INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Framework for secure blockchain interoperability with homomorphic encryption

A Dissertation

by

Miss Jinali Wijetunge

Supervised by

Mr Ragu Sivaraman

Submitted in partial fulfilment of the requirements for the MSc in Advanced Software Engineering degree at the University of Westminster.

July 2023

Abstract

A major difficulty in the modern day of blockchain technology is the safe and easy transmission of data and assets between various blockchain networks. Interoperability solutions are necessary to facilitate communication and collaboration among diverse blockchain ecosystems while preserving data privacy and integrity. This research proposes an innovative mechanism to achieve secure cross-chain data transfer and asset exchange using homomorphic encryption for complex data formats.

In order to overcome the difficulties associated with cross-chain data transfer and asset exchange while protecting data privacy, we propose an advanced algorithm and mechanism that leverages homomorphic encryption for handling complex data formats. Homomorphic encryption enables computation on encrypted data without requiring decryption, ensuring data privacy even during computations. By integrating homomorphic encryption with smart contracts and interchain communication protocols, solution establishes a robust and secure cross-chain data transfer system. When a user initiates a data transfer request between two blockchain networks, utilizing homomorphic encryption methods, the data is secured. The encrypted data is then securely transmitted to the receiving blockchain, where a designated smart contract processes the encrypted data through homomorphic computations. The smart contract ensures that the computation results remain encrypted until they are safely decrypted by the intended recipient, ensuring that sensitive data remains confidential throughout the process.

The proposed mechanism demonstrates promising results, providing secure and seamless data transfer between blockchain networks. By handling complex data structures and preserving data privacy, our solution opens new possibilities for blockchain interoperability, with potential applications in supply chain management, healthcare, finance, and beyond. The proof-of-concept implementation validates the feasibility and security guarantees of our approach, contributing to the advancement of privacy-preserving blockchain interoperability solutions.

Keywords: Blockchain, Interoperability, Security, Ethereum, Homomorphic Encryption, off-chain oracle