Mining Bitcoin Using Grover's Algorithm

Shazil Arif

December 9, 2021

Contents

1 Introduction

In this paper we cover the basics of Bitcoin, Blockchain and Bitcoin's Proof-of-Work Consensus Algorithm and explore what mining is. We will discuss why mining is difficult and the existing solutions that exist for it. Then we will look at how we can attempt to solve it (at a very small scale) using Grover's Algorithm.

Disclaimer: I'm not an expert in any of the topics discussed in this paper.

2 Blockchain

A blockchain is simply a ledger. It records transactions. It records the sender, receiver and the amount being sent by the sender to the receiver. It's a concept that has been around for thousands of years.

In ancient times, in places like Babylon and Mesopotamia, people used clay tablets and carved details of transactions onto these tablets. Slowly these evolved into papyrus documents. In the 15h century, italian mathematician Luca Pacioli introduced the idea of double entry bookkeeping. It became the underlying principle of today's field of accounting. It's very simple, each transaction involves a credit entry for one party and a debit entry for another party.

Blockchain is essentially a modern versional of a ledger. It is digital but also **decentralized**. We'll discuss the concept of decentralization more in depth but, at a high level what it means is that nobody owns or controls the ledger. In ancient times, ledgers were stored in temples, then banks in more modern times. Instead, the blockchain is stored on various computers referred to as a 'network'.