2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. Sep 3-4, 2021

2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) | 978-1-6654-1703-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICRITO51393.2021.9596171

Quantum Internet: An Approach towards Global Communication

Naman Sandilya
Department of Computer Science and Engineering
ABES Institute of Technology,
Ghaziabad, Uttar Pradesh, India
namansandilya@gmail.com

Avinash Kumar Sharma
Department of Computer Science and Engineering
ABES Institute of Technology,
Ghaziabad, Uttar Pradesh, India
avinash.sharma@abesit.in

***Abstract*— A revolution was sparked by the introduction of the internet to the world. In every domain, it has expanded the application scope, and it is still growing. Throughout history, there were many sources of information, including those not connected to computers. Throughout our whole computing process, we have dealt with this information. Unlike classical computers, quantum computers exhibit certain properties. A quantum device is a device whose operation is governed by quantum physics. In order to implement such advanced communication among quantum devices or computers, a link that can provide the same level of security and allow for such secure communication has to be created. When quantum internet and classical internet are effectively used together, we can achieve unparalleled capabilities with quantum information processing. Our survey paper has discussed more of the technologies that make up quantum internet and its concept.**

Keywords*— *Quantum Internet, Qubit, QKD, Quantum Teleportation, Quantum Swapping, Quantum Repeater

I. Introduction

Quantum Internet is an interesting network technology which is different and not so different from the classical internet that we use. Classical Internet is basically a network which connects computers or devices with web access and makes communication among them possible. [1] On the other hand, Quantum internet facilitates quantum communication through quantum bits among quantum devices or quantum nodes, remotely. Quantum Communication is very similar to normal communication except that it transfers qubits, which behave differently than normal bits. Qubits are the most essential and special elements of quantum computers, devices or networks. These qubits exhibit certain characteristics which are desirable in a network or during a communication [2]. As per the law of quantum mechanics which governs these qubits, it is not possible to determine the state of the system without collapsing its current state. This phenomenon, in other words, is called Superposition. Superposition states that these qubits can be in more than one state at a point of time or an instance and in order to determine its value or measurement, superposition must collapse resulting in only one state of a qubit at that moment.

Another phenomenon that governs these qubits is Entanglement. Entanglement refers to a correlation of qubits which are placed at remote places, devices or nodes. Entanglement provides some extended properties to qubits and the complete connection i.e. this correlation is inherently private, no other qubit can become part of this entanglement [3]. And qubits can not be a clone which means that every qubit is unique in itself so it makes entanglement more secure. Another sub-property of entanglement is that qubits are in maximal coordination.

With so many features and properties, qubits still are prone to losses. These losses generally occur when they are transmitted over long distances. There are various steps that can be taken to increase these transmission distances such as use of quantum repeaters [4]. But generally which qubits to use in such a case becomes an issue as this is critical for it to work.

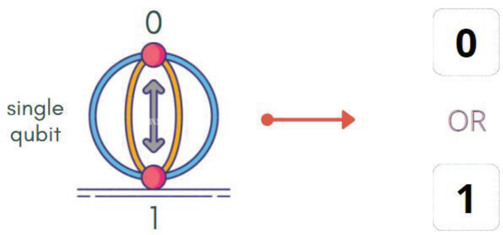

Fig. 1 Superposition collapses to either of two states

The Internet has become an integral part of every industry today, and it is the backbone of every industry. Two or more parties using the internet for communication need to keep their communication secure. It is not intended that the quantum Internet will replace the classic internet. Instead, the company intends to use existing internet technology as a base and high-performance optical fibers for local communication while using wireless repeaters [5]. Even after quantum internet is developed, normal devices such as smartphones, desktop PCs and every Internet-enabled device will still use classical internet. One of the most interesting applications of quantum technology is cryptography, which takes advantage of no-cloning principles of quantum mechanics. Quantum key distribution has made the greatest progress in quantum cryptography. To provide secure computing in the cloud or even for communication between parties, Quantum Key Distribution uses a variety of protocols.

Researchers and recently US government officials are putting great effort in advancing Quantum Internet at a rapid pace [6]. It is already being studied by tech giants such as Google, Microsoft, Alibaba, Intel, IBM, and many more. These companies have developed a very interactive model for achieving or providing a quantum internet in the future. A quantum supercomputer has been declared by Google, which means that such a power of computation can be achieved which cannot be attained in a short period of time [8]. Currently, the Department of Energy (DoE) of the United States is working on quantum internet, which is controlled and transmitted through interplay between subatomic particles. DoE claims that quantum-based networks are virtually unhackable as information passes across different sites with minimal chance of eavesdropping. The Netherlands has also contributed significantly to quantum technology and quantum internet development.

II. QUANTUM COMPUTING AND QUBITS

Traditionally, information is stored as bits, commonly known as binary bits, in a digital system. Bits can have values of 0 or 1. Qubits are used in quantum computation systems to store or to transmit quantum information from one node to another [7]. Quantum bits exhibit a phenomenon known as Superposition, i.e. a qubit can be at one and another point in time, for instance a qubit can be zero and one at the same time. There are two states of an electron: its excited state and its ground state [9]. In a state of superposition, an electron would be in both a ground state and an excited state simultaneously. When an electron state is observed, superposition collapses, and we can determine its state at any moment.

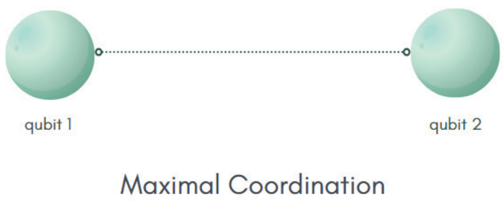

Fig. 2 Quantum Entanglement Property (A)

An individual qubit system is a 2D system that is generally called such. The implementation of quantum technology requires more complex systems, such as multi qubit systems. The computational basis states of a multiple-qubit system increase exponentially with the addition of a single qubit. Consequently, it provides a larger computational space for complex and physically impossible computations. Quantum gates are used to manipulate qubit states in these computations and states [11-13]. Quantum circuits with teleportation and entanglement properties can be built using these gates.

In a two-qubit system, there are four computational basis states i.e. 00, 01, 10, 11. This can now be called Bell States, representing quantum states of two qubits [14]. These qubits in Bell State are also called as EPR pairs and these are responsible for entanglement generation and distribution in the case of quantum teleportation. There is no classical aspect to quantum entanglement. For instance, an EPR pair is a maximally entangled pair of bits and are in superposition as well; whenever a state of one qubit is measured, the state of another entangled qubit is also fixed. Entanglement allows obtaining only mutual information unlike classical systems where remote nodes can share any kind of information.

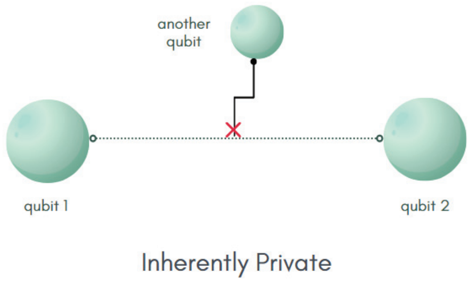

Fig. 3 Quantum Entanglement Property (B)

In order to transfer information between remote nodes, qubits need to be transferred. Quantum teleportation, which is a fundamental characteristic of quantum networks, is an entirely different phenomenon [16]. It is very important to generate and distribute quantum entanglement in order to achieve quantum teleportation.

There are various methods which are applied in order to achieve such a property such as -

- Spontaneous Parametric Down Conversion
- Single Atom Excitation by Laser Beam
- Two Atoms simultaneous Excitation by Laser Beam

Various approaches on qubit generation have been discussed in past research, each having their merits & demerits. Few of these approaches are as follows:

- Cavity quantum electrodynamics
- Photonic qubits
- Trapped ions
- Solid state approach
- Superconducting approach

Quantum Internet is simply an extended quantum network which works over a wider range. Quantum networks require functionalities like quantum teleportation, end nodes, etc. [17]. Quantum Internet extends this with the help of quantum repeaters, quantum channels, etc.

III. QUANTUM TELEPORTATION

In quantum teleportation, qubits are transmitted from one node to another without the particle storing the qubit being physically transferred. Teleportation allows quantum networks or quantum internet links to communicate with efficiency and fidelity [18]. Teleported information is less efficient when there is noise and incoherence in the channel. In order to achieve maximum fidelity, technologies opted for quantum teleportation play an important role in minimizing decoherence. The first time quantum optical states were successfully transmitted was in 1997 [19].

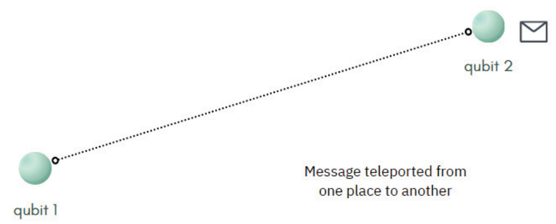

Fig. 4 Message Teleportation from one node to another

The first teleportation distance measurement was accomplished in 2003, and the second one was achieved in 2007. Using the free space channel, distances within teleportation have increased from 600m in 2004 to 144km in 2012. Distance increased fidelity, but decreased it with increasing distance. Today, technologies offering advanced teleportation technology have been developed that can achieve fidelity of 90% in teleportation over long distances [20]. Quantum teleportation uses two links for achieving successful communication -

- Classical Channel Link, for exchange of measurement result of source qubit among both source node and destination node. It uses classical bits to exchange such information.
- Quantum Channel Link, for generation and distribution of entangled pair of qubits i.e. EPR pair between source node and destination node.

IV. QUANTUM REPEATER

Using quantum switches, entangled information is distributed through noisy channels with superposition of causal order on available channels. By propagating simultaneously through multiple space-times, quantum particles can follow multiple trajectories via superposition principle. A concept called superposition is used to propagate information through multiple channels [21, 22].

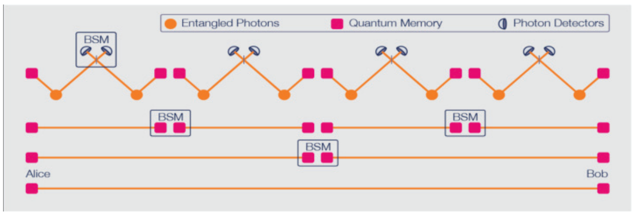

Fig. 5 Working of a quantum repeater [31]

Using a quantum repeater allows quantum teleportation to be utilized over greater distances. Quantum repeaters are also used for extending transmissions over longer distances, as they serve the same purpose as classical repeaters. The nature of the signal may be altered or may not, keeping information intact, in order for the information to be transmitted over very long distances [24].

A quantum repeater, however, operates in another manner. Putting two nodes far apart generates maximally entangled pairs of EPR. Through segmentation, it entangles endpoints across distances. In general, when transmission requires long distances, the transmitting photons lose information as a result of channel attenuation or environmental factors. A quantum repeater, which can't clone information carrying qubits, is a repeater which clones information and forwards it at regular intervals so as to amplify signals [25, 27]. For complete information transfer from one node to another, Biegel proposed a quantum repeater model in 1998. There have been three generations of quantum repeaters since they were introduced in 1998.

Initial repeater stations are positioned so that they are adjacent and entanglement is more likely to occur among them compared to stations in the next generation. Using entanglement swapping, these intermediate stations, source nodes, and destination nodes are linked to each other. With the aid of a control qubit, the quantum switch controls the order in which channels are traversed. Quantum switches thus enable the quantum teleportation process to be fast and precise. Entanglement swapping is essentially a transition between quantum states via quantum teleportation. An overall entanglement is obtained by projecting the states of two particles onto an entangled state. Throughout each station is special hardware for detecting, processing, and transmitting classical as well as quantum information. Due to their reliance on classical communication, first generation quantum repeaters are limited by bottlenecks as distance increases.

Quantum repeaters of the second generation use single-way communication (QEC). The number of qubits waiting for entanglement acknowledgment is reduced when this kind of communication system is used. In order to minimize error generation during the entire process, two-way communication will be utilized.

One-way signaling, using loss-tolerant codes, replaces two-way signaling in third generation quantum repeaters. Photons transmitting quantum information are sent through a channel from sender to receiver. Quantum information is encoded in matter qubits. As the quantum state is re-transmitted to matter qubits at the receiver, it is converted to matter states, again. Matter quanta serve as quantum storage in this third-generation setup. Quantum repeaters and schematics of this generation of quantum systems have been described in 2014 as completely fault tolerant.

Quantum channels are capable of transmitting both quantum and classical information, as described in the previous section. Quantum channels come in various forms and they are customized for each network. Every type has its own particular purpose. A quantum channel is a first-order quantum channel. Quantum information is transmitted over larger distances using free space channels. Photons carry information quickly, but are vulnerable to loss due to evaporation. Free space channels have the benefit that the majority of these information-transferring photons lose their information below 10-30 km of atmosphere. It is not uncommon to see dispersion effects whenever light leaves the atmosphere. Due to this, free space channels maintain the integrity of the information in photons and maintain fidelity. Another type of communication channel is a Fiber based one, which transmits quantum information over shorter distances.

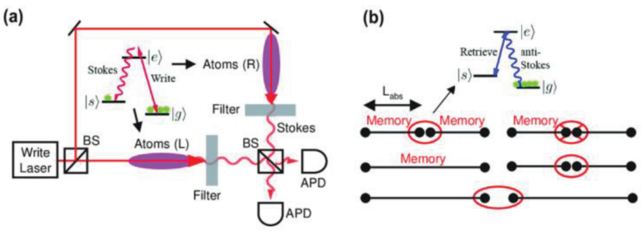

Fig. 6 Working of DLCZ quantum repeater scheme [32]

V. QUANTUM KEY DISTRIBUTION

Cryptography ensures that any information being transmitted through any medium is protected and can only be accessed by the intended recipient. Messages can be encrypted and decrypted using symmetric, asymmetric, and hybrid cryptography, methods that use some type of key [28].

The private key cryptography method refers to systems which use the same key for encryption and decryption. On the other hand, public key cryptography relies on a public key as the encryption key and a private/secret key as the decryption key. It is considered a weakness of private key cryptography that the keys cannot be distributed securely. The quantum key distribution protocol provides excellent privacy and solves key distribution problems based on quantum cryptography.

There can be many applications for quantum internet, as it is a broad field. In its early stages, it is impossible to predict exactly what applications this technology will be able to provide [29]. Nevertheless, as this technology develops, many applications are already predicted and proven in relevant literature. Here we discuss a few like secure communication, blind computing, clock synchronization, longer baselines of telescopes, and the internet of things.

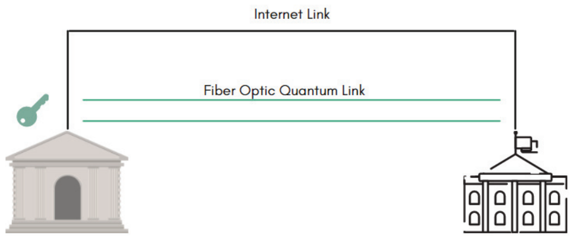

Fig. 5 Representation of QKD

Various applications of Quantum Internet can be -

- Secure Communication: In today's society, secure communications are of the utmost importance. Quantum Internet with multiple QKD protocols will maintain the security and privacy of the information exchanged over the internet that is used for online banking, stock exchange trading, online shopping, military applications, national security, IoT, etc.
- Longer Baseline Telescope: Interferometry between telescopes with very long baselines is the source of all modern astronomical research, which can resolve objects up to ten times better than a single telescope. As photons enter different telescopes in today's world, they must be gathered substantially if an interferometry is to measure interference. Both infrared and optical arrays can be used.
- Clock Synchronization: For QCS (Quantum Clock Synchronization) to solve, quantum algorithms are needed [30]. Among two spatially separated time sources with least communication resources, it is necessary to minimize time differences, i.e. δ. The δ can be calculated accurately and is determined by the stability of clock frequency and the time inconsistency of messages sent across the distance between the two time inputs.
- Blind Computing: The concept of blind quantum computing enables a client who lacks quantum technologies to delegate her quantum calculations to a remote quantum server while maintaining privacy. Verifiability can be achieved with some blind quantum computing protocols, allowing the client to verify the accuracy of the server's quantum computation. A verifiable cloud quantum computing model is important since Bob could accidentally provide Alice with a wrong result, or even if Bob's quantum computer is a fake. Blind quantum computing has been experimented with as well. Two kinds of methods have been used primarily to verify blind quantum computing protocols. There are two types of trap techniques. During the test, Alice hides some unimportant 'trap qubits' in the register, and later checks whether the trap qubits have not been disturbed by Bob. Bob, since he does not know where every trap qubit is, has a high probability of disturbing a trap qubit if he veers off from the correct procedure. In a quantum error correcting computation, Bob cannot change a logical state without affecting any trap qubit, so the probability of Bob changing its state quickly becomes exponentially low.

VI. CONCLUSION & FUTURE WORK

In this survey, we have discussed various factors forming the quantum internet with which it is realized that it is a collaboration of various technologies forming a network of networks. Quantum internet depends completely on quantum computation and various other factors evolving around quantum mechanics phenomena. Researchers and Scientists have come a long way since the advent of quantum computation and therefore quantum networks have been realized. Small scale networks are easy to build and maintain but building a complete large scale network, quantum internet, is no small feat and will take some time before it is in a usable state. There are various future perspectives which can become a reality with more advancement in quantum internet, such as Implementation of trusted network repeater, Exploration of solid-state memories, evolution of quantum processors, integration of qubits with other technologies, etc.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to Computer Science & Engineering Department, ABES Institute of Technology, Ghaziabad for their complete and constant support throughout this study and this opportunity.

REFERENCES

[1] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless Myths, Realities, and Futures: From 3G/4G to Optical and Quantum Wireless," Proceedings of the IEEE (Special Centennial Issue), vol. 100, pp. 1853–1888, Apr. 2012.

[2] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science, vol. 362, no. 6412, Oct. 2018.

[3] R. Van Meter, "Quantum Networking and Internetworking," IEEE Network, vol. 26, no. 4, pp. 59–64, Aug. 2012.

[4] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[5] H. Dai, Q. Shen, C.-Z. Wang, S.-L. Li, W.-Y. Liu, W.-Q. Cai, S.- K. Liao, J.-G. Ren, J. Yin, Y.-A. Chen et al., "Towards satellite-based quantum-secure time transfer," Nature Physics, vol. 16, no. 8, pp. 848– 852, May. 2020.

[6] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," Nature Physics, vol. 10, no. 8, pp. 582–587, Jun. 2014.

[7] T. B. Bahder, "Quantum Positioning System," in Proceedings of the 36th Annual Precise Time and Time Interval Systems and Applications Meeting, Dec. 2004, pp. 53–76.

[8] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Physical review letters, vol. 67, no. 6, p. 661, Aug. 1991.

[9] M. A. Nielsen, I. Chuang, and L. K. Grover, "Quantum Computation and Quantum Information," American Journal of Physics, vol. 70, no. 5, pp. 558–559, May. 2002.

[10] C. Crépeau, D. Gottesman, and A. Smith, "Secure multi-party quantum computation," in Proceedings of the thiry-fourth Annual ACM Symposium on Theory of Computing, May. 2002, pp. 643–652.

[11] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-Enhanced Measurements: Beating the Standard Quantum Limit," Science, vol. 306, no. 5700, pp. 1330–1336, Nov. 2004.

[12] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," Physical Review A, vol. 96, no. 1, p. 012303, Jul. 2017.

[13] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," Physical Review Letters, vol. 68, no. 21, p. 3121, May. 1992

[14] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, "Entanglement distribution over 300 km of fiber," Optics Express, vol. 21, no. 20, pp. 23 241–23 249, Sep. 2013.

[15] J. Kelly, Z. Chen, B. Chiaro, B. Foxen, J. Martinis, and Q. H. T. Team, "Operating and characterizing of a 72 superconducting qubit processor"bristlecone": Part 1," in APS Meeting Abstracts, Jan. 2019.

[16] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing," IEEE Network, Jan. 2019.

[17] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in Proceedings of the International Conference on Computers, Systems and Signal Processing, Dec. 1984

[18] D. Bohm, "A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I," Physical Review, vol. 85, no. 2, p. 166, Jan. 1952.

[19] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of Modern Physics, vol. 74, no. 1, p. 145, Mar. 2002

[20] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, "Experimental Demonstration of Four Photon Entanglement and High Fidelity Teleportation," Physical Review Letters, vol. 86, no. 20, p.4435, May. 2001.

[21]] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""Eventready-detectors" Bell experiment via entanglement swapping," Physical Review Letters, vol. 71, no. 26, Dec. 1993.

[22] W. Gao, P. Fallahi, E. Togan, A. Delteil, Y. Chin, J. Miguel-Sanchez, and A. Imamoglu, "Quantum teleportation from a propagating photon ˇ to a solid-state spin qubit," Nature communications, vol. 4, no. 1, pp. 1–8, Nov. 2013

[23] C. E. Shannon, "A Mathematical Theory of Communication," The Bell System Technical Journal, vol. 27, no. 3, pp. 379–423, Jul. 1948

[24] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," Scientific Reports, vol. 6, no. 1, pp. 1–10, Feb. 2016

[25] F. Furrer and W. J. Munro, "Repeaters for continuous-variable quantum communication," Physical Review A, vol. 98, no. 3, p. 032335, Sep. 2018

[26] A. Kuzmich, W. Bowen, A. Boozer, A. Boca, C. Chou, L.-M. Duan, and H. Kimble, "Generation of non classical photon pairs for scalable quantum communication with atomic ensembles," Nature, vol. 423, no. 6941, pp. 731–734, Jun. 2003

[27] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New Journal of Physics, vol. 4, no. 1, p. 43, Jan. 2002.

[28] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, "HighDimensional Quantum Communication: Benefits, Progress, and Future Challenges," Advanced Quantum Technologies, vol. 2, no. 12, p. 1900038, Oct. 2019.

[29] A. Tunick, T. Moore, K. Deacon, and R. Meyers, "Review of representative free-space quantum communications experiments," in Quantum Communications and Quantum Imaging VIII, vol. 7815. International Society for Optics and Photonics, Aug. 2010, p. 781512

[30] P. Arrighi and L. Salvail, "Blind Quantum Computation," International Journal of Quantum Information, vol. 4, no. 05, pp. 883–898, May. 2006.

[31] https://qt.eu//app/uploads/2018/11/quantum-repeater.png

[32] https://www.researchgate.net/profile/Michael-Hohensee/publication/228803109/figure/fig1/AS:669027236061191@1536519931165/DLCZ-quantum-repeater-scheme-a-First-step-entanglement-generation-Interference-of.png