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 ($\nexists U : U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$) prevents copying but not unlimited generation of new quantum money states in Hilbert space $\mathcal{H} = \mathbb{C}^{2^n}$. As quantum computational power $Q(t)$ grows exponentially, generation rate $R \propto Q/D$ yields unbounded supply—**quantum inflation**. Zhandry (2017) demonstrated quantum lightning (QL) states satisfy cryptographic unforgeability but did not address supply control. Coladangelo & Sattath (2020) proposed blockchain-based tracking but required classical infrastructure.

Our Approach: We investigate whether *intrinsic quantum resource constraints* can bound supply through: (1) **Resource Token (RT) mechanism** coupling generation to physical costs (gate count G, circuit depth L, coherence time T_2, ancilla entanglement χ); (2) **Theoretical analysis** proving bounded equilibrium $M(t) \to M_{\max} = R_{\text{total}}/\langle\text{RT}\rangle$; (3) **Qiskit simulation** on classical hardware validating dynamics under realistic NISQ noise models, demonstrating $> 99\%$ inflation suppression without requiring quantum hardware access.

2. Technical Approach

2.1 Quantum Lightning Framework & Inflation Dynamics

Zhandry's Quantum Lightning: each unit $|\psi_y\rangle = \frac{1}{\sqrt{N_y}} \sum_{x:H(x)=y} |x\rangle$ is superposition over polynomial hash pre-images with $H : \{0,1\}^m \to \{0,1\}^n$ degree-2 over $\mathbb{F}_2$. State purity: density matrix $\rho = |\psi_y\rangle\langle\psi_y|$ has $S(\rho) = -\text{Tr}(\rho \log \rho) = 0$, distinguishing from counterfeit mixed states with $S(\rho_{\text{fake}}) > 0$. Verification protocol: measure in Hadamard basis, apply quantum Fourier transform $\mathcal{F}|x\rangle = 2^{-n/2} \sum_k e^{2\pi i x k/2^n} |k\rangle$, check polynomial constraints via phase estimation (success probability $P_{\text{verify}} \geq 1 - \epsilon$ for $\epsilon = 2^{-\Omega(n)}$).

Inflation Dynamics: Quantum capability growth $Q(t) = Q_0 e^{\lambda t}$ (e.g., logical qubit count scaling, $\lambda \in [0.1, 1.0]$ yr^{-1}). Generation success $P(y) \approx Q/2^D$ from Grover amplitude amplification. Lindblad master equation with decoherence:

$$\frac{d\rho}{dt} = -i[\hat{H}, \rho] + \sum_k \gamma_k \left(L_k \rho L_k^\dagger - \frac{1}{2}\{L_k^\dagger L_k, \rho\} \right), \quad L_k \in \{\sigma_-, \sigma_z\} \text{ (amplitude damping, dephasing)}$$

Unbounded regime ($R_{\text{total}} = \infty$): $\frac{dM}{dt} = \frac{Q_0 e^{\lambda t}}{2^D} \Rightarrow M(t) \sim \frac{Q_0}{\lambda 2^D} e^{\lambda t}$. For $\lambda = 0.5$ yr^{-1}, M doubles every $\ln 2/\lambda \approx 1.4$ years.

2.2 Resource Token (RT) Mechanism

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

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

Three Implementations: (A) *Gate-Count*: $\text{RT} = \alpha G + \beta L$ with rotations $R_\theta(\phi) = e^{-i\theta\sigma_\phi/2}$ and CNOT gates; (B) *Decoherence*: $\text{RT} = \gamma \int_0^T \Gamma(t)dt$ where $\Gamma = 1/T_1 + 1/T_2$, modeled via Kraus operators $\{E_0, E_1\}$; (C) *Ancilla Budget*: finite entangled ancillas $|\Phi^+\rangle$ with Schmidt rank χ consumption.

Quantum Protocol: (1) Initialize $|\phi_0\rangle = |0\rangle^{\otimes m}$, allocate RT; (2) Apply $U_{\text{mint}} = \prod_{j=1}^{L} U_j$; (3) Measure and verify via SWAP test $|\langle\psi_{\text{target}}|\psi_{\text{measured}}|\psi_{\text{target}}|\psi_{\text{measured}}\rangle|^2 > 1 - \epsilon$; (4) Deduct RT via quantum process tomography; (5) Adjust difficulty $D(t)$.

Security: RT preserves quantum lightning uniqueness under $(2k+2)$-NAMCR. Adversaries face: (1) No-cloning (Wootters-Zurek); (2) Multi-collision resistance ($\Omega(2^{n/2})$ queries); (3) Circuit obfuscation lower bounds $\Omega(n \log n)$.

2.3 NISQ Implementation Strategy

Parameters: Toy ($n = 3, k = 2, m = 12$) requires $\sim$36 qubits (IBM Falcon topology). Degree-2 polynomial hash $H(x) = \sum_{i<j} a_{ij} x_i x_j + \sum_i b_i x_i \pmod 2$.

Circuit Design: *Generation*: Grover oracle U_f with diffusion $D = 2\left|+\right\rangle\left\langle+\right|^{\otimes m} - \mathbb{I}$. Total: $G \sim O(m^2\sqrt{2^m/N_y})$ gates. *Verification*: HHL algorithm for matrix inversion, requiring $\kappa(A) \cdot \mathrm{poly}(\log N)$ gates; SWAP test for fidelity $\mathcal{F}$. *RT Tracking*: Qiskit transpiler outputs (G, L); IBM noise: $T_1 \sim 100\,\mu$s, $T_2 \sim 50\,\mu$s, $\epsilon_1 \sim 10^{-3}$, $\epsilon_2 \sim 10^{-2}$.

Study: Simulate unbounded vs. RT-bounded scenarios. Track: supply $M(t)$, RT depletion $R(t)$, fidelity $\mathcal{F}(t)$, entanglement entropy S_{ent} via Pauli tomography.

2.4 Validation Framework

Model: Coupled equations $\frac{dM}{dt} = R(Q, D, R_{\mathrm{avail}})$, $\frac{dR_{\mathrm{avail}}}{dt} = -\langle \mathrm{RT}_{\mathrm{cost}} \rangle \cdot R$, $\frac{d\rho}{dt} = -i[\hat{H}, \rho] + \sum_k \gamma_k \mathcal{D}[L_k]\rho$ where $\mathcal{D}[L]\rho = L\rho L^\dagger - \frac{1}{2}\{L^\dagger L, \rho\}$ (Lindblad dissipator). Solve with quantum trajectory method; show equilibrium $M_\infty = R_{\mathrm{total}}/\langle \mathrm{RT} \rangle$.

Simulation: Scenarios $\lambda \in \{0.1, 0.5, 1.0\}$, $R_{\mathrm{total}} \in \{10^3, 10^5\}$. IBM noise: thermal relaxation (E_0, E_1), depolarizing channel, readout errors.

Metrics: Inflation reduction $I_{\mathrm{RT}}/I_{\mathrm{unbounded}} < 0.01$; circuit complexity $O(n^3)$; fidelity $\mathcal{F} = \mathrm{Tr}(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})^2$; concurrence $C(\rho)$; quantum Fisher information $\mathcal{F}_Q$.

2.5 Deliverables

(1) Analytical solutions with Lyapunov stability proofs; (2) Qiskit circuits with gate decomposition to $\{R_x, R_y, R_z, \mathrm{CNOT}\}$, depth $D \leq 20$, three RT variants transpiled to IBM Falcon; (3) Comparative plots: supply curves, fidelity surfaces $\mathcal{F}(\epsilon, T_1, T_2)$, concurrence decay; (4) Complexity analysis: $O(n^3)$ scaling vs. lower bounds, quantum volume V_Q; (5) Feasibility: qubit requirements ($\sim$36), coherence constraints ($T_2 \gtrsim 100\mu s$), error mitigation strategies.

3. Expected Outcomes

- **Inflation dynamics:** Demonstrate unbounded growth $M(t) \sim e^{\lambda t}$ in baseline model; extract growth rate λ from Liouvillian eigenspectrum

- **RT stabilization:** Show bounded equilibrium $M(t) \to M_{\max} = R_{\mathrm{total}}/\langle \mathrm{RT} \rangle$ with convergence rate $\tau \sim 1/\gamma_{\mathrm{diss}}$; verify no-cloning preservation

- **NISQ circuits:** Implement polynomial hash on $n \leq 6$ qubits (36-qubit system); transpile to IBM Falcon with SWAP overhead $< 20\%$; quantum process tomography confirming $\|\mathcal{E}_{\mathrm{ideal}} - \mathcal{E}_{\mathrm{noisy}}\|_\diamond < 0.15$

- **RT comparison:** Quantify three mechanisms: gate-count (resilient to noise), decoherence (time-limited), ancilla (qubit-intensive)

- **Hardware analysis:** Quantum volume $V_Q = 2^n$; optimal: $D \in [10, 20]$, $\epsilon_1 < 10^{-3}$, $\epsilon_2 < 10^{-2}$

- **Complexity theory:** Link no-cloning to Holevo bound $\chi \leq S(\rho)$; place RT in $\mathrm{BQP}^{\mathrm{NP}}$; explore channel capacity $C(\mathcal{N})$ under constraints

4. Timeline

Date	Milestone
Oct 30 - Nov 3	Literature review; setup (Qiskit 1.0+, Python 3.10+); GitHub repository
Nov 4 - Nov 10	[**Ding**] Derive $M(t)$ solutions, master equation solver; [**Zheng**] Prove no-cloning under RT, Lindblad equations
Nov 11 - Nov 17	[**Tian**] Design circuits: polynomial hash, Grover oracle; [**Zheng**] Implement HHL, SWAP test; gate decomposition
Nov 18 - Nov 24	[**All**] Implement three RT mechanisms; transpile to IBM Falcon; test with noise models
Nov 25 - Nov 30	[**Ding**] Simulations: varying λ, R_{total}; [**Tian**] Complexity analysis, V_Q calculations; [**Zheng**] Process tomography, fidelity
Dec 1 - Dec 5	[**Zheng**] Draft report; [**Tian**] Design poster; [**Ding**] Finalize proofs
Dec 6 - Dec 8	Team review, rehearse presentation, prepare Q&A
Dec 9	Poster presentation & defense; submit report

5. Division of Labor

Xiaoyang Zheng: Theory (no-cloning, Lindblad equations, stability), quantum algorithm simulation (Grover, HHL, SWAP test), project structure, report writing.
Tian Ariyaratrangsee: Poster design, quantum algorithm calculations (gate complexity, circuit depth), circuit implementation (gate decomposition, IBM transpilation), optimization.
Juncheng Ding: Inflation simulation (master equation integration, supply curves), equilibrium calculations, RT mechanism analysis, stability studies.

6. Evaluation & Risk Mitigation

Success: (1) >99% inflation reduction; (2) Stable $M_{\max}$; (3) $O(n^3)$ scaling confirmed; (4) Simulations within Qiskit limits.

Risks: Circuit too large (use $n = 2$ toy); RT breaks security (formal proof); time constraints (baseline + one RT as minimum).

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.