**Research:**

**Videos:**

<https://www.youtube.com/watch?v=QuR969uMICM>

* Controls behaviour of fundamental particles
* Qubit contains certain probability of being 1, certain probability of being 0, exists as a superposition of 1 and 0
* Allows for uncertainty
* Quantum uncertainty in private keys causes hackers to be unable to break the key without breaking laws of quantum physics
* Quantum simulations for drugs could be more accurately modelled by quantum computers
* Information can be teleported across internet without physically transporting information

<https://youtu.be/JhHMJCUmq28?si=FTiZQN_JofFA6wJZ>

* Exponential advancements of computers is reaching limit, can not get smaller than an atom so quantum is a new form of advancement
* While unobserved, qubit can be in superposition but once observed must be 1 or 0
* Entanglement allows for qubits with close connections to react to each other’s states instantaneously
  + From 1 entangled qubit, properties of partner qubits can be directly deduced
* Qubit manipulation involved qubit gates taking superpositions as inputs and returning a superposition as an output through manipulating inputs and rotating probabilities
* Allows all possible calculations to be done at the same time
  + Only 1 result can be measured and if not result desired, must try again
  + Can be exponentially more efficient than normal computers regardless
* Quantum computers use root(n) time complexity where computers use n time complexity.
* Can be used to crack public and private keys rapidly, ruining security

<https://youtu.be/e3fz3dqhN44?si=dSGT51cF3ERw_mGj>

* Kept at temperatures colder than space, 15 mK
* Consists of quantum chip + dilution refrigerator and cables carrying signals from fridge into processor + cables returning information to room temperature control electronics translating into things humans can understand
* Qubits act like waves, when multiple are working in close proximity, they can interfere constructively or destructively
* Instead of doing every calculation, it calculates most probable answer
* Quantum computers are good at finding structure in lots of data
* Useful in battery technology and creation of new materials
* If it is physically possible, engineers will find a way to make it happen

<https://youtu.be/CMdHDHEuOUE?si=CdzRw6ntSxT9EZLs>

* 2 objects in quantum entanglement can be strongly related to each other while far apart
* Can be used to solve optimisation problems as they get larger

<https://youtu.be/-UrdExQW0cs?si=COK9I6_q2oDU_nzM>

* Sndl relies on future quantum computers
  + Information from now will still be valuable in a decade, eg. research and secret intelligence
  + People required to use quantum-resistant encryption now to prevent this
* Quantum computers are useless for most applications
* Quantum fourier transform can be used to extract frequency information from a periodic superposition
* Idk what this guy is saying anymore hes just using words and maths
* Quantum can be used to speed up finding r such that g^r = mN + 1, when finding N, product of 2 primes
  + Should only take thousands of perfect qubits
  + Currently only have imperfect qubits so extra qubits required to act as redundant information

<https://youtu.be/OWJCfOvochA?si=0Rr-i-oex_b4tUTz>

* Once entangled, they are very difficult to separate
* Uses spins instead of transistors
* Constructive interference used to amplify signals towards right answer
* Destructive interference used to cancel signals towards wrong answer
* Superconducting qubits made from superconducting materials
* Assembly languages being built for quantum computers
* State of qubits controlled using microwave pulses
* Measured using microwave pulses
* Microwave pulses calibrated to change qubits, flip/entangle, etc.
* Old algorithms designed with perfect fault tolerant computers in mind, are not currently available
* Millions of error-correcting qubits required to run old algorithms on current quantum computers
* More qubits = more problems
* Decoherence limits how much information can be held at once

<https://youtu.be/60OkanvToFI?si=oZEp-gMvXHObg-op>

* Most quantum computers available for public research on the cloud
* Liquid nitrogen filter removes impurities from he3 and he4 mixture used to cool down systems
* Can take up to 2 days to cool from room temp and 4 weeks to recalibrate
* 16 layers of shielding protect signals from quantum chip
* Cooling system consists of 5 plates/stages, each stage getting lower temperatures
  + Final stage uses mixture of he3 and he4
* Chip connected with 400 superconducting wires
  + Uses quantum mechanical effects to process information
  + At higher temperatures data would become noisy due to heat-related quantum effects
* Processors consume no power and output no heat so all power dedicated to cooling system
  + Can use any number of qubits without needing more power

<https://youtu.be/g_IaVepNDT4?si=QO2eGBtpomU19p10>

* Electrons’ magnetic fields = spin, causing electrons to spin when placed in magnetic field
* Spin down = lowest energy state, when they align in the magnetic field
* Spin up takes energy, highest energy state
* N qubits contain same info as 2^N classical bits

<https://youtu.be/-ZNEzzDcllU?si=qRHuqyko6BMUYakf>

* Quantum supremacy = reach a point where classical computer can not simulate what is happening on quantum computer

<https://youtu.be/6yaY4Fw-ovM?si=DYjzhzWhbPVYJu1k>

* Superconducting Qubit = metal on a silicon chip
* Superconducting allows electrons to pass with 0 resistance, allowing them to take individual quantum states
* Circuit board must be kept in dust free environment as dust can contaminate small features on chip.
* Cryocoolers pulse helium gas into and out of refrigerator system drawing heat out of system.
* Resonator sensitive to state of qubit allows for reading of state of qubit
  + More easily accessible than qubit
* At some point energy decays from cupid causing it to fall from spin up to spin down state

<https://youtu.be/jHoEjvuPoB8?si=8WGPmyrV1YnA2rDj>

* Classical computers are not scalable for modelling quantum mechanics
* Quantum algorithms consist of qubit gates causing amplitudes to add up constructively so they can boost the outcome of the correct answers
* Most likely to be useful for modelling nature and physics

<https://youtu.be/u1XXjWr5frE?si=qrR80wQhiVtQ9PPr>

* Ibm disproved google’s quantum supremacy
* Qubits have amplitudes between 0 and 1
* 2 different quantum states of current flow through coils in chip representing 1 or 0
* Coils interact using josef’s injunctions, generating entangled states
* Interactions between qubits is fully programmable

<https://youtu.be/uOJCS1W1uzg?si=keDKIgdABB51Joey>

* Provides evidence for er=epr

<https://youtu.be/_C5dkUiiQnw?si=uoIpt5gHlJ3tvZ1T>

* Quantum cryptography = cryptography done on quantum computers
* Post-quantum cryptography = cryptography done on classical computers protecting against quantum computers
* Nist organised competition to find post quantum encryption methods
* Lattice, code, hash, multivariate, supersingular isogeny - methods

<https://youtu.be/QDdOoYdb748?si=0-YKkxv4g9EyKbxv>

* 2 very different vector pairs can generate the same lattice
* Shortest vector problem is ok in 2 dimensions, gets harder in multiple dimensions
* Believed to be difficult for classical and quantum computers
* eavesdroppers only have bad bases whereas people involved have good bases
* Current encryption + Sndi + quantum computers breaking encryption
* Quantum supremacy
* Quantum safe/post quantum cryptography
* Quantum cryptography

**How the world can be protected against the quantum computers of the future:**

The current encryption systems for information use the RSA encryption algorithm to encode data. This algorithm uses asymmetric encryption, where either the private or public key can encrypt the data and the other key can decrypt it. It involves 2 large primes being multiplied together to create an integer, n, which is then used to create both the private and public key. In order to break the key, any unauthorised user would have to deduce the 2 primes used to calculate n, and due to their large size, this is said to take classical computers approximately 19.8 quadrillion years using brute force. This is the current standard for encryption worldwide, and has protected data for over 40 years, but it is not prepared to protect against the quantum computers of the future.

Where a classical computer takes millions of aeons to decrypt the RSA encryption algorithm, it would take a quantum computer approximately 104 days to brute force the algorithm, an insignificantly small amount of time in comparison to the reward that could be achieved from cracking it. Using Shor’s algorithm, a quantum computer would be able to crack the RSA algorithm incredibly quickly, due to its ability to execute multiple calculations at once, allowing it to find the correct exponent to raise any number to such that it is equal to 1 above a multiple of n. This is the part that is the lengthiest for classical computers, as these numbers are so big, and due to being able to decrease the time taken for this step, quantum computers are thus able to crack the algorithm rapidly.

Though this many not seem to be such a large threat currently, as quantum computers are not powerful enough to do this, requiring 4000 qubits whilst the largest only contains 1121 qubits, hackers have become hopeful, and are now using the SNDL strategy - Save Now, Decrypt Later. This allows for them to save and download data now, that is still using RSA encryption, and then once quantum computers advance enough, decrypting the data. This is particularly dangerous as the data they are saving must be useful in 10 or more years for this to be worthwhile, and so hackers are downloading secret intelligence documents and important research documents, as they will still be valuable in the future.

Although quantum computers are often said to work differently to classical computers, not being necessarily better than them, this has been proved false. Quantum supremacy was achieved by Google in late 2019, conducting an experiment on a 70-qubit system that would take a supercomputer 47 years to conduct. While this is exciting, this is also alarming, as the above statement regarding the little time taken for a quantum computer to crack RSA was just a theory, supposed to be used in an ideal world with perfect fault-tolerant computers - quantum supremacy being achieved on imperfect systems proves that the theory could probably become a very real future.

Due to this theory, NIST - the National Institute of Standards and Technology in the USA, created a new competition, similar to their competition for new hash functions, this time focused on Post-Quantum, or Quantum-Safe, cryptography. Post-Quantum cryptography is often mistaken for Quantum cryptography, and while both very powerful and secure, they are completely different. Quantum cryptography is cryptography produced by a quantum computer to be run on a quantum computer, and is incredibly powerful and secure, as the qubits can only be measured in 1 state, whilst the key may be any of the other states the qubit is currently superposed in. Post-Quantum cryptography, however, is cryptography produced by classical computers to be run on classical computers, but to protect against the incredibly rapid decryption of quantum computers. The idea behind post-quantum cryptography is that ideally it should take equally long for a classical computer and a quantum computer to crack the key, and should also be incredibly secure against both types of computers.