Future-Proofing Blockchain & Cryptocurrencies Against Growing Vulnerabilities & Q-Day Threat with Quantum-safe Ledger Technology (QLT)

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

Abstract: Blockchain/DLT is projected to be a $3 trillion industry by 2030, although cryptocurrency market cap already crossed $3 trillion in 2021. With one billion users using 380 exchanges, 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 stolen in 2022. Cryptocurrency hacks negatively impact cryptocurrency markets introducing volatility. Each major scam/hack incident results in 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 not only secures DLTs/cryptocurrencies and exchanges from current vulnerabilities but protects it from the impending Q-day threats from future quantum computers. As blockchain-agnostic technology, QLT can be easily adopted 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 was first introduced in 2008 by Satoshi Nakamoto (Nakamoto, 2008) as a peer-to-peer electronic cash system or cryptocurrency called bitcoin. Blockchain and cryptocurrency are inseparably linked. As much as a decentralized form of money simply cannot exist without the security provided to it by blockchain, a public blockchain cannot be created without giving people incentives to create it (van Haaren, et al., 2022). 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 (Buterin, et al., 2013) and its commercial launch as Ethereum blockchain in 2015 (Arslanian, 2022) further revolutionized the blockchain technology. It has since drawn broad attention from academia and industry alike. A growing body of literature envisions how its decentralized approach can disrupt current business models, financial systems, organizations, and civic governance (Efanov & Roschin, 2018).

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 (McGovern, 2022). There are over 1,000 blockchains and 245 NFT marketplaces in the world (Bhuel & Rahulamathavan, 2022). In November 2021, cryptocurrency market cap reached all time high of $3 trillion, and achieved it faster than any other industry in the history, in just about a dozen years. Projected to be a $3 trillion industry (Horch, et al., 2022), 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. Present public-key infrastructure (PKI) that blockchain deploys depend 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 the creation and encryption of blockchain wallets. When creating a cryptocurrency wallet, a public address and a private key are generated. Shor's quantum algorithm can solve the integer factorization problem in polynomial time and break PKI (Edwards, 2021). The exponential growth in quantum computing has opened the possibility of performing attacks based on Shor's algorithms and Grover's algorithms that threaten the PKI and hash functions in the near future (Fernandez-Carames & Fraga-Lamas, 2020). Therefore, it has become necessary for the development of a post-quantum secure signature scheme or quantum-resistant blockchain for post-quantum blockchain security.

2. Problem Statement

Hailed as a panacea for economic growth and sustainability (Shin & Rice, 2022), blockchain's envisioned omnipresence in human computer interactions so far lags (Fröhlich, et al., 2022). 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 (Nzimakwe, 2018), 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.

2.1 Perpetual scams & hack attacks on cryptocurrencies

Since the launch of bitcoin as a cryptocurrency, the blockchain / cryptocurrency industry is blemished with countless crypto scams and hacks over the years estimated to be as high as $88 billion (Charoenwong & Bernardi, 2021) 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 (Mackenzie, 2022 and O'Rourke, 2022). The year 2022 turned out to be the worst year for crypto thieves with the biggest loss $3 billion reported in October 2022 by Money Control (Merchant, 2022) followed by two biggest exchanges, Binance (Ephrat, 2022) and FTX (Tobi, 2022) reporting $570 and $600 million respectively lost to hack attacks totaling $1.17 billion in losses in just a single month. Another billion dollar was reported lost to hacking attacks by Chainalysis in August 2022 (Chainalysis Team, 2022). Cryptocurrency hacking incidents affect the cryptocurrency market introducing volatility, which increases significantly both contemporaneously and as a delayed effect (Grobys, 2021). Each major hack results in significant price dip for bitcoin and all major cryptocurrencies (Chang, 2019). Frequent hacking incidents are detrimental to the growth of the blockchain economy (Groopman, 200?). Securing blockchain against hackers remains the top priority for this potentially multi-trillion industry (Boireau, 2018).

The challenge is further amplified by the advent of quantum computers, which are feared to present an existential threat to the encryption dependent Internet protocols and to the blockchain networks (Kearney & Perez-Delgado, 2021). Several research groups are exploring PQC for developing quantum-resistant blockchain (Unogwu, et al, 2021). Even the questions of impending end of blockchain are raised (Kappert, et al, 2021).

2.2 The Q-Day threat to blockchain

Two recent articles in Nature journals emphasize the seriousness of the impending threats from quantum computers to the Internet (Castelvecchi, 2022), and an actual quantum attack on several cryptocurrencies that lead to the latest crypto crash of 2022 (Rozell, 2022). Theoretically, all cryptographic algorithms are vulnerable to quantum attacks. Given the ubiquity of cryptographic schemes in our everyday online activities, this could be catastrophic (Majot and Yampolskiy). Already overwhelmed with ever increasing scourge of hack attacks, blockchain appears to be moving closer to the cryptography apocalypse threat from quantum computers (Grimes, 2019). Q-day is when quantum computers will break the Internet (Majot and Yampolskiy). McKinsey predicts that the first-wave industries may start to significantly benefit from quantum computers as early as 2025 (Ménard, et al., 2020). There is an urgent need to counter the looming Q-Day threat as quantum algorithms already exist for all major public-key cryptosystems, and it is only a matter of time before they are completely broken. It is of serious concern that many of the algorithms that have been cracked during the NIST (National Institute of Standards and Technology) tests are still in commercial use. For example, Rainbow is deployed by the ABCmint cryptocurrency (Ding, 2019). The fact that so many post-quantum encryption methods have been cracked and none has stood the rigors of the NIST testing reveals that it is time to explore alternate cybersecurity strategies.

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 (Raheman, et al., 2022) beyond the minimalist hardware wallet client device. 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 (Raheman, et al.,

2022). More recently, ZVC was explored (Raheman, 2022a) as an alternative to PQC (Post Quantum Cryptography) candidate algorithms that entered NIST's (National Institute of Standards in Technology) PQC standardization process initiated in 2017 (Computer Security Research Center, 2022). Five years into the standardization process, 80 of the 82 candidate PQCs failed (Sparkes, 2022) 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 (Raheman, 2022a & Raheman, 2022b). This paper explores a strategy similar to the QaaS architecture to secure DLT / blockchain 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 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.

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 3rd party permissions that all hardware and software are designed to grant 3rd party vendors and developers of computer applications (Raheman, et al., 2022), while second category is an upshot of the impending threats from future quantum computers (Raheman, 2022a & Raheman, 2022b). In this paper the QLT solution proposes a new paradigm in tackling each of those vulnerabilities to render blockchain / cryptocurrencies virtually unhackable. A review of the state-of-the-art therefore warrants a two-fold inquiry.

4.1 Crypto exchange vulnerabilities

In contrast to 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 retain 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 (Adamik & Sokol, 2018). On the contrary, in decentralized exchange the user assets remained in the custody of the user (Lin, 2019). Hence, theoretically, the decentralized exchanges apparently evolved as more secure platforms than the centralized exchanges. However, with the advent 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 (Zamyatin, 2019). 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 (Lee, 2022). This made the bridge custodian become the target (Chainalaysis Team, 2022) rendering decentralized exchanges vulnerable (Helal, 2022).

As reasons therefore cryptocurrency exchanges, whether centralized or decentralized with cross-chain bridging, remain vulnerable to hack attacks. In fact, more than ever. In October 2022 CBS News reported $3 billion stolen from several exchanges (Brooks, 2022), shattering the previous record of $2.1 billion set in 2021. The last quarter of 2022 saw two biggest exchanges, Binance (Ephrat, 2022) and FTX (Tobi, 2022) report $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 (Chainalysis Team, 2022). While the FTX hack happened as cybersecurity breach of the custodial assets in a centralized exchange, the Binance hack was a cross-chain exploit.

4.2 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 (Bernstein & Lange, 2017). Cryptocurrencies (Gupta, et al., 2021) 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 (Kearney & Perez-Delgado, 2021).

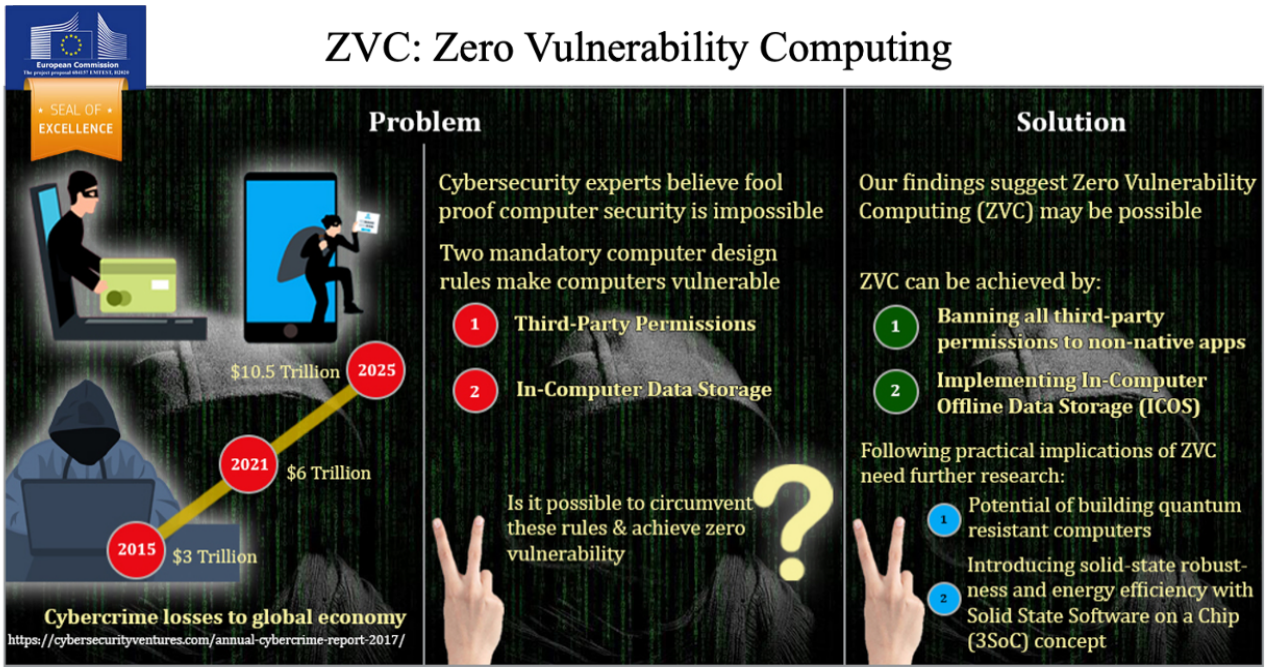
Many reports on quantum-safe blockchain have appeared in peer reviewed literature (Fernandez-Carames & Fraga-Lamas, 2020). Marcos, et al (2021), deployed PQC as a layer 2 solution to make blockchains quantum resistant. Zhu et al (2022) recently proposed a hybrid encryption scheme for quantum secure video conferencing combined with blockchain. However, with over 90% of PQC candidates failing NIST's standardization process, Quantum computers appear to be more detrimental to human interests than the benefits they deliver (Laura, 2022). In fact, one of the recent cryptocurrency crashes was because of actual quantum attack on several cryptocurrencies (Rozell, 2022). Moreover, PQC algorithms are computationally expensive (Banerjee, et al., 2020 & Jain, et al., 2021)) and will add to the already high cost 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 (Rimba, et al., 2017). Attempts at making blockchain resilient with PQC primitives will further escalate the already exorbitant blockchain transaction costs.

5. Beyond state-of-the-art

All state-of-the-art computing systems, whether based on the von Neumann architecture (Arikpo, et al 2007) or the Harvard architecture (Francillon & Castelluccia, 2008) are designed to grant 3rd party permissions to the software applications developed by programmers and software vendors. 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 which keeps growing and can never be eliminated (Rajput, 2020). 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 (Raheman, et al., 2022). Such a system of Zero Vulnerability Computing (ZVC) did not rely on cryptography for securing the computers. Because ZVC was encryption agnostic, 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. Seal of Excellence winning ZVC Technology (Raheman, et al 2022)

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. While several European Consortia continue to investigate ZVC in diverse use case scenarios, a recent report explored the ZVC hypotheses for quantum resilient cybersecurity (Raheman, 2022a). As the full scope and relevance of ZVC to overall cybersecurity of Internet remains 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 that was 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 as well. (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 Quantum-as-a-Service (QaaS) business model (Raheman, 2022a).

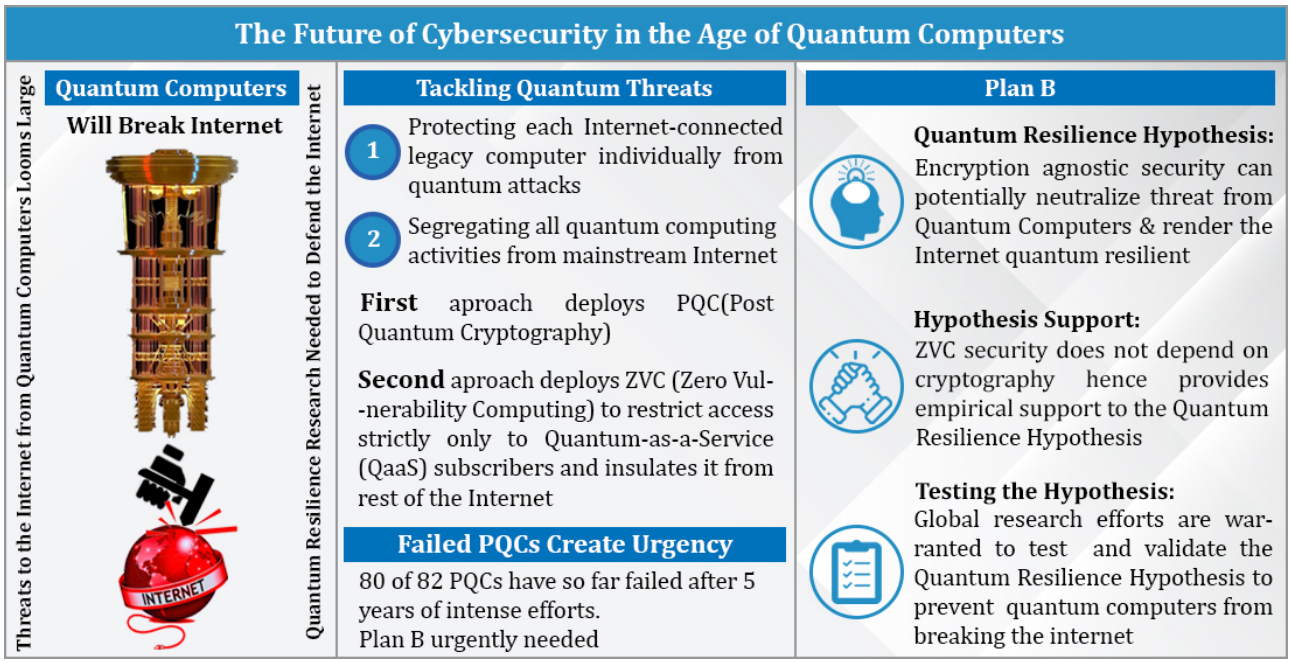


Fig. 2: Quantum Cybersecurity Graphical Abstract- Raheman. (2022a). *Future Internet* 2022, *14*(11), 335

Just as ZVC framework provides zero vulnerability and zero attack surface quantum resilient environment for the exchange of 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 that was recently disclosed for quantum-proofing the Internet (Raheman, 2020a). While the QaaS framework was a routing service, the QLT architecture proposed in this paper deploys the blockchain / cryptocurrency infrastructure directly on the ZVC's Solid State Software on a Chip (3SoC) servers (Raheman, 2020b & Raheman 2020c). 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 first phase (Raheman et al., 2022), and the second phase builds the quantum-resistant server currently been taken up by a consortium constituted under Horizon Europe program (Raheman, 2022a & 2022b).

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 is provided with a switchable 3SoC drive with QLT user interface that securely connects to the blockchain nodes installed on 3SoC remote servers as QLT nodes creating a secure 3SoC tunnel. 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 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 quantum computer can penetrate the zero attack surface, encryption agnostic security of the QLT framework

operating as an Intranet. Thus, a ZVC/3Soc powered QLT intranet can potentially offer defense against misuse of quantum computing against blockchain by bad actors. QLT framework provides freedom from the impending threats from quantum computers even if the PQC algorithms that are currently under 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 (Kumar, 2022) and come with significantly higher costs.

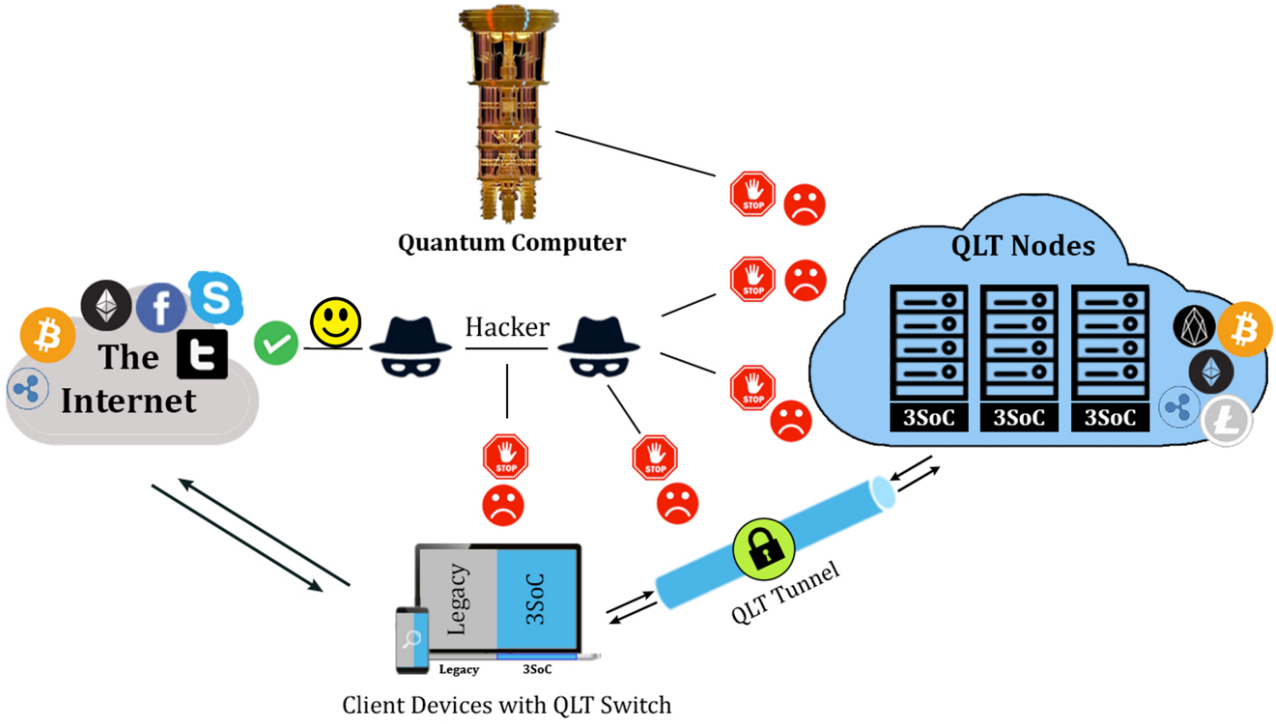


Fig. 3. Switchable QLT framework for quantum-proofing blockchain infrastructure

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

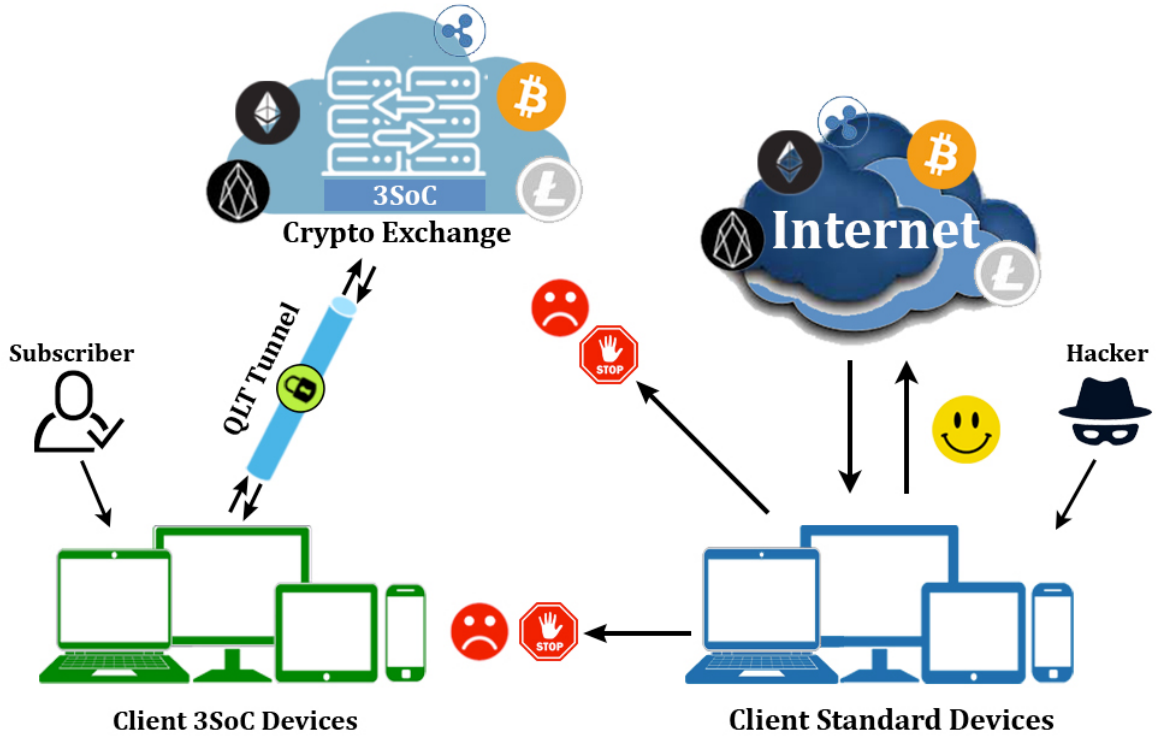


Fig. 3. A hack-proof crypto exchange (HEX) rendered unbreachable with 3SoC powered QLT framework

Although termed as quantum-safe ledger technology, QLT is equally effective in protecting blockchain and crypto exchanges from the traditional hacking attacks. This is particularly important in hack-proofing crypto exchanges (HEX) hundreds of crypto exchanges out there that remain vulnerable to hack attacks. As illustrated in Fig. 4, a novel QLT architecture for a 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 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 entire framework components comprising of 3SoC client, tunnel and the exchange server are encryption agnostic with banned 3rd party permissions with 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 or a custodial cross-chain bridge or an NFT marketplace.

6. Study Limitations

This paper provides theoretical support to the deployment of a new cybersecurity paradigm that was originally tested in a minimalist hardware wallet device (Raheman, 2022) 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, in particular. As any hypothesis-generating research demands, great care is warranted in projecting the conclusions of this report to real-world scenarios for the following reasons:

(i) The QLT architecture is designed based on empirical data from a series of minimalist hardware wallet experiments (Raheman, et al., 2022), and need to be validated in diverse blockchain ecosystems before any extrapolation 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 blockchains.
(iv) Notably, 3SoC devices inherently restrict the porting of generic or non-conforming third-party peripheral devices (Raheman 2022c).
(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.
(vi) 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, NFT Marketplaces and rendering them resistant to the 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.

7. Conclusion and future prospects

One billion users, 20,000 cryptocurrencies, over 1,000 blockchains, 380 crypto exchanges and 245 NFT marketplaces (McGovern, 2022), remain vulnerable to hackers and scammers. This has resulted in as much as $88 billion lost to thefts over a dozen years that blockchain has existed (Charoenwong, & Bernardi, 2021). The torment of blockchain/cryptocurrency vulnerabilities continues, and in fact 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, or 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 steel 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 so many post-quantum encryption methods have been cracked so far, 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, currently 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 the access to 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 potentially 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, any cryptocurrency exchange or any 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.
5. QLT business model makes it easier to regulate the blockchain economy, both technologically and legally as compared to the legacy systems.
6. Like the QLT framework described in this paper and the QaaS framework disclosed previously (Raheman, 2022c), the ZVC/3SoC architecture can be adapted to secure any online activity.

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

Declarations

Conflict of interest: The author declares no conflict of interest.

References

Adamik, Filip, and Sokol Kosta (2018). "Smartexchange: Decentralised trustless cryptocurrency exchange." *International Conference on Business Information Systems*. Springer, Cham, 2018.

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

Arslanian, Henri (2022). "Ethereum." *The Book of Crypto*. Palgrave Macmillan, Cham, 2022. 91-98.

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

Bavdekar, Ritik, et al. (2022). "Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research." *arXiv preprint arXiv:2202.02826* (2022).

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

Bhujel, S., & Rahulamathavan, Y. (2022). A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces. *Sensors*, *22*(22), 8833.

Boireau, Olivier (2018). "Securing the blockchain against hackers." *Network Security* 2018.1 (2018): 8-11.

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)

Buterin Vitalik (2013). Ethereum white paper. GitHub repository 1 (2013), 22–23

Castelvecchi D (2022). *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.

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).

Chang, Samanta (2019). 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/ (accessed on December 5, 2022).

Charoenwong, Ben and Bernardi, Mario (2021). 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

Computer Security Research Center (2022). 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).

Ding, J.A. (2019). 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.

Edwards, N., Haynes, J. B., & 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*(1), 136-138.

Efanov, D &Roschin, P. (2018). The all-pervasiveness of the blockchain technology. Procedia Computer Science 123 (2018), 116–121. https://doi.org/10. 1016/j.procs.2018.01.019

Ephrat Livni (2022). 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 (accessed on December 5, 2022).

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, *8*, 21091-21116.

Francillon, A.; Castelluccia, C (2008). 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.

Fröhlich, Michael, et al (2022). "Blockchain and Cryptocurrency in Human Computer Interaction: A Systematic Literature Review and Research Agenda." *arXiv preprint arXiv:2204.10857* (2022).

Grimes, Roger A. (2019). *Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto*. John Wiley & Sons, 2019.

Grobys, Klaus (2021). "When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market." *Quantitative Finance* 21.8 (2021): 1267-1279.

Groopman, Jessica (20-?). Top blockchain security attacks, hacks and issues. TechTarget.com. Available at https://www.techtarget.com/searchsecurity/tip/Top-blockchain-security-attacks-hacks-and-issues (accessed on December 5, 2022).

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

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

Horch A, Schunck C H., and Ruff C. (2022). "*Adversary Tactics and Techniques specific to Cryptocurrency Scams.*" *Open Identity Summit 2022*. Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022, 119 doi:18.18420/OID2022-10

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

Kappert, Noah, Erik Karger, and Marko Kureljusic (2021). "Quantum Computing-The Impending End for the Blockchain?." *Pacific Asia Conference on Information Systems (PACIS), Dubai, UAE*. 2021.

Kearney, Joseph J., and Carlos A. Perez-Delgado (2021). "Vulnerability of blockchain technologies to quantum attacks." *Array* 10 (2021): 100065.

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

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).

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).

Lin, Lindsay X.(2019). "Deconstructing decentralized exchanges." *Stan. J. Blockchain L. & Pol'y* 2 (2019): 58.

MacKenzie Sigalos (2022). 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).

Majot and Yampolskiy (2015). Global catastrophic risk and security implications of quantum computers. Futures. Volume 72, September 2015, Pages 17-26m

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

McGovern, Thomas (2022). CRYPTOCURRENCY STATISTICS 2022: HOW MANY PEOPLE USE CRYPTO? EARTHWEB, Dec 3, 2022. Available at https://earthweb.com/cryptocurrency-statistics/ (accessed Dec 8, 2022).

Merchant, Murtuza (2022). 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).

Ménard, A.; Ostojic, I.; Patel, M.; Volz, D. (2020). 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).

Nakamoto, Satoshi (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review (2008), 21260.

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.

O'Rourke, Morgan (2022). "CRYPTOCURRENCY CRIME COSTA RECORD $14 BILLION IN 2021." *Risk Management* 69.1 (2022): 30-30.

Raheman, Fazal, et al. (2022). "Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis." *Future Internet* 14.8 (2022): 238.

Raheman, Fazal (2022a). "The Future of Cybersecurity in the Age of Quantum Computers." *Future Internet* 14.11 (2022): 335.

Raheman Fazal (2022b). 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]

Raheman, F (2022c). 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.

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

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

Rozell DJ. (2022). *Cash is king.* Nature. 2022 Feb 16. doi: 10.1038/d41586-02

Shin, Donghee, and John Rice (2022). "Cryptocurrency: A Panacea for Economic Growth and Sustainability? A Critical Review of Crypto Innovation." *Telematics and Informatics* (2022): 101830.

Sparkes, Mathew (2022). 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/ (accessed on 8 Dec 2022)

Tobi Opeyemi Amure (2022). 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 (accessed on December 5, 2022).

Unogwu, Omega John, et al. (2022). "Introduction to Quantum-Resistant Blockchain." *Advancements in Quantum Blockchain With Real-Time Applications*. IGI Global, 2022. 36-55.

van Haaren Duijn, B, et al. (2022). "The dynamics of governing enterprise blockchain ecosystems." *Administrative Sciences* 12.3 (2022): 86.

Zamyatin, A.; Harz, D.; Lind, J.; Panayiotou, P.; Gervais, A.; Knottenbelt, W. (2019). 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

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