1. Introduction

The rapidly evolving landscape of blockchain technology, the need for robust and efficient cryptographic mechanisms is increasingly critical. Digital signatures play a fundamental role in ensuring the security, integrity, and authenticity of transactions within blockchain systems. Traditional digital signature schemes, while effective, often face limitations when scaled to meet the demands of modern blockchain applications. These limitations include issues related to computational efficiency, storage overhead, and vulnerability to emerging cryptographic threats.

To address these concerns, this paper introduces a new digital signature primitive designed specifically for blockchain environments. The proposed signature scheme leverages advanced cryptographic techniques to overcome the limitations of existing methods. By incorporating elements such as elliptic curve cryptography and hash-based message authentication codes, the new primitive offers a more secure and efficient alternative.

The approach aims to streamline the process of signature generation and verification, thereby reducing computational overhead and storage requirements while enhancing overall security. The proposed digital signature scheme is tailored to integrate seamlessly with existing blockchain protocols, ensuring compatibility with a wide range of blockchain platforms.

1.1 Purpose

The goal is to design and implement a novel digital signature primitive that enhances the security, efficiency, and scalability of blockchain technology. Digital signatures are essential to blockchain systems, ensuring the authenticity and integrity of transactions. This new primitive aims to overcome current limitations in existing signature schemes such as high computational overhead, poor scalability, and vulnerability to quantum attacks while significantly improving transaction verification speed and overall security.

1.2 Scope

The development of a new digital signature primitive tailored for blockchain applications represents a crucial step toward advancing the security, efficiency, and scalability of decentralized systems. This novel cryptographic signature scheme aims to enhance resistance against a wide range of threats, including quantum computing attacks and signature forgeries, thereby strengthening overall system security. By reducing computational complexity and improving transaction processing speeds, the new scheme can support higher throughput and better scalability, addressing one of the major limitations of current blockchain networks. Seamless integration into blockchain frameworks will ensure that transactions are validated securely and efficiently. Additionally, features such as multi-signature and aggregate signature support enable efficient group authentication, which is particularly valuable for smart contracts and multi-party interactions. To maximize its practical applicability, the signature scheme is designed for cross-platform usability, ensuring compatibility with a variety of blockchain architectures—whether public, private, or hybrid.

1.3 Need for System

The widespread adoption of blockchain technology across diverse sectors—including finance, healthcare, logistics, and supply chain management—has led to a growing demand for robust, scalable, and efficient cryptographic mechanisms. Among these, digital signature schemes play a pivotal role in ensuring the authenticity, integrity, and non-repudiation of transactions. However, conventional digital signature algorithms such as RSA, ECDSA, and EdDSA are increasingly encountering critical limitations. These include high computational costs, reduced efficiency in high-throughput environments, and limited scalability when applied to large and decentralized networks. Furthermore, the looming threat posed by quantum computing technologies renders many of these classical algorithms insecure in the long term, as quantum algorithms like Shor's algorithm could potentially break their underlying mathematical assumptions.

To address these shortcomings, the development of novel, optimized digital signature schemes is imperative. Such advancements can significantly enhance blockchain performance by reducing signature generation and verification times, lowering energy consumption, and improving overall network throughput. Additionally, the integration of post-quantum cryptographic techniques—such as lattice-based, hash-based, and multivariate polynomial cryptography—provides a pathway toward building quantum-resistant blockchains, ensuring long-term data security and system resilience.

In parallel, privacy and data confidentiality are becoming increasingly vital as blockchains evolve beyond financial applications into domains that handle sensitive personal or organizational information. Traditional blockchain models, which emphasize transparency, often struggle to reconcile openness with privacy. As a solution, advanced cryptographic constructs—such as ring signatures, zero-knowledge proofs (ZKPs), and homomorphic encryption—offer powerful tools for achieving privacy-preserving transactions. These techniques enable users to prove the validity of a transaction or computation without revealing any underlying data, thereby enhancing user anonymity and trust in decentralized networks.

1.3.1 Existing System

As blockchain technology continues to advance and gain widespread adoption, the demand for robust and efficient digital signature schemes has become increasingly critical. Traditional digital signature algorithms, while secure, often encounter performance issues and limitations when applied to the growing and complex demands of blockchain systems. These issues include high computational overhead, increased storage requirements, and scalability constraints, which can affect the overall efficiency and security of blockchain networks. Additionally, existing signature schemes may be vulnerable to emerging cryptographic attacks and may not adequately address the evolving threat landscape. The challenge, therefore, is to develop a new digital signature primitive that not only mitigates these limitations but also enhances the scalability and security of blockchain applications. This necessitates the exploration of innovative cryptographic approaches that can seamlessly integrate with blockchain technology while providing improved performance and resilience against potential threats.

Disadvantages

- increased computational demands during the initial deployment phase.
- potential integration challenges with legacy systems.
- This can lead to increased development time and costs, as well as potential integration challenges with legacy systems.

1.3.2 Proposed System

To address the challenges associated with traditional digital signature schemes in blockchain systems, this paper proposes a new digital signature primitive designed to enhance both security and efficiency. The proposed scheme introduces novel cryptographic algorithms and protocols that streamline the signature generation and verification processes, thereby reducing computational overhead and storage requirements. This digital signature primitive is built upon advanced cryptographic techniques such as elliptic curve cryptography and hash-based message authentication codes, which offer improved performance and resistance against common attacks.The proposed signature scheme is specifically tailored for blockchain applications, ensuring compatibility with existing protocols while offering significant improvements in scalability and security. By integrating this new digital signature primitive into blockchain networks, the system benefits from faster transaction processing, reduced latency, and enhanced overall security. The paper further explores the practical implementation of the proposed scheme within blockchain environments, demonstrating its effectiveness through various use cases and performance benchmarks. This innovative approach aims to set a new standard in digital signatures for blockchain technology, addressing current limitations and paving the way for more secure and efficient blockchain applications.

Advantages

- By optimizing the signature generation and verification processes, it enables faster transaction processing and lower latency.
- collectively contribute to a more secure, efficient, and scalable blockchain environment, positioning the new signature scheme as a valuable advancement in digital cryptography.

1.4 Architecture

A new digital signature primitive, called Lattice-based Multivariate Group Signature (LMGS), has been designed to provide a secure and efficient solution for blockchain applications. This primitive combines the benefits of lattice-based cryptography, multivariate polynomials, and group signatures to create a robust and scalable digital signature scheme. The LMGS architecture consists of a key generation algorithm, a signing algorithm, and a verification algorithm. The key generation algorithm is used to generate a set of public parameters and a private key for each group member. The signing algorithm is used by a group member to create a signature using their private key and the public parameters. The verification algorithm is used by anyone to verify the signature using the public parameters and the group's public key.

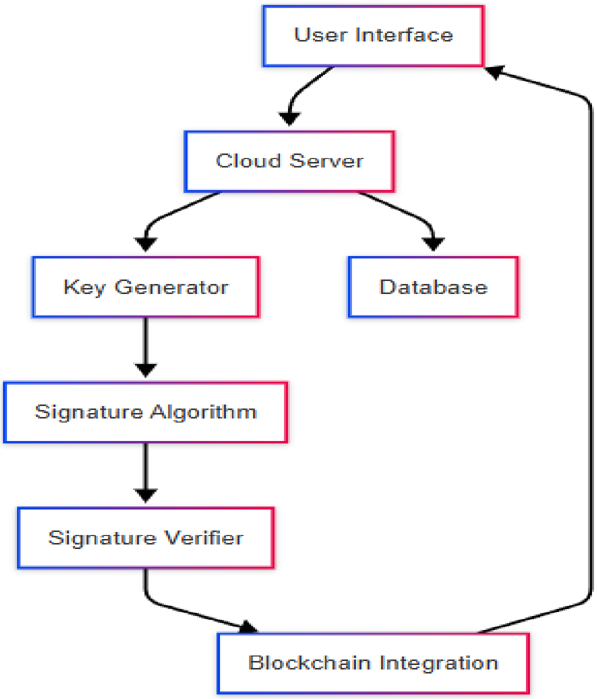

Fig.no: 1.4 System Architecture