**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