# An Introduction to Quantum Computers and Their Effect on Banking Institutions

Tae L. Aderman[1]

[1] Antonin Scalia Law School, George Mason University, Arlington, Virginia, USA

Correspondence: Tae L. Aderman, Antonin Scalia Law School, George Mason University, Arlington, Virginia, USA.

Received: April 24, 2019 Accepted: May 21, 2019 Online Published: May 28, 2019

doi:10.5430/ijfr.v10n4p17 URL: https://doi.org/10.5430/ijfr.v10n4p17

**Abstract**

Quantum computers leverage the incredible and dynamic properties behind quantum physics. In doing so, these computers are able to solve mathematical equations that, as of now, cannot be solved using today's conventional computers. Realizing the potential that quantum computers represent, banking institutions are beginning to both analyze and apply these computers' use potential, particularly in increasing the efficiency and speed of complex transactions. Simultaneously, banking institutions must also carefully examine quantum computers' ability to bolster cybersecurity defenses. In the age of quantum computers, existing defenses will prove inadequate, even to lattice-based cryptography. At the dawn of the quantum age, banking institutions are in a unique position to leverage not only quantum computers' vast computing power in completing complex transactions, but also to use such computers to counter the threat of quantum cybersecurity threats.

**Keywords:** quantum computers, cybersecurity, banking institutions, superposition, entanglement

## 1. Introduction

Quantum computers are computers of tomorrow. Operating at the particle level, quantum computers use spinning subatomic particles to solve equations so complex that current computers cannot solve or solve within any reasonable timeframe. Using principles of quantum physics, such as superposition and entanglement, quantum computers may sound like science fiction. To the contrary, not only are quantum computers reality today, albeit in limited form, they have a profound ability to affect the financial industry, specifically banking institutions, in the near future. However, the boundless technological potential which quantum computers represent is a double-edged sword. While quantum computers can exponentially increase banks' efficiency, for instance, so too can nefarious actors, including hackers and nation-states, leverage quantum computers to break existing encryption keys and attack consumer information.

Banking institutions must quickly foresee a world that has realized quantum computers. Some anticipate a working quantum computer that can solve real-world mathematical problems within ten years. Solving such problems will overcome great difficulties in comporting and resolving complex transactions. Banking institutions must understand quantum computers' future ability to shore up cybersecurity defenses in preparation for the exponential risks posed by the same computers used in the wrong hands. Some individuals propose existing lattice-based cryptography as a sufficient defense to quantum computer-based attacks. This proposition incorrectly presupposes a ceiling on quantum computers' future abilities, abilities which in their infancy cannot be so readily calculated. By advancing the use of quantum computers as a powerful tool to counter quantum computer-based cybersecurity threats, banking institutions will find themselves well-prepared for the coming quantum age.

## 2. The Amazing Potential of Quantum Computers

Computers of today are constrained by the laws of physics. These so-called "classical" computers rely upon "bits" to communicate information. A bit is a binary digit because it can represent either "1" or "0" at any given time but cannot represent both 1 and 0 simultaneously. The bit can only represent one value at a time because information is stored on tiny magnets. An electrical pulse orients the magnet in a particular direction, thereby representing 1, while no pulse allows the magnet to represent zero. It takes at least eight sequential bits to represent one "byte." A byte can "represent a letter, a number, a symbol, or other information a computer or program can use" (Mitchell, 2019). For instance, the letter "K" could be represented by "01001011 (although this would then be translated into a hexadecimal code of "4B" for ease of use)" (New Jersey Institute of Technology). A 100 Mbps (megabytes per second) network speed transfers

"100 million bits per second" (Mitchell, 2019). In searching for a "needle" in a haystack, a classical computer examines each piece of hay individually.

Unlike classical computers, which rely upon bytes, quantum computers transcend "traditional laws of physics" through the use of quantum physics (Marr, 2017). In doing so, quantum algorithms "zero-in on the most probable solution and then progressively uncover the actual needle" (Trounson, 2018). This more efficient and far quicker calculation requires a special quantum bit, or "qubit," which can represent both 1 and 0 simultaneously. But any conversation about qubits and quantum physics necessarily requires a dive into the particle level of our world. For one, gravity "produces a negligible effect at the particle level" (Lin, 2018). So-called "quantum elements, like atomic or subatomic particles (electrons and photons), or microscopic circuits that . . . behave quantum mechanically" are particularly fragile and complex, thereby presenting unique challenges (Trounson, 2018).

Qubits require special testing environments including cryogenic freezers to "simulate the quantum structure of the universe" (Rogoway, 2018). Testing at temperatures as low as -460 degrees Fahrenheit (-273,33 degrees Celsius) are conducive for liquid helium in a superfluid state of zero viscosity. Particles are then suspended in the helium. Suspended in this almost otherworldly substance, a qubit applies superposition and entanglement to create an exponential increase in calculating speed.

The dual-state ability to represent both 1 and 0 simultaneously is explained by superposition, a principle illustrated by Erwin Schrödinger's famous thought experiment involving a cat. Here, Schrödinger set forth a hypothetical in which a cat was placed in a box with some form of explosive. The outside viewer would be unable to ascertain whether the explosive had detonated and killed the cat, or if the explosive remained intact thereby leaving the cat alive and well. Prior to inspection, the cat existed in a superposition. The cat was both alive and dead because its actual state was only made known by the outside viewer examining the box.

This thought experiment is important to understand because it illustrates a key component of quantum computers, namely superposition, which explains how two qubits can represent four states simultaneously. In 2018, Aldeniz Rashidov succinctly stated that

"[i]n the classic computer, 2 bits stored two data, 2 qubits stored 4 different data, 3 bits stored 3 data, 3 qubits stored 8 data. While the total information stored by the bits is equal to their sum (1 + 1 + 1 + … = n), the information stored by the qubits increases exponentially (2 x 2 x 2 . . . = 2n)" (Rashidov, 2018).

Were one to input "101" into a classical computer in order to calculate all combinations of the three digits, the classical computer might first produce an output of "110." Subsequently, the classical computer could then output "011" and so forth until all combinations of the original input of "101" were deduced. In contrast, a quantum computer can deduce all combinations of the input simultaneously, thereby producing an exponentially higher power output. For instance, while two qubits produce 2^2 times processing power, an additional qubit would provide 2^3 times processing power, or "eight states at the same time" (O'Connell, 2016). "And 64 qubits would provide 2^64 "possibilities . . . [equaling] one million terabytes worth" of processing power (O'Connell, 2016).

Just as the cat is either alive or dead the moment the box lid is opened, so too does a qubit exhibit a particular value upon reaching its calculation. At the conclusion of the calculation, the superposition "collapse[s], leaving the outcome of said calculation for examination" (Hardesty, 2015).

Alongside superposition, the quantum principle of entanglement explains how qubits "behave in unison" (Solenov, D., *et al.,* 2018). Entanglement is key because if the qubits are not working in unison, "then all you [have] . . . is a very expensive classical computation" (Vance, 2018). In Schrödinger's thought experiment, the cat and the explosive are entangled. The cat's fate rests upon, or is entangled with, the existence of the explosive. Entangled qubits act together in order to yield greater simultaneous states, and thereby bring calculations to greater scale. Last year, German and Austrian scientists were able to entangle 20 qubits. The scientists used lasers and a magnetic field to trap, and then entangle, individual calcium ions.

IBM has created 20 qubit and 50 qubit quantum computers while Google has created a 72-qubit quantum computer. However, these three quantum computers have not yet entangled qubits at any high rate (for instance, Google has focused on entangling nine qubits). When scientists are able to entangle a greater number of qubits, quantum computer usability will sky rocket. At that moment, society will reach "quantum supremacy." This term refers to the defining moment when quantum computers "best a classical [computer] in a useful task" (Ornes, 2019). Scientists theorize that this moment will be achieved when 100 qubits are successfully entangled. Mathematically, 100 "qubits can represent 1.3 quadrillion quadrillion" states simultaneously (Hutchinson, 2016). That is, quantum supremacy would be reached at googol, or 10^100, a number made famous by the search engine of a similar name, "Google." Even without reaching

quantum supremacy, Google's quantum computer, named Bristlecone, can "solve problems a *billion times* faster than a classical computer" (Ornes, 2019). That is, in entangling nine qubits, Bristlecone's qubits are simultaneously representing 10^9 states. But the calculations are less useful and more demonstrative in nature. Bristlecone's lack of practicality demonstrates that quantum computers must improve before their use becomes widespread.

For one, quantum computers must reduce their current error rate. Quantum error correction seeks to address undesired entanglements. Two qubits that are improperly entangled will yield an incorrect result upon the superposition's collapse. "Noise," such as "[t]he feeblest magnetic field or stray microwave pulse," can corrupt a qubit (Wolchover, 2019). Scientists are working on complex algorithms to reduce the error rate and bring greater stability to qubits. Google researchers are "aiming for an error correction of 10^-3 in about 10^3 qubits" (Trader, 2018). Separately, in 2014, scientists theorized that quantum algorithms that might explain the interconnectivity between space and time might also be applied to reduce a quantum computer's error rate. Other theories have been posited by Peter Shor (who, in 1994, set forth Shor's Algorithm, "an algorithm that would enable a quantum computer to factor large numbers exponentially faster than a conventional computer can" (Hardesty, 2016)) showing that a qubit suspended in superposition could be determined relative to its entangled qubits without collapsing the superposition. If the determination found that the qubit had a different value than the qubit which it was entangled with, the first would correct its value accordingly. Unfortunately, as recently as late 2018, even Professor Shor noted that "it's not obvious that quantum error correction is possible" (Shor, 2018). This statement should be taken as less a definite proclamation and more an observation that scientists must reduce noise before quantum supremacy is reached. Regardless, as error rates decrease, the number of entangled qubits will continue to increase, all leading towards the inevitable moment scientists achieve quantum supremacy.

### 3. Banking Institutions' Future With Widespread Use of Quantum Computers

Notwithstanding the recent entanglement of 20-qubits, much of quantum computers' application remains theoretical. Regardless, both the future threat and use potential that this nearly unlimited computing power represents to banking institutions cannot be emphasized enough. Quantum computers have opened a gateway into the imagination by taking what was once theoretical and turning it into a tangible. Their incredible potential is still constantly being explored and built upon. For instance, in March of 2019, researches used a quantum computer to reverse simulate a single particle's wave function. A wave function's value "at a given point of space and time is related to the likelihood of the particle's being there at the time" (Editors of Encyclopaedia Britannica ). Though it is a misnomer to describe this successful simulation as having reversed time, the quantum computer had effectively undone "time's effect" (Fore, 2019). The simulation provides a glimpse of the unlimited, and perhaps yet to be imagined, potential yet to come.

While companies like Microsoft, Google, and IBM are bringing quantum computers to life, and in doing so transcending science fiction, these companies' application of quantum computers computing power remains limited. However, with some estimates placing quantum computers' dependable use coming as soon as 2025, many banking institutions such as Barclays, JPMorgan Chase, and Morgan Stanley are already gravitating towards quantum computers for their exponential increase in computing power and future reduction in energy use thereby making transactions more stable in reducing the frequency of errors within a respective transaction. Indeed, through the use of IBM's Q Network, a quantum computer with cloud capabilities, mathematicians are working on optimizing the efficiency of complex transactions that may "have varying credit, collateral and liquidity constraints" (Crosman, 2017). These banks have identified what quantum computers are "really good at: crunching numbers . . . and searching databases" (Lafrance, 2014).

Alongside increased efficiency and an anticipated reduction in energy consumption, banking institutions should also gravitate towards quantum computers' application specific to anticipated increases in cyber security necessitated, in part, by quantum computers' potential use as a weapon. Crunching numbers is intrinsically a "math problem," or in other words, is directly related to cybersecurity and cryptography. Ensuring data is secure from attack is paramount. Banks hold not just money but also valuable consumer information. For instance, "[a]bout 10% to 15% of [banks'] data . . . [is] considered nonpublic, such as Social Security numbers" (Sperling, 2010).

Currently, the National Institute of Standards and Technology (or "NIST"), which sits under the U.S. Department of Commerce, has established private data standards. Industry standards include "AES (128 bits and higher), TDES (minimum double-length keys), RSA (2048 bits and higher), ECC (160 bits and higher), and EIGamal (1024 bits and higher)" (Probasco, 2017). Additionally, the Gramm-Leach-Bliley Act (the "Act'), in conjunction with the Federal Financial Institutions Examination Council ("FFIEC"), require specific data be encrypted including (1) personally identifiable information, (2) financial information such as payment history or credit/ debit card purchases, and (3) information obtained while providing services such as court records.

While the Act and the FIIEC require banking institutions safeguard certain information, the industry is left to determine the best type of encryption for its respective data. Leaving the method of encryption to banks is beneficial though this method has drawbacks. Because of the various bit rates that have been embraced by the industry, banks are able to determine which is best for the particular data being encrypted. For instance, a transfer of data that is otherwise a small byte size might be quickly transferred using AES. If the data is particularly sensitive, the banking institution might opt for a more secure RSA encryption method.

Were the Act to be amended to require specific encryption methods be adopted, smaller banking institutions such as local credit unions might have difficulty onboarding complex encryption methods regardless of the sensitivity of the data being stored or transferred. A harsh cybersecurity regulatory burden might cause smaller institutions to merge with a larger regional institution due to transactional costs associated with implementing a complex cybersecurity platform. However, by gradually requiring banking institutions embrace certain encryption methods would reduce the transactional costs associated with embracing new or complex technology. This gradual approach would, in theory, also offset the technology's reduction in price over time.

Currently, quantum computers' technology might be too nascent for the Act, the FIIEC, and other governmental stakeholders to create quantum computer industry standards for banking institutions. With quantum supremacy not yet reached, the ambitious outlook for quantum computers' power might leave crafting a regulatory framework imprecise and vulnerable to being theoretical instead of practical. For instance, were the Act to require a banking institution develop methods to counter a quantum computer's attack, and were the banking institution required to counter such attack by embracing its own quantum algorithm, either through a cloud platform such as IBM's Q Network or through its own brick-and-mortar application (assuming the cost of doing so had decreased), the algorithm might necessarily have to assume a certain number of qubits involved in the attack in order to successfully defend itself. Scientists are still philosophizing about the qubit size necessary to make a quantum computer sufficiently dangerous. It might be similarly imprudent to ask government agencies, such as NIST, to develop regulations specific enough to determine the qubit size required for a sufficient defense.

Yet, in a quantum world where everything might seem backwards, even this logic is susceptible to attack because it hinges upon knowing the qubit rate required for an attack before acting upon a defense. By then, an attack could already be launched before a regulation has even finished with the notice and comment period.

Perhaps for this reason, amongst myriad others, government agencies are acting with existing technology that is currently accessible. NIST is in the process of creating a post-quantum cryptography standardization. Also referred to as quantum-resistant cryptography, this standardization seeks to "develop cryptographic systems that are secure against both quantum and classical computers" (Probasco, 2017). The standardization process would set forth minimum acceptability requirements for "candidate algorithms" (Probasco, 2017). NIST's quantum-resistant cryptography relies on algorithms running on classical computers. Known as "lattice-based cryptography," (Alwen, 2018) classical algorithms could provide a basis for securing existing networks employed by banking institutions to secure sensitive information without investing in quantum technology.

The lattice-based cryptography counterargument to institutions having to deploy quantum computers to counter equally well-armed nefarious actors predicates on an assumed ceiling as to the ability of quantum computers. The argument is strong in part because, while quantum supremacy may very well be reached at 100 entangled qubits, Brian LaMacchia of Microsoft estimated that a quantum computer will require 1000 entangled qubits to "represent a serious cryptographic threat" (Hutchinson, 2016). In contrast, Konstantinos Karagiannis of Black Hat hypothesized that current public-key cryptography will be vulnerable to a quantum computer simply running Shor's Algorithm. Once a sufficient number of qubits are entangled, Shor's Algorithm should be able to effectively break public-key encryptions. Shor's Algorithm is designed specifically for quantum computers. However, it remains unclear how many qubits are needed to break various bit-size public-key codes.

Outside of governmental organizations such as NIST, non-governmental entities such as the International Organization for Standardization ("ISO") are working to bring cybersecurity standards up to speed. ISO recently published ISO/IEC 27000:2018, a broad document relevant for information security management systems. Although this document is not specific to banking institutions, it is designed to "help organizations to assess and review their current controls that are being managed through" ISO's complementary standards (Naden, 2019).

Even then, as standards are constantly evolving to match the threat posed by nefarious actors, banking institutions remain vulnerable. Last year, the Boston Consulting Group ("BCG") identified seven key risk areas.

- A misunderstanding or lack of information related to threats;

- A failure to prioritize cybersecurity including the tendency to isolate information technology departments;
- A habitual focus on prevention instead of focus upon detection and response;
- A failure to hire qualified cybersecurity professionals;
- A tendency to outsource cybersecurity coupled with a tendency to build weak third-party management and oversight;
- A lack of a "security-aware" culture; and
- A failure to marry human capital with technology, thereby leading to operational breakdowns in responding to, or preventing, threats. (Grasshoff, G., *et al.*, 2018).

These weaknesses should not come as a surprise. Ultimately, BCG's study illustrates a seemingly reactive approach to cybersecurity. Cybersecurity needs that are outsourced or de-emphasized cannot be expected to approach the looming threat posed by quantum computers in an active manner.

Government regulations such as those found in the Act are similarly insufficient for the quantum age. For one, the regulatory language tends to be broad. The Federal Trade Commission ("FTC") has promulgated myriad regulations affecting the security measures of entities engaged in commercial practices. Any financial institution as defined by the Act is required to comply with the FTC's Safeguards Rule. § 314.4 sets forth more specific requirements including designating an employee to manage an information security program, design and implement safeguards, and monitor and evaluate the implemented safeguards. Yet, the regulatory landscape lacks an awareness of evolving threats posed by quantum technology, specifically in relation to a future involving nefarious actors using quantum computers to break existing cryptographic systems designed to protect classical computers. Regulations' broad language sets forth numerous requirements yet fails to specify demanding technical requirements that would strengthen banking institutions' existing cyber security defenses.

Additionally, local or regional banking institutions that are smaller than JPMorgan Chase or other large banks may have the resources to comply with the Act, but not have the necessarily resources to actively implement a sufficient defense to a future quantum attack. The government can continue to rely on NIST and organizations like the ISO to create tailored industry standards that are considerate of banks' varied abilities while still implementing regulations that safeguard consumer's personally identifiable information. Simultaneously, banking institutions can continue to apply a "defense in-depth" method by layering protections before the first quantum attack. A layered defense may include lattice-based cryptography operating on a classical computer and quantum algorithms operating on a third-party's quantum cloud system. By using a combination of quantum algorithms and lattice-based cryptography, banking institutions can be better prepared for the transitional period during which nefarious actors' transition from using classical computers to quantum computers.

## 4. Conclusion

It seems certain that quantum computers will reach quantum supremacy sooner rather than later. Just 25 years have passed since Peter Shor mathematically demonstrated the possibility of a quantum computers' relevance in achieving what a classical computer could not. As Moore's Law continues to plateau, quantum computers open the door to continued growth.

Banking institutions are already aware of the possible benefits of quantum computers. Yet, as scientists continue to entangle qubits at a greater rate while reducing the error rate, banking institutions must also be responsive to the rapidly evolving technological landscape, and not just to capitalize on the amazing computing power quantum algorithms provide to transaction speeds. NIST, the FIIEC, and the ISO must continue to help shape industry standards in order to ensure that banking institutions well-prepared to defend against the new age of cyber security.

## Acknowledgements

I would like to thank Noori Ali for her support and encouragement, Professor Robert Ledig and Professor Adam Golodner of the Antonin Scalia Law School at George Mason University for their inspiration and guidance, Asif Ali for his post-review technical assistance, and Sanah Ali for her post-review proof reading and writing assistance.

## References

(Author unknown). (Date unknown). *Bits vs. Bytes*. New Jersey Institute of Technology. Retrieved from https://web.njit.edu/~walsh/powers/bits.vs.bytes.html

(Author unknown). (Date unknown). *Post-Quantum Cryptography*. National Institute of Standards and Technology. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

16 C.F.R. §313.3(k).

16 C.F.R. §314.4.

Alwen, J. (2018, June 15). What is Lattice-based cryptography & why should you care. *Medium*. Retrieved from https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717

Ball, P. (1990, January 14). Entangled photons and quantum computers. *Nature.* https://doi.org/10.1038/news990114-9

Beall, A., & Reynolds, M. (2018, February 16). *What are quantum computers and how do they work? WIRED explains*. Wired. Retrieved from https://www.wired.co.uk/article/quantum-computing-explained

Beebe, J. (2018, October 31). *How old-school silicon could bring quantum computers to the masses*, Fast Company. Retrieved from https://www.fastcompany.com/90242006/old-school-silicon-could-bring-quantum-computers-to-the-masses

Bergy. (2016). Quantum computing and cryptography: Are Steemit and bitcoin safe?. *Steemit*. Retrieved from https://steemit.com/steemit/@bergy/quantum-computing-and-cryptography-is-bitcoin-safe

Castelvecchi, D. (2018, September 18). Reimagining of Schrödinger's cat breaks quantum mechanics - and stumps physicists. *Nature*. Retrieved from https://www.nature.com/articles/d41586-018-06749-8

Cox, J. (2014, September 18). Your Encryption Will BE Useless Against Hackers with Quantum Computers. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/vvbz9m/your-encryption-will-be-useless-against-hackers-with-quantum-computers

Crosman, P. (2017, December 14). JPMorgan Chase, Barclays join IBM quantum computing network. *American Banker*. Retrieved from https://www.americanbanker.com/news/jpmorgan-chase-barclays-join-ibm-quantum-computing-network

Crosman, P. (2018, July 16). Why banks like Barclays are testing quantum computing. *American Banker*. Retrieved from https://www.americanbanker.com/news/why-banks-like-barclays-are-testing-quantum-computing

Editors of Encyclopaedia Britannica. (Date unknown). *Wave function*. Encyclopaedia Britannica. Retrieved from https://www.britannica.com/science/wave-function

Evenden, I. (2017, April 14). *Quantum computing comes of age*. alphr. Retrieved from https://www.alphr.com/science/1006617/quantum-computing-comes-of-age

Federal Trade Commission. (Date unknown). *Financial Institutions and Customer Information: Complying with the Safeguards Rule*. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

Fore, M. (2019, March 15). Physicists Reverse Time for Tiny Particles Inside a Quantum Computer. *Live Science.* Retrieved from https://www.livescience.com/65000-quantum-computer-turns-back-time.html

Galeon, D. (2017, November 11). IBM Just Announced an Insanely Powerful 50-Qubit Quantum Computer. *Science Alert.* Retrieved from https://www.sciencealert.com/ibm-50-qubit-quantum-computer-breakthrough-news

Gibney, E. (2017, March 8). *Magnetic hard drives go atomic*. https://doi.org/10.1038/nature.2017.21599

Grasshoff, G., Bohmayr, W., Papritz, M., Leiendecker, J., Dombard, F., & Bizimis, I. (2018, August 1). *Banking's Cybersecurity Blind Spot-and How to Fix It*. BCG. Retrieved from https://www.bcg.com/en-us/publications/2018/banking-cybersecurity-blind-spot-how-to-fix-it.aspx

Greenemeier, L. (2018, May 30). How Close Are We-Really-to Building a Quantum Computer?. *Scientific American.* Retrieved from https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer/

Hardesty, L. (2015, May 26). Researchers Develop a New Quantum Error Correcting Code. *SciTechDaily*. Retrieved from https://scitechdaily.com/researchers-develop-a-new-quantum-error-correcting-code/

Hellemans, A. (2018, April 16). 20 Entangled Qubits Bring the Quantum Computer Closer. *IEEE Spectrum*. Retrieved from

https://spectrum.ieee.org/tech-talk/computing/hardware/20-entangled-qubits-brings-the-quantum-computer-closer

Holden, J. (2017, December 27). How Classical Cryptography Will Survive Quantum Computers. *Nautilus*. Retrieved from http://nautil.us/blog/-how-classical-cryptography-will-survive-quantum-computers

Hui, J. (2018, December 12). QC - Cracking RSA with Shor's Algorithm. *Medium*. Retrieved from https://medium.com/@jonathan_hui/qc-cracking-rsa-with-shors-algorithm-bc22cb7b7767

Hutchinson, A. (2016, September 26). Hacking, Cryptography, and the Countdown to Quantum Computing. *The New Yorker*. Retrieved from https://www.newyorker.com/tech/annals-of-technology/hacking-cryptography-and-the-countdown-to-quantum-computing

*ISO/IEC 27000*. (2018). *International Organization for Standardization*. Retrieved from https://www.iso.org/standard/73906.html

Jones, B. (2018, March 7). Google Just Unveiled the World's Most Advanced Quantum Processor by Far. *Science Alert*. Retrieved from https://www.sciencealert.com/google-bristlecone-quantum-computing-72-qubits-chip

Kahn, J. (2018, June 29). Why Quantum Computers Will Be Super Awesome, Someday. *Bloomberg Businessweek.* Retrieved from https://www.bloomberg.com/news/articles/2018-06-29/why-quantum-computers-will-be-super-awesome-someday-quicktake

Kramer, M. (2013, August 14). The Physics Behind Schrödinger's Cat Paradox. *National Geographic.* Retrieved from https://news.nationalgeographic.com/news/2013/08/130812-physics-schrodinger-erwin-google-doodle-cat-paradox-science/

Krupansky, J. (2018, September 30). Some Preliminary Questions About Shor's Algorithm for Cracking Strong Encryption Using a Quantum Computer. *Medium.* Retrieved from https://medium.com/@jackkrupansky/some-preliminary-questions-about-shors-algorithm-for-cracking-strong-encryption-using-a-quantum-b3470546249c

Kumar, A. (Year unknown, February 7). (Almost) everything you ever wanted to know about quantum computers. *freeCodeCamp.* Retrieved from https://medium.freecodecamp.org/almost-everything-you-ever-wanted-to-know-about-quantum-computers-5ee6bc2f40ba

Lafrance, A. (2014, June 4). The NSA Probably Really, Really Wants a Quantum Computer. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2014/06/the-nsa-probably-really-really-wants-a-quantum-computer/372145/

Lin, T. (2018, November 14). How Holography Could Help Solve Quantum Gravity. *Quanta Magazine*. Retrieved from https://www.quantamagazine.org/albert-einstein-holograms-and-quantum-gravity-20181114/

Marr, B. (2017, July 4). What is Quantum Computing? A Super-Easy Explanation for Anyone. *Forbes*. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/07/04/what-is-quantum-computing-a-super-easy-explanation-for-anyone/#1340303a1d3b

Mitchell, B. (2019, January 2). What is a Bit in Computer Networking. *Lifewire.* Retrieved from https://www.lifewire.com/definition-of-bit-816250

Naden, C. (2019, February 4). Stronger data protection with updated guidelines on assessing information security controls. *International Organization for Standardization.* Retrieved from https://www.iso.org/news/ref2367.html

O'Connell, C. (2016, August 8). Quantum computing for the qubit curious. *Cosmos.* Retrieved from https://cosmosmagazine.com/physics/quantum-computing-for-the-qubit-curious

Okinawa Institute of Science and Technology (OIST) Graduate University. (2019, February 12). To design future quantum technologies, scientists pinpoint how microwaves interact with matter. *ScienceDaily*. Retrieved from https://www.sciencedaily.com/releases/2019/02/190212094842.htm

Ornes, S. (2019, January 15). State of Science: Approaching Quantum Supremacy. *Discover*. Retrieved from http://discovermagazine.com/2019/jan/quantum-supremacy

Probasco, L. (2017, April 25). Encryption Requirements for Banks & Financial Services. *Townsend Security Data Privacy Blog*. Retrieved from https://info.townsendsecurity.com/encryption-requirements-for-banks-financial-services

Rashidov, A. (2018, January 16). Bits vs. qubits. Difference between conventional computer and the new generation quantum computer. *Aldeniz Rashidov: Personal Blog*. Retrieved from https://blog.aldeniz.eu/?p=434&lang=en

Rogoway, M. (2018, October 5). Intel plots a weird, spooky future in quantum computing. *The Oregonian*. Retrieved from https://www.oregonlive.com/silicon-forest/2018/10/intel_plots_a_weird_spooky_fut.html

Shor, P. (transcription by Wei, A). (2018, December 7). Peter Shor on Quantum Error Correction. *Windows on Theory*. Retrieved from https://windowsontheory.org/2018/12/07/quantum-error-correction/

Simonite, T. (2016, May 13). Moore's Law Is Dead. Now What?. *Technology Review*. Retrieved from https://www.technologyreview.com/s/601441/moores-law-is-dead-now-what/

Skillcrush. (2019, January 24). The Horrible Name that Google Was ALMOST Called-And How They Came up with Google Instead. *Skillcrush*. Retrieved from https://skillcrush.com/2013/11/12/horribly-google-called-google/

Solenov, D., Brieler, J., & Scherrer, J. F. (2018, September-October). *The Potential of Quantum Computing and Machine Learning to Advance Clinical Research and Change the Practice of Medicine*, 115 Mo. Med. 463. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6205278/

Sperling, Ed. (2010, March 29). Banks: Keeping Customer Data Safe. *Forbes*. Retrieved from https://www.forbes.com/2010/03/29/capitalsource-bank-security-technology-cio-network-honan.html#50bb709da848

Starr, M. (2018, April 16). Physicists Just Broke a Quantum Record, Taking Entanglement to a Spooky New Level. *Science Alert*. Retrieved from https://www.sciencealert.com/quantum-computing-broken-20-qubit-quantum-register

Trader, T. (2018, April 27). Quantum Error Correction: Google Takes on Qubit Accuracy. *Enterprise AI*. Retrieved from https://www.enterpriseai.news/2018/04/27/quantum-error-correction-googles-strategy-for-qubit-accuracy/

Trounson, A. (2018, October 3). Grasping the 'Spooky' in Quantum Physics. *Pursuit*. Retrieved from https://pursuit.unimelb.edu.au/articles/grasping-the-spooky-in-quantum-physics

Vance, E. (2018, April 30). These 'Spooky' Entangled Atoms Just Brought Quantum Computing One Step Closer. *Live Science*. Retrieved from https://www.livescience.com/62433-most-entangled-qubits-quantum-computer.html

Wilczek, F. (2019, March 14). The Quantum Computers in Our Future. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/the-quantum-computers-in-our-future-11552579161?mod=searchresults&page=1&pos=2

Wolchover, N. (2019, January 3). How Space and Time Could Be a Quantum Error-Correcting Code. *Quanta Magazine*. Retrieved from https://www.quantamagazine.org/how-space-and-time-could-be-a-quantum-error-correcting-code-20190103/

Zaccaria, E. (2018, January 9). Quantum computers: cyber-security threats for the banking and financial sector. Global *Banking & Finance Review*. Retrieved from https://www.globalbankingandfinance.com/quantum-computers-cyber-security-threats-for-the-banking-and-financial-sector/