Quantum Money and Inflation Control

Final Project Proposal for PHYS C191A

Juncheng Ding, Tian Ariyaratrangsee, Xiaoyang Zheng
University of California, Berkeley – Fall 2025

1. Problem Statement

The quantum no-cloning theorem prevents copying states but not unlimited generation of new valid quantum money states. As quantum power $Q(t)$ grows, generation rate $R \propto Q/D$ yields unbounded supply $M(t) \to \infty$—**quantum inflation** (Zhandry 2017). Recent theoretical work (Coladangelo & Sattath 2020) coupled quantum states to classical systems for supply control, but left open *physical implementation*.

Our Approach: We investigate whether **quantum circuit complexity** naturally limits state generation through: (1) inflation dynamics modeling via circuit parameters; (2) Resource Token (RT) mechanism using physical constraints (gates, coherence, ancillas); (3) NISQ implementation demonstrating bounded $M(t) \to M_{\max}$.

2. Technical Approach

2.1 Quantum Lightning Framework & Inflation Dynamics

Zhandry's Quantum Lightning: each currency unit $|\psi_i\rangle$ is a superposition over polynomial-degree hash pre-images. Verification: public hash H with criterion $H(|\psi_i\rangle) < D$.

Unbounded Case: Fixed difficulty D, growing capability $Q(t) = Q_0 e^{\lambda t}$ (quantum Moore's law), probability $P \sim Q/2^D$ gives:

$$\frac{dM}{dt} = \frac{Q_0 e^{\lambda t}}{2^D} \quad \Rightarrow \quad M(t) \sim e^{\lambda t}.$$

2.2 Resource Token (RT) Mechanism — Quantum Complexity Constraints

Principle: Couple generation to *physical quantum resources*. For bolt $|\psi_y\rangle$ with circuit depth L, G gates on m qubits:

$$\mathrm{RT}_{\mathrm{cost}} = \alpha G + \beta L + \gamma m, \quad M_{\max} = \frac{R_{\mathrm{total}}}{\langle \mathrm{RT}_{\mathrm{cost}} \rangle}.$$

Three Physical Implementations: (A) *Gate-Count*: $\mathrm{RT} = \alpha G + \beta L$; tracks computational complexity via Qiskit transpilation. (B) *Decoherence-Limited*: $\mathrm{RT} = \gamma \int_0^T \Gamma(t)dt$; models hardware errors from T_1, T_2 times. (C) *Ancilla Budget*: Finite N_{ancilla} pool; each generation consumes a ancillas (NISQ-realistic).

Protocol: (1) Initialize seed $|\phi_0\rangle$, allocate RT; (2) Apply U_{mint} circuit; (3) Measure serial s, verify $|\langle\psi|\psi_s|\psi|\psi_s\rangle|^2 > 1 - \epsilon$; (4) Deduct RT based on (G, L, m); (5) Adjust $D(t)$ if $R_{\mathrm{obs}} > R_{\mathrm{target}}$.

Security: Under $(2k+2)$-NAMCR for degree-2 polynomials, RT preserves quantum lightning uniqueness. Adversaries cannot: clone states (no-cloning); generate non-affine multi-collisions (NAMCR); bypass RT (circuit measurement enforced).

2.3 NISQ Implementation Strategy

Parameters: Toy ($n = 3, k = 2, m = 12$) requires $\sim$36 qubits (IBM/IonQ accessible). Degree-2 polynomial hash over $\mathbb{F}_2$ with Zhandry verification via Hadamard transforms.

Circuits: Generation: seed $\to$ polynomial evaluation $\to$ Grover-like amplification. Verification: measure y, Hadamard for derivatives, solve linear system. RT: Qiskit transpiler tracks (G, L); noise model estimates $\Gamma(t)$.

Study: Compare unbounded (fixed D) vs. RT-bounded (adaptive R_{avail}). Run 1000 attempts; measure supply $M(t)$, RT depletion rates, verification fidelity.

2.4 Validation Framework

Mathematical Model: Derive coupled differential equations:

$$\frac{dM}{dt} = R(Q, D, R_{\text{avail}}), \quad \frac{dR_{\text{avail}}}{dt} = -\langle \mathrm{RT}_{\text{cost}} \rangle \cdot R,$$

where $R = \min\{Q/2^D, R_{\text{avail}}/\mathrm{RT}_{\text{cost}}\}$. Solve numerically; show equilibrium $M_\infty = R_{\text{total}}/\langle \mathrm{RT} \rangle$ is stable.

Qiskit Simulation: Compare quantum growth scenarios $\lambda \in \{0.1, 0.5, 1.0\}$ (annual doubling to monthly) across RT budgets $R_{\text{total}} \in \{10^3, 10^5\}$. Implement all three RT variants (gate, decoherence, ancilla) with realistic noise models from IBM hardware.

Physics Metrics:

- **Inflation reduction:** $I_{\text{RT}}/I_{\text{unbounded}} < 0.01$ (target: 99% suppression)
- **Circuit complexity:** Verify $O(n^3)$ gate scaling via log-log regression
- **Fidelity dependence:** Measure success rate vs. hardware error rates $(10^{-2}, 10^{-3}, 10^{-4})$
- **Resource efficiency:** Compare RT costs across three implementations; identify optimal for NISQ

2.5 Expected Deliverables

(1) Analytical solutions for $M(t)$ in unbounded and RT-bounded regimes with stability proofs; (2) Qiskit implementation of miniaturized quantum lightning with all three RT variants; (3) Comparative plots: supply curves, RT depletion rates, fidelity sensitivity; (4) Circuit complexity analysis confirming polynomial scaling; (5) Discussion of physical feasibility: qubit requirements, coherence time constraints, error mitigation needs.

3. Expected Outcomes

- Demonstration of unbounded inflation $M(t) \sim e^{\lambda t}$ in baseline quantum lightning model
- Proof-of-concept showing RT-based quantum resource constraints achieve bounded $M(t) \to M_{\max}$
- NISQ-compatible Qiskit circuits implementing polynomial hash verification on <50 qubits
- Quantitative comparison: gate-count vs. decoherence vs. ancilla-based RT mechanisms
- Analysis of quantum hardware requirements: optimal circuit depth, error rates, qubit connectivity
- Connection to broader quantum complexity theory: linking no-cloning to computational resource bounds

4. Timeline

Date	Milestone
Oct 30	Finalize proposal; set up Qiskit environment
Nov 10	Implement baseline model; validate exponential inflation
Nov 17	Study Zhandry's verification protocol; design RT circuits
Nov 24	Implement & test three RT mechanisms (gate, decoherence, ancilla)
Nov 30	Run comparative simulations; analyze circuit complexity
Dec 5	Complete report with physics analysis; prepare poster
Dec 9	Poster presentation & defense

5. Division of Labor

Xiaoyang Zheng: Theoretical development (no-cloning under RT, Lindblad dynamics, Lyapunov stability), quantum algorithm simulation in Qiskit (Grover, HHL, SWAP test, noise modeling), project integration, LaTeX report writing.
Tian Ariyaratrangsee: Poster design and presentation, quantum circuit complexity calculations (gate counts, depth analysis, scaling verification), circuit implementation (oracle construction, gate decomposition, transpilation), Fisher information analysis.
Juncheng Ding: Inflation dynamics modeling (ODE derivation, scipy numerical integration), mathematical analysis (equilibrium computation, convergence rates, Jacobian eigenvalues), comparative simulation (9-scenario parameter sweep), RT mechanism feasibility studies.

6. Evaluation Criteria & Risk Mitigation

Success Criteria: (1) Clear demonstration of >99% inflation reduction under RT constraints; (2) Stable equilibrium $M_{\max}$ achieved; (3) Circuit complexity confirms polynomial scaling $O(n^3)$; (4) All simulations complete within Qiskit's computational limits.

Risks: Circuit too large for simulation (mitigation: use $n = 2$ toy parameters); RT mechanism breaks quantum security (mitigation: formal no-cloning proof); Time constraints (priority: baseline + one RT variant as minimum viable project).

7. References

- Wiesner, S. "Conjugate Coding." *ACM SIGACT News*, 15(1), 78–88 (1983).
- Zhandry, M. "Quantum Lightning Never Strikes the Same State Twice." *EUROCRYPT 2019*, arXiv:1711.02276v3.
- Coladangelo, A. & Sattath, O. "A Quantum Money Solution to the Blockchain Scalability Problem." *Quantum*, 4, 297 (2020).
- Aaronson, S. & Christiano, P. "Quantum Money from Hidden Subspaces." *STOC 2012*.
- Lutomirski, A. et al. "Breaking and Making Quantum Money." *ICS 2010*, arXiv:0912.3825.