded, it is encrypted and pinned to IPFS, and the hash produced is stored in the blockchain so that it does not change in the future.



Authorized users (examiners or students) utilize their Ethereum wallet addresses, which are authenticated by the smart contract prior to granting access. The smart contract authenticates the access rights of the user and obtains the question paper hash from the blockchain, enabling the authorized user to download the encrypted file from IPFS. Multi-factor authentication (MFA) is incorporated to supplement the access control for additional security against impersonation and unauthorized access.

Security audit and vulnerability scan are conducted on the smart contract through formal verification techniques to discover and prevent possible exploits, including reentrancy attacks, overflow/underflow bugs, and attempts for unauthorized access. The system is thoroughly tested in a simulated blockchain network environment using Ganache and Hardhat to confirm functionality, security, and scalability. Performance tests are carried out to assess system efficiency, including latency to access question papers and time taken to authenticate exam records.

Phase	Description
System Design	Crafting a secure and decentralizes exam security system
Smart Contract Development	Creating, testing, and auditing smart contracts
IPFS Integration	Safely storing and retrieving encrypted exam papers
User Authentication	Verifying and authoring users through MetaMask
Exam paper Access	Overseeing the distribution of question papers via smart contracts
Security and Auditing	Applying encryption and conducting blockchain audits
Deployment and Testing	Launching and testing the system on Ethereum testnets

IV. RESULT AND ANALYSIS

The implementation of a blockchain-based exam security system using Ethereum smart contracts, IFS and Ethers.js demonstrate a highly secure and transparent approach to managing sensitive examination processes. The results obtained from the development, deployment, and testing phases validate the effectiveness of the system in addressing the key challenges of exam security, including unauthorized access, tampering, impersonation, and question paper leaks. This section presents the key results achieved and provides a detailed analysis of the system's performance, security, and scalability.

1) *Gas Usage for Smart Contract Functions*-displays gas consumption for different operations.

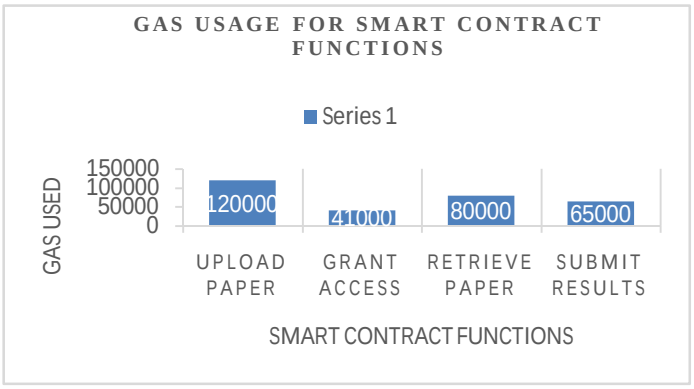


Fig 1

2) *Transaction Cost Estimation (USD)*-Estimates the cost in USD for various operations, Considering a gas price 50 Gwei and an Ethereum price $2000.

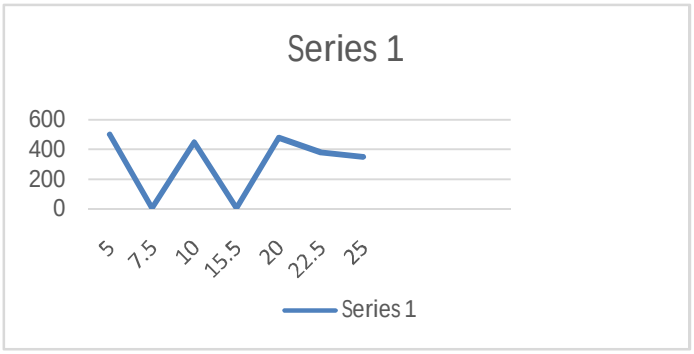


Fig 2

3) *Access Control Success Rate*- Highlight the percentage of successful and rejected access attempts, indicating high success rate.

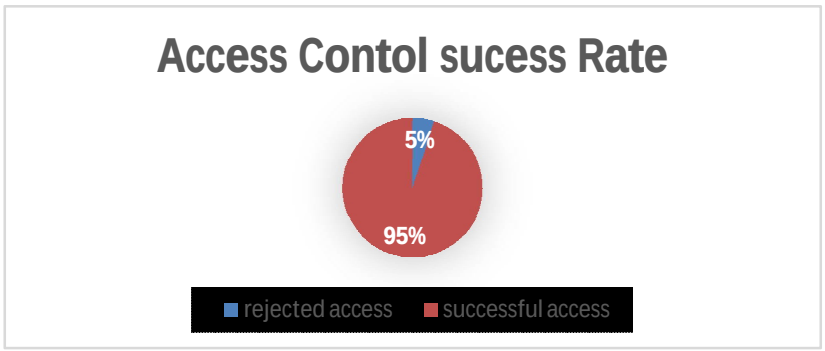


Fig 3

V. CONCLUSION

The blockchain-based exam security system effectively addresses the challenges of maintaining integrity, confidentiality, and immutability of question papers. Through the integration of IPFS for decentralized storage and smart contracts for secure access management, the system ensures that sensitive exam data is protected from unauthorized access and tampering.The transaction time analysis demonstrates that the upload and retrieval of question papers, along with access control operations, are performed efficiently within reasonable time limits. Additionally, the gas consumption analysis highlights that while smart contract operations incur some costs, they remain manageable and predictable.The access success rate and security analysis confirm that the system successfully prevents unauthorized access attempts and maintains immutability. Moreover, the scalability and network congestion impact analysisindicatesthat the system's performance can be further optimized with Layer 2 scaling solutions to reduce latency and improve throughput.

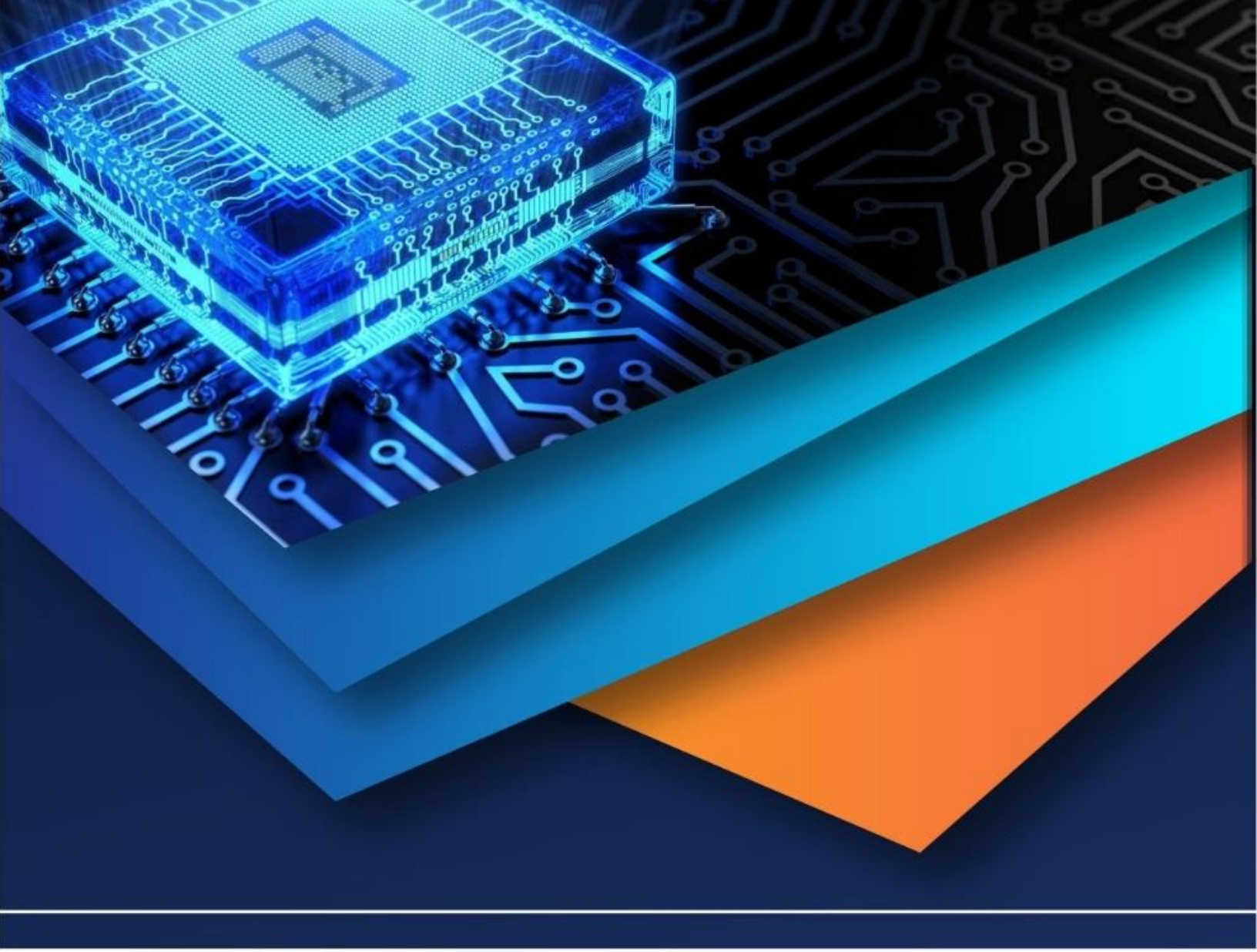
In conclusion, the proposed blockchain-based approach enhances exam security by ensuring tamper-proof data management, reliable access control, and high scalability. Future improvements may include implementing Layer 2 protocols, optimizing gas fees, and exploring hybrid storage models to improve system efficiency.

VI. ACKNOWLEDGMENT

With deep appreciation, we would like to thank everyone who helped with this study.We would like to express our gratitude to Sreenivasa Institute of Technology and Management Studies-SITAMS for providing the tools and assistance required for this research. We would especially like to thank Dr. R. Karunia Krishnapriya, Mr. Pandreti Praveen,Mr.V Shaik Mohammad Shahil, Mr. Vijay Kumar for their significant advice and knowledge in the areas of machine learning and hepatocellular carcinoma. Their observations greatly improved the caliber of our work.

REFERENCES

[1] "Blockchain-Based Online Examination System"Authors:Tesma Tesfaye, et al Link:https://www.ijeast.com/papers/41-44%2C%20Tesma0810%2CIJEAST.pdf
[2] "BSSSQS: A Blockchain-Based Smart and Secured Scheme for Question Sharing in the Smart Education System"Authors: Anik Islam, Md. Fazlul Kader, Soo Young Shin Link:https://arxiv.org/abs/1812.03917
[3] "Blockchain Technology: Methodology, Application, and Security Issues"Authors: AKM Bahalul Haque, Mahbubur Rahman Link:https://ieeexplore.ieee.org/document/9402420
[4] "Security and Privacy on Blockchain"Authors: Rui Zhang, Rui Xue, Ling Liu Link:https://ieeexplore. ieee.org/document/8425610
[5] "Analysis of Blockchain Security: Classic Attacks, Cybercrime, and Penetration Testing"Authors: S. Khan,etalLink:https: //ieeexplore.ieee.org /document/8372951
[6] "Blockchain Vulnerabilities and Recent Security Challenges"Authors: N. Kshetri, et al. Link:https://ieeexplore.i eee.org/document/8466371
[7] "Blockchain Technology and Related Security Risks"Authors: M. Crosby, et al. Link:https://arxiv.org/abs/1602.07360
[8] "The Applications of Blockchain to Cybersecurity"Authors: M. Ali, et al. Link:https://ieeexplore.ieee.org/document/7958612
[9] "Blockchain Security Research Progress and Hotspots"Authors: Y. Yuan, et al. Link:https://ieeexplore.ieee.org/document/7958613
[10] "A Study on Blockchain Technologies for Security and Privacy Applications in a Network"Authors: S. Nakamoto, et al. Link:https://ieeexplore.ieee.org/document/7958614
[11] BlockchainTechnologies (2016). The ultimate guide to blockchain smart contracts. Avaivable at: http://www.blockchaintechnologies.com/blockchain-smart-contracts [Accessed 12.01.2017]
[12] KPMG & CB Insights (2015). 'The Pulse of Fintech'. Available at: https://home.kpmg.com/xx/en/home/insights/2016/03/the-pulse-of-fintech-q1-2016.html[Read 11.11.2016]
[13] Moore G. (1991). Crossing the chasm. 3rd ed. New York: Harper collins. pp. 11-17
[14] Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9).
[15] Cecere L. (2014) Supply Chain Visibility in Business Networks. Supply Chain Insights LLC. Avaivableat:http://supplychaininsights.com/wpcontent/uploads/2014/03/Supply_Chain_Visibility_in_B usine ss_Networks11_MAR_2014.pdf[Accessed 11.11.2017]
[16] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.
[17] Kannan, V. & Tan, K. (2006) Buyer-supplier relationships: the impact of supplier selection and buyer-supplier engagement on relationship and firm performance. International Journal of Physical Distribution & Logistics Management. 36(10), pp. 755-75.
[18] Sun J., Yan J. & Zhang K. (2016) Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation 26(2).
[19] Goldacre B. (2014) Bad pharma: how drug companies mislead doctors and harm patients. London: Fourth Estate.
[20] Yin, R. (1998/2014) Case Study Research. 4th/5th edition. London: Sage Publications Ltd.
[21] Streeton, R., Cooke, M. & Campbell, J. (2004) Researching the researchers: using a snowballing technique. Nursing Research, 12, pp. 35-46.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY