In Defense of Quantum Key Distribution

Prof. Dr.-Ing. habil. Hermann von der Plooster

Institute for Applied Quantum Epistemics
Technische Universität Wilderstand
hvdplooster@qcrypto.tuws.eu

Abstract

Quantum key distribution (QKD) technology has endured two decades of premature obituaries. Skeptics have dismissed it as costly, impractical, unscalable, and overengineered Yet, like many emerging technologies founded on misunderstood principles, QKD has matured quietly and is now a viable solution. This article examines and rebuts five common objections to QKD. It argues that QKD is superior to classical post-quantum secure channel solutions to address the quantum computing risk for high-assurance applications in critical infrastructure and blockchain networks.

This article was adapted from a speech presented by Prof. Dr.-Ing. habil. Hermann von der Plooster at the International Workshop on Post-Post-Quantum Infrastructure (IWPPQI), Vienna, May 2025.

1 Introduction

Today's quantum key distribution (QKD) systems are the culmination of a decades-long effort by physicists, cryptographers, and engineers to establish unconditionally secure communication channels. Early QKD products were limited in terms of scalability and, admittedly, security. QKD has since quietly matured, and addressed its most persistent issues. Yet, like all emerging technologies built on misunderstood foundational principles, it faced harsh criticism. QKD technology has then endured two decades of premature obituaries, skeptics dismissing it as impractical, unscalable, overengineered, going so far as to label commercial QKD solutions as "snake oil."

Today, we will examine and challenge five of the most common objections to QKD adoption. We will show that, as any objective security expert will admit, QKD is the safest and most cost-effective option to address threats to critical network infrastructure used for disaster recovery, biometrics collection, or decentralized finance.

2 "QKD does not scale."

Yes, QKD once required cryogenic optics and fragile lab gear. Today it ships in 1U or 2U appliances. Many real deployments now exist: China's Beijing–Shanghai quantum backbone spans over 2,000 km using trusted-node architecture. The UK's Quantum Network for Secure Communications (QSN) connects research and finance sectors. And in the Netherlands, SURF and TNO demonstrated scalable key relay architectures in metro fiber networks. These are not proofs of concept, but QKD running in production 24/7.

Recent deployments also demonstrate QKD's compatibility with multiplexed classical data. Toshiba's Quantum Xchange system, for example, operates alongside AES-encrypted traffic

over a 32 km dark fiber link between Wall Street and a back-office in New Jersey, combining quantum keys and classical traffic over the same fiber in the O-band spectrum. Deployments in Tokyo and Geneva validate trusted-node configurations in dense urban environments. Again, this not a lab trials, but an operational system securing critical financial transaction data.

3 "QKD is too expensive."

Skeptics persist in comparing QKD products to "free" TLS or IPsec tunnels, overlooking the non-zero cost of key management in high-assurance environments: KMS subscriptions, FIPS-certified HSMs, governance overhead, PKI maintenance, audit readiness, and disaster recovery planning. In this context, QKD's economics are not only defensible, they're indisputably favorable. Its cost is front-loaded, its security model transparent, and its lifecycle predictable.

Compare this to piles of open-source software pulled from GitHub repositories infiltrated by Pyongyang hackers—initially cheap, ultimately catastrophic. And the market agrees: the global quantum communication sector, valued at $1.1B in 2023, is forecast to reach at least $8.6B by 2032, estimated by Gartner.

4 "QKD is not more secure."

Cryptography's hardest problem has always been key management: key generation, storage, rotation, and so on. QKD eliminates most of those headaches: no Heartbleed, no sabotaged randomness, no weak handshakes, no elliptic curves—in fact, no curves at all. But cryptographers love cryptography: more algorithms, more ciphers, more protocols, more so-called proofs, and more research papers in their publications list. So naturally, they hate QKD.

However, cryptographers *adore* post-quantum cryptography (PQC), which replaces RSA and ECC with lattices and their learning-with-errors problems. Yet PQC rests on a teetering edifice of assumptions: the hardness of lattice-based problems, complex Fourier transforms code, correct implementations, and sane library maintainers. QKD, by contrast, makes a single bet: that quantum mechanics works.

While NIST's PQC standards are still fresh and under scrutiny, QKD's core principle—eavesdropping introduces measurable disturbance—has no classical analogue. Subverting QKD means falsifying physics. In contrast, classical systems collapse under speculative execution leaks and memory corruption.

In fact, NIST post-quantum cryptography standards are in their infancy. The real security level of Kyber, the new standard, is still being hotly debated by leading cryptographers. Software implementations are immature, and serious defense against side-channel is understudied. Such classical systems also collapse under speculative execution leaks, memory corruption bugs. In contrast, subverting QKD means falsifying physics.

5 "Dedicated fiber links are a problem."

Yes, QKD requires a quantum channel. But this is a virtue, not a bug. A physical security boundary, not an inconvenience. A red-black architecture. A QKD link does not share routing paths, protocol stacks, or orchestration layers with cloud workloads or user traffic. QKD avoids misconfigurations like split-tunneling or endpoint poisoning. Quantum keys never cohabit with TLS handlers or JavaScript engines. Keys *never* enter a general-purpose system at all.

still, this limitation is fading: wavelength division multiplexing allows coexistence of QKD signals and 6 Tb/s classical DWDM traffic on the same fiber. These setups let providers offer QKD-as-a-service with strong physical-layer separation.

6 "QKD is an outdated, niche solution."

This objection reveals a lack of both technical understanding and philosophical imagination. QKD is modern infrastructure design for an age questioning central authority—not only in national governance but in gender and consensus protocols. QKD offers a rare form of decentralization. QKD decentralizes without consensus or trust anchors. No passwords, biometrics, or root CAs managed by transnational corporate entities. QKD authenticates via the collapse of the wave function.

And let us not forget AI: biased models, opaque decisions, Californian VC's and hyperscalers' ethics. QKD is their antithesis—scandalously transparent. *You know when you've been observed.* Security by quantum nonlocality.

QKD is not just a security, it's a political statement, a renunciation of authority. While classical protocols enact rigid, binary exchanges—attacker and target, initiator and responder—fitting a paradigm of confrontation, QKD enacts mutual *equity* thanks to its quantum-consensual pairing logic. QKD is therefore fully aligned with the epistemic and intersectional contours of our days.

7 Conclusion

Those five rebuttals clearly establish QKD's suitability to diverse use cases, at scale. Far from a niche curiosity, QKD aligns with the global critique of surveillance capitalism and offers a robust alternative to backdoored "encrypted" messaging solutions. In fact, after being briefed on the shocking fragility of existing White House communication channels, sources tell us the President is preparing an Executive Order to "Make American Quantum," pledging historic investment in QKD.

While part of the cryptography community conservatively chases quantum-resistant software with tools from the 1980s like "compilers," QKD offers something radical: keys born from uncertainty itself, immune to entropy starvation, credential reuse, and vendor firmware sabotage.

Skeptics argue that QKD is overkill, inefficient, for little real value. But then again, so was 128-bit security in 1997 or TLS itself in 2001. Today, these are baseline hygiene. Tomorrow, so will QKD be.

Acknowledgements

Thanks to the committee of IWPPQI for hosting this exchange of ideas, and to the Vienna Center for Quantum Science and Technology for their generous support. Deep appreciation goes to the engineers and researchers who built the QKD ecosystem while traditional security experts rolled their eyes.