# Exploring the Feasibility of Using Quantum Machine Learning to Detect Cryptocurrency Trading Anomalies

*By: Atharv Attri, Irvine Valley College*
*Mentor: Prof. Carrie Goulding*

## Abstract

Cryptocurrency markets are known for their high volatility and 24/7 trading, which creates significant challenges for effective anomaly detection. Traditional methods, while useful in the past, often struggle with the speed and complexity of the data produced by these non-traditional markets. This paper explores the potential of using Quantum Machine Learning (QML) as an alternative solution that can tackle some limitations of classical machine learning models, such as slow computational speeds and delayed detection. Despite the theoretical benefits of QML, the current state of quantum computing hardware makes it ill-suited for real-world use at this time. In the interim, hybrid quantum-classical approaches seem far more feasible in the near term. Ultimately, although fully quantum anomaly detection is still a distant goal, integrating quantum technologies into existing frameworks may be key to improving market stability and security in the near future.

## Fundamentals of Cryptocurrency Trading

Cryptocurrency is a fairly new market, whose origins can be traced back to the early 1980s, however, the modern era of this market can be attributed to Bitcoin (ElBahrawy et al., 2017). In 2009, an individual under the pseudonym “Satoshi Nakamoto” released a thesis paper that laid the fundamentals for an idea to change global payments and data management as a whole. This paper became known as the Bitcoin Whitepaper and the first decentralized digital currency to use blockchain technology, a method for secure transactions. Following Bitcoin’s profound success, numerous other cryptocurrencies emerged, often referred to as “altcoins.” For example, Ethereum introduced the concept of smart contracts in 2015, which enabled more complex financial instruments and decentralized applications (Said et al., 2021). The rapid development of diverse cryptocurrencies has created a complex ecosystem, presenting unique challenges and opportunities for trading and anomaly detection. Cryptocurrency markets are notorious for their extreme price fluctuations, experiencing volatility levels that significantly exceed those of traditional financial markets. There are several contributors to the high volatility seen in these markets, the first one being market sentiment. This causes cryptocurrency prices to be highly susceptible to changes in investor confidence and feelings, which are often driven by news events or social media trends. As a result of market sentiment, cryptocurrencies are often unpredictable, and price movements reflect the collective mood of investors rather than fundamental factors. Possible policy changes and technological developments or vulnerabilities can also lead to significant price changes. The extreme volatility in cryptocurrency markets emphasizes the importance of strong anomaly detection systems. Eventually, traditional methods for identifying unusual price movements may become less impactful in such a quickly changing environment. Quantum machine learning models, with their potential to adapt to changing market conditions faster, could offer significant advantages (Herman et al., 2023). Liquidity varies widely across the cryptocurrency market. Major cryptocurrencies like Bitcoin and Ethereum tend to have higher liquidity, making them easier to buy and sell, while smaller altcoins have lower liquidity, making them harder to trade.  The differing levels of liquidity have important implications for anomaly detection. In markets with low liquidity, inefficiencies arise making anomalies more prominent as large trades can cause substantial price fluctuations. This volatility complicates the accuracy of anomaly detection and increases false positives

*© Think You?! The Proceedings of the Bay Honors Research Symposium, 2024. All Rights Reserved.*

because normal market movements are mistakenly flagged. There is also the additional challenge of these markets being open at all times, unlike traditional markets that have set open and closing times. This continuous trading environment poses more challenges, such as the need for nonstop real-time analysis and consideration of global influences. Efficient anomaly detection is critical for maintaining the integrity of cryptocurrency markets, as anomalies can lead to serious consequences like flash crashes, pump-and-dump schemes, and other forms of harmful market manipulation. Accurate detection helps prevent these disruptive events and safeguards market stability. Real-time anomaly detection could help mitigate risks, prevent these disruptive events, and safeguard market stability.

## Overview of Classical Machine Learning in Financial Markets

The application of machine learning to financial markets has completely revolutionized the way we make predictions and detect anomalies. Before discussing how quantum machine learning could be used in financial markets, it is important to understand how classical machine learning has already paved the way for more advanced analysis. Traditionally, economic experts have relied on statistical methods to identify outliers or unusual patterns in the market; these approaches form the foundation for the complex machine learning models in use today. Understanding these methods is crucial for appreciating the evolution of anomaly detection in financial markets.

One of the most essential tools used is the moving average, which helps to smooth out short-term fluctuations in the market data. One of the simplest forms of anomaly detection is detecting significant price deviations from the simple moving average, which calculates the average price over a specified period (Chen et al., 2022). In the 1980s, John Bollinger built upon this idea to create Bollinger bands. These bands are plotted around a moving average, with the width of the band determined by the standard deviation of the security's price, reflecting its volatility. If a price moves outside these bands, it could be considered an anomaly as it deviates from the expected range. However, these models are often slow, lagging too far behind the current price. Exponential smoothing places a higher emphasis on recent price moves, making it more responsive to recent changes. This is very useful for cryptocurrencies which are known to have rapid price changes, potentially allowing for faster detection of anomalies. While these techniques do provide valuable insights, they are not able to capture complex patterns, time series such as Autoregressive Integrated Moving Average (ARIMA) models are able to address this. These models combine autoregression, integration, and moving averages to create a more accurate baseline for normal behavior, making it easier to spot anomalies and deviations from expected patterns (Hayes, 2024). Given the volatility of cryptocurrencies, ARIMA models have proven to be especially useful; in a 2024 study by Alanood Alkamali at the Rochester Institute of Technology - Dubai, they found ARIMA models can be used to predict Bitcoin prices, with their specific experimentation achieving a RMSE of 0.03099 and MAE of 0.02121. However, they indicate, "traditional time series techniques are limited by their use of only past values to predict future ones, especially considering that cryptocurrency prices are influenced by various other features and external factors." (Alanood, 2024). He suggests that machine learning models such as Convolutional Neural Networks (CNN) or Long Short-Term Memory (LSTM) networks paired with ARIMA may improve predictions.

As the volume and complexity of financial data have grown, more sophisticated machine-learning models have been used to detect anomalies by analyzing patterns. Supervised learning models such as XGBoost, which is an implementation of Gradient Boosting Machines, have gained significant traction for detecting anomalies due to their exceptional predictive performance. In a study called "Cryptocurrency Pump and Dump Schemes: Quantification and Detection," Victor and Hagemann demonstrated the XGBoost was highly effective in detecting pump-and-dump schemes, achieving an AUC of approximately 0.995. Manual inspection further confirmed that most of the pump-like events identified by the model were plausible, showcasing the power of machine learning in detecting cryptocurrency trading anomalies. However, this supervised approach relies on

labeled data, which is often scarce and costly to obtain. Unsupervised learning can solve this issue by identifying patterns in unlabeled data. Autoencoders are a type of artificial neural network that has become popular because they're able to learn compact representations of the inputted data. For anomaly detection, autoencoders reconstruct normal instances of the data; therefore, when the reconstruction error is higher than expected, the instance can be flagged as an anomaly (Angiulli et al., 2023). In a study conducted in 2023 titled "Block-chain Abnormal Transaction Detection Method Based on Auto-encoder and Attention Mechanism" Xiong et al. state that autoencoders are very effective at detecting anomalies, especially when paired with some attention mechanisms, with the GraphAEAtt method reading AUC scores of up to 90.92%. This begs the question, why even use quantum machine learning? While classical machine learning has unquestionably expanded our ability to detect anomalies in financial markets, they are still plagued by various limitations and challenges associated with cryptocurrency. The main issue is the computational resources needed by classical machine learning models to analyze the vast amount of data produced by these 24/7 markets. This issue is escalated by the need for real-time analysis and detection of anomalies. The facts are that complex classical machine learning models have a tradeoff with computational efficiency (Metz et al, 2022), meaning that oftentimes, the need for instantaneous results outpaces computational capabilities. Complex machine learning models also often are "black box" in nature, meaning that no one outside of the model can understand the rationale behind the decisions made by the model. This is a major limitation in a financial environment because the rationale is often just as important as the decision itself; Leichtmann et al. found in 2023, that in a high-risk decision task, people tended to trust AI models more if they received an explanation regarding the decision. Therefore, the lack of explainability could lead to a lack of trust in machine learning models by regulators and traders alike. Another challenge is the fact that cryptocurrency markets change very fast, meaning models can quickly become outdated, especially when faced with high-impact events. Given that most classical models cannot be continually trained, but rather trained in batches, classical machine learning approaches face various other issues such as excessive false positives and general loss in accuracy.

## Introduction to Quantum Computing

Quantum computing represents a shift in computational capabilities, offering potential solutions to problems that classical computers are not capable of. This unique type of computing leverages the principles of quantum mechanics to perform calculations through an ability known as superposition. This enables quantum systems to exist in multiple states simultaneously, allowing tiny particles known as qubits to be represented as both 0 and 1 at the same time– unlike a traditional bit which must be either 0 or 1 (Gamble, 2018). This allows quantum computers to process multiple possibilities concurrently, potentially offering faster computational power and allowing for quantum parallelism, where a single quantum operation can be performed on multiple data values simultaneously. Due to this faster computation, a phenomenon known as quantum entanglement occurs which refers to separate particles becoming correlated in a way that each particle cannot be described independently. Quantum entanglement facilitates the creation of quantum circuits that can perform complex operations more efficiently than classical circuits. Another phenomenon that occurs is known as quantum interference where the wavelike nature of quantum systems results in constructive or destructive interference of quantum states (Microsoft Azure Quantum, n.d.). This property is critical for quantum algorithms, as it allows for the amplification of desired computational outcomes while suppressing the unwanted ones, and this can play a significant role in algorithms applied to data mining in financial applications. These computations are performed using quantum gates, which are reversible operations that manipulate the states of qubits. Common quantum gates include the Hadamard and Controlled NOT (CNOT) gates, which both use quantum entanglement (Abdessaied et al., 2014). These gates can be combined to create quantum circuits that are capable of executing highly complex computations. By simultaneously creating and manipulating superpositions, these advanced systems hold the potential to perform certain financial calculations at exponentially faster rates than traditional computers. Currently, there are many different types of quantum

computers under development, each with a unique approach and focus. One is based on superconducting qubits and is the most advanced in terms of qubit count and gate fidelity (Smith-Goodson, 2019). The second type uses trapped ions, offering longer coherence times. The third approach leverages photonic qubits for light-based computation, pursued by companies such as PsiQuantum. Each approach presents a distinct advantage and challenge, though it remains uncertain which will ultimately lead to large-scale quantum computation success. Unfortunately, currently building a large-scale quantum computer with millions of qubits poses many challenges, specifically in financial applications. The high-precision calculations needed in many financial models require a minimal error rate, which is currently a major restriction. Also, large datasets typically found in financial applications require quantum computers to hold a significant amount of qubits, which is currently unsustainable.

## Quantum Machine Learning: Foundations and Algorithms

The field of quantum machine learning is a convergence of quantum computing and classical machine learning, aiming to use the properties of quantum physics to enhance the algorithms and models currently being used. As the cryptocurrency market continues to grow and becomes increasingly complex, QML represents a promising solution to break past the limitations of classical machine learning.

When examining quantum machine learning, there are three main approaches, each with varying degrees of computing requirements and near-term to enhance feasibility. The first category is quantum-inspired algorithms, which utilize techniques from pre-existing quantum algorithms to enhance existing classical models without requiring any quantum computing hardware. These often employ quantum annealing-like optimization or quantum-inspired sampling to enhance existing classical machine-learning models. In the context of cryptocurrency anomaly detection, they can improve pattern recognition while remaining compatible with classical hardware, thus removing the limitations of relatively new quantum computing hardware. A 2020 study by Arrazola et al, titled “Quantum-inspired algorithms in practice,” found that, “quantum-inspired algorithms can perform well in practice provided that stringent conditions are met: low rank, low condition number, and very large dimension of the input matrix. By contrast, practical datasets are often sparse and high rank, precisely the type that can be handled by quantum algorithms.” Although this shows great potential for quantum-inspired algorithms, they currently do not perform as well under practical conditions. Therefore, the remaining approaches may yield better results, at least in the near future. The second approach is hybrid, combining quantum and classical systems, offering a balanced method to leverage current quantum capabilities while mitigating the limitations of quantum computing. These algorithms distribute tasks related to the algorithm between quantum and classical processors, with quantum systems typically applied to specific routines where they can provide a clear advantage (Herman, 2022). This approach is particularly relevant for near-term applications in cryptocurrency anomaly detection as it allows us to incorporate quantum computing into existing classical models. Variational quantum algorithms (VQAs) appear especially promising, as they use classical algorithms to optimize parameterized quantum circuits. VQAs already demonstrated success at solving optimization problems and have been applied to portfolio optimization and risk assessment within cryptocurrency markets (Arrazola et al, 2020). In the 2022 paper titled, “Hybrid Quantum-Classical Algorithms for Loan Collection Optimization with Loan Loss Provisions,” Thangpanitanon et al. found that using a Quantum Alternating Operator Ansatz (QAOA) algorithm on a 35-qubit quantum simulator improved net profit by 70% compared to not using it. Although this study focused on traditional markets, the fundamental principles can be extended to anomaly detection in cryptocurrency, potentially leading to a more sensitive model that is capable of identifying subtle market irregularities. Fully Quantum Algorithms represent the third approach and the long-term vision for quantum computing. These algorithms hold the potential to solve problems exponentially faster than classical models, however, they require large-scale, fault-tolerant quantum computers, which are both technically challenging and expensive to develop. As a result, the practical

implementation of fully quantum algorithms for real-world financial applications remains a prospect, dependent on furthering advancements in quantum computing hardware.

Quantum Neural Networks (QNNs) are the quantum versions of classical neural networks, designed to use the power of quantum systems for machine learning. In QNNs, the input data is encoded into quantum states, which are processed through a series of parameterized quantum gates (Schuld, 2014). In QNNs, the quantum gates function similarly to weights and activation functions that are seen in classical neural networks, with the quantum circuit's output serving as the network's final result. The quantum circuits underlying QNNs take advantage of phenomena like superposition, enabling the simultaneous processing of multiple states. This parallelism leads to potentially faster computation times (Farhi, 2018). In the context of cryptocurrency anomaly detection, QNNs can employ these quantum phenomena to efficiently process high-dimensional data. By doing so, they can identify complex relationships across a vast number of features and indicators, potentially finding subtle patterns that classical computers may overlook.

Training Quantum Neural Networks (QNNs) comes with its own set of advantages and challenges, depending on the architecture of the model. One of the most popular QNN architectures is the Variational Quantum Circuit (VQC), which consists of a series of parameterized quantum gates as mentioned before; however, the parameters in the VQCs are optimized using classical algorithms, allowing for a hybrid quantum-classical training process that helps in circumventing the current limitations of quantum hardware (Benedetti et al, 2019). The flexibility of VQCs makes them especially promising for financial applications, as they can be specifically tailored to cryptocurrency data. Despite their potential, training QNNs also presents some unique challenges. One major issue is the "barren plateau" problem, where the gradient of the cost function of the QNNs diminishes exponentially as the number of qubits increases, making optimization more difficult (Cerezo et al, 2021). This is further applied by the fact that, unlike classical neural networks that rely on backpropagation, QNNs face additional challenges due to principles like the no-cloning theorem and the inherently probabilistic nature of quantum measurements. The work of Schuld et al. (2019) on evaluating analytic gradients on quantum hardware has been instrumental in developing practical training methods for QNNs, allowing them to run on near-term quantum computers. This brings us closer to applying quantum machine learning to cryptocurrency anomaly detection. However, it is important to recognize these algorithms and practices have only been demonstrated in small-scale experiments. Significant advances in both quantum computing hardware and algorithms are necessary before QNNs can be applied to large-scale cryptocurrency data. Issues with current Noisy Intermediate-Scale Quantum (NISQ) devices, such as low gate fidelities and short qubit coherence times, must be addressed to unlock the full potential of QNNs in financial markets.

## Quantum vs. Classical Machine Learning for Cryptocurrency Anomaly Detection

Evaluating machine learning models for cryptocurrency trading anomaly detection requires a complex understanding of both classical performance metrics and their quantum counterparts. While accuracy, precision, and recall are the cornerstones of model evaluation in both classical and quantum machine learning models, however, their interpretations and calculations differ. Grasping these differences is essential for a fair comparison between the two types of models. In classical systems, accuracy is the ratio of correct predictions to total predictions, precision is the percentage of how many positive predictions were true positives, and recall is the percentage of how many true positives were found (Google Machine Learning, 2024). These metrics provide insights into a model's ability to correctly identify abnormal market behavior while minimizing false alerts. However, in quantum systems, outputs are often problematic due to quantum superposition, requiring multiple measurements to determine the most probable outcome. As a result, these metrics must be reinterpreted for quantum machine learning models. In their 2023 paper, "Evaluating Three Levels of Quantum Metrics on Quantum-Inspired Hardware," Schoot et al. discuss a quantum-inspired accuracy metric that

incorporates the uncertainty inherent to quantum measurements, offering a more nuanced understanding of model correctness. While this metric improves precision in detecting true anomalies, it also has the potential to increase false positives. In the context of cryptocurrency trading anomalies, a Receiver Operating Characteristic (ROC) curve analysis is a more reliable performance indicator due to the rarity of anomalies, which can result in a high number of false positives (Bradley, 1997). The ROC curve plots the true positive rate against the false positive rate, with the Area Under the ROC Curve (AUC-ROC) serving as a single number summary of the model's performance. This metric has been used in various papers that analyze the performance of QML models, such as Wu et al.'s 2021 paper, "Application of quantum machine learning using the quantum kernel algorithm on high energy physics analysis at the LHC," which drew inspiration from the use of AUC-ROC in Mott et al.'s 2017 paper, "Solving a Higgs optimization problem with quantum annealing for machine learning." A standardized metric like AUC-ROC is crucial for comparing potential QML-based cryptocurrency anomaly detection models with modern classical models. This comparison is essential because the ultimate goal is to develop a fully quantum model that significantly outperforms classical approaches, and a consistent metric allows us to quantify progress toward that goal.

Computational efficiency is yet another critical factor in the fast-paced, high-volume world of cryptocurrency trading. While classical models do perform well in detecting anomalies, they struggle to keep up with the massive amounts and speeds of data generated by cryptocurrency markets (Li, 2022). Although quantum algorithms theoretically offer significant speedups for certain tasks, they are not always faster in practice. Doosti et al (2024) highlight this struggle in their paper "A Brief Review of Quantum Machine Learning for Financial Services": "While such speedups have been demonstrated for certain specific problems, achieving them in the realm of data science, and moreover for industry applications, remains an ongoing challenge with much active research in QML attempting to address it." Currently, no comprehensive case study has directly compared quantum methods against classical ones for trading anomaly detection. The gap in research highlights the need for further investigation into the practical performance and computational efficiency of QML in real-world financial applications.

## Regulatory and Ethical Considerations

Quantum machine learning and cryptocurrency are already complex enough topics on their own when it comes to regulatory and ethical concerns. Combining them only deepens the complexity, especially in such an uncharted space. Regulatory frameworks for cryptocurrencies remain in a state of flux, with different jurisdictions worldwide adopting varying approaches to govern decentralized currencies. The lack of a central authority and the pseudo-anonymous nature of the transactions make it difficult for regulators to treat cryptocurrencies as they would traditional securities. In the United States, the Securities and Exchange Commission has taken a cautious approach to cryptocurrencies, particularly in classifying certain cryptocurrencies as securities (Hayes, 2024). This regulatory uncertainty has significantly impacted the cryptocurrency market, influencing trading patterns and investor's trust and confidence. Internationally, cryptocurrency regulation policies vary. In their 2024 paper, "Crafting the Future of Finance: A Comparative Analysis of Cryptocurrency Regulation in the Global Economy," Frediani highlights key elements for an effective regulatory framework: "1) clear definitions and terminology; 2) rules designed for the main uses of the digital assets; 3) clear requirements on regulated financial institutions… regarding the potential exposure to crypto assets; and a 4) a structure that allows adjustments in order to keep the regulation up to date with developments from crypto technology." As such regulations are fully implemented, QML has the potential to enhance regulatory oversight. As mentioned earlier, quantum-enhanced anomaly detection models can identify market manipulation schemes and other anomalies with greater accuracy than classical models, potentially detecting market disruptions before they escalate. When this is combined with QML's capacity for real-time, comprehensive monitoring of cryptocurrency markets, this could empower regulators to play a more active role in overseeing and stabilizing these markets.

While the potential benefits of using quantum-enhanced anomaly detection models are significant, they also raise important ethical considerations. Privacy and anonymity are highly valued by many users within cryptocurrency networks and the services it provides (García-Corral et al., 2022); the enhanced capabilities of quantum machine learning models may compromise user trust, raising concerns about how the multi-billion-dollar crypto market may be affected. Some might argue that this is a worthwhile trade-off, especially considering there was an estimated 20.6 billion USD involved in crypto-related illicit activity in 2022 (Pocher et al, 2023). Given the potential power and ethical implications of quantum machine learning in cryptocurrency markets, it is crucial to develop frameworks responsible for their development and deployment.

Existing frameworks for machine learning provide a useful starting point for developing ethical guidelines, but the unique properties of quantum computing may require significant adaptation, especially concerning explainability. Ensuring transparency and explainability for quantum machine learning models is essential for building trust in these systems and enabling effective oversight. Power and Guha (2024), in their paper "Feature Importance and Explainability in Quantum Machine Learning," highlight that there may be a need for entirely new quantum-specific methods of explainability because "there is likely a need for not only amending these tools but, perhaps a need to come up with completely new quantum specific methods of explainability." The paper discusses how explainability, already a significant challenge in classical machine learning systems, amplifies in complexity with quantum machine learning due to the absence of explainability methods specifically tailored for quantum systems. As quantum technologies advance, establishing clear ethical guidelines will be vital to ensuring both innovation and accountability in their use within cryptocurrency markets.

## Limitations and Challenges

While quantum machine learning undoubtedly shows immense potential for enhancing cryptocurrency anomaly detection, there are several limitations and challenges that must be addressed before quantum machine learning can become a mainstream tool. The most significant struggle is the current state of quantum hardware.  Despite advances in the number of operational qubits, modern systems are still rather rudimentary for tackling complex problems like anomaly detection in cryptocurrency markets. The number of qubits in today's quantum computers is insufficient for these tasks, however, IBM is set on building a 100,000-qubit machine within 10 years, and Google hopes for a million by the end of the decade (Stackpole, 2024). As the complexity of problems increases, the required number of qubits also grows exponentially, meaning that even small performance improvements may demand much larger quantum systems. Additionally, the issue of coherence time– how long can a qubit maintain its state– further complicates scaling quantum systems. For example, superconducting qubits struggle to stay coherent for longer than a few microseconds to milliseconds (IonQ Staff, 2024), limiting the depth of quantum circuits that can be implemented. Therefore, it is not just about having more qubits, but rather, having qubits that can remain stable long enough to train and execute a machine learning model. These hardware limitations severely impact the feasibility of applying quantum algorithms to anomaly detection models, especially in fast-paced, high-stakes environments like cryptocurrency trading. Error rates in quantum computing are another major challenge. Every gate operation on a quantum computer introduces some level of error, and current error rates hover around 1% to 0.1% per operation (Microsoft Azure Quantum, n.d.). Given the complexity of financial models requires many qubit operations, error rates compound rapidly. Cryptocurrency models demand a high level of precision– any inaccuracies could undermine investor and regulator confidence. This is where error correction comes in, however, the trade-off is costly. Error correction requires additional qubits, which are already limited, leading to exponentially larger systems just to maintain accuracy, further complicating the application of QML in cryptocurrency anomaly detection. Lastly, the cost of owning or accessing quantum systems is prohibitively high for many financial institutions, particularly smaller ones. A quantum computer with 2000 qubits costs

around USD 15 million, not considering the cost of operation (Gartenberg, 2017). For the finance industry, where the margins for improvement need to justify the investment, this represents a significant barrier to entry.

Even if issues with quantum hardware were addressed, designing algorithms that take full advantage of quantum computing remains a significant challenge. Quantum algorithms for finance are still very new; much of the progress has been theoretical, with most algorithms being adaptations of general quantum techniques. There is a noticeable gap in the development of algorithms specifically tailored to cryptocurrency anomaly detection. To date, most research has focused on more traditional financial problems, such as portfolio optimization or derivative pricing, but cryptocurrency presents a unique set of challenges including volatility and decentralization which make it difficult to simply adapt existing quantum methods. Another overlooked challenge is data encoding. For quantum computing to tackle any real-world problem, classical data must be efficiently transformed into quantum states. As discussed throughout this paper, cryptocurrency data is often highly dimensional and complex. The choice of an encoding scheme is crucial, as it directly affects the performance and efficiency of the quantum algorithm. While recent approaches have made progress by incorporating features like temporal trends and network dynamics (Takaki, 2021), these methods still require a large number of qubits– far more than what is currently feasible on today's quantum systems. Hybrid quantum-classical systems have been proposed to address this limitation but identifying which parts of the machine learning process are best suited for quantum computing is still an ongoing challenge. In the case of cryptocurrency anomaly detection, this is still a work in progress. It is understood that quantum systems are likely to excel at tasks such as pattern recognition or correlation analysis, but the anticipated revolutionary impact on cryptocurrency anomaly detection is still out of reach.

Another major challenge lies in the data itself. Cryptocurrency data is fundamentally different from traditional financial data, and translating classical financial data into quantum states is computationally expensive– often more than running the quantum algorithm itself. Some studies have shown that the time required to prepare data for quantum processing can exceed the runtime of the quantum algorithm, rendering the entire process inefficient. Cryptocurrency markets also operate 24/7, continuously generating large volumes of data at a high velocity. Current quantum systems are simply unable to handle this, so while quantum computing holds promise for anomaly detection in theory, it is far from being practical at this stage. Furthermore, there is the challenge of benchmarking quantum machine learning models and comparing them with their classical counterparts. Without standardized metrics for performance, especially in rapidly evolving environments like cryptocurrency trading, it is difficult to determine whether quantum models offer a tangible improvement over classical machine learning models.

## Conclusions

The intersection between quantum machine learning and cryptocurrency anomaly detection offers the vast potential to revolutionize how we monitor the integrity of cryptocurrency markets. While the theoretical benefits of applying QML to anomaly detection are very compelling, they remain more theoretical than actionable for now. Currently, quantum computing faces significant hurdles that prevent the real-world application of QML to cryptocurrency anomaly detection. These limitations include the low qubit counts available in current quantum systems, short coherence times, and high error rates, all of which severely hinder performance. The technology for quantum computing is also expensive, making it potentially prohibitive for the financial sector. Nonetheless, the promise of quantum models stands, with their ability to process high-dimensional and complex data potentially even faster than classical machine learning models, could one day lead to the accurate and timely detection of anomalies in cryptocurrency markets. In the meanwhile, hybrid quantum-classical approaches provide a pathway forward, allowing the integration of quantum technologies into existing financial systems. By leveraging the strengths of both classical and quantum models, hybrid approaches can bridge the gap between today's technology and future possibilities. Moreover, the regulatory and ethical

challenges around the deployment of quantum machine learning in financial markets warrant careful consideration. As with any revolutionary technology, transparency, user privacy, and market integrity must be prioritized. With sustained research, we may eventually witness a quantum leap in the ability to safeguard cryptocurrency markets. Until then, the integration of quantum technologies will be slow but steady, and their impact on cryptocurrency trading will continue to evolve.

## Author's Note

Acknowledgments to Carrie Goulding and Kaylyn Duong for helping make this paper possible; and to Emily Liu and the Irvine Valley College Honors Program for supporting my research and allowing me to present it. Correspondence regarding this article should be directed to Atharv Attri, atharv.attri@outlook.com.

## References

Abdessaied, N., Soeken, M., & Drechsler, R. (2014). Quantum circuit optimization by Hadamard gate reduction. Lecture Notes in Computer Science, 149–162. https://doi.org/10.1007/978-3-319-08494-7_12

Alkamali, Alanood, "Bitcoin Short-term Price Prediction Using Time Series Analysis" (2024). Thesis. Rochester Institute of Technology. Accessed from RIT Repository.

Angiulli, F., Fassetti, F., & Ferragina, L. (2024). Reconstruction Error-based Anomaly Detection with Few Outlying Examples. ArXiv. https://arxiv.org/abs/2305.10464

Arrazola, J. M., Delgado, A., Bardhan, B. R., & Lloyd, S. (2020). Quantum-inspired algorithms in practice. Quantum, 4, 307. https://doi.org/10.22331/q-2020-08-13-307

Benedetti, M., Lloyd, E., Sack, S., & Fiorentini, M. (2019). Parameterized quantum circuits as machine learning models. Quantum Science and Technology, 4(4), 043001. https://doi.org/10.1088/2058-9565/ab4eb5

Bradley, A.P. (1997). The use of the area under the ROC curve in the evaluation of machine learning algorithms. Pattern Recognit., 30, 1145-1159.

Cerezo, M., Sone, A., Volkoff, T., Cincio, L., & Coles, P. J. (2021). Cost function dependent barren plateaus in shallow parametrized quantum circuits. Nature Communications, 12(1). https://doi.org/10.1038/s41467-021-21728-w

Chen, C.-H., Lai, W.-H., Hung, S.-T., & Hong, T.-P. (2022). An advanced optimization approach for long-short pairs trading strategy based on correlation coefficients and Bollinger bands. Applied Sciences, 12(3), 1052. https://doi.org/10.3390/app12031052

Doosti, M., Wallden, P., Hamill, C. B., Hankache, R., Brown, O. T., & Heunen, C. (2024). A Brief Review of Quantum Machine Learning for Financial Services. ArXiv. https://arxiv.org/abs/2407.12618

ElBahrawy, A., Alessandretti, L., Kandler, A., Pastor-Satorras, R., & Baronchelli, A. (2017). Evolutionary Dynamics of the cryptocurrency market. Royal Society Open Science, 4(11), 170623. https://doi.org/10.1098/rsos.170623

Explore quantum. Microsoft Azure Quantum. (n.d.-a). https://quantum.microsoft.com/en-us/insights/education/concepts/interference

Farhi, E., & Neven, H. (2018). Classification with Quantum Neural Networks on Near Term Processors. ArrXiv. https://arxiv.org/abs/1802.06002

Frediani, M. E. (2024). Crafting the future of finance: A comparative analysis of cryptocurrency regulation in the global economy. Journal of Financial Risk Management, 13(01), 193–206. https://doi.org/10.4236/jfrm.2024.131010

García-Corral, F. J., Cordero-García, J. A., de Pablo-Valenciano, J., & Uribe-Toril, J. (2022). A bibliometric review of cryptocurrencies: How have they grown? Financial Innovation, 8(1). https://doi.org/10.1186/s40854-021-00306-5

Gartenberg, C. (2017, January 25). D-wave is now shipping its new $15 million, 10-foot tall quantum computer. The Verge. https://www.theverge.com/circuitbreaker/2017/1/25/14390182/d-wave-q2000-quantum-computer-price-release-date

Google Machine Learning. (2024, August 15). Classification: Accuracy, recall, precision, and related metrics. https://developers.google.com/machine-learning/crash-course/classification/accuracy-precision-recall

Hayes, A. (2024a, July 24). How sec regs will change cryptocurrency markets. Investopedia. https://www.investopedia.com/news/how-sec-regs-will-change-cryptocurrency-markets/

Hayes, A. (2024b, July 31). Autoregressive integrated moving average (ARIMA) prediction model. Investopedia. https://www.investopedia.com/terms/a/autoregressive-integrated-moving-average-arima.asp

Herman, A. (2022, April 29). The Quantum Revolution is here, its name is hybrid. Forbes. https://www.forbes.com/sites/arthurherman/2022/04/29/the-quantum-revolution-is-here-its-name-is-hybrid/

Herman, D., Googin, C., Liu, X., Sun, Y., Galda, A., Safro, I., Pistoia, M., & Alexeev, Y. (2023). Quantum Computing for Finance. Nature Reviews Physics, 5(8), 450–465. https://doi.org/10.1038/s42254-023-00603-1

IonQ Staff. (2024, January 18). Quantum Computing 101: Introduction, evaluation, and applications. IonQ. https://ionq.com/resources/quantum-computing-101-introduction-evaluation-applications

Jui, T. D., & Rivas, P. (2024). Fairness issues, current approaches, and challenges in machine learning models. International Journal of Machine Learning and Cybernetics, 15(8), 3095–3125. https://doi.org/10.1007/s13042-023-02083-2

Leichtmann, B., Humer, C., Hinterreiter, A., Streit, M., & Mara, M. (2023). Effects of explainable artificial intelligence on trust and human behavior in a high-risk decision task. Computers in Human Behavior, 139, 107539. https://doi.org/10.1016/j.chb.2022.107539

Li, M. (2022). A survey on Ethereum illicit detection. Lecture Notes in Computer Science, 13340, 222–232. https://doi.org/10.1007/978-3-031-06791-4_18

Metz, L., Freeman, C. D., Harrison, J., Maheswaranathan, N., & Sohl-Dickstein, J. (2022). Practical tradeoffs between memory, compute, and performance in learned optimizers. ArXiv. https://doi.org/10.48550/arXiv.2203.11860

Microsoft Azure Quantum. (n.d.-b). Quantum error correction. Explore Quantum. https://quantum.microsoft.com/en-us/insights/education/concepts/quantum-error-correction

Mott, A., Job, J., Vlimant, J.-R., Lidar, D., & Spiropulu, M. (2017). Solving a higgs optimization problem with quantum annealing for machine learning. Nature, 550(7676), 375–379. https://doi.org/10.1038/nature24047

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electronic Markets, 33(1). https://doi.org/10.1007/s12525-023-00654-3

Power, L., & Guha, K. (2024). Feature Importance and Explainability in Quantum Machine Learning. ArXiv. https://arxiv.org/abs/2405.08917

Schuld, M., Bergholm, V., Gogolin, C., Izaac, J., & Killoran, N. (2019). Evaluating analytic gradients on quantum hardware. Physical Review A, 99(3). https://doi.org/10.1103/physreva.99.032331

Schuld, M., Sinayskiy, I., & Petruccione, F. (2014). An introduction to quantum machine learning. Contemporary Physics, 56(2), 172–185. https://doi.org/10.1080/00107514.2014.964942

Smith-Goodson, P. (2019, September 16). Quantum Computer Battle Royale: Upstart ions versus Old Guard superconductors. Forbes. https://www.forbes.com/sites/moorinsights/2019/09/16/quantum-computer-battle-royale-upstart-ions-versus-old-guard-superconductors/

Stackpole, B. (2024, January 11). Quantum Computing: What leaders need to know now. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now

Takaki, Y., Mitarai, K., Negoro, M., Fujii, K., & Kitagawa, M. (2021). Learning temporal data with a variational quantum recurrent neural network. Physical Review A, 103(5). https://doi.org/10.1103/physreva.103.052414

van der Schoot, W., Wezeman, R., Eendebak, P. T., Neumann, N. M. P., & Phillipson, F. (2023). Evaluating three levels of quantum metrics on quantum-inspire hardware. Quantum Information Processing, 22(12), Article 451. https://doi.org/10.1007/s11128-023-04184-x

Victor, F., & Hagemann, T. (2019). Cryptocurrency pump and dump schemes: Quantification and detection. 2019 International Conference on Data Mining Workshops (ICDMW), 38, 244–251. https://doi.org/10.1109/icdmw.2019.00045

Wu, S. L., Sun, S., Guan, W., Zhou, C., Chan, J., Cheng, C. L., Pham, T., Qian, Y., Wang, A. Z., Zhang, R., Livny, M., Glick, J., Barkoutsos, P. Kl., Woerner, S., Tavernelli, I., Carminati, F., Di Meglio, A., Li, A. C., Lykken, J., … Wei, T.-C. (2021). Application of quantum machine learning using the quantum kernel algorithm on High Energy Physics Analysis at the LHC. Physical Review Research, 3(3). https://doi.org/10.1103/physrevresearch.3.033221

Xiong, A., Qiao, C., Tong, Y., Qi, B., & Jiang, C. (2023). Block-Chain Abnormal Transaction Detection Method Based on Auto-Encoder and Attention Mechanism. https://doi.org/10.21203/rs.3.rs-2969521/v1