Scientific Research Publishing

Open Journal of Applied Sciences, 2024, 14, 1530-1549
https://www.scirp.org/journal/ojapps
ISSN Online: 2165-3925
ISSN Print: 2165-3917

Defining Quantum Advantage for Building a Sustainable MVP to Deliver Quantum Computing Services

Fazal Raheman

Blockchain 5.0 Ltd Kesklinnalinnaosa, Tallinn, Estonia
Email: drfazal@bc5.eu

How to cite this paper: Raheman, F. (2024) Defining Quantum Advantage for Building a Sustainable MVP to Deliver Quantum Computing Services. *Open Journal of Applied Sciences*, **14**, 1530-1549.
https://doi.org/10.4236/ojapps.2024.146102

Received: May 22, 2024
Accepted: June 21, 2024
Published: June 24, 2024

Abstract

Quantum Computing (QC) is hailed as the future of computers. After Google's claim of achieving Quantum Supremacy in 2019, several groups challenged the claim. Some QC experts attribute catastrophic risks that unrestrained QC may cause in the future by collapsing the current cryptographic cybersecurity infrastructure. These predictions are relevant only if QC becomes commercially viable and sustainable in the future. No technology can be a one-way ticket to catastrophe, and neither can the definition of superiority of that technology be. If there are catastrophic risks, large-scale QC can never enter the public domain as a minimum viable product (MVP) unless there are safeguards in place. Those safeguards should obviously become an integral part of the definition of its superiority over the legacy systems. NIST (National Institute of Standards & Technology) is pursuing the standardization of Post Quantum Cryptography (PQC) as that safeguard. However, with all the 82 candidate PQCs failing and companies already offering QC as a service, there's an urgent need for an alternate strategy to mitigate the impending Q-Day threat and render QC sustainable. Our research proposes a novel encryption-agnostic cybersecurity approach to safeguard QC. It articulates a comprehensive definition of an MVP that can potentially set a sustainable gold standard for defining commercially viable quantum advantage over classical computing.

Keywords

Cybersecurity, NIST, PQC, Quantum Computers, Quantum Advantage, Quantum Supremacy

1. Introduction

When Shakespeare averred, "a rose by any other name would smell as sweet", we

precisely knew the attributes associated with this thing called "ROSE". But do we really know what Quantum supremacy [1] or Quantum advantage [2] exactly entails within the Quantum Computing (QC) space, except that the latter appears more politically correct than the former? How do we achieve supremacy or advantage unless we precisely know what threshold needs to be reached to qualify? Can that threshold be totally oblivious to ethics and humane interests? What good a nuclear chain reaction is if it cannot be controlled to serve humanity? In the same breadth, the definition of quantum advantage cannot be just limited to achieving algorithmic superiority over legacy computing systems, particularly when a section of the experts attributes catastrophic threat [3] that unrestrained QC may cause by collapsing the current cryptographic infrastructure [4] resulting in amplified existential risk to humanity [5]. These predictions are relevant only if QC becomes commercially viable and deployable in the service of humanity. No technology can be a one-way ticket to catastrophe, and neither can the definition of superiority of that technology be. If there are catastrophic risks, QC can never enter the public domain as a minimum viable product (MVP) unless safeguards are in place. So obviously, those safeguards should become an integral part of the definition of its superiority over conventional computers and a standard to be met to pass the MVP threshold. NIST (National Institute of Standards & Technology) is pursuing the standardization of Post Quantum Cryptography (PQC) as that safeguard [6]. However, with 80 of the 82 candidate PQCs failing in initial rounds [7] and companies already offering QC as a service [8], there is an urgent need for an alternate strategy. Our research proposes a novel encryption agnostic approach [9] to secure our infrastructure from the impending threats from QC [10] and articulates a comprehensive definition of an MVP that can potentially set a gold standard for defining commercially viable quantum advantage over classical computing.

In recent years, quantum computing has made great leaps in its promise to offer breakneck computational speeds by using quantum phenomenon to break the bounds of classical computation and reach "Quantum supremacy" [1] or, more politically correct—"Quantum advantage" [2]. Despite these exciting new advances, quantum computing has its limitations. NISQ, or the Noisy Intermediate Scale Quantum, defines a current era of quantum computers' handling of intermediate executions of 50 - 100 qubits, which can surpass classical computing abilities but still suffer from quantum gate noise rendering fault-tolerant quantum computing, a prospect that for now remains beyond reach [11] [12] [13]. In any case, for real-world general-purpose tasks, quantum computers will never replace classical computers, nor are they intended to do so. At best, they will become an integral part of high-performance computing (HPC) for specialized use cases for various important scientific tasks [14].

In 2012, John Preskill coined the phrase "quantum supremacy" to describe the moment when quantum computers solve tasks and problems that conventional computers cannot realistically solve [13]. He later claimed that 30 years is "not an unrealistic timescale" for achieving general-purpose quantum computing su-

premacy [14]. However, in 2019, Google claimed that their Sycamore quantum processor solved a problem in three minutes, which would take a classical computer over a thousand years [15]. Not letting Google's claim go unchallenged, IBM rushed a preprint report claiming that they solved the same problem in 2.5 days using a classical technique [16], dismissing Google's quantum supremacy claim (the point where quantum computers can do things that classical computers can't). When Nature published Google's breakthrough on quantum supremacy [15], quantum researchers objected to using the term "supremacy", calling it irresponsible to override the historical context of the descriptor, which risks sustaining divisions in race, gender, and class. They called on the community to use "quantum advantage" instead [2]. In response to the controversy, Preskill explained why he called it "quantum supremacy" [17].

According to a recent report, private investors have funded at least 52 quantum-technology companies globally since 2012, and governments and large companies have poured billions into hardware that does not yet exist [18]. Quantum research is progressing faster than originally predicted [19], and the race for supremacy is getting hot and confrontational, with peers challenging Google's claim of supremacy [15] [16]. While it is abundantly clear that quantum supremacy or advantage is far from being achieved, it is worth taking a step back and precisely defining [20] what it should entail, or rather, what we want quantum supremacy to be.

2. Problem Statement

The EuroQCI (European Quantum Communication Infrastructure) initiative was launched in 2019. Seven Member States initially signed the EuroQCI Declaration, and all EU Member States subsequently joined the initiative [21]. The US Congress passed the Quantum Computing Cybersecurity Preparedness Act (H.R.7535) in July 2022 [22], and on December 21, 2022, President Biden signed it into law [22], which encourages "federal government agencies to adopt technology that will protect against quantum computing attacks". These legislations mark a major milestone in the global effort to develop and deploy quantum-resilient cybersecurity, making the world move quickly against the coming quantum computing threat since it takes significant effort and years to upgrade existing governmental and commercial cryptography infrastructure. Moreover, as many companies have already started offering commercial QC services for specialized computing needs [8], many questions demand urgent answers. How do you judge the performance of QC in the absence of a gold standard? How would anyone know a candidate QC has succeeded without a gold standard? How do you define a gold standard? Researchers predict that QC can cause havoc, resulting in a global catastrophe [3]. The same characteristics that make QC exponentially powerful also make it devilishly difficult to control if it breaks every possible encryption that makes today's Internet work [23]. Some experts claim the possibility of QC causing the collapse of the current cryptographic infrastructure is real [4], and the existential risk to humanity is amplified [5]. All these predictions are relevant only if QC becomes commercially viable and dep-

loyable in the service of humanity. And if they do, can they achieve supremacy without effective control to prevent their exploitation against humanity by bad actors? In other words, just as autonomous mobility cannot reach supremacy without an efficient braking mechanism, quantum computing cannot go anywhere without culling its catastrophe-causing capabilities. Technological supremacy can never trump humanity and humane interests. No technology can be allowed to go rogue. Not challenging the political correctness of the term, can 'quantum supremacy or advantage' be achieved merely by solving tasks beyond the capacity of classical computers? Unless safeguards are in place, can a new technology become commercially deployable and deliver any tangible value, particularly when experts associate catastrophic or existential risk with the technology? What good is an autonomous car or a nuclear chain reaction without the safeguard of a braking mechanism? If the risks limit its full commercial deployment, will QC ever be expected to achieve supremacy/advantage over classical computing? The answers to all the questions would come over time as QC evolves, but what is urgently needed is clearly defining the four corners of quantum supremacy/advantage as it is the most widely used terminology in quantum research and a goal that every quantum researcher is striving to achieve. Complete clarity of the goal will keep the quantum research focused.

2.1. The Blockchain Conundrum

Projected to be a multi-trillion industry [24], blockchain and cryptocurrencies exclusively rely on adversary-facing cryptography [25]. Several research groups are exploring PQC (post-quantum cryptography) for developing quantum-resistant blockchains [26]. Implementing PQC primitives in real-world use cases is prohibitively expensive [27]. The cost of a typical Ethereum blockchain transaction is already very high, clocking as high as 360 times the cost of a conventional database [28]. Attempts at making blockchain resilient with PQC will further accentuate the already prohibitory costs of blockchain transactions.

2.2. The Q-Day Quandary

The more powerful a technology is, the more likely it will be abused. QC community defines Q-day as a day when quantum computers will break the Internet [29]. Theoretically, all cryptography algorithms are vulnerable to quantum attacks [30]. Given the ubiquity of cryptographic schemes in our everyday online activities [31], this could be catastrophic [3] [4] [5]. Quantum supremacy/advantage should not just be our competence in getting closer to the Q-Day but our ability to cope with the perils of the Q-Day. Cryptography researchers worldwide are building PQC algorithms to sustain QC's computing power. However, with 80 of the 82 PQC candidates failing NIST's final round of the standardization process concluded in 2022, QC appears more detrimental to human interests than its benefits [32]. More recent Swedish and French cryptographers' reports suggest that CRYSTALS-Kyber and CRYSTALS-Dilithium, the two finalist PQCs, can also be compromised [33] [34]. Furthermore, a recent comprehensive survey confirms

that the security of most PQC algorithms is unfortunately insufficient, rendering them vulnerable [35]. After a six-year standardization process, no PQC algorithm has proven robustness and resilience, placing the NIST initiative in serious jeopardy.

2.3. Defining Quantum Supremacy/Advantage

Any new technology must be researched, conceived, discussed, developed, and implemented within a very simple principle—its existence should be perceived as a vehicle for human advancement. To achieve those objectives, the first order of business is benchmarking the standards that define the technology. So, what exactly does Quantum Supremacy/Advantage entail? Notwithstanding the controversy over the political correctness of the term, the four corners of quantum supremacy/advantage need to be clearly defined, even before any gold standard or benchmarking ideas are designed and standardized for establishing key performance indicators (KPIs) [36].

3. Research Purpose and Related Work

The principal objective of this research is to alleviate the looming catastrophic threats to the Internet from QC, as QC research advances from a futuristic concept to a near-term reality as companies have already commenced offering NISQ (Noisy Intermediate-Scale Quantum) computing services to their customers [8]. As discussed in detail in section 4.1, QaaS (Quantum-as-a-Service) is fast evolving as a preferred cloud-based QC business model. As today's Internet security is almost entirely cryptography-dependent [33], it remains vulnerable to the impending threats from the enormous computing power of the future QC. Currently, PQC is the only defense that has been explored to secure the Internet from the Q-Day threat. As reasons, therefore it is incumbent upon us to:

i) Firstly, articulate a comprehensive definition of quantum supremacy/advantage that sets the ethical goals to render QC sustainable;

ii) Secondly, design a plan B if ongoing PQC standardization by NIST and other standardization authorities falter.

Recently, a new encryption-agnostic cybersecurity paradigm of Zero Vulnerability Computing (ZVC) was proposed [9] [10]. The ZVC computing devices essentially merged all the conventional layers of firmware, drivers, operating system (OS), and the application layer to deliver a compact Solid-State Software on a Chip (3SoC) system that was completely secure with zero attack surface, was robust and energy efficient [10]. ZVC was explored as an alternative to PQC (Post Quantum Cryptography) as most of the 82 candidate PQC algorithms failed [7] [34] [35], seriously jeopardizing NIST's PQC standardization initiative [6]. ZVC's novel encryption agnostic 3SoC client-server framework was proposed as an Intranet solution to segregate QC from the mainstream Internet as QC companies deliver QC service in a QaaS business model. Based on the zero third-party permissions architecture ZVC/3SoC technology, an absolute zero trust (AZT) network that extends the zero trust concept to trust no application and

trust no code was recently introduced [37].

Arriving at a precise definition of quantum supremacy/advantage will largely depend on:

i) The evolution of the business model for delivering QC services to the end users (Section 4);

ii) The safeguards that secure the Internet from quantum threats and are relevant to that business model (Section 4).

Each of these elements is discussed in detail in the succeeding section, along with the description of the novel QaaS framework architecture proposed in this study (see Section 5).

4. State-of-the-Art

Research in QC is advancing exponentially, and the prospects of its future potential to deliver "quantum advantage" look bright [11]-[19]. However, before QC delivers the quantum advantage, NISQ (Noisy Intermediate Scale Quantum) defines the current era of quantum computers' handling executions of 50-100 qubits. For now, NISQ suffers from quantum gate noise, rendering fault-tolerant QC beyond reach [11]. Our problem statement identifies the inadequacies in dealing with future Q-Day threats when QC with sufficient qubits eventually becomes a reality. The first order of business in planning a defense of the Internet from the impending Q-Day threat is articulating a precise definition of the quantum supremacy/advantage, which will help us understand what exactly it entails and help us set specific goals and KPIs to achieve the quantum supremacy/advantage. This largely depends on the following:

i) Understanding the evolution of the business model for delivering QC services to the end users;

ii) The safeguards that secure the Internet from quantum threats are relevant to that business model. The relevant state-of-the-art in each of these areas is presented herein.

4.1. The Evolving Quantum-as-a-Services Business Model

By most estimates, a single qubit costs around $10,000 [38] [39] [40]. An encryption-breaking QC is estimated to require approximately 317 million qubits [39]. On top of the actual cost of the qubits, a host of sophisticated electronics, coaxial cabling, and other materials that achieve near absolute zero operational temperatures, housed in a large, controlled room, costs a fortune. Even if the price of each qubit comes down by a thousand times, an encryption-breaking QC will still cost in the range of $3 billion, a price far beyond the reach of ordinary mortals and certainly not an ordinary hacker's cup of tea. The only possible business model that can make QC accessible to end users is through cloud-based services. Quantum-as-a-Service (QaaS) is rapidly evolving as a likely business model [41]. At least six QCSPs (Quantum Computing Service Providers), including Amazon and IBM, have already launched their QaaS offerings to scientists, researchers, and developers of cloud services for building, testing, and run-

ning QC algorithms [42]. Some of these QCSPs even offer their QaaS for free [43]. Governments can regulate QCSPs to restrict subscription to verified subscribers under terms and conditions that allow target quantum algorithms only to be deployable to pre-registered domains and mandate specific security protocols and KYC (know your customers) procedures to access the QC services. The QaaS business model is easier to regulate as compared to regulating the randomly scattered desk-top hackers. The standardizing and policy-making agencies, e.g., the NIST in the US [6] and ENISA [23], its equivalent in Europe, are currently focusing exclusively on PQC (post-quantum cryptography) to endure the decryption capabilities of powerful QCs. The recent failure of candidate PQC algorithms [7] [32] [33] [34] [35] [36], and the evolving QaaS business model compels us to rethink our QC safeguarding strategy. It persuades us to look beyond the state-of-the-art to safeguard classical computers from future quantum hackers.

4.2. QC Safeguards

Not all existing security tools are vulnerable to attacks with QC [44] [45]. The quantum threat to legacy computers can be broadly dealt with in any one of the following two ways:

- Protecting each Internet-connected legacy computer individually from quantum attacks with one of the state-of-the-art PQC algorithms.
- Segregating all QC activities from the mainstream Internet with a new encryption agnostic ZVC (Zero Vulnerability Computing) technology [10].

4.3. State-of-the-Art Safeguards with PQC

Cryptography is omnipresent in securing data and authenticating its access [31] [46] [47], and is used in almost all inter-device communications, whether within the network or in non-network scenarios [48]. Cryptography remains the foundation of Internet security [49]. State-of-the-art, therefore, takes the first approach to protecting individual computers with PQC algorithms. It is also a natural culmination of prevailing cybersecurity practices in prior art. As it will be impossible to instantly modernize and upgrade the encryption algorithms of all and sundry IT systems operating across the Internet today, preparations must commence well ahead of time to handle the new situation [50]. Securing a computer in a network without cryptography is inconceivable in legacy systems. For this reason, quantum threats exist, and it is for the same reason that standardization bodies are currently working on standardizing PQC processes. These efforts are being led by the US-based NIST, the International Standards Organization (ISO), the Internet Engineering Task Force (IETF), and the European Telecommunications Standards Institute (ETSI). Each one of these initiatives is at a different stage and covers different PQC schemes. With the recent setbacks that NIST has faced and no clear success emerging out of NIST's PQC standardization process initiated six years ago [6], it becomes important to explore the possibilities beyond PQC. In that context, a new hypothesis on quantum resilient computing is worth investigating (**Figure 1** Graphical Abstract).

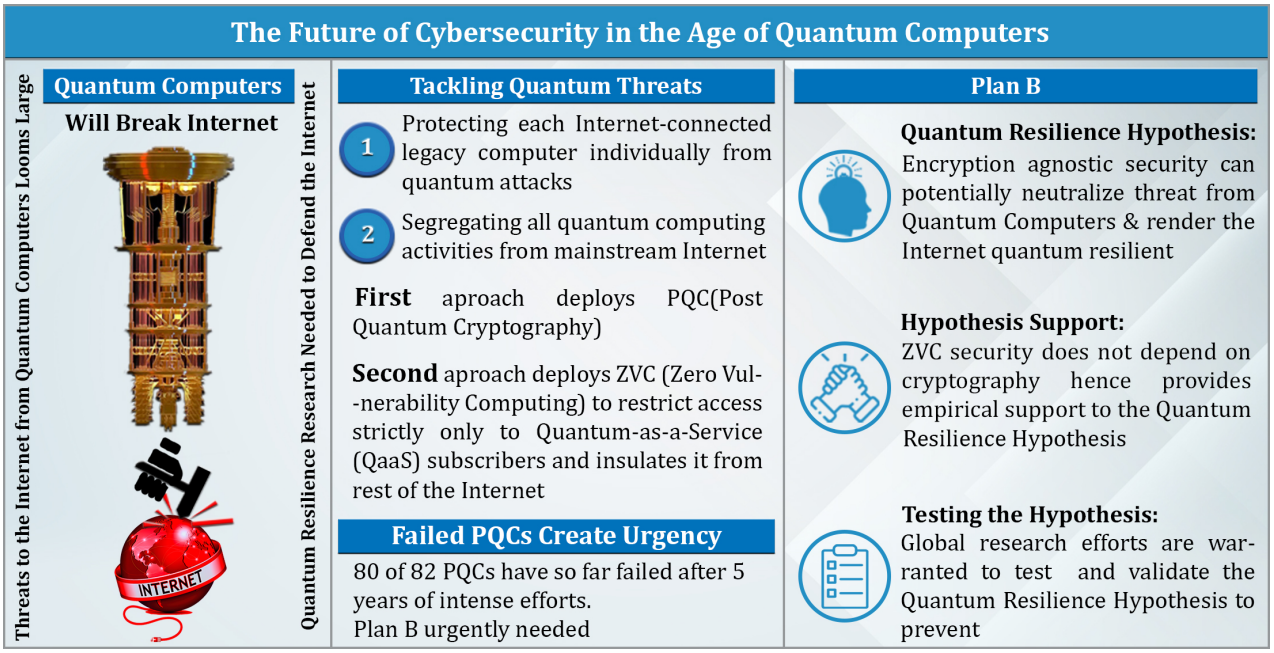


Figure 1. Quantum Cybersecurity Graphical Abstract: *Future Internet*, 2022, 14(11), 335 [10].

5. Beyond State-of-the-Art

Since the birth of the modern computer, cryptography has remained the mainstay of the security of our computing infrastructure. Internet security is inconceivable without cryptography [46] [47] [48] [49]. Also inconceivable in the prior art is building computer hardware or software devoid of 3rd party permissions [9] [10] [37]. These permissions allow diverse applications to run on a computer and make the computer useful. Without these permissions, a computer would be useless. However, on the flip side, these 3rd party permissions allow bad actors to access the computer's computing resources and create attack vectors that exploit those permissions to inject malware. As long as the 3rd party permissions exist, a computer will remain vulnerable to an attack surface that a bad actor can target with malware. A computer with zero attack surface is impossible in prior art, and for the same reason, foolproof cybersecurity remains impossible [9] [10] [37]. Because a computer always remains at risk of being accessible to a non-native rogue program or code, a strong encryption scheme is required to authenticate such access. However, if all non-native programs or codes are by design declined permissions to access a computer's resources, the need for encryption to authenticate 3rd party access becomes inconsequential. Zero Vulnerability Computing (ZVC) is a new cybersecurity paradigm developed on these encryption-agnostic security hypotheses (**Figure 1**) [9] [10] [37]. If a technology can secure a connected computer without needing user-facing access authorizing encryption algorithms, it will automatically make the connected device quantum safe. ZVC is the encryption agnostic approach recently proposed as an alternative to the Internet-wide deployment of the resource-intensive and expensive PQC [10]. Winning a Seal of Excellence from the European Commis-

sion (Figure 2), ZVC revolutionizes the classical architecture of computers by completely obliterating a computer's attack surface by banning all 3rd party permissions, and as illustrated in the graphical abstract in Figure 1, transforms the multilayered legacy computing systems to solid state software on a chip (3SoC) [51].

5.1. Encryption Agnostic Cybersecurity

As stated, in legacy computing systems, all hardware and software are designed to grant 3rd party permissions so that vendors and developers can create various applications that make computers useful. It is impossible to build a computer without incorporating 3rd party permissions. Most computer vulnerabilities originate from those inherent permissions [9] [10]. As illustrated in Figure 2, ZVC achieves zero vulnerability by

1) Banning all 3rd party permissions, thus completely obliterating the attack surface.

2) Creating switchable in-computer offline storage within the connected device itself.

As illustrated in Figure 3, multilayered legacy computing systems are built on granting third-party permissions at each layer. This introduces an attack surface at each layer, leading to variabilities analogous to the moving parts setting of old-generation electronic devices. The ZVC permissionless architecture merges all the layered components in the legacy software to render it free of any attack surface, resulting in zero vulnerabilities (Figure 3).

Complexities and variabilities create a situation similar to the pre-Solid-State electronics era, wherein moving parts in electronic devices of that era made the devices fragile, bulky, energy inefficient, and vulnerable to external risks. The advent of Solid-State technology revolutionized electronics and made today's portable computing devices possible. Drawing an analogy from solid-state electronics' zero moving parts characteristics, the legacy computing systems' complex multi-layered architecture with 3rd party permissions at every layer can be likened to the pre-solid-state era bulky, fragile, and energy-swigging electronics. Because ZVC eliminates all the variables that the complex multi-layered legacy computing architecture introduced and obliterates the attack surface by banning 3rd party permissions, it creates a scenario akin to no moving parts of Solid-State electronics [10] [51]. The variabilities in the layered architecture of legacy software systems are analogous to the moving parts in old non-solid-state electronic devices. The direct implementation of ZVC on the nonvolatile memory chip of a computing device eliminates the need for piggybacking on the device's firmware or OS, enabling us to design a radically novel concept of Solid-State Software on a Chip (3SoC) with no conventional layers of firmware, drivers, OS, and application (all moving parts) between the hardware and the human-computer interface [51]. Such a 3SoC approach creates a compact solid-state software milieu that is robust, energy efficient, and free of attack surface that bad actors often exploit to breach security [9] [10] [37] [51].

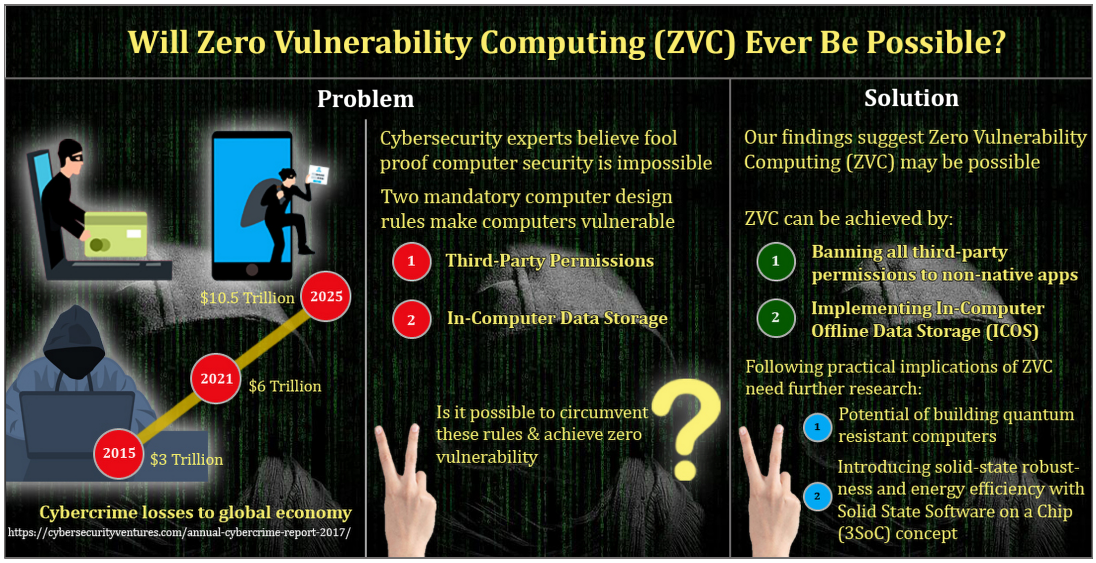
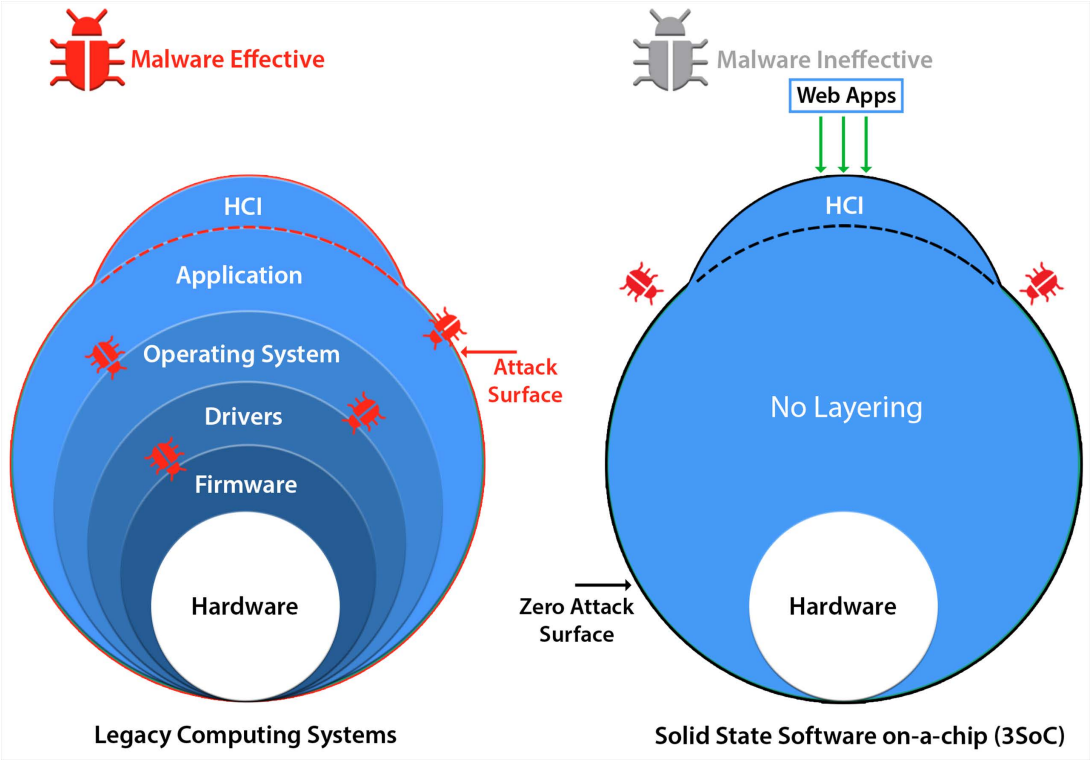


Figure 2. ZVC Graphical Abstract—Future Internet 14.8 (2022): 238 (2022) [10].



Credit: Image adapted from Future Internet 14.8 (2022): 238.

Figure 3. Layered Legacy System (A); Vs 3SoC (B).

5.2. ZVC-Powered 3SoC Client-Server QaaS Network

As illustrated in **Figure 4**, this encryption-agnostic approach essentially segregates QC from the mainstream computing infrastructure within the Internet. In this ZVC-powered novel QaaS architecture, a typical QCSP (Quantum Computing Service Provider) provides its cloud-based quantum computing services to

its subscribers in a business model that's quite like any cloud computing service provider today. As we have seen in a previous section, such isolation of QC from legacy Internet is supported by QC's evolving subscription-based QaaS business model that caters to the highly specialized, high-power computing needs of specific industry users. In the proposed QaaS framework, as a term of service, the subscribers are provided with a 3SoC client to access the quantum computing services of the QCSP. The QCSP routes access to the quantum computer through a 3SoC server that exclusively accepts authentication requests from a 3SoC client device. All other requests from non-subscribers or hackers with legacy computing devices are declined (Figure 4).

As further illustrated in Figure 5, this novel QaaS architecture can potentially provide unbreakable end-to-end security to access QC and isolate it from the rest of the Internet. This means that the genuine, KYC-verified subscribers of the QaaS platform can be mandated to deploy specific security protocols to access QC within a secure Intranet segregated from the rest of the Internet. The 3SoC tunnel connecting the user to the QC is encryption agnostic and immune to encryption-breaking quantum algorithms. Such a QaaS framework makes QC inaccessible to bad actors. Most importantly, this strategy nullifies the need for an Internet-wide, device-focused deployment of the resource-intensive PQCs that demand significant processing time and power [52], which is a significant incumbrance on most of the 75 billion connected devices to populate the Internet by 2025 [53]. Thus, a 3SoC intranet can potentially defend against misuse of quantum computing by bad actors even if the PQC algorithms currently under pursuit [6] fail to deliver the promise.

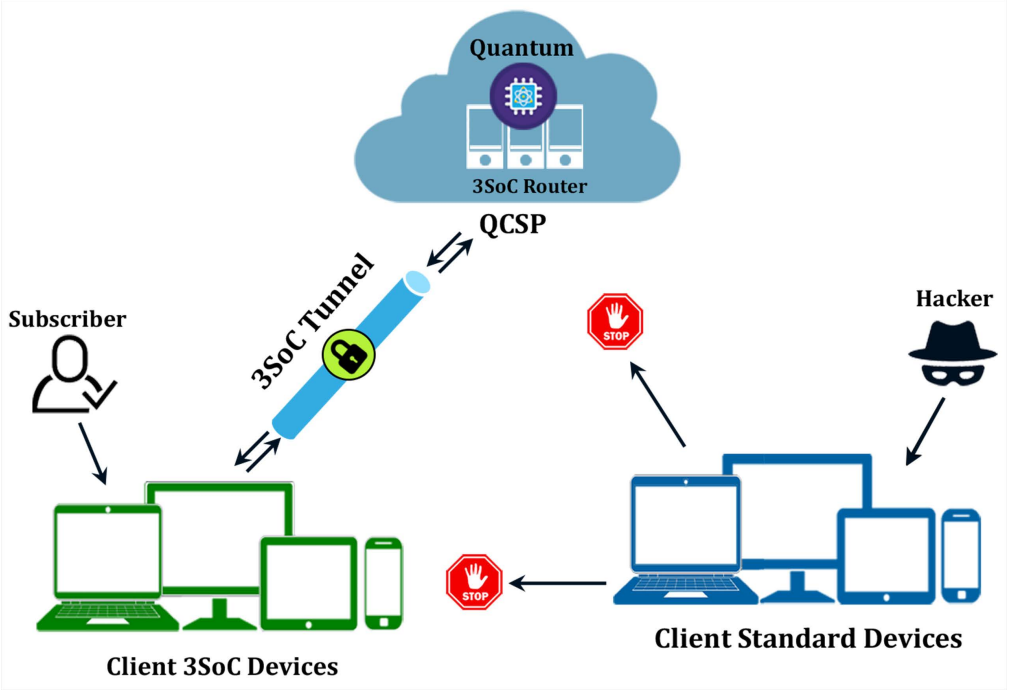


Figure 4. 3SoC gateway to keep QC inaccessible to hackers.

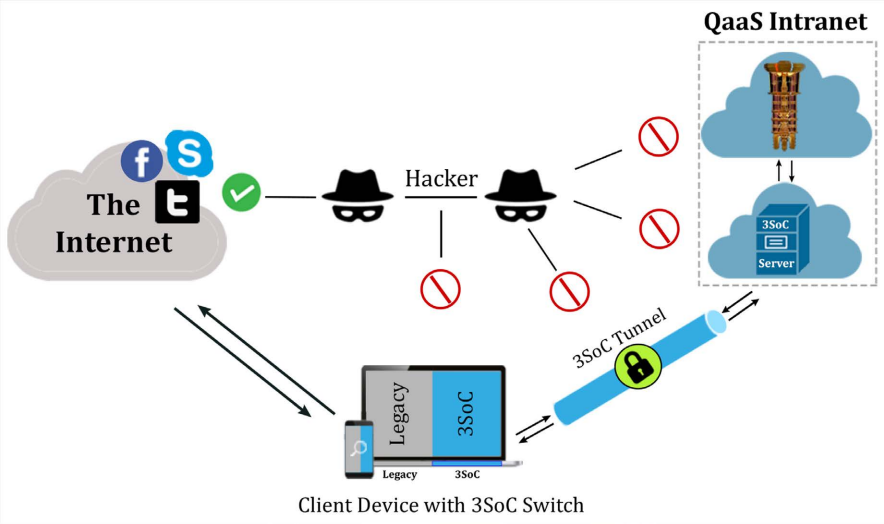


Figure 5. Switchable QaaS Intranet for segregating QC from mainstream Internet.

6. The Inflection Point & Quantum-Safe Internet

As stated, a good majority of the 75 billion devices connected to the Internet by 2025 [53] will have minimal computing and energy resources, posing significant restrictions on their hardware and software [52]. The communication between these devices, their limited energy source, and their limited processing power make running any cryptographic algorithm with longer keys challenging [52]. 95% of current Internet security is cryptography-based [31], bearing significant resource and cost consequences on the devices connected to the Internet. Moreover, in the future, quantum machine learning [54] and quantum generative learning models (QGLMs) [55] may surpass their classical counterparts and will be able to train faster, delivering a clear advantage over the classical models to become mainstream. The IoT devices with limited resources will be impacted the most.

All the evidence suggests that QC is experiencing an inflection point [56] [57] [58] [59] [60], compelling us to prepare for this new computing paradigm. Moreover, as companies have already commenced offering QaaS cloud services [8], the need to secure the Internet from impending quantum threats is greater than ever. Recent setbacks may jeopardize the original NIST timeline for PQC standardization, estimated at 15 years for a full transition to Quantum-safe Internet (**Figure 6**). Global PQC implementation is a massive undertaking impacting each computing device in the entire Internet ecosystem. It is not just time-consuming but a resource-intensive and expensive undertaking [60]. However, the alternate approach for quantum resilience that this paper proposes limits its implementation to QCSPs offering discerning QaaS subscription exclusively to highly selective special need clients, warranting no Internet-wide implementation of QC. Thus keeping the QC from exploiting bad actors at bay. Therefore, as illustrated in Fig. 6, the process of validation and full transition to quantum-safe internet via ZVC/3SoC can be accomplished much faster than the PQC timeline projected by NIST.

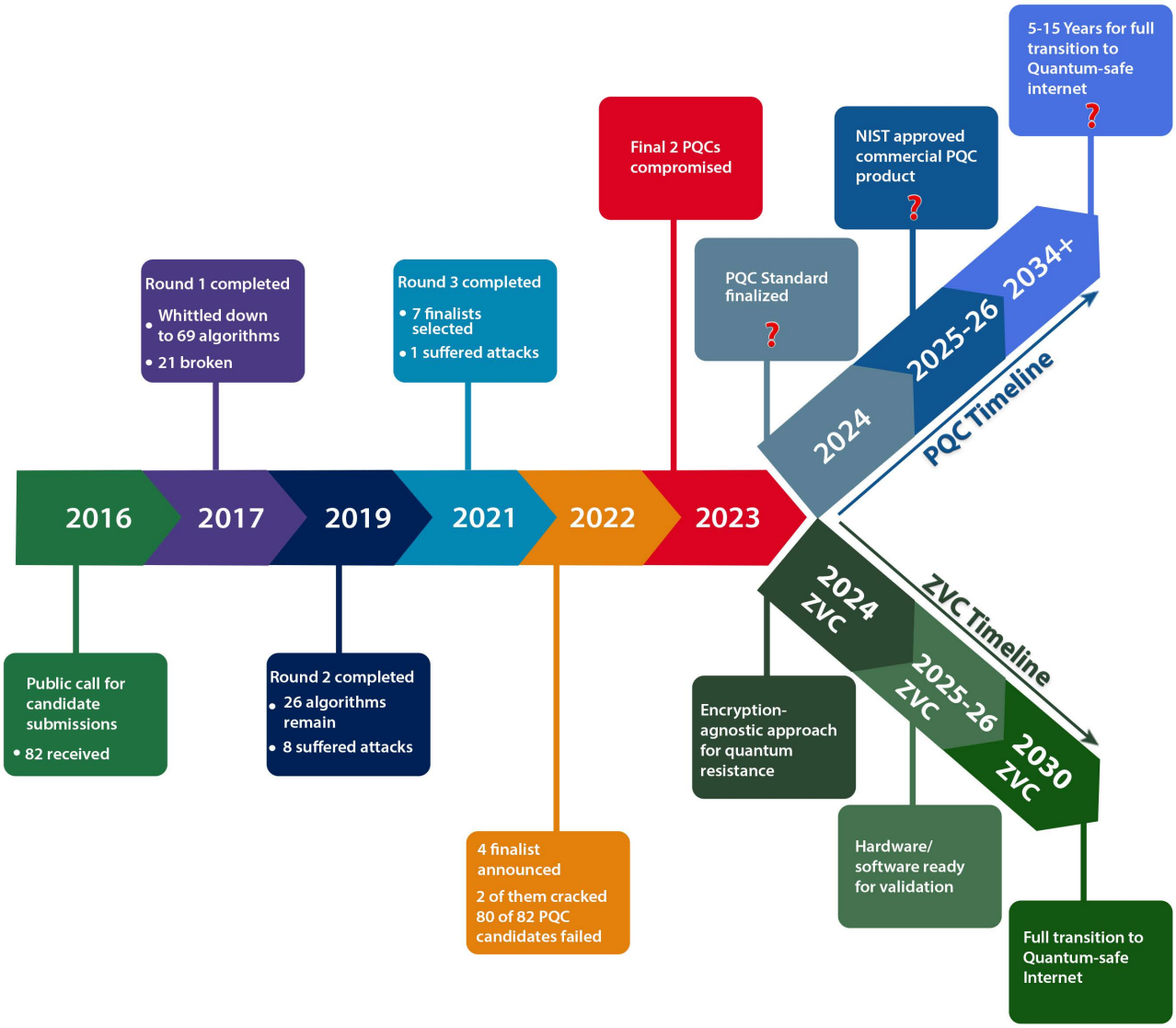


Figure 6. Quantum Resilience reaches the Inflection Point and Beyond (timeline based on extrapolation of data from NIST). Adapted from *Journal of Computer and Communications* 12.3 (2024): 252-282 [37].

7. Conclusions

The astronomically high cost of QC virtually rules out universal, unfettered access to quantum algorithms by all and sundry. As a natural corollary, the QaaS business model evolves as relatively more sustainable. QaaS can be implemented by enforcing regulatory policies and rendering all malicious activities by bad actors technologically out of bounds. The regulatory authorities can control the former and the latter by deploying the ZVC-powered 3SoC client-server QaaS network architecture proposed in this paper. The impending quantum threats to the Internet can be best dealt with by segregating all subscription-based QC activities from the mainstream Internet by regulating the QaaS access rather than attempting to protect each Internet-connected device individually from quantum attacks. The findings of this study can be summarized as follows:

1) The astronomically high cost of QC makes it unaffordable for the common man, so QC can never be as accessible as legacy computers are to everyone.

2) Because of QC's prohibitory costs, QaaS is fast evolving as a subscription-based cloud computing business model for offering quantum computing services.

3) QaaS' business model makes it easier to regulate QC technologically and legally than securing each Internet-connected computing device individually with PQC.

4) A new encryption-agnostic cybersecurity paradigm can secure the Internet from any impending quantum threats by segregating QC and not letting QC it go wild, and significantly shorten the timeline for making the Internet Quantum-safe.

5) Universal Internet-wide implementation of computationally intense and expensive PQC may not be warranted to secure the Internet from the potential Q-Day threat.

Finally, for the purpose of benchmarking and developing KPIs for defining quantum advantage, Quantum Supremacy/Advantage can be articulated as "*deemed to have been achieved when a quantum computer measurably and sustainably solves algorithmic problems that conventional computers cannot realistically solve in a timeframe and manner that restrains rogue elements from its misuse in disrupting a classical computer's cybersecurity and compromising the integrity of the Internet*".

8. The Limitations of the Study

This paper provides theoretical support for deploying a new cybersecurity paradigm that was originally tested in a minimalist hardware wallet device [9] to secure the scam-prone, hack-prone blockchain economy. 3SoC, QaaS, Quantum Ledger Technology (QLT), and other use case scenarios are currently being explored under several collaborative research projects. These investigations have far-reaching implications on our understanding of solid-state electronics and computer hardware/software, in general, and on enhancing their security and resilience in building a robust Internet. Nevertheless, the principal objective of this study remains limited to arriving at a precise definition of "quantum supremacy/advantage" to guide future research in safeguarding the Internet from potential Q-day threats. This research generates a theoretical definition of QC as a minimal viable product (MVP) capable of commercial deployment. This will help in setting empirical KPIs (key performance indicators) to measure the outcomes of QC research for testing and validating the commercial viability of QC. The following limitations of this research should be considered before any extrapolations of the results of this study are made to the real-world scenarios:

i) The QaaS architecture is designed based on empirical data from a series of minimalist hardware wallet experiments [10] and needs to be validated in diverse QC ecosystems before it can be extrapolated to real-world computing en-

vironments.

ii) The ZVC/3SoC research is ongoing [9] [10] [37] [51], and the inferences drawn from the available data are preliminary and subject to updates as and when available.

iii) Currently, all hardware and software architectures are based on granting third-party permissions to non-native applications. The proposed approach changes that, imposing certain limitations on the universal accessibility of computing resources to third-party applications. How that pans out in real-world practice cannot be precisely predicted.

iv) 3SoC devices inherently restrict the porting of generic or non-conforming third-party peripheral devices [9] [10] [51] and hence operate within a restricted intranet.

v) Rigorous experimentation by peer researchers is warranted for testing, replicating, and validating the conclusions before ZVC/3SoC can be established as a new encryption-agnostic security paradigm for making the Internet quantum safe.

vi) Appropriate key performance indicators (KPIs) should be identified to justify the quantity and quality of the case studies designed to investigate the proposed ecosystem.

As stated, this is hypothesis-generating research designed explicitly with the specific objective of exploring and articulating the following:

i) A comprehensive definition of quantum supremacy/advantage that sets ethical goals to render QC sustainable;

ii) A plan B if ongoing PQC standardization initiatives [6] by NIST and other standardization authorities fail.

As much as the limitations of this research warrant a cautious interpretation of the results, the report provides compelling evidence to serve both the objectives of this study. It helps us define the four corners of the term quantum supremacy/quantum advantage so that quantum research can clearly identify the goals in designing and building a sustainable QC. It also helps establish the theoretical possibility of quantum-proofing the Internet and rendering it resistant to future Q-Day threats by deploying an encryption-agnostic approach to segregate QC from the mainstream Internet. The proposed ZVC/3S0C framework not only affords protection against future quantum threats but also secures the current computing infrastructure in a less resource-intensive and cost-effective way than the cryptographic approaches.

Patents

Raheman, Fazal. Solid State Software on a Chip (3SoC) for Building Quantum Resistant Web 3.0 Computing Device. US Patent Application US29/842,535, 15 June 2022.

Ethical Approval

This article does not contain any studies with human participants or animals

performed by any of the authors.

Research Data Policy and Data Availability Statements

All data are either included in the paper or can be found in the sources cited in the paper.

Acknowledgment

The author is grateful to Dr Brecht Vermeulen and Professor Peter Van Daele (IMEC—Ghent University, IDLab iGent Tower—Department of Information Technology, Technologiepark-Zwijnaarde 126, B 9052 Ghentechnot, Belgium) for support in the initial hypothesis building research, and to Mr. Tejas Bhagat and Ms. Sadiya Khan for their help in preparing this manuscript. The author is also grateful to Dr. Kotzanikolaou Panayiotis of the University of Piraeus and Dr. Kostas Kolomvatsos of the University of Thessaly for being trusted partners in several consortia and initiatives involved in the development of the Zero Vulnerability Computing (ZVC) concept.

Conflicts of Interest

The author declares that no known competing financial interests or personal relationships could have appeared to influence the work reported in this paper.

References

[1] Gibney, E. (2019) Hello, Quantum World! Google Publishes Landmark Quantum Supremacy Claim. *Nature*, **574**, 461-463. https://doi.org/10.1038/d41586-019-03213-z

[2] Palacios-Berraquero, C., Mueck, L. and Persaud, D.M. (2019) Instead of 'Supremacy' Use 'Quantum Advantage'. *Nature*, **576**, 213-214. https://doi.org/10.1038/d41586-019-03781-0

[3] Majot, A. and Yampolskiy, R. (2015) Global Catastrophic Risk and Security Implications of Quantum Computers. *Futures*, **72**, 17-26. https://doi.org/10.1016/j.futures.2015.02.006

[4] Stoll, L. (2022) Quantum Computing's Impact on General Cryptography Implementations. FSOKx Podcast.

[5] Schiffer, B.F. (2022) Quantum Computers as an Amplifier for Existential Risk. arXiv: 2205.02761. https://arxiv.org/abs/2205.02761

[6] Computer Security Research Center (2022) Post Quantum Cryptography PQC: Workshops and Timeline. https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

[7] Sparkes, M. (2022) Encryption Meant to Protect against Quantum Hackers Is Easily Cracked. New Scientist. https://www.newscientist.com/article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked/

[8] Hossenfelder, S. (2019) Quantum Supremacy Is Coming. It Won't Change the World. The Guardian. https://www.theguardian.com/technology/2019/aug/02/quantum-supremacy-comp

uters

[9] Raheman, F., Bhagat, T., Vermeulen, B. and Van Daele, P. (2022) Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. *Future Internet*, **14**, Article 238. https://doi.org/10.3390/fi14080238

[10] Raheman, F. (2022) The Future of Cybersecurity in the Age of Quantum Computers. *Future Internet*, **14**, Article 335. https://doi.org/10.3390/fi14110335

[11] Preskill, J. (2018) Quantum Computing in the NISQ Era and beyond. *Quantum*, **2**, 79. https://doi.org/10.22331/q-2018-08-06-79

[12] Johanssona, M.P., *et al.* (2021) Quantum Computing—A European Perspective. https://prace-ri.eu/wp-content/uploads/TR-Quantum-Computing-A-European-Perspective.pdf

[13] Preskill, J. (2012) Quantum Computing and the Entanglement Frontier. arXiv: 12035813.

[14] Brooks, M. (2019) Beyond Quantum Supremacy: The Hunt for Useful Quantum Computers. *Nature*, **574**, 19-21. https://doi.org/10.1038/d41586-019-02936-3

[15] Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., *et al.* (2019) Quantum Supremacy Using a Programmable Superconducting Processor. *Nature*, **574**, 505-510. https://doi.org/10.1038/s41586-019-1666-5

[16] Pednault, E., *et al.* (2019) Leveraging Secondary Storage to Simulate Deep 54-Qubit Sycamore Circuit. arXiv: 1910.09534. https://arxiv.org/abs/1910.09534

[17] Preskill, J. (2019) Why I Called It "Quantum Supremacy?" Quanta Magazine. https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/

[18] Gibny, E. (2019) Quantum Gold Rush: The Private Funding Pouring into Quantum Start-Ups. *Nature*, **574**, 22-24. https://doi.org/10.1038/d41586-019-02935-4

[19] Hasanovic, M., Panayiotou, C., Silberman, D., Stimers, P. and Merzbacher, C. (2022) Quantum Technician Skills and Competencies for the Emerging Quantum 2.0 Industry. *Optical Engineering*, **61**, Article ID: 081803. https://doi.org/10.1117/1.oe.61.8.081803

[20] Supremacy Definition (2023) Britannica Dictionary. https://www.britannica.com/dictionary/supremacy

[21] Ribezzo, D., Zahidy, M., Vagniluca, I., Biagi, N., Francesconi, S., Occhipinti, T., *et al.* (2022) Deploying an Inter-european Quantum Network. *Advanced Quantum Technologies*, **6**, Article ID: 2200061. https://doi.org/10.1002/qute.202200061

[22] Sanzeri, S. (2023) What the Quantum Computing Cybersecurity Preparedness Act Means for National Security. https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/

[23] Lin, H. (2023) The Mother of All Data Breaches: Quantum Computing Holds New Promises and Dangers. Such Devices Could Overturn Our Whole Cybersecurity Regime, Revealing Not Just Mountains of Data But Secrets from Years Past. *Hoover Digest*, **1**, 79-83.

[24] Horch, A., Schunck, C.H. and Ruff, C. (2022) Adversary Tactics and Techniques specific to Cryptocurrency Scams. Open Identity Summit 2022. Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn.

[25] Kearney, J.J. and Perez-Delgado, C.A. (2021) Vulnerability of Blockchain Technologies to Quantum Attacks. *Array*, **10**, Article ID: 100065. https://doi.org/10.1016/j.array.2021.100065

[26] Unogwu, O.J., Doshi, R., Hiran, K.K. and Mijwil, M.M. (2022) Introduction to Quantum-Resistant Blockchain. In: Shrivas, M.K., Hiran, K.K. and Bhansali, A., Eds., *Advancements in Quantum Blockchain with Real-Time Applications*, IGI Global, 36-55. https://doi.org/10.4018/978-1-6684-5072-7.ch002

[27] Aji, A., Jain, K. and Krishnan, P. (2021) A Survey of Quantum Key Distribution (QKD) Network Simulation Platforms. 2*nd Global Conference for Advancement in Technology* (*GCAT*), Bangalore, 1-3 October 2021, 1-8. https://doi.org/10.1109/GCAT52182.2021.9587708

[28] Rimba, P., *et al.* (2017) Comparing Blockchain and Cloud Services for Business Process Execution. 2017 *IEEE International Conference on Software Architecture* (*ICSA*), Gothenburg, 3-7 April 2017, 257-260. https://doi.org/10.1109/ICSA.2017.44

[29] Castelvecchi, D. (2022) The Race to Save the Internet from Quantum Hackers. *Nature*, **7896**, 198-201. https://doi.org/10.1038/d41586-022-00339-5

[30] Laura, D. (2022) Post-Quantum Crypto Cracked in an Hour with One Core of an Ancient Xeon. The Register. https://www.theregister.com/2022/08/03/nist_quantum_resistant_crypto_cracked/

[31] Google (2019) Transparency Report: HTTPS Encryption by Chrome Platform. https://transparencyreport.google.com/https/overview

[32] Townsend, K. (2023) AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm. Security Week. https://www.securityweek.com/ai-helps-crack-a-nist-recommended-post-quantum-encryption-algorithm/

[33] Yanning, J. and Dubrova, E. (2023) A Side-Channel Attack on a Masked Hardware Implementation of CRYSTALS-Kyber. Cryptology ePrint Archive. https://eprint.iacr.org/2023/1084

[34] Berzati, A., *et al.* (2023) A Practical Template Attack on CRYSTALS Dilihium. Cryptology ePrint Archive. https://ia.cr/2023/050

[35] Canto, A.C., *et al.* (2023) Algorithmic Security Is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security. arXiv: 2305.13544.

[36] Becker, C., *et al.* (2022) Towards a Quantum Benchmark Suite with Standardized KPIs. 2022 *IEEE* 19*th International Conference on Software Architecture Companion* (*ICSA-C*), Honolulu, 12-15 March 2022, 160-163.

[37] Raheman, F. (2024) From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. *Journal of Computer and Communications*, **12**, 252-282. https://doi.org/10.4236/jcc.2024.123016

[38] Levy, J. (2022) 1 Million Qubit Quantum Computers: Moving beyond the Current "Brute Force" Strategy," SEEQC. https://seeqc.com/blog/1-million-qubit-quantum-computers-moving-beyond-the-current-brute-force-strategy

[39] Koetsier, J. (2022) Million-Qubit Quantum Computing? How SEEQC Plans to Scale Quantum Computers. https://www.forbes.com/sites/johnkoetsier/2022/01/11/million-qubit-quantum-computing-how-seeqc-plans-to-scale-quantum-computers/?sh=53ee0cf35b46

[40] Webber, M., Elfving, V., Weidt, S. and Hensinger, W.K. (2022) The Impact of Hardware Specifications on Reaching Quantum Advantage in the Fault Tolerant Regime. *AVS Quantum Science*, **4**, Article ID: 013801. https://doi.org/10.1116/5.0073075

[41] Casati, N.M. (2021) Use of Quantum Computers in Understanding Cultures and

Global Business Successes. In: Thakkar, B.S., Ed., *Culture in Global Businesses*, Palgrave Macmilla, 77-103. https://doi.org/10.1007/978-3-030-60296-3_5

[42] Scott III, F. (2021) A Buyer's Guide to Quantum as a Service: Qubits for Hire. https://www.zdnet.com/article/a-buyers-guide-to-quantum-as-a-service-qubits-for-hire/

[43] Sharma, S.K. and Khaliq, M. (2021) The Role of Quantum Computing in Software Forensics and Digital Evidence: Issues and Challenges. In: Kumar, N., Agrawal, A., Chaurasia, B.K. and Khan, R.A., Eds., *Limitations and Future Applications of Quantum Cryptography*, IGI Global, 169-185. https://doi.org/10.4018/978-1-7998-6677-0.ch009

[44] Wallden, P. and Kashefi, E. (2019) Cyber Security in the Quantum Era. *Communications of the ACM*, **62**, 120. https://doi.org/10.1145/3241037

[45] Marcelo, G., Mendonça, F. and Albuquerque, R.D.O. (2022) Assessments on National Cyber Capability: A Brazilian Perspective in a Comparison with Spain. 2022 17*th Iberian Conference on Information Systems and Technologies* (*CISTI*), Madrid, 22-25 June 2022, 1-6.

[46] Riebe, T., Kühn, P., Imperatori, P. and Reuter, C. (2022) U.S. Security Policy: The Dual-Use Regulation of Cryptography and Its Effects on Surveillance. *European Journal for Security Research*, **7**, 39-65. https://doi.org/10.1007/s41125-022-00080-0

[47] Sriadhi, S., Rahim, R. and Ahmar, A.S. (2018) Rc4 Algorithm Visualization for Cryptography Education. *Journal of Physics*: *Conference Series*, **1028**, Article ID: 012057. https://doi.org/10.1088/1742-6596/1028/1/012057

[48] Liu, X., Lee, W., Bui, Q., Lin, C. and Wu, H. (2018) Biometrics-Based RSA Cryptosystem for Securing Real-Time Communication. *Sustainability*, **10**, Article 3588. https://doi.org/10.3390/su10103588

[49] Joshi, S., Bairwa, A.K., Pljonkin, A.P., Garg, P. and Agrawal, K. (2023) From Pre-Quantum to Post-Quantum RSA. *Proceedings of the* 6*th International Conference on Networking*, *Intelligent Systems & Security*, Larache, 24-26 May 2023, 1-8. https://doi.org/10.1145/3607720.3607721

[50] Koczka, F. (2020) Security of Encryption Procedures and Practical Implications of Building a Quantum Computer. *Academic and Applied Research in Military and Public Management Science*, **19**, 5-22. https://doi.org/10.32565/aarms.2020.3.1

[51] Raheman, F. (2022) Solid State Software on a Chip (3SoC) for Building Quantum Resistant Web 3.0 Computing Device. US Patent Application US29/842,535.

[52] Kumar, M. (2022) Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis. *Array*, **15**, Article ID: 100242. https://doi.org/10.1016/j.array.2022.100242

[53] Banafa, A. (2023) The Industrial Internet of Things (IIoT): Challenges, Requirements, and Benefits. In: Banafa, A., Ed., *Introduction to Internet of Things* (*IoT*), River Publishers, 5-10. https://doi.org/10.1201/9781003426240-2

[54] Tychola, K.A., Kalampokas, T. and Papakostas, G.A. (2023) Quantum Machine Learning—An Overview. *Electronics*, **12**, Article 2379. https://doi.org/10.3390/electronics12112379

[55] Jain, S., Geraci, J. and Ruda, H.E. (2023) Comparing Classical and Quantum Generative Learning Models for High-Fidelity Image Synthesis. *Technologies*, **11**, Article 183. https://doi.org/10.3390/technologies11060183

[56] Bhasin, A. and Tripathi, M. (2021) Quantum Computing at an Inflection Point: Are We Ready for a New Paradigm. *IEEE Transactions on Engineering Management*,

70, 2546-2557.

[57] Sotelo, R. (2021) Quantum Computing Entrepreneurship and IEEE TEMS. *IEEE Engineering Management Review*, **49**, 26-29. https://doi.org/10.1109/EMR.2021.3098260

[58] Baca, M. (2022) Post-Quantum and Pre-Quantum Security Issues Grow. Semiconductor Engineering. https://semiengineering.com/post-quantum-and-pre-quantum-security-issues-grow/

[59] Joseph, D., *et al.* (2022) Transitioning Organizations to Post-Quantum Cryptography. *Nature*, **605**, 237-243. https://doi.org/10.1038/s41586-022-04623-2

[60] Mosca, M. and Piani, M. (2021) Quantum Threat Timeline Report 2021. Global Risk Institute. https://globalriskinstitute.org/publication/quantum-threat-timeline/