



ARTIFICIAL INTELLIGENCE AND QUANTUM COMPUTING FOR FINANCIAL CRIME DETECTION IN FINANCIAL NETWORKS

Wisdom Sahr Korsor

Master's Student, Rashtriya Raksha University, Gujarat, India, School of Behavioural Sciences and Financial Investigations,
Email ID: wisdomskorsor@gmail.com, ORCID ID: 0009-0006-2493-4109

Received:- 01-07-2026 Revised:- 18-08-2026 Acceptance:- 16-09-2026 Published:-05-10-2026

Abstract

Increasing volumes and complexity of transactions, financial account interconnection, more cross-border transactions, fraud techniques continuously shifting, and other issues are creating a more complex transaction landscape that is increasingly hard to define. AI, machine learning, deep learning, graph analytics, and newfound quantum machine learning (QML) have, therefore, become more and more popular as financial fraud detection and financial-crime prevention tools. Moreover, this paper aims to compare classical machine learning methods, deep learning methods, graph/network methods, quantum machine learning with classical machine learning, and hybrid quantum-classical methods for financial-crime detection based on evidence-based synthesis. The study addresses four research questions concerning existing AI-based financial-crime detection methods, comparative performance, evidence for QML and quantum optimization, and technical and operational implementation challenges. The comparative synthesis of recent peer-reviewed research indicates that the classical family of ML is the most practically matured and support vector machines, neural network approach and anomaly detection approach were among the approaches. The data set sizes for which it has been demonstrated as valid are rather limited and, in some cases, very few in number, for low-dimensional feature spaces, experimental setups, and/or problems. As argued here, the most secure short-term architecture would be to utilize classical AI while complementing it with network analytics to complete the truly essential tasks – but complementing the most with quantum and hybrid processors for subproblems that are hard to solve with classical methods. The paper concludes with an agenda of research avenues concerning realistic networks of financial transactions, standardization of metrics for evaluating financial networks, testing over time, explainability, learning in a privacy-preserving way, test drift, as well as benchmarks (classical/quantum) with reproducible results.

Keywords: *artificial intelligence; financial crime; financial fraud; anti-money laundering; machine learning; deep learning; graph neural networks; quantum machine learning; quantum computing; financial networks; anomaly detection.*

1. Introduction

Financial crime is no longer conducted on an ad hoc basis, but is the part of more complex financial series of transactions in a complex and interconnected digital financial ecosystem. The suspicious event may be a cross-jurisdiction event, which may be cross-device event, cross-accounts event, cross-merchant event, cross-payment channel event and/or cross-corporate event. This system is statistical, temporal, relational and operational in nature and is a detection problem. While it's important to keep monitoring known patterns with traditional rules, where a crime shifts rapidly – or where activity that may be regarded as suspicious is occurring across many apparently normal transactions, adhering to a set of rules becomes difficult.

With the advent of artificial intelligence, there have been an increasing number of detection methods. Patterns can be difficult to manually encode, but can be learnt by machine learning models that can be used for risk estimation and to classify transactions and detect anomalies. Ali et al. found out from a systematic literature review (SVM) some of the commonly used techniques including use of artificial neural network (ANN) and from fraud type analysis, the most commonly used fraud type was credit card fraud [1]. In more recent studies by Hernandez Aros et al (PRISMA and Kitchenham) it was found that over 100 studies had been examined in the last 12 years (between 2012-2023), with studies still underway that are using machine-learning techniques for financial fraud [2].

At the same time, quantum computing has brought about a new field of research. The application of machine learning is either based on quantum circuits, or based on the optimization in machine learning assisted by quantum. Some suggested techniques are: quantum support vector machines (QSVM), variational quantum classifiers (VQC); quantum neural networks (QNN); quantum kernels; quantum optimisation algorithms. In 2026, a systematic review on the state-of-the-art of classical and quantum machine learning applications in finance was performed by abovementioned authors, confirming that the area of quantum machine learning is a newly emerging frontier of finance and the authors pointed out various quantum finance applications, technical challenges and possible hybrid quantum/classical systems [3].

The question now is whether they'll be able to detect fraud or not with quantum computing. More relevant question actually is how good are classical AI, deep learning, graph analytics, quantum techniques, and hybrids at predicting outcomes of such learning, how much data do they need as inputs, how easily and widely can they be scaled, how easily can they be explained, what is their cost, and how easily they can be used in real-world. It's worth to note this distinction is not necessarily observed in the financial-crime industry where the false-positive rates are typically much higher, labels are less accessible, there is more emphasis on rules for privacy instead of concepts, there is more emphasis on concept drift, and the labels are often not known until much later.

1.1 Research Problem

This could be a significant body of resources available, though it's quite fragmented. Most of the studies employ only one fraud database and/or only one algorithm. Other reviews are focused on classical machine learning, and they don't cover more recent literature on quantum information; new work on quantum information may take advantage of settings that have great control, and cannot really be equalized with the setting of the financial system in action. An integrated view is required, that is, a single financial-crime-detection system that incorporates the different approaches: classical AI, deep learning, graph based and quantum/hybrid.

1.2 Research Questions

- RQ1. Which are some of the financial-crime detection methods that are based on techniques of artificial-intelligence and machine learning?
- RQ2. Discuss pros and cons of classical machine-learning technique, deep-learning technique and network-based techniques—when it comes to financial fraud and financial fraud detection.
- RQ3. After all what is the real proof for the use of quantum machine learning, hybrid quantum/machine learning, and hybrid quantum/classical in the detection of financial crimes?
- RQ4. What will be the technical, computational, regulatory and operational hurdles involved with the implementation of AI and quantum computers in the finance sector related to financial certainly or financial crime detection in financial networks?

1.3 Objectives

- To develop an overview of the main pattern recognition techniques which are based on AI and ML in the detection process of financial crimes.
- To compare classical ML, deep learning, graph/network analytics, QML, and hybrid approaches using performance and deployment criteria.
- To test the strength of the current evidence in support of the possibility of quantum advantage to the detection of financial crimes.
- To create a comprehensive theoretical approach to monitoring financial networks with the help of AI and quantum technologies.
- To cast light on the areas of research which needed to be investigated and suggest a feasible research programme for future empirical research.

2. Background and Literature Review

2.1 Financial Crime Detection

In financial crime, every type or context of payment, card, account takeover, insurance, securities, cyber-enabled financial crime, money laundering and other types of financial crime are involved. For these categories, a detection problem is different in two respects: labels are different and the structure of the transactions is different as is the time horizon and investigative workflow. A supervised fraud classifier might be more appropriate if there is an established pattern or organized activity that occurs; if there is not an established pattern or a coordinated activity (or maybe not), use anomaly detection or network analytics might be more appropriate.

One of the issues is that of class unbalance. Typically, fraud and/or unusual transactions are a small percentage of the total number of observations. A sense of timescales also doesn't mean much: If a newly designed classifier had been very accurate, but caught only a small amount of cases where there was fraud, there was little value in its accuracy. For many applications, therefore, precision, recall, F1 score, area under the precision-recall curve (AUPRC), false positive rate and ability to detect a negative (false negative rate) and cost-sensitive measures are more informative [1,2].

2.2 Classical Machine Learning

Currently, the most old technology used for financial fraud detection is the classical ML. Logistic regression is a simple model that can be used to obtain interpretable baseline classification and decision trees can model rules that are easily interpretable; random forest and gradient boosting models are appropriate for high dimensional classification problems, because they can model nonlinear relationships. There is a lot of classical applications for ML as scanned by Ali et al. in [1] and it features two of the popular approaches, SVM and NN based.

Classical ML is highly matured and has developed software ecosystems, low hardware requirements, a wellknown training process and the ability to integrate engineered financial characteristics. When the transactions, however, differ in their behaviour over time then their performance can become problematic. Class imbalance, leaky data and label delay and temporal dependence are also important issues to deal with carefully for models.

2.3 Deep Learning

Deep-learning models are able to learn high dimensional representations that are nonlinear from large sets of data. Recurrent architectures – such as LSTM networks – can be used for the order of transactions is important and autoencoders can be used to detect artefacts. If the transactions are structured (sequences, feature matrices or other structures) more complex patterns can be identified using convolutional or transformer-based approaches. Deep learning is great because it isn't all that much computation, or it doesn't require the engineer to mess with a ton of features, but it can be somewhat expensive and it can be very hard for people to understand what out comes of deep learning.

2.4 Graph and Financial-Network Analytics

Financial crime is often committed 'relational'. Even if a transaction is suspicious, it may be hard to find evidence of the suspiciousness within that single transaction, but can be very suspicious when combined with a series of transactions, merchants, devices, companies or beneficiaries. Graph analytics is a mapping solution for visualizing people, objects and relationships as nodes, details on these can be linked together and patterns of relationship can be highlighted. Another particularly

salient type of networks is graph neural networks (GNNs) which can learn representations from features of the nodes and the graph structure. Detecting financial frauds have been already achieved in recent years by using explicit GNNs along with CNN and LSTM [6].

2.5 Quantum Machine Learning

Quantum machine learning will be the linkage of quantum circuits with the machine-learning workflow. These are: QSVM, Variational Quantum Classifiers, Quantum Neuro networks, Quantum Kernels and Quantum-assisted optimization. The motivation for the theory is that, if quantum computation exist, there might be certain problems in which computation is more advantageous in terms of the quantum state representation and the structure of the algorithm as compared to classical computation. But there are compulsory differences between the benefits and the true benefits.

What has occurred in recent literature is a transition from 'concept' to 'real comparison? El Alami et al. [5] made a comparison of how 2026 credit card fraud detection could be done in 2 different architectures. Weinberg and Faccia also examined quantum algorithms as one of the next chances for financial-crime prevention, thereby illustrating the capability of quantum algorithms, but it's put in parallel with traditional ML [4]. They are not an exact indicator of the growing prominence of quantum research – they are simply measures of growing activity in research.

2.6 Hybrid Quantum-Classical Approaches

In the foreseeable future hybrid may be more practical, owing to the noise, limited number of qubits, depth and cost of data encoding in the existing quantum hardware. To perform a given optimization or classification problem, a combination of classical computing for data processing, feature engineering, large-scale processing and/or decision support along with a quantum circuit. For the detection of financial fraud, Yu and Luo have proposed a deep belief networks and quantum optimization algorithm based financial fraud detection system which comprises of CNN, LSTM and GNN modules [6]. They have been found to be promising up to now, however not replicated in other designs of financial systems and shouldn't be assumed to be true in all financial systems.

2.7 Synthesis of Existing Evidence

Evidence source	Scope	Main contribution	Implication for this study
Ali et al. (2022) [1]	93 ML fraud studies	Maps ML algorithms, datasets, and evaluation practices	Classical ML has substantial empirical maturity
Hernandez Aros et al. (2024) [2]	104 studies, 2012–2023	PRISMA/Kitchenham review of ML fraud detection	Evidence base is broad but heterogeneous
Murugaraj et al. (2026) [3]	Classical and QML in finance	Integrates ML/QML applications and limitations	Hybrid models merit focused investigation
Weinberg & Faccia (2026) [4]	Quantum algorithms and financial crime	Examines quantum potential for crime prevention	Quantum research is emerging, not yet operationally established
El Alami et al. (2026) [5]	QML architectures for card fraud	Comparative QML evaluation	Direct benchmarking is increasingly important
Yu & Luo (2025) [6]	Hybrid DBN + quantum optimization	Combines CNN/LSTM/GNN with quantum optimization	Network-aware hybrid models are promising but need replication

3. Materials and Methods

This study adopts a structured comparative literature-synthesis approach. Rather than developing and experimentally testing a new fraud-detection model, the study organizes published evidence across classical machine learning, deep learning, graph and network analytics, quantum-classical approaches. The literature is compared according to financial-crime application, model family, dataset characteristics, evaluation metrics, network representation, quantum component, explainability, computational requirements, and evidence of real-world deployment. This approach enables a comparative assessment of the maturity, strengths, limitations, and potential roles of different computational approaches in financial-crime detection.

3.1 Search Strategy

The literature was examined using established academic sources, including IEEE Xplore, ScienceDirect, SpringerLink, Scopus, ACM Digital Library, and Google Scholar. The search focused on literature addressing financial crime and fraud detection, artificial intelligence and machine learning, deep learning, financial networks and anti-money laundering, quantum computing, and quantum machine learning. Particular attention was given to peer-reviewed studies between 2019 and 2026, while selected landmark studies were retained to provide conceptual foundations. The identified literature was comparatively synthesized according to model family, financial-crime application, evaluation criteria, network representation, quantum component, explainability, and deployment considerations.

3.2 Inclusion Criteria

- Any peer reviewed research journal/conference publications that are specifically dedicated to financial fraud, financial crime, AML, suspicious-transaction detection or financial-risk detection in general.
- Comparisons between approaches using machine learning (deep learning, graph/network based, quantum based, hybrid quantum-classical based) and a comparison to an approach using classical computing.
- Empirical studies reporting results, comparative studies reporting results, methodologically-related studies, and/or a structured review related to the research questions
- The works and articles in English published in academically recognised databases.
- Special attention has been paid to the latest studies (2019-2026) and landmark studies have been presented as conceptual foundations.

3.3 Exclusion Criteria

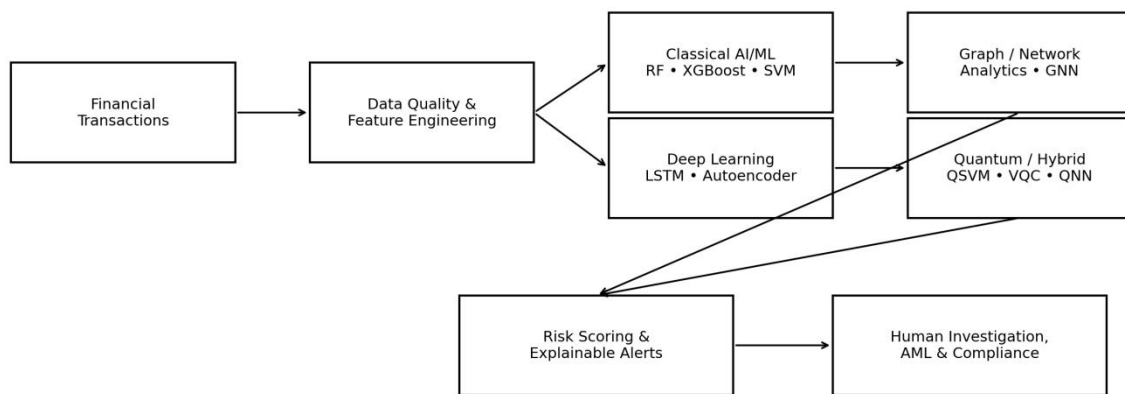
- The articles that do not have any relevance to the financial crime / financial-risk-detection have been removed.
- Studies containing unsupported claims of quantum advantage without sufficient empirical or methodological evidence were excluded.
- Studies without methodology description or appropriately to analyse the obtained result.
- If publishing more than once in the same study, multiple articles and/or multiple copies of a single study.
- Theoretical papers only relevant to quantum computing, and not finance.

3.4 Data Extraction Framework

A standardized data-extraction matrix was used to record the characteristics of eligible studies. The extracted variables included study identification, Crime type, Dataset, Number and type of observations, Class-imbalance strategy, Model Family, Feature representation (where applicable), Network representation (where applicable), Training/validation strategy, Evaluation metrics, Key result, Computational environment, Explainability approach, Limitations, and Evidence of real-world deployment.

Variable	Extraction rule
Crime/application	Fraud, AML, suspicious transactions, card fraud, etc.
Dataset	Public, proprietary, synthetic, simulated, or mixed
Model	LR, RF, XGBoost, SVM, ANN, LSTM,

	GNN, QSVM, VQC, QNN, hybrid, etc.
Validation	Random split, cross-validation, temporal split, external validation
Metrics	Precision, recall, F1, ROC-AUC, PR-AUC/AUPRC, false-positive rate, cost
Quantum component	None, quantum kernel, QSVM, VQC, QNN, optimization, hybrid
Network component	None, graph features, graph algorithms, GNN
Explainability	SHAP, feature importance, rules, attention, none reported
Deployment evidence	Laboratory, simulation, pilot, operational, unknown



Integrated detection architecture: classical AI, deep learning, network analytics, and emerging quantum/hybrid methods

Figure 1. Proposed integrated AI–quantum architecture for financial-crime detection.

4. Comparative Results and Evidence Synthesis

4.1 Classical AI/ML

The available literature suggests that classical machine learning currently provides the most practically mature baseline for financial-crime detection. Major advantages are that of being method mature, supported by software, having some lower infrastructure requirements and it can be compatible with a large transaction processing setup. Any feature with nonlinear relations with other features can also be aggregated into a single feature and features like tabular transaction features may be tempting to aggregate into a single feature. Anomaly-detection techniques are relevant if there is no fraud label or it has been known to have a time delay; while SVM neural network are important. [1,2]

However, from reading the literature it is clear that there is a general problem of measurement – no two sets of data can be directly compared. There are many factors involving the occurrence of fraud, fraud type, data leakage prevention, the time involved and sampling techniques that can have a tremendous impact on the actual performance counts. Therefore, a good score of F1 on one piece of data doesn't necessarily indicate that the algorithm is effective in all situations.

4.2 Deep Learning

The capability is extended using deep learning, to learn representations for transaction variables and enhance the ability to design transaction variables. LSTM models can be trained with the transactions in sequence and the autoencoders can capture the sequence and detect anomalies in the reconstruction process. Deep models can be of great benefit if the financial institution has large amounts of data in the past, and the computing resources to train and monitor the models. However, deep-learning models have several limitations, including substantial data requirements, limited

<http://eijas.com/index.php/as>

interpretability, computational costs, and sensitivity to distributional changes.

4.3 Graph and Network-Based Detection

Graph-based detection is relevant since it might be the relationships that emit this suspicious signal in the case of coordinated fraud and money laundering. The nodes could be customers, accounts, companies, devices, merchants, wallets, beneficiaries, and transactions; or the nodes and the transactions or other relationships. With this knowledge, GNNs can find local neighbourhoods, recognize the structure of networks. Conceptually, the method can be combined coupled with other approaches of classification: the individual transaction can be classified using classical ML techniques; and the graph analytics can be used to see if the transaction is linked to a suspicious subnetwork.

4.4 Quantum and Quantum-Hybrid Evidence

In recent research, it was shown that quantum methods were actively experimented. In their 2026 paper [5] El Alami et al. have made a comparison of the various QML architectures to counter credit-card fraud. Murugaraj et.al. spot the drawbacks of the existing technologies and delve into the different classical and QML financial studies, and ultimately state that fraud detection is one of the crucial application of QML [3]. A hybrid Deep Learning and Quantum Optimization approach is proposed in [6] by Yu and Luo and consists of CNN, LSTM and GNN.

However, this evidence should be interpreted cautiously. Features that are reduced in quantum studies are usually the data specific to the problem, a limited number of qubits, a simulated/scaled down circuit and/or reduced features. These considerations will make it more difficult to determine if any improvements observed is really a true improvement on the scalable quantum advantage or is caused by differences in pre-processing or design. Therefore, claims of QML superiority should be evaluated under statistically comparable conditions, with sufficient attention to reproducibility, scalability, and economic benefit.

4.5 Comparative Evidence Matrix

Approach	Strengths	Main weaknesses	Current maturity	Best-fit role
Logistic regression / linear models	Transparent; fast; strong baseline	Limited nonlinear capacity	High	Benchmarking and interpretable risk scoring
Random forest/boosting	Strong tabular performance; nonlinear relationships	Can be sensitive to drift and imbalance	Very high	Operational transaction classification
SVM	Effective in high-dimensional settings	Scaling and calibration challenges	High	Classification with engineered features
Deep learning	Learns complex representations; temporal modelling	Data/computation/interpretability demands	High–moderate	Large-scale sequence and anomaly detection
Graph / GNN	Captures relationships and coordinated activity	Graph construction; scalability; explainability	Moderate	Network-level AML/fraud detection
QSVM /	Emerging	Noise, qubit limits, encoding	Early	Experiment

VQC / QNN	quantum representations; research potential	cost, immature benchmarks		al evaluation of selected subproblems
Hybrid quantum-classical	Can combine mature classical pipeline with quantum component	Integration and reproducibility challenges	Early–emerging	Optimization or specialized classification components

5. Discussion

5.1 Is Quantum Computing Currently Better Than Classical AI?

The data used in this resource does not guarantee a benefit to quantum computing over classical AI in the detection of financial crime per se. The classical models are well established with a good empirical basis, and are already well adapted to operational data-processing infrastructures. In contrast, QML remains an emerging research area in which hardware specification, data encoding, circuit depth, noise, and experimental reproducibility are important determinants of performance.

The current lack of demonstrated advantage does not imply that quantum computing has no potential value. Sometimes it may be interesting to research and determine some specific subproblems to be solved numerically (e.g., optimization, selection of features, the evaluation of kernels, and some special classification task). So the realistic near-term architecture is much more hybrid, rather than classical and quantum: Generally, for classical systems, most inference is done in a classical way; for most quantum systems, the tasks are performed if there is a new profitable benefit based on computing; classical data is ingested, preprocessed, then built classical representation, then graphitized.

5.2 Financial Networks Change the Detection Problem

However, the notion that a single detection approach can be adequately address all forms of financial crime is therefore inappropriate. A typical real estate transaction could be flagged as a suspicious string of wire transfers, multiple devices, multiple beneficiaries, a series of transfers, or joint beneficiary companies. A multi-layered architecture of transaction-level ML, temporal modelling and graph analytics are possible. Quantum methods can therefore be considered as an additional layer within the detection architecture rather than as a replacement for the entire detection stack.

5.3 Evaluation Must Reflect Operational Costs

Lots of false positives in financial crime detection can be expensive for investigations and false negatives can allow losses and/or financial crimes to continue. Therefore, precision, recall, investigator workload, alert volume, time to alert, calibration, and financial costs should be considered when selecting models. An F1 score just a little bit higher, but with much higher number of volumes of false positives, could be less effective in the field if a slightly less effective model had a more manageable number of volumes.

5.4 Explainability and Governance

In financial institutions there are environments of regulation and audit and there are decisions that are defensible with respect to finances. Explainability shouldn't be thought of as a technical option, though. It's easy to get a sense of feature importance and explanations of SHAP from classical models, but not so much in the cases of graph models and quantum circuits. In future research on QML, it is therefore important that predictive metrics with model descriptions explain the quality and the degree of reproducible model; the circuit architecture; the hardware involved and the relations model ΔQ to investigative decisions in future research.

5.5 Data Privacy and Concept Drift

Financial data is not readily shareable and very sensitive. As a result, there is reduced independent duplication and can result in a mismatch in target and purpose. There are a couple of problems that can be partially alleviated by privacy-preserving learning, federated learning, secure computation, <http://eijas.com/index.php/as>

and correctly-formulated synthetic data. Another major concern is 'concept drift' – tactics in committing crimes vary, how people pay change and there are new means of payment. Time-aware validation should thus be considered as a way to evaluate models, rather than just relying on random train-test splits.

6. Proposed Conceptual Framework

In this paper, a multi-layer financial-crime detection system is suggested, via comparative evidence. The first layer contains transaction and entity data. The second layer takes care of data quality control, feature engineering, entity resolution, and temporal alignment. The third is the classical models of transaction-level risk and deep-learning-based models. The fourth layer is graph/network analytics, an ability that allows you to discover relationships that lie at the graph level. The fifth is an experimental layer that can be used for some optimization or classification jobs; a quantum/hybrid layer. The final layer is based on the combination of model outputs with alerts for investigators as risk scores.

It is a modular structure so that the framework can be adapted. The use of quantum computing should not put any burden on any institutions, and it's perfectly okay to immediately start using it. Instead, it creates a "sanitized environment" in which only a quantum component can be grafted on at the measured time when the same classical component is tuned almost perfectly by itself, with its performance not being significantly undershot.

6.1 Proposed Benchmarking Protocol

- Use an imbalanced real or realistically simulated financial dataset.
- Avoid temporal leakage by using temporally separated training, validation, and test sets.
- Report PR-AUC/AUPRC, precision, recall, F1, ROC-AUC, false positive rate and calibration.
- Consider reporting inference/training time, and computational resources.
- The circuit depth, simulations/hardware details, assumptions about the noise and the number of shots as well as the encoding of qubits should be provided for QML.
- Repeat runs of experiments on several data ensembles as available (if more than one) and on several seeds.
- Assess effectiveness in case of concept drift and changes in the potential for fraud.
- Including assessments of explainability and investigator workload.

7. Limitations

This study has several limitations. First, the available literature is heterogeneous with respect to datasets, fraud labels, feature representation, evaluation metrics, and validation procedures, which limits direct numerical comparison across studies. Second, many quantum machine-learning studies remain experimental and are evaluated using limited datasets, reduced feature spaces, simulated environments, or hardware with constrained qubit availability. Third, because financial crime datasets are frequently proprietary and difficult to share, independent replication and cross-institutional validation remain challenging. Consequently, the comparative findings should be interpreted as an evidence synthesis rather than as a direct head-to-head experimental benchmark of all model families.

8. Recommendations and Future Research

In the literature there is support for a research program geared towards appropriate benchmarking, rather than towards technology "buzz". First of all, future studies are needed and could yield common datasets and/or well controlled benchmark suites, for comparison of classical and quantum models and under what conditions. Secondly, assessment should be done using the time-based validation and metrics, which are cost sensitive. Thirdly, the transaction based models should be included in the financial-network representation. Fourth, QML scientists need to provide enough detail for following their implementation as to allow for a repeat of the experiment.

- Develop privacy-preserving and federated- learning approaches for multi-institutional financial-crime detection.
- When considering accuracy, take into account the AUPRC, recall, precision, false positive

burden, calibration, and financial cost.

- Measure coordinated fraud / AML with the methods of GNN / Temporal network.
- Develop standardized financial-fraud benchmark datasets for evaluating classical and quantum approaches.
- Compare the performance of the models in realistic class imbalance and concept drift scenario.
- Develop out Audit/ Regulatory Review Explainable AI/ Explainable QML techniques.
- Multi-institutional fraud detection – get to know privacy preserving and federated learning.
- Carry out cost benefits analysis (including calculating cost of Computing, cost of model, cost of investigation and false alarms).
- Until before quantum computing finds real-world uses, the same (although not definitive) QML results are attained when working with independent financial information being utilized.

9. Conclusion

The industry of financial-crime detection is evolving from a rule-based monitoring process to more comprehensive solutions that incorporate machine learning, deep learning, graph analytics and: more and more, quantum computing. From the evidence found in the current paper, it can be concluded that at this time classical AI is the most viable, deep learning and graph-based methods also have a significant value in the case of temporal and relational detection. On one hand, the research fields of quantum machine learning and quantum optimization appear promising (especially in combination with classical methods), but for now, there is no sufficient evidence to say that quantum approaches generalize to be more superior than classical approaches.

Best defense, short term is an evidence-based multi-layered design. Good operational baselines should be already in place through the use of classical AI; network analysis should be capable of profiting from identifying and linking different criminals; a judicious application of quantum/hybrid should be paired with classical baselines. The findings therefore support a cautious and evidence-based approach to quantum computing in financial-crime detection. Quantum and hybrid approaches should currently be regarded as emerging technologies whose practical utility must be demonstrated through reproducible comparative studies using realistic financial datasets, appropriate evaluation metrics, and clearly reported computational conditions.

10. References

1. Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, 12(19), 9637. <https://doi.org/10.3390/app12199637>
2. Hernández Aros, L., Bustamante Molano, L. X., Gutiérrez-Portela, F., Moreno Hernández, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, 11, 1130. <https://doi.org/10.1057/s41599-024-03606-0>
3. Murugaraj, G., Krishnan, R., Harikrishnan, L., & Kandasamy, M. S. (2026). Systematic review on the influence of classical and quantum machine learning in the financial sector. *Decision Analytics Journal*. <https://doi.org/10.1016/j.dsm.2026.01.001>
4. Weinberg, A. I., & Faccia, A. (2026). Quantum algorithms: A new frontier in financial crime prevention. *Quantum Machine Intelligence*, 8, 78. <https://doi.org/10.1007/s42484-026-00418-0>
5. El Alami, M., Innan, N., Shafique, M., & Bennai, M. (2026). Comparative performance analysis of quantum machine learning architectures for credit card fraud detection. *Applied Intelligence*, 56, 83. <https://doi.org/10.1007/s10489-026-07110-7>
6. Yu, G., & Luo, Z. (2025). Financial fraud detection using a hybrid deep belief network and quantum optimization approach. *Discover Applied Sciences*, 7, 454. <https://doi.org/10.1007/s42452-025-06999-y>
7. Sahoo, A., Bertl, M., Draheim, D., & Sinno, S. (2026). Classical and quantum machine learning for financial fraud detection: A systematic review. *SSRN Electronic Journal*. Posted August 5, 2026.
8. Triyanto, D. N., & Ali, S. (2026). The role of big data analytics in financial fraud detection: A systematic literature review. *International Review of Economics & Finance*, 109, 105453. <https://doi.org/10.1016/j.iref.2026.105453>

9. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review. *Decision Support Systems*, 50(3), 559–569.
10. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235–255.
11. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234–245.
12. Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, 133, 113303.
13. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: A survey. *Data Mining and Knowledge Discovery*, 29, 626–688.
14. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.
15. Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2, 79.
16. Schuld, M., & Petruccione, F. (2021). *Machine Learning with Quantum Computers* (2nd ed.). Springer.
17. Cerezo, M., Arrasmith, A., Babbush, R., et al. (2021). Variational quantum algorithms. *Nature Reviews Physics*, 3, 625–644.