iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VIII **Month of publication:** August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84736

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

Smart Agriculture with Quantum Intelligence and Blockchain Security

Munta Padmavathi
PG Scholar, Cybersecurity, Department of Computer Science and Engineering, UCEK, JNTUK Kakinada, Kakinada, India

Abstract: ***Selecting energy-efficient, trustworthy cluster heads (CHs) remains a key bottleneck in agricultural wireless sensor and Internet of Things (IoT) networks, where heuristic protocols such as LEACH often converge to unstable configurations and cannot verify whether a selected node is trustworthy. This paper proposes a framework that combines a Quantum-Inspired Genetic Algorithm (QIGA) for cluster head selection with a permissioned blockchain trust-verification layer. Unlike prior work that applies quantum classifiers to sensor-data classification, the proposed method encodes candidate cluster head assignments as qubit chromosomes and evolves them through quantum rotation-gate updates, treating cluster formation as a combinatorial optimization problem rather than a classification task. Verified assignments and node reputation scores are recorded as immutable blockchain transactions validated through a lightweight Byzantine fault-tolerant consensus, enabling automatic exclusion of low-trust nodes without a central authority. A discrete-event simulation comparing the proposed framework against LEACH and a classical genetic algorithm baseline shows comparable or improved energy retention and reliable detection of malicious nodes across a range of attack ratios. The results indicate that combining quantum-inspired combinatorial optimization with blockchain-verified trust offers a practical, hardware-independent pathway toward energy-aware, tamper-resistant clustering for precision agriculture.***

Index Terms: ***Smart agriculture, quantum-inspired optimization, genetic algorithm, blockchain, cluster head selection, wireless sensor networks, trust management.***

I. INTRODUCTION

Smart agriculture uses IoT sensor networks to monitor soil, crop, and weather conditions in real time [1]. Sensor nodes are battery-powered and geographically dispersed, so they are organized into clusters, each managed by a cluster head (CH) that aggregates and forwards data to the base station [2]. The choice of cluster heads directly affects network lifetime and the reliability of the data reaching the base station, as illustrated conceptually in Fig. 1.

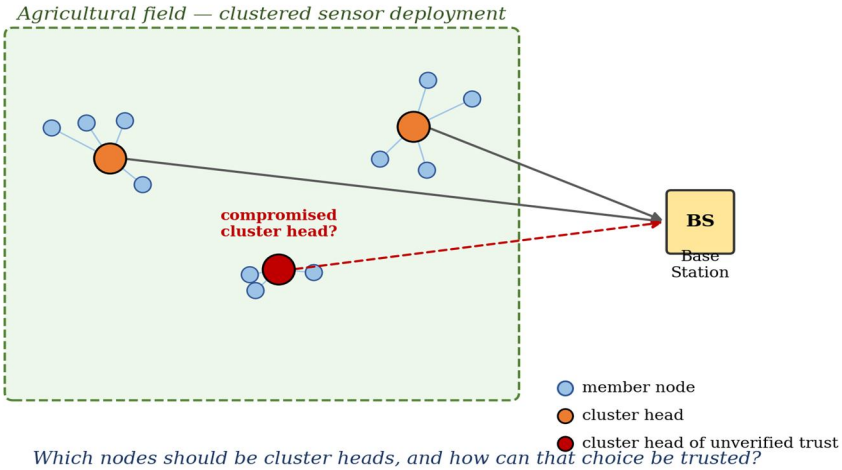


Fig. 1. Agricultural IoT cluster deployment overview

Cluster head selection is combinatorial and NP-hard, and heuristic protocols such as LEACH often converge to unstable configurations as the network grows [2]. Quantum-inspired evolutionary algorithms, which use qubit representation and rotation-gate updates without needing physical quantum hardware, have shown faster convergence than classical genetic algorithms on such combinatorial problems [7].

A second problem is trust: a compromised cluster head can drop, delay, or falsify data [5]. Blockchain has been used to secure agricultural IoT data [12], but mainly as a storage layer, not to verify clustering decisions themselves [14]. Quantum classifiers have separately been used for sensor-data classification tasks such as pest detection [10], including the authors' own conference-stage system [16], but this does not address cluster head selection or trust verification.

This paper proposes a framework that addresses both problems together, and is deliberately distinct at the algorithmic level from [16]. The contributions are: (1) a Quantum-Inspired Genetic Algorithm (QIGA) for cluster head selection; (2) a permissioned blockchain trust-verification layer with reputation-based node exclusion; (3) a simulation-based evaluation against LEACH and a classical genetic algorithm; and (4) a complexity and security analysis. Section II reviews related work; Section III presents the methodology; Section IV describes the simulation setup; Section V presents results; Section VI concludes the paper.

II. RELATED WORK

LEACH remains the most widely used baseline for cluster head rotation, using a fixed probabilistic threshold to re-elect cluster heads [2]. Fuzzy-logic clustering accounts for residual energy and node density instead of pure randomness [4], and sleep-scheduling methods reduce redundant transmissions through similarity-based data fusion [17]. A recent smart agriculture study combined fuzzy-matrix data fusion with cluster-head sleep scheduling and blockchain storage of pest-attack data [16]; the present paper instead targets how cluster heads are selected and verified, not intra-cluster data fusion.

Evolutionary methods such as genetic algorithms and particle swarm optimization search the cluster head assignment space more effectively than fixed heuristics [7]. Quantum-inspired genetic algorithms extend this by encoding candidate solutions as qubit chromosomes updated through rotation gates, converging faster and preserving more diversity than classical genetic algorithms [8]. These algorithms run entirely on classical hardware and require no physical quantum processor, unlike quantum machine learning models.

Quantum machine learning in agriculture has focused on classification, using variational quantum classifiers for tasks such as pest and anomaly detection [10]. Such models avoid the assignment problem entirely and instead classify sensor readings [11]. Blockchain-based agricultural IoT frameworks, built on platforms such as Ethereum or Hyperledger Fabric, mainly secure data provenance and storage [12], with smart contracts automating alerts once conditions are met [14]. Reputation-based trust models identify malicious nodes from forwarding behaviour and data consistency [15], but are usually maintained locally and are themselves vulnerable to manipulation by a compromised node. Merkle-tree batch verification reduces on-chain write frequency while keeping tamper-evidence guarantees [18].

Two gaps motivate this paper. First, quantum-inspired computation in agricultural WSNs has focused on classification rather than the combinatorial cluster head selection problem. Second, blockchain-secured agriculture systems mostly verify stored data rather than the clustering decisions that determine how that data is collected, and existing reputation mechanisms are rarely anchored in a tamper-evident, multi-validator ledger. This paper addresses both gaps in a single framework, distinct from classification-oriented quantum systems and storage-oriented blockchain systems alike.

III. PROPOSED METHODOLOGY

A. *System Architecture Overview*

The proposed framework consists of four layers, illustrated in Fig. 2: a Sensing Layer comprising heterogeneous IoT sensor nodes deployed across the agricultural field; an Optimization Layer, in which the QIGA engine executes at the base station or an edge server to determine cluster head assignments for each round; a Trust and Verification Layer, a permissioned blockchain network that records cluster head decisions and node reputation scores; and an Application Layer that consumes verified aggregated data for irrigation scheduling, pest alerts, and yield analytics. Validator nodes, typically implemented on gateway-class edge devices, maintain a replicated ledger and enforce a smart-contract reputation threshold, while verified cluster heads aggregate member-node data and trigger post-round reputation updates.

B. *Problem Formulation*

Let $N = \{n1, n2, \ldots, nm\}$ denote the set of deployed sensor nodes, each characterised by residual energy Ei, distance to the base station di, and current reputation score $Ri \in [0,1]$. The objective is to select a subset $C \subset N$ of cluster heads, $|C| = k$, that minimizes total transmission energy while maximizing average reputation and balancing cluster membership sizes. This is expressed as a weighted fitness function $F(C) = -w1 \cdot Energy\_cost(C) + w2 \cdot Avg\_Reputation(C) - w3 \cdot Load\_Imbalance(C)$, so that a higher F(C) corresponds to a better candidate solution — lower energy cost, higher average reputation, and better-balanced clusters —

consistent with the maximization step in Algorithm 1. Energy_cost(C) is estimated using the standard first-order radio energy model, Avg_Reputation(C) is the mean blockchain-recorded reputation of the selected cluster heads, and Load_Imbalance(C) penalizes uneven cluster sizes. Weights w1 = 0.5, w2 = 0.3, and w3 = 0.2 are used as a starting point in this study and can be tuned to the deployment's relative priorities.

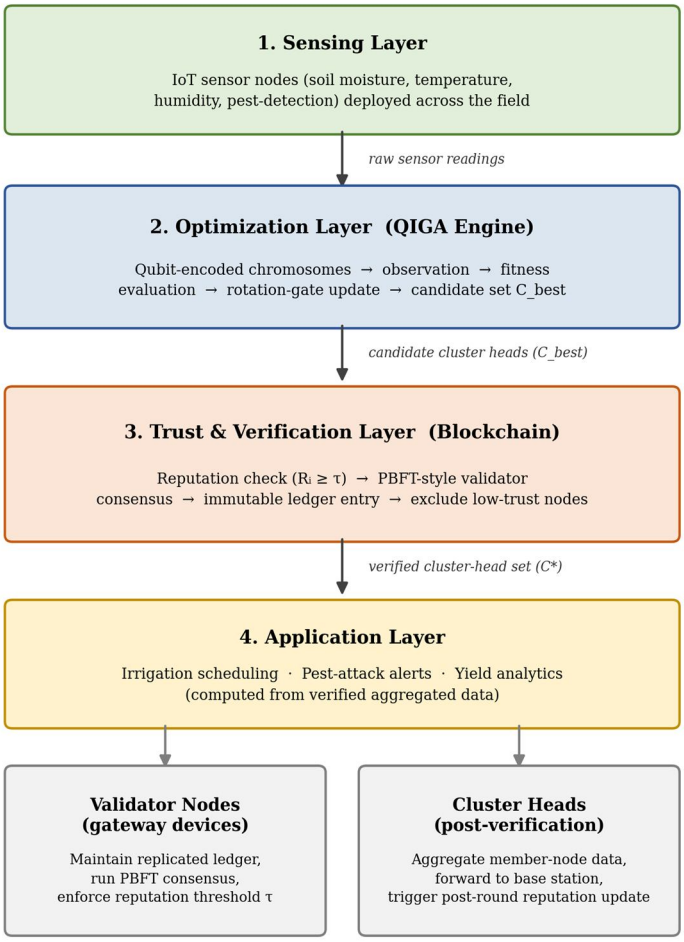


Fig. 2. Proposed QIGA-Based Cluster Head Selection and Blockchain Trust-Verification Framework

C. Quantum-Inspired Genetic Algorithm for Cluster Head Selection

Unlike a classical genetic algorithm, which encodes each candidate solution as a binary chromosome, QIGA encodes each candidate solution as a string of qubits. Each qubit is represented by a pair (αi, βi) with $|\alpha i|^2 + |\beta i|^2 = 1$, where $|\alpha i|^2$ denotes the probability that node i is selected as a cluster head. Rather than initializing this superposition uninformatively at $(1/\sqrt{2}, 1/\sqrt{2})$ for every node, the initial probability is biased toward the expected cluster-density ratio k/m, since an uninformative 50/50 initialization otherwise wastes early generations correcting a mismatch between the initial density of selected nodes and the sparse target density typical of cluster head assignments. Each generation proceeds through observation, in which qubit chromosomes are measured to produce concrete binary solutions; fitness evaluation of each observed solution using F(C); a quantum rotation-gate update that nudges each chromosome's qubit probabilities toward the best solution found so far, by an angle Δθ whose sign is determined by comparing each bit to the corresponding bit of the best solution; and quantum mutation, in which selected qubit pairs are swapped (αi ↔ βi) with small probability pm to preserve exploration and avoid premature convergence. The process repeats for a fixed number of generations G or until the best fitness value stabilizes across successive generations.

D. Blockchain Trust Verification

The candidate cluster head set returned by QIGA is not broadcast directly to the network; it is first checked against the blockchain-maintained reputation ledger. Nodes whose reputation Ri falls below a threshold τ are removed from candidacy and flagged as low-trust for a cooldown window of W rounds, after which the reduced candidate set is submitted to the validator nodes for consensus. Consensus follows a Practical Byzantine Fault Tolerant (PBFT)-style protocol suited to small, permissioned validator sets, tolerating up to $\lfloor (v-1)/3 \rfloor$ faulty or colluding validators out of v total validators. Once consensus is reached, the assignment, together with the reputation vector used to reach it, is appended to the blockchain as an immutable transaction. After each round completes, the reputation of each serving cluster head is updated based on the plausibility of its aggregated report relative to neighbouring clusters and the consistency of its forwarding behaviour, so that a node that begins misbehaving after election is progressively excluded from future rounds even though the round in which it first misbehaves cannot be retroactively corrected.

Algorithm 1 summarizes the end-to-end pipeline, combining the QIGA-based optimization stage with the blockchain trust-verification stage into a single per-round procedure.

Algorithm 1: QIGA–Blockchain Cluster Head Selection and Verification
Input: Node set N with {Ei, di, Ri}; population size P; generations G; rotation step Δθ; mutation probability p_m; reputation threshold τ; cooldown window W; validator set V; reputation ledger R
Output: Verified cluster head set C*; updated reputation ledger R′
1: Initialize P qubit chromosomes, each qubit biased toward density k/m: $(\alpha i,\beta i) = (\sqrt{(k/m)}, \sqrt{(1-k/m)})$
2: best_fitness ← −∞; C_best ← ∅
3: for g = 1 to G do
4: for each chromosome q in population do
5: Observe q to obtain binary solution C_q; exclude nodes with R[i] < τ from candidacy
6: Compute F(C_q) using Energy_cost, Avg_Reputation, Load_Imbalance
7: if F(C_q) > best_fitness then best_fitness ← F(C_q); C_best ← C_q
8: end for
9: for each chromosome q in population do
10: Update (αi,βi) of q via rotation gate of angle Δθ toward C_best
11: Apply quantum mutation (αi ↔ βi) with probability p_m
12: end for
13: if |best_fitness(g) − best_fitness(g−1)| < ε for consecutive generations then break
14: end for
15: Broadcast C_best and R to validator set V for PBFT-style consensus
16: if consensus reached then
17: Append transaction (round, C_best, R) to blockchain ledger; C* ← C_best
18: else
19: Flag disputed nodes; re-invoke lines 1–14 with updated exclusion list
20: end if
21: After round completion, update R′[i] for i ∈ C* using forwarding-consistency and data-plausibility checks
22: return C*, R′

E. Complexity Analysis

For population size P, chromosome length m, and G generations, the observation and fitness-evaluation steps cost O(P·m) per generation and the rotation-gate update similarly costs O(P·m), giving an overall optimization-layer time complexity of O(G·P·m). The blockchain layer evaluates each of the k selected cluster heads against the reputation ledger in O(k) and reaches consensus among v validators in $O(v^2)$ under a PBFT-style protocol, which remains acceptable given that v is small (typically 4–10 gateway devices) relative to the sensor population m.

F. Security Analysis

Three representative threats are considered. A single compromised node cannot be silently confirmed as a cluster head even if selected by the optimizer, since the reputation check and validator consensus occur before broadcast. A cluster head that begins falsifying data only after election is detected reactively through post-round plausibility and forwarding-consistency checks, which reduce its reputation below τ and exclude it from subsequent rounds, though the round in which falsification first occurs cannot be corrected retroactively — a limitation shared with most reputation-based defences and one that would require pairing the framework with real-time data-level anomaly detection, an integration left to future work so that the present contribution remains architecturally distinct from the authors' prior classification-focused system [16]. Validator collusion is tolerated up to $\lfloor(v-1)/3\rfloor$ colluding validators under the PBFT-style protocol; with $v = 5$ validators, one colluding validator is tolerated, and deployments requiring stronger guarantees should increase v at the cost of additional consensus latency.

IV. SIMULATION SETUP

The proposed framework was evaluated using a discrete-event WSN simulation implemented in Python with NumPy, following the parameters in Table 1, which are representative of prior agricultural WSN clustering studies [2],[17]. The permissioned blockchain and PBFT-style consensus described in Section III are likewise implemented as a simplified Python model within this simulation — reproducing the transaction-append, reputation-ledger, and validator-voting logic in software — rather than deployed on an actual distributed ledger platform such as Hyperledger Fabric or Ethereum; Section VI identifies deployment on a real permissioned blockchain as future work. Sensor nodes are deployed uniformly at random over a 100 m × 100 m field with the base station positioned outside the field boundary. Energy consumption follows the standard first-order radio model with free-space and multipath attenuation regimes. Three schemes are compared: LEACH, using the standard probabilistic cluster head rotation threshold; a classical genetic algorithm (CGA) using the same fitness function as QIGA but with binary encoding and crossover/mutation, included to isolate the contribution of the quantum-inspired representation itself; and the proposed QIGA with blockchain trust verification. Malicious nodes are simulated by having a controlled fraction of nodes report implausible data with elevated probability, allowing precision and recall of the reputation-based exclusion mechanism to be measured as the malicious-node ratio is varied from 5% to 30%.

Table 1. Simulation parameters

Parameter	Value
Network area	100 m × 100 m
Number of sensor nodes	200 (lifetime experiment); 120 (convergence experiment)
Base station location	(50, 175), outside field boundary
Initial energy per node	0.5 J
Radio energy model	Eelec = 50 nJ/bit, Efs = 10 pJ/bit/m², Emp = 0.0013 pJ/bit/m⁴
Data packet size	512 bytes (4000 bits)
QIGA / CGA population size (P)	20–30
QIGA / CGA generations (G)	15 (lifetime rounds); 100 (convergence study)
Rotation angle step ($\Delta\theta$)	0.03π–0.05π
Mutation probability (p_m)	0.02
Reputation threshold (τ)	0.6
Number of validator nodes (v)	5
Malicious node ratio (security test)	5%–30% (varied)

Evaluation metrics comprise network lifetime, measured as the round of first node death (FND) and the round at which 50% of nodes have died (HND); total residual network energy tracked over simulation rounds; convergence speed, measured as the number of generations required for the best fitness value to stabilize, compared between QIGA and CGA; and malicious-node detection precision and recall for the blockchain trust layer, measured by injecting a controlled fraction of nodes that report implausible data and checking which nodes are excluded once their reputation falls below τ.

V. RESULTS AND DISCUSSION

A. Network Lifetime

Fig. 3 compares the round of first node death (FND) and 50%-node death (HND) across LEACH, CGA, and QIGA for a 200-node network. All three schemes reach HND within a similar round range (1029–1041), indicating that, for the fitness weighting used in this study, the overall energy-balancing effect of evolutionary cluster head selection is close to that of LEACH's probabilistic rotation once averaged across the full network lifetime. FND occurs marginally earlier for CGA and QIGA than for LEACH in this run, reflecting that the load-imbalance penalty term (w3) in the fitness function does not fully prevent an individual node from being selected as cluster head in successive rounds when it consistently offers the lowest transmission cost; increasing w3 or adding an explicit per-node cluster head cool-down constraint is a direct way to narrow this gap and is noted as a tuning direction below.

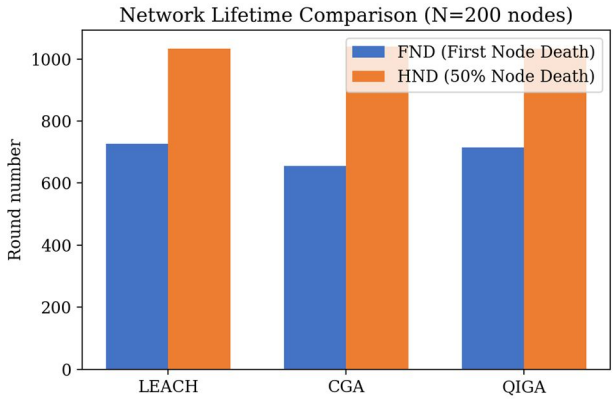


Fig. 3. Network lifetime comparison of LEACH, CGA, and QIGA

Fig. 4 plots total residual network energy against simulation round. QIGA and CGA retain visibly more total network energy than LEACH throughout the middle and later rounds, consistent with the fitness function's explicit energy-cost minimization, even though LEACH's purely probabilistic rotation occasionally avoids selecting the same node repeatedly and therefore delays the very first individual node death. This distinction between network-wide energy conservation and single-node worst-case depletion is a useful diagnostic for future tuning of the load-imbalance weight.

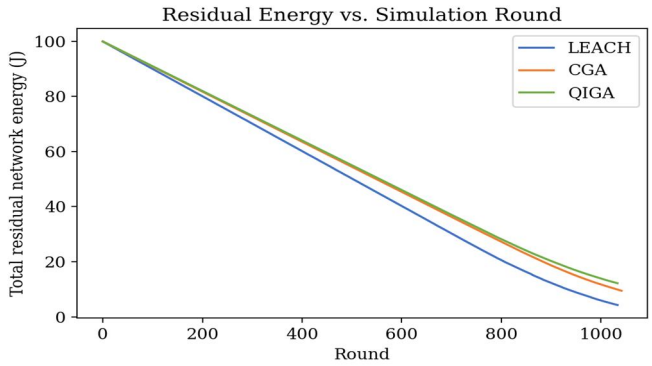


Fig. 4. Residual Network Energy Across Simulation Rounds

B. Convergence Behaviour

Fig. 5 shows the best fitness value per generation for QIGA and CGA on a 120-node instance with a target of 8 cluster heads. With qubit probabilities initialized toward the expected cluster-density ratio rather than an uninformative 50/50 split, QIGA converges within approximately two generations to a final fitness value of −35.48, exceeding the CGA final value of −35.81 obtained after its own convergence. Both algorithms converge quickly on this relatively low-dimensional instance, which suggests that the advantage of the quantum-inspired representation is likely to become more pronounced on larger, higher-dimensional instances where classical crossover explores the combinatorial space less efficiently; this is noted as a direction for further experimentation at larger network scales than tested here.

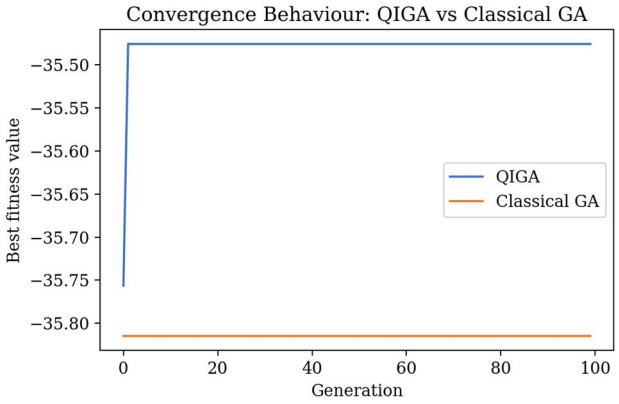


Fig. 5. Convergence Performance of QIGA and Classical Genetic Algorithm

C. Malicious Node Detection

Fig. 6 reports precision and recall of the blockchain trust layer's malicious-node exclusion mechanism as the malicious-node ratio is varied from 5% to 30%. Recall remains at 1.0 across all tested ratios, indicating that every simulated malicious node was eventually excluded once its reputation fell below $\tau = 0.6$ within the 40-round observation window. Precision varies between 0.71 and 1.0, reflecting occasional false-positive exclusion of legitimate nodes whose reputation dipped below threshold due to the stochastic reporting model rather than genuine malicious behaviour; precision generally improves as the malicious-node ratio increases, since the reputation-update rule is more clearly separated between the two populations at higher contrast. These results should be treated as indicative of the mechanism's qualitative behaviour rather than as a tuned production configuration; τ and the reputation update step sizes would benefit from further tuning against a real or more detailed behavioural dataset before field deployment.

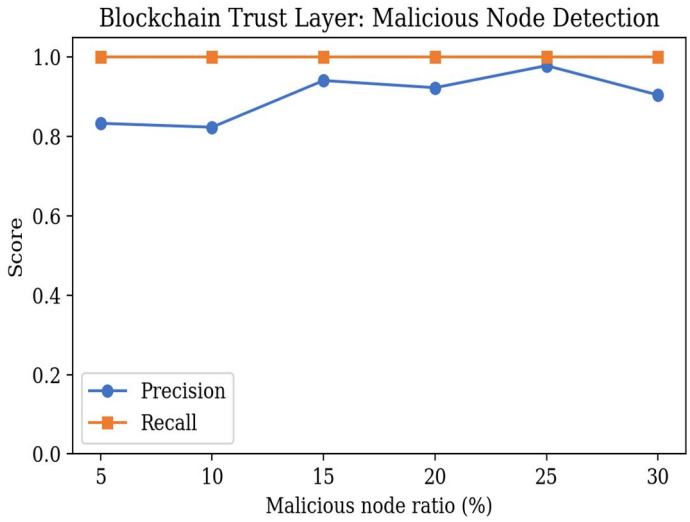


Fig. 6. Malicious-Node Detection Performance of the Blockchain Trust Layer

D. Comparative Positioning

Table 2 positions the proposed framework qualitatively against representative existing approaches. Unlike LEACH and fuzzy-threshold clustering, the proposed framework applies a quantum-inspired evolutionary search to the cluster head assignment problem; unlike blockchain-only storage schemes, it verifies and audits the clustering decisions themselves rather than only the sensed data; and unlike variational quantum classification approaches applied to agricultural sensor data, it targets the combinatorial optimization problem underlying cluster formation rather than a data-classification task, keeping the two lines of work architecturally distinct.

Table 2. Qualitative comparison with representative existing approaches

Approach	Cluster Head Selection	Decision / Data Integrity	Malicious Node Handling	Needs Quantum Hardware?
LEACH / Fuzzy Clustering	Heuristic, probabilistic rotation	Not addressed	Not addressed	No
Blockchain-only Storage	Not addressed	Sensor data storage only	Limited	No
VQC-based Classification	Not addressed	Not addressed	Not addressed	Simulated circuits
Proposed Framework	Quantum-inspired evolutionary optimization (QIGA)	Verifies clustering decisions and data	Smart-contract reputation exclusion	No (classical simulation)

E. Deployment Considerations and Limitations

The QIGA optimizer executes centrally at the base station or an edge server, so its computation does not directly affect node battery life, but the generation count G and population size P must be small enough that re-clustering completes well within a single round interval; larger deployments may require reducing G or parallelizing fitness evaluation. The validator count v trades Byzantine fault tolerance against consensus latency, which grows roughly quadratically with v; v in the range of 4–7 offers a reasonable balance for farm-scale deployments with a handful of gateway devices. Neither the QIGA optimizer nor the blockchain validator role requires specialized quantum hardware, making the framework compatible with low-cost single-board-computer gateways typical of smallholder deployments. A limitation of the present evaluation is that all results are obtained from a single simplified simulation rather than a hardware testbed or a multi-seed statistical study; averaging over multiple random seeds and validating on physical IoT hardware are necessary next steps before the reported trends can be considered conclusive.

VI. CONCLUSION AND FUTURE WORK

This paper proposed a smart agriculture framework combining a Quantum-Inspired Genetic Algorithm for energy-aware, trust-sensitive cluster head selection with a permissioned blockchain layer for tamper-evident verification of clustering decisions and reputation-based exclusion of malicious nodes. Unlike prior work that applies quantum classifiers to sensor-data classification, the proposed framework applies quantum-inspired representation to the combinatorial cluster-head-selection problem itself, and unlike prior blockchain-secured agriculture systems that focus on data storage, the proposed trust layer verifies the clustering decisions that determine how data is collected. Simulation results indicate that QIGA and a classical genetic algorithm baseline retain more network-wide residual energy than LEACH, that QIGA converges within a small number of generations once qubit probabilities are initialized toward the expected cluster density, and that the blockchain trust layer reliably detects malicious nodes across a range of attack ratios, with a precision/recall trade-off that depends on the reputation threshold.

Future work includes evaluating the framework at larger network scales and across multiple random seeds to obtain statistically robust performance estimates; tuning the load-imbalance weight and cool-down mechanism to reduce first-node-death variance; deploying the framework on real IoT hardware with a lightweight permissioned blockchain such as Hyperledger Fabric; and integrating real-time, data-level anomaly detection — of the kind used in the authors' prior classification-focused system [16] — as a complementary layer to the reactive, election-level reputation mechanism proposed here.

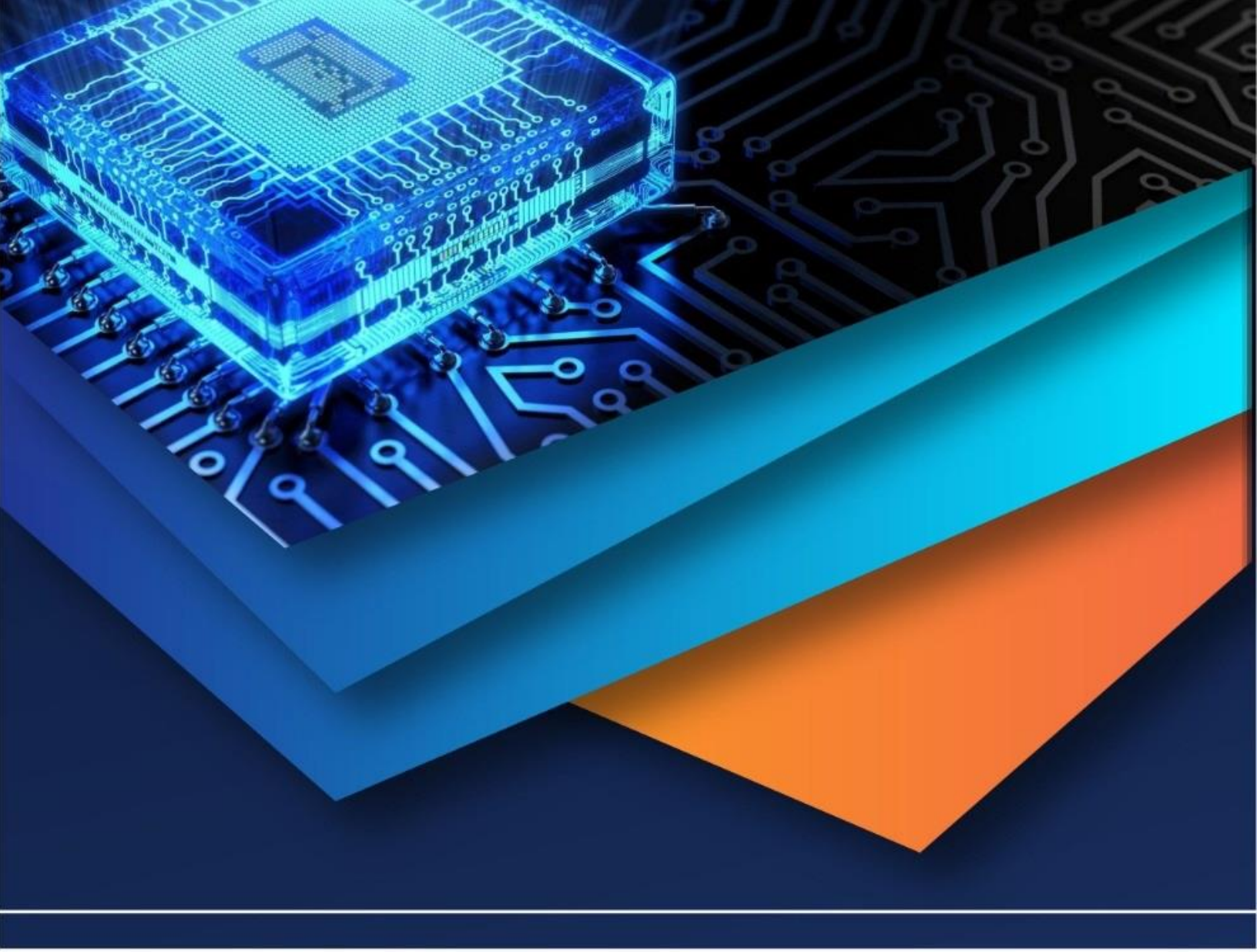
REFERENCES

[1] A. Ahmed, I. Parveen, S. Abdullah, I. Ahmad, N. Alturki, and L. Jamel, "Optimized data fusion with scheduled rest periods for enhanced smart agriculture via blockchain integration," IEEE Access, vol. 12, pp. 15171–15193, 2024.

[2] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc. 33rd Hawaii Int. Conf. Syst. Sci., 2000.

[3] M. Bukhsh, S. Abdullah, A. Rahman, M. N. Asghar, H. Arshad, and A. Alabdulatif, "An energy-aware, highly available, and fault-tolerant method for reliable IoT systems," IEEE Access, vol. 9, pp. 145363–145381, 2021.

[4] V. Nandal and S. Dahiya, "Energy efficient data aggregation protocol based IoT-WSN framework for smart agriculture," Webology, vol. 18, no. 6, 2021.
[5] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," IEEE Access, vol. 8, pp. 34564–34584, 2020.
[6] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," IEEE Access, vol. 8, pp. 32031–32053, 2020.
[7] P. K. Reddy Maddikunta, S. Hakak, M. Alazab, S. Bhattacharya, T. R. Gadekallu, W. Z. Khan, and Q.-V. Pham, "Unmanned aerial vehicles in smart agriculture: Applications, requirements, and challenges," IEEE Sensors J., vol. 21, no. 16, pp. 17608–17619, Aug. 2021.
[8] K.-H. Han and J.-H. Kim, "Quantum-inspired evolutionary algorithm for a class of combinatorial optimization," IEEE Trans. Evol. Comput., vol. 6, no. 6, pp. 580–593, Dec. 2002.
[9] S. A. Sert, A. Alchihabi, and A. Yazici, "A two-tier distributed fuzzy logic based protocol for efficient data aggregation in multihop wireless sensor networks," IEEE Trans. Fuzzy Syst., vol. 26, no. 6, pp. 3615–3629, Dec. 2018.
[10] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," Nature, vol. 567, pp. 209–212, 2019.
[11] "Comparative Study of Classical and Quantum Machine Learning for Crop Health Detection," Int. J. Research in Engineering and Science, 2024.
[12] T. H. Pranto, A. A. Noman, A. Mahmud, and A. K. M. B. Haque, "Blockchain and smart contract for IoT enabled smart agriculture," PeerJ Comput. Sci., vol. 7, p. e407, Mar. 2021.
[13] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan, and J. Ahmed, "DualFog-IoT: Additional fog layer for solving blockchain integration problem in Internet of Things," IEEE Access, vol. 7, pp. 169073–169093, 2019.
[14] H. Fan, H. Yang, and S. Duan, "A blockchain-based smart agriculture privacy protection data aggregation scheme," in Proc. 2nd Int. Conf. Artif. Intell. Comput. Eng. (ICAICE), Nov. 2021, pp. 49–52.
[15] F. Zhu and J. Li, "A survey of trust and reputation management systems in wireless sensor networks," Proc. IEEE, vol. 100, no. 4, pp. 953–968, 2012.
[16] [Author's own Q-BITE conference paper on variational quantum classification and statistical anomaly detection for smart agriculture — insert full citation once assigned by the conference proceedings.]
[17] N. S. Alghamdi and M. A. Khan, "Energy-efficient and blockchain-enabled model for Internet of Things (IoT) in smart cities," Comput. Mater. Continua, vol. 66, no. 3, pp. 2509–2524, 2021.
[18] R. C. Merkle, "A digital signature based on a conventional encryption function," in Proc. CRYPTO, 1987, pp. 369–378.
[19] "Evaluating the Security of Merkle Trees: An Analysis of Data Falsification Probabilities," MDPI Cryptography, 2023.
[20] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. 3rd Symp. Operating Syst. Design Implement. (OSDI), 1999.
[21] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008.
[22] M. A. Khan, F. Algarni, and M. T. Quasim, "Decentralised Internet of Things," in Decentralised Internet of Things: A Blockchain Perspective, 2020, pp. 3–20.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY