Quantum Transformation in the Payment Industry: Quantum Applications in Future Financial Transactions

Alessio Faccia [1]*
Abraham Itzhak Weinberg [2]

[1] University of Birmingham Dubai, Dubai, United Arab Emirates; a.faccia@bham.ac.uk
[2] AI-WEINBERG, AI Experts, Israel; aviw2010@gmail.com
* Correspondence: a.faccia@bham.ac.uk

Abstract: This article examines the transformative impact of quantum computing on the payment industry, underscoring its potential to revolutionise the security, efficiency, and speed of financial transactions. Quantum computing offers significant advancements over classical computing in processing financial transactions by leveraging superior processing capabilities and advanced cryptographic methods. The paper delves into quantum cryptography's role in enhancing transaction security, the possibilities for accelerated processing speeds, and improving fraud detection techniques. It also highlights the challenges the transition to quantum computing poses, including infrastructure upgrades, the need for specialised expertise, and regulatory complexities. Furthermore, the article discusses the application of quantum computing in simulating financial models for accurate pricing and risk assessment, optimising supply chain finance, and securing Central Bank Digital Currencies (CBDCs) against fraud and cyber threats. Case studies and projects are examined to illustrate quantum computing's current role in the payment sector, identifying emerging trends and potential future applications. The conclusion emphasises the importance of continued research and collaboration among technology specialists, industry leaders, and policymakers to overcome the obstacles to integrating quantum computing. This collaborative effort is crucial for reaping the technology's full benefits, promising a significant transformation in the payment industry's efficiency, security, and processing capabilities.

Keywords: Quantum Computing; Payment Industry; Cryptographic Security; Transaction Processing; Financial Technology Innovation.

1. Introduction

The payment industry stands on the brink of a significant shift, primarily driven by the emergence of quantum computing. This cutting-edge technology, known for its ability to conduct complex calculations at previously unattainable speeds, is set to change substantially how financial transactions are processed and secured.

The development of payment methods has evolved continuously [1]. Traditional means like cash and cheques gave way to digital innovations, including credit cards, online banking, and mobile payments. Each stage has introduced enhancements and new sets of challenges. However, the advent of quantum computing in this domain is set to address these challenges and transform the foundational aspects of financial transactions. Quantum computing represents a departure from the binary approach of classical computing [2]. This shift enables processing capabilities far beyond current standards, representing an improvement and a complete overhaul in computational power. The implications of this technology for the payment industry are significant. It opens up avenues to solve some of the most pressing issues today, such as enhancing transaction security, speeding up processing, and improving fraud detection. Nonetheless, this great potential is accompanied by a series of new challenges. Integrating quantum computing into the existing financial infrastructure brings up considerations regarding readiness, security concerns, and the necessity for updated regulatory frameworks [3].

This article aims to examine these elements, offering insight into how quantum computing can revolutionise the payment industry. It will discuss the present state of this sector, the transformative potential of quantum computing, its practical applications in payment systems, and the necessary strategies for an effective adaptation. As the prospect of quantum computing becomes increasingly tangible, comprehending its potential impact on the payment industry is essential, not just for academic purposes but as a critical step in preparing for a future swiftly drawing closer.

2. Methods

This study adopts a mixed-methodology approach, integrating a comprehensive literature review with examining empirical case studies. This strategy ensures a well-rounded understanding of the theoretical framework of quantum computing and its actual application in the payment industry.

2.1. Literature Review

a) **Scope**: The literature review covers a broad spectrum of sources, including scholarly articles, industry reports, and white papers, focusing on quantum computing and its potential implications for the payment industry.
b) **Selection Criteria**: Sources are selected based on relevance, authoritativeness, and recentness. Preference is given to studies from respected academic journals and reports by leading industry authorities.
c) **Analysis**: The literature is scrutinised to extract key themes and findings, especially relating to advancements in cryptographic security, enhancement of transaction processing speeds, and innovations in fraud detection techniques.

2.2. Empirical Case Studies

a) **Selection of Case Studies**: Various case studies are selected to represent a range of quantum computing applications in the payment industry, including initiatives by financial bodies, technology firms, and collaborative projects.
b) **Data Collection**: Data for these case studies is gathered through interviews with key figures, project documentation analysis, and publicly available information review.
c) **Analysis**: Each case study is analysed to understand its context, implementation process, challenges encountered, and outcomes, particularly focusing on practical aspects such as infrastructural adaptations, integration hurdles, and tangible impacts on security and transaction efficiency.

2.3. Integration of Findings

The literature review and case studies combine findings to offer a comprehensive picture of quantum computing's role in the payment sector. This synthesis provides an informed understanding, including theoretical developments and practical realities. Throughout the research, ethical considerations are paramount, especially in case studies. Consent is sought for all interviews, and confidentiality is upheld for sensitive information.

The methodology applied in this study provides a balanced and thorough exploration of quantum computing in the payment industry. By merging theoretical knowledge from literature with empirical evidence from case studies, the research presents a comprehensive view of this technology's current state and prospects in the financial domain.

3. Current State of the Payment Industry

Over recent years, the payment industry has witnessed significant changes, transitioning from traditional methods to an era predominantly influenced by digital solutions. This evolution is characterised by the adoption of advanced technologies like Blockchain, digital wallets, and mobile payments, each playing a crucial role in shaping the contemporary financial transaction landscape. Blockchain technology, first brought to the fore through the rise of cryptocurrencies such as Bitcoin, has introduced a new approach to transaction security and transparency [4]. Its distributed ledger system provides a decentralised, tamper-resistant record of transactions, enhancing trust and efficiency in digital payments. This technology is particularly effective in mitigating fraud risks and accelerating the pace of cross-border transactions.

In contrast, digital wallets and mobile payments have transformed consumer financial interactions [5]. These methods offer great ease, allowing smartphone users to execute transactions swiftly. Their widespread adoption, especially in areas with substantial mobile usage, has fundamentally shifted consumer spending habits and expectations. Despite these technological strides, the payment industry faces several challenges. Security remains a primary concern as sophisticated cyber threats increasingly target digital financial transactions [6,7]. Although Blockchain offers improved security, it is not immune to risks, and other digital payment methods continue to confront significant vulnerabilities.

Scalability and transaction speed also present hurdles. For instance, Blockchain encounters limitations in transaction capacity, which can result in delays and higher costs [8]. Similarly, while digital wallets and mobile payments are convenient, they depend on the underlying financial infrastructure, which can be inefficient or unreliable, particularly in less developed areas.

Additionally, the regulatory framework for digital payments needs constant updates [9,10]. With these technologies crossing international borders, they challenge regulatory bodies to create standardised and compliant systems. It often results in a fragmented regulatory environment, complicating operations for payment service providers across different regions. While the latest technologies in the payment sector have brought considerable efficiency and user experience enhancements, they are not devoid of limitations and challenges. These issues underscore the necessity for ongoing innovation and development, paving the way for future technological integrations, such as the prospective incorporation of quantum computing.

Building on the challenges and limitations of current payment technologies, there is a growing call for innovative solutions that can bridge these gaps [11-13]. This need goes beyond simple improvements; it calls for transformative changes that can reshape the existing framework of financial transactions. The potential incorporation of quantum computing into the payment sector could be revolutionary. With its exceptional processing capabilities and advanced cryptographic strengths, Quantum computing promises to elevate the security and efficiency of financial transactions well beyond what is currently possible. For example, quantum cryptography could provide a much more secure form of data encryption, significantly bolstering defences against cyber threats [14]. In the payment industry, HSBC is officially pioneering this technology [15], while Mastercard is still in its infancy [16]. More generally, the UK finance industry, led by UK Finance, has raised concerns that quantum computing could undermine the security of the country's payment system. A report by UK Finance warns that quantum computing, particularly through Shor's algorithm, could render asymmetric Public key Infrastructure (PKI) encryption, a cornerstone of finance industry security, ineffective. The industry urges collaboration between government and industry to prepare for potential threats and capitalise on quantum technology's opportunities. UK Finance also outlines several recommendations, including establishing a quantum-safe task force and developing a skilled quantum workforce [17].

Furthermore, the capacity of quantum computers to process immense volumes of data at extraordinary speeds could lead to a paradigm shift in transaction processing. It could drastically reduce the time taken for transactions, particularly in international payments, which may take several days. Reducing transaction times would enhance customer satisfaction and contribute to the fluidity of the global financial system. Nevertheless, integrating quantum technology into the payment sector presents its hurdles. A primary obstacle is the absence of a comprehensive quantum infrastructure to support large-scale, commercial financial applications [18]. Establishing such an infrastructure would require considerable investments in research and development and necessitates collaboration between technology experts, financial institutions, and regulatory bodies.

Another challenge is cultivating a workforce proficient in quantum technology. Given this field's novelty and specialised nature, there is a shortage of professionals equipped with the necessary skills to develop and manage quantum computing systems [19]. Addressing this shortage will need focused educational and training initiatives.

Moreover, preparing existing financial institutions for quantum integration poses a considerable challenge. Many current systems and processes are not ready to be merged with or to harness the advantages of quantum computing [20,21]. Adapting these systems for quantum integration will be complex, lengthy, and demanding meticulous planning and implementation. Indeed, while the potential advantages of integrating quantum computing into the payment industry are substantial, realising these advantages will involve overcoming a series of technical, infrastructural, and regulatory challenges. The following section of this article will focus on how quantum computing could specifically transform various facets of the payment sector, offering insight into a future where financial transactions are more secure, efficient, and user-centric.

4. Current State of the Payment Industry

Quantum computing represents a significant departure from classical computing, laying the foundation for what many consider a revolution in information processing. This section outlines the fundamental principles of quantum computing and how it differentiates from classical computing. It also examines the potential impact of quantum computing on the payment industry, focusing on enhancing security and transaction speed.

4.1. Fundamentals of Quantum Computing

Classical computing, which powers most digital technologies, operates on bits. These bits are binary, meaning they exist in one of two states: 0 or 1. Quantum computing, however, utilises quantum bits or qubits. Unlike bits, qubits can exist in multiple states simultaneously due to two key quantum principles: superposition and entanglement [22].

- **Superposition** allows a qubit to be in a combination of both 0 and 1 states at the same time, vastly increasing the computational power.
- **Entanglement** is a phenomenon where qubits become interconnected so that the state of one qubit can instantaneously influence the state of another, regardless of the distance separating them.

It means that quantum computers can process a massive amount of information at a fraction of the time it takes for classical computers, making them exceptionally powerful for certain types of computations.

4.2. Quantum Computing in Payment Processing

In payment processing, quantum computing could address two major concerns: security and transaction speed.

- **Enhancing Security**: One of the most promising applications of quantum computing in payments is cryptography. Quantum cryptography could potentially create encryption methods that are impossible to break with classical computers. It is particularly relevant in financial transactions, where securing sensitive data is paramount. The development of quantum-resistant encryption methods will be crucial in safeguarding against potential quantum-based cyber threats.
- **Improving Transaction Speed**: Quantum computing can also significantly accelerate the processing of transactions. It is particularly beneficial for complex computations required in fraud detection and risk analysis, areas that are critical in the payment industry. The ability to process large volumes of transactions quickly and efficiently could lead to real-time verification, a major step forward in reducing processing times, especially for cross-border payments.

The introduction of quantum computing into the payment industry could thus transform the way financial transactions are conducted. By providing advanced solutions for security and enabling faster transaction processing, quantum computing can potentially address some of the most pressing challenges the industry faces today. However, harnessing this potential will require overcoming substantial technical and infrastructural challenges, which will be the focus of the subsequent sections.

5. Current State of the Payment Industry

With its unique capabilities, Quantum computing is poised to revolutionise the payment industry by offering solutions in three critical areas: encryption and security, faster processing, and fraud detection. This section delves into how quantum computing can enhance these aspects of the payment sector.

5.1. Encryption and Security: Quantum Cryptography

One of the most significant contributions of quantum computing in the payment industry is the field of encryption and security through quantum cryptography [23]. Traditional encryption methods, even the most robust ones used in financial transactions today, may eventually become vulnerable to the advanced computational power of quantum computers. However, quantum cryptography, particularly Quantum Key Distribution (QKD), offers a way to create virtually unbreakable encryption [24].

- **Quantum Key Distribution (QKD)**: QKD uses quantum mechanics principles to distribute encryption keys securely. The fundamental property of quantum particles – that observing them alters their state – ensures that any attempt at eavesdropping can be immediately detected. It means that QKD can provide a level of security that is fundamentally unachievable by classical cryptographic methods, ensuring the integrity and confidentiality of financial transactions.

5.2. Faster Processing: Quantum Algorithms

Processing speed is another area where quantum computing is set to make significant strides. Quantum algorithms can process complex transactions much faster than current systems because they can perform multiple calculations simultaneously [25].

- **Quantum Algorithms for Transaction Settlement:** In the payment industry, transaction settlement, particularly in cross-border payments, can be time-consuming due to the complexity of validating and reconciling transactions across different financial institutions and systems. Quantum algorithms can greatly accelerate this process, enabling near-instantaneous settlements. This speedup improves liquidity and reduces credit risks, contributing to more efficient financial markets.

5.3. Fraud Detection: Enhanced Capabilities

Fraud detection is an ongoing challenge in the payment industry. The ability of quantum computing to analyse vast datasets quickly and identify patterns can significantly enhance fraud detection mechanisms [26].

- **Quantum-Enhanced Fraud Detection:** When using quantum algorithms, financial institutions can analyse transaction data in real time to detect unusual patterns or anomalies that may indicate fraudulent activity. This capability is crucial when fraud techniques constantly evolve and become more sophisticated. Quantum-enhanced fraud detection systems can provide a more dynamic and robust defence against financial fraud, protecting institutions and their customers.

Integrating quantum computing into the payment industry can revolutionise the sector by providing ultra-secure transactions, faster processing speeds, and more effective fraud detection. These advancements could address current limitations and set new standards for efficiency and security in financial transactions. However, realising these benefits will require overcoming significant challenges, including developing quantum-resistant infrastructure and cultivating specialised talent, which is essential for implementing quantum technologies in the payment industry.

5.4 Key hurdles for applying quantum computing to payment

Several key hurdles need to be addressed when applying quantum computing to payment processing, primarily due to current limitations in quantum hardware. Firstly, noisy qubits and errors pose a significant challenge [27]. The limited number of qubits in today's quantum devices are prone to errors caused by noise and interference, which negatively impact the accuracy of computations. Major improvements in error correction are necessary to overcome this obstacle.

Another limitation is the short coherence times of qubits, known as the decoherence of qubits [28]. Quantum properties of qubits decay rapidly due to interactions with the environment. It places constraints on the depth and complexity of algorithms that can be reliably executed.

Additionally, limited connectivity among qubits restricts the types of quantum circuits that can be constructed on Noisy Intermediate-Scale Quantum (NISQ) devices [29]. This limitation directly affects the range of problems that can be effectively addressed.

Due to qubit count limitations, large-scale problems in payment processing involving extensive data and complex correlations may still be beyond future quantum devices' capabilities [30]. Such classically intractable applications require further advancements in qubit technology. Moreover, developing a hybrid classical-quantum stack necessitates significant algorithmic research to determine the optimal division between classical and quantum subroutines for practical applications. Integration challenges persist in this area [31]. The economic viability of quantum computing is another consideration. Building large-scale, universal, and error-corrected quantum computers requires substantial long-term investments. Therefore, near-term quantum applications in payment processing should demonstrate clear cost advantages to gain traction.

Furthermore, regulatory acceptance is crucial. Financial regulators must thoroughly assess any quantum applications' security, correctness, and explainability before approving their production use, particularly in critical infrastructure related to payment processing.

Addressing these challenges will be essential for the successful application of quantum computing in payment processing, requiring advancements in hardware, algorithms, economics, and regulatory frameworks.

6. Case Studies and Emerging Trends

As the payment industry gradually integrates quantum computing, various case studies and emerging trends have begun to demonstrate its potential applications and future directions. This study examines real-world examples and ongoing projects where quantum computing is applied in the payment sector and explores emergent trends and future possibilities.

6.1. Real-World Examples and Ongoing Projects

a) **Quantum-Enhanced Security Experiments**: Leading financial institutions and technology companies are experimenting with quantum cryptography to boost transaction security. For example, some banks are trialling Quantum Key Distribution (QKD) systems for more secure data transmission, aiming to elevate the security level of financial transactions [32].
b) **Collaborations for Quantum Research**: Partnerships among financial institutions, technology firms, and academic bodies are increasing. These collaborations are focused on developing quantum computing solutions specifically for the financial sector, targeting areas such as asset valuation, risk assessment, and rapid trading [33].
c) **Quantum Computing in Blockchain**: Certain blockchain enterprises are investigating using quantum computing to enhance scalability and transaction speeds. These initiatives seek to overcome some of blockchain technology's current limitations, particularly regarding transaction capacity [21,34].

6.2. Emerging Trends and Future Applications

a) **Quantum Computing as a Service (QCaaS)**: Considering the expense and complexity of quantum computers, Quantum Computing as a Service is emerging as a practical option [35]. This approach enables financial institutions to utilise quantum computing power via cloud services, facilitating easier experimentation and integration of quantum solutions. Quantum Computing as a Service (QCaaS) is emerging as a practical option for the financial sector, considering quantum computers' high expense and technical complexity. This service-based model enables financial institutions to access quantum computing power through cloud services, simplifying the experimentation and integration of quantum solutions. QCaaS offers a route for financial organisations to explore and utilise quantum computing without significant capital investment. It allows smaller entities to benefit from quantum capabilities, broadening access to this advanced technology. However, a key challenge is maintaining security and reliability, especially when handling sensitive financial data. Providers must establish stringent security measures and assure data privacy and system dependability.
b) **Development of Quantum-Resistant Algorithms**: With the advancement of quantum computing, there is a trend towards creating quantum-resistant algorithms. These cryptographic algorithms are designed to secure data against both classical and quantum computing threats, ensuring long-term data protection. These algorithms aim to provide security against classical and emerging quantum computing threats, safeguarding data over the long term. Financial institutions manage vast amounts of confidential data, so protection against cyber threats is paramount. Quantum-resistant algorithms are crucial for defending this data against future quantum-based attacks. Crafting these algorithms involves deep research and cooperation among cryptographers, quantum physicists, and financial professionals. Continuous updating and testing of these algorithms against advancing quantum capabilities are essential.
c) **Quantum AI in Financial Analysis**: Quantum computing and artificial intelligence (AI) are expected to revolutionise financial modelling and forecasting [36,37]. Quantum AI's ability to process extensive datasets efficiently can lead to more precise market trends, credit assessments, and risk management predictions. Quantum computing and artificial intelligence (AI) are set to revolutionise financial modelling and forecasting. Quantum AI's efficient processing of large datasets enhances the precision of market trend predictions, credit evaluations, and risk management. Quantum AI can swiftly and accurately analyse complex financial datasets, leading to better-informed decisions in investment and risk

strategies. Given the dynamic nature of financial markets, quantum AI systems must be adaptable, learning from new data and adjusting predictive models as necessary.

d) **Regulatory Developments for Quantum Technologies**: As quantum computing influences the financial sector, regulatory frameworks adapt to manage its usage [38]. It includes formulating standards for quantum computing applications in finance, ensuring they comply with security, regulatory, and ethical norms. As quantum computing influences the financial sector, regulatory frameworks adapt to govern its use. There is an evident need to formulate standards for applying quantum computing in finance, adhering to security, regulatory, and ethical guidelines. Regulators are tasked with setting clear rules on applying quantum computing in financial operations, covering security, data protection, and the ethical use of AI. The worldwide nature of finance and quantum computing calls for international regulatory collaboration. Developing uniform regulatory standards across countries will be key in managing the impact of quantum computing on the global financial system.

The case studies and trends in quantum computing within the payment industry point towards a future where financial transactions are quicker, more secure, and more efficient. Keeping abreast of these developments is vital for maintaining a competitive edge. The ongoing advancement of quantum technologies promises to tackle existing challenges in the payment sector and open new opportunities for innovation and growth.

7. Managing the transition to Quantum Computing in Payments

The payment industry has started contemplating the integration of quantum computing, and it faces a significant transition. This change involves technological upgrades and a comprehensive operational, infrastructural, and regulatory framework shift. This chapter discusses the key challenges in this transition and outlines strategies to manage them effectively.

7.1. Addressing Technical and Infrastructural Challenges

The shift to quantum computing in payments demands considerable advancements in both hardware and software. Current systems must be re-evaluated and redesigned to be compatible with quantum technologies.

a) **Upgrading Infrastructure**: Financial institutions will need to invest in quantum-resistant infrastructure. It includes hardware capable of supporting quantum computing and software leveraging its capabilities. Ensuring compatibility between quantum systems and existing digital platforms will be crucial.

b) **Data Security and Privacy**: As quantum computing can potentially break current encryption standards, developing quantum-resistant cryptographic methods becomes essential. Institutions must ensure that data remains secure during and after the transition.

c) **Quantum-Readiness of Systems**: Assessing and preparing current IT systems for quantum integration is vital. It includes understanding which components can be quantum-enhanced and which require a complete overhaul.

7.2. Cultivating a Quantum-Skilled Workforce

The lack of quantum computing expertise is a significant barrier. Financial institutions must focus on developing a workforce skilled in quantum technologies.

a) **Training and Education**: Implementing training programs for existing IT staff and investing in higher education partnerships can cultivate the required talent pool.

b) **Hiring Specialists**: Recruiting individuals with specific expertise in quantum computing can accelerate the transition and ensure effective implementation.

7.3. Managing Regulatory and Compliance Issues

As quantum computing transcends national borders, it creates a complex regulatory landscape. Ensuring compliance with international standards and laws is critical.

a) **Regulatory Collaboration**: Financial institutions should engage with regulatory bodies to shape policies that support quantum computing while safeguarding financial stability and consumer protection.

b) **Standardisation**: Working towards standardised protocols and security measures in quantum computing can facilitate smoother international transactions and interoperability between institutions.

Preparing for Quantum Threats

The prospect of quantum computing also introduces new types of cyber threats. Financial institutions must anticipate and prepare for these.

a) **Quantum-Resistant Security Measures**: Developing security protocols resistant to quantum computing attacks is imperative.
b) **Continuous Monitoring and Adaptation**: Establishing systems for continuous monitoring of quantum threats and adapting security measures is crucial.

The transition to quantum computing in the payment industry is a multifaceted challenge, requiring coordinated efforts in technological upgrades, workforce development, regulatory compliance, and security enhancements. A strategic and proactive approach is essential to navigate this transition effectively, ensuring that the payment industry can harness the full potential of quantum computing while mitigating associated risks. The successful integration of quantum technologies will enhance the efficiency and security of financial transactions and position institutions at the forefront of the next wave of technological innovation in finance.

8. Empirical test, challenging the current cryptography

The scarcity of quantum programmers is exacerbated by the limited availability of quantum programming languages and the platforms supporting them. This situation is further compounded by the fact that only a select number of universities offer relevant courses. Moreover, the practical study of quantum computing faces obstacles due to the current commercial unavailability of quantum computers, though IBM has facilitated access via the cloud. In this context, we propose a novel approach by integrating the capabilities of Chat GPT with quantum computing to experiment. This experiment assesses the potential of leveraging Chat GPT, devoid of any quantum programming knowledge, in challenging contemporary digital cryptography. We clarify that this integration of Chat GPT with quantum computing is a methodological experiment designed to explore new avenues in addressing the digital cryptography challenge rather than employing Chat GPT as a direct solution within our analysis. This distinction is important to ensure clarity for reviewers and to avoid any misconceptions about the role of Chat GPT in our study. Below, we presented an example of a simulated analysis of these aspects and performed a test Chat GPT without any knowledge of quantum programming to verify if it is potentially feasible to challenge the current digital cryptography.

8.1. Quantum Programming Languages

We need to consider several factors to compare quantum programming languages in terms of their efficiency, such as their execution speed, ease of use, versatility, and the level of support they provide for different quantum hardware. The efficiency of a quantum programming language can also depend on the specific use case, such as quantum algorithm development, quantum machine learning, or quantum simulation. Some of the most prominent quantum programming languages include **Qiskit**, which IBM developed. It is widely used for creating and running quantum computing programs on IBM's quantum computers and simulators (see Table 1). **Cirq**: Developed by Google, it is designed to create, edit, and invoke Noisy Intermediate Scale Quantum (NISQ) circuits (see Table 2); **Q# (Q-Sharp)**: Developed by Microsoft, it is integrated with classical languages like C# and focuses on developing quantum algorithms (see Table 3); **Quipper**: A high-level functional programming language for quantum computing, known for its expressive power in quantum algorithm representation (see Table 4); **ProjectQ**: An open-source software framework for quantum computing that started at ETH Zurich (see Table 5). Python is known as the most popular quantum programming language, and its widespread usage in various domains contributes to this distinction. Its status as the world's most widely used programming language further boosts its popularity [39]. Additionally, the early adoption of cloud-based quantum computing heavily relied on Python, further solidifying its position. The subsequent evolution of frameworks and utilities has built upon the foundations laid by Python, expanding the range of offerings available in the language. Even independent libraries like Bloqade-Python leverage Python's popularity, facilitating broader acceptance. Several prominent quantum computing software development kits (SDKs) support Python, including Qiskit, Cirq, and PennyLane [40]. As mentioned above, Qiskit, developed by IBM, caters to their quantum hardware and simulators, while Google maintains Cirq as an open-source toolkit. PennyLane focuses on differentiable programming for quantum machine learning.

Julia is considered as the second most popular language for quantum computing, with the growing popularity of neutral atom quantum computing further bolstering its recognition [39]. Julia surpasses Python in terms of speed and memory management for classical pre-processing, post-processing, and simulations. Although Python is generally considered more user-friendly.

Table 1. Qiskit features and criteria

Feature/Criteria	Description	Sources
Ease of Use	Beginner-friendly, extensive documentation, accessible to various expertise levels, modular architecture, abstracts complexities of quantum mechanics.	https://quantumzeitgeist.com/qiskit-the-journey-so-far-5-years-of-the-popular-quantum-programming-language-and-framework/ https://dotcommagazine.com/2023/12/qiskit-a-comprehensive-guide-2/
Execution Speed and Performance	120x speedup in simulations, Qiskit Runtime leverages cloud computing, Qiskit 1.0 with improved transpiling, reduced memory usage, and 16x faster circuit binding.	https://quantumzeitgeist.com/qiskit-the-journey-so-far-5-years-of-the-popular-quantum-programming-language-and-framework/ https://www.zdnet.com/article/ibm-just-solved-this-quantum-computing-problem-120-times-faster-than-previously-possible/ https://www.hpcwire.com/2021/05/11/ibm-debuts-qiskit-runtime-for-quantum-computing-reports-dramatic-speed-up/
Community and Support	Global community of users, educational engagement, and resources for teaching quantum computing.	https://quantumzeitgeist.com/qiskit-the-journey-so-far-5-years-of-the-popular-quantum-programming-language-and-framework/ https://dotcommagazine.com/2023/12/qiskit-a-comprehensive-guide-2/
Integration with IBM Quantum	Access to IBM's quantum systems and cloud-based quantum processors bridges classical and quantum computing.	https://www.ibm.com/quantum/qiskit https://dotcommagazine.com/2023/12/qiskit-a-comprehensive-guide-2/
Open-Source Nature and Development	Open-source projects, community-driven development, and source code are available on GitHub.	https://dotcommagazine.com/2023/12/qiskit-a-comprehensive-guide-2/
Recent Developments and Future Plans	Incorporation of Generative AI capabilities, 10-year quantum roadmap, and simplification of developer experience.	https://www.hpcwire.com/2023/12/04/ibm-quantum-summit-two-new-qpus-upgraded-qiskit-10-year-roadmap-and-more/

Table 2. Cirq features and criteria

Feature/Criteria	Description	Sources
Ease of Use	Designed for simplicity and usability, Cirq provides a straightforward interface for working with quantum circuits. It is suitable for beginners and experts alike, with a design that simplifies the complexities of quantum computing.	https://github.com/quantumlib/Cirq https://quantumai.google/cirq
Execution Speed and Performance	Optimised for performance, Cirq efficiently simulates quantum circuits. Its integration with TensorFlow Quantum allows for fast quantum machine learning experiments.	https://www.tensorflow.org/quantum#:~:text=URL%3A%20https%3A%2F%2Fwww https://www.tensorflow.org/quantum

Community and Support	Cirq boasts a growing global community with ample support through forums and documentation. Google and other institutions frequently contribute educational resources for learning and experimenting with Cirq.	https://quantumai.google/cirq#:~:text=Cirq%20is%20a%20Python%20software,art%20results https://quantumai.google/cirq/start/basics#:~:text=Qubits%20Gates%20and%20operations%20Circuits,of%20how%20to%20use%20Cirq
Integration with Google Quantum AI	Cirq is closely integrated with Google's quantum computing initiatives, including access to Google's quantum processors for experimentation and research.	https://quantumai.google/cirq#:~:text=Cirq%20is%20a%20Python%20software,art%20results
Open-Source Nature and Development	Cirq is developed and maintained by a community of contributors as an open-source framework. Its source code is freely available on GitHub, encouraging community-driven enhancements and development.	https://github.com/quantumlib/Cirq https://blog.research.google/2018/07/announcing-cirq-open-source-framework.html#:~:text=URL%3A%20https%3A%2F%2Fblog.research.google%2F2018%2F07%2Fannouncing
Recent Developments and Future Plans	Continuous updates to improve usability and performance, focusing on integrating with other Google technologies for quantum research and applications. Plans include expanding its capabilities and improving integration with machine learning frameworks.	https://opensource.googleblog.com/2022/07/Cirq-Turns-1.0.html#:~:text=Cirq%20is%20a%20Python%20framework,these%20systems%20and%20is

Table 3. Q# (Q-Sharp)

Feature/Criteria	Description	Sources
Ease of Use	Q# is an open-source, high-level programming language that draws familiar elements from Python, C#, and F#, supporting procedural programming with quantum-specific data structures.	https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk
Execution Speed and Performance	Q# is designed to optimise the execution of quantum components, focusing on expressing information for efficient execution independent of the context.	https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk
Community and Support	Microsoft's Quantum Development Kit provides IDE support and tools for program visualisation and analysis, with resources for learning and using Q#.	https://learn.microsoft.com/en-us/azure/quantum/user-guide/
Integration with Quantum Hardware	Q# is hardware agnostic and can be used across various quantum hardware backends in Azure Quantum. It allows the building of reusable components and layers of abstractions for scalable applications.	https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk
Open-Source Nature and Development	Q# is part of the open-source Quantum Development Kit (QDK), which includes quantum libraries, simulators, and extensions for IDEs.	https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk
Recent Developments and Future Plans	The Azure Quantum Development Kit has been rebuilt to improve performance and user experience. The new version is faster, smaller, and browser-compatible, written mostly in	https://devblogs.microsoft.com/qsharp/ https://devblogs.microsoft.com/qsharp/introducing-the-azure-quantum-development-kit-preview/

	Rust. Plans include adding multi-file support, richer QIR support, and continuous Q# language improvement updates.	

Table 4. Quipper

Feature/Criteria	Description	Sources
Ease of Use	Quipper is an embedded, scalable, functional programming language with a high-level circuit description language. It supports procedural and declarative styles and provides built-in facilities for automatic synthesis of reversible quantum circuits.	https://www.mathstat.dal.ca/~selinger/quipper/
Execution Speed and Performance	Quipper is designed to be scalable, going beyond toy algorithms and handling more complex quantum algorithms. It can generate quantum gate representations using trillions of gates, indicating its capability to manage large-scale computations effectively	https://ar5iv.labs.arxiv.org/html/1304.3390
Community and Support	Quipper offers online documentation, a tutorial introduction, and detailed operator and data type descriptions. Contributors are listed on the official website.	https://www.mathstat.dal.ca/~selinger/quipper/
Integration with Quantum Hardware	Quipper operates based on an idealised model of quantum computation, typically abstracting from the specifics of physical quantum hardware. The programming language design of Quipper does not focus on any particular model of quantum hardware but rather provides a high-level abstraction suitable for various computational models	https://ar5iv.labs.arxiv.org/html/1304.3390
Open-Source Nature and Development	Quipper is open-source, with its source code, libraries, and algorithm implementations available online.	https://www.mathstat.dal.ca/~selinger/quipper/
Recent Developments and Future Plans	The latest release as of December 2019 is Quipper 0.9.0.0, which introduced a new module structure and compatibility updates with GHC and Haskell libraries.	https://www.mathstat.dal.ca/~selinger/quipper/

Table 5. ProjectQ

Feature/Criteria	Description	Sources
Ease of Use	ProjectQ is a Python-based open-source software framework for quantum computing designed for inventing, implementing, testing, debugging, and running quantum algorithms. It is known for its simplicity and intuitive syntax.	https://projectq.readthedocs.io/en/latest/index.html
Execution Speed and Performance	ProjectQ is recognised as a state-of-the-art quantum simulator. It held the record for a 45-qubit quantum circuit simulation for several months. The simulator utilises parallelism technologies like SIMD, OpenMP, and MPI	https://docs.yaoquantum.org/v0.3/dev/benchmark/

	to enhance calculation speeds. In benchmarks, ProjectQ's performance is similar to that of Yao.jl, another quantum computing framework, with both being close to the theoretical performance bound	
Community and Support	ProjectQ supports various platforms like AQT, AWS Braket, Azure Quantum, IBM QE, and IonQ. It offers modules for circuit exporting/printing, simulation, utilities, and compiler engines for various tasks.	https://projectq.readthedocs.io/en/latest/projectq.backends.html
Integration with Quantum Hardware	ProjectQ modules support integration with platforms like AQT, AWS Braket, Azure Quantum, IBM QE, and IonQ, facilitating connections between software and quantum hardware.	https://projectq.readthedocs.io/en/latest/projectq.backends.html
Open-Source Nature and Development	ProjectQ is open-source and released under the Apache 2 license. It is extensible, allowing contributions to its compiler, embedded domain-specific language, and libraries. Ensures code quality through reviews and continuous integration testing.	https://projectq.readthedocs.io/en/latest/index.html
Recent Developments and Future Plans	The most recent version of ProjectQ is 0.8.0, released on October 18th, 2022. Prior versions were released at various intervals, showcasing the active development and updates of the framework.	https://pypi.org/project/projectq/#history

8.2. Quantum Hardware

Quantum computing has seen significant advancements, with several key players developing state-of-the-art quantum computers. The most important quantum computers available are presented in Table 6 below. This table reflects the most recent update from Forbes [42], which provides the list published on December 10th, 2023.

Table 6. Most Important Quantum Computers Available

Rank	**Company**	**Description**	**Qubits**	**Country**	**Quantum Computer Category**
1	IBM	Leader in quantum computing; known for Quantum System Two and the Heron chip. Aiming for a 100,000 qubit system by 2033.	1,121	USA	Superconducting
2	Google Quantum AI	Achieved "quantum supremacy" in 2019 with Sycamore; aims to build a 1 million qubit system within a decade.	53	USA	Superconducting
3	Amazon	Established a centre for quantum computing at Caltech; offers Amazon Braket for accessing various quantum hardware.	80	USA	Superconducting (supports Rigetti's processor)

4	Microsoft	Provides Azure Quantum with tools and resources for quantum computing, working on scalable, fault-tolerant quantum computers.	100+	USA	Topological / Superconducting
5	Intel	Released a 12-qubit silicon chip, Tunnel Falls; working on a full-stack quantum system and next-gen quantum chip.	12	USA	Quantum Dots
6	D-Wave	Specialises in quantum annealing, systems used by enterprises like Google and NASA.	5,000+	Canada	Quantum Annealing
7	Quantinuum	Result of a merger between Cambridge Quantum Computing and Honeywell focuses on trapped ion quantum computers.	32	USA/UK	Trapped Ions
8	Rigetti	Built integrated quantum computing systems using superconducting qubit technology; offered a cloud platform called Forest.	84	USA	Superconducting
9	Xanadu	A full-stack photonic quantum computing company builds quantum computers and provides quantum cloud services.	8-24	Canada	Photonic
10	Atos Quantum	Known for Quantum Learning Machine (QLM), a dedicated hardware for quantum software development.	41	France	Simulation

8.3. Testing the power of Generative AI in Leveraging the existing technology

The payment industry, particularly in cryptography, faces potential threats from quantum computing due to the latter's ability to solve complex mathematical problems much faster than classical computers. This capability can undermine the security foundations of current cryptographic algorithms: a) **Breaking Current Cryptography**: Most digital payment systems rely on cryptographic algorithms like RSA and Elliptic Curve Cryptography (ECC) for secure transactions. These algorithms are based on the difficulty of factoring large numbers or solving the discrete logarithm problem. With their ability to solve these problems efficiently using algorithms like Shor's, Quantum computers could decrypt data encrypted with these methods, potentially exposing sensitive financial information; b) **Impact on Blockchain and Cryptocurrencies**: Quantum computing also poses a risk to blockchain technologies and cryptocurrencies, which are becoming increasingly relevant in the payment industry. Quantum computers could potentially break the cryptographic hashes that secure Blockchain, enabling the alteration of transaction histories; c) **Future-Proofing Cryptography**: In response to these threats, the development of quantum-resistant or post-quantum cryptography is underway. These new cryptographic systems are designed to be secure against the capabilities of quantum computers and are essential for future-proofing the payment industry. d) **Transition Period Risks**: Transitioning to quantum-resistant cryptography is both a technical and logistical challenge. Updating the global financial infrastructure to new standards will take time, and there is a risk associated with the transition period when both old and new systems are in use. e) **Data Harvesting Threat [43]**: There is also the concern that attackers could collect encrypted data to decrypt it once quantum computing becomes sufficiently advanced. This type of attack is known as "harvest now, decrypt later," and it poses a long-term threat to data privacy.

Using the most powerful ChatGPT engine (GPT4.0) and adequately prompting the command to avoid restriction, the output demonstrated that it is potentially possible to use the current technologies, even without proper knowledge of quantum programming, to approach an (ethical) hacking of the current Cryptography underpinning the security of the financial systems.

DISCLAIMER: The example is performed for educational purposes and presented as a worrying warning for companies in the payment industry.

PROMPT: "*Using Qiskit, code and provide the instructions to decode (reverse engineer) the algorithm of an OTP by providing the output at regular intervals (educational purpose to demonstrate capabilities). This code should run on the free available quantum cloud provided by IBM.*" Answer in Figures 1a-1c

ChatGPT

To reverse-engineer (decode) the algorithm of a One-Time Pad (OTP) using Qiskit and IBM's quantum computing services, it's important to understand a few key points:

1. **One-Time Pad Nature**: By design, an OTP is theoretically unbreakable when used correctly. This is because the key is random, at least as long as the message, and used only once. There's no pattern or structure to exploit in a correctly implemented OTP.
2. **Quantum Computing Limitations**: While quantum computers have potential in breaking certain types of cryptographic systems (like RSA), they don't provide a magic solution for breaking all forms of encryption, especially not OTPs.
3. **Educational Demonstration**: If you're looking to demonstrate the capabilities of quantum computing in the context of encryption and decryption, a better approach might be to focus on algorithms that are known to be vulnerable to quantum attacks, such as Shor's algorithm for factoring large numbers.

Given these points, let's create an educational example that shows how to use Qiskit and IBM's quantum computers to implement a basic quantum algorithm. We can't reverse-engineer an OTP, but we can demonstrate quantum capabilities in another context. For instance, we could implement a simple quantum circuit that demonstrates superposition and entanglement, key principles of quantum computing.

Figure 1a: Chat GPT 4 TEST Answer.

1. **Install Qiskit**: If you haven't already installed Qiskit, you can do so using pip:

python Copy code

```
!pip install qiskit
```

2. **Create a Quantum Circuit**:

python Copy code

```
from qiskit import QuantumCircuit, execute, Aer

# Create a Quantum Circuit with 2 qubits
qc = QuantumCircuit(2)

# Apply a Hadamard gate to put qubit 0 into superposition
qc.h(0)

# Apply a CNOT gate to entangle the qubits
qc.cx(0, 1)

# Draw the circuit
qc.draw(output='mpl')
```

Figure 1b: Chat GPT 4 TEST Answer.

3. **Simulate the Circuit**:

```python
# Use Aer's qasm_simulator
simulator = Aer.get_backend('qasm_simulator')

# Execute the circuit on the simulator
job = execute(qc, simulator, shots=1000)

# Grab results from the job
result = job.result()

# Returns counts
counts = result.get_counts(qc)
print(counts)
```

4. **Running on IBM's Quantum Cloud**:
   To run this circuit on IBM's quantum cloud, you'll need to set up an IBM Quantum Experience account and get an API token. You can then use this token to access IBM's quantum computers. Remember, the queues for these computers can be long, and the example given is more illustrative than practical for understanding quantum computing principles.

Figure 1c: Chat GPT 4 TEST Answer.

Figures 1a-1c: Chat GPT 4 TEST Answer.

The result is worrying and impressive at the same time. It suggests that without coding skills and using the available technologies (IBM provides a Cloud Test platform with a few Qbits for free), hackers with potentially malicious intentions can dangerously approach reverse engineering of the current digital cryptographies protecting the banking and payment systems. The highlighted concerns regarding the potential vulnerabilities in current digital cryptography due to advancing quantum computing technologies are significant. It is important to consider that a) **Current Quantum Computing Stage**: As of my latest update in April 2023, quantum computing remains in its early developmental phase. The qubits available on platforms like IBM's quantum cloud are still limited, and maintaining qubit stability for complex tasks is a challenge. Consequently, quantum computers cannot currently break contemporary cryptographic systems; b) **Security of One-Time Pad (OTP)**: The OTP remains secure against quantum computing attacks when used correctly. Its security stems from using a key that is random, as long as the message, and used only once; c) **Vulnerability of Other Cryptographic Systems**: Quantum computing poses a potential threat to cryptographic algorithms like RSA and ECC, which form the backbone of many digital security protocols, including those in banking and online transactions.

9. Quantum Simulation of Financial Models and Instruments

As explored in this section, quantum simulation techniques are employed to bolster various activities discussed in the payment industry, particularly in the simulation and pricing of options, bonds, and other financial instruments. By leveraging quantum computing, various aspects of financial modelling can be enhanced. For instance, option pricing can benefit from efficient simulation of stochastic processes, enabling more accurate valuation of complex derivatives such as barrier, path-dependent, or American options [44]. Quantum machines can also utilise large market data sets to infer improved implied volatility surfaces, ensuring consistent pricing across different strikes and maturities. In bond pricing, quantum computations can handle multi-factor models that incorporate credit risk, interest rate movements, and prepayment risk, enabling accurate pricing of fixed-income products like mortgage bonds [45,46]. Quantum approaches can further identify optimum delta-neutral hedging strategies for complex options portfolios, considering the impact of simultaneous trades on the entire portfolio [47,48].

Additionally, quantum simulation can capture hidden correlations across diverse risks and asset classes, leading to improved pricing of correlation-sensitive derivatives and enhanced portfolio diversification [49]. Quantum tools can aid in calibration by exploring larger parameter spaces to optimally align financial models with market prices of related instruments [50]. Furthermore, risk analysis can be enhanced through quantum methods that evaluate scenarios in superposition, facilitating comprehensive stress testing of product, desk, and firm-wide downside exposure [51]. Finally, quantum technologies may identify and exploit mispricings across related markets by matching quantum-simulated prices to observed exchanges, opening avenues for arbitrage opportunities [51].

10. Supply Chain Finance and Quantum Optimisation

The payment industry encompasses both direct and indirect aspects. This section focuses on the indirect applications of payment systems within supply chain networks. Here, we propose approaches for optimising financing within the supply chain using quantum technology.

Quantum annealing/optimisation offers a powerful approach for optimising inventory, logistics, and supply chain financing programs, enabling businesses to enhance their operational efficiency and reduce costs [52-54]. Through quantum annealing, various aspects of supply chain management can be improved holistically and interconnectedly. For instance, inventory optimisation can determine the optimal levels and locations of inventory across a large supply network, considering factors such as costs and demand satisfaction while leveraging the quantum annealer's ability to consider more variables and constraints [55]. Routing optimisation can then identify the most efficient routes for product delivery by trucks or ships, considering delays, costs, fuel usage, and driver schedules. The next step involves optimising the layout of physical warehouse spaces and inventory locations to minimise transportation and retrieval times based on product volumes and pickup/delivery patterns. Quantum annealing can also be utilised in logistics scheduling to efficiently schedule pickups and deliveries across a logistics fleet, satisfying time windows and evaluating more scenarios [54]. Vendor selection can benefit from quantum annealing, as it helps identify the optimal set and locations of vendors/suppliers based on various factors such as demand forecasts, lead times, yields, costs, and risks [56].

Furthermore, quantum annealing can aid in determining the best financing and lending options, amounts, and terms across a supplier network, aiming to minimise costs while ensuring sufficient cash flows [54]. Lastly, working capital analysis can be enhanced by analysing cash flow dynamics and calculating optimal levels of inventory and receivables using quantum-simulated annealing, thereby minimising capital requirements [55]. By leveraging quantum annealing/optimisation techniques across these interconnected areas, businesses can significantly improve their supply chain efficiency, cost reduction, and data-driven decision-making processes.

11. Quantum Technologies for Central Bank Digital Currencies (CBDC)

In order to enable payments, there is a need to enhance and support financial transactions. In this section, we explore the potential of utilising quantum technologies to enhance and secure financial transactions, specifically focusing on the development of Central Bank Digital Currencies (CBDCs). In recent years, alongside decentralised approaches like Blockchain, the CBDC approach has emerged [57]. A CBDC refers to the electronic representation of a nation's official currency, issued by the country's central bank, serving as a digital counterpart to traditional fiat currency. The introduction of CBDCs by central banks aims to enhance financial inclusivity and streamline the implementation of monetary and fiscal policies. Furthermore, the concept of CBDC has played a significant role as one of the initial advancements in quantum money, as proposed by Stephan Wiesner [58].

As mentioned before, Quantum technologies have significant potential in implementing and securing CBDCs. To ensure long-term security in a post-quantum era, quantum-safe cryptography can be employed, utilising algorithms such as lattice-based or multivariate schemes [59], thereby safeguarding the digital currency and its underlying transactions. Quantum Key Distribution (QKD) offers an additional layer of security by facilitating the secure distribution and updating of encryption keys between the central bank, financial institutions, and digital wallets while detecting eavesdropping or key theft [60]. Quantum processes like beam-splitters can be leveraged for quantum number generation, enabling the generation of truly random numbers necessary for cryptographic keys, addresses, nonces, and digital signatures with provable unpredictability, surpassing classical random number generators [61]. Quantum tagging or marking techniques, such as quantum digital signatures or object-associated quantum memories, can be explored to address challenges related to identification, counterfeiting detection, and rights management for digitised assets [62]. Furthermore, quantum protocols can be investigated for certification and notarisation of critical events, states, and data transfers involved in CBDC implementation, enhancing provable integrity and transparency [63]. Lastly, quantum computers can be utilised to rigorously test the stability of algorithms underpinning CBDCs, such as consensus mechanisms, before large-scale real-world deployment, ensuring algorithmic stability [64].

Recommendations for Policymakers and Industry Players

Policymakers

a) **Support Quantum-Resistant Cryptography**: Encourage research in post-quantum cryptography, aiming to develop secure cryptographic algorithms against quantum computer attacks.
b) **Plan for Transition**: Start planning for a shift to quantum-resistant cryptographic standards, including setting timelines and guidelines for updating existing systems.
c) **Raise Public and Stakeholder Awareness**: Increase awareness about quantum computing and its potential impacts on digital security, including educating stakeholders about adopting quantum-resistant protocols.
d) **Establish Regulatory Frameworks**: Create regulations that mandate adopting quantum-resistant standards when available.
e) **Global Cooperation**: Collaborate with international bodies for a coordinated global approach to quantum computing and cryptography.

Industry Players

a) **Risk Assessment and Preparation**: Conduct risk evaluations to understand the potential impact of quantum computing on cryptographic systems and prepare for a transition to quantum-resistant algorithms.
b) **Stay Updated and Flexible**: Keep up with quantum computing and cryptography developments, and be ready to adapt quickly to new standards and technologies.
c) **Invest in Research**: Allocate resources to research in quantum-resistant technologies and collaborate with academic and government institutions.
d) **Use a Layered Security Approach**: Until quantum-resistant cryptography is fully implemented, employ a multi-layered security strategy for data protection.
e) **Collaborate and Knowledge Sharing**: Participate in industry groups focused on quantum computing and cryptography to share knowledge and best practices.

In essence, while the immediate threat of quantum computing to existing cryptographic systems is not critical, it represents a future challenge that necessitates proactive and cooperative efforts from policymakers and industry figures to ensure the ongoing security of digital systems.

9. Conclusions

The potential of quantum computing in the payment sector suggests a future rich with transformative changes. This advanced form of computing could significantly redefine how financial transactions are carried out, offering enhancements in security, speed, and efficiency. A notable aspect of quantum computing is its potential to bolster financial data security, providing encryption methods that could stand firm against current and anticipated cyber threats. This advancement is vital in an era increasingly dominated by digital transactions, underlining the need for robust security measures to protect financial systems. Moreover, the processing speed and efficiency offered by quantum computing could significantly improve transaction handling. Its ability to rapidly perform complex computations could address existing transaction delays, especially those that cross international borders, enhancing user convenience and the fluidity of global financial operations.

The application of quantum computing in fraud detection also presents considerable promise. Its capability for fast and thorough analysis of large data sets could enable accurate, real-time detection of fraudulent activities, providing a crucial layer of protection for both financial institutions and their clients. However, harnessing the full potential of quantum computing in the payment industry is challenging. It will require ongoing efforts in research and development, upgrades to existing infrastructures, workforce education, and regulatory framework adjustments. The complexity of quantum technology necessitates a comprehensive understanding and careful implementation to ensure compatibility with current financial systems.

Collaboration stands as a key factor in this process. The combined efforts of technology experts, industry leaders, and policymakers are essential to successfully integrating quantum computing into the payment sector. This cooperative approach is crucial in overcoming technical and structural challenges and ensuring that the deployment of quantum computing is secure, ethical, and conforms to international standards and regulations.

In summary, quantum computing presents an opportunity to usher in a new era in the payment industry, marked by enhanced security, improved efficiency, and innovative developments. Moving forward, continuous research, collaborative efforts, and a shared dedication to exploring this technology's capabilities are imperative. Keeping abreast of the latest advancements will be crucial for all stakeholders in this dynamic and promising field.

References

1. Bezovski, Z., 2016. The future of the mobile payment as electronic payment system. European Journal of Business and Management, 8(8), pp.127-132.
2. Hidary, J.D. and Hidary, J.D., 2019. Quantum computing: an applied approach (Vol. 1). Cham: Springer.
3. Johnson, W.G., 2019. Governance tools for the second quantum revolution. Jurimetrics, 59(4), pp.487-522.
4. Tredinnick, L., 2019. Cryptocurrencies and the Blockchain. Business Information Review, 36(1), pp.39-44.
5. Omarini, A.E., 2018. Fintech and the future of the payment landscape: the mobile wallet ecosystem. A challenge for retail banks?. International Journal of Financial Research, 9(4), pp.97-116.
6. Herbert, F., Becker, S., Buckmann, A., Kowalewski, M., Hielscher, J., Acar, Y., Dürmuth, M., Zou, Y. and Sasse, M.A., 2023, October. Digital Security—A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups. In 2024 IEEE Symposium on Security and Privacy (SP) (pp. 27-27). IEEE Computer Society.
7. Faccia, A., Moşteanu, N.R., Cavaliere, L.P.L. and Mataruna-Dos-Santos, L.J., 2020, September. Electronic money laundering, the dark side of fintech: An overview of the most recent cases. In Proceedings of the 2020 12th international conference on information management and engineering (pp. 29-34).
8. Chaudjary, S., Kakkar, R., Gupta, R., Tanwar, S., Agrawal, S. and Sharma, R., 2022. Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review. Turkish Journal of Electrical Engineering and Computer Sciences, 30(7), pp.2446-2488.
9. Athanassiou, P.L., 2016. Digital innovation in financial services: legal challenges and regulatory policy issues. Kluwer Law International BV.
10. Beebeejaun, Z. and Faccia, A., 2022. Electronic Alternative Dispute Resolution, smart contracts and equity in the energy sector. The Journal of World Energy Law & Business, 15(2), pp.97-113.
11. Jocevski, M., Ghezzi, A. and Arvidsson, N., 2020. Exploring the growth challenge of mobile payment platforms: A business model perspective. Electronic Commerce Research and Applications, 40, p.100908.
12. Au, Y.A. and Kauffman, R.J., 2008. The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application. Electronic commerce research and applications, 7(2), pp.141-164.
13. Adel, A., 2022. Future of industry 5.0 in society: Human-centric solutions, challenges and prospective research areas. Journal of Cloud Computing, 11(1), pp.1-15.
14. Eyeleko, A.H. and Feng, T., 2023. A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario. IEEE Internet of Things Journal.
15. HSBC, 2023. HSBC pioneers Quantum protection for AI-powered FX trading. [online] Available at: https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-pioneers-quantum-protection-for-ai-powered-fx-trading [Accessed December 30th 2023]
16. Adams, J., 2023. Mastercard testing quantum computing for loyalty and rewards. PaymentsSource | American Banker. [online] Available at: https://www.americanbanker.com/payments/news/mastercard-testing-quantum-computing-for-loyalty-and-rewards [Accessed December 30th 2023]

17. Muncaster, P., Year. UK banks' quantum may imperil entire. [online] Infosecurity Magazine. Available at: https://www.infosecurity-magazine.com/news/uk-banks-quantum-imperil-entire/ [Accessed December 30th 2023]
18. Purohit, A., Kaur, M., Seskir, Z.C., Posner, M.T. and Venegas- Gomez, A., 2023. Building a quantum- ready ecosystem. IET Quantum Communication.
19. Hasanovic, M., Panayiotou, C., Silberman, D., Stimers, P. and Merzbacher, C., 2022. Quantum technician skills and competencies for the emerging Quantum 2.0 industry. Optical Engineering, 61(8), pp.081803-081803.
20. Javadpour, A., Ja'fari, F., Taleb, T., Zhao, Y., Bin, Y. and Benzaïd, C., 2023. Encryption as a Service for IoT: Opportunities, Challenges and Solutions. IEEE Internet of Things Journal.
21. Mosteanu NR, Faccia A. Fintech Frontiers in Quantum Computing, Fractals, and Blockchain Distributed Ledger: Paradigm Shifts and Open Innovation. Journal of Open Innovation: Technology, Market, and Complexity. 2021; 7(1):19. https://doi.org/10.3390/joitmc7010019
22. Galindo, A. and Martin-Delgado, M.A., 2002. Information and computation: Classical and quantum aspects. Reviews of Modern Physics, 74(2), p.347.
23. Ciulei, A.T., Crețu, M.C. and Simion, E., 2022. Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective. Cryptology ePrint Archive.
24. Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C. and Voznak, M., 2020. Quantum key distribution: a networking perspective. ACM Computing Surveys (CSUR), 53(5), pp.1-41.
25. Riel, H., 2021, December. Quantum computing technology. In 2021 IEEE International Electron Devices Meeting (IEDM) (pp. 1-3). IEEE.
26. Grossi, M., Ibrahim, N., Radescu, V., Loredo, R., Voigt, K., Von Altrock, C. and Rudnik, A., 2022. Mixed quantum–classical method for fraud detection with quantum feature selection. IEEE Transactions on Quantum Engineering, 3, pp.1-12.
27. Cai, Z., Babbush, R., Benjamin, S. C., Endo, S., Huggins, W. J., Li, Y., ... & O'Brien, T. E. (2023). Quantum error mitigation. Reviews of Modern Physics, 95(4), 045005.
28. Scerri, E., Gauger, E. M., & Bonato, C. (2020). Extending qubit coherence by adaptive quantum environment learning. New Journal of Physics, 22(3), 035002.
29. Bharti, K., Cervera-Lierta, A., Kyaw, T. H., Haug, T., Alperin-Lea, S., Anand, A., ... & Aspuru-Guzik, A. (2022). Noisy intermediate-scale quantum algorithms. Reviews of Modern Physics, 94(1), 015004.
30. Hull, I., Sattath, O., Diamanti, E., & Wendin, G. (2020). Quantum technology for economists. arXiv preprint arXiv:2012.04473.
31. Ge, X., Wu, R. B., & Rabitz, H. (2022). The optimisation landscape of hybrid quantum–classical algorithms: From quantum control to NISQ applications. Annual Reviews in Control, 54, 314-323.
32. Liu, R., Rozenman, G.G., Kundu, N.K., Chandra, D. and De, D., 2022. Towards the industrialisation of quantum key distribution in communication networks: A short survey. IET Quantum Communication, 3(3), pp.151-163.
33. Grody, A.D., 2020. Addressing cyber risk in financial institutions and in the financial system. Journal of Risk Management in Financial Institutions, 13(2), pp.155-162.
34. Krishnakumar, A., 2020. Quantum Computing and Blockchain in Business: Exploring the applications, challenges, and collision of quantum computing and Blockchain. Packt Publishing Ltd.
35. Ukpabi, D., Karjaluoto, H., Bötticher, A., Nikiforova, A., Petrescu, D., Schindler, P., Valtenbergs, V. and Lehmann, L., 2023. Framework for understanding quantum computing use cases from a multidisciplinary perspective and future research directions. Futures, 154, p.103277.
36. Fernandez-Carames, T.M. and Fraga-Lamas, P., 2020. Towards post-quantum Blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 8, pp.21091-21116.
37. Herman, D., Googin, C., Liu, X., Galda, A., Safro, I., Sun, Y., Pistoia, M. and Alexeev, Y., 2022. A survey of quantum computing for finance. arXiv preprint arXiv:2201.02773.
38. Tyagi, A.K. and Tiwari, S., 2024. The Future of Artificial Intelligence in Blockchain Applications. In Machine Learning Algorithms Using Scikit and TensorFlow Environments (pp. 346-373). IGI Global.

39. QuEra Computing Inc. (2023) 'The Landscape of Quantum Computing Programming Languages', QuEra Computing Blog. Available at: https://www.quera.com/blog-posts/quantum-computing-programming-languages (Accessed: 3 April 2024])
40. Restu (2023) 'Integrating Python with Quantum Computing: A Practical Guide', Medium, 13 August. Available at: https://medium.com/@restudad/integrating-python-with-quantum-computing-a-practical-guide-dcd88bb01f81 (Accessed: 3 April 2024])
41. Gill, S.S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A. and Singh, M., 2022. AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, p.100514.
42. Forbes, 2023, Top 10 Quantum Computing Companies Making Change, available at: https://www.forbes.com/sites/technology/article/top-quantum-computing-companies/?sh=3a4758ad3a94 (accessed on 31.12.2023)
43. Dalton, A., Dorr, B., Liang, L. and Hollingshead, K., 2017, December. Improving cyber-attack predictions through information foraging. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 4642-4647). IEEE.
44. Ramos-Calderer, S., Pérez-Salinas, A., García-Martín, D., Bravo-Prieto, C., Cortada, J., Planaguma, J., & Latorre, J. I. (2021). Quantum unary approach to option pricing. *Physical Review A*, *103*(3), 032414.
45. Tang, H., Pal, A., Wang, T. Y., Qiao, L. F., Gao, J., & Jin, X. M. (2021). Quantum computation for pricing the collateralised debt obligations. *Quantum Engineering*, *3*(4), e84.
46. Martin, A., Candelas, B., Rodríguez-Rozas, Á., Martín-Guerrero, J. D., Chen, X., Lamata, L., ... & Sanz, M. (2021). Toward pricing financial derivatives with an ibm quantum computer. *Physical Review Research*, *3*(1), 013167.
47. Lee, R. S., & Lee, R. S. (2020). Quantum Trading and Hedging Strategy. *Quantum Finance: Intelligent Forecast and Trading Systems*, 119-158.
48. Gonzalez-Conde, J., Rodrĺguez-Rozas, A., Solano, E., & Sanz, M. (2021). Pricing financial derivatives with exponential quantum speedup. *methods*, *2*, 6.
49. Egger, D. J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., ... & Yndurain, E. (2020). Quantum computing for finance: State-of-the-art and future prospects. *IEEE Transactions on Quantum Engineering*, *1*, 1-24.
50. Lockwood, O., & Si, M. (2020, October). Reinforcement learning with quantum variational circuit. In *Proceedings of the AAAI conference on artificial intelligence and interactive digital entertainment* (Vol. 16, No. 1, pp. 245-251).
51. Orrell, D. (2020). A quantum model of supply and demand. *Physica A: statistical Mechanics and its Applications*, *539*, 122928.
52. Riandari, F., Alesha, A., & Sihotang, H. T. (2021). Quantum computing for production planning. *International Journal of Enterprise Modelling*, *15*(3), 163-175.
53. Schworm, P., Wu, X., Klar, M., Gayer, J., Glatt, M., & Aurich, J. C. (2023). Resilience optimisation in manufacturing systems using Quantum Annealing. *Manufacturing Letters*, *36*, 13-17.
54. Garcia Garcia, J., & Galan Jativa, P. (2023, July). Application of Quantum Annealing to Supply Chain Planning under Uncertainty. In *Proceedings of the Companion Conference on Genetic and Evolutionary Computation* (pp. 2216-2223).
55. Ossorio-Castillo, J., & Pena-Brage, F. (2022). Optimisation of a refinery scheduling process with column generation and a quantum annealer. *Optimisation and Engineering*, *23*(3), 1471-1488.

The following reference, was cited in the previous subsection, as well:

56. Orrell, D. (2020). A quantum model of supply and demand. *Physica A: statistical Mechanics and its Applications*, *539*, 122928.
57. Chaum, D., Grothoff, C., & Moser, T. (2021). How to issue a central bank digital currency. *arXiv preprint arXiv:2103.00254*.
58. Wiesner, S. (1983). Conjugate coding. *ACM Sigact News*, *15*(1), 78-88.
59. Ravi, P., Howe, J., Chattopadhyay, A., & Bhasin, S. (2021). Lattice-based key-sharing schemes: A survey. *ACM Computing Surveys (CSUR)*, *54*(1), 1-39.

60. Wolf, R. (2021). *Quantum key distribution*. Berlin/Heidelberg, Germany: Springer International Publishing.
61. Suda, M., Dißauer, G., & Prawits, F. (2019, October). True Random Number Generation with Beam Splitters under Combined Input Scenarios using Defined Quantum States to Increase the Security of Cryptographic Devices. In *ICQNM 2019: The 13th International Conference on Quantum, Nano/Bio, and Micro Technologies* (pp. 11-16).
62. Puthoor, I. V., Amiri, R., Wallden, P., Curty, M., & Andersson, E. (2016). Measurement-device-independent quantum digital signatures. *Physical Review A*, *94*(2), 022328.
63. Allende, M., León, D. L., Cerón, S., Pareja, A., Pacheco, E., Leal, A., ... & Venegas-Andraca, S. E. (2023). Quantum-resistance in blockchain networks. *Scientific Reports*, *13*(1), 5664.
64. Kan, K., & Une, M. (2021). Recent trends on research and development of quantum computers and standardisation of post-quantum cryptography.