**In relation to a Turing machine**:

* The Turing machine is a theoretical device able to compute any and all computational problems. It is a tape of infinite length containing 0’s and 1’s. A read-write device reads the tape as data and uses instructions to compute the tape. In quantum computing, a Turing machine would exist in a quantum state meaning you could not only read 0 and 1 but also a super position of 0 AND 1 at the same time allowing for an infinite number of extra states held on the tape.
  + This means that whilst the Turing machine can only compute one calculation at a time, a quantum Turing machine can do multiple calculations at once.

**In relation to computational programming today:**

* Current computers use bits and bytes to compute problems. A 0 and 1 are used to compute and simulate everything. A quantum computer is not restricted to two states as they can encode data as quantum bits (often referred to as qubits) which can exist in superposition.
  + Super position is the idea/theory from quantum mechanics that the position of an object or state can be represented as a sum of two or more other distinct states.
    - Further into this; superposition is that idea that an object or state can be 1 or 0 or anything in between and cannot be concluded until observed.
* The superposition of qubits is what powers quantum computers and what allows for this innate parallel computational power. “*According to physicist David Deutsch, this parallelism allows a quantum computer to work on a million computations at once, while your desktop PC works on one*” (Bonsor & Strickland, 2019)

**In relation to computational power:**

* A 30-qubit quantum computer is roughly equal in power to a “normal” computer running at 10 *teraflops* (10 trillion floating-point operations per second)
* Another aspect of quantum computing is a quantum science mechanic called entanglement. The basic idea is that if two particles (qubits in this case) become entangled, any superposition imposed on one will have the opposing super effect on the other. The issue with quantum computing and why it’s so difficult is because under observation, a qubit will “drop” out of superposition and gain the value of either 1 or 0 instead of having its quantum state. This means that scientists have to find a way to indirectly read a qubits state. Quantum entanglement might be the answer.

**In relation to computer software development today with security:**

* “*many national government and military funding agencies support quantum computing research to develop quantum computers for both civilian and national security purposes, such as cryptanalysis*” (Quantum Computer, n.d.)
  + The current problem that cryptanalysis and security companies are worried about is that quantum computers could easily be used to crack large hash keys and security vaults. Most bank security is based of an absolutely massive has key value unique to an individual. Most normal computers would take centuries to crack such a code because they can only compute one brute force test per second, but a quantum computer, running multiple calculations per second and per calculation could crack these security keys within a realistic time (only months or possibly weeks) (Numberphile, 2012)

Some other links

* <https://www.sciencedaily.com/terms/quantum_computer.htm>
* <https://www.alphr.com/technology/1006491/what-is-quantum-computing-and-why-does-the-future-of-earth-depend-on-it>
* <https://www.sciencedaily.com/releases/2018/10/181018141107.htm>
* <https://en.wikipedia.org/wiki/Quantum_superposition>

# References

Bonsor, K., & Strickland, J. (2019, July 22). *How Quantum Computers Work*. Retrieved from howstuffworks: https://computer.howstuffworks.com/quantum-computer1.htm

Numberphile. (2012, December 9). *Encryption and HUGE numbers - Numberphile.* Retrieved from YouTube.com: https://www.youtube.com/watch?v=M7kEpw1tn50

*Quantum Computer*. (n.d.). Retrieved from ScienceDaily: https://www.sciencedaily.com/terms/quantum\_computer.htm