*future internet*

*Brief Report*

# The Future of Cybersecurity in the Age of Quantum Computers

**Fazal Raheman**

Blockchain 5.0 Ltd., Kesklinna Linnaosa, Ahtri tn 12, 10151 Tallinn, Estonia; drfazal@bc5.eu

**Abstract:** The first week of August 2022 saw the world's cryptographers grapple with the second shocker of the year. Another one of the four post-quantum cryptography (PQC) algorithms selected by the NIST (National Institute of Standards and Technology) in a rigorous 5-year process was cracked by a team from Belgium. They took just 62 min and a standard laptop to break the PQC algorithm to win a USD 50,000 bounty from Microsoft. The first shocker came 6 months earlier, when another of the NIST finalists (Rainbow) was taken down. Unfortunately, both failed PQC algorithms are commercially available to consumers. With 80 of the 82 PQC candidates failing the NIST standardization process, the future of the remaining two PQC algorithms is, at best, questionable, placing the rigorous 5-year NIST exercise to build a quantum-safe encryption standard in jeopardy. Meanwhile, there is no respite from the quantum threat that looms large. It is time we take a step back and review the etiology of the problem de novo. Although state-of-the-art computer security heavily relies on cryptography, it can indeed transcend beyond encryption. This paper analyzes an encryption-agnostic approach that can potentially render computers quantum-resistant. Zero-vulnerability computing (ZVC) secures computers by banning all third-party permissions, a root cause of most vulnerabilities. ZVC eliminates the complexities of the multi-layered architecture of legacy computers and builds a minimalist, compact solid-state software on a chip (3SoC) that is robust, energy-efficient, and potentially resistant to malware as well as quantum threats.

**Keywords:** quantum computers; quantum threat; cybersecurity; computer vulnerabilities; PQC; computer architecture; NIST; hacking; solid state

check for updates

**Citation:** Raheman, F. The Future of Cybersecurity in the Age of Quantum Computers. *Future Internet* **2022**, *14*, 335. https://doi.org/10.3390/fi14110335

Academic Editors: Agostino Forestiero and Mohamed Abd Elaziz

Received: 31 August 2022
Accepted: 9 November 2022
Published: 16 November 2022

## 1. Introduction

Over four decades ago, the idea of quantum computers was conceived by Richard Feynman and Yuri Manin [1]. In the past decade, research on quantum computers has picked up substantial momentum. The possibility of a fully functional quantum computer appears within reach (Figure 1). The idea that certain computational tasks might be executed exponentially faster than all the known state-of-the-art algorithms is an experimental realization of quantum supremacy [2].

While quantum scientists are banking on the numerous benefits of quantum computers [3], scholars are concerned about saving the Internet from quantum hackers [4]. Projected to grow to a USD 10.5 trillion industry by 2025 [5], the advent of quantum computers will make cybercrime unassailable [6]. Earlier this year, quantum attacks on several cryptocurrencies led to the latest crypto crash [7]. While the cybersecurity community is busy addressing the adverse technology implications of quantum computing [8], some evangelists are alerting to a quantum apocalypse [9], and others are even warning about an existential risk similar to that concerning artificial intelligence [10].

The quantum threat to legacy computers can be broadly dealt with in two ways:

(i) Protecting each Internet-connected legacy computer individually from quantum attacks;
(ii) Segregating all quantum computing activities from mainstream Internet.

As illustrated in Section 2, the state of the art is mostly taking the first approach in protecting individual computers with PQC (post-quantum cryptography) algorithms. However, as discussed in Sections 3 and 4, the approach proposed in this paper follows the second strategy, and instead of the Internet-wide deployment of PQC, it essentially isolates quantum computing, which, in any case, is evolving as a preferred business model of a subscription-based QaaS (quantum-as-a-service) offering rather than an unregulated free offering for all technology. For the reasons discussed in Section 5, it is clear that quantum computing is fast evolving into a highly specialized QaaS business model for the high-power computing needs of specific industry users. This means that the subscribers of such a QaaS offering can be mandated to deploy specific security protocols to access QaaS.

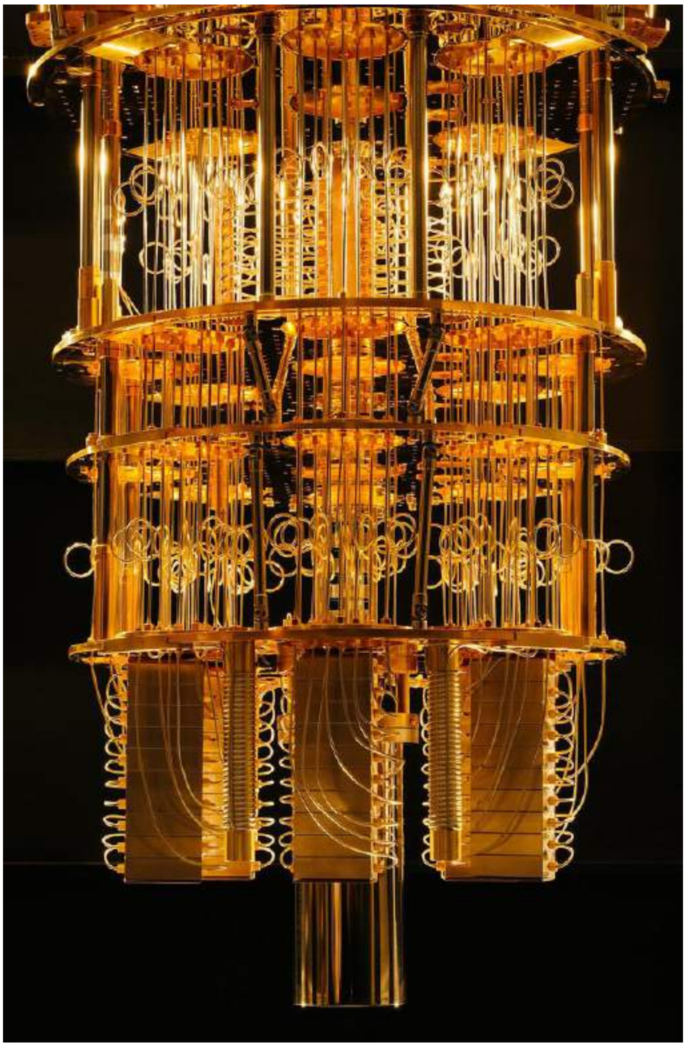


**Figure 1.** IBM quantum computer. Image Credit: Flickr.

- There is a growing interest in cloud-based quantum computers;
- Recent advances indicate that **quantum-as-a-service** (QaaS) is currently a real option [11];
- At least six QaaS providers [12], including Amazon and IBM, have already launched their "Quantum-as-a-Service" for scientists, researchers, and developers to build, test, and run quantum computing algorithms;
- IBM is even offering its QaaS free [13];
- Subscription to such a QaaS offering can be mandated to deploy specific security protocols to access the QaaS;
- Based on a recent report on "zero-vulnerability computing (ZVC)" [14], this paper builds rational support for a hypothetical question that is relevant to the safety of quantum computing: will ZVC's encryption agnosticism make it quantum-safe?
- ZVC's encryption-agnostic security protocol can potentially provide unbreakable end-to-end security to access QaaS and isolate it from the rest of the Internet;

- Since the QaaS access authentication approach proposed in this paper virtually eliminates all the probabilities of exposing legacy computers to encryption-breaking quantum algorithms, the recent failures of PQC algorithms become inconsequential.

Based on the aforementioned information, this paper presents observational research that compiles empirical data to build support for the quantum-safe hypothesis on the future of cybersecurity, and in Section 6, it concludes that the impending quantum threats to the Internet can be best dealt with by segregating all subscription-based quantum computing activities from the mainstream Internet by regulating the QaaS access, rather than attempting to protect each Internet-connected device individually from quantum attacks.

## 2. Problem Statement

In November 2017, 82 candidate algorithms were submitted to the NIST (National Institute of Standards and Technology) for consideration in a public competition for the process of selecting PQC (post-quantum cryptography) algorithms [15]. This initiative was launched to counter the impending security threats from quantum computers that may become real by 2030 when fully functional quantum computers become available [16]. These quantum systems will be able to run the algorithms that have the capability of decrypting most of today's asymmetric security protocols, such as the commonly used RSA or elliptical curve algorithms.

Experts suggest that industries should prepare for PQC based on data shelf life and system lifetime [17]. For example, according to a McKinsey Digital report, and as illustrated in Figure 2, some data with a long shelf life—such as classified government documents, personal health data, or corporate trade secrets—will still be valuable when the first quantum computers are expected to become available. Any such data that remain relevant for a long time, transferred today on public networks, will be at risk of interception and future decryption by quantum computers. For instance, a long-term life insurance plan or a 30-year home mortgage loan contract may already be vulnerable to future quantum threats because such data will still be active in the future when quantum computers become commercially available.

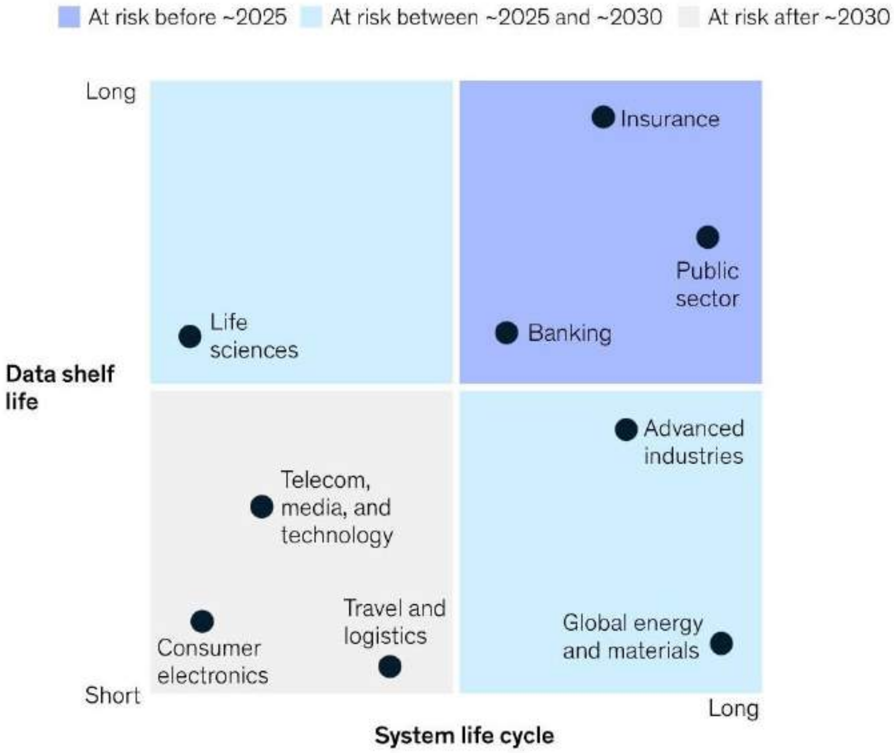


**Figure 2.** Risk of quantum-powered attack by industry. Source: McKinsey Digital [17].

After a rigorous evaluation process sieving through the initial submissions from the international crypto research community over a five-year period that included three "NIST PQC Standardization Conferences" [18] and countless deliberations on NIST's PQC forum, four finalists were selected by the NIST [19]. Early this year, *New Scientist* reported that a post-quantum encryption algorithm (Rainbow) verified and approved by the NIST could be easily cracked using a standard laptop [20]. More recently, using a single core of a regular Intel Xeon CPU (2013 release), researchers from the Security and Industrial Cryptography group (CSIS) at KU Leuven [21] were able to crack the second (named SIKE, short for Supersingular Isogeny Key Encapsulation) of the four encryption algorithms that the NIST considered as likely candidates to resist decryption by quantum computers [22]. SIKE was built by a consortium comprising Amazon, Infosec Global, Microsoft Research, Texas Instruments, and a number of international universities. The KU Leuven team won a USD 50,000 bounty for their breakthrough that startled the quantum world. With two of the four candidate PQC algorithms that reached the fourth round of the NIST validation process failing, the future of the remaining two candidates is, at best, shaky. Actual quantum computers do not exist yet, but the cryptography to defeat them is already here. If PQC can be cracked so easily, the future of cybersecurity indeed looks dreary.

## 3. Is the Quantum Threat Unassailable?

Historically, cryptography has been used to hide any sensitive information away from an intruder. Essentially, there are two ways to keep sensitive information secure from intrusion:

(i) Scrambling the information to make it undecipherable to the intruder;
(ii) Automatically making the information physically inaccessible to an unauthorized intruder.

The former is carried out using cryptography, and the latter by gating the physical access to the sensitive data. While cryptography has been the cornerstone of computer security since modern personal computers came into existence [23], gating access to computer resources is literally impossible, as legacy computers are designed to grant third-party permissions to all applications by default. Permissions introduce vulnerabilities, enhancing the need for the development of more complex encryption algorithms [24]. The vulnerabilities keep growing exponentially with the increase in connected devices [25]. This trend has shifted the security spotlight exclusively to cryptography, pushing the permissions issue to obscurity, so much so that almost all of today's computer security is cryptography-based. As computer security heavily relies on encryption, it remains vulnerable to impending threats from the enormous computing power of quantum computers of the future. It is time we revisit the much-ignored component of security, i.e., gating the physical access to the information.

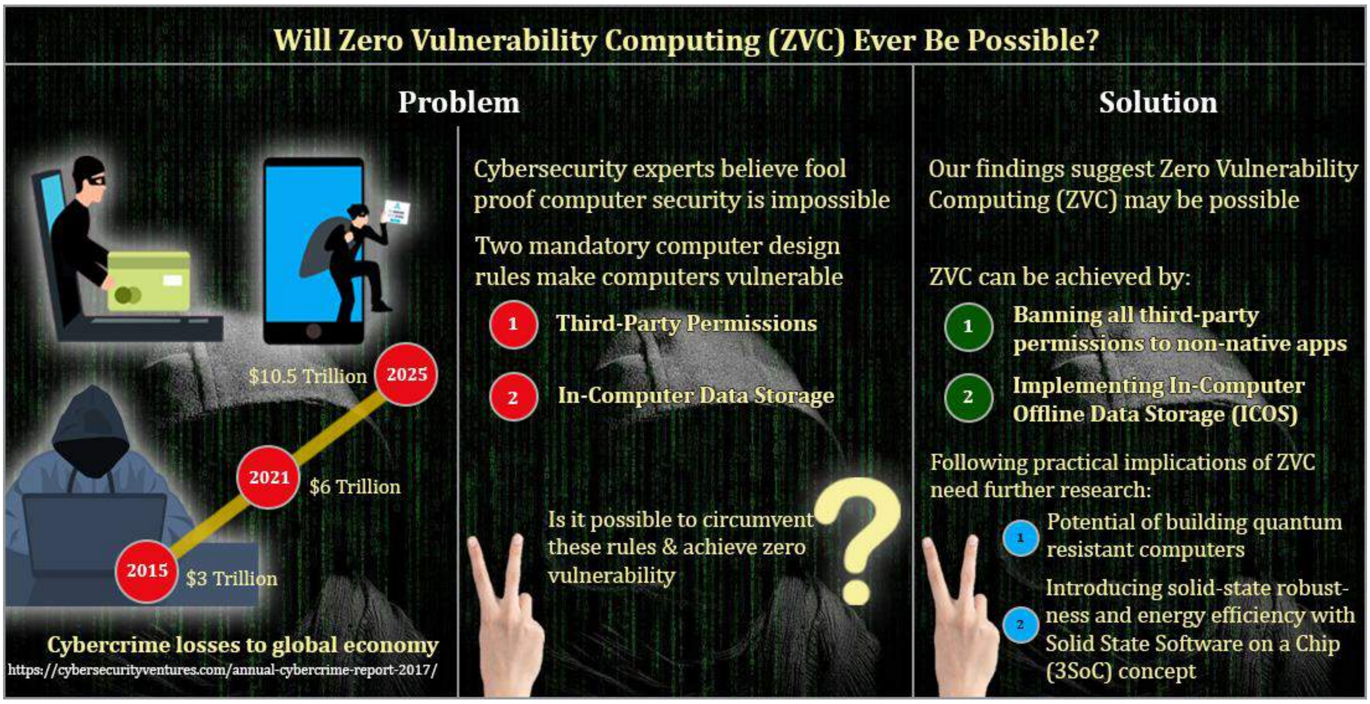
A recent report on zero-vulnerability computing (ZVC) offers some hope in that respect [14]. ZVC is a new encryption-agnostic cybersecurity paradigm supported by 30+ European partners in the European Commission's Horizon program [26]. The published ZVC experiments produced data that resulted in the formulation of the following hypotheses:

(1) As ZVC security is encryption-independent, will it be quantum-resistant by design?
(2) As the ZVC architecture lacks layering, rendering it conceptually analogous to the zero-moving-parts nature of solid-state electronics, will it deliver the same advantages to computers as the solid state did to revolutionize the electronics industry in the 1960s–1970s?

Although these new hypotheses are a subject of ongoing research pursued by a European consortium of experts constituted to test and prove them, it is possible and indeed pertinent to examine the technological rationale that supports these hypotheses. Such a de novo analysis will not only open a possible alternate approach for quantum proofing of future computers but will also pioneer a new era of solid-state software on a chip (3SoC) that introduces the integrity and robustness of solid-state electronics into software design [27]. With that intent, a deeper dive into the elements of ZVC is presented herein.

## 4. How Does ZVC Work?

Legacy computers, whether based on the von Neumann architecture [28] or the Harvard architecture [29], cannot become functional unless they grant permissions to third-party applications. These permissions create vulnerabilities. As legacy computers cannot be built without third-party permissions, they can never be free of vulnerabilities. Moreover, the mandatory online status of the stored data in a connected computer adds to the vulnerabilities (Figure 3). Hence, achieving zero vulnerability is an impossibility unless the established computer architecture is transformed into one that places limitations on permissions and imposes restrictions on the accessibility of the victim data stored in a connected device. ZVC imposes those restrictions to achieve zero vulnerability, as the following definition states [14]:



Will Zero Vulnerability Computing (ZVC) Ever Be Possible?

Problem

Cybersecurity experts believe fool proof computer security is impossible

Two mandatory computer design rules make computers vulnerable

1. Third-Party Permissions
2. In-Computer Data Storage

Is it possible to circumvent these rules & achieve zero vulnerability

Solution

Our findings suggest Zero Vulnerability Computing (ZVC) may be possible

ZVC can be achieved by:

1. Banning all third-party permissions to non-native apps
2. Implementing In-Computer Offline Data Storage (ICOS)

Following practical implications of ZVC need further research:

1. Potential of building quantum resistant computers
2. Introducing solid-state robustness and energy efficiency with Solid State Software on a Chip (3SoC) concept

Cybercrime losses to global economy

https://cybersecurityventures.com/annual-cybercrime-report-2017/

**Figure 3.** Zero vulnerability computing (ZVC): A graphical abstract. Data Source: Raheman et al. [22].

ZVC is a cybersecurity paradigm that proposes a new zero-attack surface computer architecture that restricts all third-party applications exclusively to a web interface only, declining permissions for any utilization of computing resources by any non-native program, and creates a switchable in-computer offline storage for securing sensitive data at the user's behest.

Understanding the definition of ZVC makes it pertinent to:

(i) Comprehend how ZVC achieves zero vulnerability without using adversary-facing encryption techniques. In the state of the art, encryption is the first and, in most cases, the only defense against intruding adversaries [30], rendering the cybersecurity of a legacy victim computer vulnerable to a quantum computer's ability to break the standard encryption algorithms;

(ii) Examine how ZVC's minimalist design can replicate, in software systems, the integrity, robustness, and energy efficiency of solid-state electronic hardware.

### *4.1. Encryption-Agnostic Security of ZVC*

In legacy computing systems, all hardware and software are designed to grant third-party permissions to vendors and developers who build a wide range of applications that make computers useful. Without these applications, computers hardly serve any purpose. In other words, it is impossible to build a computer without incorporating third-party permissions. Although it is permissions that allow computers to run a diverse range of applications, almost all computer vulnerabilities originate from these inherent permissions. These permissions are exploited by hackers who deploy attack vectors, creating an attack surface that cannot be eliminated entirely. Furthermore, a connected device cannot hold data offline, leaving it exposed to online threats. These computing rules render fool-proof cybersecurity practically impossible. These rules, although perfect for the pre-Internet era, have failed to stop cybercrimes, compelling experts to conclude that **fool-proof cybersecurity is impossible**. **ZVC** achieves zero vulnerability by (Figure 3):

1. *Banning all third-party permissions, thus completely obliterating the attack surface;*
2. *Creating switchable in-computer offline storage within the connected device itself.*

For any encrypted data to be vulnerable to a quantum computer (QC), they must be discoverable and exposed to a quantum cryptographic algorithm. From that perspective, all encrypted data under PKI (private–public-key infrastructure) fall into two categories:

(i) Device access authentication data;
(ii) Data stored on the device's memory.

In both scenarios, ZVC can protect the data from potential quantum attacks in the following ways:

(1) **Device access authentication data:** Quantum computers (QCs) can break today's encryption standards remotely, but that requires online accessibility to the victim resource and freedom of unlimited decryption attempts. ZVC's ICOS (in-computer offline storage) module automatically goes offline after three failed attempts, rendering the private data inaccessible to the QC algorithms.

(2) **Data stored on the device's memory:** Assuming a QC algorithm succeeds in overcoming the access authentication barrier, it will be able to access all the exposed and discoverable data. However, ZVC stores all private data on NAND memory hidden behind two security gates. To pass those gates, the remote QC must run its algorithms locally on the device in the same fashion as typical malware, i.e., it must be installed on the device, and execute its algorithm. ZVC bans all third-party permissions at the hardware level not only to run any non-native algorithm locally but also to find and recognize the data on the device targeted for breaching. A QC can run its access-breaching algorithm remotely to break the encrypted access credentials, but once the access is breached, the QC cannot transfer codes to run locally in the absence of third-party permissions. In other words, breaking the encryption for access authentication is of no avail, as no further local execution of any remote malicious code is possible for compromising the ZVC-secured data. ZVC secures the native data by setting up two gates that need to be passed before the data become accessible, as illustrated in Figure 4.

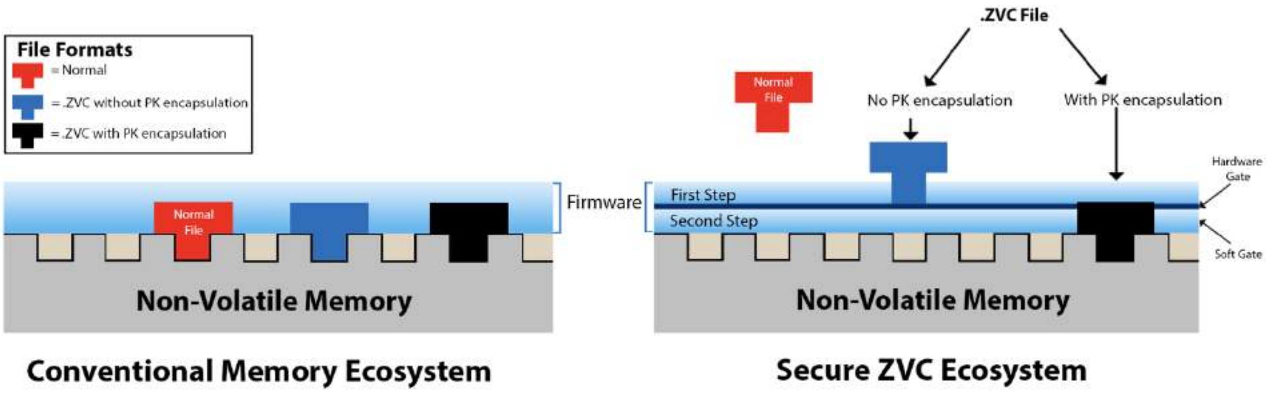


**Figure 4.** Hardware- and firmware-level exclusion of non-native data by ZVC to obliterate the attack surface.

The soft gate works at the firmware level, filtering all the data in two steps (Figure 4). The first step only allows the data files with **.ZVC** extension, and the second step checks for the private key before authorizing any storage rights to the data file. Now, any decryption algorithm, whether quantum or not, must run locally, as any malware must. However, this is not possible with ZVC, as the ZVC soft gate does not allow any malware, non-self-program, or non-native/non-ZVC code to run on the non-volatile memory. Any non-native data missed by the soft gate are stopped by the hardware gate. The hardware gate is basically a tiny controller that assigns memory registry addresses only to the authenticated **.ZVC** file format. All the non-ZVC non-native data are denied permission to access the memory.

### *4.2. Solid-State Software on a Chip (3SoC) and Potential Quantum Resistance*

The legacy computer architecture is layered and allows third-party permissions in all the layers, creating complexities and variabilities that construct a situation similar to the multiple moving parts of electronic devices of the pre-solid-state electronic era [14]. Thus, according to the 3SoC abstraction, the proposed ZVC ecosystem merges all the layered components in the legacy software by banning all third-party permissions, resulting in freedom from permission-related vulnerabilities. These constructs result in the zeroing of the attack surface and a situation analogous to the zero moving parts of solid-state electronics [22]. The 3SoC abstraction of the ZVC ecosystem renders it portable, robust, energy-efficient, and resilient.

A 3SoC consortium is currently pursuing the validation of the 3SoC hypothesis in a minimalist IoT device setting and extending the 3SoC design attributes to mainstream computers for implementing ZVC. This is carried out by providing a switchable 3SoC module on a NAND non-volatile flash memory chip that can be ported to any legacy computer's motherboard via one of its data ports, as illustrated in Figure 5.

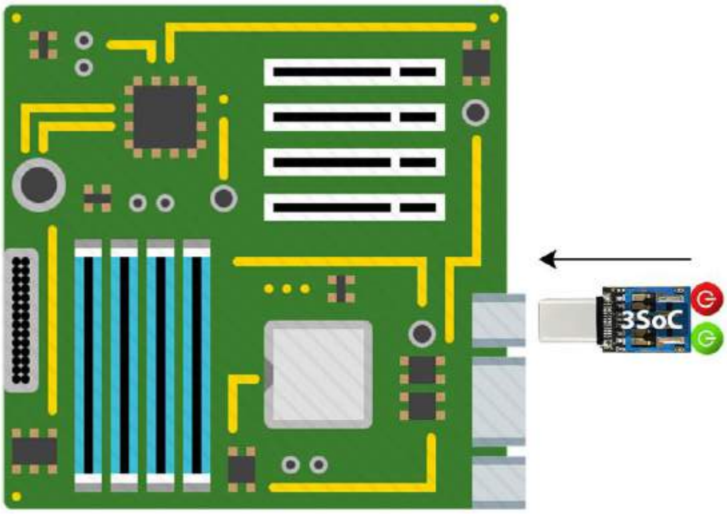


**Figure 5.** Integration of switchable 3SoC module with a computer motherboard.

The legacy computer motherboard illustrated in Figure 5 can be a laptop, a desktop, or a remote server, making it possible to engineer a 3SoC client computer and a 3SoC server for building a 3SoC network that operates as a fully secure malware-proof and quantum-resistant intranet, totally isolating all adversary client devices (Figure 6). Such a 3SoC network will be potentially impervious to malware because it bans all third-party permissions, and it will conceptually be quantum-resistant because its human–computer interface is encryption-agnostic. This is further explained in the next section.

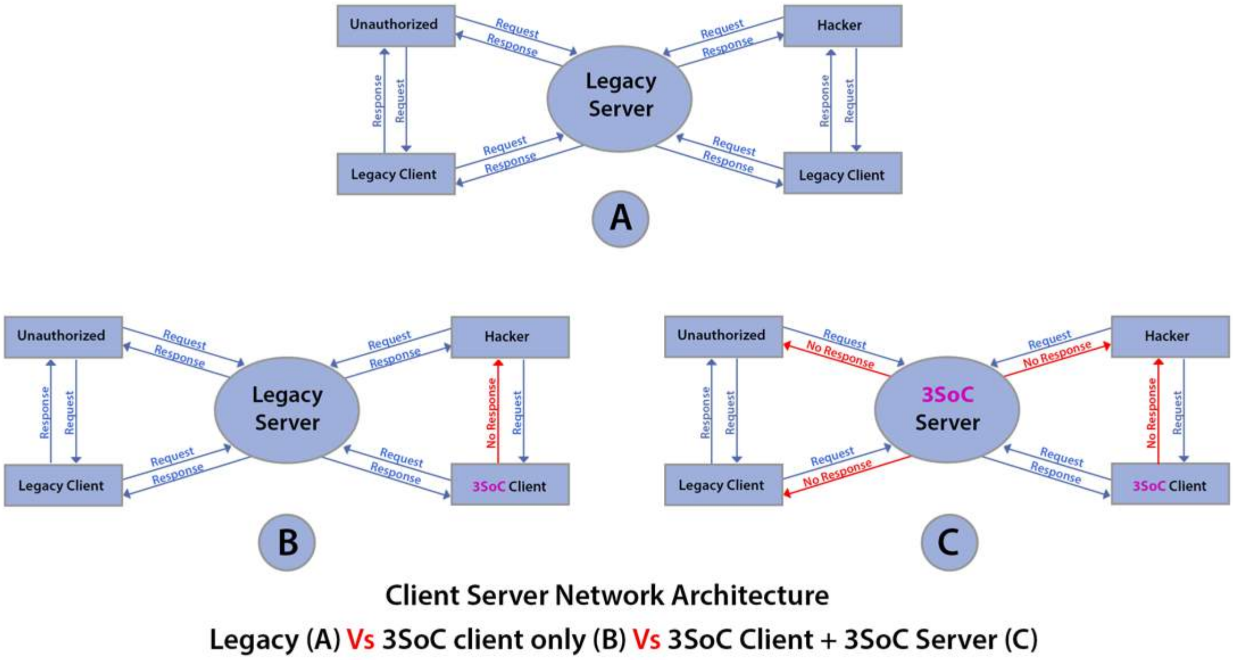


**Figure 6.** Three scenarios of client–server network architecture: (**A**) legacy, (**B**) 3SoC client only, and (**C**) 3SoC client + 3SoC server (intranet).

## 5. Quantum Supremacy and the Q-Day Threat

There is a race among companies to achieve supremacy in quantum technology because it will drastically reduce computing time from years to hours or even minutes. The power of quantum computing will be a boon for data-intensive industries such as pharmaceuticals, artificial intelligence, industrial design, logistics, and national security [31]. However, it raises serious threats to the cybersecurity of classical computing devices. Theoretically, all cryptography algorithms are vulnerable to quantum attacks. Q-Day is when quantum computers will break the Internet [4]. Given the ubiquity of cryptographic schemes in our everyday online activities, this could be catastrophic. Computer scientists are predicting how quantum computers can cause havoc with encryption, resulting in a global catastrophe [32].

With Google's declaration of quantum supremacy in 2019, claiming that they solved a problem in three minutes that would take a classical computer over a thousand years, quantum computing is no longer a hypothetical idea [33]. Nevertheless, the millions of qubits of computing power required to break modern cryptography remains a challenging goal. Practical quantum computers with millions of qubit capacity will be able to break nearly all modern public-key cryptographic systems. Before quantum computers arrive with sufficient qubits, we must be ready with quantum-safe cryptographic algorithms, tools, techniques, and deployment strategies to protect the classical ICT infrastructure.

### *5.1. Potential Quantum Computing Business Model*

It is estimated that breaking the classical encryption will require 317 million qubits [34]. Today, each qubit costs around USD 10,000 a piece [35]. Even if the qubit price comes down a hundredfold, an encryption-breaking quantum computer will cost hundreds of millions apiece. Due to the very high costs and the race to protect trade secrets, the expected business model for quantum computing is likely to resemble the current model for cloud-based computing dominated by Amazon/AWS (33%) [36]. This essentially means that, unlike a standard computer that almost anyone can own, ordinary citizens or, for that matter, hackers cannot afford a quantum computer. They will have to rely on the quantum computing service providers (QCSPs) for leasing quantum computing resources to design and execute their quantum malware to launch a quantum attack on any victim computing device remotely. The astronomical cost of quantum computers rules out the possibility of an encryption-breaking personal desktop version anytime in the future and, in fact, comes as a blessing in disguise. The QCSP business model makes the job of standard-regulating authorities such as the NIST in the US and ENISA, its equivalent in Europe, a lot easier. Building standards to regulate cloud service providers is much easier than regulating a desktop hacker. These standardizing and policy-making agencies are currently focusing exclusively on PQC (post-quantum cryptography) to withstand the decryption capabilities of powerful quantum computers. Although we have seen over 90% of the candidate PQC algorithms that the NIST reviewed over the past 5 years fail [20,21], even if none of the candidate PQC algorithms succeed, these agencies can draft technical standards for operating QCSPs and let government regulatory agencies implement those standards as rules for availing quantum computing services. However, in the given circumstances, it is worth looking beyond PQC for safeguarding classical computers from future quantum hackers.

### *5.2. Securing Quantum Computing Service Provider (QCSP) Network*

As illustrated in Figure 7, a typical QCSP provides its cloud-based quantum computing services to its subscribers in a business model that is quite similar to any cloud computing service provider of today. As a term of service, the subscribers are provided with a 3SoC client for accessing the quantum computing services of the QCSP. The QCSP routes access to the quantum computer through a 3SoC server that only accepts authentication requests from a 3SoC client device. All other requests from non-subscribers or hackers with legacy computing devices are declined. Thus, a 3SoC intranet can potentially offer defense against misuse of quantum computing by bad actors even if the PQC algorithms fail to deliver the promise.

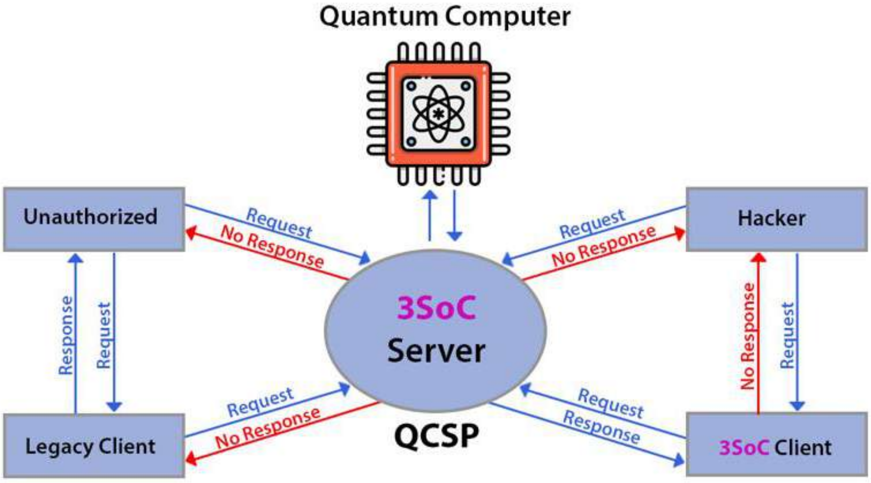


**Figure 7.** Quantum computer service provider (QCSP) providing quantum computing via 3SoC Intranet to subscribers.

## 6. Limitations and Caveats

This paper provides theoretical support to two new hypotheses that are currently under investigation. These hypotheses have far-reaching implications for our understanding of solid-state electronics and computer hardware/software, in general, and for enhancing their security and resilience in building a robust Internet, in particular. As any hypothesis-generating research demands, great care is warranted in projecting the conclusions of this report to real-world scenarios for the following reasons:

(i) These hypotheses are formulated based on empirical data from a limited-use hardware wallet experiment [14] and need to be validated in diverse mainstream computing environments before any extrapolation to more complex computing environments;

(ii) The ZVC/3SoC research is ongoing, and the inferences drawn from the available data are preliminary and subject to updates as and when available;

(iii) Currently, cloud services seem to be the only way quantum computing can become available to end users in the near future;

(iv) Notably, 3SoC devices inherently restrict the porting of generic or non-conforming third-party peripheral devices [27];

(v) Rigorous experimentation by peer researchers is warranted for testing and proving or disproving the ZVC/3SoC hypotheses and replicating the conclusions;

(vi) Appropriate key performance indicators (KPIs) should be framed to justify the quantity and quality of the case studies designed to investigate the formulated hypotheses.

Despite its limitations, this study adds compelling evidence that quantum-safe security of computing devices is theoretically possible by using an encryption-agnostic approach to securing computing devices. ZVC is a novel encryption-agnostic method of securing future computers that can potentially render computers quantum-resistant. ZVC's 3SoC abstraction also supports the feasibility of de-layering the legacy computer architecture for enhancing and replicating the robustness, energy efficiency, portability, and resilience of solid-state devices.

## 7. Conclusions and Future Prospects

Quantum computing (QC) is a nascent and rapidly growing field [37]. QC can potentially crack RSA and ECC algorithms, impacting almost 100% of encrypted Internet traffic. Businesses around the world are pouring in resources to further QC knowledge and practices. McKinsey predicts that the first-wave industries may start to significantly benefit from QC as early as 2025 [37]. As of now, quantum algorithms already exist for all major public-key cryptosystems, and it is only a matter of time before they are completely broken. There is an urgent need to counter the looming QC threat.

Without the NIST PQC selection process, the candidate PQC algorithms could have raised very little attention and security scrutiny by cryptographers and mathematicians and would likely have ended up being used by the industry as proprietary encryption methods. It is of serious concern that many of the algorithms that have been cracked during the NIST tests are still in commercial use. For example, Rainbow is deployed by the ABCmint cryptocurrency [38], and SIKE is implemented by the AWS Key Management Service, Cloudflare, and Google [39]. The fact that so many post-quantum encryption methods have been cracked and none has stood the rigors of NIST testing reveals that it is time to explore alternate cybersecurity strategies.

As the preferred business model that the quantum computing industry is moving towards is unquestionably QaaS, the possibility of the individual ownership of astronomically priced quantum computers by bad actors is virtually ruled out. This implies that the only way that an adversary can exploit quantum computing for malicious attacks on victims is through a subscription to a QaaS provider. Hence, the impending quantum threats to the Internet can be best dealt with by segregating all subscription-based quantum computing activities from the mainstream Internet by regulating the QaaS access, rather than attempting to protect each Internet-connected device individually from quantum attacks. The 3SoC consortium is currently exploring such quantum sequestering possibilities to secure the Internet from the feared perils of quantum computers.

Although the ZVC-powered 3SoC network architecture is still under development as a potentially robust cyber-secure framework, its early dissemination among the cybersecurity research community will accelerate the process of its validation and standardization as an alternative to the existing vulnerability-prone legacy computing infrastructure that feeds a multi-trillion cybercrime industry. It will also open new possibilities to counter the recent PQC failures in preparing for an impending quantum threat. This paper will serve its purpose if it spurs enough interest amongst cybersecurity researchers and cryptographers in the critical evaluation of the encryption agnosticism of ZVC/3SoC by testing and proving or disproving its quantum-safe hypothesis.

**Funding:** This research received no external funding.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** The author is grateful to Tejas Bhagat and Sadiya Khan for their assistance in preparing this manuscript.

**Conflicts of Interest:** The author declares no conflict of interest.

## References

1. Preskill, J. Quantum computing 40 years later. *arXiv* **2021**, arXiv:2106.10522.
2. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Martinis, J.M. Quantum supremacy using a programmable superconducting processor. *Nature* **2019**, *574*, 505–510. [CrossRef] [PubMed]
3. Bova, F.; Goldfarb, A.; Melko, R.G. Commercial applications of quantum computing. *EPJ Quantum Technol.* **2021**, *8*, 2. [CrossRef] [PubMed]
4. Castelvecchi, D. The race to save the Internet from quantum hackers. *Nature* **2022**, *602*, 198–201. [CrossRef] [PubMed]
5. Steve, M. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. *Cybercrime Magazine*. 13 November 2020. Available online: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021 (accessed on 8 August 2022).
6. Cornea, A.A.; Obretin, A.M. *Security Concerns Regarding Software Development Migrations in Quantum Computing Context*; Department of Informatics and Economic Cybernetics, Bucharest University of Economic Studies: Bucharest, Romania, 2002; Volume 5, pp. 12–17, ISSN 2619-9955. [CrossRef]
7. Rozell, D.J. Cash is king. *Nature* **2022**, *16*, 2022. [CrossRef] [PubMed]
8. De Wolf, R. The potential impact of quantum computers on society. *Ethics Inf. Technol.* **2017**, *19*, 271. [CrossRef]
9. Grimes, R.A. *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto*; John Wiley & Sons: Hoboken, NJ, USA, 2019.
10. Schiffer, B.F. Quantum computers as an amplifier for existential risk. *arXiv* **2022**, arXiv:2205.02761.
11. Casati, N.M. Use of Quantum Computers in Understanding Cultures and Global Business Successes. In *Culture in Global Businesses*; Palgrave Macmillan: Cham, Switzerland, 2021; pp. 77–103.
12. Scott, F., III. A Buyer's Guide to Quantum as a Service: Qubits for Hire. Available online: https://www.zdnet.com/article/a-buyers-guide-to-quantum-as-a-service-qubits-for-hire/ (accessed on 21 May 2021).
13. Sharma, S.K.; Khaliq, M. The role of quantum computing in software forensics and digital evidence: Issues and challenges. *Limit. Future Appl. Quantum Cryptogr.* **2021**, 169–185.
14. Raheman, F.; Bhagat, T.; Vermeulen, B.; Van Daele, P. Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. *Future Internet* **2022**, *14*, 238. [CrossRef]
15. Alagic, G.; Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Smith-Tone, D. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*; US Department of Commerce, National Institute of Standards and Technology: Washington, DC, USA, 2019. Available online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303 (accessed on 8 August 2022).
16. Hoschek, M. Quantum security and 6G critical infrastructure. *Serb. J. Eng. Manag.* **2021**, *6*, 1–8. [CrossRef]
17. Lennart, B.; Benjamin, K.; Niko, M.; Anika, P.; Henning, S. When—And How—To Prepare for Post-Quantum Cryptography. *McKinsey Digital*. 4 May 2022. Available online: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography (accessed on 8 August 2022).
18. Computer Security Research Center. Post Quantum Cryptography PQC: Workshops and Timeline. NIST; 7 July 2022. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline (accessed on 8 August 2022).
19. Edlyn, T. The NIST Announcement on Quantum-Resistant Cryptography Standards is Out. Act Now! *Cryptomathic*. 6 July 2022. Available online: https://www.cryptomathic.com/news-events/blog/the-nist-announcement-on-quantum-resistant-cryptography-standards-is-out.-act-now (accessed on 8 August 2022).
20. Mathew, S. Encryption Meant to Protect Against Quantum Hackers is Easily Cracked. *New Scientist*. 8 March 2022. Available online: https://www.newscientist.com/article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked/ (accessed on 28 May 2022).
21. Castryck, W.; Thomas., D. An efficient key recovery attack on SIDH (preliminary version). *Cryptol. Eprint Arch.* **2022**. Available online: https://eprint.iacr.org/2022/975 (accessed on 8 August 2022).
22. Laura, D. Post-Quantum Crypto Cracked in an Hour with One Core of an Ancient Xeon. *The Register*. 3 August 2022. Available online: https://www.theregister.com/2022/08/03/nist_quantum_resistant_crypto_cracked/ (accessed on 8 August 2022).
23. Xue, W.; Wang, C.; Wang, J. Research on Cryptography as a Service Technique Based on Commercial Cryptography. In Proceedings of the 2022 IEEE 2nd International Conference on Electronic Technology, Communication and Information (ICETCI), Changchun, China, 27–29 May 2022; pp. 260–264. [CrossRef]

24. Scala, N.M.; Reilly, A.C.; Goethals, P.L.; Cukier, M. Risk and the five hard problems of cybersecurity. *Risk Anal.* **2019**, *39*, 2119–2126. [CrossRef] [PubMed]
25. Davis, G. 2020: Life with 50 billion connected devices. In Proceedings of the 2018 IEEE International Conference on Innovative Research and Development (ICCE), Las Vegas, NV, USA, 12–15 January 2018; p. 1.
26. DrFazal. Why Computers Are Inherently Vulnerable? *Medium*. 3 August 2022. Available online: https://drfazal.medium.com/why-computers-are-inherently-vulnerable-fd7a34afaec6 (accessed on 8 August 2022).
27. Raheman, F. Solid State Software On A Chip (3SOC) For Building Quantum Resistant Web 3.0 Computing Devices. U.S. Patent US29/842,535, 15 June 2022.
28. Arikpo, I.I.; Ogban, F.U.; Eteng, I.E. Von Neumann architecture and modern computers. *Glob. J. Math. Sci.* **2007**, *6*, 97–103. [CrossRef]
29. Francillon, A.; Castelluccia, C. Code injection attacks on Harvard-architecture devices. In Proceedings of the 15th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 27–31 October 2008.
30. Moon, Y.H.; Kim, J.H.; Kim, D.S.; Kim, H.K. Hybrid Attack Path Enumeration System Based on Reputation Scores. In Proceedings of the 2016 IEEE International Conference on Computer and Information Technology (CIT), Nadi, Fiji, 8–10 December 2016; pp. 241–248. [CrossRef]
31. Hassija, V.; Chamola, V.; Saxena, V.; Chanana, V.; Parashari, P.; Mumtaz, S.; Guizani, M. Present landscape of quantum computing. *IET Quantum Commun.* **2020**, *1*, 42–48. [CrossRef]
32. Majot, A.; Yampolskiy, R. Global catastrophic risk and security implications of quantum computers. *Futures* **2015**, *72*, 17–26. [CrossRef]
33. Elizabeth, G. Hello Quantum World! Google Publishes Landmark Quantum Supremacy Claim—The Company Says That Its Quantum Computer Is the First to Perform a Calculation That Would Be Practically Impossible for a Classical Machine. *Nature* **2019**, *574*, 461–463.
34. Webber, M.; Elfving, V.; Weidt, S.; Hensinger, W.K. The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime. *AVS Quantum Sci.* **2022**, *4*, 013801. [CrossRef]
35. Chauhan, V.; Negi, S.; Jain, D.; Singh, P.; Sagar, A.K.; Sharma, A.K. Quantum Computers: A Review on How Quantum Computing Can Boom AI. In Proceedings of the 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 28–29 April 2022.
36. Aboy, M.; Timo, M.; Mauritz, K. Mapping the Patent Landscape of Quantum Technologies: Patenting Trends, Innovation and Policy Implications. *IIC-Int. Rev. Intellect. Prop. Compet. Law* **2022**, *53*, 853–882. [CrossRef]
37. Ménard, A.; Ostojic, I.; Patel, M.; Volz, D. A game plan for quantum computing. *McKinsey Q.* **2020**, 7–9. Available online: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing (accessed on 8 August 2022).
38. Ding, J.A. New Proof of Work for Blockchain Based on Random Multivariate Quadratic Equations. In *Applied Cryptography and Network Security Workshops*; Zhou, J., Deng, R., Li, Z., Majumdar, S., Meng, W., Wang, L., Zhang, K., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 97–107.
39. Schwabe, P.; Douglas, S.; Thom, W. Post-quantum TLS without handshake signatures. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, 9–13 November 2020.