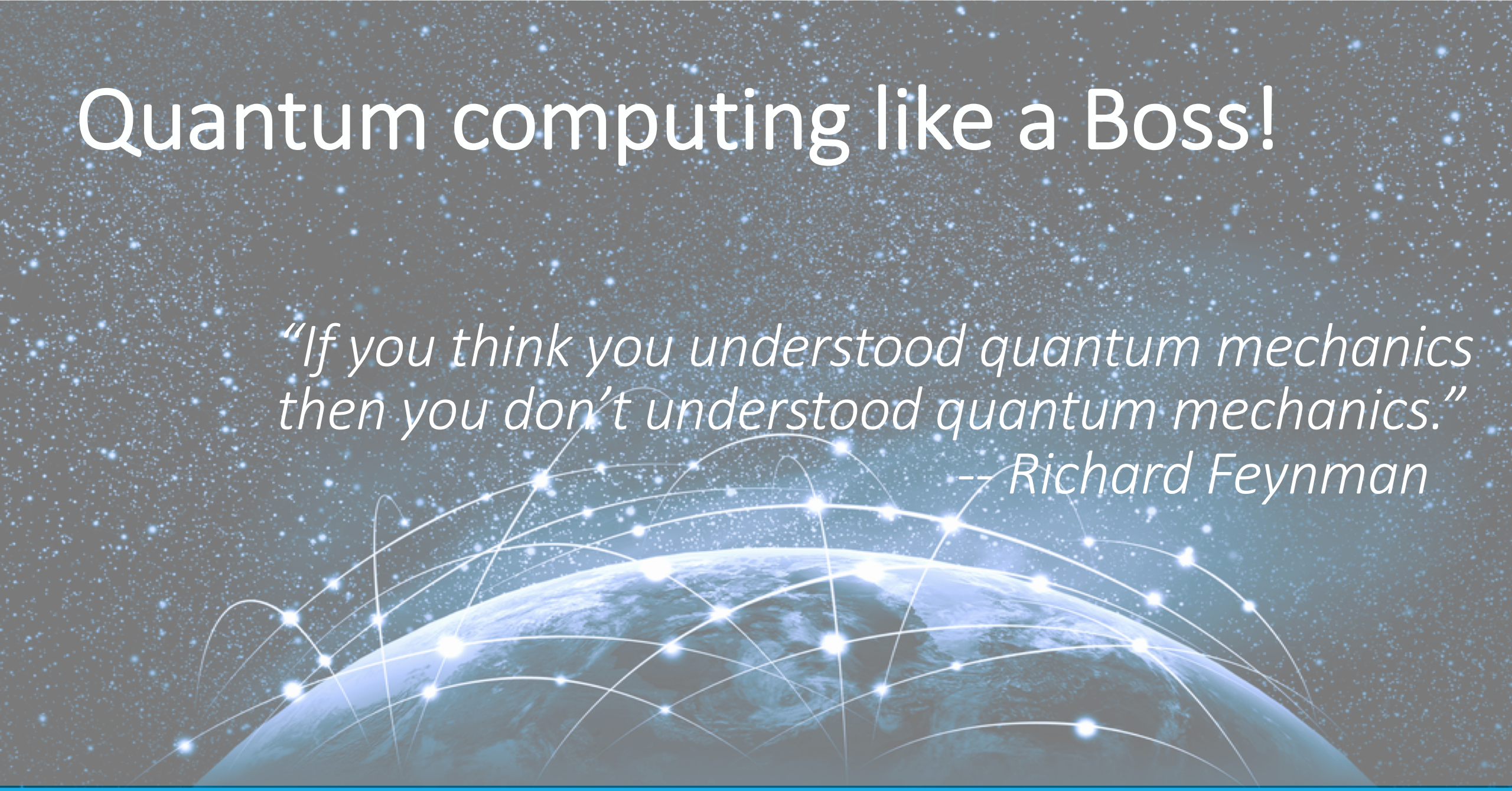
Quantum computing like a Boss!



"If you think you understood quantum mechanics then you don't understood quantum mechanics."

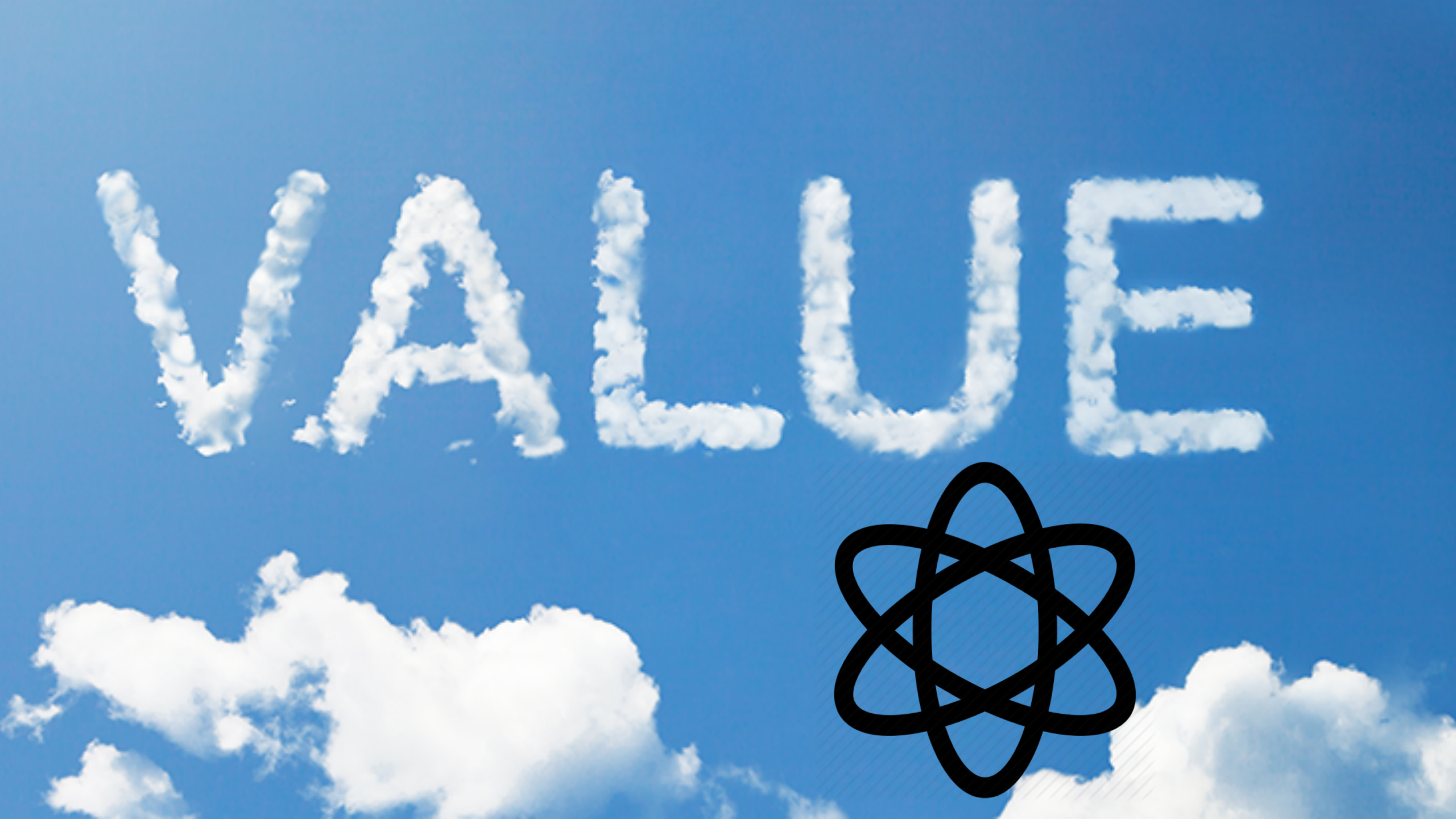
-- Richard Feynman

by Riccardo Terrell - @trikace

Introduction - Riccardo Terrell

- Originally from Italy, currently - Living/working in Charlotte NC
- +/- 20 years in professional programming
  - C++/VB → Java → .Net C# → Haskell → C# & F# → Scala
- Author of the book “Concurrency in .NET” – Manning Publisher
- *Polyglot programmer - believes in the art of finding the right tool for the job*
- *Organizer of the DC Pure Functional User Group*

@trikace *www.rickyterrell.com* *tericcardo@gmail.com*


VALUE

“Quantum computing could solve problems that would take today's computers eons in the time it takes to grab a cup of coffee.”

https://developer.microsoft.com/en-us/events/build/content/the-quantum-revolution-with-q

Von Neuman, Turing Machine and Quantum Computing

Quantum Mechanical Computers

By Richard P. Feynman

Introduction

This work is a part of an effort to analyze the physical limitations of computers due to the laws of physics. For example, Bennett[1] has made a careful study of the free energy

such. We see we really have two more logical primitives, FAN OUT when two wires are connected to one, and EXCHANGE, when wires are crossed. In the usual computer the NOT and NAND primitives are implemented by transis-

could be stored in an inductance, or other reactive element.

However, it is apparently very difficult to make inductive elements on silicon wafers with present techniques. Even Nature, in her DNA copying ma-

"All our machines, no matter how fancy and parallel are basically bells and whistles on top of the original Turing machine. There's the classical model, which is the Turing model, and there's the quantum model, and making this transition, jumping from the first to the second, is kind of like getting a peek at the inner workings of the universe, looking behind the screen."

-- Richard Freedman

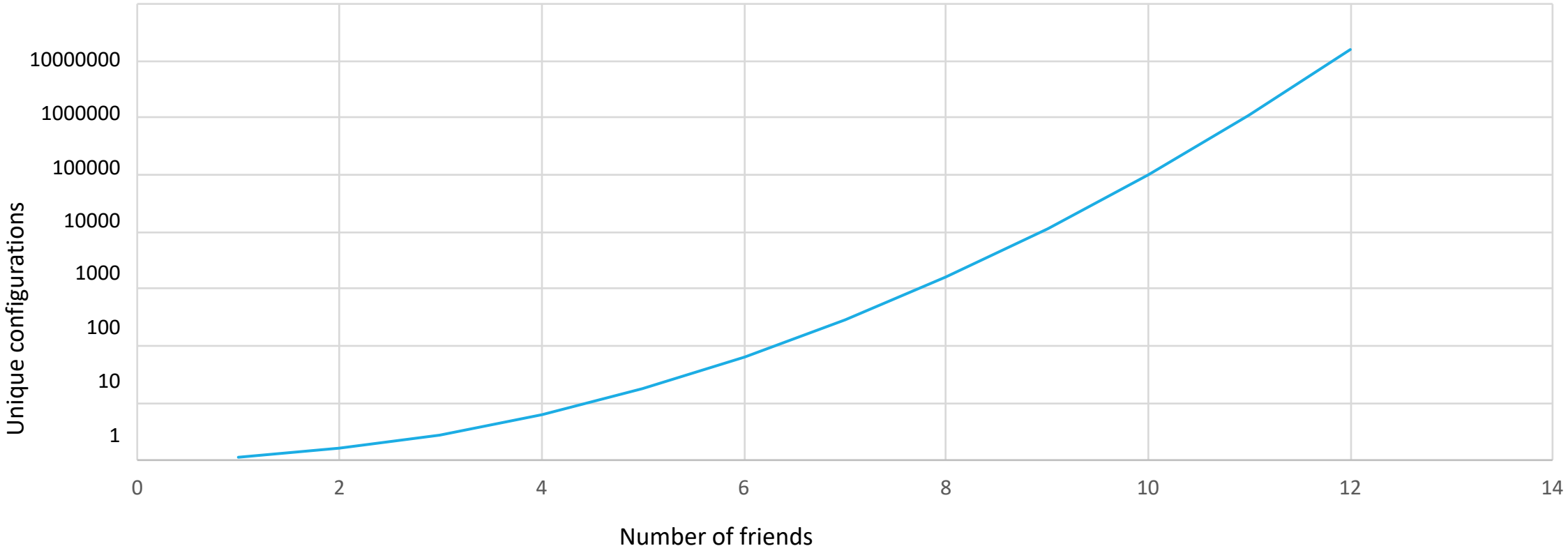
"There's this plane flying through the sky. If you drop a coin from the plane, it still falls – it's not like the laws are different for the plane – it's just that in flying the plane you are controlling those laws of classical physics and thermodynamics to your advantage with things like jet fuel and controls. We understand Newton's laws so well that we can use them to our advantage. This is what we're trying to do with quantum computing."

-- Sankar Das Sarma

https://news.microsoft.com/stories/stationq/

Nature computes using **quantum**

Von Neuman, Turing Machine and Quantum Computing



The problem of breaking RSA Encryption

RSA-2048 Encryption Problem

25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357

The problem of breaking RSA Encryption

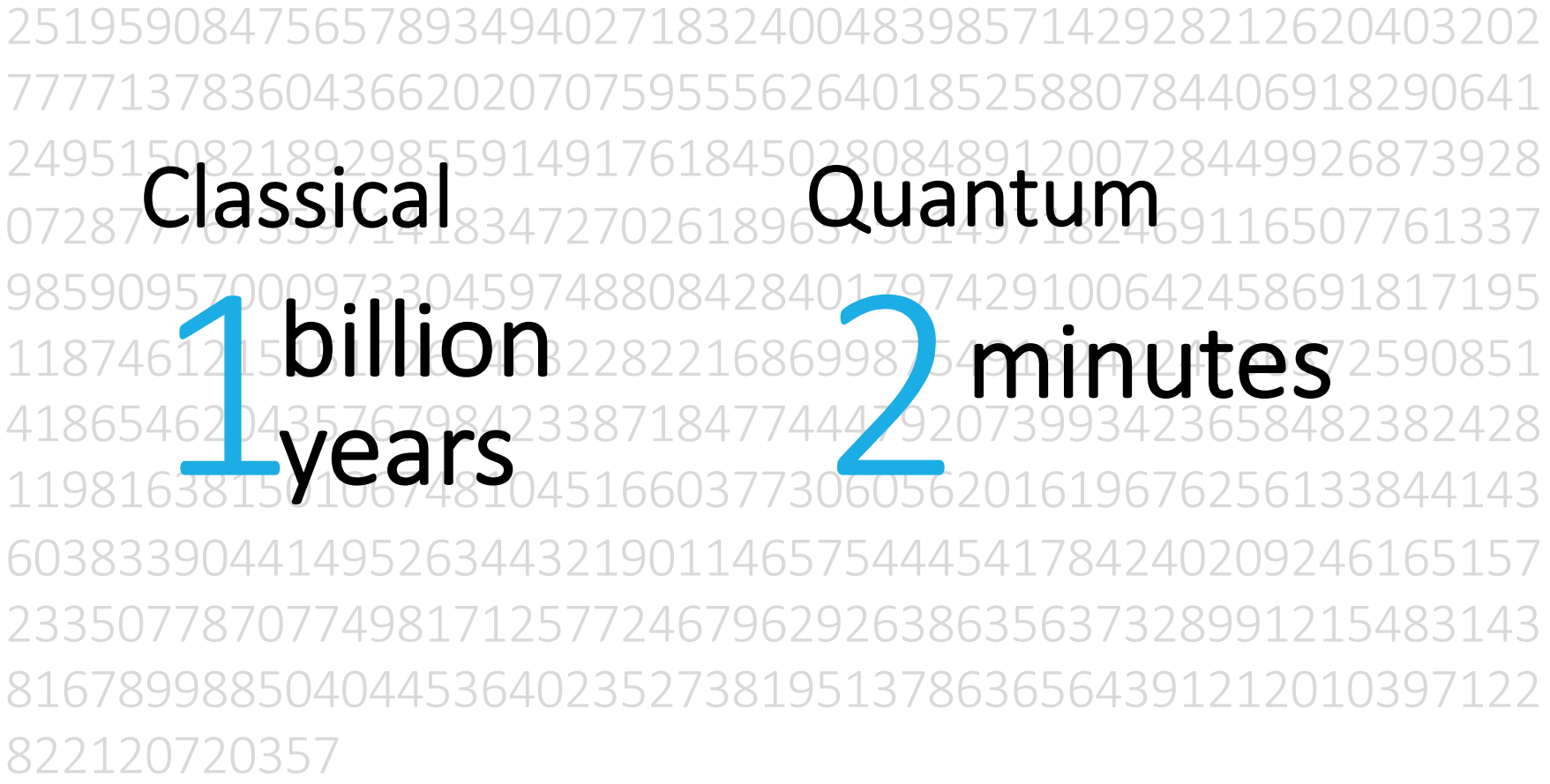
RSA-2048 Encryption Problem

Classical

1 billion years

Quantum

2 minutes

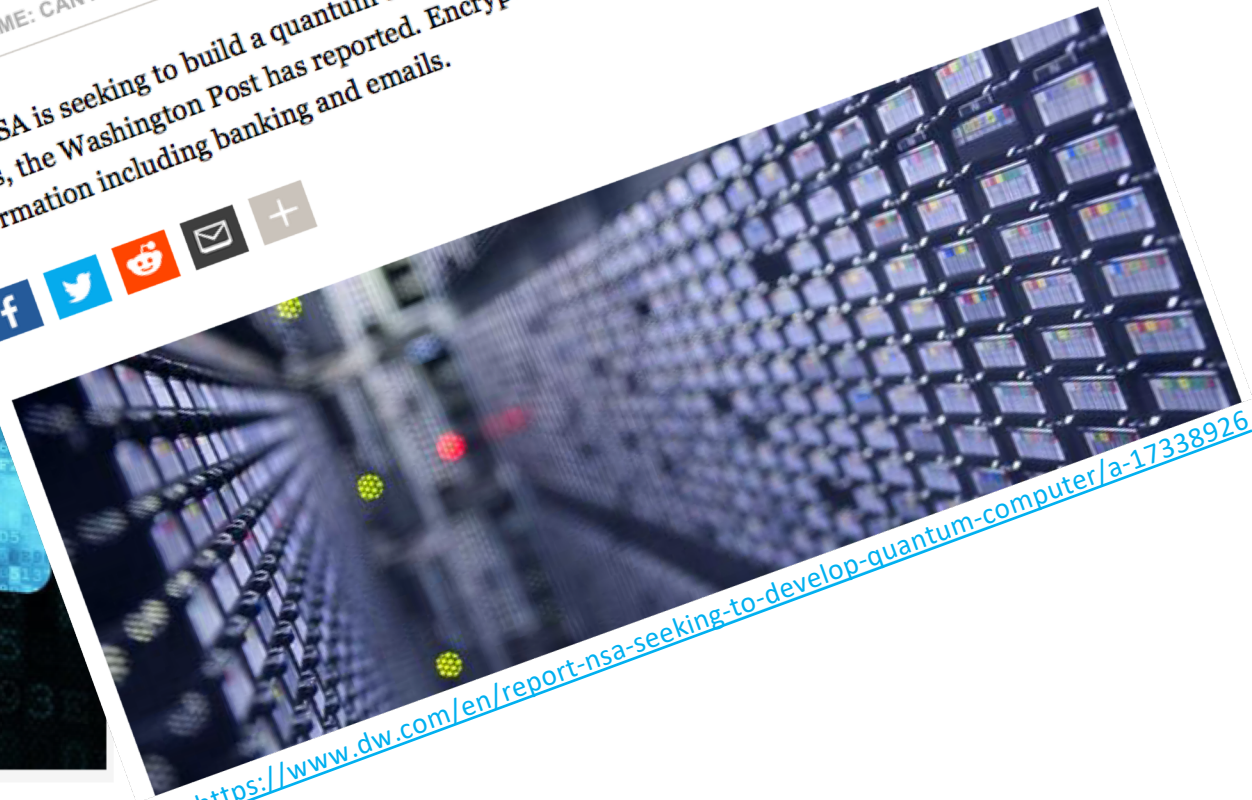


No more secrets!

Report: NSA seeking to develop 'quantum computer'

SPY GAME: CAN ANYONE CONTROL THE NSA?

The NSA is seeking to build a quantum computer capable of breaking most encryption codes, the Washington Post has reported. Encryption is used to protect sensitive information including banking and emails.

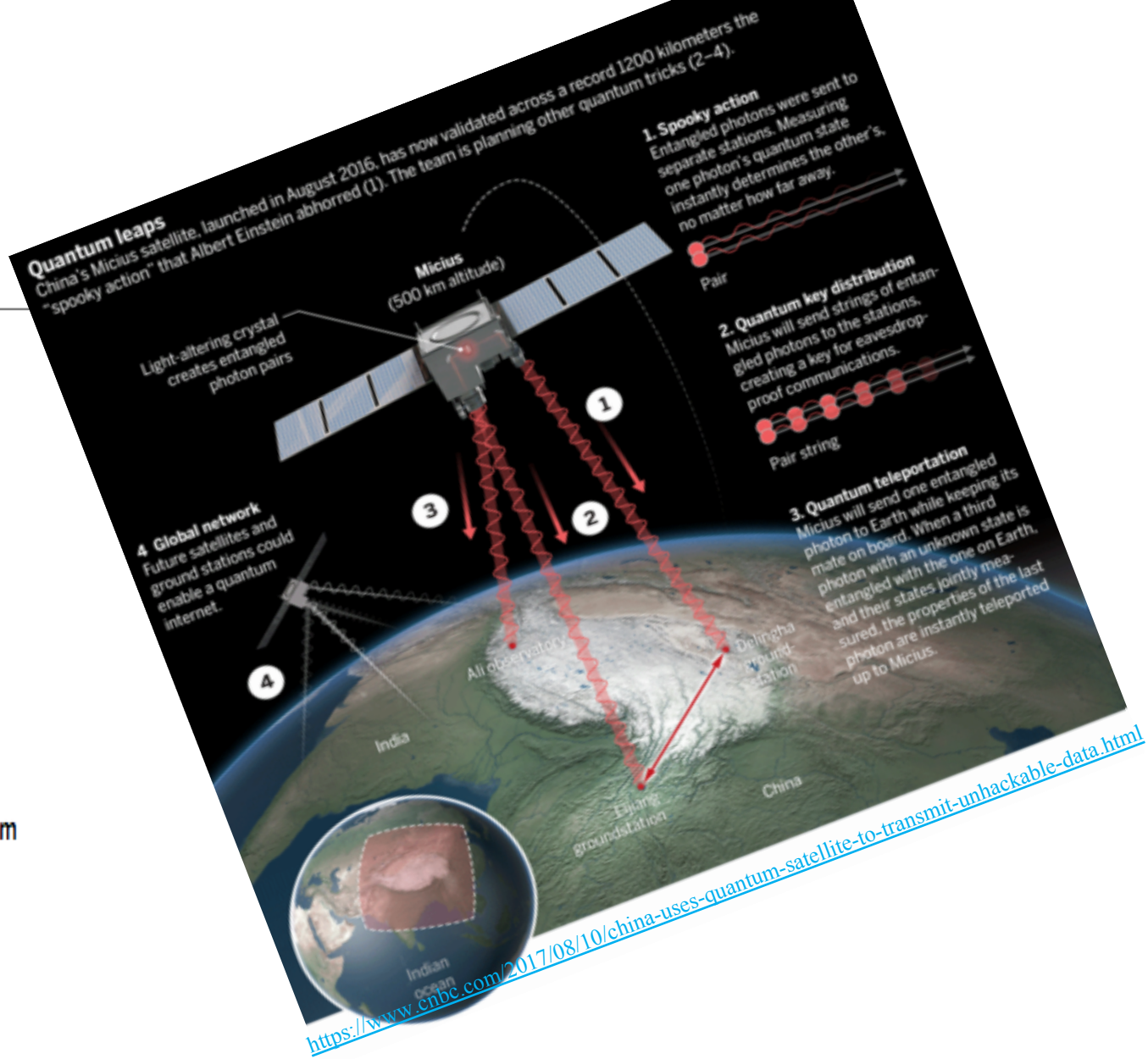


https://www.dw.com/en/report-nsa-seeking-to-develop-quantum-computer/a-17338926

Time to re-think security

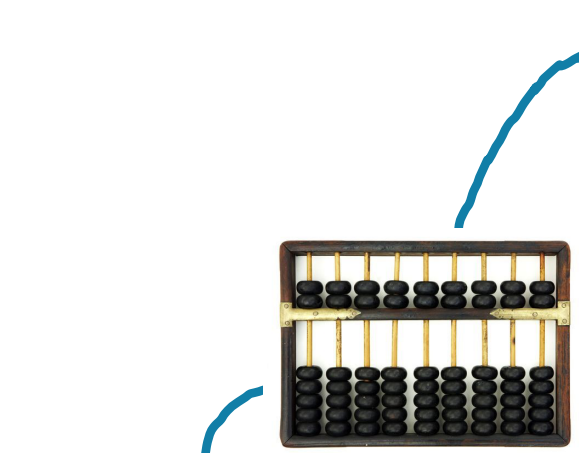
China uses a quantum satellite to transmit potentially unhackable data

- China has demonstrated way to send data over long distances which is potentially unhackable.
- It relies on "quantum cryptography" and a satellite sending data via photons from space to earth.
- The implications could be huge for cybersecurity, making businesses safer, but also making it more difficult for governments to hack into communication.



https://www.cnbc.com/2017/08/10/china-uses-quantum-satellite-to-transmit-unhackable-data.html

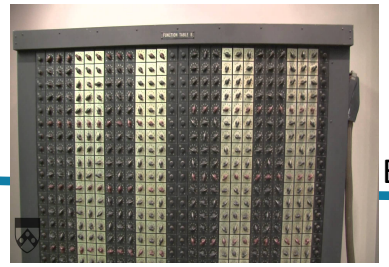
Quantum computing is part of the evolution



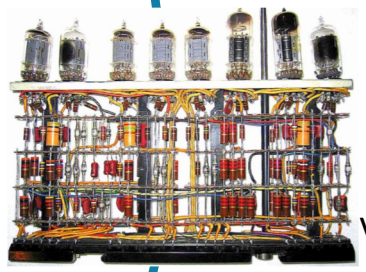
Antikythera
100 BC

Abacus

Z3 programmable
Computer 1943



ENIAC
1946



Vacuum Tube
Computer

Computer
Terminal

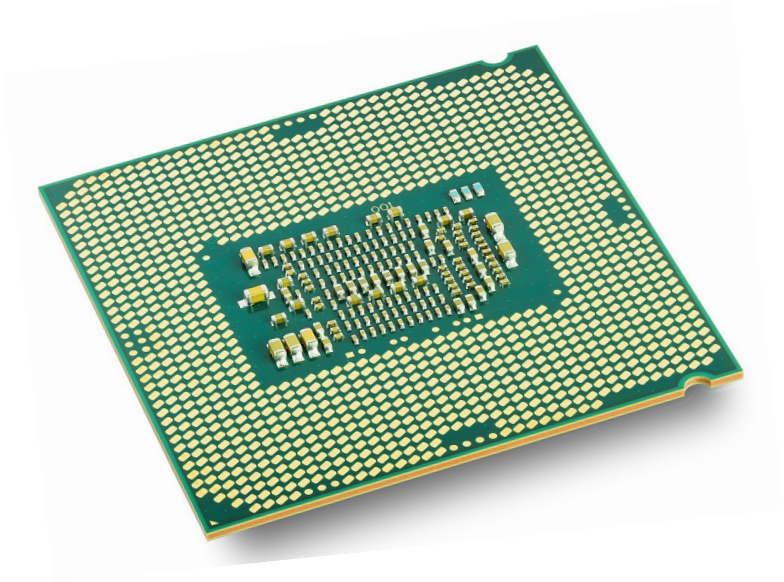
quantum computation started as early as 1982 with the physicist Richard Feynman

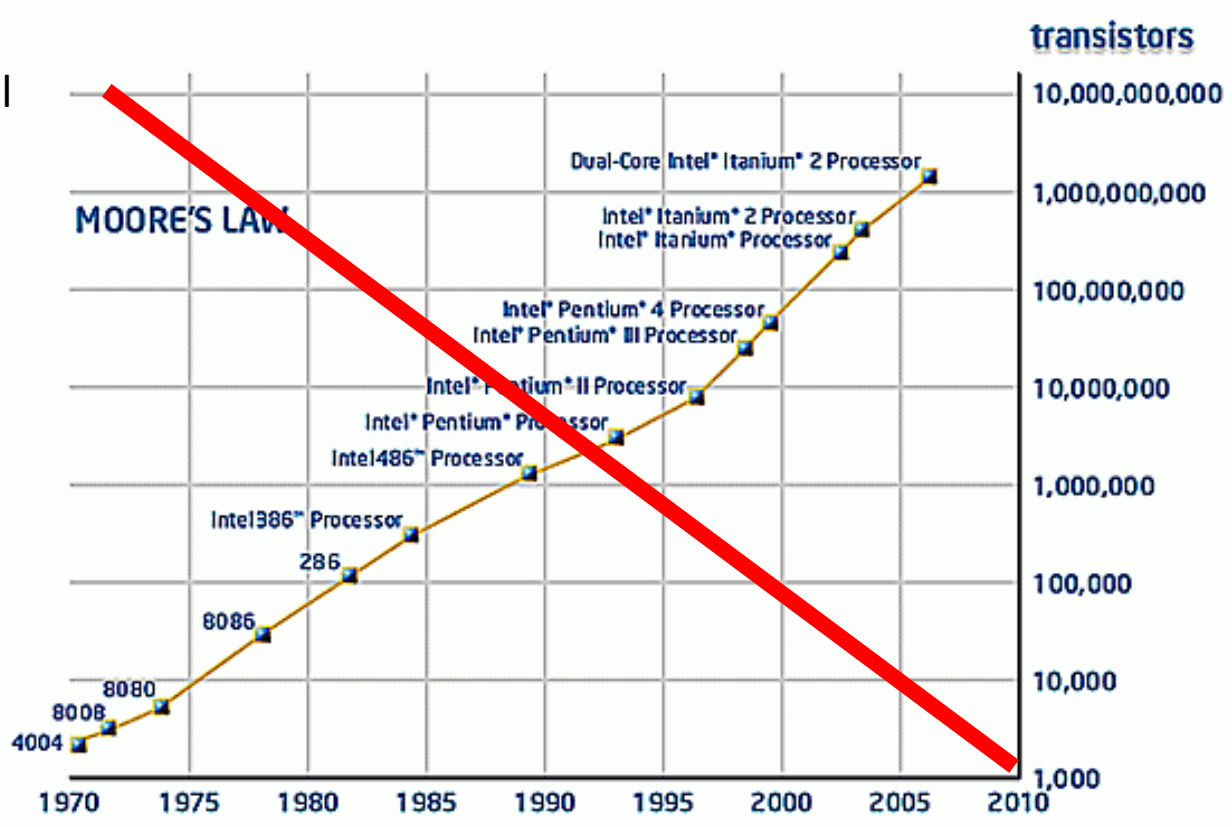
Modern
Computer

xBox

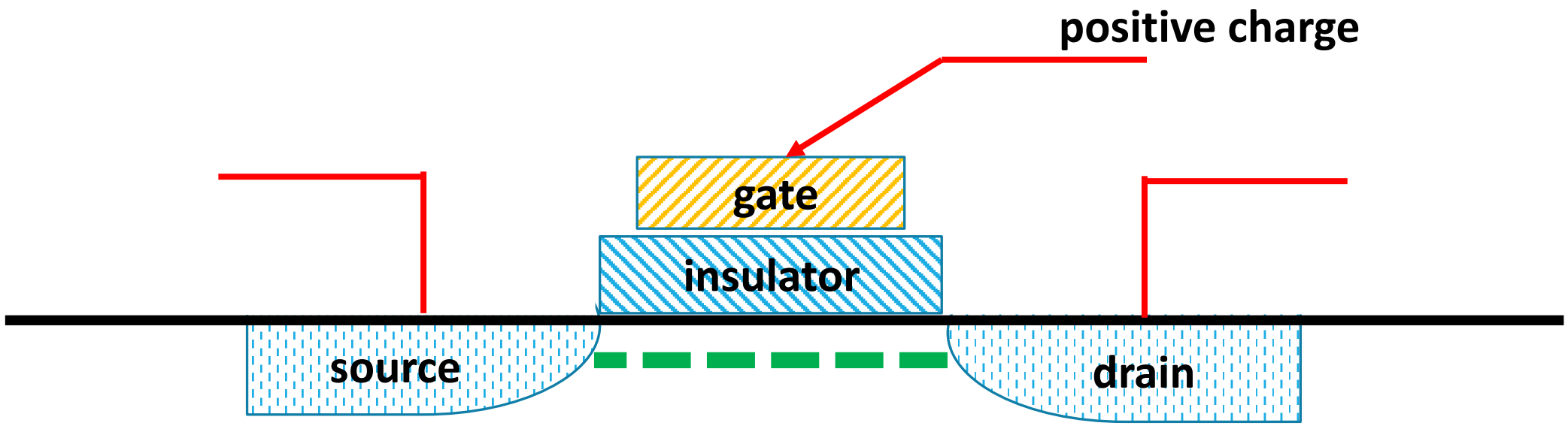
Moore’s law -The classical computer is reaching quantum state

"The number of transistors incorporated in a chip will approximately double every 24 months."
-- Gordon Moore, Intel Co- Founder

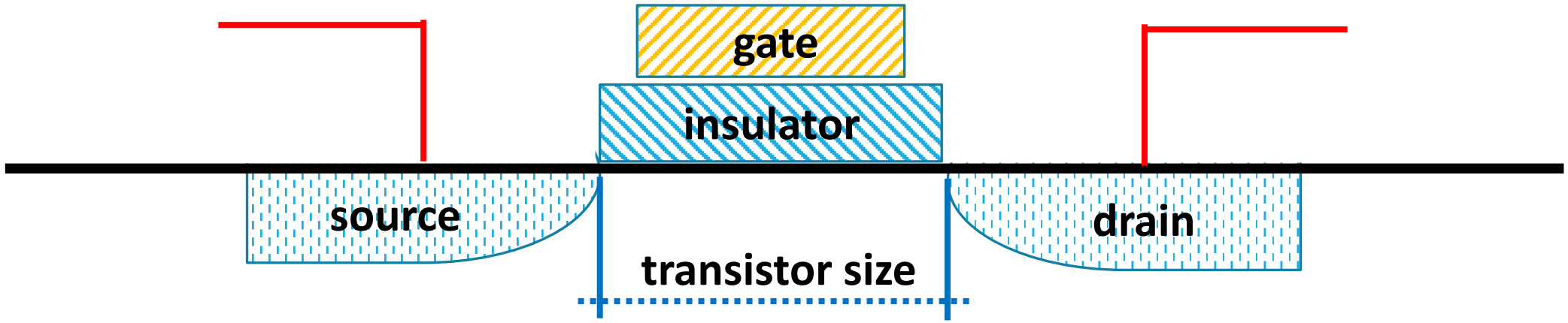




Transistors and the “End of Moore’s Law”

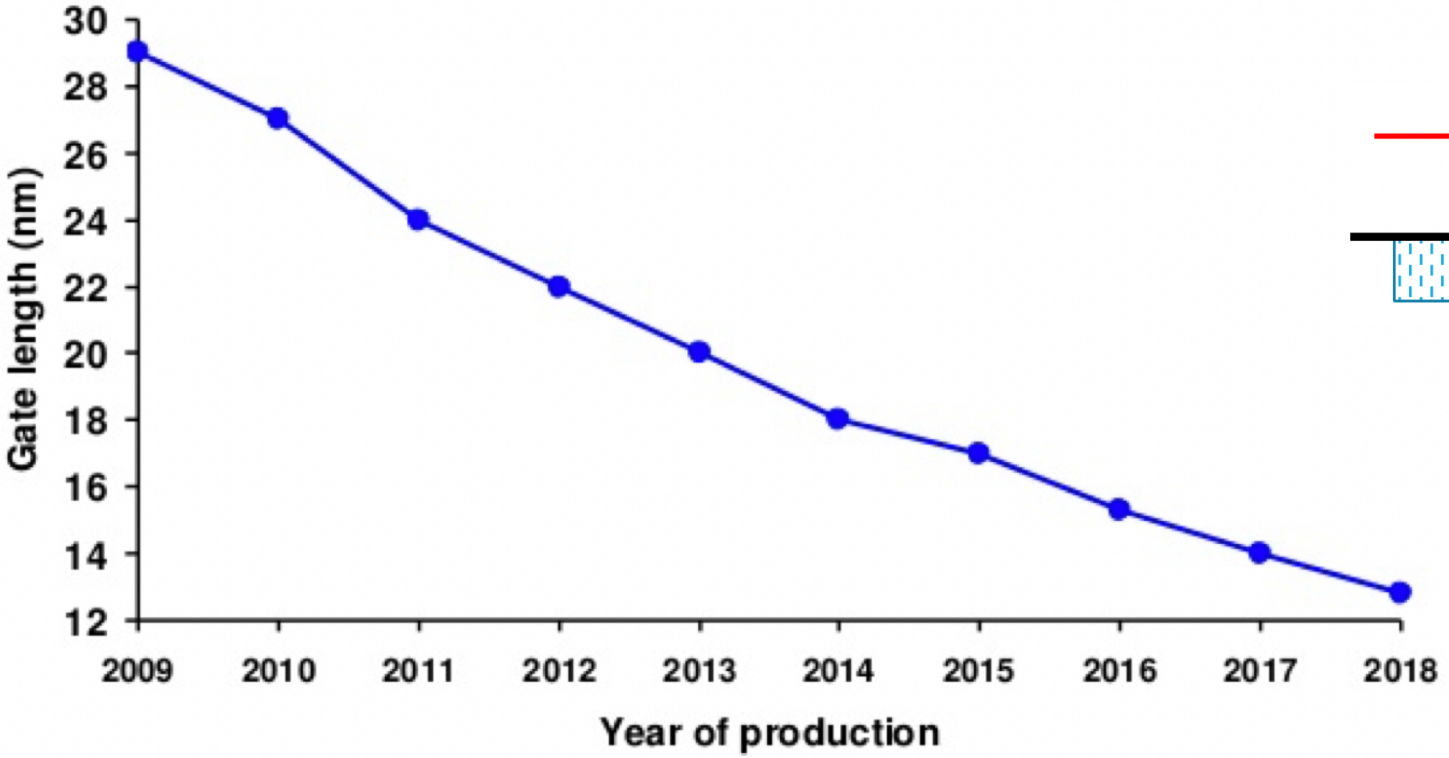


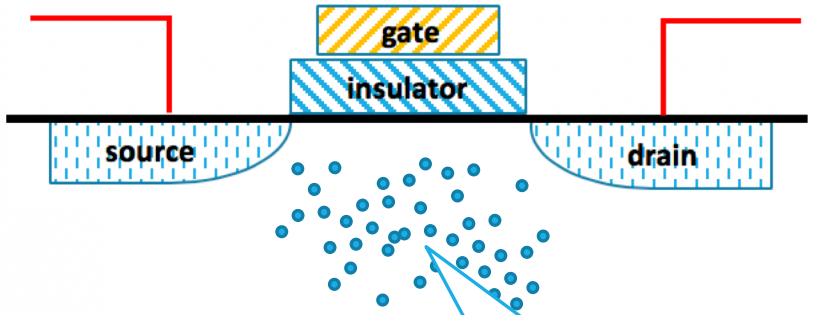
Transistors and the “End of Moore’s Law”



Transistors and the “End of Moore’s Law”

32 nm
22 nm
14 nm
10 nm
7 nm
5 nm
END





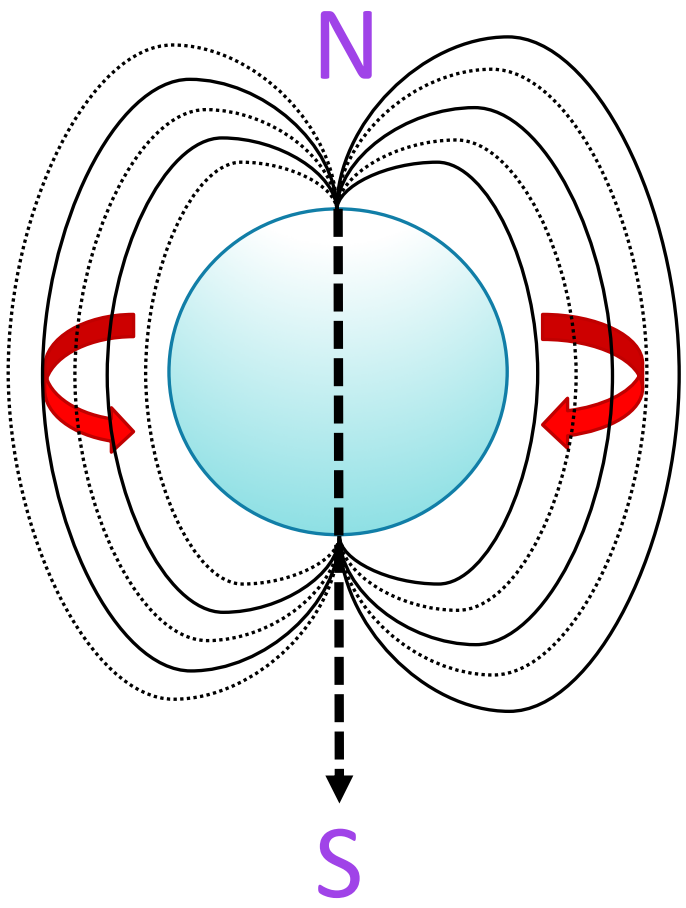
In a 22nm transistors there are about 50 silicon atoms between source and drain

Quantum tunneling

If we cannot avoid
Quantum Mechanics…

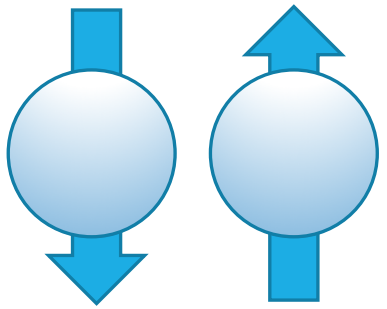
we must use it!

Digital Quantum Computation

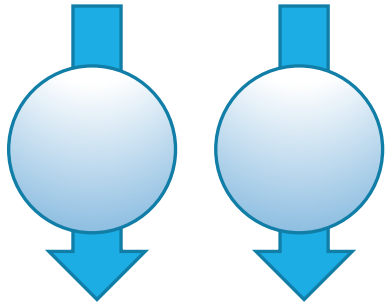


- We can operate on the qubit state by rotations to obtain whichever state we want.
- A bit of data is represented by a single atom that is in one of two states denoted by |0> and |1>
- We cannot know *which* combinations of |0> and |1> are present in an arbitrary state.

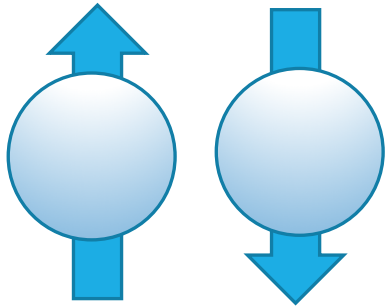
Taking two electrons to make Qubit



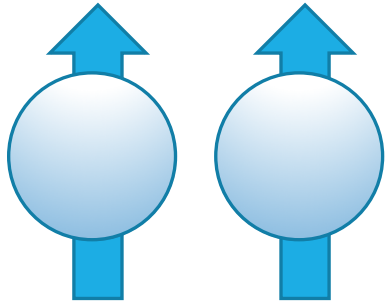
= 10



= 11

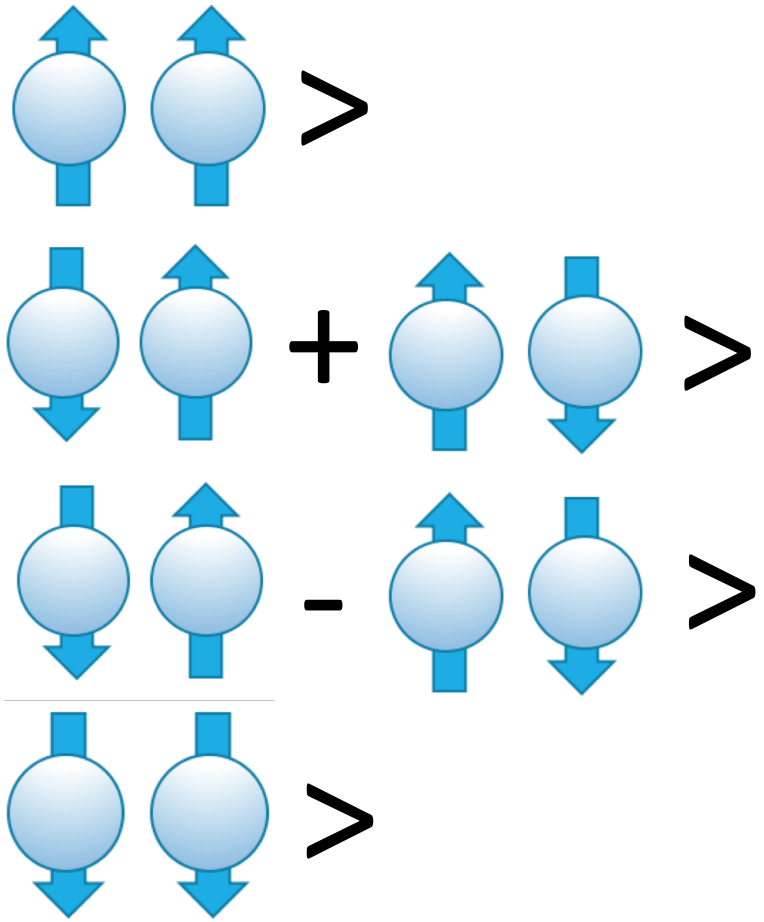


= 01

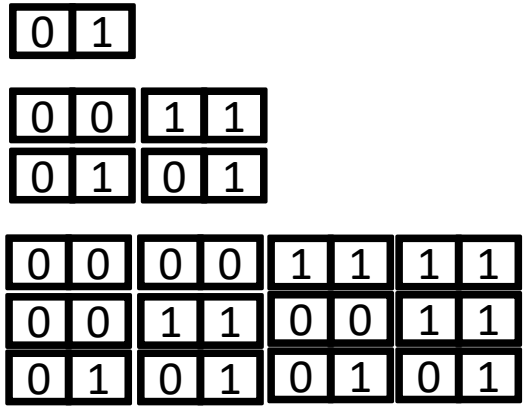


= 00

Taking two electrons to make Qubit



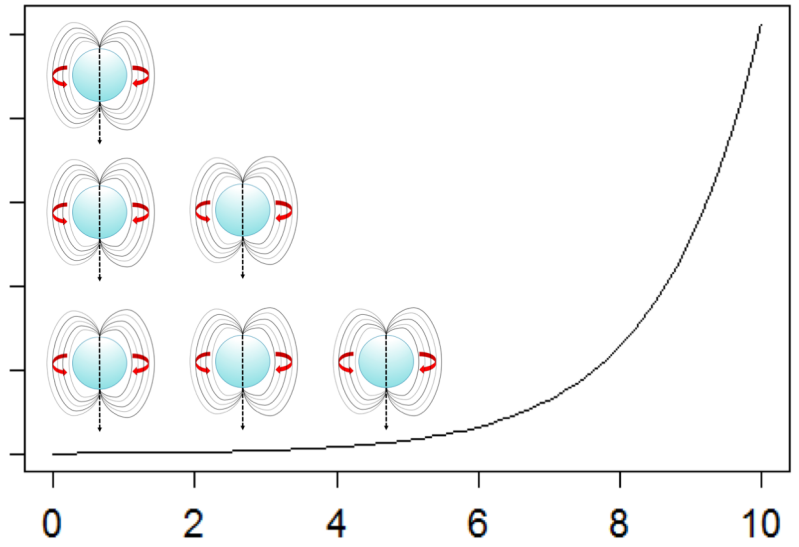
The power of Quantum Computing Exponential Scaling



2^1 → 2

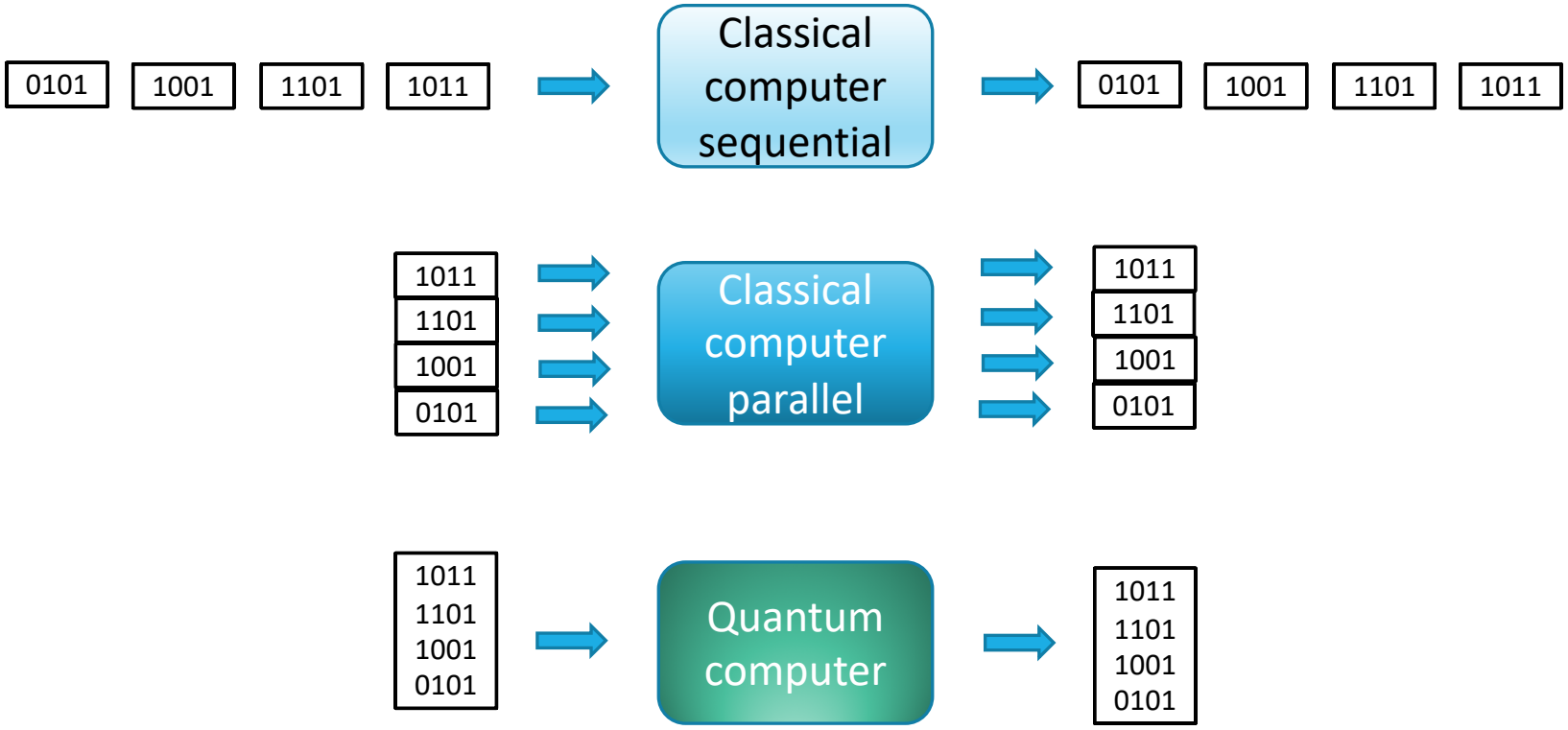
2^2 → 4

2^3 → 8

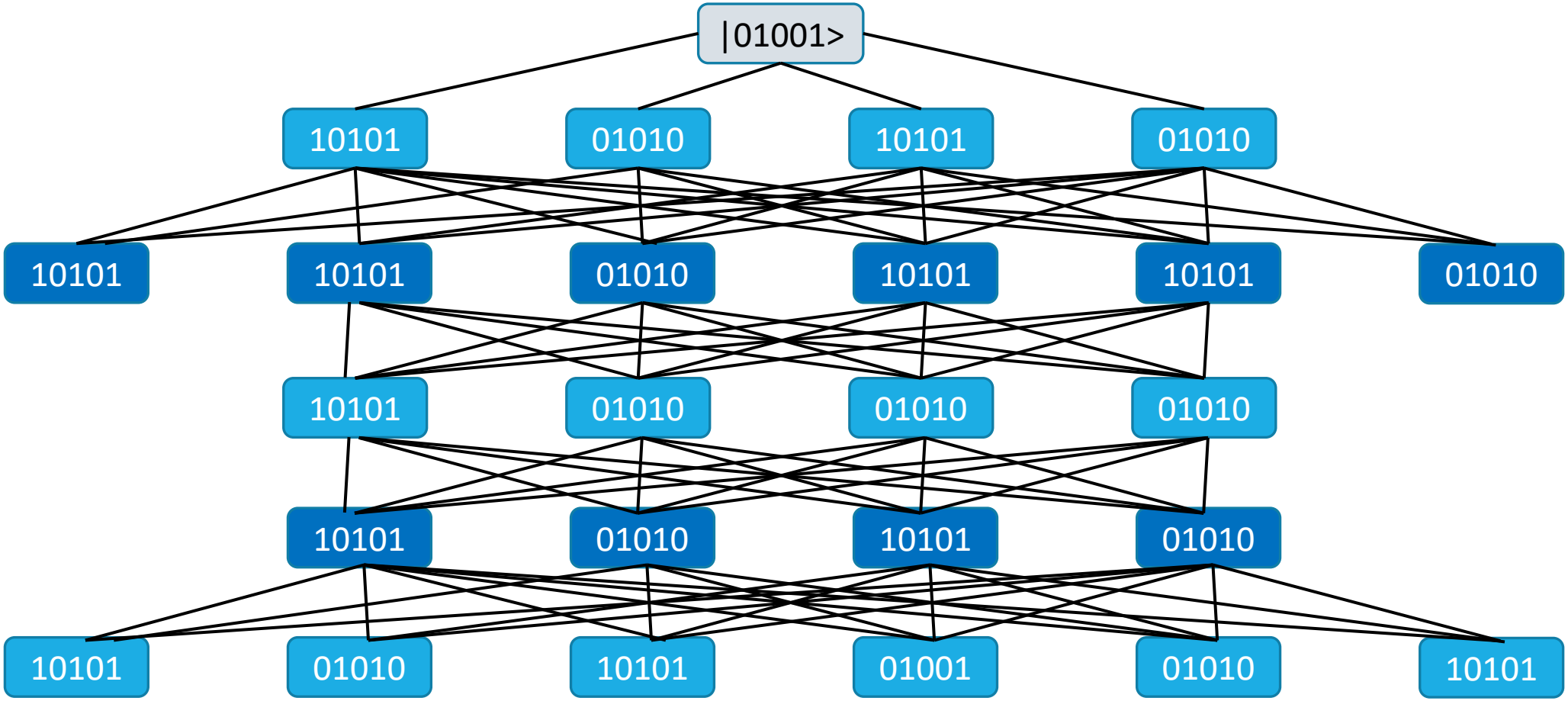


250 qubits provide the same amount of work that 10^{80} classical bits can do
this is more states than atoms in the visible universe

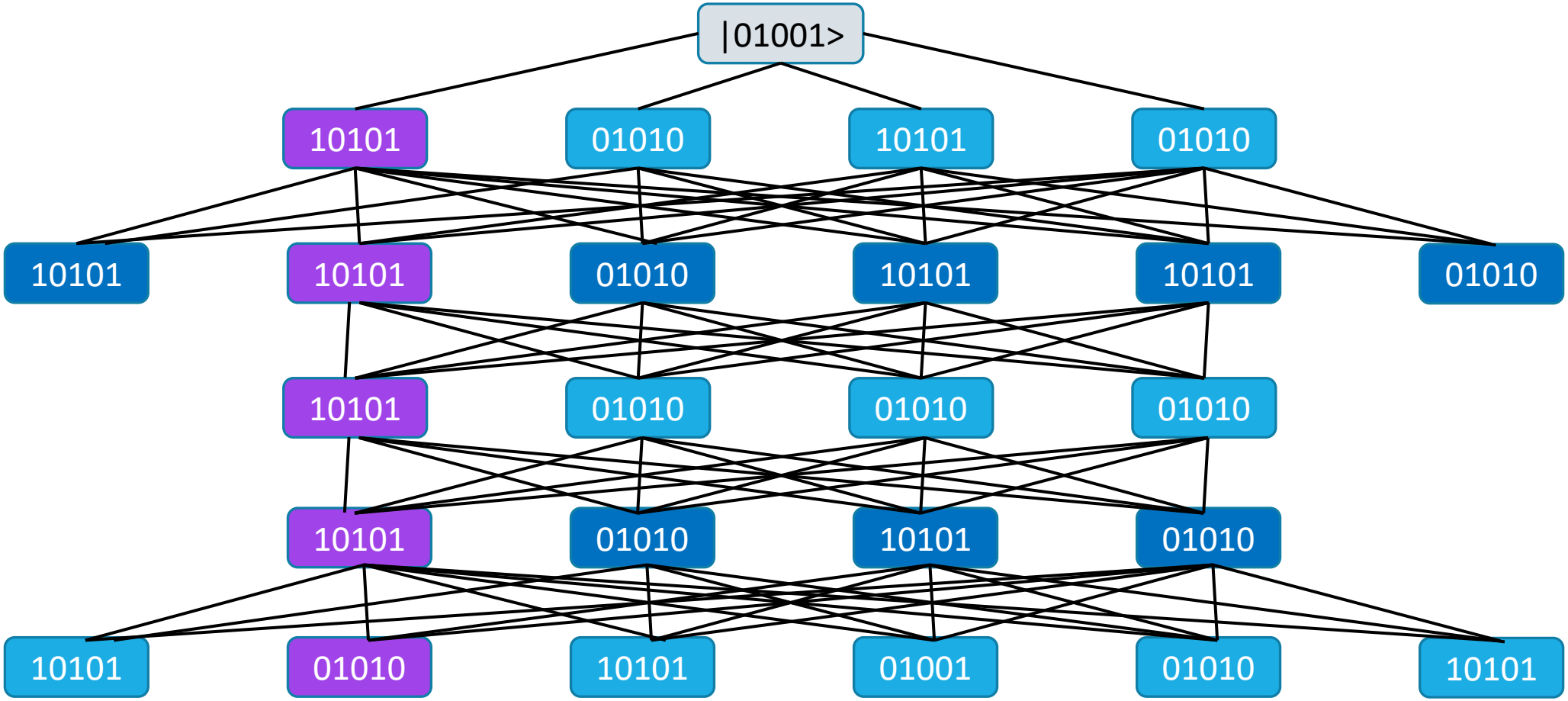
How fast is really fast – Quantum parallelism



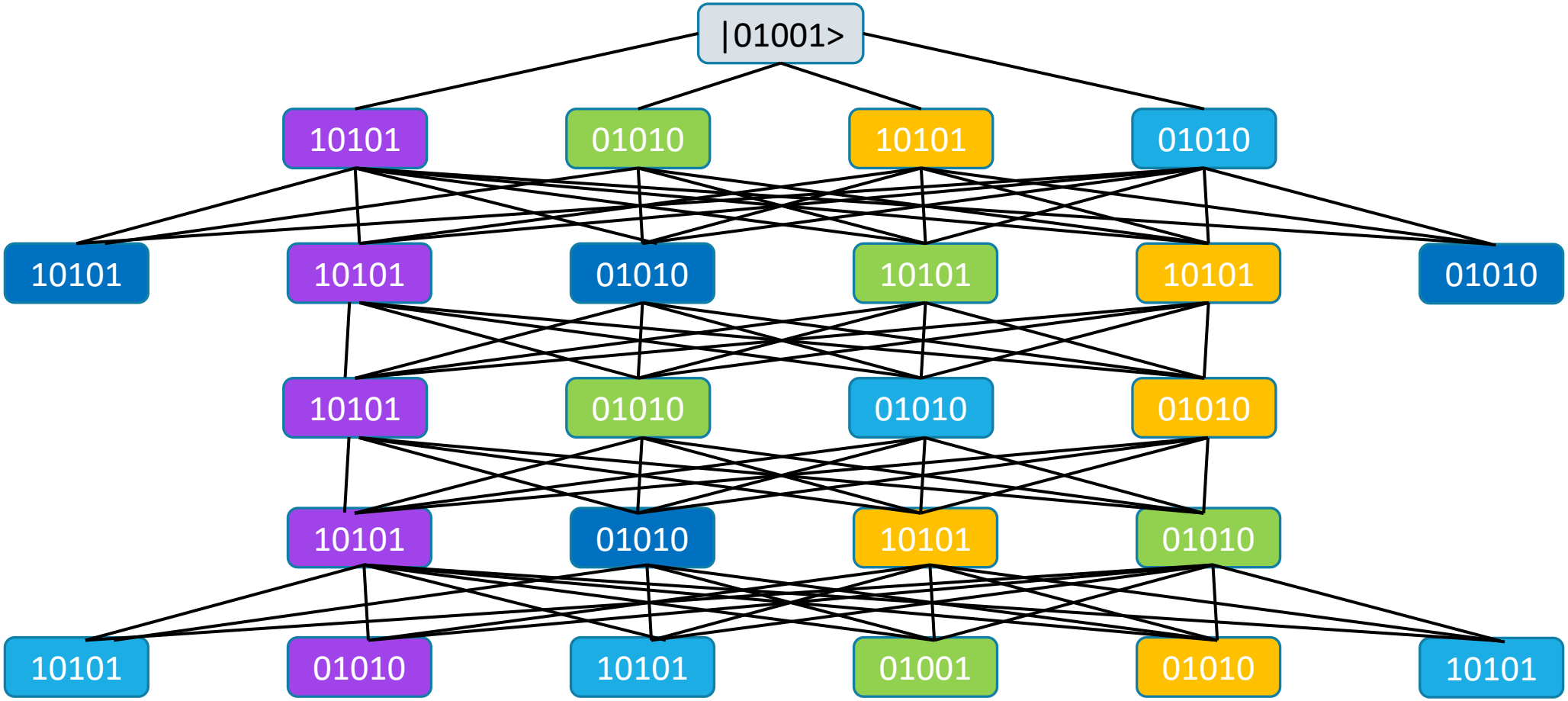
How fast is really fast



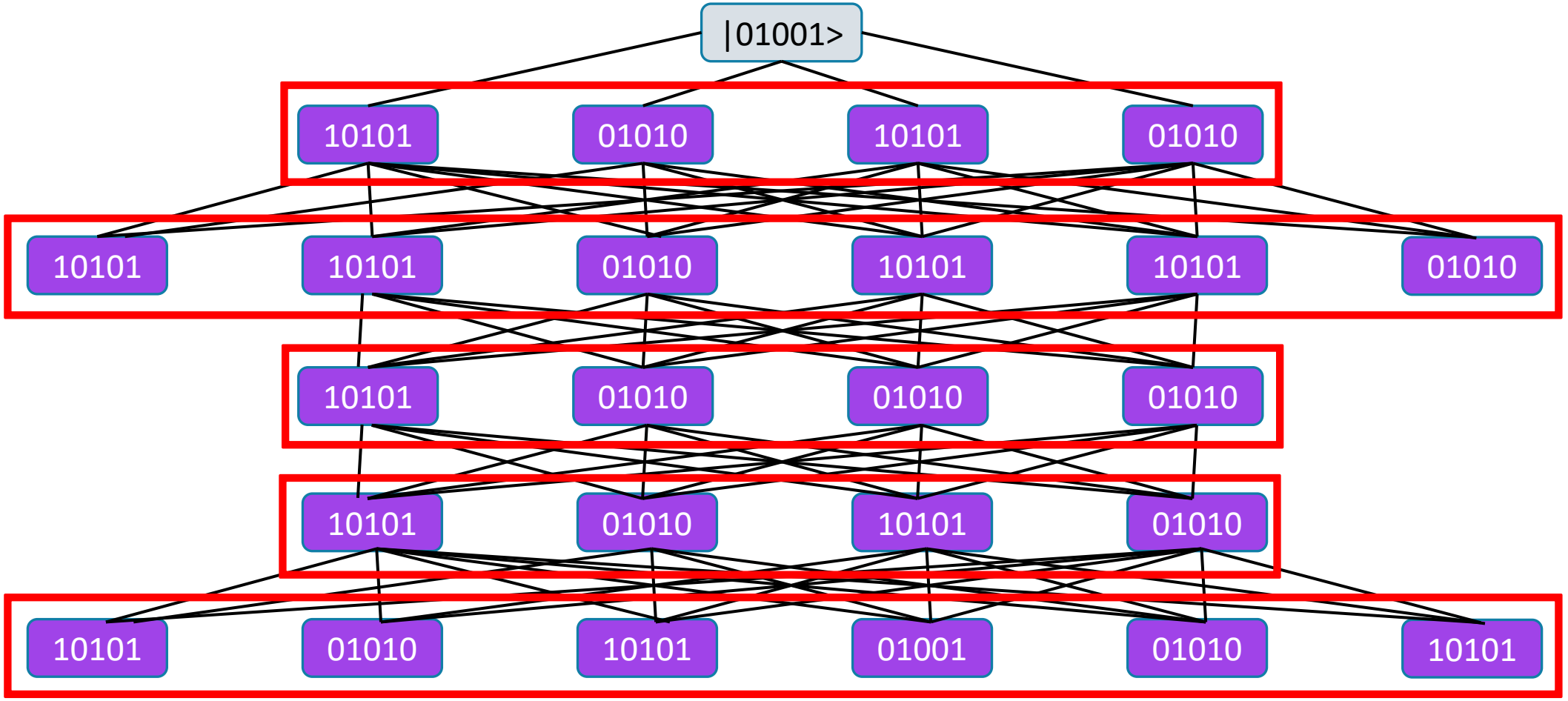
How fast is really fast



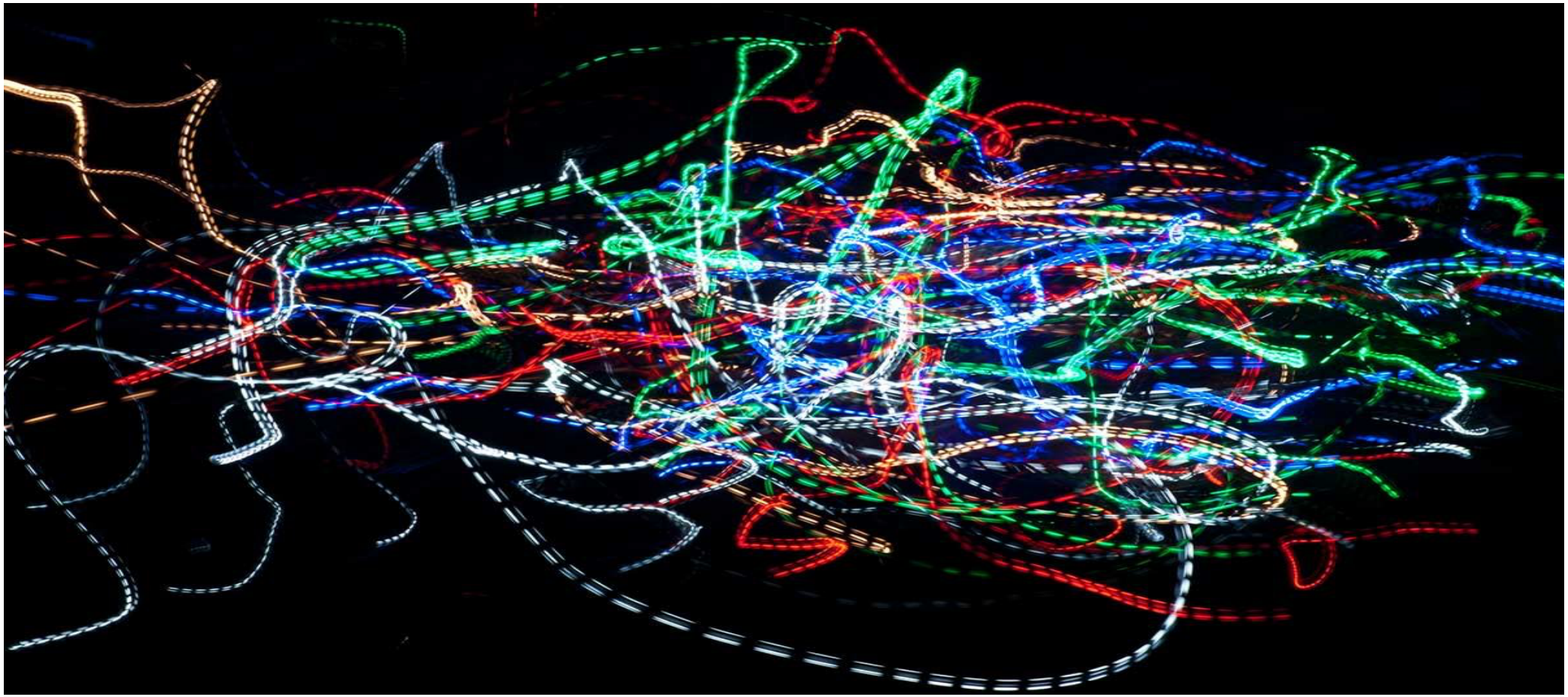
How fast is really fast



How fast is really fast



Relationships among data - Entanglement



Quantum Gate

Quantum Gate

The instant you measure the Qubit, it collapses into one of the definite states.

The decoherence effect – interference

One of the biggest problem that faced by scientists is the issue of “Decoherence”.

How is a Quantum computer built

Navigating the obstacles of building Quantum computers

- 1.5 Degrees Kelvin
  temperature needed
- 100 microseconds coherence time
  the window you have to perform calculations
- 50 nanoseconds time
  to perform a single quantum gate operation
- 10-24 joules energy
  difference between 0 and 1 state

300K .. 80.33F ← Room temp

100 .. -279.67 ← Nitrogen

30 .. -405.67

10 .. -441.67

Helium →

Cryogenic Computer ←

3 .. -454.27

Deep Space →

1 .. -457.87

0.3 .. -459.13

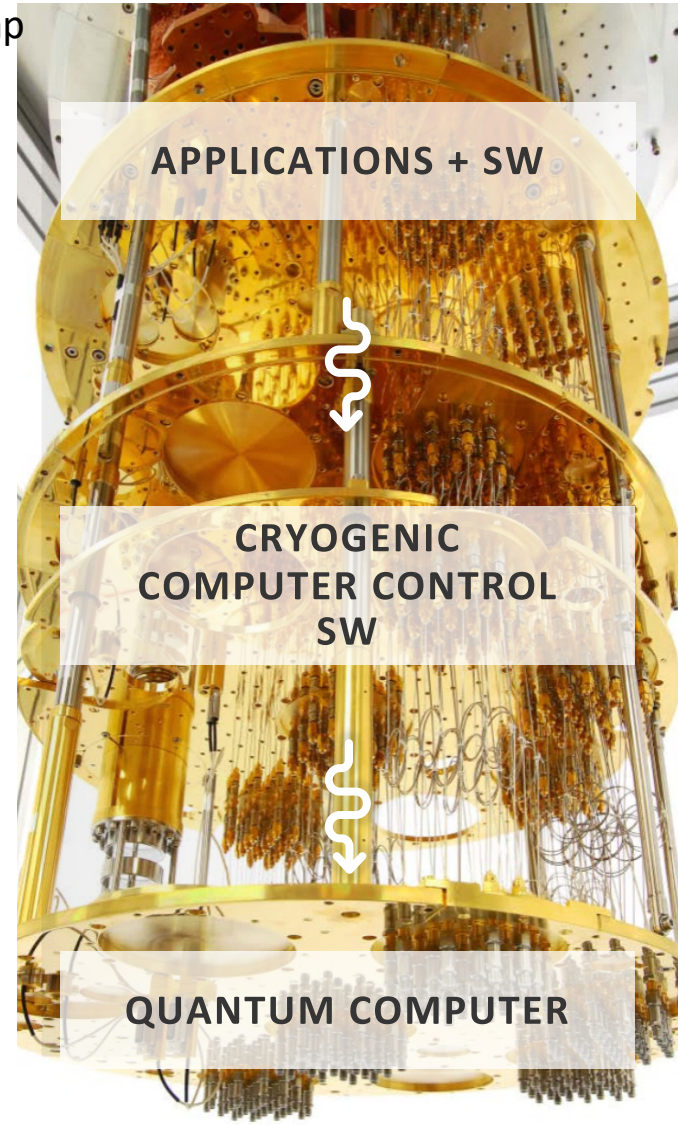
0.1 .. -459.49

0.03 .. -459.65

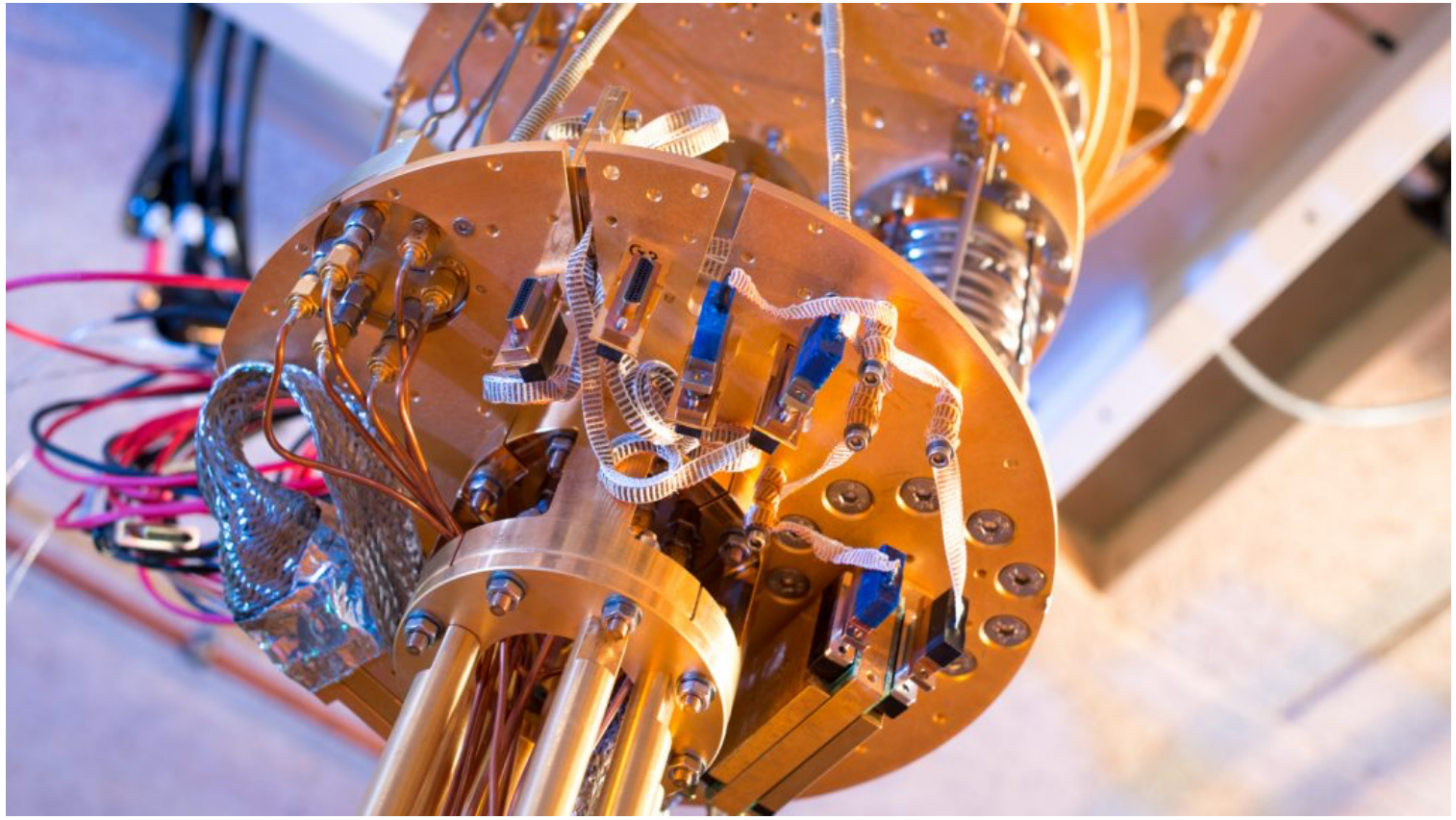
Quantum Computer →

Quantum World ←

0.01K .. -459.65F



Quantum computer or co-processor



https://cloudblogs.microsoft.com/quantum/2018/06/06/the-microsoft-approach-to-quantum-computing/

The Microsoft solution

Majorana Fermions
Predicted by Ettore Majorana
in 1937

The topological approach - the Majorana quasi-particle

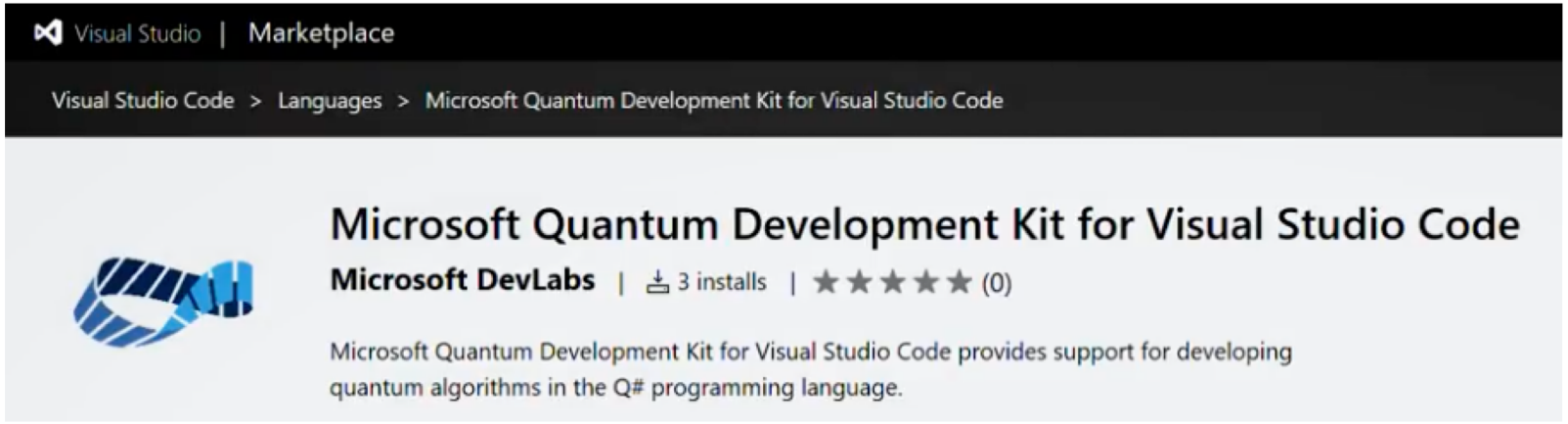
- **A unique approach for true scalability**
- **Topological qubits deliver 3 to 4 orders of magnitude better fidelity**

Microsoft Q#

Quantum focused programming language

Getting started with Microsoft's Quantum Development Kit

The Quantum Development Kit



Scalable: Q# allows us to write a code that can be executed on machines of varying computing abilities. We can use it to simulate a few Qubits on our local machine or even thousands of Qubits for an enterprise level application.

Multi-paradigm: Q# is a multi-paradigm programming language as it supports both, functional as well as imperative, programming styles. If you are new to the programming paradigm

Domain-specific: Q# is a programming language for quantum computing. It is to be used for writing algorithms/code snippets to be executed on quantum processors.

Quantum Simulator

```
using (var sim = new QuantumSimulator())
{
    var rand = new System.Random();


    foreach (var idxRun in Enumerable.Range(0, 8))
    {
        var sent = rand.Next(2) == 0;
        var received = TeleportClassicalMessage.Run(sim, sent).Result;

        System.Console.WriteLine($"Round {idxRun}:\tSent {sent},\tgot {received}.");
        System.Console.WriteLine(sent == received ? "Teleportation successful!!\n" : "\n");
    }
}
```

Target machines

State-of-the-Art Local Simulator

- Simulate 30 qubits in 16 GB
- Run locally on your PC

State-of-the-Art Azure Simulator

- Simulate more than 40 qubits
- Run in Azure

Quantum Trace Simulator

- Profile your code and determine resource costs of quantum program
- Scale to large algorithms and numbers of qubits

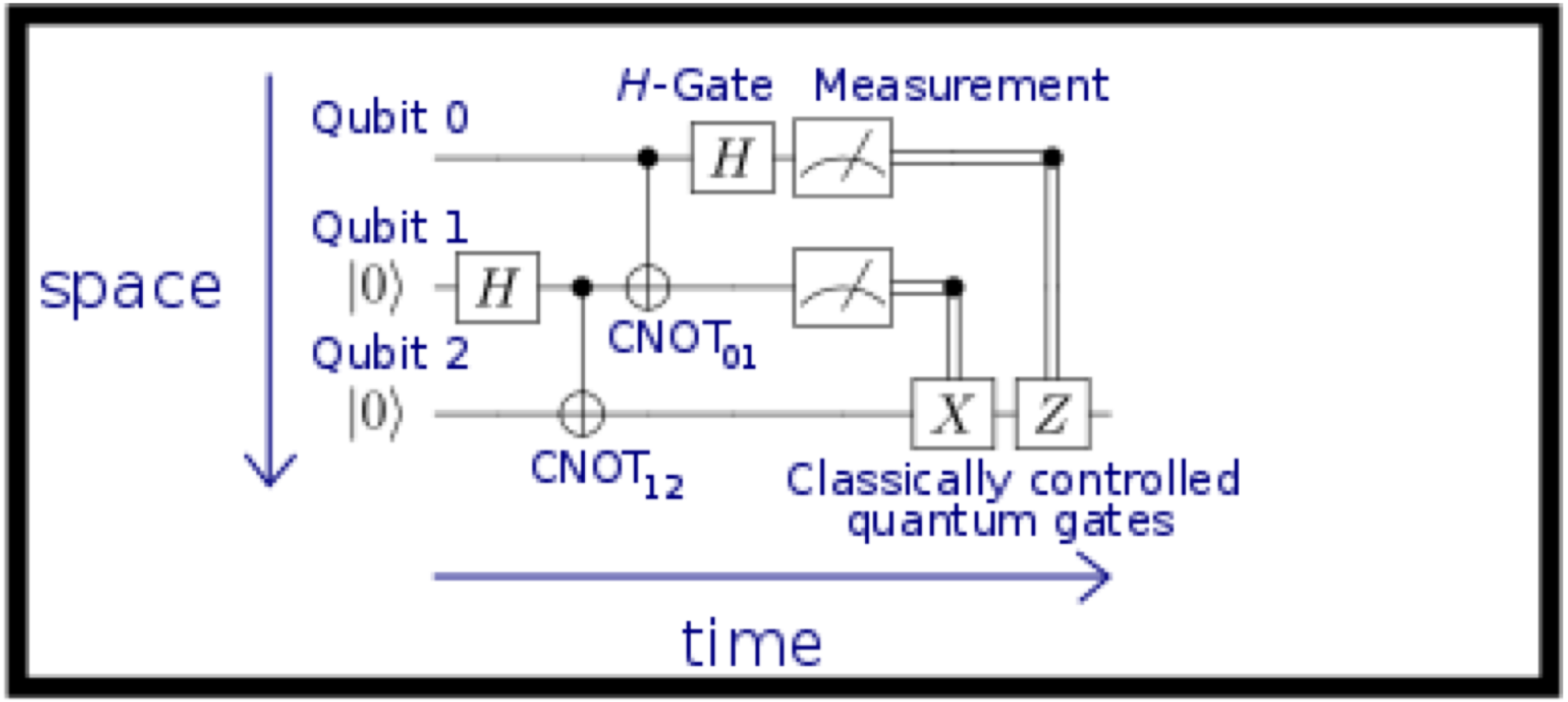
Microsoft’s Quantum System

Hello World example in Quantum computing

Teleportation

no cloning

Example: Teleport Basis State



Annotated Teleportation Circuit

Example: Teleport Basis State

```
operation Teleport(msg : Qubit, there : Qubit) : () {
    body {
        using (register = Qubit[1]) {
            // Ask for an auxillary qubit that we can use to prepare for teleportation.
            let here = register[0];

            // Create some entanglement that we can use to send our message.
            H(here);
            CNOT(here, there);

            // Move our message into the entangled pair.
            CNOT(msg, here);
            H(msg);

            // Measure out the entanglement.
            if (M(msg) == One)  { Z(there); }
            if (M(here) == One) { X(there); }

            // Reset our "here" qubit before releasing it.
            Reset(here);
        }
    }
```

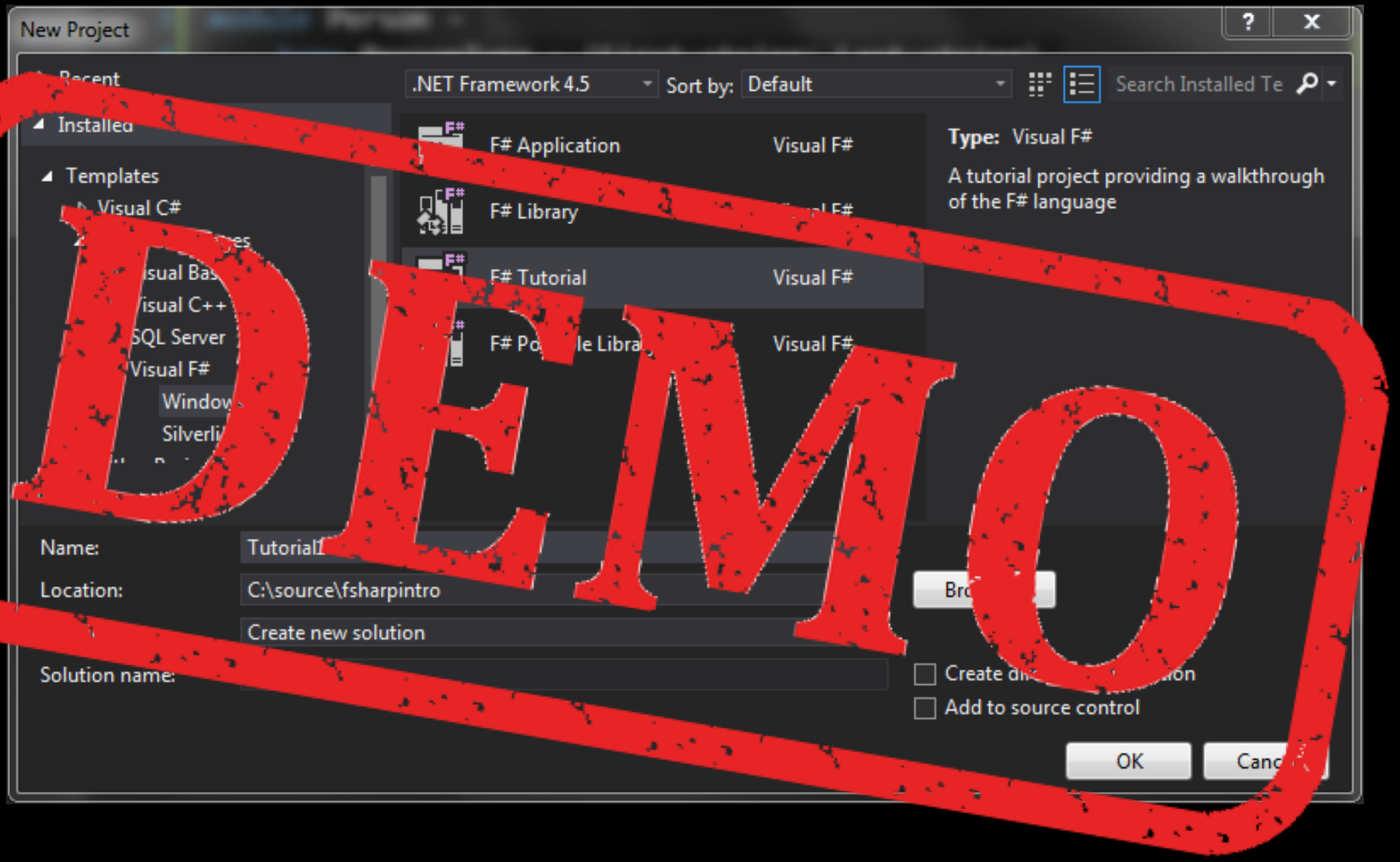
Example: Teleport Basis State

```
operation TeleportClassicalMessage(message : Bool) : Bool {
    body {
        mutable measurement = false;

        using (register = Qubit[2]) {
            // Ask for some qubits that we can use to teleport.
            let msg = register[0];
            let there = register[1];

            // Encode the message we want to send.
            if (message) { X(msg); }

            // Use the operation we defined above.
            Teleport(msg, there);
            // Check what message was sent.
            if (M(there) == One) { set measurement = true; }
            // Reset all of the qubits that we used before releasing them.
            ResetAll(register);
        }
        return measurement;
    }
}
```


New Project
.NET Framework 4.5
Sort by:
Default
Search Installed Te
Installed
Templates
Visual C#
Visual C++
SQL Server
Visual F#
Silverli
F# Application
Visual F#
F# Library
F# Tutorial
Visual F#
Visual F#
Type: Visual F#
A tutorial project providing a walkthrough of the F# language
Name:
Tutorial1
Location:
C:\source\fsharpintro
Create new solution
Solution name:
Add to source control
OK
DEMO

Quantum Search - $O(\sqrt{N})$

The phonebook problem

…	…
…	…
Monic, Nielsen	75812499
Richard, Bell	34057287
Frank, Brown	39814450
…	…
…	…

The phonebook problem

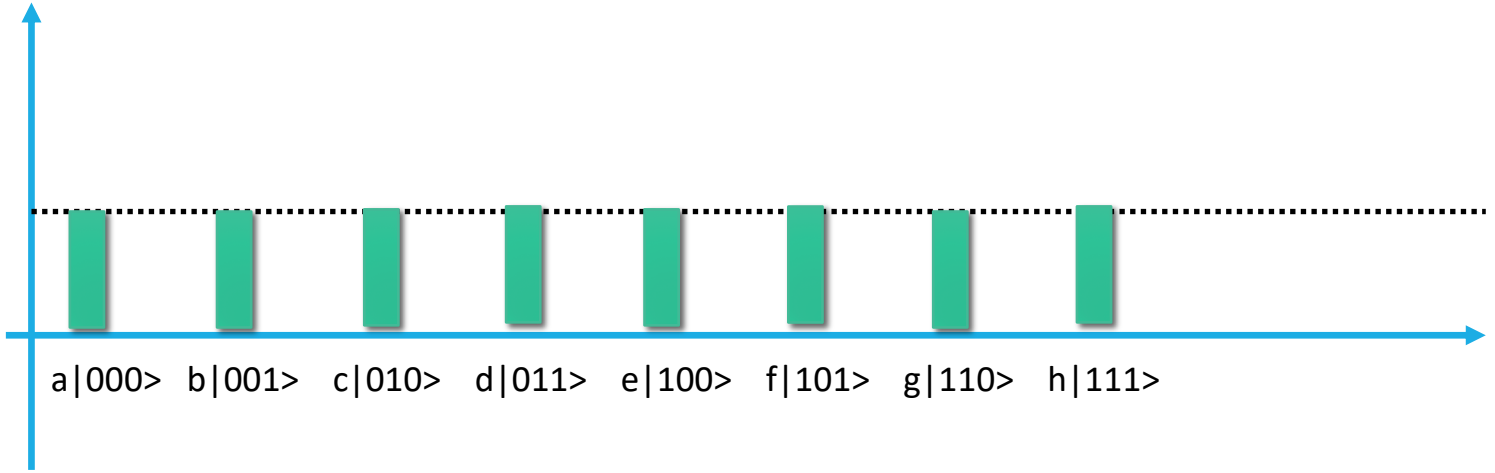
$|\psi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$

$a = b = c = d = e = f = g = h = {}^{1}/_{\sqrt{8}}$

The phonebook problem

$|\psi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$

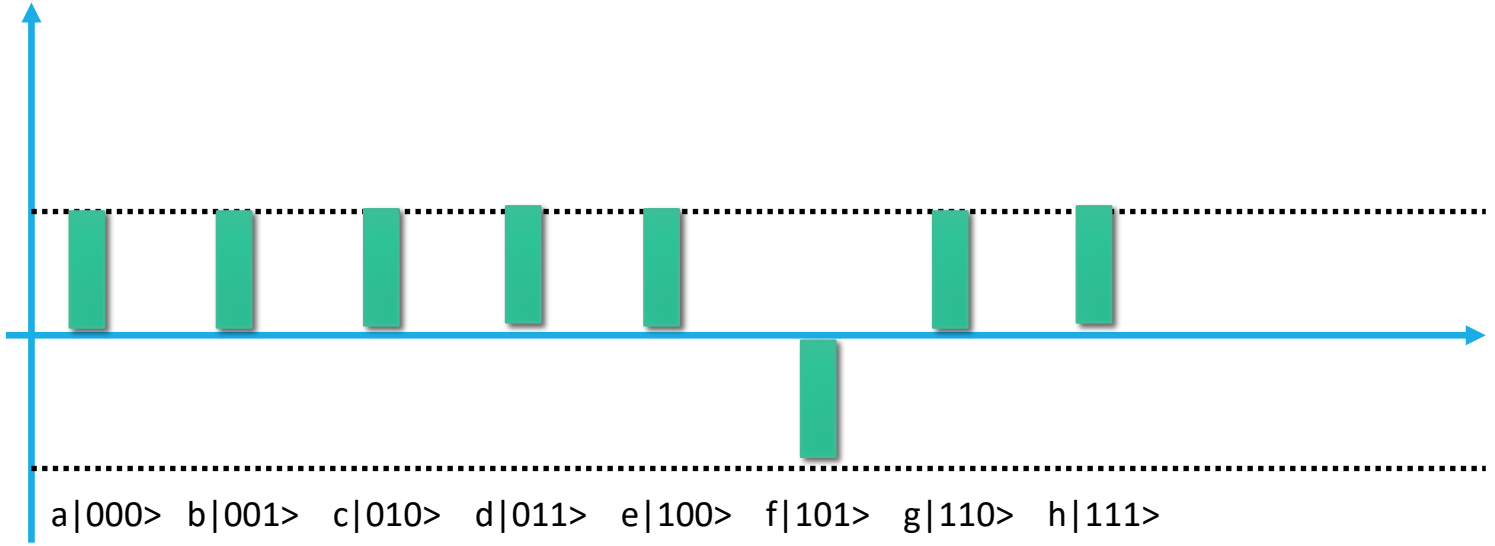
$a = b = c = d = e = f = g = h = 1/\sqrt{8}$



The phonebook problem

$|\psi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$

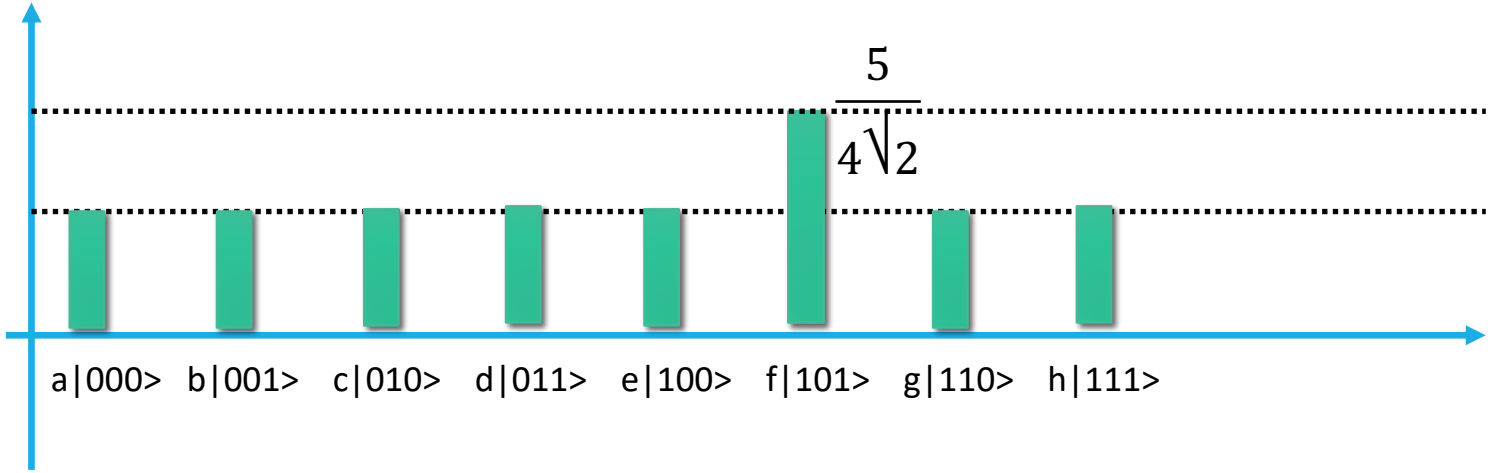
$a = b = c = d = e = f = g = h = 1/\sqrt{8}$



The phonebook problem

$|\psi\rangle = a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$

$a = b = c = d = e = f = g = h = 1/\sqrt{8}$

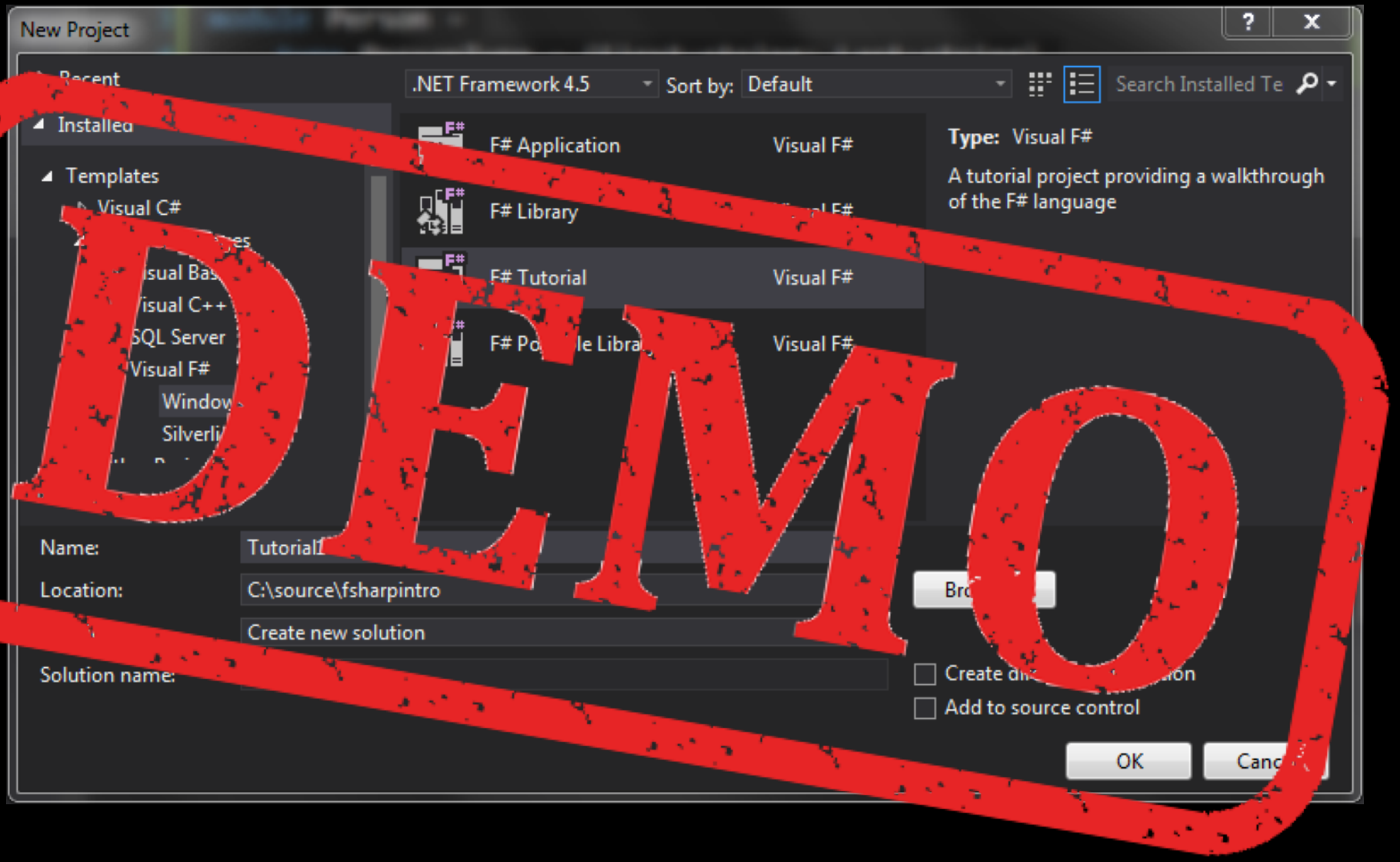


The phonebook problem

Number to search	Traditional Computer	Quantum Computer
100	100	10
1,000	1,000	32
10,000	10,000	100
100,000	100,000	316
1,000,000	1,000,000	1,000
10,000,000	10,000,000	3,162
100,000,000	100,000,000	10,000
1,000,000,000	1,000,000,000	31,623

The phonebook problem

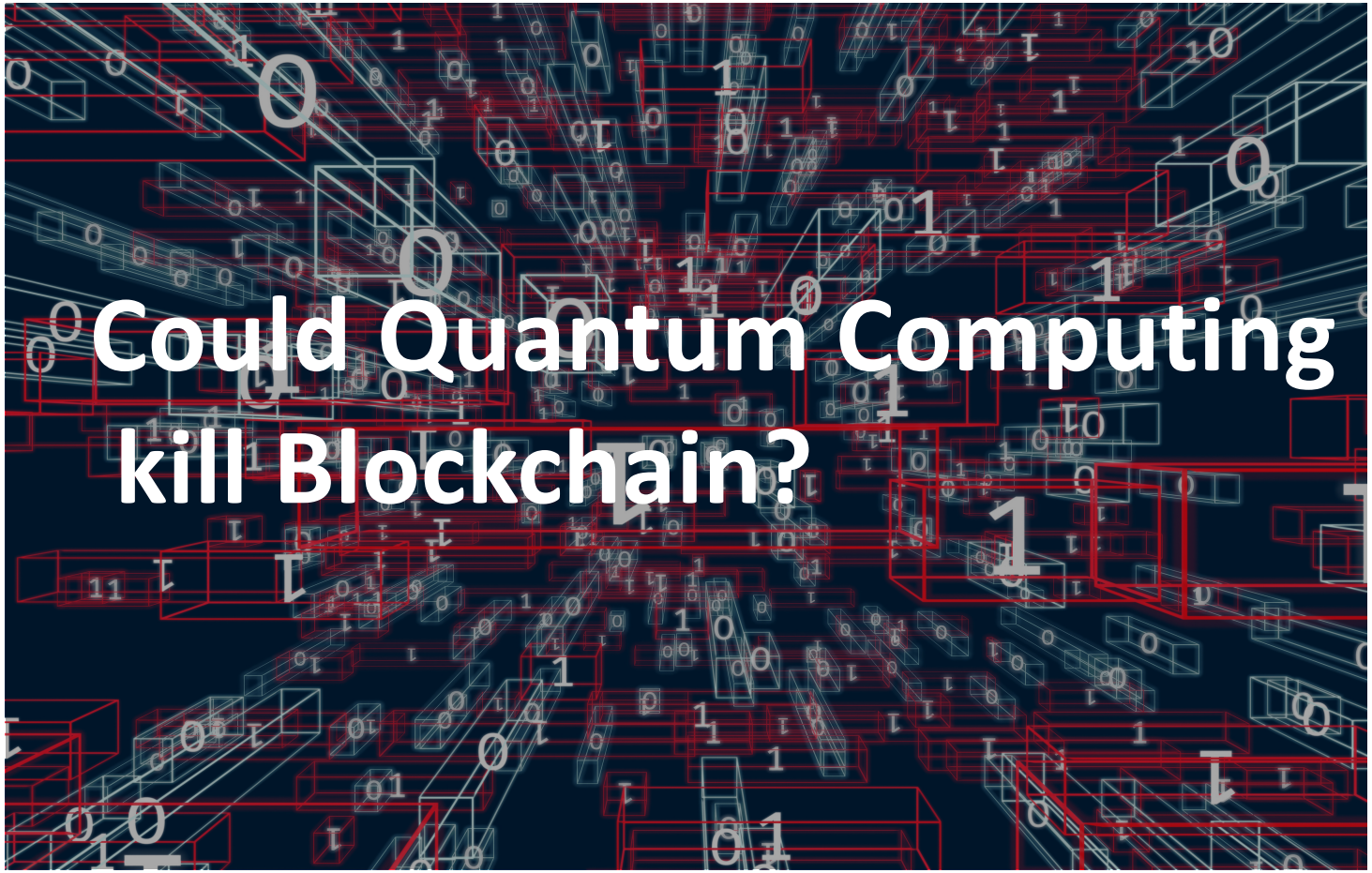
```
operation ApplyQuantumSearch(nIterations : Int, nDatabaseQubits : Int) : (Result, Result[]) {
    body{
        // Allocate variables to store measurement results.
        mutable resultSuccess = Zero;
        mutable resultElement = new Result[nDatabaseQubits];
        // Allocate nDatabaseQubits + 1 qubits. These are all in the |0⟩ state.
        using (qubits = Qubit[nDatabaseQubits+1]) {
            let markedQubit = qubits[0];
            // Let all other qubits be the database register.
            let databaseRegister = qubits[1..nDatabaseQubits];
            QuantumSearch(nIterations, markedQubit, databaseRegister);
            // Measure the marked qubit. On success, this should be One.
            set resultSuccess = M(markedQubit);
            // Measure the state of the database register post-selected on the state of the marked qubit.
            set resultElement = MultiM(databaseRegister);
            if (resultSuccess == One) {
                X(markedQubit);
            }
         return (resultSuccess, resultElement);         // Returns the measurement results of the algorithm.
```


New Project
.NET Framework 4.5
Sort by:
Default
Search Installed Te
Installed
Templates
Visual C#
Visual C++
SQL Server
Visual F#
Silverli
F# Application
Visual F#
F# Library
F# Tutorial
Visual F#
Visual F#
Type: Visual F#
A tutorial project providing a walkthrough of the F# language
Name:
Tutorial1
Location:
C:\source\fsharpintro
Create new solution
Solution name:
Add to source control
OK
DEMO

Advantages and Disadvantage of Quantum computing

Advantages	Disadvantages
Increase in computing power	Although a qubit can hold many possible values, only one classical result can be obtained from every run
Advance in security	Repeated runs may be necessary to obtain the desired result
Teleportation	It is not possible to copy qubits (no-cloning)

Just a thought…



https://www.investinblockchain.com/could-quantum-computing-kill-blockchain/abstract-digital-background/

Resources

Q# https://github.com/rikace/presentations/quantum

MSFT Build 2018

https://developer.microsoft.com/en-us/events/build/content/the-quantum-revolution-with-q

MSFT quantum documentation

https://docs.microsoft.com/en-us/quantum/q

Q# Katas

https://github.com/Microsoft/QuantumKatas

Q# source code

https://github.com/Microsoft/Quantum

contacts

Source	https://github.com/rikace/presentations/quantum
Twitter	*@trikace*
Blog	*www.rickyterrell.com*
Email	*tericcardo@gmail.com*