

Open FinTech Forum

AI, Blockchain & Kubernetes on Wall Street

The Reality of Quantum Computing

Now and in the Future

- @qant

Christoph Lameter
<cl@linux.com>
Jump Trading LLC

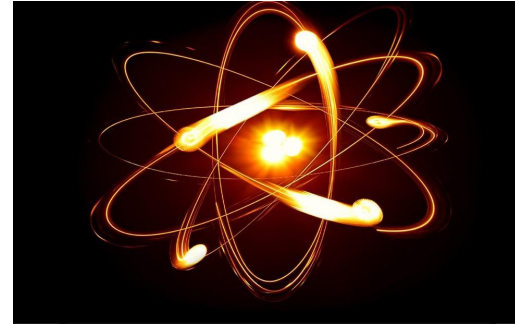


- But the current state: Wild West
 - Funding: Governments see a chance to win a tech race in a new field. Billions of dollars are being spent
 - Confusion: Quantum Theory is counterintuitive. People dream of revolutionary solutions that are mostly based on missing some of the basics of QM.

A survey of existing approaches to quantum computing and their usefulness to current issues in the financial industry and an outlook to the future giving an estimate as to when competitive approaches to help solve issues may emerge from this direction of investigation.

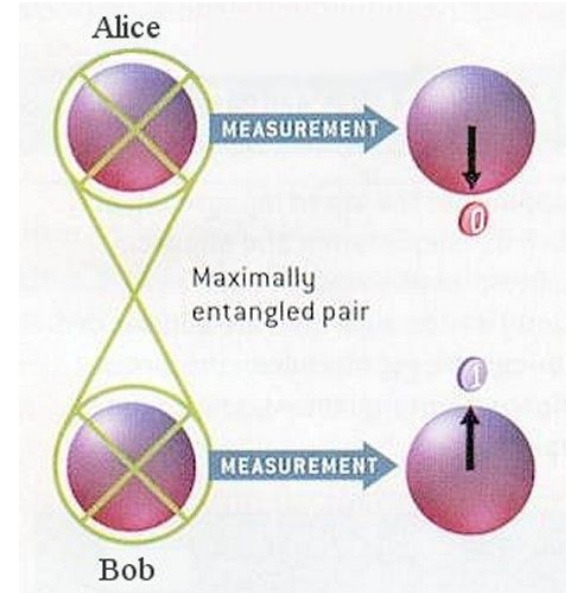


- ❑ Basic law at the lowest level. Everything is governed by QM.
- ❑ Schroedingers Wave function describes potentials of events
- ❑ Outcomes happen *measurements*
- ❑ von Neumann put down the basic theoretical work on Computer Science after publishing a book on the basics of QM.
- ❑ Numerous strong opinions on QM by Scientists



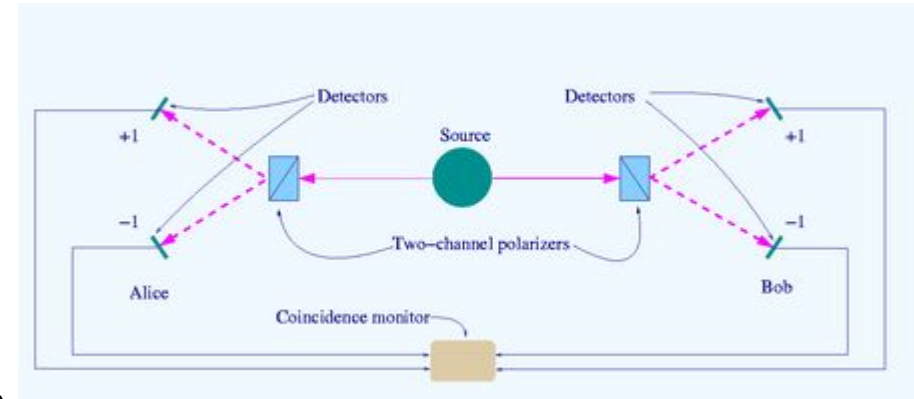
Quantum Mechanics: EPR Paradox

- ❖ Two quantum entangled particles in a “superposition”. One quantum system.
- ❖ Measurement of the spin on one determines the spin at the other after particles have separated.
- ❖ Spooky action at a distance?
- ❖ Communication faster than light?



Quantum Mechanics: Bells Inequality

- Mixed vs Entangled state changes statistics.
- If we create two entangled particles we can verify that the quantum system is not leaking information (which would be a measurement)
- John Bell: Proof that quantum mechanics is wrong was possible!
- This is the basic of *quantum secured communication*



Warning: Scientist utterly frustrated with QM

- Einstein: Unreasonable concept of Reality
- Schroedinger: Suggest the wave does not represent probabilities.
- Bell: We can prove that QM is wrong
- Bohm: Pilot wave makes QM deterministic
- Hawking: GUT will explain indeterminacies.
They ultimately do not matter since they are restricted to a very low level.



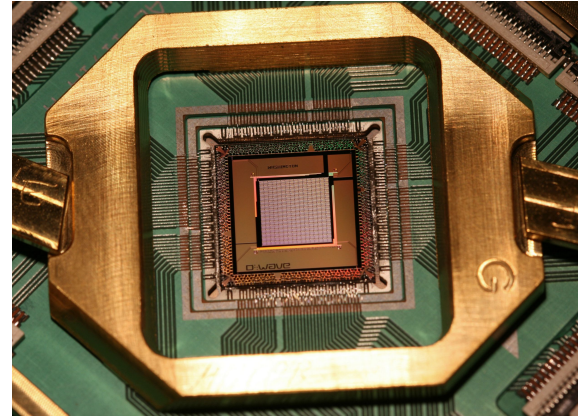
(use of QM phenomena for crypto)

- Single entangled system that provides detection of someone listening in.
- Securing keys against quantum computing approaches to break them by increasing the difficulties to break them using classical methods.
- Using Quantum mechanical systems to create new type of keys that are not breakable anymore with classic approaches even if more computational power becomes available.



Things called a “Quantum Computer”

- Miniaturized experiment in chip form to explore quantum effects.
- Quantum Cryptography
- D-WAVE Quantum Computer
- Quantum gates/Qubit based systems
- Experimental Computers in Labs and Research facilities
 - ◆ Photon based on chip technology. On chip mirrors.
 - ◆ Superconducting quantum computing



Shor's algorithm

- A Quantum factorization algorithm (quantum fourier transformation) that is probability based. Solutions must be verified classically.
- Classic algorithms are exponential, quantum based ones are polynomial.
- Points to the possibility to develop quantum algorithms that can solve time intensive algorithms faster which could be an advantage for a company doing so in financial services. However, that may not be feasible given the effort that Shor's algorithm required. Maybe when other quantum algorithms become workable.



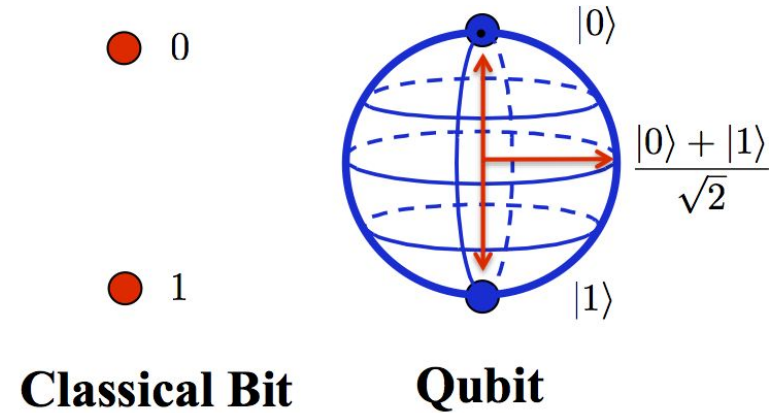
D-Wave Quantum Computer

- First commercially available Quantum computer
- Origins not in quantum informatics but condensed matter physics.
- D-Wave 2000Q has 2048 Qubits.
- Controversy if this is a real quantum computer or not.
- Divergent claims of performance increases and counterclaims of doing the same performance on a classical computer.



Qubit: Maybe 0 and maybe 1

- Quantum Gates
- Reversibility
- Decoherence
- Scaling problems:
Exponential relations
- Qubit max is Google: 72 bit, IBM: 50 Intel:
49 D-Wave: 2048

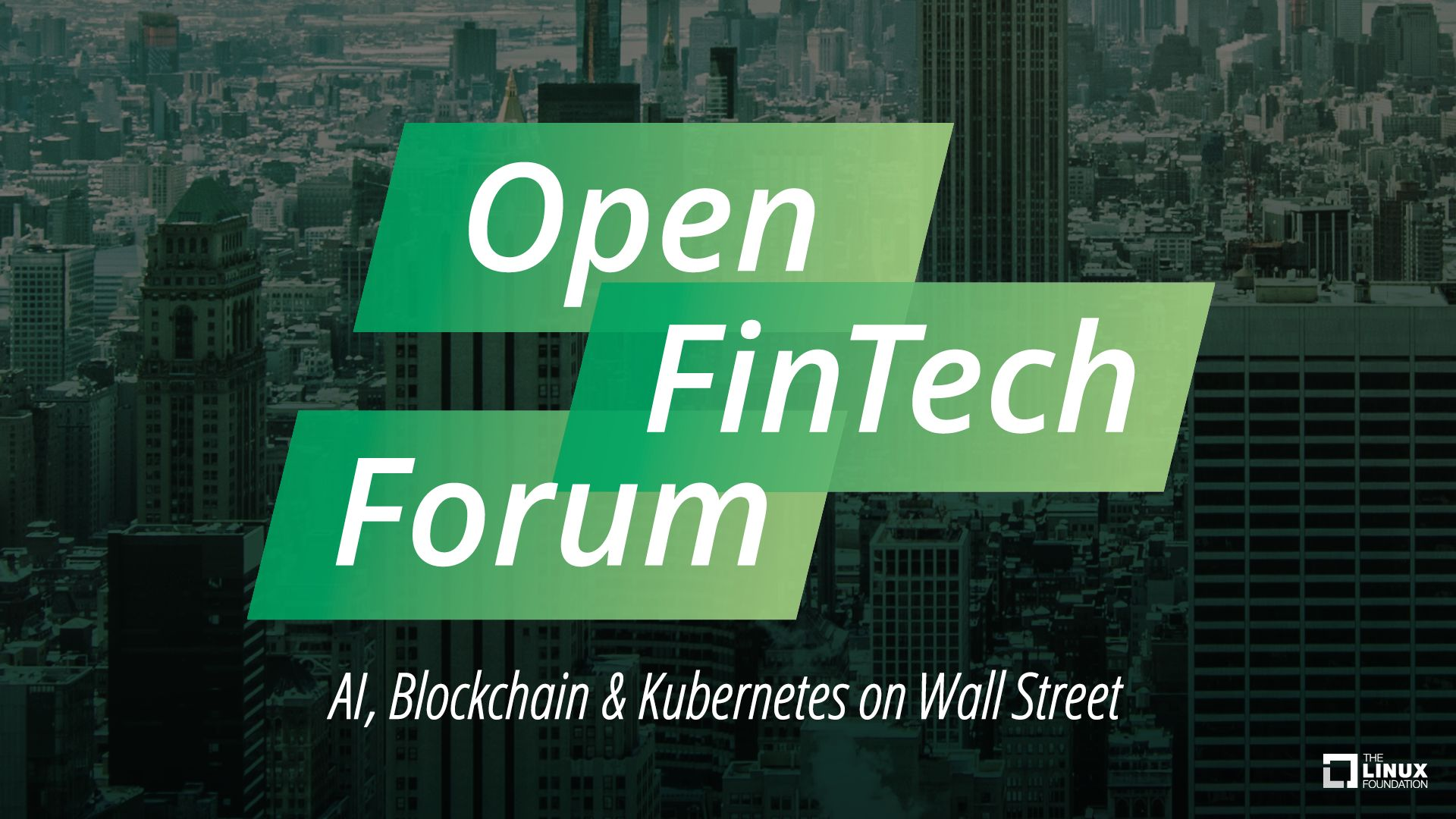


- Cryptography. Key breaking.
- Solving complex mathematical problems.
- Machine learning
- Health
- HPC areas
- Searching through large data sets (?)

What is useful for Financial Technology?

- Generally these approaches improve High performance computing which is key to various use cases.
- Quantum cryptography is likely going to be mandatory to secure communication in the future. Security is an ever increasing set of issues.
- Qubits and Quantum Operator point to a future in which we can design algorithms using quantum concepts.
- Currently quantum computing is a pretty confusing field that would need to stabilize before it can be useful in the financial technology sector.





Open FinTech Forum

AI, Blockchain & Kubernetes on Wall Street