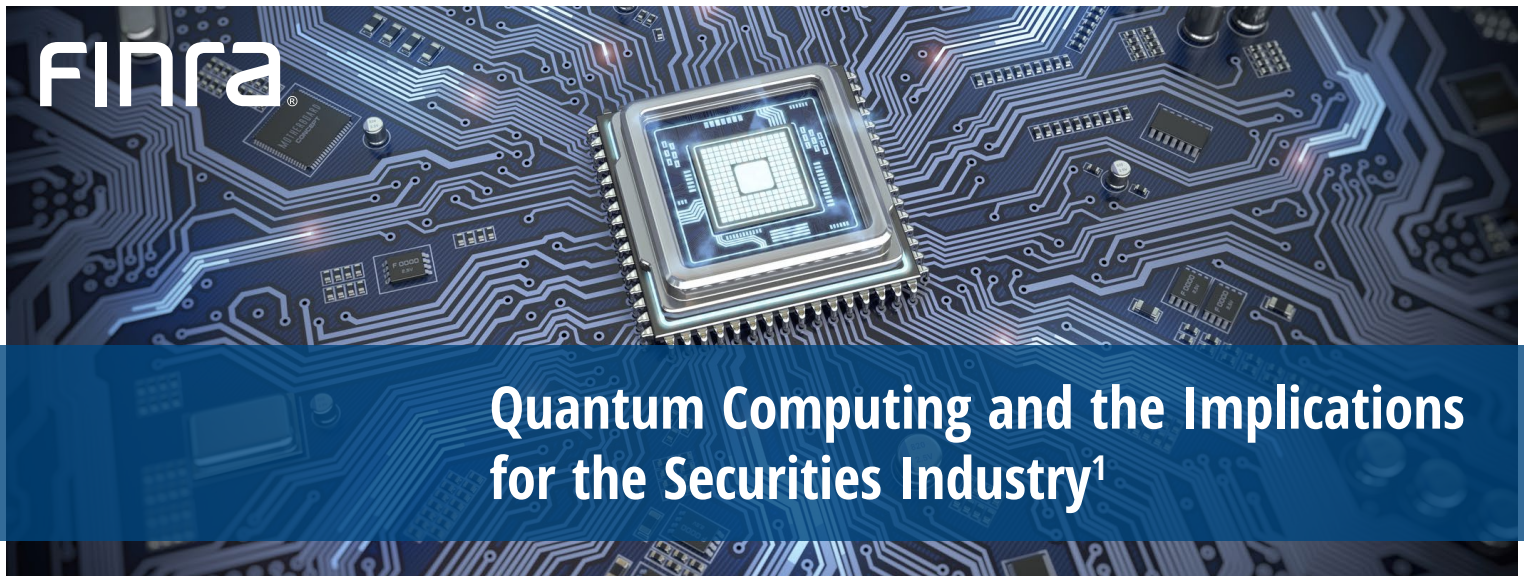


Quantum Computing and the Implications for the Securities Industry[1]

Contents

INTRODUCTION

Quantum mechanics is a branch of physics that deals with the complex properties of atoms and sub-atomic particles.[2] Quantum computing leverages the principles of quantum mechanics to solve problems too large or complex for traditional computers. Although quantum computing is still in its early stages, numerous financial institutions have begun experimenting with this evolving technology, given its potential to dramatically alter the types, and speed, of computations that are possible. In addition, some regulators and other key market participants are exploring the implications of quantum computing for the securities industry.[3] In December 2022, President Biden signed the bipartisan Quantum Computing Cybersecurity Preparedness Act into law, recognizing the potential threat that quantum decryption (*i.e.*, the ability for quantum computers to bypass existing data safeguards) may pose to the government, and encouraging U.S. regulators to adopt technologies to protect against quantum computing attacks.[4]

In recent years, several major financial institutions have reportedly identified quantum computing as a technology with the potential to dramatically disrupt the securities industry over the next decade and beyond.[5] While reportedly only one percent of companies budgeted for quantum-related expenses during 2018, by some estimates as many as 20 percent may do so in some form by 2023, with up to $850 billion in investments anticipated over the next 30 years.[6] In addition, equity investment in quantum computing has significantly increased in recent years.[7] For example, funding in the quantum computing space has reportedly seen record levels—$2.35 billion in investments in quantum technology start-ups (both hardware and software) in 2022—with a significant ramp-up in the last two years.[8] In addition, major financial institutions have committed significant resources to the technology.[9] Some of these firms are actively working with major cloud service providers to most efficiently access quantum computers.[10]

The public sector has also committed to investing in quantum computing. Last year, the U.S., European Union and Canada collectively invested over $3.1 billion.[11] There were also notable technical breakthroughs in the area, as demonstrated by the Nobel Prize in Physics in 2022 being awarded to quantum computing research groups.[12] These investments and accomplishments can be seen as a sign of increasing confidence in the potential for quantum computing. While the extent of technical achievement in the field of quantum computing has been debated,[13] global investment and interest in the potential of quantum computing continues to steadily grow. Despite having an uncertain timetable for its development, quantum computing has the potential to reshape the financial services industry by presenting newfound capabilities and challenges for firms.

In light of the potentially transformative impact that quantum computing may have on the securities industry, staff from FINRA's Office of Financial Innovation (OFI) initiated a research initiative focusing on the opportunities and risks quantum computing presents, culminating in this report. As part of this research, OFI staff engaged more than 20 stakeholders, including financial institutions, quantum computing hardware and software providers, academics, industry observers, government entities, security specialists and trade institutions. We conducted this research, in part, to better understand the implications of quantum computing, including the most likely applications within the financial industry and potential threats to data security.

This report summarizes the main findings of our research:

- **Section I** provides a brief overview of quantum computing, highlighting certain basic principles.
- **Section II** identifies and analyzes the potential applications for quantum computing that the securities industry is exploring.
- **Section III** addresses the potential threats to cybersecurity that quantum computing may pose.
- **Section IV** outlines some potential regulatory considerations associated with quantum computing.

This report is intended to raise awareness among FINRA member firms and the broader the securities industry by providing an overview of how developments in quantum computing may impact business models and processes. While the true implications of quantum computing may not be known for years, this report is designed to serve as an initial step in beginning an important dialogue with market participants about the use of quantum computing in the securities industry. Accordingly, FINRA requests comments on all areas this report covers.[14]

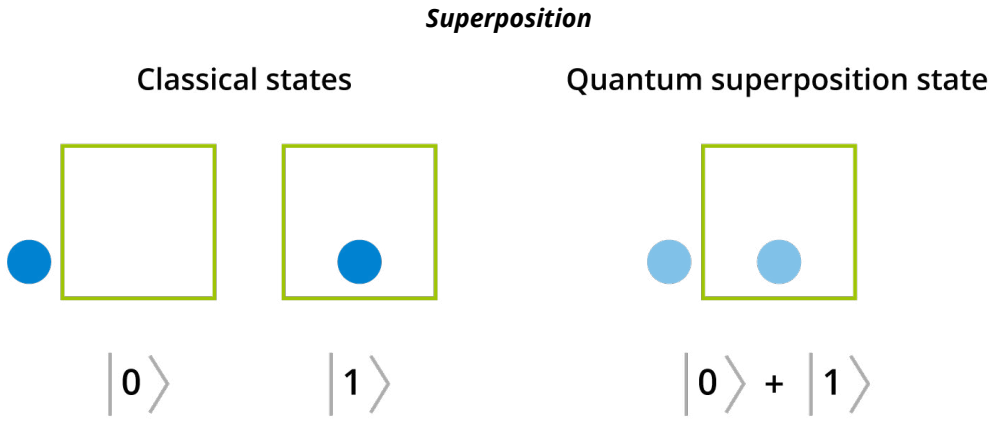
SECTION I: Overview of Quantum Computing

Quantum computing is an emerging technology that relies on quantum mechanics to perform calculations not possible for even the most powerful classical supercomputers.[15] To better understand what is behind quantum computing's exponentially faster processing times, the National Institute of Standards and Technology (NIST) notes that it may help to think of computers like "microscopic cities" with electricity running through roads using "logic gates" and "bits."[16]

- **Logic gates:** The streets in these "microscopic cities" contain gates, known as logic gates, which operate similar to gates on a road that move up and down to direct the flow of traffic by either allowing or blocking vehicles from passing.[17] Logic gates enable computers to function, as they essentially follow a similar up and down movement to allow or block flows of electricity.[18] Logic gates are used to make circuits and, in turn, circuits are used to form central processing units (CPUs), which are the principal parts of computer systems.[19]
- **Bits:** Flows of electricity that travel through logic gates produce outputs known as bits. Bits are what classical computers use for storing and processing information. Bits are configured in only two formats: 0 and 1, which represent the flow of an electrical signal either being allowed through the logic gate or blocked by it.[20] Logic gates are arranged sequentially, with electricity traveling through each gate like a flowchart. This flow of information through gates is what forms circuits. Information flowing through circuits allows computers to carry out logical functions, such as mathematical calculations.[21]

For quantum computing, this flow of electricity involves "quantum logic gates," "qubits," "reversibility," "superposition," and "entanglement."

- **Quantum Logic Gates and Qubits:** Quantum logic gates are the basic building blocks of quantum computers. They can control and direct incoming electricity levels, to result in the desired output. Quantum logic gates are also the mechanisms that enable non-binary flows of information in quantum computers to produce quantum bits (or qubits). Qubits exist in more than one state simultaneously, such that they represent not just as a 0 *or* 1, but instead represent both 0 *and* 1 at the same time.[22] Qubits allow quantum computers to process multiple possibilities simultaneously.[23]
- **Superposition:** The simultaneous existence of more than one configuration—or state—at one time is a fundamental principle of quantum mechanics known as superposition.[24] In the case of quantum computing, qubits in superposition are represented by a complex linear combination of a 1 state and a 0 state. As described further below, the ability for quantum computers to consider multiple states simultaneously facilitates finding a solution to problems that might otherwise seem to have an impossibly large number of potential outcomes.
- **Reversibility:** Reversibility means that all the outputs quantum logic gates produce can be reversed or undone.[25] Theoretically, the fact that qubits can go in reverse and essentially "re-trace" their flows, or steps, means that information that passes through quantum gates can be retrieved, which is not currently possible in classical computers.[26]
- **Entanglement:** The power of superposition is amplified by another central principle of quantum physics known as entanglement, where qubits in superposition are capable of generating even more results by interacting with one another.[27] Entanglement is a special connection between two pairs of quantum elements where the changing state of one element impacts others, even at a distance.[28] By entangling qubits, the number of represented states can rise exponentially, making it feasible to both explore a massive number of possibilities instantly and also conduct parallel calculations on a scale beyond the reach of classical computers.[29]



Source: Investor Place

Financial institutions have generally avoided purchasing or attempting to build their own quantum computers because of the challenges and expenses associated with purchasing and maintaining quantum systems. [30] Instead, firms typically rent access to quantum machines hosted by cloud service providers.[31] Accessing quantum computing through the cloud can come in the form of subscription models or, more flexible, pay-per-use access models.[32] Leveraging quantum computers through the cloud may enable economies of scale, sharing of resources at lowers costs, and increased access.[33]

SECTION II: Potential Applications of Quantum Computing in the Securities Industry

In FINRA staff's survey of quantum computing use cases, several firms indicated that they are examining how they can benefit from quantum computers when conducting various activities, including trade execution, portfolio management, risk assessments and fraud detection.[34] Additional firms indicated to FINRA that they are assessing the potential risk quantum computers may pose to current encryption standards for securing critical data. Government bodies from around the world, including NIST, are attempting to address this potentially systemic issue related to data security by developing standards for post-quantum cryptography.

As market efforts related to quantum accelerate, the influx of attention and investment has led some market participants to worry about hype overtaking reality, with one group of researchers from the Massachusetts Institute of Technology (MIT) indicating that "quantum computing has a hype problem."[35] Some market participants have questioned the ability to develop commercialized applications for quantum computing in the near future. While the timeline for any practical changes resulting from quantum computing is a topic of ongoing debate, the theory behind how quantum computing works and its potential to solve large or complex computational problems is well documented.

Seizing on the potential associated with quantum computing, several financial institutions, including broker-dealers, have begun exploring how leveraging quantum for exponential improvements in computing performance could enhance business operations. Based on research and interviews with a range of market participants, the financial services industry has identified three potential areas involving computational challenges where quantum computing may have a significant impact: optimization systems, simulation systems and artificial intelligence.[36]

Optimization Systems

The ability of quantum computers to efficiently analyze and process numerous potential outcomes in real time may benefit optimization systems firms use. Market participants have indicated that computationally intense quantum models may process large sets of variables and allow for faster and more accurate optimizations, such as best determining valuations that can deliver competitive advantages; calculating more precise estimates of credit exposure; and better allocating capital across a range of corporate financial activities, among other uses.[37]

Financial institutions seeking to leverage quantum computing for enhancing optimization systems have focused on areas such as enhancements for trade execution, trade settlement and portfolio management. Market participants have indicated that quantum-based algorithms may be used to efficiently determine the optimal solution among various options[38] because of the ability to survey multiple possible solutions simultaneously. Accordingly, quantum computers hold the potential to complete solutions for optimization problems in a fraction of the time it would take classical computers and firms are exploring its potential to more effectively navigate complex trading and investment environments involving large sets of variables.[39] As outlined below, market participants believe that quantum computing's capabilities for optimization may in the future streamline trade execution and settlement processes as well as enable investment managers to improve portfolio management.

- **Trade Execution Optimization**

  Financial institutions are frequently tasked with determining how best to execute trades. Such efforts entail weighing a variety of factors, such as trade sizes, venues, timing and sequencing. These factors can impact the quality of trade execution and it is computationally challenging for even the most advanced classical computers to consider all the possible permutations given the number of potential variables. One report by a technology firm notes that "[t]o help put this type of optimization problem in perspective, consider that selecting the optimal order of execution for 5,000 trades has more than $4.2 \times 10^{16,325}$ possibilities."[40] Some firms are assessing how quantum computing could offer a potential breakthrough for these trade execution challenges due to its ability to survey multiple possible solutions simultaneously, such as determining the optimal values for the sequencing, grouping and timing of trading activities.

- **Trade Settlement Optimization**

  The trade settlement process involves securities being delivered by a seller against payment made by a purchaser, frequently facilitated by a clearinghouse, which can help to mitigate counterparty risk. Clearinghouses run trade settlement optimization analyses, which they use to determine the optimal routing trajectory for settling thousands of trades and matching up buyers and sellers at millisecond speeds, while also accounting for other legal, business, and operational factors.[41] Given the different variables that need to be considered in the trade settlement process, determining an optimal solution may be computationally complex. Typically, there is greater complexity where there are more trades involved, which presents increased challenges for classical computers.[42]

  In the view of some market participants, quantum computing may help optimize the trade settlement process by using quantum-based optimization algorithms to discover links for multi-party settlements, thereby making the process faster and more efficient. These market participants believe that a faster settlement process could potentially reduce cost risks related to replacement (*i.e.*, the risk of loss from unrealized gains caused by delayed settlement); liquidity (*i.e.*, market pressure that may result if firms fail to settle their positions); and credit (*i.e.*, the possibility of loss where a party fails to meet its repayment obligations).[43] Of note, the U.S. Securities and Exchange Commission (SEC) recently approved a rule change to shorten the settlement cycle to T+1,[44] and reductions in settlement time may impact the benefits and risks associated with the potential future use of quantum computing to facilitate settlement.

- **Investment Portfolio Optimization**

  Portfolio optimization involves determining the optimal mix of investment assets to achieve a desired objective, such as maximizing return and minimizing risk, over a given period of time. Investment portfolio optimization problems are frequently dependent on a number of variables and may at times result in calculations that take classical computers several days to conclude.[45] As noted by some industry observers, the complexity associated with portfolio optimization can be attributed to a number of factors such as valuation adjustments (for credit, debit, funding, capital and margin); transaction costs; and regulatory and tax requirements; among others.[46]

  Firms are researching whether quantum computing has the potential to improve the portfolio optimization process by offering the computational capacity to assess various scenarios involving a multitude of assets and related factors. As a result, some market participants believe that the use of quantum computers may at some point give firms a competitive advantage by allowing them to develop optimized portfolio options that are able to analyze more variables in a shorter timeframe and thereby better able to achieve the desired results. For example, quantum computers may potentially offer an enhanced ability to

allocate weights to assets over a period of time (with the aim of maximizing returns), forecast asset returns, assess volatility and measure risk.[47] In determining the optimal portfolio over time, quantum computers may seek to measure the return per unit of risk and do so while factoring in dynamic changes in the marketplace, measuring transaction costs and operating consistent with investment mandates.[48]

Simulation Systems

Quantum-based simulations could enhance firms' abilities to understand and account for uncertainty related to market activity. Firms are examining ways to use quantum computers to run simulations of market-related activity that would otherwise be difficult or potentially impossible to capture with classical computers. In particular, financial institutions are exploring the use of quantum computers to assist with analyzing market activity related to risk assessments.

One such risk assessment method, the Monte Carlo simulation, which takes random samples of a number of variables to simulate probable outcomes, is a common technique for incorporating risk and uncertainty in financial models and evaluating potential risks.[49] Firms may use a Monte Carlo simulation to determine the likelihood of possible outcomes for determining factors such as Value at Risk to help identify potential financial losses. The Monte Carlo simulation is also instrumental in pricing financial derivatives. For example, The Bank for International Settlements (BIS) has noted that, each year, more than $10 trillion worth of options and derivatives are exchanged globally, many priced using Monte Carlo methods.[50] However, the Monte Carlo simulations typically use methods that are computationally intensive, especially in the face of an array of uncertainties, with some calculations taking classical computers several hours, or even days, to perform.[51] Accordingly, firms are looking into ways to leverage quantum computers to more efficiently price complex derivatives—a task that can require a great deal of computing power, resources and time.[52]

Firms are engaging quantum computers to determine whether they offer the potential for a significant increase in processing power that could reduce the computation time for a typical Monte Carlo-based risk assessment from days or hours to near real-time.[53] Some firms believe that a faster simulation process, provided by quantum computing, has the potential to provide benefits in circumstances, including regularly re-evaluating portfolios against risk factors such as liquidity and credit risk. Moreover, these firms are studying whether the greater processing power from quantum computers may also provide the capacity to consider additional market factors with the potential to improve the accuracy of risk assessments, enabling firms to better limit financial losses or enhance potential gains.[54]

In addition, some firms believe that quantum computing may assist with risk assessments related to anti-money laundering (AML) and know-your-customer (KYC) compliance systems. Quantum-based algorithms have the potential to improve AML and KYC programs by expanding the ability to analyze various elements of individual identity, transaction history, fund flows and relationships in real time. One relatively recent analysis of financial institutions suggested that even a one to two percent improvement in overall efficiency could save over $1.5 billion annually for the industry.[55]

Artificial Intelligence

As addressed in FINRA's Artificial Intelligence (AI) in the Securities Industry report, the financial services industry, including broker-dealers, has allocated considerable resources to researching, developing and adopting artificial intelligence (AI) tools, including by leveraging computing power to analyze large data sets. Though quantum computing is still in a developmental phase, some market participants view it as a potential accelerant for AI because of its potential to enhance the ability to process and analyze large data sets.

The term "quantum AI" refers to a growing field in quantum computing that focuses on improving quantum-based computations and algorithms that are used to train models within various AI tools and applications. Some industry analysts have made the case that quantum computers may offer the ability to enlarge and enhance the type of datasets that AI algorithms and training models can use, resulting in a more efficient process and more accurate outputs, as well as helping AI models become more scalable.[56] For example, quantum-based machine learning could potentially allow for the ability to process greater amounts of data while also analyzing that data at faster speeds, accelerating the pace at which machine learning models can learn.[57] In addition, quantum-based natural language processing (QNLP) applies key quantum properties, such as superposition and entanglement, to allow deeper textual analysis and classification to train natural language processing models.[58] Accordingly, some market participants are hopeful that quantum computing may be able to assist in the process of efficiently and accurately obtaining meaning and value from complex text and sentence structures to potentially assist with tasks, such as providing financial advice.[59]

However, as quantum computing may accelerate the potential beneficial impact of AI, it may similarly accelerate related risks. As noted in FINRA's Artificial Intelligence (AI) in the Securities Industry report, model explainability and data bias are some of the key risks that need to be addressed when deploying AI-based tools, and these risks may be compounded by the complexity enabled through the use of quantum computing.[60] As previously noted: "[f]irms that employ AI-based applications may benefit from reviewing and updating their model risk management frameworks to address the new and unique challenges AI models may pose."[61] This would be particularly true in the context of any quantum AI application.

SECTION III: Potential Threats to Cybersecurity

Overview

The financial services industry heavily relies on cryptography to safeguard digital information. Whether to securely store customers' personally identifiable information (PII), access the internet through a virtual private network (VPN) or ensure the integrity of a trade order placed on a mobile application, cryptographic algorithms play a central role in many critical functions within the financial system. Such algorithms are based on mathematical problems that are prohibitively time-consuming for today's classical computers to solve. For instance, a hacker would need *trillions* of years using a conventional computer to break the encryption securing internet-based communications, such as a VPN.[62]

Quantum computing is uniquely positioned to offer, in the future, a streamlined way to crack today's standard encryption safeguards. This is possible because quantum computing can leverage specialized algorithms to significantly reduce the amount of time to solve the mathematical problems behind today's encryption. At a high level, this type of solution is possible because a quantum computer uses qubits in superposition to simultaneously see across several potential solutions to an algorithm (*i.e.*, quantum parallelism) and select the correct one.[63]

The following section highlights the potential quantum-related threats, methods for mitigating those threats and areas of consideration for firms seeking quantum resistance.

Potential Quantum Security Threat

Encryption is widely discussed as the main vulnerability for firms to a quantum attack. This is due to a quantum computer's ability to leverage algorithms to degrade certain security methods, such as asymmetric key cryptography (systems using different pairs of private/public keys between sender and recipient for encryption), hashing (systems using algorithms to scramble a message of any size into a coded fixed-length value), and symmetric key cryptography (systems using a shared private key between sender and recipient for encryption).[64] There are two principal algorithms that hackers could use in a quantum attack on encrypted data:

- **Shor's Algorithm.** Shor's Algorithm is particularly efficient at solving the mathematical problems that underlie asymmetric key cryptography. Shor's Algorithm provides quantum computers exponential speedup advantages for conducting calculations to break asymmetric key encryption. In other words, if a classical computer required 2^50 steps to break encryption based on asymmetric key infrastructure, it might only take a quantum computer only 50 steps.[65] Hackers could use Shor's Algorithm to engineer an attack on a crypto standard such as RSA (Rivest-Shamir-Adleman), which is a common standard for securing data transmission.
- **Grover's Algorithm.** Grover's Algorithm is not as well-suited for breaking asymmetric key cryptography but, instead, hackers may use it to provide so-called quantum speedup advantages in breaking symmetric key cryptography and hashing, where the time to find a possible solution is drastically reduced. For example, a computation that requires $1{,}000^2$ (or 1,000,000) steps for a classical computer may require 1,000 steps for a quantum computer.[66] Hackers could also deploy Grover's Algorithm to weaken a standard such as Advanced Encryption Standard (AES), which is commonly used to protect sensitive data.

Given the significant speedup advantage Shor's Algorithm offers, the threat of a quantum attack is potentially greatest with asymmetric key encryption. Although Grover's Algorithm may be improved upon, in its current state, symmetric key cryptography and hashing are still generally regarded to be quantum-resistant.[67] For example, a quantum computer with over 6,000 logical qubits would still need over 10^{32} years to break AES-256 symmetric key encryption using Grover's algorithm.[68] However, a quantum computer with 2,000 logical qubits using Shor's Algorithm could potentially only need less than four hours to break asymmetric encryption based on the RSA-1024 standard.[69]

Methods of Quantum Resistance

We discuss the NIST standards for upgrading existing encryption practices that will likely influence the financial services industry in greater detail below. In addition, we note other methods for providing quantum resistance.

- **New Cryptographic Standards.** In response to the rising threat to today's encryption standards, NIST has focused on creating readily available replacement algorithms with mathematical properties that would be difficult to break even if large-scale quantum computers became available.[70]

  Cybersecurity specialists have been developing post-quantum cryptography (PQC) standards for public key encryption standards that could protect key exchange and signature applications. In a competition that resembles a previous effort that produced new hashing algorithms,[71] NIST submitted a call for proposals for new algorithms in 2016, with designs submitted by more than 80 teams from 25 countries.[72] NIST evaluated proposals based primarily on security and performance criteria[73] and narrowed the candidates in three successive rounds, with the most recent round occurring in the first half of 2022.[74] NIST reportedly plans to release draft PQC standards in 2023 for public comment and may seek to publish final standards in 2024.[75] In addition, NIST recently developed a factsheet to inform organizations on matters related to migration to post-quantum cryptography.[76]

  Noteworthy among NIST's efforts is that it identified a group of four encryption algorithms that are expected to be a part of its new standards. In addition, NIST identified four other algorithms that remain under consideration for inclusion in the new standards. NIST has pursued a portfolio approach of selecting a variety of algorithms in recognition of the need to identify suitable tools for different encryption applications and systems as well as the need for redundancy in case any of the tools prove vulnerable.[77]

- **Key Length Upgrades.** Perhaps the most expeditious route to quantum resistance is a lengthening of existing keys. For example, today's standard of RSA-2048[78] could be extended to 4096-bits to lengthen the amount of time required to break encryption. Nevertheless, this solution may only be a short-term one, due to the exponential speed quantum computing offers.[79] Moreover, lengthening key sizes may be disruptive and introduce potential hardware incompatibility (*e.g.*, for certain smart cards) and operational issues.[80]
- **Quantum Communications.** Another way to potentially bypass a quantum attack is to remove the mathematical equations involved in cryptography that can be decoded by a quantum computer. Instead, quantum computing could be leveraged in a way where keys could be shared through qubits that travel in a state of superposition, potentially making them extremely difficult for bad actors to intercept.[81] However, as with any new and emerging technology, quantum communications may also present new challenges and vulnerabilities.[82]

Firm Considerations for Quantum Resistance

The use of cryptography is embedded in almost every firm's data, including storage and transmission. In addition, cryptography is the basis for securing more than 90 percent of internet-based connections[83] and plays a significant role on blockchain platforms.[84] Cryptography may play a key role in firms' data security architecture through a variety of ways, including securing communication links with customers and other firms, verifying identify (including through the use of digital signatures or certifications) and securing sensitive information. Accordingly, some firms have begun exploring potential upgrades to their cryptographic security in light of the potential disruptions that any future quantum attack may pose and considering the time that it may take to finalize a set of new cryptographic algorithms, implement them in firms' hardware and software stacks, and adequately train personnel.[85]

Considering all that is involved in designing and implementing new standards, the path to quantum resistance could encompass a sequence of steps that takes several years. The National Academy of Science has indicated that it would take at least a decade to fully replace a widely used cryptographic standard, and this would come after the already lengthy PQC design and standardization process is complete.[86] After NIST finalizes its suite of new algorithms, the selections are likely to be considered for broader standardizations for public infrastructure, such as the internet.[87]

Some firms have begun to monitor the progress of encryption updates designed to provide enhanced protection through quantum-resistant encryption. Potential factors to consider include, for example, re-encrypting sensitive data or re-signing documents while older versions are destroyed. The steps towards quantum resistance may be involved and complex and may have implications for operational performance. In light of this, some standard-setting bodies have started to prescribe steps that can be taken toward achieving quantum resistance. Of note are guidance from NIST and the European Telecommunications Standards Institute (ETSI), a non-profit standardization organization in the areas of information and communications.

- **ETSI guidance.** In a technical paper published in 2020, ETSI lays out three main steps to work towards Fully Quantum-Safe Cryptographic State (FQSCS).[88] The first involves an inventory compilation so that any migration effort can be informed by the assets that will most likely be impacted. The second step involves redesigning or retiring assets and employing quantum-safe or classical algorithms, as needed, and adopting an agile stance to upgrade when appropriate. The third step entails the execution phase and managing the transition through simulations and exercises to ensure that nothing has been overlooked in the initial inventory and planning stages.[89]

- **NIST guidance.** The National Cybersecurity Center of Excellence (NCCoE), which is part of NIST, sought to raise awareness by issuing a publication detailing the potential steps and associated challenges of migrating to PQC.[90] The publication assessed the quantum risks and complexities involved in migrating key assets and enumerated considerations for a migration plan, some of which mirror the ETSI report, including taking inventory of the ways that cryptography is used in the enterprise to inform how a migration plan may be formed.[91] NCCoE has since collaborated with public and private stakeholders to continue to raise awareness and develop processes for a migration plan.[92]

SECTION IV: Regulatory Considerations for Quantum Computing

As with any new technology, quantum computing brings with it both opportunities as well as risks. Quantum computing may have a profound impact on the securities industry, whether for larger and more well-resourced firms seeking to leverage quantum advantage or for firms of all sizes preparing to defend against attacks on present-day cryptography. In this context, market participants must consider that quantum computing can not only change the way firms do business but may also have various regulatory implications. Specifically, firms considering whether to incorporate quantum computers into their internal systems and processes as well as firms contemplating the potential threat quantum computing poses may wish to consider the following regulatory issues: cybersecurity, third-party vendor outsourcing, data governance and supervisory controls. This section provides an overview of each of these areas.

While this section underscores broad areas of regulatory importance, it does not provide an exhaustive or cumulative list of all factors and regulatory issues associated with the use of quantum computing. Moreover, this report does not create new legal or regulatory requirements or new interpretations of existing requirements, nor does it relieve firms of any existing obligations under federal securities laws and regulations. Member firms may consider the information in this report in developing new, or modifying existing, practices that are reasonably designed to achieve compliance with relevant regulatory obligations based on the member firm's size and business model. In addition, broker-dealers should conduct their own risk assessments regarding the potential regulatory implications of quantum computing as it pertains to their unique use cases and business models.

- **Cybersecurity.** Quantum computers may eventually have the capacity to break certain encryption standards broker-dealers and other members of the financial services industry currently use.[93] As a result, developments related to quantum computers may impact common applications, such as securing private communications (containing sensitive financial and account information) over the internet and verifying digital signatures. This report is in part designed to help firms become more aware and knowledgeable about the potential future opportunities and risks related to quantum. Firms that seek to move towards post-quantum readiness may also wish to consider taking inventory of their encrypted data, prioritizing the different levels of importance of such data, analyzing procedures to manage digital identity (including securing digital signatures) and migrating over time to quantum-resistant encryption methods. Firms may wish to engage NIST in their efforts to support post-quantum cryptography migration efforts.[94] In addition, if any quantum anticipatory changes relate to how firms maintain and secure customer records and information, firms should consider rules pertaining to safeguarding such data, including obligations under SEC Regulation S-P, SEC Regulation S-ID, FINRA's *Regulatory Notice 21-18* and *Notice to Members 05-49*. For additional resources, including applicable rules and guidance, firms may refer to FINRA's various reports and alerts on cybersecurity.

- **Outsourcing and Third-Party Vendor Management.** Some firms have already begun to explore quantum computing to enhance various systems and processes by accessing quantum computers through a cloud environment, in part due to the high costs and level of resources required to individually acquire, build or maintain a quantum computer. When working with third parties, including those providing services related to quantum computing, firms should be mindful of relevant FINRA guidance on outsourcing.[95] Firms that use cloud service providers to access quantum computing capabilities retain ultimate responsibility to ensure they comply with securities regulations relating to securing data. As such, depending on the type of cloud service model and the level of service, firms may consider developing controls regarding the types of software and hardware systems that the cloud service provider or the firm manages and controls. Firms may also wish to consider whether their systems are appropriately configured for the cloud and quantum computing environment, if they have proper data governance systems in place (*e.g.*, establishing data access protocols to determine which parties have access to data in the cloud) and if rollouts of the quantum related initiatives are targeted and effective. In addition, firms may refer to FINRA's Cloud Computing in the Securities Industry report for a comprehensive review of key regulatory considerations related to cloud computing, including those pertaining to recordkeeping.
- **Data Governance.** Quantum technology offers the possibility to process more data at far greater speeds, which has the potential to lead to a proliferation of data inputs. The enhanced use of different types of data enabled by quantum computing may potentially become a source of the following risks: data source verification and quality, questions around the purpose and use cases of data, and data security. As such, the importance and benefits of developing appropriate governing principles around the use and safeguarding of data may increase with the future adoption of quantum computing.[96] As a result, in the future, firms may desire to consider data quality benchmarks and metrics to assess the data inputs that they supply to quantum systems as well as how data will be stored, protected and properly used. Firms should also consider how they meet data protection requirements for safeguarding customer records and information, which are addressed in SEC Regulation S-P, SEC Regulation S-ID as well as in *Regulatory Notice 21-18* and *Notice to Members 05-49.*
- **Supervision and Controls.** Developments in quantum computing that facilitate enhanced operations by firms or result in potential threats to current encryption techniques may pose unique and complex challenges. As noted in FINRA's 2020 Risk Monitoring and Exam Priorities Letter, "[f]irms' increasing reliance on technology for many aspects of their customer-facing activities, trading, operations, back-office, and compliance programs creates a variety of potential benefits, but also exposes firms to technology-related compliance and other risks." Accordingly, based on the nature of any future developments in quantum computing, firms may wish to consider the potential impacts to their existing supervisory procedures and business continuity plans.
  - ***Supervisory Procedures.*** Quantum computers are likely to have the ability to process far greater volumes of data at far greater speeds than today's classical computers through an increasingly complex set of algorithms. The more complex the model and the application, the more vulnerable it may be to potential sources of error that could go undetected without the appropriate risk management models and supervisory controls (including enhanced testing). FINRA rules require firms to establish, maintain and enforce written procedures to supervise the types of business in which they engage and the activities of their associated persons that are reasonably designed to achieve compliance with applicable securities law and regulations, and with applicable FINRA rules. In addition, FINRA rules require firms to establish, maintain and enforce reasonable supervisory policies and procedures related to supervisory control systems that, among other things, require firms to test and verify such policies and procedures (*i.e.,* FINRA Rules 3110 and 3120).

Moreover, in the algorithmic trading context, FINRA has previously stated in the trading context that:

> As the use of algorithmic strategies has increased, the potential of such strategies to adversely impact market and firm stability has likewise grown. When assessing the risk that the use of algorithmic strategies creates, firms should undertake a holistic review of their trading activity and consider implementing a cross-disciplinary committee to assess and react to the evolving risks associated with algorithmic strategies.[97]

Similarly, with regard to algorithms used for quantum computers, firms may wish to consider potentials impact to the firm or market's stability as part of their supervisory procedures.

- ***Business Continuity Plans (BCPs)***. Firms may also wish to consider how the use of quantum computing may impact their obligations under FINRA Rule 4370, which requires firms to create and maintain a written BCP identifying policies and procedures for emergencies or other significant business disruption. The rule stipulates that such policies and procedures must be reasonably designed to enable the firm to meet its existing obligations to customers, counterparties and other broker-dealers. Developments in quantum computing may pose risks to existing methods of encryption. Accordingly, based on the nature of any future developments in quantum computing, firms may wish to consider appropriate BCP-related safeguards or contingency plans, with a particular emphasis on mission critical functions.

SECTION V: Request for Comments

FINRA encourages comments on this paper, including areas where FINRA may:

- offer guidance or modifications to its rules to address the adoption of quantum computing;
- foster greater crypto agility within firms to prepare for post-quantum cryptography; and
- seek to prepare for a quantum future while maintaining investor protection and market integrity.

FINRA also seeks input from financial industry market participants who:

- are currently exploring quantum computing, or considering how they may leverage the technology;
- are taking measures to enhance safeguards on their encrypted data, including those for quantum resistance; and
- have identified other use cases for quantum computing in the securities industry.

Comments are requested by March 15, 2024, though FINRA staff will continue to engage with market participants and welcomes input after the comment period closes. Member firms and other interested parties may submit their comments using the following methods:

- online using FINRA's comment form for this paper;
- emailing comments to pubcom@finra.org; or
- mailing comments in hard copy to:

Jennifer Piorko Mitchell
Office of the Corporate Secretary
FINRA 1735 K Street, NW
Washington, DC 20006-1506

To help FINRA process comments more efficiently, persons should use only one method to comment on the proposal.

Important Notes: All comments received in response to this paper will be made available to the public on the FINRA website. In general, FINRA will post comments as they are received.[98]

Direct inquiries regarding this paper to:

- Haimera Workie, Vice President, Office of Financial Innovation, at (202) 728-8128 or Haimera.Workie@finra.org;
- Michael Oh, Senior Director, Head of Blockchain Lab, Office of Financial Innovation, at (202) 728-8305 or Michael.Oh@finra.org; or
- Alex Khachaturian, Director, Office of Financial Innovation at (202) 728-8275 or Alex.Khachaturian@finra.org.

ENDNOTES

1 This report is not intended to express any legal position and does not create any new regulatory requirements or suggest any change in any existing regulatory obligations, nor does it provide relief from any existing regulatory obligations. This report summarizes key findings from FINRA's outreach and research on the use of quantum computing in the financial services industry, and does not endorse or validate the use or effectiveness of any of these applications. While this report highlights certain regulatory areas that broker-dealers may wish to consider, it does not cover all applicable regulatory requirements or considerations. FINRA encourages all member firms to conduct a comprehensive review of all applicable securities laws, rules and regulations to determine potential implications including any regulatory implications of using quantum computing.

2 PBS, *Quantum Mechanics*.

3 *See, e.g.*, Pavle Avramovic et al., *A Quantum Leap for Financial Services*, UK Financial Conduct Authority (FCA) Insight (July 4, 2021); DTCC, *Post-Quantum Security Considerations for the Financial Industry*, DTCC – A Whitepaper for the Industry (Sept. 2022).

4 H.R. 7535, *Quantum Computing Cybersecurity Preparedness Act*, Dec. 21, 2022.

5 Richard Waters, *Wall Street Banks Ramp Up Research Into Quantum Finance*, The Financial Times, (Jan. 6, 2020); Chris Matthews, *Quantum Computing Will be the Smartphone of the 2020s, Says Bank of America Strategist*, MarketWatch (Dec. 12, 2019).

6 Jean-Francois Bobier et al., *What Happens When "If" Turns to "When" in Quantum Computing?*, BCG (July 21, 2021) [hereinafter *Bobier Quantum*].

7 *Id.*

8 McKinsey, *Quantum Technology Sees Record Investments, Progress on Talent Gap*, April 24, 2023 [hereinafter *McKinsey Quantum*].

9 Major financial services firms such as Goldman Sachs, JPMorgan Chase and HSBC are seen as early adopters of quantum computers. Greg Noone, *Who are the Early Adopters of Quantum Computers? Big Banks, That's Who*, Tech Monitor (Jan. 12, 2023).

10 *See* Grant Salton et al., *Goldman Sachs and AWS Examine Efficient Ways to Load Data into Quantum Computers*, Amazon Web Services (AWS) Quantum Technologies Blog (Oct. 12, 2022).

11 *McKinsey Quantum* (noting $1.8 billion from the United States, $1.2 billion from the European Union and $100 million from Canada); *see also Can Europe Beat China and the US in Quantum Computing?*, Goldman Sachs (Mar. 31, 2023).

12 The Nobel Prize, press release, *The Nobel Prize in Physics 2022*.

13 Google engineers had reportedly employed a quantum computer powered by a 54 qubit processor to perform a specific computational task in 200 seconds. Such a task would have taken even the most powerful supercomputer over 10,000 years. However, other companies in the quantum space, as well as government-run enterprises, have offered differing opinions on the level of progress being made. Jose Deodoro et al. *Quantum Computing and the Financial System: Spooky Action at a Distance*, IMF Working Paper (Mar. 12, 2021) [hereinafter *IMF Quantum*]; Alvin Powell, *Harvard Quantum Initiative Co-Director Lukin on 'Quantum Supremacy' and Google's Announcement of its Achievement*, The Harvard Gazette (Oct. 29, 2019).

14 *See* Request for Comments section of this paper.

15 Cade Metz, *Google Claims a Quantum Breakthrough That Could Change Computing*, The New York Times (Oct. 23, 2019).

16 National Institute of Standards & Technology (NIST), *Quantum Logic Gates* [hereinafter *NIST Quantum Logic Gates*].

17 *Id.*

18 Joint Quantum Institute, *A Quantum Logic Gate Between a Solid-State Quantum Bit and a Photon* (Mar. 2013).

19 BBC BiteSize, *Computing Fundamentals*.

20 University of Waterloo, Institute for Quantum Computing, *What is a Qubit?*.

21 Larry Wissel, *How Does a Logic Gate in a Microchip Work? A Gate Seems Like a Device That Must Swing Open and Closed, Yet Microchips are Etched Onto Silicon Wafers That Have No Moving Parts. So How Can the Gate Open and Close?*, Scientific American (Oct. 21, 1999).

22 *NIST Quantum Logic Gates*. *See also*, Amj Dawar, *Quantum Computing, Lecture 1*, University of Cambridge, Department of Computer Science and Technology.

23 Michael Tabb et al. *How Does a Quantum Computer Work?* (July 7, 2021).

24 Carnegie Endowment for international Peace, *Implications of Quantum Computing for Encryption Policy* (Apr. 2019).

25 Daniel Colomer, *The Importance of Uncomputation: Is Quantum Mechanics Reversible?*, The Quantum Insider (May 18, 2020).

26 Monica Hernandez, *Breakthrough in Quantum Universal Gate Sets: A High-Fidelity iToffoli Gate*, Science Daily (May 24, 2022).

27 *NIST Quantum Logic Gates*.

28 Jesse Emspak, *Quantum Entanglement: A Simple Explanation*, Space.com (Mar. 16, 2022).

29 Martin Giles, *Explainer: What is a Quantum Computer? How it Works, Why It's So Powerful, and Where it's Likely to be Most Useful First*, MIT Technology Review (Jan. 29, 2019).

30 Quantum systems can be sensitive and unstable because qubits are exceptionally fragile and easily disrupted. Their coherence (*i.e.*, keeping a state of superposition and entanglement) can break down (or decohere) due to environmental "noise." Rob Matheson, *Uncovering the Hidden "Noise" That Can Kill Qubits*, MIT News (Sept. 16, 2019).

31 Jonathan Ruane, Andrew McAfee & William D. Oliver, *Quantum Computing for Business Leaders*, Harvard Business Review (Jan.–Feb. 2022).

32 Accenture, *Get Ready for the Quantum Impact*.

33 AWS, *Six Advantages of Cloud Computing*.

34 *See, e.g.,* JPMorgan Chase, *Global Technology Applied Research;* Goldman Sachs, *Engineering Quantum Algorithms*; Fidelity Center for Applied Technology (FCAT), *Observations*; HSBC, *HSBC and Quantum*; and Barclays, *Quantum Computing*.

35 Sankar Das Sarma, *Quantum Computing Has a Hype Problem*, MIT Technology Review (Mar. 28, 2022).

36 *See, e.g.,* IBM, *Exploring Quantum Computing Use Cases for Financial Services* [hereinafter *IBM Exploring Quantum*]; Sandia National Laboratories, *Quantum Optimization and Learning and Simulation* (QOALAS).

37 Jens Backes et al., *How Quantum Computing Could Change Financial Services*, McKinsey (Dec. 18, 2020).

38 *Bobier Quantum*.

39 *Commercialising Quantum Computers*, Economist (Sept. 26, 2020); Jonathan Ruane et al., *Quantum Computing for Business Leaders*, Harvard Business Review (Feb. 2022); Jens Backes et al., *How Quantum Computing Could Change Financial Services*, McKinsey (Dec. 18, 2020).

40 IBM, *Getting Your Financial Institution Ready for the Quantum Computing Revolution* (April 2019).

41 Lee Braine et al., *Quantum Algorithms for Mixed Binary Optimization Applied to Transaction Settlement* (Oct. 15, 2019) [hereinafter *Braine Quantum Algorithms*].

42 Cliff Saran, *Barclays Demonstrates Proof-of-Concept Quantum Clearing Algorithm*, Computer Weekly (Oct. 17, 2019), ("When there are hundreds of trades, classical computer algorithms begin to experience limitations.").

43 *Braine Quantum Algorithms*.

44 SEC, press release, *SEC Finalizes Rule to Reduce Risks in Clearance and Settlement* (Feb. 15, 2023).

45 BBVA, press release, *BBVA Pursues the Financial Sector's 'Quantum Advantage'* (July 17, 2020).

46 *IBM Exploring Quantum*.

47 Samuel Mugel et al., *Dynamic Portfolio Optimization with Real Datasets Using Quantum Processors and Quantum-Inspired Tensor Networks*, Physical Review Research (Jan. 3 2022).

48 *Id.*

49 *IBM Exploring Quantum*.

50 *Bobier Quantum*.

51 *Id.*; Stefan Wörner and Daniel Egger, *Speeding Up Risk Assessment Through Quantum Algorithms*, IBM (Mar. 17, 2019) [hereinafter *Wörner and Egger*].

52 Richard Waters, *Goldman Sachs Predicts Quantum Computing 5 Years Away From Use in Markets*, Financial Times (Apr. 29, 2021).

53 *Wörner and Egger*.

54 Katia Moskovitch, *Quantum Computers Could be the Ultimate Defence Against the Next Global Financial Crisis*, Wired (Jan. 3, 2019) ("[I]nstead of looking back and analysing the risk taken yesterday, a quantum computer would make it possible to react quickly to changing economic environments and make – or propose – decisions nearly instantly."); *McKinsey & Company, Quantum Computing: An Emerging Ecosystem and Industry Use Cases* (Dec. 2021) [hereinafter *McKinsey Quantum Emerging Ecosystem*].

55 *McKinsey Quantum Emerging Ecosystem*, (demonstrating that the largest global financial institutions collectively held $800 billion as a capital buffer, with an annual cost of capital worth $80 billion; one to two percent of this could free up $0.8 billion to $1.6 billion per year).

56 Tom Taulli, *Quantum Computing: What Does It Mean For AI (Artificial Intelligence)?,* Forbes (Aug. 14, 2020).

57 Maciej Lewenstein et al., *Storage Capacity and Learning Capability of Quantum Neural Networks*, Quantum Science and Technology (July 7, 2021).

58 *See, e.g.,* Dominic Widdows, *Quantum Natural Language Processing with IonQ Hardware*, IonQ (June 13, 2022).

59 *McKinsey Quantum Emerging Ecosystem*.

60 FINRA, *Artificial Intelligence (AI) in the Securities Industry*, June 2020.

61 *Id.*

62 Stephen Shankland, *Quantum Computers Could Crack Today's Encrypted Messages. That's a Problem*, CNET (May 24, 2021). The specific encryption standard cited is RSA (Rivest-Shamir-Adleman).

63 AJ Rasumsson, *The Power of Quantum Computing: Parallelism*, Conversations in Science at Indiana University, (July 13, 2019).

64 *See* Elaine Barker, *Recommendation for Key Management Part I: General,* NIST (Jan. 2016) (providing a detailed accounting of different cryptographic approaches).

65 *IMF Quantum*.

66 *Id.* (citing Grover's ability to work with unstructured data as akin to "finding a needle in a haystack").

67 Tammy Xu, *What are Quantum-Resistant Algorithms—and Why Do We Need Them?* MIT Technology Review, (Sept. 14, 2021).

68 National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (2019), [hereinafter *NAS Quantum Computing*].

69 *Id.*

70 NIST, *Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms* (Dec. 20, 2016).

71 NIST, press release, *NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat* (Apr. 28, 2016).

72 Lily Chen and Matthew Scholl, *The Cornerstone of Cybersecurity – Cryptographic Standards and a 50-Year Evolution*, NIST (May 26, 2022) [hereinafter *Chen and Scholl*].

73 Post Quantum Cryptography Team, *A Quantum World and How NIST is Preparing for Future Crypto*, NIST, (Mar. 2014) (noting the importance of performance criteria, including encryption/decryption time, key sizes, key generation time, signature size and generation/verification time).

74 NIST, press release, *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms* (July 5, 2022) [hereinafter *NIST Press Release*].

75 *Id*.

76 On August 21, 2023, NIST published a plan for post-quantum cryptography. NIST, *Quantum Readiness: Migration to Post-Quantum Cryptography* (Aug. 21, 2023).

77 *NIST Press Release*. NIST chose algorithms based on properties that lent themselves to different functions, whether general cryptography or digital signatures.

78 RSA-2048 has a key size 2048 bits long.

79 *Chen and Scholl* (noting that a doubling in key size for public keys does not equate to a doubling in key security; doubling in symmetric key size, however, may yield a doubling in key security).

80 John Carl Villanueva, *Should We Start Using 4096 bit RSA Keys?*, JScape (Oct. 3, 2022).

81 Martin Giles, *Explainer: What is Quantum Communication?*, MIT Technology Review (Feb. 14, 2019). The main advantage of quantum communications is that should an eavesdropper attempt to intercept the key, the qubits' superposition would be disturbed and collapse to a state of 0 and 1, effectively revealing the intrusion. *Id.*

82 For example, while quantum communication may theoretically provide guaranteed security, in practice, the limitations of hardware constrain such security guarantees and can even introduce new forms of attack. Moreover, quantum communications still do not get around the problem of authenticating the transmission source that, today, requires asymmetric cryptography (*i.e.*, secure key exchange).

83 Google, *HTTPS Encryption on the Web*. Https is the protocol commonly used to connect to browsers and web-based apps. https relies upon public key infrastructure, namely SSL (Secure Socket Layer) or TLS (Transport Layer Security) encryption technologies, to secure the connections.

84 Crypto assets networks, such as Bitcoin and Ethereum, face a unique challenge in upgrading their cryptographic standards due to the coordination required in distributed networks, which operate on consensus. Upgrading cryptographic standards may require a soft fork (*i.e.*, backwards compatible upgrade) whereby the network would continue to operate as users migrate to the new standard. *See* proposed approach for upgrading Bitcoin network: Dragos Ilie, *Making Bitcoin Quantum Resistant*, Imperial College London, Meng Individual Project (June 18, 2018).

85 The window of time needed to implement upgraded encryption standards is framed by Mosca's Theorem, whereby the summation of the time required to re-tool plus the time required for existing encrypted data to be secure should be less than the expected time for a large-scale quantum computer to be deployed. *See* Michele Mosca, *Cybersecurity in a Quantum World: Will We Be Ready?*, University of Waterloo, Institute for Quantum Computing, Apr. 3, 2015. *See also, HSBC Moves to Protect Operations From Quantum Cyber Threats*, Finextra (July 5, 2023); Thomas Seal, *HSBC Tests Quantum Tech in London to Guard Against Futures Hacks*, Bloomberg (July 4, 2023).

86 *NAS Quantum Computing*. NIST has also recognized in a best case scenario that a full migration would take five to 15 years. *See* William Barker et al., *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*, NIST Cybersecurity White Paper (Apr. 28, 2021) [hereinafter *Barker et al.*].

87 For example, through the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), all of which contribute to governing security on the world's infrastructure, such as the internet.

88 European Telecommunications Standards Institute (ETSI), *Cyber: Migration Strategies and Recommendations to Quantum Safe Schemes, Technical Report* (2020).

89 *Id.*

90 William Barker and William Polk and Murugiah Souppaya, *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*, NIST (Apr. 28, 2021).

91 *NAS Quantum Computing*; NIST has also recognized in a best case scenario that a full migration would take five to 15 years; *see Barker et al*.

92 NIST, *Migration to Post-Quantum Cryptography*, (June 2020) [hereinafter *NIST Migration to Post-Quantum Cryptography*].

93 It is important to note that sound cyber practices that prevent malicious actors from accessing sensitive data in the first place provides an additional security layer.

94 *NIST Migration to Post-Quantum Cryptography*.

95 *See e.g.*, *Notice to Members 05-48*, Members' Responsibilities When Outsourcing to Third Party Providers; FINRA *Regulatory Notice 21-29*, FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors.

96 World Economic Forum, Insight Report, *Quantum Computing Governance Principles*, Jan. 2022.

97 FINRA, *Regulatory Notice 15-09* on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies, Mar. 2015.

98 Parties should submit in their comments only personally identifiable information, such as phone numbers and addresses, that they wish to make available publicly. FINRA, however, reserves the right to redact or edit personally identifiable information from comment submissions. FINRA also reserves the right to redact, remove or decline to post comments that are inappropriate for publication, such as vulgar, abusive or potentially fraudulent comment letters.