



Paper Type: Original Article

Quantum-Classical Hybrid Architectures for Blockchain and Contextual AI

Eman Sayed ^{1,*}  and Sara M. Mosaad ² 

¹ Department of Decision Support, Faculty of Computers and Informatics, Zagazig University, Harayah Raznah, Zagazig 44519, Sharqiyah, Egypt; essayed@fci.zu.edu.eg.

² Department of Information System, Faculty of Commerce and Business, Helwan University, Ain Helwan, Cairo 11795, Egypt; sara.mosaad@commerce.helwan.edu.eg.

Received: 13 Jan 2025

Revised: 01 Apr 2025

Accepted: 30 Jul 2025

Published: 02 Aug 2025

Abstract

The convergence of quantum computing, blockchain technologies, and contextual artificial intelligence offers a transformative opportunity to meet the growing demands of secure, adaptive, and decentralized systems. However, most existing approaches focus on isolated or pairwise integrations of these technologies and do not provide a comprehensive architectural synthesis. This paper introduces a quantum-classical hybrid architecture that unifies quantum-enhanced cryptographic processing, blockchain-based trust mechanisms, and context-aware AI reasoning within a modular and interoperable system design. The proposed architecture consists of four interoperable layers: a quantum layer for cryptographic functions and computational enhancements, a classical layer for coordination and orchestration, a contextual AI layer for real-time inference and adaptation, and a blockchain layer for transparent and tamper-resistant record keeping. A key innovation of this architecture lies in its use of contextual AI models, such as transformers, to interpret dynamic environments and guide decisions across quantum and blockchain components. This paper presents use cases in healthcare, finance, and supply chain domains which are theoretical, yet based on realistic challenges and operational demands. These scenarios illustrate how each layer of the architecture contributes to practical decision-making, enhancing the feasibility of future deployments. The paper also discusses implementation challenges such as quantum hardware limitations, integration complexity, and data privacy, and outlines a trajectory for advancement through quantum middleware, explainable AI, and post-quantum cryptographic integration. By aligning emerging technologies within a unified structure, this study offers a forward-looking blueprint for secure, intelligent, and context-aware systems in decentralized environments.

Keywords: Quantum Computing; Blockchain; Contextual Artificial Intelligence; Hybrid Architecture; Smart Contracts; Post-Quantum Security.

1 | Introduction

The accelerating complexity of digital ecosystems, driven by vast data generation, real-time interactions, and increasing demands for trust and security, has revealed the limitations of traditional computing paradigms. Classical architectures are often constrained in their ability to process large-scale data securely, adapt to dynamic environments, and support decentralized systems. As a result, there is growing interest in integrating emerging technologies such as quantum computing, blockchain, and contextual artificial intelligence to form more resilient and intelligent architectures.



Corresponding Author: essayed@fci.zu.edu.eg



<https://doi.org/10.61356/j.mawa.2025.8572>



Licensee **Multicriteria Algorithms with Applications**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

Quantum computing introduces a fundamentally new model of computation based on superposition, entanglement, and quantum interference. It offers the potential to solve problems intractable for classical systems, particularly in the domains of cryptography, optimization, and simulation [1, 2]. As quantum systems evolve, hybrid approaches that integrate discrete- and continuous-variable modalities have become essential for implementing scalable quantum information protocols [3]. Simultaneously, blockchain technology has evolved as a foundational pillar for trust in decentralized systems. It provides tamper-resistant ledgers, transparent transaction histories, and programmable smart contracts, making it suitable for domains where data integrity and autonomy are paramount [4]. However, blockchains face scalability and long-term security limitations, especially in the context of quantum threats to classical cryptography [5].

Contextual Artificial Intelligence has emerged as a key enabler of adaptive and interpretable decision-making across complex and dynamic environments. These systems leverage transformer-based architectures and attention mechanisms to model situational awareness, personalize responses, and adapt to evolving data in real time. While contextual AI focuses on adjusting behavior based on environment and input conditions, explainable AI serves a complementary role by making those decisions transparent and understandable to human users. The demand for both capabilities is increasingly evident in sectors such as healthcare, finance, and smart manufacturing, where AI must not only act intelligently but also maintain reliability, traceability, and user trust [6, 7]. Achieving this level of dependability requires contextual AI systems to operate within verifiable and secure infrastructures. This reinforces the importance of aligning contextual AI with blockchain-backed trust and quantum-enhanced cryptographic protections in hybrid architectures designed for next-generation intelligent systems.

While the individual benefits of quantum computing, blockchain, and contextual AI are well recognized, their integration remains underexplored. Most existing research focuses on pairwise combinations, such as quantum-secured blockchains or AI-enhanced smart contracts, without addressing how these technologies can be unified into a single interoperable framework. This paper addresses this gap by proposing a quantum-classical hybrid architecture that integrates quantum-enhanced cryptographic processing, blockchain-based decentralization, and context-aware AI within a multi-layered, modular system. Although the use cases examined are theoretical, they are modeled on realistic challenges in healthcare, finance, and supply chains. These scenarios provide a practical lens through which to assess the architectural components and their interrelations.

The contribution of this work lies in presenting a novel quantum-classical hybrid architecture that unifies quantum-enhanced cryptographic processing, blockchain-based decentralization, and context-aware AI within a modular, interoperable system. Unlike prior studies that examine these technologies in isolation or pairwise combinations, this framework offers a triadic integration supported by a layered architectural design. Although the use cases presented are theoretical, they are modeled on realistic challenges across healthcare, finance, and supply chains, offering a practical lens through which to assess component interactions and deployment feasibility. By addressing both technical interoperability and forward-looking integration strategies, this study provides a foundation for advancing hybrid computing in both academic and applied innovation contexts.

2 | Technical Foundations

This section presents the core technologies that form the foundation of the proposed hybrid architecture. The discussion focuses on quantum computing, blockchain, and contextual artificial intelligence, each examined in terms of fundamental principles, current capabilities, known limitations, and relevance to system-level integration.

2.1 | Quantum Computing

Quantum computing is a novel computational paradigm that leverages the principles of superposition, entanglement, and quantum interference to perform operations on data. Quantum computing leverages the

principles of quantum mechanics, such as superposition and entanglement, to perform calculations that are infeasible for classical systems. Unlike classical bits that represent binary states, quantum bits (qubits) can exist in a superposition of states, enabling parallelism at the quantum level. This allows quantum algorithms to explore large solution spaces more efficiently, particularly in problems involving combinatorics, optimization, cryptography, and machine learning.

Qubits are manipulated using quantum gates, which are unitary transformations preserving probability distributions. These gates form the building blocks of quantum circuits, which can amplify desired solutions and suppress incorrect ones through interference. Although the output of quantum algorithms is probabilistic, repeated runs increase confidence in the results. Quantum computing holds potential for exponential speedup in select domains but remains limited by hardware noise, error correction requirements, and data encoding challenges.

Fundamentally, quantum computation operates in a complex Hilbert space where the state of a qubit is represented as a linear combination of basis states. The evolution of quantum states is governed by unitary transformations, which ensures reversibility and probability conservation. Single-qubit gates such as the Hadamard, Pauli-X, and phase gates, along with multi-qubit gates such as the Controlled-NOT and SWAP, enable construction of universal quantum circuits capable of solving classically intractable problems. Algorithms such as Grover's algorithm, for unstructured search, and Shor's algorithm, for prime factorization, demonstrate the theoretical advantage of quantum computation in database search and integer factorization, respectively [8]. These foundational techniques highlight the potential of quantum systems to disrupt classical cryptographic and optimization methods [9].

In the context of secure and decentralized architectures, quantum computing introduces advanced capabilities for cryptographic processing. Quantum Key Distribution (QKD) protocols, for example, enable information-theoretic secure communication through principles of quantum measurement and no-cloning. These protocols are particularly significant for protecting sensitive data against the threats posed by quantum decryption of classical cryptographic schemes [10]. Moreover, hybrid models that combine quantum subroutines with classical control loops are emerging as practical approaches to harness quantum advantages on near-term noisy intermediate-scale quantum (NISQ) hardware [11, 12].

Within the proposed hybrid architecture, quantum computing functions as the foundational layer responsible for cryptographic primitives, secure randomness generation, and optimization tasks that benefit from quantum speedup. These capabilities complement the classical orchestration layer and strengthen the overall trust framework when integrated with blockchain-based consensus and contextual AI inference. By leveraging quantum-enhanced modules for privacy preservation, secure communication, and probabilistic inference, the system achieves computational robustness that classical architectures alone cannot provide.

2.2 | Blockchain and Decentralized Trust Infrastructures

Blockchain is a distributed ledger technology designed to ensure data immutability, consensus-driven validation, and transparent recordkeeping without relying on centralized authorities. It achieves trust through cryptographic hash functions, digital signatures, and consensus protocols, enabling distributed nodes to agree on a shared state. While public blockchains such as Bitcoin and Ethereum rely on energy-intensive Proof-of-Work (PoW) mechanisms, alternative protocols like Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Directed Acyclic Graphs (DAGs) have emerged to improve scalability and reduce computational costs [13, 14].

To address threats posed by quantum computing to classical cryptographic primitives, quantum-resilient blockchain models have been proposed. One line of work focuses on post-quantum cryptography (PQC), including lattice-based and hash-based schemes, to replace vulnerable components such as digital signatures and key exchange protocols [15]. Another approach involves leveraging Quantum Key Distribution (QKD) to secure peer-to-peer communication among blockchain nodes, enabling symmetric key generation with

information-theoretic security [16]. Recent advances have demonstrated device-independent QKD protocols based on random quantum states, which provide robustness even against general and optimal collective attacks [17].

Beyond cryptographic primitives, emerging blockchain architectures increasingly integrate intelligent decision logic and context-aware automation. The fusion of blockchain with contextual Artificial Intelligence enables explainable inference logging and real-time decision traceability, which are essential for regulatory compliance and adaptive system behavior. For instance, AI-enhanced smart contracts can respond to dynamic environmental inputs or user-specific conditions, allowing decentralized applications to maintain verifiability while incorporating contextual responsiveness. Recent reviews highlight that artificial intelligence methods, such as machine learning and deep learning, have been effectively applied to optimize blockchain consensus mechanisms, improve smart contract vulnerability detection, and enhance privacy-preserving strategies including federated learning and differential privacy. These applications address longstanding challenges in scalability, security, and trust [18].

Recent research has also explored advanced consensus mechanisms suitable for quantum environments. Quantum consensus protocols utilize entanglement and distributed quantum states to achieve agreement among network nodes, extending Byzantine fault tolerance into the quantum domain [19-21]. Additional studies evaluate the resilience of such protocols under noisy intermediate-scale quantum (NISQ) conditions, finding that noise and channel imperfections may constrain practical implementation to modular or enterprise-scale deployments [22]. Despite their conceptual promise, quantum-enhanced consensus models face critical challenges including hardware immaturity, entanglement fragility, scalability constraints, and limited interoperability with classical systems. Overall, blockchain remains a robust foundation for decentralized trust. However, its sustained relevance in a quantum computing era will depend on the proactive integration of quantum-safe cryptographic methods, secure key distribution mechanisms, and adaptable consensus designs.

2.3 | Contextual AI Foundations

Contextual Artificial Intelligence refers to intelligent systems capable of interpreting and adapting to dynamic environments by modeling situational variables, user intent, and environmental feedback. Unlike traditional AI pipelines relying on static datasets or fixed rules, contextual AI systems support real-time responsiveness and adaptability in data-rich, temporally evolving settings. Techniques such as transformer-based architectures, multi-head self-attention mechanisms, and reinforcement learning are central to enabling AI agents to generate insights, personalize outputs, and anticipate behavior in multi-agent or uncertain contexts [23, 24].

Traditional supervised and unsupervised learning paradigms form the foundational layer of modern AI systems. Supervised learning enables models to learn mappings from labeled inputs to outputs, optimizing prediction accuracy using known outputs. In contrast, unsupervised learning discovers latent patterns, clusters, or embeddings from unlabeled data [25]. While both approaches underpin many AI applications, they assume static data distributions and minimal feedback, reducing their effectiveness in environments that evolve over time. Contextual AI extends these paradigms by incorporating live data, feedback loops, and situational awareness to support continual learning, personalized adaptation, and sequential decision-making in dynamic environments.

Recent advances in contextual AI architectures integrate meta-learning and online learning mechanisms, allowing models to adapt to new tasks or environments with minimal data [26]. These adaptive capabilities are particularly crucial in edge and federated scenarios where heterogeneous hardware, local data characteristics, and privacy constraints prevail [27]. Contextual AI plays a decisive role as the inference layer in hybrid quantum-blockchain-AI architectures. It interprets environmental signals and agent states, dynamically triggering cryptographic protocols, smart contract actions, or quantum-secured communication channels based on real-world context. For example, in federated learning environments, contextual agents

can decide whether to initiate encrypted model updates or adjust communication policies according to edge device conditions [28]. Integrating these contextual decisions with blockchain ensures transparency and auditability, while quantum-enhanced modules strengthen trust and randomness [29].

In decentralized and privacy-sensitive use cases such as IoT, supply chains, or autonomous systems, contextual AI achieves near human adaptability. It enables systems to detect anomalies, respond to threats, adjust workflows, or personalize services in real time while maintaining verifiable traces of decisions across distributed nodes. By bridging secure quantum mechanisms and immutable blockchain records, contextual AI enables intelligent, trustworthy, and context aware automation across complex environments.

3 | Quantum-Classical Hybrid Architecture Design

The integration of quantum computing, blockchain, and contextual AI necessitates a multi-layered architecture that capitalizes on the distinct strengths of each technology while ensuring interoperability, scalability, and trustworthiness. The hybrid architecture serves as a foundational model for secure, adaptive, and decentralized systems operating in real-time environments. At the quantum layer, quantum computing contributes capabilities for cryptographic primitives, secure randomness generation, and optimization tasks. Quantum-enhanced modules can accelerate operations such as key generation, consensus optimization, and privacy preservation through algorithms like Grover's and Shor's, along with quantum key distribution protocols. These primitives are particularly vital in threat scenarios where classical cryptography becomes vulnerable to quantum adversaries.

Above these capabilities, the blockchain layer provides an immutable and decentralized ledger for data integrity, distributed consensus, and auditable traceability. This layer ensures that actions taken by contextual AI agents or decisions derived from quantum modules are transparently recorded and verifiable. Smart contracts act as programmable logic units that enforce rules, execute policies, and integrate contextual inputs. When enhanced with post-quantum cryptography or quantum-resilient consensus protocols, the blockchain layer becomes robust against both classical and quantum attacks.

At the contextual AI layer, machine learning models interpret real-time data streams, user behavior, and environmental feedback to generate adaptive insights. Techniques such as transformer-based models, attention mechanisms, and reinforcement learning enable AI agents to personalize services, anticipate threats, and dynamically coordinate system behavior. This layer augments smart contracts with semantic reasoning and probabilistic inference, allowing intelligent automation that is responsive to changing conditions. The architecture is orchestrated through a cross-layer coordination interface that enables secure data exchange, synchronization of decision states, and feedback propagation. This coordination is essential for aligning quantum computations, blockchain validations, and AI-generated decisions. For example, AI models may request secure randomness from quantum modules, validate inputs through blockchain records, or execute stateful interactions via smart contracts.

To maintain trust and transparency, the architecture incorporates end-to-end observability mechanisms. These include explainable AI outputs, verifiable decision trails, and tamper evident audit logs, ensuring that system operations remain accountable across stakeholders. Privacy is preserved using federated learning, homomorphic encryption, or differential privacy. These are further augmented by blockchain backed access control and quantum secured communication channels. In high-stakes domains such as autonomous mobility, financial systems, or critical infrastructure, this hybrid design supports mission-aware resilience. Failures or anomalies in one layer can be mitigated through fallback mechanisms in the others. For instance, a compromised AI agent's decisions can be overridden by blockchain consensus, or a latency bottleneck in the blockchain can be addressed by offloading optimization tasks to quantum subroutines. Overall, the hybrid architecture establishes a cohesive computational trust framework that leverages the unique capabilities of quantum, blockchain, and contextual AI to support intelligent, secure, and scalable applications.

3.1 | Layered Architecture

The proposed quantum-classical hybrid architecture is designed as a multi-layered framework that enables seamless integration of contextual intelligence, quantum-enhanced cryptography, decentralized governance, and classical computing resources. As illustrated in Figure 1, the architecture comprises four interoperable layers: the Contextual AI Layer, Quantum Layer, Blockchain Layer, and Classical Layer. Sections 3.1.1 to 3.1.4 discuss each layer in detail, including the inbound and outbound activities summarized in the associated tables. These subsections highlight the multidirectional interactions that collectively enable secure, explainable, and high-performance decision-making within the proposed hybrid architecture.

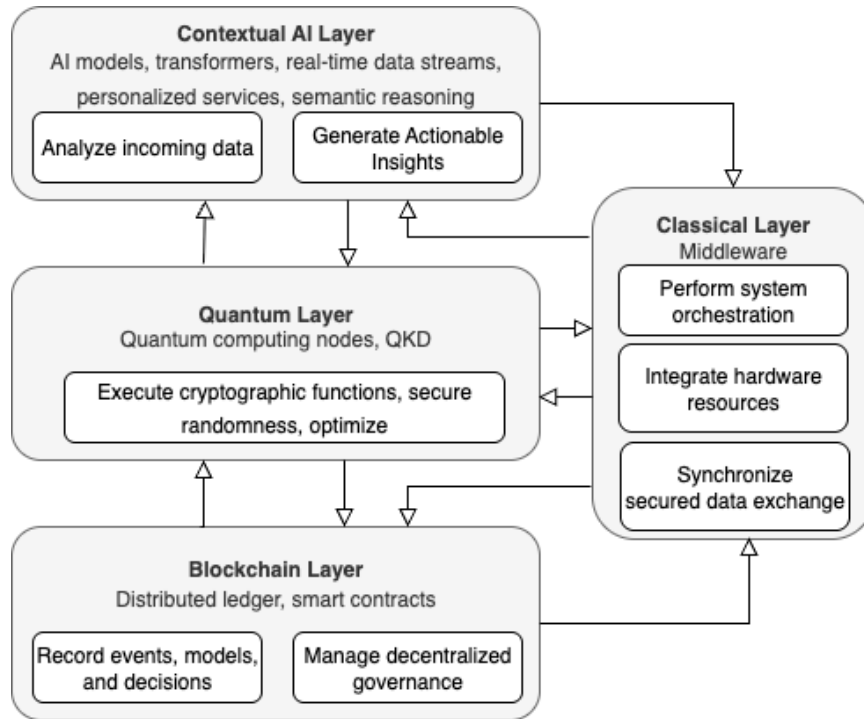


Figure 1. Quantum-classical hybrid architecture.

3.1.1 | Contextual AI Layer

The Contextual AI Layer serves as the cognitive engine of the architecture, responsible for analyzing incoming data, inferring situational context, and generating actionable insights. It employs advanced machine learning models, including transformer-based architectures and reinforcement learning agents, to interpret dynamic inputs such as sensor streams, user interactions, or transactional logs. These models enable the system to personalize responses, detect anomalies, and adapt behavior based on changing environmental conditions. This layer maintains a direct connection with the Classical Layer, which facilitates the execution of learning models, manages memory and compute resources, and ensures synchronized integration with hardware infrastructure. Tasks such as preprocessing, scheduling, and operational feedback control are routed through the Classical Layer to ensure practical execution of AI-generated decisions.

The Contextual AI Layer also interfaces with the Quantum Layer to request cryptographic primitives, secure randomness, or optimization subroutines. These quantum-enhanced functions are integrated to strengthen the quality and security of AI-driven inferences, particularly in domains requiring secure identity verification or constrained optimization. Furthermore, the Contextual AI Layer transmits verified outputs to the Blockchain Layer for immutable recording and traceable enforcement through smart contracts. For example, routine threshold breaches from IoT data may be logged directly for auditability. In contrast, sensitive decisions related to identity or financial transactions may be routed first through the Quantum Layer for enhanced cryptographic assurance before being committed to the blockchain.

Although the typical data flow from the Contextual AI Layer to the Blockchain Layer is outbound, the interaction can also be bidirectional. The Blockchain Layer may return smart contract outcomes, access permissions, or policy enforcement parameters, which in turn influence the decision logic or data access scope of the AI agents. This bidirectional link enhances system adaptability and enables decentralized governance mechanisms to shape AI behavior in real time. Table 1 summarizes the inbound activities that enable the Contextual AI Layer to operate in a context-sensitive, secure, and policy-aligned manner across the hybrid architecture. Table 2 summarizes the outbound flows which ensure that the Contextual AI Layer actively contributes to the system's intelligence, security, and accountability across quantum-classical and decentralized environments.

Table 1. Inbound activities to the contextual AI layer.

Source Layer	Inbound Activity to Contextual AI Layer
Classical Layer	- Execution of machine learning models (e.g., transformer inference, RL agents) - Pre-processed input data - System-level orchestration signals (e.g., hardware availability, job scheduling) - Feedback signals from real-world actuators or IoT devices
Quantum Layer	- Quantum-generated randomness for stochastic AI models - Optimization results (e.g., quantum-enhanced scheduling or routing) - Cryptographic functions for secure AI decision-making (e.g., authentication, encryption primitives)
Blockchain Layer	- Smart contract outputs affecting AI decision logic - Access control permissions for data usage - Policy updates or decentralized governance rules - Historical trace data or provenance for informed inference

Table 2. Outbound activities from the contextual AI layer.

Target Layer	Outbound Activity from Contextual AI Layer
Classical Layer	- Model execution requests (e.g., start inference, reinforcement learning update) - Preprocessing/postprocessing task delegation - Feedback control instructions for real-world actuators - System coordination signals (e.g., resource requests, scheduling instructions)
Quantum Layer	- Requests for quantum-secured randomness (e.g., entropy sources for probabilistic reasoning) - Requests for quantum optimization (e.g., path planning, resource allocation) - Requests for cryptographic support (e.g., key generation or signature validation)
Blockchain Layer	- Verified decisions or inferences for immutable logging - Triggers for smart contracts based on contextual conditions - AI-driven governance decisions (e.g., policy enforcement, threshold violations) - Annotated metadata for auditability and traceability (e.g., model version, timestamp, data used)

Through these interconnected operations, the Contextual AI Layer enables context-aware intelligence that is robust, explainable, and aligned with secure and transparent system-level goals.

3.1.2 | Quantum Layer

Quantum Layer executes quantum-enhanced cryptographic functions and optimization routines using quantum circuits. It operates as a specialized component that delivers cryptographic primitives, secure randomness, and quantum-enhanced optimization to the broader architecture. It receives inbound requests from the Contextual AI Layer for quantum-secured keys, random number generation, or optimization routines that support decision-making processes. These services enhance the trustworthiness and robustness of AI-generated insights, particularly in environments requiring secure multi-party coordination or privacy

preservation. The Classical Layer orchestrates these requests, handling the execution of hybrid quantum-classical workflows and managing the integration of quantum results into the overall system operation.

The Quantum Layer also maintains a collaborative relationship with the Blockchain Layer. While it frequently provides outbound services such as quantum key distribution, post-quantum digital signatures, or secure hashing mechanisms for blockchain records, it can also receive inbound requests from the Blockchain Layer. These include scenarios where the blockchain system employs quantum-resilient consensus protocols, decentralized identity frameworks, or post-quantum verification techniques. In such cases, the Blockchain Layer may call upon the Quantum Layer to verify quantum cryptographic proofs, generate secure entropy for consensus randomization, or validate identity credentials secured by quantum techniques.

This bidirectional interaction ensures that the Quantum Layer is not isolated but instead functions as a dynamic security and optimization module within the hybrid architecture. Its contributions support both proactive protection against quantum threats and enhanced performance across secure AI, blockchain governance, and multi-agent coordination tasks. These multidirectional connections position the Quantum Layer as both a responsive and generative unit in the system. It receives inbound service requests from other layers and delivers quantum-enhanced outputs that strengthen cryptographic integrity, improve inference quality, and support post-classical consensus mechanisms. Table 3 summarizes the inbound activities directed to the Quantum Layer, detailing the nature of quantum service requests from the Contextual AI, Classical, and Blockchain Layers. In parallel, Table 4 outlines the outbound activities through which the Quantum Layer contributes cryptographic and optimization outputs, reinforcing secure computation and cross-layer coordination throughout the architecture.

Table 3. Inbound activity to quantum layer.

Source Layer	Inbound Activity to Quantum Layer
Contextual AI Layer	- Requests for quantum-secured key generation - Requests for randomness sources for probabilistic inference - Requests for optimization subroutines (e.g., scheduling, routing)
Classical Layer	- Orchestration of hybrid quantum-classical workflows - Transmission of input parameters for quantum circuits - Management of execution logic and result integration
Blockchain Layer	- Requests for quantum-resilient consensus support - Calls for verifying post-quantum cryptographic proofs - Entropy generation for secure randomization - Identity verification using quantum-secured credentials

Table 4. Outbound activity from quantum layer.

Target Layer	Outbound Activity from Quantum Layer
Contextual AI Layer	- Quantum-generated randomness for AI model inputs - Quantum-optimized solutions for decision-making - Cryptographic primitives to secure inference outcomes
Classical Layer	- Quantum computation results for classical postprocessing - Intermediate data for hybrid execution control - Status or error signals from quantum circuit evaluations
Blockchain Layer	- Quantum key distribution for secure transactions - Post-quantum digital signatures or secure hashes - Entropy or verification support for consensus and identity services

3.1.3 | Blockchain Layer

Blockchain Layer ensures transparent, tamper-resistant recording of events, models, and decisions while enabling decentralized identity and governance. This layer functions as the integrity backbone of the hybrid architecture, ensuring that all transactions, model outputs, and decision events are securely recorded,

traceable, and tamper resistant. It receives verified outputs from the Contextual AI Layer, either directly or routed through the Quantum Layer for additional cryptographic assurance. These outputs include AI-generated insights such as control signals, threshold violations, or data access decisions that require transparent logging and enforcement via smart contracts.

This layer also interacts with the Classical Layer for operational execution tasks. These include transaction processing, ledger updates, and synchronization with external systems such as IoT platforms or enterprise software. The Classical Layer handles the orchestration of computing resources, executes smart contract workflows, and ensures that blockchain activities integrate seamlessly into system-wide operations. In addition, the Blockchain Layer maintains a tightly coupled relationship with the Quantum Layer. It may issue inbound requests for quantum-enhanced cryptographic functions such as secure key regeneration, quantum-secured signatures, or entropy generation for randomized consensus protocols. In turn, it receives outbound cryptographic outputs from the Quantum Layer to reinforce data integrity, identity verification, and consensus mechanisms. These interactions are particularly valuable in high-risk environments requiring post-quantum resilience and long-term security guarantees.

By anchoring trust across the system, the Blockchain Layer enables decentralized governance, secure coordination among distributed agents, and traceable accountability for all system actions. It enforces global system rules through immutable recordkeeping, policy execution, and verifiable state transitions. Table 5 summarizes the inbound interactions to the Blockchain Layer, identifying inputs from AI, classical, and quantum components. These inputs collectively support tamper-proof data logging, automated smart contract enforcement, and secure consensus participation. Table 6 presents the outbound activities from the Blockchain Layer, capturing how it relays governance signals, historical records, and policy enforcement triggers to other layers to support traceability, access control, and coordinated system behavior.

Table 5. Inbound activity to blockchain layer.

Source Layer	Inbound Activity to Blockchain Layer
Contextual AI Layer	- Verified insights and decisions for logging (e.g., threshold breaches, access grants) - Smart contract triggers (e.g., anomaly alerts, policy violations) - Annotated metadata (e.g., timestamps, model ID)
Classical Layer	- Transaction orchestration and formatting - Execution of smart contract logic - Ledger update requests and synchronization signals
Quantum Layer	- Quantum-secured signatures or cryptographic proofs - Random seeds for consensus protocols - Identity verification using post-quantum credentials

Table 6. Outbound activity from blockchain layer.

Target Layer	Outbound Activity from Blockchain Layer
Contextual AI Layer	- Policy updates and access permissions - Smart contract execution results - Historical trace data for inference enrichment
Classical Layer	- Ledger update confirmation - Smart contract execution triggers - Synchronization instructions for external system integration
Quantum Layer	- Requests for cryptographic reinforcement (e.g., key regeneration, entropy) - Validation requests for quantum-resistant protocols

3.1.4 | Classical Layer

Classical Layer performs general computation, system orchestration, and integration with hardware resources. Thus, it functions as the operational backbone of the hybrid architecture, enabling all other layers to communicate and function in a synchronized and coherent manner. It governs orchestration across the system, manages classical computing workloads, and ensures the seamless integration of hardware resources across AI, quantum, and blockchain environments. This layer maintains a direct connection to the Contextual AI Layer and serves four essential roles. First, it facilitates model execution and inference. While the Contextual AI Layer is responsible for cognitive reasoning and adaptive logic, it depends on classical computing infrastructure such as CPUs, GPUs, and TPUs to run machine learning models, manage memory, and process inputs. This includes transformer-based models, reinforcement learning agents, and federated learning processes.

Second, the Classical Layer provides hardware orchestration by interfacing with sensors, communication networks, and physical compute units. It ensures that data pipelines are synchronized, and that contextual data is efficiently routed to AI modules. Third, it performs data preprocessing and scheduling of workflows. Tasks such as normalization, feature extraction, and data formatting are typically handled within classical environments. Additionally, the Classical Layer is responsible for system-level functions such as memory allocation, job scheduling, and computational optimization. Fourth, the layer supports feedback propagation and operational control. When the Contextual AI Layer generates insights that require real-world action, such as adjusting IoT devices or initiating smart contracts, these instructions are transmitted through the Classical Layer to ensure proper execution.

Beyond its coordination with the Contextual AI Layer, the Classical Layer maintains dedicated interfaces with both the Quantum Layer and the Blockchain Layer. In relation to the Quantum Layer, it orchestrates and executes hybrid quantum-classical workflows by coordinating classical control logic with quantum subroutines and managing the necessary hardware resources. In relation to the Blockchain Layer, it supports the execution of blockchain-related processes, including transaction processing, data formatting, and synchronization with consensus protocols and distributed ledgers.

These multidirectional interactions define the Classical Layer as a central coordination hub for operational tasks. Table 7 presents the inbound activities that originate from other layers and enable classical execution and system management. Table 8 outlines the outbound activities initiated by the Classical Layer, which enable communication and coordination across the hybrid architecture.

Table 7. Inbound activity to classical layer.

Source Layer	Inbound Activity to Classical Layer
Contextual AI Layer	- Model execution and inference requests - Preprocessing and data handling tasks - Feedback signals for actuator control - Scheduling and resource requests
Quantum Layer	- Quantum subroutine orchestration triggers - Hybrid workflow execution instructions - Hardware synchronization requirements
Blockchain Layer	- Smart contract activation commands - Transaction formatting and signing requests - Synchronization signals for ledger updates or external events

Table 8. Outbound activity from classical layer.

Target Layer	Outbound Activity from Classical Layer
Contextual AI Layer	- Pre-processed data for AI inference - Execution status and results - Actuator feedback and sensor loop completion signals

Quantum Layer	- Trigger signals for quantum execution - Input data or parameters for quantum optimization - Coordination signals for hardware integration
Blockchain Layer	- Transaction formatting and execution - Smart contract orchestration - Ledger update instructions and state synchronization

3.2 | System-Wide Data Flow and Layer Interoperability

The hybrid architecture supports a structured and interoperable data flow across four foundational layers: Contextual AI, Classical, Quantum, and Blockchain. Figure 2 illustrates the sequential movement of data through the system, beginning with external inputs and culminating in high-confidence outputs, actionable decisions, and real-world responses. The process begins with incoming data streams such as IoT sensor readings, user interactions, or transactional events, which enter the system as raw input. This input is first processed by the Contextual AI Layer, where machine learning pipelines extract situational understanding, detect anomalies, and generate preliminary decisions. At this stage, context-aware insights are produced through advanced inference mechanisms that frame the semantic meaning of the data within the application domain.

Following this, the Classical Layer takes over the orchestration and computational execution of AI workflows. It executes the necessary model inferences using CPUs or GPUs, manages data preprocessing, and coordinates hardware-level operations. In parallel, it routes the relevant data or decisions to subsequent layers based on operational requirements. For instance, if secure optimization or cryptographic reinforcement is required, it prepares the requests and manages the execution logic necessary to interface with the Quantum Layer. Within the Quantum Layer, specialized quantum subroutines process the inbound requests received from the AI and Classical layers. These may include the generation of quantum-secured keys, the computation of optimal configurations, or the production of high-entropy randomness for secure operations. The outputs of these computations are then integrated back into the system via the Classical Layer, which handles the insertion of quantum-enhanced results into the ongoing workflow.

Processed insights and validated decisions are subsequently transferred to the Blockchain Layer. Here, they are logged immutably to ensure transparency, tamper resistance, and long-term auditability. This includes decisions made by the AI, cryptographically reinforced outputs from the Quantum Layer, or policy enforcement actions derived from smart contracts. The Blockchain Layer also facilitates feedback loops, where verification outcomes or access permissions are sent back to other layers, thereby supporting secure system-wide governance. The final stage of the pipeline represents the Output / Decision / Action phase. It reflects the cumulative result of all upstream processes and encapsulates the meaningful impact of the hybrid architecture. This may include alerting medical personnel, executing a financial transaction, or updating a smart contract. Each action is grounded in verified AI reasoning, secured by quantum computation, and transparently recorded via blockchain technology, thus ensuring that system responses are not only intelligent but also trustworthy and enforceable.

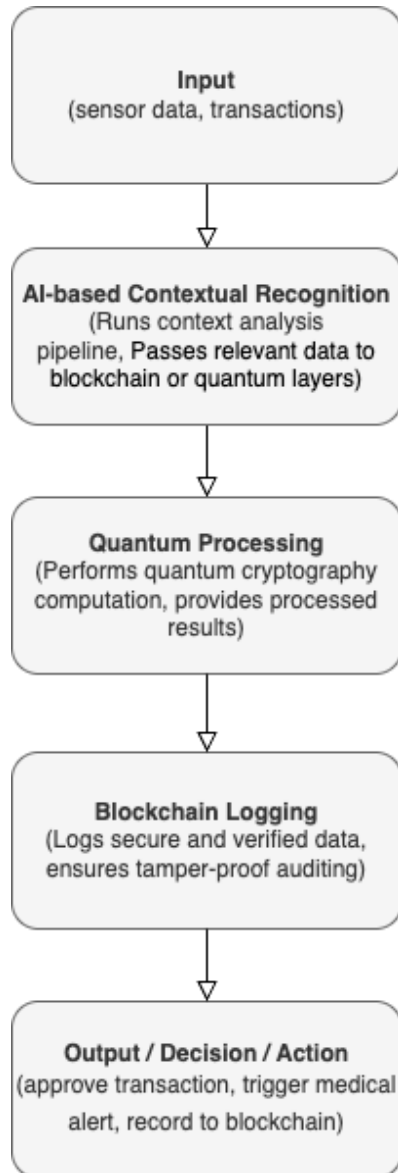


Figure 2. Classical Orchestration and Execution.

3.3 | Quantum-Assisted Blockchain

The integration of quantum computing with blockchain systems introduces a new class of security and consensus mechanisms that can enhance the resilience and performance of decentralized architectures. In the proposed hybrid framework, the Quantum Layer plays a pivotal role in reinforcing the cryptographic integrity and operational efficiency of the Blockchain Layer through three key capabilities:

a. **Quantum Key Distribution (QKD)**

Quantum key distribution enables the generation and exchange of cryptographic keys with provable security rooted in quantum mechanics. Unlike classical key exchange methods, QKD allows two parties to detect any interception attempts in real time, thereby ensuring secure ledger communication and protecting sensitive transactions against man-in-the-middle attacks. Within the hybrid system, QKD can be used to establish trust anchors for smart contract execution, identity verification, and data integrity validation across distributed nodes.

b. **Quantum-Enhanced Consensus Models**

Emerging research suggests that quantum circuits can be employed to accelerate or parallelize consensus algorithms in blockchain networks. These quantum consensus models exploit quantum parallelism to explore

multiple validation paths simultaneously, potentially reducing confirmation times and improving scalability in high-throughput environments. In adversarial settings, quantum-generated randomness may also be used to increase the unpredictability and fairness of leader election or validator selection protocols.

c. Post-Quantum Cryptographic Algorithms

To future-proof blockchain operations against quantum adversaries, the system can adopt post-quantum cryptographic techniques. These include lattice-based, hash-based, and code-based digital signatures that are resistant to known quantum attacks, such as those leveraging Shor's algorithm. The Quantum Layer not only supports the verification of these cryptographic primitives but may also assist in generating secure entropy and cryptographic proofs required for long-term data protection and regulatory compliance. Together, these capabilities position the Quantum Layer as a foundational trust enabler within the blockchain domain, providing both proactive and reactive defenses against quantum-era threats. The synergy between quantum algorithms and decentralized infrastructure ensures that smart contracts, consensus mechanisms, and data provenance remain robust, scalable, and secure under evolving computational paradigms.

4 | Use Cases Applications

The proposed quantum-classical hybrid architecture is purposefully designed to address critical challenges across real-world domains that demand secure, intelligent, and auditable computational systems. By integrating four interoperable layers including Contextual AI, Classical processing, Quantum computation, and Blockchain storage, the architecture provides a unified framework capable of handling sensitive data, optimizing under uncertainty, and enabling traceable decision-making. This section presents three illustrative application domains: healthcare, finance, and supply chain. Each scenario demonstrates how the architecture supports domain-specific objectives such as privacy preservation, fraud prevention, and logistics resilience through coordinated action across its layered components.

4.1 | Healthcare: Privacy-Preserving Intelligence and Quantum-Backed Record Access

In healthcare environments, sensitive patient data must be interpreted with clinical precision while remaining secure, traceable, and compliant with regulatory policies. The proposed hybrid architecture enables this through the coordinated operation of four distinct layers. At the Blockchain Layer, clinical records are stored in tamper-evident ledgers protected by post-quantum cryptographic keys, drawing on advances in quantum-safe blockchain infrastructure and post-quantum cryptography standards [30, 31]. This provides a resilient foundation for auditability and secure recordkeeping.

The Contextual AI Layer processes doctor-patient conversations, diagnostic text, and unstructured clinical notes to generate real-time insights and treatment recommendations. These AI models operate under local data privacy regulations and employ domain-specific ontologies and embeddings to support accurate and explainable predictions [32], [33], [34], [35], [36]. When a user or system requests access to data, the Quantum Layer provides cryptographic enforcement through quantum-enhanced key distribution and authentication mechanisms. These tools support dynamic policy enforcement, ensuring that access decisions reflect contextual factors such as user role, location, and purpose [37, 38]. The integration of quantum security at this layer adds a level of protection against adversaries with quantum capabilities.

The Classical Layer orchestrates data flow and computational coordination across the system. It invokes AI pipelines, executes smart contract logic, and interfaces with hospital information systems, ensuring system responsiveness and operational reliability. This layered integration achieves both real-time interpretability and long-term data sovereignty, enabling healthcare institutions to offer intelligent decision support while maintaining trust, privacy, and compliance in sensitive clinical environments.

4.2 | Finance: Context-Aware Fraud Detection with Quantum-Secured Ledger Provenance

In financial systems, the ability to detect fraud, maintain regulatory transparency, and ensure transaction integrity is paramount. The proposed hybrid architecture facilitates this through the coordinated operation of its four core layers. At the Blockchain Layer, financial transaction records are stored in immutable ledgers that utilize post-quantum digital signature schemes and cryptographic primitives to resist both classical and quantum adversaries [39]. These secure logs form the verifiable foundation for interbank audits, regulatory reporting, and digital forensics. The Contextual AI Layer analyzes real-time transaction streams, behavioral patterns, and contextual metadata to flag anomalous activities indicative of fraud or cyber threats. These models employ advanced embeddings, probabilistic reasoning, and sequential pattern recognition, drawing from recent research on quantum-accelerated fraud detection and contextual modeling in finance [40]. The AI outputs inform proactive alerts and adaptive risk scoring mechanisms, enabling faster response to evolving threats.

Access control and inter-institutional data exchange are secured by the Quantum Layer, which enables quantum key distribution, quantum safe session initialization, and authenticated message integrity between cooperating banks or financial entities. These capabilities support confidential multi-party computation without requiring data centralization, allowing regulatory compliance and analytics across borders while preserving privacy [37, 38]. This layer ensures secure interoperability between financial actors operating under heterogeneous privacy policies.

The Classical Layer coordinates smart contract execution, policy orchestration, and integration with compliance engines and core banking platforms. It ensures end-to-end responsiveness while managing logic-driven enforcement of alerts and reporting workflows. By aligning each layer to specific analytical, cryptographic, and operational functions, the architecture delivers robust fraud detection, transparent auditability, and improved resilience in a globalized financial ecosystem. This layered design not only enhances system trust and accountability but also enables scalable and secure financial intelligence across jurisdictions.

4.3 | Supply Chain: Resilient Coordination through Predictive Intelligence and Secure Traceability

In high complexity supply ecosystems, which are characterised by volatility from geopolitical disruption, regulatory demands, and fluctuating demand, the architecture supports resilience by combining predictive insights, immutable traceability, and quantum accelerated optimisation. Each layer of the architecture contributes distinct capabilities aligned with domain needs. At the Blockchain Layer, inter-organisation shipment logs, supplier certifications, and sensor data are immutably stored using post-quantum cryptographic primitives. This supports verifiable provenance and audit integrity across manufacturers, distributors, and retailers [41], [42], [43]. The Contextual AI Layer ingests heterogeneous inputs from demand forecasts, weather data, geopolitical alerts, and inventory metrics. It produces scenario planning, risk forecasts, and disruption mitigation strategies that improve operational agility under uncertainty [43].

The Quantum Layer enhances logistics planning through quantum-inspired or hybrid quantum-classical algorithms, such as quantum annealing or QAOA, to tackle combinatorial challenges in routing, scheduling, and supplier selection tasks that are computationally intractable for classical approaches [44], [45], [46], [47]. It also supports secure multi-party coordination via quantum key distribution for inter-organisation communications where sensitive proprietary data remains hidden [48]. The Classical Layer executes system workflows like route adjustments, contract enforcement, and ERP or IoT platform integration. It triggers operations based on AI insights and quantum-optimised recommendations, ensuring practical actuation across distributed nodes.

Together, this layered approach delivers AI-driven foresight in supply chain risk and demand volatility, Blockchain-anchored traceability and compliance with auditability, and Quantum-enhanced optimisation and secure coordination. This ensures that supply chains operate with intelligence, transparency, and resilience.

5 | Challenges and Limitations

While the proposed quantum classical hybrid architecture offers transformative potential, its realization faces several technical, infrastructural, and ethical challenges. These limitations span across the foundational technologies including quantum computing, contextual AI, and blockchain systems, as well as their interoperability within a unified architecture. One of the most significant obstacles lies in the limitations of current quantum hardware. Issues such as qubit instability, high error rates, and limited coherence times restrict the scalability and reliability of quantum-enhanced computations. These constraints affect both cryptographic services and optimization tasks that the architecture relies on.

Interfacing between quantum systems, classical computing infrastructure, and blockchain networks also presents a major barrier. The lack of standardized protocols and the complexity of synchronizing computation across fundamentally different paradigms complicate system-level integration. Seamless orchestration between these components requires advanced middleware and tightly coupled coordination layers. The blockchain component introduces concerns related to energy efficiency and transaction scalability. Many blockchain systems are resource intensive, and layering additional cryptographic workloads or quantum verification routines may exacerbate latency and energy consumption challenges. This becomes especially critical in real-time applications such as medical alerts or financial fraud detection.

Contextual AI introduces additional privacy and compliance risks. Because contextual models process sensitive patterns such as user behavior or clinical interactions, they raise ethical concerns about data usage, consent, and inference-based privacy breaches. Furthermore, blockchain's immutability conflicts with emerging privacy regulations that require data erasure or redaction. Taken together, these challenges underscore the need for coordinated advances across quantum engineering, AI interpretability, and decentralized infrastructure, alongside regulatory frameworks that address ethical implications.

6 | Future Directions

To advance the proposed hybrid architecture and mitigate current limitations, several key areas of research and development are emerging. These directions aim to enhance computational intelligence, privacy, and operational interoperability across quantum, AI, and blockchain layers. Post Quantum Cryptography is a foundational priority. As quantum algorithms pose increasing risks to classical encryption, the adoption of lattice based and hash-based schemes within blockchain smart contracts will provide long term security for digital identities and decentralized systems. Integrating these cryptographic methods ensures resilience against quantum level adversaries.

Federated learning with quantum AI introduces a scalable and privacy preserving approach to training contextual models. By distributing model training across edge nodes or institutional boundaries and applying quantum privacy guarantees through variational circuits, this paradigm offers robust solutions for domains such as healthcare, where sensitive data cannot be centralized. Another critical direction involves blockchain interoperability through quantum teleportation inspired simulations. These communication techniques may enable secure and real time synchronization of state and logic between heterogeneous blockchain platforms, enhancing agility in multi chain environments.

The need for explainable contextual AI is increasingly recognized, particularly in regulated sectors. Research into interpretable model architectures, AI alignment strategies, and transparent reasoning mechanisms will strengthen trust and accountability in automated decision systems, allowing for meaningful human oversight and regulatory compliance. Quantum middleware platforms are expected to play a central role in coordinating this architecture. These platforms abstract hardware level variability and offer unified APIs for managing

interactions between AI engines, quantum processors, and blockchain consensus mechanisms. Their development is essential for seamless orchestration and deployment of hybrid workflows.

Collectively, these future directions outline a comprehensive path toward more secure, scalable, and ethically aligned intelligent systems that bring together the strengths of distributed ledgers, contextual intelligence, and quantum computing.

7 | Conclusion

This paper presents a unified quantum-classical hybrid architecture that integrates contextual AI, quantum computing, and blockchain technologies into a cohesive and interoperable framework. By combining contextual understanding, quantum-enhanced computation, and distributed trust mechanisms, the proposed architecture enables intelligent and secure systems suitable for high-impact domains such as healthcare, finance, and supply chain management.

The primary contribution of this work is the systematic design of a four-layered architecture where each layer plays a distinct role while maintaining seamless interoperability. Unlike isolated implementations of AI or quantum or blockchain technologies, this architecture enables cross-layer integration that supports secure data processing, context-aware reasoning, cryptographic reinforcement, and tamper-proof auditability. The inclusion of a classical coordination layer ensures operational practicality using existing technologies. This work also introduces detailed data flow models, interaction tables, and real-world application scenarios to demonstrate how the proposed architecture can be applied in practice. It provides a conceptual blueprint that bridges theoretical advancements in quantum and AI with implementable strategies grounded in blockchain governance and classical infrastructure.

Although several technical, ethical, and interoperability challenges remain, the paper identifies concrete future directions including post quantum encryption schemes, federated quantum learning, explainable AI mechanisms, and middleware orchestration platforms. These directions reflect a multidisciplinary pathway toward robust, transparent, and scalable next-generation systems. In conclusion, the architecture proposed in this paper offers a foundational step toward building intelligent and trustworthy digital ecosystems. It contributes a forward-looking vision for researchers and practitioners seeking to operationalize the convergence of quantum computing, AI, and blockchain in real-world environments.

Funding

This research has no funding source.

Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Author Contributions

All authors contributed equally to this work.

References

- [1] M. Schuld, I. Sinayskiy, and F. Petruccione, "An introduction to quantum machine learning," *Contemp Phys*, vol. 56, no. 2, pp. 172–185, 2015.
- [2] M. Cerezo *et al.*, "Variational quantum algorithms," *Nature Reviews Physics*, vol. 3, no. 9, pp. 625–644, 2021.
- [3] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, "Hybrid discrete- and continuous-variable quantum information," *Nat Phys*, vol. 11, no. 9, pp. 713–719, 2015, doi: 10.1038/nphys3410.
- [4] E. O. Kiktenko *et al.*, "Quantum-secured blockchain," *Quantum Sci Technol*, vol. 3, no. 3, p. 035004, 2018.
- [5] M. Edwards, A. Mashatan, and S. Ghose, "A review of quantum and hybrid quantum/classical blockchain protocols," *Quantum Inf Process*, vol. 19, no. 6, p. 184, 2020.
- [6] K. Nikiforidis *et al.*, "Enhancing transparency and trust in AI-powered manufacturing: A survey of explainable AI (XAI) applications in smart manufacturing in the era of industry 4.0/5.0," *ICT Express*, vol. 11, no. 1, pp. 135–148, 2025.
- [7] A. Puthanveetil Madathil, X. Luo, Q. Liu, C. Walker, R. Madarkar, and Y. Qin, "A review of explainable artificial intelligence in smart manufacturing," *Int J Prod Res*, pp. 1–44, 2025.
- [8] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.
- [9] I. Sabeshuly, A. Akzhalova, and S. Ben Yahia, "A Hybrid Quantum-AI Architecture for Enhanced Blockchain Consensus," in *International Symposium on Business Modeling and Software Design*, Springer, 2025, pp. 144–156.
- [10] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv Opt Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.
- [11] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, 2018.
- [12] M. Allende *et al.*, "Quantum-resistance in blockchain networks," *Sci Rep*, vol. 13, no. 1, p. 5664, 2023.
- [13] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PLoS One*, vol. 11, no. 10, p. e0163477, 2016.
- [14] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.
- [15] L. Chen *et al.*, *Report on post-quantum cryptography*, vol. 12. US Department of Commerce, National Institute of Standards and Technology ..., 2016.
- [16] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev Mod Phys*, vol. 74, no. 1, p. 145, 2002.
- [17] S. Bera, S. Gupta, and A. S. Majumdar, "Device-independent quantum key distribution using random quantum states," *Quantum Inf Process*, vol. 22, no. 2, p. 109, 2023, doi: 10.1007/s11128-023-03852-2.
- [18] F. Yuan *et al.*, "AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection," *Algorithms*, vol. 18, no. 5, 2025, doi: 10.3390/a18050263.
- [19] J. Ramoliya and N. Doshi, "A review on quantum blockchain based consensus mechanism approaches," in *International Conference on ICT for Sustainable Development*, Springer, 2023, pp. 59–64.
- [20] X.-J. Wen, Y.-Z. Chen, X.-C. Fan, W. Zhang, Z.-Z. Yi, and J.-B. Fang, "Blockchain consensus mechanism based on quantum zero-knowledge proof," *Opt Laser Technol*, vol. 147, p. 107693, 2022, doi: <https://doi.org/10.1016/j.optlastec.2021.107693>.
- [21] D. Chawla, S. Kumari, R. S. Rathore, P. S. Mehra, A. K. Das, and N. Kumar, "Quantum Blockchain for Internet of Things: A systematic review, proposed solutions and challenges," *Computers and Electrical Engineering*, vol. 126, p. 110524, 2025, doi: <https://doi.org/10.1016/j.compeleceng.2025.110524>.
- [22] M. A. Ullah, J. W. Setiawan, J. ur Rehman, and H. Shin, "On the Robustness of Quantum Algorithms for Blockchain Consensus," *Sensors*, vol. 22, no. 7, 2022, doi: 10.3390/s22072716.
- [23] S. G. Thomas and P. K. Myakala, "Beyond the cloud: Federated learning and edge ai for the next decade," *Journal of Computer and Communications*, vol. 13, no. 2, pp. 37–50, 2025.
- [24] S. Ghaith, "The triple attention transformer: advancing contextual coherence in transformer models," *Evol Intell*, vol. 17, no. 5, pp. 3723–3744, 2024, doi: 10.1007/s12065-024-00954-3.
- [25] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, "A systematic review on supervised and unsupervised machine learning algorithms for data science," *Supervised and unsupervised learning for data science*, pp. 3–21, 2020.
- [26] A. and P. B. Dippel Oliver and Lisitsa, "Contextual Transformers for Goal-Oriented Reinforcement Learning," in *Artificial Intelligence XLI*, F. Bramer Max and Stahl, Ed., Cham: Springer Nature Switzerland, 2025, pp. 207–220.
- [27] Z. Jovanovic, Z. Hou, K. Biswas, and V. Muthukkumarasamy, "Robust integration of blockchain and explainable federated learning for automated credit scoring," *Computer Networks*, vol. 243, p. 110303, 2024, doi: <https://doi.org/10.1016/j.comnet.2024.110303>.
- [28] D. Gurung, S. R. Pokhrel, and G. Li, "Performance analysis and evaluation of postquantum secure blockchained federated learning," *Computer Networks*, vol. 255, p. 110849, 2024, doi: <https://doi.org/10.1016/j.comnet.2024.110849>.
- [29] J. Ahmad *et al.*, "Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches: A comprehensive review," *Appl Energy*, vol. 393, p. 126118, 2025, doi: <https://doi.org/10.1016/j.apenergy.2025.126118>.
- [30] K. Cherkaoui Dekkaki, I. Tasic, and M.-D. Cano, "Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process," *Technologies (Basel)*, vol. 12, no. 12, 2024, doi: 10.3390/technologies12120241.
- [31] F. Wu, B. Zhou, J. Song, and L. Xie, "Quantum-resistant blockchain and performance analysis," *J Supercomput*, vol. 81, no. 3, p. 498, 2025, doi: 10.1007/s11227-025-07018-y.

- [32] N. K. Parida, C. Jatoth, V. D. Reddy, Md. M. Hussain, and J. Faizi, “Post-quantum distributed ledger technology: a systematic survey,” *Sci Rep*, vol. 13, no. 1, p. 20729, 2023, doi: 10.1038/s41598-023-47331-1.
- [33] R. Knevel and K. P. Liao, “From real-world electronic health record data to real-world results using artificial intelligence,” *Ann Rheum Dis*, vol. 82, no. 3, pp. 306–311, 2023.
- [34] Y. Juhn and H. Liu, “Artificial intelligence approaches using natural language processing to advance EHR-based clinical research,” *Journal of Allergy and Clinical Immunology*, vol. 145, no. 2, pp. 463–469, 2020.
- [35] R. Venkatesh and B. Savadatti Hanumantha, “Electronic medical records protection framework based on quantum blockchain for multiple hospitals,” *Multimed Tools Appl*, vol. 83, no. 14, pp. 42721–42734, 2024.
- [36] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. M. Sam, and G. A. L. N. Samy, “Effect of quantum computing on blockchain-based electronic health record systems,” in *2022 4th International Conference on Smart Sensors and Application (ICSSA)*, IEEE, 2022, pp. 179–184.
- [37] M. Fischlin, J. von der Heyden, M. Margraf, F. Morgner, A. Wallner, and H. Bock, “Post-quantum Security for the Extended Access Control Protocol,” in *International Conference on Research in Security Standardisation*, Springer, 2023, pp. 22–52.
- [38] P. N. Mahalle, S. S. Raskar, A. P. Patil, and S. Ithape, “Access Control Scheme for Medical Cyber-Physical Systems Using Quantum Cryptography,” in *International Conference on ICT for Sustainable Development*, Springer, 2024, pp. 319–327.
- [39] A. S. Naik, E. Yeniaras, G. Hellstern, G. Prasad, and S. K. L. P. Vishwakarma, “From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance,” *Financial Innovation*, vol. 11, no. 1, pp. 1–67, 2025.
- [40] G. Yu and Z. Luo, “Financial fraud detection using a hybrid deep belief network and quantum optimization approach,” *Discover Applied Sciences*, vol. 7, no. 5, p. 454, 2025, doi: 10.1007/s42452-025-06999-y.
- [41] R. Toorajipour, V. Sohrabpour, A. Nazarpour, P. Oghazi, and M. Fischl, “Artificial intelligence in supply chain management: A systematic literature review,” *J Bus Res*, vol. 122, pp. 502–517, 2021, doi: <https://doi.org/10.1016/j.jbusres.2020.09.009>.
- [42] Ö. Karaduman and G. Gülhas, “Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand,” *Applied Sciences*, vol. 15, no. 9, 2025, doi: 10.3390/app15095168.
- [43] A. R. Teixeira, J. V. Ferreira, and A. L. Ramos, “Intelligent Supply Chain Management: A Systematic Literature Review on Artificial Intelligence Contributions,” *Information*, vol. 16, no. 5, 2025, doi: 10.3390/info16050399.
- [44] J. Choi and J. Kim, “A tutorial on quantum approximate optimization algorithm (QAOA): Fundamentals and applications,” in *2019 international conference on information and communication technology convergence (ICTC)*, IEEE, 2019, pp. 138–142.
- [45] R. Fakhimi and H. Validi, “Quantum approximate optimization algorithm (QAOA),” in *Encyclopedia of Optimization*, Springer, 2023, pp. 1–7.
- [46] L. Abualigah *et al.*, “Quantum approximate optimization algorithm: a review study and problems,” *Metaheuristic optimization algorithms*, pp. 147–165, 2024.
- [47] R. K. Vaddy, B. Dhamodharan, and A. Jain, “Quantum computing applications in real-time route optimization for supply chains,” in *Quantum Computing and Supply Chain Management: A New Era of Optimization*, IGI Global, 2024, pp. 113–124.
- [48] P. Azevedo, J. Gomes, and M. Romão, “Supply chain traceability using blockchain,” *Operations Management Research*, vol. 16, no. 3, pp. 1359–1381, 2023, doi: 10.1007/s12063-023-00359-y.

Disclaimer/Publisher’s Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.