# Abstract: Quantum Cryptography-Based Secure Blockchain

**Introduction:**
The rapid advancement of quantum computing poses a significant threat to traditional cryptographic techniques used in blockchain systems. Many existing security mechanisms, such as RSA and public-key cryptography, rely on the computational difficulty of factoring large numbers. However, with the advent of quantum computing and algorithms like Shor's algorithm, these encryption methods become vulnerable. This project aims to integrate Quantum Key Distribution (QKD) with blockchain to establish a quantum-secure decentralized ledger, ensuring resilience against future quantum attacks. By leveraging the BB84 protocol, the system facilitates secure key exchange between blockchain nodes, preventing unauthorized access and eavesdropping.

**Objectives:**
The primary objectives of this project are:

- To develop a quantum-secure cryptographic system that can replace RSA and other vulnerable encryption techniques.
- To integrate Quantum Key Distribution (QKD) into blockchain technology for enhanced security.
- To design a modular cryptographic framework adaptable to various secure communication systems.
- To demonstrate the application of this quantum security system in blockchain and other digital communication channels.

**Methods/Approach/Proposed Solution:**
To address the security risks posed by quantum computing, this project proposes the implementation of QKD, which uses quantum physics principles for unbreakable encryption. The approach includes:

- **Quantum Key Distribution (QKD):** Replaces RSA-based encryption with quantum-generated keys that are inherently resistant to quantum attacks.
- **BB84 Protocol Implementation:** Ensures secure key exchange by leveraging quantum properties such as superposition and entanglement.
- **Blockchain Integration:** Demonstrates the feasibility of applying quantum cryptography in decentralized ledger systems.
- **Modular System Design:** Enables integration with various secure communication systems, including VPNs, email security, and enterprise applications.
- **Use of Qiskit for Quantum Simulations:** Simulates quantum cryptographic operations and evaluates their security in practical use cases.

**Conclusion/Implications:**

The developed system successfully demonstrates quantum-secure key generation and universal applicability beyond blockchain, making it suitable for secure email communications, VPNs, and messaging applications. By providing quantum-resistant security, this solution addresses the vulnerabilities of traditional cryptographic methods and ensures long-term data protection against quantum threats. The implementation of this technology could revolutionize digital security, making it future-proof and adaptable to evolving technological advancements.


**INSTITUTION : Dayananda Sagar University**

**Team**

| | | |
|---|---|---|
| Name : Satwik Kashyap | Email : Kashyapsatwik29@gmail.com | Phone No: 9019900897 |
| Name : Sathish S | Email : vanetha137@gmail.com | Phone No: 6361002354 |
| Name : Shaik Fahad | Email : sheikfahad365@gmail.com | Phone No: 8217410633 |
| Name : Shashank S | Email : shashankthor295@gmail.com | Phone No: 7829069295 |