Safeguarding Data In The Quantun Age

Dharshan.R[1], Dharaneesh R[2], Baranidharan S[3], Kishor D[4]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[1, 2, 3, 4] SNS College of Engineering (Autonomous)

I. INTRODUCTION

Quantum computing is a revolutionary paradigm in the field of computer science that leverages the principles of quantum mechanics to perform computations in ways that classical computers cannot. While classical computers use bits to represent information as either a 0 or a 1, quantum computers use quantum bits, or qubits, which can exist in multiple states simultaneously, thanks to a phenomenon called superposition

Researchers and engineers are actively working on developing practical quantum computers and exploring their potential applications, such as in cryptography, optimization, and simulating quantum systems. While quantum computing is still in its early stages, it holds great promise for solving problems that are currently intractable for classical computers.

What is quantum computing?

Quantum computing is a type of computing that takes advantage of the principles of quantum mechanics, a branch of physics that describes the behaviour of matter and energy at the smallest scales, such as the level of atoms and subatomic particles. Quantum computers use quantum bits, or qubits, as the basic units of information, and they leverage unique quantum phenomena to perform computations in ways that classical computers cannot.

Quantum computing is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

Today, IBM Quantum makes real quantum hardware — a tool scientists only began to imagine three decades ago — available to hundreds of thousands of developers. Our engineers deliver ever-more-powerful superconducting quantum processors at regular intervals, alongside crucial advances in software and quantum-classical orchestration. This work drives toward the quantum computing speed and capacity necessary to change the world.

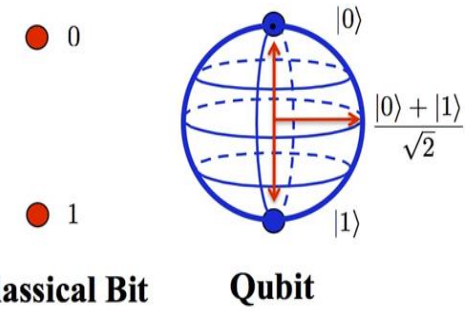
These machines are very different from the classical computers that have been around for more than half a century. Here's a primer on this transformative technolog

II. ALL ABOUT QUANTUM COMPUTING

WHAT IS QUANTUM COMPUTING?

This branch of computer science is based on the principles of the superposition of matter and quantum entanglement and uses a different computation method from the traditional one. In theory, it would be able to store many more states per unit of information and operate with much more efficient algorithms at the numerical level, such as Shor's or quantum annealing. This new generation of supercomputers uses knowledge of quantum mechanics — the area of physics that studies atomic and subatomic particles — to overcome the limitations of classic computing. Although in practice, quantum computing faces evident problems regarding scalability and incoherence, it makes it possible to perform multiple simultaneous operations and eliminates the tunnel effect that limits current nanometric scale programming.

2.1WHAT IS A QUBIT?



Quantum computing uses the qubit as the basic unit of information rather than the conventional bit. The main

characteristic of this alternative system is that it permits the coherent superposition of ones and zeros, the digits of the binary system around which all computing revolves. Bits, on the other hand, can only have one value at a time — either one or zero —.

This aspect of quantum technology means that a qubit can be both zero and one at the same time, and in different proportions. This multiplicity of states makes it possible for a quantum computer with just 30 qubits, for example, to perform 10 billion floating-point operations per second, which is about 5.8 billion more than the most powerful PlayStation video game console on the market.

2.2DIFFERENCES BETWEEN QUANTUM COMPUTING AND TRADITIONAL COMPUTING

Quantum and traditional computing are two parallel worlds with some similarities and many differences, such as the use of qubits rather than bits. Let's take a look at three of the most significant:

Programming language

Quantum computing does not have its own programming code and requires the development and implementation of very specific algorithms. However, traditional computing has standardised languages like Java, SQL and Python, to name but a few.

Functionality

Quantum computers are not intended for widespread, everyday use, unlike personal computers (PC). These supercomputers are so complex that they can only be used in the corporate, scientific and technological fields.

Architecture

Quantum computers have a simpler architecture than conventional computers and they have no memory or processor. The equipment consists solely of a set of qubits that makes it run.

Why use quantum computers

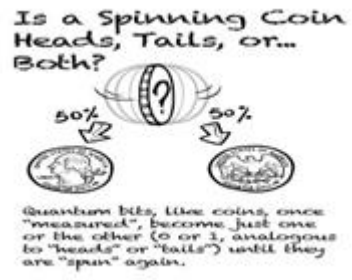
There are many ways to understand why quantum mechanics is hard to simulate. Perhaps the simplest is to see that quantum theory can be interpreted as saying that matter, at a quantum level, is in a multitude of possible configurations (known as *states*). Unlike classical probability theory, these many configurations of the quantum state, which can be potentially observed, may interfere with each other like waves in a tide pool. This interference prevents the use of statistical sampling to obtain the quantum state configurations. Rather, we have to track *every possible* configuration a quantum system could be in if we want to understand the quantum evolution.

III. EXCEPTIONAL COMPONENTS OF QC

Quantum computing is special and distinct from classical computing due to several fundamental principles and properties that arise from the principles of quantum mechanics.

Here are some key aspects that make quantum computing unique

Qubits: In classical computing, information is stored in bits, which can exist in one of two states: 0 or 1. Qubits, on the other hand, can exist in multiple states simultaneously, a property known as superposition.

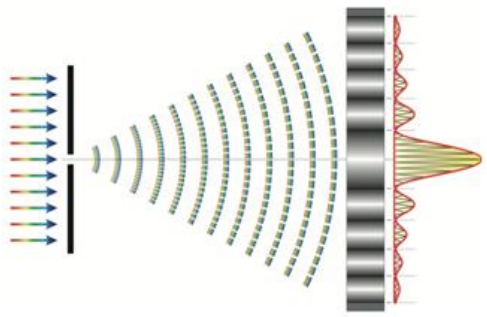


This allows quantum computers to perform parallel computations and explore multiple possibilities at once.

Superposition: Qubits can exist in a superposition of both 0 and 1 at the same time. This is in contrast to classical bits, which must be in one state or the other. Superposition is a key quantum principle that enables quantum computers to process information in a highly parallel way.

Entanglement: Qubits can be entangled, meaning the state of one qubit is directly related to the state of another, regardless of the physical distance between them. Entanglement allows quantum computers to establish correlations between qubits and perform certain computations more efficiently.

Quantum gates: Quantum computers use quantum gates to manipulate the states of qubits and perform computations. These gates, analogous to classical logic gates, enable the creation of quantum circuits that implement quantum algorithms.



Quantum parallelism: Quantum computers can process a large number of possibilities simultaneously due to superposition. This inherent parallelism is particularly advantageous for certain types of computations, such as factoring large numbers, searching databases, and solving optimization problems.

Quantum interference: Quantum algorithms make use of interference effects to enhance correct outcomes and reduce the likelihood of incorrect ones. This interference is a quantum phenomenon that contributes to the efficiency of quantum algorithms.

Quantum speedup: Quantum computers have the potential to solve certain problems much faster than the best-known classical algorithms. This is known as quantum speedup, and it arises from the unique quantum properties of superposition and entanglement.

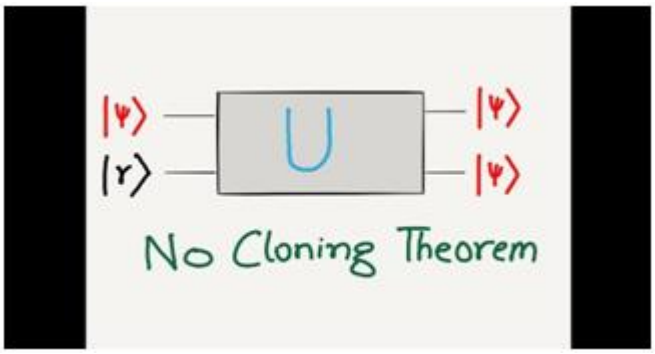
Quantum computing is still in the early stages of development, and building practical quantum computers poses significant technical challenges, such as dealing with errors caused by decoherence and developing scalable qubit architectures. Researchers and engineers are actively working on advancing the field to unlock the full potential of quantum computing for solving complex problems in areas such as cryptography, optimization, and materials science.

Exponential Speedup: Quantum computers have the potential to provide exponential speedup for specific problems. Algorithms such as Shor's algorithm for integer factorization and Grover's algorithm for unstructured search demonstrate this advantage over the best-known classical algorithms.

Quantum Gates and Circuits: Quantum computers use quantum gates to perform operations on qubits. These gates manipulate the quantum states of qubits, and quantum circuits are constructed by combining these gates. Quantum circuits enable the implementation of quantum algorithms.

Quantum Uncertainty and Measurement: Quantum mechanics introduces inherent uncertainty into the properties of quantum particles. When a quantum system is measured, its "collapses" into one of its possible states with a certain probability. Quantum algorithms exploit this uncertainty and carefully manage the probabilities of measurement outcomes.

No-Cloning Theorem: In quantum mechanics, the no-cloning theorem states that it is impossible to create an exact copy of an arbitrary unknown quantum state. This has implications for quantum information processing and quantum communication. It's important to note that while quantum computing offers unique advantages for certain types of problems, it does not replace classical computing. Quantum computers are expected to excel in specific domains, such as factoring large numbers, simulating quantum systems, and solving optimization problems, while classical computers remain well-suited for many everyday computing tasks.



Building practical quantum computers is a significant technical challenge, and researchers are actively working on addressing issues such as error correction, decoherence, and scalability to make quantum computing more robust and widely applicable.