Cross-chain data integrity verification with blockchain

*Smt. Kundanben Dinsha Patel Department of Information Technology,*

*Chandubhai S. Patel Institute of Technology, Charusat University, Changa,Gujarat.*

19IT109 SHIVAM PATEL-19IT113 VEDANT PATEL

***Abstract: Blockchain has shown promise in a variety of application areas in recent years, but it still faces technical hurdles such as security and scalability.*** ***As the number of transactions increases, blockchains face data storage challenges.*** ***Cross-chain solutions are connecting multiple blockchains and relieving data storage load.*** ***However, previous research usually focuses on the technical implementation of cross-chain contact, with little in-depth study on consistency concerns such as data integration verification of cross-chain interaction.***

**INTRODUCTION**

Blockchain is steadily expanding from small-scale applications to numerous areas, indicating a promising future. The increased quantity of transactions on the blockchain puts a burden on blockchain data storage, reducing the efficiency of on-chain queries and calculations. To alleviate the burden of data storage, we can store data on many blockchains. When the blockchain requires data from other chains, the data can be called across chains. Notary schemes, sidechains/relays, and hash-locking are currently popular cross-chain technologies.

Cross chain realizes chain interaction by connecting independent blockchain networks, relieving blockchain data storage pressure of blockchain. However, the majority of cross-chain applications focus on asset transfer rather than information call. Because each blockchain has its own internal security mechanism and does not participate in other blockchains' consensus processes, it is difficult for blockchains to determine the integrity of the received data. As a result, steps should be made to ensure the integrity of data in cross-chain interactions. Currently, data integrity verification methods are largely seen in cloud storage. Users outsource local data to the cloud and access data remotely over the Internet to alleviate the strain of data storage management. Without acquiring entire data details, users can assess whether the outsourced data is well kept by the cloud. Traditional verification systems, on the other hand, check the integrity of the data saved by the data receiver, which does not applicable to cross-chain scenarios. We must audit the behaviour of the chain that transmits data in cross-chain interactions in cross-chain scenarios. As a result, typical integrity verification methods in this research cannot be easily applied to cross-chain circumstances.

In previous research on integrity verification, third-party auditors were frequently used to evaluate the data integrity on an untrusted cloud. However, the employment of third-party auditors in cross-chain scenarios impairs the blockchain system's decentralisation, and there is also the chance that the auditors collaborate with the cloud to provide a biassed verification result in order to fool consumers. As a result, several academics have turned to blockchain for auditing. The laws and contracts for auditing blockchains can be transformed into simple and deterministic code-based rules that are automatically executed by the underlying blockchain network, ensuring that the blockchain always outputs a fair audit result and maintaining the decentralisation of the entire scheme in cross-chain interaction.

**ACKNOWLEDGMENT**

I would like to express our gratitude and thanks

to our professor Mr. Chandrashekhar Goswami sir & Mr. Pritesh Prajapati sir, Dept. of Information Technology for their continuous motivation towards making my research and giving helpful and important guidelines that leads my project more and more towards achieving its efficiency.