SRM INSTITUTE OF SCIENCE & TECHNOLOGY

A NATIONAL LEVEL TECHNO-MANAGEMENT FEST

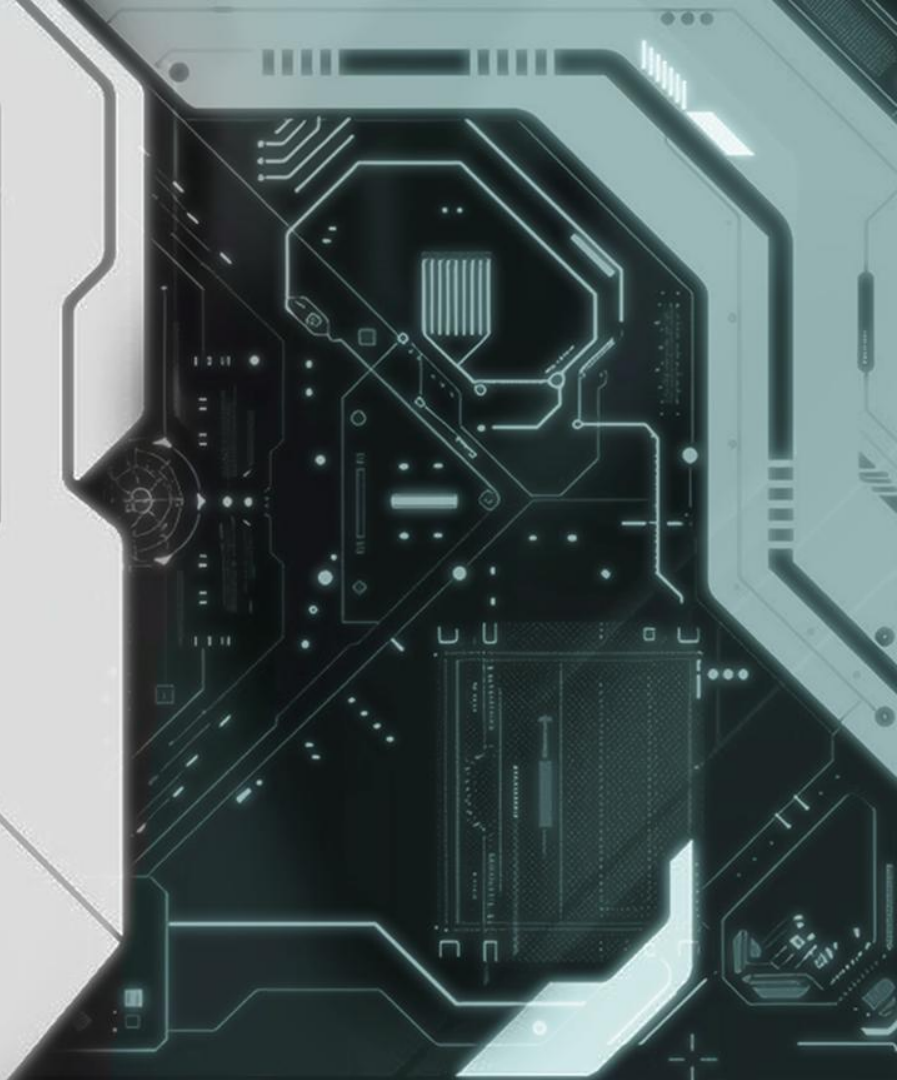
AARUUSH '25

...rising in the spirit of innovation

HACK SUMMIT

TEAM : OUTLIERS

Design of a Quantum-Resistant Communication Protocol Using Blockchain

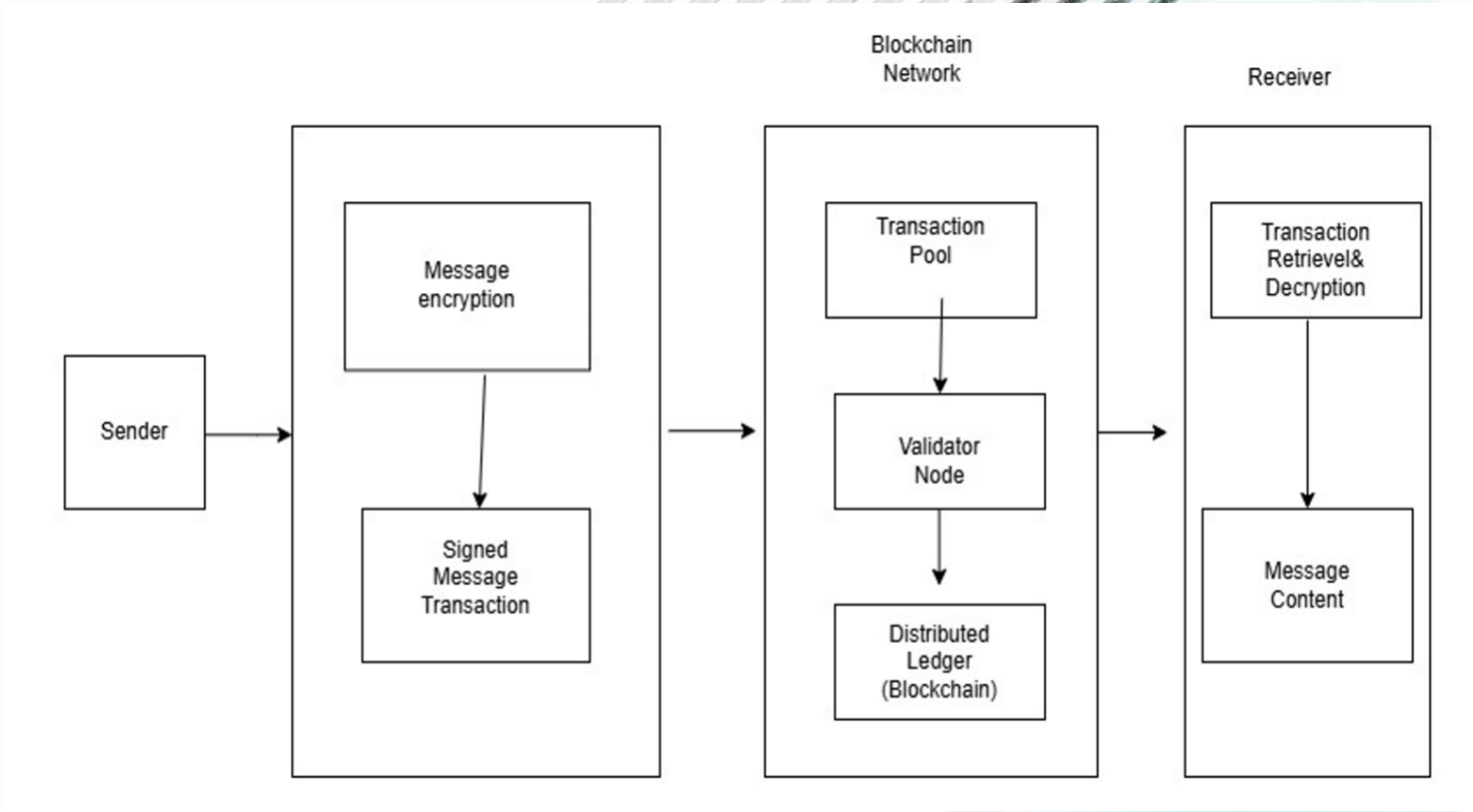


ABSTRACT

Our solution is a quantum-resistant communication protocol built on a public blockchain, designed to provide secure, end-to-end encrypted messaging for the quantum era. The core idea is to treat every message as a fully authenticated and encrypted transaction. The protocol is built exclusively using NIST-standardized Post-Quantum Cryptography (PQC) primitives to guarantee the privacy and integrity of communications against both classical and quantum threats, delivering a scalable and user-friendly platform

TECHNICAL APPROACH

Language & Prototyping:
The prototype is developed in **Python** for its extensive cryptographic libraries and rapid development.
Core Cryptography:
The architecture is built on the **CRYSTALS (Cryptographic Suite for Algebraic Lattices)** suite.
Encryption:
CRYSTALS-Kyber is used for secure key encapsulation and message delivery.
Authentication:
CRYSTALS-Dilithium is used for digital signatures to ensure authenticity, integrity, and non-repudiation.
Consensus Mechanism:
A novel hybrid model, **Delegated Proof of Luck (DPoL)**, is used.
•It avoids the high energy use of Proof of Work and mitigates the centralization risks of Proof of Stake.
•Token holders elect trusted delegates, and a block producer is chosen from this pool via a verifiable, luck-based lottery (VRF).
System Flow:
A sender encrypts and signs a message as a transaction, which is broadcast to the network. A validator node processes it, and upon consensus, it's recorded on the distributed ledger for the receiver to retrieve and decrypt.


Blockchain Network
Receiver
Sender
Message encryption
Signed Message Transaction
Transaction Pool
Validator Node
Distributed Ledger (Blockchain)
Transaction Retrievel& Decryption
Message Content

FEASIBILITY & VIABILITY

Potential Challenges: The primary challenge is the performance cost or **"PQC Tax"** associated with post-quantum algorithms.
Size Overhead: PQC signatures are substantially larger than classical ones (~35x for Dilithium), increasing the on-chain data footprint.
Throughput Reduction: Larger transaction sizes are estimated to reduce the number of transactions per block by over 90%.
Risk: As large-scale quantum computers are not yet available, security validation must be conducted through **theoretical analysis** and threat modeling against known quantum algorithms (e.g., Shor's, Grover's).

IMPACT & BENEFITS

Economic: Protects cryptocurrencies and digital assets from being stolen by future quantum attackers. An estimated 25% of all Bitcoin is currently vulnerable.

Social: Preserves long-term privacy by defeating "Harvest Now, Decrypt Later" strategies, ensuring today's encrypted communications remain secure in the future.

Strategic: Provides a clear and viable path for organizations and critical infrastructure to meet urgent government mandates (U.S. 2035, E.U. 2030) for migrating to PQC.

FUTUTRE SCOPE

•**Scalability & Long-Term Vision:** The DPoL consensus mechanism is designed for high speed and scalability. The long-term vision is to develop a fully functional, public quantum-resistant blockchain.

•**Immediate Next Steps:**
1.Performance Evaluation: Deploy the prototype in a simulated network to measure Transaction Throughput (TPS), latency, and data overhead.
2.Security Analysis: Conduct a rigorous theoretical review of the cryptographic implementations and perform protocol-level threat modeling.
•**Adoption Strategy:** Target enterprises and critical infrastructure sectors that are under mandate to upgrade their security to PQC standards

OUR TEAM

JANEESH P	111722202016	janeeshpofficial@gmail.com
KISHORE L	3122223002066	silverfoxx2k4@gmail.com
Vijay RS	3122225002156	vijaysaravanan124@gmail.com
Vignesh M	3122225002154	vigneshmt27@gmail.com