Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA) for Web 3.0 Security in the Post-Quantum Era

Ali Raheman
[0000-0002-0817-1176]
Magpie Markets Limited
P.O. Box 4301, Road Town,
Tortola, VG1110, British
Virgin Islands
Ali@magpiefi.xyz

Tejas Bhagat
[0000-0001-7364-6361]
Qloud Technologies
Ahtri 12-512, E-10151 Tallinn,
Estonia
tejas@bc5.eu

Fazal Raheman
[0000-0002-7766-6949]
Qloud Technologies
Ahtri 12-512, E-10151 Tallinn,
Estonia
drfazal@bc5.eu

ABSTRACT

The arrival of quantum computing (QC) is no longer a hypothetical concept. Google claims its new quantum computer is 241 million times faster than the one released in 2019, while the Chinese Zuchongzhi-3 claims to have achieved speeds trillions of times faster. The encryption-breaking speeds of QC will render our existing encryption obsolete within 5–10 years, presenting a catastrophic threat to our cryptography-dependent, ubiquitous digital infrastructure. Unless our digital infrastructure is secured from quantum threats, QC cannot become mainstream. In 2016-17, the National Institute of Standards and Technology (NIST) initiated a post-quantum cryptography (PQC) initiative; however, so far, it has failed to produce a stable standard, as all of the top 82 candidates have already been compromised. Moreover, PQC is expensive and too resource-intensive with latency issues, particularly in the $3 Trillion Crypto/blockchain economy that entirely relies on user-facing cryptography. In an earlier study, we disclosed Quantum-Safe Quantum Ledger Technology (QLT), a blockchain-agnostic framework for securing cryptocurrencies and blockchains from Q-Day threats. In this presentation, we discuss a Quantum Resilient user Evasive Cryptographic Authentication (QRUECA) protocol that secures QLT by replacing traditional user-facing PKI-based methods. QRUECA authorizes access through a multi-gate cryptographically sealed device-to-device handshake, thereby eliminating the need for the traditional user-facing cryptography. Because Gate 1 of the QRUECA process uses no user-facing cryptography, and Gate 2 is only activated by authenticated devices, the entire protocol becomes inherently resistant to threats from QC. Beyond blockchain, the QUERCA protocol can be applied to any Web 3.0 use case. Thus, QRUECA addresses a significant hurdle in the mainstream introduction of QC. Just as an automobile cannot exist without a braking system, quantum computers cannot exist without securing our life-sustaining digital infrastructure.

Keywords

Quantum-Resilient Authentication, Post-Quantum Cryptography (PQC), Quantum Ledger Technology (QLT), Zero Vulnerability Computing (ZVC)

1. INTRODUCTION

The advent of quantum computing (QC) represents a paradigm shift with profound implications for digital security. No longer confined to theoretical physics, quantum computers are demonstrating exponential increases in computational power [Car25a], with recent claims of speeds trillions of times faster than conventional supercomputers [Gao25a]. This unparalleled processing capability poses an existential threat to the vast majority of our modern digital infrastructure, which relies heavily on cryptographic primitives like RSA and Elliptic Curve Cryptography (ECC) for data confidentiality, integrity, and authentication [Maj15a]. These algorithms, while robust against classical computers, are fundamentally vulnerable to quantum algorithms such as Shor's algorithm for factoring large numbers and Grover's

algorithm for searching unsorted databases. Experts predict that within the next 5-10 years, a sufficiently powerful quantum computer, often referred to as "Q-Day," could render current encryption standards obsolete, leading to a catastrophic compromise of sensitive data, financial transactions, and critical infrastructure [Maj15a].

In response to this impending threat, the National Institute of Standards and Technology (NIST) launched a comprehensive post-quantum cryptography (PQC) standardization initiative in 2016-2017. The goal was to identify and standardize cryptographic algorithms believed to be secure against attacks from large-scale quantum computers. However, the journey has been fraught with challenges. Many of the initial PQC candidates have been subsequently compromised, highlighting the inherent complexity and ongoing fragility of developing new, quantum-resistant cryptographic schemes [Lav24a]. Furthermore, PQC protocols often come with significant computational overhead, larger key sizes, and increased latency, making them less suitable for resource-constrained environments or high-throughput applications, particularly within the burgeoning $3 trillion cryptocurrency and blockchain economy, which is entirely reliant on user-facing cryptography [Rah24a].

This paper introduces a novel approach to securing digital infrastructure against quantum threats, moving beyond the limitations of current PQC efforts. We delve into Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA), a protocol designed to safeguard Web 3.0 security. QRUECA is intrinsically linked to Quantum Ledger Technology (QLT), a blockchain-agnostic framework previously introduced for securing cryptocurrencies and blockchains from Q-Day threats (Raheman, 2024). The core innovation of QRUECA lies in its departure from traditional user-facing cryptographic authentication methods. Instead, it employs a multi-gate, cryptographically sealed device-to-device handshake, thereby eliminating the attack surface exposed by conventional user-facing cryptography. This design choice, coupled with its foundation on Zero Vulnerability Computing (ZVC) and Solid-State Software on a Chip (3SoC) architecture, provides inherent resilience to quantum attacks.

The remainder of this paper is structured as follows: Section 2 elaborates on the quantum threat and the shortcomings of existing mitigation strategies. Section 3 introduces Quantum Ledger Technology (QLT) and its foundational architectural components, ZVC and 3SoC. Section 4 provides a detailed exposition of the QRUECA protocol, explaining its multi-gate authentication process and its user-evasive nature. Section 5 discusses the operational benefits of QRUECA and its broad applicability across various Web 3.0 use cases. Finally, Section 6 concludes the paper and outlines future research directions.

2. THE QUANTUM THREAT AND LIMITATIONS OF CURRENT APPROACHES

The security of modern digital communications and data storage hinges on the computational intractability of certain mathematical problems. Public-key cryptography, foundational to secure online interactions, relies on the difficulty of factoring large numbers (RSA) or solving discrete logarithms on elliptic curves (ECC). Symmetric-key cryptography, used for bulk data encryption, derives its strength from the vastness of its key space, making brute-force attacks computationally infeasible. Quantum computers, however, leverage principles of quantum mechanics—superposition and entanglement—to perform computations in fundamentally different ways, undermining these cryptographic assumptions.

Shor's algorithm, first proposed in 1994, demonstrates that a sufficiently powerful quantum computer can efficiently factor large integers and compute discrete logarithms. This directly threatens the security of widely deployed public-key algorithms like RSA, DSA, and ECC, which are integral to digital signatures, secure key exchange (e.g., Diffie-Hellman and Public Key Infrastructure (PKI). A quantum computer running Shor's algorithm could break current public-key encryption in minutes, compromising encrypted communications, digital certificates, and authenticated transactions [Ugw20a]. Similarly, Grover's algorithm offers a quadratic speedup for searching unsorted databases [Yua24a]. While it doesn't break symmetric-key algorithms outright, it effectively halves the security strength, meaning a 256-bit key would only offer 128 bits of security against a quantum adversary, potentially necessitating much larger key sizes to maintain current security levels.

The global response to this impending "Q-Day" has primarily centered on Post-Quantum Cryptography (PQC). NIST's PQC standardization process, initiated in 2016, aimed to solicit, evaluate, and standardize new cryptographic algorithms robust against quantum attacks [Che16a]. These algorithms typically fall into categories such as lattice-based, code-based, hash-based, and multivariate polynomial cryptography.

While significant progress has been made, the journey has been marked by repeated setbacks. As recent as 2024, it was reported that top PQC candidates have been compromised [Lav24a], demonstrating the inherent difficulty in designing and validating truly quantum-resistant primitives. This continuous cycle of development, vulnerability discovery, and revision highlights the immaturity and instability of the current PQC landscape.

Beyond the technical challenges of cryptographic design, PQC algorithms often present practical hurdles. They generally involve larger key sizes, increased computational requirements, and higher latency compared to their pre-quantum counterparts. These characteristics pose significant challenges for adoption, particularly in resource-constrained environments like Internet of Things (IoT) devices, or in performance-critical applications like blockchain networks, where efficiency and low latency are paramount. The blockchain ecosystem, with its reliance on cryptographic hashing, digital signatures for transaction validation, and decentralized trust mechanisms, is particularly vulnerable. User-facing cryptographic operations, such as signing transactions with private keys, present a clear attack surface that existing PQC solutions struggle to efficiently and effectively secure without introducing considerable overhead. The very nature of many blockchain applications, which are built upon user-initiated cryptographic actions, exposes their vulnerability to quantum adversaries who can intercept and decrypt keys or transactions. Therefore, a fundamentally different approach is required that can offer immediate quantum resilience without relying on the still-evolving and resource-intensive PQC standards.

3. QUANTUM LEDGER TECHNOLOGY (QLT): AN ARCHITECTURAL RESPONSE TO QUANTUM THREATS

Recognizing the limitations of reactive cryptographic upgrades, Quantum Ledger Technology (QLT) emerges as a proactive, architectural solution to secure digital assets and infrastructure from the quantum threat. QLT is conceived as a blockchain-agnostic framework, providing a robust security layer for various distributed ledger technologies (DLTs) and cryptocurrencies [Rah24a]. Unlike piecemeal cryptographic updates, QLT addresses the root causes of systemic vulnerability by fundamentally rethinking system architecture at its deepest levels. This is achieved through the integration of two proprietary, foundational technologies: Zero Vulnerability Computing (ZVC) and the Solid-State Software on a Chip (3SoC) hardware model.

3.1 Zero Vulnerability Computing (ZVC) and 3SoC Architecture

At the heart of QLT's inherent security lies Zero Vulnerability Computing (ZVC). ZVC is a revolutionary computational paradigm that directly addresses one of the most pervasive sources of cyberattacks: unauthorized software execution and the proliferation of Third-Party Permissions (TPPs) [Rah22a]. By design, ZVC explicitly bans all TPPs, meaning that no external or unauthorized software, libraries, drivers, or runtime code can execute on a ZVC-enabled system. This architectural constraint eliminates the vast majority of attack vectors, including malware injection, supply chain attacks, and exploits leveraging vulnerabilities in third-party components. The result is a truly "zero attack surface" infrastructure, where the system's operational integrity is guaranteed by preventing any deviation from its pre-approved, immutable software stack.

The practical realization of ZVC is intrinsically tied to the proprietary hardware model, Solid-State Software on a Chip (3SoC). 3SoC represents a fundamental shift from traditional software deployment to a hardware-enforced, immutable execution environment [Rah22b]. In a 3SoC device, the critical software components and cryptographic routines, are loaded from a storage medium that has zero TPPs to write. Thus, they run from a hardware that is non-modifiable by third parties remaining in a solid-state format. This architecture provides an unparalleled level of security and integrity:

- **Immutability:** The embedded software cannot be altered, overwritten, or tampered with once provisioned, effectively preventing rootkits, persistent malware, and unauthorized code injection.
- **Tamper Resistance:** The physical nature of the 3SoC makes it significantly more difficult for adversaries to physically access or manipulate the core software and cryptographic keys.
- **Secure Boot:** The system inherently boots into a known, secure state, bypassing typical attack points that exploit mutable boot processes.
- **Elimination of Vulnerabilities:** By tightly integrating software and hardware, and removing the ability to load arbitrary code, 3SoC systems dramatically reduce the potential for software vulnerabilities that can be exploited for privilege escalation or remote code execution.

The synergy between ZVC and 3SoC is critical. ZVC defines the protocol of banning TPPs and achieving a zero attack surface, while 3SoC provides the secure, immutable hardware platform necessary to enforce this

protocol. Together, they create an environment where the integrity of computations and data is guaranteed at the architectural level, providing a foundational layer of security that is inherently resistant to both classical and emerging quantum threats, as the very avenues for attack (e.g., software vulnerabilities, code injection) are eliminated.

4. THE QUANTUM-RESILIENT USER-EVASIVE CRYPTOGRAPHIC AUTHENTICATION (QRUECA) PROTOCOL

Building upon the robust foundation of QLT's ZVC and 3SoC architecture, Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA) introduces a revolutionary paradigm for secure access, specifically designed to withstand the quantum threat [Rah24b]. Traditional authentication mechanisms, predominantly relying on Public Key Infrastructure (PKI) and user-facing cryptographic operations (e.g., entering passwords, biometric scans, or signing transactions with user-controlled private keys), inherently expose an attack surface. QRUECA fundamentally alters this dynamic by shifting the primary authentication burden from the user-entered credentials to a secure, concealed device-to-device handshake.

4.1 Paradigm Shift: Device-to-Device Handshake vs. User-Initiated Authentication

In legacy systems, the authentication handshake is typically initiated and controlled by the user. This involves the user providing credentials (e.g., username/password), possessing a device (e.g., for 2FA codes), or presenting biometric data. All these methods are inherently visible and usable by an adversary. In contrast, QRUECA implements a "user-evasive" approach where the initial authentication process is orchestrated and executed entirely between trusted computing devices, without direct user intervention or exposure of cryptographic prompts or keys. This architectural choice is central to its quantum resilience.

4.2 Gate 1: The Concealed Device-to-Device Handshake

The first and most critical phase of the QRUECA protocol is Gate 1: a completely concealed device-to-device handshake. This gate operates at the hardware level, rendering it inaccessible to the user's discretion and, crucially, to quantum adversaries. This handshake is facilitated by a unique component: the **QRUECA Crypto Certificate (QCC)**.

The QCC is not a traditional software certificate; it is securely embedded within authorized QLT devices (e.g., a 3SoC client device attempting to access a 3SoC server). The QCC provides a pair of private and public keys. However, unlike conventional PKI, these keys are used exclusively for a hardware-level, device-to-device handshake inaccessible to user-dependent credentials (see **Fig.1**). The process unfolds as follows:

1. An authorized QLT device (client) initiates a connection to a QLT-enabled server.

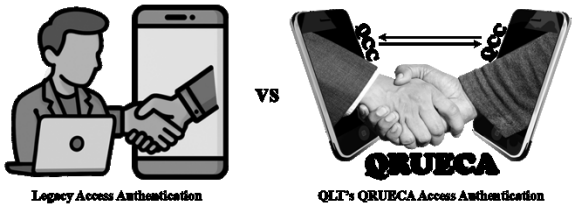

Figure 1. Legacy VS QRUECA Access Authentication

2. The devices engage in a cryptographic handshake using the private and public keys provisioned by their embedded QCCs. This exchange happens entirely within the secure hardware environment, abstracted away from the user interface and the traditional software stack.
3. Because this handshake occurs at the hardware level and does not expose cryptographic prompts, key material, or user-visible challenge-response interactions, quantum adversaries have no available surface to attack. They cannot intercept the challenge, perform Shor's algorithm on an exposed public key, or attempt to brute-force a password or passphrase. The cryptographic operations are sealed within the secure hardware, making the "user-evasive" aspect synonymous with "quantum-resilience" (see **Fig. 1**).

4.3 Gate 2: Continued Access Authorization

Only after a successful Gate 1 handshake, signaling that the requesting device is a legitimate, authorized QLT entity, does the system proceed to a second cryptographic gate. A key feature of Gate 1 of the QRUECA protocol is its **strictly non-retry** mechanism. Such a **zero-retry timeout (ZRTO)** protocol ensures that a failed device-to-device handshake is not repeated. In Gate 2, access authorization continues, but critically,

it does so without exposing any reusable credentials to quantum computers. This means that even if an adversary were to compromise the session *after* Gate 1, they would not obtain any static, replayable, or decryptable credentials that could be used for future unauthorized access. This immediate termination of connection attempts at Gate 1 effectively blocks brute-force attacks, denial-of-service attempts by repeatedly guessing, and replay attacks, where captured legitimate handshakes are re-transmitted. This design choice dramatically reduces the window of opportunity for any potential adversary, classical or quantum.

4.4 The 4-Factor Authentication (4FA) Model

As illustrated in **Fig. 2**, QRUECA replaces the

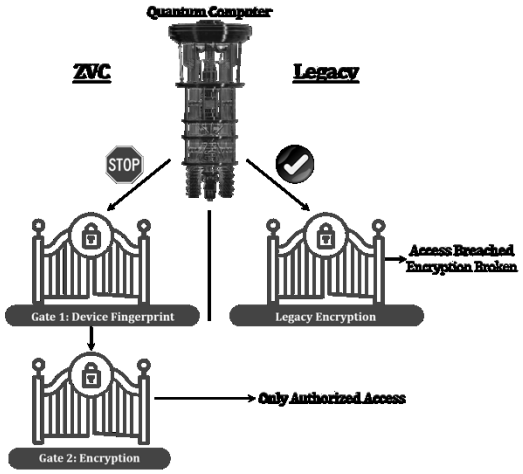

Figure 2. QRUECA's two-gates Access Authentication escapes encryption breaking power of quantum computer

limitations of legacy 2-Factor Authentication (2FA) protocols, which often rely on what a user knows (password), has (device), or is (biometric data) – all of which remain visible and potentially vulnerable to sophisticated adversaries. QRUECA introduces a more robust, hardware-sealed, and user-evasive 4-Factor Authentication (4FA) model:

1. **Device-to-device hardware verification:** This is the core of Gate 1, ensuring that only authenticated QLT hardware devices can initiate a connection.
2. **Hardware-originated challenge response:** Subsequent challenges and responses are generated and processed within the secure hardware environment, preventing their interception or manipulation in transit.
3. **Time-limited access token validation:** Access is granted via ephemeral, short-lived tokens, which expire rapidly, minimizing the window for compromise even if a token were somehow captured.
4. **Behavioral or environmental signal matching (optional & non-invasive):** This optional factor adds an adaptive layer of security, leveraging contextual data (e.g., user's typical login patterns, network environment, device location) to further validate the legitimacy of the access attempt. This factor is non-invasive and operates in the background, further contributing to a seamless user experience.

4.5 Inherent Quantum Resistance by Design

The fundamental strength of QRUECA against quantum threats lies in its design philosophy: **prevention of exposure rather than complex post-quantum encryption of exposed data.** Because Gate 1 of the QRUECA process uses no user-facing cryptography, and Gate 2 is only activated by authenticated devices and does not expose reusable credentials, the entire protocol becomes inherently resistant to quantum attacks (see **Fig. 2**). If a quantum adversary cannot intercept the challenge, cannot observe the private key in use, and cannot gain access to any static credentials, they cannot attempt to decrypt it using Shor's algorithm or any other quantum algorithm. This design ensures that authentication in QLT systems is invisible, immutable, and quantum-safe by design, providing a level of security that current PQC efforts struggle to match in terms of efficiency and immediate deployability.

5. OPERATIONAL BENEFITS AND WEB 3.0 APPLICATIONS

Beyond its foundational quantum resilience, QRUECA offers significant operational advantages that enhance both security and user experience, making it particularly well-suited for the evolving landscape of Web 3.0 and the blockchain economy.

5.1 Operational Advantages

- **Seamless User Experience:** The most apparent benefit for end-users is the elimination of first-gate passwords or manual challenges. Since the initial authentication occurs invisibly at the hardware level between devices, users are freed from the cognitive burden and friction associated with traditional login procedures. This dramatically improves usability, reducing barriers to entry for decentralized applications and services.

- **Reduced Cognitive and Operational Risk:** A fundamental principle of security is that users cannot leak what they do not see or control. By making cryptographic operations and initial authentication credentials user-evasive, QRUECA drastically reduces the human element as a vulnerability. Phishing, social engineering, and credential stuffing attacks become largely ineffective against the initial authentication layer, as there are no user-exposed credentials to compromise. This shifts operational risk away from individual user vigilance to architectural system design.
- **Increased Compatibility with Low-Resource or Embedded Environments:** Unlike computationally heavy PQC protocols, which often demand significant processing power and memory, QRUECA's reliance on hardware-level handshakes and its focus on preventing exposure rather than complex, computationally intensive post-quantum encryption make it highly compatible with low-resource or embedded environments. This is crucial for the proliferation of IoT devices, edge computing, and specialized blockchain hardware wallets, where computational efficiency is paramount.

5.2 Independence from PQC Standardization

A critical differentiator for QRUECA is its independence from the ongoing and often precarious Post-Quantum Cryptography (PQC) standardization efforts. While PQC algorithms are still undergoing rigorous scrutiny, iterative revisions, and demonstrating repeated fragility (as evidenced by the compromise of various candidates), QRUECA offers quantum resilience *today*. It achieves this not by attempting to create new, unproven cryptographic primitives, but by fundamentally preventing the exposure of cryptographic material and authentication flows in the first place. This architectural approach delivers immediate quantum safety, bypassing the uncertainties and delays inherent in the PQC development cycle. QRUECA transforms authentication from a visible, vulnerable challenge into a sealed, autonomous access protocol.

5.3 Application in Web 3.0 and Blockchain

The implications of QRUECA and the underlying QLT framework for Web 3.0 are profound, especially for the blockchain ecosystem where endpoint integrity is everything. The current reliance on user-facing cryptographic authentication (e.g., managing private keys for wallets, signing transactions) represents the most commonly exploited vulnerability in blockchain and cryptocurrency infrastructure. QRUECA replaces this with a secure, invisible, and user-evasive post-quantum alternative.

QLT is deployed as a novel client-server cybersecurity framework, built on Qloud Technologies' proprietary ZVC and 3SoC architecture. Its design specifically targets the elimination of the two root causes of systemic vulnerability in digital systems: third-party permissions (TPPs) and user-facing cryptographic authentication, both addressed at the architectural level.

- **Server-Side Deployment:** At the server end, QLT's ZVC on 3SoC can deliver the full benefits of a zero-attack surface infrastructure. This is critical for securing vital components of the blockchain ecosystem, such as validator nodes, cryptocurrency exchanges, and other blockchain infrastructure endpoints. By running these critical services on 3SoC-enabled servers, the risk of unauthorized software execution, internal breaches, and quantum attacks on core network components is drastically mitigated.
- **Client-Side Deployment:** On the client end, QLT is envisioned as a standalone 3SoC hardware device. This device would integrate blockchain wallet functionality, providing unparalleled secure key storage, robust transaction approval mechanisms, and cryptographic isolation. Unlike software wallets susceptible to malware, or even hardware wallets that rely on user interaction for key exposure, the 3SoC client device integrates QRUECA for a truly user-evasive and quantum-safe interaction.
- **Closed, Post-Quantum-Resilient Intranet:** While each QLT component (server-side ZVC/3SoC and client-side 3SoC) operates independently and provides significant security benefits on its own, their true potential is realized when both ends are 3SoC-enabled. In such a scenario, the framework establishes a closed, quantum-resilient intranet. This creates an even higher level of isolation, trust, and cryptographic invisibility, as all communication and authentication within this network bypasses traditional vulnerable points and leverages the inherent security of the 3SoC-QRUECA ecosystem.

5.4 Application in 6G

The projected convergence of 6G deployment and quantum computing in 2030 presents a critical security dilemma. While PQC aims to protect against Q-Day threats, its large key sizes, computational overhead, and latency implications directly conflict with 6G goals such as sub-microsecond response times and drastic

cost reductions. With none of the NIST PQC candidates proving consistently secure, reliance on these unstable standards jeopardizes the feasibility of 6G's performance benchmarks.

QRUECA offers an architectural resolution to this impasse by eliminating exposure rather than encrypting it. Its concealed, device-level handshake—executed entirely through hardware-sealed, user-evasive mechanisms enabled by ZVC and 3SoC—prevents quantum adversaries from accessing any usable cryptographic material [Rah24c]. Aligned with the AZT model, QRUECA supports fast, autonomous, and low-cost authentication, making it inherently compatible with the operational demands and security requirements of 6G networks.

QRUECA and 6G Performance Goals

Latency: Unlike PQC, which introduces processing delays due to computational complexity, QRUECA's hardware-sealed device-to-device authentication operates below the software stack and requires no user intervention, making it capable of meeting 6G's <1µs latency target.

Cost Efficiency: 6G networks aim for a 1000x price-performance improvement over 5G. By avoiding the need for resource-intensive encryption, QRUECA reduces the computational burden and power draw at endpoints, making it viable for deployment across energy-constrained edge devices, IoT nodes, and mobile hardware.

Autonomy & Scalability: As 6G pushes toward self-organizing networks, dynamic mesh topologies, and massive machine-type communications, QRUECA's autonomous, certificate-based authentication supports trustless onboarding and roaming across decentralized nodes—without requiring cloud validation, policy enforcement, or cryptographic prompts.

Quantum Resilience: QRUECA does not rely on unproven post-quantum primitives. It achieves resilience by design, not by cryptographic strength, but by removing the very attack surfaces quantum computers seek to exploit.

Enabling a Post-QC 6G Security Infrastructure

QRUECA, embedded within 3SoC devices, allows the creation of closed, quantum-resilient intranets within 6G ecosystems, where both client and server operate in a fully sealed, immutable environment. This forms the basis for Quantum-as-a-Service (QaaS) delivery models that segregate quantum computation from the broader digital infrastructure without exposing it to vulnerabilities. In doing so, QRUECA enables a new class of quantum-aware 6G applications, such as:

1. Real-time autonomous mobility systems (e.g., drones, vehicles) requiring sub-millisecond authentication.
2. Edge-native industrial control systems where latency and trust are critical to operational integrity.
3. Ubiquitous identity validation for metaverse, AR/VR, and space-based communications, where human-free interactions must still be secure.

By adopting QRUECA, 6G networks can sidestep the latency, cost, and standardization barriers of PQC and deploy a security architecture that is inherently quantum-safe, user-transparent, and ready for scale. In a world where quantum computing may threaten to render our digital foundations obsolete, QRUECA positions itself not just as a stopgap—but as a long-term paradigm shift in how we build, protect, and trust next-generation communication systems.

6. CONCLUSION AND FUTURE WORK

The quantum threat to our digital infrastructure is no longer a distant theoretical possibility but an imminent challenge that demands immediate and innovative solutions. Current approaches, particularly Post-Quantum Cryptography, face significant hurdles in terms of stability, efficiency, and real-world deployability, especially for the dynamic and user-centric Web 3.0 environment. This paper has presented Quantum-Resilient User-Evasive Cryptographic Authentication (QRUECA) as a transformative protocol that fundamentally redefines secure access in the post-quantum era.

QRUECA's core innovation lies in its architectural shift away from user-facing cryptography towards a concealed, multi-gate, device-to-device authentication handshake. By embedding QRUECA Crypto Certificates (QCCs) within proprietary Solid-State Software on a Chip (3SoC) hardware and leveraging Zero Vulnerability Computing (ZVC) to eliminate third-party permissions, QRUECA achieves inherent quantum resistance. This is because the critical cryptographic operations occur in a user-evasive and hardware-sealed environment, denying quantum adversaries the attack surface needed to intercept or decrypt credentials. The 4-Factor Authentication model further enhances security without compromising user experience.

The integration of QRUECA within the Quantum Ledger Technology (QLT) framework provides a comprehensive solution for securing critical blockchain/cryptocurrency infrastructure, including validator nodes and exchanges, as well as enabling ultra-secure client-side wallet functionality. QRUECA

not only delivers immediate quantum resilience but also offers substantial operational benefits, including a seamless user experience, reduced operational risk, energy efficiency, and compatibility with resource-constrained environments. By decoupling quantum safety from the still-evolving PQC standards, QRUECA represents a practical and deployable solution that addresses a significant hurdle for the mainstream introduction of quantum computing.

Future work should focus on formal verification of the QRUECA protocol to rigorously prove its security properties against known quantum attacks and other sophisticated adversaries. Empirical performance studies across various Web 3.0 environments would also be beneficial to demonstrate its efficiency and scalability in diverse real-world scenarios. Furthermore, exploring standardized interfaces for integrating QRUECA-enabled 3SoC devices with a broader range of decentralized applications and services would be crucial for widespread adoption. As quantum capabilities continue to advance, such architectural-level security innovations, rather than mere cryptographic upgrades, will be paramount to safeguarding our interconnected digital future. Just as an automobile cannot exist without a braking system, quantum computers cannot exist without securing our life-sustaining digital infrastructure.

7. ACKNOWLEDGMENTS

The authors acknowledge the support and cooperation of the participants in the PROSEC Consortium (Horizon Europe Consortium), which collaborated on this project

8. REFERENCES

[Car25a] Carnell, M. Buckle Up. Quality Progress, 58(3), 2025.

[Che16a] Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Smith-Tone, D., et al. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology, Vol. 12, 2016. doi:10.6028/NIST.IR.8105.

[Gao25a] Gao, D., et al. Establishing a new benchmark in quantum computational advantage with 105-qubit Zuchongzhi 3.0 processor. Physical Review Letters, 134(9), 090601, 2025.

[Lav24a] Lavich, M., Kuchukhidze, T. Investigating CRYSTALS-Kyber vulnerabilities: attack analysis and mitigation. Cryptography, 8(2), 15, 2024.

[Maj15a] Majot, M., Yampolskiy, R. Global catastrophic risk and security implications of quantum computers. Futures, 72, 17–26, 2015.

[Rah22a] Raheman, F., et al. Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. Future Internet, 14(8), 238, 2022.

[Rah22b] Raheman, F. The future of cybersecurity in the age of quantum computers. Future Internet, 14(11), 335, 2022.

[Rah24a] Raheman, F. Futureproofing blockchain and cryptocurrencies against growing vulnerabilities and Q-Day threat with quantum-safe ledger technology (QLT). Journal of Computer and Communications, 12(7), 59–77, 2024.

[Rah24b] Raheman, F., et al. Revisiting the first principles of software engineering for validating a new computing paradigm's automated and proactive cybersecurity. (under peer review). Available at www.bc5.eu/prosec.pdf.

[Rah24c] Raheman, F. Formulating and Supporting a Hypothesis to Address a Catch-22 Situation in 6G Communication Networks. Journal of Information Security, 15, 340–354, 2024.

[Ugw20a] Ugwuishiwu, C.H., et al. An overview of quantum cryptography and Shor's algorithm. International Journal of Advanced Trends in Computer Science and Engineering, 9(5), 2020.

[Yua24a] Yuan, G., et al. Quantum computing for databases: Overview and challenges. arXiv preprint, arXiv:2405.12511, 2024.