How Quantum Computing Impacts Cyber Security

Abdulbast A. Abushgra
Cybersecurity Department, Utica University
Utica, NY 13502 USA
aaabushg@utica.edu

***Abstract*— Cybersecurity confronts several challenges in the current and upcoming decades. Quantum computing might be one of these challenges that is the worst. Usually, cybersecurity provides techniques, standards, policies, configurations, and recommendations to protect classical system assets. According to the CIA triad (Confidentiality, Integrity, and Availability) fundamentals and the current domain structures used in the classical IT infrastructure systems, vulnerability may occur at any time and place, where several technical and non-technical foundations have been breached aggressively during the past ten years. These breaches are based on classical weaknesses, whether in the offensive or defensive platforms. Quantum computing might be the solution to these problems. However, quantum computing will be a part of the problem, since quantum usage requires a variety of devices, software, applications, and policies. Most of these requirements are still not ready to be approved or even exist. This paper focuses on the logical readings of the near future when quantum computers become available or before. In addition, some advantages and disadvantages are concluded to declare some circumstances that probably face cybersecurity in the upcoming decades.**

Keywords—cybersecurity, quantum computing, quantum key distribution (QKD), Security, and Privacy.

I. INTRODUCTION

Computers are designed to do arithmetic calculations. These arithmetic calculations represent different types of tasks, for instance, solving different problems. These problems are generally classified as solvable or unsolvable based on the classical system scale. Classical computers during the past decades have processed a variety of complicated problems. However, the classical scale may be interrupted by quantum computers, where quantum systems initially can perform more complicated problems in a short time. Hence, the classical system could no longer be an option for securing data and systems. As a challenge, cybersecurity may face tremendous issues that are perhaps generated by the gap between classical and quantum systems. The governments have highlighted the close relationship between these movements that should be addressed between the quantum computers and how data remains secure in the classical system.

One of the desired achievements that companies and researchers are willing to approach is narrowing the gap between the threat of quantum computing power and cybersecurity. As is obvious, the classical system uses many types of cryptographic methods to keep data encrypted or secure, whether the actual data is in transit, at rest, or in use. Although quantum computers are unavailable commercially right now, the potential threat of breaking most of the classical system encryption and decryption methods, if not all, is possible. The most technical and cryptographic methods used in the classical system, such as RSA, have been considered secure methods for decades. However, Shor's algorithm could deliver another approach that considers the RSA no longer secure if quantum computers become fully functional and reliable. In this paper, there will be a brief description of the classical system's fundamentals in Section II. Section III describes the quantum system, the future of potential services, and the cryptographic tools. Section IV discusses cybersecurity challenges, and Section V discusses the benefits and drawbacks of quantum systems, respectively.

II. CLASSICAL SYSTEM

A. Classical Computing

A set of combined processes and processors could solve a complicated problem in a short time. This combination represents a physical and logical process, where the physical processors reflect the hardware in the computerized devices. The logical process is more elastic compared to the physical components. In addition, the logical process illustrates some of the functional actions, these actions are written and designed based on the algorithm. This algorithm may be written in any programming language that provides more availability. This in general covers the client (Alice) and server (Bob), and those sides could be any device or application. For instance, clicking on an application icon on any operating system (e.g., Windows, Mac, Linux, or Unix) and requesting access to any service means client and server communications. The requester is usually the client, and the web application or any service represents the server. Nowadays, these communications are mostly processed through the Internet.

B. Services

Worldwide, users of the Internet have reached more than 5.00 billion users, or 66.2% of the global population according to 2022 statistics [1]. Hence, giant infrastructures were built to deliver these services to consumers. As the number of users is still increasing every second, keeping the flow of data smooth and secure is difficult and costly. Banks, schools, energy plants,

979-8-3503-3556-9/23/$31.00 ©2023 IEEE

manufacturers, transportation infrastructure, and health systems are part of the digital world. In addition, according to census.gov, the number of populations who use the Internet from 1984 to 2011 increased dramatically, as illustrated in Table 1.

TABLE 1, HOUSEHOLDS WITH A COMPUTER, AND INTERNET USE: 1984 TO 2011(IN THOUSANDS).

Selected Characteristics	Total	Household with a computer at home (%)	Households with Internet use at home (%)
2011	119,250	75.6	71.7
2010	119,545	76.7	71.1
2009	119,296	74.1 2	68.7
2007	117,840	69.7 2	61.7
2003	113,126	61.8	54.7
2001	109,106	56.3	50.4
2000	105,247	51.0	41.5
1997	102,158	36.6	18.0
1993	98,736	22.9	$(x)^3$
1989	94,061	15.0	$(x)^3$
1984	87,073	8.2	$(x)^3$

Source: U.S. Census Bureau, Current Population Survey, October 1984, 1989, 1993, 1997, 2000, 2001, 2003, 2007, 2009, 2010, 2011.

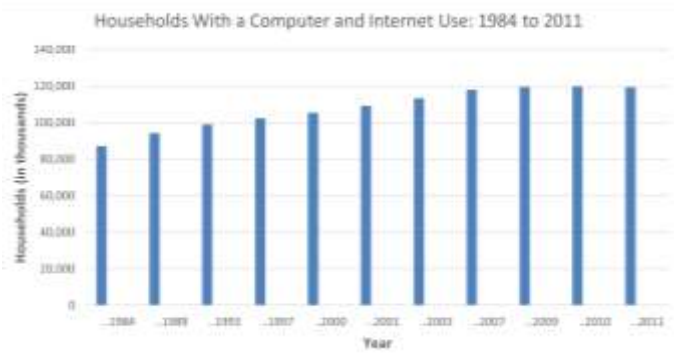

Fig 1. The number of households in the US who use computers and the Internet from 1984 – 2011.

Increasing the number of Internet users requires more IT infrastructure capacities to maintain all these expected services, as illustrated in Figure 2. In addition, the level of security should be increased, even though the percentage of users may exceed 100%. For instance, in New York State, the total number of households that use computers and smartphones is around 91% of the state's population, as illustrated in Figure 1. Furthermore, the population in the state that has Internet access is around 85.5% of the users [2]. Cybersecurity stands in the front line to protect these assets under different specializations and colors (*e.g.*, blue, red, and other teams). All these specializations were invented recently to close the gap between the development and configuration sides and the user end. Once again, all these cybersecurity specializations are not necessary to be named as cybersecurity professionals, as the field of cybersecurity has expanded after being widely considered and is now an entity as opposed to being a part of the computer science and engineering umbrella as it was before.

According to the National Institute of Standards and Technology (NIST), cybersecurity contains several pathways and technical areas such as cryptography, cybersecurity measurement, privacy engineering, and others. As is well known, cryptography is a set of mathematical techniques that utilize a variety of algorithms to protect data from being exposed. The remaining challenge in the upcoming decades will be maintaining the classical systems, data, and IT infrastructures besides the development of quantum systems. Several cryptographers, mathematicians, and physicists are approaching quantum systems based on quantum rules.

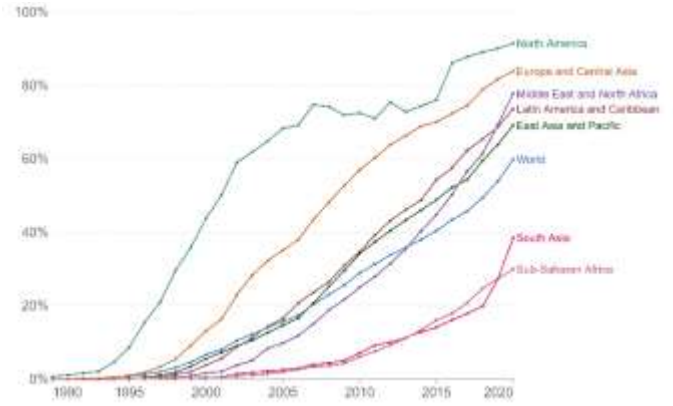

Fig. 2. The data illustrates the Internet users from 1990 to 2020, which is defined by the International Telecommunication Union as anyone who has accessed the Internet from any location in the last three months from a device such as a computer, mobile phone, personal digital assistant, gaming machine, smart TV, or any technological device [3].

As a result, theoretically, increasing demand causes a high rate of supply. However, this theory may not be applicable in the case of a lack of cybersecurity workforces and tools. The challenge of covering and protecting all these assets in case quantum computers become real before figuring out the cryptographic aspects will be a disaster. Moreover, increasing security awareness is a priority in the field of cybersecurity in general and the entire technical aspect in particular.

III. QUANTUM SYSTEM

A. Quantum Computing

Some predictions assume that commercial quantum computers may be available in the next five years. If it takes longer, at least the quantum system should appear within a short period. Although some scientists consider quantum states too fragile and subject to the accumulation of errors for large-scale quantum computation, several components of the real quantum computer have appeared in some events by some tech companies. So, what is a quantum computer? A quantum computer is a type of computer that utilizes the principles of quantum mechanics to perform computations. Unlike classical computers that use bits to represent and process information, quantum computers use quantum bits or qubits. Qubits can exist in multiple states simultaneously, which belong to a property called superposition, allowing several photons to represent and process a vast amount of information simultaneously.

One of the fundamental principles of quantum computing is the ability of qubits to be in a state of superposition, which means they can be in a combination of both 0 and 1 states, as in Equation 1. This enables quantum computers to perform parallel computations and potentially solve certain problems more efficiently than classical computers. Another important concept

in quantum computing is entanglement. Entanglement allows qubits to be correlated in such a way that the state of one qubit can be instantly influenced by the state of another, even if they are physically separated. This property enables quantum computers to perform certain calculations or algorithms more efficiently, taking advantage of the interdependence between qubits.

Quantum computers are expected to have significant applications in various fields, including cryptography, optimization, simulation of quantum systems, and machine learning. They have the potential to solve complex problems that are currently intractable for classical computers, offering breakthroughs in areas such as drug discovery, optimization of logistical operations, and advanced data analysis. While the development of practical and scalable quantum computers is still a major technological challenge, significant progress has been made in recent years. Tech companies, research institutions, and governments are investing in quantum research and development to harness the power of quantum computing.

However, it is important to mention that quantum computers are not intended to replace classical computers entirely. Instead, they are expected to complement classical computing systems by providing specialized capabilities for specific types of problems. The coexistence of classical and quantum computers is envisioned to create a hybrid computing approach, where classical and quantum algorithms can work together to solve a wide range of problems more efficiently. As the field of quantum computing advances, researchers are striving to overcome technical challenges, such as minimizing errors, improving qubit stability, and developing robust error-correction techniques. These efforts aim to make quantum computers more practical and reliable for real-world applications.

$$0 \approx |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, and\ 1 \approx |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \quad (1)$$

B. Future Services

Several organizations and tech companies such as Google, IBM, Microsoft, Intel, Atos, Baidu, and Alibaba have been conducting quantum research for decades [4]. Recently, some achievements have been demonstrated by these parties that quantum computers are physically close to the end. Without any doubt, there are many unanswered questions. For instance, will the quantum system use the same networking layers as the classical system? The structure of the back end may remain the same, such as the binary readings by binary devices. However, the speed and acceleration of treating and calculating multi-mathematical equations will decide if the classical system can handle this flood of data. It's still early to judge whether the quantum system requires a different structure or not, and the battle is still in the soft area.

Regardless of the challenges that the quantum computing era has brought, the benefits and services that can be harvested and gained paint a positive picture. Look at how many health issues will be resolved based on the accuracy and speed of figuring out the outcomes of complicated experiments. Banks are not far from this battle, where most financial organizations are involved passively or actively. The main target of these organizations is the encryption key, which stands behind the whole security of financial applications and systems. Banks such as J.P. Morgan, HSBC, CITI Group, Wells Fargo, and Goldman SACHS have initiated their investments in quantum banking. The quantum system is supposed to be efficient, secure, and able to handle and compute a massive amount of data and transactions in a limited time. Moreover, there are other benefits of using quantum technology in financial services, such as enhancing investment gains, reducing capital requirements, and improving the identification and management of risk and compliance [5].

C. Quantum Cryptography

The classical system is protected by cryptographical methods, and these methods protect several elements such as authentication, integrity, confidentiality, non-repudiation, and others. RSA is one of these methods that provide a stable and secure key exchange between parties. The RSA [6] is based on the prime number factorization, which is much more difficult to be cracked by a classical system computer, even supercomputers. Recently, and after physical experiments, Shor's algorithm [7] raises a real concern about the security of the RSA anymore. More precisely, classical cryptography perhaps is exposed if quantum computers are consumed, where quantum computers are faster than classical computers by many years of calculations. Therefore, cryptographers have been involved in many experiments to initiate a temporary shield in case quantum computers appeared somewhere without alerting. Quantum cryptography is the target, specifically the mechanism of creating a solid secret key. Quantum Key Distribution (QKD) partially has solved the issues, where many QKD protocols have been released since 1984 [8].

Furthermore, the quantum system could be a challenge right now regarding the availability of quantum chips, hardware, memory, regulations, standards, and others. However, post-quantum cryptography (Quantum-Resistant Cryptography) is a solution to be located on both classical and quantum systems as a hybrid platform. Some post-quantum protocols have been experimented with and approved to operate on both systems such as Lattice-based cryptography, Code-based cryptography, Multivariate polynomial cryptography, Hash-based signatures, and others [9].

D. Quantum Cybersecurity

As the digital world has become one of the necessities in our business, education, health systems, entertainment, research, homes, and others that are growing every second, there is another growth of the cybercrime ecosystem with many criminal enterprises. These enterprises support threat actors with complementary data exfiltration, ransomware, and malware-as-a-service operations [10]. In addition, these cybercrime activities threaten every corner of our life and infrastructures. However, classical defensive and offensive skill sets are not prepared or even not ready for quantum attacks. Quantum cybersecurity may become another order and term in the technology world to differentiate between neutral systems. According to [11], the average cost of a data breach in the United States was $9.44 million in 2022. Also, the global average total cost of a data breach reached $4.35 million. These cyber-attacks cannot be ignored because the stability of the numbers of ransoms and various damages depends on the level of security provided by the cybersecurity teams. On the one hand, this will lead to a

decisive decision for the attackers on whether to stop or continue causing these illegal actions.

IV. CYBERSECURITY CHALLENGES

Cybersecurity has become the top demand in the national and international markets because of the extensive usability of digital infrastructure. Most security specialists are familiar with the classical systems, either private or public structures. However, those specialists may not be skilled enough to deal with quantum or post-quantum systems. The World Economic Forum has addressed the fact that quantum computing will change the current cybersecurity rules. In 2018, the US passed the Quantum Initiative Act, where cybersecurity was at the top of the list of issues discussed [12]. Furthermore, scientists and researchers have been challenged to create several algorithms that match today's needs. For instance, the US National Institute of Standards and Technology (NIST) oversees a number of these quantum-based technologies. Some of these quantum algorithms are still under experiment, whereas others are considered overestimates [13].

Some proposals, for instance [14], suggested cybersecurity landscapes that provide a future vision for the cybersecurity field. Three categories of research refer to three different communication resources such as classical computation and classical communication, small quantum device and quantum communication, and large quantum computer and classical or quantum communication respectively as in Figures 3, 4, and 5. All these categories will determine who can access quantum technologies and utilize the power of computation. Moreover, applications, tools, hardware, and software will determine the priority of users, at least in the first decades. Myth and reality perhaps conflict on several occasions and events. Quantum technologies might be a complicated event to determine the gap between theory and application. The reason could be hidden behind the availability and the overwhelming cost of quantum technology.

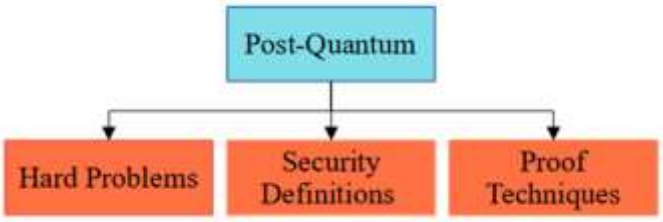

Fig 3. Classical computation and classical communication between honest parties and adversaries (Full Quantum).

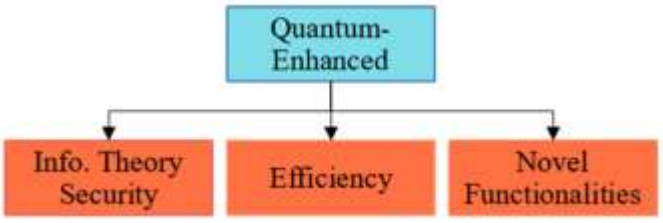

Fig 4. Small quantum device and quantum communication between parties.

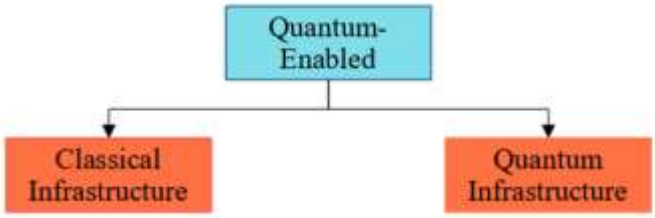

Fig 5. A large quantum computer, classical or quantum communication.

Cybersecurity entities, regardless of the type or size of their services, reshape the design of infrastructural systems to facilitate a smooth transition from the Newtonian system to the quantum system. The question here that may raise some concerns is about the availability of quantum tools and materials before and after utilizing the quantum systems. For instance, most of the materials such as experiments, data, tools, and software available in this term belong to the conceptual side that represents scientists, physicists, and engineers' efforts to build the final piece of the whole picture. The real concern is that quantum computing is still treated as a big secret. However, some academic and non-academic institutions have begun this journey early to discover the power of quantum systems. In general, on the technical aspects of usability of cybersecurity, quantum awareness lacks a real definition, or at least it's not presented as a feature or a threat.

V. QUANTUM ADVANTAGES VS. DISADVANTAGES

It's all about time consumption, where a quantum computer is potentially light-years faster than conventional computers. Quantum computers will revolutionize every aspect of technology. Data science, health systems, economics, marketing, engineering, energy production, security, and privacy, as well as solving problems, will be affected positively or negatively by quantum usage based on a variety of factors that illustrate the goals behind the use. Next, there are two sections to demonstrate the pros and cons of using quantum computers and quantum technology.

A. Quantum Advantages

Several unsolvable mathematical problems may change the future of many industries and research. Also, the difficulty has become the process of securing several classical systems in terms of current vulnerabilities found such as software and hardware as illustrated in Figure 6. Some may understand the difficulty in the wrong concept, which is a negative sign. However, it's one of the fundamentals of cryptography, and most encryption/decryption algorithms are based on this concept. The difficulty here should match the simplicity, and both must produce the security elements. This term of difficulty is well-known in the cryptocurrency field, where the formula of how difficult it is to locate a hash for the target value. The difficulty represents a long time of computation to find out the matched hash, and this is calculated as:

$$D = \frac{Target_{hash}}{Current_{hash}} \quad (2)$$

where *D* is the difficulty of finding the hash compared with the current hash, *Target* is the target hash, and *Current* is the current hash.

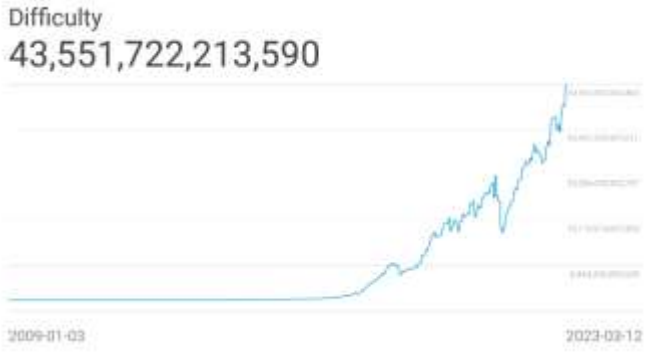

Fig 6. The Network Difficulty from 2009 to 2023: A relative measure of how difficult it is to mine a new block for the blockchain [15].

Since the early cryptographic algorithms, the difficulty of breaking encryption messages has been raising and becoming smarter. Recently, the RSA is a mathematical challenge, which is considered the classical system defender. Finding the prime number factorization of a large digit cannot be simple for nowadays computers. The only thing that could cause an extraordinary action is a quantum computer. According to Shor's Algorithm [16], cracking an RSA key may be implemented in a few milliseconds. However, to prevent this case scenario from happening and causing severe damage, quantum scientists have taken an early step to protect classical (conventional) systems. Post-Quantum is an immediate solution [17], where some cryptographers have focused on Quantum Key Distribution (QKD). Making solid, random, and long secret keys can resist any quantum attacks only shortly.

Furthermore, some mathematical unsolvable equations, as well as some difficult problems such as quantum encryption, simulation of quantum systems, ab-inito calculations, solving difficult combinatorics, supply chain logistics, optimization, finance, drug development, data analysis, and weather forecasting, will have a great opportunity to be solved. In addition, Quantum Machine Learning (qML) reserved a spot with the quantum system, where the quantum system promises powerful tools to find patterns in data [18]. Without a doubt, the diameter of the non-deterministic scope will increase dramatically, and several unsolved equations will enter the deterministic domain.

B. Quantum Disadvantages

As logically found with any technology, most of the new technologies have both considerations whether advantages and disadvantages. Quantum computing may carry a lot of risks, specifically regarding availability and standard policies. As is obvious, a few countries have been funding research and studies on quantum computing since the quantum computer was approved for its high capabilities to calculate difficult mathematical equations. Technically, some problems are still understudied, and these studies' progress may reach a low rate because of the complexity of these problems. For instance, the factor of noise in the quantum system is considered a fundamental factor to assign the system as a functional system or not. The calculations of different equations and their accuracy depend on the rate of noise existing in the channel between the sender and receiver.

For several years, cybersecurity specialists and their organizations have realized that the threat of quantum computing is real, and the concern had been theoretical. Now, the concern has been elevated to be more about waiting for the first physical quantum computers. Until today, there are no real criteria to measure the risk elements of using quantum computers. However, based on experiments of quantum algorithms, the expectations of causing a lot of damage are possible. As some technology platforms have begun to shine, such as Machine Learning, Artificial Intelligent, and Blockchain, the power of quantum computations could lead to a huge vulnerability in the system. Recently, ChatGPT caught a lot of attention from individuals and organizations, even governments. This capability of mapping a tremendous amount of collected data with respect to the runtime execution could blow up our minds if the platform runs over a quantum system.

Machine learning models are vulnerable to several attacks that can modify or change the output of readings. These attacks appear in the classical system, and this may affect services such as facial recognition, automobility, and others that require accuracy and efficiency in a critical time. Malicious models, for instance, can impact the reading and accuracy of ML models such as reading signs that control automobile behavior [19]. Quantum algorithms make these attacks worse. According to [20], experiments were conducted as Adversary Resource Investment, where three case-scenarios were implemented as classical, balanced, and quantum. The attack success probability shows the Quantum-enabled Adversary with relatively the highest probability of attack success.

Furthermore, after skeptical decisions, some banks and financial organizations have started using blockchain in their systems regardless of cryptocurrency usage and the story of Bitcoin [21]. The power of blockchain is hidden under the hood of cryptography, where it provides transparency, privacy, and security. The security of blockchain algorithms relies on hashing function algorithms, and it provides principles of cryptography, decentralization, and consensus. Obviously, the speed of quantum algorithms such as Shor's algorithm and Grover's algorithm can be a risk to hash calculations, where locating a collision is possible by quantum and not by brute-force attacks. The second risk that may impact the mechanism of blockchain is the encryption/decryption key exchange, where quantum computers can break the shared key between the parties or more precisely find out the hash value [22]. The ability of quantum computers to generate a long hash value (nonce) makes the difficulty rate high.

VI. CONCLUSION

Several potential solutions may have been created to prevent any shortage or weakness against quantum attacks. One of these solutions is post-quantum cryptography which could work on the existing hardware and software of the classical system. Another solution also has attracted many scientists' and cryptographers' attention, it is quantum cryptography. The problem with this solution is the availability, which includes quantum hardware, noise, and quantum channels. However,

quantum key distribution protocols lead the field to initiate a secure exchange between the communicated legitimate parties. Cybersecurity has been involved in the quantum domain as long as the quantum system has become a real threat. Awareness of the quantum structure and power of its particles during a variety of computations may increase the resistance against some of the quantum attacks, which the challenge will include the smart tools and applications, such as firewalls, Intrusion Detections IDs, Intrusion Prevention IPs, Antivirus applications, Sensors, System Information and Event Management SIEM, Automobile software, health devices, and others. The change from classical to quantum systems is coming, sooner or later. Early preparation and awareness of quantum mechanics can prevent massive damage to infrastructure assets, datasets, and servers.

REFERENCES

[1] "Key Internet Statistics to Know in 2022 (Including Mobile)," *BroadbandSearch.net*. https://www.broadbandsearch.net/blog/internet-statistics (accessed Jun. 25, 2022).

[2] "Digest of Education Statistics, 2019." https://nces.ed.gov/programs/digest/d19/tables/dt19_702.60.asp (accessed Jan. 07, 2023).

[3] M. Roser, H. Ritchie, and E. Ortiz-Ospina, "Internet," 2015. https://ourworldindata.org/internet

[4] E. Gibney, "The quantum gold rush," *Nature*, vol. 574, no. 7776, pp. 22–24, 2019.

[5] "Quantum computing use cases for financial services," *IBM*, Sep. 12, 2019. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/exploring-quantum-financial (accessed Feb. 21, 2023).

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[7] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, 1994, pp. 124–134.

[8] A. A. Abushgra, "Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review," *Cryptography*, vol. 6, no. 1, p. 12, 2022, [Online]. Available: https://doi.org/10.3390/cryptography6010012

[9] L. Chen *et al.*, "Report on Post-Quantum Cryptography," National Institute of Standards and Technology, NIST IR 8105, Apr. 2016. doi: 10.6028/NIST.IR.8105.

[10] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for Quantum Computing." arXiv, Oct. 27, 2021. Accessed: Jun. 24, 2022. [Online]. Available: http://arxiv.org/abs/2110.14701

[11] "Cost of a data breach 2022," Mar. 14, 2023. https://www.ibm.com/reports/data-breach (accessed Mar. 14, 2023).

[12] F. Bova, A. Goldfarb, and R. G. Melko, "Commercial applications of quantum computing," *EPJ Quantum Technol.*, vol. 8, no. 1, p. 2, Dec. 2021, doi: 10.1140/epjqt/s40507-021-00091-1.

[13] W. Buchanan and A. Woodward, "Will quantum computers be the end of public key encryption?," *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 1–22, Jan. 2017, doi: 10.1080/23742917.2016.1226650.

[14] P. Wallden and E. Kashefi, "Cyber security in the quantum era," *Commun. ACM*, vol. 62, no. 4, pp. 120–120, Mar. 2019, doi: 10.1145/3241037.

[15] "difficulty.png (PNG Image, 1440 × 810 pixels) — Scaled (69%)." https://api.blockchain.info/charts/preview/difficulty.png?timespan=all&h=810&w=1440 (accessed Jul. 26, 2022).

[16] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[17] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[18] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, 2017.

[19] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical black-box attacks against machine learning," in *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, 2017, pp. 506–519.

[20] M. Barbeau and J. Garcia-Alfaro, "Cyber-physical defense in the quantum Era," *Scientific Reports*, vol. 12, no. 1, p. 1905, 2022.

[21] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[22] B. Rodenburg, "Blockchain and Quantum Computing".