Quantum-Enabled 6G Wireless Networks: Opportunities and Challenges

SUBMISSION DATE / POSTED DATE

15-06-2021 / 18-06-2021

CITATION

DOI

10.36227/techrxiv.14785737.v1

Quantum-Enabled 6G Wireless Networks: Opportunities and Challenges

Chonggang Wang, *Fellow, IEEE,* and Akbar Rahman

Abstract

With the increasing number of commercial 5G deployments, research on Beyond 5G (B5G) and 6G has started in earnest. Although it is too early to clearly identify what 6G systems will look like or how they will be designed, it is certain that 6G systems will support novel use cases with challenging Key Performance Indicators (KPIs), which will be empowered by new enabling technologies and network architectures. In parallel with the evolution of cellular systems from 5G towards 6G, Quantum Information Technology (QIT) has been evolving rapidly in recent years in terms of quantum communications and quantum computing. It is envisioned that QIT will enable and boost future 6G systems from both communication and computing perspectives. For example, secure quantum communications such as Quantum Key Distribution (QKD) can be leveraged to improve 6G security. This paper aims to provide a technology-driven and visionary description and exploration on how QIT can be leveraged for future 6G wireless networks

Index Terms

6G, internet, quantum information technology, quantum communication, quantum computing, wireless networks.

I. INTRODUCTION

Many disruptive Information and Communication Technologies (ICT) such as Quantum Information Technology (QIT) have been emerging as critical enablers and catalysts to empower a range of new paradigms from several key perspectives including computing, communication, security, and intelligence. In fact, QIT has attracted extensive attention in recent years and a new

C. Wang is with the InterDigital Communications, Conshohocken, USA. E-mail: Chonggang.Wang@InterDigital.com.

A. Rahman is with the InterDigital Communications, Montreal, Canada. E-mail: Akbar.Rahman@InterDigital.com.

* A short version of this article has been submitted to an IEEE Magazine and is currently under review.

wave of QIT research and development has arisen, although quantum mechanical principles have been known and studied for decades. Many countries and regions have announced their national strategy and roadmaps for QIT. For example, the US government published National Strategic Overview for Quantum Information Science in 2018 and The National Quantum Initiative Act was signed into law in the same year. The EU also launched its Quantum Technologies Flagship in 2018 and published a new strategic research agenda on QIT including quantum communication, quantum computing, quantum simulation, quantum sensing and metrology.

To pursue faster computing speed is always one of ICT's goals as we have witnessed in the evolution of compute processing unit (i.e., CPU and GPU). Quantum computing leverages quantum superposition to realize the advantage of quantum parallelism, which will enable exponentially faster computing than classical computing and eventually achieve quantum supremacy for certain classes of problems (e.g., optimization problems). Next-generation processor units using quantum computing will be termed Quantum Processing Units (QPUs). For example, Sycamore is the 53-physical-qubit QPU from Google. On one hand, quantum computing will greatly enhance computation-intensive applications such as prime factorization using Shor's algorithm, and quantum machine learning and chemistry simulations for medical drug design. On the other hand, attackers may leverage quantum computing to break classical cryptography systems and algorithms such as RSA that are based on prime factoring difficulty. To this end, researchers have started to work on Post-Quantum Cryptography (PQC), which aims to provide quantum-safe cryptographic solutions that are resistant to attacks by both quantum computers and classical computers.

A niche but growing area of ICT is sensing and mapping the physical environment using sensors of various types. Examples include accelerometers and gyroscopes currently used in every smart phone to orient the screen images and play electronic games. QIT has introduced potential for large improvements in sensing because quantum devices with just a few physical qubits can detect minute changes in certain environmental properties such as gravity and temperature which are beyond the sensitivity of existing sensors. Quantum sensors are already in use in medical, remote sensing and mining fields. The expectation is that if quantum sensors are fully networked then many new applications will be enabled.

Another important ICT trend is related to telecommunications. Living in a fully connected world and the internet-of-everything era, it becomes paramount to guarantee secure communications. As mentioned above, many classical cryptography solutions are not quantum-safe, or

in other words, are not resistant to attacks by quantum computers. The good news is that QIT can also enable secure quantum communications using approaches known to be information-theoretically secure. In general, quantum communications leverage quantum principles such as the no-cloning theorem and entanglement to achieve quantum-resistant secure communications. For example, Quantum Key Distribution (QKD) achieves information-theoretically secure key agreement between two nodes. QIT can also be leveraged to improve communication efficiency and capacity. For example, it was reported in 2020 that Telecom Italia successfully used D-Wave's quantum annealing technology to implement quantum computing algorithms in their mobile networks for optimal cell and radio planning.

QIT is still evolving, but it is no doubt that QIT will enable novel ICT applications by leveraging quantum computing, quantum communications, and even quantum sensing [1]. With ever-increasing progress in quantum hardware and numerous successes in practical quantum experiments, some QIT applications such as QKD have become increasingly commercially viable. Another example is that IBM has provided their quantum computers as a cloud service, allowing users to access and manipulate qubits using classical cloud APIs. SK Telecom has also deployed a form of QKD in its 5G mobile networks to provide increased security in its 5G network. Verizon also tested QKD over fiber optic links in its network in 2020. In China, researchers successfully realized entanglement-based QKD across 1000 km between two ground nodes, using their quantum enabled satellite, called Micius, as a trusted node. As such, it is expected that 6G as the future mobile cellular system will benefit from quantum computing, quantum communications, and even quantum sensing. Quantum communication can thus improve 6G security. For example, QKD may be deployed over the backhaul (e.g., fiber optic links) connecting radio access networks and the core network. Quantum communications can also be leveraged for securing communications between an SDN controller and SDN-enabled devices as successfully demonstrated by Telefonica. Quantum computing can also solve computationally difficult optimization problems in 6G such as wireless resource allocation to find optimal solutions. Blind quantum computing can also be leveraged to guarantee data privacy in 6G. In addition, quantum machine learning can greatly promote ubiquitous wireless Artificial Intelligence (AI) in 6G as well. It is also possible that quantum sensing can enable new types of haptic (i.e., touch-based) communications in 6G.

Although 6G is not yet fully defined, it is expected that QIT will be one of the critical 6G enablers. We believe quantum-enabled 6G will bring many advantages such as quantum-safe

security, improved privacy protection, and improved communication efficiency and capacity from quantum-based real-time optimizations. Since both 6G and QIT are evolving, it is currently too early to define a specific quantum-enabled solution for 6G. Rather, this paper aims to provide our view on how QIT will accelerate 6G and focuses on discussing challenges and opportunities in quantum-enabled 6G.

The rest of this paper is organized as follows. Section 2 briefly describes some use cases and feature requirements for 6G. Section 3 explains QIT more from ICT perspectives with succinct introduction of quantum mechanics. QIT opportunities for 6G will be presented in Section 4. Some challenges and future directions are described in Section 5. Finally, Section 6 concludes the whole paper.

II. 6G OVERVIEW

The base 5G standards are now finalized, and commercial systems are being rapidly deployed. Specifically, the 5G standards were specified by 3GPP in Releases 15/16 and published in 2020 [2]. According to industry estimates over 100 commercial systems were deployed by the end of 2020 [3]. This has given impetus to researchers to start considering the next generation 6G systems. 6G is expected to be a mixture of evolutionary and revolutionary improvements over 5G [4]. The expected time frame of 6G started from 2020 where initial vision setting and applied research commenced and stretching to approximately 2030 when 6G trials are expected to occur.

There is currently no agreed upon definition of what applications 6G will support. However, Fig. 1 shows one potential view of what 6G may support in relation to previous cellular generations. From Fig. 1, the overall trend that can be observed is that a new cellular generation appears approximately every ten years with much higher throughput, and support for 1-2 key new applications. Projecting this trend to 6G we make the following detailed observations. 6G will most likely support the basic voice (VoIP) and text message services as per previous generations. 6G will also support large scale M2M deployments as has been done since 4G. The main KPI improvements for 6G are expected to be from increased throughput and reduced delay (see also Fig. 2). From Fig. 1, this improvement in throughput and delay for 6G will translate into support of more demanding high-speed data applications like immersive (i.e., 360 degree) 8k video, and critical delay sensitive applications like remote surgery with haptic feedback. The biggest enhancements in 6G, however, will be in the areas of AI and quantum information technology. The AI support in 5G is for network-based features such as automated network self-configuration

and automated network-slicing. 6G networks will need native security and privacy mechanisms, higher efficiency, and ubiquitous intelligence. In 6G, it is expected that AI enablement will be extended to the devices. So, for example, the device-based AI may dynamically configure the device radio and communicate with the base station radio to agree on the optimal radio protocol for the given air interface conditions. Finally, it is expected that 6G will support QIT in the form of quantum computing and quantum communications. This will be discussed in much greater detail in subsequent sections of this document.

Cellular Generation	Commercial Deployment	Voice	Text Messages	High-Speed Data (Example)	Large-Scale M2M	Low-Delay Critical Control (Example)	AI-Enabled	Quantum Info Technology
1G	1983	Analog						
2G	1991	Digital	Yes					
3G	2001	Digital	Yes	Web browsing				
4G	2010	VoIP	Yes	Streaming video	Yes			
5G	2020	VoIP	Yes	4k video	Yes	Self-driving cars	Network	
6G	(~2030)	VoIP	Yes	Immersive 8k video	Yes	Remote surgery	Network& Device	Comms & Computing

Fig. 1: Cellular Generations and Key Applications

Fig. 2 shows details of important cellular radio characteristics for 3G, 4G and 5G with the expected target values for 6G. The key points to note for 6G is that it is expected to have an access technology that will be based on what is referred to as "Tera Hertz (TeraHz) technology". This refers to technology that will be in the 300 GHz to 1 THz range which will require new waveforms and antenna technology. This is due to the high frequency nature of this spectrum, which places extreme demands on hardware and software processing requirements.

In general, from Fig. 2, we see that 6G is expected to have throughput and latency that will be from 5x to at least 20x better than 5G. This will enable the improvements in high-speed data applications and low delay critical control applications that were described in Fig. 1. Finally, it is interesting to consider the potential device types to be used in 6G by human users (as opposed to M2M and other non-human users). We note first that the smart phones have been the main device type in 3G, 4G and so far in 5G. It is expected that smart phones will still be relevant

in 6G. However, with the increased throughput supported in both 5G and 6G, it is likely that Virtual Reality (VR) headsets and other new device form factors may also become important.

Characteristics	3G	4G	5G	6G (Expected)
Access Technology	WCDMA	OFDMA	MIMO-OFDMA & mmWave beamforming	"TeraHz technology" (i.e., 300 GHz − 1 THz with new waveforms & antenna technology)
Peak Data Rate (Downlink)	>10 Mbps	>200 Mbps	>20 Gbps	>400 Gbps
Typical User Data Rate (Downlink)	>1 Mbps	>20 Mbps	>200 Mbps	>1 Gbps
Typical Latency	<200 ms	<100 ms	<1 ms	<0.1 ms
Canonical Device Type (for human users)	Feature phone, Smart phone	Smart phone	Smart phone, VR headset	Smart phone, VR headset, New form factors

Fig. 2: Important Radio Characteristics of Cellular Generations

III. QUANTUM INFORMATION TECHNOLOGY

Quantum Information Technology (QIT) generally includes four main areas: quantum mechanics, quantum communications, quantum computing, and quantum sensing and metrology (See Fig. 3). Quantum mechanics provides the theoretical foundations and building blocks for quantum communications, quantum computing, and quantum sensing and metrology. For example, entanglement can be leveraged for not only quantum communications, but also quantum computing and quantum sensing. In addition, quantum communications and quantum computing can leverage each other and can be integrated together to revolutionize classical internet toward future quantum internet. For instance, quantum teleportation as one of basic quantum communications protocols can be used to facilitate teleportation of quantum states between quantum computers.

A. Quantum Mechanics

Quantum physics, and specifically quantum mechanics, have principles such as non-cloning theorem, superposition, and entanglement, which do not have counterparts in classical systems. On one hand, quantum mechanics describes unique constraints on quantum states of atoms and subatomic particles such as photons; on the other hands quantum mechanics if leveraged appropriately can create many new quantum procedures and applications (e.g., quantum communications, quantum computing, and quantum sensing) and enable new paradigms of quantum
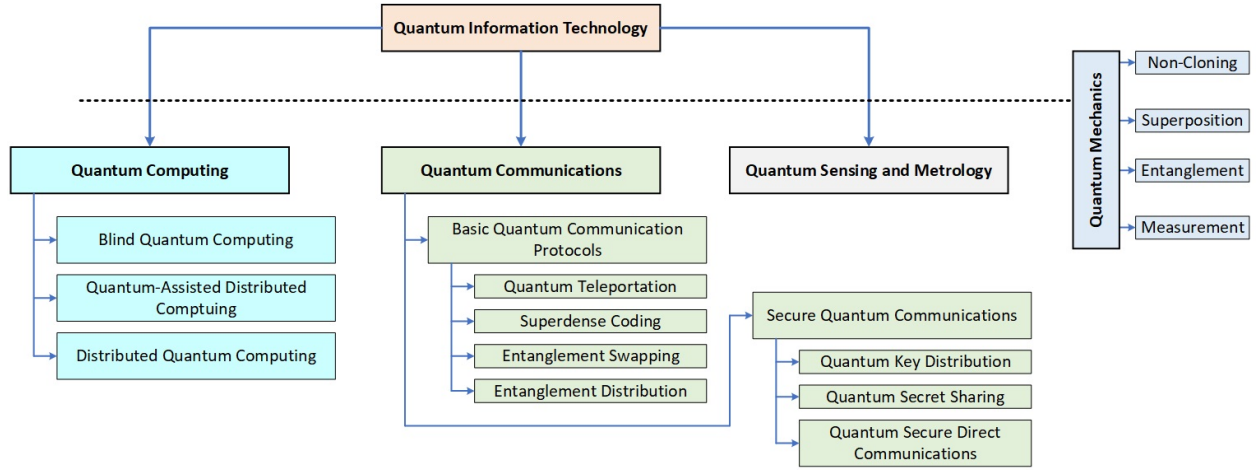
Fig. 3: Taxonomy of Quantum Information Technology

information technology. These quantum mechanical principles are described in more detail as follows:

1) **Non-cloning theorem** states that it is impossible to duplicate an existing quantum state. In other words, the state of a quantum particle or a qubit cannot be copied or reproduced. This provides the foundation for information-theoretical security. For example, if an eavesdropper tries to intercept a photon in the middle of the path from a sender to a receiver, it will be automatically detected by the receiver due to the non-cloning theorem; this phenomenon is leveraged in quantum key distribution protocols. The non-cloning theorem is very different from existing classical communications and computing systems, where the state of an existing classical bit (i.e., 0 or 1) can be easily copied to generate a new classic bit with the same state

2) **Superposition** is another unique quantum mechanical phenomenon describing quantum states. In classical systems, the state or the value of a classical bit is deterministic (i.e., 0 or 1). However, a quantum state is non-deterministic and can be a superposition of two (or more) basic states. As a result, measuring a quantum state will generate a random result. For example, $|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle$ shows that: 1) the quantum state $|\varphi\rangle$ is a superposition of $|0\rangle$ and $|1\rangle$, where $|0\rangle$ and $|1\rangle$ are two basic states. When $|\varphi\rangle$ is measured or read-out, the result could be $|0\rangle$ or $|1\rangle$. Thanks to superposition, a qubit can concurrently represent two states (i.e., $|0\rangle$ and $|1\rangle$) and n qubits can denote 2^n potential states in total. As a result, computation on n qubits can be regarded as computation on 2^n states simultaneously. This is

the origin of quantum computation speedup, as demonstrated in many quantum computation algorithms such as Shor's algorithm and Grover's algorithm.

3) **Entanglement** is an even more strange but extremely useful phenomenon, where quantum states of two (or more) qubits are maximally entangled. In other words, the quantum state of one entangled qubit is fully dependent on the state of any other entangled qubit, no matter how far away the entangled qubits are physically located. If the quantum state of an entangled qubit A is known, the quantum state of other entangled qubit will also be deterministic. The well-known entangled quantum states are four Bell states (i.e., $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$), each of which defines an entangled quantum state of two qubits. For example, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$ or $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$ indicates that two qubits A and B are entangled with the identical state. Please note that Bell states can be easily generated using two quantum logic gates (e.g., Hadamard and CNOT) with two basic $|0\rangle$ qubits as input. Entangled qubits are the most crucial resources in QIT systems, and they can enable new quantum procedures and applications such as quantum teleportation and quantum superdense coding.

4) **Quantum Measurement** is the process to transform a quantum state to a classical state. One quantum measurement principle is deferred measurement, which means that any quantum measurement can be moved to the end of a quantum circuit. In other words, to leverage quantum information technology, the last step is often to store and measure quantum states or physical qubits (e.g., photons, trapped ions) in the target quantum system and to generate measurement results in classic bits for future use. This process is a type of quantum capability, referred to as quantum measurement or readout. Quantum measurement is required for quantum communications, quantum computing and quantum sensing. For example, in typical Quantum Key Distribution (QKD) protocols like BB84, the quantum receiver receives physical qubits (e.g., polarized photons) from the quantum sender and measures them to generate classical bits, which will be fed back to the quantum sender via classical channel as a part of QKD protocols. In quantum computing systems based on trapped ions, ions as physical qubits pass through quantum logic gates and then are readout to generate classical bits as the solution to a computation problem.

B. Quantum Communications

Leveraging quantum mechanics, some fundamental quantum communication procedures become possible such as: quantum teleportation, superdense coding, and entanglement distribution.

1) **Quantum Teleportation** allows to transmit the state of a data qubit $|\varphi\rangle$ from one quantum node A to another quantum node B without physically transmitting the qubit A, but relying on: 1) consuming a pair of entangled qubits; 2) leveraging Bell measurement; and 3) transmitting two classical bits [5]. Both quantum node A and B basically perform Local Operations and Classical Communication (LOCC). First, a shared entanglement has been established between A and B (i.e., there are two entangled qubits: $|q_A\rangle$ at A and $|q_B\rangle$ at B); second, A generates the data qubit $|\varphi\rangle$; third, A performs a Bell measurement of the entangled qubit $|q_A\rangle$ and the data qubit $|\varphi\rangle$; fourth, the result from this Bell measurement will be encoded in two classical bits, which will be physically transmitted via a classical channel from A to B; last, based on the received two classical bits, B modifies the state of the entangled qubit $|q_B\rangle$ in the way to generate a new data qubit, which state is identical to the data qubit $|\varphi\rangle$ at A. In order to generate a data qubit with the same state of $|\varphi\rangle$, a node (B or other nodes) must have received two classical bits and possess $|q_B\rangle$. Essentially, quantum teleportation uses two classical bits to transmit the state of one qubit. As a basic quantum communication protocol, quantum teleportation can be used to enable more advanced quantum procedures and applications. For example, in distributed quantum computing, data qubits from one Noisy Intermediate-Scale Quantum (NISQ) computer to another NISQ computer are very sensitive and cannot be lost. For this purpose, quantum teleportation can be leveraged to teleport sensitive data qubits from one quantum computer A to another quantum computer B. Note that measurement-based distributed quantum computing may not need quantum teleportation. Entanglement swapping protocols are also based on quantum teleportation.

2) **Superdense Coding** can be regarded as an opposite process of quantum teleportation. Using superdense coding, quantum node A achieves the goal of sending two classical bits to quantum node B without physically transmitting these two classical bits but relying on: 1) transmitting one qubit; 2) consuming a pair of entangled qubits; and 3) leveraging Bell measurement. Similar to quantum teleportation, both quantum node A and B in superdense coding perform Local Operations and Classical Communication (LOCC). First, a shared

entanglement has been established between A and B (i.e., there are two entangled qubits: $|q_A\rangle$ at A and $|q_B\rangle$ at B); second, A has two classical bits to be sent to B; third, according to these two classical bits (i.e., four possibilities), A performs a quantum gate to the qubit $|q_A\rangle$ to change the state of $|q_A\rangle$ (i.e., encode two classical bits on $|q_A\rangle$); fourth, A transmits $|q_A\rangle$ to B ; fifth, B receives $|q_A\rangle$; last, B performs quantum gate on $|q_A\rangle$ and $|q_B\rangle$ to decode these two classical bits. In order to decode the two classical bits, a node (B or other nodes) must possess $|q_A\rangle$ sent by A and $|q_B\rangle$ hosted by B. Essentially, superdense coding uses one qubit to transmit two classical bits from A to B, which can be regarded as the increased quantum channel capacity.

3) **Entanglement Distribution** is the procedure and related communications protocols that can distribute entangled qubits to quantum nodes in remote locations. As described above, entanglement is required in both quantum teleportation and superdense coding, it can also enable more advanced quantum applications such as quantum key distribution and distributed quantum computing. However, the two quantum nodes A and B that need to use entanglement may be too distant to directly share entangled bits. As such, a third node C in the middle can act as an entanglement relay to establish and distribute entanglement between A and B. For example, a satellite as the node C can first establish a pair of entangled qubits (e.g., $|q_C\rangle$ at C and $|q_A\rangle$ at A) between itself and a ground station A, and a pair of entangled qubits (e.g., $|p_C\rangle$ at C and $|p_B\rangle$ at B) between itself and a ground station B. Then, leveraging quantum teleportation and consuming $|p_C\rangle$ and $|p_B\rangle$, the satellite C can teleport the state of $|q_C\rangle$ to the ground station B (referred to as $|q_B\rangle$); eventually, both ground stations A and B now share a pair of entangled qubits (i.e., $|q_A\rangle$ at A and and $|q_B\rangle$ at B). This process is referred to as entanglement distribution or entanglement swapping. Pease note that there could be multiple nodes in the middle (similar to the satellite C) to perform entanglement swapping, which can be referred to as multi-hop entanglement distribution.

The basic quantum communication procedures described above can be extended to create even more advanced quantum communication protocols such as Quantum Key Distribution (QKD), Quantum Secure Direct Communications (QSDC), and Quantum Secret Sharing (QSS).

1) **QKD** leverages quantum mechanics to establish a security key between quantum node A and quantum node B, which is information-theoretically secure. QKD protocols typically consist of two stages: key-sharing stage and post-processing stage. In the first key-exchange

stage, A and B employs prepare-and-measure protocols (like BB84) or entanglement-based protocols (like E91) to share a set of classical bits, based on private quantum measurement with random measurement basis at each side. In prepare-and-measure protocols, A prepares qubits and transmits them via quantum channels such as optical fibers to B; then, B measures received qubits on random measurement basis (e.g., vertical, or horizontal polarizations for photons) to generate classical bits; A and B exchanges their measurement basis (not the classical bits from measurement) via classical channels; A and B take the classical bits from the same measurement basis as the shared ones. In the second post-processing stage, A and B aims to generate the final security key from the shared classical bits that have been produced in the first stage; basically, A and B perform information reconciliation and privacy amplification to correct errors and reduce privacy leakage of A and B. Post-processing stage is usually done via an authenticated classical channel.

2) **QSDC** provide direct secure communications between two nodes A and B based on quantum mechanics without relying on security key distribution and management. In contrast, QKD only provides secure key establishments, and the follow-up communications are still based on classical communications only encrypted using the established key. Using QSDC, node A can send secret information directly and securely to node B via quantum channels, without using an established security key. The first QSDC protocol as described in [6] leverages entanglement (e.g., Bell states) to achieve secure direct communications. Basically, node A as the sender prepare a list of N Bell states according to the message bit sequence to be sent to node B; note that each Bell states stands for a pair of two entangled qubits. Node A splits N Bell states to two sequences: Seq1 and Seq2. Seq1 (or Seq2) contains N qubits and each qubit in Seq1 is entangled with a qubit in Seq2. Then, node A sends Seq2 to node B; node B receives Seq2 and measures some of qubits in Seq2 to work with node A to detect eavesdropping, similar to eavesdropping detection in QKD. Last, node A sends Seq1 to node B; node B performs Bell measurement on each entangled qubit pair from Seq1 and Seq2 to recover the encoded classical bits; node B also works with node A by announcing the measurement basis to node A to estimate error rate and detect any eavesdropping for the second time. Similar to quantum teleportation, QSDC realizes secure transmission of classical bits using qubits, but quantum teleportation does not have an eavesdropping check.

3) Secret sharing aims to distribute a secret key among multiple nodes by letting each node know a share or a part of the secret key. However, no single node can know the entire

secret key. The secret key can only be re-constructed via collaboration from a sufficient number of nodes. **QSS** typically refer to the scenario: The secret key to be shared is based on quantum states instead of classical bits. QSS enables to split and share such quantum states among multiple nodes.

C. Quantum Computing

Examples of quantum computing include Blind Quantum Computing (BQC) also referred to as secure quantum computing with privacy preservation. Other examples are Quantum Machine Learning (QML), and Distributed Quantum Computing (DQC). These enable new types of computing services and applications for quantum-enabled 6G.

BQC provides a way for a client to delegate a computation task to one or more remote quantum computers without disclosing the source data to be computed over. Basically, a client node with source data delegates the computation of the source data to a remote computation node (i.e., a server); furthermore, the client node does not want to disclose any source data to the remote computation node and thus preserve the source data privacy; there is no assumption or guarantee that the remote computation node is a trusted entity from the source data privacy perspective. As a new client/server computation model, BQC generally enables: 1) The client delegates a computation function to the server; 2) The client does not send original qubits to the server but sends transformed qubits to the server; 3) The computation function is performed at the server on the transformed qubits to generate temporary result qubits, which could be quantum-circuit-based computation or measurement-based quantum computation. The server sends the temporary result qubits to the client; 4) The client receives the temporary result qubits and transform them to the final result qubits. During this process, the server cannot figure out the original qubits from the transformed qubits. Also, it will not take too much efforts on the client side to transform the original qubits to the transformed qubits or transform the temporary result qubits to the final result qubits. One of the very first BQC protocols follows this process, although the client needs some basic quantum features such as quantum memory, qubit preparation and measurement, and qubit transmission.

DQC refers to distributing quantum computing tasks to multiple quantum computers. This is especially useful when it is impossible or highly inefficient to perform the task on any single quantum computer. For example, a NISQ computer may only support less than 100 physical qubits and so cannot execute complex quantum computing tasks. However, multiple NISQ

computers can be connected via classical and/or quantum channels to gain higher computation power before fully-fledged quantum computers become available. As a result, it becomes possible for them to jointly and efficiently perform the complex quantum computing task. In a broader context, DQC may refer to quantum-aided classical distributed computing, where the solution is to leverage quantum mechanics to solve classical distributed computing problems with a better performance. For instance, entanglement and entangled qubits can be exploited to improve leader election in classical distributed computing.

IV. QIT OPPORTUNITIES FOR 6G NETWORKS

QIT has been envisioned as one of the critical enabling technologies for future 6G wireless systems. For example, secure quantum communication protocols like QKD can make 6G systems secure against post-quantum cryptography attacks. Quantum computing also can be leveraged to solve challenging wireless resource optimization problems in 6G systems. In addition, as has been witnessed in 5G, 4G and 3G systems, the deployment of a new technology will usually be implemented in phases. QIT is similarly expected to be deployed in future 6G systems in stages namely near-term, middle-term, and long-term as described in Fig. 4:

1) Each evolution stage will gradually introduce one or more quantum solutions based on technological and commercial maturity. For example, QKD is a good choice for near-term 6G since commercial QKD products are currently available. In contrast, quantum computing may only be commercially available for long-term 6G systems.

2) For a specific quantum solution, different features may be deployed in various stages. For example, BB84 as the classical QKD can be deployed immediately for the first 6G systems, while entanglement-based QKD protocols may become available only for mid-term and/or long-term 6G systems.

3) In each evolution stage, one or multiple quantum technologies may be deployed starting from a small scale and gradually expanding to a large scale. For example, quantum computing may be first deployed in 6G core networks and gradually extend to other locations like edge networks and even end devices after a long-term evolution. In general, quantum hardware (e.g., quantum measurement devices) may be first become available in core network and accessed remotely by other network entities. When quantum hardware grows more mature (e.g., miniaturized hardware that can operate at room temperature), it may be deployed towards the edge of 6G systems.

Stages of Quantum-Enabled 6G Systems	New Functions/Services	Enabling Technology
Near-Term (2-3 Years)	Secure Communications for Backhaul	Fiber QKD
Middle-Term (3-5 Years)	Secure Satellite Communications; Satellite-Assisted Secure Communications	Satellite QKD
	Optimal Wireless Resource Management	Quantum Computing
Long-Term (5-10 Years)	Data Computing with Privacy-Preservation	Blind Quantum Computing
	Realtime Wireless AI	Quantum Machine Learning

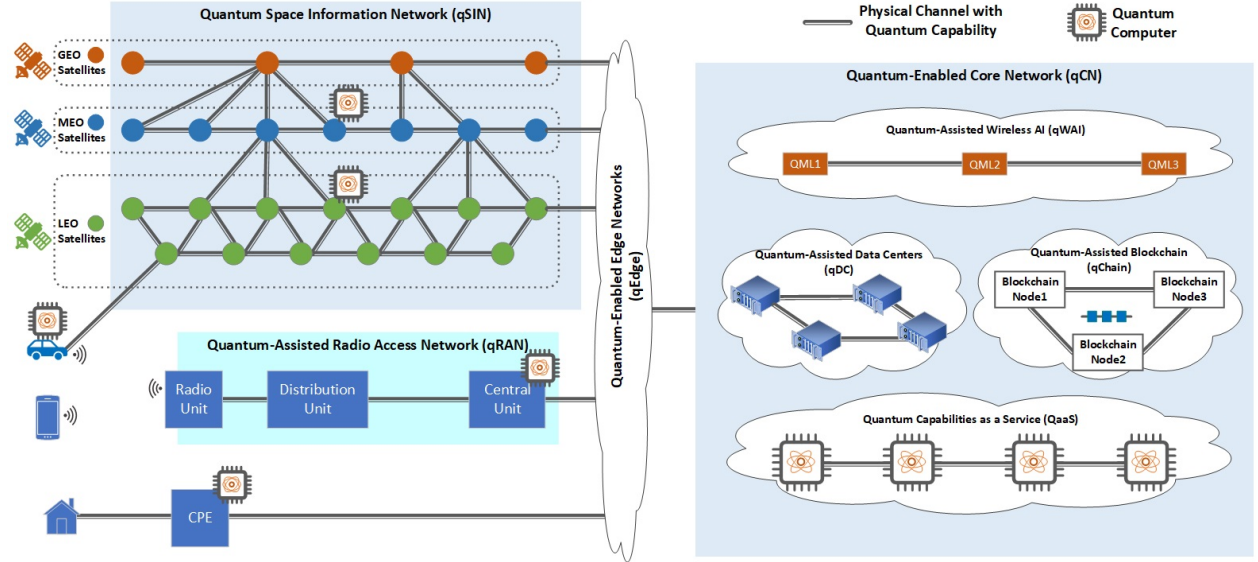Fig. 4: Evolution of Quantum-Enabled 6G Systems

Fig. 5: Quantum-Enabled 6G System

Fig. 5 illustrates a quantum-enabled 6G system, where QIT is exploited to realize new 6G functionalities and services as listed in Fig. 6 such as Quantum-Assisted Radio Access Network (qRAN) and others which are described further below. All the physical channels between the various nodes have quantum capability which typically will mean a photonic based system such as laser or fiber-optic cable. Certain nodes, but not all, will also have full quantum computing capability. However, many nodes may have the basic quantum capability to generate, transmit and receive qubits.

A. Quantum-Assisted Radio Access Networks (qRAN)

Both quantum computing and quantum communications can be leveraged to improve RAN efficiency and security. Some existing work [7] has well demonstrated the optimal wireless resource allocation using quantum annealing over D-Wave quantum computers. In general, with

Features	Leverage Quantum Communication	Leverage Quantum Computing	Leverage Entanglement	Improve Quantum Communications
Quantum-Assisted Radio Access Network (qRAN)	Yes	Yes		
Quantum Space Information Network (qSIN)	Yes	Yes	Yes	Yes
Quantum-Assisted Edge Networks (qEdge)	Yes	Yes		
Quantum-Assisted Data Centers (qDC)	Yes	Yes		
Quantum-Assisted Blockchain (qChain)	Yes	Yes	Yes	
Quantum-Assisted Wireless AI (qWAI)	Yes	Yes	Optional	
Quantum as a Service (QaaS)	Yes	Yes	Optional	
Quantum-Enabled Novel Applications (qApp)	Yes	Yes	Yes	

Fig. 6: Quantum-Enabled 6G System

powerful quantum computing, it becomes possible to find the optimal solution for radio resource allocation and cell planning which leads to higher energy efficiency and spectrum efficiency, for instance, leveraging quantum search algorithms [8].

In addition, quantum communication can be exploited and integrated with O-RAN to enable high security. As an example, O-RAN components such as O-RAN Distribution Unit (O-DU) and O-RAN Central Unit (O-CU) may, by definition, be obtained from different equipment suppliers. Thus, it is very important that they may be dynamically deployable and securely connected to each other in a simple manner. Otherwise, all subsequent user traffic flowing through the O-RAN nodes may be subject to security attacks such as eavesdropping, man-in-the-middle attacks, etc. Quantum communications like QKD can be used to establish security keys between different O-RAN components, and in turn alleviate this problem in an extremely effective manner.

B. Quantum Space Information Networks (qSIN)

As a part of 6G it is expected that thousands of satellites (e.g., LEO, MEO, and GEO) will continue to be deployed in different space orbits and form mesh-like Space Information Networks (SIN). Satellite nodes are usually connected via free-space optic links and a powerful satellite node can host a quantum computer. Quantum Space Information Network (qSIN) has two-fold advantages. On one hand, quantum communications between two satellite nodes, and between a satellite node and ground stations have been practically demonstrated [9], using free-

space optics as quantum channels. If satellite nodes aim to leverage entanglement for quantum communications, entanglement distribution for distant satellites nodes needs to be carefully designed. In addition, powerful satellite nodes with a quantum computer can provide quantum computing as a service for other satellites nodes and ground stations. On the other hand, a satellite node can be used as a trust node or a quantum repeater to aid and improve quantum communications such as satellite-based QKD [10].

C. Quantum-Assisted Edge Networks (qEdge)

It is expected that an increasing number of edge nodes (e.g., vehicles) will be deployed in or connected to 6G systems to offer pervasive edge computing services. Challenges in such pervasive edge computing environment include security, task offloading and edge resource allocation. Secure quantum communications can be leveraged to guarantee secure communications to, from, and between edge nodes, while quantum computing can help to find the optimal solution for task offloading and edge resource allocation. For example, edge resource allocation can easily turn into an NP problem given a big number of edge nodes and multiple factors to consider, which quantum computing could solve quickly. It is predicted that room-temperature quantum computing may be widely available in the next decade [11]. At that time, quantum computers may be deployed in edge networks and provide power quantum computing, referred to as quantum edge computing.

D. Quantum-Assisted Data Center (qDC)

Optical links such as optical fiber and free-space optics are used in modern data centers for inter-rack communications to increase data rates and reduce interference in contrast to using wireless links [12]. These optical links can be leveraged as quantum channels simultaneously. As a result, quantum communication and quantum cryptography can be realized to improve inter-rack security. For example, [13] proposed a hybrid approach that jointly leveraged quantum random number generation, QKD and PQC to a multi-level cryptographic solution with quantum-safe data communications between server racks. Quantum computing can also be leveraged for solving computation-intensive problems in data centers such as optimal data flow and energy consumption management.

E. Quantum-Assisted Blockchain (qChain)

Blockchain or distributed ledger technology elegantly combines a set of mechanisms (e.g., distributed consensus protocols, distributed database, cryptography, and hashing) to realize a decentralized system with multiple advantages such as transparency and immutability. As a 6G enabler, blockchain technology may be used in many applications such as decentralized authentication and distributed wireless resource sharing among parties that may not trust each other. However, blockchain technology also inherits some potential issues such as security attacks from malicious nodes, low transaction speed due to consensus protocols and privacy breach due to transparent data contained in blocks. These issues may be solved or mitigated using QIT, referred to as Quantum-Assisted Blockchain (qChain). For example, quantum communications can be used to improve communication security among blockchain nodes; non-separability of entangled qubits can be used to simulate the link relationship between blocks; entanglement can also be used for designing new consensus protocols without introducing high communications overhead and in turn increase transaction speed. [14] provides more examples on quantum-assisted blockchain protocols.

F. Quantum-Assisted Wireless Artificial Intelligence (qWAI)

6G system will be more intelligent and autonomous thanks to the availability of massive data from ubiquitous devices and network nodes and the application of AI algorithms such as deep learning, deep reinforcement learning, federated learning, and transfer learning [15]. QIT can benefit wireless AI in several ways [16]. First, decentralized AI such as federated learning introduces model exchange and communications among participants, which can be quantum-safe secured using quantum cryptography. Second, both AI training process and inference process are computation-intensive, which can be expedited using quantum computing. Third, blind quantum computing could be leveraged to realize privacy-preserving AI training. Last, quantum machine learning [17] may introduce novel and more efficient wireless AI algorithms.

V. FUTURE DIRECTIONS

5G systems have already started to leverage basic QKD and quantum computing technology as demonstrated by telecom carriers like SK Telecom and Telecom Italia. As previously discussed, QIT brings many opportunities for 6G systems. However, both 6G systems and QIT are still evolving. For example, modular quantum processors, quantum internet component and quantum

sensors are far from large-scale commercial deployment toward quantum internet [18] and will be gradually developed as predicted in [19]. To fully leverage potential advantages of QIT for 6G systems, new solutions for quantum-enabled 6G functionalities and services should be carefully designed. In addition, the following research directions are worthy for further investigation.

A. Quantum Internet Management and Control

With the unique quantum features such as superposition and entanglement, quantum communications and computing could enable more secure web applications. For example, QKD allows to securely distribute security keys between an HTTP client and an HTTP server and ultimately; with such QKD-enabled security keys, the HTTP client and the HTTP server can establish more secure Internet connections. In the meantime, many recent QKD protocols rely on entanglement, which is also required in quantum teleportation and quantum superdense coding.

Essentially, it is critical to manage and control quantum networks efficiently. Two research issues include quantum capability management and quantum link services.

1) Quantum capability refers to quantum resources (e.g., quantum memory, quantum channel) and quantum operation abilities (e.g., entanglement creation, entanglement swapping, entanglement distillation) at a quantum node such as a quantum repeater. To enable a quantum network, the first demand is to efficiently manage quantum capabilities of all quantum nodes within the quantum network. A quantum network may consist of many quantum nodes, which are connected by quantum channels and classic channels. In addition, quantum capability could be dynamically changing, for example, due to qubit memory time and entanglement coherence time. This poses challenges for efficiently managing quantum capabilities of a quantum network.

2) Quantum link layer should provide flexible and complete services to higher layer. Ideally, Link Layer Services should be designed in the way that the higher layer quantum applications can easily access and manage the quantum link layer in an efficient way considering unique characteristics and constraints of qubits, quantum channel, entanglement, etc. For example, the higher layer may need to cancel a pending request for creating entangled qubits.

B. Quantum Capability as a Service

An example of quantum capability is quantum measurement. Quantum measurement is usually done by a quantum measurement equipment, which unavoidably introduces noise or errors. In fact, quantum measurement errors are a major error source to the whole quantum system, regardless of whether it is quantum communications system, quantum computing system or quantum sensing system. One of the reasons is that quantum measurement may take a long time to reach a stable probability distribution of measured quantum states (i.e., $|1\rangle$ or $|0\rangle$); when the measurement time exceeds physical qubit decoherence time, a qubit in $|0\rangle$ state could be measured in $|1\rangle$ state or vice versa. Thus, methods for achieving fast and high-fidelity (i.e., low measurement error rate) quantum measurement have been proposed. But such high-performance measurement methods and equipment may not be available or feasible to be deployed in large-scale and anywhere in the system due to hardware and environment constraints. A quantum computer has a control and measurement plane, which "includes a very precise laser (or microwave) source that can be directed at a specific ion to affect its quantum state, another laser to 'cool' and enable measurement of the ions, and a set of photon detectors to 'measure' the state of the ions by detecting the photons that they scatter" [20]. On the other hand, quantum measurement technology is still evolving, and different types of quantum measurement methods and equipment could be proposed and deployed for different application scenarios. In addition, quantum measurement has potential attacks and security threats. Giving these considerations, it will be beneficial (e.g., higher utilization, higher measurement performance, better flexibility, better security) to provide quantum measurement as a service, which can be easily and securely managed (e.g., scale up, scale down) to cater for different needs.

In the context of 6G, such quantum measurement as a service could be hosted within 6G core network, by central units of 6G radio access network, and/or even by powerful 6G devices such as quantum-capable drones and vehicles. As an example, advanced devices like cars or quantum dock stations could share quantum capabilities, which regular devices can leverage. In another example for QKD-enabled O-RAN, O-CU may not have good quantum measurement capability (e.g., quantum measurement hardware such as fast and high-fidelity readout), which CN provides. Then, O-CU can leverage the quantum measurement capability provided by CN. In order to exploit the quantum measurement capability in CN, O-CU can simply pass all received qubits to CN via the quantum channel between O-CU and CN. CN receives the

qubits from O-CU; CN measures the qubits using random measurement basis according to the QKD protocol and generate measurement results in classical bits. Then, CN sends the used measurement basis and the generated measurement results to O-CU via the classical channel, assuming secure communications between CN and O-CU have been established. After receiving the measurement basis and the measurement results from CN, O-CU follows the QKD protocol and sends designated feedback (e.g., measurement basis) to O-DU. O-DU receives the feedback from O-CU; both of them will follow other steps as specified by the QKD protocol. Finally, O-CU and O-DU will be able to exchange and establish a shared security key between them.

C. Entanglement Distribution in 6G Systems

An immediate use of a quantum network is to establish two (or more) entangled qubits between any two (or more) quantum nodes so that such entangled qubits can be consumed to enable quantum applications such as QKD, quantum teleportation or quantum superdense coding and eventually support distributed quantum applications. Note that the existence of entangled qubits which are distributed and maintained among multiple quantum nodes are referred to as quantum connection. As such, to establish a quantum connection means to distribute entangled qubits to two or more quantum nodes, referred to as entanglement distribution. Entanglement distribution heavily relies on entanglement swapping techniques to extend quantum connection to distant quantum nodes across multiple hops. However, current quantum physics and devices set limitations on entanglement generate rate (not high) and entanglement coherence time (short). This makes it challenging to efficiently establish quantum connections. As a result, quantum connection management is even harder even if it is one of the most essential components to enable new distributed quantum applications.

Most existing entanglement distribution solutions are designed for generic network topologies. It remains a question if they are applicable or efficient for 6G systems. There are a few specific scenarios in 6G systems, where entanglement distribution is needed and may require redesign.

1) 6G systems will include Non-Terrestrial Networks (NTN) or Space Information Networks (SIN). An NTN will likely be a multi-hop mesh network consisting of thousands of satellites with free space optics as both classical channels and quantum channels. Entanglement distribution is required to establish quantum connection between two or more distant satellites. The issue is how to efficiently generate entangled qubits and distribute them (e.g., using entanglement swapping) to any pair of two distant satellites considering multiple factors

such as entanglement coherence time, entanglement fidelity, quantum memory size, and entanglement consumption rate.

2) NTNs in 6G systems will not be an island but will be interconnected with ground networks to form SAGIN. Entanglement distribution will not only consider satellites in the space, but also quantum nodes on the ground such as ground stations and vehicles. This introduces new variables and new complexity, which need new entanglement distribution solutions.

3) In addition, with the introduction of O-RAN, 6G systems will consist of multiple hops or segments (i.e., fronthaul, middlehaul, and backhaul). Nodes in each hop will have different quantum capabilities and different quantum channels. How to efficiently distribute entangled qubits among them remains unsolved.

D. Hybrid Classical-Quantum Network Evolution

A final research direction is the evolution of hybrid classical-quantum networks. QIT will not fully replace classical ICT including the classical internet. Instead, the classical ICT and QIT will complement each other and evolve together to enable hybrid classical-quantum systems with better performance.

1) For example, QKD and PQC likely will co-exist as cryptography options satisfying different security requirements. Furthermore, a hybrid PQC-QKD is proposed in [13] to achieve hierarchical and better security solution for data centers.

2) In fact, even QKD itself is a hybrid protocol in the sense that it requires both quantum channels and classical channels. CV-QKD and DV-QKD can also be jointed used as a hybrid approach with better performance [21].

3) When deploying QKD protocols in ICT backbone networks, a hybrid solution is to use existing optical fibers to support both classical transmissions and QKD quantum photon transmissions, for example, over different wavelengths. In another example, satellite QKD and ground QKD may be jointed leveraged as a hybrid solution to potentially achieve better performance in terms of end-to-end distance and key rate.

4) From a computing perspective, classical computers will co-exist with quantum computers as quantum computers are specialized for certain types of problems. In addition, quantum computers usually need classical computers or classical circuit for controlling the quantum unit. So it is expected that classical computers and quantum computers (e.g., NISQ

computers) will be combined to realize hybrid classical-quantum computing algorithms to maximize the advantages of each technology [22]

5) From an architectural perspective, the quantum internet will drive the classical internet to evolve towards a hybrid internet in a systematic evolution which demands substantial improvements and adaptation from both technologies [18]

The quantum-enabled 6G is thus expected to be a hybrid system. The challenge lies in efficiently designing QIT and classical ICT to co-exist in a modular and extensible approach. This needs a thorough assessment and understanding of each technology's pros and cons to determine optimal matching scenarios and solutions to cater for various user requirements (e.g., security requirements and expected quantum fidelity); different hardware components constraints (e.g., ICT and QIT equipment cooling requirements); and available ICT infrastructure (e.g., types of physical fiber links, data center configurations).

VI. CONCLUSION

Quantum Information Technology (QIT) can benefit and empower 6G, the next generation wireless cellular system. On one hand, with unique quantum mechanical properties such as the non-cloning theorem, superposition, and entanglement, QIT creates the new paradigm of quantum communications and quantum computing. For example, quantum teleportation, superdense coding and entanglement distribution are fundamental quantum communication features, which enable secure quantum communications including quantum key distribution, quantum secure direct communications and quantum secret sharing. Quantum computing not only brings more powerful computation based on superposition and entanglement, but also enables new quantum computing features such as blind quantum computing, distributed quantum computing and quantum machine learning. On the other hand, 6G is expected to be a mixture of evolutionary and revolutionary improvements over 5G. For example, 6G networks need to be more efficient, secure, intelligent, and autonomous, in order to support emerging applications and services such as holographic and haptic communications. QIT itself has been envisioned as one of the critical enabling technologies to enable efficient, secure, and intelligent 6G networks. For example, quantum computing also can be leveraged to solve challenging wireless resource optimization problems in 6G systems. QIT can also benefit and be jointly used with other 6G enablers such as AI and Space Air Ground Integrated Network (SAGIN). We expect QIT will play an important role in numerous 6G areas including but not limited to, quantum-assisted radio access networks, quantum space

information network, quantum-assisted edge network, quantum-assisted data center, quantum-assisted blockchain and quantum-assisted wireless AI.

However, QIT is still evolving and quantum-enabled 6G networks face some challenges. For example, quantum hardware (e.g., modular quantum processors, and quantum sensors) are far from large-scale commercialization. Such quantum hardware constraints pose large challenges in designing efficient and scalable quantum communication equipment for 6G networks. Also, the 6G network will be a hybrid network containing both classical ICT and QIT equipment which must be made to smoothly integrate. On the positive side, recent advances in photonic quantum computing means that room temperature based quantum hardware are now within technological reach. Also, photonic based quantum hardware will most easily be able to integrate with the vast existing base of fiber-optical based communication equipment leading to a potential realistic path towards 6G.

REFERENCES

[1] C. Wang, A. Rahman, R. Li, and M. Aelmans, "Applications and use cases for the quantum internet," *IETF/IRTF Quantum Internet Research Group (QIRG)*, 2021. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-qirg-quantum-internet-use-cases/

[2] NGMN Alliance, "5g white paper 2," 2020. [Online]. Available: https://www.ngmn.org/wp-content/uploads/NGMN-5G-White-Paper-2.pdf

[3] GSMA, "Gsma intelligence shares 'global mobile trends 2021'," 2020. [Online]. Available: https://www.gsma.com/newsroom/press-release/gsma-intelligence-shares-global-mobile-trends-2021/

[4] EU HORIZON 2020, "Empowering transatlantic platforms for advanced wireless research," *EMPOWER White Paper*, 2020. [Online]. Available: https://www.gsma.com/newsroom/press-release/gsma-intelligence-shares-global-mobile-trends-2021/

[5] A. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3808–3833, 2020.

[6] G. Long, "Quantum secure direct communication: Principles, current status, perspectives," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–5.

[7] M. Kim, D. Venturelli, and K. Jamieson, "Leveraging quantum annealing for large mimo processing in centralized radio access networks," in *Proceedings of the ACM Special Interest Group on Data Communication (SIGCOMM'2019)*, 2019, pp. 241–255.

[8] P. Botsinis, D. Alanis, Z. Babar, H. Nguyen, D. Chandra, S. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2019.

[9] S. Liao and et al, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017.

[10] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, "Satellite-based QKD," *OSA Optics & Photonics News*, vol. 29, no. 2, pp. 26–33, 2018.

[11] U.S. Army Research Laboratory, "Path to quantum computing at room temperature," *ScienceDaily*, 2020. [Online]. Available: www.sciencedaily.com/releases/2020/05/200501184307.htm

[12] N. Hamedazimi and et al, "Firefly: A reconfigurable wireless data center fabric using free-space optics," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, 2014.

[13] L. Huang, K. Feng, and C. Xie, "A practical hybrid quantum-safe cryptographic scheme between data centers," in *Proceedings of SPIE 11540, Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III*, 2019, pp. 241–255.

[14] M. Edwards, A. Mashatan, and S. Ghose, "A review of quantum and hybrid quantum/classical blockchain protocols," *Quantum Information Processing*, vol. 19, 2020.

[15] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, "The roadmap to 6g: Ai empowered wireless networks," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[16] J. Biamonte and et al, "Quantum machine learning," *Nature*, vol. 549, 2017.

[17] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6g communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46 317–46 350, 2019.

[18] W. Kozlowski and et al, "Architectural principles for a quantum internet," *IETF/IRTF Quantum Internet Research Group (QIRG)*, 2021. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-qirg-principles/

[19] D. Awschalom and et al, "Development of quantum interconnects (quics) for next-generation information technologies," *APS PRX Quantum*, 2021.

[20] National Academies of Sciences, Engineering, and Medicine, "Quantum computing: Progress and prospects," *The National Academies Press*, 2019.

[21] I. B. Djordjevic, "Hybrid qkd protocol outperformance both dv- and cv-qkd protocols," *IEEE Photonics Journal*, vol. 2, no. 1, 2020.

[22] S. Endo, Z. Cai, S. C. Benjamin, and X. Yuan, "Hybrid quantum-classical algorithms and quantum error mitigation," *Journal of the Physical Society of Japan*, vol. 90, no. 3, 2021.