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. As quantum power $Q(t)$ grows exponentially, generation rate yields unbounded supply—**quantum inflation**. Zhandry (2017) proved quantum lightning (QL) unforgeability but lacked supply control. Coladangelo & Sattath (2020) proposed blockchain tracking requiring classical infrastructure.

Our Approach: We investigate *intrinsic quantum resource constraints* for bounded supply via: (1) **Resource Token (RT) mechanism** coupling generation to physical costs (gates G, depth L, coherence T_2, entanglement χ); (2) **Theoretical proof** of equilibrium $M_\infty = R_{\text{total}}/\langle\text{RT}\rangle$; (3) **Qiskit simulation** on classical hardware validating $> 99\%$ inflation suppression under realistic noise.

2. Technical Approach

2.1 Quantum Lightning & Inflation

Each unit $|\psi_y\rangle = N_y^{-1/2}\sum_{x:H(x)=y}|x\rangle$ is superposition over polynomial hash pre-images ($H : \{0,1\}^m \to \{0,1\}^n$, degree-2/$\mathbb{F}_2$). Pure state: $\rho = |\psi_y\rangle\langle\psi_y|$, $S(\rho) = 0$. Verification via quantum Fourier transform, phase estimation ($P_{\text{verify}} \geq 1 - 2^{-\Omega(n)}$).

Inflation: Capability $Q(t) = Q_0 e^{\lambda t}$ ($\lambda \in [0.1, 1.0]$ yr^{-1}). Lindblad $\frac{d\rho}{dt} = -i[\hat{H},\rho] + \sum_k \gamma_k(L_k\rho L_k^\dagger - \frac{1}{2}\{L_k^\dagger L_k, \rho\})$, $L_k \in \{\sigma_-, \sigma_z\}$. Unbounded: $\frac{dM}{dt} = Q_0 e^{\lambda t}/2^D \Rightarrow M(t) \sim e^{\lambda t}$, doubling time $\ln 2/\lambda$.

2.2 Resource Token (RT) Mechanism

Principle: $\text{RT}_{\text{cost}} = \alpha G + \beta L + \gamma m$, $M_{\max} = R_{\text{total}}/\langle\text{RT}_{\text{cost}}\rangle$, $\frac{dM}{dt} = \min\{Q/2^D, R_{\text{avail}}/\text{RT}_{\text{cost}}\}$.

Implementations: (A) *Gate-Count*: $\text{RT} = \alpha G + \beta L$, tracks rotations $R_\theta(\phi) = e^{-i\theta\sigma_\phi/2}$ + CNOT via Solovay-Kitaev ($G = O(\log^c(1/\epsilon))$); (B) *Decoherence*: $\text{RT} = \gamma\int(1/T_1 + 1/T_2)dt$, Kraus $\{E_0 = \sqrt{1-p}\mathbb{I}, E_1 = \sqrt{p}\sigma_-\}$, $p = 1 - e^{-t/T_1}$; (C) *Ancilla*: entangled $|\Phi^+\rangle$, Schmidt rank χ.

Protocol: (1) Init $|0\rangle^{\otimes m}$, check R_{avail}; (2) Apply $U_{\text{mint}} = \prod_{j=1}^{L} U_j$; (3) SWAP test verify $|\langle\psi_{\text{target}}|\psi|\psi_{\text{target}}|\psi\rangle|^2 \geq 1 - \epsilon$; (4) Process tomography via Choi $\rho_{\mathcal{E}} = (\mathcal{E}\otimes\mathbb{I})|\Phi^+\rangle\langle\Phi^+|$ extracts (G, L, m); (5) Deduct RT, adjust $D(t)$.

Security: Under $(2k+2)$-NAMCR, RT preserves QL. Barriers: No-cloning (Wootters-Zurek); multi-collision $\Omega(2^{n/(2k+1)})$ queries; circuit extraction violates $\Omega(n\log n)$ lower bound (adversary method).

2.3 Simulation Strategy

Parameters: Miniaturized toy model ($n = 3, k = 2, m = 12$) for classical simulation (full statevector $2^{12} = 4096$ amplitudes). Polynomial hash $H(x) = \sum_{i<j} a_{ij}x_ix_j + \sum_i b_ix_i \pmod 2$ over $\mathbb{F}_2$. Security: $2^n = 8$ hash values, $\approx 2^{m/2} \approx 64$ pre-images per valid y (birthday bound saturation).

Circuit Design: *Generation*: (1) Hadamard superposition $H^{\otimes m}|0\rangle^{\otimes m} = |+\rangle^{\otimes m}$ (m gates); (2) Oracle $U_f|x\rangle|b\rangle = |x\rangle|b\oplus f(x)\rangle$ implements polynomial via CNOT cascade (depth $O(m^2)$, gate count $G_{\text{oracle}} \sim m(m-1)/2 \approx 66$ for quadratic terms); (3) Grover diffusion $D = 2|+\rangle\langle+|^{\otimes m} - \mathbb{I} = H^{\otimes m}(2|0\rangle\langle 0|^{\otimes m} - \mathbb{I})H^{\otimes m}$. Iterations: $O(\sqrt{2^m/N_y}) \approx \sqrt{64} = 8$. Total complexity: $G \sim O(m^2\sqrt{2^m/N_y})$, $L \sim O(\sqrt{2^m/N_y})$ depth. *Verification*: (1) Measure in Z-basis, collapse to $|\psi_y\rangle$; (2) HHL algorithm (Harrow-Hassidim-Lloyd): solve $A\vec{x} = \vec{b}$ for constraint matrix A via quantum phase estimation + controlled rotations, complexity $O(\kappa(A)\log N)$ where κ is condition number (assume $\kappa \sim 10$ for well-conditioned polynomial systems); (3) SWAP test: $|\langle\psi|\phi|\psi|\phi\rangle|^2 = \frac{1+\langle\text{SWAP}\rangle}{2}$ via controlled-SWAP + ancilla measurement.

Noise Models (Qiskit AerSimulator): (1) *Thermal relaxation*: Kraus $E_0 = \begin{pmatrix}1 & 0\\ 0 & \sqrt{1-p}\end{pmatrix}$, $E_1 = \begin{pmatrix}0 & \sqrt{p}\\ 0 & 0\end{pmatrix}$, $p = 1 - \exp(-t_{\text{gate}}/T_1)$. Typical: $T_1 = 100\mu s$, $t_{\text{gate}} = 50ns \Rightarrow p \sim 5\times 10^{-4}$. (2) *Depolarizing*: $\mathcal{E}(\rho) = (1-p)\rho + \frac{p}{3}\sum_{i=x,y,z}\sigma_i\rho\sigma_i$, single-qubit $p_1 = 10^{-3}$, two-qubit $p_2 = 10^{-2}$. (3) *Readout error*: confusion matrix $M_{ij} = P(\text{measure } j|\text{state } i)$, off-diagonal $\sim 1\%$.

Comparative Study: Scenarios: $\lambda \in \{0.1, 0.5, 1.0\}$ yr^{-1}, $R_{\text{total}} \in \{10^3, 10^5\}$ tokens. Track: (i) Supply $M(t)$ (unbounded: exponential, RT-bounded: logistic saturation); (ii) RT depletion $R_{\text{avail}}(t)$; (iii) Quantum metrics: fidelity $\mathcal{F}(\rho,\sigma) = [\text{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2$, purity $\text{Tr}(\rho^2)$, concurrence $C(\rho) = \max\{0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\}$ (eigenvalues of $\rho\tilde{\rho}$ where $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$), entanglement entropy $S_{\text{ent}} = -\text{Tr}(\rho_A \log \rho_A)$ for bipartition. Validation: Pauli tomography $\rho = \frac{1}{2^m}\sum_{\vec{\alpha}} \text{Tr}(\sigma_{\vec{\alpha}}\rho)\sigma_{\vec{\alpha}}$ reconstructs ρ from 4^m measurements ($m = 2$ subsystem: 16 Pauli strings).

2.4 Theoretical Validation & Analysis

Mathematical Model: System of coupled ODEs:

$$\frac{dM}{dt} = R_{\text{gen}}(Q, D, R_{\text{avail}}), \quad \frac{dR_{\text{avail}}}{dt} = -\langle \text{RT}_{\text{cost}} \rangle \cdot R_{\text{gen}}, \quad \frac{d\rho}{dt} = -i[\hat{H}, \rho] + \sum_k \gamma_k \mathcal{D}[L_k]\rho$$

where $R_{\text{gen}} = \min\{Q/2^D, R_{\text{avail}}/\text{RT}_{\text{cost}}\}$, $\mathcal{D}[L]\rho = L\rho L^\dagger - \frac{1}{2}\{L^\dagger L, \rho\}$ (Lindblad dissipator), $L_k \in \{\sigma_-, \sigma_z\}$ (jump operators). Solve via: (1) Classical ODE solver (scipy.integrate.odeint) for $M(t)$, $R(t)$ deterministic trajectories; (2) Quantum trajectory Monte Carlo for stochastic $\rho(t)$ including measurement backaction.

Equilibrium Analysis: RT-bounded regime reaches fixed point (M_*, R_*) satisfying $R_{\text{gen}}(M_*, R_*) = 0$. Stability: Lyapunov function $V(M,R) = \frac{1}{2}[(M - M_*)^2 + (R - R_*)^2]$ with $\dot{V} = (M - M_*)\dot{M} + (R - R_*)\dot{R} < 0$ for all $(M, R) \neq (M_*, R_*)$ (proven via Jacobian eigenvalue analysis: $\lambda_{\max} < 0$). Convergence rate $\tau^{-1} \sim |\lambda_{\max}|$ determines relaxation time. Prediction: $M_\infty = R_{\text{total}}/\langle \text{RT}_{\text{cost}} \rangle$ independent of λ; time to reach $M_\infty(1 - e^{-1}) \approx 0.63 M_\infty$ is $\tau \sim (\lambda + \gamma_{\text{diss}})^{-1}$.

Metrics: (1) *Inflation suppression*: $I_{\text{ratio}} = M_{\text{RT}}(t_f)/M_{\text{unbound}}(t_f) < 0.01$ (target: 99% reduction at $t_f = 10$ yr). (2) *Circuit scaling*: Log-log regression confirms $G(m) \sim Am^{3+\delta}$ ($\delta < 0.1$ acceptable), compare to Grover theoretical $\Omega(\sqrt{N})$, Shor $O(\log^3 N)$. (3) *Fidelity decay*: $\mathcal{F}(t) = \mathcal{F}_0 \exp(-\Gamma t)$ where $\Gamma = p_1 G_1 + p_2 G_2$ ($G_{1,2}$ are single/two-qubit gate counts), diamond norm $\|\mathcal{E} - \mathcal{I}\|_\diamond = \sup_\rho \|\mathcal{E}(\rho) - \rho\|_1 \leq \epsilon_{\text{thresh}}$. (4) *Entanglement evolution*: Concurrence $C(t)$ decay rate $\propto 1/T_2$, entropy production $\Delta S = S(\rho_{\text{final}}) - S(\rho_{\text{initial}}) \geq 0$ (second law). (5) *Fisher information*: $\mathcal{F}_Q[\rho, \hat{A}] = 2\sum_n \frac{(\partial_\theta p_n)^2}{p_n}$ quantifies parameter estimation precision (Cramér-Rao bound: $\text{Var}(\theta) \geq 1/\mathcal{F}_Q$).

2.5 Deliverables

(1) Analytical solutions: closed-form $M(t)$ for unbounded ($M \sim Q_0 e^{\lambda t}/(\lambda 2^D)$) and RT-bounded ($M \to R_{\text{total}}/\langle \text{RT} \rangle$) with Lyapunov stability proof; (2) Qiskit simulation code: complete circuit implementations (Grover generation, HHL verification, SWAP test) with noise models, transpilation to gate basis $\{R_x, R_y, R_z, \text{CNOT}\}$, depth optimization $L \leq 20$; (3) Comparative analysis: supply curves $M(t)$ vs. t for 9 scenarios ($3 \times \lambda \times 3 \times R_{\text{total}}$), fidelity surfaces $\mathcal{F}(p_1, p_2, T_1)$, concurrence decay $C(t)$, parameter sensitivity via Fisher information; (4) Complexity validation: log-log plots confirming $G \sim O(m^3)$ scaling, comparison to lower bounds; (5) Report sections: theoretical framework (no-cloning under RT, Lindblad dynamics), numerical results (convergence rates, suppression ratios), feasibility discussion (classical simulation limits $m \leq 16$, error mitigation strategies).

3. Expected Outcomes

- **Inflation characterization:** Quantify unbounded growth $M(t) \sim e^{\lambda t}$ with extracted rates $\lambda \in [0.1, 1.0]$ yr^{-1} from Liouvillian eigenspectrum; demonstrate supply doubling times $\tau_2 = \ln 2/\lambda$

- **RT stabilization proof:** Show bounded equilibrium $M_\infty = R_{\text{total}}/\langle \text{RT} \rangle$ with convergence time $\tau \sim 1/(\lambda + \gamma_{\text{diss}})$; Lyapunov stability guarantees; verify no-cloning preservation

- **Simulation validation:** Complete QL protocols on Qiskit AerSimulator (statevector/density matrix modes); $m = 12$ qubits ($2^{12} = 4096$ dimensions); noise with $T_1/T_2 \in [50, 200]\mu s$, $p_{1,2} \in [10^{-4}, 10^{-2}]$; diamond norm $\|\mathcal{E}_{\text{ideal}} - \mathcal{E}_{\text{noisy}}\|_\diamond < 0.15$

- **Mechanism comparison:** Three RT variants: (1) Gate-count (Cost $\propto m^3$, robust); (2) Decoherence (Cost $\propto L/T_2$, time-limited); (3) Ancilla (Cost $\propto \chi$, entanglement-based)

- **Theoretical insights:** Connect to quantum information: Holevo bound $\chi(\mathcal{N}) \leq S(\rho)$, complexity class BQP$^{\text{NP}}$, channel capacity $C(\mathcal{N}_{\text{RT}}) < C(\mathcal{N}_{\text{ideal}})$

4. Timeline

Date	Milestone
Oct 30 - Nov 3	Literature review (Zhandry, Coladangelo-Sattath); setup Qiskit 1.0+, Python 3.10+, Jupyter; GitHub repo
Nov 4 - Nov 10	[**Ding**] Derive analytical $M(t)$, implement ODE solver (scipy); [**Zheng**] No-cloning proof under RT, Lindblad master equation derivation
Nov 11 - Nov 17	[**Tian**] Circuit design: polynomial hash oracle, Grover iteration; [**Zheng**] HHL & SWAP test in Qiskit; gate basis decomposition
Nov 18 - Nov 24	[**All**] Implement 3 RT variants with noise models (thermal, depolarizing, readout); test on AerSimulator; validate complexity $O(m^3)$
Nov 25 - Nov 30	[**Ding**] Run 9 comparative scenarios (λ, R_{total} sweep); [**Tian**] Complexity plots, Fisher information; [**Zheng**] Tomography, concurrence analysis
Dec 1 - Dec 5	[**Zheng**] Draft report (theory, results, figures); [**Tian**] Poster design; [**Ding**] Finalize Lyapunov stability proofs
Dec 6 - Dec 8	Team review, presentation rehearsal, Q&A preparation (quantum complexity, simulation limits)
Dec 9	Poster presentation & defense; submit final report

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 & Risk Mitigation

Success Criteria: (1) $> 99\%$ inflation reduction: $M_{\text{RT}}(10\text{ yr})/M_{\text{unbound}}(10\text{ yr}) < 0.01$; (2) Stable equilibrium reached: $|M(t_f) - M_\infty|/M_\infty < 0.05$; (3) Polynomial scaling confirmed: $R^2 > 0.95$ for $\log G$ vs. $\log m$ regression with slope 3 ± 0.2; (4) Simulations complete on classical hardware within computational limits (statevector $m \leq 16$, density matrix $m \leq 8$).
Risks & Mitigation: (1) *Memory limits for large m*: Start with $m = 12$ (4096 amplitudes, $\sim$32 KB); if exceeded, reduce to $m = 6$ (64 amplitudes) toy model. (2) *RT mechanism weakens security*: Formal proof that RT tracking doesn't violate no-cloning; adversary cannot extract (G, L, m) without executing circuit (query complexity lower bound). (3) *Time constraints*: Priority order: (a) Unbounded baseline + analytical solution (minimum viable); (b) One RT variant (gate-count preferred); (c) Full comparison if time permits. (4) *Noise model accuracy*: Validate against published IBM/IonQ calibration data; sensitivity analysis on $T_1, T_2, p_{1,2}$ variations $\pm 50\%$.

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.