Quantum Money and Inflation Control: Theoretical Frameworks for Decentralized Quantum Currency

Topic Choice: Quantum Money

Juncheng Ding, Tian Ariyaratrangsee, Xiaoyang Zheng

Abstract

This report explores the transition from classical cryptocurrencies to quantum money, focusing on inflation control mechanisms. While Bitcoin's security relies on computational assumptions vulnerable to quantum attacks, quantum money leverages the no-cloning theorem for physical unforgeability. We review centralized (Wiesner) and decentralized (Quantum Lightning) architectures, then propose four theoretical strategies to prevent uncontrolled currency issuance: computational difficulty adjustment, state space restriction, chain-based validation, and hybrid economic mechanisms. Each exploits distinct quantum properties to regulate monetary supply. While promising theoretically, substantial technological challenges remain before practical implementation.

Keywords: bitcoin, quantum money, quantum lightning, inflation control, no-cloning theorem, quantum cryptography.

1 From Bitcoin to Quantum Money

Bitcoin pioneered decentralized digital currency through blockchain and Proof of Work,[1] where computational difficulty ensures scarcity and network consensus maintains security. However, its classical cryptographic foundationsrelying on the hardness of integer factorization and discrete logarithmsare vulnerable to quantum algorithms like Shor's[2] and Grover's,[3] threatening its long-term viability.

Quantum money offers a fundamentally different approach: leveraging the no-cloning theorem of quantum mechanics,[4] where the physical impossibility of copying unknown quantum states guarantees unforgeability. Unlike Bitcoin's computational security, quantum money grounds trust in the laws of nature itself. While current implementations face practical challengesquantum state fragility, specialized hardware requirementsthe paradigm represents a conceptual leap toward physics-based currency systems.

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

2. Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing* 26, no. 5 (1997): 1484–1509, https://doi.org/10.1137/S0097539795293172.

3. Lov K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, 212–219, https://doi.org/10.1145/237814.237866.

4. Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010), https://doi.org/10.1017/CBO9780511976667.

2 Architectures of Quantum Money: Centralized Schemes and Quantum Lightning

2.1 Centralized Quantum Money

Stephen Wiesner's foundational scheme[5] uses a trusted bank to issue quantum banknotes, each consisting of a classical serial number paired with a quantum state in random non-orthogonal bases. The bank maintains a private database for verification. While the no-cloning theorem prevents counterfeiting, this design suffers from centralization: all verification requires the bank, creating scalability and privacy bottlenecks unsuitable for large-scale decentralized economies.

2.2 Quantum Lightning and Public-Key Verification

Mark Zhandry's Quantum Lightning framework[6] addresses centralization through publicly verifiable quantum money. Each currency unit is a unique quantum "bolt"a state that cannot be recreated even by its generator. Using collision-resistant quantum hash functions, the system ensures no two identical bolts can exist. Verification is public: any party can run a polynomial-time quantum algorithm to validate authenticity.

The key innovation is self-scarcity: without a central issuer, duplication remains physically and algorithmically impossible. This makes Quantum Lightning the quantum analogue of decentralized cryptocurrencies, with scarcity emerging from quantum mechanics rather than computational cost.

3 Preventing Infinite Minting and Inflation

Despite solving the problem of counterfeiting, a new challenge emerges in decentralized quantum money: how to prevent uncontrolled currency creation. If any participant could generate valid quantum bolts at will, the monetary supply would inflate indefinitely, destroying the currency's value. Thus, quantum money must incorporate a mechanism to regulate issuance the equivalent of Bitcoin's mining difficulty or fiat monetary policy.

Several strategies have been proposed to address this issue, each with distinct technical implementations.

3.1 Computational Difficulty Adjustment

One straightforward method is to tie the generation of valid quantum states to a hard computational problem. In Zhandry's formulation,[7] a bolt is valid only if it satisfies a specific public hash condition that is, it is a quantum state whose measurement outcomes correspond to a preimage of a cryptographic hash value. Because finding such states is computationally difficult, this naturally limits the rate of new currency creation. The difficulty level can be adjusted dynamically, analogous to Bitcoin's mining difficulty, thereby maintaining a stable rate of issuance.

Technical Implementation: Consider a quantum money scheme where a valid state $|\psi\rangle$ must satisfy $H(|\psi\rangle) < D$, where H is a quantum-accessible hash function and D is a difficulty threshold. The minting process involves:

1. *Quantum State Preparation:* Generate a trial quantum state $|\psi_{\text{trial}}\rangle$ using a parameterized quantum circuit with random inputs.

2. *Hash Verification:* Apply the quantum hash operator $\hat{H}$ and measure the output. If the result falls below the target difficulty D, the state is accepted as valid currency.

5. 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.

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

7. Zhandry.

3. *Dynamic Adjustment:* The difficulty parameter D is updated every N blocks based on the actual issuance rate versus the target rate: $D_{n+1} = D_n \times \frac{T_{\text{target}}}{T_{\text{actual}}}$, where T represents time intervals.

This mechanism mirrors Bitcoin's halving schedule but operates at the quantum level. The key advantage is that the quantum hash function can be designed to be collision-resistant even against quantum adversaries, using techniques from quantum cryptography such as quantum-secure one-way functions or extractable witness encryption. The computational cost of finding valid states grows exponentially with the difficulty parameter, ensuring that the currency supply expands at a controlled, predictable rate regardless of advances in quantum computing power.

3.2 Restricting the Quantum State Space

Another approach is to constrain the set of admissible quantum states. If the system's hash function or verification operator defines only a finite number of valid states, then the total monetary supply is inherently capped. This approach imposes scarcity directly at the level of the underlying Hilbert space only a limited number of orthogonal states satisfy the verification criteria, preventing inflation by physical limitation rather than protocol-level enforcement.

Technical Implementation: Define the monetary state space as a finite-dimensional subspace $\mathcal{H}_{\text{money}} \subset \mathcal{H}$ of the full Hilbert space. Specifically:

1. *Orthogonal Basis Construction:* Select a finite set of N mutually orthogonal quantum states $\{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_N\rangle\}$ that form a complete basis for $\mathcal{H}_{\text{money}}$. These states are chosen such that they are eigenstates of a specially designed verification operator $\hat{V}$ with distinct eigenvalues.

2. *Superposition Encoding:* Each valid quantum money token is a coherent superposition within this subspace: $|\psi_{\text{valid}}\rangle = \sum_{i=1}^{N} \alpha_i |\phi_i\rangle$, where the coefficients α_i encode a unique serial number via quantum fingerprinting.

3. *Hard Cap Enforcement:* Since the dimensionality is fixed at N, the maximum number of distinguishable (approximately orthogonal) money states is bounded by N. Any attempt to create additional states either falls outside $\mathcal{H}_{\text{money}}$ (and fails verification) or is non-orthogonal to existing tokens (violating uniqueness).

This scheme can be implemented using topological quantum codes or stabilizer codes,[8] where the code space itself acts as $\mathcal{H}_{\text{money}}$. For example, using a quantum error-correcting code with parameters $[[n, k, d]]$, the logical code space has dimension 2^k, providing exactly 2^k orthogonal money states. The verification process checks whether a given state lies within the code space by measuring stabilizer generators.[9] This approach naturally prevents inflation: once all 2^k tokens are issued, no new valid tokens can be created without violating the orthogonality constraint or the code structure.

3.3 Chain-Based or Signature-Based Validation

A more sophisticated strategy involves linking each valid state to the previous one through a chain of quantum signatures.[10] In such a "quantum blockchain," each newly minted bolt contains encoded information derived from the measurement results of earlier bolts. This enforces a chronological issuance order and provides public traceability of the monetary supply. While still theoretical, such

8. Daniel Gottesman and Isaac L. Chuang, "Quantum Digital Signatures," *arXiv preprint quant-ph/0105032*, 2001, https://arxiv.org/abs/quant-ph/0105032.

9. Nielsen and Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition.*

10. Gottesman and Chuang, "Quantum Digital Signatures"; Shalev Ben-David and Or Sattath, "Quantum Tokens for Digital Signatures," *Quantum Information and Computation* 17, nos. 9-10 (2017): 811–831, https://doi.org/10.26421/QIC17.9-10.

chained validation mechanisms could establish decentralized monetary policy enforced entirely by quantum laws and cryptographic consistency.

Technical Implementation: Construct a quantum blockchain where each money state $|\psi_n\rangle$ at position n in the chain satisfies:

$$|\psi_n\rangle = U_n(\vec{m}_{n-1})\,|\phi_{\text{seed}}\rangle \tag{1}$$

where U_n is a unitary operator parameterized by the measurement outcomes $\vec{m}_{n-1}$ obtained from the previous state $|\psi_{n-1}\rangle$, and $|\phi_{\text{seed}}\rangle$ is a fixed initial seed state. The implementation proceeds as follows:

1. *Genesis State:* The blockchain begins with a publicly verifiable genesis state $|\psi_0\rangle$ chosen through a distributed randomness protocol (e.g., quantum coin flipping among founding participants).

2. *Chained Minting:* To mint a new token, a participant must:

   - Obtain the most recent valid state $|\psi_{n-1}\rangle$ from the network
   - Perform a predetermined set of measurements in a specific basis, yielding classical outcomes $\vec{m}_{n-1}$
   - Use these outcomes to parameterize a quantum circuit $U_n(\vec{m}_{n-1})$
   - Apply this circuit to generate the next state: $|\psi_n\rangle = U_n(\vec{m}_{n-1})\,|\phi_{\text{seed}}\rangle$

3. *Public Verification:* Any party can verify the chain by:

   - Starting from the genesis state $|\psi_0\rangle$
   - Sequentially verifying that each subsequent state was correctly derived using the published measurement outcomes
   - Checking that each state passes a collision-resistant quantum hash test

4. *Inflation Control:* The rate of issuance is controlled by making the measurement and circuit-construction process computationally expensive. For instance, the measurement basis can be chosen such that finding outcomes that produce a valid next state (one that passes the hash test) requires solving a computationally hard problem, similar to proof-of-work in Bitcoin.

This approach has several advantages: it provides an immutable audit trail of all currency creation, prevents arbitrary minting by enforcing sequential dependencies, and allows for algorithmic monetary policy through difficulty adjustment of the quantum circuit construction. However, it requires maintaining quantum coherence across the entire blockchain, which presents significant practical challenges with current technology.

3.4 Hybrid Approaches and Economic Mechanisms

Real-world quantum money systems will likely combine multiple anti-inflation strategies. For example, one could implement a two-tier system:

1. *Layer 1 (Base Layer):* Use state space restriction to impose a hard cap on the total number of "primary" quantum tokens. These tokens exist in a fixed-dimensional code space and cannot exceed a predetermined maximum supply.

2. *Layer 2 (Transaction Layer):* Implement computational difficulty adjustment for "secondary" tokens that facilitate everyday transactions. These tokens can be created more freely but require proof-of-work, and they must be periodically redeemed or validated against primary tokens to maintain value.

Additionally, economic mechanisms familiar from traditional monetary policy can be adapted:

- *Quantum Token Burning:* Implement a protocol where tokens can be deliberately destroyed by measuring them in a way that collapses their superposition irreversibly, effectively removing them from circulation
- *Stake-Based Issuance:* Limit minting rights to participants who hold and lock up existing tokens, creating an economic incentive structure that naturally regulates supply
- *Time-Locked Release:* Encode newly minted tokens in quantum states that require a minimum number of quantum operations (and hence time) before they can be verified and spent, preventing sudden supply shocks

Taken together, these strategies demonstrate that even in a physics-based monetary system, economic stability demands regulation whether through difficulty tuning, space limitation, chained validation, or hybrid economic mechanisms. Quantum money thus combines the rigidity of physical unforgeability with the flexibility of algorithmic governance, potentially offering a new paradigm for secure and inflation-resistant value exchange.

4 Conclusion

Quantum money represents a conceptual shift from computational to physical foundations of trust. While Bitcoin relies on computational assumptions vulnerable to quantum attacks, quantum money leverages the no-cloning theorem to guarantee unforgeability through the laws of nature itself.

This report has outlined four theoretical strategies for inflation control: computational difficulty adjustment, state space restriction, chain-based validation, and hybrid mechanisms. Each approach exploits different quantum propertiescomputational hardness, Hilbert space constraints, measurement dependencies, and state collapse irreversibility.

However, substantial obstacles remain. Current quantum technology cannot yet provide the reliable quantum memories, low-noise communication channels, and scalable verification protocols required for practical implementation. The theoretical frameworks presented here require significant experimental validation and technological advancement before quantum money can become viable. Nonetheless, if these challenges are overcome, quantum money could fundamentally redefine digital currency as an embodiment of physical law rather than computational convention.

References

Ben-David, Shalev, and Or Sattath. "Quantum Tokens for Digital Signatures." *Quantum Information and Computation* 17, nos. 9-10 (2017): 811–831. https://doi.org/10.26421/QIC17.9-10.

Gottesman, Daniel, and Isaac L. Chuang. "Quantum Digital Signatures." *arXiv preprint quant-ph/0105032*, 2001. https://arxiv.org/abs/quant-ph/0105032.

Grover, Lov K. "A Fast Quantum Mechanical Algorithm for Database Search." *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, 212–219. https://doi.org/10.1145/237814.237866.

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

Nielsen, Michael A., and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. https://doi.org/10.1017/CBO9780511976667.

Shor, Peter W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." *SIAM Journal on Computing* 26, no. 5 (1997): 1484–1509. https://doi.org/10.1137/S0097539795293172.

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.