Quantum Money and Inflation Control

Final Project Proposal for PHYS C191A

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

1. Introduction

Following our first report and critique, this proposal focuses on the simulation and theoretical modeling of **quantum money inflation**. Previous studies identified that while the no-cloning theorem prevents counterfeiting, it does not inherently prevent the *unlimited issuance* of valid quantum states ("quantum inflation"). The project aims to quantitatively demonstrate this inflation effect through simulation and propose a physically realizable method to limit it.

The work builds on Wiesner's *Conjugate Coding* and Zhandry's *Quantum Lightning* frameworks, as well as the complexity analysis described by Aaronson's *The Complexity of Quantum States and Transformations.* By examining how the minting difficulty of quantum tokens scales with quantum computational power, we will simulate the inflationary behavior and test improved models for stability.

2. Project Objectives and Structure

We divide the project into four main parts, with corresponding submilestones:

Part 1: Demonstrating Unlimited Inflation

We will create a simple numerical model simulating the inflationary dynamics of quantum money issuance. The model will assume that the rate of successful minting scales inversely with computational difficulty D, but exponentially with quantum computational speed Q, approximated by

$$R \propto \frac{Q}{D}.$$

As Q grows exponentially, we expect inflation $I \to \infty$ unless compensating mechanisms are applied. This simulation will serve as a quantitative justification for the inflation problem.

Part 2: Model Design for Limiting Inflation

2.1 Existing Model Analysis: We will analyze the current Quantum Lightning framework and show, through simulation and mathematical reasoning, that it can exhibit unbounded inflation when the quantum circuit complexity of token generation decreases faster than verification cost.

2.2 Improved Model Proposal: We propose adding a *complexity-based issuance control*, in which each minting operation consumes a quantized "energy token" proportional to the Hilbert-space dimensionality of the generated state. This couples money creation to physical cost, ensuring bounded growth even with exponential hardware gains.

2.3 Physical Feasibility: We will discuss whether the improved model could be implemented via quantum circuits using current architectures—e.g., through gate-count-dependent penalties or decoherence-aware token generation.

Part 3: Testing the Improved Model

Using the same simulation environment, we will reintroduce the improved model and test:

- Whether inflation stabilizes under increasing computational power.

- Whether the currency retains scarcity and uniqueness.
- Whether the protocol remains verifiable in polynomial time.

The simulation results will be analyzed for both theoretical safety and practical stability.

Part 4: Conclusion

We will summarize our findings and discuss whether the inflation-limited model can form a bridge between theoretical and physical realizations of quantum currency, addressing both security and economic stability.

3. Expected Outcomes

- A simulation demonstrating uncontrolled inflation in existing models.
- A modified issuance model that stabilizes monetary growth.
- Discussion of physical constraints linking computational complexity and currency supply.

4. Timeline and Sub-Milestones

Date	**Milestone / Deliverable**
Oct 30	Submit final proposal; finalize simulation framework selection (Python / Qiskit).
Nov 10	Implement base inflation simulation (Part 1). Validate unlimited inflation behavior.
Nov 17	Analyze Quantum Lightning model, identify inflation variables (Part 2.1).
Nov 24	Implement and test improved model (Part 2.2, 2.3).
Nov 30	Perform comparative simulation of inflation-limited vs. inflation-free models (Part 3).
Dec 5	Complete final report (Part 4) and prepare poster visualization.
Dec 9	Poster presentation and final defense of model results.

5. References

- Wiesner, S. "Conjugate Coding." *ACM SIGACT News*, 15(1), 78–88 (1983).
- Zhandry, M. "Quantum Lightning Never Strikes the Same State Twice." *arXiv:1711.02276v3*, 2019.
- Aaronson, S. *The Complexity of Quantum States and Transformations: From Quantum Money to Black Holes.* Bellairs Institute Lectures (2016).
- Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." (2008).