Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.2, May : 2024

BLOCKCHAIN BASED E-COMMERCE ONLINE APPLICATION

Mrs.G.Jyothi, Assistant Professor, Department of Information Technology, Vignan's Institute of Information Technology(A), Visakhapatnam-530049.
Ms.Vinusha Chiluvuri, MCA Student, Department of Master of Computer Applications, Vignan's Institute of Information Technology(A), Visakhapatnam-530049.

ABSTRACT:
All client and product information is stored and controlled on a single, centralized server in the current configuration of the e-commerce application.This does, however, come with a risk: services become unavailable to other users in the event that the server crashes from an excessive number of requests or is hacked. I am converting the e-commerce platform to Blockchain technology in order to address this difficulty. This change entails spreading data around several servers or nodes so that users can still access data from other nodes that are still up and running in the event of a node failure. Moreover, Blockchain provides data immutability—the inability of unauthorized users to alter the data—and data encryption. Every piece of information is regarded as a block or transaction, and the storage of every block is identified by a distinct hash code.

Keywords:
E-Commerce Application, Centralized Server, Server Crash, Overwhelming Requests, Hacking, Transition, Blockchain Technology, Distributed Data, Data Retrieval, Data Encryption, Immutability, Unauthorized Access, Transactions, Hash Code, Data Validation.

INTRODUCTION :

E-Commerce, this sector depends on large amounts of power and storage to handle massive volumes of data and services. Even though it's already effective, blockchain technology can make improvements possible.

Blockchain technology has emerged as a potential answer to these problems. The world's leading E-commerce sector depends on significant processing and storage capacity to handle enormous volumes of data and services. Although it is already effective, blockchain technology can make it much better. Blockchain provides better data management through a secure network that organizes information about users, products, orders, deliveries, manufacturers, and sellers. The e-commerce industry benefits from its well-known security features, which simplify transactions and lower the need for middlemen.The organization of user, product, order, delivery, manufacturer, and seller data within a secure network is how blockchain improves data management. By simplifying transactions and lowering the need for middlemen, its well-known security features support the e-commerce industry. Enhanced advantages encompass accelerated transactions, reduced chargeback fraudulent activity, validated client testimonials, and customized product portfolios. Customers may track their orders in real time and verify the legitimacy of products thanks to blockchain's traceability.

LITERATURE SURVEY

The project's main goals are to construct a Security and transcation in blockchain. We have cited a few previously published publications and the contributions of other experts in this subject in support of this. Blockchain technology, a cutting-edge storage system is the major topics of our literature review. Our first paper was presented by Zibin Zheng , ShaoanXie, Hong-Ning Dai. An Overview of Blockchain Technology[1], the title of our paper offers an extensive exploration of blockchain, elucidating key concepts including "smart contracts." Within the blockchain, data hashes are stored in preceding blocks, forming a continuous chain of nodes. Any alteration to the data results in a change in its hash, which no longer corresponds with the previous block's hash, serving as an indicator of tampering.

Decentralization stands out as a disruptive attribute of blockchain technology. Transactions occur within applications installed on individuals' devices, eliminating the need for central institutions or servers. Verification, accounting, storage, maintenance, and data transmission within the blockchain rely on a distributed system. This approach not only conserves resources and streamlines transactions but also mitigates the potential for control by centralized entities. Blockchain technology employs a timestamped structure to store data, introducing a time element that enhances security and traceability.
The second paper was titled as smart contract and Ethereum[2], presented by Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen. Smart contracts are coded instructions designed to enforce predefined rules, facilitating the Transfer of digital assets within the blockchain. These contracts are invoked by external applications to execute various transactions. In blockchain-based asset transactions governed by smart contracts, the code autonomously triggers to finalize the specific transaction between involved parties. This code constitutes the smart contract itself.Utilizing Ethereum as the platform, developers have the capability to craft their own blockchain applications. Ethereum is a decentralized open-source blockchain that incorporates smart contract capabilities. It serves as a prime illustration of blockchain technology and operates as a cryptocurrency system, widely recognized as the second most valuable digital currency after bitcoin.
The third paper was titled as "blockipfs (Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability)[3]" which shed light on integrating IPFS with Blockchain. It compared traditional IPFS with Blockchain-enabled IPFS, showing that blockipfs outperformed in various categories like upload, read, and download transactions.

CONCLUSION:

Blockchain-based e-commerce online platform provides substantial benefits in terms of security, transparency, and trust. This platform lowers the risk of fraud by using blockchain technology to guarantee transactions are tamper-proof and unchangeable. Furthermore, smart contracts provide safe and automated payment procedures, which increase productivity. But as technology advances, it's critical to take consumer acceptance and scalability issues into account. All things considered, blockchain-based e-commerce has a lot of potential to completely transform online buying, but its effective adoption in the always shifting digital environment will depend on smart planning and adaptability.

REFERENCES:

[1] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.
[2] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.
[3] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.
[4] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain
[[5] K. Chatterjee and A.De "A Novel Multi-Server Authentication Scheme for E-commerce Applications Using Smart Card", Wireless Personal Communication, vol. 91, no.1, pp.293-312, 2016
[6] E. Alomari, S. Manickam, B. B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art", International Journal of Computer Applications, vol. 49, no. 7, 2012 .
[7] P. Francesco, S. Ricciardi, and U. Fiore, "Evaluating network-based DoS attacks under the energy consumption perspective: new security issues in the coming green ICT area", IEEE International

Conference on Broadband and Wireless Computing,Communication and Application pp.374-379, 2011.
[8] Y. Yanli, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Journal of Network and Computer Applications, vol. 35, no. 3, pp. 867-880, 2012.
[9] B. David, S. Sezer, and J. McCanny, "New sensing technique for detecting application layer DDoS attacks targeting back-end database resources", IEEE ICC Communication and Information Systems Security Symposium, pp. 1-7, 2017.
[10] K. C. Abdelaziz, N. Lagraa, C. T. Calafate, and A. Lakas, "TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs", Vehicular Communications, vol. 9, pp. 254-267, 2017.
[11] Roy, K.; Islam, N.; Khan, T.; Khan, M.M. A novel approach to data storage using blockchain technology. In Proceedings of the 2019 International Conference on Information Technology (ICIT), Shanghai, China, 20–23 December 2019; pp. 245–250.
[12] Taherdoost, H.; Madanchian, M. Blockchain-Based New Business Models: A Systematic Review. *Electronics* 2023, *12*, 1479.
[13] Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
[14] Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* 2018, *82*, 395–411.
[15] Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *Ieee Access* 2016, *4*, 2292–2303.
[16] Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* 2014, *3*, 1–36.