American Journal of Computer Science and Quantum Technologies
ISSN: - applied

Quantum Secure Satellite Networks and Post Quantum Blockchain Infrastructures for Global Trust Architectures

[1] Rafael Dominguez
[1] Universidad de Buenos Aires, Argentina

Received: 30th Oct 2025 | Received Revised Version: 11th Nov 2025 | Accepted: 23th Nov 2025 | Published: 09th Dec 2025

Volume 01 Issue 02 2025 | Crossref DOI: 10.64917/ajcsqt/V01I02-001

Abstract

The emergence of large scale quantum computing and long distance quantum communication represents a fundamental disruption to all classical cryptographic and digital trust systems. Classical public key cryptography that currently secures global internet traffic, financial networks, and digital identity frameworks is mathematically vulnerable to quantum algorithms that can efficiently solve factorization and discrete logarithm problems. At the same time, experimental breakthroughs in satellite based quantum communication have demonstrated that quantum entanglement and quantum key distribution can be extended to continental and intercontinental scales. These two forces together generate both an existential threat to existing digital infrastructure and a historic opportunity to build a new generation of cryptographically provable trust systems. This article develops a unified theoretical and architectural framework that integrates satellite based quantum key distribution, post quantum cryptography, and blockchain based distributed ledgers into a coherent global trust fabric.

Using the foundational satellite experiments by Liao, Yin, and their collaborators, which demonstrated satellite to ground quantum key distribution, thousand kilometer entanglement distribution, and satellite relayed intercontinental quantum networks, the article first establishes that quantum communication is no longer a laboratory curiosity but a deployable infrastructure technology. These quantum links provide information theoretic security based on the laws of physics rather than computational assumptions, enabling symmetric keys that are immune to both classical and quantum attacks. However, quantum channels alone cannot solve the full problem of global trust, identity, and transaction verification. They must be embedded into layered network architectures that resemble and extend classical open systems models such as the ISO OSI reference framework.

The article then analyzes the parallel evolution of post quantum cryptography as standardized by the National Institute of Standards and Technology and evaluated by agencies such as the National Security Agency. Hash based signatures such as SPHINCS and XMSS, lattice based encryption, and code based schemes provide algorithmic defenses that are believed to resist quantum attacks. These schemes are essential for digital signatures, authentication, and blockchain consensus in environments where quantum communication is not always available or practical.

Keywords: Quantum key distribution, satellite quantum communication, post quantum cryptography, blockchain security, quantum digital signatures, global trust networks.

Cite This Article: Rafael Dominguez. 2025. Quantum Secure Satellite Networks and Post Quantum Blockchain Infrastructures for Global Trust Architectures. American Journal of Computer Science and Quantum Technologies 1, 02, 1-7. https://doi.org/10.64917/ajcsqt/V01I02-001

1. Introduction

The digital world of the early twenty first century is built on a fragile mathematical foundation. Nearly every secure

communication channel, financial transaction, and digital identity system depends on cryptographic algorithms whose security rests on the practical difficulty of solving certain mathematical problems. Public key cryptography, in particular, relies on the fact that while it is easy to multiply two large prime numbers, it is extremely difficult for classical computers to factor the resulting product. Similarly, elliptic curve cryptography relies on the difficulty of the discrete logarithm problem. These assumptions have held for decades and have enabled the explosive growth of electronic commerce, cloud computing, social media, and blockchain based digital currencies. However, the theoretical discovery of quantum algorithms such as Shor's algorithm revealed that a sufficiently powerful quantum computer could solve these problems in polynomial time, rendering most existing public key cryptography obsolete.

This looming vulnerability has driven two parallel research trajectories. One is the development of post quantum cryptography, which seeks to design new mathematical schemes that remain secure even in the presence of quantum adversaries. The other is the development of quantum communication technologies, particularly quantum key distribution, which promise security based on the laws of physics rather than on computational assumptions. In recent years, these trajectories have converged with unprecedented experimental demonstrations of satellite based quantum communication. The Chinese quantum science satellite, often referred to as Micius, has enabled satellite to ground quantum key distribution, entanglement distribution over distances exceeding one thousand kilometers, and satellite relayed intercontinental quantum networks (Liao et al., 2017; Yin et al., 2017; Liao et al., 2018). These achievements have shown that quantum communication is no longer confined to optical fibers and laboratory benches but can operate on a planetary scale.

At the same time, the rise of blockchain technology has transformed how trust is established in distributed systems. Originally introduced as the foundation of Bitcoin, blockchain provides a decentralized ledger in which transactions are recorded in a cryptographically linked chain of blocks, creating an immutable history that does not depend on any central authority (Nakamoto, 2008). Subsequent platforms such as Ethereum have generalized this idea to support programmable smart contracts and decentralized applications (Wood, 2014). Blockchain has been widely adopted in finance, supply chain management, identity systems, and governance. However, blockchain itself relies heavily on classical cryptographic primitives, particularly digital signatures based on elliptic curves, which are vulnerable to quantum attacks (Aggarwal et al., 2017).

This convergence of quantum computing, quantum communication, and blockchain raises a profound question: how can we construct a global digital trust infrastructure that remains secure in a quantum future. This article argues that the answer lies in the integration of satellite based quantum key distribution, post quantum cryptographic algorithms, and blockchain based distributed ledgers. By combining the information theoretic security of quantum channels with the algorithmic robustness of post quantum cryptography and the decentralization of blockchain, it is possible to build a trust architecture that is resilient to both classical and quantum adversaries.

The literature already provides many of the building blocks for this vision. Liao and colleagues demonstrated that quantum keys can be exchanged between a satellite and multiple ground stations, enabling secure communication across thousands of kilometers (Liao et al., 2017). Yin and colleagues showed that entangled photon pairs could be distributed over distances greater than one thousand kilometers, laying the foundation for a quantum internet (Yin et al., 2017). Liao and collaborators extended this to an intercontinental quantum network mediated by satellites (Liao et al., 2018). These experimental achievements were widely recognized as proof that quantum communication is practical, not just theoretical (Conover, 2017).

On the cryptographic side, NIST and other organizations have been leading a global effort to standardize post quantum cryptographic algorithms that can replace or complement existing public key systems (Chen et al., 2016). Hash based signature schemes such as SPHINCS and XMSS have been proposed as practical alternatives to elliptic curve signatures, offering strong security guarantees based on minimal assumptions (Bernstein et al., 2015; Buchmann et al., 2011). National security agencies have acknowledged the inevitability of quantum computing and have begun to define cryptographic suites designed to be quantum resistant (NSA, 2016).

Meanwhile, research into quantum digital signatures and quantum secure blockchains has shown that quantum communication can be used not only for key distribution but also for authentication and non repudiation (Gottesman and Chuang, 2001; Donaldson et al., 2016; Croal et al., 2016; Yin et al., 2017; Collins et al., 2018; Kiktenko et al., 2018). These developments suggest that quantum technologies can be deeply integrated into the logic of distributed ledgers, providing new forms of security and trust.

Despite this rich body of work, there remains a gap in the literature. Most studies focus either on the physics of quantum communication, the mathematics of post quantum cryptography, or the computer science of blockchain. Few attempt to synthesize these domains into a unified architecture that could realistically support global scale digital trust. Moreover, there is a need to place these technologies within a systems engineering framework that accounts for network layers, security perimeters, and defense in depth principles as articulated in standards such as ISO 7498 and in security engineering literature (ISO, 1994; Holl, 2003).

2. Methodology

The methodological approach of this research is theoretical synthesis grounded in experimental and standards based evidence. Rather than presenting new laboratory data or simulations, the study integrates and analyzes existing results from quantum communication experiments, cryptographic standardization efforts, and blockchain architectures to construct a comprehensive model of a quantum secure global trust system.

The first methodological step involves a detailed examination of satellite based quantum communication experiments. The satellite to ground quantum key distribution experiments conducted by Liao and colleagues demonstrated that a low Earth orbit satellite can distribute quantum keys to ground stations separated by thousands of kilometers (Liao et al., 2017). The methodology of those experiments involved the generation of polarized photons aboard the satellite, their transmission through the atmosphere to optical ground stations, and the use of quantum key distribution protocols to detect eavesdropping and distill secure keys. The entanglement distribution experiment by Yin and colleagues extended this by generating entangled photon pairs on the satellite and sending each photon to a different ground station, verifying that quantum correlations were preserved over more than one thousand kilometers (Yin et al., 2017). These experiments provide empirical validation of the feasibility of a global quantum communication layer.

The second methodological step is the analysis of post quantum cryptographic frameworks. The NIST report on post quantum cryptography outlines the threat posed by quantum computers and the criteria for selecting new cryptographic standards (Chen et al., 2016). This includes requirements for security, performance, and implementability. The NSA's CNSA suite similarly defines cryptographic algorithms suitable for national security systems in a quantum era (NSA, 2016). By examining these documents, the study identifies which cryptographic primitives are appropriate for integration into blockchain systems and network protocols.

Hash based signature schemes such as SPHINCS and XMSS are examined in detail because they are explicitly designed to be secure against quantum attacks and because they provide digital signatures, which are essential for blockchain transactions and identity verification (Bernstein et al., 2015; Buchmann et al., 2011). These schemes rely on the one way and collision resistant properties of cryptographic hash functions, which are believed to remain secure even in the presence of quantum algorithms, although with some reduction in security margins.

The third methodological step is the examination of blockchain architectures and their cryptographic foundations. Bitcoin introduced a peer to peer electronic cash system based on proof of work, cryptographic hashes, and elliptic curve digital signatures (Nakamoto, 2008). Ethereum generalized this to a programmable transaction ledger (Wood, 2014). The cryptographic primitives used in these systems, particularly the secp256k1 elliptic curve, are vulnerable to quantum attacks (Aggarwal et al., 2017). Therefore, the methodology involves analyzing how these systems can be modified to use post quantum signatures and how their network layers can be secured with quantum key distribution.

The fourth methodological step involves integrating these components into a layered security architecture. The ISO OSI model provides a conceptual framework for understanding how different network functions operate at different layers, from physical transmission to application level protocols (ISO, 1994). Security engineering principles such as defense in depth emphasize that no single security mechanism is sufficient and that multiple layers of protection are necessary (Holl, 2003). By mapping quantum communication, post quantum cryptography, and blockchain protocols onto these layers, a coherent architecture can be constructed.

Finally, the methodology draws on research into quantum digital signatures and quantum secured blockchains to validate that the proposed architecture is not merely hypothetical. Experimental demonstrations of quantum digital signatures over tens and hundreds of kilometers show that quantum based authentication is feasible (Donaldson et al., 2016; Croal et al., 2016; Yin et al., 2017; Collins et al., 2018). Theoretical and experimental work on quantum secured blockchain further supports the integration

of these technologies (Kiktenko et al., 2018).

3. Results

The synthesis of the referenced literature leads to several key results that define the structure and capabilities of a quantum secure global trust architecture.

The first result is that satellite based quantum communication provides a viable global key distribution layer. The experiments by Liao et al. demonstrated that quantum keys can be distributed from a satellite to multiple ground stations, enabling secure communication between any pair of stations that share keys with the satellite (Liao et al., 2017). This effectively creates a star network in which the satellite acts as a trusted or semi trusted node that facilitates key exchange. The entanglement distribution experiment by Yin et al. further showed that a satellite can distribute entangled pairs to distant nodes, enabling device independent quantum key distribution and other advanced protocols (Yin et al., 2017). The satellite relayed intercontinental quantum network demonstrated that these techniques can be extended across continents, creating the backbone of a global quantum network (Liao et al., 2018).

These results imply that it is technically feasible to establish quantum secured channels between major data centers, financial hubs, and government institutions around the world. The atmospheric channel losses, pointing and tracking challenges, and photon detection efficiencies that once limited free space quantum communication have been overcome to a degree that allows operational deployment, as recognized by the broader scientific community (Conover, 2017).

The second result is that post quantum cryptographic primitives can replace vulnerable classical algorithms in digital identity and blockchain systems. Hash based signatures such as SPHINCS and XMSS provide digital signatures that are secure against quantum adversaries under minimal assumptions about hash functions (Bernstein et al., 2015; Buchmann et al., 2011). These schemes can be used to sign blockchain transactions, authenticate nodes, and verify software updates. While they may have larger signature sizes and different performance characteristics than elliptic curve signatures, their security properties make them suitable for long term deployment in a quantum era.

The NIST and NSA frameworks further support this result by providing institutional validation and guidance for the adoption of post quantum cryptography (Chen et al., 2016; NSA, 2016). These organizations recognize that migration to quantum resistant algorithms must begin well before large scale quantum computers become available, because data encrypted today may be stored and decrypted in the future.

The third result is that blockchain can be made quantum secure by integrating quantum communication and post quantum cryptography. Aggarwal et al. showed that quantum attacks could undermine the security of Bitcoin by allowing an adversary to derive private keys from public keys and thereby steal funds or rewrite transaction histories (Aggarwal et al., 2017). However, by replacing elliptic curve signatures with hash based signatures and by using quantum key distribution to secure communication channels between nodes, these vulnerabilities can be mitigated.

Moreover, quantum digital signatures provide a fundamentally new way to authenticate messages and transactions. Gottesman and Chuang proposed quantum digital signature schemes that leverage quantum states to ensure that a message cannot be forged or repudiated (Gottesman and Chuang, 2001). Experimental demonstrations have validated that such signatures can be implemented over free space and fiber channels (Donaldson et al., 2016; Croal et al., 2016; Yin et al., 2017; Collins et al., 2018). These signatures can be integrated into blockchain protocols to provide quantum level non repudiation and authenticity.

The fourth result is that a layered architecture based on ISO OSI principles and defense in depth can integrate these technologies into a coherent system. At the physical and data link layers, quantum channels provided by satellites and optical fibers deliver raw quantum states. At the network and transport layers, quantum key distribution protocols establish symmetric keys that are used to encrypt classical data channels. At the session and presentation layers, post quantum cryptographic protocols manage authentication, key management, and data integrity. At the application layer, blockchain protocols record transactions, manage smart contracts, and provide decentralized trust.

This layered approach ensures that even if one component is compromised, others continue to provide security. For example, if a post quantum cryptographic algorithm is later found to be weaker than expected, the quantum key distribution layer still provides information theoretic security for communication channels. Conversely, if a quantum channel is temporarily unavailable due to weather or satellite outages, post quantum cryptography can maintain secure communication over classical channels.

The fifth result is that quantum memory and quantum

internet research supports the scalability of this architecture. Advances in quantum memory capacity and coherence times enable the storage and synchronization of quantum states over extended periods, which is essential for a global quantum network (Phys.org, 2017). The vision of a quantum internet articulated by research organizations such as QuTech further reinforces the idea that quantum communication will become a standard component of future networks (QuTech, 2018).

Taken together, these results demonstrate that a quantum secure blockchain based global trust architecture is not only conceptually sound but also grounded in existing experimental and theoretical work.

4. Discussion

The integration of satellite quantum communication, post quantum cryptography, and blockchain represents a paradigm shift in how digital trust is constructed. Rather than relying solely on computational hardness assumptions, this architecture leverages physical laws, mathematical rigor, and decentralized consensus to create a multi layered security fabric.

One of the most significant implications of this work is that trust can be established without centralized authorities even in a quantum era. Traditional public key infrastructures depend on certificate authorities that vouch for the identities of users and servers. These authorities become single points of failure and targets for attack. Blockchain already reduces this dependency by distributing trust across a network of nodes. Quantum communication further strengthens this by providing channels that cannot be eavesdropped without detection. When combined with post quantum signatures, it becomes possible to create identity and transaction systems that are resistant to both classical and quantum attacks.

However, this vision is not without challenges. Satellite based quantum communication, while demonstrated, remains expensive and technically complex. Launching, maintaining, and coordinating a constellation of quantum communication satellites requires significant investment and international cooperation. Atmospheric conditions, line of sight constraints, and orbital dynamics impose limitations on availability and coverage. While these challenges are being addressed through engineering advances, they represent a barrier to rapid global deployment (Liao et al., 2017; Yin et al., 2017).

Another challenge lies in the performance and usability of post quantum cryptographic algorithms. Hash based signatures often produce large signatures and may require state management or tree structures that complicate implementation (Bernstein et al., 2015; Buchmann et al., 2011). Blockchain systems that handle millions of transactions may need to adapt their data structures and consensus protocols to accommodate these changes. There is also the risk that some post quantum algorithms may later be found vulnerable, requiring further migration.

Governance and standardization present additional issues. The NIST post quantum cryptography standardization process aims to produce widely accepted algorithms, but the transition from classical to post quantum systems will be complex and lengthy (Chen et al., 2016). Different countries and organizations may adopt different standards, potentially leading to fragmentation. International coordination will be essential, particularly for satellite based quantum networks that inherently cross national borders.

There are also philosophical and societal implications. Quantum secure blockchains could enable unprecedented levels of privacy and security, but they could also be used to hide illicit activity or evade lawful surveillance. Balancing security, privacy, and accountability will require careful policy design and public debate.

Despite these challenges, the trajectory of research and development suggests that the convergence of these technologies is inevitable. Quantum computers will continue to advance, increasing the urgency of migrating away from vulnerable cryptography. Quantum communication technologies will continue to mature, reducing costs and improving reliability. Blockchain and distributed ledger technologies will continue to evolve, driven by economic and social demand for decentralized trust.

Future research should focus on several key areas. First, more experimental work is needed to integrate quantum key distribution with real world network protocols and blockchain systems. Pilot projects that connect quantum communication links to distributed ledgers would provide valuable insights into performance, reliability, and security. Second, further development of post quantum cryptographic libraries and hardware acceleration will be necessary to make these algorithms practical at scale. Third, international frameworks for the governance of quantum networks and quantum secured blockchains should be developed to ensure interoperability and trust across borders.

5. Conclusion

The digital infrastructure of the modern world stands at the

threshold of a quantum revolution. The same quantum technologies that threaten to break classical cryptography also offer the tools to build a more secure and trustworthy global network. Satellite based quantum communication, as demonstrated by Liao, Yin, and their collaborators, provides a physical layer of security that can span continents. Post quantum cryptography, as advanced by NIST, NSA, and the cryptographic research community, provides algorithmic defenses that can replace vulnerable classical schemes. Blockchain technology provides a decentralized framework for recording and verifying transactions, identities, and agreements.

By integrating these three pillars into a unified architecture, it is possible to construct a quantum secure global trust system that is resilient to both present and future threats. This architecture embodies the principles of defense in depth and layered security articulated in classical standards while extending them into the quantum domain. It offers not only technical security but also a new foundation for social and economic trust in a digital age.

The research synthesized in this article demonstrates that such a system is not a distant fantasy but a realistic near term possibility. The challenge now lies in translating this vision into operational networks, standards, and institutions that can support the complex and interconnected world of the future.

References

1. Aggarwal D, Brennen G, Lee T, Santha M, Tomamichel M. Quantum attacks on Bitcoin and how to protect against them. arXiv quant-ph 1710.10377v1.
2. Allende Lopez M, Colina Unda V. Blockchain Como desarrollar confianza en entornos complejos para generar valor de impacto social. Inter American Development Bank. DOI 10.18235/0001139.
3. Allende Lopez M, Colina Unda V. Aprende los tres elementos clave de blockchain con este ejemplo practico. IDB Blog Abierto al publico 2018.
4. Allende Lopez M, Colina Unda V. Conoce los distintos tipos de blockchain. IDB Blog Abierto al publico 2018.
5. Bernstein D J, Hopwood D, Hulsing A, Lange T, Niederhagen R, Papachristodoulou L, Schneider M, Schwabe P, Wilcox O. SPHINCS Practical stateless hash based signatures. Advances in Cryptology EUROCRYPT 2015 368 397.
6. Bitcoin. A peer to peer electronic cash system.
7. Buchmann J, Dahmen E, Hulsing A. XMSS A practical forward secure signature scheme based on minimal security assumptions. PQCrypto 2011 Post Quantum Cryptography 117 129.
8. Chen L, Jordan S, Liu Y K, Moody D, Peralta R, Perlner R, Smith T. Report on Post Quantum Cryptography. NIST Internal Report 8105 2016.
9. Collins R J, Donaldson R J, Buller G S. Progress in experimental quantum digital signatures. Proceedings of SPIE Quantum Communications and Quantum Imaging XVI 107710F 2018.
10. Conover E. A quantum communications satellite proved its potential in 2017. Science News 192 11 27.
11. Croal C, Zhang Z, Xiong C, Zhang C, Zhang Q, Walmsley I A. Free space quantum signatures using heterodyne measurements. Physical Review Letters 117 100503 2016.
12. Donaldson R J, Collins R J, Kleczkowska K, Amiri R, Wallden P, Dunjko V, Andersson E, Jeffers J, Buller G S. Experimental demonstration of kilometer range quantum digital signatures. Physical Review A 93 012329 2016.
13. Gottesman D, Chuang I. Quantum digital signatures. arXiv quant-ph 0105032v2 2001.
14. Haber S, Stornetta W S. How to time stamp a digital document. Journal of Cryptology 3 2 99 111 1991.
15. Holl K. Global Information Assurance Certification Paper OSI Defense in depth to increase application security 2003.
16. ISO IEC 7498 1. Information technology Open Systems Interconnection Basic Reference Model 1994.
17. Kiktenko E O, Pozhar N O, Anufriev M N, Trushechkin A S, Yunusov R R, Kurochkin Y V, Lvovsky A I, Fedorov A K. Quantum secured blockchain. Quantum Science and Technology 3 3 2018.
18. Liao S K, Cai W Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J G, Liu W Y, Li Y, Shen Q, Cao Y, Li F Z, Wang J F, Huang Y M, Deng L, Chen T, Li L, Zhang N L, Zhou F, Chen Y A, Lu C Y, Shu R, Peng C Z, Zeilinger A, Pan J W. Satellite to ground quantum key distribution. Nature 549 43 47 2017.
19. Liao S K, Cai W Q, Liu W Y, Zhang L, Li Y, Ren J G, Yin J, Shen Q, Cao Y, Li Z P, Li F Z, Chen X W, Sun L H, Jia J J, Wu J J, Jiang X J, Wang J F, Huang Y M, Deng L, Liu Y C, Guo Q, Liu H L, Chen Y A, Peng C Z, Lu C Y, Pan J W. Satellite relayed intercontinental quantum network. Physical Review Letters 120 030501 2018.

20. Nakamoto S. Bitcoin A peer to peer electronic cash system.
21. National Security Agency. CNSA suite and quantum computing FAQ MFQ U OO 815099 15 2016.
22. Phys.org. Quantum memory record breaking capacity based 2017.
23. QuTech. Quantum internet A vision 2018.
24. Vinzenzo D. The physical interpretation of quantum computation. Fortschritte der Physik 48 9 11 2000.
25. Wood G. Ethereum A secure decentralized generalized transaction ledger EIP 150 revision.
26. Yin H L, Fu Y, Chen Z B, Tang Y L, Liao S K, Chen Y A, Pan J W. Experimental quantum digital signature over 102 km. Physical Review A 95 032334 2017.
27. Yin J, Cao Y, Li Y H, Ren J G, Liao S K, Zhang L, Cai W Q, Liu W Y, Li B, Dai H, Li G B, Lu Q M, Gong Y H, Xu Y, Li S L, Li F Z, Yin Y Z, Jiang Z Q, Li M, Jia J J, Ren G, He D, Zhou Y L, Zhang X X, Wang N, Chang X, Zhu Z C, Liu N L, Chen Y A, Lu C Y, Peng C Z, Pan J W. Satellite based entanglement distribution over 1200 kilometers. Science 356 6343 1140 1144.