A discussion on Quantum-safe Ledger Technology (QLT)

Fazal Raheman[1]

[1] *Fazal Raheman*
drfazal@bc5.eu
Blockchain 5.0 Ltd, Kesklinna linnaosa, Ahtri tn 12, 10151, Tallinn, Estonia.

Conflict of Interest Statement:

The author has no conflicts of interest to disclose

Author's contribution:

The corresponding author is the sole contributor of this paper.

Acknowledgement: The author is grateful to Mr Tejas Bhagat and Ms Sadiya Khan, Blockchain 5.0 Ltd, Estonia for their support in preparing this manuscript.

A discussion on Quantum-safe Ledger Technology (QLT)

Abstract: Blockchain/DLT is projected to be a $3 trillion industry by 2030, although the cryptocurrency market cap already crossed $3 trillion in 2021. With one billion users using 380 exchanges, the security of cryptocurrencies remains a major concern as billions are lost to hackers every year. A record $14 billion was lost in 2021, and $3 billion was stolen in 2022. 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 1,000 existing blockchains against scammers/hackers remains a top priority for this industry. This research proposes a novel Quantum-safe Ledger Technology (QLT) framework that secures DLTs/cryptocurrencies and exchanges from current vulnerabilities and protects them from the impending Q-day threats from future quantum computers. QLT can be easily adopted as blockchain-agnostic technology to secure any blockchain or crypto exchange.

Keywords: Cybersecurity; Cryptocurrencies; Crypto exchange; Quantum Threat; PQC, Crypto Hacks

1. Introduction

The Digital Ledger Technology (DLT) blockchain, used interchangeably throughout this paper, was first introduced in 2008 by Satoshi Nakamoto [1] as a peer-to-peer electronic cash system or cryptocurrency called Bitcoin. DLT and cryptocurrency are inseparably linked. As much as a decentralized form of money cannot exist without the security provided by a blockchain, a public blockchain cannot be built without incentivizing people to create it [2]. Cryptocurrency is that incentive. The introduction of smart contracts in blockchain [3] and its commercial launch as Ethereum blockchain in 2015 [4] further revolutionized DLT to disrupt current business models, financial systems, organizations, and civic governance [5].

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 [6]. There are over 1,000 blockchains and 245 NFT marketplaces worldwide [7]. 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 about a dozen years. Projected to be a $3 trillion industry [8], blockchain exclusively relies on adversary-facing cryptography that faces a severe threat from the massive computing power of quantum computers, necessitating the urgency of developing quantum-resistant blockchain [9,10].

2. Problem Statement

Hailed as a panacea for economic growth and sustainability [11], blockchain's envisioned omnipresence in human-computer interactions so far lags [12]. 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 [13], and cryptosystems are no exception. No wonder it has been the target of perpetual scams and hacks, resulting in billions of dollars lost yearly.

2.1 Perpetual scams hack attacks on cryptocurrencies

Since the launch of Bitcoin as a cryptocurrency, the cryptocurrency industry has been blemished with countless crypto scams and hacks over the years, estimated to be as high as $88 billion [14] and counting. In early 2022, CNBC [15] reported 2021 as a record-breaking year of crypto scams totaling $14 billion [16]. 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 [17], followed by the two most prominent exchanges, Binance [18] and FTX [19], reporting $570 and $600 million respectively lost to hack attacks totaling $1.17 billion in losses in just a single month. In August 2022, Chainalysis reported another billion dollars lost to hacking attacks [20]. Cryptocurrency hacking incidents affect the cryptocurrency market by introducing volatility, which increases significantly both contemporaneously and as a delayed effect [21]. Each major hack results in a significant price dip for Bitcoin and all major cryptocurrencies [22]. Frequent hacking incidents are detrimental to the growth of the blockchain economy [23]. Securing cryptocurrencies against hackers remains the top priority for this multi-trillion industry [24]. The advent of quantum computers further amplifies the threat to encryption-dependent Internet protocols and blockchain networks [25].

2.2 The Q-Day threat to blockchain

Recent reports emphasize the seriousness of the impending threats from quantum computers to the Internet [26]. Even the questions of the imminent end of blockchain are raised [27]. An actual quantum attack on several cryptocurrencies led to the crypto crash in 2022 [28]. Theoretically, all cryptographic algorithms are vulnerable to quantum attacks, which could be catastrophic [29] as cryptography is omnipresent in today's networked lifestyle. Already overwhelmed with the ever-increasing scourge of hack attacks, blockchain appears to be moving closer to the cryptography apocalypse threat from quantum computers [30,31]. Quantum computers with cryptographically significant qubits are predicted to start premiering as early as 2025 [31]. Quantum algorithms already exist for all significant public-key cryptosystems, necessitating an urgent response to the imminent Q-Day threat. Several research groups are exploring PQC (post-quantum cryptography) for developing a quantum-resistant blockchain [32]. QChain was one of the first PQC blockchain initiatives initiated in 2018 [33]. Since 2017, the process of standardization of PQC initiated by NIST (National Institute of Standards and Technology) has resulted in 80 failed PQC algorithms [34]. Rainbow is an example of PQC deployed by the ABCmint cryptocurrency [35]. Dey et al. recently reported that Bitcoin, Ethereum, and Corda are launching PQC initiatives [36]. However, with so many PQC methods failing the standardization process [34], it is time to explore alternate cybersecurity strategies to secure blockchains from the peril of quantum threats.

3. 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 [37]. The ZVC concept 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 robust and energy efficient [37]. More recently, ZVC was explored [38] as an alternative to PQC candidate algorithms that entered NIST's PQC standardization process and failed [39,34], warranting 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 [38,40]. This paper explores a strategy similar to the proposed QaaS architecture [40] to deliver a Quantum-safe Ledger Technology (QLT) framework. To place the development of the QLT concept in proper perspective, a discussion on state-of-the-art is presented in Section 4. Section 5 illustrates details of the universal design of the QLT framework architecture in conventional and quantum computing scenarios. Section 6 discusses the limitations of this study, and Section 7 presents the conclusion and future of the QLT approach.

4. The state-of-the-art

Our problem statement identifies two categories of cybersecurity breaches possible in legacy DLT/blockchain systems. 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 [37]. In contrast, the second category is an upshot of the impending threats from future quantum computers [38, 40]. In this paper, the QLT solution proposes a new paradigm for tackling each vulnerability to render DLT virtually hackproof. A review of the state-of-the-art, therefore, warrants a two-fold inquiry.

4.1 Crypto exchange vulnerabilities

In contrast to classical stock exchanges, which facilitate trading but do not hold securities on behalf of clients, centralized cryptocurrency exchanges store virtual currencies for their clients, making cryptocurrency exchanges vulnerable. Compared to centralized exchanges, decentralized exchanges are presumed to be more secure because, as against the user assets remaining in service provider custody [41], the user assets stay in the user's control [42]. However, with the advent of cross-chain bridges, most cross-chain schemes were found to be vulnerable to malicious Internet-based attacks [43]. This was because these cross-chain protocols were essentially custodial schemes taking interim custody of the user asset while transferring the asset from one chain to another [44]. This made the bridge custodian the target [20], rendering decentralized exchanges vulnerable [45]. Hence, cryptocurrency exchanges, whether centralized or decentralized with cross-chain bridging, remain susceptible to hack attacks. As reported by CBS News, they are more vulnerable now than ever [46], and the top security risk appears to have shifted to cross-chain bridge protocols deployed in decentralized exchanges [20].

4.2. Post-quantum blockchain vulnerabilities

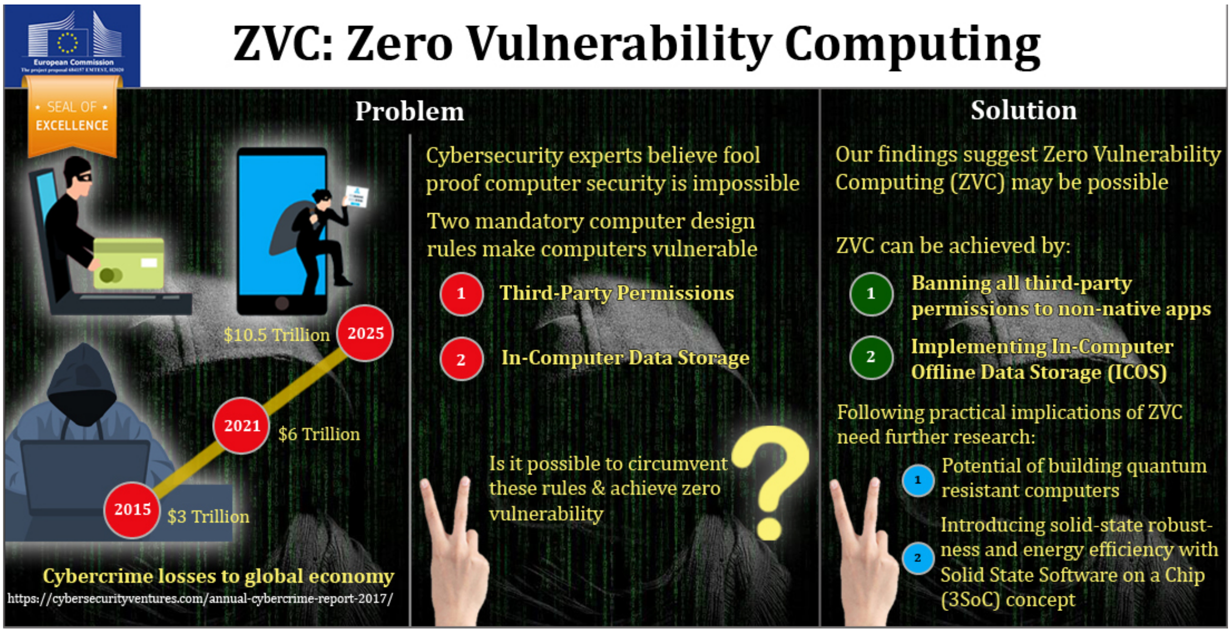
Post Quantum Cryptography (PQC) encompasses a new generation of algorithms for creating asymmetric keys that are believed to resist attacks by quantum computers [47]. Cryptocurrencies [48] and blockchain transactions rely on distributed ledgers and require solutions that guarantee quantum resistance to preserve the integrity of data and assets in their public and immutable ledgers [25].

Many reports on quantum-safe blockchains have appeared in the peer-reviewed literature [10]. Marcos et al. [49] deployed PQC as a layer 2 solution to make blockchains quantum-resistant. Zhu et al. [50] recently proposed a hybrid encryption scheme for quantum secure video conferencing combined with blockchain. However, with most PQC schemes failing NIST's standardization process, quantum computers appear to be more detrimental to human interests than the benefits they deliver [51]. One recent cryptocurrency crash occurred because of a quantum attack on several cryptocurrencies [29].

Moreover, PQC algorithms are computationally expensive [52, 53] and will add to the already high cost and slow speed of blockchain transactions. The cost of a typical Ethereum blockchain transaction is already very high, clocking as high as 360 times the cost of a conventional database [54]. Attempts at making blockchain resilient with PQC primitives will further escalate the already exorbitant blockchain transaction costs and hamper blockchain scalability.

5. Beyond state-of-the-art

All state-of-the-art computing systems, whether based on the von Neumann architecture [55] or the Harvard architecture [56], are designed to grant third-party permissions to the software applications developed by programmers and software vendors. It is a mandate that can only be circumvented by making the computers useless. These permissions are also the targets that bad actors manipulate to create attack vectors for gaining



ZVC: Zero Vulnerability Computing

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/

Fig 1. Seal of Excellence winning ZVC Technology. Data Source : *Future Internet* 14.8 (2022): 238.

unauthorized access to a network or a computer system to extract data. For this reason, a legacy computer or network will always bear an attack surface that keeps growing and can never be eliminated [57]. A significant paradigm shift in computing was recently developed and tested, obliterating the third-party permissions and reducing the attack surface to zero [37]. Such a system did not rely on cryptography for securing 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?

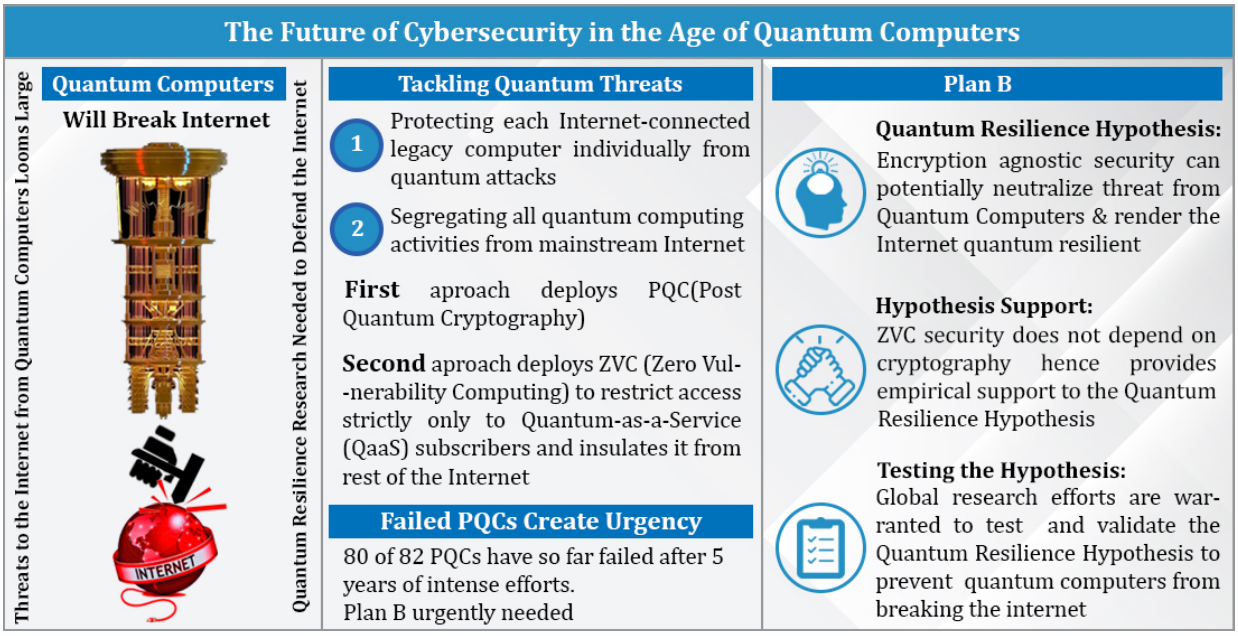
(2) As the ZVC architecture lacks layering, rendering it conceptually analogous to the zero-moving-parts nature of solid-state electronics, will it deliver the same advantages to computers as the solid-state did to revolutionize the electronics industry in the 1960s–1970s?

Fig. 1 illustrates a graphic summary of the ZVC as a new encryption-agnostic cybersecurity paradigm that won a Seal of Excellence from the European Union's Horizon Europe program [37]. While several European Consortia continue to investigate ZVC in diverse use case scenarios, a recent report explored the ZVC hypotheses for quantum resilient cybersecurity [38]. As the full scope and relevance of ZVC to the overall cybersecurity of the Internet remain a subject of ongoing research, it is advantageous to continue to explore new fields of application. One such area of very high unmet need is the security of blockchain and cryptocurrency infrastructure. A de novo analysis will open a possible new approach for securing cryptocurrencies from the menace of frequent hack attacks and future-proofing the blockchain against the impending threats from quantum computers. The following rationale recently applied to protecting the Internet from the impending quantum threats to legacy computers can also be applied to the security of blockchain/cryptocurrency and crypto exchanges (**Fig.2**):

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

ii) Segregating all quantum computing activities from mainstream Internet with encryption agnostic ZVC in a Quantum-as-a-Service (QaaS) business model [38].

Just as the ZVC framework provides zero vulnerability and zero attack-surface quantum resilient environments for exchanging information between computers, 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 recently disclosed for quantum-proofing the Internet [40]. While the QaaS framework was a routing service, the QLT architecture proposed in this paper deploys the DLT/cryptocurrency infrastructure directly on the ZVC's Solid State Software on a Chip (3SoC) servers [38, 58]. This paper discloses a novel Quantum-safe Ledger Technology (QLT) approach to render any blockchain network node or cryptocurrency exchange quantum-resistant and hackproof.



The Future of Cybersecurity in the Age of Quantum Computers

Threats to the Internet from Quantum Computers Looms Large

Quantum Computers

Will Break Internet

Quantum Resilience Research Needed to Defend the Internet

Tackling Quantum Threats

1 Protecting each Internet-connected legacy computer individually from quantum attacks

2 Segregating all quantum computing activities from mainstream Internet

First aproach deploys PQC(Post Quantum Cryptography)

Second aproach deploys ZVC (Zero Vul- -nerability Computing) to restrict access strictly only to Quantum-as-a-Service (QaaS) subscribers and insulates it from rest of the Internet

Failed PQCs Create Urgency

80 of 82 PQCs have so far failed after 5 years of intense efforts.
Plan B urgently needed

Plan B

Quantum Resilience Hypothesis:
Encryption agnostic security can potentially neutralize threat from Quantum Computers & render the Internet quantum resilient

Hypothesis Support:
ZVC security does not depend on cryptography hence provides empirical support to the Quantum Resilience Hypothesis

Testing the Hypothesis:
Global research efforts are warranted to test and validate the Quantum Resilience Hypothesis to prevent quantum computers from breaking the internet

Fig. 2: Quantum Cybersecurity Graphical Abstract- Raheman. *Future Internet* 2022, *14*(11), 335

Implemented in two phases, the QLT research builds a quantum-resistant hardware wallet as a client device in the first phase [37], and the second phase builds the quantum-resistant server currently being taken up by a consortium constituted under the Horizon Europe program [38, 40].

5.1 A Quantum-safe blockchain/DLT architecture

As illustrated in **Fig. 3**, this encryption-agnostic approach essentially segregates blockchain infrastructure from the mainstream computing infrastructure within the Internet. In this framework, the client computer has a switchable 3SoC drive with a QLT user interface that securely connects to the blockchain nodes installed on 3SoC remote servers as QLT nodes. As a term of service, the peers are provided with a 3SoC client device hardware for securely accessing the blockchain infrastructure distributed across the 3SoC servers that exclusively accept authentication requests from a 3SoC client device. All other requests from unauthorized peers or hackers with legacy computing devices are declined (**Fig. 3**). Whenever an authorized peer desires to execute a blockchain transaction, he/she must 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. Both the client node device and the blockchain node ban third-party permissions to completely obliterate the attack surface, creating a secure 3SoC tunnel (**Fig. 3**). Thus, a ZVC/3SoC-powered QLT intranet can offer defense against misuse of quantum computing against blockchain by bad actors. Thus the QLT framework provides freedom from the impending threats from quantum computers even if the PQC algorithms 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 [59] and come with significantly higher costs [52, 53]. Most importantly, QLT framework is DLT agnostic, and can be deployed with any DLT.

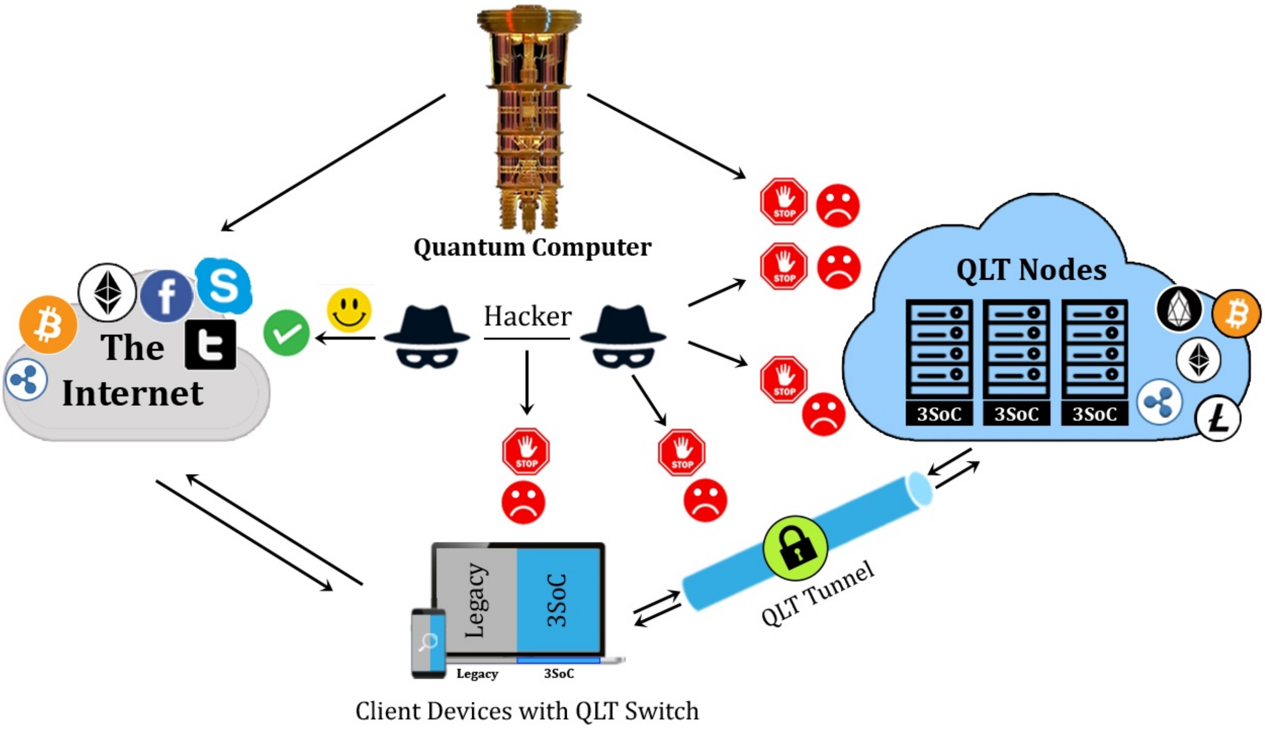


Fig. 3. Switchable QLT framework for quantum-proofing blockchain infrastructure

5.2 Hack-proof crypto exchanges (HEX) with QLT framework

Although termed 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 hundreds of crypto exchanges (HEX) vulnerable to attacks. As illustrated in **Fig. 4,** a novel QLT architecture for a HEX can potentially provide unbreakable end-to-end security to access the ZVC-powered 3Soc server hosting the crypto exchange application and isolate it from the rest of the Internet (**Fig. 4**). 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 computer, tunnel, and exchange server are encryption agnostic with banned third-party permissions and zero attack surface, immune to intrusions by unauthorized peers using legacy client devices. This makes the crypto exchange inaccessible to bad actors using legacy devices (**Fig. 4**). The QLT framework can be implemented across the board irrespective of whether the exchange is centralized, decentralized, a custodial cross-chain bridge, or an NFT marketplace.

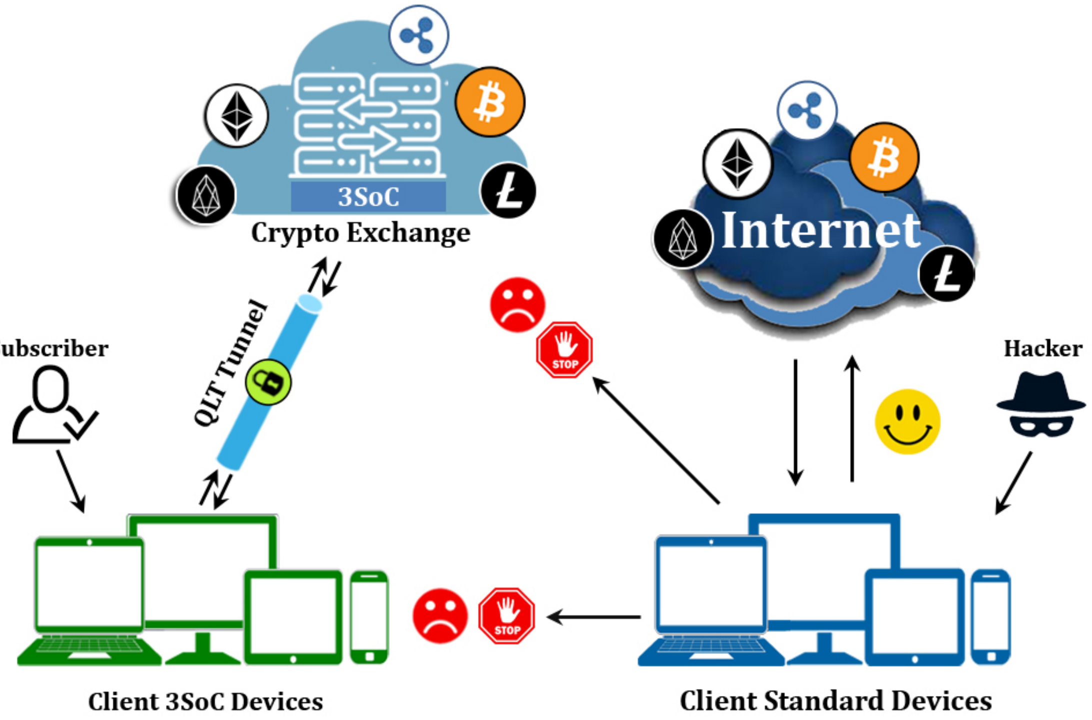


Fig. 4. A hack-proof crypto exchange (HEX) rendered unbreachable with 3SoC powered QLT framework

6. Study Limitations

This paper provides theoretical support for deploying a new cybersecurity paradigm initially tested in a minimalist hardware wallet device [37] to secure the scam-prone, hack-prone blockchain economy. QLT, QaaS, 3SoC, and other use case scenarios for ZVC are currently under exploration under 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. However, great caution is warranted in projecting the conclusions of this report to real-world scenarios for the following reasons:

(i) The QLT architecture is designed based on empirical data from minimalist hardware wallet experiments [37]. It must be validated in diverse blockchain ecosystems before extrapolating to real-world 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, all encryption in the blockchain systems is open and adversary-facing, but QLT changes that, imposing certain limitations in the universal accessibility to blockchain networks.
(iv) Notably, 3SoC devices inherently restrict the porting of generic or non-conforming third-party peripheral devices [58].
(v) Rigorous experimentation by peer researchers is warranted for testing, replicating, and validating the conclusions before QLT can be established as a new security paradigm for blockchains and cryptocurrencies.

Despite its limitations, this study provides compelling evidence that hack proofing blockchain, cryptocurrencies, crypto exchanges, and NFT Marketplaces and rendering them resistant to future Q-Day threats is theoretically possible 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.

7. Conclusion and prospects

One billion users, 20,000 cryptocurrencies, over 1,000 blockchains, 380 crypto exchanges, and 245 NFT marketplaces [8] 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 [14]. The torment of blockchain/cryptocurrency vulnerabilities continues and intensifies with the impending threat from quantum computers. The security of blockchain and crypto assets is 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, effectively combating quantum computing threats and dealing with the traditional vulnerabilities that hackers use to steal funds. PQC is aggressively pursued worldwide to boost the security of blockchain/cryptocurrency assets. However, a proven quantum-proof PQC is still eluding as so many post-quantum encryption methods have been cracked, and none has stood the rigors of NIST testing. Even if a PQC algorithm passes all the validation and standardization steps, its deployment in blockchain will further worsen blockchain's current shortcomings of 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 crypto exchanges are not as strictly regulated as other financial businesses, 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 to enforce regulatory policies and render all malicious activities by bad actors technologically out of bounds. The impending quantum threats to the blockchain can be best dealt with by segregating all blockchain-specific activities from the mainstream Internet by regulating access to the blockchain rather than attempting to protect each Internet-connected device individually from malicious attacks. 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 secure the entire decentralized blockchain/cryptocurrency ecosystem from the traditional cyber-attacks of today, as well as 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 is resource-efficient.
5. The QLT business model makes it easier to regulate the blockchain economy, both technologically and legally, compared to the legacy systems.
6. Like the QLT framework described in this paper and the QaaS framework disclosed previously [40], the ZVC/3SoC architecture can be adapted to secure any online activity.

A proposed 3SoC consortium under the EU's Horizon Europe program explores 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. In the future, the framework described in this paper may also be adapted for securing traditional financial and banking services and all such online activities that require high security without compromising user experience.

Declarations

Availability of data and material

Not applicable

Funding

Not applicable

Acknowledgment
Please see the title page.

References

References

1) Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review (2008), 21260.
2) van Haaren Duijn, B, et al. "The dynamics of governing enterprise blockchain ecosystems." *Administrative Sciences* 12.3 (2022): 86.
3) Buterin Vitalik (2013). Ethereum white paper. GitHub repository 1 (2013), 22–23
4) Arslanian, Henri (2022). "Ethereum." *The Book of Crypto*. Palgrave Macmillan, Cham, 2022. 91-98.
5) Efanov, D &Roschin, P. The all-pervasiveness of the blockchain technology. Procedia Computer Science 123 (2018), 116–121. https://doi.org/10. 1016/j.procs.2018.01.019
6) Bhujel, S., & Rahulamathavan, Y. A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces. *Sensors*, *22*(22), 8833.
7) Horch A, Schunck C H., and Ruff C. "*Adversary Tactics and Techniques specific to Cryptocurrency Scams.*" *Open Identity Summit 2022*. Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022, 119 doi:18.18420/OID2022-10
8) McGovern, Thomas. CRYPTOCURRENCY STATISTICS 2022: HOW MANY PEOPLE USE CRYPTO? EARTHWEB, Dec 3, 2022. Available at https://earthweb.com/cryptocurrency-statistics/ (accessed Dec 8, 2022).
9) Edwards, N., Haynes, J. B., & Kiser, S. B. Post-Quantum Security: CoreVUE Breaks Through PKI A Look at an Emerging Technology in Cybersecurity. *Journal of Strategic Innovation and Sustainability*, *16*(1), 136-138.
10) Fernandez-Carames, T. M., & Fraga-Lamas, P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, *8*, 21091-21116.
11) Shin, Donghee, and John Rice. "Cryptocurrency: A Panacea for Economic Growth and Sustainability? A Critical Review of Crypto Innovation." *Telematics and Informatics* (2022): 101830.
12) Fröhlich, Michael, et al. "Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda." *arXiv preprint arXiv:2204.10857* (2022).
13) Nzimakwe, T. I. (2018). Government's Dynamic Approach to Addressing Challenges of Cybersecurity in South Africa. In *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (pp. 364-381). IGI Global.
14) Charoenwong, Ben and Bernardi, Mario. A Decade of Cryptocurrency 'Hacks': 2011 – 2021 (October 1, 2021). Available at SSRN: https://ssrn.com/abstract=3944435 or http://dx.doi.org/10.2139/ssrn.3944435
15) MacKenzie Sigalos. Crypto scammers took a record $14 billion in 2021. CNBC, Jan 6, 2022. Available at https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html. Accessed on Dec 5, 2022.
16) O'Rourke, Morgan. "CRYPTOCURRENCY CRIME COST A RECORD $14 BILLION IN 2021." *Risk Management* 69.1 (2022): 30-30.
17) Merchant, Murtuza. Crypto hackers steal $3 billion in 2022, set to be biggest year for digital-asset heists. Money Control, Oct 18, 2022. Available at 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. Accessed on December 5, 2022.
18) Ephrat Livni. Binance Blockchain Hit by $570 Million Hack, Exposing Crypto Vulnerabilities. The New York Times, Oct 7, 2022. Available at https://www.nytimes.com/2022/10/07/business/binance-hack.html
19) Tobi Opeyemi Amure. FTX Collapse Worsens After a $600 Million Hack And Criminal Charges. Investopedia, Nov 14, 2022. Available at https://www.investopedia.com/ftx-got-hacked-6828458
20) Chainalysisis Team. Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk, Chainalysis, Aug 2, 2022. Available at https://blog.chainalysis.com/reports/cross-chain-bridge-hacks-2022/ (accessed on Dec 1, 2022).

21) Grobys, Klaus. "When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market." *Quantitative Finance* 21.8 (2021): 1267-1279.
22) Chang, Samanta. Bitcoin Price Sinks Amid Hack Attempt on Cryptocurrency Exchange Binance. Investopedia, June 25, 2019. Available at https://www.investopedia.com/news/bitcoin-price-sinks-amid-hack-attempt-cryptocurrency-exchange-binance/
23) Groopman, Jessica. Top blockchain security attacks, hacks and issues. TechTarget.com. Available at https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues
24) Boireau, Olivier. "Securing the blockchain against hackers." *Network Security* 2018.1 (2018): 8-11.
25) Kearney, Joseph J., and Carlos A. Perez-Delgado. "Vulnerability of blockchain technologies to quantum attacks." *Array* 10 (2021): 100065.
26) Castelvecchi D. *The race to save the Internet from quantum hackers.* Nature. 2022 Feb;602(7896):198-201. doi: 10.1038/d41586-022-00339-5. PMID: 35136223.
27) Kappert, Noah, Erik Karger, and Marko Kureljusic. "Quantum Computing-The Impending End for the Blockchain?." *Pacific Asia Conference on Information Systems (PACIS), Dubai, UAE*. 2021.
28) Rozell DJ. *Cash is king.* Nature. 2022 Feb 16. doi: 10.1038/d41586-02
29) Majot and Yampolskiy. Global catastrophic risk and security implications of quantum computers. Futures. Volume 72, September 2015, Pages 17-26m
30) Grimes, Roger A. *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto*. John Wiley & Sons, 2019.
31) 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 Dec 2022).
32) Unogwu, Omega John, et al. "Introduction to Quantum-Resistant Blockchain." *Advancements in Quantum Blockchain With Real-Time Applications*. IGI Global, 2022. 36-55.
33) An, H., & Kim, K. QChain: Quantum-resistant and decentralized PKI using blockchain. In *2018 Symposium on Cryptography and Information Security (SCIS 2018)*. IEICE Technical Committee on Information Security.
34) Sparkes, Mathew. Encryption meant to protect against quantum hackers is easily cracked. New Scientist, March 8, 2022. Available at https://www.newscientist.com/article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked/
35) 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.
36) Dey, N., Ghosh, M., & Chakrabarti, A. Quantum solutions to possible challenges of Blockchain technology. In *Quantum and Blockchain for Modern Computing Systems: Vision and Advancements* (pp. 249-282). Springer, Cham.
37) Raheman, Fazal, et al. "Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis." *Future Internet* 14.8 (2022): 238.
38) Raheman, Fazal. "The Future of Cybersecurity in the Age of Quantum Computers." *Future Internet* 14.11 (2022): 335.
39) Computer Security Research Center. Post Quantum Cryptography PQC: Workshops and Timeline. NIST, July 7, 2022. Available at https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline (accessed on Aug 8, 2022).
40) Raheman Fazal. The Q-Day Dilemma and the Quantum Supremacy/Advantage Conjecture, 09 December 2022, PREPRINT (Version 1) available at Research Square [https://doi.org/10.21203/rs.3.rs-2331935/v1]
41) Adamik, Filip, and Sokol Kosta. "Smartexchange: Decentralised trustless cryptocurrency exchange." *International Conference on Business Information Systems*. Springer, Cham, 2018.
42) Lin, Lindsay X. "Deconstructing decentralized exchanges." *Stan. J. Blockchain L. & Pol'y* 2 (2019): 58.
43) Zamyatin, A.; Harz, D.; Lind, J.; Panayiotou, P.; Gervais, A.; Knottenbelt, W. XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 193–210
44) Lee, Sung-Shine, et al (2022). "SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks." *arXiv preprint arXiv:2210.16209* (2022).

45) Helal, Maha, Anas Ratib Alsoud, and Hazzaa Alshareef. "Cross-Chain Interoperability-Validating Smart Contracts to Interoperate Over Diverse Blockchain Networks Using Interoperable Blockchain Framework Design (IBFD)." 2022. https://doi.org/10.21203/rs.3.rs-2217138/v1

46) Brooks, Khristopher. Hackers have stolen record $3 billion in cryptocurrency this year. CBS News, Oct 12, 2022. Available https://www.cbsnews.com/news/cryptocurrency-theft-hacker-chainalysis-blockchain-crime/ (accessed on Dec 1, 2022)

47) D.J. Bernstein and T. Lange (2017). Post-quantum cryptography. Nature, 549(7671):188–194, 2017.

48) Gupta, Kishor Datta, et al (2021). "Utilizing Computational Complexity to Protect Cryptocurrency Against Quantum Threats: A Review." *IT Professional* 23.5 (2021): 50-55.

49) Marcos, A. et al (2021). "Quantum-resistance in blockchain networks." *arXiv preprint arXiv:2106.06640* (2021).

50) Zhu, Dexin, et al (2022). "A hybrid encryption scheme for quantum secure video conferencing combined with blockchain." *Mathematics* 10.17 (2022): 3037.

51) 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 30 August 2022).

52) Banerjee, Utsav, Siddharth Das, and Anantha P. Chandrakasan. "Accelerating post-quantum cryptography using an energy-efficient tls crypto-processor." *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2020.

53) Jain, Aji, Aravind, Kurunandan Jain, and Prabhakar Krishnan. "A Survey of Quantum Key Distribution (QKD) Network Simulation Platforms." *2021 2nd Global Conference for Advancement in Technology (GCAT)*. IEEE, 2021.

54) Rimba P, et al. "Comparing blockchain and cloud services for business process execution." *2017 IEEE international conference on software architecture (ICSA)*. IEEE, 2017.

55) Arikpo, I.I.; Ogban, F.U.; Eteng, I.E. Von Neumann architecture and modern computers. *Glob. J. Math. Sci.* 2007, *6*, 97–103.

56) 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.

57) Rajput, Balsing. "Changing Landscape of Crime in Cyberspace." *Cyber Economic Crime in India*. Springer, Cham, 2020. 13-23.

58) 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.

59) Kumar, Manish. "Post-Quantum Cryptography Algorithms Standardization and Performance Analysis." *arXiv preprint arXiv:2204.02571* (2022).