Quantum Computing

Sanskar Mishra
Department of Humanities and Science Thakur College of Engineering and technology
Kandivali East, Mumbai
mishrasanskar60@gmail.com

Abstract:-Quantum computer is a device that follows the collective properties of quantum mechanics i.e. superposition, quantum entanglement, interference, etc, to perform calculations. A Quantum computer performs complex problems in a more rapid and efficient way than a classical computer With the help of Quantum algorithms one can easily perform huge calculations which are not efficient in a classical one. With the help of quantum computing, we'll understand its effect on current crypto technologies and how a quantum key distribution will help the current blockchain system.

Keywords:- Superposition, quantum entanglement, Quantum algorithms, quantum key distribution.

I. Introduction

Quantum theory is one of the finest and most important scientific achievements of the twentieth century. It presents a uniform framework for many modern theories. After almost half a century from its inception, quantum principle got merged with computer technology, another triumph of the 20th century and this led to the birth of quantum computing.

Quantum computing was first conceived by Nobel Laureate physicist Richard Feynman in 1982. He said that no classical computer would simulate quantum phenomena without facing an exponential slowdown, thus he found that quantum mechanical results outright provide something in a reality that is new to computation.

II. Quantum registers

A quantum system is used to store and efficiently process information which is carried in a two-state subsystem, called the "quantum bits" or "qubits". These qubits can be bodily found with the help of a degree quantum mechanical machine, e.g. horizontal and vertical polarisation of photons, Mathematically, qubits are represented using the unit vector within a two-dimensional complex Hilbert space, and it can be written as follows:

$$|\psi\} = \alpha_0|0\} + \alpha_1|1\} \quad \text{.....(1)}$$

In which $|0\}$ and $|1\}$ are foundation states, α_0 and α_1

Are complex numbers with $|\alpha_0| + |\alpha_1| = 1$.

The states $|0\}$ and $|1\}$ are known as computational foundation states of qubits. They correspond to the 2 states 0 and 1 of classical bits.

The range of α_0 and α_1 are referred as possibility amplitudes of the state $|\psi|$. The difference between classical bits and qubits is that qubits can be in a superposition of $|0\}$ and $|1\}$.

An instance of a qubit is $|-\} = 1/\sqrt{2}(|0\} - |1\})$.

A quantum register is shaped from multiple qubits collectively. A state of quantum signs up inclusive of n qubits is defined in the following way:

$$|\psi\} = = \sum_{t\in[0,1]n} (\alpha t|t\}) = \sum_{t1,t2,...tn\in[0,1]} \alpha t1t2 \ldots tn\ |t1t2 \ldots tn\} \quad \text{.....(2)}$$

In which complex numbers $\alpha_{t|t2.....tn}$ are required to meet normalisation condition:

$$\sum_{t\in[0,1]n} (\alpha t)^2 = \sum_{t1,t2,...,tn\in[0,1]} |\alpha t1t2 \ldots tn|^2 = 1$$

The state $|\psi\}$ in Eq, (2) is a superposition on the computational basis states $|t_1t_2\ldots..t_n\}$ {t1,t2,.....,tn =0,1) of the quantum registers. The number $\alpha_{t|t2.....tn}$**'s** are the possible amplitudes of $|\psi\}$.

We can also write it in the following way:

Suppose a non-negative integer is

$$t_1 2^{n-1} + t_2 2^{2n-2} + \cdots\ldots\cdot + t_n 2^0$$

is identified with its binary illustration

$$t = t_1 t_2 \ldots\ldots\ldots t_{n-1}.$$

Another way to symbolize the state |ψ} is t put in writing it with the shape of the column vector:
|ψ =(α0. ,. . . α2n−1)
Several registers can be put together to shape a , larger sign-up whose notation is given up in the terms of tensor manufactured from the states of its thing registers.

$$|\psi i\} = \sum_{t(i)} \alpha i,t\ (i)\ |t\{i\ 1\ \}$$

Be a qubit notation for each 1≤i≤k. Then their tensor product is defined as

$$|\psi 1\}.....|\psi k\} = i=1 \otimes k\ |\psi i\} = \sum t(1)\ ,....,t\ (k)\ \alpha 1,t(1) \ldots \alpha k,t(k)\ |t^{(1)}\ , \ldots ,t^{(k)}$$

We often write e |ψ^⊗k for (|ψ...|ψ)/k.
In quantum computing, entanglement acts like a qubit multiplier. So as we entangle more and more qubits the ability of the system to perform calculations wouldn't grow linearly but will burst out exponentially. However, it also acts as a problem for the quantum computer.
As we further discussed, a QC(Quantum Computer) is really attractive if it's "universal". So the quantum computation is known universal as long as arbitrary single-qubit and non-local (entangling) two-qubit unitary operations can be applied in an arbitrarily structured sequence which is called a quantum circuit. These operations are a result of the physical structure of the systems and control fields which are embodied in the Hamiltonian of the system. The solution to the problem of a lack of universality of numerous intrinsic physical interactions can be constructed by the encoding states representing quantum logic into a two and higher-dimensional subspace of the system Hilbert space. This concept is known as "encoded universality". The significance of encoded universality for quantum computation lies in the fact that it requires active manipulation of the only two-particle exchange interaction and thus it is also referred to as "exchange only computation" to avoid any other sources of decoherence like additional control fields. application

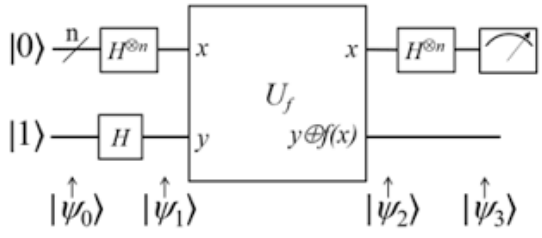

Fig-1 Deutsch-Jozsa Algorithm

A. .Deutsch-Jozsa Algorithm

In 1985, Deutsch more formalized and elaborated the idea of Feynman and published in a seminal paper where a quantum Turing gadget was defined. Importantly Deutsch described the approach of quantum parallelism that is primarily based on the superposition principle of quantum mechanics by using which a quantum Turing machine can encode many inputs at an identical tape and perform calculations on all the inputs simultaneously. Furthermore, he proposed that quantum computers might be capable of performing certain calculations that classical computers perform inefficiently.
Quantum computation also offers different possibilities of speedup over classical computation with the help of the superposition of quantum states.

B. Shor's prime factorization algorithm

In 1994, further one of the most important was made by Shor. With aid of exploring further quantum parallelism, he determined a polynomial-time algorithm on the quantum computer system for prime factorization of which the best-recognized set of rules on the classical computer is exponential. Shor showed in his prime factorization algorithm that a quantum computer could do much better than a classical computer. Due to this, Shor's algorithm had sparked a worldwide interest in quantum computing.
Shor showed that a QC could do better than a classical computer. Importantly, the difficulty in factoring a large number is the basis of the Rivest-Shamir-Adleman(RSA) public-key encryption scheme that is widely used in present times. A method for performing Shor's quantum algorithm over a function encoded with n qubits is provided. The method includes performing a superimposition vector, performing an entanglement operation for a corresponding entanglement vector, and performing an interference operation for generating a corresponding output vector. Shor's algorithm is applicable to only a specific problem.

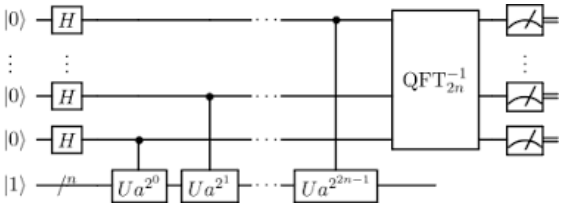

Fig-2 Shor's prime factorization algorithm

C. Grover's Algorithm

In 1996, Grover devised an algorithm that is applicable to many problems. Gover's quantum search algorithm solves the problem of unsorted database searching. Finding a marked state from an unsorted database requires N/2 searches in the case of a classical computer. Grover's algorithm finds a marked item in only $\sqrt{N}$ steps where N is the size of the database. Grover's algorithm has many applications such as deciphering the digital encryption scheme (DES) optimization.
Grover's algorithm achieves quadratic speed-up over classical algorithms but this algorithm suffers from one problem: the probability of finding the marked state may never be exactly.

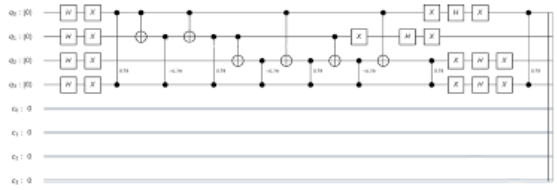

Fig 3. Grover's Algorithm

A. Quantum Key Distribution:

Blockchain is an open, public, distributed that has many applications including digital currencies. The security of the ledger depends on the difficulty of solving certain types of cryptographic problems which are threatened by the potential of quantum computation. Especially, hashes are used in signing the blocks of a ledger which can be compromised. The principal threat is Grover's algorithm which can speed up function inversion dramatically. This allows the generation of a pre-modified image from a given hash allows the signed data block to be modified. This destroys the authenticity of the ledger risking the entire blockchain.
Another threat is Shor's algorithm which would apply to any part of the blockchain that relies on asymmetric key cryptography. The main problem here is the breaking of the RSA encryption. RSA here relies on the ease of multiplying prime numbers in contrast to the difficulty of factoring large numbers into prime factors. Shor's algorithm speeds up the process, eventually breaking the RSA encryption.
To prevent this few quantum-resistant-cryptographic tools have been developed. Presently it comprises a system for generating a blockchain which comprises the first circuitry for receiving the first group of data. The blockchain processing circuitry performs the first hash using the group of data and the first the quantum key distribution(QKD) using N-state qudits where N is greater than 2. Similarly, a second hash happens with another group of data. And similar steps are taken respectively.

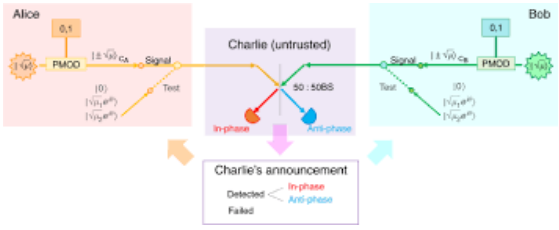

Fig 4. An example of Quantum key distribution.

Applications:

Similarly, just like how we saw the application of QC in blockchain technology on creating it more secure. There are various applications in other fields too such as:

1. Drug development
2. Weather forecasting and climate change
3. Artificial Intelligence
4. Financial Modelling
5. Traffic Optimization
6. Complex manufacturing

Quantum computers will even help us in searching for Higgs events and the origins of the universe. There would be more applications possible with quantum computers. With every advance in the field of quantum technology, we'll see its use increasing exponentially. We might also get a better hybrid version of both classical and quantum computers.

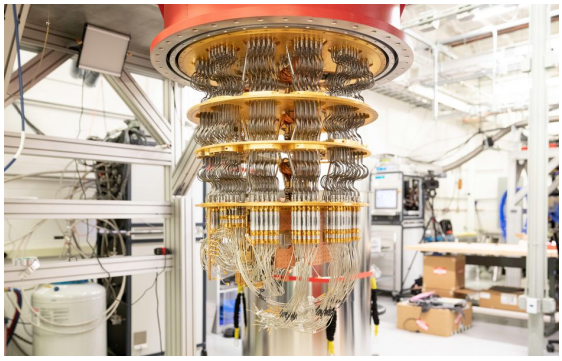

Fig 5. An image of a Quantum computer

Conclusion:

So here in this paper, we have seen what a quantum computer is and how it will help us to overcome the

limitations of a classical computer. The fundamentals of a quantum computer. Various algorithms are related to the quantum computer and Shor's algorithm, Deutsch algorithm, and Grover's algorithm. We already had discussed the effects of quantum computers on blockchain technology. This technology will further be mature in the future so the different aspects of this technology will be further elaborated in the future.

References:

[1].https://patentimages.storage.googleapis.com/23/8f/75/21d071dd85b397/US7529717.pdf
[2].file:///C:/Users/user/Downloads/QuantumComputingResearchPaper.pdf
[3].https://patentimages.storage.googleapis.com/da/d9/b3/b2854c3474730b/US10708046.pdf
[4]https://patentimages.storage.googleapis.com/27/15/3d/1fb267ed0bf504/US20040179622A1.pdf
[5]https://quantum-journal.org/papers/q-2018-08-06-79/pdf/
[6].https://www.pnas.org/content/pnas/98/21/11847.full.pdf
[7]https://www.geeksforgeeks.org/introduction-quantum-computing/
[8]https://www.google.co.in/books/edition/Quantum_Computing_for_Computer_Scientist/U1chAwAAQBAJ?hl=en&gbpv=1&dq=quantum+computing&pg=PT14&printsec=frontcover