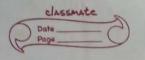
Name:Nithin

Srn:PES1UG22CS399

Quantum key Distribution and Blockchain In this white poper from Toshiba . JPMorgan chose and crent tells about countermeasure for the emerging quantum computing threats in block chain & asymmetric cryptography like "horvest now and decrypt later" verng quantum key Distribution [OKD]. In this paper demonstrated practical applications of this technology son froncial institutions anostutistant Lossonit transaction Becuity. Paper Summary :-Blockchain technology's distributed ledgies model transformed Stanceal transactions but it is still susceptible to attacks using quantum computing. The study demanstrates how the public- key cryptography (RSA, & 119ptic + come) currently used to secure blockchash networks could be compromised by quantum computers using shors algosithm. According to this paper "howest now decrypt loter," attacks ore especially worrisome, because on this attackers stone encrypted data to decrypt : + : n Suture when quantum computers advance . It is extremely worresome because of may expose some critical data it is addressed by OKD which uses quantum mechanics 80 that eaves diopping become impossible as it is decible by encoding cryptographic keys on and vidual photons. The Seasibility of OKD was shown an a metro-scale test bed : 800 Gaps Secured Channels maintained Low latency for video conferencing and high frequency trading demonstrating compatibility with the current financial infrostructure, high deployment costs lowsky

generation rates (-1 Mbps) and a lack of NIST Standarzation are among the difficulties a phased adoption poth for books ?s provided by the hybred approach COKD + Post - quantum algorithms). ewhich secures dota at rest as well as dota on tronsot In what ways can OKD enhance the considentiality and security of Permissioned black chain networks? . OKD uses quantum mechanics for security : the no claning theorem photon duplication and it uses he insenberg unsertently pranciple which ensures eaved copping alters the photon states which will trigger alists. we can detect of there os ony interception on between · permissioned black chain network benefited from OKDs controlled node occess above it will secure the commous tion chanel between authorised node and ensures · lamper - proof key destribution. . JP morgon entergrated OKD with creno's optical networks and achieved 800 Gbps through hput with intrusion detection enithout 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 tempering maintains honesty and confidence . Resilient identity verification where each porticipant con be assigned quantum - generated keys for dentity vertication which is stronger than traditional quantum digital signatures and immune to man in the middle attacks while exchanging reys



Conclusion :-

Jos Senonceal enstitutions that handle Benestive transaction data. OKD Provides a Physics based delense against quantum computing threats to black that networks the IPmagon chase implementation demanstrates that akd is prepared for practical use in permissioned black that self-ings. A complete security framework that safeguards data in transit and at rest is created by OKD's integration with post quantum algorithms despite its current limitations due to distance restrictions and specific hardware needs.