

Blockchain and Smart Contracts in a Decentralized Health Infrastructure

Dr. Aniruddha S. Rumale, Gaurav Kolte, Gita Mutadak, Sanket Baviskar, Devashish Baviskar

Department of Information Technology

Sandip Institute of Technology and Research centre Nashik, India

Abstract: *The blockchain typically described as a decentralized system in which transactional or ancient statistics are recorded, stored, and maintained throughout a peer-to-peer community of personal computers referred to as nodes. Counterfeit drugs are one consequence of such limitations within existing supply chains, which not only has serious adverse impact on human health but also causes severe economic loss to the healthcare industry. Blockchain technology has gained tremendous attention, with an escalating hobby in a plethora of several applications like safe and relaxed healthcare records management. Similarly, blockchain is reforming the traditional healthcare practices to an extra reliable means, in phrases of powerful prognosis and treatment through safe and cosy facts sharing using SHA Hash Generation Algorithm. Within the future, blockchain will be an era that can probably assist in personalized, authentic, and at ease healthcare by means of merging the entire actual-time scientific information of a patient's fitness and offering it in an up-to-date cosy healthcare setup. In this paper, we evaluation each the present- and modern-day trends inside the subject of healthcare with the aid of imposing blockchain as a model. We also talk the packages of blockchain, at the side of the demanding situations confronted and destiny views. The proposed system executed blockchain implementation in distributed computing surroundings and it gives the automated restoration of invalid chain by using Consensus and Mining Algorithm. In this system, we present a Custom blockchain-based approach leveraging smart contracts and decentralized off-chain storage for efficient product traceability in the healthcare supply chain. The smart contract guarantees data provenance, eliminates the need for intermediaries and provides a secure, immutable history of transactions to all stakeholders. We present the system architecture and detailed algorithms that govern the working principles of our proposed solution. We perform testing and validation, and present cost and security analysis of the system to evaluate its effectiveness to enhance trace-ability within pharmaceutical supply chains.*

Keywords: Blockchain Technology, Decentralization / Decentralized System, Distributed Computing, Peer-to-Peer Network, Healthcare, Supply chains, etc

REFERENCES

- [1] L. Guo, C. Zhang, J. Sun, Y. Fang. "A privacy-preserving attribute based authentication System for Mobile Health Networks," IEEE Transactions on Mobile Computing, 2014, vol. 13, no. 9, pp. 1927- 1941.
- [2] A. Abbas, S. Khan, "A review on the state-of-the-art privacy preserving approaches in e-health clouds," IEEE Journal of Biomedical Health Informatics, 2014, vol. 18, pp. 1431-1441.
- [3] J. Yang, J. Li, Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, 2015, vol. 43-44, pp. 74-86.
- [4] <http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/>.
- [5] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS'06), pp. 89-98, 2006.
- [6] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-based encryption with nonmonotonic access structures," in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195-203.
- [7] J. Han, W. Susilo, Y. Mu. "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption," IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 3, 665-678

- [8] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou. "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE transactions on parallel and distributed systems, 2013, 24(1): 131-143.
- [9] M. Green, S. Hohenberger, B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.
- [10] J. Lai, R. H. Deng, C. Guan, J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.
- [11] B. Qin, R. H. Deng, S. Liu, S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1384-1394, JULY. 2015
- [12] Spvryan's International Journal of Engineering Sciences & Technology (SEST) ISSN : 2394-0905 "Design of a Cloud Based Emergency Healthcare Service Model"