Proposal

The idea of a quantum computers was first proposed by Richard Feynman back in 1982 as a possible solution to solve programs that could not be solved in polynomial time on a classical computer [1]. Development of large-scaled quantum computers have recently risen to the forefront in many tech giants such as Google, IBM, and Microsoft, and Alibaba [2]. Preliminary results on smaller-scale quantum processors with up to 20 qubits have demonstrated the capability of the hardware to be programmed and controlled and while the biggest challenge lies ahead in efforts to reduce the hardware limitations currently available, there is optimism. This is an incredible challenge going forward as it requires physical qubits well isolated from the environment and capable of being addressed and coupled to more than one extra qubit [3]. However, there has been massive progress recently, as the largest tech giants compete to build the first commercially available quantum computer [2]. For example, Google recently announced Bristlecone, their new 72-qubit quantum processor. Although Google is 'cautiously optimistic', this is very exciting as it has been proposed that quantum devices with more than ~50 qubits are expected to perform certain algorithms better than classical computers, thus achieving quantum supremacy [4][5].

The implications of the emergence of quantum computing are very great, particularly when considering the strength of modern data security for major companies, banks and blockchains [7]. Two quantum algorithms that are of utmost importance in this context are Shor's (prime factorization) and Grover's (unstructured database query) algorithms [9][13]. Classical computers do not posses the power to overcome the computational effort required to break modern encryption methods, which in the case of, for example, RSA key encryption require the prime factorization of very large numbers and lattice-based encryption schemes often require solving a variant of the shortest vector problem (SVP). Although the emergence of Shor's algorithm is of main concern in the most recent future due to it's threat on the most popular encryption algorithms such as RSA encryption, Grover's algorithm presents further threats to encryption algorithms proposed in response to Shor's due to its ability to solve cryptographic hashing and ease the complexity in solving SVP and AES encryption [6][7][8].

While Grover's algorithm is a clearly defined problem as of this point, and early versions do exist, there is room to invest in its practicality and scalability as quantum computers continue to evolve past their current limitations. Grover's algorithm assumes the existence of a "magical" black-box oracle function that identifies when any "winning" value exists when searching in a database, while the early implementations use quantum circuits with oracles precompiled for predefined values [9][10][11][12]. The objective of this research is to develop a practical oracle function for use in Grover's algorithm in any scalable system. To do so, and initial step of extensive literature review and public consultation of forums specific to the quantum computing community is considered to test and validate what has been done. These tests will imply small-scale circuits being built for execution and testing on currently available simulation engines such as Rigetti Forest and IBM Quantum Experience. The hardware will be accessed through IBM Quantum Experience's 16 qubit processor available for public use over the cloud using their python SDK. For each test attempted, the complexity and accuracy of each presented oracle will be judged. Once confident that a valid practical implementation of an oracle has been tested on, the remainder of the paper would deal with introducing parametrization and scalability of the algorithm for future implementations where hardware limitations are eliminated.