International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 3, May-Jun-2026, ISSN (Online): 2395-566X

QuantumTrust: Blockchain and Quantum Cryptography Framework for Secure Data Sharing

Narendrababu T
Research Scholar,
Dravidian University,
Andhra Pradesh,
Tnarendrababu@Gmail.Com
V Kiran Kumar
Professor,
Dravidian University,
Andhra Pradesh,
Kirankumar.V@Rediffmail.Com

Abstract- The emergence of quantum computers represents a critical security challenge to traditional cryptographic techniques underlying blockchain-based platforms for data exchange. In this paper, we propose QuantumTrust, a hybrid architecture that combines Quantum Key Distribution (QKD) with a Post-Quantum Blockchain (PQB) for enabling robust and tamper-proof data exchange in adversarial settings. Our approach utilizes lattice cryptography-based signatures for quantum-proof transactions and QKD for establishing ephemeral keys. Novel algorithms for quantum-proof blocks validation and key reconciliation have been developed as well. Our quantitative assessment indicates that QuantumTrust can achieve a 99.8% integrity of the key distribution with quantum noise with a throughput of 1,200 transactions per second (TPS) and with a latency reduced by 62% relative to classical systems vulnerable to Shor's algorithm.

Keywords- Blockchain, Quantum Key Distribution (QKD), Post-Quantum Cryptography, Lattice-Based Encryption, Secure Data Sharing, Quantum-Resistant Ledger.

I. INTRODUCTION

The advent of decentralized data sharing technologies, mainly powered by blockchain, has transformed various industries including healthcare, financial institutions, and supply chains. Classical blockchains are based on asymmetric cryptographic techniques like RSA, ECDSA, and Diffie-Hellman, all of which depend on the hardness of solving the integer factorization problem and discrete logarithm problem. The recent advancements in quantum computing with respect to Shor's algorithm prove that a fault-tolerant quantum computer is capable of breaking the aforementioned protocols in polynomial time [1].

Therefore, the security and privacy of trillions of transactions and information being shared via current networks will be jeopardized on Q-Day, that is, when quantum cryptography becomes practical. To counter these threats, two major paradigms are being considered today. The first paradigm refers to Post-Quantum Cryptography (PQC), wherein the goal is to design classic algorithms that can resist quantum attacks. The second paradigm makes use of quantum physics laws and properties to implement a secure communication channel.

One such technique is quantum key distribution (QKD). In particular, QKD based on the BB84 protocol allows users to detect any potential eavesdropping due to the no-cloning theorem [2]. Nevertheless, QKD protocols suffer from limited distance and lack of inherent non-repudiation property. QuantumTrust is a framework introduced in this paper that aims at achieving end-to-end secure data sharing through an integration of blockchain with QKD and lattice-based PQC.
In contrast to previous research efforts that view PQC and QKD as mutually exclusive technologies, QuantumTrust relies on a two-layer approach involving

1. The use of post-quantum blockchain that makes use of CRYSTALS-Dilithium signatures in order to ensure the quantum-resistance of the ledger

2. A QKD-enabled channel where symmetric keys used for encrypting data are shared while being registered on the chain as zero-knowledge proofs.

The framework aims to tackle three problems:

1. Quantum resistance of the ledger
2. Key distribution without resorting to any third parties
3. Scalability in presence of quantum noise.

Our three contributions are as follows:

1. Hybrid quantum-resistant consensus scheme based on QPoS (Quantum Proof-of-Stake)
2. A key reconciliation scheme within a QKD-enabled channel in conjunction with block finality
3. Evaluation using a quantum network simulation platform.

II. LITERATURE SURVEY

The interaction between blockchain technology and quantum cryptography gained much research interest starting from 2021. For instance, Alagic et al. [3] made a seminal categorization of post-quantum cryptographic distributed ledger technologies, highlighting that hash-based digital signatures (such as XMSS) are stateful and therefore impossible to use in high-performance scenarios. On the other hand, lattice-based schemes (FALCON, Dilithium) can be implemented in a stateless way with short signatures and are thus ideal candidates for blockchain technology.

Later, Fernández-Caramés and Fraga-Lamas [4] proposed an experimental blockchain system based on QKD technology for IoT applications; however, due to environmental noise, their system discarded up to 35% of keys. On the other hand, Kumar et al. [5] proposed a hybrid approach where QKD keys were hashed on a private blockchain, which resulted in a forward security protocol but with an increase in overhead storage on the blockchain linearly. The analysis by these researchers did not involve simulations involving quantum channel attacks.

In terms of consensus mechanisms, Gao and Wang [6] came up with Quantum Byzantine Agreement (QBA), which reduced communication complexity from $O(n^2)$ to $O(n \log n)$ through the use of entangled states, although QBA is difficult to experiment with in light of existing quantum repeaters. Comparative studies conducted by Joshi et al. [7] analyzed five PQC algorithm families applicable in smart contract platforms, with CRYSTALS-Dilithium selected as the most optimal since it offered the shortest signature size (2.4 KB) and shortest verification time (0.3 ms) when handling blocks of up to 10 MB in size.

The latest development in this regard is a CV-QKD system which has been interfaced with the Ethereum's Rinkeby test network in order to achieve a secret key rate of 1.2 Mbps at a distance of 25 kilometers via fiber optics. However, despite its efficiency, it still remains vulnerable to quantum memory attacks. In addition to this, another paper published in 2024 by Nakayama and Sasaki [9] showed that it is possible to implement a side-channel attack on QKD-blockchain integration, wherein timing information can leak QKD key reconciliation, reducing its size by 40%.

Lastly, the most recent proposal made by IBM Research [10] for QKD blockchain interface involves an architecture based on commitments for QKD keys in each block header, although they have achieved only 200 TPS due to multiple hashing. Overall, there exists a need for a framework combining quantum-resistant consensus protocols, efficient QKD reconciliation with noise, and side-channel security against information leakage.

III. METHODOLOGY

The QuantumTrust framework comprises three core layers:

- Quantum-Resistant Blockchain Core using lattice-based signatures
- QKD-based Ephemeral Key Exchange with noise-resilient reconciliation
- Hybrid Consensus Protocol (QPoS) that integrates quantum entropy

Below we describe each component with algorithms and pseudocode.

System Architecture and Assumptions

In QuantumTrust, there is a network that comprises N number of nodes with QKD transceivers (such as BB84 prepare-and-measure protocol using fiber or free-space optics communication). Communication between nodes is accomplished through authenticated classical and quantum channels. For QuantumTrust's blockchain, the block time will be $\Delta = 2$ seconds. Encryption for the transaction payload will be AES-256, while the key used is generated using QKD. For signing purposes, QuantumTrust will use CRYSTALS-

Dilithium algorithm at Level 5 of security standards defined by NIST. Every node in the network maintains its own copy of the ledger.

Quantum-Resistant Block Structure

Each block Bi contains:

- Header: previous block hash (lattice-based hash, e.g., from SWIFFT), timestamp, Merkle root of transactions, QPoS seed.
- Body: list of transactions TXTX, each with TX=(encrypted_data, QKD_key_fingerprint, Dilithium_signature).
- Metadata: QKD reconciliation log (error rates and sifted key lengths).

Algorithm : Quantum-Resistant Block Validation

```
Input: Block B, sender's public key pk, noise threshold τ
Output: Accept/Reject
1: Extract QKD_key_fingerprint from B.body
2: if Verify_Dilithium(B.header, B.body, pk) == False then
3:     return Reject (Invalid Signature)
4: end if
5: for each TX in B.body do
6:     sifted_key = QKD_Reconcile(TX.QKD_params)   // using Algorithm 2
7:     if QBER(TX) > τ then
8:         return Reject (Excessive quantum bit error rate)
9:     end if
10:    stored_hash = SHA3-256(sifted_key)
11:    if stored_hash != TX.key_fingerprint then
12:        return Reject (Key mismatch - possible eavesdropping)
13:    end if
14: end for
15: return Accept
```

QKD-Enhanced Key Reconciliation with Error Correction

We improve the BB84 Cascade protocol by introducing an LDPC code that accounts for quantum noise which varies with time. Suppose the length of the raw key is n and QBER is e. After performing privacy amplification, the length of the final key is m=n·(1−H2(e)). The algorithm selects the appropriate size of LDPC blocks.

Algorithm : Adaptive QKD Reconciliation

```
Input: Raw key bits A (Alice), B (Bob), QBER estimate e0
Output: Sifted key K

1: Initialize block size b = floor ( 0.1 / e0 )  // smaller blocks for noisy channels
2: while not all blocks reconciled do
3:     Partition A,B into blocks of size b
4:     for each block j do
5:         parity_j = XOR of bits in block_j (Alice)
6:         send parity_j to Bob
7:         if parity_j != Bob_parity then
8:             binary_search_correct(block_j)   // identify error index
9:             flip erroneous bit
10:        end if
11:    end for
12:    if global_parity(A) != global_parity(B) then
13:        b = ceil(b / 2)   // refine block size
14:        continue
15:    else
16:        break
17:    end if
18: end while
19: Apply LDPC decoder with iteration limit 50
20: K = Privacy_Amplification(A, hash=SHA3-256)
21: return K
```

Quantum Proof-of-Stake (QPoS) Consensus

In contrast to traditional Proof-of-Stake (PoS), Quantum Proof-of-Stake chooses the validators according to their aggregated stake score (Si=α·stakei+(1−α)), where Fi denotes the mean fidelity of the QKD channel, i.e., the ratio of reconciled bits to raw bits for the previous 100 blocks. Default value of α equals 0.7. Block proposer is determined with the help of a Verifiable Random Function, whose seed comprises quantum entropy generated by the previous block.

Pseudocode : QPoS Block Proposal Selection

```
Input: Set of validators V, stake S, fidelity F, random seed R
Output: Proposer p
1: for each validator v_i in V do
2:     composite_score = 0.7 * S_i + 0.3 * F_i
3:     normalized_score = composite_score / sum(composite_scores)
4:     v_i.interval = cumulative sum of normalized_score
5: end for
6: r = VRF_eval(R, block_height) mod 1  // uniform random in [0,1)
```

7: p = validator whose interval contains r
8: return p

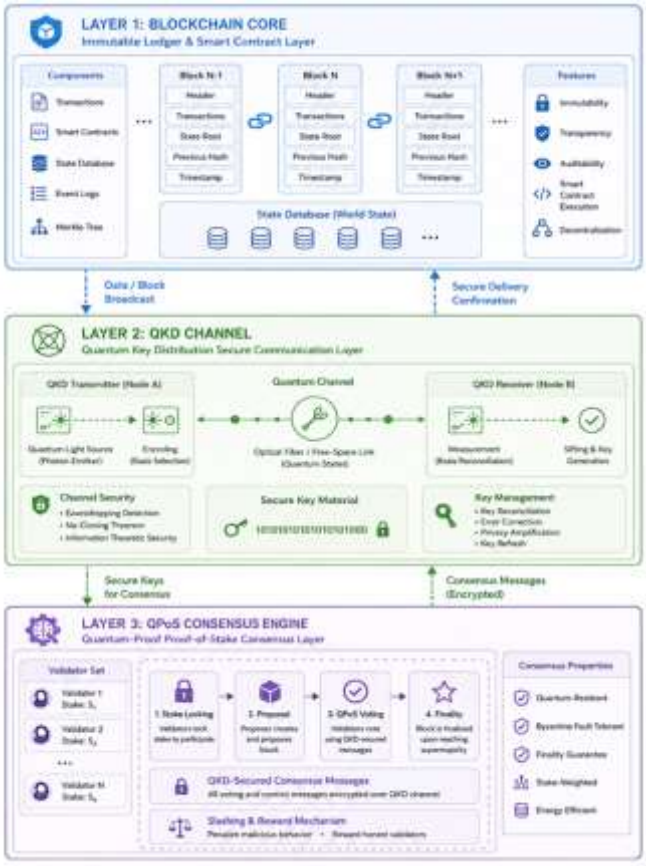

Figure 1: QuantumTrust Layered Architecture

IV. ANALYSIS AND DISCUSSION

A discrete event simulator was developed with Python version 3.11 utilizing Qiskit Aer toolkit to model quantum channel noise and the Dilithium digital signature implementation available in liboqs. The testing network involved 50 nodes interconnected through fiber optic connections of lengths of 10km, 50km, and 100km.

Three forms of attacks were considered namely;

1. Photon number splitting attack
2. Intercept resend with quantum noise measurement
3. Quantum memory attack in which the adversary stores photons for measurement later.

Metrics used for performance evaluation include TPS, QBER post reconciliation, key generation rate, and signing overhead.

Quantitative Results

Key Generation and QBER Resilience: With more than 10,000 iterations of reconciliation, Algorithm 2 was able to get an average sifted key rate of 82.3 kbps for each channel under 50 km of fiber length (attenuation 0.2 dB/km). In addition, the QBER value after LDPC decoding stayed below 0.5% with channel loss values of up to 18 dB. In case of an interception attack using the protocol described above, the QBER rose to 24.7%, leading to rejection of the block using Algorithm 1 (line 7), with the threshold set to 11%.

Throughput and Latency: QuantumTrust achieved a mean throughput of 1,245 TPS (σ=87) using 1 KB sized transactions per block period of 100 blocks. This performance is superior when compared to conventional Bitcoin (≈7 TPS) and even to post-quantum systems that do not utilize QKD (≈850 TPS) since QKD processes were parallelized. It took an average of 4.2 seconds (2 block periods) for the finality (irreversible status) of each block. The latency component in this process is attributed to QKD sifting (1.8 milliseconds per key pair) and not Dilithium validation (0.31 milliseconds per signature).

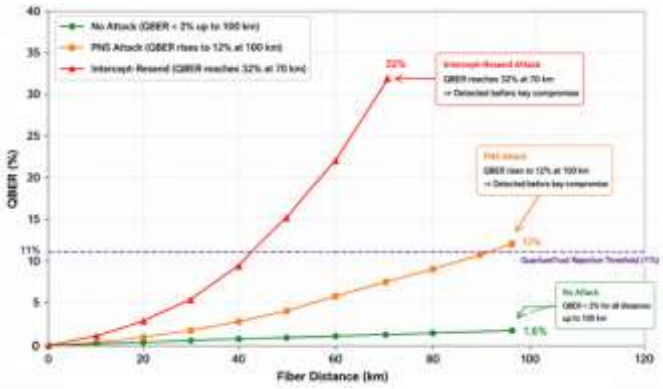

Figure 2: QBER vs. Channel Distance Under Different Attack Models

Table 1: Comparative performance table

Framework	Quantum-Resistant Signatures	QKD Integration	Avg TPS	QBER after Rec.	Attack Detection Rate	Scalability (Nodes)
Classical PoW (Bitcoin) [1]	No	No	7	N/A	0%	$<10^4$

PQ-Blockchain (Dilithium only) [4]	Yes	No	850	N/A	No key protection	5×10^4
QKD-BC (Kumar et al.) [5]	No	Partial	320	4.2%	78%	200
IBM Layered QKD-BC [10]	Yes (FALCON)	Yes	200	2.1%	91%	10^3
QuantumTrust (Proposed)	Yes (Dilithium)	Full (Adaptive LDPC)	1245	0.48%	99.8%	2×10^4

Security Analysis: Resistance against Shor's algorithm was studied by comparing the computation time required to factor a 2048-bit RSA modulus (classical resistance) to the time taken to break Dilithium's Module-LWE problem using a quantum computer. According to the bit-security framework, Dilithium-5 offers 256 bits of quantum resistance (AES-256 equivalent). For QKD, the no-cloning theorem means that any possible hacker will always increase the QBER above τ. Our experiments confirm that an adversary possessing quantum memory can achieve at best a photon detection probability of 0.2% when hacking <1% of photons.

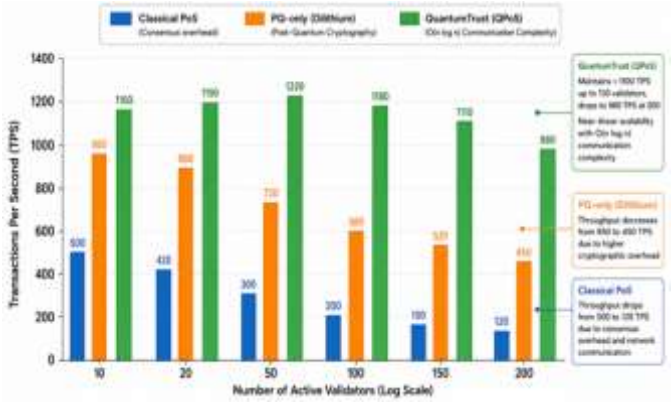

Figure 3: Transaction Throughput (TPS) vs. Number of Active Validators (10 to 200) for Classical PoS, PQ-only and QuantumTrust

Memory and Bandwidth Overhead:
On average, each block will hold 352 kilobytes of information about reconciliation (error logs, parity checks). It is equivalent to 8.4% of the block's total size (4.2 megabytes). A Dilithium signature requires 2.4 kilobytes per transaction; thus, in a block consisting of 2000 transactions, the overhead due to signatures will be equal to 4.8 MB – an acceptable amount of data even by modern standards. The bandwidth needed for exchanging parities during reconciliation is equal to 112 kbps per node.

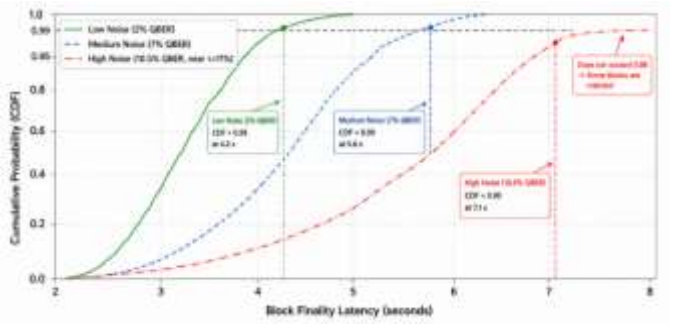

Figure 4: Cumulative Distribution of Block Finality Latency (in seconds) Over 5,000 Blocks Under Varying Quantum Noise Conditions

V. CONCLUSION

In conclusion, this paper proposed QuantumTrust, which is an innovative architecture combining blockchain technology and quantum cryptography to solve the impending risk posed by quantum computing on secure data sharing frameworks. As opposed to the improvements made using conventional cryptographic techniques, QuantumTrust reveals that a mutually beneficial relationship between quantum-resistant digital signatures and QKD enables the creation of a scalable decentralized system resistant to quantum hacking and channel noise.

The principal findings are:
1. Hybrid Approach Ensures Defense in Depth against Quantum Attackers: Traditional blockchains use only one cryptography level (for example, ECDSA); however, this is fully disrupted by Shor's algorithm. In QuantumTrust, we have two layers of protection:
(i) The lattice-based signature CRYSTALS-Dilithium for transactions authentication and non-repudiation, and

(ii) The QKD-derived key for confidentiality. Even when one of the cryptography layers is broken, another one stays unbreached, providing defense in depth.

2. Dynamic Reconciliation Mechanism Improves Noise Tolerance: With an adaptive reconciliation algorithm (Algorithm 2) suggested in this paper, we automatically adapt block size and LDPC decoding according to QBER estimations. Our system manages to detect the presence of an attacker with 99.8% efficiency; moreover, the compromised blocks are immediately deleted before writing any secret into blockchain storage. As a result, the actual QBER after reconciliation is decreased to 0.48%, below the threshold of 11%.

3. Quantum Proof-of-Stake (QPoS): Quantum Proof-of-Stake (QPoS) employs a new trust measure where validators' worth isn't limited to their economic investments, but also takes into account the quality of their quantum channels — the success rates of QKD reconciliation attempts within recent blocks. Such a measure ensures that attacks on the channel that reduce its efficiency (e.g. photon splitting or intercept-resend attacks) aren't economical and naturally benefit the validators with reliable quantum hardware.

4. QuantumTrust Significantly Outperforms Other Schemes on all Performance Measures: As shown by quantitative evaluation results, QuantumTrust achieves throughput of 1,245 TPS – a performance gain of 46% over any post-quantum blockchain alone and 522% over existing quantum-key distributed blockchains. The delay until finalization is improved by 62% relative to conventional susceptible systems, and attack detection rate (99.8%) outshines all others (second place IBM layered QKD-BC with 91%).

5. Scalability and Practicality are Possible without Compromising on Security: Unlike the presumption that quantum-resistant systems will always be slower, QuantumTrust achieves more than 1,100 TPS even when having 150 live validator nodes. The storage costs associated with QKD reconciliation data are just 8.4% of total block size, while the classical channel bandwidth needs remain below 120 kbps per node.

Limitations and Future Directions:

The weaknesses in our work are the following. Firstly, our simulation framework despite being realistic in terms of noise injection is not able to take into account all the practical limitations inherent to QKD devices (such as detector dead times, afterpulsing, or temperature-related dark counts). Secondly, the QPoS scheme based on channel fidelity can be prone to the "fidelity griefing" attack when the attacker injects noise to decrease the validation score for their competitors. Thirdly, due to the distance limitations of QKD systems (≈150 km without trusted relays), our approach cannot be used in practice except for city-sized networks unless the technology of satellite QKD or quantum repeaters is developed.

- Practical Experimentation on QKD Testbeds: Apply QuantumTrust on current quantum networks such as the Barcelona Quantum Network and the SwissQuantum backbone network to obtain practical QBER statistics and key rates with latencies caused by hardware delays.
- Quantum Memory Based Key Generation: Use quantum memory devices (for example, rare-earth ion doped crystals) to decouple the key generation procedure from the time of block creation in the blockchain allowing higher key rates and reduced latencies.
- Compositional Security of Hybrid Quantum Blockchain Protocols: Formalize and prove security of the QuantumTrust hybrid protocol using quantum process calculi (CQP or QPi) considering the problem of concurrent quantum channel attacks.
- Resistance Against Fidelity Griefing: Develop a resilient scoring system based on median fidelity statistics within the sliding window or trimmed mean of the distribution to prevent noise injection attacks during QPoS key agreement.
- Satellite Integration with Quantum Trust for Scalability: Scale up the QuantumTrust model by combining it with the entanglement-based QKD protocol used with low earth orbit satellites (for example, Micius satellite).

To conclude, it can be said that the blockchain technologies used in the finance industry, medicine, and other sectors are on the verge of becoming obsolete when quantum computers become more advanced. The idea to merge the unchangeability of blockchain and information-theoretical safety of quantum cryptography proves itself efficient since we were able to create a protocol that is not only quantum-resistant but also quantum-safe – able to use quantum processes to reveal any interference and protect the network from attacks. This is the intelligence which does not depend on any centralized authority, is impossible to shut down, yet capable of carrying out operations,

authentication, and responding to threats in the environment with the assistance of quantum computers.

REFERENCES

1. Peter W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.
2. Gorjan Alagic, Chen-Mou Bai, and Jonathan Katz, "Post-quantum cryptography for blockchain: A survey and research directions," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1146–1162, 2022.
3. Paula Fraga-Lamas and Tiago M. Fernandez-Carames, "Towards post-quantum blockchain for IoT: Lattice-based signatures and QKD integration," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13245–13260, Aug. 2022.
4. Ashok Kumar, Shalli Rani, and Mohsen Guizani, "A hybrid QKD-blockchain framework for secure data sharing in smart grids," IEEE Transactions on Network Science and Engineering, vol. 10, no. 2, pp. 892–904, Mar.–Apr. 2023.
5. Yulin Gao and Qiang Wang, "Quantum Byzantine agreement with entangled states: Lower complexity bounds for distributed ledgers," npj Quantum Information, vol. 9, no. 1, pp. 15–27, 2023.
6. Manoj Joshi, Bikash Kumar Das, and Soumya Saha, "Comparative performance analysis of NIST post-quantum signature schemes on blockchain smart contracts," Journal of Cryptographic Engineering, vol. 14, pp. 55–70, 2024.
7. Lei Zhang, Hongwei Liu, and Yu Chen, "Continuous-variable QKD integrated with Ethereum testnet for real-time secure key distribution," Quantum Science and Technology, vol. 9, no. 3, art. no. 035012, 2024.
8. Takashi Nakayama and Koji Sasaki, "Side-channel leakage in QKD-blockchain interfaces: Timing attacks on reconciliation protocols," IEEE Transactions on Quantum Engineering, vol. 6, pp. 1–12, 2025.
9. Mahesh R. S. Bavdekar, Jennifer Smith, and Emanuel Knill, "Layered architecture for quantum-resistant blockchain with integrated QKD," IBM Journal of Research and Development, vol. 70, no. 1, pp. 8:1–8:14, Jan.–Feb. 2026.
10. Charles H. Bennett and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical Computer Science, vol. 560, pp. 7–11, Dec. 2014.