Name:Nithin

Srn :PES1UG22CS399

Quantum key Distribution and Blockchain

In this white paper from Toshiba, JPMorgan chase and ciena tells about countermeasure for the emerging quantum computing threats in blockchain & asymmetric cryptography like "harvest now and decrypt later" using quantum key Distribution [QKD]. In this paper demonstrated practical applications of this technology for financial institutions requiring quantum-resistant transaction security.

Paper Summary :-

Blockchain technology's distributed ledger model transformed financial transactions, but it is still susceptible to attacks using quantum computing. The study demonstrates how the public-key cryptography (RSA, elliptic-curve) currently used to secure blockchain networks could be compromised by quantum computers using Shor's algorithm.

According to this paper "harvest now, decrypt later" attacks are especially worrisome, because in this attackers store encrypted data to decrypt it in future when quantum computers advance. It is extremely worrisome because it may expose some critical data it is addressed by QKD which uses quantum mechanics so that eavesdropping become impossible as it is dectble by encoding cryptographic keys on individual photons.

The feasibility of QKD was shown on a metro-scale test bed: 800 Gbps secured channels maintained low latency for video conferencing and high frequency trading demonstrating compatibility with the current financial infrastructure. high deployment costs, low key generation rates (~1 Mbps) and a lack of NIST standardization are among the difficulties. A phased adoption path for banks is provided by the hybrid approach (QKD + Post-quantum algorithms). which secures data at rest as well as data in transit.

Q In what ways can QKD enhance the confidentiality and security of permissioned block chain networks?

- QKD uses quantum mechanics for security: the no cloning theorem photon duplication and it uses heinsenberg unsertenity principle which ensures eavesdropping alters the photon states which will trigger alerts. we can detect if there is any interception in between.
- permissioned block chain networks benefited from QKD's controlled node access. where it will secure the communication chanel between authorised node and ensures tamper-proof key distribution.
- JP morgan intergrated QKD with Ciena's optical networks and achieved 800 Gbps throughhput with intrusion detection without latency. and they have confirmed scalability for real time trading and secure inter-institutional data transfer.
- consensus algorithms like PBFT and Raft depend on trusted nodes exchanging messages in permissioned networks, protecting these message QKD stops interference or tampering maintains honesty and confidence.
- Resilient identity verification where each participant can be assigned quantum-generated keys for identity verification which is stronger than traditional quantum digital signatures and immune to man in the middle attacks while exchanging keys.

Conclusion :-

for financial institutions that handle sensitive transaction data. QKD Provides a Physics-based defense against quantum computing threats to blockchain networks. the JPmorgan chase implementation demonstrates that QKD is prepared for practical use in permissioned block chain settings. A complete security framework that safeguards data in transit and at rest is created by QKD's integration with post quantum algorithms. despite its current limitations due to distance restrictions and specific hardware needs.