**Quantum computing and quantum cryptography in a rapidly evolving environment of blockchain technology: Technical and societal impact**

**Alexander Ntoko**

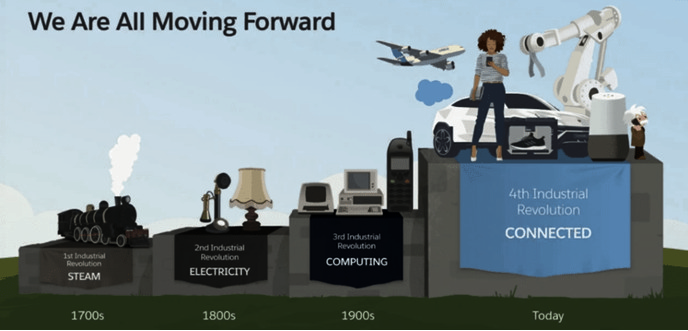
Operations and Planning Department, Telecommunication Standardization Bureau, International Telecommunication Union (ITU), Geneva, Switzerland

**Introduction**

In information technology security, maintaining the integrity of sensitive information is critical. As one thriving technology, blockchain is able to link transactions while making sure it remains uncompromised through the introduction of cryptographic algorithms such as asymmetric cryptography. Consequently, the blockchain is able to make information transparent and secure at the same time. While it appears to bring great promises, there is yet a threat that could well loom. Quantum computing is a technology that uses the properties of quantum mechanics to enable particles to exist in more than one state at the same time. This has the impact of improving computational power drastically such that it accelerates the discovery of new information and, on the other hand, threatens existing security mechanisms, as it would require less time to break encryptions. While the technology is still at its early stages of development, one should question the impact that quantum computing will have in industries, businesses and other organizations in the public sector that are slowly shifting towards using blockchain in their respective environment.

**The Fourth Industrial Revolution (4IR)**

The arrival of the Fourth Industrial Revolution (4IR) introduced an era in which humans and technologies become interconnected. While the 4IR was a natural consequence of the acceleration and widespread of computing technologies offered by the Third Industrial Revolution, the former is significantly different. In the 4IR, technologies try to merge with people’s physical environment (working, social and private life) to build cyber-physical spaces. In this regard, the founder of the World Economic Forum, Klaus Schwab, has defined the 4IR as “a technology revolution where the fusion of technologies blurs the lines between physical, digital and biological spheres”.[1] It is thus expected that the prominent technologies of the 4IR will be responsible for some of the major disruptions in labour markets, economic laws, rules and cultures that govern our lives.



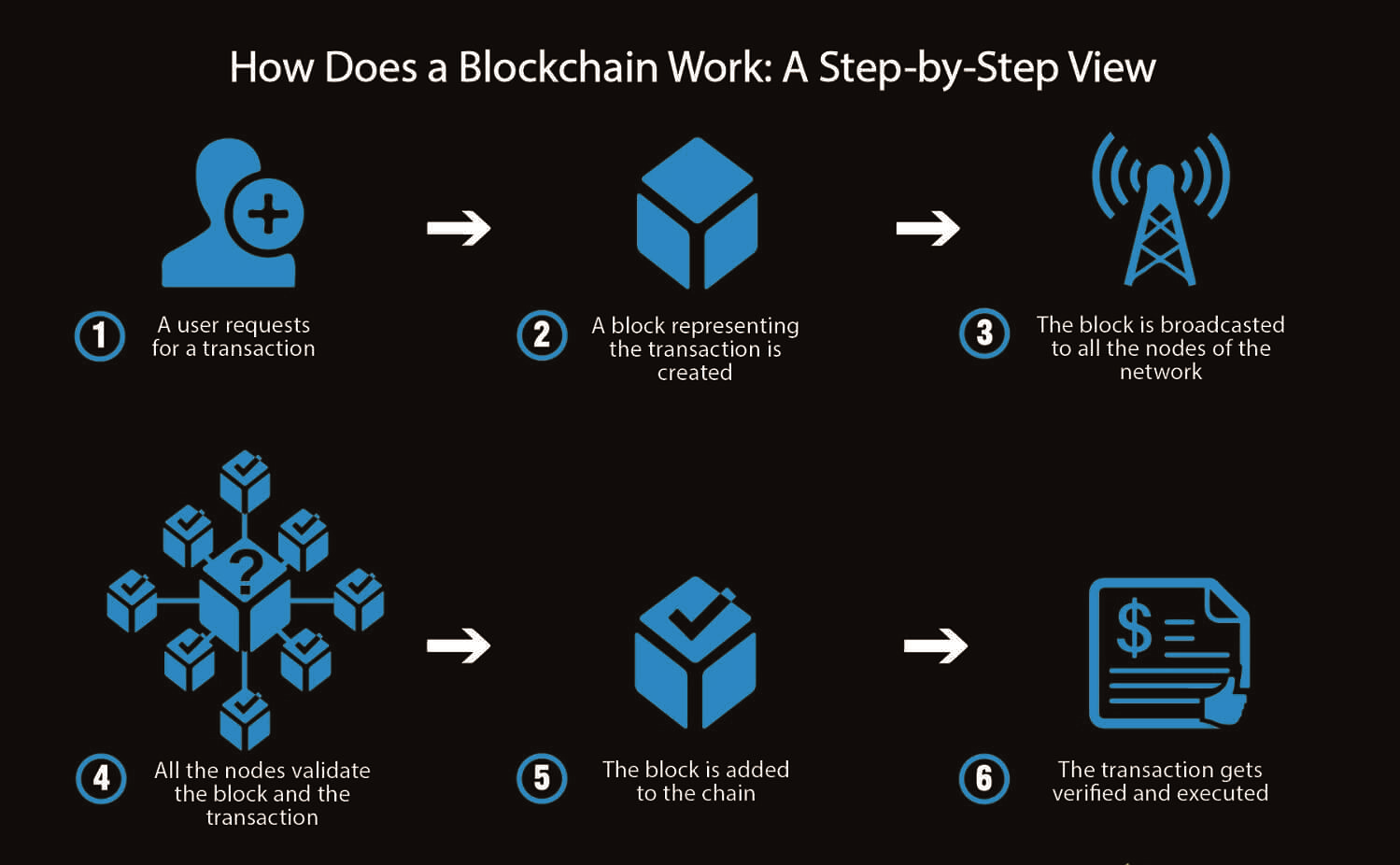
**Figure 1 ‒ Transition from the First to the Fourth Industrial Revolution[2]**

In this era of technological transformation, one particular threat that is more and more at the heart of every conversation is security in general, and more particularly, the security of personal information. With the increase of connected physical devices and gadgets, the amount of cyberattacks carried out have been drastically rising over the years. For example, in 2019, reported computer security mechanisms at Kaspersky[3] and F-Secure[4] recorded 105 million and 2.9 billion attacks respectively, compared to 12 million and 231 million respectively in 2018. More importantly, with raising public concerns on data privacy, it has become vital for companies and policy makers to implement rules to monitor online identities and protect them from lurkers or actors that may use personal information without the data owner’s consent. Yet, because some 4IR technologies are both enablers and disablers, developing a governance model becomes complex and requires the application of ideas that go beyond the scope of existing IT management frameworks. This paper assesses the contribution of two particular 4IR technologies in the context of information security: blockchain and quantum computing.

**Blockchain**

The first concept of blockchain (or digital ledger technology) was introduced in 2008 by an entity under the alias of Nakamoto that had developed the idea of a digital currency called bitcoin.[5] However, it was not until very recently that an actual definition of blockchain became available. The *Merriam-Webster* *dictionary* defines blockchain as a “digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large, decentralized, publicly accessible network*”*.[6] The key words mentioned in the definition are *digital*, *decentralized* and *shared*. Blockchain is digital, meaning that its information is represented in a series of digits, decentralized so that it is accessible from anywhere around the globe, and shared such that it is collectively maintained by a group of users or members (also called a peer-to-peer network) rather than by one central administration. Transactions are grouped into a block that is verified by each user in the blockchain. A consensus must be reached to decide whether an entry block should be added. If approved by 51%of members, the new block is added to the communal ledger. The approved block is “hashed**”**, meaning that a value is generated to represent the block, the data it contains and information about previous blocks to ensure that the new candidate block has a validation path all the way down to the first block of the chain. Consequently, the integrity of the entire ledger is maintained and can be checked by anyone running a hash calculation.

Blockchain offers a technical infrastructure that is trustable. Operations are permanently recorded in blockchain without the possibility to change or hide them. Another advantage is that there is no official trusted third party intervention, which means that blockchain members can transact directly with one another. Bitcoinis an example of how blockchain principles are applied to allow money transfers outside of any Government oversight. Another application of the blockchain is Ethereum*,* a platform that enables smart contracts that are self-executing. In permissionless (open to all) blockchains, parties that perform transactions can be pseudonymous and can recognize each other in a secure manner using public key cryptography.

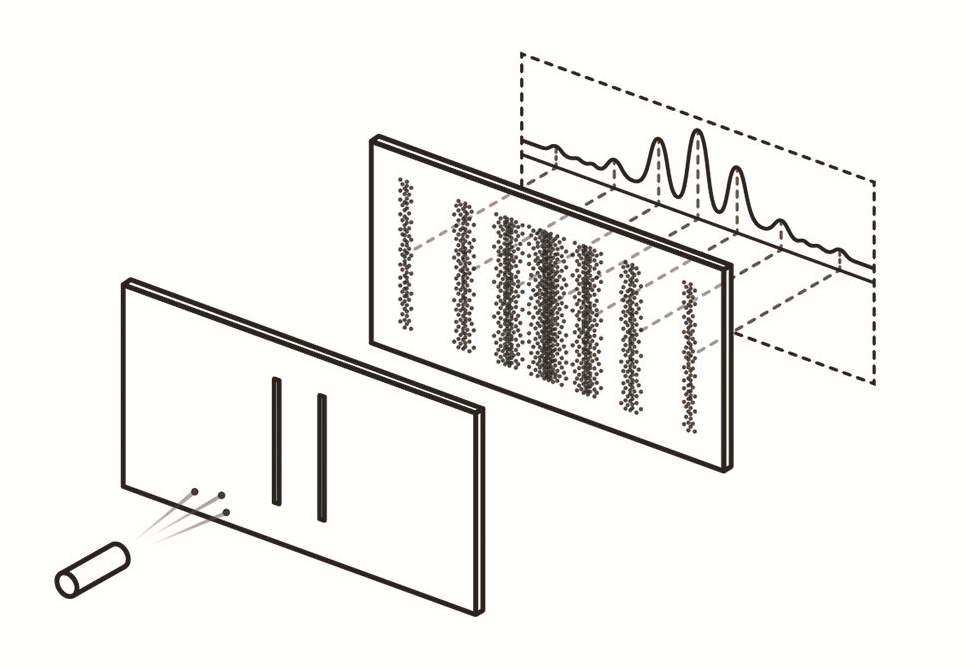


**Figure 2 ‒ How does a blockchain work: a step-by-step view[5]**

While there is evidence that blockchain can enhance information security in many businesses, there are some challenges in applying it to use cases in practice. To start with, the lack of regulation on blockchain utilization fosters uncertainty among many users and businesses. Most notably, there are some signs of resistance among certain industries to introduce blockchain in day-to-day business. Bucovetchi *et al*.[7] identified that the trend describing the interest of non-specialists suddenly decreased after 2017 due to the negative marketing campaigns that have been conducted by conventional financial organizations against blockchain. Nevertheless, experts predict that financial institutions, and sectors like healthcare, supply chain and agriculture, will invest more in the technology in the future.

**Quantum computing and quantum cryptography**

Quantum computing is the discipline that develops computer technologies based on quantum mechanics, where matter is presented as subatomic level particles called qubits.[8] One of the first observations of quantum mechanical phenomena was in Thomas Young’s double slit experiment. Initially, it was postulated that through the governing laws of classical probability, particles of light would go through two slits at an equal probability. However, the end result showed that in some environments, the laws of probability no longer apply, because particle interference took place. When complex numbers were introduced to the existing probability model to explain quantum interference, which is when a particle has the ability to cross its own trajectory and interfere with the direction of its own path, a phenomenon similar to the concept of wave interference observed in classical physics. For this reason, quantum mechanics suggests that a quantum entity can be described as either a particle or a wave.



**Figure 3 ‒ Quantum interference observed through the double slit experiment[9]**

The quantum interference phenomenon experienced by particles is a consequence of two main properties: superposition and entanglement. In superposition, particles can exist in more than one state at the same time. When a qubit is unstable and interacts with its environment, it loses its superposition property (and only appears in one state) and is said to become decoherent. Qubits are also entangled, meaning that particles are correlated to one another such that any action performed on one particle will affect the other, regardless of the distance separating them. When computations are performed, qubits need to be kept in a cold environment so that their superposition and entanglement can be maintained. Additionally, quantum error correctioncodes and techniques are needed to reverse any calibration errors and random fluctuations that also cause qubits to be unstable.

The properties of quantum computing can be used to improve information security. One of its applications is in the generation of random numbers used for encryption, called quantum cryptography. Quantum key distribution (QKD) uses a random number generator to create secret keys that will be used to encrypt and decrypt messages between two communicating parties. While classical computers are said to generate pseudo-random numbers, quantum computers can generate true random numbers, since quantum states are probabilistic rather than deterministic. Additionally, due to the properties of superposition and entanglement, any snooping or eavesdropping on data transmitted under a quantum state will invoke disturbance on particles, changing the content of the information. Also, it will be impossible for eavesdroppers to create a copy of the information sent using quantum computers if they do not know its content.

**Quantum computing in the blockchain environment**

Over the next few years, blockchain will affect several sectors in the economy. Some of the expected applications of blockchain will include the creation of a virtual currency adopted by governments in different countries, the development of self-sovereign identities, and improved tracking and authenticity certification of products in supply chains. Quantum computing will have an important role in the blockchain environment, as it can either improve or jeopardize its security.

The backbone of blockchain security relies on public key cryptography. The reliability of this method is based on the trust given to one-way functions, where running a calculation to find the public key (used for encryption of messages) is easy, but running a calculation to find the private key (used for decryption of messages) is computationally intensive. However, if one is able to increase computational processes, the mathematical problem required to find the private key will be solved faster, making the foundations of the one-way function fall apart. This is what quantum computers are capable of doing using the ability of qubits to perform multiple calculations simultaneously.

Two possible ways for quantum computers to bring security threats to blockchain and its encryption are by using Shor’s algorithm[10] and Grover’s algorithm. The former uses a process that facilitates the search of prime factors in a number by reducing the amount of search steps. The latter solves an unstructured search problem (finds the input used in an unstructured or black box process) by performing several queries in parallel. Using either of these algorithms, quantum computation can be used to take control of the blockchain network. In the hands of bad actors, a quantum computer could engage in double spending(same currency spent more than once in an ultra-fast transaction) of digital financial resources or block transactions. While quantum technology is still in its infancy, in practice digital ledgers could be downloaded today and decrypted later when quantum computers’ computational capabilities have improved.

Preventive measures to protect the blockchain from quantum computers exist. QKD and a quantum random generator (QRNG) have been proven to be quantum safe measures to encrypt communications and make ledgers quantum-resistant. Another option, using the quantum Internet, would be to develop the quantum blockchain[11]**‒** a representation of transaction records in chronological order using entangled quantum particles. Although it is still a concept for now, quantum blockchain would address scalability issues with the current blockchain system by bypassing some computationally intensive steps of verification and consensus, and would make sure that any action that would try to tamper with records in the different blocks would become invalid.

While quantum encryption methods seem to offer promising security measures, it is important to mention that some of the more common encryption methods available in the market today are reliable enough to protect the blockchain. For example, a blockchain using a 1 024-bit Rivest–Shamir–Adleman (RSA) key can only be decoded by a quantum computer having 2 000 qubitsor more, which currently does not exist (as of today, the largest quantum computer built by Google only contains 53 qubits). Even a blockchain system that uses an elliptic curve digital signature algorithm (ECDSA) to develop its public key cryptography, which uses a key of 256 bits, would still be insufficient against quantum attacks in the near future. Another possibility would be to use an extended Merkle signature scheme (XMSS), which creates a one-time signature, where a single key is used to sign only one transaction.

**The future of quantum computing and quantum cryptography**

Views about the predicted impact of quantum computing and quantum cryptography seem to diverge. For some businesses, quantum computers will impose a serious threat. A survey conducted by DigiCert[12] suggests that 71% of security professionals anticipate that quantum computing will pose a threat, and that it is just a matter of time before it happens. ThePentagon has itself suggested that quantum computing will be part of the next arms race.[13] Yet, other specialists and researchers in the field suggest that by the time quantum computing becomes widely available, cryptography will have developed stable quantum-proof algorithms. For now, experts estimate that quantum computers will start going mainstream within a decade.

Most technology-advanced countries have started investing in quantum technology. For example, China has tested quantum encryption techniques via satellite, has spent US$80 million to develop a quantum communication network between Shanghai and Beijing and another US$10 billion to build a quantum technology lab. The European Union (EU) has launched the Quantum Technologies Flagship, €1 Billion initiative to support quantum technologies research in Europe.[14] EU Member States**[[1]](#footnote-1)** have signed a declaration agreeing on their collaboration to explore, develop and deploy Quantum Communication Infrastructure(QCI)[[2]](#footnote-2) in Europe. QCI will integrate quantum technology to secure critical infrastructure and encrypt systems against cyber threats, provide safe exchange of information and preserve privacy of government data, as well as developing the future backbone of Europe’s quantum internet. In the USA, the National Quantum Initiative has allocated US$1.275 billion to quantum research from 2019 to 2023.[15],[16] Additionally, the US Department of Defense has the intention of using quantum computing to encrypt its data and systems, and to maintain a competitive advantage over their adversaries.[17]

In the private sector, there is a race to be the first at harnessing the power of quantum computing. Microsoft and IBM are both developing cloud-based quantum-computing tools. Google, in collaboration with other institutions, has developed a quantum computer that was able to solve a problem. However, it is currently not ready for practical application. In general, businesses will have to not only address engineering issues in the implementation of quantum computers, but also make sure to hire the best talents in quantum computing research, which is predicted by some experts to be the next technology talent shortage.[16] Despite this, companies in different sectors have shown interest in using quantum computing to gain advantages in their respective businesses in fields as diverse as battery chemistry, traffic routing or the pharmaceutical and aircraft industries.

**General remarks**

One of the key mechanisms used to enhance online trust and security is to rely on the current problem areas or difficulties in breaking asymmetric cryptographic algorithms. This is mostly dependent on our knowledge of classical computing based on binary digits (bits). Quantum computing is still in its infancy and the development of the power needed to break current asymmetric algorithms might take some years. However, we have not always been very accurate in predictions, especially in the domain of computer science. Thus, the development of quantum computing and quantum cryptography needs to be carefully monitored*.*

**Contribution of the International Telecommunication Union (ITU) to the field of cybersecurity, quantum computing and quantum cryptography**

The ITU plays an important role in leading the development and implementation of security in the use of information and communication technologies (ICTs). It participates in the World Summit on the Information Society (WSIS)*,* a process carried out by governments, international organizations, the private sector, civil society and other entities to develop action lines and projects that would encourage the creation and sharing of information. Of particular interest is the ITU contribution to WSIS action line C5 on “building confidence and security in the use of ICTs”. The action line involves several programmes, including the development of a Global Cybersecurity Agenda[18] – a framework used for international cooperation aimed at enhancing confidence and security in information society, and the Global Cybersecurity Index[19] – a metric developed to measure the cybersecurity capabilities of nation states. In addition to WSIS activities, ITU Plenipotentiary Conferences, Assemblies and Conferences provide additional means to strengthen the role of ITU in cybersecurity.

In the Telecommunication Standardization Sector of ITU (ITU-T), one of the main ITU-T Study Groups responsible for the production of ITU-T Recommendations in the field of quantum computing is ITU-T [Study Group 17(SG17)](https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx).[20] SG17 is an expert group coordinating work for the development of security related standards in technology. Another key ITU-T Study Group is ITU-T [Study Group 13(SG13)](https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx),[21] which covers topics related to networks, with focus on fifth generation (5G), cloud computing and trusted network infrastructure. SG13 and SG17 also organize workshops on secure quantum communication and quantum IT for networks. The list of ITU-T Technical Reports, ITU-T Work Items and ITU-T Recommendations in the area of quantum computing, quantum key distribution and quantum safe algorithms are available on the [ITU-T Work Programme website](https://www.itu.int/itu-t/workprog/wp_search.aspx).

Additionally, an ITU-T Focus Group on Quantum Information Technology (QIT) for Networks (FG-GQIT4N) was established in 2019. Its main purpose is to study the evolution and application, terminologies and use cases of QIT for networks, and to provide technical background and collaborative conditions to support standardization work related to Quality Improvement Network (QIN) in different ITU-T Study Groups.

Quantum-specialized ITU members are also an important asset to the development and implementation of quantum-related projects. As of today, ITU members include seven companies and two universities. Their first priorities will be to develop ITU-T Recommendations for best practice in the implementation of QKD networks and to provide interoperability of QKD equipment produced by different vendors. It is expected that the QIT field will bring an increased participation of interested parties.

**Conclusion**

This article provides a general overview of quantum computing and quantum cryptography, their impact on blockchain security, predictions of their possible usage and future work to be done by inter-governmental agencies, the private sector and academia. Whether it is considered to be a threat or not, quantum computing is already generating interest, and several businesses and sectors desire to understand it better so that it can replace existing solutions or solve problems that currently have no solution. Undeniably, the first challenge is to overcome the technical challenges in the implementation of quantum computers, which include dealing with qubit fragility (i.e. minimizing cases of quantum decoherence), improving the capabilities of quantum error correction, aggregating larger numbers of qubits in quantum computer chips, decreasing the time taken to convert data input into quantum state input, as well as implementing a debugging system for quantum hardware and software codes. Nevertheless, with continued research in the field of quantum technologies, there is no doubt that powerful quantum computers will see the light of day in the near future.

**References**

[1] Schwab, K. *The Fourth Industrial Revolution: What it means, how to respond*. Geneva: World Economic Forum, 2016. Retrieved from <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>

[2] McGinnis, D. *What is the Fourth Industrial Revolution?* San Francisco, CA: Salesforce, 2018. Retrieved from <https://ww.salesforce.com/blog/2018/12/what-is-the-fourth-industrial-revolution-4IR.html>

[3] Bayern, M. *Kaspersky honeypots find 105 million attacks on IoT devices in first half of 2019.* Louisville, KY: Tech Republic, 2019. Retrieved from <https://www.techrepublic.com/article/kaspersky-honeypots-find-105-million-attacks-on-iot-devices-in-first-half-of-2019/>

[4] Doffmann, Z. *Cyberattacks on IoT devices surge 300% in 2019, ‘measured in billions’, report claims*. Jersey City, NJ: Forbes, 2019, Retrieved from <https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/>

[5] Anwar, H.*The ultimate blockchain technology guide: A revolution to change the world*. New York, NY: 101 Blockchains, 2018. Retrieved from <https://101blockchains.com/ultimate-blockchain-technology-guide/>

[6] Merriam Webster. blockchain. In: *Merriam-Wester.com dictionary*. Springfield, MA: Merriam Webster, 2020. Retrieved from https://www.merriam-webster.com/dictionary/blockchain

[7] Bucovetchi, O., Badea, D., Stanciu, R. (2018), Blockchain technology – A new approach in business environment*.* *MATEC Web of Conferences*, Vol. 184, 04016.. Retrieved from: <https://www.researchgate.net/publication/326712566_Blockchain_technology_-_a_new_approach_in_business_environment>

[8] Beall, A., Reynolds, M. *What are quantum computers and how do they work? Wired explains*. London: Conde Nast. Retrieved from <https://www.wired.co.uk/article/quantum-computing-explained>

[9] Ananthaswamy, A.. *Through two doors at once: The elegant experiment that captures the enigma of our quantum reality*. New York, NY: Dutton, 2018. 304 pp.

[10] Keplinger, K. Is quantum computing becoming relevant to cyber-security? *Network Security*, 2018, **9**, pp. 16-19. Retrieved from <https://www.sciencedirect.com/science/article/pii/S1353485818300904>

[11] Rajan, D., Visser, M. Quantum blockchain using entanglement in time. arXiv preprint arXiv:1804.05979. Retrieved from <https://arxiv.org/pdf/1804.05979.pdf?source=post_page--------------------------->

[12] DigiCert. *Quantum’s promise and peril: 2019 DigiCert post quantum crypto survey*. Lehi, UT: DigiCert, 2019. 8 pp. Retrieved from https://www.digicert.com/resources/industry-report/2019-Post-Quantum-Crypto-Survey.pdf

[13] Nextgov, *Pentagon seeks an edge in quantum computing*. Retrieved from: <https://www.nextgov.com/emerging-tech/2018/07/pentagon-seeks-edge-quantum-computing/149718/>

[14] Lewis, A. M., Ferigato, C., Travagnin, M., Florescu, E. *The impact of quantum technologies on the EU’s future policies – Part 3: Perspectives for quantum computing*. JRC Science Hub. Brussels: European Commission, 2018. 153 pp. Retrieved from <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110412/quantum_computing_report_v5.4.pdf>

[15] Knapp, A. *Congress just passed a bill to accelerate quantum computing. Here’s what it does*. Jersey City, NJ: Forbes, 2018. Retrieved from <https://www.forbes.com/sites/alexknapp/2018/12/20/congress-just-passed-a-bill-to-accelerate-quantum-computing-heres-what-it-does/>

[16] Metz, C. The next tech talent shortage: Quantum computing researchers. *New York Times* 2018-10-21. Retrieved from <https://www.nytimes.com/2018/10/21/technology/quantum-computing-jobs-immigration-visas.html?source=post_page--------------------------->

[17] Department of Defense, Office of prepublication and security review. (2019). *DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY 19-23*. Washington, DC: Department of Defense, 2019. 72 pp. Retrieved from <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>

[18] ITU. *Global Cybersecurity Agenda.* Geneva: International Telecommunication Union, 2020. Retrieved from <https://www.itu.int/en/action/cybersecurity/Pages/gca.asp>x

[19] ITU. *Global Cybersecurity Index.* Geneva: International Telecommunication Union, 2020. Retrieved from <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

[20] ITU. *ITU Study Group 17 at glance.* Geneva: International Telecommunication Union, 2020. Retrieved from <https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx>

[21] ITU. *ITU Study Group 13 at a glance.* Geneva: International Telecommunication Union, 2020. Retrieved from <https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx>

**Disclaimer**

This report is the result of research carried out by Alexander Ntoko, Chief of the Operations and Planning Department at the Telecommunication Standardization Bureau of ITU, as part of a presentation made at the 52nd Session on the International Seminars on Planetary Emergencies, August 2019, Erice, Italy.

The objective of this report is to provide an overview of concepts, research and possible applications related to quantum computing, quantum cryptography and blockchain. The information gathered in this report is the compilation of material obtained from the different referenced sources.

The opinions expressed are those of the author and do not commit ITU in any way.

1. As of July 2019, 10 countries have signed the declaration: Belgium, Germany, Italy, Luxembourg, Malta, Spain, Hungary, Portugal, Poland and the Netherlands. [↑](#footnote-ref-1)
2. QCI is part of the Quantum Technologies Flagship, a €1 billion, 10-year initiative launched by the European Commission in October 2018 pooling resources around a commonly agreed science and technology roadmap. Fields covered include quantum communication, quantum computing, quantum simulation, quantum metrology and sensing and the basic science behind quantum technologies. [↑](#footnote-ref-2)