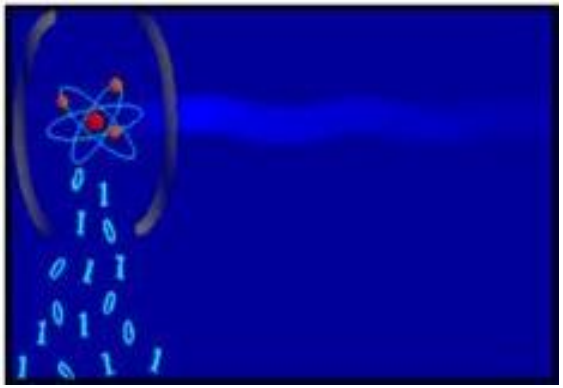
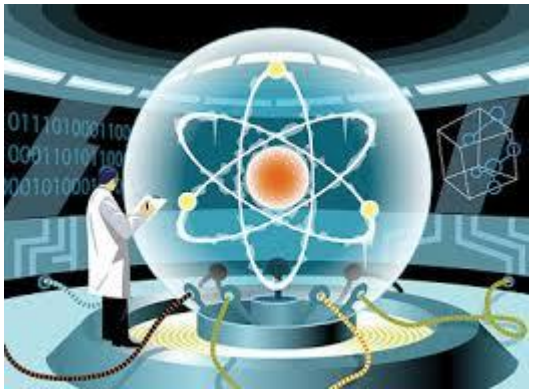
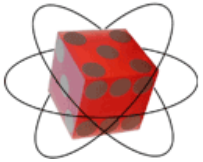




A gentle and practical introduction to quantum computing

by Doug Matzke. Ph.D.

Presented at IEEE-CS
at UTD TI Foundation Auditorium
Wed Oct 31, 2018

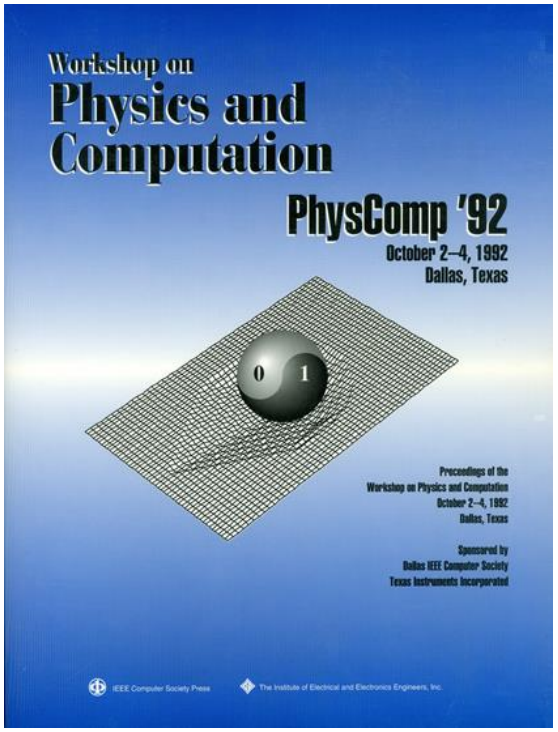


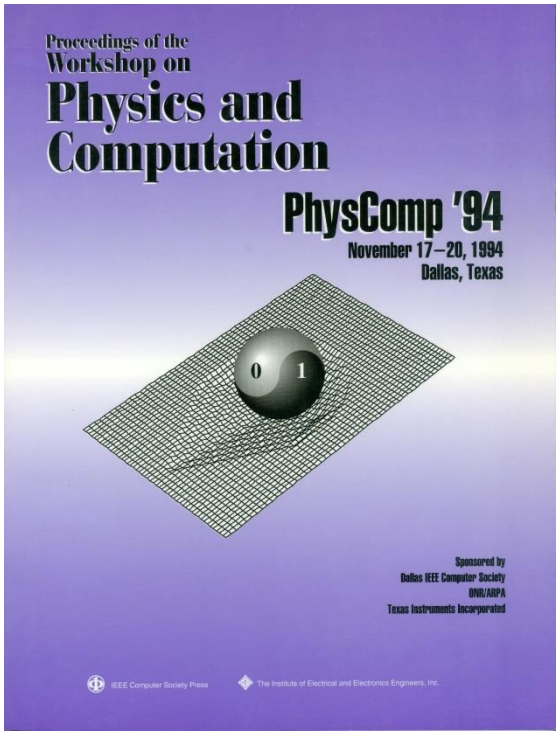
Abstract

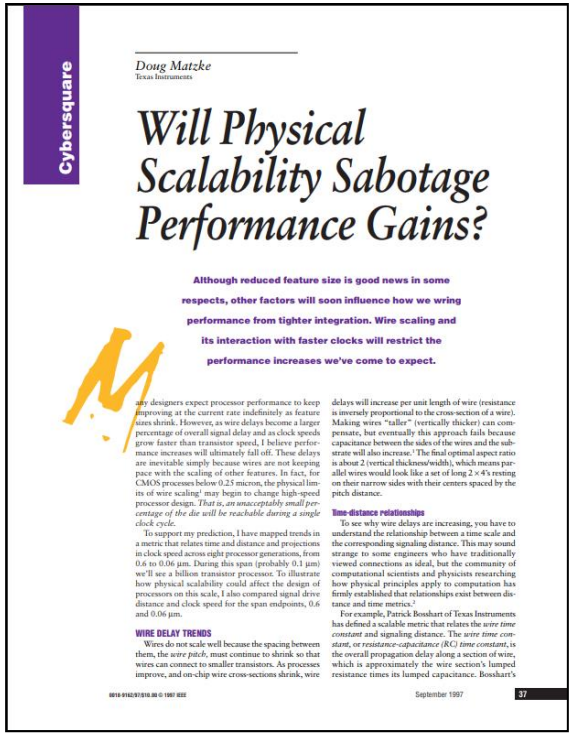
Quantum computing and Quantum Physics contains important concepts about how the world is built. The fundamentals of the classical world is bits with its mutually exclusive 1/0 values. Quantum computing is based on qubits that are the superposition (or mixture) of two classical bits, and this property means that bits and probabilities are fundamental to physics. Two qubits are combined in quantum registers to form ebits, which represents the smallest case of entanglement. Quantum registers can run Shor's algorithm that factors numbers faster than any classical algorithm. Due to ebits' strange properties Einstein call them "spooky action at a distance", but now shown to be very real. Typically these properties of superposition and entanglement are studied with complex mathematics, but they can be learned conceptually, which will be the basis of this gentle introduction.

Once these concepts are understood that the universe is fundamentally probabilistic and informational then they can help describe such phenomena as: it from bit, universe as simulation, tunneling, particle/wave duality, Schrodinger's cat, Bose-Einstein condensate, zero-point energy and even apply these concepts to software. Take away from this talk a better appreciation of the spectacular nature of how the universe is organized as hyperdimensional collections of bits.

My Background in PhysComp







Cybersquare

Doug Matzke
Texas Instruments

Will Physical Scalability Sabotage Performance Gains?

Although reduced feature size is good news in some respects, other factors will soon influence how we wring performance from tighter integration. Wire scaling and its interaction with faster clocks will restrict the performance increases we've come to expect.

Many designers expect processor performance to keep improving at the current rate indefinitely as feature sizes shrink. However, as wire delays become a larger percentage of overall signal delay and as clock speeds grow faster than transistor speed, I believe performance increases will ultimately fall off. These delays are inevitable simply because wires are not keeping pace with the scaling of other features. In fact, for CMOS processes below 0.25 micron, the physical limits of wire scaling[1] may begin to change high-speed processor design. *That is, an unacceptably small percentage of the die will be reachable during a single clock cycle.*

To support my prediction, I have mapped trends in a metric that relates time and distance and projections in clock speed across eight processor generations, from 0.6 to 0.06 µm. During this span (probably 0.1 µm) we'll see a billion transistor processor. To illustrate how physical scalability could affect the design of processors on this scale, I also compared signal drive distance and clock speed for the span endpoints, 0.6 and 0.06 µm.

WIRE DELAY TRENDS

Wires do not scale well because the spacing between them, the *wire pitch*, must continue to shrink so that wires can connect to smaller transistors. As processes improve, and on-chip wire cross-sections shrink, wire delays will increase per unit length of wire (resistance is inversely proportional to the cross-section of a wire). Making wires "taller" (vertically thicker) can compensate, but eventually this approach fails because capacitance between the sides of the wires and the substrate will also increase.[1] The final optimal aspect ratio is about 2 (vertical thickness/width), which means parallel wires would look like a set of long 2 × 4's resting on their narrow sides with their centers spaced by the pitch distance.

Time-distance relationships

To see why wire delays are increasing, you have to understand the relationship between a time scale and the corresponding signaling distance. This may sound strange to some engineers who have traditionally viewed connections as ideal, but the community of computational scientists and physicists researching how physical principles apply to computation has firmly established that relationships exist between distance and time metrics.[2]

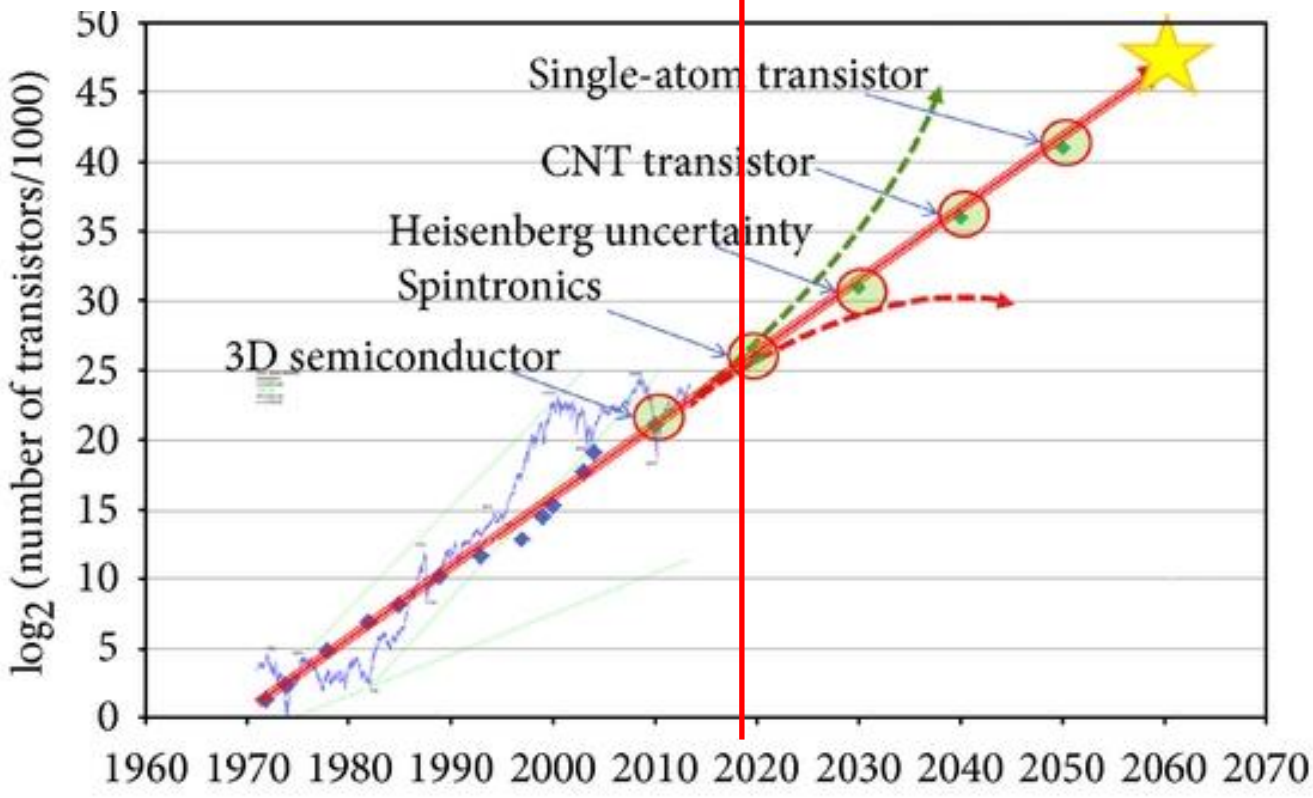
For example, Patrick Bosshart of Texas Instruments has defined a scalable metric that relates the *wire time constant* and signaling distance. The *wire time constant*, or *resistance-capacitance (RC) time constant*, is the overall propagation delay along a section of wire, which is approximately the wire section's lumped resistance times its lumped capacitance. Bosshart's

0018-9162/97/$10.00 © 1997 IEEE

September 1997 37

Chairman of two PhysComp workshops on Physics and Computation
Lead off article in Computer Magazine Sept 1997 "Billion Transistor Computers"
Ph.D. at UTD in Quantum Computing using Geometric Algebra in 2002
Principle Investigator SBIR Grants for Quantum/Neural Computing 2003-2005
Created 13 patents issued or filed

Importance of Computational Scaling

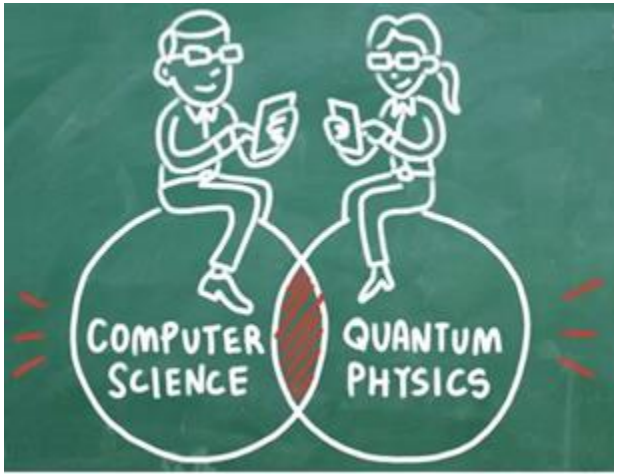


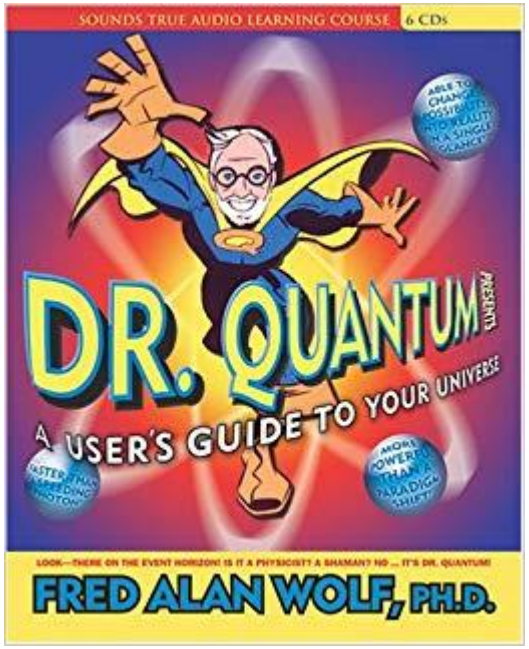
End of Moore's Law is soon!!

YEAR OF PRODUCTION	2010	2012	2013	2015	2016	2018
Technology Node	hp45		hp32		hp22	
DRAM ½ Pitch (nm)	45	35	32	25	22	18
MPU/ASIC M1 ½ Pitch (nm)	54	42	38	30	27	21
MPU/ASIC Poly Si ½ Pitch (nm)	45	35	32	25	22	18
MPU Printed Gate Length (nm)	25	20	18	14	13	10
MPU Physical Gate Length (nm)	18	14	13	10	9	7

Quantum Computing from Physics

- Particle wave duality
- Schrodinger's Cat
- Quantum States
- Quantum Probabilities
- Quantum Tunneling
- Quantum Noise
- Quantum Measurement
- Coherence/decoherence
- Heisenberg Uncertainty
- Reversible Phase Computing
- Dr. Quantum on YouTube
- PBS Spacetime on YouTube



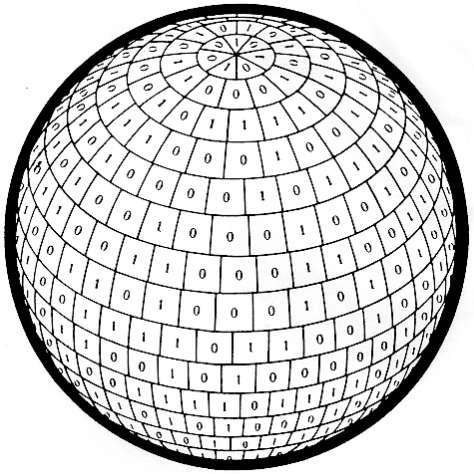


Information is Physical

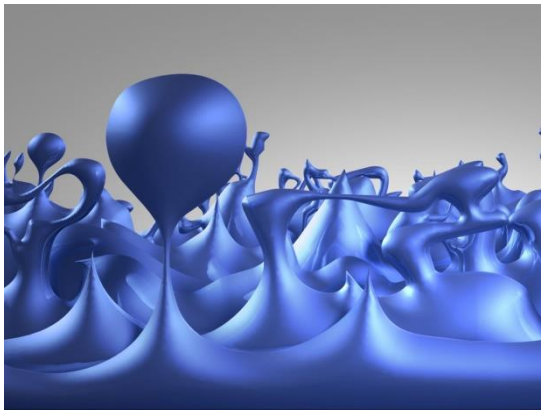
Bits are part of physics, not just computer science

- Rolf Landauer: Information is Physical (bit = $kT \ln 2$)
- Erasing of information effects thermodynamics
- Reversible computing is essential to QuComputing
- Bit is smallest increment to Black Hole (Planck area)
- John Wheeler: “It from Bit” (quantum matrix)
- Particle/Wave duality and Uncertainty Principle

“Quantum Matrix”

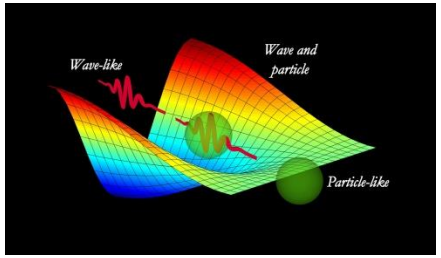


“It from Bit”



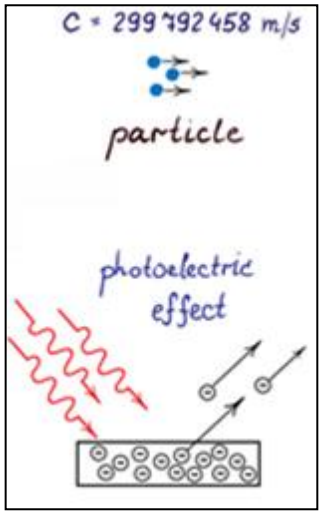
“Quantum Foam”

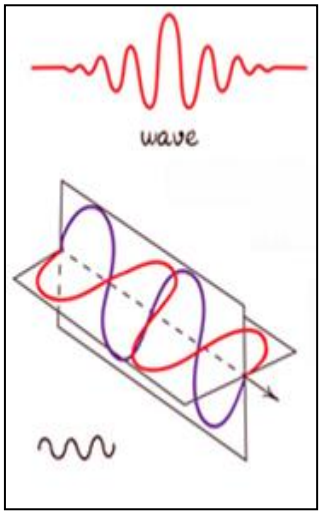
Quantized Waves

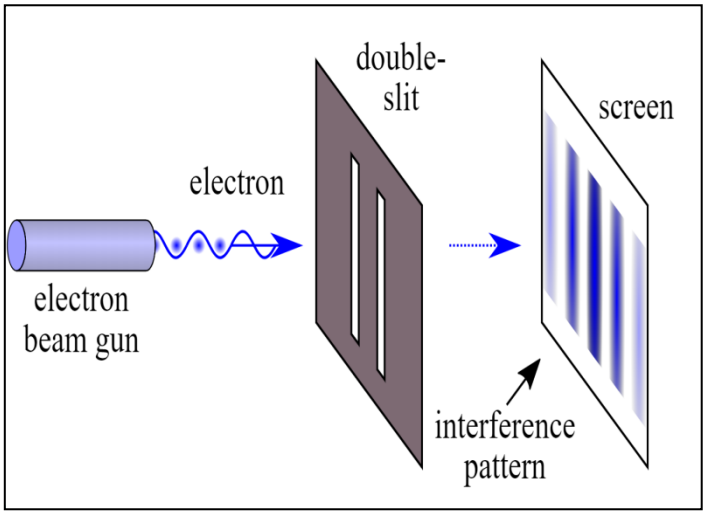


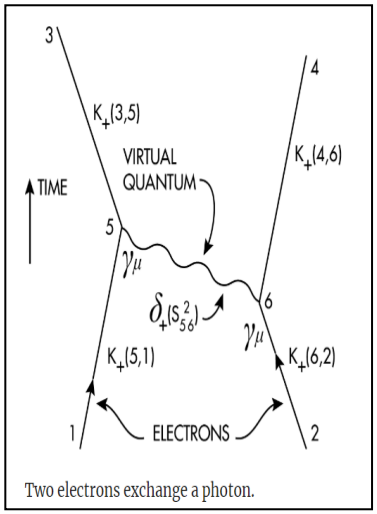
- Quantum states are distributed probability waves
- Photons/particles are quantized
- Waves/particles depending on measurement
- Waves construct even Planck Scale spacetime
- Self Consistent over all paths (Feynman diagrams)

Wave-Particle Duality





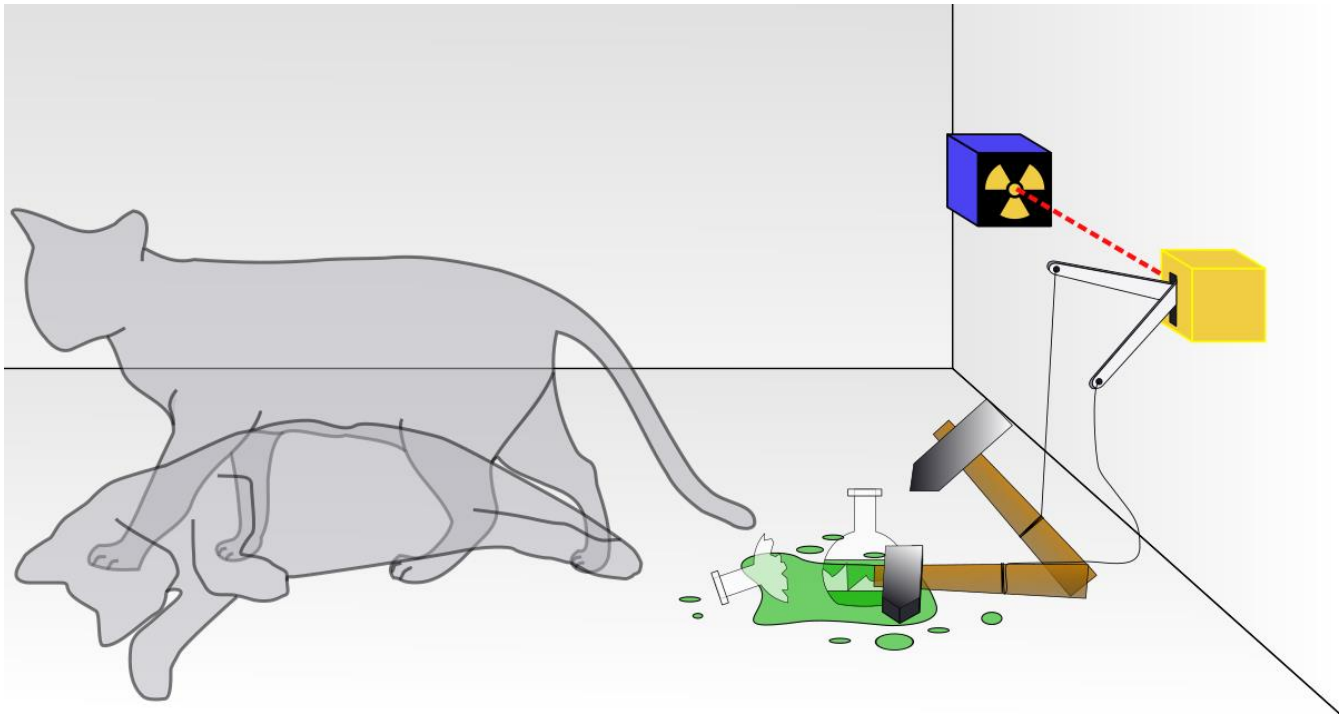




Schrodinger's Cat

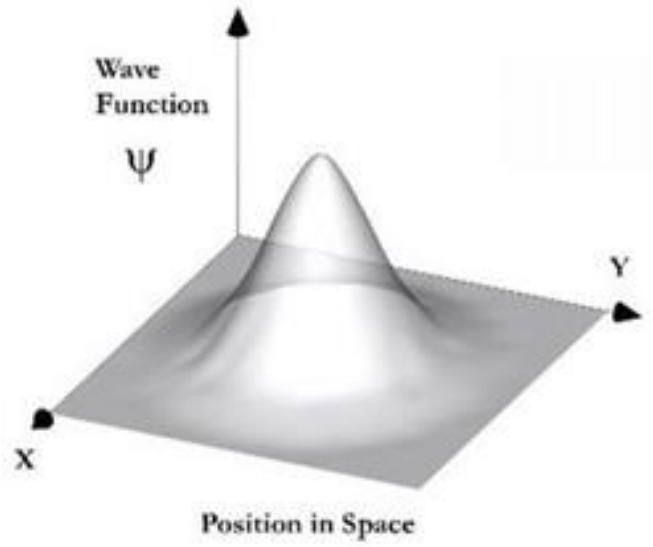
Thought experiment about extent of probabilities:

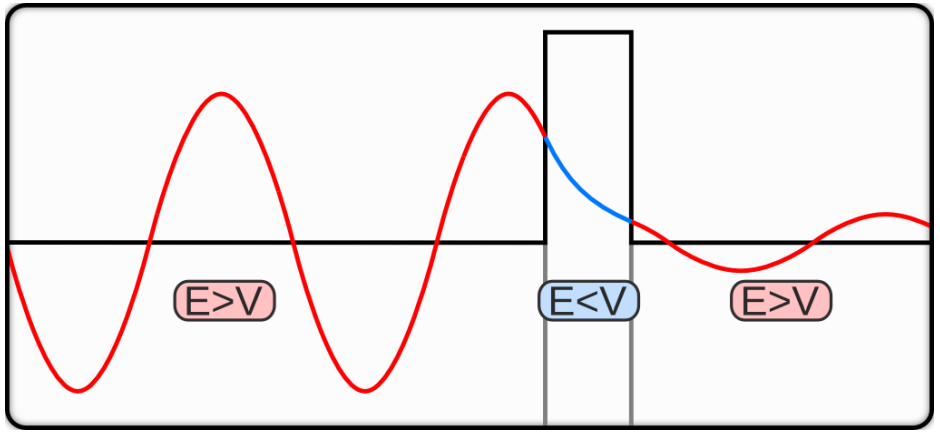
- Quantum Probabilities at the Macro Scale?
- Cat Dead and/or Alive due to quantum prob



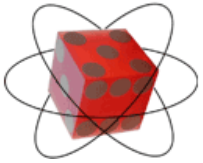
Quantum Tunneling

- Particle position is also a probability amplitude
- Probability amplitude is non-zero thru barrier (p>0)
- Probability the particle escapes energy barrier
- Superposition of position at atom/molecular level





Heisenberg Uncertainty Principle



The position and the velocity of an object cannot both be simultaneously measured exactly, even in theory. This duality is due to non-commutative properties and is similar to how Fourier series frequency vs time conjugate information. So quantum mechanical systems have intrinsic uncertainty.

Uncertainty in momentum

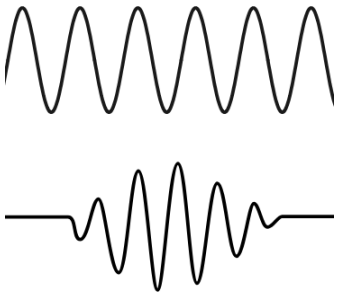
Uncertainty in position

$$\Delta p \, \Delta x \geq \frac{1}{2} \hbar$$

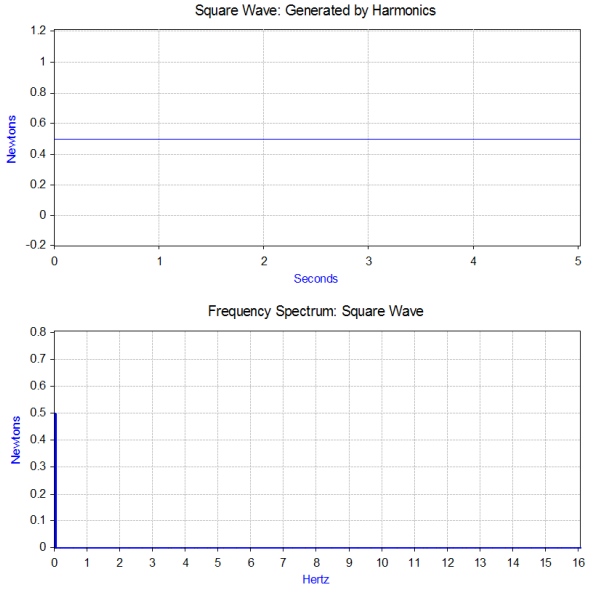
$$\Delta E \, \Delta t \geq \frac{1}{2} \hbar$$

Uncertainty in energy

Uncertainty in time

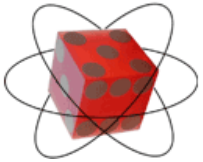


Wave packets



Affects our spacetime models

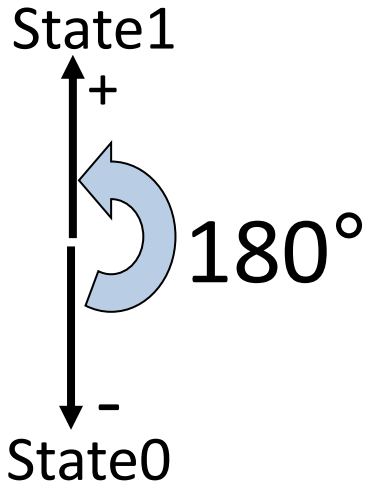
Qubit: two bits in Superposition

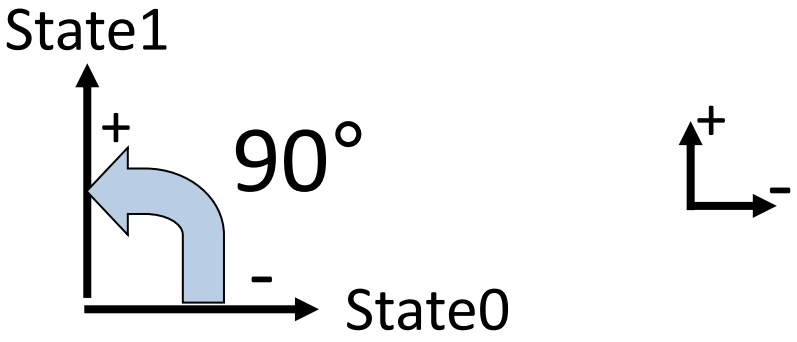


Superposition is a quantum property:

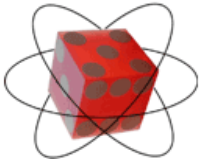
- Phase computing is source of all probabilities
- All states are simultaneous/concurrently present

Classical bit states: Mutually Exclusive	Quantum bit states: Orthogonal





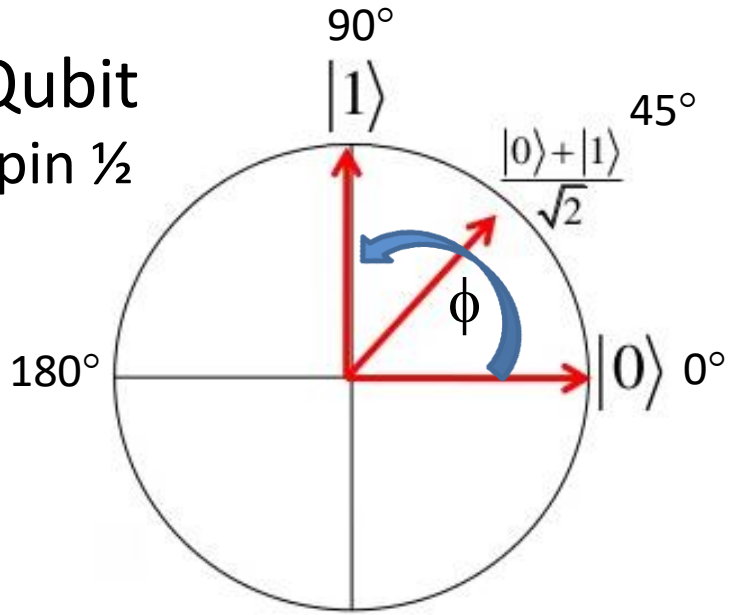
Probabilities from Qubits



- Bra-ket notation for matrices (Hilbert Spaces)
- Coefficients c_x are complex probability amplitudes
- Amplitudes squared c_x^2 are probabilities
- Unitarity: $c_0^2 + c_1^2 = 1$ (sum of probabilities is 1)
- Reversible phase based computing
- No-Cloning Theorem

Qubit

spin ½



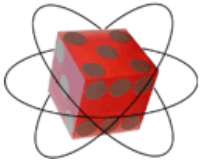
Superposition

$$c_0|0\rangle + c_1|1\rangle$$

$$state0_0 = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

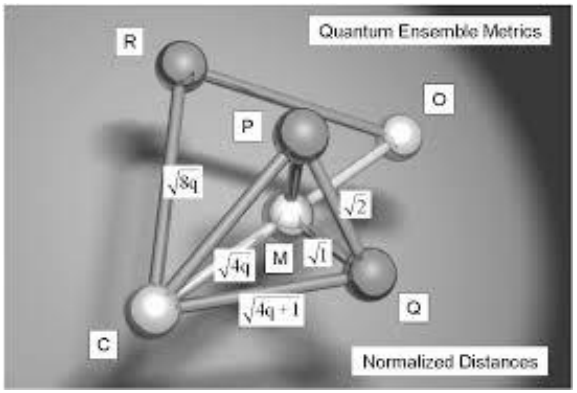
$$state1_0 = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Superposition in Software States



Use Case during the UI Design in ClicBank:

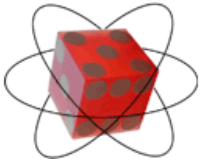
1) Editing atomic entity
2) Editing evolves to include extended states
3) Operator could cancel or complete entire edit state space
4) Created superposition of Done/Cancel



Use Case for neural network Software:

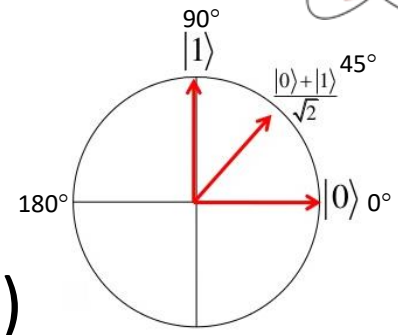
1) State space naturally forms phase relationships
2) Macroscopic equivalent of qubit phases
3) Probabilities result from these phase relationships
4) Related to probabilities of predictive analysis
5) Mutually exclusive states are abnormal in hyper dimensional spaces

Operators for a Qubit



Reversible operations on a qubit

- Unitary Gate (no phase change)
- Phase Gate (rotate by some phase angle)
- Hadamard Gate (rotate by 45 degrees)
- Not Gate (rotate by 90 degrees)
- Invert Gate (rotate by 180 degrees)

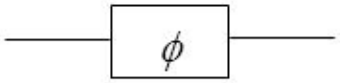


$H|0\rangle \rightarrow \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

$X|0\rangle \rightarrow |1\rangle$

Phase Shift gate

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$



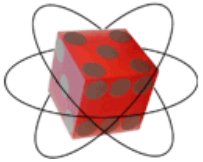
Hadamard gate
$\sqrt{NOT}$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Pauli Noise gates
X=Not gate

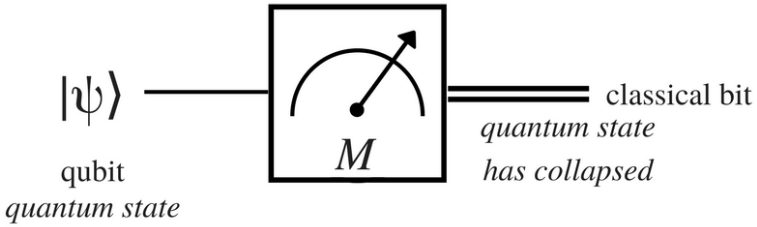
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

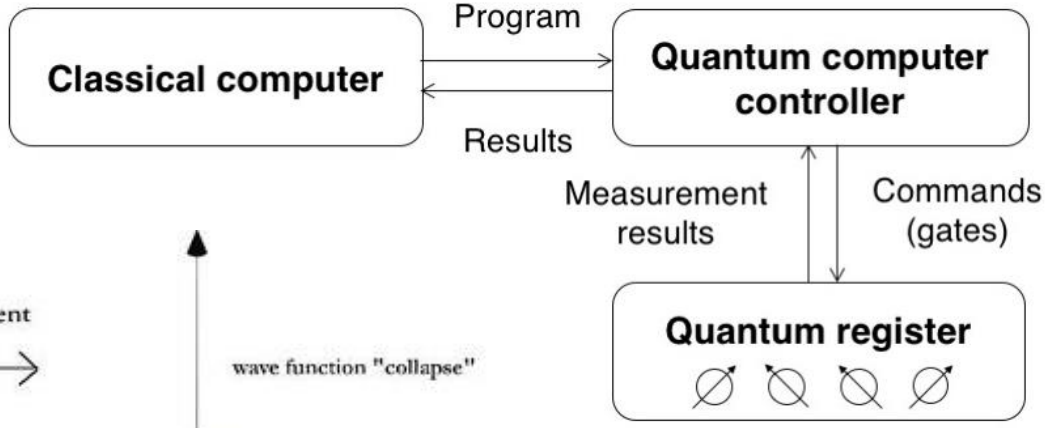
Measurement on a Qubit

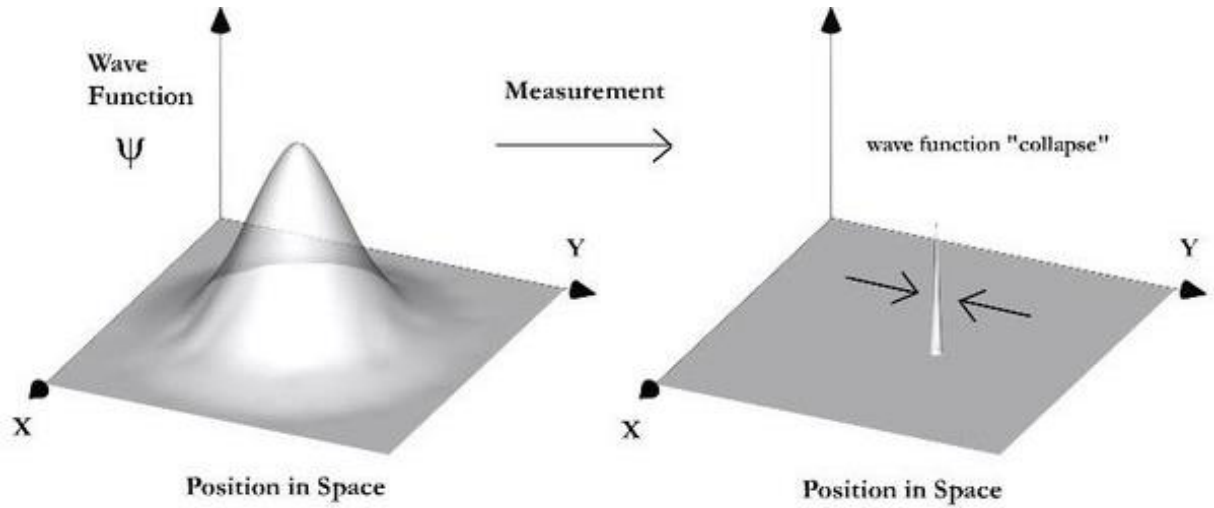


Irreversible operation on a qubit

- Measurement gives probabilistic result
- Probability is based on relative phase angle
- Collapse the wave function (Copenhagen Interpretation)







Operators for 2 Qubits

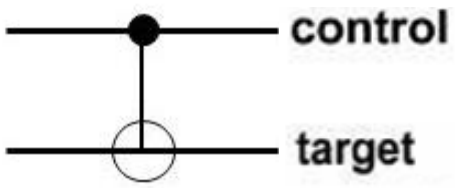
Reversible operations on two qubits

- Two or more qubits form a quantum register
- Quantum register has 2^q states (tensor product)
- CNOT: Controlled-NOT (conditional flip)
- SWAP: Controlled-phase

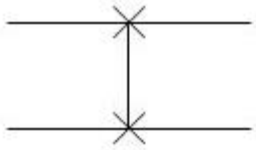
$$|0\rangle \otimes |1\rangle$$

Feynman Gate
CNOT (controlled-NOT)

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

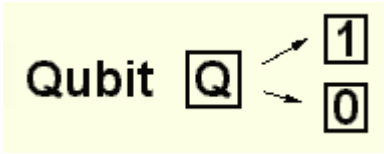


Swap (controlled-phase)

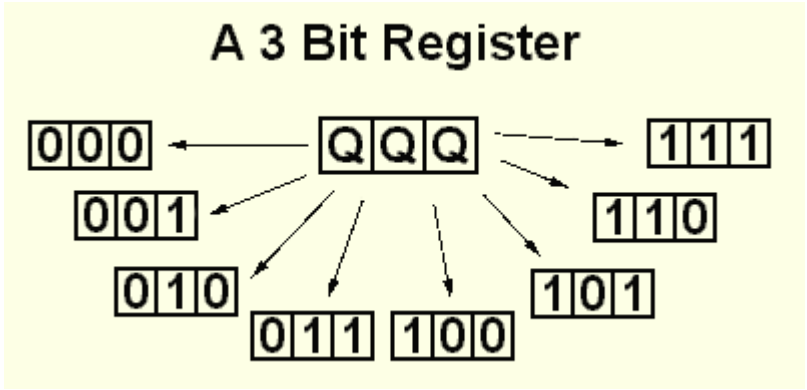


$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

QuReg Amplifies Phase Computing



Q=R=S=$(c_0|0\rangle + c_1|1\rangle)$



$$Q \otimes R \otimes S$$

$$+c_0|000\rangle$$
$$+c_1|001\rangle$$
$$+c_2|010\rangle$$
$$+c_3|011\rangle$$
$$+c_4|100\rangle$$
$$+c_5|101\rangle$$
$$+c_6|110\rangle$$
$$+c_7|111\rangle$$

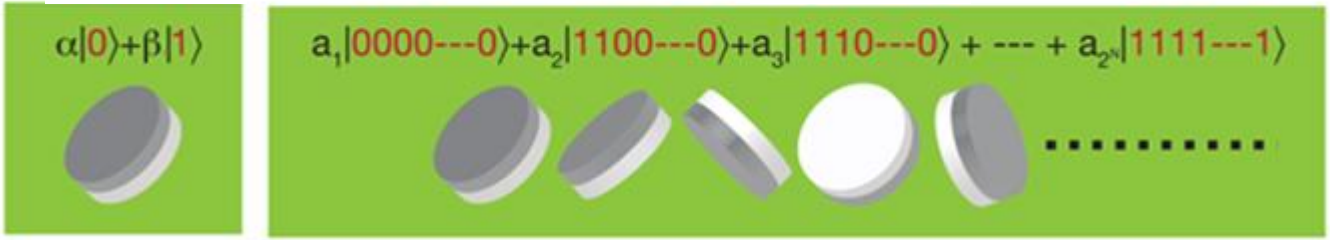
1 Bit *N Bits*

Either 0 or 1

One out of 2^N possible permutations

$$\sum c_i^2 = 1$$

1 Qubit *N Qubits*



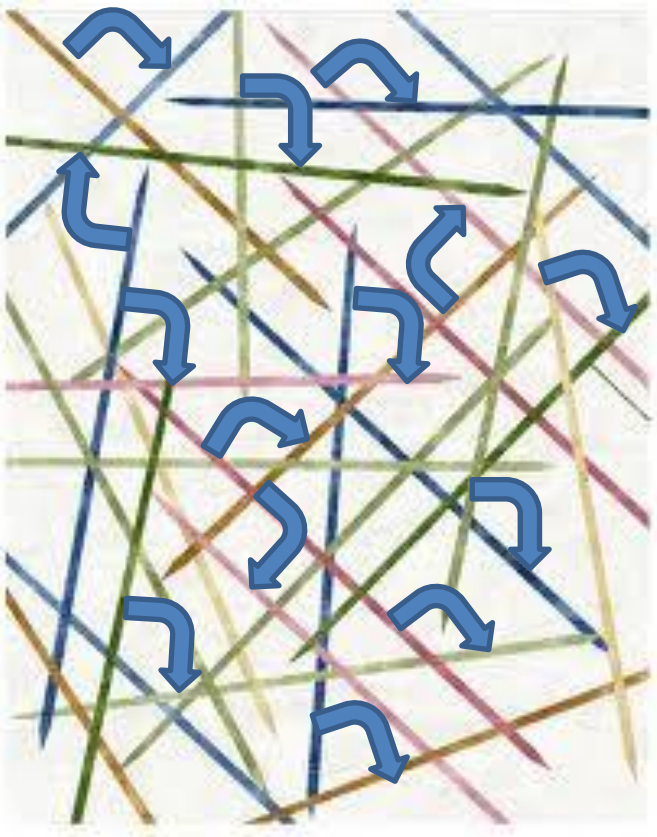
Both 0 and 1

All of 2^N possible permutations

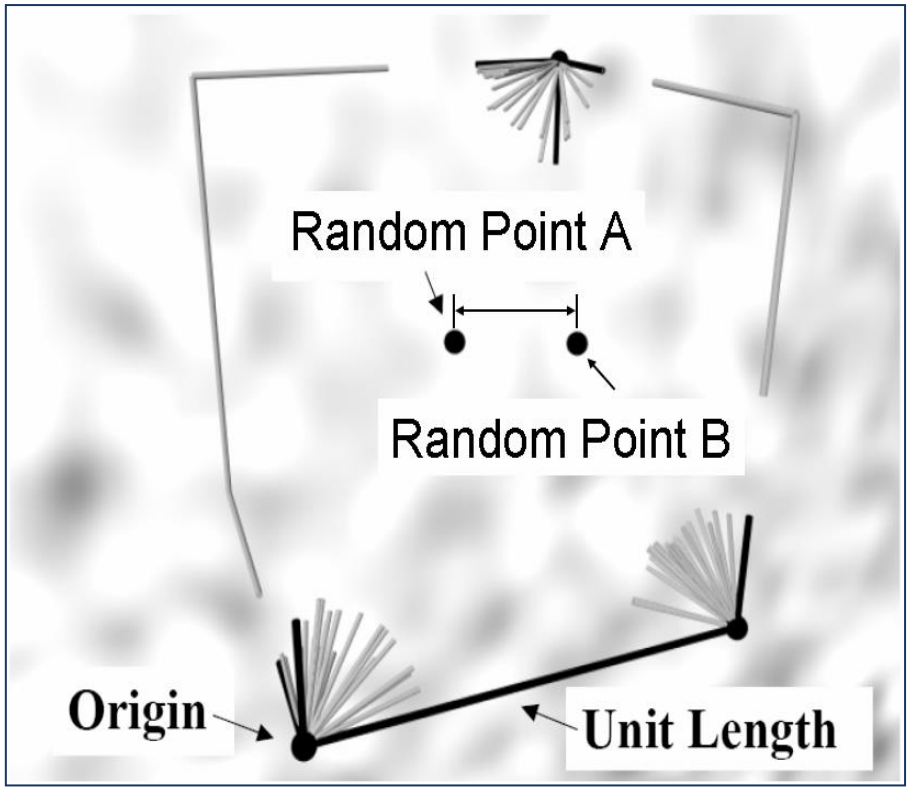
for q=300 qubits, 2^{300} > # particles in known universe

Visualizing hyperdimensions

Orthogonal dimensions

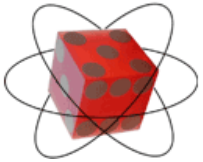


Points in hyperdimensions



Cannot be embedded in three dimensions or 2D hologram!!

Operators for 3 Qubits (Qutrit)

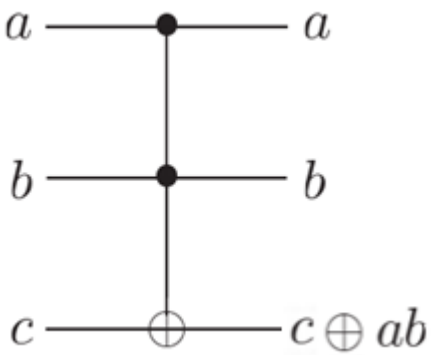


Universal Reversible operations on three qubits

- Gates don't erase information (Landauer's principle)
- Can be run forward/backward (billiard ball computing)
- Boolean complete since supports Boolean logic

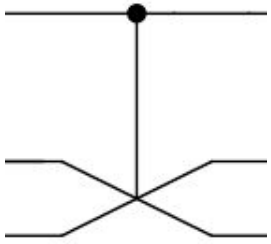
Toffoli Gate
CCNOT

NOT(x)=Toffoli'(1,1,x)
AND(a,b)=Toffoli'(a,b,0)
OR(a,b)=NOT(AND(NOT(a),NOT(b))



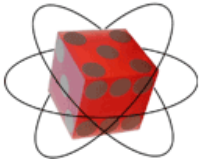
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Fredkin Gate
CSWAP



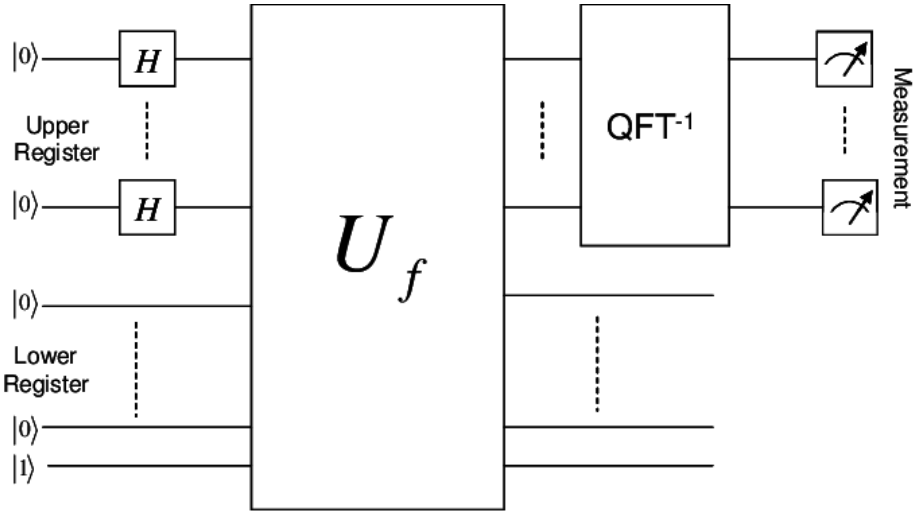
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

1994 Peter Shor's algorithm



Shor's algorithm is a quantum algorithm:

- Uses all 2^q simultaneous states to solve problem (QFT)
- Efficiently solves factoring, impossible by classical computers
- Killer application for Quantum Computers
- Defined new complexity class: Quantum Polynomial time

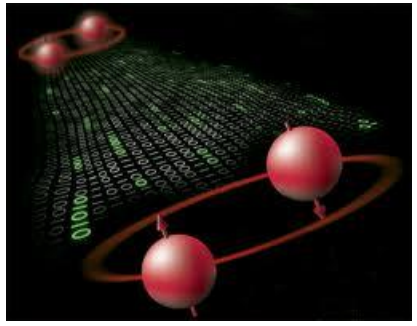


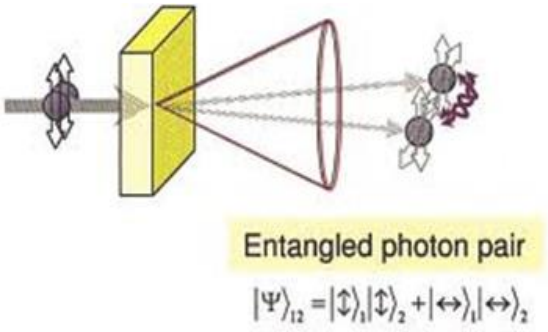
Spurred the development of quantum computing, quantum encryption technology and other quantum algorithms.

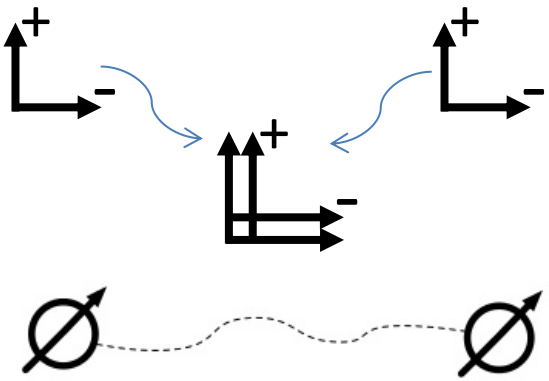
Ebits: Entangled Qubits

Entanglement is a quantum property:

- Multiple things (2 Qubits) acting as one
- Contains *inseparable* quantum states
- Non-locality due to >3 dimensions
- Einstein's "Spooky action at a distance"
- EPR and Bell/Magic states/operators are well defined







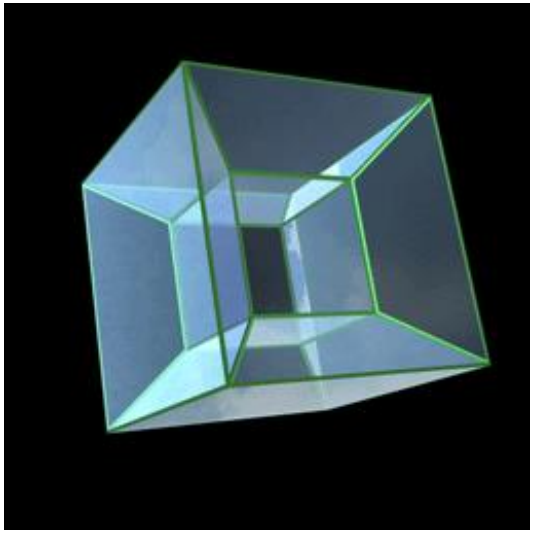
$$\Phi^{\pm} = |00\rangle \pm |11\rangle$$

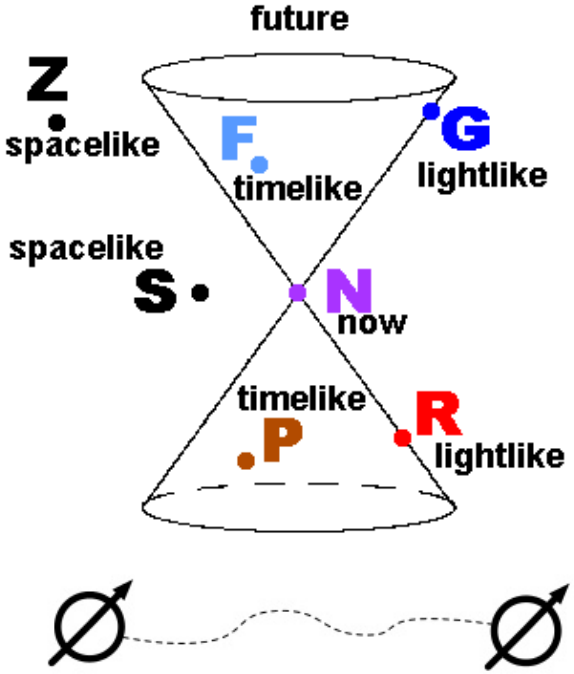
$$\Psi^{\pm} = |01\rangle \pm |10\rangle$$

Entanglement is Space-like

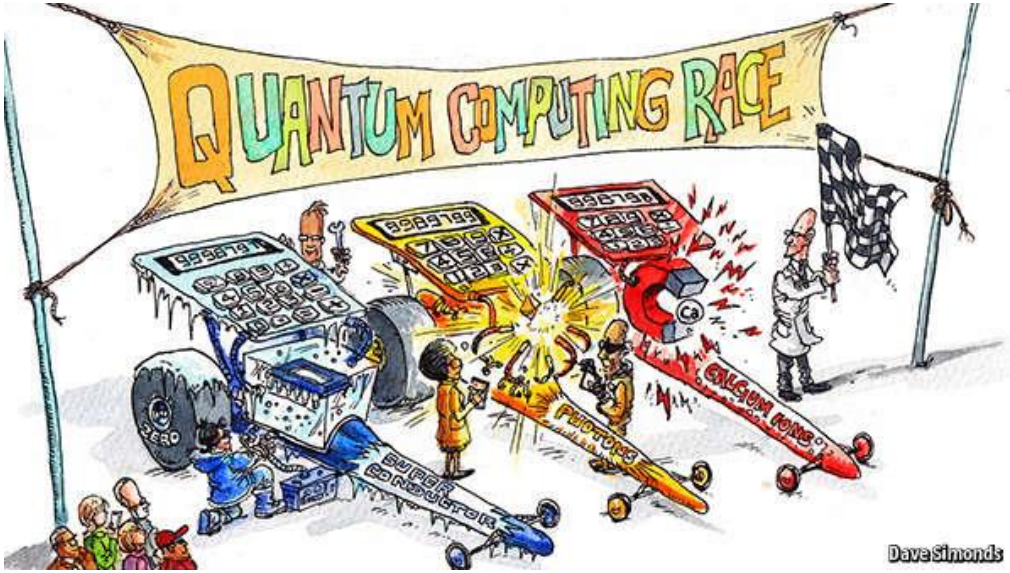
Non-local connection due to 4 dimensional states

- Every ebit contains 4 private dimensions (beyond 3d+1t)
- Self consistency even though space-like states
- Ebits useful for secure communication Quantum Key Distribution
- My research shows space-time itself is entangled (tauquernions)
- My research shows dark-matter/energy is entangled





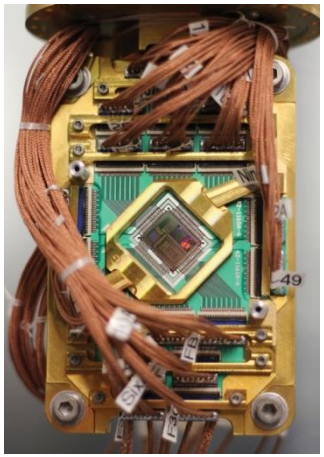
Quantum Supremacy



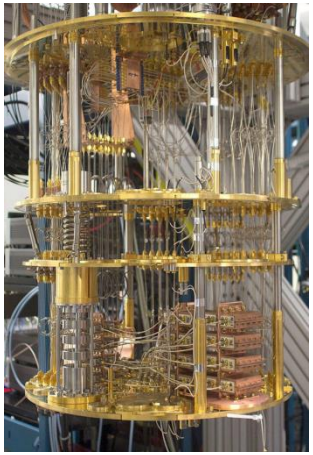
A universal quantum computer >50 Qubits will quickly solve problems no classical computer can solve!!

Killer app is Shor's algorithm.

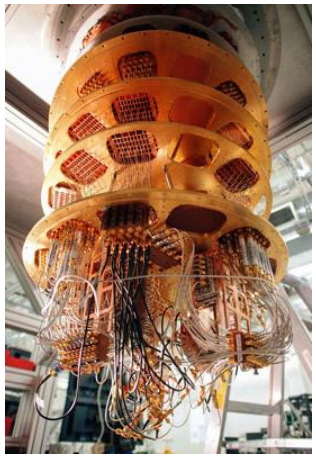
D-Wave



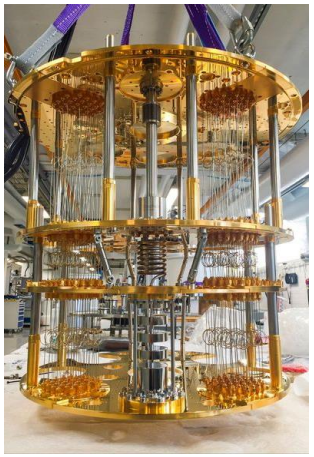
IBM



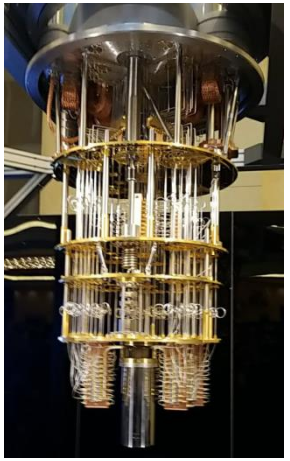
Google



Microsoft



Intel



Investments in Quantum Computing

Billions of investment dollars are being spent and patents world wide by countries, governments, organizations, universities, companies and investment companies.

Private Quantum Computing Companies

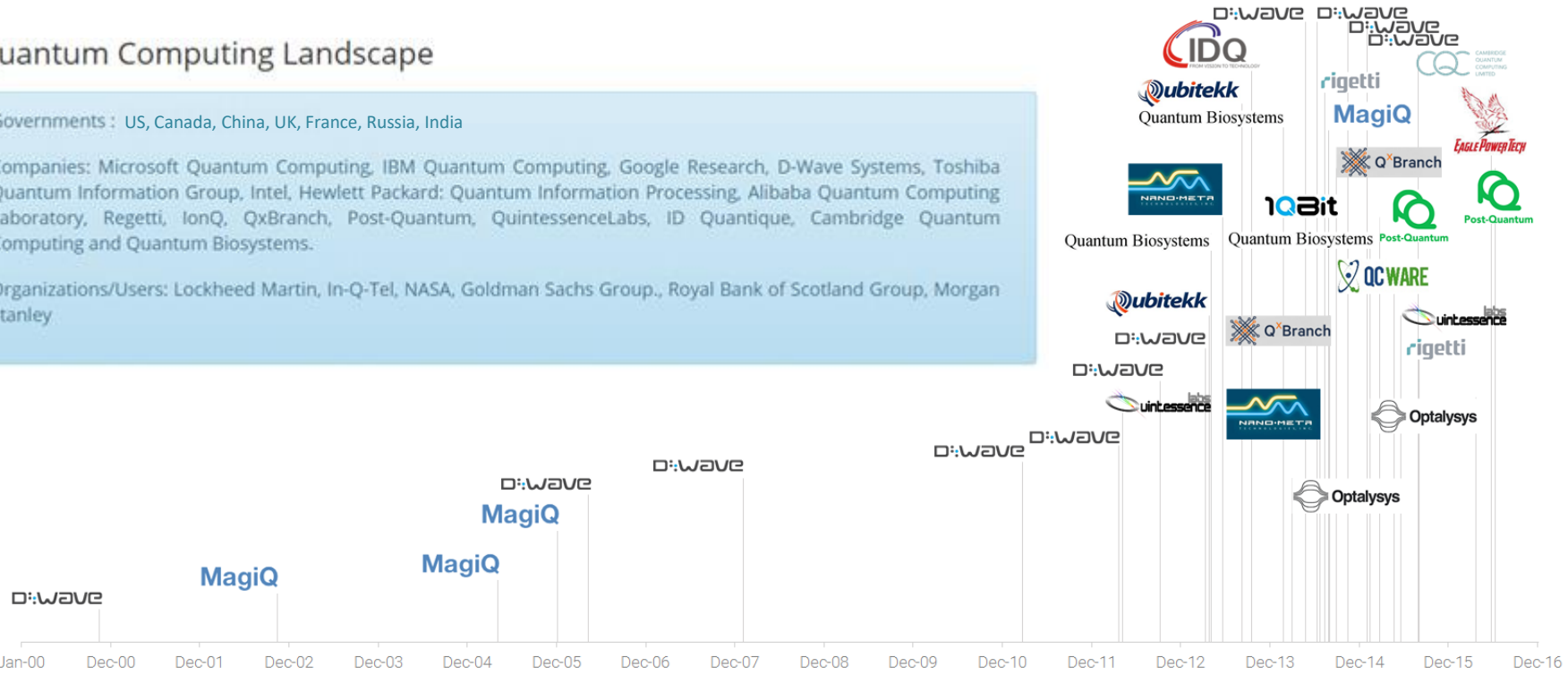
A TIMELINE OF EQUITY FUNDING(S) 2000-2016 YTD (9/6/2016)

Quantum Computing Landscape

Governments : US, Canada, China, UK, France, Russia, India

Companies: Microsoft Quantum Computing, IBM Quantum Computing, Google Research, D-Wave Systems, Toshiba Quantum Information Group, Intel, Hewlett Packard: Quantum Information Processing, Alibaba Quantum Computing Laboratory, Regetti, IonQ, QxBranch, Post-Quantum, QuintessenceLabs, ID Quantique, Cambridge Quantum Computing and Quantum Biosystems.

Organizations/Users: Lockheed Martin, In-Q-Tel, NASA, Goldman Sachs Group., Royal Bank of Scotland Group, Morgan Stanley



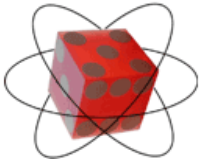
CBINSIGHTS

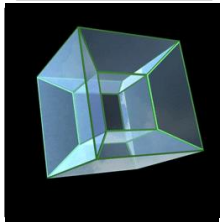
Quantum and Neural Computing

Both quantum and neural computing uses hyperdimensional math models

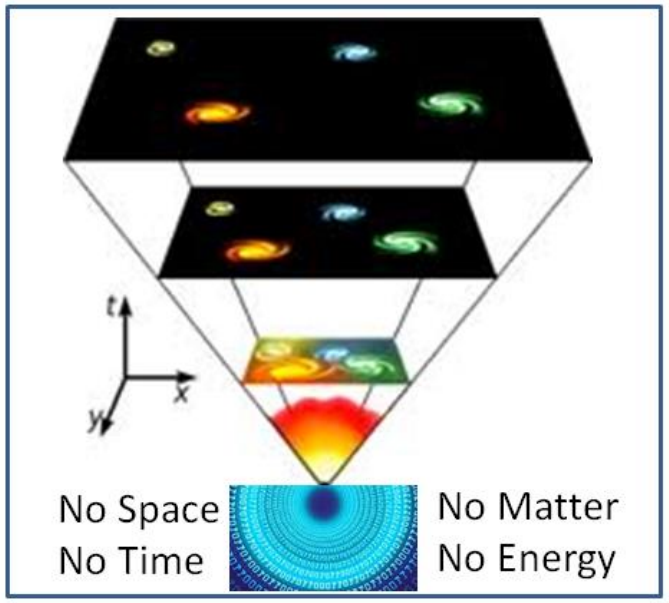
Company	Qubits	Quantum Computing	AI Computing Technology
IBM	50 qubits	Longest Researcher - IBM Q	Deep Blue & IBM Watson
Google	72 qubits	D-Wave and Bristlecone chip	TensorFlow & AlphaGo Chip
Intel	49 qubits	Tangle-Lake chip	neuromorphic chip “Loihi”
Microsoft	unknown	Topological qubits (anyons)	FPGA computing and Augmented Reality
D-Wave	2000 qubits	Adiabatic Computing	Optimization algorithms
many		Computers & Communications	deep learning neural nets

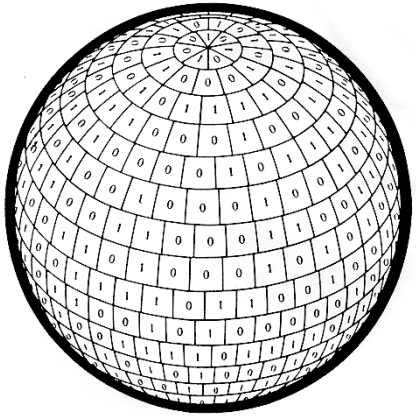
Universe is qu-simulation from proto-bits



Space	Dims	Vectors
G_4		18.9 bits
G_3		7.29 bits
G_2		2.17 bits
G_1		0.58 bits

complexity



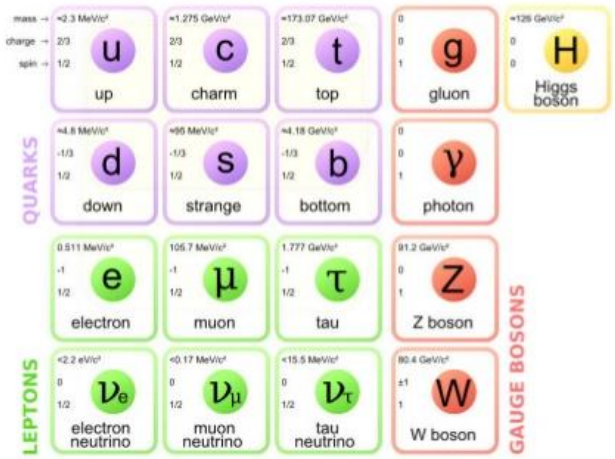


Singularity in big-bit-bang & black holes is due to near infinite # of dimensions!

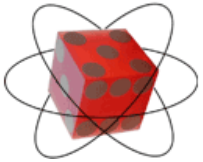
Conclusions: Quantum is fundamental

Following emerges from quantum information **bits**:

- Quantum probability amplitude waves
- Quantum **superposition** (**qubits** and probabilities)
- Quantum **entanglement** (**ebits** and "spooky action")
- All strange quantum physics principles
- Spacetime, zero point energy and quantum foam
- All particles (fermions=mass) and energy (bosons=massless)
- All energy/mass/space/time of classical/relativistic world
- All sequential/parallel computing (time-like & light-like)
- All space-like quantum speedup
- Most likely human intelligence also
- Apply quantum concepts to software
  - Idempotent operators $(I*I)=I$
  - Reversible operators
  - Mutual exclusion vs superposition
  - Superposition of states (i.e. Done/Cancel)
  - Wholistic consistency of states



Quantum computing is so fundamental since exposes the infinite quantum bit reality of the entire universe.



Question and Answers