Emerging issues in computer science

Week 3: Quantum Computing

Lecturer: Ikwap Flavia Agatha

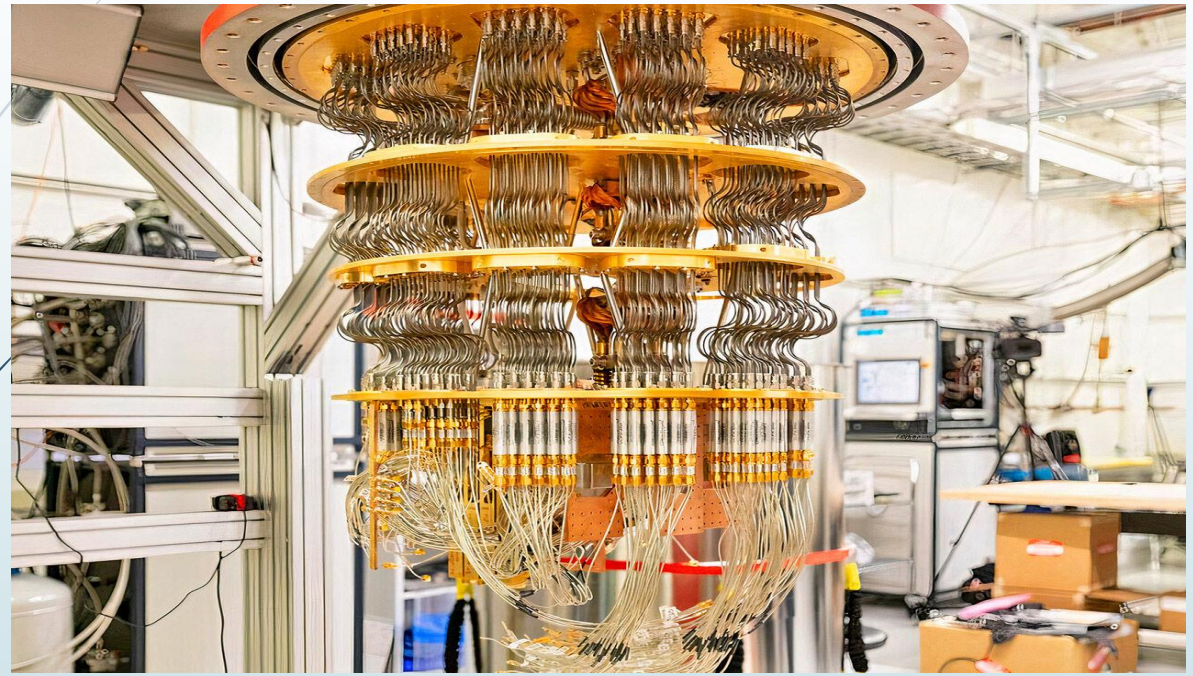
Lecture out come

- At the End of Lecture 3 you will be able to:
- Understand the concept of Quantum computing
- Understand the difference between classical computer and Quantum Computer
- Understand the history of Quantum computing
- Understand the adoption of Quantum computing
- Understand the Benefits and limitations of Quantum Computing

Introduction to Quantum computing

- Quantum computing leverages principles from quantum mechanics, the theory that explains the behavior of matter and energy at microscopic levels like atoms and subatomic particles.
- Unlike traditional computers, which use binary bits (0 or 1) to process information, quantum computers use quantum bits or qubits. Qubits are unique because they can exist in multiple states simultaneously, a phenomenon known as superposition. This ability allows quantum computers to process vast amounts of data and perform complex calculations much more efficiently than classical computers.

Quantum Computer



- https://kardashev.fandom.com/wiki/Quantum_computer?file=Google-quantum-supercomputer.jpg

DIFFERENCES BETWEEN A CLASSICAL COMPUTER AND QUANTUM COMPUTER

	Classical Computer	Quantum Computer
Units of Information	bit, which can be either 0 or 1.	(quantum bit), which can represent 0, 1, or both 0 and 1 simultaneously due to quantum superposition.
Data Representation	Data is processed and stored in binary form, with each bit representing a distinct state (either 0 or 1).	Data is represented using qubits, which can be in multiple states at once allowing for parallel processing of multiple possibilities.
Processing Power	Processing is sequential; a classical computer can only perform one calculation at a time per bit	Can process many possibilities simultaneously due to superposition and can explore multiple solutions in parallel
Operations and Logic Gates	• use logical gates (AND, OR, NOT, etc.) to manipulate bits in deterministic ways.	Quantum computers use quantum gates to manipulate qubits.
Speed and Efficiency	Relatively Fast in solving a number of problems	Very fast at solving complex problems

DIFFERENCES AND SIMILARITIES BETWEEN A CLASSICAL COMPUTER AND QUANTUM COMPUTER		
Parallelism	• Parallelism is possible in classical systems but each processor or core works on a single task at a time.	can achieve a form of quantum parallelism-processing a large number of possibilities at once due to superposition
Error Correction	Use error-correcting codes to ensure data integrity and reliability in computations	• Faces challenges due to quantum noise and decoherence. Quantum error correction is much more complex and resource-intensive than classical error correction
Physical Implementation	• Based on traditional semiconductor technology (e.g., silicon chips).	• Relies on quantum mechanical phenomena and are still in the experimental stage. They can be built using various technologies, such as trapped ions, superconducting qubits, and topological qubits.
	Well-suited for tasks like word processing, gaming, simulations, and most business applications.	• Solving complex problems that are difficult or impossible for classical computers, such as: o Factoring large numbers (cryptography) o Simulating quantum systems o Optimization problems (e.g., in logistics, AI, finance)

Similarities

- **Problem-Solving Approach**: Both classical and quantum computers are designed to process information and address problems, although quantum computers are focused on solving specific problems more efficiently.
- **Computational Models**: Both types of computers depend on a computational model and require programming to perform tasks—classical computing uses traditional programming languages, while quantum computing uses specialized quantum programming languages.
- **Components:** Both involve hardware, software, and algorithms, though quantum computers are still in the experimental stage, with practical applications being limited.

History of Quantum Computing

- The history of quantum computing is built upon advancements in both quantum mechanics and classical computing. It encompasses significant discoveries, theoretical milestones, and the progression of experimental technologies. Below is a brief summary of its history:
- **History of Quantum Computing**
- Quantum computing has its foundations in the development of quantum mechanics, a field of physics that emerged in the early 20th century.
  - **Max Planck (1900)**: Introduced the idea of quantization through his work on black-body radiation, paving the way for quantum theory.

History of Quantum Computing

- **Albert Einstein (1905)**: Offered an explanation for the photoelectric effect, for which he won the Nobel Prize, helping to shape the understanding of light as both a wave and a particle (photon).
- **Niels Bohr (1913)**: Developed the Bohr model of the atom, contributing to quantum theory by explaining atomic spectra.
- **Werner Heisenberg and Erwin Schrödinger (1925-1926)**: Made significant contributions to quantum mechanics with concepts like uncertainty and wave mechanics, which would later play a crucial role in quantum computing.

Classical Computers and Theoretical Foundation (1930s–1950s):

- The evolution of classical computing laid the groundwork for the development of quantum computing. Key milestones include:
- **Alan Turing (1936)**: Introduced the Turing machine, a foundational concept of computation that underpins classical computing.
- **John von Neumann (1945–1950s)**: Developed the architecture for modern computers, proposing the idea of storing both data and instructions in the same memory, which became the foundation for all digital computers.

Quantum Computing Conceptualized (1960s–1970s)

- During this time, the theoretical basis for quantum computing started to take form.
- **Richard Feynman (1981)**: Feynman argued that quantum systems could not be efficiently simulated by classical computers, suggesting the need for a new type of computer—one based on quantum mechanics.
- **David Deutsch (1985)**: Building on Feynman's ideas, Deutsch introduced the first formal model for quantum computing, known as the Deutsch model.

Quantum Computing in the 1980s and 1990s

- The 1980s and 1990s were crucial decades in the development of quantum computing, as important concepts and algorithms started to take shape:
- **1980s**: The concept of utilizing quantum mechanics for computation gained momentum. Researchers began investigating how quantum systems could be applied to information processing.
  - **1985 (David Deutsch)**: Introduced the **Deutsch model of quantum computing**, establishing a formal structure for quantum computation.
  - **1987 (Joseph Giordmaine)**: Proposed the idea of **quantum parallelism**, which suggested that quantum computers could simultaneously process multiple possibilities, significantly boosting computational power.

1990s:

- This period saw the advancement of quantum algorithms and more in-depth theoretical exploration.
  - **1994 (Peter Shor)**: Developed **Shor's algorithm**, a revolutionary quantum algorithm capable of factoring large numbers far more efficiently than classical algorithms, highlighting the potential of quantum computing to break common encryption systems.
  - **1996 (Lov Grover)**: Introduced **Grover's algorithm**, which showed how quantum computers could accelerate the search process in unsorted databases, providing a quadratic speedup compared to classical approache

Foundational concepts in Quantum Computing

- **Quantum Bits (Qubits):** • In classical computing, the fundamental unit of information is a bit, which can represent either 0 or 1. • In quantum computing, the fundamental unit is a qubit. Unlike a standard bit, a qubit can exist in a superposition, allowing it to be both 0 and 1 at the same time. This capacity to exist in multiple states simultaneously is a crucial characteristic of quantum computing.
- **Superposition**
- **Superposition** is a key concepts in quantum mechanics and quantum computing. It describes a situation where a quantum system can exist in multiple states at the same time, rather than being limited to a single state as in classical computing.

Classical vs. Quantum States

- In the case of classical computing, a **bit** can be in one of two states: either **0** or **1**. These states are distinct and mutually exclusive. For example, a light switch can either be **off** (0) or **on** (1).
- In quantum computing, a **qubit** (quantum bit) can exist in a **superposition** of both states simultaneously. This means that, rather than just being in a state of **0** or **1**, a qubit can be in a state that is a combination (or "superposition") of both **0** and **1** at the same time.

Mathematical Representation

- A qubit in a superposition can be represented mathematically as a **linear combination** of the basis states **|0⟩** and **|1⟩**. The general form of a qubit state is:
- |ψ⟩=α|0⟩+β|1⟩|\psi⟩ = \alpha |0⟩ + \beta |1⟩|ψ⟩=α|0⟩+β|1⟩
- Where: **|0⟩** and **|1⟩** are the basis states (representing classical 0 and 1).
- **α** and **β** are complex numbers (called **amplitudes**) that determine the probability of measuring the qubit in either state. The probabilities of observing **|0⟩** or **|1⟩** are given by the squared magnitudes of the amplitudes:
  - Probability of **|0⟩** = **$|\alpha|^2$**
  - Probability of **|1⟩** = **$|\beta|^2$**
- The condition that the qubit must be in a valid state is that the total probability must add up to 1:
- |α|2+|β|2=1|α|² + |β|² = 1|α|2+|β|2=1

Key aspects in Superposition

- **Both States Simultaneously**: A qubit in superposition is not just 0 **or** 1; it is both 0 **and** 1 at the same time. This allows quantum computers to explore multiple possibilities simultaneously.
- **Measurement**: When you measure a qubit, the superposition collapses to one of the basis states (**|0⟩** or **|1⟩**), and the qubit "chooses" one state with a probability determined by the amplitudes. This is an example of **wavefunction collapse**, a key concept in quantum mechanics.
- **Superposition and Parallelism**: Due to superposition, quantum computers can perform many calculations at once. If you have **n qubits** in superposition, the system can represent and process 2^n possible states simultaneously. This parallelism can give quantum computers an exponential speedup for certain types of problems.

Superposition in Quantum Algorithms

- Quantum computing has the ability to leverage superposition in quantum algorithms. For example:
- **Grover's Algorithm**: A quantum search algorithm that takes advantage of superposition to search an unsorted database of NNN items in **√N** steps, compared to the **N** steps required by classical algorithms.
- **Shor's Algorithm**: A quantum algorithm for factoring large numbers that exploits superposition and quantum interference to solve the problem exponentially faster than classical algorithms.

Example: Coin Flip Analogy

- A good analogy to understand superposition is to imagine flipping a coin. In classical computing, the coin can only land on either heads (**0**) or tails (**1**) when it is flipped. However, in quantum computing, before the coin lands, it is in a **superposition** of heads and tails at the same time, like spinning the coin and not knowing whether it's heads or tails until you look.

Entanglement

- Quantum entanglement is a key phenomenon in quantum mechanics where two or more particles become interconnected, so that the state of one particle directly impacts the state of another, no matter how far apart they are. This link remains intact even over great distances, meaning any change to one particle's state will instantly affect the other, regardless of separation.
- Superposition are closely linked to quantum entanglement. Superposition involves a single qubit existing in multiple states at once, whereas entanglement describes a situation where two or more qubits are interconnected, with the state of one qubit affecting the state of another, regardless of the distance between them.

The Basics of Entanglement

- When two particles (such as photons, electrons, or atoms) become entangled, their properties become linked in such a way that they cannot be described independently. For example, measuring a property like spin or position of one particle immediately reveals the corresponding property of the other, even if they are light-years apart.
- **Non-locality**

  In classical physics, interactions or information transfer occur locally and at a finite speed, never exceeding the speed of light. However, in quantum entanglement, particles appear to "communicate" instantly, regardless of the distance between them.

Quantum Superposition and entanglement

Before measurement, entangled particles exist in a superposition of multiple states. For example, an entangled pair may each have an uncertain spin.

Once one particle is measured, the state of the other particle is immediately determined. This does not mean information is traveling faster than light, but rather reflects the deep connection between the particles.

Applications of Quantum Entanglement

- **Quantum Computing:** Entanglement is used in quantum algorithms to create quantum parallelism, where multiple possibilities are processed at the same time.
- **Quantum Cryptography:** Entanglement forms the basis of quantum key distribution protocols like **Quantum Key Distribution (QKD)**, which can provide secure communication channels. Any attempt to eavesdrop on the entangled particles would immediately disturb the system and alert the communicating parties.
- **Quantum Teleportation:** Quantum entanglement is also used in **quantum teleportation**, a process where the state of a quantum particle is transferred from one location to another, without the particle itself physically moving.

Gates:

- In quantum computing, gates are used to modify the state of qubits. These gates function similarly to classical logic gates, which manipulate bits in traditional computing. However, quantum gates leverage quantum mechanical principles like superposition and entanglement to carry out computations.
- **Hadamard Gate (H Gate)**
- The Hadamard gate creates superposition. It transforms a qubit from a definite state (|0⟩ or |1⟩) into an equal superposition of both states. For example, it transforms |0⟩ into (|0⟩ + |1⟩)/√2 and |1⟩ into (|0⟩ - |1⟩)/√2.

Pauli Gates and Phase Gates

- **X Gate (NOT Gate)**: The X gate flips the state of a qubit. If the qubit is in state $|0\rangle$, it will change to $|1\rangle$, and vice versa. Very similar to the NOT gate in classical computers.
- **Y Gate**: The Y gate is similar to the X gate but introduces a phase shift along with the flip. It applies a 90° rotation around the Y axis of the Bloch sphere.
- **Z Gate**: The Z gate applies a phase flip to the qubit, changing its state from $|0\rangle$ to $|0\rangle$ (no change) but applying a phase shift of 180° to $|1\rangle$.
- **Phase Gates**
- **S Gate**: The S gate applies a phase shift of 90° ($\pi/2$) to the qubit. It transforms $|0\rangle$ into $|0\rangle$ and $|1\rangle$ into $i|1\rangle$.
- **T Gate**: The T gate applies a phase shift of 45° ($\pi/4$) to the qubit. It transforms $|0\rangle$ into $|0\rangle$ and $|1\rangle$ into $e^{(i\pi/4)}|1\rangle$.

CNOT Gate (Controlled-NOT Gate) and SWAP Gate

- The CNOT gate is a two-qubit gate that flips the state of the target qubit if and only if the control qubit is in state $|1\rangle$. It's a fundamental gate for creating entanglement in quantum circuits.
- **SWAP Gate**
- The SWAP gate exchanges the states of two qubits. If one qubit is in state $|0\rangle$ and the other in state $|1\rangle$, the SWAP gate swaps their states.

Toffoli Gate (CCNOT Gate) and Controlled Gates

- The Toffoli gate is a three-qubit gate that flips the third qubit (the target) if and only if the first two qubits (the controls) are both in state $|1\rangle$.
- **Controlled Gates**
- A **controlled gate** is a two-qubit gate where one qubit controls the operation on the second qubit. Examples include the controlled-Z (CZ) gate, controlled-Hadamard (CH) gate, and controlled-phase (CP) gate.

Interference

- Interference is a fundamental concept in quantum computing, stemming from the wave-like nature of quantum states. In quantum mechanics, particles, such as qubits, are represented by wave-functions, which can interfere with one another, similar to how water or light waves interact. In quantum computing, this interference enables quantum computers to enhance and amplify correct results while canceling out incorrect ones. This feature is crucial for many quantum algorithms and allows quantum computers to significantly outperform classical computers in certain tasks.

How Interference Works in Quantum Computing:

- When a quantum computer processes information, it works with **superpositions** of states. These superpositions can be thought of as a combination of different possibilities (like **0** and **1**). The goal of quantum algorithms is to manipulate these superpositions in a way that **constructively interferes** with the correct solutions and **destructively interferes** with the incorrect ones.
- **Constructive Interference**: This occurs when the amplitudes of specific quantum states combine in a way that boosts the likelihood of measuring the correct state.

  Destructive Interference: This happens when the amplitudes of certain states cancel each other, lowering the probability of measuring incorrect states.

Quantum Interference and Quantum Algorithms

- Interference is used strategically in quantum algorithms to amplify the probability of finding the correct answer. Below are a few examples where quantum interference plays a crucial role:
- **Grover’s Search Algorithm:**
- Grover's algorithm is a quantum search algorithm that solves the unstructured search problem more efficiently than classical algorithms. It begins by placing all possible states into a superposition, then uses interference to increase the probability of the correct answer. The algorithm applies operations repeatedly, creating constructive interference for the correct state and destructive interference for the incorrect ones.

Grover's Search Algorithm

- **Amplitude Amplification**: With each iteration, the amplitude (probability) of the correct solution grows, while the amplitude of incorrect solutions diminishes. This process is repeated several times to maximize the likelihood of obtaining the correct answer.

Quantum Phase Estimation:

- Quantum phase estimation is another quantum algorithm that uses interference. It estimates the phase (or eigenvalue) of an eigenstate of a unitary operator. The quantum phase estimation algorithm uses interference to **amplify** the correct phase estimation while **canceling out** incorrect ones.

- **Constructive and Destructive Interference:** By applying a series of controlled operations, the algorithm creates constructive interference for the correct phase and destructive interference for incorrect phases, leading to a high probability of measuring the correct value.

- **The Role of Measurement in Interference:**

Before measurement, qubits exist in superpositions of states, and the outcome of measuring the qubit is probabilistic. Quantum interference manipulates these superpositions so that the measurement outcome is more likely to produce the desired result.

- **Before measurement**: The system is in a superposition of all possible states.

- **During measurement**: The superposition collapses, and the interference patterns determine which state is most likely to be observed.

Measurement

- Measurement in quantum systems is used to extract information, but unlike classical systems where measurements yield definite results, quantum measurements are probabilistic and cause wave-function collapse. The result of a measurement depends on the quantum system's state prior to measurement, and the act of measuring changes that state in a way that differs fundamentally from classical measurements.

Key Concepts of Quantum Measurement

- **Wave-function Collapse:** Before measurement, a quantum system exists in a superposition, where it can be in multiple possible states at once. For example, a qubit can be in a superposition of both $|0\rangle$ and $|1\rangle$ simultaneously. Upon measurement, the quantum state "collapses" into one of the possible states (e.g., either $|0\rangle$ or $|1\rangle$ for a qubit). The specific outcome is random, but its likelihood is determined by the amplitudes of the superposition.
- **Probability of Outcomes:** In quantum mechanics, the probability of observing a particular state is tied to the amplitude of that state within the superposition. The probability is the square of the amplitude. For a qubit in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the probability of measuring $|0\rangle$ is $|\alpha|^2$, and the probability of measuring $|1\rangle$ is $|\beta|^2$, with the condition that $|\alpha|^2 + |\beta|^2 = 1$ (the total probability must sum to 1).

- **Measurement in the Computational Basis:** The most common measurement in quantum computing is in the computational basis, where qubits are measured in the states $|0\rangle$ and $|1\rangle$. When a qubit is measured, it collapses to either $|0\rangle$ or $|1\rangle$, with the outcome determined probabilistically based on the qubit's state before the measurement.

- **The Impact of Measurement:**

  - **Collapse:** After measurement, the qubit collapses into one of the basis states (either $|0\rangle$ or $|1\rangle$). For example, if a qubit is in a superposition such as $(1/\sqrt{2})(|0\rangle + |1\rangle)$, measuring it will cause the qubit to collapse to either $|0\rangle$ or $|1\rangle$, and the superposition is lost.

  - **Loss of Information:** Measurement is an irreversible process. Once the system is measured, the information about the superposition is permanently lost.

Software Development Framework

- **Qiskit (IBM)**

  Qiskit is a set of tools for creating, simulating, and running quantum circuits on both simulators and real quantum devices. Developed by IBM, it is designed to make quantum computing more accessible to developers, researchers, and students through an easy-to-use interface.

- **Cirq (Google)**

  Cirq, a Python library developed by Google, is intended for quantum algorithm developers. It is focused on designing, simulating, and running quantum circuits for gate-model quantum computers, especially for hardware based on this model.

- **PyQuil (Rigetti Computing)**

  PyQuil, developed by Rigetti Computing, is a Python library for writing and simulating quantum programs, enabling developers to work with quantum systems more easily.

Software Development Framework

- **Forest (Rigetti Computing)**
  Forest is Rigetti Computing's cloud-based quantum computing platform, offering access to both simulators and real quantum hardware for quantum computing tasks.
- **Microsoft Quantum Development Kit (QDK)**
  Microsoft's Quantum Development Kit (QDK) includes tools for developing quantum algorithms with Q#, a language created by Microsoft. It offers simulators and integrates with Visual Studio.
- **Ocean (D-Wave Systems)**
  Ocean, developed by D-Wave Systems, is a software suite designed for creating quantum applications, particularly focusing on optimization problems with quantum annealers, such as D-Wave's quantum hardware.
- **Strangeworks**
  Quantum Development Kit (QuDev)

Adoption of quantum computing in various sectors

- Even in its early stages, quantum computing is greatly promising to revolutionize fields like cryptography, drug discovery, optimization, artificial intelligence, and materials science
  - **Cryptography:**
- Quantum computers have the potential to undermine current encryption methods, like RSA encryption, which depend on the difficulty of factoring large numbers. Shor's algorithm, for instance, could factor these numbers much faster than classical computers, making existing encryption vulnerable.
- However, quantum computing also paves the way for advanced encryption methods such as Quantum Key Distribution (QKD). This technique uses quantum mechanics to ensure secure communication, where any attempt to intercept the data would disrupt the system, making eavesdropping detectable.

- **Drug Discovery and Healthcare:**
- Classical computers face challenges in simulating large molecules due to the complexity of quantum interactions. Quantum computers, however, can simulate molecules at the quantum level, accelerating the design of better drugs and materials.
- **Energy Optimization**: Quantum computing has the potential to improve energy grid efficiency by optimizing the distribution and management of resources, which will be increasingly important as the world shifts towards more sustainable energy sources.
- **Carbon Capture:** Quantum models could assist in simulating advanced materials for carbon capture, playing a vital role in efforts to address climate change.
- **Fundamental Science:** Quantum computing could also aid in advancing our understanding of the fundamental principles of physics. By simulating quantum systems more effectively than classical computers, it could lead to significant breakthroughs in quantum mechanics, cosmology, and other profound scientific areas.

Adoption of quantum computing in various sectors

Weather Forecasting and Climate Modeling:

- Climate modeling and weather prediction involve complex simulations with massive data sets. Quantum computers can process these interactions more effectively, potentially enhancing predictions and providing deeper insights into climate change, weather events, and environmental science.

Search and Data Retrieval:

- Grover's algorithm, a quantum algorithm, can search an unsorted database significantly faster than classical methods—quadratically faster, to be precise. While this may seem like a minor advantage for small databases, it could lead to substantial speed improvements in large datasets, benefiting fields like bioinformatics, search engines, and big data analytics.

Adoption of quantum computing in various sectors

- **Quantum Communication:** Quantum technologies, such as quantum key distribution (QKD), can enable highly secure communications that are immune to interception or hacking without detection.
- **Material Science and Nanotechnology:** • Quantum computing has the potential to transform the discovery of new materials by simulating atomic-level interactions and properties.
- **Financial Modeling:** • Quantum computers can assist with risk analysis, financial forecasting, and derivative pricing. By applying quantum algorithms to simulate complex financial systems, institutions could achieve more accurate predictions and optimize their strategies. • Monte Carlo simulations, commonly used in finance for stochastic modeling, could be processed much faster using quantum systems.

Benefits of Quantum computing

- **Exponential Speedup for Certain Problems**

  Quantum computers can solve specific problems, like factoring large numbers, much faster than classical computers, offering exponential speedup. This advantage extends to areas like optimization, machine learning, and simulations, where classical systems would take too long.

- **Handling Complex Simulations**

  Quantum computers excel at simulating complex systems at the atomic or molecular level, offering breakthroughs in fields like quantum chemistry, material science, and drug discovery, which are challenging for classical computers.

Benefits of Quantum computing

- **Improved Optimization**

  Quantum computing can enhance optimization tasks in industries such as finance and logistics. By exploring multiple solutions simultaneously, quantum algorithms enable faster and more accurate results in areas like route planning and resource allocation.

- **Enhancing Machine Learning**

  Quantum computing accelerates machine learning, improving algorithm efficiency in tasks like training deep neural networks and analyzing large datasets. This can lead to faster pattern recognition, more accurate models, and real-time data processing.

Benefits of Quantum computing

- **Better Security (Quantum Cryptography)**

  Quantum computing supports unbreakable encryption through Quantum Key Distribution (QKD), ensuring secure data transmission. It also aids in developing post-quantum cryptography to protect against quantum-enabled attacks on current encryption systems.

- **Revolutionizing Drug Discovery and Healthcare**

  Quantum simulations can significantly speed up drug discovery by providing detailed models of biological systems. They also help simulate protein folding, aiding in understanding and treating diseases like Alzheimer’s and Parkinson’s.

Benefits of Quantum computing

- **Advancing Materials Science**

  Quantum computing helps design new materials with specific properties, like superconductors or energy-efficient materials for batteries and solar cells. This could lead to advancements in electronics, pharmaceuticals, and various industries.

- **Increased Accuracy in Data Search and Retrieval**

  Quantum computing can accelerate data search and retrieval, using algorithms like Grover's Algorithm to process large datasets quickly, improving industries like healthcare and e-commerce.

Limitations of Quantum computing

- **Error correction**: Quantum systems are highly susceptible to noise, and correcting quantum errors is both complex and resource-demanding.
- **Scalability:** Existing quantum computers are small and can only manage a limited number of qubits. Expanding them to solve practical problems requires major technological breakthroughs.
- **Hardware limitations:** Quantum computers require highly controlled environments, such as extremely low temperatures or vacuum chambers, to function properly. Creating scalable and more accessible quantum hardware remains a significant challenge.

Limitations of Quantum computing

- **Limited Qubits**

  Quantum computers require a large number of stable, high-quality qubits to perform large-scale computations, but producing and maintaining these qubits is challenging. Currently, quantum computers can only manage a few dozen qubits, limiting their capabilities.

- **Algorithm Development**

  Many quantum algorithms are still under development, and the specific problems where quantum computing offers a clear advantage are still being explored. Quantum software also lags behind the maturity of classical software frameworks.

Limitations of Quantum computing

- **Classical-Quantum Hybrid Systems**

  A hybrid system combining classical and quantum computers may be more practical for many applications, but integrating the two is still a work in progress. It remains uncertain how effectively the systems can collaborate to solve real-world problems and provide an overall performance boost.

- **Ethical and Security Concerns**

  Quantum computers have the potential to break widely used encryption methods, like RSA, posing a threat to data security across various sectors.

Limitations of Quantum computing

- **Lack of Practical Applications**

  Quantum computing has theoretical benefits in areas like cryptography, material science, and optimization, but there are few real-world applications so far. While quantum supremacy has been demonstrated in solving specific problems, quantum computers are still far from offering broad practical use beyond these niche cases.

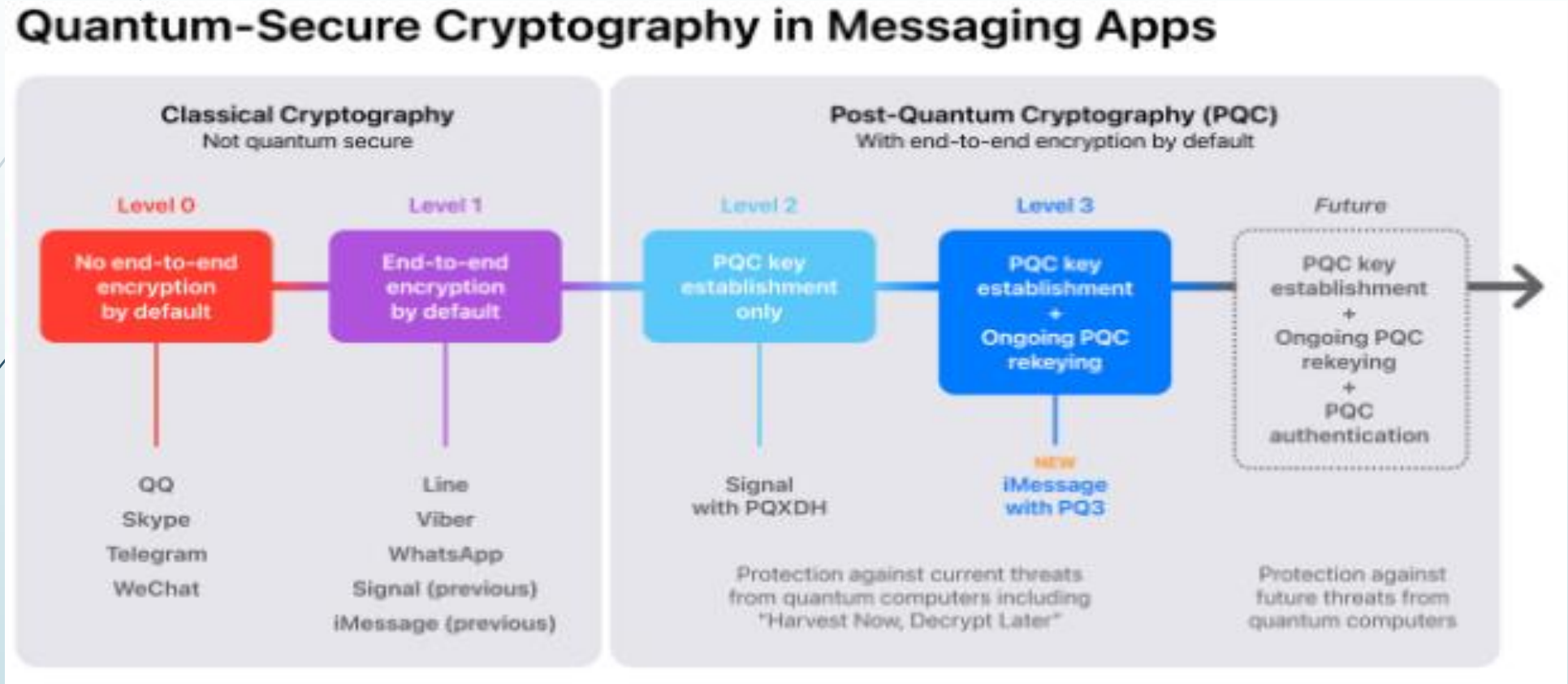
- **Cost**

  Building and maintaining quantum computers is prohibitively expensive due to the specialized equipment, infrastructure, and expertise required. Although quantum computing services are available from companies like IBM and Google, they rely on remote access, and real-time interaction with quantum systems remains a challenge.

The future of quantum computing

- **Quantum Cryptography and Security**
- **Post-Quantum Cryptography:** Quantum computers could break current encryption methods like RSA, prompting the development of quantum-resistant cryptography to safeguard data against quantum attacks.
- **Quantum Key Distribution (QKD):** Quantum key distribution promises ultra-secure communication by using quantum principles to detect any interception attempts. This could lead to tamper-proof systems for secure data transmission.

The future of quantum computing

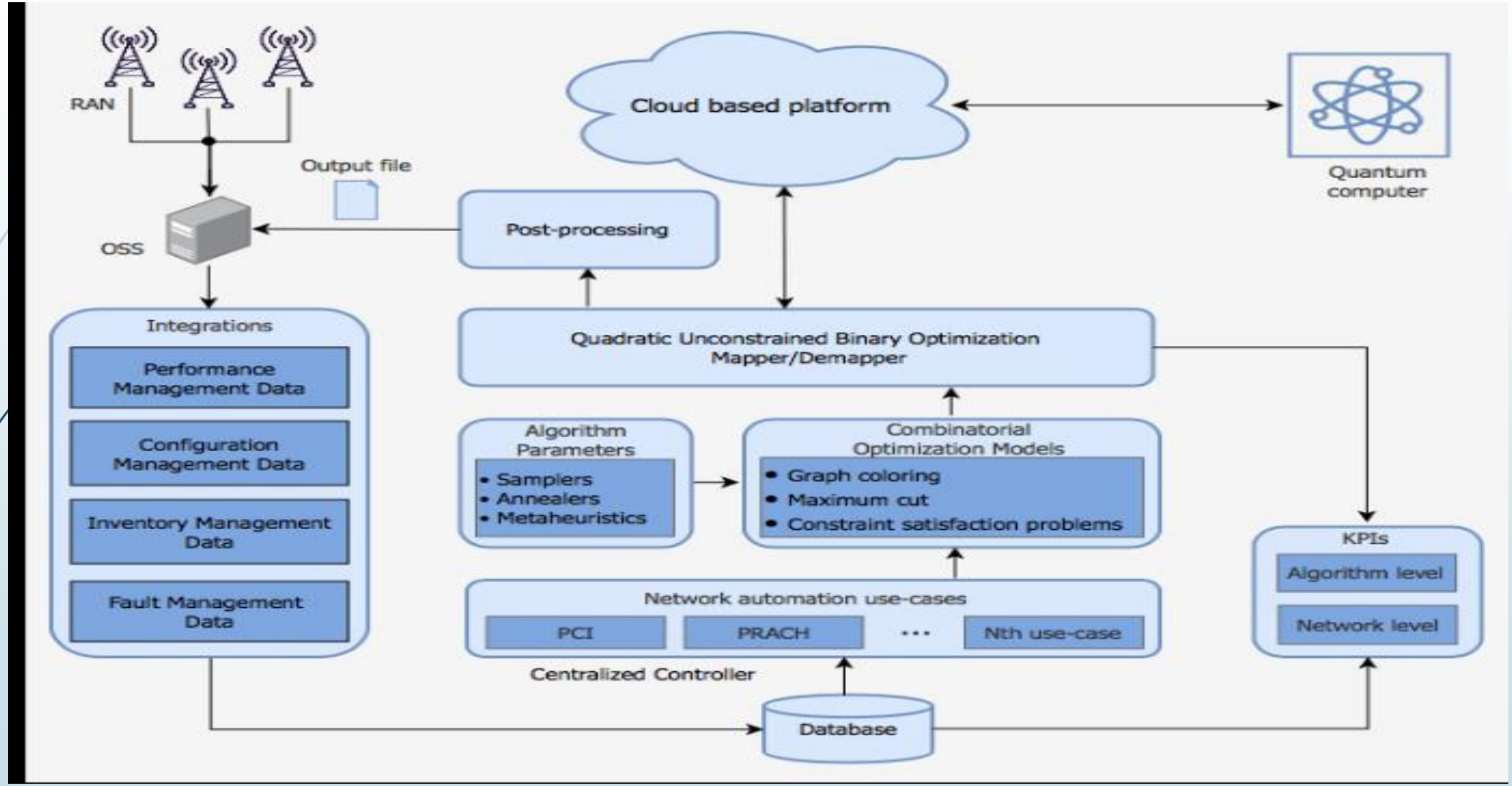


- https://www.linkedin.com/pulse/post-quantum-cryptography-what-do-you-really-need-edgar-ter-danielyan-ucdte/

Hybrid Quantum-Classical Systems

- **Cloud-Based Quantum Computing:** Major companies are offering quantum computing as a service via the cloud, making it more accessible to businesses, universities, and individuals without the need for costly hardware

Cloud-Based Quantum Computing



- https://www.researchgate.net/figure/A-QUBO-based-cloud-quantum-computing-framework-for-mobile-network-automation_fig1_353066250

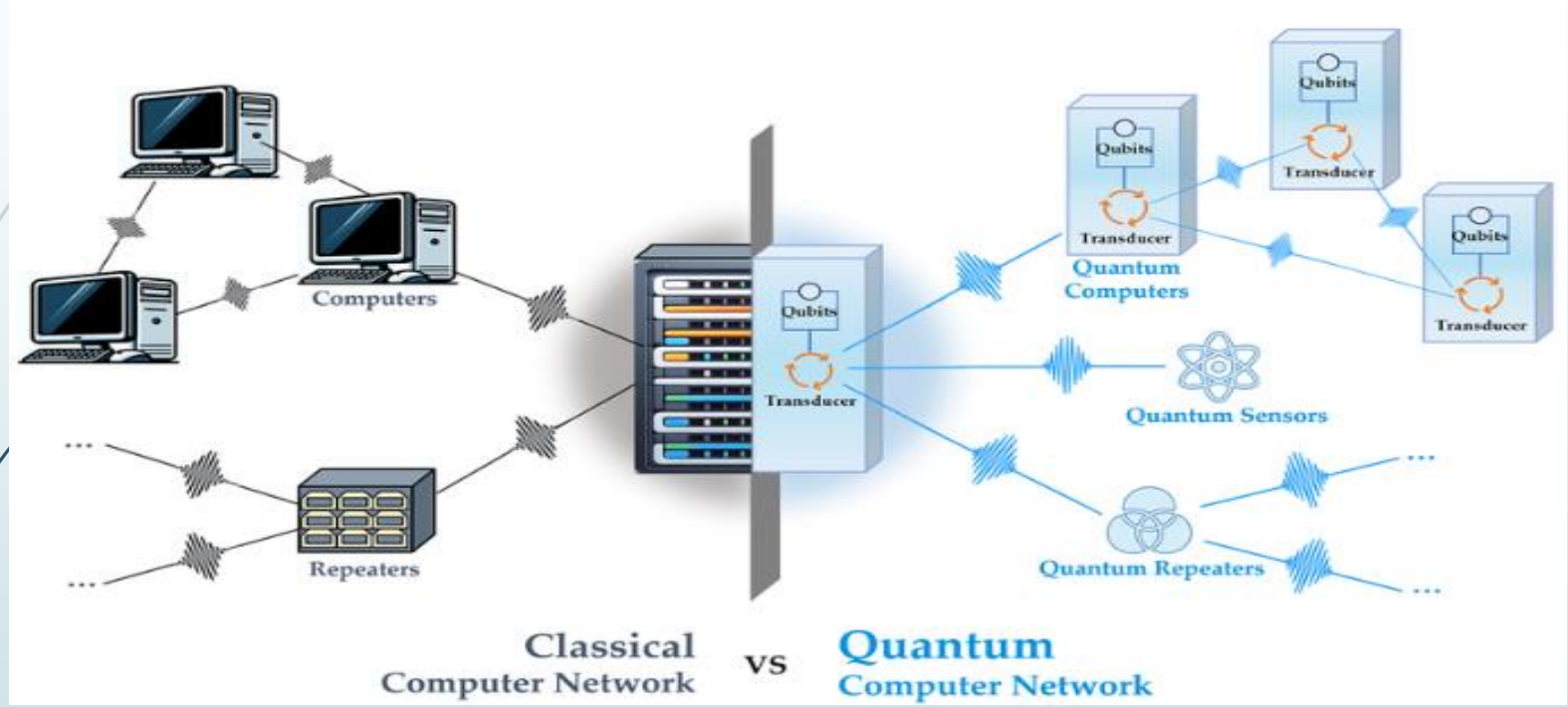
Improved Quantum Hardware

- **Different Types of Qubits:** Researchers are exploring various qubit technologies, such as superconducting, trapped ions, and topological qubits, and future quantum computers may use a combination of these methods.
- **Quantum Software and Algorithms**
- **New Quantum Algorithms:** While a few quantum algorithms have made significant breakthroughs, many are still in early stages. The development of new algorithms will expand quantum computing’s capabilities.

Quantum Networking and the Quantum Internet

- **Quantum Internet:** The development of a quantum internet could provide ultra-secure communication using entangled particles, creating a new way for secure data transmission between quantum systems.
- **Distributed Quantum Computing:** As quantum computers evolve, distributed quantum systems will allow multiple quantum computers to work together, harnessing their combined power for complex tasks.

Quantum Networking and the Quantum Internet



- https://www.researchgate.net/figure/Comparison-of-classical-and-quantum-computer-networks-The-left-illustrates-the-classical_fig1_379454279

References

1. Preskill, J. (2021). Quantum computing 40 years later. *Institute for Quantum Information and Matter*, 1-49.
2. Rasool, R. U. (2023). Quantum Computing for Healthcare: A Review. *Future Internet*, 1-36.
3. Rietsche, R. (2022). Quantum computing. *Electronic Markets*, 1-12.
4. Steane, A. (1997). Quantum computing. *Reports On progress in Physics*, 1-58.

Next Lesson

- Cyber security and Privacy Challenges