REVIEW

Open Access

From portfolio optimization to quantum blockchain and security: a systematic review of quantum computing in finance

Abha Satyavan Naik[1], Esra Yeniaras[2], Gerhard Hellstern[3*], Grishma Prasad[4] and Sanjay Kumar Lalta Prasad Vishwakarma[5]

*Correspondence: gerhard.hellstern@dhbw-stuttgart.de

[1] VVM's Shree Damodar College of Commerce and Economics, Goa, India
[2] KEA - Copenhagen School of Design and Technology, Copenhagen, Denmark
[3] Center of Finance, Baden Württemberg Cooperative State University (DHBW), Herdweg 29, D-70174 Stuttgart, Germany
[4] Bloq Quantum, Kollam, India
[5] IBM Quantum, Almaden Lab, California, USA

Abstract

The rapid advancement of quantum computing has sparked a considerable increase in research attention to quantum technologies. These advances span fundamental theoretical inquiries into quantum information and the exploration of diverse applications arising from this evolving quantum computing paradigm. The scope of the related research is notably diverse. This paper consolidates and presents quantum computing research related to the financial sector. The finance applications considered in this study include portfolio optimization, fraud detection, and Monte Carlo methods for derivative pricing and risk calculation. In addition, we provide a comprehensive analysis of quantum computing's applications and effects on blockchain technologies, particularly in relation to cryptocurrencies, which are central to financial technology research. As discussed in this study, quantum computing applications in finance are based on fundamental quantum physics principles and key quantum algorithms. This review aims to bridge the research gap between quantum computing and finance. We adopt a two-fold methodology, involving an analysis of *quantum algorithms*, followed by a discussion of *their applications* in specific financial contexts. Our study is based on an extensive review of online academic databases, search tools, online journal repositories, and whitepapers from 1952 to 2023, including CiteSeerX, DBLP, ResearchGate, Semantic Scholar, and scientific conference publications. We present state-of-the-art findings at the intersection of finance and quantum technology and highlight open research questions that will be valuable for industry practitioners and academicians as they shape future research agendas.

Keywords: Portfolio optimization, Fraud detection, Derivative pricing, Risk calculation, Monte carlo, Quantum blockchain, Quantum-resistant blockchain, Digital signature algorithms, Post-quantum cryptography, Security, Privacy-preserving blockchain, Quantum computing

© The Author(s) 2025. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Introduction and related work

In recent years, quantum computing has attracted considerable attention from researchers in physics, computer science, and various other fields of application (Preskill 2018a; Ukpabi et al. 2023; Hassija et al. 2020). Finance is one area where quantum computing is expected to have benefits or risks (Orús et al. 2019). This is because financial research and development involve several challenging, computationally intensive problems, many of which have substantial potential to benefit from the opportunities provided by quantum computing (Orús et al. 2019). This study addresses the following research questions:

> *What are the potential applications of quantum computing in finance? What are the recent advances? How do these advancements influence the financial sector? What are the risks, limitations, and benefits of applying quantum computing to real-world financial problems? Finally, what are the future research directions identified based on the current state-of-the-art?*

To address these questions, we studied several reviews and research papers examining the potential quantum computing effects on finance. One of the earliest reviews addressing the relationship between quantum computing and finance is authored by a group of IBM engineers (Egger et al. 2020). This review covers topics such as Monte Carlo simulation, optimization, and machine learning, with a focus on how IBM's quantum hardware and software have been applied. However, a more comprehensive analysis is required, as the review does not address hardware and software considerations in depth. Although we do not address hardware or software analysis in the current review, it should be noted that not all reviews comprehensively address all related concepts within the field.

Another review (Bouland et al. 2020) covers topics such as Monte Carlo simulation, portfolio optimization, and machine learning, aiming to address financial professionals who may lack a background in quantum computing. To address this knowledge gap, we provide a comprehensive introduction to quantum computing in conjunction with financial topics, focusing on both the finance and quantum computing communities.

In Orús et al. (2019), similar topics are presented from a physicist's perspective, and they may not offer the in-depth insights required for financial researchers. Another review (Herman et al. 2022) focuses on foundational quantum algorithms and explores quantum finance research in terms of stochastic modeling, optimization, and machine learning. We examine recent studies from that review and summarize the contributions of the quantum community from 2021 to 2023, with an emphasis on practical applications.

In the field of portfolio optimization, several reviews (Orús et al. 2019; Albareti et al. 2022; Herman et al. 2022), and (Gunjan and Bhattacharyya 2022) have explored various aspects related to our study. However, these surveys include algorithmic implementation details that extend beyond the scope of this review. The 2022 survey by Herman et al. (2022) categorizes portfolio optimization problems into two types: convex and combinatorial formulations. In contrast, Orús et al. (2019) in 2019 focused on applying quantum computing to optimization problems, with an emphasis on portfolio optimization. Albareti et al. (2022), in their 2022 study, reviewed the literature on portfolio optimization and introduced a structured framework to systematically evaluate proposals for integrating quantum computing into finance.

The survey by Herman et al. (2022) explored the use of quantum support vector machine (QSVM) and quantum k-nearest neighbor (QKNN) as quantum counterparts to the classical algorithms—support vector machine (SVM) and k-nearest neighbor (KNN)—used in machine learning for classification and regression tasks. The QSVM and QKNN algorithms leverage quantum feature embedding maps to encode data in quantum circuits. The inner product between the states obtained after embedding individual data points using these feature maps serves as the primary distance metric. Once the data is encoded and the quantum kernel (for QSVM) or inner products (for distance calculation) is derived, the classification or regression process follows standard classical optimization methods. The key quantum advantage of these algorithms lies in the flexibility of the feature maps, which allows them to be tailored to specific datasets and use cases. Herman et al. (2022) also mentioned the use of quantum generative adversarial networks (QGANs) for unsupervised anomaly detection, particularly in fraud detection. In this study, we expand on these discussions by including studies that use QSVM for feature selection and classification in supervised settings, as well as employing QSVM as an analog to a one-class SVM for unsupervised anomaly detection. In addition, we present a pioneering quantum fraud detection approach that involves data and parameter encoding using a single qubit, followed by classical optimization.

To the best of our knowledge, previous studies have not fully addressed blockchain and cryptocurrencies, or the contributions and risks posed by quantum computers to the fintech and crypto-asset domains. Therefore, we conduct an extensive analysis of quantum computing applications in blockchain. Notably, the ongoing research gaps in quantum-resistant cryptography, secure key management in quantum environments, and robust financial systems capable of withstanding quantum attacks must be highlighted. Further research is required to develop methods for integrating quantum technologies into existing financial infrastructure while maintaining compatibility and performance. The key research gaps in quantum blockchain for finance include the development of quantum-resistant consensus mechanisms for financial transactions, scalability for large-scale financial operations, security vulnerabilities between quantum and classical financial systems, and the impact of quantum blockchain on financial market infrastructure and regulatory compliance. In addition, designing quantum-enhanced financial instruments and trading platforms that leverage quantum computing capabilities is an area that requires further exploration. The potential influence of quantum efficiency gains on *Bitcoin mining* is another critical concept that warrants attention from both security and finance professionals. In this context, studies such as Alagic et al. (2020), Ciulei et al. (2022), Fernández-Caramès and Fraga-Lamas (2020), Torres et al. (2020), and, Punathumkandi and Boscovic (2022) provide the foundation for this study, along with other proposals on quantum-resistant blockchains, including privacy-focused designs. In addition, we delve into *quantum blockchain* and *quantum mining*, offering insights into the challenges and advantages of their real-world implementation. The influence of quantum technology on cryptocurrencies and blockchain is a critical subject that requires thorough analysis to fully understand quantum computing's role in the financial sector.

Previous studies on blockchain and crypto-assets Fernández-Caramès and Fraga-Lamas (2020), Baum et al. (2023), Torres et al. (2020) have typically focused on isolated aspects of the field. Some studies have focused solely on analyzing quantum-resistant digital signature algorithms, addressing factors such as space complexity, time complexity, and security implications Alagic et al. (2020). Other studies have focused exclusively on privacy-preserving blockchain systems (Baum et al. 2023), without considering quantum computing-related perspectives. Some surveys have also narrowed their scope to quantum computing applications and quantum mining (Punathumkandi and Boscovic 2022; Benkoczi et al. 2022), neglecting critical security and privacy challenges arising in the quantum era.

In this review, one of our primary goals is to integrate diverse survey domains, incorporating both blockchain and quantum technologies, post-quantum applications, and cryptographic security vulnerabilities. We aim to provide a comprehensive exploration of the current and potential future effects and applications of quantum computing in the fintech and crypto-asset investment landscape. In addition, we present a concise analysis of the economic relevance of cryptocurrencies, such as Bitcoin, which is often considered the digital equivalent of gold.

Furthermore, this study compiles and presents an updated catalog of real-world quantum-resistant cryptocurrencies—a task not previously undertaken. We assess the threats posed by quantum algorithms, particularly Grover's and Shor's algorithms, which could undermine existing cryptographic primitives. These quantum algorithms pose substantial security risks to cryptocurrencies lacking quantum-resistant digital signature algorithms. To address these risks, we begin by examining the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) standardization process and the competition surrounding quantum-resistant digital signature algorithms, highlighting the strengths and limitations of various approaches. In addition, we summarize the challenges involved in developing a fully quantum-secure system and propose potential solutions.

It is crucial to explore how various factors—scalability, security, and compatibility in quantum blockchain, along with the technological limits of quantum computing—could impede the successful integration of quantum technologies into financial systems. Addressing these problems is critical for fully exploiting the transformative potential of quantum technologies in finance. Another primary objective of this study is to consolidate the aforementioned concepts and offer a comprehensive perspective on quantum finance. Our aim is to present an up-to-date analysis of developments in the quantum finance domain by integrating the distributed discussions from previous studies into a single, extensive study. In doing so, we provide these insights and background information to benefit quantum and finance researchers. Our examination covers various financial topics and their applications in quantum computing: portfolio optimization, fraud detection, Monte Carlo methods for derivative pricing and risk calculation, and blockchain-based cryptocurrencies.

We conducted an exhaustive full-text search across diverse research datasets, followed by a thorough review and detailed analysis of papers that made notable contributions to advancing knowledge or demonstrated practical relevance to real-world applications.

The remainder of this paper is organized as follows. In Fundamentals of Quantum Computing section, we provide a concise overview of the fundamental principles of quantum computing, including key concepts from quantum physics, such as superposition, entanglement, and quantum gates. We also introduce relevant quantum algorithms, including variational quantum algorithms (VQAs), quantum phase estimation (QPE), quantum Fourier transform (QFT), Grover's algorithm, and Shor's algorithm.

In Portfolio Optimization section, we focus on recent portfolio optimization developments from the quantum computing perspective. Section Fraud Detection and Credit Scoring presents an in-depth discussion of fraud detection and credit scoring, and Section Monte Carlo Methods in Finance examines derivative pricing and the application of Monte Carlo methods with a quantum computing insight and analysis.

In Blockchain in Quantum Finance section, we comprehensively explore quantum blockchain, quantum-resistant blockchain, and security vulnerabilities posed by quantum attacks on cryptographic primitives in the digital signature algorithms used in cryptocurrencies. Finally, Section Conclusion and Future Work concludes the paper and provides insights into future research directions and challenges.

Methodology

This comprehensive review investigates the multifaceted effects of quantum computing on financial technology, exploring its potential benefits and associated risks. Our methodology is two-fold, focusing on algorithms and their practical applications. Central to our review are quantum algorithms, which form the foundation for practical implementations in real-world financial scenarios.

In this review, we analyze the implications and applications of quantum algorithms in key financial areas, namely, portfolio optimization, fraud detection, credit scoring, Monte Carlo methods, and blockchain. We gathered relevant literature using diverse online academic databases and search tools, such as Google Scholar, Semantic Scholar, journal repositories, CiteSeerX, DBLP, ResearchGate, scientific conference proceedings, and whitepapers from cryptocurrency-related websites. Our review covers publications from 1952 to 2023, thoroughly analyzing 225 research papers.

In each section of this review, we present tables that highlight the most salient and relevant studies on the subject matter. These studies were carefully chosen to provide a comprehensive overview of key milestones in the evolution of the subject matter, from its origins to its latest developments. We prioritized cutting-edge studies with strong academic influence and practical relevance to the financial industry. In view of this, we thoroughly reviewed the reference sections of relevant articles to bridge the gap between algorithm design and real-world applications. As a general strategy, we excluded studies that merely repeated previously covered concepts unless they introduced new insights. Nevertheless, we have included all studies that have made notable contributions to both academia and the practical application of these concepts. For instance, in Section Monte Carlo Methods in Finance, which discusses Monte Carlo methods in finance, we provide a brief overview of the classical Monte Carlo method and its use in different financial areas. We then highlight a seminal study of Rebentrost et al. (2018), which proposed a quantum algorithm that achieves quadratic speedup. Following this is the discussion on subsequent studies that improve this approach and extend its application to other problems in finance. Previous studies have focused on derivative pricing; quantum Monte Carlo methods are now used for risk calculations.

In Section Blockchain in Quantum Finance which addresses blockchain applications in quantum finance, we first present rudimentary blockchain propositions and algorithms and trace their evolution through successive enhancements. This progression culminates in the most evolved iterations, such as Bitcoin. In addition, we discuss quantum and post-quantum digital signature algorithms, which are crucial for applications in cryptocurrencies and digital money. For each algorithm, we present a representative study along with its associated references and relevant whitepapers on various cryptocurrencies. Our selection prioritized the most influential studies on each topic, avoiding redundant studies unless recurring concepts offered novel perspectives. We also focused on fundamental milestone studies that demonstrated real-life applications. For example, we have included a study on the post-quantum NTRU Prime algorithm, which has practical relevance in Google's Combined Elliptic-Curve and Post-Quantum 2 (CECPQ2) experiment. CECPQ2, a quantum-secure modification to TLS 1.3 developed by Google (although not explicitly financial) plays a critical role in selecting quantum-resistant algorithms for cryptocurrencies, safeguarding them against potential quantum attacks aimed at cryptocurrency theft. This meticulous inclusion and exclusion criterion was applied consistently throughout the review.

Fundamentals of quantum computing

Quantum computing is an emerging and rapidly developing field. Considerable research and funding from the government, public, and private sector have been directed toward this area because of its potential to solve NP-hard problems with high accuracy (Preskill 2012). However, with current technology, quantum computers can only accommodate up to approximately 100 qubits, which are prone to errors and are thus referred to as called *noisy* (Baheri et al. 2022). Researchers are actively working on designing fault-tolerant quantum computers and developing error mitigation techniques to improve accuracy, with the goal of demonstrating a quantum advantage (Preskill 2018a).

Quantum mechanics

Quantum mechanics is a branch of physics that explores the behavior of matter and energy at the atomic and subatomic scales.Unlike classical mechanics, quantum mechanics is based on probabilistic theory, implying that it predicts the likelihood of a particle being in a certain state rather than its exact position or velocity. The two most important quantum mechanics phenomena are superposition and entanglement (Barletta 2023).

Superposition

Superposition enables particles to exist in multiple states simultaneously. Specifically, the wavefunction of a quantum system can be expressed as a linear combination of wavefunctions corresponding to its individual states.

Consider two states, $|0\rangle$ and $|1\rangle$, which can be combined in a superposition as follows:

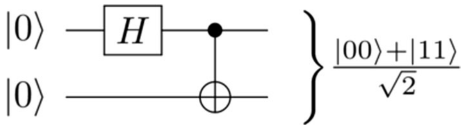

Fig. 1 Quantum circuit of the Bell state

$$\begin{aligned}|\psi\rangle =&\alpha|0\rangle + \beta|1\rangle,\\ |0\rangle =& \begin{bmatrix}1\\0\end{bmatrix},\\ |1\rangle =& \begin{bmatrix}0\\1\end{bmatrix}.\end{aligned}$$

Here, α and β are complex coefficients that represent the amplitudes of the states. The probability of measuring the system in the state $|0\rangle$ is α, and the probability of measuring it in the state $|1\rangle$ is β. The coefficients α and β are constrained by the normalization condition, ensuring that the total probability is 1. Superposition is a fundamental principle of quantum mechanics, with important applications in quantum computing and quantum cryptography.

Entanglement

Entanglement refers to the phenomenon where two or more quantum systems become intertwined in such a way that the state of one system cannot be described independently of the others. Even if these systems are separated by large distances, measuring one system can instantaneously influence the state of the others. This phenomenon is key to quantum communication and quantum cryptography.

The simplest entangled state involves two qubits and is called the Bell state. The corresponding quantum circuit for generating a Bell state is shown in Fig. 1.

Quantum computing

Quantum computing is a new paradigm in which quantum bits or qubits, the fundamental unit of information, can simultaneously represent multiple states, unlike classical bits. In classical computing, a bit—the fundamental unit of information in classical computing—can exist in only one of two states: 0 or 1. In contrast, a qubit-can exist in a superposition of both 0 and 1, as well as other quantum states, providing a distinct advantage over classical bits (Prashant 2007).

This unique property of qubits allows quantum computers to perform certain types of computations much faster than classical computers. For example, quantum computers excel at factoring large numbers—a key challenge in cryptography. Quantum computers can also simulate complex physical systems, solve optimization problems, and handle tasks that require processing large volumes of data. The characteristics of qubits can vary depending on the hardware used.

Similar to the manipulation of bits by classical gates, quantum gates manipulate and control qubit behaviors. A combination of quantum gates acting on qubits forms a quantum circuit. Quantum gates are primarily divided into two categories: single- and multiple-qubit gates.

Single-Qubit Quantum Gates

Single-qubit quantum gates operate on individual qubits to manipulate their quantum states. The single-qubit X-gate, also called the "NOT" gate, is a commonly used quantum gate in quantum computing. This gate corresponds to a rotation of the qubit state vector by π radians about the Bloch sphere's x-axis. The Bloch sphere is a three-dimensional representation of a qubit's quantum state, where the north and south poles represent the quantum states $|0\rangle$ and $|1\rangle$, respectively. The sphere's equator represents the superpositions of these two states, which can be expressed as a linear combination of $|0\rangle$ and $|1\rangle$.

In classical computing, the NOT gate flips the value of a bit from 0 to 1 or from 1 to 0. Similarly, the X-gate transforms a qubit in the $|0\rangle$ state to $|1\rangle$, and a qubit in $|1\rangle$ to $|0\rangle$. This behavior makes the X-gate the quantum analog of the classical NOT gate.

The matrix representation of the X-gate is as follows:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

The Hadamard gate, also known as the H-gate, is another single-qubit quantum gate. This gate is commonly used to create superposition states by performing a combination of qubit state vector rotations: a 90° rotation around the x-axis followed by a 180° rotation around the z-axis of the Bloch sphere. When applied to state $|0\rangle$, H-gate creates the superposed state $\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$, and when applied to state $|1\rangle$, H-gate yields the superimposed state represented as $\frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$.

The matrix representation of the H-gate is as follows:

$$\frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

.

Multiple-qubit quantum gates

Multiple-qubit quantum gates operate on two or more qubits simultaneously and are essential for performing complex quantum operations and implementing quantum algorithms. The most commonly used multiple-qubit quantum gates are the controlled-NOT (CNOT) and SWAP gates. The H-gate and CNOT gates can create entangled pairs of qubits when used together. Most quantum algorithms in circuit-based approaches rely on a set of fundamental two-qubit gates, such as Toffoli, CNOT, and SWAP gates.

Quantum algorithms

Quantum algorithms are specifically designed to use quantum mechanics phenomena—superposition and entanglement—to perform computations more efficiently than classical algorithms (Zhang and Li 2022). These algorithms exploit the unique

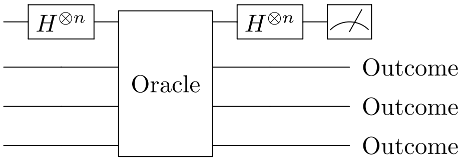

Fig. 2 Grover's algorithm simple circuit design with oracle

characteristics of quantum systems to overcome the challenges associated with classical computing. One of the most well-known quantum algorithms is Shor's algorithm, which can factor large numbers—a capability that has notable implications for cryptography. For example, Shor's algorithm can break the RSA encryption, which is a widely used method for securing online communications. Another important quantum algorithm is Grover's algorithm, which searches for unsorted databases and can provide quadratic speedup for various optimization problems. Quantum algorithms also hold promise for machine learning and artificial intelligence, enabling the analysis of large datasets and complex computations. In addition, quantum algorithms are expected to make remarkable contributions to fields such as pharmaceutical research, materials science, and financial modeling. For example, quantum algorithms can accelerate the discovery of new drugs and materials by modeling molecular behavior (Santagati et al. 2023). In finance, they can be employed for risk assessment and portfolio optimization (Herman et al. 2022). This section explores key quantum algorithms and their applications in quantum finance.

Grover's and Shor's Algorithms

Grover's algorithm, developed in 1996 by Lov Grover, is a quantum algorithm designed to find a specific item in an unstructured dataset or search an unsorted database. It is regarded as one of the most important quantum algorithms. Grover's algorithm employs the amplitude amplification phenomenon and offers a quadratic speedup, requiring fewer operations to search a database of N unsorted items, compared with O(N) operations needed by classical algorithms. The algorithm begins by creating a superposition of all possible solutions, represented as quantum states. It then iteratively modifies this superposition using two key components: a quantum oracle(U_f) and a quantum diffusion operator(U_ψ). Grover's oracle acts as a black box (Fig. 2), marking the desired item by flipping the phase of its corresponding state. Grover's diffusion operator amplifies the amplitude of the marked state, thereby increasing its probability of detection during measurement. By repeating this process multiple times, the algorithm enhances the likelihood of observing the correct solution, thereby narrowing down the search space (Grover 1996).

Grover's algorithm holds enormous importance in the context of quantum-resistant blockchain and cryptography because it highlights the potential vulnerabilities of classical cryptographic techniques in the quantum computing era. Its potential to undermine traditional encryption systems motivates the development and adoption of quantum-resistant algorithms to maintain the security and integrity of blockchain systems and

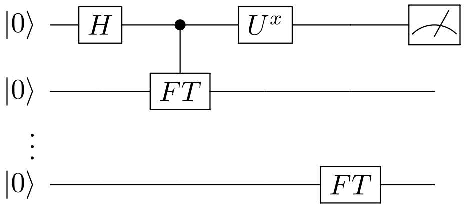

Fig. 3 Shor's algorithm simple circuit design with Fourier transform (FT)

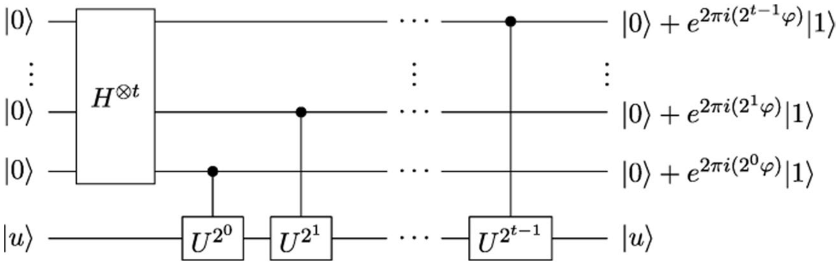
$|0\rangle$
$|0\rangle$
$|0\rangle$
$|u\rangle$
$H^{\otimes t}$
U^{2^0}
U^{2^1}
$U^{2^{t-1}}$
$|0\rangle + e^{2\pi i(2^{t-1}\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^1\varphi)}|1\rangle$
$|0\rangle + e^{2\pi i(2^0\varphi)}|1\rangle$
$|u\rangle$

Fig. 4 Quantum circuit for the quantum phase estimation

cryptographic communications. For a detailed explanation of the steps involved in Grover's algorithm, please refer to Section Blockchain in Quantum Finance.

Portfolio optimization in traditional finance is a computationally intensive process that involves evaluating numerous potential portfolios. Quantum computing, using Grover's algorithm, can substantially expediate this search. Another promining application of Grover's algorithm in finance is credit scoring. The algorithm can analyze credit datasets to identify trends and locate high-risk clients, helping lenders make better decisions while minimizing default risks.

QFT, a prerequisite of Shor's algorithm, is a quantum algorithm that performs a Fourier transform on quantum states. It serves a crucial subroutine in many quantum algorithms, including Shor's algorithm for factoring large numbers and QPE (Fig. 3). The use of Shor's algorithm arises from the QFT's ability to determine a function's periodicity (Kashani et al. 2022).

QPE is another quantum procedure that is used to estimate the eigenvalues of a unitary operator. Specifically, QPE determines values for which the equation $U|u\rangle = \lambda|u\rangle$ holds, where U is an operator, $|u\rangle$ is an eigenvector, and λ represents the eigenvalues.

Figure 4 displays the quantum circuit for QPE.

Estimating eigenvalues is a critical step in many quantum algorithms, with Shor's algorithm for factoring large numbers being a prominent example. In QPE, the quantum state $|\psi\rangle$ serves as an eigenvector of a unitary operator U associated with an unknown eigenvalue. QPE employs a sequence of controlled-U gates, where each gate is controlled by a qubit in a superposition of states. As the process repeats, more qubits are added to the superposition, enabling progressively precise estimation of the eigenvalue.

The QFT subroutine plays a pivotal role in the recursive QPE method. By applying a Fourier transform to the superposition of states, the QFT extracts the phase information of the eigenvalue (Svore et al. 2013). Then, QPE measures the qubits in the superposition and finalizes the eigenvalue estimation. The versatility of QPE extends to quantum finance applications. For example, one of the most promising areas is pricing financial derivatives (Section Monte Carlo Methods in Finance), which is computationally demanding and requires eigenvalue predictions of large matrices. Another important application is portfolio optimization (Section Portfolio Optimization), where QPE can enhance efficiency.

Shor's algorithm (3) is a quantum algorithm capable of efficiently factoring large composite numbers (Shor 1997). Its importance lies in its profound implications for computer security and cryptography. The security of many contemporary encryption methods hinges on the computational difficulty associated with factoring large numbers, which can take years using classical computing methods. Shor's algorithm, however, can accomplish this task exponentially faster on a quantum computer, posing a considerable threat to modern encryption schemes.

In addition, Shor's algorithm is critically important in the fields of cryptography and quantum-resistant blockchain (cryptocurrency) technology. This algorithm underscores the vulnerabilities of classical cryptographic techniques, especially those relying on factorization and discrete logarithm problems (DLPs), in quantum computing. This has spurred the development of quantum-resistant cryptographic algorithms and blockchain systems to safeguard digital communications and transactions against quantum-based attacks. For a detailed breakdown of Shor's algorithm's steps, refer to Section Blockchain in Quantum Finance.

VQAs

While the quantum algorithms discussed in the previous section generally require numerous fault-tolerant qubits, VQAs are designed to run on near-term quantum computers that are limited by a small number of qubits and high error rates. VQAs are a type of quantum algorithms that use classical optimization to search for solutions to complex problems. The basic goal of VQAs is to minimize the quantum resource usage by using quantum hardware as a co-processor for classical optimization procedures. The fundamental idea behind VQAs is to start with a quantum circuit that is parameterized by a set of variables, known as the "ansatz." The ansatz circuit is a quantum circuit with a fixed structure but configurable parameters. These variables are selected to maximize the quantum circuit's output while minimizing a specific cost function, typically a classical cost function (Cerezo et al. 2021).

The optimization is performed by running the ansatz circuit on a quantum computer, measuring the result, and updating the parameters. This procedure is repeated until the cost function is minimized or the desired precision is attained (Cerezo et al. 2021). Numerous problems, including optimization tasks, machine learning challenges, and quantum chemistry simulations, have been successfully solved using VQAs.

The quantum approximate optimization algorithm (QAOA) is a quantum optimization algorithm with high potential in the field of quantum finance (Canabarro et al. 2022). Using a series of parameterized quantum gates, the QAOA solves an optimization problem as closely as possible. Portfolio optimization is one of the most promising applications of quantum computing in the field of finance. This involves dividing capital investments among the members of a group of assets to maximize returns while reducing risk.

The portfolio optimization problem can be solved using QAOA by determining the optimal weight set for a given collection of assets. A quantum circuit encodes the weights of the assets, and the QAOA measures the resulting cost function. The optimal weights for a given set of assets are then determined by optimizing the cost function using conventional optimization techniques (Zhou et al. 2020). Other financial optimization problems, such as credit risk evaluation and option pricing, can be solved using QAOA in addition to portfolio optimization. However, these applications are still in the early stages of development and require further study.

In conclusion, QAOA can be a highly effective tool in quantum finance for solving challenging optimization problems that are beyond the capabilities of classical computers. The applications of QAOA and other quantum optimization algorithms in finance are expected to increase as quantum technology advances.

Portfolio optimization

In this section, we introduce the application of quantum methods to solve optimization problems in finance. We provide an overview of various approaches and their limitations.

Constant improvement in portfolio management techniques is essential for enhancing returns while maintaining an acceptable level of risk. Portfolio management and optimization have long been challenging problems that have attracted considerable interest from both the technical and financial domains. When these problems are formulated based on the Markowitz model, they become a quadratic programming task, which is generally an NP-hard problem. As the problem size increases, solving these NP-hard problems becomes exponentially time-consuming. In such cases, quantum computing offers great potential to overcome these challenges.

Specifically, noisy intermediate-scale quantum (NISQ) devices have considerable commercial potential to solve such optimization problems Herman et al. (2022).

A portfolio is a collection of financial assets from the same or different asset classes, designed to achieve a specific objective. Financial assets include gold, stocks, bonds, and others. The goal of a portfolio can range from earning aggressive or moderate returns to minimizing risk or balancing both risk and returns. An efficient portfolio achieves maximum returns for a given level of risk. Portfolio optimization is a critical aspect of the portfolio selection and management process, allowing a portfolio manager to make the best selection among available portfolios under dynamic market conditions, such as fluctuating market prices, changing interest rates, and shifting political or legal environments.

A previous study (Markowitz 1952) proposed an investment model that greatly influenced and encouraged further investigation into portfolio optimization. The Markowitz portfolio model provides the capital market line, which represents the risk–return tradeoff in the capital market and is formulated as follows:

$$r_p = i_{rf} + \frac{(r_m - i_{rf})\sigma_p}{\sigma_m}$$

where,

r_p = expected portfolio return,

i_{rf} = risk-free rate of interest,

r_m = market portfolio return,

σ_p = standard deviation of portfolio,

σ_m = standard deviation of market.

This model aims to reduce risk by diversifying the portfolio and accounting for the risk–return tradeoff, thereby providing investors with an efficient portfolio based on their risk appetite.

Previous surveys

Portfolio optimization techniques (Gunjan and Bhattacharyya 2022) have evolved from methods such as mean variance (Durand 1960), variance with skewness (Samuelson 1975), value-at-risk (VaR) (Jorion 1996; Wipplinger 2007), conditional value-at-risk (CVaR) (Rockafellar and Uryasev 2000), mean absolute deviation (Konno and Yamazaki 1991), and minimax (Park et al. 1998) to more advanced heuristic and metaheuristic methods. Evolutionary algorithms and swarm intelligence have become popular approaches for portfolio optimization. In addition to the aforementioned classical methods, the financial industry is also exploring several quantum and quantum-inspired algorithms for portfolio optimization. However, as an optimization problem, portfolio optimization suffers from the "curse of dimensionality" (Kuo and Sloan 2005; Bellman 1956), where the dimensionality of the data increases rapidly, causing the data volume to increase as well. This causes the data to become increasingly scattered and more difficult to cluster. Quantum computing holds promise for addressing this problem due to its ability to handle larger computations faster than classical computing. Each asset class in a portfolio optimization problem is assigned a weight, and assets are selected based on factors such as risk, return, average maturity, and liquidity. A previous study (Herman et al. 2022) categorized portfolio optimization problems into two categories: convex and combinatorial formulations. Combinatorial formulations rely on integer optimization, specifically, binary optimization problems. Integer optimization involves mathematical optimization in which some or all variables are restricted to integers. Binary optimization is a subset of integer optimization that uses only 0 s and 1 s as variables. Financial optimization problems can often be transformed into quadratic unconstrained binary optimization (QUBO) problem (Wikipedia contributors 2023b), which can then be mapped to an Ising Hamiltonian. Solving the ground state of the Ising Hamiltonian is equivalent to finding the optimal solution to the QUBO problem, representing the optimal portfolio. Researchers have employed QUBO formulations to integrate budget constraints and correlation considerations, determining asset inclusion based on risk, as well as the decision to take long or short positions. Binary-variable-constrained mean variance portfolio optimization also influences the desired return level. These formulations facilitate dynamic decision-making over multiple time steps. Quantum algorithms addressing these problems are particularly suited for the noisy intermediate-scale quantum (NISQ) era, with quantum annealing(Kadowaki and Nishimori 1998) being a common choice because of its capability to handle larger numbers of qubits than gate-based

Table 1 Categorization of the studies based on the quantum computation models

Quantum computing models	Related work surveyed
Quantum annealing-based	Elsokkary et al. (2017), Venturelli and Kondratyev (2019), Mattesi et al. (2023), Cohen et al. (2020a), Cohen et al. (2020b), Cohen and Alexander (2020), Lang et al. (2022), Palmer et al. (2022)
Quantum aiabatic-based	Hegade et al. (2022)
Gate-based	Barkoutsos et al. (2020), Wang (2022), Liu et al. (2022), Herman et al. (2023), Veselý (2022), Yalovetzky et al. (2023), Lim and Rebentrost (2023)

models. In contrast, convex formulations use quantum algorithms designed for convex optimization (Wikipedia contributors 2023a). The mean variance portfolio optimization problem can be reformulated as a convex optimization problem. The solution to these problems informs users of the proportion of the amount to be invested in the asset rather than whether to include the asset in the portfolio.

Recent developments

Two major computational models used by researchers for portfolio optimization are quantum annealing (e.g., D-wave systems) and gate-based models (e.g., IBM devices) (Orús et al. 2019) (Table 1). Quantum annealing is suitable for specific problems, such as optimization tasks, while gate-based models are applicable to a wider range of problems. Quantum annealing systems have achieved more stable qubits than gate-based systems, although these qubits exhibit low connectivity (Herman et al. 2022).

In a previous study (Elsokkary et al. 2017), the Markowitz portfolio optimization problem for stocks from the Abu Dhabi Securities Exchange was formulated as a QUBO problem and solved using the D-wave simulator for its quantum optimizer, QBSOLV. The authors utilized the Chimera architecture of the D-wave system.

In another study (Venturelli and Kondratyev 2019), the authors explored a quantum–classical hybrid approach to the Markowitz portfolio optimization problem using the D-Wave 2000Q quantum annealer. They found that the best time-to-solution return, as a function of the number of variables, was obtained by seeding the quantum annealer with a solution candidate found by a greedy local search (classical component) and subsequently applying a reverse quantum annealing protocol (quantum component). The time-to-solution is defined as the expected number of independent runs required for the method to find the ground state with a given probability (confidence level). The application involved a fund of funds manager selecting a suitable fund from a universe of funds using a particular trading strategy. This approach outperformed the classical solution, the genetic algorithm, for problem sizes in the range of 42–60 assets in terms of time-to-solution. On average, the optimized reverse annealing protocol was 100 times faster than the corresponding forward quantum annealing. The authors also suggested that transitioning from the Chimera to the Pegasus architecture can greatly improve performance. Enhancing the embedding process is essential for improving the performance of D-wave devices. An improvement in the QUBO formulations of a previous study (Venturelli and Kondratyev 2019) was proposed in Mattesi et al. (2023), allowing investors to determine the optimal amount of investment in each asset rather than focusing only on the selection of optimal assets. This was achieved by discretizing the problem variables and employing continuous portfolio weights.

In other studies (Cohen et al. 2020a) and (Cohen et al. 2020b), the authors performed portfolio optimization for 40 and 60 US stocks, respectively, using the D-Wave 2000 quantum annealer with a buy-and-hold strategy. The results were compared with those of classical algorithms. According to the authors, their results indicated that quantum advantage becomes more pronounced as the number of assets under consideration increases. They developed the Chicago quantum ratio (CQR) and Chicago quantum net score (CQNS) as improvements over the Sharpe ratio, as the D-wave quantum annealer can only handle linear quadratic equations and not ratios.

The CQR is defined as

$$CQR_a(w) = \frac{w \cdot Cov_{im}}{\sigma_a},$$

where Cov_{im} represents the covariance of the i^{th} asset over the entire market, w is a vector of weights for assets in the portfolio, and σ_a is the standard deviation of the collection of assets.

In addition, the CQNS is defined as

$$CQNS(w; \alpha) = Var(R_w) - \mathbb{E}[R_w]^{2+\alpha},$$

where R_w is a weighted portfolio return, and $\alpha \in \mathbb{R}$ was selected to maintain equal weighting, namely, $w_i = 1/n$, where n represents the number of assets included. Here, α was kept close to 1.

For a portfolio of 40 assets, the D-Wave 2000 quantum annealer performed well. It achieved better results in terms of CQNS than Monte Carlo methods, selecting stocks with better returns for the specified amount of risk. However, it performed worse than genetic algorithms. In the case of 60 assets, the D-wave quantum annealer was also able to identify the optimal portfolio including classical methods, as simulated annealing. This research was extended in another study (Cohen and Alexander 2020), which performed portfolio optimization on 3,171 US equity stocks. The approach was to first select several promising portfolios from the entire universe of portfolios using classical solvers such as Monte Carlo, followed by quantum annealing to identify the best portfolio. The study employed the D-wave advantage quantum annealer.

Another study using the D-wave advantage quantum annealer (Lang et al. 2022) proposed using a classical preprocessing step with a modified QUBO model. This preprocessing step included backtesting a trading strategy and computing the Sharpe ratio and variance of the returns. Then, the top 18 asset combinations based on the Sharpe ratio were selected for the QUBO formulation for portfolio optimization. The implementation of this method using quantum annealing demonstrated potential but was outperformed by simulated and digital annealing in terms of the Sharpe ratio.

QAOA (Farhi et al. 2014) and the variational quantum eigensolver (VQE) (Peruzzo et al. 2014) are promising algorithms for solving combinatorial optimization problems on NISQ-era devices. In particular, QAOA is well suited for gate-model quantum devices. In a previous study (Barkoutsos et al. 2020), the authors proposed using CVaR to improve the optimization results.

The main objective of QAOA and VQE is to identify the optimal solution for the problem by determining the global minimum (or a point sufficiently close to it) of the energy landscape describing the problem. The energy of the system is represented by the expected value of the Hamiltonian, given by $\langle \psi(\theta)|H|\psi(\theta)\rangle$. This is referred to as the objective function. Both QAOA and VQE aim to solve the following equation:

$$min_{\theta}\langle \psi(\theta) H \psi(\theta)\rangle,$$

whose solution is the global minimum.

A reasonable approximation for the above quantity can be achieved using a sample mean. The Hamiltonian for combinatorial optimization problems is generally framed such that it is diagonalizable, thereby ensuring the existence of a basis state that is the ground state. The eigenvalues lie along the diagonal of the diagonalized Hamiltonian, and the minimum eigenvalue corresponds to the ground state. However, it is difficult to diagonalize a Hamiltonian of large dimensions; therefore, an alternative method is to perform finite measurements and select the minimum eigenvalue corresponding to those measurements. The minimum of finite values is not a smooth objective function; thus, a CVaR-based approach is employed. A measurement system using CVaR as the objective function is particularly suitable in this case. CVaR, as the objective function, is the expected value of the lower α tail of the distribution of X, where X represents all eigenvalues corresponding to the measured states. The use of $min_{\theta}\mathrm{CVaR}_{\alpha}(X(\theta))$ (instead of X(θ)) as the objective function both smoothens the objective function and improves the best-measured outcome. This approach facilitates faster convergence to the solution compared to using the sample mean, providing faster results.

In a previous study (Mugel et al. 2021), the authors developed a classical-quantum dynamic portfolio optimization algorithm with a minimal holding period constraint to leverage tax benefits, enforced through post-selection. The study utilized a 50-asset portfolio as a use case. Using brute-force methods to successively check whether a given investment trajectory satisfies the minimum holding period constraint is computationally prohibitive due to the exponential growth in the number of investment trajectories. With post-selection, the investment trajectories are efficiently eliminated in a tree-like pattern if they fail to meet the constraints. Following this approach, the problem was formulated as a QUBO problem and solved using the D-Wave 2000 quantum annealer. Post-selection proved to be faster than the brute-force classical search approach, which faced challenges due to the exponential increase in the required number of qubits as the number of assets increased.

In addition to QAOA and quantum annealing, another approach is the adiabatic quantum optimization algorithm. To enable implementation on a gate-model quantum computer, a digitized version of adiabatic quantum computing was introduced in Barends et al. (2016). In another study (Hegade et al. 2022), digitized counterdiabatic quantum computing and the digitized counterdiabatic quantum approximate optimization algorithm (DC-QAOA) were studied. When solving a portfolio optimization problem using the adiabatic theorem, the optimal portfolio is represented by the ground state of the problem Hamiltonian. The aim is to increase the probability of successfully identifying this ground state while accounting for limited coherence time and device noise. This is achieved using approximate counterdiabatic driving (CD) terms (Sels and Polkovnikov 2017).

In adiabatic systems, the solution is obtained by allowing the initial Hamiltonian to evolve into a Hamiltonian whose ground state overlaps with the ground state of the problem Hamiltonian. The system must be allowed enough time to evolve into the desired Hamiltonian. However, in current devices, this is difficult due to the limited coherence time and device noise. Forcing an adiabatic system to evolve quickly results in nonadiabatic transitions between eigenstates, which negatively impacts the results. Thus, a solution was proposed in Torrontegui et al. (2013), Guéry-Odelin et al. (2019), in which the CD term was introduced to compensate for the excitations, causing the resulting evolution to be quasi-adiabatic. In DC-QAOA, CD is utilized to introduce an additional unitary operator $U_D(\alpha)$, known as the CD term. This study demonstrated instances where DC-QAOA outperformed QAOA in terms of the success probability of identifying the ground state.

QAOA requires modifying the cost function to enforce constraints using a penalty term. However, this approach is less effective as it involves searching for the best solution in a very large solution space. In a previous study (Wang 2022), the authors used a hybrid algorithm that employed classical methods to identify an approximate solution (called the seed) followed by a continuous-time quantum walk algorithm (Marsh and Wang 2019, 2020). This approach reduced the search area to a smaller subspace. The empirical evaluation of both constrained and unconstrained problems indicated that the proposed algorithm outperformed classical alternatives.

Financial index tracking is an important problem in which a small subset of assets is required to describe the behaviour of a large number of assets. Cardinality constraints help to limit the number of assets in the portfolio; however, they also introduce nonconvexity into the optimization problem. In a previous study (Palmer et al. 2022), the authors employed discretized portfolio optimization to directly implement cardinality constraints in a single optimization procedure. Discretized portfolio optimization is challenging to implement with classical devices but can be efficiently implemented with quantum computers. This approach successfully generated smaller portfolios that closely tracked the returns of the NASDAQ 100 and Standard & Poor's 500 indices. The study also explored enhanced index tracking and constructed tracking portfolios that maintained a high degree of correlation with the target indices.

In another study (Rubio-García et al. 2022), the authors used the integer version of the simulated annealing method to identify the optimal portfolio when discretized convex and nonconvex cost functions were considered. The study included a multiperiod portfolio optimization problem, where nonconvexity was introduced due to fixed transactional costs. In a multi-period portfolio optimization problem, assets are traded at each rebalancing step, incurring transactional costs. The results indicated that ignoring fixed transactional costs when formulating the cost function led to poorer performance than when these costs were incorporated into the discrete simulated annealing algorithm (Rubio-García et al. 2022).

Investors may occasionally be required to make decisions without complete information or with information that is revealed incrementally. These problems are part of a subfamily of optimization problems called online optimization problems. In a previous study (Lim and Rebentrost 2023), the authors developed a quantum sampling version of an existing classical online portfolio optimization problem Helmbold et al. (1998). Their approach achieved a quadratic speedup relative to the number of assets in the portfolio and had a transaction cost independent of the number of assets.

The effectiveness of quantum computers in solving portfolio optimization problems using QAOA-based mean-variance portfolio optimization was benchmarked in another study (Baker et al. 2022). The study compared the performance of quantum simulators (dense state vector simulation and stochastic shot-based simulation) and real devices provided by IBM (superconducting qubits), Rigetti (superconducting qubits), and IonQ (trapped-ion qubits). Solution quality was determined using the normalized and complementary Wasserstein distance, η, which allows QAOA to be viewed as a transporter of probability. The authors emphasized the need for application-specific benchmarking instead of general benchmarking to evaluate application performance.

Benchmarking various versions of QAOA in terms of their suitability to current hardware is essential for determining which version is most appropriate for a developer's needs. In a previous study (Brandhofer et al. 2022), the authors addressed this problem, presenting a detailed analysis of the performance of different versions of QAOA. They also studied the influence of statistical sampling errors as well as gate and readout errors. The performance of QAOA in identifying the optimal solution was found to vary for different instances based on the composition of assets in the portfolio. The authors defined a criterion for distinguishing between "easy" and "hard" instances of the portfolio optimization problem, suggesting that instances involving stocks with broadly distributed correlations and returns are easier to optimize than those with more similar correlations. This can be attributed to the fact that the high variance of the correlation and returns causes the variance of the objective function values to increase. This increase in the variance of the objective function leads to a more distinctive energy landscape in which portfolios are easily distinguishable from each other. The study focused on optimizing a portfolio of assets from the German stock index DAX.

In another study (Liu et al. 2022), the authors introduced a variation of VQE called Layer-VQE for combinatorial optimization problems. The principle behind Layer-VQE is to begin with one layer of parameterized rotations and then increase the size of the ansatz by adding entangling gates and other parameterized rotations. A new layer is added before convergence is reached, which helps to avoid the problem of local minima. This iterative layering is a critical requirement for achieving the optimal solution, which, in portfolio optimization, is the optimal portfolio. L-VQE was numerically demonstrated to greatly outperform QAOA in terms of gate count. The gate count of QAOA increased quadratically, while that of LVQE increased linearly. L-VQE also outperformed VQE in terms of handling finite sampling errors and the approximation ratio (a ratio used to assess the quality of the result, where a higher value indicates better performance). This ratio increased with each layer of the L-VQE ansatz, whereas it decreased with each layer of the VQE ansatz. In addition, the many-body terms in the Hamiltonian also made the implementation of QAOA more difficult.

In Certo et al. (2022), the authors included constraints that accounted for the fundamentals of the companies, and handled the allocation of assets in each industry. It is necessary to ensure that optimization problems correctly handle constraints, including arbitrary constraints, to ensure compliance with evolving market dynamics and regulations and provide an optimal solution. In Herman et al. (2023), the authors addressed the problem of portfolio optimization with the following constraints:

Case 1: an inequality constraint on the total size of the portfolio:

$$\sum_j x_j \leq C$$

Case 2: In addition to the portfolio size constraint above, the authors included a constraint on the total expected return:

$$\sum_j \mu_j x_j \geq R$$

Constraints in the portfolio optimization problem can be achieved by either introducing a penalty term or restricting the evolution of the solution system to an in-constraint subspace. In QAOA, the mixing operator ensures that the evolution occurs in the constraint-following subspace. However, designing an efficient mixing operator is difficult, with additional requirements for efficient Trotterization, a process that breaks down the evolution into smaller components (Fuchs et al. 2022). In Herman et al. (2023), the authors enforced constraints in the evolution using quantum Zeno dynamics through repeated projective measurements, which restricted the evolution of the system to an in-constraint "subspace by adding repeated projective measurements to the mixing operator in QAOA. This approach allows both equality and inequality constraints to be enforced, which is achieved by constructing a quantum oracle. For QAOA, the scaling rule derived by the authors indicates that the number of measurements increases linearly with the number of layers in QAOA and quadratically with the number of qubits.

A performance comparison between QAOA with Zeno dynamics and QAOA using a penalty component demonstrated that the former consistently achieved higher approximation ratios than the latter. Furthermore, the penalty approach required independent tuning of the penalty factor. When Zeno dynamics was employed in L-VQE, the researchers achieved high approximation ratios and a high in-constraint probability. In addition, multiple constraints could be employed in L-VQE but not in QAOA due to prohibitively expensive tuning. For both QAOA and L-VQE, the in-constraint probability could be increased by using more measurements.

In Veselý (2022), the authors discussed the application of quantum computers in forex management, focusing on risk management and portfolio construction. For risk management, they used an algorithm based on quantum Monte Carlo methods Woerner and Egger (2019), while for portfolio construction, they used QUBO with

QAOA and the Harrow-Hassidim-Lloyd (HHL) approach using IBM quantum processors. A small-scale portfolio optimization problem with five assets was used in their study. For portfolio construction using QUBO with QAOA, the simulators performed comparably to classical devices, selecting the most efficient portfolios. The quantum devices also returned the correct solutions, but they exhibited differences in performance with respect to the number of iterations. The number of iterations is greatly influenced by the quantum volume (Wikipedia contributors 2023c). However, in portfolio optimization using HHL, the quantum devices failed due to decoherence and the inability of current devices to handle negative eigenvalues in matrices. The risk management algorithm failed to calculate risk parameters, likely due to the difficulty in differentiating between the low percentiles, which stemmed from the extremely small difference between the angles of the rotational gates.

HHL algorithms face challenges such as those mentioned above due to the limitations of current NISQ devices. The authors of Yalovetzky et al. (2023) thus proposed a NISQ-HHL algorithm that was used to solve small-scale mean-variance portfolio optimization problems involving 6 and 14 assets. Their study enhanced the methods in Lee et al. (2019) by replacing standard QPE with quantum conditional logic (QCL)-enhanced QPE for eigenvalue estimation. This enhancement helped to reduce the ancillary qubit count, the SWAP gate count, and the need for qubit connectivity. The authors also used additional features such as mid-circuit measurement and qubit reset and reuse. The trapped-ion Quantinuum system model H1 was employed because it supported QCL, mid-circuit measurements, and qubit reset and reuse. In their study, QCL-enhanced QPE achieved higher fidelity than standard QPE.

In Campos et al. (2022), the authors developed an open source software solution that employed the quantum Metropolis-Hastings algorithm (Szegedy 2004) to solve optimization problems. This algorithm achieves a speedup over its classical counterpart by employing quantum walks to reduce the gap between eigenvalues, leading to shorter mixing times and faster convergence to the minimum energy state. The authors tested the software on the N-queens problem, an NP-complete search problem used as a benchmark for artificial intelligence algorithms. They found that as the problem size increased, the quantum Metropolis-Hastings algorithm outperformed the classical Metropolis-Hastings algorithm in terms of time-to-solution (i.e., the ability to reach the solution in the least amount of time).

In addition to quantum strategies, there is another category of strategies that employs quantum-inspired algorithms. For example, researchers employed the global-best guided quantum-inspired tabu search with a self-adaptive strategy and quantum NOT gate (ANGQTS) for portfolio optimization as it demonstrated better searchability than the traditional approach in Chou et al. (2022) on US stocks in the Dow Jones 30 index. This also enabled flexible fund allocation in a high-dimensional solution space. The global-best guided quantum-inspired tabu search with a quantum NOT gate (GNQTS) is a variant of quantum-inspired tabu search that aims to achieve the global-best solution by utilizing the quantum NOT gate. The strategy of using the quantum NOT gate makes it possible to avoid the problem of local minima. The addition of a self-adaptive mechanism allows the algorithm to handle more complex solution spaces, transforming it into ANGQTS. Statistical testing demonstrated that

Table 2 Classification of the gate-based model studies based on the algorithms they use

Algorithms	Related work surveyed
QAOA	Barkoutsos et al. (2020), Wang (2022), Herman et al. (2023), Veselý (2022); Benchmarking QAOA:Baker et al. (2022), Brandhofer et al. (2022)
VQE	Barkoutsos et al. (2020), Liu et al. (2022)
HHL	Veselý (2022), Yalovetzky et al. (2023)

Table 3 Studies that discuss the implementation constraints

Works on constraint implementations
Mugel et al. (2021), Palmer et al. (2022), Rubio-García et al. (2022), Certo et al. (2022), Herman et al. (2023)

ANGQTS achieved considerable improvement over GNQTS in weighted allocation portfolio optimization. A similar strategy was applied to Singapore stocks in Lai et al. (2022).

The content discussed in this section is categorized according to the quantum computation models utilized by the respective systems. This categorization is crucial because two different systems may achieve the same task through distinct physical methodologies, despite maintaining identical core mechanisms. Thus, special attention must be paid to the quantum computation model employed. Table 1 provides a categorization of the reviewed literature based on the quantum computation models. Among gate-based models, different algorithms operate at distinct efficiencies and computational costs. It is necessary to understand the advantages and limitations of each algorithm and select the algorithm that best suits the requirements of a given situation. The literature on gate-based models reviewed in this paper is categorized by the algorithms employed, as presented in Table 2. Furthermore, constraints are critical for stimulating real-world scenarios using portfolio optimization. Studies that highlight the implementation of constraints are presented in Table 3. A summary of the discussion in this section is provided by the key references in Table 4.

Fraud detection and credit scoring

In this section, we explore two primary applications of quantum machine learning in finance: fraud detection and credit scoring. Parallel discussions on these topics are currently unavailable in the literature, highlighting the transformative potential of quantum algorithms in these domains.

Fraud detection is essential for banks to maintain customer trust and safeguard financial assets. Traditional fraud detection methods primarily rely on rule-based systems and statistical analyses; however, such methods often struggle to identify sophisticated and evolving fraud schemes.

Quantum computing offers promising capabilities in this area by enabling the processing of vast datasets and uncovering complex patterns that may remain hidden with classical approaches. For example, quantum computing allows the analysis of diverse data sources, including transaction records, social media, and public information, to identify anomalies indicative of fraudulent activity.

Table 4 Summary of the discussions in 3.2

Work surveyed	Contribution
Elsokkary et al. (2017)	Formulated a portfolio optimization problem for stocks from the Abu Dhabi Securities Exchange as a QUBO problem and solved it using the D-Wave simulator
Venturelli and Kondratyev (2019)	Proposed a quantum-classical hybrid solution to the Markowitz portfolio optimization problem using the D-Wave quantum annealer, where the quantum annealer was seeded with a solution candidate found by a greedy local search (classical component), followed by a reverse quantum annealing protocol (quantum component)
Cohen et al. (2020a)	Optimized a portfolio of 40 US stocks using the D-Wave quantum annealer, introducing the Chicago quantum ratio (CQR) and Chicago quantum net score (CQNS) as an improvement over the Sharpe ratio with respect to ease of handling for the annealer.
Cohen et al. (2020b)	Extended the research in Cohen et al. (2020a) and optimized a portfolio of 60 US stocks using the D-Wave quantum annealer.
Cohen and Alexander (2020)	Extended the research in Cohen et al. (2020a) and Cohen et al. (2020b), performing portfolio optimization for 3,171 US equity stocks.
Barkoutsos et al. (2020)	Proposed a method to improve the measurement system results using conditional value-at-risk (CVaR).
Chou et al. (2022)	Introduced a quantum-inspired algorithm for portfolio optimization: the global-best guided quantum-inspired tabu search with a self-adaptive strategy and quantum NOT gate (ANGQTS).
Yalovetzky et al. (2023)	Proposed the NISQ-HHL algorithm, which was used to solve small-scale mean-variance portfolio optimization problems.
Liu et al. (2022)	Introduced Layer-VQE, a variation of VQE, for combinatorial optimization problems.
Baker et al. (2022)	Benchmarked the success of quantum computers to solve Portfolio optimization problems using QAOA-based mean-variance portfolio optimization(QAOA-MVPO)
Wang (2022)	Employed a hybrid algorithm that used classical methods to find an approximate solution (called a seed) and a continuous-time quantum walk algorithm.
Certo et al. (2022)	Included constraints that portray the fundamentals of the companies
Veselý (2022)	Discussed the application of quantum computers in forex management by comparing the performance of QAOA and HHL for the same
Campos et al. (2022)	Developed an open source software-solution that used the quantum Metropolis-Hastings algorithm for solving optimization problems.
Lim and Rebentrost (2023)	Developed a quantum sampling version of an existing classical online portfolio optimization problem
Palmer et al. (2022)	Tackled the problem of Financial Index Tracking by using discretized portfolio optimization to directly implement cardinality constraints in a single optimization procedure
Herman et al. (2023)	Ensured that the portfolio optimization problem correctly handled arbitrary constraints using quantum Zeno dynamics though repeated projective measurements.
Mugel et al. (2021)	Developed a classical–quantum dynamic portfolio optimization algorithm with a minimal holding period constraint to leverage tax benefits, enforced through post-selection.
Rubio-García et al. (2022)	Investigated optimal portfolio selection for discretized convex and nonconvex cost functions (introduced through a fixed transactional cost) using the integer version of the simulated annealing method.
Lang et al. (2022)	Employed the D-Wave annealer and proposed using a classical preprocessing step with a modified QUBO model for solving portfolio optimization problems.
Brandhofer et al. (2022)	Benchmarked various versions of QAOA in terms of suitability for current hardware.
Hegade et al. (2022)	Studied digitized counterdiabatic quantum computing and digitized counterdiabatic QAOA (DC-QAOA) for portfolio optimization.
Mattesi et al. (2023)	Improved the QUBO formulations in Venturelli and Kondratyev (2019), allowing investors to determine the optimal fund allocation for each asset.

In addition, quantum computing may bolster banks' cybersecurity efforts by introducing advanced encryption techniques to secure sensitive data. Such improvements could mitigate data breach and cyberattack risks, thereby safeguarding both customers and institutions from financial losses. While quantum applications for fraud detection remain in their infancy, ongoing research is focused on developing the required algorithms and infrastructure for practical deployment. The potential benefits of quantum computing in this field highlights its future importance as a critical tool in the banking industry.

Quantum fraud detection involves processing vast transaction and account data to identify irregularities and potential fraudulent activities using quantum machine learning approaches. Beyond the core purpose, these approaches also contribute to portfolio optimization. For instance, patterns or anomalies in transaction data may reflect broader market trends or shifts in investor sentiment, which can inform strategic investment decisions. Fraud detection systems can pinpoint unusual patterns or high-risk transactions, and these insights can be applied to portfolio optimization by adjusting investment strategies or reallocating assets to minimize exposure to high-risk positions. Quantum computing's exceptional processing speed enables real-time fraud detection and rapid decision-making. This capability can also be harnessed in portfolio optimization, allowing for quick adjustments in response to market dynamics or fraud-related insights that could influence the portfolio.

In addition, quantum fraud detection and quantum blockchain technologies complement each other to enhance the security, transparency, and integrity of financial transactions. Together, they contribute to a robust, fraud-resistant financial ecosystem that benefits both users and organizations, fostering trust and operational resilience.

The study by Grossi et al. (2022) presents the first end-to-end application of a quantum support vector machine (QSVM) algorithm in the financial payment industry. By using IBM Safer Payments and IBM Quantum Computers with Qiskit software, the study employed real-world card payment data to evaluate the performance of state-of-the-art quantum machine learning algorithms compared with the classical approach. The authors also proposed a new method to identify optimal features based on the feature map characteristics of a QSVM. Key performance indicators (KPIs), such as accuracy, recall, and false positive rate were analyzed across three models: classical machine learning algorithms (random forest and XGBoost), quantum-based machine learning algorithms using QSVM, and human expertise (decision-rule-based model). In addition, the authors explored a hybrid classical–quantum approach to improve fraud prevention decisions by combining classical and quantum algorithms.

Three approaches were compared on the same dataset:

1. Domain-expert-created rule-based model (no machine learning)
2. State-of-the-art artificial intelligence/machine learning using boosted trees (random forest, XGBoost)
3. QSVM model

The authors used dataset comprising 2.4 million payment transactions, of which 3,000 transactions were labeled fraudulent. Among the 12 features derived from transactional

Table 5 Comparison between the KPIs obtained with XGB, RF, and QSVM

KPI	XGB (XGBoost)	RF (random forest)	QSVM
Accuracy (Test)	0.76 ± 0.01	0.76 ± 0.01	0.78 ± 0.01
AUC(Test)	0.81 ± 0.01	0.81 ± 0.01	0.81 ± 0.01

data, two originated from demographic data, and the remaining features were generated using discovery techniques. Due to the highly imbalanced nature of the data, the authors implemented undersampling techniques to address this challenge effectively.

Among various quantum approaches, Grossi et al. (2022) focused on QSVM, aimed at using QSVM to optimize fraud detection system in two areas. First was to identify notable features to reduce dataset dimensionality, ensuring the experiment is computationally feasible on a quantum system. Second was to extract fraud-related KPIs from the QSVM model. A quantum approach necessitates restricting the database to few important features, reducing the number of qubits and data points for processing. Therefore, using undersampling techniques to scale down the dataset is essential. All data values were normalized using MinMaxScaler, which is better suited for quantum processing requirements.

The data utilized by the authors comprised real payment transactions from a European cross-border processing portfolio, consisting of approximately 80% debit and 20% credit card transactions. Principal component analysis (PCA) was not employed because it is most effective for data consisting of continuous features, whereas fraud detection data often contain categorical features. The authors experimented with factorial analysis of mixed data (FAMD), which is effective for both categorical and continuous features, unlike PCA. However, the authors rejected this approach because they found that the FAMD components had significant overlap, limiting the amount of information that could be captured after dimensionality reduction. The quantum approach involves the following steps:

1. Initially, three features are selected from the entire list of features.
2. QSVM is applied with the three features selected in Step 1.
3. KPIs such as accuracy, precision, and recall from the results of Step 2 are compared with the KPIs of classical approaches, such as random forest and XGBoost.
4. If Step 3 indicates that QSVM exhibits superior performance, additional features are added, and Steps 2 and 3 are repeated to verify whether the performance continues to improve. The same process is performed if Step 3 indicates that QSVM performs worse than other approaches.
5. The conclusion is based on the KPI values in one of two scenarios: (i) when all features are taken into account and the best results are achieved with all features, indicating that the approach does not offer dimensionality reduction or that all features are essential in building the fraud detection system; or (ii) or when adding new features does not further improve the performance.

The authors employed the Qiskit framework, which included the QuantumKernel class and ZZFeatureMap, in their implementation. ZZFeatureMap was utilized to map each data point to a quantum state, and the resulting inner products of these states were utilized to generate the kernel matrix. This methodology was inspired by the feed-forward feature selection approach, which is based on statistical metrics such as AUC (area under curve) and accuracy. Using this approach, the authors iteratively selected an increasing number of features for the problem, beginning with only 3 out of 69 features.

In the study, the authors employed random undersampling of the majority class data (non-fraud) before running QSVM, random forest, and XGBoost. Due to this random approach, they performed five trials to minimize bias. With random forest and XGBoost, the accuracy was 0.76 with a deviation of 0.01 across the five trials. With QSVM, the accuracy was 0.78 with a deviation of 0.01 across the five trials. Thus, the accuracy of QSVM was 2% higher than that of random forest and XGBoost. Another KPI was AUC, which yielded a value of 0.81 with a deviation of 0.01 across the five trials for all three approaches. The results are presented in Table 5.

To improve classification performance, the authors employed a mixed quantum-classical approach, combining the strengths of quantum and classical algorithms. To achieve this, they identified transactions or data points where quantum and classical algorithms provided different classifications. They then trained a metaclassifier on these conflicting data points to predict the correct classification. They trained both the quantum and classical algorithms on the training dataset and identified transactions for which the two algorithms disagreed. These transactions formed a smaller dataset, which was used to train a metaclassifier that could employ any feature from the original dataset. Due to the limited number of discrepant data points, a simple metaclassifier was most effective.

To summarize, the authors demonstrated that quantum classifiers can detect patterns that classical algorithms find challenging, and a mixed quantum-classical ensemble can improve the final model. The results were obtained on a simulated quantum computer, with future efforts directed toward implementation on real hardware. The authors also demonstrated that data preprocessing is a crucial step before proceeding to the quantum stage.

Fraudulent transactions can be considered anomalous events, as non-fraudulent or genuine transactions are typically more dominant. A previous study Kyriienko and Magnusson (2022) focused on a quantum approach to detect fraud using anomaly detection. Anomaly detection is an unsupervised approach, as it does not require predefined labels for categorizing transactions as fraudulent or non-fraudulent. The approach involved using the instantaneous quantum polynomial (IQP) as a feature map, which mapped the original data into a high-dimensional space. In addition, a quantum kernel approach (i.e. QSVM) was used. While SVM or QSVM are generally considered supervised learning approaches, the approach described in the paper is a quantum analogue of the classical one-class SVM, which is a popular classical approach for anomaly detection. The principle is that the inner products of the resulting quantum states used in the kernel matrix can effectively display greater distances between data points in different classes than between data points in the same class. For feature enhancement or feature engineering prior to embedding the data with IQP, the authors employed various scaling strategies for all features. However, this did not lead to performance improvement.

To define and simulate the quantum circuits, the authors employed the Pennylane library with the JAX interface, which enabled compiling the circuits using the Accelerated Linear Algebra (XLA) compiler. XLA utilizes just-in-time compilation techniques to speed up extensive machine learning workloads, resulting in fast, parallelized operation across CPU and GPU resources. Additionally, the authors implemented batched Gram matrix evaluation, with kernel evaluations streamlined over different values.

For a small number of features, the authors observed an increase in average precision, reaching 0.9 for 5 to 10 features. The performance of the classical kernel model deteriorated as the feature count exceeded 10. In contrast, the performance of the quantum kernel model did not deteriorate, achieving new peaks around 17 features/qubits. At $N =$ 20, the authors observed a clear performance difference between quantum and classical kernels, suggesting that quantum kernels avoid overfitting. This indicates an increased expressivity and learning advantage for specific tasks performed on classical datasets.

In Tapia et al. (2022), the authors presented a novel classification technique, with a focus on fraud detection as a real-world application, utilizing a single qubit. This approach is particularly advantageous in the current NISQ era, where quantum hardware with a large number of qubits is not yet widely available, and systems with a larger number of qubits are susceptible to noise and errors. This approach is motivated by the concept of data reloading proposed in Pérez-Salinas et al. (2020), which enables the encoding of mathematical functions into the degrees of freedom of a series of gates applied to a single-qubit state. This technique is inspired by the concept of classical neural networks, where computations are performed by neurons organized in interconnected layers. In this quantum analogy, unitary rotations correspond to neurons, forming processing units that can be replicated to create layers. Each subsequent neuron re-uploads the classical input data and is able to capture a particular feature of the distribution. Additionally, in Pérez-Salinas et al. (2021), the authors demonstrated that a quantum neural network based on a single-qubit circuit can approximate any bounded complex function by storing its information in the degrees of freedom of a series of quantum gates.

In single-qubit quantum neural network classification, the feature map and ansatz are both parametrized as arbitrary single-qubit rotations. Each combination of the data-encoding single-qubit rotation and parameterized rotation is analogous to a layer in the classical neural network architecture:

$$U(\vec{\phi},\vec{x}) \equiv U(\vec{\phi_N})U(\vec{x})...U(\vec{o_1})U(\vec{x}).$$

For a simple case in which the classical data have three dimensions, $\vec{x}$ represents a sample data point expressed as a vector. Therefore, $U(\vec{x})$ corresponds to a unitary gate, where each angle corresponds to a single dimension of the data point, as $U(\phi_1,\phi_2,\phi_3) \in SU(2)$, $\vec{\phi_N}$ represents the N-th set of three parameters used as rotation angles in $U(\vec{\phi_N})$. Alternating unitary operators are thus applied for the given data point (data encoding with re-uploading Pérez-Salinas et al. (2020)) and for the set of three parameters. For N such layers, there can be $3N$ parameters and a circuit depth of $2N$

The higher the number of layers in a circuit, the greater its representational ability. However, a high number of layers in a circuit leads to an increased runtime, which may negatively affect the quality of the results due to the limited coherence times in current quantum processing units. Therefore, in Pérez-Salinas et al. (2020), the authors proposed a unitary operator of the form

$$L(i) = U(\vec{\theta}_i + \vec{\omega}_i \odot \vec{x}).$$

Here, each layer combines the parameters and dimensions of the data points into a single unitary operator. For a simple case of three-dimensional data, $\vec{x}$ represents a given sample data point expressed as a vector, $\vec{\theta}_i$ represents the i-th set of three parameters, and $\vec{\omega}_i$ represents a vector of weights assigned to each dimension of the data. Both $\vec{\theta}_i$ and $\vec{\omega}_i$ are trainable parameters. Here, $\vec{\omega}_i \odot \vec{x}$ denotes the Hadamard product of $\vec{\omega}_i$ and $\vec{x}$). It should be noted that if the data have less than three dimensions, the remaining dimensions of $\vec{x}$ are set to 0. If the data have more than three dimensions, the circuit can be expressed as follows, where the dimensions of a given data point are split into k sets of three values. A layer can then be expressed as

$$L(i) = U(\vec{\theta}_i^{(k)} + \vec{\omega}_i^{(k)} \odot \vec{x}^{(k)})...U(\vec{\theta}_i^{(1)} + \vec{\omega}_i^{(1)} \odot \vec{x}^{(1)}),$$

where $\vec{x}^{(k)}$ represents the k-th set of three dimensions from $\vec{x}$, and $\vec{\theta}_i^{(k)}$ and $\vec{\omega}_i^{(k)}$ denote the k-th set of trainable parameters and weights each consisting of three elements. Thus, for N layers, the depth is $k \times N$, and the total number of trainable parameters is $6 \times k \times N$. The complexity of the circuit increases linearly with the size of the input space. Since this leads to high computational complexity at greater depths, in Pérez-Salinas et al. (2021), the authors proposed using a single-qubit universal approximate gate based on the fundamental universal approximation theorem (UAT):

$$U^{UAT}(\vec{x}, \vec{w}, \alpha, \varphi) = R_y(2\varphi)R_z(2\vec{\omega} \cdot \vec{x} + 2\alpha), (\vec{\omega}, \alpha, \varphi) \in (R_m, R, R),$$

where $\vec{\omega}, \alpha, and \varphi$ are all trainable parameters.

Once the feature map and ansatz are defined for a target variational quantum circuit, it can be trained following the typical hybrid procedure. The input data are loaded into the network with an initial set of arbitrary parameter values. Gates are then applied, followed by a measurement operation. The measurement result is fed into a specific cost function that is used to guide a classical optimizer to determine the next set of parameters. This process is performed iteratively until the optimizer obtains the minimum cost.

A quantum measurement strategy was incorporated to determine the optimal way to associate outputs from quantum observations with the target classes. A standard approach is to use thresholds to map measurement outputs to a target class. For example, in binary classification, if the conditional probability P(|0⟩||ψ⟩) is less than or equal to the threshold, the data point is mapped to class 0; otherwise, it is mapped to class 1.

A fidelity-based loss function was employed, and LBFGS was used as the classical optimizer:

$$X^2{}_f(\vec{\theta}, \vec{\omega}) = \sum_{\mu=1}^{M}(1 - |\langle\psi_s^{\mu}|\psi(\vec{\theta}, \vec{\omega}, \vec{x}_\mu)\rangle|^2),$$

where μ represents the data point, $|\psi_s^{\mu}\rangle$ represents the correct label state, and $\psi(\vec{\theta}, \vec{\omega}, \vec{x}_{\mu})$ represents the single-qubit state obtained after applying all the unitary operators. M denotes the number of data points, and the loss is summed over all data points.

The authors evaluated their approaches on both simulated data and real credit card data from Kaggle. The original approach, which used data encoding unitary operators and parameterized unitary operators separately, achieved superior accuracy on both training and test data compared to compressed unitary operators and UAT.

To enhance the training process with UAT, an initial data-loading layer was proposed. The initial hypothesis was that a data preparation step using a Hadamard gate can take advantage of the superposition state to facilitate the parameter optimization. Based on this idea, the authors considered that it may be even more advantageous to prepare the data state using a generic parametrized unitary gate whose parameters are optimized jointly with those of the ansatz. On the toy data, initial loading with parameterized unitary gate U achieved better training and test accuracy than not having an initial loading or using a Hadamard gate as the initial loading.

The authors also experimented with different numbers of layers and observed that using four layers with UAT, combined with initial loading with an arbitrary unitary rotation, yielded the optimal results in terms of training and test accuracy. The authors also compared the results of UAT with and without initial data loading using a parameterized unitary gate. With initial loading, the test accuracy was 2% higher than that without initial loading. However, the training accuracy was 2% higher without initial loading. This suggests that initial loading can help mitigate potential overfitting.

For the real data, the authors also performed PCA for dimensionality reduction and data sampling to reduce the number of data samples and address class imbalance. The algorithm results for the UAT+U method were presented in terms of true positives, true negatives, false positives, false negatives, accuracy, precision, and recall. Using two layers produced considerably better results than using a single layer and slightly better results than using four layers. The overall benchmarking results demonstrated that using two layers of UAT combined with initial loading outperformed the best classical approach with two layers.

While these findings are promising, they should not be regarded as definitive evidence of any quantum advantage. Classical machine learning continues to dominate because it can handle large datasets within the framework of deep neural networks. However, if a single qubit can effectively learn the relevant relationships between data and the corresponding labels, future architectures incorporating multiple qubits can refine certain quantum characteristics, such as entanglement, potentially offering an advantage.

Quantum computing, while promising, continues to face hardware and algorithmic limitations. Addressing potential ethical concerns, particularly in fraud detection, such as data privacy and algorithmic bias, is vital to ensure responsible and sustainable adoption in the field of finance. A balanced perspective that highlights both advantages and limitations is crucial for providing a comprehensive understanding of the topic. Nevertheless, research on robust quantum hardware, quantum error correction, and quantum error mitigation is promising. Advancements in these areas can lead to improved quantum fraud detection and prevention approaches, which can greatly benefit financial institutions. Specifically, for data privacy and security, post-quantum cryptography (PQC) is being extensively researched and incorporated.

Monte carlo methods in finance

This section introduces the application of quantum algorithms for performing Monte Carlo calculations in finance. It provides an overview of the development and different application areas, providing a comprehensive compilation that does not exist in the literature. The topics discussed in the previous two sections—portfolio optimization and quantum machine learning algorithms—may play a role in the near future, as the related methods are compatible with NISQ technology. However, this is not the case for quantum Monte Carlo, which is the focus of this section. As demonstrated in the following discussion, most potential real-world applications require a large number of error-free qubits, which are not yet available.

The application of Monte Carlo methods to finance began in 2018 with the seminal study by Rebentrost et al. Rebentrost et al. (2018). In their paper, the authors applied earlier theoretical work regarding the use of quantum methods to speed up Monte Carlo simulations, particularly Brassard et al. (2000) and Montanaro (2015). For this review of Monte Carlo methods in finance, we use Rebentrost et al. (2018) as the starting point.

In the following two subsections, we discuss the primary areas in finance where Monte Carlo methods are used: derivative pricing and risk calculation. A survey addressing these two topics, focusing on calculation details, is provided in Gómez et al. (2022).

Derivative pricing

Basics of Quantum Computational Finance

The application of quantum computing for solving simulation-based problems in finance began with Rebentrost et al. (2018). One of the classical problems in finance addressed in the study was the pricing of derivative contracts, which is expressed as

$$\Pi = e^{-rT} E_P[f(S_T)], \tag{1}$$

where r denotes the risk-free interest rate, T denotes the runtime of the contract, E_P denotes the expectation value under the risk-free measure P, and $f(S_T)$ denotes the payoff function of the derivative at time T, depending on the corresponding underlying asset. For example, the case of a plain-vanilla European call or put option is considered. A European call (put) option gives the owner of the contract the right to buy (sell) the underlying option for a predefined price at a certain time in the future. Here, Eq. (1) can be solved analytically (Hull 1993). However, when the payoff of a derivative becomes more complex, this is usually no longer the case, and other approaches are used instead, such as Monte Carlo simulation, to calculate the price Π in Eq. (1). When the payoff $f(S_T)$ has bounded variance λ^2, achieving a constant success probability requires

$$k = \mathcal{O}\left(\frac{\lambda^2}{\epsilon^2}\right) \tag{2}$$

samples to estimate the expected value up to an error ϵ. Using the exact result available for European call options, Rebentrost et al. (2018) demonstrates that a

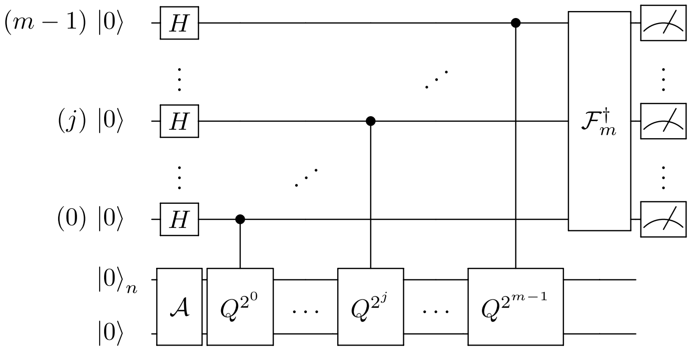

Fig. 5 Full quantum circuit for the Monte-Carlo algorithm, c.f. Brassard et al. (2000). *H* is the Hadamard gate and $\mathcal{F}_m^\dagger$ denotes the inverse Quantum Fourier Transform on *m* qubits

quantum-enhanced Monte Carlo method requires only $k = \mathcal{O}(\frac{\lambda^2}{\epsilon})$ steps, resulting in an exponential speedup.

The principle of using a quantum algorithm to perform a Monte Carlo simulation is described as follows. Consider a quantum state

$$|\psi\rangle_n = \sum_{i=0}^{N-1} \sqrt{p_i}|i\rangle_n, \tag{3}$$

where $p_i \in [0,1]$, $\sum_{i=0}^{N-1} p_i = 1$, and $N = 2^n$. Here, p_i represents the probability of measuring the state $|i\rangle_n$, which is one of the N possible realizations of a bounded discrete random variable X.

Now, consider a function $f : \{0, ..., N-1\} \to [0,1]$, which models the payoff of the derivative, and a corresponding operator

$$\mathcal{A} : |i\rangle_n|0\rangle \mapsto |i\rangle_n\Big(\sqrt{1-f(i)}|0\rangle + \sqrt{f(i)}|1\rangle\Big), \tag{4}$$

for all $i \in \{0, ..., N-1\}$, acting on an ancilla qubit. Applying $\mathcal{A}$ to $|\psi\rangle_n|0\rangle$ leads to the state

$$\sum_{i=0}^{N-1} \sqrt{1-f(i)}\sqrt{p_i}|i\rangle_n|0\rangle + \sum_{i=0}^{N-1} \sqrt{f(i)}\sqrt{p_i}|i\rangle_n|1\rangle. \tag{5}$$

Finally, defining a suitable unitary operator Q, as per (Rebentrost et al. 2018), and applying $Q^k, k = 0, 2^{n-1}$ in a controlled way to the circuit amplifies the desired amplitude. With an inverse QFT, it is possible to extract the phase of this state, which is then measured as a bit-string. The structure of the proposed algorithm consisting of amplitude amplification and phase estimation is displayed in Fig. 5.

The results of Rebentrost et al. (2018) can be summarized as follows:

1. A quadratic speedup by quantum algorithms compared to classical Monte Carlo is demonstrated under a relatively mild assumption (bounded variance of the random distribution).
2. For a European call option with a normal random distribution, the gates for preparing the algorithm are explicitly provided, serving as a guide.

3. A numerical study for a small setup demonstrates the quadratic speedup of quantum Monte Carlo (see Fig. 3 in Rebentrost et al. 2018).

Improvements to the basic Monte Carlo method

The derivative pricing approach presented in the previous section is promising from an application perspective, as it offers a quadratic speedup compared to classical Monte Carlo methods. However, its implementation in a realistic setup is beyond the capability of current and near-future quantum hardware. The required number of qubits and circuit length are not currently available now and will likely not be available in the the near future. Therefore, soon after the publication of Rebentrost et al. (2018), the search for modifications began, aiming to find alternatives using quantum amplitude amplification and QPE together. In a recent review (Intallura et al. 2023), the authors presented and discussed the technical details of the different improvements.

In Suzuki et al. (2020), the authors proposed a method for amplitude amplification without phase estimation. Instead of applying all controlled Q^k operations followed by an inverse Fourier transform, this method applies Q^k only once, followed by a direct measurement. Repeating this several times with different values of k produces a likelihood function for the desired target parameter, which can then be maximized. In Aaronson and Rall (2020), the authors theoretically examined how to achieve a quadratic speedup of Monte Carlo algorithms without QFT. In a subsequent publication (Tanaka et al. 2020), the authors presented results of the maximum likelihood method in a realistic environment, namely, on an IBM quantum device. The study demonstrated the effects of different errors on the theoretical results. Another study (Brown et al. 2020) provided a comparative analysis using theoretical noise models instead of real quantum devices.

Following the work in Tanaka et al. (2020), in Uno et al. (2021), the authors proposed a modification of the Grover operator, which demonstrated superior performance in cases where noise existed on physical devices. In addition, based on Suzuki et al. (2020), in Plekhanov et al. (2022), the authors developed variational quantum amplitude estimation (QAE). This method employs a variational ansatz to reduce the circuit depth of the traditional amplitude estimation algorithm. The maximum likelihood method was applied for post-processing, and the results demonstrated that classical Monte Carlo was outperformed.

Another approach to circumvent the expensive circuit described above was proposed in Grinko et al. (2019). The authors called their method iterative quantum amplitude estimation (IQAE) and reported that it achieved better results than comparable algorithms. The principle of their method is to iteratively determine the optimal power k of the Grover operator Q^k. The authors provided an algorithm to achieve this and presented the numerical results. Furthermore, they compared their method to the maximum likelihood method discussed above. However, a drawback of their method is that calculations cannot be performed in parallel.

A Monte Carlo algorithm without QFT but with extensive post-selection was also proposed in Ramos-Calderer et al. (2019). Here, the authors employed unary encoding of the asset value. This leads to a reduction in circuit depth; however, considerably more qubits are required than by the traditional approach. The authors stated that this approach may be advantageous in the NISQ era.

While most studies considered the pricing of a plain-vanilla European option, in Kaneko et al. (2022), the authors extended the framework to pricing options using a local volatility model, in which the volatility of the underlying asset varies with price and time. The solution is obtained using amplitude encoding, where the probability distribution of the derivative's payoff is encoded into the probabilistic amplitude. Additionally, in a second method, sequences of pseudorandom numbers are used to simulate the evolution of asset prices, as in classical Monte Carlo simulation. The principle of using pseudorandom numbers was further discussed in Kaneko et al. (2021). If the integrand used in the Monte Carlo calculation exhibits a separable structure with respect to contributions from distinct random numbers, combining nested QAE and pseudorandom numbers can accelerate the calculation.

In Stamatopoulos et al. (2020), the authors applied the quantum Monte Carlo framework to the pricing of different option types: plain vanilla options, multi-asset options, and path-dependent options, such as barrier options. The authors described implementation details and demonstrated how nontrivial payoff functions can be encoded into a quantum circuit. For evaluation, the authors employed the approach of Suzuki et al. (2020), specifically, without QFT and with maximum likelihood postprocessing. Results were obtained using IBM hardware, and a sophisticated error reduction scheme was applied. In a subsequent paper (Stamatopoulos et al. 2022), the authors extended the calculation to determine the option Greeks, which are the derivatives of the option price with respect to the input parameters. The calculation of these derivatives is essential for determining the market risk of financial options. Another approach to calculating the derivatives of financial options was discussed in Miyamoto (2022).

Furthermore, in Chakrabarti et al. (2021), the authors established an upper bound on the resources required to achieve quantum advantage in derivative pricing. They considered a special types of derivatives, Autocallable, and Target Accrual Redemption Forward (TARF) derivatives as benchmark use cases. Despite improving the existing algorithm by combining pretrained variational circuits with fault-tolerant quantum computing, the authors reported that the benchmark use cases required 8,000 logical qubits and a circuit depth of 54 million gates. However, pricing could be performed in only one second.

Another more complex financial derivative was examined in Miyamoto (2022). For the pricing of Bermudan options, which can be executed at specific dates, it is necessary to model the payoff more thoroughly. The authors demonstrated how a combination of Chebyshev interpolation and QAE can be employed in this case. In the domain of interest rate derivatives, the LIBOR market model plays an important role. In Tang et al. (2022), the authors examined how caps can be priced using a quantum Monte Carlo approach based on this model.

The limitations of the full Monte Carlo algorithm, particularly in the NISQ era, inspired additional studies to improve the procedure on a fundamental level. The authors of Herbert (2022) proposed a method for Monte Carlo integration by expanding the integral as a Fourier series and estimating each component individually using quantum amplitude estimation. Theoretical and numerical results indicated that this method achieved a full quadratic speedup. A fundamentally different approach was described in Saha et al. (2022). To perform the quantum Monte Carlo algorithm without any ancilla qubits, the authors suggested using intermediate qutrit states, which have three levels instead of two. To avoid the computational requirements of the full Monte Carlo approach, the authors of Braun et al. (2022) proposed a method where the quantum amplitude part of the algorithm is performed in parallel. This approach reduces the circuit depth; however, it requires a larger number of qubits. Whereas most analyses assumed that the payoff function characterizing the relevant option is positive, in Manzano et al. (2023), the authors removed this assumption. In their study, the authors presented a detailed calculation of different options using the above-mentioned QAE schemes.

A crucial aspect of all quantum Monte Carlo methods is the encoding of the probability distribution into the quantum state. If this is not performed sufficiently carefully, the computational advantages can be reduced. In Vazquez and Woerner (2021), the authors proposed an approach that simplifies state preparation. Together with a circuit optimization technique, this approach can considerably reduce the circuit complexity for QAE state preparation. Results were presented for option pricing under a specific stochastic volatility process, the Heston model, using real hardware. Another approach was described in Zoufal et al. (2019), where a quantum generative adversarial network (QGAN) was used for learning and encoding random distributions into the quantum circuit, which could then be utilized in subsequent Monte Carlo steps. Due to their flexibility, QGANs have a number of potential applications in finance, including asset management and risk management for generating stress scenarios.

An extension of the derivative pricing method using Monte Carlo to another class of financial products was investigated in Tang et al. (2021). The authors described how tranches of collateralized debt obligations can be priced using a quantum Monte Carlo method. As the underlying algorithm, IQAE introduced in Grinko et al. (2019) was implemented, and the Gaussian copula was used as the credit default model for the underlying dynamics.

Finally, in Alcazar et al. (2022), the authors presented a detailed calculation of credit valuation adjustments. This topic was also addressed in Han and Rebentrost (2022), but from a purely theoretical perspective.

Risk calculation

The application of quantum Monte Carlo methods to risk calculations in the financial industry was first described in Woerner and Egger (2019). The authors used the full algorithm (i.e., QAE including QFT) to calculate the value-at-risk (VaR) of a fixed-rate treasury bond. The basis of this algorithm is Eq. (5). Directly applying amplitude estimation to approximate the probability of measuring $|1\rangle$ in the last qubit leads to $\sum_{i=0}^{N-1} p_i f(i)$ and thus also $\mathbb{E}[f(X)]$. For a given confidence level $\alpha \in [0,1]$, $\mathrm{VaR}_\alpha(X)$ can be defined as the smallest value $x \in \{0, ..., N-1\}$ such that $\mathbb{P}[X \leq x] \geq (1-\alpha)$. Similarly, CVaR—the expectation value of all values exceeding VaR— can be calculated.

Table 6 Categorization of studies based on the algorithms or applications used

Algorithms and applications	Related work surveyed
Basic Monte Carlo algorithm for derivative pricing	Brassard et al. (2000), Montanaro (2015), Rebentrost et al. (2018).
Improvements of basic algorithm	Grinko et al. (2019), Ramos-Calderer et al. (2019), Suzuki et al. (2020), Aaronson and Rall (2020), Tanaka et al. (2020), Intallura et al. (2023), Brown et al. (2020), Uno et al. (2021), Plekhanov et al. (2022), Herbert (2022), Saha et al. (2022), Braun et al. (2022), Vazquez and Woerner (2021), Zoufal et al. (2019).
Application to non-vanilla derivatives	Kaneko et al. (2021), Kaneko et al. (2022), Stamatopoulos et al. (2020), Miyamoto (2022), Chakrabarti et al. (2021), Miyamoto (2022), Tang et al. (2021), Tang et al. (2022), Manzano et al. (2023).
CVA and Risk Calculation	Alcazar et al. (2022), Han and Rebentrost (2022), Woerner and Egger (2019), Egger et al. (2020), Miyamoto et al. (2019), Miyamoto (2022), Gómez et al. (2022), Dri et al. (2022), Matsakos and Nield (2023), Wilkens and Moorhouse (2023).

In Woerner and Egger (2019), the authors further reduced the simple example (only one asset), allowing the calculation to be performed using four qubits. They demonstrated the expected theoretical quadratic speedup and provided results obtained on a physical quantum device. A direct extension of their study to credit risk was provided in Egger et al. (2020). The conditional independent Gaussian model considered in the study is very simple but enables a straightforward implementation of a quantum algorithm. In this paper, the authors demonstrated how CVaR can be caculated in this framework.

In Miyamoto et al. (2019), the authors presented a credit portfolio risk calculation. They demonstrated that it is possible to reduce the number of qubits while maintaining quantum speedup by performing the calculation similarly to the classical one. This involves estimating the average of integrand values sampled by a pseudorandom number generator implemented on a quantum circuit. However, the reduced number of qubits is a trade-off against increased circuit depth.

In Dri et al. (2022), the authors described a method for implementing a more realistic and complex risk model for the default probability of each portfolio's asset, capable of considering multiple systemic risk factors. Additionally, the constraint that the loss given default may only take integer values was removed. This approach was implemented, and the corresponding gate structure was presented.

In Miyamoto (2022), the authors addressed a critical question for potential applications in finance: how to calculate risk contributions in a quantum-enhanced credit risk model. The authors theoretically discussed the necessary circuit structure and derived the speedup compared to classical approaches. Another extension of the quantum Monte Carlo approach for risk calculation was provided in Matsakos and Nield (2023). The authors incorporated scenario generation into quantum computation by simulating the evolution of risk factors over time. To achieve this, they assembled quantum circuits to implement stochastic models for equity risk factors (geometric Brownian motion), interest rate risk factors (mean reversion models), and credit risk factors (structural and reduced-form credit models). These scenarios served as inputs for quantum Monte Carlo simulations, providing end-to-end examples for both market and credit risk use cases.

We conclude this section by referring to Wilkens and Moorhouse (2023), which reviewed different approaches for calculating market and credit risk using quantum Monte Carlo methods. Considering the current state of research on quantum Monte Carlo methods in finance, a nuanced picture emerges. The promises offered by a quadratic speedup cannot be achieved using current NISQ technology. Consequently, several more years of hardware advances are necessary before business advantages can be achieved. Table (6) lists all the papers considered in this section and their covered topics.

Blockchain in quantum finance

Quantum computing and blockchain systems are two emerging technologies with the potential to revolutionize modern business models. Recent advancements in quantum computing have considerably enhanced the computational efficiency of key algorithms, posing serious security challenges to cryptography-based technologies, such as blockchain. In this section, we provide a detailed analysis of blockchain-based financial systems within the context of the emerging quantum era. We begin by discussing the fundamentals of blockchain and its real-world applications, including specific financial use cases such as cryptocurrencies, smart contracts, digital payment, exchange systems, and nonfungible tokens (NFTs). This is followed by an examination of the security and privacy aspects of financial blockchains, with a specific focus on the quantum threats they face. Next, we discuss strategies to mitigate these possible quantum attacks and outline the differences between quantum-resistant and quantum-safe blockchains. In addition to security analysis, we address privacy-preserving quantum-resistant cryptocurrencies apart and introduce quantum blockchains. It should be noted that while several reviews address the relationship between blockchain and quantum technologies, most focus on a single aspect, such as quantum-resistance, blockchain security without considering the quantum attacks, or quantum computing and mining. On the other hand, this review comprehensively addresses all the abovementioned aspects along with a focus on privacy-preserving coins and their relevance to finance. The primary objective of this review is to consolidate essential data from diverse sources, reducing the effort required by researchers to search for and analyze the latest advancements. Furthermore, this review aims to provide insights into the challenges and opportunities of integrating quantum technologies into blockchain systems and utilizing cryptoassets in fintech applications. By offering an expansive and thorough perspective, this review addresses critical security issues and explores topics often overlooked in recent surveys.

Blockchain basics

This section introduces a conceptual description of blockchain systems, their basic structure and use cases in various real-world applications. Blockchain is a digital, distributed, and decentralized ledger system that functions as a database. Unlike traditional databases, blockchain divides data into multiple blocks distributed across various computers, referred to as peers (nodes). Its data structure resembles a public record where all completed transactions are sequentially recorded in blocks. This sequence continuously expands as new blocks are added. The governance of this distributed system relies on consensus algorithms. The evolution of blockchain systems is driven by the idea of constructing a secure peer-to-peer (P2P) digital payment system that eliminates the need for a trusted third party, such as banks. User security and ledger consistency are achieved through asymmetric cryptography and distributed consensus algorithms. Key characteristics of blockchain are as follows:

- **Decentralization** Blockchain consensus algorithms eliminate the need for a trusted third party, reducing the associated costs and avoiding performance limitations.
- **Persistency (immutability)** Once transactions are added to the blockchain, they become highly resistant to removal or alteration, ensuring data integrity.
- **Anonymity** Users are identified by unique addresses, such as, Bitcoin addresses, which are generated as a 160-bit hash of the user public key.
- **Auditability** The unspent transaction output model employed in blockchain enables straightforward verification and tracking of all transactions, ensuring auditability.

Real-world applications of Blockchain technology

Blockchain technology has broad applications across various sectors, particularly in financial services, such as digital assets, online payments, and remittances, because it enables transactions without the need for banks or central authorities. In addition to finance, blockchain can also be implemented in areas such as smart contracts, security services, reputation systems, public services, and the Internet of Things (IoT). The key real-world scenarios in which blockchain technology is applied include the following:

- **P2P Global transactions** Although services like PayPal [1], [2] offer international payment processing, they often charge significant transaction fees. In contrast, blockchain technology provides a secure, cost-effective, and fast method for transferring funds globally without the need for a trusted third-party. In addition, many P2P payment services impose limitations, such as location restrictions and minimum transfer amounts. As a result, an increasing number of businesses and individuals are turning to cryptocurrencies for international transactions.
- **Supply chain management and quality assurance** Blockchain technology offers advantages in supply chain management by enhancing traceability and cost-effectiveness. With blockchain technology, goods can be tracked from their origins, including details such as quantity and other relevant information. This increased transparency simplifies various supply chain processes, such as payment, production process verification, and ownership transfers. In the event of any irregularities in the supply chain, a blockchain system can trace the issue back to its point of origin, allowing businesses to investigate and take corrective actions. In the food industry, maintaining quality and safety is crucial, and blockchain technology can help track important information like origin, batch details, and other relevant factors [2].
- **Accounting** Blockchain technology notably reduces the risk of human error and protects data from tampering by securely recording transactions. Each time records are passed between blockchain nodes, they are verified, ensuring accuracy. This process

not only guarantees the integrity of financial records but also creates a traceable and immutable history of transactions (Han et al. 2023).

- **Smart contracts** Lengthy contractual processes can hinder business growth, especially for companies that regularly manage a high volume of communications. Smart contracts automate the validation, signing, and enforcement of agreements using a blockchain framework. This eliminates the need for intermediaries, thus saving both time and money. In 1994, cryptographer Nick Szabo [3] recognized the potential of decentralized ledgers to create smart contracts, also known as self-executing digital contracts. In this approach, contracts are transformed into computer code, stored and replicated on the blockchain, and managed by a network of computers.
- **Voting** Blockchain technology could considerably reduce the risk of electoral fraud in local elections, which remains a major concern despite the use of electronic voting systems. NASDAQ [4] used blockchain technology to streamline shareholder voting. The initiative, known as the "e-voting" project, involved collaboration with a blockchain technology partner and local digital identity solutions that issued government-authorized identity cards. The project proved to be disruptive, practical, and necessary, yielding positive results.
- **Stock exchange** Blockchain technology is a potential solution to securities and commodity trading due to its reliability and transparency. As a result, stock exchanges are exploring their potential as a notable advancements in their operations. For example, the Australian Stock Exchange (ASX) [5], [2] has planned to transition to a blockchain-based system using technology developed by the blockchain startup Digital Asset Holdings. In December 2017, ASX announced that it had chosen Digital Asset Holdings to develop a new distributed ledger technology-based system to replace its existing Clearing House Electronic Subregister System platform. The updated system is expected to offer several benefits, including faster settlement times, enhanced efficiency, and greater security and resilience.
- **Energy supply** Blockchain technology is enabling sustainable energy solutions by providing precise tracking of energy usage through "transactive grids," which are available to both commercial establishments and households in certain regions. For example, Powerpeers [6] in the Netherlands and Exergy [7], [2] in Brooklyn, New York are using blockchain to manage energy distribution. In addition, blockchain technology can enhance the monitoring and management of clean energy.
- **IoT devices** Blockchain technology offers a secure, decentralized network for the IoT [8], reducing the risks associated with traditional central server models. This will create a platform for a communal economy based on machine-to-machine interactions. Through blockchain, data generated by IoT sensors can be monetized, allowing owners of IoT devices to sell such data in exchange for digital currencies.
- **e-Auction** Integrating blockchain technology into e-auctions can improve transparency, security, and efficiency. By adopting a decentralized platform, blockchain eliminates intermediaries and ensures secure, tamperproof transaction records. This fosters trust between buyers and sellers because all participants have real-time visibility into the entire bidding process, thereby reducing the likelihood of fraudulent

activities. In addition, the use of smart contracts in blockchain-based e-auctions automates the bidding process and ensures that all parties adhere to agreed terms and conditions. As a result, blockchain technology has the potential to revolutionize the e-auction industry by offering a more secure and efficient platform for online auctions. The privacy-preserving features further enhance security systems. In traditional e-auctions, participants can view the bids of others, potentially exposing sensitive information and deterring bidders. In contrast, privacy-preserving e-auctions encrypt bids and protect bidder identities, thus ensuring the confidentiality and security of bid information. Advanced techniques like homomorphic encryption and secure multiparty computation, allow an auctioneer to calculate winning bids without revealing individual bids (Baum et al. 2023).

- **NFTs** NFTs are unique digital assets stored on a blockchain, typically the Ethereum blockchain, that cannot be divided. Unlike fungible tokens such as Bitcoin or Ether, which can be exchanged on a one-to-one basis, NFTs are distinct and indivisible. NFTs (non-fungible tokens), [2] are primarily used to represent the ownership of digital assets, such as art, music, videos, and other forms of creative content. This allows creators to sell their digital works as one-of-a-kind, valuable items, much like physical art. Buyers can verify the ownership and authenticity of these digital assets through the blockchain.

One can refer to Prewett et al. (2019) for potential future barriers to blockchain adoption, including scalability issues, system integration challenges, lack of standardization, complexity of blockchain applications, regulatory uncertainty, and risks related to architecture, design, endpoints, storage, data security and confidentiality, smart contracts, compliance, and vendor or contractual issues.

Evolution of blockchain and cryptocurrencies in finance

In this section, we briefly discuss the historical evolution of digital cash systems from the most primitive forms to today's complex Bitcoin form. In 1982, David Chaum introduced a digital cash and blind signature system (Ciulei et al. 2022; Chaum 1983), and although he went bankrupt in later years, he founded the electronic cash company *DigiCash*, which enabled an untraceable digital payment system based on cryptographic digital signatures. In 1997, Adam Back developed the Proof-of-Work (PoW) algorithm (Back 2002; Ciulei et al. 2022), another important concept in blockchain systems, through *Hashcash*, initially designed as a countermeasure to denial-of-service attacks, spam emails, and unauthorized internet sources. In 1998, Nicholas Szabo proposed *Bit gold*—a simpler version Bitcoin—integrating PoW into a computer network and using the Byzantine agreement protocol, which prioritized the majority's addressess rather than computational power (Ciulei et al. 2022). That same year, Wei Dai proposed *b-money* an untraceable, distributed, electronic cash system that could enforce contracts between pseudonymous entities (Ciulei et al. 2022), [10]. In 2008, the concept of Bitcoin, a P2P electronic cash system, was introduced by an author or group under the pseudonym Satoshi Nakamoto. The proposed system provided a solution to the double-spending problem (Ciulei et al. 2022; Nakamoto 2008), [11]. The following year, in 2009, the first Bitcoin network was established as a decentralized ledger. This technology, known as Bitcoin 1.0, stores transactions in an immutable, decentralized, and distributed manner across blockchain nodes. In 2013, Vitalik Buterin conceived the idea of Ethereum, a blockchain that supports smart contract functionality. Today, Ethereum's native token, *Ether*, ranks second in market capitalization only behind *Bitcoin* [12], (Ciulei et al. 2022).

Consensus mechanism in blockchain

Consensus is a flexible collaborative process in which agreement is reached within a group considering the perspectives and interests of all members. Unlike voting, which often reflects majority opinion, consensus seeks to find a solution that benefits the group as a whole. In blockchain technology, there are several types of consensus, including state, payment, and network rule consensus. Before the advent of Bitcoin, earlier attempts at creating P2P decentralized currency systems struggled to overcome the critical challenge of achieving consensus known as the "Byzantine Generals Problem." This problem illustrates the difficulty of reaching agreement in a decentralized system, where malicious actors or unreliable communication can disrupt coordination (Lamport et al. 1982). For example, consider sending 7 Ether from your wallet to another person. How can a third-party ensure that the transaction amount is not altered by the third-party in the network to, for example, 70 Ether? Consensus mechanisms address these kind of issues. To protect the integrity of the transaction during transmission, the transaction is broadcast to the network and verified by its nodes. Once sufficient nodes validate the transaction, it is recorded in the blockchain. Once in the blockchain, a transaction cannot be altered or deleted without agreement from most nodes; thus, tampering is extremely difficult, if not impossible. This ensures that the recipient can trust that they have received the exact amount sent. The following are some widely used consensus mechanisms:

- **PoW** In this system, special nodes called "miners" compete to solve complex cryptographic hash puzzles to add a block to the blockchain. These puzzles are computationally intensive and require considerable power and energy. Once a miner successfully solves the puzzle, they propose their block to the network, which then verifies its validity—a straightforward process. One disadvantage of the PoW mechanism is its inefficiency, as it requires substantial power and energy consumption. This high resource requirement creates an uneven playing field where individuals or entities capable of acquiring faster and more powerful ASICs have a greater probability of successful mining. Consequently, this disparity poses a risk to the decentralization concept. Bitcoin (BTC), Ethereum Classic (ETC), Litecoin (LTC), Monero (XMR), and Bitcoin Cash (BCH) are examples of blockchains using the PoW consensus protocol.
- **Proof-of-Stake (PoS)** The PoS consensus mechanism eliminates the need for solving complex mathematical puzzles. In contrast, the creator of a new block is selected deterministically based on their "stake" in the network, which refers to the number of coins or tokens they hold. In this system, the higher the stake, the greater the probability of being chosen as the next block validator. One major benefit of PoS is its

increased energy efficiency, as it does not rely on the energy-intensive mining process, making it a potentially more environmentally friendly alternative to PoW. However, a disadvantage of PoS is that it incentivizes large stakeholders to accumulate more cryptocurrency to increase their chances of being selected as validators and earning rewards, potentially leading to centralization. Examples of cryptocurrencies that use the PoS consensus mechanism include Cardano (ADA), Casper, and Algorand (ALGO).

Other consensus algorithms are listed below:

- Practical Byzantine fault tolerance, delegated Proof-of-Stake, Proof-of-Importance, Proof-of-Burn, Proof-of-Luck, delegated Byzantine fault tolerance, Proof-of-Concept, Proof-of-Exercise, Proof-of-Capacity, Proof-of-Elapsed Time, Proof-of-Weight, and others.

Cryptographic aspects of blockchain

Cryptography is the underlying mechanism of blockchain **security** and **privacy**. The primary cryptographic primitives in blockchains are **hash functions** and **digital signature algorithms**, both of which resist unauthorized alterations and modifications to the ledger, facilitate consensus, and ensure public verifiability.

Digital signature algorithms

Digital signature algorithms are based on public key cryptographic systems. They are used to sign transactions with the signer's private key, while verification is performed by other nodes using the public key. These algorithms ensure the *authenticity* of the transaction source, *data integrity* (i.e., that the data are not tampered with by a malicious attacker), and *non-repudiation*. Non-repudiation is the ability to prove that a certain action or transaction has been performed by a specific party and that this party cannot deny having performed this action or transaction. In other words, it is the assurance that the originator of a message or a transaction cannot deny their involvement in it. The most commonly used digital signature algorithms are as follows:

- **Rivest-Shamir-Adleman (RSA) digital signature algorithm** The RSA (Rivest et al. 1978a) encryption algorithm is a widely used public-key cryptographic system employed for secure data transmission and digital signatures. In this algorithm, messages are signed with a private key, and the signature can be verified with the corresponding public key. The cryptographically challenging problem underlying the RSA digital signature algorithm is the integer factorization problem (Boudot et al. 2019). Examples of cryptocurrencies utilizing this algorithm include Namecoin, Hedera, and Arweave. Although this algorithm is not always the primary digital signature algorithm in certain cryptocurrencies, such as Bitcoin, Litecoin, and Dogecoin, it is utilized in certain aspects of these protocols. For example, it is used in Bitcoin for key generation and signature verification for multi-signature transactions (Bitcoin), in Dogecoin for encryption and decryption of private keys, and in Namecoin for generating and verifying SSL (Secure Socket Layer) certificates for websites hosted on its decentralized domain name system.

- **Elliptic curve digital signature algorithm (ECDSA)** This digital signature algorithm is based on the mathematically hard discrete logarithm problem (DLP) (Shor 1997; Rosen 2011) on elliptic curves. ECDSA offers an advantage over the RSA algorithm by providing equivalent security with smaller key sizes. As a result, ECDSA is more efficient in terms of storage and transmission, as smaller keys require fewer computational resources. Popular cryptocurrencies that employ ECDSA include Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Bitcoin Cash (BCH), Ripple (XRP), Binance Coin (BNB), Cardano (ADA), Polkadot (DOT), Chainlink (LINK), and Dogecoin (DOGE). ECDSA is widely used as it provides strong security while using smaller key sizes than traditional digital signature algorithms.
- **Edwards curve digital signature algorithm (EdDSA)**
  While not as widely used as ECDSA, EdDSA (Josefsson and Liusvaara 2017) has been adopted by some cryptocurrencies and blockchain networks as their digital signature algorithm. Examples include Monero (XMR), Zcash (ZEC), Stellar (XLM), Nano (NANO), Grin (GRIN), and Solana (SOL). EdDSA provides strong security and faster signature generation than other digital signature algorithms, making it an attractive option for blockchain networks.

There are various types of digital signature algorithms, each offering distinct advantages, including enhanced **"privacy"**. Privacy can be achieved when digital signature algorithms are used in conjunction with relevant cryptographic primitives. Examples of such algorithms include ring signatures, blind signatures, threshold signatures, multi-signature schemes, and zero-knowledge proof commitments (Baum et al. 2023; Ciulei et al. 2022). The signature schemes used in various blockchains to achieve specific privacy-related features are listed below:

- **Multisignatures** A multisignature scheme (Yao 1982) is a cryptographic protocol that allows a group of individuals to collectively authorize a transaction or access a resource. This process requires a specific number of private keys distributed among participants. Each participant is required to provide approval by signing a transaction document or requesting approval using their private key. Multisignatures are implemented using several cryptographic techniques, such as multiparty computation, threshold encryption, homomorphic encryption, and secret-sharing schemes.
- **Threshold signatures** A threshold signature (Camenisch and Stadler 1997; Boldyreva 2003) is a digital signature scheme that allows a group of signers to collaboratively sign a message. This process requires a minimum number of signers, t (known as the threshold), out of a total of n signers to generate a valid signature. This threshold is established during setup. Threshold signature schemes offer enhanced security compared to traditional signatures because they require the collaboration of a minimum number of signers, reducing the risk of a single compromised device or malicious signer being able to forge a signature. In addition, these schemes provide greater efficiency than traditional signatures by minimizing the need for multiple rounds of signing and key exchange; thus, they are particularly useful in resource-constrained environments. By distributing the secret key among multiple parties,

these schemes also mitigate the risk of key exposure. While threshold signatures do not inherently provide anonymity, they can be combined with other cryptographic techniques to achieve robust anonymity in various applications.

- **Schnorr multisignatures** A Schnorr signature, introduced by Claus-Peter Schnorr in 1991, is a type of multisignature scheme (Schnorr 1991; Maxwell et al. 2019). The primary advantage of this scheme over standard multisignatures is its ability to perform key aggregation and batch verification, which allows multiple signatures to be verified simultaneously, thereby improving the verification speed. Another advantage is that they are *provably secure* (Rivest et al. 1978b); that is, their security can be mathematically demonstrated without relying on unproven assumptions about the fundamental cryptographic building blocks.
- **Ring signatures** A ring signature scheme (Rivest et al. 2001) allows a user to sign a message anonymously on behalf of a group, referred to as a ring or a set, while keeping the signer's identity concealed. Only members of the ring can authenticate the signature, thereby ensuring anonymity. Any member of a ring can generate a signature, and it becomes infeasible to determine the actual signer. This makes ring signatures useful in applications requiring robust anonymity, such as cryptocurrencies, voting systems, and whistleblowing. Although other signature types can offer anonymity, ring signatures are uniquely used to ensure signer's anonymity in blockchain transactions (Raikwar et al. 2019). Furthermore, they are instrumental in enabling untraceable payments (van Saberhagen 2013; Wang et al. 2019; Bender et al. 2005; Fujisaki and Suzuki 2007; Feng et al. 2021).
- **Blind signatures** Blind signatures allow a signer to sign a message without the signer seeing its content. These signatures allow a user to obtain a signature on a message or transaction in cryptocurrencies without disclosing the content of the message to the signer. Blind signatures provide anonymity and unlinkability (Ciulei et al. 2022; Heilman et al. 2016; Chaum 1982; Raikwar et al. 2019).
- **Zero-knowledge succinct noninteractive argument of knowledge (ZK-SNARKs)** ZK-SNARKs are cryptographic protocols that allow one party to prove to another party that they possess certain information without disclosing that information or without requiring any interaction between the parties. ZK-SNARKs is widely used in blockchain applications, particularly privacy-focused coins, because they enable transaction verification while concealing the identities of the parties or transaction amounts involved [13], (Bitansky et al. 2011; Ben-Sasson et al. 2014). DLP (Shor 1997; Rosen 2011) is the underlying cryptographically challenging problem that ZK-SNARKs rely on Kearney and Perez-Delgado (2021); Ciulei et al. (2022). An example of an ZK-SNARKs implementation is ZCash [82],—a cryptocurrency launched in 2016 that emphasizes privacy. Although ZCash is based on the same underlying code as Bitcoin, ZCash includes an additional privacy layer that enables user transactions without disclosing their identities and transaction amounts. ZCash provides two categories of addresses: *transparent* and *shielded*. Transparent addresses, similar to Bitcoin addressess, are observable on the blockchain. Shielded addresses, in contrast, are entirely confidential, using ZK-SNARKs to hide all transaction data from being visible on the blockchain. This dual-address structure makes ZCash a popular choice for individuals and corporations seeking secure and private financial transactions.

- **Bulletproofs** Bulletproofs (Bünz et al. 2018) are a type of noninteractive zero-knowledge proof system that allows one party to prove the validity of a statement to another without disclosing any additional information beyond the statement's truth. Bulletproofs represent a newer advancement in zero-knowledge proof systems, offering improved efficiency compared to ZK-SNARKs, particularly in terms of proof generation time and size. Unlike ZK-SNARKs, Bulletproofs do not require a trusted setup and use a distinct mathematical approach to generate more compact and faster-to-validate proofs. Cryptocurrencies such as Monero (XMR), Grin (GRIN), and Beam (BEAM) implement Bulletproofs to enhance privacy and efficiency.

  In addition to the aforementioned digital signatures, there exist **post-quantum digital signatures**, which are designed to provide security against potential attacks by quantum computers. These signatures are discussed in section PQC and quantum-safe blockchain

Hash functions

A hash function is a mathematical function that accepts an input (e.g., message, data, or transaction) of any length and produces a fixed-length output called a hash value or digest. These functions are designed to be one-way, implying that while computing the hash value from the input is simple, reversing the process is computationally infeasible. Commonly used hash functions include *Secure Hash Algorithm 256-bit (SHA-256), Secure Hash Algorithm 3 (SHA-3), BLAKE2, and RACE Integrity Primitives Evaluation Message Digest (RIPEMD)*. Popular hash functions used in cryptocurrencies are listed below:

- *SHA-256* Used by Bitcoin and other cryptocurrencies
- *Scrypt* Used by Litecoin, Tenebix, Fairbix, and other cryptocurrencies
- *Ethash* Adopted by Ethereum and Ethereum-based cryptocurrencies
- *Blake2b* Employed by Siacoin and other cryptocurrencies
- *Equihash* Integrated into Zcash and other cryptocurrencies
- *X11* Implemented by Dash, Darkcoin, and other cryptocurrencies
- *CryptoNight* Used by Monero and other cryptocurrencies

Hash functions play critical roles in blockchain technology, including: solving cryptographic puzzles in the mining (PoW) process, generating public and private key addresses, creating blocks using the Merkle tree approach, and producing pseudorandom numbers (Ciulei et al. 2022).

Bitcoin mining (PoW) and hash functions

Bitcoin employs the *SHA256d* hash function in its mining process. To add a new block to the blockchain, miners must discover a **nonce**—a 32-bit random number used once in a block header. The nonce is incremented by miners until the hash of the block header satisfies the following condition: $SHA256d(X||nonce) \leq n$, where n is the 256-bit target value. In addition, the first k blocks of the hashed value must all be zeros, where k is adjusted every 2, 016 blocks to maintain an average generation time of approximately

10 min. The primary objective of PoW, based on Back's concept introduced in 1997 Back (2002), is to allow a decentralized group to reach a consensus on a consistent transaction history without requiring pre-established trust among participants while also preventing double-spending attacks (Ciulei et al. 2022).

Blockchain forking

A blockchain fork occurs when the blockchain splits into separate chains because different segments of the network hold conflicting views of the transaction history. In general, a fork represents a divergence in the blockchain's state. This divergence often arises when multiple nodes in a decentralized network discover a suitable nonce simultaneously, thereby creating concurrent valid blocks and branching the chain. To address this issue, nodes in the network prioritize extending the chain of blocks with the highest PoW, which is often referred to as the longest chain or the chain with the greatest cumulative difficulty. Blockchain forks can be broadly categorized into two types:

- **Soft fork** A soft fork occurs when changes to the blockchain protocol are backward-compatible, meaning nodes running older software versions can still validate new blocks as valid. This ensures the blockchain remains unified, even if all nodes do not immediately upgrade to the new protocol. Soft forks are typically introduced to add new functionalities or improve efficiency without causing a split in the network. Unlike hard forks, soft forks do not require all nodes to upgrade their software.For example, **Segregated Witness (SegWit)** is a Bitcoin soft fork implemented on the Bitcoin blockchain to enhance network efficiency and increase transaction capacity by separating signature data from transaction data, thereby freeing up space in each block and enabling a higher number of transactions to be processed simultaneously. Other examples of Bitcoin soft forks include **BIP65, BIP66, and Pay-to-Script-Hash (P2SH)**, where the modifications to the blockchain protocol are backward-compatible, allowing nodes running older software versions to continue participating in the network without interruptions or difficulties.
- **Hard fork** A hard forks introduces fundamental changes to the blockchain protocol that are not backward-compatible, unlike soft forks. When a hard fork occurs, older nodes cannot validate new blocks, resulting in the creation of two separate chains. Typically, hard forks arise from disagreements among network participants over blockchain's operational rules, such as modifications to transaction fees or block size. To maintain compatibility with the updated blockchain, all nodes must upgrade to the latest software version. Nodes that do not upgrade remain on the original chain, resulting in the development of a new cryptocurrency. **Bitcoin Cash (BCH)** and **Bitcoin Gold (BTG)** are hard forks from the Bitcoin blockchain, while **Ethereum Classic (ETC)** is a hard fork from Ethereum.

Bitcoin and economics

The Bitcoin network is designed to maintain a constant block creation rate, producing six blocks per hour or one block every 10 min. This rate is intentionally maintained to prevent **inflation** within the Bitcoin network. As the mining hash rate increases, the difficulty of mining also increases to keep the block creation rate constant. When Bitcoin was introduced in 2009, the initial block reward for successful mining was 50 Bitcoin (BTC). This reward halves approximately every four years, after every 210,000 blocks have been mined. Currently, the block reward stands at 6.25 BTC, and this halving process will continue until approximately 2110–2140, by which time the total supply of Bitcoin will have reached 21 million BTC.

Bitcoin's limited supply, similar to gold, suggests that its value will likely increase over time. Therefore, Bitcoin is often referred to as **digital gold** (Gkillas and Longin 2018). The Bitcoin value is expected to increase until the last Bitcoin is mined, after which it may stabilize. While fluctuations in its value are inevitable, Bitcoin's status as the first-cryptocurrency has helped stabilize its value in recent years. In deflationary models, with less money being produced each year, the value of Bitcoin (or fiat currency) tends to increase. Bitcoin, as a currency, may contribute to an increase in the overall money supply, potentially leading to rising price levels. This rise is based on the assumption that the velocity of money and the quantity of goods and services remain constant, which is a simplifying assumption often used in economic models. However, Bitcoin is inherently deflationary because of its limited supply, which may result in a decrease in the value of other currencies while experiencing an appreciation in its value.

Gold has long been recognized as a limited commodity and a popular asset for hedging against expansive monetary policies. Similarly, Bitcoin shares the characteristics of gold as a finite asset, although it lacks intrinsic value. When the value of gold began to decline, partly due to reaching its price cap and the partial recovery of financial markets, Bitcoin's value notably increased. This increase can be attributed to Bitcoin's ingenious-design as a financial product with a capped supply, making it an attractive alternative as a store of value.

Security vulnerabilities of blockchain systems

Bitcoin is currently under consideration as a stock in the financial market (Dasgupta et al. 2019). It should be noted that blockchain is in fact computer software that enables transactions among participants in a P2P network. Thus, important questions regarding blockchain security are under discussion. In this section, we provide an overview of various security concerns related to **quantum threats** to blockchain. Blockchains face numerous security vulnerabilities beyond quantum-related concerns. Reviews such as Dasgupta et al. (2019), Wang et al. (2019), Li et al. (2017), Cain and Hosseinian-Far (2020) provide a comprehensive analysis of not only quantum-related threats, but other security threats against blockchains, including double-spending attacks, 51% attacks, selfish mining, Sybil attacks, replay attacks, manipulation-based attacks, eclipse attacks, transaction malleability, timejacking, reputation-based attacks, race attacks, Distributed Denial of Service (DDOS) attacks, Finney attacks, vector76 attacks, collusion attacks, and malware attacks. However, our main focus in this section is cryptographic vulnerabilities, which are more relevant to the goal of this paper, that is to explore the effects and risks of quantum computing in finance. The reason why we mostly focus on the cryptographic vulnerabilities is due to the potential effect of quantum algorithms which can break the current cryptographic schemes that underpin the basic security of blockchain transactions.

Cryptographic vulnerabilities

The three fundamental cryptographic primitives used in blockchain systems are digital signature algorithms, hash functions, and random number generators (RNGs). Below, we discuss attacks and threats associated with each of these primitives.

- **Digital signature algorithm vulnerabilities** Digital signature algorithms, which are based on public key cryptography, are the main security foundation of blockchain in conducting transactions and tracking past activities. Each blockchain uses its own specific digital signature algorithms and hash functions. Commonly used digital signature algorithms for blockchains include ECDSA and EdDSA. These algorithms are both based on a mathematically difficult elliptic curve discrete logarithm problem (ECDLP). This problem is NP-hard, signifying that it is computationally infeasible to find a solution in a reasonable amount of time. In other words, breaking the cryptographic structure of ECDSA requires solving the ECDLP within a reasonable amount of time and computational resources. Any vulnerabilities in the cryptographic foundation of ECDSA or EdDSA can cause serious security violations.

  Some cryptographers are skeptical about the secp256k1 curve, which is used in ECDSA of Bitcoin and Ethereum, due to its poorly explained curve parameter derivation process, which allows for potential manipulation. This uncertainty raises concerns that intentional weaknesses or limitations potentially leading to security vulnerabilities may exist within the curve (Dasgupta et al. 2019; Bernstein and Lange 2014). Furthermore, the operations of addition and doubling in elliptic curve cryptography have distinct time and power consumption characteristics, which can potentially be exploited through side-channel attacks, fault analysis, timing attacks, and power attacks (University of Stanford 2011).
- **Hash function vulnerabilities** SHA-256 is a secure hash algorithm that is commonly used in blockchain systems and is vulnerable to length-extension attacks (Dasgupta et al. 2019). These attacks are based on modifying the hash of a signed message or transaction by appending certain data without requiring access to the shared secret. A countermeasure to this attack is provided in Ferguson and Schneier (2003), which suggests the double use of SHA256. Hash algorithms are also vulnerable to birthday attacks, which are based on finding hash collisions. Such attacks broke the SHA-1 algorithm (Stevens et al. 2017). Due to these attacks, the SHA-1 and MD5 hash algorithms are considered broken and no longer secure for cryptographic purposes.
- **RNG vulnerabilities** (RNGs) play a crucial role in blockchain technology, serving several purposes such as selecting validators or miners, verifying transactions, and creating new blocks. Miners use an RNG to produce a random **nonce (a number that is used once)**, which is then combined with transaction data and hashed with the block header to authenticate transactions. This process is repeated until the hash value meets a predefined difficulty threshold. The miner who discovers the correct hash is then rewarded with cryptocurrency. Another common use of RNGs is in

PoS-based blockchains, where validators are selected to create new blocks based on the amount of cryptocurrency they hold. To ensure fairness and prevent centralization, an RNG is often employed in the selection process. RNGs are also integral to the ECDSA (to generate a secret nonce used in the signing process). This nonce is a randomly generated value that ensures the uniqueness of each signature, thereby preventing the generation of identical signatures for different messages. However, the security of RNGs, particularly those used in cryptographically secure protocols like ECDSA, can be compromised if the random numbers are poorly selected. A weak or biased RNG allows an attacker to recover a private key from its corresponding public key. One such example is an attack on Android Bitcoin wallets, where the pseudorandom number generator in Java was found to be weak and vulnerable to exploitation (Dasgupta et al. 2019). In addition, attacks leveraging lattices have been discussed in Breitner et al.'s study (Breitner and Heninger 2019), where biased nonces in ECDSA, combined with partial knowledge of some bits, can lead to the recovery of private keys using hidden number problem and lattice reduction algorithms. Therefore, ensuring that the nonce is generated by a cryptographically secure and unbiased RNG is critical for maintaining the security of ECDSA and similar protocols. The vulnerabilities related to poor pseudorandom number generators can theoretically be overcome by using **quantum RNGs**, which are true RNGs (Shi et al. 2022), providing the necessary security against bias-related attacks.

Quantum vulnerabilities

Quantum computers (Yeniaras and Cenk 2022; Martinis and Boixo 2019; Pednault et al. 2019; Yeniaras and Cenk 2021) are believed to have the potential to solve difficult computational problems, such as the integer factorization problem (Boudot et al. 2019) and DLP (Shor 1997; Rosen 2011), which form the security foundations of most cryptographic protocols. Shor's quantum factoring algorithm (Shor 1994, 1982) makes commonly used asymmetric cryptographic systems—such as RSA (Rivest et al. 1978a), Diffie–Hellman (Merkle 1978; Diffie and Hellman 1976), and elliptic curve Diffie–Hellman (Adrian et al. 2015; US National Security Agency 2016; NIST 2006; Certicom Research 2009; NSA 2009)—vulnerable to sufficiently powerful quantum computer attacks. In addition, Grover's algorithm (Grover 1996) enhances brute-force attacks by considerably reducing the number of operations needed to search for private keys, as well as to find pre-images and collisions in hash functions. These cryptographic algorithms are essential for securing sensitive data, such as governmental and military information, emails, and financial data (such as blockchain transactions and wallets). Compromising these would have serious consequences for digital security and privacy. As discussed in section Cryptographic Vulnerabilities, many blockchain systems employ DLP-based digital signature algorithms such as ECDSA, EdDSA, and RSA, all of which are vulnerable to quantum attacks in the near future. Consequently, research and investment in quantum computing have recently surged across various sectors in, driving efforts to develop reliable quantum-resistant cryptographic protocols. In section PQC and quantum-safe blockchain we discuss quantum-resistant cryptographic alternatives that can replace ECDSA, EdDSA, or RSA in blockchain

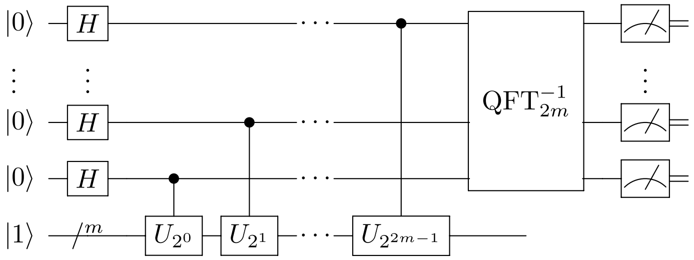

Fig. 6 Quantum circuit design for period finding (Hwang et al. 2022)

systems to mitigate the risks of quantum attacks. These quantum algorithms are briefly described below.

Shor's Algorithm: Shor's algorithm (Shor 1994, 1982) is a quantum integer factorization algorithm that considerably outperforms its classical counterpart. Compared to Shor's algorithm, the classical one has an exponentially higher time complexity. Shor's algorithm closely resembles the classical algorithm but replaces one step with a quantum algorithm. Given an integer $N = p.q$, where p and q are prime numbers, the classical method requires $\sqrt{N}$ trials to find p or q. This method becomes cumbersome for large N (e.g., $N = 2^k$, requiring $e^{(k/2)\ln 2}$ trials). Instead, Shor's algorithm proceeds as follows:

Step 1. Select a random integer $n \leq N$ and use the Euclidean algorithm to calculate the greatest common divisor $gcd(n, N)$. If $gcd(n, N) \neq 1$, then n is a factor of N (either $n = p$ or $n = q$).

Step 2 (Quantum part). If $gcd(n, N) = 1$, define a function $h : N \mapsto N$ such that $x \mapsto n^x \mod N$. Then find the **order** or **period** T of n which is the smallest integer such that $n^T \equiv 1 \mod N$. This step is exponential in time using classical algorithm but can be performed in polynomial time with Shor's quantum algorithm. The quantum part is only used for this step; all subsequent steps are classical. The quantum parts of this step works as follows:

Choose an integer m such that $N^2 \leq 2^m \leq 2N^2$, and define $V = 2^m$. Let $h_v : V_m \rightarrow V_m$ with $x \mapsto n^x$ where $V_m = \{0, 1, ..., V - 1\}$.

Step 2.1. Initialize two quantum registers r_1 and r_2, each with m qubits, in the state:

$$|\phi_0\rangle = |r_1\rangle|r_2\rangle = |00...0\rangle|00...0\rangle$$

Step 2.2. Apply QFT to the first register:

$$|\phi_0\rangle = |0\rangle|0\rangle \mapsto |\phi_1\rangle = (1/\sqrt{V}) \sum_{x=0}^{V-1} |x\rangle|0\rangle$$

The first register is now in a superposition of all states $|x\rangle$, where $0 \leq x \leq V - 1$.

Step 2.3. Assume that the unitary gate interprets the function h_v as $U_{h_v}|x\rangle|0\rangle = |x\rangle|h_v(x)\rangle$. Apply the unitary gate in Step 2.2 to obtain

$$U_{h_v}|\phi_1\rangle = |\phi_2\rangle \equiv (1/\sqrt{V}) \sum_{x=0}^{V-1} |x\rangle|h_v(x)\rangle,$$

which demonstrates that the two registers are entangled.

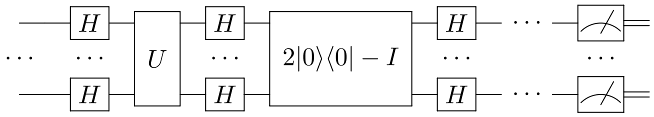

Fig. 7 Quantum circuit design for one step of Grover's algorithm

Step 2.4. Applying QFT to $|r_1\rangle$ yields

$$
\begin{aligned}
|\phi_3\rangle =&(\mathcal{F} \otimes I)|\phi_2\rangle = (1/\sqrt{V}) \sum_{x=0}^{V-1} \sum_{y=0}^{V-1} \omega_m^{-xy} |y\rangle |h_\nu(x)\rangle \\
=&(1/\sqrt{V}) \sum_{y=0}^{V-1} |y\rangle |\psi(y)\rangle = (1/\sqrt{V}) \sum_{y=0}^{V-1} \| |\psi(y)\rangle \| \cdot |y\rangle \frac{|\psi(y)\rangle}{\| |\psi(y)\rangle \|},
\end{aligned}
$$

where $|\psi(y)\rangle = \sum_{x=0}^{V-1} \omega_m^{-xy} |h_\nu(x)\rangle$.

Step 2.5. The measurement of $|r_1\rangle$ yields $y \in V_m$ with the probability $Prob(y) = \frac{\| |\psi(y)\rangle \|^2}{V^2}$. Simultaneously, the state collapses to $|y\rangle \frac{|\psi(y)\rangle}{\| |\psi(y)\rangle \|}$.

Step 2.6. Extract the order T from this final measurement we get in the previous step

Step 3. If T is odd, return to Step 1 and repeat until an even period T is found. When T is even, the following equality holds:

$$
(n^{T/2} - 1)(n^{T/2} + 1) = n^T - 1 \equiv 0 \mod N
$$

If $n^{T/2} + 1 \equiv 0 \mod N$, then $gcd(n^{T/2} - 1, N) = 1$. In this case, return to Step 1 and select another n. Assuming that $n^{T/2} - 1$ is not a multiple of N, if $n^{T/2} + 1 \not\equiv 0 \mod N$, then proceed to Step 4, as $n^{T/2} - 1$ includes either p or q as factors.

Step 4. Either p or q is equal to $gcd((n^{T/2} - 1, N)$, and the factorization is complete.

Figure 6 presents a visualization of the period-finding circuit design used in Shor's algorithm.

In 2001, a team at IBM implemented Shor's algorithm on a quantum computer consisting of 7 qubits (Amico et al. 2019), successfully factoring the number 15 into its prime factors, 3 and 5. The number of qubits required for Shor's factoring algorithm depends on the size of the number being factorized. Generally, Shor's algorithm requires approximately $2n$ qubits to efficiently factorize an n-bit number. However, the precise number of qubits can vary depending on the implementation details and optimization methods employed. For example, to efficiently factorize a 2,048-bit RSA modulus—widely utilized component in modern cryptography—would typically necessitate approximately 4,096 qubits. Quantum computers are currently capable of factoring large numbers relevant to cryptography have not been realized. Nevertheless, with rapid advances in quantum computing, this may become possible within the next few decades. Therefore, it is critical to be invested in research and development of PQC algorithms and transition from classical cryptographic algorithms to post-quantum cryptography in the interim.

Grover's algorithm Grover's algorithm (Grover 1996) is a quantum algorithm designed to solve the unsorted search problem. This algorithm provides quadratic speedup over classical algorithms. In classical computing, searching an unsorted database typically requires a linear search with time complexity of $O(N)$. In contrast, Grover's algorithm obtains the fastest possible search time for an unsorted database with a time complexity of $O(\sqrt{N})$. The basic steps of Grover's algorithm are as follows:

Step 1. Choose a random value to search for among the qubits.
Step 2. Apply the H-gate to create a superposition state across all the qubits:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

Step 3. Create an oracle that alters the amplitude of the target object by flipping it.
Step 4. Build the diffuser to perform an inversion operation around the mean:

$$U_s = 2|s\rangle\langle s|| - I$$

Execute Grover's iterations (Steps 3 and 4) $t(N)$ times.
Step 5. Finally, measure the resulting quantum state in the computational basis and compare the results with values in the database to identify the target.

Fig. 7 presents the circuit design for one step of Grover's algorithm.

Grover's algorithm provides considerable asymptotic speedup for various brute-force attacks on symmetric-key cryptography, including collision and pre-image attacks. To mitigate the potential effect of Grover's algorithm on cryptography, various strategies can be implemented. One approach is to increase the key length of symmetric key encryption algorithms. Doubling the key length maintains the security level against quantum attacks. For instance, while a 128-bit key is considered secure against classical attacks, a 256-bit key is recommended to counter Grover's algorithm. Another approach involves adopting PQC algorithms. These algorithms are explicitly designed to resist attacks from both classical and quantum computers. Numerous PQC schemes are presently under development and standardization to ensure the long-term security of encrypted data. In addition, quantum key distribution (QKD) (Jasim et al. 2015; Gyongyosi et al. 2019; Sharma et al. 2019) offers a cryptographic solution based on quantum mechanics principles for secure encryption key distribution. QKD establishes secure encryption keys while also detecting potential eavesdropping attempts.

PQC and quantum-safe blockchain

(PQC) involves research and development into cryptographic algorithms that can withstand quantum computer attacks. As quantum computing advances, this technology poses a threat to many existing cryptographic algorithms. Therefore, it is increasingly important to develop PQC algorithms that provide long-term security. (NIST started the PQC standardization process in 2016 to evaluate and standardize PQC algorithms. This round comprises several competitive rounds in which participants submit their PQC algorithms for comparison and evaluation. Their algorithms are assessed from several perspectives, such as security vulnerabilities and efficiency. In July 2022, NIST

(Alagic et al. 2020) announced the progression of 17 PQC algorithms from the original pool of 69 submissions to the third round of the PQC standardization process. The third round is expected to continue through 2023 and beyond, with the final selection of standardized algorithms being announced in coming years. Standardized algorithms include public-key encryption, key-establishment, and digital signature algorithms.

The PQC algorithms submitted to NIST can be divided into five categories based on their underlying mathematically difficult problem, which ensures quantum security for certain input sizes. These five quantum-resistant approaches are listed below, along with examples:

- **Lattice-based algorithms:** The security of lattice-based cryptography is based on the difficulty of solving problems such as the shortest vector problem (SVP), closest vector problem, shortest independent vector problem, learning with errors, ring learning with errors, and module learning with errors problems. These problems are considered quantum secure in a high-dimensional lattice. Examples of lattice-based NIST candidates include Saber, CRYSTALS-Kyber, CRYSTALS-Dilithium, New Hope, Frodo KEM, NTRU, and NTRU Prime (Alagic et al. 2020; Bernstein et al. 2017, 2019). Another lattice-based algorithm, independent of the NIST candidates, is the bimodal lattice signature scheme (BLISS). This scheme provides resistance to classical and quantum computer attacks. In addition, the scheme employs a post-quantum digital signature scheme based on a short integer solution and learning with error problems in the lattices. These problems are difficult to solve by both classical and quantum computers, making BLISS a potential candidate for post-quantum digital signature applications.
- **Code-based algorithms**: The security of code-based PQC algorithms is based on the computational infeasibility of decoding specific linear error-correcting codes, which are used to protect data from transmission errors. Code-based NIST PQC candidates include BIKE, Classic McEllice, and HQC.
- **Hash-based algorithms:** Hash-based PQC algorithms provide security based on the difficulty of finding a collision, which involves identifying two distinct inputs that produce the same hash output. This problem remains challenging even for quantum computers. Hash-based signatures are categorized into two groups (Buchmann et al. 2009): hash-based one-time signatures (e.g., Lamport 2016 and Merkle 1990)

Table 7 NIST PQC third-round competition candidates and alternatives

Type	Round 3 main candidates		Round 3 alternative candidates	
	Algorithm	**Category**	**Algorithm**	**Category**
Key encapsulation mechanisms	NTRU	Lattice-based	NTRU Prime	Lattice-based
	Saber	Lattice-based	FrodoKEM	Lattice-based
	Crystals Kyber	Lattice-based	BIKE	Code-based
	Classical McEliece	Code-based	HQC	Code-based
			SIKE	Isogeny-based
Digital signature agorithms	Crystals Dilithium	Lattice-based	GeMMS	Multivariate-based
	Falcon	Lattice-based	Picnic	Hash-based
	Rainbow	Multivariate-based	Sphincs+	Hash-based

Table 8 First set of post-quantum cryptography standards announced by NIST (2022)

Key establishment standarts	Timeline	Digital signature algorithm standarts	Timeline
CRYSTALS-KYBER	2016-present	CRYSTALS-Dilithium	2016-present
		FALCON	2016-present
		SPHINCS+	2016-present

Table 9 Blockchain examples with quantum-resistant digital signature algorithms

Blockchain/coin/cryptocurrency	Quantum-resistant digital signature algorithm
QRL	XMSS
IOTA	WOTS (Winternitz one-time signature scheme)
Mochimo	WOTS (Winternitz one-time signature scheme)
Nexus	FALCON
Hcash	BLISS
Quantum Resistant Coin (QRC)	XMSS
QAN	XMSSMT (hybrid)
enQlave	XMSS

and those based on the Merkle signature scheme (MSS Merkle 1990). Various adaptations of MSS are discussed in Martos et al. (2021), including XMSS, XMSS-T, XNYSS, PICNIC, and SPHINCS$^+$ (Ciulei et al. 2022).

- **Supersingular Isogeny–Based Algorithms:** The security of supersingular isogeny–based PQC algorithms is rooted in the complexity of the isogeny problem, which involves determining the isogeny linking two elliptical curves. These algorithms assume that quantum computers cannot compute such isogenies, thereby providing a reliable foundation for their security. An example of such an algorithm is supersingular isogeny key encapsulation (SIKE)—a NIST PQC candidate. However, on August 5, 2022, Castryck and Decru published a preprint describing an efficient classical key recovery algorithm that breaks both (SIKE) and supersingular isogeny Diffie–Hellman. The preprint includes code demonstrating the algorithm's practicality. As a result, the SIKE team acknowledged that these algorithms are considered insecure and unsuitable for PQC [14].
- **Multivariate-based algorithms:** Multivariate-based PQC algorithms are built on the principle that solving systems of multivariate polynomial equations is difficult, even for quantum computers. This complexity makes multivariate-based PQC algorithms a promising candidate for PQC. Examples of multivariate-based algorithms include NIST candidates such as GeMSS and Rainbow.

Table 7 lists the third-round and alternative candidates for the NIST PQC competition, categorized by their underlying problem types.

After thorough deliberation in the third round of the NIST PQC standardization process, NIST identified four algorithms as candidates for standardization. In 2022, NIST announced the first set of PQC standards: Kyber, Dilithium, Falcon, and SPHINCS+

(NIST 2022). NIST has proposed that two main algorithms—CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium for digital signatures—be implemented for most use cases. Additionally, the signature schemes FALCON and SPHINCS+ have been selected for standardization (Table 8).

Considering that the NIST post-quantum standardization process began in 2016, the aforementioned algorithms have withstood various attacks over this period until 2022. However, this does not guarantee that there will not be successful attacks in the near future. For cryptographic algorithms, their security tends to increase with time as they face various cryptographic attacks, thereby gaining trust and maturity. Therefore, the subsequent key encapsulation mechanisms have been selected by NIST to progress to the fourth round: BIKE (public-key encryption/KEM), Classic McEliece, HQC, and SIKE. For a detailed comparative review of these post-quantum digital signature algorithms from the perspectives of efficiency, security, and size, one can refer to Fernández-Caramès and Fraga-Lamas (2020), which is a useful reference for those seeking to implement post-quantum algorithms for practical applications in cryptocurrencies or other secure digital platforms.

Furthermore, NIST issued a request for additional proposals for post-quantum signature algorithms (NIST 2023) to enhance their initial selection. By 2023, they received 50 submissions, 40 of which were considered suitable as first-round candidates for potential future standardization.

Quantum-resistant blockchain

Currently, several blockchain initiatives focus on developing solutions that are resistant to quantum computing attacks to ensure the long-term security of their networks. The construction of a cryptographically quantum-resistant blockchain requires the integration of a post-quantum digital signature algorithm and a hash function. A suitable post-quantum digital signature algorithm can be selected from those previously mentioned. An important finding presented by Bennett et al. (1997) highlights that quantum computing does not provide an exponential advantage for searching problems. Consequently, all symmetric encryption and hash algorithms remain secure against quantum attacks because performing brute-force searches for keys and finding collisions remains computationally infeasible in such scenarios (Ciulei et al. 2022).

In addition to studies listed in Table 9, several research papers propose alternative constructions of quantum-resistant blockchains as described below:

- In 2018, a quantum-resistant blockchain based on a generalization of the BLISS signature was proposed as a privacy-preserving, one-time linkable ring signature, providing ring confidential transactions in the blockchain (Torres et al. 2018), which is referred to as Lattice RingCT v1.0.
- Another study used quantum-resistant SPHINCS$^+$ signature algoritm for enhanced efficiency (Lucena et al. 2020).
- However, lattice cryptosystems face challenges due to the large size of public keys and signatures, which limit the number of transactions in each block of a blockchain. The large size can greatly reduces blockchain speed and performance. To address this

challenge, Zhang et al. (2021) proposed storing only the hash values of public keys and signatures in the blockchain while maintaining the complete contents of these values in the InterPlanetary File System. This approach greatly reduces the number of bytes required for each transaction. The authors also developed a Bitcoin exchange scheme to evaluate the performance of this quantum-resistant blockchain system.

- Another post-quantum blockchain proposal used the FALCON signature algorithm, which is considered time efficient with a smaller key size than other signature algorithms from the NIST PQC competition (Brindha et al. 2022).
- In 2018, Gao et al. proposed a cryptocurrency based on a post-quantum blockchain designed to withstand quantum computing attacks (Gao et al. 2018). However, their approach required a specialized blockchain and was incompatible with existing blockchains (Far et al. 2022).
- In 2020, Torres et al. presented a post-quantum linkable ring signature scheme that allowed auditors to sign confidential transactions in a distributed manner (Torres et al. 2020). Although their approach was innovative and promising, it was restricted by large signature sizes and communication overhead it produced (Far et al. 2022; Torres et al. 2020).
- In 2020, Shahid et al. proposed a distributed ledger designed for lightweight IoT devices used in financial transactions. Their approach employed hash-based one-time signatures that were quantum-attack resistant (Shahid et al. 2020).
- Li et al. proposed a lattice-based signature scheme for post-quantum blockchains (Li et al. 2019). Their approach involved using Bonsai Trees for key generation, thereby enhancing the system's cryptographic efficiency (Ciulei et al. 2022).
- Chen et al. proposed a lightweight, quantum-resistant blockchain for smart cities using an identity-based multivariate-quadratic signature scheme called ID-Rainbow for transaction security (Chen et al. 2021, 2019; Ciulei et al. 2022).
- A PoW scheme based on lattices was introduced, utilizing the difficulty of Hermite-SVP, a variation of the SVP, as a computational challenge (Behnia et al. 2022).

Notably, Far et al. (2022) introduced a method to transition non-quantum-resistant blockchains to quantum-resistant ones through a hard fork based on a Proof-of-Burn consensus. Therefore, instead of implementing an entirely new blockchain, the study proposes modifying an existing one to make it quantum-resistant.

Quantum-secure blockchain

Recently, there has been increasing interest in protecting blockchain against potential quantum computer attacks. Two primary approaches have emerged: quantum-resistant and quantum-secure (or quantum-safe) blockchains (Punathumkandi and Boscovic 2022). Quantum-resistant blockchain uses digital signature algorithms designed to withstand quantum computing threats. Notably, hash functions are inherently quantum-resistant with increased bit sizes; however, relying solely on quantum-resistant signature algorithms and strong hash functions is insufficient to address all quantum threats. Each layer in the blockchain bears its own set of security risks. The quantum-secure blockchain technology addresses quantum threats across all blockchain layers. The network layer, which is responsible for the interaction and communication between blockchain nodes, ensures the reliability of the network. Therefore, this layer will likely require the implementation of a quantum network in the future. The hardware layer, where nodes play a critical role, involves physical devices that connect to the network and participate in the blockchain consensus. To strengthen infrastructure security, limiting or preventing unauthorized node access is standard practice. Therefore, infrastructure upgrades are necessary to fully establish quantum-secure blockchains.

Quantum blockchain

Quantum blockchain is a distributed, encrypted database that uses the principles of quantum computing and quantum information theory to facilitate decentralization (Li et al. 2019), and is specifically designed to protect the security and integrity of blockchains against potential quantum computer-posed risks. Quantum computers can solve complex mathematical problems much faster than classical computers, potentially compromising the security of blockchain networks. To mitigate this risk, quantum blockchain incorporates sophisticated cryptographic methods, including QKD, quantum random number generation, quantum network channels, and quantum information theory, to protect the network and prevent malicious attacks. In addition, quantum blockchains may use quantum-resistant algorithms and protocols to realize enhanced security. Rajan et al. introduced a quantum blockchain scheme that uses entanglement in time (Rajan and Visser 2019; Li et al. 2019), a quantum phenomenon in which microscopic particles, such as photons, that have never interacted can still become entangled. Additional information on various quantum blockchain approaches and quantum bitcoin mining is provided in Ahubele and Musa (2022), Benkoczi et al. (2022), Yang et al. (2022a), Edwards et al. (2019), Wang et al. (2022), Iovane (2021).

Similar to traditional blockchains, quantum blockchains also exhibit decentralization. However, the key advantages of quantum blockchain are enhanced security and efficiency. Ensuring the security of a quantum blockchain is critical. QKD and quantum secure direct communication are two methods that can be employed to secure communication between nodes. These methods rely on quantum mechanics principles to authenticate the network and prevent unauthorized access (Punathumkandi and Boscovic 2022). To address vulnerabilities in digital signature algorithms, quantum blockchains implement quantum digital signature mechanisms (Punathumkandi and Boscovic 2022), which impart quantum security properties to the blockchain. This method ensures that quantum computers cannot compromise the security of quantum blockchains (Punathumkandi and Boscovic 2022).

Another characteristic of blockchain technology is its potential for high-speed transaction processing. The use of analog Hamiltonian optimizers can reduce transaction times, potentially accelerating the adoption of Bitcoin and other blockchain applications. In addition, integrating Grover's algorithm into the blockchain framework could enhance mining efficiency. However, those with access to universal quantum computers could have an unfair advantage in acquiring mining rewards until quantum technology become more widespread. As quantum technology becomes widely adopted, it may lead to situations where classical-computer users will be unable to compete with quantum-powered mining, leaving classical hardware behind. In general, quantum blockchain offers advantages over traditional blockchain, particularly in security, efficiency, and performance (Punathumkandi and Boscovic 2022).

Advantages and limitations of implementing quantum blockchain

Implementing blockchain systems on quantum computers through quantum programming offers significant benefits, such as enhanced computational efficiency, improved security mechanisms, and innovative applications leveraging quantum properties. Quantum computers possess superior capabilities for specific tasks, enabling blockchain systems to execute complex operations faster and improve consensus among participants regarding the validity and sequence of transactions (Preskill 2018b; Seet and Griffin 2019; Gacon 2024). Quantum blockchain systems employ quantum mechanics principles, such as quantum cryptography, particularly QKD, to enhance transaction security (Alagic et al. 2020; Diamanti et al. 2016). By using quantum phenomena like entanglement and superposition, quantum blockchain systems introduce novel consensus mechanisms, ensuring faster and safer agreement while protecting against potential quantum attacks (Seet and Griffin 2019; Yang et al. 2022b). In addition, quantum computing offers transformative potential for data analysis, particularly in finance, by effectively processing large datasets, thereby improving decision-making processes (Orús et al. 2019; Kaul et al. 2018; Weinstein 2022). Quantum blockchains also unlock opportunities for specialized applications using quantum abilities such as machine learning and optimization, to develop innovative solutions in fields like finance, healthcare, and logistics (Umer and Sharif 2022; Mugel et al. 2020; Srivastava 2023; Bentley et al. 2022). Moreover, integrating quantum computing into blockchain will prepare for the future of quantum technology, ensuring the security of sensitive data against potential threats posed by advanced quantum computers (Alagic et al. 2020; Punathumkandi and Boscovic 2022). However, realizing these benefits requires overcoming challenges, including limitations in quantum hardware, such as qubit stability and scalability, advancements in quantum programming languages, and the development of robust quantum algorithms tailored for blockchain applications.

Blockchain-based quantum computing faces numerous challenges because of its nascent stage of quantum computing. A major limitation is the need for quantum computers to have a specific number of qubits and extremely low error rates—requirements that are still under development and costly to achieve, leading to limited resource availability (Hull 2019). In addition, quantum programming differs considerably from traditional programming, demanding proficiency in specialized languages such as *Q#*, Qiskit, or Cirq, incorporating quantum mechanics phenomena of superposition and entanglement (Gay 2006). Another critical challenge lies in the incompatibility of traditional blockchain algorithms with quantum computers, which necessitates the development of new algorithms that can effectively use quantum capabilities (Rajan and Visser 2019; Seet and Griffin 2019; Torres et al. 2020). Furthermore, mitigating errors caused by factors such as noise and decoherence in quantum systems is both technically challenging and resource-intensive (Roffe 2019). Integrating quantum blockchains into traditional computing systems adds further complications, particularly in terms of ensuring secure communication and seamless data interchange (Wehner et al. 2018; Stephens et al. 2013). The lack of standardization in quantum programming also hinders the development of

Table 10 A categorization table of the works that are surveyed

Topic	Related work surveyed
Blockchain basics and real-world applications: cryptocurrencies, e-voting, smart contracts, IoT, NFT, consensus, PoW, PoS.	https://www.paypal.com, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, https://www.nasdaq.com, https://www.asx.com.au, https://www.powerpeers.nl, https://www.exergy.solutions, https://www.entrepreneur.com/money-finance/8-benefits-of-blockchain-to-industries-beyondcryptocurrency/306420, https://iot.ieee.org/definition.html, https://www.investopedia.com/terms/e/e-auction.asp, Baum et al. (2023), https://www.coindesk.com/what-are-non-fungible-tokens-nfts, Prewett et al. (2019), Ciulei et al. (2022); Chaum (1983), Back (2002), http://www.weidai.com/bmoney.txt, Nakamoto (2008), http://www.iota.org, https://en.wikipedia.org/wiki/Ethereum, Lamport et al. (1982)
Cryptographic Aspects of Blockchain: Digital Signature Algorithms, RSA, ECDSA, EdDSA	Rivest et al. (1978a), Boudot et al. (2019), Shor (1997); Rosen (2011)
Privacy Preserving Blockchains: Multi-Signatures, Threshold Signatures, Schnorr Multi-Signature, Ring Signatures, Blind Signatures, ZK Snarks, Bulletproofs	Yao (1982), Camenisch and Stadler (1997); Boldyreva (2003), Schnorr (1991); Maxwell et al. (2019), Rivest et al. (1978b), Rivest et al. (2001), Raikwar et al. (2019), van Saberhagen (2013); Wang et al. (2019); Bender et al. (2005); Fujisaki and Suzuki (2007); Feng et al. (2021), Ciulei et al. (2022); Heilman et al. (2016); Chaum (1982); Raikwar et al. (2019), [13], Bitansky et al. (2011); Ben-Sasson et al. (2014), Shor (1997); Rosen (2011), Kearney and Perez-Delgado (2021), [82], Bünz et al. (2018)
Security Vulnerabilities of Blockchain: Digital Signatures Based, Hash Based, Random Number Generator Based	Dasgupta et al. (2019); Wang et al. (2019); Li et al. (2017); Cain and Hosseinian-Far (2020), Bernstein and Lange (2014), University of Stanford (2011), Ferguson and Schneier (2003), Stevens et al. (2017), Breitner and Heninger (2019), Shi et al. (2022)
Quantum-computing-based security vulnerabilities	Yeniaras and Cenk (2022); Martinis and Boixo (2019); Pednault et al. (2019); Yeniaras and Cenk (2021), Boudot et al. (2019), Shor (1997); Rosen (2011), Shor (1994, 1982), Rivest et al. (1978a), Merkle (1978); Diffie and Hellman (1976), Adrian et al. (2015); US National Security Agency (2016); NIST (2006); Certicom Research (2009); NSA (2009), Amico et al. (2019), Grover (1996)
Post-quantum cryptography, Quantum-resistant blockchain, Quantum Bitcoin Mining, Quantum Key Distribution, and Quantum-secure blockchain	Alagic et al. (2020), Bernstein et al. (2017, 2019), Buchmann et al. (2009), Jasim et al. (2015), Lamport (2016), Merkle (1990), Martos et al. (2021), Ciulei et al. (2022), [14], Fernández-Caramès and Fraga-Lamas (2020), Bennett et al. (1997), Torres et al. (2018), Lucena et al. (2020), Zhang et al. (2021), Brindha et al. (2022), Gao et al. (2018), Far et al. (2022), Torres et al. (2020), Shahid et al. (2020), Li et al. (2019), Chen et al. (2021, 2019), Behnia et al. (2022), Punathumkandi and Boscovic (2022), Li et al. (2019), Rajan and Visser (2019), Ahubele and Musa (2022); Benkoczi et al. (2022); Yang et al. (2022a); Edwards et al. (2019); Wang et al. (2022); Iovane (2021)

reliable and interoperable quantum blockchain systems (Varga et al. 2024; Gay 2006). Despite these challenges, ongoing research continues to address them. Improvements in quantum computing resources, programming frameworks, and algorithm development are expected to facilitate the integration of quantum blockchains into financial systems. A summary of the relevant research papers is presented in Table 10.

In light of the points discussed above, the adoption of quantum cryptocurrencies and blockchains in finance is a promising research direction. However, practical implementation and widespread adoption remain in their infancy, as no fully quantum blockchain system exists due to the abovementioned limitations and challenges. Current research is focused on investigating the theoretical aspects of quantum blockchains and exploring how quantum computing can improve the scalability, security, and functionality of blockchain systems. While researchers have successfully implemented quantum-resistant blockchains, the NIST competition for quantum-secure cryptographic algorithms is ongoing, and the long-term security of quantum-resistant digital signature algorithms remains unproven. Over time, potential attacks on these cryptographic systems can affect the reliability of quantum-resistant ledgers. Existing quantum-resistant ledgers provide secure transactions; however, their future resilience is uncertain. Further discussions are warranted on topics such as the development of quantum-resistant encryption methods, the integration of quantum technologies into existing financial systems, and potential regulatory concerns regarding quantum computing in finance. However, ongoing research and development in this field indicate high potential for future advances in blockchain technology. With continued efforts, quantum-resistant blockchains can revolutionize various industries. Therefore, progress in both quantum computing and blockchain technologies is crucial to unlock their full potential, particularly in the financial sector.

Conclusion and future work

The research in portfolio optimization and quantum computing applications is gaining momentum, with increasing interest from banks and quantum computing companies due to their potential for substantial economic benefits. The current research focuses on developing algorithms tailored for NISQ era, aiming to efficiently address challenges such as local minima, scaling issues, and the combinatorial, convex, or nonconvex natures of problems arising from various investor constraints. Algorithms that can handle many constraints are particularly valuable when tackling real-world problems. Although quantum computing offers promising advantages in terms of optimization and machine learning, it may not improve Monte Carlo methods in the NISQ era. These quantum algorithms typically require several qubits and deep circuits. Nonetheless, several strategies are being explored to mitigate these requirements. The use of quantum algorithms in the valuation of derivatives is particularly important for large institutions, particularly those in investment banking, which handle more complex derivatives. The potential to accelerate risk calculations through quantum algorithms could have far-reaching implications, benefiting banks across the financial sector. Therefore, research in this field is expected to intensify over the next few years. In this review, we also discussed recent studies on quantum applications for fraud detection. Quantum computing has demonstrated the potential to revolutionize fraud detection by enabling faster and more efficient analysis of large datasets. While quantum computing is still in its early stages, with challenges such as the development of reliable quantum hardware and algorithms to be addressed, the use of quantum computing in fraud detection appears promising. As research and development progress, quantum computing is expected to play an increasingly important role in preventing and detecting fraud in various industries. Our analysis of quantum algorithms for optimization, machine learning, and simulation revealed that certain quantum algorithms have advanced beyond the proof-of-principle stage. It is now essential to develop a business case for their application in finance.

Given the wide variety of existing solution algorithms, it is crucial to apply quantum algorithms when traditional methods reach their limits or become inefficient. The primary limitation in the current applications of quantum computing is the number of available qubits and their errors rate, with the latter especially limiting the depth of the corresponding quantum circuits. However, it is expected that progress will be made in both aspects in the upcoming years. Therefore, it is reasonable to begin preparing for these developments now. In this study, we also discussed some of the most important fintech concepts—blockchain and cryptocurrencies—from the perspective of quantum computing. Quantum advancements, particularly Shor's factoring algorithm and Grover's search algorithm, present security risks to current cryptographic protocols. While a sufficiently efficient quantum computer has not yet been developed to execute these attacks, the threat is imminent. The "store now, decrypt later" strategy means that even today's sensitive information could be vulnerable to future quantum attacks on blockchain-based financial systems. We not only addressed the quantum computing-related vulnerabilities in blockchain but also reviewed several non-quantum security threats. This comprehensive overview of blockchain security–related studies is intended to guide researchers, fintech developers, and entrepreneurs. To mitigate quantum-related risks, we also explored countermeasures such as PQC and quantum-resistant blockchain technologies, along with the post-quantum digital signature algorithms introduced by NIST's PQC Standardization Process, which began in 2016. Additionally, a detailed analysis of both quantum-resistant and privacy-preserving blockchain applications are provided. We examined systems using zero-knowledge proof techniques, such as ZK-SNARKs, threshold signatures, multisignatures, ring signatures, bulletproofs, and blind signatures. After clarifying the difference between quantum-resistant and quantum-secure blockchains, we reviewed the latest research on quantum blockchain and quantum mining. Quantum computing has the potential to enhance efficiency in Bitcoin mining and can enable the development of true random number generators, which would enhance the randomness in current pseudorandom number generators. We also addressed security concerns related to hash functions, which are essential building blocks of blockchain systems.

Our comprehensive analysis of existing quantum-resistant blockchains and cryptocurrencies, as well as the ongoing PQC competition, offers valuable research insights. These insights span from theoretical foundations to practical applications in financial sector, making them relevant for curious readers, aspiring developers, cryptoasset investors, and enthusiasts alike. Our review also highlights the importance of privacy when choosing cryptocurrencies with *privacy-preserving* transactions. In today's digitalized world, *privacy* is a critical factor when selecting appropriate crypto-assets for investors. Furthermore, we discuss efficiency in terms of time and space by referencing the most relevant sources in the literature for readers interested in these aspects. This discussion is crucial for the development of cryptocurrencies and the related regulatory challenges. For instance, privacy-preserving stock exchange systems with post-quantum secure capabilities require regulatory frameworks by governing powers to prevent unfair stock exchanges between parties. In addition, we analyzed the limitations of implementing a fully quantum blockchain or quantum cryptocurrency system. Although quantum blockchain is still in its infancy and there is no established quantum blockchain system yet, we addressed the challenges from all possible perspectives, providing a roadmap for researchers and enthusiasts by offering realistic yet innovative expectations and applications.

Lastly, we have addressed the most prominent applications of quantum computing in finance, reviewing the latest studies in the field, presenting a comprehensive state-of-the-art survey. This analysis is a valuable resource for researchers delving into emerging quantum technologies, while also offering practical insights for fintech developers, banks, and financial institutions aiming to launch new projects in this transformative field.

Future work

Improving the efficiency of digital signature algorithms and identifying the most suitable cryptographic protocols to construct the fastest and most secure quantum-resistant cryptocurrency challenges remain open. To address the tradeoff between security and space–time complexity, researchers are actively proposing new quantum-resistant tokens that surpass the security and efficiency of currently implemented solutions. Another pressing issue is the development of quantum blockchains with robust and adaptable network infrastructures. This endeavor will likely require interdisciplinary collaboration among experts in cybersecurity, networking, hardware, software development, and quantum physics.

Furthermore, future research can design quantum and post-quantum secure privacy-preserving systems for financial activities, including stock exchanges, online banking systems, and cryptocurrencies. These systems require the design and implementation of quantum or post-quantum secure protocols, such as multiparty computation, multisignature or threshold signatures, and quantum differential privacy. These areas are attracting increasing interest because *privacy* in financial transactions is a critical concern in the digital era.

In addition, hybrid quantum–classical approaches in portfolio optimization and quantum machine learning are promising areas for future exploration. Combining quantum computing with classical techniques, these approaches exploit the strengths of both paradigms. For example, developing quantum algorithms for dynamic portfolio optimization can enable real-time adaptation to changing market conditions and investment objectives. Similarly, more efficient quantum algorithms for risk assessment and stress testing can offer more accurate and timely results than classical methods. From a financial perspective, there is an urgent need to study the economic implications of improved optimization, simulation, and machine learning processes enabled by quantum algorithms. For instance, how might financial company business models evolve when current risk calculations are completed almost instantaneously? Historical technological advancements, such as artificial intelligence and cloud computing, have shown that what initially appears to be purely technical improvement can lead to profound and long-term economic influences.

Acknowledgements
Not applicable

Author contributions
The authors contributed equally to the review. All authors read and approved the final manuscript.

Funding
The work of Gerhard Hellstern is partly funded by the Ministry of Economic Affairs, Labour and Tourism Baden-Württemberg in the frame of the Competence Center Quantum Computing Baden-Württemberg (QORA II).

Data availability and materials
Not applicable.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The author declare that they have no Conflict of interest.

Received: 27 June 2023 Accepted: 6 January 2025
Published online: 26 February 2025

References

https://www.paypal.com
https://www.entrepreneur.com/money-finance/8-benefits-of-blockchain-to-industries-beyond-cryptocurrency/306420
https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
https://www.nasdaq.com
https://www.asx.com.au
https://www.powerpeers.nl
https://www.exergy.solutions
https://iot.ieee.org/definition.html
https://www.coindesk.com/what-are-non-fungible-tokens-nfts
http://www.weidai.com/bmoney.txt
http://www.iota.org
https://en.wikipedia.org/wiki/Ethereum
https://z.cash/technology/zksnarks/
https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf
https://www.investopedia.com/terms/e/e-auction.asp
Aaronson Scott, Rall Patrick (2020) Quantum approximate counting, simplified. In Symposium on Simplicity in Algorithms, pages 24–32. Society for Industrial and Applied Mathematics
Adrian D, Bhargavan K, Durumeric Z, Gaudry P, Green M, Halderman JA, Heninger N, Springall D, Thomé E, Valenta L, VanderSloot B, Wustrow E, Zanella-Béguelin S, Zimmermann P (2015) Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. Association for Computing Machinery, pp. 5–17
Ahubele B, Musa M (2022) Towards a scalable and secure blockchain based on post-quantum cryptography. IJARCCE 11:07
Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Kelsey J, Liu Y, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Smith-Tonel D (2020) Status report on the second round of the nist post-quantum cryptography standardization process, july 2020. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf
Albareti Franco D, Ankenbrand Thomas, Bieri Denis, Hänggi Esther, Lötscher Damian, Stettler Stefan, Schöngens Marcel (2022) A structured survey of quantum computing for the financial industry
Alcazar Javier, Alcazar Javier, Cadarso Andrea, Cadarso Andrea, Katabarwa Amara, Mauri Marta, Mauri Marta, Peropadre Borja, Peropadre Borja, Wang Guoming, Wang Guoming, Cao Yudong, Cao Yudong (2022) Quantum algorithm for credit valuation adjustments. New J Phys
Back A (2002) Hashcash - a denial of service counter-measure. 09
Baheri B, Guan Q, Chaudhary V, Li A (2022) Quantum noise in the flow of time: a temporal study of the noise in quantum computers. In: 2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS), pp. 1–5
Baker JS, Radha SK (2022) Wasserstein solution quality and the quantum approximate optimization algorithm: a portfolio optimization case study
Barends R, Shabani A, Lamata L, Kelly J, Mezzacapo A, Las Heras U, Babbush R, Fowler AG, Campbell B, Yu Chen Z, Chen B, Chiaro A, Dunsworth E, Jeffrey E, Lucero A, Megrant JY, Mutus M, Neeley C, Neill PJJ, O'Malley C, Quintana P, Roushan D, Sank A, Vainsencher J, Wenner TC, White E, Solano HN, Martinis JM (2016) Digitized adiabatic quantum computing with a superconducting circuit. Nature 534(7606):222–226
Barletta A (2023) An introduction to quantum mechanics ... for those who dwell in the macroscopic world
Baum Carsten, yu Chiang James Hsin, David Bernardo, Frederiksen Tore Kasper (2023) Sok: Privacy-enhancing technologies in finance. Cryptology ePrint Archive, Paper 2023/122, https://eprint.iacr.org/2023/122

Behnia R, Postlethwaite EW, Ozmen MO, Yavuz AA(2022) Lattice-based proof-of-work for post-quantum blockchains. In Joaquin Garcia-Alfaro, Jose Luis Muñoz-Tapia, Guillermo Navarro-Arribas, and Miguel Soriano, editors, Data Privacy Management, Cryptocurrencies and Blockchain Technology, pages 310–318, Cham, Springer International Publishing

Bellman R (1956) Dynamic programming and Lagrange multipliers. Proc Natl Acad Sci 42(10):767–769

Ben-SE, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M (2014) Zerocash: decentralized anonymous payments from bitcoin. In 2014 IEEE Symposium on Security and Privacy, pages 459–474. IEEE

Bender A, Katz J, Morselli R (2005) Ring signatures: stronger definitions, and constructions without random oracles. https://eprint.iacr.org/2005/304

Benkoczi R, Gaur D, Nagy N, Nagy M, Hossain S (2022) Quantum bitcoin mining. Entropy (Basel) 24(3):323

Bennett CH, Bernstein E, Brassard G, Vazirani U (1997) Strengths and weaknesses of quantum computing. SIAM J Comput 26(5):1510–1523

Bentley Christopher DB, Marsh S, Carvalho André RR, Kilby P, Biercuk MJ (2022) Quantum computing for transport optimization

Bernstein DJ, Chuengsatiansup C, Lange T, van Vredendaal C (2017) Ntru prime. NIST Post-Quantum Cryptography Standardization Process-Round-1, https://ntruprime.cr.yp.to/nist/ntruprime-20171130.pdf

Bernstein DJ, Chuengsatiansup C, Lange T, van Vredendaal C (2019) Ntru prime. NIST Post-Quantum Cryptography Standardization Process-Round-2, https://ntruprime.cr.yp.to/nist/ntruprime-20190330.pdf

Bernstein DJ, Lange T(2014) SafeCurves: Choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to/, Accessed: 2023-04-06

Bitansky N, Canetti R, Chiesa A, Tromer E (2011) From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. Cryptol ePrint Archive 2011:443

Boldyreva A (2003) Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. pp. 31–46, 01

Boudot F, Gaudry P, Guillevic A, Heninger N, Thomé E, Zimmermann P (2019) https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2019-December/001139.html

Bouland Adam, Bouland Adam, van Dam Wim, van Dam Wim, van Dam Wim, Joorati Hamed, Kerenidis Iordanis, Prakash Anupam (2020) Prospects and challenges of quantum finance. arXiv: Computational Finance

Brandhofer S, Braun D, Dehn V, Hellstern G, Hüls M, Ji Y, Polian I, Bhatia AS, Wellens T (2022) Benchmarking the performance of portfolio optimization with qaoa. Quantum Inf Process 22(1):25

Brassard G, Høyer Peter, Hoyer PF, Mosca M, Tapp A (2000) Quantum amplitude amplification and estimation. 53-74, Contemp. Math., 305, Amer. Math. Soc., Providence, RI, 2002, 2000

Braun MC, Decker T, Hegemann N, Kerstan SF (2022) Error resilient quantum amplitude estimation from parallel quantum phase estimation

Breitner J, Heninger N (2019) Biased Nonce Sense: lattice attacks against weak ECDSA signatures in cryptocurrencies, pages 3–20. 09

Brindha S, Kamatchi TP, Ram RVH, Balaji PSG, Karthikeyan T (2022) Quantum resistant blockchain using post-quantum cryptography. Int J Appl Innov Eng Manag (IJAIEM) 11(5):219–229

Brown EG, Goktas O, Tham WK (2020) Quantum amplitude estimation in the presence of noise

Buchmann J, Dahmen E, Szydlo M (2009) Hash-based Digital Signature Schemes, pp. 35–93. 02

Bünz B, Bootle J, Boneh D, Poelstra A, Wuille P, Maxwell G (2018) Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE Symposium on Security and Privacy (SP), pp. 315–334

Cain TW, Hosseinian-Far A (2020) A systematic review of blockchain security. IEEE Access 8:175239–175253

Camenisch J, Stadler M (1997) Efficient group signature schemes for large groups. In: Kaliski Burton S (ed), Advances in cryptology — CRYPTO '97, pages 410–424, Berlin, Heidelberg, Springer Berlin Heidelberg

Campos Roberto, Casares Pablo AM, Martin-Delgado MA (2022) Quantum metropolis solver: a quantum walks approach to optimization problems

Canabarro A, Mendonça TM, Nery R, Moreno G, Albino, AS, de Jesus GF, Chaves R (2022) Quantum finance: a tutorial on quantum computing applied to the financial market

Cerezo M, Arrasmith A, Babbush R, Benjamin SC, Endo S, Fujii K, McClean JR, Mitarai K, Yuan X, Cincio L, Coles PJ (2021) Variational quantum algorithms. Nature Reviews Physics 3(9):625–644

Certo S, Pham AD, Beaulieu D (2022) Comparing classical-quantum portfolio optimization with enhanced constraints

Certicom Research (2009) Standards for efficient cryptography, sec 1: Elliptic curve cryptography, version 2.0. https://www.secg.org/sec1-v2.pdf

Chakrabarti S, Krishnakumar R, Mazzola G, Stamatopoulos N, Woerner S, Zeng WJ (2021) A threshold for quantum advantage in derivative pricing. Quantum 5:463

Chaum D (1982) Blind signatures for untraceable payments. In annual international cryptology conference

Chaum D (1983) Blind signatures for untraceable payments. In: Chaum D, Rivest RL, Sherman AT (eds) Adv Cryptol. Springer US, Boston, MA, pp 199–203

Chen J, Gan W, Hu M, Chen CM (2021) On the construction of a post-quantum blockchain. In 2021 IEEE conference on dependable and secure computing (DSC), pages 1–8

Chen J, Ling J, Ning J, Ding J (2019) Identity-based signature schemes for multivariate public key cryptosystems. Comput J 62:1132–1147, 08

Chou Y-H, Jiang Y-C, Hsu Y-R, Kuo S-Y, Kuo S-Y (2022) A weighted portfolio optimization model based on the trend ratio, emotion index, and angqts. IEEE Trans Emerg Topics Comput Intell 6(4):867–882

Ciulei A-T, Cretu M, Simion E (2022) Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective. IACR Cryptol ePrint Arch 2022:26

Cohen J, Alexander C (2020) Picking efficient portfolios from 3171 us common stocks with new quantum and classical solvers

Cohen J, Khan A, Alexander C (2020) Portfolio optimization of 40 stocks using the dwave quantum annealer

Cohen J, Khan A, Alexander C (2020) Portfolio optimization of 60 stocks using classical and quantum algorithms

NSA Suite B Cryptography (2009) Suit b implementers' guide to nist sp 800-56a. https://web.archive.org/web/20160306033416/http://www.nsa.gov/ia/_files/SuiteB_Implementer_G-113808.pdf
Dasgupta D, Shrein J, Gupta KD (2019) A survey of blockchain from security perspective. J Bank Financ Technol, 3, 01
Diamanti E, Lo HK, Qi BYZ (2016) Practical challenges in quantum key distribution. NPJ Quantum Inf, 2(1)
Diffie W, Hellman M (1976) New directions in cryptography. IEEE Trans Inf Theory 22(6):644–654
Dri EA, Giusto E, Aita A, Montrucchio B (2022) Towards practical quantum credit risk analysis. J Phys: Conf Ser
Durand D (1960) The american economic review, 50(1):234–236, 2023/04/07/ 1960. Full publication date
Edwards M, Mashatan A, Ghose S (2019) A review of quantum and hybrid quantum / classical blockchain protocols. 12
Egger DJ, Gambella C, Marecek J, Marecek J, McFaddin S, Mevissen M, Raymond R, Simonetto A, Woerner S, Yndurain E (2020) Quantum computing for finance: State-of-the-art and future prospects. null
Egger DJ, Gutierrez RG, Gutiérrez Ricardo, Mestre JC, Mestre JC, Woerner S (2020) Credit risk analysis using quantum computers. IEEE Trans Comput
Elsokkary N, Khan FS, La Torre Davide, Humble T, Gottlieb J (2017) Financial portfolio management using d-wave's quantum optimizer: The case of abu dhabi securities exchange
Far SB, Rad AI, Asaar MR (2022) Goodbye Bitcoin: a general framework for migrating to quantum-secure cryptocurrencies. 5
Farhi E, Goldstone J, Gutmann S (2014) A quantum approximate optimization algorithm
Fast E Cryptography behind the top 100 cryptocurrencies. http://ethanfast.com/top-crypto.html?fbclid=IwAR0 81BN9s7-gTc6zjuub7-2ofSYstRP1G3PoZBUaSHmXpCcRHNjwrqOfn4
Feng H, Liu J, Li D, Li Y-N, Wu Q (2021) Traceable ring signatures: general framework and post-quantum security. Des Codes Crypt 89:06
Ferguson N, Schneier B (2003) Pract Cryptography. John Wiley and amp; Sons Inc, USA
Fernández-Caramès TM, Fraga-Lamas P (2020) Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 8:21091–21116
Fuchs FG, Lye KO, Nilsen HM, Stasik AJ, Sartor G (2022) Constraint preserving mixers for the quantum approximate optimization algorithm. Algorithms 15(6):202
Fujisaki E, Suzuki K (2007) Traceable ring signature. In: Okamoto Tatsuaki, Wang Xiaoyun (eds), Public Key Cryptography – PKC 2007, pp. 181–200, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg
Gacon Julien S (2024) Scalable quantum algorithms for noisy quantum computers
Gao Y-L, Chen X-B, Chen Y-L, Sun Y, Niu X-X, Yang Y-X (2018) A secure cryptocurrency scheme based on post-quantum blockchain. IEEE Access 6:27205–27213
Gay SJ (2006) Quantum programming languages: survey and bibliography. Math Struct Comput Sci 16:581–600
Gkillas K, Longin F (2018) Is bitcoin the new digital gold? evidence from extreme price movements in financial markets. SSRN Electron J, 01
Grinko D, Gacon J, Zoufal C, Woerner S (2019) Iterative quantum amplitude estimation. NPJ Quantum Inf
Grossi M, Ibrahim N, Radescu V, Loredo R, Voigt K, von Altrock C, Rudnik A (2022) Mixed quantum-classical method for fraud detection with quantum feature selection. IEEE Trans Quantum Eng 3:1–12
Grover LK (1996) A Fast Quantum Mechanical Algorithm for Database Search. Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, pp. 212–219
Grover LK (1996) A fast quantum mechanical algorithm for database search
Guéry-Odelin D, Ruschhaupt A, Kiely A, Torrontegui E, Martínez-Garaot S, Muga JG (2019) Shortcuts to adiabaticity: Concepts, methods, and applications. Reviews of Modern Physics, 91(4), oct 2019
Gunjan A, Bhattacharyya S (2022) A brief review of portfolio optimization techniques. Artific Intell Rev
Gyongyosi L, Bacsardi L, Imre S (2019) A survey on quantum key distribution. InfocommunJ, pp. 14–21, 01
Gómez Andrés, Leitao Álvaro, Manzano Alberto, Musso Daniele, Nogueiras María R, Ordóñez Gustavo, Vázquez Carlos (2022) A survey on quantum computational finance for derivatives pricing and var. Archives Comput Methods Eng
Han H, Shiwakoti RK, Jarvis R, Mordi C, Botchie D (2023) Accounting and auditing with blockchain technology and artificial intelligence: a literature review. Int J Account Inf Syst 48:100598
Han JY, Rebentrost P (2022) Quantum advantage for multi-option portfolio pricing and valuation adjustments
Hassija V, Chamola V, Saxena V, Chanana V, Parashari P, Guizani SMM (2020) Present landscape of quantum computing. IET Quantum Commun 1(6):42–48
Hegade NN, Chandarana P, Paul K, Chen Xi, Albarrá n-Arriagada F, Solano E (2022) Portfolio optimization with digitized counterdiabatic quantum algorithms. Phys Rev Res, 4(4)
Heilman E, Baldimtsi F, Goldberg S (2016) Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions. IACR Cryptol ePrint Arch 2016:56
Helmbold DP, Schapire RE, Singer Y, Warmuth MK (1998) On-line portfolio selection using multiplicative updates. Math Finance, 8
Herbert S (2022) Quantum monte carlo integration: the full advantage in minimal circuit depth. Quantum 6:823
Herman D, Googin C, Liu X, Galda A, Safro I, Sun Y, Pistoia M, Alexeev Y (2022) A survey of quantum computing for finance
Herman D, Shaydulin R, Sun Y, Chakrabarti S, Hu S, Minssen P, Rattew A, Yalovetzky R, Pistoia M (2023) Portfolio optimization via quantum zeno dynamics on a quantum processor
Hull JC (1993) Options, futures, and other derivative securities, 2 edition. Prentice Hall
Hull JC (2019) Quantum Computing: Progress and Prospects. National Academies Press; Illustrated edition (2019), ebook (nap openbook edition) edition, 2019
Hwang CC, Tseng CY, Su CF(2022) Quantum circuit design for computer-assisted shor's algorithm, 02
Intallura P, Korpas G, Chakraborty S, Kungurtsev V, Marecek J (2023) A survey of quantum alternatives to randomized algorithms: Monte carlo integration and beyond. ArXiv
Iovane G (2021) Murequa chain: multiscale relativistic quantum blockchain. IEEE Access 9:39827–39838

Jasim OK, Abbas S, El-Horbaty El-SM, Salem ABM (2015) Quantum key distribution: Simulation and characterizations. Procedia Computer Science, 65:701–710, International conference on communications, management, and information technology (ICCMIT'2015)
Jorion P (1996) Value at risk: the new benchmark for controlling market risk
Josefsson S, Liusvaara I (2017) Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032
Kadowaki T, Nishimori H (1998) Quantum annealing in the transverse Ising model. Phys Rev E 58:5355–5363
Kaneko K, Miyamoto K, Takeda N, Yoshino K (2021) Quantum speedup of monte carlo integration with respect to the number of dimensions and its application to finance. Quantum Inf Process 20(5):185
Kaneko K, Miyamoto K, Takeda N, Yoshino K (2022) Quantum pricing with a smile: implementation of local volatility model on quantum computer. EPJ Quantum Technol 9(1):7
Kashani S, Alqasemi M, Hammond J (2022) A quantum Fourier transform (qft) based note detection algorithm
Kaul D, Raju H, Tripathy BK (2018) Quantum-Comput-Inspired Algorithms Mach Learn. 03 2018
Kearney JJ, Perez-Delgado CA (2021) Vulnerability of blockchain technologies to quantum attacks. Array 10:100065
Kl BP, Giacomo N, Anton R, Ivano T, Stefan W (2020) Improving variational quantum optimization using CVaR. Quantum 4:256
Konno H, Yamazaki H (1991) Mean-absolute deviation portfolio optimization model and its applications to Tokyo stock market. Manage Sci 37:519–531
Kuo FY, Sloan IH (2005) Lifting the curse of dimensionality
Kyriienko O, Magnusson EB (2022) Unsupervised quantum machine learning for fraud detection
Lai YT, Chang MH, Tong YF, Jiang YC, Chou YH, Kuo SY (2022) Portfolio optimization decision-making system by quantum-inspired metaheuristics and trend ratio. In: 2022 IEEE International conference on systems, man, and cybernetics (SMC), pp. 1748–1753
Lamport L (2016) Constructing digital signatures from a one way function
Lamport L, Shostak R, Pease M (1982) The byzantine generals problem. ACM Trans Program Lang Syst 4(3):382–401
Lang J, Zielinski S, Feld S (2022) Strategic portfolio optimization using simulated, digital, and quantum annealing. Appl Sci 12:12288, 12
Lee Y, Joo J, Lee S (2019) Hybrid quantum linear equation algorithm and its experimental test on IBM quantum experience. Scientific Reports, 9(1)
Li C-Y, Chen X-B, Chen Y-L, Hou Y-Y, Li J (2019) A new lattice-based signature scheme in post-quantum blockchain network. IEEE Access 7:2026–2033
Li C, Xu Y, Tang J, Liu W (2019) Quantum blockchain: a decentralized, encrypted and distributed database based on quantum mechanics. J Quantum Comput 1(2):49–63
Li X, Jiang P, Chen T, Luo X, Wen Q (2017) A survey on the security of blockchain systems. Futur Gener Comput Syst 107:08
Lim D, Rebentrost P(2023) A quantum online portfolio optimization algorithm
Liu X, Angone A, Shaydulin R, Safro I, Alexeev Y, Cincio L (2022) Layer VQE: a variational approach for combinatorial optimization on noisy quantum computers. IEEE Trans Quantum Eng 3:1–20
Lucena Antônio, Henriques Marco (2020) A study on fitting sphincs+ to blockchain usage. In: Anais do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, pages 83–96, Porto Alegre, RS, Brasil, SBC
Manzano Alberto, Ferro Gonzalo, Leitao Álvaro, Vázquez Carlos, Gómez Andrés (2023) Real option pricing using quantum computers
Markowitz H (1952) Portfolio selection*. J Financ 7(1):77–91
Marsh S, Wang JB (2019) A quantum walk-assisted approximate algorithm for bounded np optimisation problems. Quantum Inf Process 18(3):61
Marsh S, Wang JB (2020) Combinatorial optimization via highly efficient quantum walks. Phys Rev Res 2:023302
Martinis J, Boixo S (2019) Quantum supremacy using a programmable superconducting processor. October 2019. https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html
Martos VC, Khan T, Thompson L, Malik T, Ross H (2021) White paper blockchain in trade facilitation version 2. https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf, Last accessed: 29th December 2021
Matsakos T, Nield S (2023) Quantum monte carlo simulations for financial risk analytics: scenario generation for equity, rate, and credit risk factors
Mattesi M, Asproni L Mattia C, Tufano S, Ranieri G, Caputo D, Corbelletto D (2023) Financial portfolio optimization: a qubo formulation for sharpe ratio maximization
Maxwell G, Poelstra A, Seurin Y, Wuille P(2019) Simple schnorr multi-signatures with applications to bitcoin. Designs, Codes Cryptogr pp. 1–26
Merkle RC (1978) Secure Communications over Insecure Channels. Assoc Comput Mach21(4):294–299
Merkle Ralph C (1990) A certified digital signature. In: Brassard Gilles (eds), Advances in Cryptology — CRYPTO' 89 Proceedings, pp. 218–238, New York, NY, Springer New York
Mirko A, Saleem Zain H, Muir K (2019) Experimental study of Shor's factoring algorithm using the IBM q experience. Phys Rev A 100:1
Miyamoto K (2022) Bermudan option pricing by quantum amplitude estimation and chebyshev interpolation. EPJ Quantum Technol 9(1):3
Miyamoto K (2022) Quantum algorithm for calculating risk contributions in a credit portfolio. EPJ Quantum Technol
Miyamoto K (2022) Quantum algorithms for numerical differentiation of expected values with respect to parameters. Quantum Inf Process 21(3):109
Miyamoto K, Miyamoto K, Shiohara K, Shiohara K (2019) Reduction of qubits in quantum algorithm for monte carlo simulation by pseudo random number generator. Phys Rev A
Montanaro A (2015) Quantum speedup of monte carlo methods. arXiv: Quantum Physics
Mugel S, Abad M, Bermejo M, Sánchez J, Lizaso E, Orús R (2021) Hybrid quantum investment optimization with minimal holding period. Sci Rep 11(1)

Mugel S, Lizaso E, Orus R (2020) Use cases of quantum optimization for finance

Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org

NIST (2006) Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography. https://csrc.nist.gov/publications/detail/sp/800-56a/revised/archive/2007-03-14

NIST (2022) Nist 's 1st announcement for pqc standarts. https://www.nist.gov/news-events/news/2023/07/nist-announces-additional-digital-signature-candidates-pqc-standardization

NIST (2023) Nist additional signatures - round 1. https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures

Orús R, Mugel S, Lizaso E (2019) Quantum computing for finance: Overview and prospects. Reviews in Physics 4:100028

Palmer S, Karagiannis K, Florence A, Rodriguez A, Orus R, Naik H, Mugel S (2022) Financial index tracking via quantum computing with cardinality constraints

Park JS, Lim BH, Lee Y, Young M (1998) A minimax portfolio selection rule with linear programming solution. Manage Sci 44:673–683

Pednault E, Gunnels J, Maslov D, Gambetta J (2019) On Quantum Supremacy. IBM Research Blog

Pérez-Salinas Adriá n, Cervera-Lierta Alba, Gil-Fuster Elies, Latorre José I (2020) Data re-uploading for a universal quantum classifier. Quantum, 4:226

Pérez-Salinas Adriá n, López-Núñez David, García-Sáez Artur, Forn-Díaz P, Latorre José I (2021) One qubit as a universal approximant. Phys Rev A, 104(1)

Peruzzo A, McClean J, Shadbolt P, Yung M-H, Zhou X-Q, Love PJ, Aspuru-Guzik A, O'Brien JL (2014) A variational eigenvalue solver on a photonic quantum processor. Nat Commun 5(1):4213

Plekhanov K, Rosenkranz M, Fiorentini M, Lubasch M (2022) Variational quantum amplitude estimation. Quantum 6:670

Prashant (2007) A study on the basics of quantum computing

Preskill J (2012) Quantum computing and the entanglement frontier

Preskill J (2018) Quantum computing in the NISQ era and beyond. Quantum 2:79

Preskill J (2018) Quantum computing in the nisq era and beyond. Quantum 2:79

Prewett K, Prescott G, Phillips K (2019) Blockchain adoption is inevitable-barriers and risks remain. J Corporate Account Financ 31:09

Punathumkandi S, Boscovic D (2022) A survey on quantum-safe blockchain system. 12 https://www.acsac.org/2022/workshops/web3sec/Swathi2022.pdf

Raikwar M, Gligoroski D, Kralevska K (2019) Sok of used cryptography in blockchain. IEEE Access 7:148550–148575

Rajan D, Visser M (2019) Quantum blockchain using entanglement in time. Quantum Reports 1(1):3–11

Ramos-Calderer S, Pérez-Salinas A, García-Martín D, Bravo-Prieto C, Cortada J, Planagumà J, Latorre JI (2019) Quantum unary approach to option pricing. arXiv:Quantum Physics

Rebentrost P, Gupt B, Bromley Thomas R (2018) Quantum computational finance: Monte carlo pricing of financial derivatives. Phys Rev A

Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Assoc Comput Mach 21(2):120–126

Rivest RL, Shamir A, Adleman LM (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126

Rivest RL, Shamir A, Kalai YT (2001) How to leak a secret. In International Conference on the Theory and Application of Cryptology and Information Security

Rockafellar RT, Uryasev S (2000) Optimization of conditional value-at risk. J Risk 3:21–41

Roffe J (2019) Quantum error correction: an introductory guide. Contemp Phys 60(3):226–245

Rosen KH (2011) Elementary Number Theory and Its Application, 6th ed. Addison-Wesley

Saha A, Chatterjee T, Chattopadhyay A, Chakrabarti A (2022) Intermediate qutrit-based improved quantum arithmetic operations with application on financial derivative pricing

Samuelson Paul A (1975) The fundamental approximation theorem of portfolio analysis in terms of means, variances and higher moments., pp. 215–220. Academic Press

Santagati R, Aspuru-Guzik A, Babbush R, Degroote M, Gonzalez L, Kyoseva E, Moll N, Oppel M, Parrish RM, Rubin NC, Streif M, Tautermann CS, Weiss H, Wiebe N, Utschig-Utschig C (2023) Drug design on quantum computers

Schnorr C-P (1991) Efficient signature generation by smart cards. J Cryptol 4(3):161–174

Seet J, Griffin P (2019) Quantum consensus. In 2019 IEEE Asia-Pacific conference on computer science and data engineering (CSDE), pp. 1–8

Sels D, Polkovnikov A (2017) Minimizing irreversible losses in quantum systems by local counterdiabatic driving. Proceedings of the National Academy of Sciences, 114(20)

Shahid F, Khan A, Jeon G (2020) Post-quantum distributed ledger for internet of things. Comput Electr Eng 83:106581

Sharma A, Kumar A (2019) A survey on quantum key distribution. In: 2019 International conference on issues and challenges in intelligent computing techniques (ICICT), volume 1, pp. 1–4

Shi J, Zhao T, Wang Y, Yu C, Lu Y, Shi R, Zhang S, Wu J (2022) An unbiased quantum random number generator based on boson sampling, 06

Shor P (1997) Polynomial-time algorithms for pime factorization and discrete logarithms on a quantum computer. SIAM J Comput 26(5):1484–1509

Shor PW (1982) Refined analysis and improvements on some factoring algorithms. J Algorithms 3(2):101–127

Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th annual symposium on foundations of computer science, pp. 124–134

Shor PW (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput 26(5):1484–1509

Srivastava R (2023) Quantum computing in drug discovery. Inf Syst Smart City, 3(1)

Stamatopoulos N, Egger DJ, Sun Y, Zoufal C, Iten R, Shen N, Woerner S (2020) Option Pricing using Quantum Computers. Quantum 4:291

Stamatopoulos N, Mazzola G, Woerner S, Zeng WJ (2022) Towards quantum advantage in financial market risk using quantum gradient algorithms. Quantum 6:770

Stephens AM, Huang J, Nemoto K, Munro WJ (2013) Hybrid-system approach to fault-tolerant quantum communication. Phys Rev A, 87(5)

Stevens M, Bursztein E, Karpman P, Albertini A, Markov Y (2017) The first collision for full sha-1. pp. 570–596, 07

Suzuki Y, Suzuki Y, Uno S, Raymond R, Tanaka T, Onodera T, Yamamoto N, Yamamoto N (2020) Amplitude estimation without phase estimation. Quantum Inf Process

Svore Krysta M, Hastings Matthew B, Freedman M (2013) Faster phase estimation

Szegedy M (2004) Quantum speed-up of markov chain based algorithms. In: 45th Annual IEEE symposium on foundations of computer science, pp. 32–41

Tanaka T, Suzuki Y, Uno S, Raymond R, Onodera T, Yamamoto N, Yamamoto N, Yamamoto N, Yamamoto N (2020) Amplitude estimation via maximum likelihood on noisy quantum computer

Tang H, Pal A, Wang T-Y, Qiao L-F, Gao J, Jin X-M (2021) Quantum computation for pricing the collateralized debt obligations. Quantum Engineering 3(4):e84

Tang H, Wu W, Jin Xian-Min (2022) Quantum computation for pricing caps using the libor market model

Tapia Elena P, Scarpa G, Pozas-Kerstjens A (2022) Fraud detection with a single-qubit quantum neural network

Torres W, Steinfeld R, Sakzad A, Liu J, Kuchta V, Bhattacharjee N, Au Man H, Cheng J (2018) Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (Lattice RingCT v1.0), pages 558–576. 06

Torres WAA, Steinfeld R, Sakzad A, Kuchta V (2020) Post-quantum linkable ring signature enabling distributed authorised ring confidential transactions in blockchain. IACR Cryptol. ePrint Arch. 2020:1121

Torrontegui E, Ibá ñez S, Martínez-Garaot S, Modugno M, del Campo Adolfo, Guéry-Odelin D, Ruschhaupt A, Chen X, Muga Juan G (2013) Shortcuts to adiabaticity. In Advances In Atomic, Molecular, and Optical Physics, pages 117–169. Elsevier

Ukpabi D, Karjaluoto H, Bötticher A, Nikiforova A, Petrescu D, Schindler P, Valtenbergs V, Lehmann L, Yakaryilmaz A (2023) Framework for understanding quantum computing use cases from a multidisciplinary perspective and future research directions

Umer M, Sharif M (2022) A comprehensive survey on quantum machine learning and possible applications. Int J E-Health Med Commun 13:1–17, 01

Uno S, Suzuki Y, Hisanaga K, Raymond R, Tanaka T, Onodera T, Yamamoto N, Yamamoto N (2021) Modified grover operator for quantum amplitude estimation. New J Phys

University of Stanford (2011) SafeCurves: Pertinent side channel attacks on elliptic curve cryptographic systems. http://theory.stanford.edu/~dfreeman/cs259c-f11/finalpapers/sidechannel.pdf

US National Security Agency (2016) Commercial national security algorithm suite and quantum computing faq. https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf

van Saberhagen N (2013) Cryptonote v 2.0. https://bytecoin.org/old/whitepaper.pdf, 2013. Last accessed: 1st December 2021

Varga T, Aragonés-Soria Y, Oriol M (2024) Quantum types: going beyond qubits and quantum gates

Venturelli D, Kondratyev A (2019) Reverse quantum annealing approach to portfolio optimization problems. Quantum Mach Intell 1(1):17–30

Veselý M (2022) Application of quantum computers in foreign exchange reserves management

Vazquez Almudena Carrera, Woerner Stefan (2021) Efficient state preparation for quantum amplitude estimation. Phys Rev Appl

Wang G (2022) Classically-boosted quantum optimization algorithm. 2022

Wang H, Wang Y, Cao Z, Li Z, Xiong G (2019) An overview of blockchain security analysis. In: Yun Xiaochun, Wen Weiping, Lang Bo, Yan Hanbing, Ding Li, Li Jia, Zhou Yu, (eds), Cyber Security, pages 55–72, Singapore, Springer Singapore

Wang L, Shen X, Li J, Shao J, Yang Y (2019) Cryptographic primitives in blockchains. J Netw Comput Appl 127:43–58

Wang W, Yu Y, Du L (2022) Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. Sci Rep 12:05

Wehner S, Elkouss D, Hanson R (2018) Quantum internet: A vision for the road ahead. Science 362(6412):eaam9288

Weinstein Y (2022) Inspiring quantum data analysts. Harvard Data Sci Rev, 4(1) https://hdsr.mitpress.mit.edu/pub/eyywouav

Wikipedia contributors (2023) Convex optimization — Wikipedia, the free encyclopedia. [Online; accessed 27-March-2023]

Wikipedia contributors (2023) Quadratic unconstrained binary optimization — Wikipedia, the free encyclopedia, [Online; accessed 27-March-2023]

Wikipedia contributors (2023) Quantum volume — Wikipedia, the free encyclopedia, [Online; accessed 9-April-2023]

Wilkens S, Moorhouse Joe (2023) Quantum computing for financial risk measurement. Quantum Information Processing

Wipplinger E (2007) Philippe jorion: Value at risk - the new benchmark for managing financial risk. Fin Markets Portfolio Mgmt 21(3):397–398

Woerner S, Egger DJ (2019) Quantum risk analysis. npj Quantum Information, 5(1)

Yalovetzky R, Minssen P, Herman D (2023) Nisq-hhl: Portfolio optimization for near-term quantum hardware

Yang Z, Salman T, Jain R, Di Pietro R (2022) Decentralization using quantum blockchain: a theoretical analysis. IEEE Tran Quantum Eng 3:1–16

Yang Z, Salman T, Jain R, Di Pietro R (2022) Decentralization using quantum blockchain: A theoretical analysis. IEEE Trans Quantum Eng 3:1–16

Yao Andrew C (1982) Protocols for secure computations. In 23rd annual symposium on foundations of computer science (sfcs 1982), pages 160–164

Yeniaras E, Cenk M (2021) Improved polynomial multiplication algorithms over characteristic three fields and applications to ntru prime. In Innovative Security Solutions for Information Technology and Communications: 14th International Conference, SecITC 2021, Virtual Event, November 25-26, 2021, Revised Selected Papers, page 125-144, Berlin, Heidelberg, Springer-Verlag

Yeniaras E, Cenk M (2022) Faster characteristic three polynomial multiplication and its application to ntru prime decapsulation. J Cryptogr Eng 12:329–348

Zhang P, Wang L, Wang W, Fu K, Wang J (2021) A blockchain system based on quantum-resistant digital signature. Secur Commun Netw 2021:6671648:1-6671648:13

Zhang S, Li L (2022) A brief introduction to quantum algorithms. CCF Trans High Perform Comput 4(1):53–62

Zhou L, Wang Sheng-Tao, Choi S, Pichler H, Lukin MD (2020) Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices. Phys Rev X, 10(2)

Zoufal C, Lucchi A, Woerner S (2019) Quantum generative adversarial networks for learning and loading random distributions. npj Quantum Information

Rubio-García Á, García-Ripoll JJ, Porras D (2022) Portfolio optimization with discrete simulated annealing

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.