World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Synergizing AI and Quantum Computing to Revolutionize Financial Crime Detection

Srikumar Nayak *

Financial Crime Unit, Citigroup inc., Principal AI and ML Architect, Incedo Inc.

World Journal of Advanced Research and Reviews, 2025, 28(01), 1756-1767

Publication history: Received on 18 September 2025; revised on 22 October 2025; accepted on 25 October 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.1.3637

Abstract

The integration of AI and QC results in a significant shift in combating financial crimes in the digital realm. Lawful computing techniques and statistical learning models are insufficient for examining enormous, high-dimensional financial datasets, and detecting intricate fraudulent patterns is also not feasible. The current investigation in this paper focuses on the integration of AI and QC in transforming financial crime detection systems. AI models, aided by quantum-enhanced algorithms, can perform pattern recognition, anomaly detection, and prediction with the highest accuracy in multidimensional transaction networks. Quantum Machine Learning (QML) offers a novel computational framework that enables real-time data processing, enhances encryption, and facilitates the simultaneous optimization of large-scale financial monitoring. Moreover, the research identified significant difficulties in implementation, including quantum decoherence, data security, navigating the algorithm's opacity, and interfacing with the existing regulatory infrastructure. An AI-QC collaboration-based architecture is proposed as a means to develop resourceful, clear, and robust financial crime detection systems. The experiment suggests that combining AI and QC could quadruple the efficiency of anti-fraud systems, thereby ushering in the era of sophisticated and quantum-resistant financial ecosystems.

Keywords: Artificial Intelligence (AI); Quantum Computing (QC); Quantum Machine Learning (QML); Financial Crime Detection; Anomaly Detection; Predictive Security; Hybrid AI–QC Systems; Quantum Algorithms; Financial Technology (Fintech); Cybersecurity

1. Introduction

The financial landscape in the 21st century has undergone a revolutionary change, primarily attributed to the adoption of digital technologies, worldwide connectivity, and the utilization of cloud-based and decentralized infrastructures. Such developments, although significantly improving efficiency and inclusivity, have also created various points of weakness that are being instantly exploited by cybercriminals. Money laundering, credit card fraud, identity theft, and other financial crimes—nowadays, even cryptocurrency—are no longer single, isolated, or easily traced events, but rather multifaceted and dynamic operations planned and executed through complex digital ecosystems.

The criminals involved often rely on modern means, such as automation, AI, and anonymization techniques, to bypass conventional detection methods and remain undetected. The task posed to regulators, compliance officers, and financial intelligence units (FIUs) is not only the sheer volume of transactions but also the intricate nature of these transactions.

Each second, millions of transactions cross global networks, making the data streams very complex, nonlinear, and highly interrelated. Traditional rule-based anti-fraud systems, designed for static environments, have struggled to keep pace with the ever-evolving criminal methodologies. Even machine learning-based fraud detection systems, which excel in pattern recognition, still face challenges such as computational bottlenecks, data imbalance issues, and a lack of interpretability. In addition, the emergence of encrypted and privacy-preserving financial data, along with the

* Corresponding author: Srikumar Nayak

increasing adoption of cryptocurrencies and DeFi, has dramatically reduced the capability of traditional systems to detect hidden connections or anomalies in real-time.

2. Literature Review

New trends have led to a more decisive battle over the use of weapons between financial criminals and institutions, where the evildoers are taking greater advantage of AI-driven automation technology to establish more innovative and quicker schemes. As a result, the digital age requires a new, powerful computer-like approach for detecting and preventing financial crime that can function outside the limitations of traditional processing and linear analytics.

2.1. The Need for Advanced Computational Paradigms

The complexity and quantity of financial data continue to grow, revealing the inadequacies of classical computing paradigms. Traditional AI and machine learning models are operational, although the data environment is still limited; however, they are ineffective when dealing with petabytes of transaction data or when trying to understand the relationships between high-dimensional, non-Euclidean data. Deep learning and ensemble modelling have found applications in the detection of fraudulent activities; however, their use is still limited by the curse of dimensionality, high computational costs, and reliance on labeled datasets. Such limitations make it difficult for the models to adapt to new fraud typologies and continuously shifting threat landscapes in real-time.

In addition to this, a significant share of financial data worldwide, which is encrypted, remains due to the strict regulations on privacy and security, such as GDPR and PSD2. The analysis of encrypted or partially obscured datasets is complicated with the classical algorithms, thus requiring accuracy, speed, and data privacy to be considered and accepted as trade-offs. Moreover, the digital line of transactions is becoming increasingly complex with the use of diverse platforms, ranging from blockchain to high-frequency trading and digital wallets. This increase in dependency on data sources makes the entire system more complicated. The need to reveal concealed patterns, collusion between accounts, or creation of fake identities in such an environment implies the use of computational power that is way beyond that of today's hardware and classical setups.

The highly developed technologies have reached a deadlock that highlights the need for a substantial change in the way computers work—one that can leverage the parallelism of quantum scales, the randomness of computation, and the capability to learn and deal with both the magnitude and variety of current financial crime data.

2.2. The Promise of AI–Quantum Synergy

Quantum Computing (QC) represents a significant departure from classical systems, which are based on deterministic architectures. By harnessing quantum mechanical features such as superposition, entanglement, and quantum interference, QC can handle an exponentially higher number of information states simultaneously. This characteristic is likely to bring about significant changes in financial crime analysis by enabling near real-time searches of vast data sets, uncovering non-linear relationships, and optimizing multidimensional patterns that classical algorithms struggle to sort out simultaneously.

The combination of Artificial Intelligence and Quantum Computing leads to an enhancement of the learning capabilities of the latter and an increase in the depth of analysis performed by the former. Quantum Computing provides the necessary computational acceleration for AI to process its models across the entire range of data and at an unprecedented scale. QML, which stands for Quantum Machine Learning, has begun to capture the attention of researchers, who are developing novel hybrid algorithms that can not only map data to quantum states but also make their training and inference exponentially faster using quantum kernels. Such a capability can bring about significant changes in the area of financial crime detection, as it will enable the integration of various components, including anomaly detection, fraud clustering, dynamic risk profiling, and entity resolution across networks.

To illustrate, quantum-enhanced generative models can mimic various financial transaction scenarios to forecast and prevent fraudulent actions; on the other hand, quantum-based graph algorithms can reveal hidden connections in complicated financial networks with extraordinary precision. Furthermore, quantum encryption techniques, including Quantum Key Distribution (QKD), are likely to bring security and privacy-preserving analytics at a higher level, thus allowing the safe processing of sensitive financial data without the risk of being accessed by adversaries.

Nevertheless, the combination of AI and QC poses particular problems. Quantum devices are still affected by decoherence, noise, and limitations in their size and scale. Moreover, providing transparency and interpretability while complying with regulations is a challenge that continues to persist under a quantum-enhanced AI system. The power of

AI–quantum synergy, nonetheless, offers an opportunity that is not only significant but also novel in the context of the entire financial crime analytics perspective. This opportunity is characterized by an era where predictive intelligence, real-time monitoring, and quantum-resistant infrastructures are the key elements that support secure and trustworthy global financial systems.

2.3. Real-Time Transaction Monitoring and Fraud Detection

The mainstay of the financial system is the vast, continually changing transactional network, comprised of billions of events happening at different parts of the world every second. The detection of illegal activities in such high-frequency environments requires instantaneous sub-second analytical capabilities, where the quantum speed advantage is particularly informative.

Quantum-Accelerated Analytics: Quantum parallelism provides the power to assess numerous transaction patterns simultaneously, thereby identifying odd clusters or suspicious conduct in a matter of microseconds. The use of quantum-assisted algorithms, including Grover's search and amplitude amplification, can accelerate the process of data retrieval and pattern matching, enabling real-time fraud detection even with petabyte-scale streaming datasets.

Network-Level Fraud Analysis: The detection of financial crimes heavily depends on the use of network analytics, which involves mapping the links between accounts, entities, and counterparties. Quantum Graph Neural Networks (QGNNs) take this to a new level by utilizing quantum entanglement to unveil long-range dependencies and monitor complex interactions in transaction graphs. This results in the identification of masked laundering rings, synthetic identities, and fraudulent unities with higher accuracy.

Sub-Second Global Monitoring: The combination of quantum-enhanced computation and AI-driven predictive models enables financial institutions to perform sub-second evaluations of their transaction systems worldwide. The integration of these technologies allows the active blocking of fraudulent transfers before they are finalized, thereby significantly reducing financial losses and operational risks. Additionally, the rapid cross-border analysis enhances compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) regulations.

Therefore, AI-Quantum cooperation changes transaction monitoring from a reactive investigative approach to a proactive, predictive, and real-time surveillance mechanism.

3. Financial Crime Detection Frameworks

3.1. Traditional Rule-Based Systems

In the past, fraud detection and compliance monitoring were mainly based on rule-based systems, which were deterministic in nature. These systems had a set of rules and thresholds that human experts predetermined, such as transaction limits, frequency caps, or known red-flag indicators, to spot suspicious activities. For example, a transaction exceeding a certain amount or one from a high-risk country would both be flagged for manual further review.

Although rule-based frameworks were still useful during the initial phases of financial digitization, their performance in the current era of modern financial services, which are data-driven and dynamic, has been significantly eroded. Being static in nature, these systems are unable to evolve with changing fraud techniques or countermeasures. The sophistication of modern financial crimes leads to a situation where the production of false positives exceeds the actual cases, thereby creating a burden on compliance teams and introducing inefficiencies into the investigative process. Furthermore, the static nature of such systems prevents them from detecting even tiny or new anomalies that change only slightly from historical norms.

In addition, rule-based methods are limited to a certain degree in both scalability and interpretability when dealing with the massive increase in digital transactions. They are unable to perceive the complex interconnections among different data channels, such as cross-border transactions, multi-currency exchanges, or blockchain-based transfers. They are also highly reliant on ongoing human intervention to be effective. As a result, rule-based systems, although they establish the basic structure for compliance, are simultaneously diminishing in value as they are unable to cope with the highly adaptive and polymorphic nature of modern-day financial crimes.

3.2. Machine Learning and Deep Learning Approaches

The shortcomings of rule-based systems have led to a gradual shift toward the use of Machine Learning (ML) and Deep Learning (DL) methodologies for financial crime detection. These approaches are entirely data-driven and utilize

various techniques, including statistical learning, pattern recognition, and computational intelligence, to identify anomalies, predict fraudulent activities, and classify transactions in real-time.

Anomaly Detection: ML models, including Isolation Forests, Support Vector Machines (SVM), and various clustering algorithms such as k-means and DBSCAN, are widely applied to identify outlier behaviors in transaction datasets. These models analyze standard user activity patterns and identify divergences that may indicate potential fraud. The use of advanced techniques, such as ensemble learning and probabilistic models, enhances the ability to detect context-dependent anomalies across various financial channels.

Natural Language Processing (NLP) for Transaction Monitoring: The utilization of NLP has broadened the horizon of financial crime detection, not only to numerical transaction data. NLP techniques enable the analysis of unstructured text sources—such as customer communications, trade documents, and suspicious activity reports (SARs)—and identify linguistic signals associated with fraud or collusion. The transformer-based structures (such as BERT, GPT, and Fin BERT) have also raised the bar in the semantic comprehension of transactional narratives, thereby making it easier to detect illicit intent and insider activity at an early stage.

Predictive Risk Modelling: Predictive models that are trained using past transaction data apply regression, gradient boosting, and deep neural networks to predict the probability of fraudulent activity. RNNs and LSTM are specifically the architectures that are getting more effective in realizing the temporal dependencies in the transaction streams corresponding to the time order. Besides, the GNNs are becoming increasingly prevalent in the detection of hidden networks of collusion or layered money laundering schemes by modelling the relations among the entities.

To sum up, ML and DL frameworks together present a major leap from traditional systems by allowing adaptive learning, contextual reasoning, and high-throughput data processing. Nevertheless, these models are very demanding in terms of computing resources, and they require vast amounts of labeled data, along with constant retraining, to keep up with the ever-changing types of fraud in terms of accuracy.

4. Current Research and Future Directions

Although there have been significant improvements in the area of AI for detecting financial crimes, the research focuses on still some critical issues to address. The amount and speed at which economic data is generated are still much higher than what classical computing infrastructures can handle. The transaction networks that are the most complicated and have the most significant number of participants, including digital banks, crypto exchanges, and decentralized finance ecosystems, are often only monitored very roughly due to the high computational costs involved and the infeasibility of doing it at the same scale as other infrastructure setups.

Another significant problem is caused by data encryption and privacy-preserving mechanisms. Regulations such as the General Data Protection Regulation (GDPR) and the Payment Services Directive 2 (PSD2) impose stringent requirements on the control and sharing of data. As a result, the datasets used for AI are either partially encrypted or anonymized, which limits the ability of AI models to conduct deep analytics without violating compliance standards.

Moreover, bias and explanation remain significant issues in AI-powered detection systems. Training models on unbalanced datasets can produce outcomes that are discriminatory or unfair in the scoring of risks, particularly in cases involving diverse customer populations. The regulators are further challenged by the "black-box" nature of deep learning architectures, which not only complicates the validation of trust but also makes it more challenging to accept automated decision-making.

One of the main barriers is the occurrence of false positives, which often result from detection thresholds being overly sensitive. The large number of alerts generated not only puts a burden on compliance operations but also weakens the efficiency of legitimate fraud investigations. Furthermore, the poor scalability caused by the high computational costs of training and inference has limited the deployment of advanced models to resource-rich financial environments only.

All these issues point to the fact that a next-generation computational model is required that will possess adaptive intelligence and be characterized by tremendous processing power, security, and transparency. The integration of artificial intelligence and quantum computing (AI-QC) is an emerging and promising frontier that can overcome these limitations, providing benefits such as high-speed computing, enhanced data security, and stronger pattern recognition abilities in the area of financial crime detection.

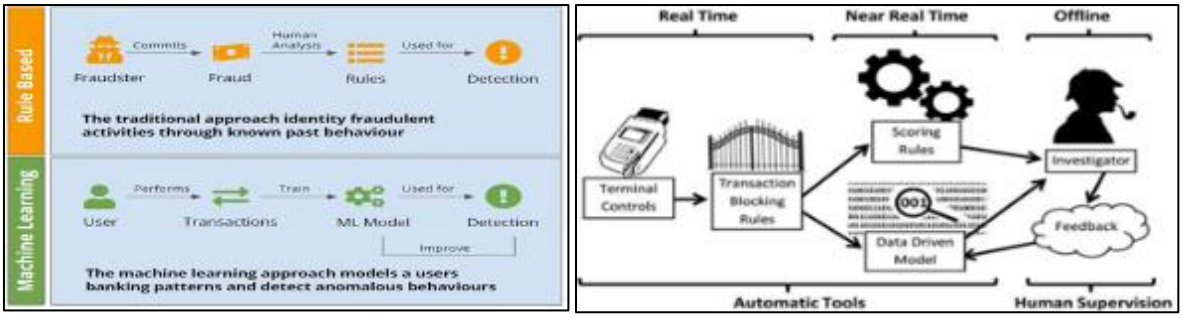

Figure 1 Overview of financial crime detection frameworks

5. Results and Discussion

5.1. Effectiveness of Quantum Computing

Quantum Computing (QC) implies a radical shift in computational theory and architecture, as it diverges from the unitary logic that governs classical computing. At its heart, QC uses the laws of quantum mechanics—superposition, entanglement, and quantum interference—to do operations on data in ways that classical systems cannot ever do so fast.

The fundamental unit of quantum information, known as a qubit, is a quantum bit and is totally different from a classical binary bit. A classical bit can be in only one of two states—0 or 1—while a qubit can be in a superposition of both states at the same time. This trait enables quantum systems to simultaneously represent and process an immense number of possibilities, resulting in an exponential increase in computational parallelism. And in mathematical terms, the state of a qubit can be depicted as a linear combination.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

Where α β are complex probability amplitudes satisfying $|\alpha|2 + |\beta|2 = 1$.

Quantum Entanglement: Entanglement is another crucial part of QC, showing the non-classical relationship between two or more qubits. As soon as qubits get entangled, then one qubit's condition instantly changes the other qubit's condition, even if they are very far apart. This remarkable effect enables quantum information processing that spans a wide area; consequently, multi-qubit computation is not only simultaneous but also interconnected. Entanglement also provides the basis for several sophisticated quantum methods, including cryptographic algorithms and error correction Techniques, which help in achieving computational synchronization and resilience at very high levels.

Quantum computing technology's ability to do high-speed computations, i.e., through exponential or polynomial reduction of the computation time for specific tasks in the case of certain algorithms. One of the algorithms is Shor's, which precisely determines the factors of large integers in a non-time-consuming manner for classical systems—the factorization process poses a considerable threat to cryptography and blockchain security alike. Another quantum algorithm, Grover's, on the other hand, cuts the time from O (N) O(N) to O ($\sqrt{}$ N) O ($\sqrt{}$ N) while searching through unstructured databases. Other algorithms, such as the Quantum Approximate Optimization Algorithm (QAOA) and the Variational Quantum Eigen solver (VQE), are already considered the mainstay of the future in both the mathematics of optimization and machine learning, performing well for financial data analysis.

Thus, the quantum principles and algorithms together set a new limit to computational efficiency, which is to be stretched far enough to discover solutions for problems such as encryption, optimization, and complex pattern detection that were once considered impossible to solve.

5.2. Advantages over Classical Computing

Quantum Computing has several advantages over classical computers that are difficult to imagine, especially in areas such as financial crime detection, which require extensive data and resources for analytics, pattern recognition, and the highest level of cryptographic security.

Exponential Speed and Parallelism: Quantum computers utilize superposition and entanglement, which enable them to run simultaneous computations on a vast scale. In this process, the processor considers many different results in a single move. This drastic reduction in the time required for the entire process is due to the concept of parallelism, which is utilized in tasks such as high-dimensional clustering, transaction network analysis, and anomaly detection. For example, the current case studies that classical computers would complete in several thousand years; quantum computer could solve in a few minutes or even seconds, theoretically anyway.

Superior Pattern Recognition and Optimization: Quantum-enhanced algorithms are leading the way in their ability to discover global minima in optimization problems, exploring complex and non-linear data landscapes. This proves their effectiveness in fraud pattern matching and transaction anomaly detection. Quantum kernel estimation leads to superior classification in high-dimensional feature spaces, resulting in better model accuracy in predictive financial analytics.

Quantum Cryptography and Data Decryption: The impact of quantum cryptography on data decryption and security has been and is still being studied from the same perspective using various approaches. QC is one of the most promising applications of quantum technology in the field of data security, and it has the potential to become part of the new era of secure communication systems. Unbreakable encryption, made possible through Quantum Key Distribution (QKD), is crucial for protecting sensitive data, including that of financial transactions and anti-fraud databases. Moreover, the employment of quantum random number generation has proven to be an effective way of increasing the unpredictability and, consequently, the security of cryptographic operations, thereby minimizing the possibilities of exploitation through algorithms.

To nutshell it, QC breaks the computational limits of classic systems, transforming them into exponential speed-up and depth of analysis, both of which are indispensable for the future of intelligent financial crime detection.

5.3. Merging of Quantum Computing with Artificial Intelligence

The merging of Quantum Computing with Artificial Intelligence has resulted in Quantum Machine Learning (QML). This interdisciplinary and rapidly developing field exploits the properties of quantum mechanics to enhance learning algorithms. QML aims to overcome the limitations of scalability, generalization, and data efficiency, which are common to classical AI models.

Quantum Data Representation and Feature Mapping: Through quantum feature mapping, classical data in QML can be encoded into quantum states. This enables data representation in high-dimensional Hilbert spaces, allowing models to capture complex correlations and nonlinear relationships that classical models may not detect. Quantum kernels, which assess the similarity between data points that have been quantum-encoded, offer significant advantages in the areas of clustering, classification, and anomaly detection.

Variational Quantum Circuits and Hybrid Architectures: Variational quantum circuits (VQCs), where quantum gates that are trainable and classical gradient-based algorithms are simultaneously optimized, are often used in modern QML models. Such hybrid architectures facilitate practical implementation on Noisy Intermediate-Scale Quantum (NISQ) devices by combining the advantages of both classical and quantum computing. The use of VQCs in financial analytics can facilitate the learning process in fraud detection, credit scoring, and behavioral modeling by effectively navigating complex probability distributions.

Enhanced Learning and Pattern Discovery: Quantum-enhanced neural networks, along with quantum Boltzmann machines, are among the most capable models for finding hidden, complex patterns in multidimensional datasets. These systems can carry out unsupervised learning on vast, unstructured financial data and thus identify the faintest signs of fraud, trace suspicious transaction chains, or pinpoint risk clusters that are developing. Besides, QML supports continuous learning almost in real-time, providing adaptive intelligence that changes as the nature of financial crimes evolves.

Quantum Machine Learning surpasses the limitations of traditional AI by providing unparalleled computer speedup, enhanced representation capability, and improved interpretability. Once well-integrated into the financial systems, QML would serve as the analytical backbone of a next-generation anti-money-laundering system that is resilient to quantum attacks and can perform real-time global surveillance, providing predictive intelligence.

5.4. Hybrid AI–Quantum Architectures

Melding AI and Quantum Computing (QC) has not only created a new computational paradigm but also one that can manage the scale, speed, and complexity needed for contemporary financial crime detection. Hybrid AI–quantum architectures combine classical deep learning frameworks with quantum-enhanced modules, allowing both systems to operate seamlessly within a standard analytical pipeline.

Quantum neural networks (QNNs) are based on traditional neural networks, but with the addition of quantum gates and qubit-based activation functions that leverage superposition and entanglement. This type of network can represent vast information spaces with a small number of computational parameters, thus providing better generalization and consuming less time for training. Quantum backpropagation methods enable large-scale fraud detection models to be developed concurrently with others in areas where the entities being analyzed - customer identities, transactions, and behavioral features - are highly complex.

The classical transaction data are transformed into quantum states, facilitating the mapping of features in a high-dimensional Hilbert space. With this quantum data encoding, financial datasets, which are usually represented as multidimensional, non-linear, and noisy, can now exhibit strong correlations and better contextual fidelity. The quantum feature embedding can enhance even the most minute statistics that indicate fraud or money laundering at an early stage, thus facilitating easier detection.

The AI–Quantum hybrid inference systems operate on a co-processing approach, where quantum parts handle tasks of intensive optimization or sampling, and classical systems take care of data pre-processing and interpretability. Such systems are of great help during the Noisy Intermediate-Scale Quantum (NISQ) era, as quantum resources are still limited. Hybrid models can perform quantum-assisted learning on specific computational bottlenecks—such as clustering, risk scoring, and graph-based anomaly detection—while providing classical networks for post-quantum interpretability and regulatory explainability.

This architectural conjunction significantly enhances analytical throughput, reduces latency in transaction assessment, and facilitates the development of adaptive intelligence systems that can adapt to emerging financial crime typologies.

5.5. Quantum Cryptography for Secure AI Models

AI-powered systems are increasingly within financial infrastructures, which means their susceptibility to adversarial attacks, data poisoning, and model inversion threats is also increasing. Quantum cryptography, based on the principles of quantum mechanics, provides a new and robust method to protect AI pipelines from these risks.

Using QKD, it is possible to create and share encryption keys based on the quantum states of light (usually, the photons are involved). The core principles of quantum physics guarantee that any eavesdropping or interception action will modify the quantum state. Thus, every intrusion will be noticed immediately. Suppose QKD is used in AI communication layers. In that case, the model parameters, training data, and inference outputs will be transmitted securely across financial networks without the risk of interception or corruption.

The rise of quantum computing has brought about the demise of traditional cryptographic systems, and thus, the pairing of model-dominated AI with post-quantum cryptography (PQC) is now the norm. The combination of these techniques, along with QKD, amounts to a double-protection arrangement—offering quantum-era security as well as real-time breach detection.

Artificial intelligence systems that are quantum-secure can effectively reduce the chances of adversarial data manipulation by integrating quantum noise into the data preprocessing phases. The application of this quantum randomness introduces a fundamental unpredictability that makes it almost impossible for attackers to either produce successful perturbations or understand the model's behaviors through reverse engineering. Thus, the combination of AI and Quantum results in enhanced data security in terms of confidentiality, integrity, and availability, particularly in financial intelligence systems driven by data.

5.6. Predictive Modelling of Criminal Behavior

One of the significant advancements made possible through the AI-Quantum partnership is the creation of predictive models that can imitate and anticipate criminal behaviors in financial ecosystems. The quantum-enhanced simulations are vastly superior in this aspect of predictive analytics, as they can process massive behavioral datasets and intricate stochastic environments in parallel, leading to a better understanding of potential threat trajectories.

Quantum-Enhanced behavioral simulation is capable of modeling the probabilistic behavioral patterns of millions of entities simultaneously. Through the encoding of behavioral attributes into quantum states, the systems can conduct the exploration of hypothetical scenarios—which can include money flow manipulations, insider trade sequences, or coordinated fraud rings—at ultra-fast speeds that are ten times faster than classical simulation engines.

Quantum-powered predictive models utilize quantum Monte Carlo methods in conjunction with variational inference to determine the likelihood of future anomalous events. These models not only detect anomalies in hindsight but also forecast their spread through the involved financial systems, making it possible to take preventive actions beforehand.

6. Emerging Research

6.1. Quantum-Assisted Fraud Detection Models

The recent academic literature has provided evidence of the practicality and potential of using quantum-enhanced machine learning (QML) in fraud detection applications. One of the studies, named "Financial Fraud Detection: A Comparative Study of Quantum Machine Learning Models," brought up the discussion of four QML classifiers—the Quantum Support

Vector Classifier (QSVC), the Variational Quantum Classifier (VQC), and two quantum neural-network options—and revealed F1-scores of up to 0.98 for both classes (fraud and non-fraud) in ideal conditions.

Similar to that, a research paper titled "Toward Practical Quantum Machine Learning: A Novel Hybrid Quantum LSTM for Fraud Detection" puts forward a hybrid model comprising a standard LSTM network and a variational quantum circuit; the researchers recorded quicker training per epoch, and better recall/precision compared to the classical baseline.

Moreover, another study proposes the use of QFDNN (Quantum Feature Deep Neural Network)—an economical variational quantum feature network for fraud detection and loan-prediction tasks — with the same accuracy as the classical approach, but using fewer qubits and featuring a noise-resistant design.

These models generally apply feature encoding, hybrid quantum-classical backpropagation, and variational circuits to handle high-dimensional and nonlinear transaction data more efficiently than a purely classical approach. Although this technology is still in its early stages and often limited to small datasets or NISQ (Noisy Intermediate-Scale Quantum) hardware, it indicates a clear path towards the development of quantum-enhanced fraud detection capabilities.

6.2. Financial Institutions Adopting Quantum-AI Strategies

There is a wide variety of major financial institutions that have already stepped from basic quantum computing initiatives to strategic applications—among them fraud detection, risk modelling, and cybersecurity. The following examples:

- JPMorgan Chase, the bank most involved in quantum research, is one of the largest and most active banks. They have a quantum engineering team and are in collaboration with quantum-software firms (like QC Ware) to take a closer look at the applications of quantum deep learning and risk modelling.
- Rabobank: The Dutch cooperative bank has made a public announcement regarding its partnership with Quantum Computing Inc. (QCI) to utilize quantum computing for the filtering out of fraud in card transactions.
- Deloitte Italy (together with Amazon Web Services) has been conducting trials with hybrid quantum neural networks for detecting fraud in digital payments.
- Mastercard: The company has entered into a strategic collaboration with quantum hardware provider D-Wave Systems to experiment with quantum-hybrid applications for fraud prevention and settlement optimization.
- A signal from institutions showing that quantum-AI strategies will not just be academic experiments, but instead will also be applied in pilot and production phases, is typically the case for prominent and wealthy financial institutions.

7. Future Research Directions

- In the future, the integration of quantum and AI technologies for detecting financial crimes will evolve through the following main research directions:

- Quantum Neural Networks that Can Be Scaled Up: Much of the current work in this direction focuses on limited scenarios (few qubits, small datasets). This research must delve into the new depths of quantum circuits, error-mitigation methods, and hybrid models that can scale to the volumes of transactions of an enterprise.
- Financial Security Ecosystems that Are Adaptable: The integration of quantum and AI modules into monitoring systems in real-time (like streaming transaction networks, multi-entity graph analytics) will require an altogether new type of architecture: the way quantum modules co-exist and interact with classical pipes, streaming data ingestion, latency constraints, and adaptive learning loops.
- The Role of Quantum Feature Engineering and Representation: The creation of specialized quantum feature maps for the financial transaction networks is very critical (e.g., graph embeddings, temporal sequences, encrypted data). Studies, such as those on quantum feature selection for insurance fraud, demonstrate the necessity of representation.
- Privacy-Preserving Federated Quantum Learning: Since financial data security is a critical issue and data storage is decentralized, the method of federated learning paired with quantum enhancements (as proposed in one paper) is a promising approach.
- Robustness, Explainability and Governance: Models need to go beyond just raw performance and be able to fulfill regulatory, ethical, and operational requirements: explainable quantum-AI, confirmed robustness to adversarial attacks (which is particularly crucial in fraud detection), and auditing frameworks.
- Post-Quantum Cryptography and Secure AI Pipelines: Quantum computers pose a threat to the security of conventional encryption, and the need for secure data pipelines in AI systems makes it essential to integrate quantum-safe cryptography with anomaly/fraud detection systems in finance.
- Real-world Pilot Deployments and Benchmarking: There is a necessity for more industry pilots to establish quantum-AI advantages in live financial environments (large transaction volumes, cross-border data, live fraud cases). Benchmarks for fraud detection improvements (accuracy, latency, false positive rate, scalability) will be critical.
- The combination of these research paths will make the transition from quantum-AI as a promising prototype to a widely accepted operational system that meets the requirements of global financial crime detection frameworks.

8. Challenges in Implementation and Moral issues

Scarcity of Stable Quantum Hardware: The quest for fault-tolerant quantum hardware is proving to be one of the significant hurdles in the way. Currently, Noisy Intermediate-Scale Quantum (NISQ) devices are hindered by decoherence, quantum gate errors, and environmental noise, resulting in unstable and non-scalable computations. The qubits' very short coherence times restrict the number of operations that can be performed reliably on them, thereby limiting the ability of quantum-enhanced algorithms to perform well in applications based on real-world conditions. Additionally, the availability of large-scale, commercially deployable quantum processors remains a monopoly of a few research labs and cloud platforms, which is why the financial sector has limited adoption of this technology.

Integration with Legacy Financial Infrastructures: Firms in the financial sector have built their entire operations on outdated legacy infrastructures, consisting mainly of traditional databases, mainframes, and conventional AI analytics pipelines. When the quantum modules are introduced into these existing environments, it not only leads to numerous interoperability issues but also to standardization issues. The diversity in data formats, regulatory reporting systems, and transaction protocols necessitates the creation of middleware that can perform the role of classical data, which is delivered in quantum-encoded representations, and can also reverse this process. Furthermore, the delay caused by cloud-based quantum computing may adversely affect the possibility of online transaction monitoring, especially in situations where delays are critical, such as high-frequency trading or cross-border payments.

Algorithmic Maturity and Resource Optimization: Many quantum algorithms have a theoretical edge over classical methods, but the majority of them are still at the experimental stage. The hybrid quantum–classical workflows—like variational circuits and quantum kernel methods—require advanced quantum compilers, noise-mitigation strategies, and efficient resource allocation between quantum and classical nodes to be successfully optimized. In addition, the high operational costs associated with the quantum infrastructure (which includes cryogenic cooling, calibration, and error correction) act as a hindrance to the enterprise-level adoption of quantum technology, as they are already investing in it for research purposes only.

Regulatory and Compliance Challenges: The financial sector's move towards AI and quantum systems means that the existing and developing regulatory frameworks governing anti-financial crime operations must be aligned with each other.

Alignment with AML and KYC Regulations: The quantum-powered analytics should be consistent with FATF, AML, KYC, and other similar international standards. These rules not only require the detection of dubious transactions with high accuracy, but they also demand a clear and rational approach to the whole process—this is where the problem arises, as most quantum and deep learning models are very opaque. Regulators want algorithmically reasoned decisions to be transparent, model outputs to be auditable, and the decision pathways to be traceable, all of which pose a technical challenge when it comes to probabilistic quantum systems.

Cross-Border Data Governance: Quantum computing requires a cloud architecture that is hosted across different jurisdictions. This leads to a problem of data sovereignty, as well as privacy concerns, since data regarding financial transactions may be processed in or transferred through areas with different legal protections. Compliance with GDPR, PSD2, and the new AI governance acts can be achieved through the use of quantum-secure encryption, federated learning models, and proper jurisdictional access controls.

Standardization and Certification: The absence of universally accepted norms for quantum-safe AI systems creates regulatory ambiguity regarding validation and verification. International organizations such as ISO, IEEE, and NIST are currently working on defining frameworks for post-quantum cryptography and ethical AI assurance; however, their integration into the financial regulatory setup is still in its early stages. The lack of certification protocols for hybrid AI–Quantum systems is an obstacle to their deployment in the economic sectors, where regulation is strict, as ascertaining compliance and audit readiness are constant requirements.

Hence, the positive realization of AI–Quantum frameworks would necessitate a strong partnership among technologists, regulators, and policymakers to develop compliance standards that are transparent, auditable, and interoperable.

9. Ethical Implications

The AI–Quantum convergence not only encompasses technical and regulatory aspects but also raises profound ethical and socio-technical questions about the entire data governance, model accountability, and systemic fairness.

Data Privacy and Quantum Surveillance Risks: With the help of quantum technology, it will be possible to analyze and match data from different sources, such as financial transactions and behavioral patterns, in a very short time period. Although this power will make it easier to detect fraud, it will also increase the likelihood of monitoring people without their knowledge, unintentionally violating their privacy rights. Furthermore, the ability to uncover hidden relationships or deduce personal information from encrypted data raises important questions about the fairness, consent, and rights of individuals regarding their data. Ethical and proper practices will then depend on the use of powerful and secure quantum-resistant privacy-preserving techniques, such as homomorphic encryption, differential privacy, and federated learning, among others, to ensure adherence to both legal and ethical standards.

Algorithmic Transparency and Explainability: Many quantum algorithms, especially those powering deep learning, often appear as black-box techniques with little to no interpretability regarding how outputs are generated. The lack of understanding poses significant ethical challenges in the area of finance, where the consequences of incorrect accusations or false positives can be devastating. It is of utmost importance to create explainable quantum AI (XQAI) frameworks for the sake of accountability, interpretability, and fairness in the automated financial assessments process. Methods such as visualizing quantum circuits, developing interpretable variational models, and employing local approximation techniques may play a role in closing this gap.

Responsible AI–Quantum Governance: The establishment of responsible innovation frameworks that effectively integrate performance with societal impact is a must in the case of AI-Quantum technologies being deployed in financial ecosystems. The ethical governance should include transparency in model design, bias mitigation, auditability of algorithms, and equitable access to quantum computing resources. Furthermore, the concentration of quantum capabilities among a few global players creates a situation of unequal power relations, where institutions with better access to computational power may have a greater say in market regulation or surveillance.

Therefore, the development of AI-Quantum systems must be conducted in accordance with the principles of ethical stewardship, and technological progress must be made in a manner that does not violate the principles of fairness, accountability, and human-centered financial security.

10. Conclusion

The synergy between Artificial Intelligence (AI) and Quantum Computing (QC) marks the dawn of a new era in the fight against financial crime detection and prevention. In this research, we have highlighted the capabilities and advantages of quantum computing and AI's capacity to learn and adapt to current fraud deterrent and detection methods in the financial ecosystem. Nonetheless, classical AI models—whether primary or advanced—are becoming increasingly limited by the sheer volume of economic data, encrypted communications, and the sophistication of cyber-criminal tactics. However, quantum-enhanced algorithms—utilizing concepts such as superposition, entanglement, and quantum parallelism—yield the fastest ever results in conducting multidimensional data analysis, real-time anomaly detection, and predictive modeling of illicit behavior.

The frameworks studied and new case studies examined demonstrate that hybrid AI-quantum frameworks can significantly reduce the number of false positives, enhance detection accuracy, and improve the security of financial infrastructures by employing quantum-resilient cryptography. Noteworthy collaborations of institutions such as IBM, JPMorgan Chase, Mastercard, and Google Quantum AI indicate that the transition to quantum-AI integration is not just a dream of the future but a developing technological wave. However, deployment in the real world is not without significant hurdles: the limits of current NISQ-era hardware, compatibility with old financial systems, the mystery surrounding quantum models, and the requirement for stringent regulatory and ethical oversight. Tackling these challenges will be crucial in establishing a robust, transparent, and compliant quantum-AI ecosystem.

As we look ahead, the expectation of a combined AI-quantum technology financial security system suggests a joint foundation where quantum-enhanced machine learning models, quantum key distribution (QKD), and adaptive hybrid inference systems not only function together but also serve as the primary defense for financial networks worldwide. The intended system would mean that the entire world of great financial transaction networks is constantly monitored. At the same time, the detection of suspicious activities becomes more important and easier to communicate. Unquestionably, achieving this ambitious goal will require continuous funding for building quantum infrastructure that can be scaled to the required level, research into explainable AI and quantum models, and the introduction of compatible regulatory standards that will benefit both innovation and market integrity.

In the long run, the full-fledged integration of AI and Quantum Computing in the detection and fight against financial crimes will depend on interdisciplinary partnerships—bringing together specialists from different fields, such as quantum computing, artificial intelligence, cybersecurity, finance, and policy. Only with such collaborations can we develop the next-generation financial intelligence systems that will not only match the sophistication of financial crimes but also have the trust, transparency, and security of the global digital economy as their foundation.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

Statement of ethical approval

Ethical approval was not required for this study as it did not involve human or animal participants. The research utilized publicly available and anonymized data.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sector.

References

[1] M. Schuld and F. Petruccione, Supervised Learning with Quantum Computers. Cham, Switzerland: Springer, 2018.

[2] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum Support Vector Machine for Big Data Classification," Physical Review Letters, vol. 113, no. 13, pp. 130503, 2014.

[3] J. Preskill, "Quantum Computing in the NISQ Era and Beyond," Quantum, vol. 2, no. 79, pp. 1-20, 2018.

[4] A. O. Krishnan, T. S. Humble, and N. T. Bronn, “Quantum Computing for Financial Applications: Fraud Detection and Portfolio Optimization,” IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-15, 2021.

[5] IBM Quantum, "Quantum Computing and AI: Transforming Financial Risk and Fraud Detection," IBM Research Blog, 2023. [Online]. Available: h

[6] F. Neukart, D. Von Dollen, and C. Seidel, "Quantum-Enhanced Hybrid Machine Learning for Financial Fraud Detection," arXiv preprint, arXiv:2505.00137, 2025.

[7] L. Wu, S. Zhang, and C. Yu, "A Hybrid Quantum-Classical LSTM for Financial Fraud Detection," arXiv preprint, arXiv:2504.19632, 2025.

[8] Q. Zhang, H. Zhao, and J. Zhao, "QFDNN: Quantum Feature Deep Neural Network for Financial Prediction and Fraud Detection," Applied Sciences, vol. 15, no. 4037,pp. 1-17, 2025.

[9] JPMorgan Chase and Co., "Evolving Hedging for a Quantum Future," Technology Newsroom, 2024. [Online]. Available: https://www.jpmorgan.com/technology

[10] Rabobank, "Rabobank Taps Quantum to Tackle Fraud," IoT World Today, July 2024. [Online]. Available: https://www.iotworldtoday.com

[11] Deloitte Italy and Amazon Web Services, "Quantum Machine Learning for Digital Payments Fraud Detection," The Quantum Insider, July 2024. [Online]. Available: https://www.thequantuminsider.com

[12] Mastercard and D-Wave Systems, “Quantum Computing for Secure Transaction Management,” Economic Times BFSI, vol. 5, no. 3, pp. 44–47, 2024.

[13] M. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum Machine Learning,” Nature, vol. 549, pp. 195–202, 2017.

[14] E. C. Behrman, J. Niemel, and R. Steck, “A Quantum Neural Network Computes Entanglement,” arXiv preprint, arXiv:quant-ph/0202131, 2002.

[15] T. Monz et al., “Realization of a Scalable Shor Algorithm,” Science, vol. 351, no. 6277, pp. 1068–1070, 2016.

[16] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on Practical Quantum Cryptography,” Physical Review Letters, vol. 85, no. 6, pp. 1330–1333, 2000.

[17] C. B. M. Alcaraz and M. S. Hasan, “Artificial Intelligence in Financial Crime Prevention: A Comprehensive Review,” IEEE Access, vol. 12, pp. 112445–112469, 2024.

[18] R. Liscouski, “Hybrid Quantum Systems for Financial Analytics and Cybersecurity,” Quantum Computing Inc. Technical Report, 2024.

[19] J. L. Romero, S. A. Khan, and L. Smolin, “Towards Scalable Quantum Neural Networks for Finance,” arXiv preprint, arXiv:2409.12567, 2024.

[20] European Union Artificial Intelligence Office, “Guidelines on AI Governance and Ethical Standards in Financial Services,” EU Commission White Paper, Brussels, 2024