Critique: Quantum Money and Inflation Control

A Critical Analysis of Our First Report

PHYS-C191A: Quantum Information Science
October 23, 2025

1 Summary and Evaluation

Our first report examined quantum money as an alternative to Bitcoin, proposing four inflation control mechanisms: computational difficulty adjustment, state space restriction, chain-based validation, and hybrid approaches. While the report successfully articulated the conceptual shift from computational to physical security, it contained critical technical ambiguities and omitted practical considerations essential for implementation.

2 Critical Technical Issues

2.1 Computational Difficulty Adjustment

The report's notation $H(|\psi\rangle) < D$ lacks precise definition. In quantum contexts, "quantum hash function" could mean either: (1) measurement-based hashmeasure $|\psi\rangle$ to get classical outcomes $\vec{m}$, then compute $h(\vec{m}) < D$; or (2) unitary hash operator applied before measurement. Without specifying the measurement basis, the scheme's collision resistance remains unclear. Additionally, the difficulty adjustment formula assumes linear scaling between difficulty and generation time, but if quantum circuit depth is rate-limiting, this relationship may be nonlinear.

2.2 State Space Restriction

The report's claim that tokens are "coherent superpositions $|\psi_{\text{valid}}\rangle = \sum_{i=1}^{N} \alpha_i |\phi_i\rangle$" creates a fundamental contradiction: if arbitrary coefficients α_i are allowed, the state space is infinite (continuous manifold), not finite. **Resolution:** Tokens must be discrete orthogonal basis states $|\phi_i\rangle$, not arbitrary superpositions, to achieve a true hard cap of N distinguishable tokens. The reference to "quantum fingerprinting" was also imprecisequantum error-correcting codes provide the correct framework.

2.3 Chain-Based Validation

Critical flaw: The scheme $|\psi_n\rangle = U_n(\vec{m}_{n-1}) |\phi_{\text{seed}}\rangle$ requires measuring $|\psi_{n-1}\rangle$ to obtain $\vec{m}_{n-1}$, which destroys the previous state. This makes the system deflationary (each minting destroys a token) and creates a sequential bottleneck. **Solutions:** (1) entanglement-based chaining using EPR pairs; (2) quantum state tomography with partial measurements; or (3) Gottesman-Chuang quantum signatures allowing non-destructive verification.

2.4 Hybrid Mechanisms

The two-tier architecture lacks detail on redemption: how Layer 2 tokens convert to Layer 1 requires a burn-and-mint protocol with dynamic exchange ratesessentially quantum fractional reserve banking. This complexity demands careful economic modeling absent from the report.

3 Areas for Future Development

Several important practical considerations remain to be addressed in future revisions. **Decoherence and error correction**: A complete analysis should specify requirements for maintaining quantum state coherence over extended pmaintaining quantum state coherence over extended periods, including the threshold for logical error rates (estimated below 10^{-15} per operation) needed for practical implementation. **Quantum communication infrastructure**: The mechanisms for transferring quantum money tokens between partieswhether through quantum teleportation or direct quantum channelswarrant detailed discussion, as they determine the feasibility of transaction networks. **Game-theoretic security**: Future work should analyze potential attack vectors such as selfish mining and nothing-at-stake scenarios, establishing robustness against rational adversarial behavior.

3.1 Establishing and Maintaining Quantum Currency Value

An important direction for future work is understanding how quantum currency would acquire and maintain value once technically feasible. In classical and digital economies, value emerges from collective trust, scarcity, and exchange utility. For quantum money, scarcity is enforced by physical laws,[1] yet market confidence and convertibility remain essential for any stable monetary system.

Future iterations could explore several approaches: pegging initial token values to classical benchmarks (such as stablecoins or fiat currencies) to enable early liquidity through exchange markets;[2] allowing value to evolve independently based on transaction demand, verification costs, and infrastructure reliability;[3] or anchoring value in the computational or physical resources required for mintinga "quantum energy cost" model.[4]

However, resource-based valuation alone may introduce volatility similar to early cryptocurrencies. A more robust framework might integrate multiple policy instrumentscontrolled redemption, staking incentives, or algorithmic stabilization mechanisms inspired by post-quantum cryptoeconomic systems.[5] Developing a comprehensive treatment of value establishment, transfer, and stabilization represents an essential next step toward transforming quantum money from theoretical construct to functioning economic system.

4 Conclusion

While the report successfully identified quantum money's conceptual foundationreconciling physical unforgeability with economic scarcitythe technical details require substantial refinement. The measurement problem in chain-based validation is particularly critical, and the gap between theoretical mechanisms and practical implementation (decoherence, infrastructure, economic value) remains vast. Future work must address these issues through both theoretical clarification and experimental validation before quantum money can transition from elegant theory to practical reality.

[1] Stephen Wiesner, "Conjugate Coding," Original manuscript written circa 1970, *ACM SIGACT News* 15, no. 1 (1983): 78–88, https://doi.org/10.1145/1008908.1008920.

[2] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin.org*, 2008, https://bitcoin.org/bitcoin.pdf.

[3] Mark Zhandry, "Quantum Lightning Never Strikes the Same State Twice," *arXiv:1711.02276v3*, 2019, https://arxiv.org/abs/1711.02276.

[4] Alexandru Gheorghiu and Michele Mosca, "Quantum Money from Modular Forms," *Quantum* 6 (2022): 830, https://doi.org/10.22331/q-2022-09-20-830.

[5] Gorjan Alagic, Stacey Jeffery, and Alex Lombardi, "Post-Quantum Money: Classical Cryptography Meets Quantum Verification," in *Proceedings of TQC 2023* (2023), https://doi.org/10.4230/LIPIcs.TQC.2023.3.

References

Alagic, Gorjan, Stacey Jeffery, and Alex Lombardi. “Post-Quantum Money: Classical Cryptography Meets Quantum Verification.” In *Proceedings of TQC 2023.* 2023. https://doi.org/10.4230/LIPIcs.TQC.2023.3.

Gheorghiu, Alexandru, and Michele Mosca. “Quantum Money from Modular Forms.” *Quantum* 6 (2022): 830. https://doi.org/10.22331/q-2022-09-20-830.

Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin.org*, 2008. https://bitcoin.org/bitcoin.pdf.

Wiesner, Stephen. “Conjugate Coding.” Original manuscript written circa 1970, *ACM SIGACT News* 15, no. 1 (1983): 78–88. https://doi.org/10.1145/1008908.1008920.

Zhandry, Mark. “Quantum Lightning Never Strikes the Same State Twice.” *arXiv:1711.02276v3*, 2019. https://arxiv.org/abs/1711.02276.