Quantum Networking

Derrick Boyer

CSCI 395, 2024, Dwight Hobbs

Abstract– Quantum mechanics has revolutionized the way that we look at the world and the technology we use. This paper looks into the properties of quantum mechanics that are used for security purposes, extend and improve existing networks, and increase communication for some of the world's most complicated technologies. This paper will reference the quantum mechanical properties of coherence, entanglement, and duality and how they are used to improve upon the world's networking abilities.

Keywords– Coherence, Duality, Entanglement, Qubit, Wave-Particle Duality

I. Introduction

Quantum mechanics, a field once considered perplexing, has evolved into a game-changer with widespread impacts. Starting from the basics of light and electrons, to today's complex quantum networks, this paper explores how quantum mechanics has reshaped technology and communication by using its fundamental properties to create better security for network connections, extend existing networks, and [1]allow communication between quantum computers using the idea of quantum networking.

II. Background to Quantum Mechanics

In the17th and 18th centuries, it was believed that light was made up of electromagnetic waves and electrons were "point-like" particles, but this could not explain certain phenomena. Quantum mechanics was the solution to this contradictory state that science appeared to be in because it allowed these fundamentally small objects to have characteristics of both waves and particles. This is called the "wave-particle duality." [2] As the Department of Energy puts it, "[...] this created problems in explaining various phenomena in physics. These include blackbody radiation—the emission of light from objects based on their temperature. Quantum mechanics also helped explain the structure of the atom. It helped make sense of the photoelectric effect, which involves how materials emit electrons when those materials are hit with light of certain wavelengths. By explaining how things can be both

---

1

particles and waves, quantum mechanics solved these problems." [2]

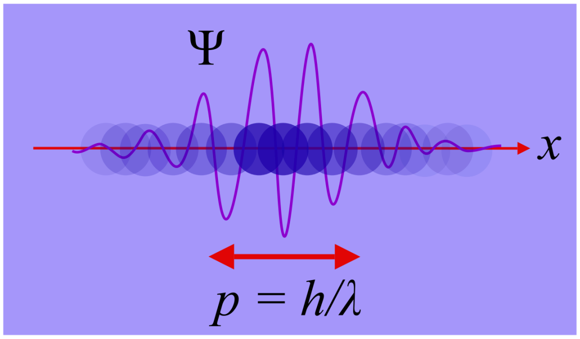


Figure 1: A representation of the two states of quantum mechanics [4]

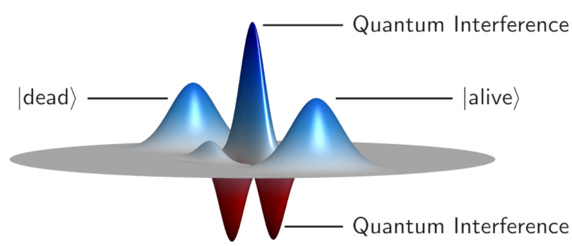
As stated, there are two aspects to this duality: the particle and the wave. The particle aspect of this idea involves the idea of these fundamentally small objects described as "quanta." [2] A quanta is the smallest possible form of an object when that object is in a bound state. For example, the quanta of a portion of electromagnetic radiation, or light, is a photon. To be in a bound state simply means the particles are trapped, such as electrons orbiting the nucleus of an atom. The wave aspect deals with the idea of particles being quantized. The Department of Energy describes this by saying, "To be 'quantized' means the particles in a bound state can only have discrete values for properties such as energy or momentum. For example, an electron in an atom can only have very specific energy levels. This is different from our world of macroscopic particles, where these properties can be any value in a range. A baseball can have essentially any energy as it is thrown, travels through the air, gradually slows down, then stops.

At the same time, tiny quantized particles such as electrons can also be described as waves. Like a wave in the ocean in our macroscopic world – the world we can see with our eyes -- waves in the quantum world are constantly shifting. In quantum mechanics, scientists talk about a particle's 'wave function.' This is a mathematical representation used to describe the probability that a particle exists at a certain location at a certain time with a certain momentum." [2] The world of quantum mechanics describes is confusing for most, as its very nature is paradoxical and seems to contradict itself. However, the theory of quantum mechanics has been developed and used throughout the 20th and 21st century to revolutionize how scientists view the microscopic world.

III. What Quantum Networks Use

From quantum mechanics, there have been multiple underlying principles that have developed. This paper will focus on three main underlying concepts. The first is the idea of quantum entanglement. This is arguably the most important concept for quantum networks as it is the idea on which it is based. John Burke at TechTarget describes quantum entanglement as such, "Quantum entanglement is the phenomenon when two quantum systems become linked and share fundamental behaviors in a unified quantum state." [1] The idea is that two quantum systems can be linked, and once they have become linked and entangled, any changes affecting one system, also affect the other. This is because, as Burke states, they are linked in a unified state. Burke uses spinning entangled photons as an example. He says, "Take, for example, two entangled photons spinning in a singlet state. The conservation principle states that the total spin of an entangled group must be zero. The two photons have opposite spin orientations and maintain a total spin momentum of zero. But, if one photon starts spinning from down to up, the other switches from up to down to keep the total spin momentum at zero." [1] This can be used to transmit information, quickly, across large distances. Because the distance between entangled systems is irrelevant, having ones that are great distances apart and changing the state of one creates an almost instant transmission of information across that large distance because the other system can be read and interpreted to determine the change that was made to the original. Quantum networks use this concept by creating and using quantum bits called qubits.

The second idea that quantum networks utilize is the idea of coherence. In order for a quantum system to work, the quantum state of that system needs to be maintained. This sustained state describing the "synchronization and correlation" of behaviors is referred to as coherence. [1] This means that the entanglement is sustained and the behaviors that are desired are not changed. For instance, if two particles are entangled, and one spins up while the other spins down, the direction of the spins is not changed, other than to spin in the opposite direction. This means the particles can spin up or down depending on which way the other is spinning, but if the state is not maintained they may spin to the side or in some diagonal direction that can be increasingly difficult to interpret. Coherence can be disrupted, and when that happens, the state is lost. Burke talks about this when he says, "Various factors can disrupt coherence, such as electromagnetic fluctuations, temperature changes and quantum measurement. For example, a qubit that



becomes entangled with surrounding matter causes decoherence with its entangled qubit." [1] When, in this example, one of the qubits becomes entangled with surrounding matter, the changes in the surrounding matter also cause changes in both of the entangled qubits in the system. This can lead to corruption of data or data loss when trying to transmit information. This is why it is very important that coherence be kept for the quantum system.

Figure 2: A representation of quantum interference disrupting coherence in a system [6]

The last concept of quantum mechanics discussed in this paper is the idea of no-cloning. This idea is part of what makes quantum networking particularly difficult. Quantum mechanics itself states that the observation of a system changes its state. This is a major issue because it means the qubits cannot be observed without the coherence of the system involving those qubits being disrupted. Burke describes a major issue that comes from this. “Quantum laws dictate that observation of a system changes its state. As a result, qubits cannot be copied directly. So, for example, the no-cloning principle prohibits exact backup copies, as that process would disturb the original state.” [1] Without being able to create backups, if something else happens where information is corrupted or lost in the transmission process, the entire transmission would have to start over, including the establishment of a new quantum system with new qubits. This differs from modern networks which do not have to recreate a connection after information loss because they can resend the packet across the same channel. This idea of no-cloning is the main reason why quantum networks are rare, as it is difficult to develop a network that can keep out almost all interference.

IV. How Quantum Networks Use These Concepts

Quantum networks use these concepts in a variety of different ways to implement the engineering behind them. The first is, as stated, the use of quantum bits, called qubits. As previously stated, changes in one end of a quantum system lead to a correlated change in the other end. This change can be interpreted to determine the change in the first end of the system. Thus, leading to a transmission of data that is incredibly fast. Qubits implement this idea by creating a quantum system of entangled bits. Burke explains this by saying, “Quantum bits (qubits) entangled with each other can transmit data. If a qubit at one end of the network changes state, the entangled qubit at the other end of the network instantly reflects the correlated changes. Bits of data are communicated by observing these changes.” [1] Using entangled bits, flipping a bit at one end of the system, flips the bit on the other end of the system. This is an almost immediate transmission of information from one destination to another. This is especially useful because once the bits are entangled, the distance between them becomes irrelevant and information can be transmitted faster than any other form of modern propagation for larger distances. The

Department of Energy explains this by saying, “But if the photon cannot be copied, how can the communication be amplified to reach distant recipients? This is where the quantum phenomenon of entanglement enters the picture. The quantum state of each entangled photon is correlated with that of its entangled partners, regardless of their distance apart.” [3]

The main issue with quantum networks is not the concepts behind it, it is the engineering to set up the quantum network in the first place. As of now, there are two main parts to the mechanical side of a quantum network. The first is what is called a quantum processor. These are needed to create the quantum bits in the first place. Creating entangled qubits is no easy task. Burke explains quantum processors as, “The end nodes on a quantum network house quantum processors that generate and receive qubits. They might also have some quantum memory capacity.” [1] These quantum processors solve two issues. The first is the development of quantum bits. Quantum processors create and receive qubits and interpret the changes in them to allow the transmission of information. It also creates a small solution to the no-cloning issue by having some capacity of quantum memory.

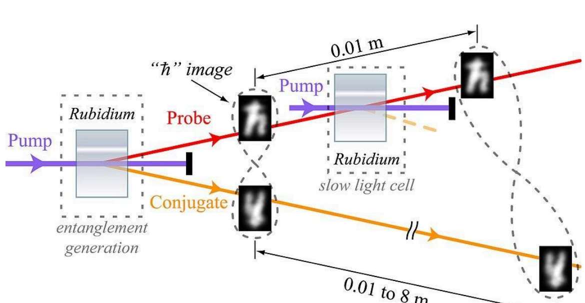


Figure 3: A Diagram of a Quantum Processor [6]

The other aspect of the mechanical side of quantum networks is what is called a quantum repeater. Quantum repeaters take in the signal from one end system and work to retransmit that signal to the other end system, via a chain of qubits. Burke explains this as, “A repeater entangles the incoming qubit with one of a pair it has generated internally. Any changes in the state of the qubit from the transmitting end node are reflected in the state of the qubit from the repeater. The second repeater qubit travels to the next repeater in line, and the process repeats and extends the entanglement until the qubit reaches the receiving end node. At that point, changes in the qubit held on a transmitting node result in changes in the sent qubit on the receiving node, enabling information to flow.” [1] There are two kinds of repeaters. The first is a trusted repeater. Trusted repeaters are more secure because along with the data from qubits, it also encrypts the data and propagates a quantum key in the process. Burke explains this as, “Trusted repeaters enable end-to-end communications via a chain of quantum key distribution (QKD) events. These events give the end nodes a securely generated and transmitted encryption key that is also known to one of the intervening repeaters.” [1] These keys are used to encrypt and decrypt data at each end of the quantum system. This is similar to encryption keys that are passed along in packets for secure traffic on modern networks. However, due to the quantum nature of the key, it is much harder for attackers to intercept and interpret to be able to decrypt traffic, as opposed to traditional keys. The other kind of repeater is an untrusted repeater. Untrusted repeaters simply use the entangled qubits to transmit data, without any form of security or encryption key. Burke explains this by stating, “Untrusted repeaters are purely quantum repeaters. These repeaters perform a quantum operation -- called a Bell measurement -- on pairs of qubits to entangle them, so changes in one are reflected in the other. A transmitting end node creates a pair of entangled qubits, holding one and sending the other through the repeater network.” [1] Untrusted repeaters work essentially the same way as trusted repeaters, just without the quantum key. While the implementation of quantum networks is far from finished, these three concepts are crucial to the engineering behind it.

V. Why Quantum Networks Are Used

Quantum networks are used for a variety of different purposes. They are used for security, extending existing networks, and allow for communication between quantum computers. They are excellent for security because, as previously stated, due to the no-cloning principle of quantum mechanics, it is naturally a secure channel for transmitting information. “Once a quantum transmission link is established, the communications channel is intrinsically secure. It can't be intercepted or copied without corrupting the data. Quantum networking is, therefore, attractive in any use case requiring completely secure networking -- within a data center, across a campus, on a metro area network or on a WAN.” [1] As stated, quantum networks sometimes use quantum keys. A less safe method of propagation would be to encrypt data using a quantum key, transmit the data on a regular, modern network, and transmit the quantum key on a quantum network. “A weaker form of quantum-secured conventional networks -- QKD -- is commercially available. The data stream is subject to interception and copying, as quantum mechanics were used only to transmit the encryption keys. But, if the system transmits long encryption keys that are used for symmetric encryption -- as opposed to public key encryption -- then the transmitted data should be resistant to decryption even by quantum computers.” [1] This is less secure, as the data is still propagated along a modern network link, but is more secure than traditionally encrypted data, because the data is safe from even the world’s most advanced computers.

Quantum networks can also be used to extend the reach of existing networks. As stated, the distance between entangled systems is irrelevant. Therefore, it can be used in tandem with existing networks to allow them to reach other parts of the world that were previously unavailable. [5]

Quantum networks can also be used to allow communication between quantum computers. Using quantum networks between quantum computers removes the need for security among such networks. "Another main use case is creating quantum-linked clusters of quantum computers, independent of the need for security on such links" [1] These are the three most useful aspects of quantum networks and why it is important to invest in their development in the future.

VI. Conclusion

Quantum networks have a variety of uses and aspects that stem from it. Its use of fundamental principles of quantum mechanics allow it to create various improvements over modern networks. They use entanglement, coherence, and no-cloning principles, along with qubits, quantum processors, and quantum repeaters to create fast, secure networks that can be used alongside established networks to extend their range or to create new networks with increased security that allow for communication between quantum computers. Quantum networks is the biggest engineering and computer science project since the creation of the internet and it is only now getting started.

References

[1] Burke, John. "An Introduction to Quantum Networks and How They Work: TechTarget." Networking, TechTarget, 11 Aug. 2023, www.techtarget.com/searchnetworking/tip/An-introduction-to-quantum-networks-and-how-they-work#:~:text=Quantum%20networking%20connects%20systems%20and,on%20photon%20or%20electron%20transmission.

[2] "Doe Explains...Quantum Mechanics." Energy.Gov, www.energy.gov/science/doe-explainsquantum-mechanics. Accessed 10 Mar. 2024.

[3] "Doe Explains...Quantum Networks." Energy.Gov, www.energy.gov/science/doe-explainsquantum-networks. Accessed 10 Mar. 2024.

[4] "File:QM Template Pic 3.SVG." Wikipedia, Wikimedia Foundation, en.wikipedia.org/wiki/File:Qm_template_pic_3.svg. Accessed 12 Apr. 2024.

[5] Lackey, Brad. "Quantum Networking: A Roadmap to a Quantum Internet." Microsoft Azure Quantum Blog, 31 Oct. 2023, cloudblogs.microsoft.com/quantum/2023/11/01/quantum-networking-a-roadmap-to-a-quantum-internet/.

[6] projects, Contributors to Wikimedia. Wikimedia Commons, Wikimedia Foundation, Inc., 8 Mar. 2024, commons.wikimedia.org/wiki/Main_Page.