

# Quantum Walks and Application to Quantum Money

Jake Doliskani\* and Seyed Ali Mousavi†

Department of Computing and Software, McMaster University

---

\*jake.doliskani@mcmaster.ca

†mousas26@mcmaster.ca

# 1 Introduction to Quantum Computation

## Introduction

Quantum computation represents a paradigm shift in the way we process information. Rooted in quantum mechanics, it leverages principles such as *superposition*, *entanglement*, and *quantum interference* to solve certain classes of problems exponentially faster than classical computers. As a field, it combines the rigor of mathematics, the elegance of physics, and the practicality of computer science to unlock new computational horizons.

## Foundations of Quantum Computation

### Qubits: The Building Blocks

A *qubit* (quantum bit) is the quantum analog of the classical bit. While a classical bit can hold a value of either 0 or 1, a qubit exists in a quantum state described as a combination of these two possibilities, written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Here:

- $\alpha$  and  $\beta$  are complex numbers that represent the probabilities of measuring the qubit in the 0 or 1 state, respectively.
- The condition  $|\alpha|^2 + |\beta|^2 = 1$  ensures the total probability is conserved.

This *superposition* property allows quantum computers to represent and process a vast amount of information simultaneously.

### Entanglement: Quantum Correlations

*Entanglement* is a uniquely quantum phenomenon where the state of one qubit becomes intrinsically linked to the state of another, regardless of the physical distance between them. For example, two qubits might be in the entangled state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

If one qubit is measured, the state of the other is instantaneously determined. This property underpins many quantum technologies, including quantum teleportation and quantum cryptography.

### Quantum Gates and Circuits

Quantum gates are the operational primitives of quantum computation. They manipulate qubits by altering their states in a manner consistent with quantum mechanics. Examples include:

- **Hadamard Gate ( $H$ ):** Creates superposition from a basis state.
- **Pauli Gates ( $X, Y, Z$ ):** Rotate qubit states around different axes.
- **CNOT Gate:** Entangles two qubits by flipping the second qubit based on the state of the first.

A sequence of quantum gates forms a *quantum circuit*, analogous to classical logic circuits but with exponentially richer possibilities due to quantum parallelism.

## Quantum Algorithms

Quantum algorithms exploit the principles of quantum mechanics to outperform classical counterparts in specific scenarios. Some groundbreaking algorithms include:

### Shor's Algorithm

Shor's algorithm efficiently factors large integers, threatening the security of classical cryptographic systems like RSA. Its speedup stems from the quantum Fourier transform and modular arithmetic in the quantum domain.

### Grover's Algorithm

Grover's algorithm provides a quadratic speedup for unstructured search problems. For instance, finding a specific item in an unsorted database with  $N$  entries takes  $O(\sqrt{N})$  queries on a quantum computer compared to  $O(N)$  on a classical one.

### Quantum Simulation

Simulating quantum systems is computationally intensive for classical computers. Quantum computers can model chemical reactions, molecular structures, and physical systems more efficiently, accelerating drug discovery and materials science.

### Quantum Approximation Optimization Algorithm (QAOA)

Used for solving combinatorial optimization problems, QAOA is particularly relevant in fields like logistics and finance.

## Applications and Impact

Quantum computation has transformative potential across industries:

- **Cryptography:** Beyond breaking classical systems, quantum computers can also enable secure communication through quantum key distribution (e.g., using entangled photons).
- **Machine Learning:** Quantum-enhanced machine learning algorithms can handle high-dimensional data spaces more efficiently.
- **Supply Chain and Logistics:** Quantum algorithms can optimize complex systems like traffic flow or supply chain logistics.
- **Physics and Chemistry:** Accurate simulation of atomic interactions can drive innovations in energy, materials, and pharmaceuticals.

## Challenges in Quantum Computation

- **Quantum Decoherence:** Quantum states are fragile and can be disrupted by interactions with their environment. Building stable quantum systems requires sophisticated error correction techniques and noise mitigation strategies.

- **Error Correction:** Quantum error correction introduces redundancy through logical qubits composed of many physical qubits. This increases resource requirements significantly.
- **Scalability:** Scaling quantum computers to hundreds or thousands of qubits is a formidable engineering challenge. Current systems, like IBM’s quantum processors and Google’s Sycamore, are still in the *noisy intermediate-scale quantum* (NISQ) era.
- **Algorithm Development:** Quantum algorithms for real-world problems are still under active research. Identifying practical applications with significant quantum advantage is a key focus.

## Current Progress and the Future of Quantum Computation

The quantum computing landscape is advancing rapidly:

- **Hardware:** Companies like IBM, Google, Rigetti, IonQ, and D-Wave are pushing the boundaries of quantum hardware.
- **Software:** Frameworks like Qiskit, Cirq, and TensorFlow Quantum make quantum programming more accessible.
- **Commercial Applications:** Financial modeling, risk analysis, and supply chain optimization are emerging areas of interest for quantum technologies.

The *quantum advantage*—where quantum computers outperform classical systems in practical tasks—has been demonstrated in specific scenarios (e.g., Google’s quantum supremacy experiment in 2019). However, achieving broad-scale quantum advantage remains a long-term goal.

## Conclusion

Quantum computation stands at the forefront of a technological revolution. By rethinking computation through the lens of quantum mechanics, it opens new pathways for solving problems that were once thought intractable. Although challenges remain, the potential benefits are vast, with the promise of transforming industries and deepening our understanding of the universe. As research and development continue, quantum computation is set to redefine the future of technology and science.

## 2 Introduction to Quantum Walks

## 3 Group Actions

## 4 Quantum Money

### Introduction to Quantum Money

Quantum money is a revolutionary concept in cryptography that uses quantum mechanics to create a form of currency that is provably secure against forgery. Originally introduced by physicist Stephen Wiesner in the 1970s, quantum money represents one of the earliest proposed applications of quantum information science. By encoding information into quantum states, quantum money

exploits the fundamental principles of quantum mechanics to provide security features unattainable by classical systems.

## How Quantum Money Works

At its core, quantum money relies on two key principles of quantum mechanics: the *no-cloning theorem* and the *observer effect*.

### Encoding Information in Quantum States

- Each quantum bill contains a unique quantum state, such as a set of qubits encoded in superposition.
- These states are generated and stored by the issuing authority (e.g., a central bank) using a secret algorithm.

### Verification Process

- The issuing authority also generates a verification protocol, allowing a legitimate quantum bill to be authenticated.
- When a user presents a quantum bill for verification, the authority measures the encoded quantum states using the pre-determined protocol.
- If the measured states align with the expected values, the bill is deemed valid.

### Unforgeability

- Due to the *no-cloning theorem*, it is impossible to copy an unknown quantum state without altering it.
- Any attempt to measure or duplicate the quantum state results in a disturbance detectable during verification.

## Key Principles Underpinning Quantum Money

1. **No-Cloning Theorem:** The no-cloning theorem states that an unknown quantum state cannot be perfectly copied. This makes quantum money inherently secure, as counterfeiters cannot reproduce the quantum states encoded in legitimate currency.
2. **Measurement Disturbance:** Observing or measuring a quantum state generally alters it. This ensures that any unauthorized attempt to inspect the quantum money will render it invalid, as the encoded states will no longer match their original form.
3. **Randomness and Superposition:** Quantum money utilizes superposition to encode information. For example, a single qubit in superposition may represent both 0 and 1 simultaneously until measured. The randomness of these states makes predicting or reproducing them without knowledge of the original encoding impossible.
4. **Entanglement (Optional Feature):** Some implementations of quantum money involve quantum entanglement, where pairs of quantum states are interconnected. Changes to one entangled state directly affect its pair, adding another layer of security against forgery.

## Benefits of Quantum Money

- **Unforgeable:** Classical currency, both physical and digital, can be counterfeited with enough effort and resources. Quantum money, however, is fundamentally unforgeable due to the laws of quantum physics.
- **Decentralized Verification:** In some theoretical models, quantum money can be verified without contacting the issuing authority, enabling decentralized systems for authentication.
- **Enhanced Privacy:** The unique encoding of each quantum bill could allow for privacy-preserving transactions, as the details of the transaction need not be linked to the bill's verification.

## Challenges and Open Questions

1. **Practical Implementation:** Generating and maintaining stable quantum states in real-world conditions is technically challenging. Quantum systems are highly sensitive to environmental noise, requiring robust error-correction mechanisms.
2. **Scalability:** For quantum money to replace traditional systems, it must scale to accommodate billions of users and transactions.
3. **Theft and Security:** While quantum money cannot be forged, it can still be stolen, much like traditional physical or digital assets. Developing secure storage and transfer mechanisms is a priority.
4. **Centralized vs. Decentralized Systems:** Most current proposals involve a centralized authority for issuing and verifying quantum money. However, decentralized quantum money systems (akin to blockchain technology) are an area of active research.

## Applications Beyond Money

The principles underlying quantum money have broader applications, such as:

- **Quantum Tokens:** Used in secure communication or access control.
- **Quantum Cryptography:** Building secure voting systems or decentralized platforms.
- **Quantum Key Distribution (QKD):** While distinct from quantum money, QKD relies on similar quantum principles to ensure the security of communication channels.

## Conclusion

Quantum money represents a paradigm shift in secure transactions, leveraging the foundational principles of quantum mechanics to create currency that is inherently secure against forgery. While still a theoretical concept, advances in quantum technology and cryptography are rapidly bringing us closer to practical implementations. If realized, quantum money could redefine financial systems, offering unparalleled security and efficiency in the digital age.

## 5 Applications

### References