Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVII, Issue I, Jan-June 2023

A STUDY OF BLOCKCHAIN BASED SOLUTION FOR KYC VERIFICATION

Anima Sharma[1], Dr. Manju Vyas[2], Deepika Bansal[3] and Mr. Gajendar Sharma[4]

Department of AI&DS[1,2] Department of IT[3], Department of CSE[4], JECRC, Jaipur, Inida.

ABSTRACT

In the today's world of digitization, it's very important to identify the individual, in order to prevent the fake transaction, like sim card issue, bank loan disbursement and more. We need to go through KYC verification in banks and other related organization for updating our data and verifying our identity. Blockchain permits the secure transfer of KYC verification stamp from one entity to another. It offers a highly immutable and detailed audit trail on all actions on KYC files. The problem which the digitization is the duplicity, that single platform is not used by the organizations banking or other for the purpose of KYC of customer, so the blockchain based platform act as a single solution for the KYC related needs or requirement. This paper summarizes and analyses the related work which is applied in the field and further proposes an algorithm which uses a 2 step process for the implementation of digitization of the process.

Keywords— Blockchain, KYC, SHA-1, SHA-2

[1] INTRODUCTION

To open an account, banks need to identify and verify the client's identity against a regulatory or government standard for anti-money laundering. Banks may close new accounts and halt business relationships with clients who do not meet strict KYC requirements. Current KYC procedures take the form of ensuring the customers are real, then assessing and monitoring risks.

The process of selecting a new customer can be difficult. However, KYC processes are useful in preventing and identifying money laundering, terrorism financing, and other illegal corrupt schemes. Certain verification steps such as ID card verification, face verification, proof of address like utility bills, and biometric verification must be completed for the customer to be accepted. Banks need to follow laws and regulations to prevent fraud, in particular KYC regulations. Banks

are responsible for compliance. Penalties can be applied if they don't comply to the rules set by the law.

Banks need to follow laws and regulations to prevent fraud, in particular KYC regulations. Banks are responsible for compliance. Penalties can be applied if they don't comply with the rules set by the law.

The United States, Europe, the Middle East and the Asia Pacific have recently been penalized with USD 26 billion in fines for non-compliance with AML, KYC and sanctions.

KYC is conducted through a reliable and inquisitive third party to assure that each client has the proper credentials to ensure identity and address. KYC verification in India can be done electronically with eKYC through Aadhaar authentication which ensures the customer's legitmacy. eKYC is the synchronizing of two ID data sources. Examples include using a physical ID in combination with a digital ID, or capturing information from IDs and digitally extracting it. if the concept of blockchain based KYC is proposed then a single platform can act as the source for all KYC relevant queries and data requirements.

[2] CONCEPT AND ADVANTAGE OF BLOCKCHAIN

Blockchain technology is a decentralized, distributed ledger that cannot be modified, which makes it the perfect solution for industries like healthcare and cyber security. Blockchain technology uses a digital ledger to record transactional records called the 'block.' This is stored across different databases called 'chain' in a network that relies on peer-to-peer nodes.

The ledger is authorized by the digital signature of the owner, ensuring the information it contains remains secure. Basically, the digital ledger is a Google spreadsheet shared among many computers in a network. Transactions are stored based on actual purchases. The interesting angle is that anyone can see the data, but they can't corrupt it.

Blockchain excludes unauthorized changes by appending a timestamp to each new block. Blockchain is the foundation for immutable ledgers.

[3] RELATED WORK

Bandara, E., Liang, X., Foytik, P., Shetty, S., & Zoysa, K. D. (2021) The vast majority of current identity systems are based on centralized storage systems. Because a variety of attacks and data breaches can occur, storing identity data on centralized storage platforms like cloud storage or central servers becomes a major privacy concern. With this examination, we are proposing blockchain and self-sovereign personality based computerized character (KYC - Know Your Client) stage "Casper" to resolve the issues on concentrated character frameworks. " Casper is a mobile identity wallet app for Android and iOS that uses a self-sovereign identity-based approach and incorporates blockchain technology. Customers' actual identities are stored in the mobile wallet application, in contrast to centralized identity systems. The evidence of these personalities is put away in the blockchain-based decentralized capacity as a self-sovereign

character verification. The Self-Sovereign Identity (SSI)-based system of Casper platforms features a Zero Knowledge Proof (ZKP) method for confirming identity details. The Casper platform can be used in a variety of fields, including banking, healthcare, and government, among others. We have talked about using the Casper platform to create a digital identity wallet for banking customers as a use case. Casper uses a blockchain and SSI-based approach to provide a secure, decentralized, and ZKP-verifiable identity. It addresses common issues with centralized and cloud-based identity system platforms, such as centralized control, data immutability, and traceability.

Chen, R., Shu, F., Huang, S., Huang, L., Liu, H., Liu, J., & Lei, K. (2021). The importance of reliable identity management and authentication has been suggested for network security. Decentralised identity management has drawn a lot of attention in academics and business recently as traditional centralised identity management systems struggle with scalability and security issues. The administration and authentication of decentralised identities, however, have increased the requirements for cross-domain trust and faced numerous implementation issues as a result of the growing sharing and interaction between each domain. We suggest BIdM, a decentralised cross-domain identity management system built on blockchain, to address these issues. We develop a consortia blockchain-based decentralised identification (DID) for naming identities. The proposed DID can be signed and issued without the involvement of a central authentication node because the identity subject has complete control over the proposed DID's life cycle and ownership.Da Silva Rodrigues, C. K., & Rocha, V. (2021) , This article analyzes the effectiveness of deploying the Blockchain technology in the implementation of the IoT ecosystem database. To this end, we assess the processing efficiency of transactions originated by smart devices and the storeddata integrity. The processing-efficiency evaluation is carried out through queue-theory-based analytical modeling, in which the average time for transaction confirmation is estimated. By its turn, the data-integrity is measured through simulations, where the probability of fraudsters altering already-stored data is estimated. Moreover, the experiments consider a set of scenarios related to different application domains. Final results show that the Blockchain technology may meet IoT efficiency requirements, besides providing adequate data integrity. Lastly, general conclusions and avenues for further research close this article.

Goud Allam, T., Mehedi Hasan, A. B. M., Maag, A., & Prasad, P. W. C. (2021) proposed that in order to improve strength and store information utilising digital storage techniques, distributed ledger technology excludes third party providers from the transaction system. For secure financial transactions, we incorporate distributed ledger technology and Blockchain in this research study. Information is transferred safely using this technique, which also addresses other problems. It includes an additional inquiry procedure in a clever logistical setting to improve the system as a whole. This research report outlines the processes it took to create an infrastructure with four key components. Input, analysis, evolution, and output are these. Peer-to-peer networking techniques should be used in digital currency modules. It facilitates more secure and stable money transfers between accounts. Researchers also offer here bitcoin strategies for the global market.

Liang, W., Zhang, D., Lei, X., Tang, M., Li, K.-C., & Zomaya, A. Y. (2021). Blockchain technology is widely used in a number of digital transaction fields, including e-government affairs and financial transaction security, thanks to its rapid development. For circuit copyright protection, we propose a Blockchain based on homomorphic encryption that effectively addresses the issues of low private data security, inefficient transaction data storage, cooperation, and supervision in circuit copyright transactions. Utilizing Blockchain and intelligent contract, we first construct a mathematical model based on homomorphic encryption. Then, we design the algorithms for generation of Blockchain, homomorphic chain encryption/decryption, and intelligent contract. A fully homomorphic encryption-based identity authentication protocol is used for Blockchain because it ensures the change operation of any third-party in Blockchain and achieves real-time verification. The intelligent contract is successfully executed in Blockchain. Due to the use of distributed identity authentication and real-time extensible storage, the system makes blockchain-based circuit copyright protection more secure and adaptable, making it suitable for use in a blockchain network. The exploratory outcomes show that the proposed calculation has decreased the transmission cost and worked on the proficiency of information stockpiling and oversight. Moreover, it is strong to a few normal assaults (e.g., twofold spending assaults), yet causes minimal expense/above and has a more elevated level of safety when contrasted with three other contending calculations.

Qu, Y., Pokhrel, S. R., Garg, S., Gao, L., & Xiang, Y. (2021). Specifically said that Industry 4.0 automation is gradually thriving thanks to cognitive computing, a ground-breaking AI approach that emulates the human brain's thinking process. Data-driven intelligent manufacturing and better decision making have already evolved as a result of the development of various AI and machine learning technologies. The poisoning assaults, performance, insufficient data resources, etc. are only a few of the new challenges that need to be addressed. Recent research studies looked at the issue superficially, which frequently results in inconsistent performance, waste, and privacy leaks. In this paper, we built a federated learning and blockchain-based decentralised paradigm for big data-driven cognitive computing (D2C). With privacy protection and effective processing, federated learning can address the "data island" problem, while blockchain offers an incentive structure that is totally decentralised.

Subramanian, G., & Thampy, A. S. (2021) , discussed that approximately 45 percent of the global carbon dioxide (CO2) emissions come from automobiles, buses, taxis, and motorcycles. Electric vehicle could be the significant supporter of contract the contamination level in a transportation area. The Forbes report predicts that worldwide demand for passenger electric vehicles will reach 15% in 2025 and 23% in 2030. A blockchain-based solution for the pre-owned electric vehicle market is presented in this study. It has the potential to foster trust, transparency, immutable records, and an effective method for tracking the entire life cycle of a futuristic electric vehicle supply chain. At present the majority of the used electric movement buy unfolds through the outsider facilities, sites, and portable applications. This does not provide accurate information regarding the driver's performance, the history of the electric conveyance, the battery's charging capabilities, the history of the charging records, or the electric conveyance's history (wear and tear

affects battery life). The implementation of our solution made use of hybrid blockchain technology. To keep track of the vehicle records as a distributed ledger, each stakeholder is given an Ethereum blockchain address. This plan considered electric vehicle maker, charging station, battery producer, street convey authority as significant partners. Smart contract made with Solidity software. The truffle platform was used to implement highly intelligent contracts in a private blockchain to guarantee electric vehicle owners' privacy and other stakeholders'. In a public blockchain, a mobile application called Meta Mask used the Kovan network to track vehicles. For each transaction, this application tested with 0.1 Ether. The Blockchain Electric Vehicle Cloud of Things (BEVCoT) idea called for the IoT-Blockchain application to be integrated into a cloud environment.

Ullah, N., Al-Dhlan, K. A., & Al-Rahmi, W. M. (2021) We talked about how the Know Your Customer (KYC) procedure is expensive and insecure in financial institutions. The future of financial institutions will depend on the acceptance of disruptive technology. For KYC optimisation, this study suggested a Hyperledger Fabric network. Using the Hyperledger Composer, the suggested system's performance was evaluated. The experiment results show that the proposed system can speed up KYC clearing transfers thanks to the robust and identity features of Hyperledger Fabric, challenge inefficiencies resulting from the repetition of similar tasks, secure data sharing, be cost-effective, and ultimately bring transparency to the existing KYC system.

Vangala, A., Sutrala, A. K., Das, A. K., & Jo, M. (2021), discovered that farmers and other smart farming users can access agricultural data on a single, integrated platform using a blockchain-based smart farming technology. In addition, the transparency, anonymity, and traceability that are simultaneously added by the persistence and auditability of the data that is stored in blocks into the blockchain provide assurance that the appropriate data will be utilized in the future. A new smart contract-based blockchain-envisioned authenticated key agreement mechanism in a smart farming environment is designed in this article to achieve this objective. Both the device-to-device (D2D) and the device-to-gateway (D2G) authentication phases facilitate mutual authentication and key agreement between two Internet of Things (IoT)-enabled devices and between an IoT device and the network's gateway node (GWN). The authenticated data of IoT devices received from the GWNs is used by the edge servers to create the blocks, which are then sent to the cloud server (CS). A peer-to-peer (P2P) CSs network is able to verify and add the formed blocks thanks to the smart contract-based consensus mechanism. The security of the proposed conspire is finished through formal and casual security examination, and furthermore utilizing the proper security confirmation instrument. A definite relative review uncovers that the proposed plot offers unrivaled security and greater usefulness highlights when contrasted with existing contending verification conventions. At last, the blockchain-based reenactment has been directed to quantify computational time for a changed number of mined blocks and furthermore a differed number of exchanges per block.

Wang, X., Qiu, W., Zeng, L., Wang, H., Yao, Y., & He, D. (2021) explained how the market-oriented structure of distributed renewable energy and the distributed network structure of blockchain are similar. Blockchain technology may be used to balance the operation of microgrids,

access to distributed power generating systems, and wholesale market operation by synchronising the real-time pricing of grid services with real-time phasor control systems. Digital assets with varying values are transported through regionally designed distributed shared energy networks. The existing energy interconnection network urgently needs to figure out how to implement the reliable interchange of energy digital assets between regions. The blockchain is now the subject of several studies on cross-chain asset exchange techniques, including hash time lock, notary, side chain, and others. These asset exchange techniques, however, are ineffective and lack sufficient oversight (KYC&AML).

[4] ALGORITHMS USED IN LITERATURE

- **SHA-512** The National Institute of Standards and Technology and the National Security Agency collaborated on the development of the Secure Hash Algorithm (SHA), which is based on the MD4 (Message Digest) algorithm developed by Ronald L. Rivest of the MIT. SHA-0, SHA-1, and SHA-2 are the three distinct SHA algorithms that define it.

In 1995, NIST published SHA-1 under the name FIPS PUB 180-1. furthermore, was viewed as a cryptographically solid one-way hash calculation and utilized in numerous applications including TLS and SSL ("https://"), SSH, PGP, Git, Irregular, Droning, and so forth. until hypothetical shortcomings were seen as in 2005.

While to some degree up-to 2015 no real SHA-1 crash had been freely recognized, in 2006, NIST and different associations deplored the utilization of SHA-1. They say that people should switch from SHA-1 to a hash function that doesn't have those theoretical flaws, like SHA-2 or SHA-3.

- **Testing and Validation:** The blockchain created in the process for the voter identity and for the vote casted can be validated on the various entropy based validation platforms for testing the strength of blockchain and other applications for validating blockchains can be used.

V. CONCLUSION & FUTURE WORK

The paper studies the related work for providing a **One Place KYC Solution using Blockchain**and analyzes the suggested platformsfor the secure concept of KYC documents storage. Banking, Financial Organizations, Network Based Companies, Employee Companies often needs the KYC documents for the verification of the customer or employees. In such a digital age it is useless to maintain the multiple copies for single person , in bank ,in financial institution and it also create the ambiguity and as well as wastage or time and resources So the related work in KYC System proposes two segments one is the document uploading and other is document verification.

Further the future work proposes an algorithm to study the current research, reviews and analyze them in the view of the security related improvements using the blockchain technology. And to design the secure and more efficient platform for KYC document sharing using

Blockchain. Further, to examine the security based performance , a comparing of the proposed work will be made with the other models available or proposed by other researchers.

REFERENCES

[1] Bandara, E., Liang, X., Foytik, P., Shetty, S., & Zoysa, K. D. (2021). A blockchain and self-sovereign identity empowered digital identity platform. *2021 International Conference on Computer Communications and Networks (ICCCN)*, 1–7.

[2] Chen, R., Shu, F., Huang, S., Huang, L., Liu, H., Liu, J., & Lei, K. (2021). BIdM: A blockchain-enabled cross-domain identity management system. *Journal of Communications and Information Networks*, *6*(1), 44–58.

[3] Da Silva Rodrigues, C. K., & Rocha, V. (2021). Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions. *IEEE Latin America Transactions*, *19*(7), 1199–1206. https://doi.org/10.1109/tla.2021.9461849

[4] Goud Allam, T., Mehedi Hasan, A. B. M., Maag, A., & Prasad, P. W. C. (2021). Ledger technology of blockchain and its impact on operational performance of banks: A review. *2021 6th International Conference on Innovative Technology in Intelligent System and Industrial Applications (CITISIA)*, 1–10.

[5] Liang, W., Zhang, D., Lei, X., Tang, M., Li, K.-C., & Zomaya, A. Y. (2021). Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection. *IEEE Transactions on Emerging Topics in Computing*, *9*(3), 1410–1420.

[6] Qu, Y., Pokhrel, S. R., Garg, S., Gao, L., & Xiang, Y. (2021). A blockchained federated learning framework for cognitive computing in industry 4.0 networks. *IEEE Transactions on Industrial Informatics*, *17*(4), 2964–2973.

[7] Subramanian, G., & Thampy, A. S. (2021). Implementation of hybrid blockchain in a pre-owned electric vehicle supply chain. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 82435–82454. https://doi.org/10.1109/access.2021.3084942

[8] Ullah, N., Al-Dhlan, K. A., & Al-Rahmi, W. M. (2021). KYC Optimization by Blockchain Based Hyperledger Fabric Network. *2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)*, 1294–1299.

[9] Vangala, A., Sutrala, A. K., Das, A. K., & Jo, M. (2021). Smart contract-based blockchain-envisioned authentication scheme for smart farming. *IEEE Internet of Things Journal*, *8*(13), 10792–10806. https://doi.org/10.1109/jiot.2021.3050676

[10] Wang, X., Qiu, W., Zeng, L., Wang, H., Yao, Y., & He, D. (2021). A credible transfer method of cross-chain assets based on DID and VC. *2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, 238–242.

[11] Alex M. Goh and Xiaoyu L. Yann, (2021), "A Novel Sentiments Analysis Model Using Perceptron Classifier" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 4, pp. 01-10, DOI 10.30696/IJEEA.IX.IV.2021.01-10.

[12] Dolly Daga, Haribrat Saikia, Sandipan Bhattacharjee and Bhaskar Saha, (2021), "A Conceptual Design Approach For Women Safety Through Better Communication Design" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 3, pp. 01-11, DOI 10.30696/IJEEA.IX.III.2021.01-11

[13]. Alex M. Goh and Xiaoyu L. Yann, (2021), "Food-image Classification Using Neural Network Model" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 3, pp. 12-22, DOI 10.30696/IJEEA.IX.III.2021.12-22

[14]. Jeevan Kumar, Rajesh Kumar Tiwari and Vijay Pandey, (2021), "Blood Sugar Detection Using Different Machine Learning Techniques" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 3, pp. 23-33, DOI 10.30696/IJEEA.IX.III.2021.23-33

[14]. Nisarg Gupta, Prachi Deshpande, Jefferson Diaz, Siddharth Jangam, and Archana Shirke, (2021), " F-alert: Early Fire Detection Using Machine Learning Techniques" Int. J. of Electronics Engineering and Applications, Vol. 9, No. 3, pp. 34-43, DOI 10.30696/IJEEA.IX.III.2021.34-43