

Blockchain Technology and AI

(Lack of Blockchain Design and standardization)

Statement of the Work:

With its distributed ledger technology, the blockchain is widely recognized as one of the most promising innovations to address current challenges in many sectors. In brief, blockchain technology is a digital record of all transactions and information that are secured through encryption. With the use of cryptography, each record is linked to the previous one creating a chain of blocks, which is why it is called Blockchain. Furthermore, every block contains data that can be split into three parts. The first part stores information related to the specific block, including its number, nonce value, and hash value. The second part shows how data is stored. This statement is research to highlight the lack of Blockchain standards regarding no information on Blockchains used. in this document, I will consider only the Technical Part of Blockchain and will not consider other Domains such as Financial and Business.

Research Objectives:

To highlight the lack of Standards/Samples of Blockchains, in terms of Artificial Intelligence (Dealing with DATA, securing the Platform, Segregating the Blockchains).

Problem Description:

1st as design architecture and Standard Blockchain are not a one-size-fits-all solution, it might impact the design architecture and Implementation of building Multi / Single Blockchains, also a lack of information about the solution being made, leads to uncertainty about using this Technology especially when dealing with critical and sensitive information. (Han et al., 2023).

2nd as a **Security perspective** securing the data is always challenging, as Cyber-Attack keeps looking to find any Breach or weakness to reach to data.

The Significance Risk the Blockchain Technology:

Blockchain technology has emerged as one of the most transformative innovations of the 21st century. However; there are multiple potential risks it might consider as below”

1. Access and Authorization: Installing block and access through this point to reach to other Block by utilizing most of the Platform capacity and then the attacker could reach to the sensitive data and change the logs and so on.
2. Data Tempering: changing data in one block in the blockchain, will affect the block percentage of the overall platform, which will lead to a change in the next Block percentage and the remaining blocks and finally it will allow the attacker to control and setup the blocks with new data, this is applicable with Small Blockchain platform.
3. Sybil Attacks.

Existing Blockchain solutions:

There is no accurate information about the existing blockchain standards, however; the technical challenges will be addressed as the technology evolves. For example, Intel is actively collaborating with R3, using silicon-based technologies like Intel® Software Guard Extensions (Intel® SGX), to help improve the privacy and security of blockchain solutions. The real challenge is with the **change management concerning the people, culture, and processes**. It involves process change, workflow change, and cultural change. Reaching the benefits might be more cumbersome than thought. As previously mentioned, blockchain can be quite situation-specific and is not a one-size-fits-all solution to all business problems. The use of technology needs to align with the organizational purpose. **Not all the data might reside on a blockchain**. The choice between permissionless or permissioned blockchain has quite significant implications in terms of security and throughput. (Han et al., 2023)

Also, it too important to consider the security Measurement ones Designing and Building a blockchain platform such as an Encryption Technique, Consensus Mechanism, Smart Auditing contract, Multifactor Authentication

Document Key Points:

- **Comparative Research Methodology** Used in this Paper to gather Data and Find Integration Points between them.
- This Paper answers the question related to the main research (Blockchain Technology in the field of AI Key Benefits Vs. Limitation), and aligns with the Objective of the research (**To highlight the weakness of Blockchains and propose solutions that will enhance the Setup and configuration in Terms of Artificial Intelligence (Dealing with DATA, securing the Platform, Segregating the Blockchains, and so on).**

References:

(Tagde et al., n.d.) , (IEEE Staff, 2019b), (Salah et al., 2019), (Han et al., 2023).

A. Sharma and P. Kaur, "Tamper-proof multitenant data storage using blockchain," Peer-to-peer Networking and Applications, 2023.springer.com

H. E. Alhazmi, F. E. Eassa, and S. M. Sandokji, "Towards big data security framework by leveraging fragmentation and blockchain technology," IEEE Access, 2022.ieee.org

J. Yang, J. Wen, B. Jiang, and H. Wang, "Blockchain-based sharing and tamper-proof framework of big data networking," IEEE Network, 2020.HTML