The Future of Cryptocurrency in the Quantum Computing Era: An Economic Perspective

PAATA J. KERVALISHVILI, MAMUKA A. TAVKHELIDZE
Grigol Robakidze University, Tbilisi, GEORGIA

Abstract: The emergence of quantum computing represents a paradigm shift with dual implications for the future of cryptocurrency: it poses an existential threat to current systems while simultaneously enabling revolutionary new ones. This paper analyzes the economic implications of this transition. We examine the vulnerabilities of classical cryptocurrencies like Bitcoin and Ethereum to quantum attacks via Shor's and Grover's algorithms and explore the rise of quantum-resistant cryptocurrencies (e.g., QRL, IOTA). Furthermore, we investigate the theoretical foundations of fully quantum-native systems, which leverage superposition, entanglement, and the no-cloning theorem to enable secure "quantum money" and novel consensus mechanisms. Key challenges such as quantum decoherence, scalability, and the necessity for hybrid transitional systems are addressed. The economic analysis contrasts the energy efficiency and hardware requirements of classical versus quantum mining, projecting a pathway towards greener and more efficient processes. The concept of "quantum money" is introduced as a tamper-proof currency, with potential applications in decentralized finance (DeFi) and central bank digital currencies (CBDCs). We also discuss hypothetical dual-use threats, such as quantum-enabled money laundering, underscoring the technology's potential for both hyper-transparency and unbreakable anonymity. We conclude that the integration of quantum computing will be phased, beginning with defensive post-quantum cryptography and evolving into a fully quantum-economic paradigm. Proactive adaptation by policymakers and industry is essential to harness the benefits and mitigate the risks of this new era.

Keywords: — Quantum Computing, Cryptocurrency, Quantum-Resistant Cryptography, Quantum Money, Economic Paradigm, Blockchain.

Received: May 11, 2025. Revised: June 18, 2025. Accepted: September 6, 2025. Published: October 16, 2025.

1. Introduction: A Quantum Approach to the Economy

Quantum computing utilizes quantum-mechanical phenomena—such as superposition and entanglement—to process information in ways fundamentally different from classical computers. This capability promises a quadratic or even exponential speedup for specific problem classes, including those central to cryptography and financial modeling [1, 2].

The foundational principles of superposition (where a quantum state exists in multiple possibilities simultaneously until measured) and entanglement (where particles remain correlated across distance) enable this computational power [3, 4]. One of the most imminent and high-impact applications lies in cryptography. The vulnerability of current public-key cryptosystems has prompted a global effort, led by institutions like the U.S. National Institute of Standards and Technology (NIST), to standardize post-quantum cryptographic (PQC) algorithms [5-7].

The shift is towards mathematical problems believed to be hard for quantum computers to solve, such as those based on lattice theory, moving away from the factorization-based

systems broken by Shor's algorithm [8-10]. The application of quantum principles is also expanding into economics and finance, where quantum algorithms are being developed for option pricing, risk management, and market optimization, signaling a potential progression from classical to digital to quantum financial systems [11-15].

2. Qubit-Based Cryptocurrency: An Overview

The development of a cryptocurrency based on quantum bits (qubits) is a nascent field that merges quantum computing with distributed ledger technology.

A. Quantum-Resistant Cryptocurrencies

Current efforts focus primarily on quantum resistance, employing classical PQC algorithms to secure ledgers against future quantum attacks. Examples include:

QRL (Quantum Resistant Ledger): Uses the XMSS (Extended Merkle Signature Scheme).

IOTA: Implements Winternitz one-time signatures (WOTS+).

Algorand: Has plans to integrate quantum-resistant schemes [16, 17].

B. True Qubit-Based Systems

A fully quantum cryptocurrency would use qubits for transactions and consensus. These remain largely theoretical due to significant engineering challenges. Proposed concepts include:

Quantum Blockchains: Ledgers secured by entangled qubits.

Quantum Money: Currency represented by unclonable quantum states, as first proposed by Wiesner [18, 20].

C. Challenges and Potential Architectures

While promising, the path to a functional qubit-based cryptocurrency is fraught with obstacles, as summarized in Table 1.

Table 1: Key Challenges in Qubit Cryptocurrency Development

Challenge	Description
Quantum Decoherence	Qubits lose coherence quickly (microseconds), requiring sophisticated error correction.
Quantum Networking	Requires a quantum internet for long-distance entanglement distribution.
Qubit Storage	No practical quantum RAM exists for long-term qubit storage.
Scalability	Current Noisy Intermediate-Scale Quantum (NISQ) processors have insufficient qubit counts for global ledgers.
Classical Interface	Hybrid systems require secure and efficient classical-quantum communication bridges.

A hybrid quantum-classical architecture presents a pragmatic transitional model. Such networks enhance cybersecurity by leveraging Quantum Key Distribution (QKD) and other quantum protocols to provide superior data confidentiality, integrity, and availability, bridging the gap between today's infrastructure and a future quantum internet [21].

3. Quantum Threats to Classical Cryptocurrencies

Quantum computing presents a clear and present danger to existing cryptocurrencies. Shor's algorithm can break the Elliptic Curve Digital Signature Algorithm (ECDSA) used by Bitcoin and Ethereum, compromising wallet security. Grover's algorithm, while less devastating, can

speed up brute-force attacks, necessitating a doubling of key sizes in symmetric encryption [22, 24]. Using the basics of blockchain, the most relevant BIoT applications are described with the objective of emphasizing how blockchain can impact traditional cloud-centered IoT applications. (Fig.1).

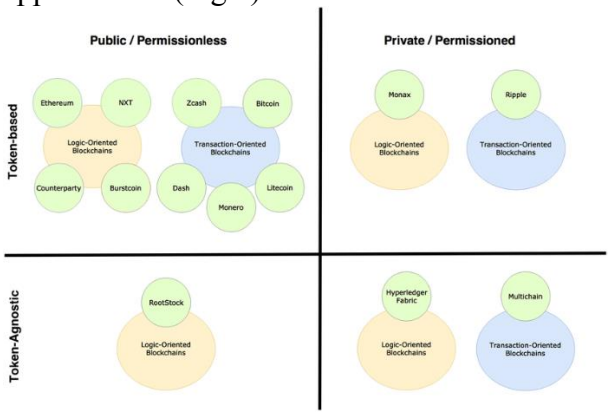

Fig. 1. Blockchain taxonomy and practical examples. [23].

The timeline for these threats underscores the urgency of adopting PQC standards. NIST's ongoing standardization process is a critical step in protecting digital infrastructure, including cryptocurrencies, from future quantum attacks [24-27].

4. Quantum Mining: Energy and Hardware Economics

Quantum computing could revolutionize cryptocurrency mining by drastically improving energy efficiency and computational throughput. The evolution from classical to quantum mining is projected to follow the pathway illustrated in Fig. 2, moving from energy-intensive Application-Specific Integrated Circuits (ASICs) to more efficient quantum and quantum-annealing systems.

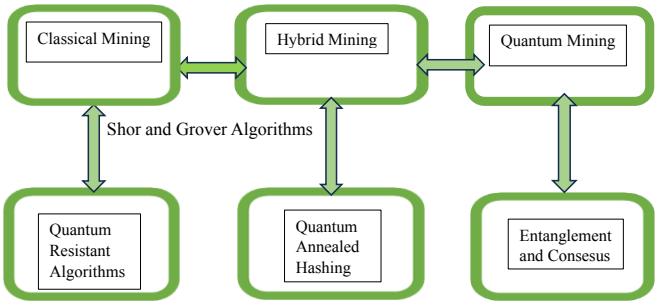

Fig. 2. Schematic representation of possible development pathways for qubit-based cryptocurrency mining. Evolution from classical to hybrid and quantum: Classical Mining (Pre-Quantum Era); Transitional Hybrid Mining (Today); Fully Quantum Mining (Nearest Future) is shown at the figure 2. [28}.

Table 2: Comparative Analysis of Mining Electricity Consumption

Mining Type	Example Currencies	Power Consumption	Hardware	Energy Efficiency
Classical	Bitcoin, Ethereum	~100 TWh/year	ASICs, GPUs	~30-50 J/TH
Hybrid	Bitcoin, Ethereum, Qubitcoin	~0.01 TWh/year	FPGAs/ASICs with PQC cores	~100-500 kWh/tx
Quantum-Annealer	Qubitcoin	~25 kW/system	Cryogenic Systems	Qubit Count: 5,000-7,000
Full Quantum	Qubitcoin	~500 kW–1 MW (per system)	Cryogenic/Optical	Hashing Acceleration: 10-100x

In the short term, quantum mining's energy cost is dominated by cryogenic cooling.

However, long-term advancements in qubit stability and error correction could make quantum mining significantly more energy-efficient than classical ASIC-based mining, offering a greener alternative for blockchain consensus [29-31].

5. Quantum Money: A New Economic Paradigm

"Quantum money" is a radical monetary concept where the unit of currency is an unclonable quantum state, secured by the no-cloning theorem of quantum mechanics [20]. This introduces a fundamental shift from classically-based digital currency.

Table 3: Classical vs. Quantum Money

Classical Money	Quantum Money
Easily copied, high counterfeit risk	Physically impossible to counterfeit
Verified by trusted third parties	Verified via quantum measurement
Based on classical computation	Based on quantum principles (entanglement, superposition)
Traceable with forensic effort	Inherent traceability via entanglement
Vulnerable to digital fraud	Security guaranteed by laws of physics

This innovation could lead to significant economic paradigm shifts, as outlined in Table 4.

Table 4: The Quantum Economic Paradigm Shift

Traditional Feature	Quantum Transition
Security	Fraud and duplication become physically impossible.
Decentralization	Enables central bank-free, trustless monetary systems.
Global Economy	Fosters tamper-proof, transparent financial ecosystems.
Inflation Resistance	Issuance can be tied to quantifiable entangled resource limits.
Automation	Integratable with quantum AI for autonomous economic agents.
Future Implications	Quantum CBDCs, quantum-secure blockchains, and post-capitalist economies based on energy-information exchange.

The lifecycle of quantum money, from minting to verification, is depicted in Fig. 3. An interdisciplinary methodology that weighs R&D costs against long-term energy savings and security benefits (Fig. 4) is crucial for evaluating its economic viability.

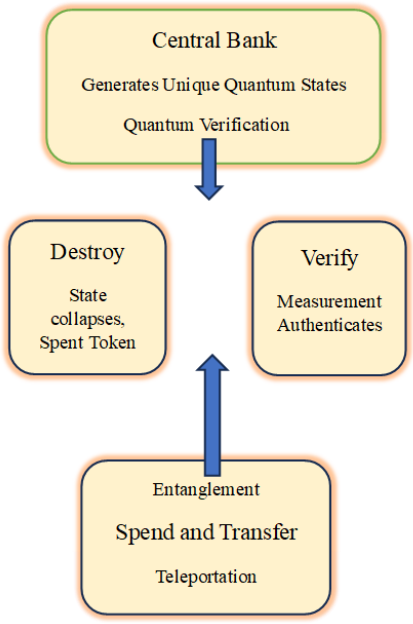

Figure 3: Quantum Money Lifecycle

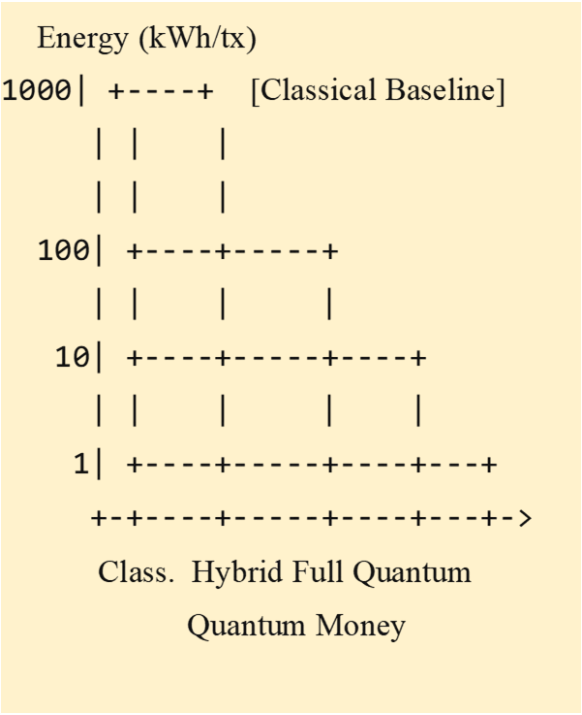

Fig. 4: Economic advantage of qubitcoins

6. Discussion and Future Trajectory

The integration of quantum computing into cryptocurrency will be phased and paradoxical—both disruptive and evolutionary. The transition will begin with quantum-resistant defenses and gradually evolve into native quantum monetary systems. Key takeaways include:

- Unclonable quantum states enable unforgeable money but require breakthroughs in quantum memory.
- Publicly verifiable quantum money avoids central banks but remains experimentally challenging.
- Large-scale quantum computers may demand 1–10 MW of power, comparable to small data centers.
- Economies that proactively navigate this transition will be well-positioned to reap the rewards, while those that delay face significant risks.

7. Case Study: A Hypothetical Quantum Laundering Scheme

As an academic exercise, we explore a hypothetical quantum laundering scheme that exploits quantum properties to evade classical blockchain analysis.

A. Concept: This scheme would use a Quantum Obfuscation Network (QON) to:

Convert classical crypto assets into quantum-encoded assets (e.g., "Qubitcoins").

Use superposition and entanglement to split and correlate funds across a network of nodes, making the transaction path non-deterministic.

Exploit quantum teleportation to move value without a classical network trail.

Convert the "cleaned" quantum assets back into classical currency at untraceable wallets.

B. Evasion Techniques: The QON would employ techniques such as:

Dynamic Entanglement Cascades: Wallets are cross-entangled, preventing linear tracking.

Quantum Zeno Effect: To control and jitter transaction timing.
Quantum Zero-Knowledge Proofs: To prove laundering completion without revealing the method.
This creates a "Heisenberg black market," where the origin and path of funds cannot be simultaneously determined (Fig. 5).

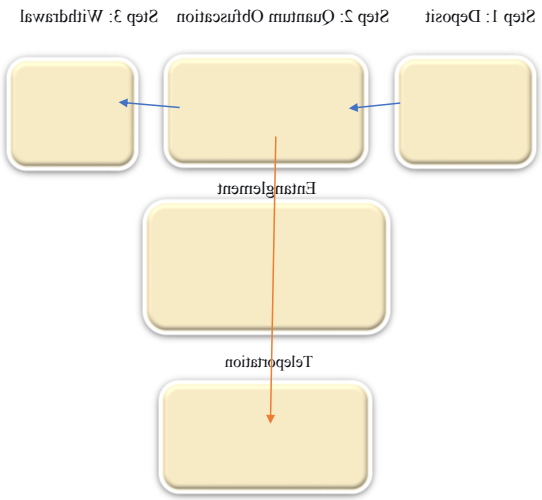

Fig.5. Quantum Obfuscation Network (QON): A theoretical model for quantum laundering. The process exploits quantum superposition and entanglement to break the deterministic transaction history of a classical blockchain, followed by quantum teleportation to obfuscate the transfer path.

This hypothetical scenario highlights the dual-use nature of quantum technology. While quantum computing could enable "unbreakable" anonymity for illicit activities, it could equally empower "hyper-transparent" ledgers through quantum auditing tools. The balance of this future will be determined by which actors—regulators or malicious ones—successfully deploy these technologies first.

References

[1] R. P. dos Santos, "Quantum Information Science," *IEEE Internet Computing*, vol. 26, no. 4, pp. 1-8, Jul./Aug. 2022.
[2] P. J. Kervalishvili, "Quantum information science: some novel views," in *Information and Computer Technologies*. New York, NY, USA: Nova Science Publishers, 2012, pp. 114-132.
[3] W. H. Zurek, "Decoherence, einselection, and the quantum origins of the classical," *Rev. Mod. Phys.*, vol. 75, no. 3, pp. 715–775, May 2003.
[4] P. J. Kervalishvili, "Quantum information technology: Theory and applications," in *Proc. 2015 IEEE Seventh Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Cairo, Egypt, Dec. 2015, pp. 1-15.
[5] P. J. Kervalishvili, "Leptons Based Quantum Computing," *Acta Scientific Computer Sciences*, vol. 5, no. 7, pp. 12-14, Jun. 2023.
[6] L. Soni, H. Chandra, D. S. Gupta, P. K. Mishra, and S. K. Mishra, "Quantum-resistant public-key encryption and signature schemes with smaller key sizes," *Cluster Comput.*, vol. 27, pp. 285–297, Jan. 2024.
[7] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization," 2022. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography.
[8] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Santa Fe, NM, USA, Nov. 1994, pp. 124-134.
[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, Philadelphia, PA, USA, May 1996, pp. 212-219.
[10] Entrust Datacard, "The quantum computer and its implications for public-key crypto systems," White Paper, 2019.
[11] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography*. Berlin, Germany: Springer, 2009, pp. 147–191.
[12] M. G. Selvaraj et al., "Quantum blockchain: Trends, technologies, and future directions," *IET*

Quantum Commun., vol. 5, no. 4, pp. 516-542, Dec. 2024.
[13] I. Barmes, B. Bosch, and O. Haalstra, "Quantum computers and the Bitcoin blockchain," Deloitte, 2025.
[14] S. Aaronson, *Quantum Computing Since Democritus*. Cambridge, U.K.: Cambridge Univ. Press, 2013.
[15] B. Morenne, "Machines That Shop for Themselves Promise to Save Time and Money," *The Wall Street Journal*, Apr. 7, 2021. [Online]. Available: https://www.wsj.com/articles/machines-that-shop-for-themselves-promise-to-save-time-and-money-11617771601.
[16] S. Almuhammadi and S. Alghamdi, "A novel transition protocol to post-quantum cryptocurrency blockchains," *Front. Comput. Sci.*, vol. 7, May 2025, Art. no. 1457000.
[17] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. Torshizi, and W. J. Knottenbelt, "Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack," *R. Soc. Open Sci.*, vol. 5, no. 6, Jun. 2018, Art. no. 180410.
[18] S. Aaronson and P. Christiano, "Quantum Money from Hidden Subspaces," in *Proc. 44th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, 2012, pp. 41-60.
[19] A. W. Harrow, "The Second Quantum Revolution," *Physics at MIT*, pp. 20-25, 2021. [Online]. Available: https://physics.mit.edu/wp-content/uploads/2021/01/physicsatmit_13_farhiharrow.pdf.
[20] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.
[21] B. T. Geetha, R. Viswanathan, S. N. Patel, M. A. Mukunthan, and S. Jindal, "Hybrid Quantum-Classical Communication Networks: New Directions In Cybersecurity," *Nanotechnol. Percept.*, vol. 20, no. S12, pp. 632-645, 2024.
[22] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.
[23] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979-33001, May 2018.
[24] G. Alagic et al., "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST IR 8413, Jul. 2022.
[25] F. Wu, B. Zhou, J. Jiang, and T. Lei, "Blockchain Privacy Protection Based on Post Quantum Threshold Algorithm," *Comput. Mater. Contin.*, vol. 76, no. 1, pp. 109-125, 2023.
[26] IBM, "What Is Quantum Computing?," Jun. 10, 2025. [Online]. Available: https://www.ibm.com/topics/quantum-computing.
[27] McKinsey & Company, "The energy challenge in quantum computing," 2023. [Online].
Available: https://www.mckinsey.com/industries/semiconductors/our-insights/the-energy-challenge-in-quantum-computing.
[28] P. Kervalishvili, M. Tavkhelidze. "Future of cryptocurrency based on quantum computing: economical viewpoint." Norwegian Journal of development of the International Science', No 161/2025. pp. 20-27.
[29] D-Wave Quantum, "The first and only quantum computer built for business," 2024. [Online].
Available: https://www.dwavequantum.com.
[30] Financial Action Task Force (FATF), "Crypto compliance risks & gaps," Report, Mar. 2025.
[31] A. Broadbent, R. A. Kazmi, C. Minwalla, M. Z. M. Khan, and V. Gheorghiu, "A Quantum Vault Scheme for Digital Currency," in *Proc. 2024 IEEE Int. Conf. Quantum Comput. Eng.*, Brisbane, Australia, Sep. 2024.