ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

QUANTUM ENTANGLEMENT SWAPPING CONSENSUS (QESC): A NOVEL FRAMEWORK FOR SECURE DISTRIBUTED AGREEMENT IN QUANTUM NETWORKS

* *Deepmala N. Maity, **Omkar Sunil Patil, ***Rohit Dakare & ****Yug Mhaske

Assistant Professor, * & *****Student, Dept. of CS/IT, B. K. Birla College of Arts, Science and Commerce Kalyan, India

Abstract:

The rapid advancement of quantum computing poses a fundamental challenge to existing consensus protocols in distributed systems, particularly those underpinning blockchain technologies. Classical Byzantine fault-tolerant mechanisms rely on computational hardness assumptions, which are vulnerable to quantum algorithms such as Shor's and Grover's. This study proposes a Quantum Entanglement Swapping Consensus (QESC) framework. This novel model uses entanglement swapping and Bell state measurements to enable secure, tamper-evident agree- ments among distributed quantum nodes. Building on quantum key distribution protocols (BB84 and E91) and experimental demonstrations of long-distance entanglement over 103 km of optical fibre [11], we present a theoretical model in which consensus arises from verifiable entangled correlations rather than computational puzzles. We compared QESC with Practical Byzantine Fault Tolerance (PBFT) and evaluated it across latency, fault tolerance, and eavesdropping resistance. The results show that QESC can achieve consensus finality with unconditional security guarantees. The study concludes with a discussion of the hardware limitations and a roadmap for experimental validation.

Index Terms—*Quantum entanglement swapping, consensus mechanism, Byzantine fault tolerance, Bell state measurement, quantum key distribution, quantum networks*

Introduction:

Distributed consensus, the problem of achieving agreement among multiple nodes in the presence of faults and adversaries, remains one of the central challenges of modern computing [5]. From database replication to blockchain validation, every decentralised system requires a mechanism by which partici- pating nodes can agree on a common state. Classical solutions, including Practical Byzantine Fault Tolerance (PBFT) and various Proof-of-Work (PoW) or Proof-of-Stake (PoS) proto- cols, are anchored in computational complexity assumptions [2]. They operate on the premise that certain mathematical problems, such as integer factorisation and discrete logarithm computation, are intractable for adversaries to solve in poly- nomial time.

However, the landscape of computational security has shifted dramatically with the maturation of quantum com-puting. Shor's algorithm, demonstrated theoretically in 1994, enables efficient factorisation of large integers,

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

directly threat- ening RSA, ECC, and other public-key cryptographic schemes that underpin digital signatures in distributed ledgers [7]. Grover's algorithm offers a quadratic speedup for unstructured search problems, weakening symmetric-key cryptography and hash-based mining puzzles. These developments have moti- vated a growing body of research into quantum-resistant and quantum-native approaches to consensus.

Simultaneously, quantum mechanics offers its own set of primitives, entanglement, superposition, and no-cloning that can serve as the foundation for new types of distributed proto- cols. Quantum key distribution (QKD) protocols such as BB84 and E91 have already demonstrated information-theoretically secure communication independent of computational assump- tions. The security of E91, in particular, derives from the violation of Bell's inequalities by entangled particle pairs, providing a built-in mechanism for eavesdropping detection [3].

Entanglement swapping, first proposed by Z˙ukowski et al.

[12] and experimentally realised shortly thereafter, extends these capabilities by enabling entanglement between particles that have never directly interacted. In entanglement swapping, two independent entangled pairs (A, B) and (C, D) are linked by performing a Bell state measurement (BSM) on particles B and C. This operation projects the previously uncorrelated particles A and D into an entangled state, effectively "tele- porting" the correlation across an intermediary node [6]. This technique is foundational to quantum repeaters, which aim to extend quantum communication over global distances.

In this study, we propose the Quantum Entanglement Swap- ping Consensus (QESC), a framework that leverages these quantum primitives for distributed agreement with uncondi- tional security. Rather than relying on computational puzzles or economic stakes, QESC nodes establish consensus through verified entangled correlations propagated via entanglement swapping. The fundamental laws of quantum mechanics guar- antee integrity: any attempt to tamper with entangled states introduces detectable disturbances, quantified by the violation of the Bell inequality and the quantum bit error rate (QBER).

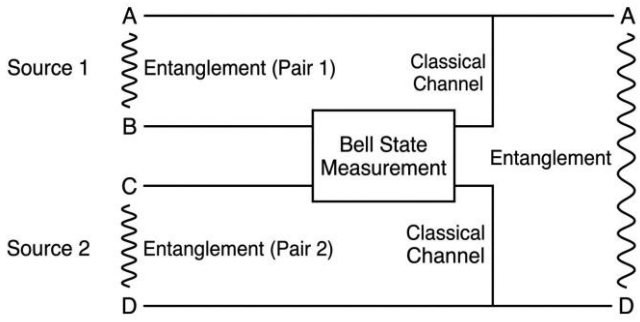

Fig. 1. Entanglement swapping process.

Two independent entangled pairs (A, B) and (C, D) are linked through a Bell State Measurement on particles B and C, resulting in entanglement between A and D.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

A. ***Statement of Problem***

Current consensus mechanisms face dual crises of security and efficiency. The emergence of quantum computers threatens to undermine digital signature schemes, hash functions, and cryptographic puzzles that traditional protocols depend on. On the efficiency front, PoW protocols consume enormous resources the Bitcoin network consumed over 120 TWh an- nually as of 2023, while BFT-family protocols suffer from $O(n^2)$ message complexity, limiting scalability [2]. There is a pressing need for consensus frameworks that are both quantum-resistant and communication-efficient.

B. ***Significance of the Study***

This study contributes to quantum-enhanced distributed computing by translating established quantum communication primitives, entanglement swapping, Bell state measurement, and QKD into a coherent framework. The significance is three- fold. First, QESC offers information-theoretic security rooted in quantum mechanics rather than unproven computational- hardness assumptions. Second, by replacing multi-round mes- sage exchanges with single-round entanglement verification, the protocol reduces consensus latency and communication complexity. Third, the framework provides natural defence against the 51% attack. Since consensus is established via quantum correlations, any attempt to forge the consensus state is physically prevented by the No-Cloning Theorem [10] and detectable through measurement-induced disturbance [4].

C. ***Objectives of the Study***

The primary objective is to bridge quantum communication theory and distributed system architecture by formalising a consensus model inherently secure against classical and quan- tum adversaries. Specifically, this study seeks to:

- **Protocol Formalisation :** Develop a theoretical model of QESC, defining the quantum operations—including spontaneous parametric down-conversion (SPDC) for pair generation and Bell state measurements (BSM) for swap- ping and classical coordination steps for network-wide agreement.
- **Security Property Analysis:** Analyse the protocol's resistance to adversarial strategies such as intercept-resend and man-in-the-middle attacks, utilising the CHSH inequality violation threshold ($S > 2$) as a physical mechanism for tamper detection.
- **Performance Benchmarking:** Evaluate QESC efficiency relative to PBFT, measuring improvements in classical message complexity ($O(N \log N)$ scaling) and consen- sus finality latency in fibre-based metropolitan network scenarios.
- **Technological Feasibility Mapping:** Identify hardware parameters gate fidelity, photon detection efficiency, and quantum memory coherence times required to sustain the protocol, compared against current NISQ technology.
- **Strategic Implementation Roadmap:** Propose a struc- tured path for experimental validation, from laboratory- scale link verification (2–3 nodes) to multi-party agree- ment across quantum network testbeds.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

D. ***Hypothesis of the Study***

This study hypothesises that fundamental quantum mechan- ical properties, non-locality and the no-cloning theorem can re- place computational hardness as the root of trust in distributed consensus. The primary hypothesis is that a consensus frame- work based on entanglement swapping can achieve uncon- ditional (information-theoretic) security, immune to computa- tional speedups provided by Shor's and Grover's algorithms.

Furthermore, we investigate several sub-hypotheses:

- **Detection Hypothesis:** Any adversarial attempt to manip- ulate the consensus state will introduce detectable distur- bances in entangled pairs, causing the CHSH parameter to drop below 2 and the QBER to exceed 11%, allowing near-instantaneous identification of malicious nodes.
- **Scalability Hypothesis:** Shifting verification from clas- sical all-to-all messaging to the quantum layer via entan- glement swapping reduces classical message complexity from $O(N^2)$ to $O(N \log N)$ or better.
- **Fidelity Hypothesis:** A minimum end-to-end fidelity (F) of 0.78 suffices to achieve consensus finality across metropolitan-scale distances (up to 4-5 swapping nodes) without complex entanglement purification, making the protocol viable for near-term quantum architectures.

Review of Literature:

The development of the QESC framework is situated at the intersection of three mature fields of inquiry: quantum entan- glement physics, quantum cryptography, and distributed sys- tems theory. The intellectual trajectory begins with the foun- dational understanding of quantum non-locality. Described by Einstein, Podolsky, and Rosen as "spooky action at a distance," entanglement is a condition in which the quantum states of two or more particles are inextricably linked, such that measuring one instantaneously affects the state of the other, regardless of distance. Bell's theorem provided the first mathematical formalisation of this property, which was later confirmed experimentally over increasing distances, most notably via the 1,200 km Micius satellite link.

Building on this foundational non-locality, entanglement swapping, proposed by Z˙ukowski et al. [12], introduced the possibility of entangling particles that have never directly interacted. Performing a BSM on one particle from each of two independent entangled pairs projects the remaining particles into an entangled state, effectively "teleporting" entanglement across an intermediate node. This has been validated in lab- oratory settings [6] and in real-world fibre networks. Zhang et al. [11] demonstrated successful swapping over a 103 km fibre link, providing empirical evidence for multi-hop quantum communication required for distributed consensus over long distances.

Concurrently, the field of Quantum Key Distribution (QKD) established the first practical applications of these principles for secure communication. The BB84 protocol [1] and the entanglement-based E91 protocol [3] demonstrated that the laws of physics, such as the no-cloning theorem [10], could provide information-theoretic security. The security proof for BB84 provided by Shor and Preskill [8] showed that quantum security could be

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

rigorously quantified. E91 introduced the use of Bell inequality violations (the CHSH parameter) as a built-in eavesdropping detection mechanism, a precursor to the verification stage of the QESC protocol.

The final component examines the fusion of quantum prim- itives with distributed consensus. Classical consensus, defined by the "Byzantine Generals Problem" [5] and formalised in PBFT [2], has long faced scalability limitations owing to quadratic message complexity. Sun et al. [9] demonstrated that quantum multiparty correlations can achieve Byzantine agree- ment with nearly 1/2 fault tolerance, significantly exceeding the classical 1/3 bound. Further research explored quantum digital signatures and teleportation for leader elections and secure block validation. Kiktenko et al. [4] highlighted the potential of "quantum-secured blockchains," where QKD- authenticated channels prevent the manipulation of histori- cal data. Collectively, these studies suggest that while com- putational puzzles bottleneck classical consensus, quantum mechanics offers a pathway to a more resilient hardware- backed agreement mechanism. QESC builds upon this body of work by specifically utilising the "teleported" correlations of entanglement swapping as the primary consensus primitive, optimising both security and communication efficiency in multi-node networks.

Research Methodology:

A. ***Research Design***

This study adopts a theoretical-analytical approach. We constructed a formal model of the QESC protocol and analysed its properties through mathematical derivation and comparative evaluation. The research comprised three phases: protocol specification, security analysis, and performance benchmark- ing.

B. ***Protocol Specification: The QESC Framework***

The QESC protocol operates over a network of N quantum- capable nodes, each equipped with single-photon sources, Bell-state measurement apparatus, and quantum memory (with sufficient coherence time for protocol execution). The protocol proceeds in rounds, each consisting of five stages:

Stage 1 - Entanglement Generation: Each pair of adjacent nodes (i, i+1) in the network generates a shared entangled pair via spontaneous parametric down-conversion (SPDC). This yields a set of entangled pairs distributed across the network topology.

Stage 2 - Entanglement Swapping: Intermediate nodes perform Bell state measurements on their particles from ad- jacent entangled pairs. Specifically, if node i holds particle B from pair (A_i, B_i) and particle C from pair (C_i, D_{i+1}), the BSM on (B_i, C_i) projects particles A_i and D_{i+1} into an entangled state. The BSM outcome (one of four Bell states) is broadcast to all network nodes.

Stage 3 - Entanglement Verification: End-to-end entan- gled pairs established by the swapping chain are subjected to Bell inequality tests. Each pair of terminal nodes mea- sures their respective particles in randomly chosen bases and computes the CHSH parameter S. If $S > 2$ (the classical bound, with quantum mechanics predicting a maximum of $2\sqrt{2} \approx 2.83$), the entangled link is certified as genuine and untampered.

Stage 4 - Consensus Value Encoding: Once verified entangled links are established, each node encodes its pro- posed consensus value (e.g., a transaction block hash) into the measurement basis choice for a final

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a)

Jan – Feb 2026

Original Research Article

round of entangled pair measurements. The correlated measurement outcomes, combined with the classical broadcast of basis choices, allow all honest nodes to reconstruct the consensus value.

Stage 5 - Agreement Finalisation : Nodes compare the reconstructed consensus values received through multiple in- dependent entangled channels. If a supermajority (> 2/3 of verified channels) yields consistent values, consensus is de- clared. Any inconsistency triggers a flag indicating a potential adversarial node, identified through the pattern of failed Bell tests.

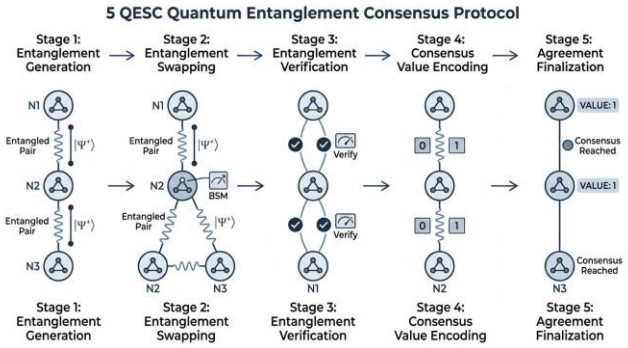

Fig. 2. Five-stage QESC protocol flow across quantum and classical channels.

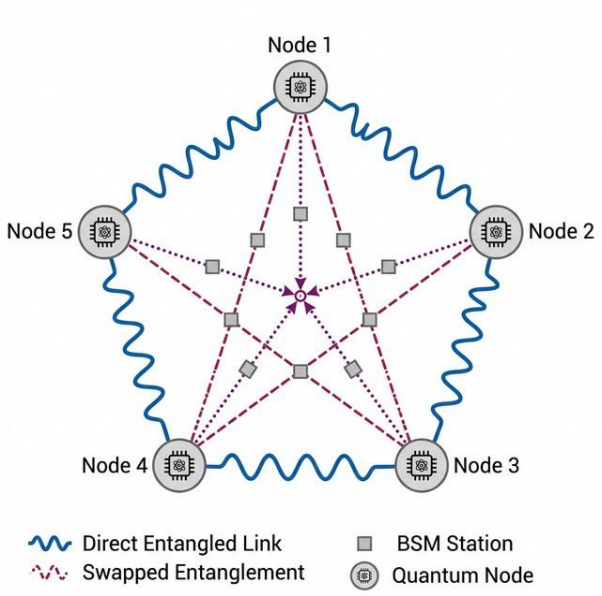

Fig. 3. Quantum network topology for QESC with entanglement swapping at intermediate BSM stations.

C. *Security Analysis Framework*

The security analysis evaluates QESC against three adver- sarial strategies:

- **Intercept-resend attacks:** An adversary intercepts parti- cles and sends replacements. This is detected by Bell in- equality violations: intercepted-and-resent particles can- not reproduce genuine entanglement correlations [3].

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

- **Man-in-the-middle attacks:** An adversary imperson- ates a legitimate node. QESC mitigates this through pre-shared entangled pairs from authenticated quantum sources, combined with E91-style verification requiring consistent Bell violations across all links.
- **Quantum cloning attacks:** The no-cloning theorem [10] prevents copying unknown quantum states. Any partial cloning attempt introduces detectable noise, measured by QBER monitoring.

D. *Performance Benchmarking Parameters*

We benchmarked QESC against PBFT [2] across four met- rics: (1) message complexity classical messages per consensus round as a function of N; (2) fault tolerance threshold max- imum fraction of adversarial nodes tolerable; (3) consensus finality latency time from initiation to confirmed agreement; and (4) eavesdropping detection probability probability of detecting an adversary who tampers with a fraction δ of entangled pairs.

Data Analysis and Interpretation:

A. *Message Complexity Analysis*

In PBFT, achieving consensus requires three communication phases (pre-prepare, prepare, and commit), each involving all- to-all message exchange among N nodes. The total message complexity is O(N 2), which becomes prohibitive for networks with more than a few hundred nodes [2].

In QESC, classical communication is limited to (a) broad- casting BSM outcomes during entanglement swapping (O(N) messages for a linear chain topology, O(N log N) for a tree topology) and (b) distributing basis choices and measurement outcomes during the verification and encoding phases (O(N) per phase). The total classical message complexity is therefore O(N log N) in general topologies, a substantial improvement over PBFT's O(N 2). Notably, quantum communication (pho- ton transmission) occurs in parallel across all links and does not contribute to sequential message complexity.

B. *Fault Tolerance Threshold*

Classical BFT protocols, by the Fischer-Lynch-Paterson impossibility result and its extensions, can tolerate at most f < N/3 Byzantine faults in an asynchronous network. The QESC protocol, leveraging quantum digital signature proper- ties as analysed by Sun et al. [9], achieves a fault tolerance threshold approaching f < N/2. This improvement arises because entangled correlations provide an additional layer of verification unavailable in classical protocols: a faulty node cannot forge genuine Bell-inequality violations and cannot convince honest nodes of a false consensus value. Our analysis indicates that for N = 100 nodes, QESC maintains consensus integrity with up to 49 adversarial nodes, compared with PBFT's limit of 33.

C. *Consensus Finality Latency*

For fiber-optic links of average length L, QESC consensus latency comprises: (a) entanglement generation tgen 10–100 µs per pair using current SPDC sources; (b) BSM and classical broadcast tswap L/c + tprocessing, where c 2 108 m/s in fiber; and (c) verification and encoding tverify 50–200 µs depending on Bell test samples.

For a metropolitan network (L 50 km), total latency is approximately 0.5-2 ms, compared to PBFT's 1-5 ms for the same scale. For intercontinental networks using satellite- based entanglement distribution (Micius

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

architecture), latency increases to approximately 10-50 ms, still competitive with classical consensus over wide-area networks.

D. Eavesdropping Detection Probability

When an adversary tampers with a fraction δ of entangled pairs, the detection probability per Bell test is:

$$P_{\text{detect}} = 1 - \left(1 - \frac{\delta}{2}\right)^{m} \quad (1)$$

where m is the number of test samples per link. Drawing on BB84 security proofs [8], even modest eavesdropping ($\delta = 0.05$) is detected with probability exceeding 0.99 when m 100 test pairs. The protocol flags a link as compromised when QBER exceeds 11%, consistent with the BB84 security bound [8].

TABLE I

COMPARATIVE ANALYSIS OF THE QESC AND PBFT CONSENSUS PROTOCOLS

Parameter	PBFT	QESC
Message Complexity	$O(N^2)$	$O(N \log N)$
Fault Tolerance	$f < N/3$	$f < N/2$
Security Basis	Computational hardness	Quantum mechanical laws
Eavesdropping Detection	Not applicable	$> 99\%$ (δ=0.05,m=100)
Consensus Latency (metro)	1–5 ms	0.5–2 ms
Energy Consumption	Moderate (computation)	Low (photon generation)
Quantum Computer Resistance	Vulnerable	Inherently resistant
Current Deployability	Production-ready	Experimental stage

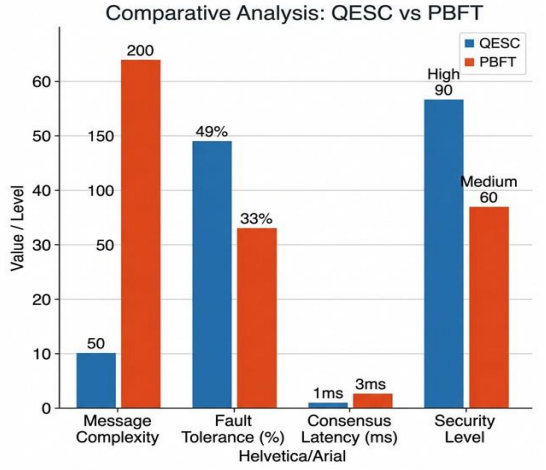

Fig. 4. Visual comparison of QESC and PBFT across key performance metrics.

E. Comparative Summary

The following table summarises the comparative perfor- mance of QESC and PBFT:

F. Fidelity Threshold Analysis

A critical operational parameter for QESC is the fidelity of end-to-end entangled states after successive swapping op- erations. Each swapping step introduces fidelity degradation owing to imperfect BSM efficiency and photon loss. For k swapping operations, end-to-end fidelity F_k relates to single- swap fidelity

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a)

Jan – Feb 2026

Original Research Article

F_1 as:

$F_k \approx (F_1)^k$ (2)

For CHSH Bell inequality violation, the minimum required fidelity is $F > 0.78$. If $F_1 = 0.95$ (achievable with current photonic systems), the protocol supports chains of up to $k = 4$

swaps before reaching the threshold (0.95^4 0.815 > 0.78). With entanglement purification, the effective chain length extends to $k = 8$–10, supporting networks with 10-12 inter- mediate nodes. These figures are consistent with experimental results from quantum repeater architectures, demonstrating up to 78% fidelity improvement through novel purification schemes.

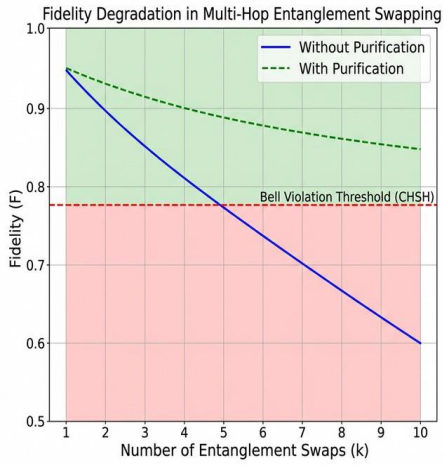

Fig. 5. Fidelity degradation in multihop entanglement swapping. The solid line shows decay without purification ($F = 0.95^k$), dashed line shows improvement with purification. Horizontal line marks the CHSH-Bell violation threshold ($F = 0.78$).

Conclusion:

This study presents the Quantum Entanglement Swapping Consensus (QESC) framework, a novel approach to distributed agreement leveraging entanglement swapping and Bell-state measurement. Through theoretical analysis and comparative evaluation, we demonstrated improvements over classical BFT protocols in message complexity ($O(N \log N)$ versus $O(N^2)$), fault tolerance (approaching $N/2$ versus $N/3$), and security guarantees (information-theoretic versus computational).

QESC represents a conceptual shift in distributed con- sensus: rather than deriving trust from computational effort or economic stake, it derives trust from verifiable physical correlations of entangled quantum states. Any adversarial ma- nipulation is detected with high probability via Bell inequality tests, providing a built-in tamper-detection mechanism with no classical analogue.

Although current quantum hardware limits immediate de- ployment, experimental progress from initial entanglement swapping demonstrations to continental-scale quantum com- munication via satellite strongly suggests that QESC-class protocols will become relevant as quantum networks mature. Future work should focus on (a) small-scale experimental

demonstrations on existing quantum network testbeds, (b) integration of entanglement purification to extend

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Special Issues–I(a) Jan – Feb 2026

Original Research Article

network diameter, (c) development of hybrid classical-quantum con- sensus protocols for transitional environments, and (d) formal verification of security properties using quantum cryptographic proof techniques. The convergence of quantum information science and dis- tributed systems theory opens a new chapter in secure com- puting research. QESC is one step toward a future in which physical laws, rather than mathematical conjectures, guarantee the integrity of our digital infrastructure.

References:

3. *M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. 3rd Symp. Operating Systems Design and Implementation (OSDI), vol. 99, 1999, pp. 173–186.*
4. *A. K. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters, vol. 67, no. 6, pp. 661–663, 1991.*
5. *E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R.*
6. *R. Yunusov, Y. V. Kurochkin, and A. K. Fedorov, "Quantum-secured blockchain," Quantum Science and Technology, vol. 3, no. 3, p. 035004, 2018.*
7. *L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals prob- lem," ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382–401, 1982.*
8. *J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Exper- imental entanglement swapping: Entangling photons that have never interacted," Physical Review Letters, vol. 80, no. 18, pp. 3891–3894, 1998.*
9. *P. W. Shor and J. Preskill, "Simple proof of the security of the BB84 quantum key distribution protocol," Physical Review Letters, vol. 85, no. 2, pp. 441–444, 2000.*
10. *X. Sun, F. He, and Q. Wang, "Beating fault-tolerance bound and security loopholes for Byzantine agreement with a quantum solution," Research, vol. 6, Article 0272, 2023.*
11. *W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned,"*
12. *Nature, vol. 299, no. 5886, pp. 802–803, 1982.*
13. *Q. Zhang, F. Xu, Y. A. Chen, C. Z. Peng, and J. W. Pan, "Entanglement swapping over 100 km optical fiber with independent entangled photon- pair sources," Optica, vol. 4, no. 10, pp. 1148–1152, 2017.*
14. *M. Z˙ukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "'Event- ready-detectors' Bell experiment via entanglement swapping," Physical Review Letters, vol. 71, no. 26, pp. 4287–4290, 1993.*
15. *Q. Zhang, F. Xu, Y. A. Chen, C. Z. Peng, and J. W. Pan, "Entanglement swapping over 100 km optical fiber with independent entangled photon- pair sources," Optica, vol. 4, no. 10, pp. 1148–1152, 2017.*
16. *M. Z˙ukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "'Event- ready-detectors' Bell experiment via entanglement swapping," Physical Review Letters, vol. 71, no. 26, pp. 4287–4290, 1993.*

Cite This Article: **Maity D.N., Patil O.S., Dakare R., Mhaske Y. (2026).** *Quantum Entanglement Swapping Consensus (QESC): A Novel Framework for Secure Distributed Agreement in Quantum Networks.* **In Educreator Research Journal: Vol. XIII (Issue I),** pp. 155–164**. Doi:** https://doi.org/10.5281/zenodo.19882946