Scientific Research Publishing

Journal of Computer and Communications, 2024, 12, 59-77
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Futureproofing Blockchain & Cryptocurrencies against Growing Vulnerabilities & Q-Day Threat with Quantum-Safe Ledger Technology (QLT)

Fazal Raheman

Quantsoft Systems Ltd., Tallinn, Estonia
Email: drfazal@bc5.eu

How to cite this paper: Raheman, F. (2024) Futureproofing Blockchain & Cryptocurrencies against Growing Vulnerabilities & Q-Day Threat with Quantum-Safe Ledger Technology (QLT). *Journal of Computer and Communications*, **12**, 59-77.
https://doi.org/10.4236/jcc.2024.127005

Received: June 25, 2024
Accepted: July 23, 2024
Published: July 26, 2024

Abstract

With one billion users using 380 exchanges, the security of blockchains and cryptocurrencies remains a major concern as billions are lost to hackers every year. Cryptocurrency hacks negatively impact cryptocurrency markets introducing volatility. Each major scam/hack incident results in a significant price dip for most cryptocurrencies, decelerating the growth of the blockchain economy. Existing blockchain vulnerabilities are further amplified by the impending existential threat from quantum computers. While there's no reprieve yet from the scam/hack prone blockchain economy, quantum resilience is being aggressively pursued by post quantum cryptography (PQC) researchers, despite 80 of 82 candidate PQCs failing. As PQC has no role in combating inherent vulnerabilities, securing over 1000 existing blockchains against scammers/hackers remains a top priority for this industry. This research proposes a novel Quantum-safe Ledger Technology (QLT) framework that not only secures DLTs/cryptocurrencies and exchanges from current vulnerabilities but protects them from the impending Q-day threats from future quantum computers. As blockchain-agnostic technology, the QLT framework can be easily adapted to secure any blockchain or crypto exchange.

Keywords

Cybersecurity, Quantum Computers, Post Quantum Cryptography, Q-Day, Zero Trust

1. Introduction

The Digital Ledger Technology (DLT)/blockchain was first introduced in 2008 by Satoshi Nakamoto as a peer-to-peer electronic cash system or cryptocurrency called Bitcoin [1]. Blockchain and cryptocurrency are inseparably linked. As much as a decentralized form of money simply cannot exist without the security provided by blockchain, a public blockchain cannot be created without incentivizing people to create it [2]. Cryptocurrency is that incentive. Hence, cryptocurrency is a digital currency that is decentralized, and it is stored and tracked through the blockchain. The introduction of smart contracts in blockchain [3] and its commercial launch as Ethereum blockchain in 2015 [4] further revolutionized blockchain technology. It has since drawn broad attention from academia and industry alike. A growing body of literature envisions how its decentralized approach can be pervasive in disrupting current business models, financial systems, organizations, and civic governance [5]. As much as we don't realize, decentralization is innate, divined, sustainable, and omnipresent in nature. While centralization is acquired, humanly, and perhaps less sustainable (To centralize is human, to decentralize divine [6]).

The latest statistics indicate that one billion people worldwide have used 380 crypto exchanges to buy/sell cryptocurrencies, and over 300 million people own one or more of the 20,000 cryptocurrencies out there [7]. There are over 1000 blockchains and 245 NFT marketplaces in the world [8]. In November 2021, the cryptocurrency market cap reached an all-time high of $3 trillion and achieved it faster than any other industry in history in just about a dozen years. Projected to be a $3 trillion industry [9], blockchain exclusively relies on adversary-facing cryptography.

Blockchain is a sequence of blocks joined by cryptographic hashes, typically shared by many peers in the network. If the hash of the final block is known, the history of the chain is immutable. In the state-of-the-art, it is computationally impossible to change previous blocks in such a way that the final hash stays the same. The present public-key infrastructure (PKI) that blockchain deploys depends on the difficulty of deciphering the discrete log and factorization problem of large prime numbers. The RSA (Rivest-Shamir-Adleman) algorithm is the basis of a PKI cryptosystem widely used to secure sensitive data, particularly when it is being sent over an insecure network. Most blockchains follow a similar method to the RSA algorithm for creating and encrypting blockchain wallets. Creating a cryptocurrency wallet generates a public address and a private key. It is suggested that Shor's quantum algorithm can solve the integer factorization problem in polynomial time and break the state-of-the-art PKI [10]. The exponential growth in quantum computing is opening up the possibility of performing attacks based on Shor's algorithms and Grover's algorithms, threatening the PKI and hash functions in the near future [11]. Therefore, it has become necessary for the development of a post-quantum secure signature scheme or quantum-resistant blockchain for post-quantum blockchain security.

1.1. Research Purpose and Related Works

The principal objective of this research is to explore the feasibility of extending the findings of recently published work on Zero Vulnerability Computing (ZVC), an encryption-agnostic cybersecurity framework that completely obliterated the attack surface on a client hardware wallet device [12]. Beyond the minimalist hardware wallet client device, the ZVC essentially merged all the conventional layers of firmware, drivers, operating system, and application layer to deliver a compact Solid-State Software on a Chip (3SoC) system that was completely secure with zero attack surface, was autonomous, robust and energy efficient [13]-[18] as an alternative to PQC candidate algorithms that entered NIST's PQC standardization process initiated in 2017 [19]. Almost seven years into the standardization process, all of the shortlisted candidate PQCs have failed [19]-[21], which warrants an urgent need to explore alternate strategies. ZVC's novel encryption agnostic 3SoC client-server framework was proposed as an Intranet solution to segregate quantum computers from the mainstream Internet to deliver quantum computing service in a Quantum-as-a-Service (QaaS) business model [13]-[17]. This paper explores a strategy similar to the proposed QaaS architecture [13]-[17] to secure blockchain/cryptocurrency infrastructures to deliver a Quantum-safe Ledger Technology (QLT). To place the development of the QLT concept in proper perspective, a discussion on state-of-the-art design is presented in Section 4. Section 5 presents details of the universal design of the QLT framework architecture in conventional as well as quantum computing scenarios. Section 6 discusses the limitations of this study, and Section 7 presents the conclusion and future of the QLT approach.

1.2. Problem Statement

Hailed as a panacea for economic growth and sustainability [22], blockchain's envisioned omnipresence in human-computer interactions so far lags [23]. Besides other challenges to blockchain's commercial viability, its vulnerability to frequent hack attacks and future threats from quantum computers is a bit stifling. There is consensus amongst cybersecurity experts that total cybersecurity is impossible to achieve [24], and blockchain is no exception. No wonder it has been the target of perpetual scams and hacks, resulting in billions of dollars lost every year. Blockchains also face smart contract vulnerabilities besides the inherent vulnerabilities in any computing system.

2. Perpetual Scams & Hack Attacks on Cryptocurrencies

Since the launch of Bitcoin as a cryptocurrency, the blockchain/cryptocurrency industry has been blemished with countless crypto scams and hacks over the years, estimated to be as high as $88 billion [25] and counting. Notwithstanding the advent of quantum computers, cryptocurrency exchanges remain vulnerable to hack attacks even today. In early 2022, CNBC reported 2021 as a record-breaking year of crypto scams totaling a whopping $14 billion [26] [27]. The year 2022 turned out to be the worst year for crypto thieves, with the biggest loss of $3 billion reported in October 2022 by Money Control [28], followed by the two biggest exchanges, Binance [29] and FTX [30], reporting $570 and $600 million respectively lost to hack attacks totaling $1.17 billion in losses in just a single month. Another billion dollars was reported lost to hacking attacks by Chainalysis in August 2022 [31]. Cryptocurrency hacking incidents affect the cryptocurrency market by introducing volatility, which increases significantly both contemporaneously and in a delayed effect [32]. Each major hack results in a significant price dip for Bitcoin and all major cryptocurrencies [33]. Frequent hacking incidents are detrimental to the growth of the blockchain economy [34]. Securing blockchain against hackers remains the top priority for this potentially multi-trillion industry [35].

The challenge is further amplified by the advent of quantum computers, which are feared to present an existential threat to encryption-dependent Internet protocols and blockchain networks [36]. Several research groups are exploring PQC for developing quantum-resistant blockchains [37]. The problem is so serious that even questions about the impending end of blockchain are raised [38].

Several research reports emphasize the seriousness of the impending threats from quantum computers to the Internet [38] and an actual quantum attack on several cryptocurrencies that led to the latest crypto crash of 2022 [39]. In theory, all cryptographic algorithms are vulnerable to quantum attacks. This could be catastrophic as cryptography is omnipresent in today's networked lifestyle [40]. Already overwhelmed with the ever-increasing scourge of hack attacks, blockchain appears to be moving closer to the cryptography apocalypse threat from quantum computers [41]. Q-day is when quantum computers will break the Internet [42]. Quantum computers with cryptographically significant qubits are predicted to start premiering as early as 2025 [42]. Quantum algorithms already exist for all major public-key cryptosystems, necessitating an urgency in responding to the imminent Q-Day threat. QChain was one of the first PQC (post quantum cryptography) blockchain initiatives initiated in 2018 [43]. The process of standardization of PQC initiated by NIST (National Institute of Standards and Technology) in 2017 resulted in 80 failed PQC algorithms in the first round itself in 2022 [19]. Subsequently, the remaining two PQCs were also breached by a Swedish and a French team of cryptographers [20] [21], placing the PQC standardization process in serious jeopardy. However, many of these failed PQCs remain in commercial use today. Rainbow is an example of PQC deployed by the ABCmint cryptocurrency [44]. Dey *et al.* recently reported that Bitcoin, Ethereum, Corda, etc., launched quantum-safe PQC initiatives [45] [38]. Moreover, encryption algorithms, in general, are neither resource-efficient nor cost-effective because of the high cost of encryption and decryption of data [46]. A recent report estimates the current cost of quantum cryptography for connecting two computers at a whopping $50,000 [40] [47]. Notwithstanding the cost and failing state of PQCs, most IoT devices with limited computing resources will be unable to support the computational implementation of PQC algorithms. Implementing

PQC on billions of IoT devices is a techno-economic futility that PQC advocates often ignore. These circumstances warrant an urgent need to explore alternate cybersecurity strategies to secure blockchains from the peril of quantum computers.

3. Literature Review

3.1. The State-of-the-Art Literature Review

Our problem statement identifies three categories of cybersecurity breaches that are possible in legacy DLT/blockchain systems.

1) The first category pertains to the inherent vulnerabilities originating from the mandatory third-party permissions that all hardware and software are designed to grant third-party vendors and developers of computer applications [12].

2) The second category is an upshot of the impending threats from future quantum computers [13]-[18].

3) The third category is smart contract vulnerabilities [48]. Because smart contracts are stored on-chain and publicly accessible, hackers can examine the public codebase for vulnerabilities due to code weakness or bugginess of the code. Such code vulnerabilities can then be misappropriated for conducting their attacks. While a bad smart contract code has no recourse other than writing robust code, this paper proposes a new paradigm for tackling each of those vulnerabilities to render blockchain/cryptocurrencies virtually hackproof. A review of the state-of-the-art is warranted to place the proposed solution in proper perspective.

3.1.1. Crypto Exchange Vulnerabilities

In contrast to classical stock exchanges, which facilitate trading but do not actually hold securities on behalf of clients, centralized cryptocurrency exchanges store virtual currencies for their clients. This makes cryptocurrency exchanges vulnerable. Compared to centralized exchanges, decentralized exchanges were presumed to be more secure because the exchange never retains the custody of the customer assets. Traditionally, centralized cryptocurrency exchanges were more vulnerable to cyber-attacks than decentralized exchanges because the users involved in the exchange had to fully trust the service provider who held the custody of the user assets [49]. On the contrary, in decentralized exchange, the user assets remain in the custody of the user [50]. Hence, theoretically, decentralized exchanges evolved into more secure platforms than centralized ones. However, with the advent of cross-chain bridges, most cross-chain schemes were found to be vulnerable to malicious Internet-based attacks, *i.e.*, man-in-the-middle (MITM) attacks, replay attacks, denial of service (DoS) attacks, and counterfeiting attacks [51]. This was essentially because these cross-chain protocols were custodial schemes taking interim custody of the user asset during the process of transferring the asset from one chain to another [52]. This made the bridge custodian become the target [31], rendering the bridging function in decentralized exchanges vulnerable [53].

For all the above reasons, cryptocurrency exchanges, whether centralized or decentralized with cross-chain bridging, remain vulnerable to hack attacks. In fact, more vulnerable now than ever. In October 2022, CBS News reported $3 billion stolen from several exchanges [54], shattering the previous record of $2.1 billion set in 2021. The last quarter of 2022 saw the two biggest exchanges, Binance [19] and FTX [20], reported $570 and $600 million, respectively, lost to hack attacks. Besides the usual cybersecurity breaches resulting from the inherent attack surface present on all legacy computing devices that centralized exchanges deploy, the top security risk appears to have shifted to cross-chain bridge protocols deployed in decentralized exchanges [19]. While the FTX hack happened as a cybersecurity breach of the custodial assets in a centralized exchange, the Binance hack was a cross-chain exploit.

3.1.2. Post-Quantum Blockchain Vulnerabilities

Post Quantum Cryptography (PQC) encompasses a new generation of algorithms for the creation of asymmetric keys that are believed to be resistant to attacks by quantum computers [55]. Cryptocurrencies [56] and blockchain transactions rely on distributed ledgers and require solutions that guarantee quantum resistance to preserve the integrity of data and assets in their public and immutable ledgers [36].

Many reports on quantum-safe blockchains have appeared in peer-reviewed literature [11]. Marcos *et al.* [57] deployed PQC as a layer 2 solution to make blockchain quantum resistant. Zhu *et al.* [58] recently proposed a hybrid encryption scheme for quantum secure video conferencing combined with blockchain. However, with all the 82 PQC candidates [19]-[21] failing NIST's standardization process, quantum computers appear to be more detrimental to human interests than the benefits they deliver [59]. In fact, one of the recent cryptocurrency crashes was caused by an actual quantum attack on several cryptocurrencies [27]. Moreover, PQC algorithms are computationally expensive [60] [61] and will add to the already high cost and slow speed of blockchain transactions. A typical Ethereum blockchain transaction costs already very high, clocking as high as 360 times that of a conventional database [62] [63]. Attempts at making blockchain resilient with PQC primitives will further escalate the already exorbitant blockchain transaction costs and hamper blockchain scalability [62] [63].

3.1.3. Smart Contract Security Flaws

As indicated earlier, smart contracts are computer programs that are also prone to programming errors. Code faults are a common cause of flaws in smart contracts. Di Angelo and Salzer identified at least 18 areas of weakness in smart contract coding that may result in vulnerabilities [64]. They evaluated 27 smart contract audit tools that can be deployed to identify and fix these vulnerabilities. Solidity is the most common Turing complete programming language in use to write smart contracts. Deploying less complicated non-Turing complete programming languages reduces the errors in smart contract codes, increasing potential security compared to complicated Turing-complete implementations. Vyper is a Python-like, non-Turing complete scripting language that can be used to write secure and maximally human-readable smart contacts to minimize the security flaws in the code [65] [66].

3.2. Beyond State-of-the-Art

All state-of-the-art computing systems, whether based on the von Neumann architecture [67] or the Harvard architecture [68], are designed to grant 3rd party permissions to the software applications developed by programmers and software vendors [12]-[18]. It is a mandate that can never be circumvented without making the computers useless. These permissions are also the targets that bad actors manipulate to create attack vectors for gaining unauthorized access to a network or a computer system to extract data. It is for this reason a legacy computer or network will always bear an attack surface that keeps growing and can never be eliminated [69]. A major paradigm shift in computing was recently developed and tested that not only obliterated the 3rd party permissions entirely but reduced the attack surface to zero [12]-[18]. Such a system of zero vulnerability computing (ZVC) did not rely on cryptography to secure the computers. Because ZVC was encryption agnostic, the following hypotheses were formulated:

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?

Defined as follows ZVC is a new encryption-agnostic cybersecurity paradigm that won a Seal of Excellence from the European Union's Horizon Europe program [70].

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 [70].

While several European Consortia continue to investigate ZVC in diverse use case scenarios, several recent reports explored the ZVC hypotheses for quantum resilient cybersecurity of the Internet [12]-[16]. As the full scope and relevance of ZVC to the overall cybersecurity of the Internet remains a subject of ongoing research, it is advantageous to continue exploring new fields of application. One such area of very high unmet need is the future security of blockchain and cryptocurrency infrastructures when quantum computers achieve the encryption-breaking computing advantage over legacy computing systems. A de novo analysis will open a possible new approach for securing cryptocurrencies from the menace of frequent hack attacks and futureproofing the blockchain against the impending threats from quantum computers.

In state-of-the-art, the following rationale is applied to protecting the Internet from the impending quantum threats to legacy computers:

- Protect each Internet-connected legacy computer individually from quantum attacks with state-of-the-art PQC.

The following paradigm shift was recently proposed for securing the Internet from the perils of quantum computing: Segregate all quantum computing activities from mainstream Internet with encryption-agnostic ZVC in a Quantum-as-a-Service (QaaS) business model that insulates the service from the rest of the Internet [12]-[16].

But how do we know that the goal of quantum advantage is achieved? A definition of "Quantum Advantage" that will help in defining a minimum viable product (MVP) that provides the quantum advantage over classical computers is provided herein [25].

3.2.1. Absolute Zero Trust (AZT) Architecture with ZVC

On May 12, 2021, President Biden issued an Executive Order entitled "Improving the Nation's Cybersecurity" [71], which requires that the US advance towards a "Zero Trust Architecture", as described by the NIST [72] [73]. NIST defined it as "a term for an evolving set of cybersecurity paradigms that move defenses from traditional static, network-based perimeters to focus on users, assets, and resources." In the prior art, zero trust is always policy-based, requiring human intervention, and therefore, autonomous absolute zero trust (AZT) is not achievable [74] [75]. Nonetheless, several papers claim to implement zero trust by design, despite all of them being policy-based models that cannot run without continuously monitoring and maintaining zero-trust policy-based rules defined by the organization running the zero-trust system. Since all these systems are policy-based [74] [75] and, therefore, strictly speaking, cannot be AZT. Blockchain systems are inherently autonomous [76], so the conventional zero-trust architecture has limitations when deployed with blockchain. On the contrary, blockchain itself can be deployed to implement zero trust [77].

Just as the ZVC framework provides an autonomous zero vulnerability and zero attack surface quantum resilient environment for exchanging information between computers [12]-[17], a similar network architecture can also be developed for accessing blockchain nodes over the Internet or in any peer-to-peer transaction. The resulting high-level client-server architecture is inspired by the Quantum-as-a-Service (QaaS) framework that was recently disclosed for quantum-proofing the Internet [13] [15] [16]. While the QaaS framework was a routing service for accessing the quantum computing services segregated from the mainstream Internet, the QLT (Quantum-safe Ledger Technology) architecture proposed in this paper deploys the blockchain/cryptocurrency infrastructure directly on the ZVC's Solid State Software on a Chip (3SoC) servers [13]

[14] [16]. This paper discloses a novel Quantum-safe Ledger Technology (QLT) approach that can render any blockchain network or cryptocurrency exchange quantum-resistant and hack-proof.

Implemented in two phases, the QLT framework research builds a quantum-resistant hardware wallet as a client device in the first phase [12], and the second phase builds the quantum-resistant server currently being taken up by a consortium constituted under the Horizon Europe program.

3.2.2. A Quantum-Safe Blockchain/DLT Architecture

As illustrated in **Figure 1**, this encryption-agnostic approach essentially segregates blockchain infrastructure from the mainstream computing infrastructure within the Internet. In this framework, the client computer is provided with a switchable 3SoC drive with a QLT user interface that securely connects to the blockchain nodes installed on the 3SoC remote servers as QLT nodes, creating a secure QLT tunnel. As a term of service, the peers are provided with 3SoC-designed QLT client device hardware for securely accessing the blockchain infrastructure distributed across the QLT server nodes that exclusively accept authentication requests from a QLT client device only. All other requests from unauthorized peers or hackers with legacy computing devices are declined (**Figure 1**). Whenever an authorized peer desires to execute a blockchain transaction, he/she just needs to switch over the client device from the legacy Internet mode to the QLT Intranet mode. Neither a legacy hacker using legacy devices nor a quantum hacker using a quantum computer can penetrate the zero-attack-surface, encryption-agnostic security of the QLT framework operating as an Intranet.

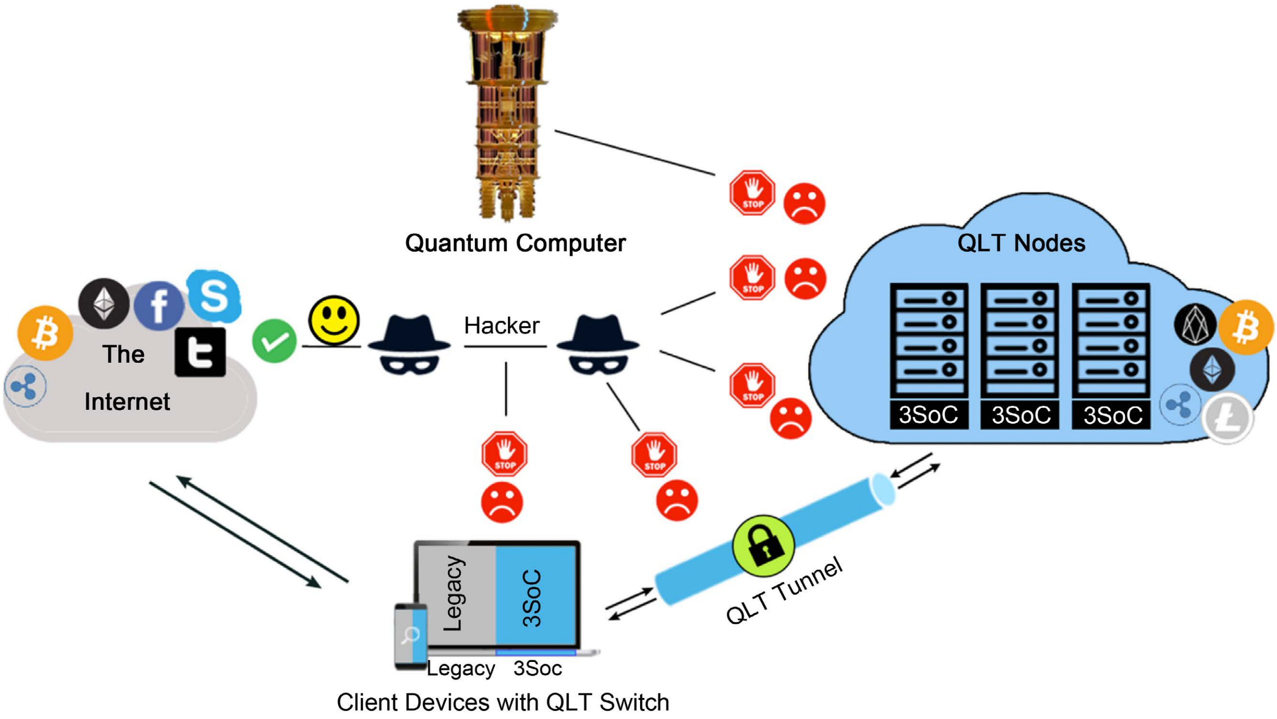

Figure 1. Switchable QLT framework for quantum-proofing blockchain infrastructure. Image Credit [15].

Thus, a ZVC/3SoC-powered QLT intranet can potentially offer a defense against the misuse of quantum computing against blockchain by bad actors. QLT framework provides freedom from impending threats from quantum computers even if the PQC algorithms currently under the NIST standardization process fail to deliver the promise. Most importantly, this strategy neutralizes the need for Internet-wide, device/resource-focused deployment of the resource-intensive PQCs that demand significant processing time and power and come with significantly higher costs [18] [78] [79].

3.2.3. Hack-Proof Crypto Exchanges (HEX) with QLT Framework

Although termed as quantum-safe ledger technology, QLT is equally effective in protecting blockchain and crypto exchanges from traditional hacking attacks. This is particularly important in hack-proofing crypto exchanges (HEX), as hundreds of crypto exchanges out there remain vulnerable to hack attacks.

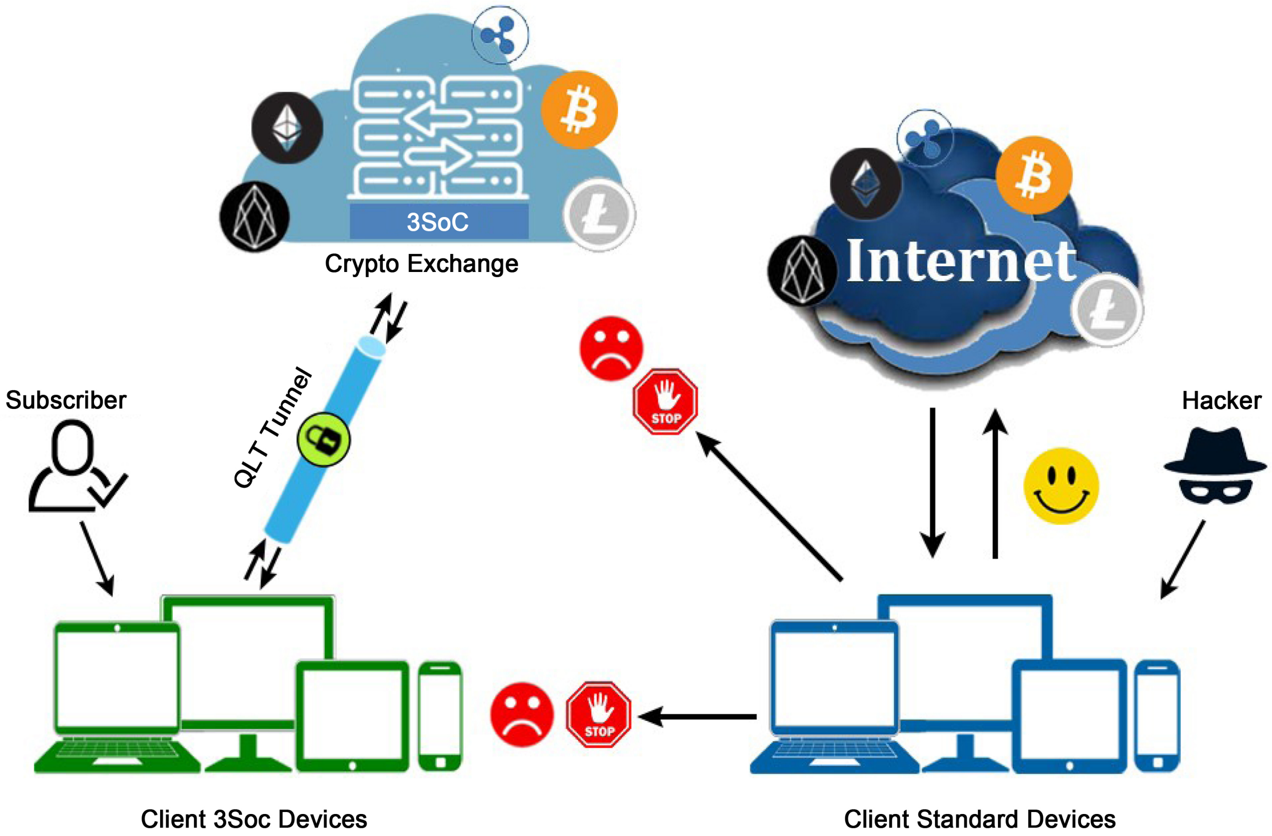

Figure 2. A hack-proof crypto exchange (HEX) rendered unbreachable with 3SoC powered QLT framework. Image Credit [15].

As illustrated in Figure 2, a novel QLT architecture for an HEX can potentially provide unbreakable end-to-end security to access ZVC-powered 3Soc server hosting the crypto exchange server application and isolate it from the rest of the Internet (Figure 2) This means that all the authorized subscribers of exchange platform can be mandated to deploy specific ZVC powered 3SoC security protocols to access the exchange resources within a ZVC-secured Intranet.

The framework components comprising the 3SoC client, tunnel, and exchange server are encryption agnostic with banned 3rd party permissions and zero attack surface, therefore immune to intrusions by unauthorized peers using legacy client devices. This makes the crypto exchange inaccessible to bad actors using legacy devices. The QLT framework can be implemented irrespective of whether the exchange is centralized or decentralized, a custodial cross-chain bridge or an NFT marketplace.

4. Study Limitations

This paper provides theoretical support for the deployment of a new cybersecurity paradigm that was originally tested in a minimalist hardware wallet device [41] to secure the scam-prone, hack-prone blockchain economy. QLT, QaaS, 3SoC, AZT, 6G, and other use case scenarios for ZVC are currently being explored in several 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. As any hypothesis-generating research, great care is warranted in projecting the conclusions of this report to real-world scenarios for the following reasons:

1) The QLT architecture is designed based on empirical data from a series of minimalist hardware wallet experiments [12]. It needs to be validated in diverse blockchain ecosystems before being extrapolated to real-world environments.

2) The ZVC/3SoC research is ongoing, and the inferences drawn from the available data are preliminary and subject to updates as and when available after real-world validation.

3) Currently, all encryption in blockchain systems is open and adversary-facing, but QLT partly changes that, imposing certain limitations on the universal accessibility of blockchain networks.

4) Notably, 3SoC devices inherently restrict the porting of generic or non-conforming third-party peripheral devices [13]-[18].

5) Currently, there is no experimental data from diverse blockchain ecosystems, which may raise questions on the practical viability of the QLT solution. QLT may face challenges when applied to specific use cases or blockchain configurations.

6) Rigorous experimentation by peer researchers is warranted to test, replicate, and validate the conclusions before QLT can be established as a new security paradigm for blockchains and cryptocurrencies.

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

Despite its limitations, this study provides compelling evidence that hack-proofing blockchain, cryptocurrencies, crypto exchanges, and NFT Marketplaces for rendering them resistant to future Q-Day threats is theoretically possible by using an encryption-agnostic approach to securing the networks. The QLT framework not only affords protection against future quantum threats but also secures the current blockchain/cryptocurrency infrastructure. 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 in a decentralized network.

5. Conclusions and Future Prospects

About a billion users, 20,000 cryptocurrencies, over 1000 blockchains, 380 crypto exchanges, and 245 NFT marketplaces remain vulnerable to hackers and scammers. This has resulted in as much as $88 billion lost to thefts over a dozen years since blockchain existed. The torment of blockchain/cryptocurrency vulnerabilities continues and, in fact, intensifies with the impending threat from quantum computers. As the Q-Day approaches, the security of blockchain and crypto assets becomes more relevant now than ever. The prevailing vulnerabilities that result in billions of dollars lost every year and the future Q-Day threats make cybersecurity of this potential multi-trillion industry a top priority. The QLT solution is platform agnostic, meaning it can be deployed irrespective of the type of blockchain and cryptocurrency, the type of crypto exchange, or the NFT marketplace. QLT is also encryption agnostic, meaning it is as effective in combating quantum computing threats as well as dealing with the traditional vulnerabilities that hackers use to steal funds. PQC is aggressively pursued worldwide for boosting the security of blockchain/cryptocurrency assets, but a proven quantum-proof PQC still seems to be eluding as all the post-quantum encryption methods have been cracked so far, and none has stood the rigors of the NIST testing process initiated 7 years ago in 2017. Even if a PQC algorithm passes all the validation and standardization steps, its deployment in blockchain will further worsen blockchain's current shortcomings in transaction costs, speed, and scaling. Searching for alternate cybersecurity strategies, therefore, becomes imperative.

QLT is cost-effective, resource-efficient, and does not limit scalability. Although current crypto exchanges are not as strictly regulated as other financial businesses are, most crypto exchanges will eventually be regulated once easy-to-implement technology that protects user interest is available. QLT makes it easy for regulators to protect public interest without encroaching on their privacy. QLT can be implemented not only to enforce regulatory policies but render all malicious activities by bad actors technologically out of bounds. The impending quantum threats to blockchain can be best dealt with by segregating all blockchain-specific activities from the mainstream Internet by regulating access to blockchain infrastructure rather than attempting to protect each Internet-connected device individually with resource-intensive PQC. While the findings presented in the paper are preliminary, demonstrating the potential feasibility of the QLT framework in multiple real-world blockchain ecosystems is urgently needed. To guide future blockchain researchers, the key takeaways from this study can be summarized as follows:

1) ZVC is a new cybersecurity paradigm that can potentially secure the entire decentralized blockchain/cryptocurrency ecosystem from today's traditional cyber-attacks and from Q-Day threats that future quantum computers present.

2) The QLT framework that ZVC builds is platform agnostic and can be deployed to secure any blockchain network, cryptocurrency exchange, or NFT marketplace, and all of them simultaneously.

3) PQC is computationally resource-intensive and expensive, and as such, quantum-proofing blockchain with PQC is likely to further diminish the commercial viability of blockchains because of its negative impact on cost, efficiency, and scalability.

4) QLT deploys minimal resources in its implementation, and therefore, it is resource-efficient and sustainable.

5) The QLT business model makes it easier to regulate the blockchain economy, both technologically and legally than legacy systems.

6) The QLT framework described in this paper and the QaaS framework disclosed previously [12]-[18] allow the ZVC/3SoC-powered AZT architecture to secure any online activity.

A proposed QLT consortium under the EU's Horizon Europe program is currently exploring QLT amongst other use cases of ZVC technology. Although the ZVC-powered 3SoC network architecture is still under development as a potentially robust cyber-secure framework, its early dissemination among blockchain researchers will accelerate the process of its validation and standardization as an alternative to the existing vulnerability-prone legacy blockchain/cryptocurrency ecosystem that loses billions of dollars annually in theft. The framework described in this paper may also be adapted to secure traditional financial and banking services and all such future online activities that require high security without compromising user experience.

Acknowledgments

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 Ghent, 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 Kotzaniko laou Panayiotis of University of Piraeus and Dr Kostas Kolomvatsos of University of Thessaly for being trusted partners in several consortia and initiatives involved in the development of the Zero Vulnerability Computing (ZVC) concept.

Authorship Contribution Statement

Fazal Raheman: Conceptualization, Methodology, Software, Validation, Writ-

ing-original draft, Writing-review & editing.

Declaration of Competing Interest

The author declares that there are no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The author declares no conflicts of interest regarding the publication of this paper.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Data Availability

All data are either included in the paper or can be found in the sources cited in the paper. Any additional data will be made available on request.

References

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] van Haaren Duijn, B., *et al.* (2022) The Dynamics of Governing Enterprise Blockchain Ecosystems. *Administrative Sciences*, **12**, Article No. 86.

[3] Buterin, V. (2013) Ethereum White Paper. *GitHub Repository*, **1**, 22-23.

[4] Arslanian, H. (2022) Ethereum. In: Arslanian, H., Ed., *The Book of Crypto*, Springer International Publishing, 91-98. https://doi.org/10.1007/978-3-030-97951-5_3

[5] Efanov, D. and Roschin, P. (2018) The All-Pervasiveness of the Blockchain Technology. *Procedia Computer Science*, **123**, 116-121. https://doi.org/10.1016/j.procs.2018.01.019

[6] DrFazal (2019) To Centralize Is Human, to Decentralize Divine. Medium. https://drfazal.medium.com/to-centralize-is-human-to-decentralize-divine-ii-7bd48681933f

[7] McGovern, T. (2022) Cryptocurrency Statistics 2024: How Many People Use Crypto? Earthweb. https://earthweb.com/cryptocurrency-statistics/

[8] Bhujel, S. and Rahulamathavan, Y. (2022) A Survey: Security, Transparency, and Scalability Issues of Nft's and Its Marketplaces. *Sensors*, **22**, Article No. 8833. https://doi.org/10.3390/s22228833

[9] Horch, A., Schunck, C.H. and Ruff, C. (2022) Adversary Tactics and Techniques specific to Cryptocurrency Scams. In: Roßnagel, H., Schunck, C.H. and Mödersheim, S., Eds., *Open Identity Summit* 2022, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, 119-124.

[10] Edwards, N., Haynes, J.B. and Kiser, S.B. (2021) Post-Quantum Security: CoreVUE Breaks through PKI A Look at an Emerging Technology in Cybersecurity. *Journal of Strategic Innovation and Sustainability*, **16**, 136-138.

[11] Fernandez-Carames, T.M. and Fraga-Lamas, P. (2020) Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, **8**, 21091-21116.

https://doi.org/10.1109/access.2020.2968985

[12] 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 No. 238. https://doi.org/10.3390/fi14080238

[13] Raheman, F. (2022) The Future of Cybersecurity in the Age of Quantum Computers. *Future Internet*, **14**, Article No. 335. https://doi.org/10.3390/fi14110335

[14] Raheman, F. (2022) The Q-Day Dilemma and the Quantum Supremacy/Advantage Conjecture. Research Square, December 9 2022.

[15] 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

[16] 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

[17] Raheman, F. (2024) Tackling the Existential Threats from Quantum Computers and Ai. *Intelligent Information Management*, **16**, 121-146. https://doi.org/10.4236/iim.2024.163008

[18] Raheman, F. (2024) Formulating and Supporting a Hypothesis to Address a Catch-22 Situation in 6G Communication Networks. Journal of Information Security, 15, 340-354. https://doi.org/10.4236/jis.2024.153020

[19] Alagic, G., *et al*. (2019) Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. US Department of Commerce, National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303

[20] Sparkes, M. (2022) Encryption Meant to Protect against Quantum Hackers Is Easily Cracked. *New Scientist*, March 8, 2022. https://www.newscientist.com/article/2310369-encryption-meant-to-pro-tect-against-quantum-hackers-is-easily-cracked/

[21] Ji, Y. and Dubrova, E. (2023) A Side-Channel Attack on a Masked Hardware Implementation of CRYSTALS-Kyber. *Proceedings of the* 2023 *Workshop on Attacks and Solutions in Hardware Security*, Copenhagen, 30 November 2023, 27-37. https://doi.org/10.1145/3605769.3623992

[22] Shin, D. and Rice, J. (2022) Cryptocurrency: A Panacea for Economic Growth and Sustainability? A Critical Review of Crypto Innovation. *Telematics and Informatics*, **71**, Article ID: 101830. https://doi.org/10.1016/j.tele.2022.101830

[23] Froehlich, M., Waltenberger, F., Trotter, L., Alt, F. and Schmidt, A. (2022) Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda. *Designing Interactive Systems Conference*, 13-17 June 2022, 155-177. https://doi.org/10.1145/3532106.3533478

[24] Nzimakwe, T.I. (2018) Government's Dynamic Approach to Addressing Challenges of Cybersecurity in South Africa. In: Fields, Z., Ed., *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, IGI Global, 364-381. https://doi.org/10.4018/978-1-5225-4763-1.ch013

[25] Charoenwong, B. and Bernardi, M. (2021) A Decade of Cryptocurrency "Hacks": 2011-2021. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3944435

[26] Sigalos, M. (2022) Crypto Scammers Took a Record $14 Billion in 2021. CNBC, January 6, 2022. https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2

021-chainalysis.html

[27] O'Rourke, M. (2022) Cryptocurrency Crime Cost a Record $14 Billion in 2021. *Risk Management*, **69**, 30.

[28] Merchant, M. (2022) Crypto Hackers Steal $3 Billion in 2022, Set to Be Biggest Year for Digital-Asset Heists. Money Control, October 18, 2022. https://www.moneycontrol.com/news/business/cryptocurrency/crypto-hackers-steal-3-billion-in-2022-set-to-be-biggest-year-for-digital-asset-heists-9347301.html

[29] Livni, E. (2022) Binance Blockchain Hit by $570 Million Hack, Exposing Crypto Vulnerabilities. *The New York Times*, October 7, 2022. https://www.nytimes.com/2022/10/07/business/binance-hack.html

[30] Amure, T.O. (2022) FTX Collapse Worsens after a $600 Million Hack and Criminal Charges. *Investopedia*, November 14, 2022. https://www.investopedia.com/ftx-got-hacked-6828458

[31] Chainalysisis Team (2022, Aug. 2) Vulnerabilities in Cross-Chain Bridge Protocols Emerge as Top Security Risk. Chainalysis. https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/

[32] Grobys, K. (2021) When the Blockchain Does Not Block: On Hackings and Uncertainty in the Cryptocurrency Market. *Quantitative Finance*, **21**, 1267-1279. https://doi.org/10.1080/14697688.2020.1849779

[33] Chang, S. (2019) Bitcoin Price Sinks amid Hack Attempt on Cryptocurrency Exchange Binance. *Investopedia*, June 25, 2019. https://www.investopedia.com/news/bitcoin-price-sinks-amid-hack-attempt-cryptocurrency-exchange-binance/

[34] Groopman, J. (2023) Top Blockchain Security Attacks, Hacks and Issues. https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues

[35] Boireau, O. (2018) Securing the Blockchain against Hackers. *Network Security*, **2018**, 8-11. https://doi.org/10.1016/s1353-4858(18)30006-0

[36] 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

[37] 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., Bhansali, A. and Doshi, R., Eds., *Advancements in Quantum Blockchain with Real-Time Applications*, IGI Global, 36-55. https://doi.org/10.4018/978-1-6684-5072-7.ch002

[38] Castelvecchi, D. (2022) The Race to Save the Internet from Quantum Hackers. *Nature*, **602**, 198-201. https://doi.org/10.1038/d41586-022-00339-5

[39] Rozell, D.J. (2022) Cash Is King. *Nature*. https://doi.org/10.1038/d41586-022-00418-7

[40] 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

[41] Grimes, R.A. (2019) Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. Wiley. https://doi.org/10.1002/9781119618232

[42] Ménard, A., Ostojic, I., Patel, M. and Volz, D. (2020) A Game Plan for Quantum Computing. McKinsey Q. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-ga

me-plan-for-quantum-computing

[43] An, H. and Kim, K. (2018) QChain: Quantum-Resistant and Decentralized PKI Using Blockchain. 2018 *Symposium on Cryptography and Information Security* (*SCIS* 2018), Niigata, 23-26 January 2018.

[44] Ding, J. (2019) A New Proof of Work for Blockchain Based on Random Multivariate Quadratic Equations. *Applied Cryptography and Network Security Workshops*: *ACNS* 2019 *Satellite Workshops*, Bogota, 5-7 June 2019, 97-107. https://doi.org/10.1007/978-3-030-29729-9_5

[45] Dey, N., Ghosh, M. and Chakrabarti, A. (2022) Quantum Solutions to Possible Challenges of Blockchain Technology. In: Kumar, A., Gill, S.S. and Abraham, A., Eds., *Quantum and Blockchain for Modern Computing Systems*: *Vision and Advancements*, Springer International Publishing, 249-282. https://doi.org/10.1007/978-3-031-04613-1_9

[46] Li, X., Luo, C., Liu, P., Wang, L. and Yu, D. (2019) Injecting Differential Privacy in Rules Extraction of Rough Set. In: *Proceedings of the* 2*nd International Conference on Healthcare Science and Engineering*, Springer, Singapore, 175-187. https://doi.org/10.1007/978-981-13-6837-0_13

[47] Markets&Markets.com. https://www.marketsandmarkets.com/Market-Reports/quantum-cryptography-market-45857130.html

[48] Sayeed, S., Marco-Gisbert, H. and Caira, T. (2020) Smart Contract: Attacks and Protections. *IEEE Access*, **8**, 24416-24427. https://doi.org/10.1109/access.2020.2970495

[49] Adamik, F. and Kosta, S. (2019) Smartexchange: Decentralised Trustless Cryptocurrency Exchange. *Business Information Systems Workshops*, Berlin, 18-20 July 2018, 356-367. https://doi.org/10.1007/978-3-030-04849-5_32

[50] Lin, L.X. (2019) Deconstructing Decentralized Exchanges. *Stanford Journal of Blockchain Law & Policy*, **2**, 58-77.

[51] Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A. and Knottenbelt, W. (2019) XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets. 2019 *IEEE Symposium on Security and Privacy* (*SP*), San Francisco, 19-23 May 2019, 193-210. https://doi.org/10.1109/sp.2019.00085

[52] Lee, S., Murashkin, A., Derka, M. and Gorzny, J. (2023) SoK: Not Quite Water under the Bridge: Review of Cross-Chain Bridge Hacks. 2023 *IEEE International Conference on Blockchain and Cryptocurrency* (*ICBC*), Dubai, 1-5 May 2023, 1-14. https://doi.org/10.1109/icbc56567.2023.10174993

[53] Helal, M., Alsoud, A.R. and Alshareef, H. (2022) Cross-Chain Interoperability-Validating Smart Contracts to Interoperate over Diverse Blockchain Networks Using Interoperable Blockchain Framework Design (IBFD).

[54] Brooks, K. (2022, October 12) Hackers Have Stolen Record $3 Billion in Cryptocurrency This Year. CBS News. https://www.cbsnews.com/news/cryptocurrency-theft-hacker-chainalysis-blockchain-crime/

[55] Bernstein, D.J. and Lange, T. (2017) Post-Quantum Cryptography. *Nature*, **549**, 188-194. https://doi.org/10.1038/nature23461

[56] Gupta, K.D., Nag, A.K., Rahman, M.L., Mahmud, M.A.P. and Sadman, N. (2021) Utilizing Computational Complexity to Protect Cryptocurrency against Quantum Threats: A Review. *IT Professional*, **23**, 50-55.

https://doi.org/10.1109/mitp.2021.3089494

[57] Marcos, A., *et al*. (2021) Quantum-Resistance in Blockchain Networks.

[58] Zhu, D., Zheng, J., Zhou, H., Wu, J., Li, N. and Song, L. (2022) A Hybrid Encryption Scheme for Quantum Secure Video Conferencing Combined with Blockchain. *Mathematics*, **10**, Article No. 3037. https://doi.org/10.3390/math10173037

[59] Laura, D. (2022, August 3) 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/

[60] Banerjee, U., Das, S. and Chandrakasan, A.P. (2020) Accelerating Post-Quantum Cryptography Using an Energy-Efficient TLS Crypto-Processor. 2020 *IEEE International Symposium on Circuits and Systems* (*ISCAS*), Seville, 12-14 October 2020, 1-5. https://doi.org/10.1109/iscas45731.2020.9180550

[61] Aji, A., Jain, K. and Krishnan, P. (2021) A Survey of Quantum Key Distribution (QKD) Network Simulation Platforms. 2021 2*nd Global Conference for Advancement in Technology* (*GCAT*), Bangalore, 1-3 October 2021, 1-8.
https://doi.org/10.1109/gcat52182.2021.9587708

[62] Rimba, P., Tran, A.B., Weber, I., Staples, M., Ponomarev, A. and Xu, X. (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

[63] Raheman, F. (2023) Economic and Social Sustainability of Legacy Blockchain for Non-Crypto Use Cases: A Reality Check. *International Journal of Blockchains and Cryptocurrencies*, **4**, 1-25. https://doi.org/10.1504/ijbc.2023.131634

[64] di Angelo, M. and Salzer, G. (2019) A Survey of Tools for Analyzing Ethereum Smart Contracts. 2019 *IEEE International Conference on Decentralized Applications and Infrastructures* (*DAPPCON*), Newark, 4-9 April 2019, 69-78.
https://doi.org/10.1109/dappcon.2019.00018

[65] Jansen, M., Hdhili, F., Gouiaa, R. and Qasem, Z. (2019) Do Smart Contract Languages Need to Be Turing Complete? In: Prieto, J., *et al*., Eds., *Blockchain and Applications*: *International Congress*, Springer International Publishing, 19-26.
https://doi.org/10.1007/978-3-030-23813-1_3

[66] Kaleem, M., Mavridou, A. and Laszka, A. (2020) Vyper: A Security Comparison with Solidity Based on Common Vulnerabilities. 2020 2*nd Conference on Blockchain Research & Applications for Innovative Networks and Services* (*BRAINS*), Paris, 28-30 September 2020, 107-111.
https://doi.org/10.1109/brains49436.2020.9223278

[67] Arikpo, I.I., Ogban, F.U. and Eteng, I.E. (2008) Von Neumann Architecture and Modern Computers. *Global Journal of Mathematical Sciences*, **6**, 97-104.
https://doi.org/10.4314/gjmas.v6i2.21415

[68] Francillon, A. and Castelluccia, C. (2008) Code Injection Attacks on Harvard-Architecture Devices. *Proceedings of the* 15*th ACM Conference on Computer and Communications Security*, Alexandria, 27-31 October 2008, 15-26.
https://doi.org/10.1145/1455770.1455775

[69] Rajput, B. (2020) Changing Landscape of Crime in Cyberspace. In: Rajput, B., Ed., *Cyber Economic Crime in India*, Springer International Publishing, 13-23.
https://doi.org/10.1007/978-3-030-44655-0_2

[70] European Commission (2023) "Seal of Excellence" Awarded to ZVC in a Horizon Europe EIC Accelerator Grant Program. https://zvchub.com/#seal

[71] Kerman, A., Borchert, O., Rose, S. and Tan, A. (2020) Implementing a Zero Trust

Architecture. National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf

[72] Ford, P. (2023) The Quantum Cybersecurity Threat May Arrive Sooner than You Think. *Computer*, **56**, 134-136. https://doi.org/10.1109/mc.2022.3227657

[73] National Security Agency (2021) Embracing a Zero Trust Security Model. https://media.defense.gov/2021/feb/25/2002588479/-1/-1/0/csi_embracing_zt_security_model_uoo115131-21.pdf

[74] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020) Zero Trust Architecture. National Institute of Standards and Technology.

[75] Nivarthi, K.S.P. and Gatla, G. (2022) Fighting Cybercrime with Zero Trust. *American Academic Scientific Research Journal for Engineering, Technology, and Sciences*, **90**, 371-381.

[76] Hardjono, T. (2018) Blockchain Interoperability and Survivability. 2018 *IEEE Global Blockchain Summit, NIST*, Gaithersburg, 17-19 September 2018.

[77] Dhar, S. and Bose, I. (2020) Securing IoT Devices Using Zero Trust and Blockchain. *Journal of Organizational Computing and Electronic Commerce*, **31**, 18-34. https://doi.org/10.1080/10919392.2020.1831870

[78] 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

[79] Gupta, N., Jati, A., Chauhan, A.K. and Chattopadhyay, A. (2021) PQC Acceleration Using Gpus: Frodokem, Newhope, and Kyber. *IEEE Transactions on Parallel and Distributed Systems*, **32**, 575-586. https://doi.org/10.1109/tpds.2020.3025691