# A Quantum of Computing

…using the Incomprehensible to solve the Intractable …


## Dave McMahon

dave@nxtgenug.net
@mcmahond
http://davemcmahon81.wordpress.com


# Your Speaker

- 15 years in Software Industry
- 9 years Software Systems Architect at Ridgian
- Co-Founder The Next Generation User Group
- Spoken at User Groups, DDD's, TechEd
- First Class Honours Degree in Theoretical Physics From York University 1983

# The Aim

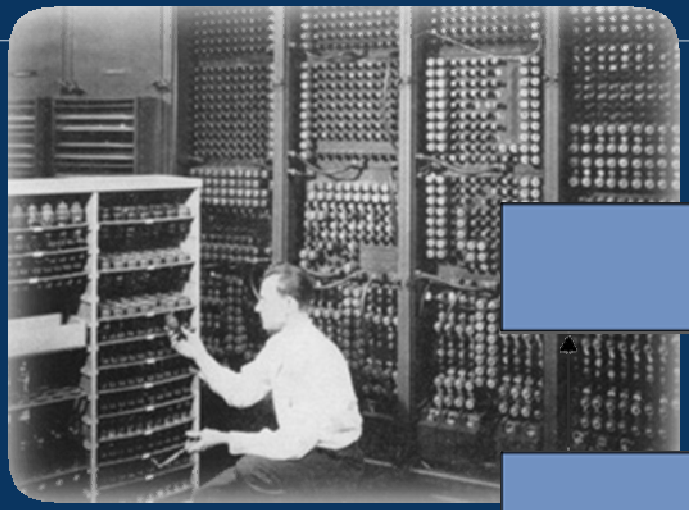
To show you how Quantum Theory and Quantum Effects are being used to bring about future generations of computers

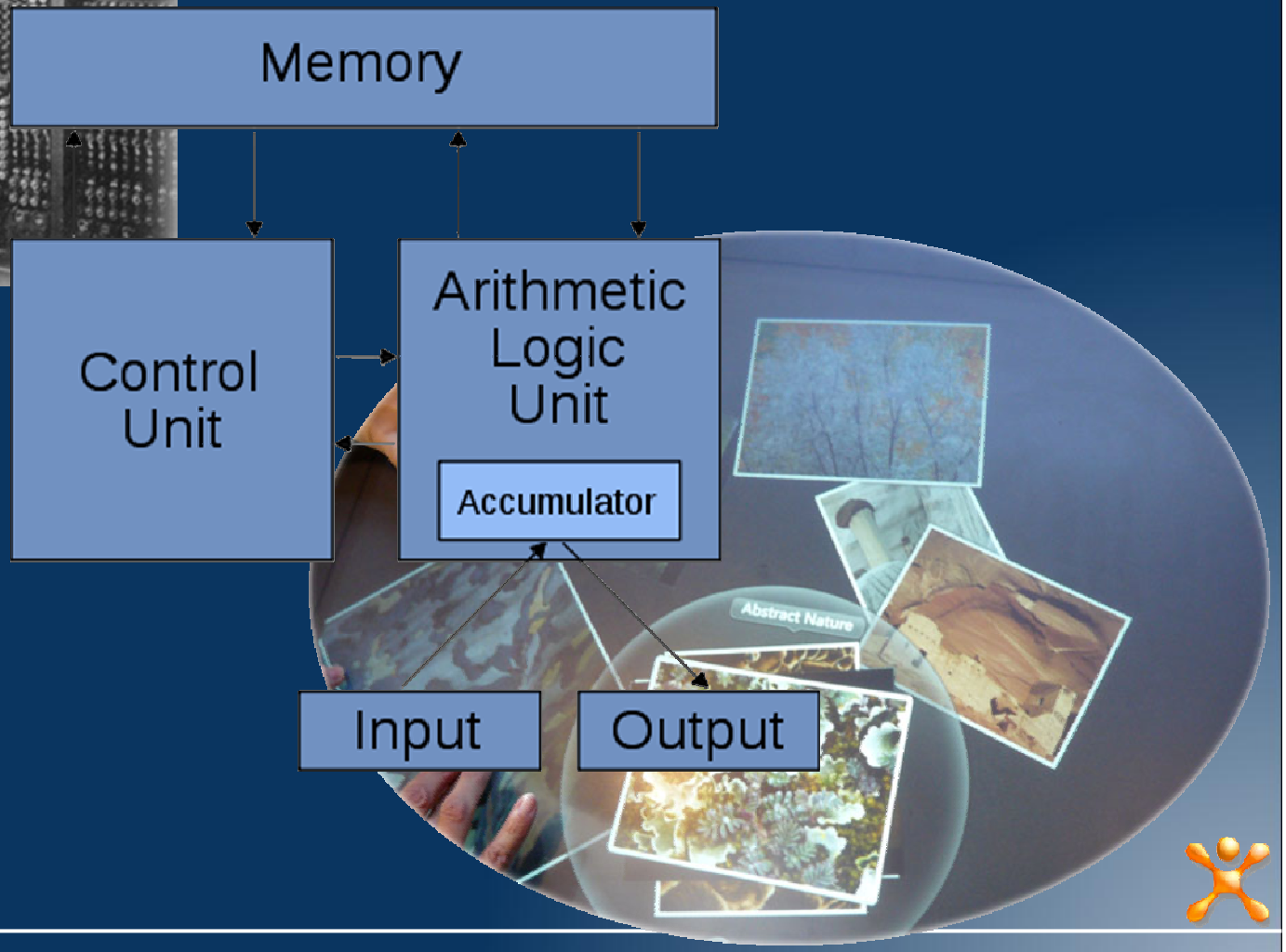
# The Agenda

- Limits of the ‘Von Neumann’ Machine
- What can Quantum Computing Offer?
- The QuBit
- A Basic Quantum Algorithm
- A Quantum Search Algorithm
- Quantum Computers Today

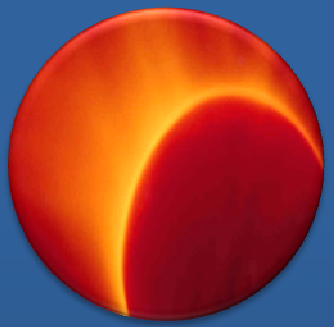
# ‘Von Neumann’ Machine

# ‘Von Neumann’ Machine

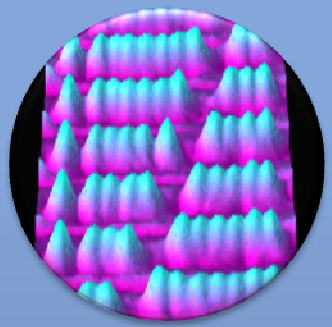




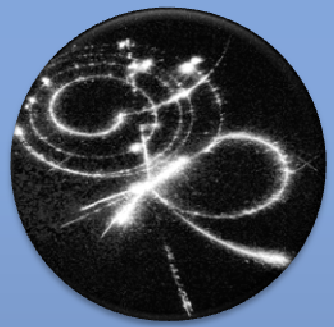
# Limits of the Von Neumann Machine



Classical Limitations



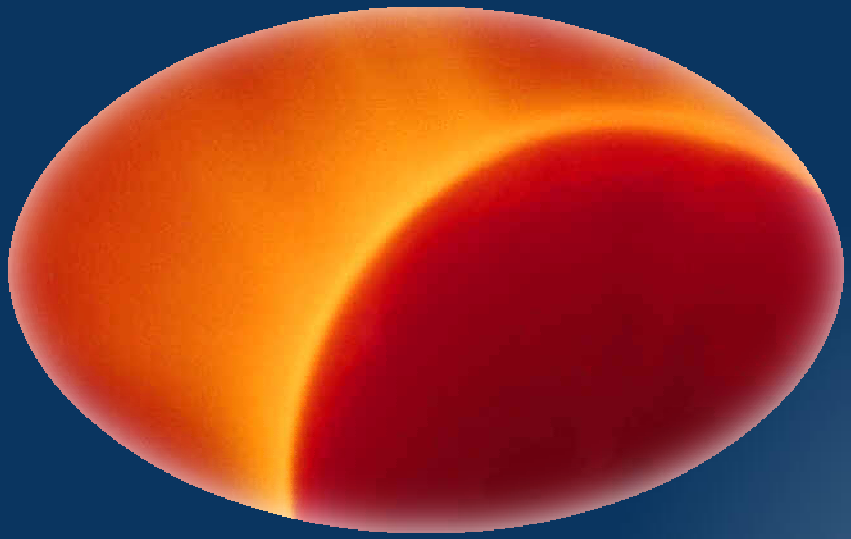
Quantum Limitations



Relativistic Limitations

# Classical Limitations

## Heat

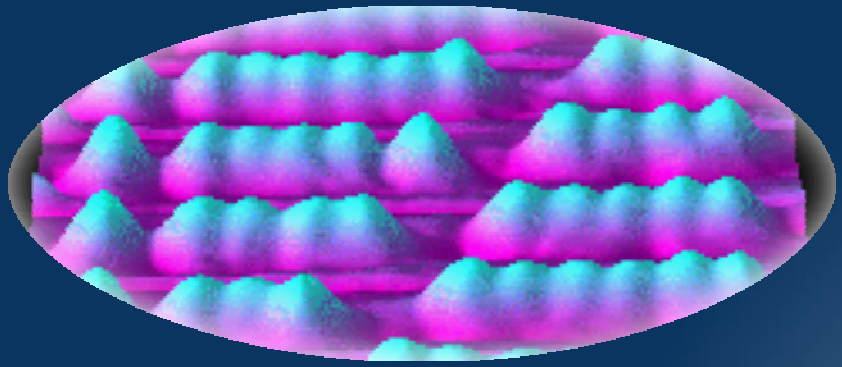


# Classical Limitations

- Heat is the main reason that:
  - Clock speeds are not increasing
  - Multi-core architectures are becoming the norm
- Heat will (probably) :
  - Signal the end of the CMOS chip
  - Result in other technologies replacing it
- However, let us assume that we do solve the heat problem ...

# Quantum Limitations

## Measurement and Manufacture

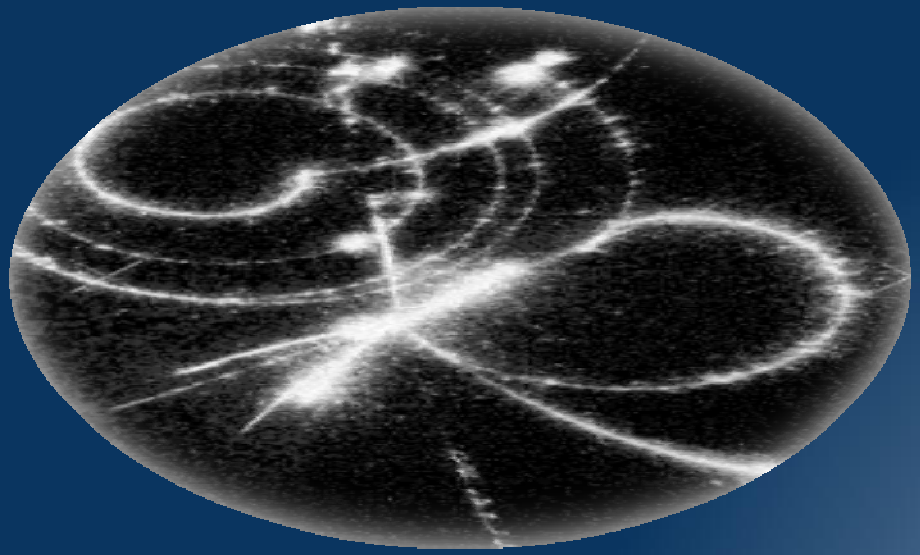


# Quantum Limitations

- Quantum Limitations will:
  - Limit the accuracy to which chips can be made with current etching technology
  - Limit the size to which individual transistor gates can be miniaturised
- Quantum Limitations are a natural limitation to evermore miniaturisation
- Let's assume however that we overcome these issues ...

# Relativistic Limitations

## Timing and Energy



# Relativistic Limitations

- Consider a 3 GHz processor (off today's shelf)
  - In 1 cycle a signal can propagate at most c/(3 GHz) = ~ 10cm
  - For a 1-cycle round-trip to cache memory and back the cache location can be at most ~5 cm away.
  - Electrical signals travel at ~0.5 c in typical materials therefore in practice, a 1-cycle memory can be at most ~2.5 cm away
- As clock speeds increase architectures must be increasingly local.

# Relativistic Limitations

- Computer systems are powered at 10V which equates to 10 eV.
- Corresponds to a max clock speed of 9.7 PHz
  - ~ 5 million times faster than today's CPUs
  - ~ 100,000 times faster than today's superconducting logics

# Where do we go from here?

perhaps

Quantum Computing

# What Can Quantum Computing Offer?

Different Modes of Computation

Reversible Computation

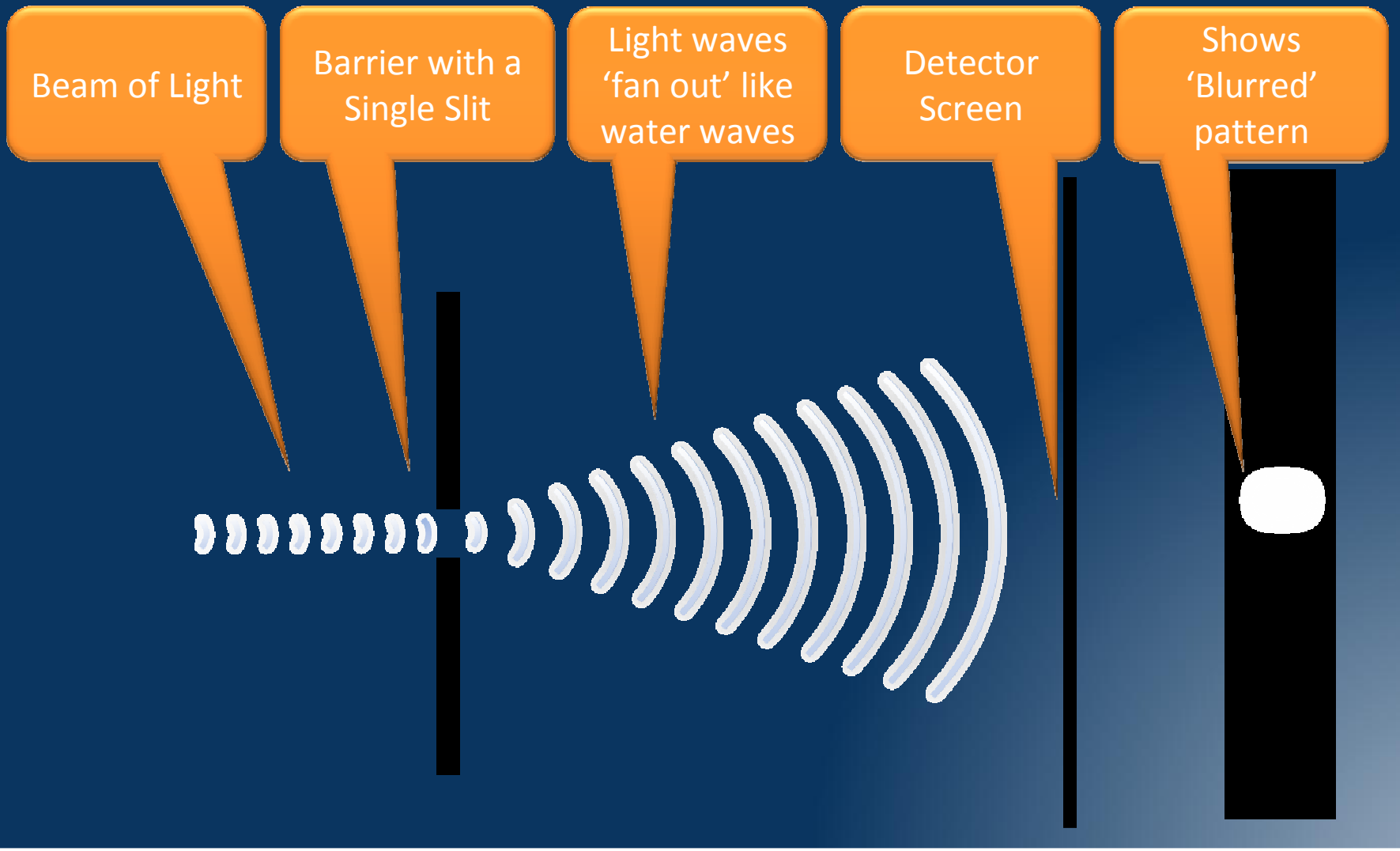
Speed of Computation

So …

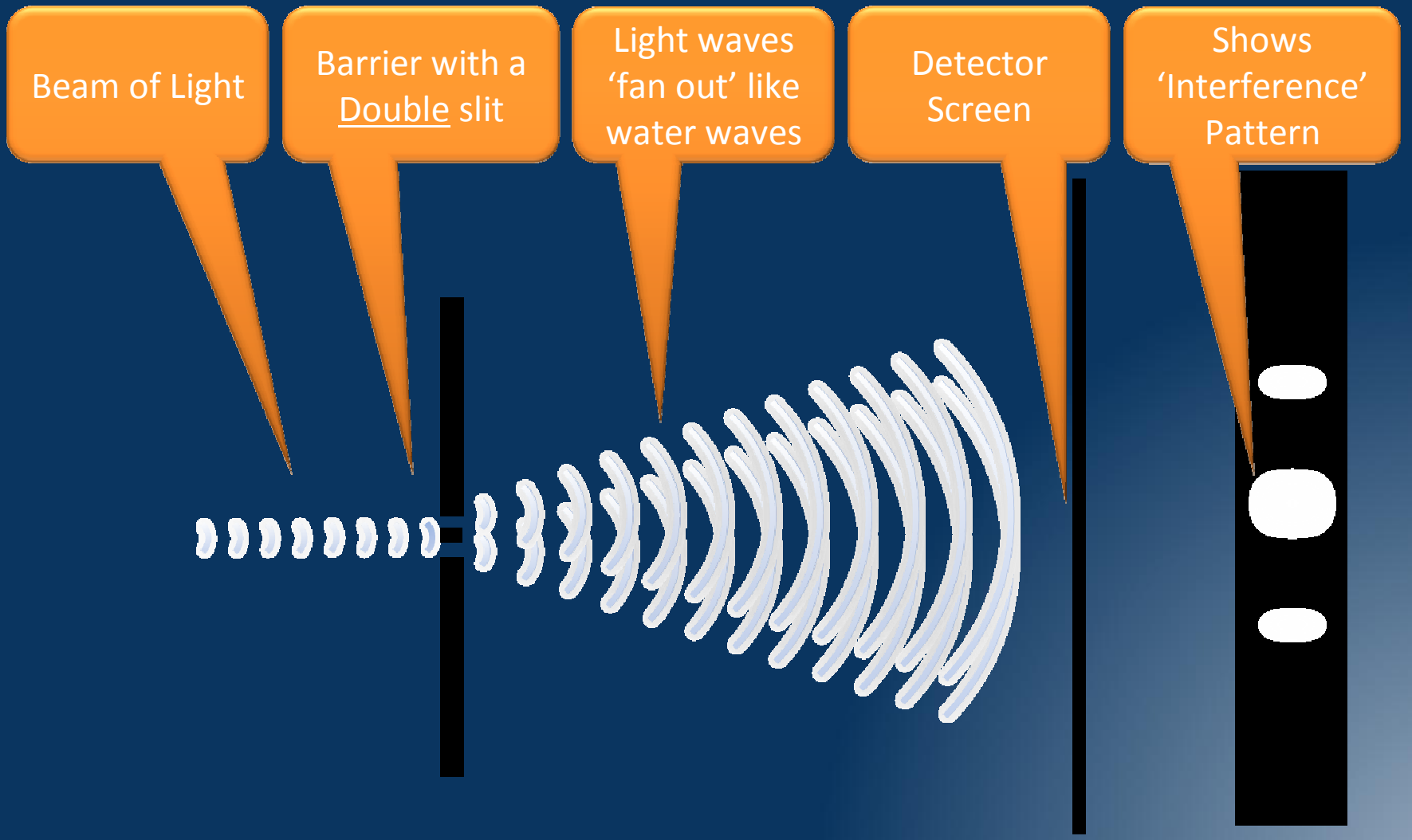
# How *can* you use Quantum Effects to do Computation?

… consider the classic ‘Double Slit’ experiment …

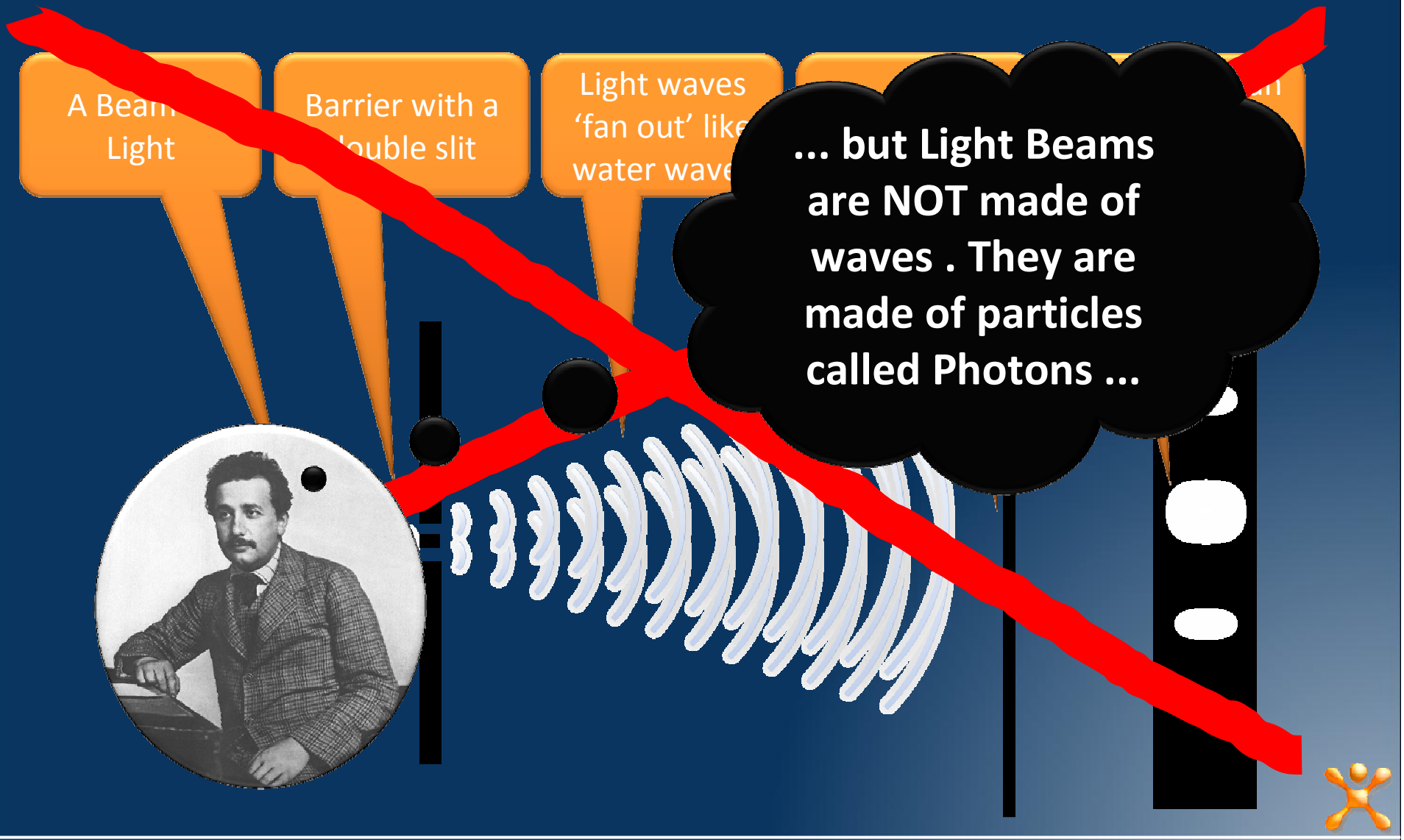
# The Double Slit Experiment – Part 1



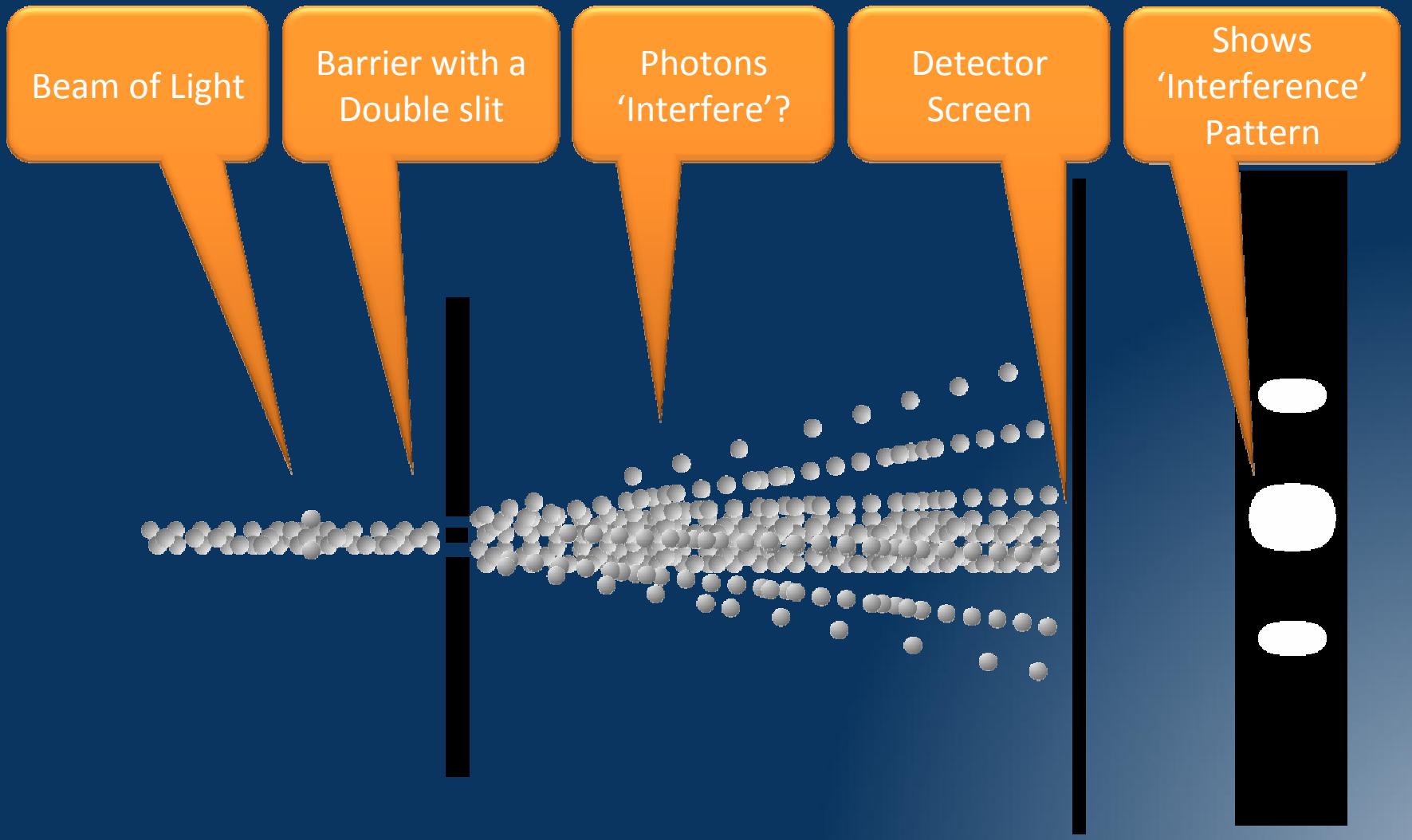
# The Double Slit Experiment – Part 2



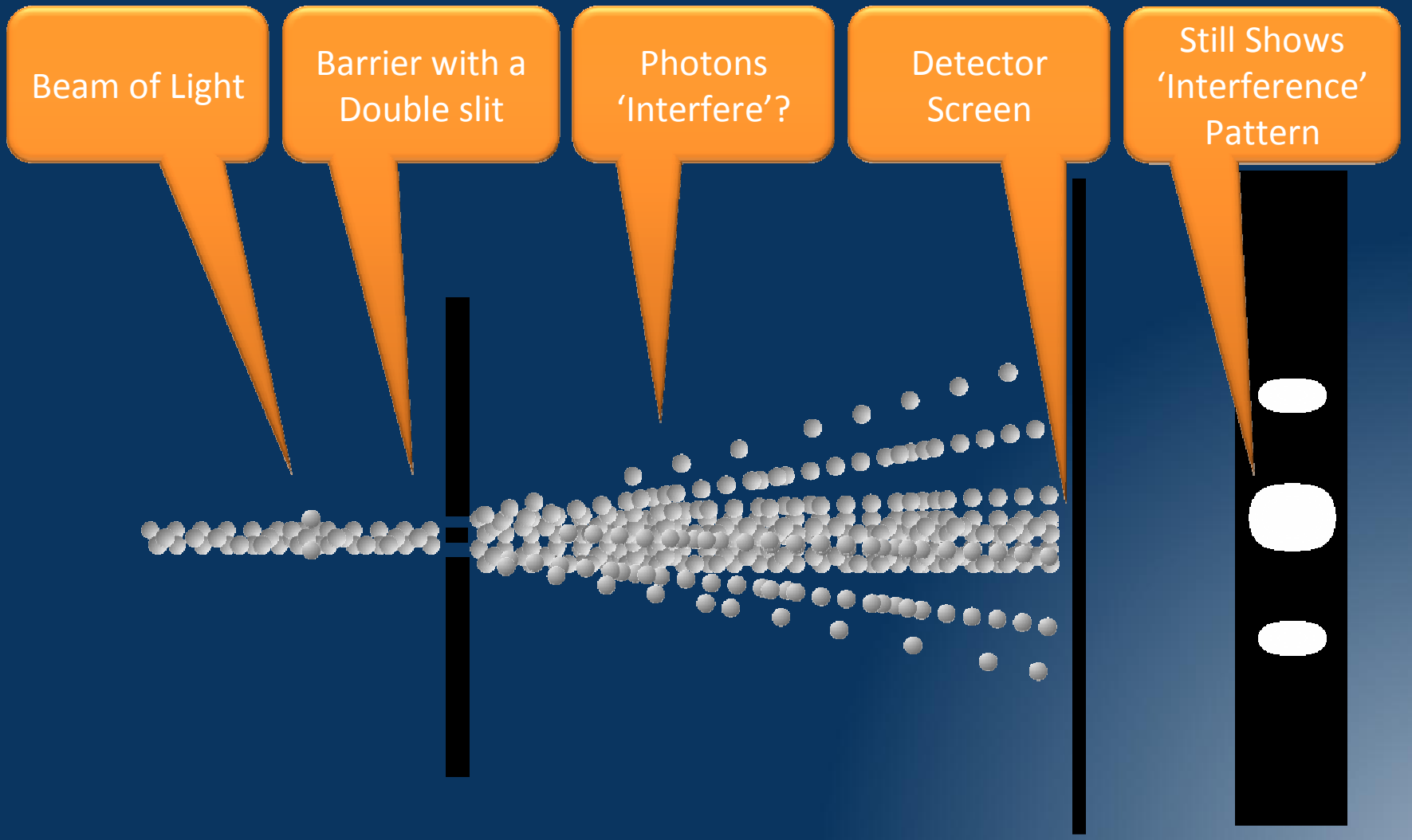
# The Double Slit Experiment – Part 2



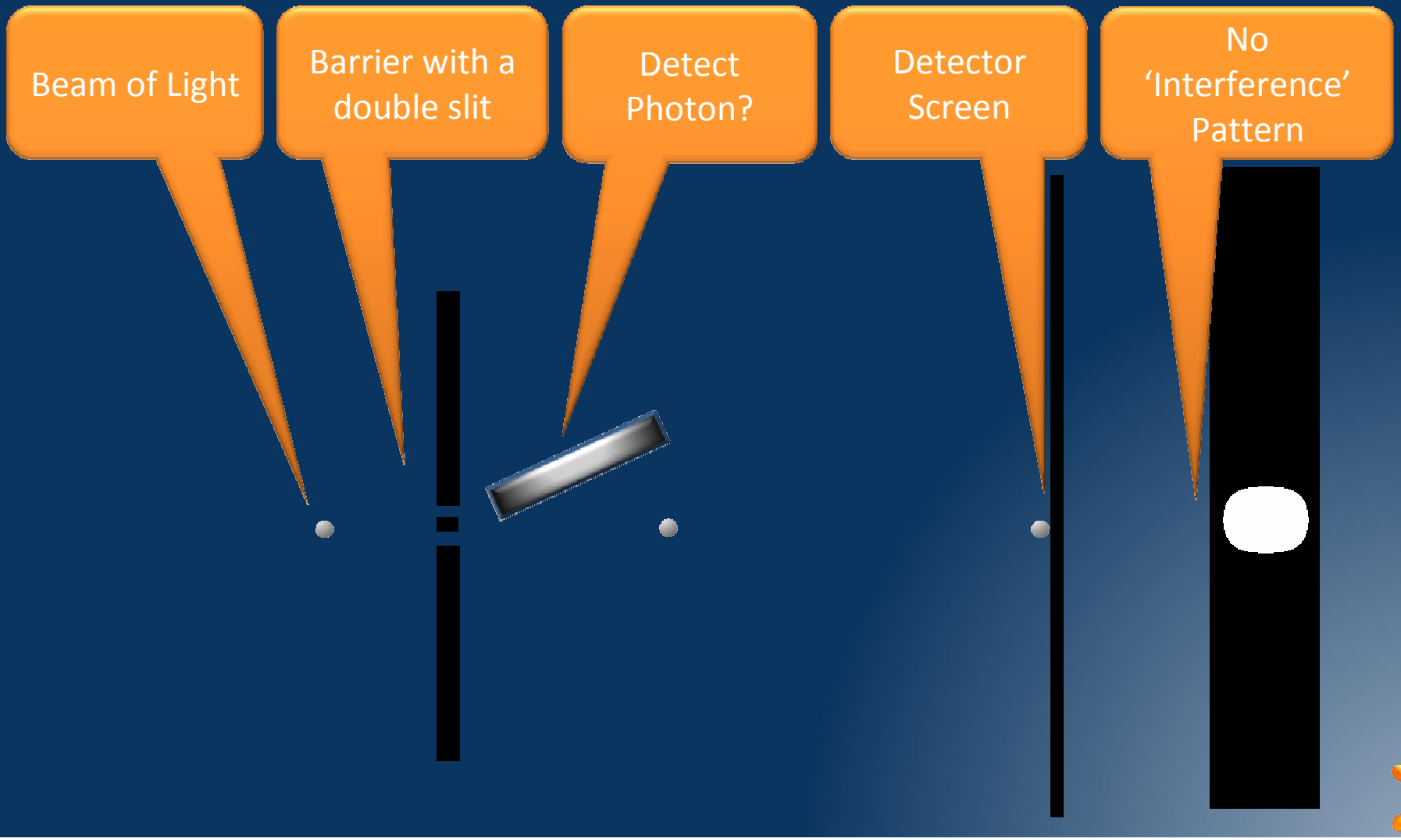
# The Double Slit Experiment – Part 3



# The Double Slit Experiment – Part 4



# The Double Slit Experiment – Part 5



# The Double Slit Experiment

- Questions:
  - How does the Photon know where to end up?
  - If there is interference, what does the Photon interfere with?
  - Why does trying to detect what is happening affect the outcome?
- There are many different *Quantum Theory Interpretations* which scientists 100 years after the discovery of quantum nature of light are still arguing about .

# Quantum Theory Interpretation

- Quantum Theory Interpretations try to *explain* what is happening
  - Copenhagen Interpretation
  - Instrumentalist - “Shut up and calculate!”
  - Others …
  - The Many Universes Interpretation (Multiverse)
- They don’t have to be true. They only have to be consistent.

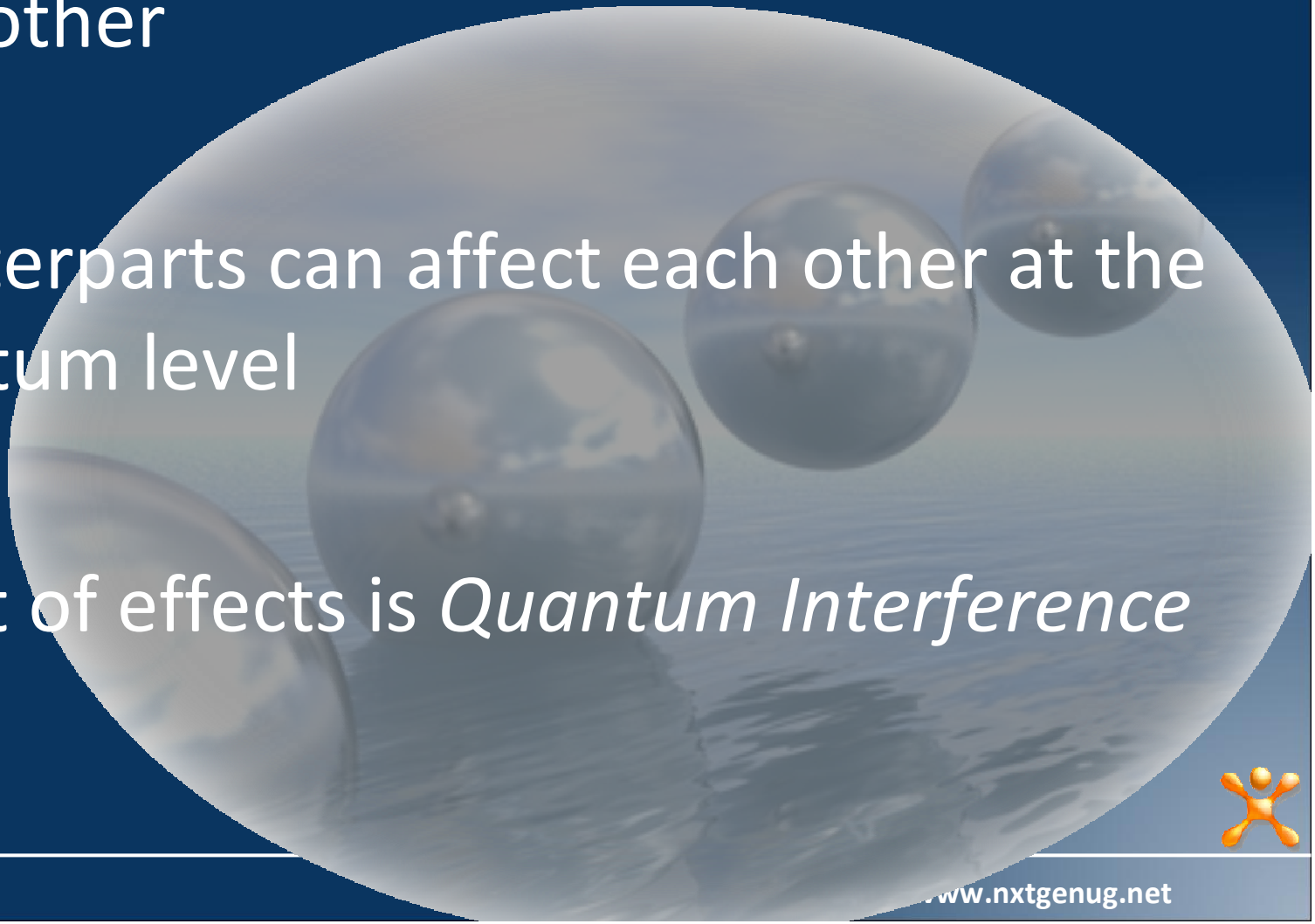
# The ‘Multiverse’

We are aware of only a part of reality

Every object in a universe has a counterpart in another universe

# The ‘Multiverse’

- Counterparts can behave differently from each other
- Counterparts can affect each other at the Quantum level
- Result of effects is *Quantum Interference*



# The ‘Multiverse’

- Across the multiverse, the photon goes through both slits at the same time a phenomenon known as *Superposition*
- The Photons experience *Quantum Interference* with each other between universes
- The final resulting  pattern is a interference pattern across the Multiverse.

# The QuBit

## A Multiversal Object

# The QuBit


The Quantum World
Superposition
Quantum Interference
QuBit

# The QuBit

- Physicists measure *Expectation* Values of Quantum Systems or Observables
- Expectation Values of Quantum Observables are:
  - The average outcome of a measurement repeated many times or ...
  - The average outcome of a measurement performed on many copies of a system over a region of the Multiverse.
- If a Quantum System has Observables which are all defined in terms of Boolean Values that system can be termed a QuBit.

# The QuBit

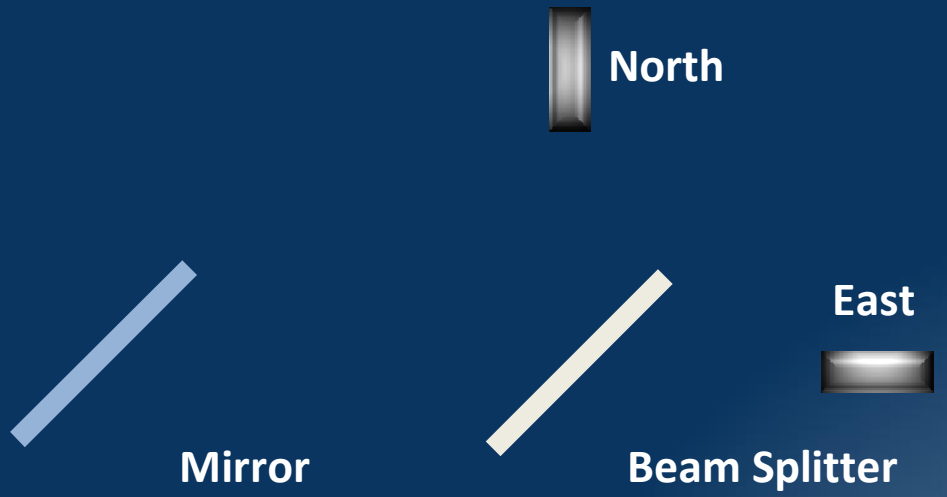
- A Bit : A classical system which can take one of two values – one or zero
- A Boolean Observable: A Quantum Observable whose spectrum contains two values and which can be either or both values simultaneously.
  - Sharp (Same Value in all Universes)
  - Non-Sharp (Superposition)
- A QuBit : A physical system, each of whose non-trivial observables is Boolean

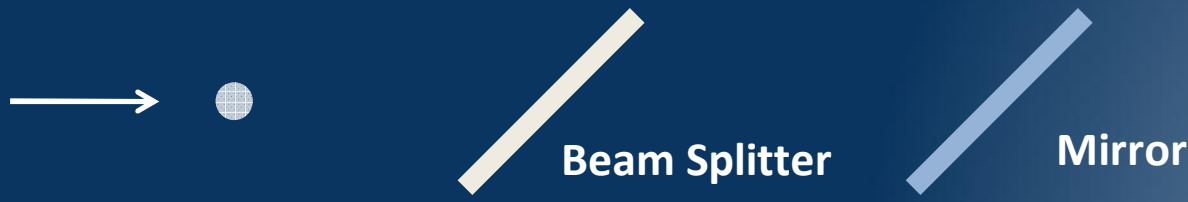
# A Single QuBit System

# A Single QuBit System

An observable ‘Z’ is deemed to be -1 when going to the North Direction and 1 when going in the East Direction. <Z(t)> is the Expectation (Average) Value being measured.

| Time | <Z(t)> |
|---|---|
| 0 | 1 |
| | |
| | |
| | |

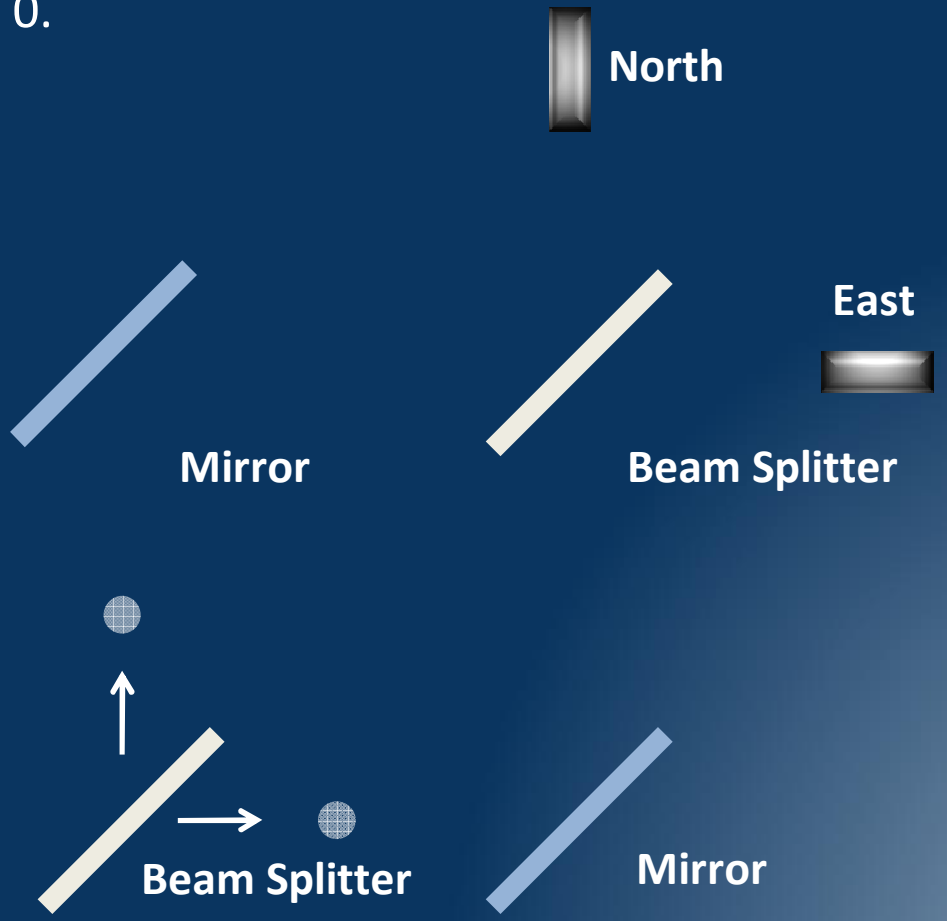


# A Single QuBit System

At Time 1 the Observable ‘Z’ is in SuperPosition with the photon going in both the North Direction and the East Direction in Different Universes. The Expectation Value of Z(t) is therefore 0.

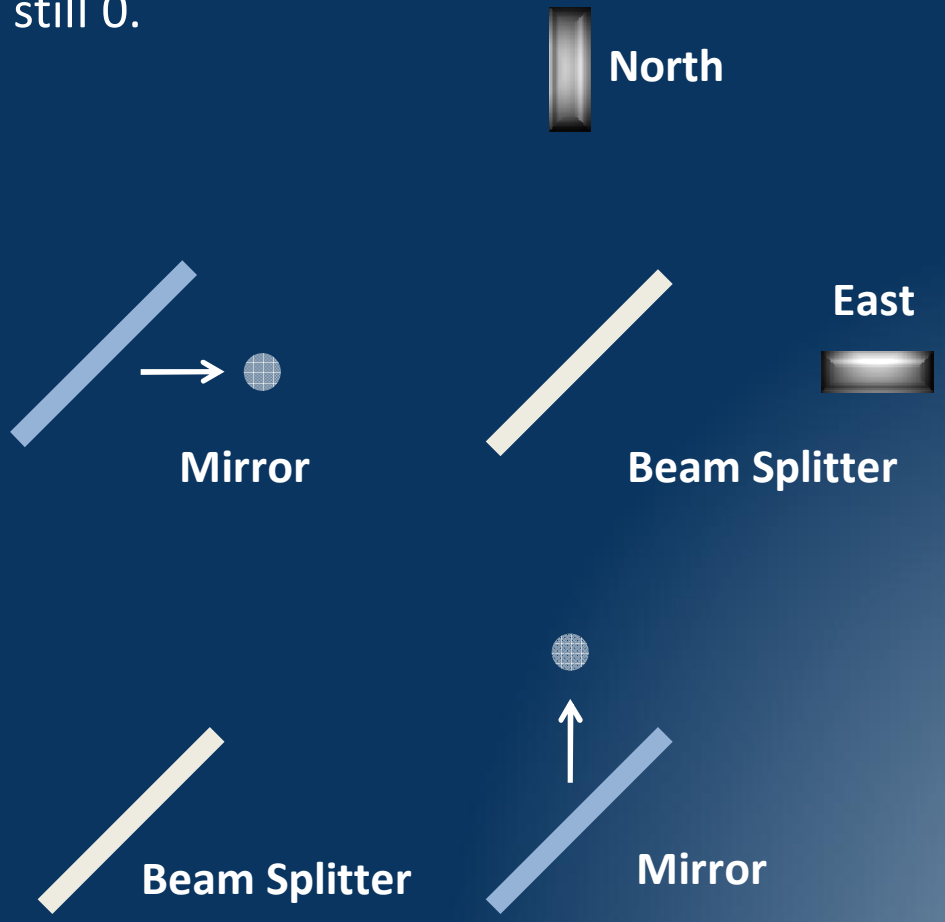
| Time | <Z(t)> |
|---|---|
| 0 | 1 |
| 1 | 0 |
| | |
| | |



# A Single QuBit System

At Time 2 the Observable ‘Z’ is in SuperPosition with the photon going in both the East Direction and the North Direction in Different Universes. The Expectation Value of Z(t) is therefore still 0.

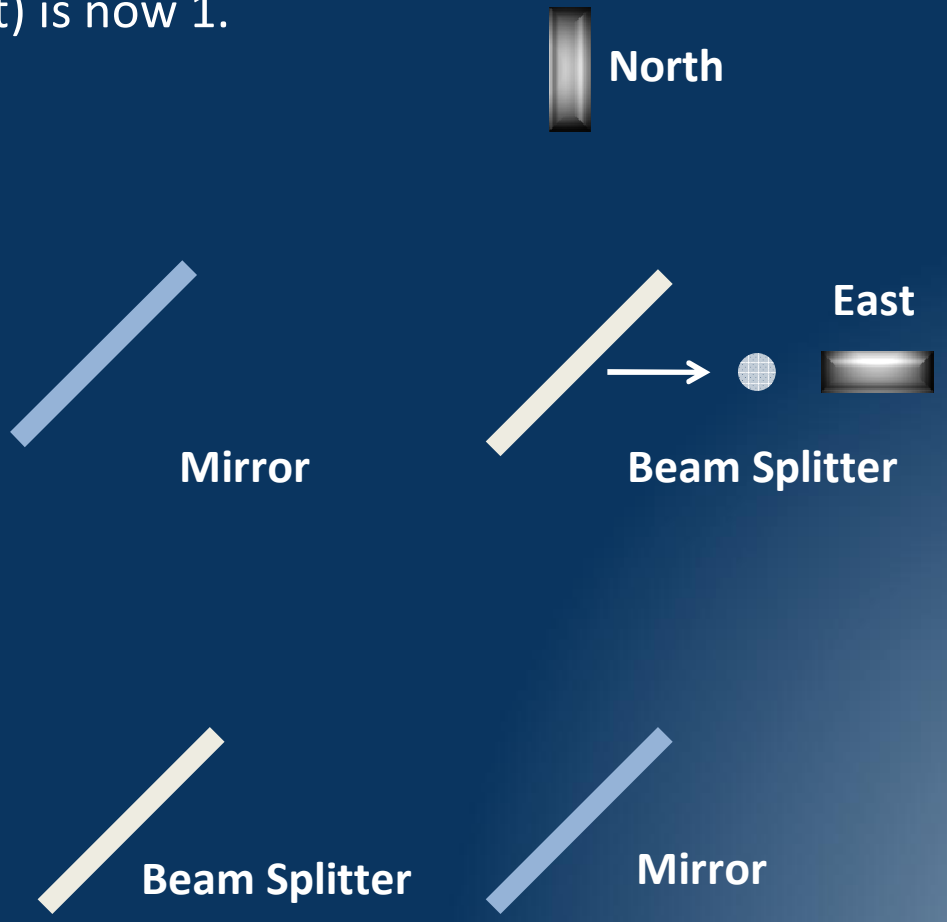
| Time | <Z(t)> |
|---|---|
| 0 | 1 |
| 1 | 0 |
| 2 | 0 |
| | |



# A Single QuBit System

Theoretical predictions backed up by experimental observations show that the East detector always picks up the Photon and the North Detector never does. So the Expectation value Z(t) is now 1.

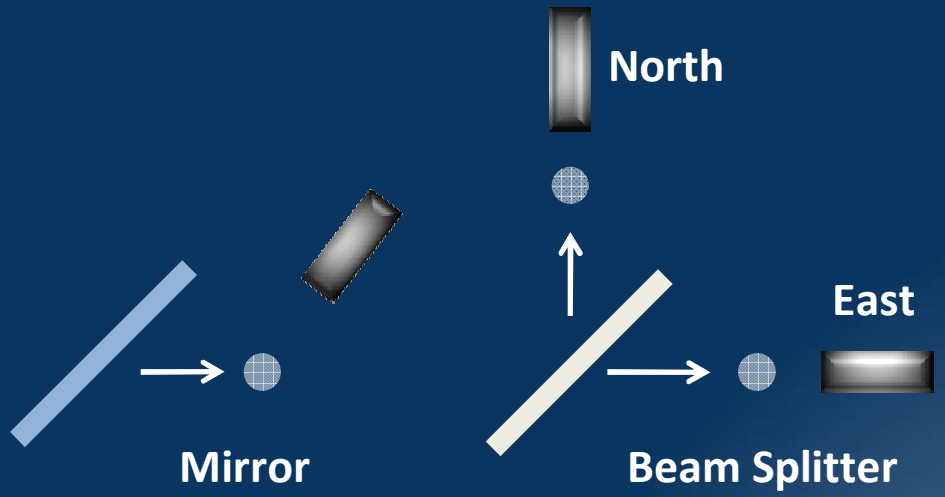
| Time | <Z(t)> |
|---|---|
| 0 | 1 |
| 1 | 0 |
| 2 | 0 |
| 3 | 1 |



# A Single QuBit System

Any attempt to determine an intermediate state results in a final expectation value for Z(t) of 0. In this case photons appear at both detectors.

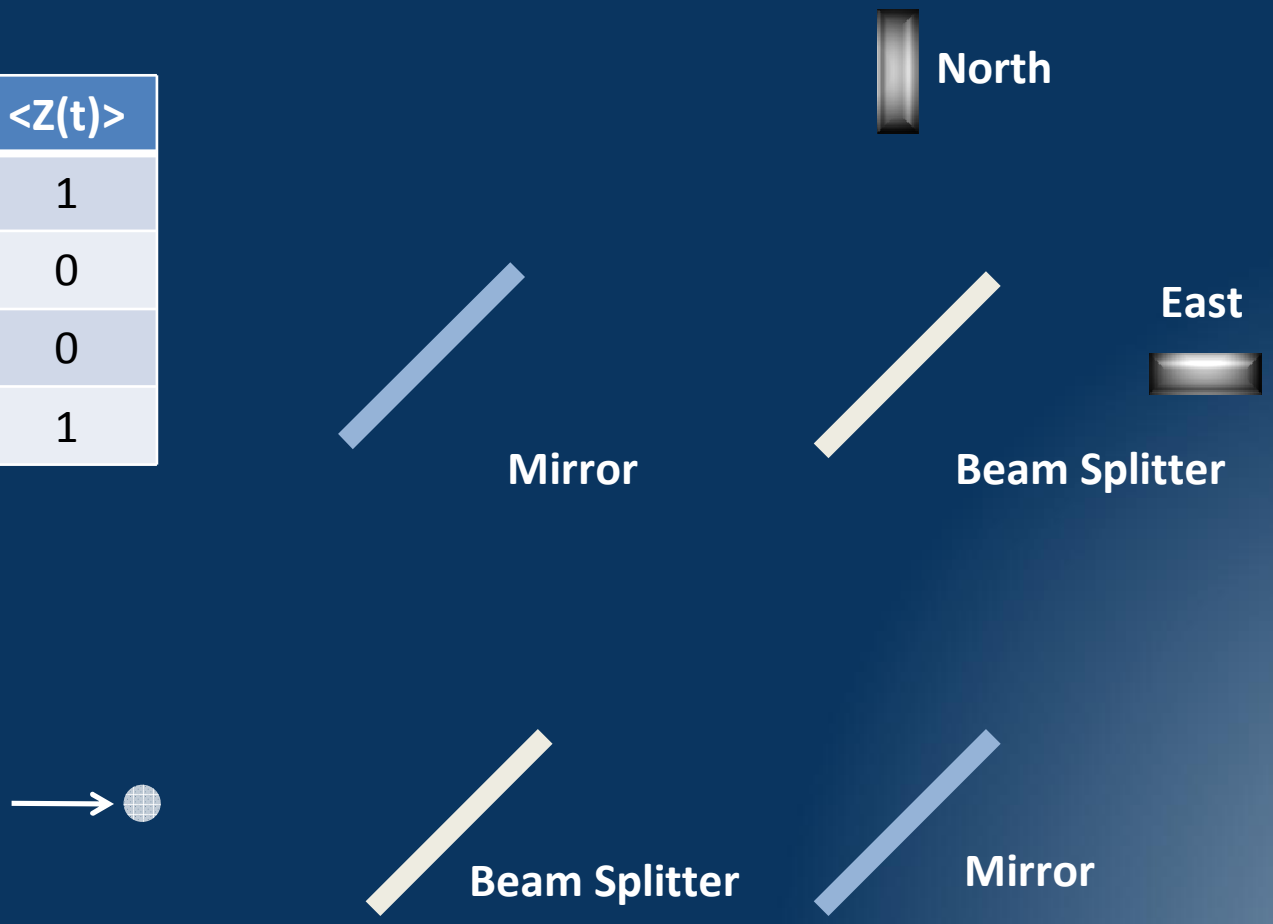
| Time | <Z(t)> |
|---|---|
| 0 | 1 |
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |



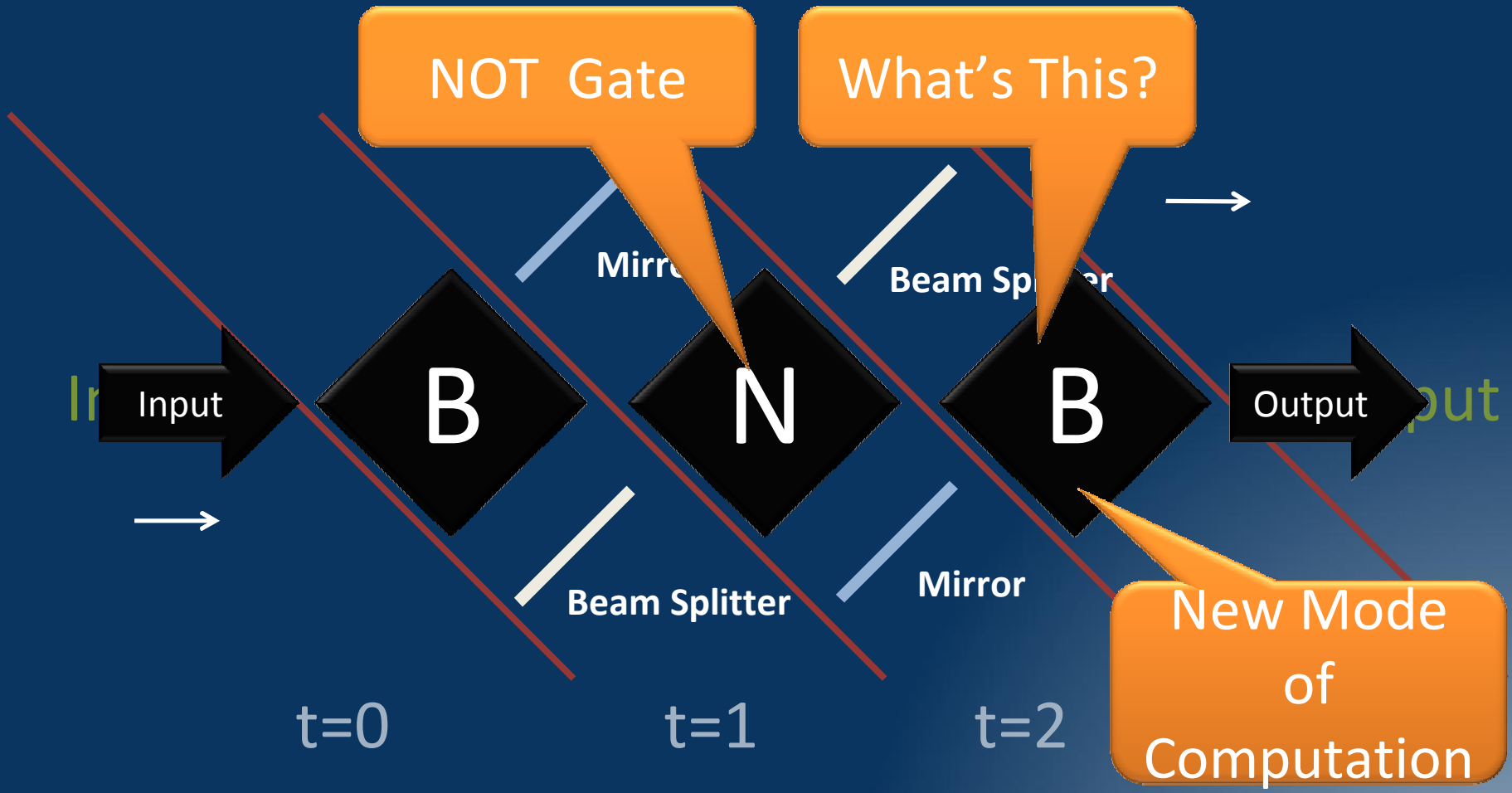

# A Real QuBit

This is how a system can use a single QuBit to measure a specific value of -1 or 1.

| Time | <Z(t)> |
|---|---|
| 0 | 1 |
| 1 | 0 |
| 2 | 0 |
| 3 | 1 |



# A Real QuBit




Operation is Unit Operator

# Quantum Computations are Reversible

WARNING!

Severe Scientific Reasoning Break ...

# Quantum Computations are Reversible

- Gates represented by unitary matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} or \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} or \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} or \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

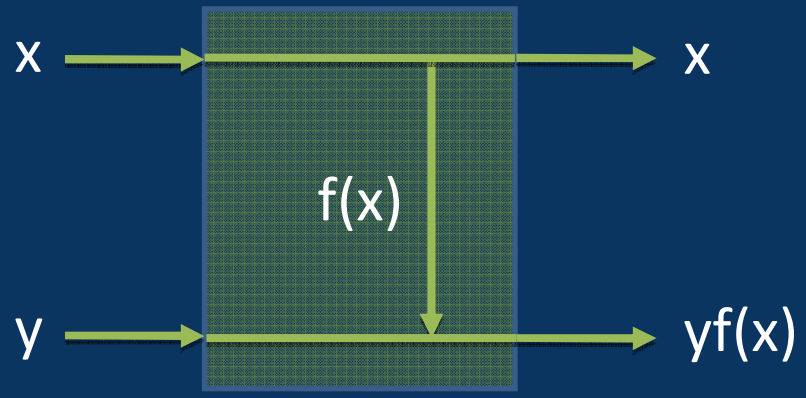
- All unitary matrices have inverse matrices that are also unitary
- … so all quantum gates are reversible …
- … gates represent computations …
- … so all quantum computations are reversible.

# Quantum Computations are Reversible

END OF

Severe Scientific Reasoning Break ...

# Quantum Computations are Reversible




- Must have same number of outputs as inputs
- Must preserve the original input
- Copies the result to the ‘control’ QuBit

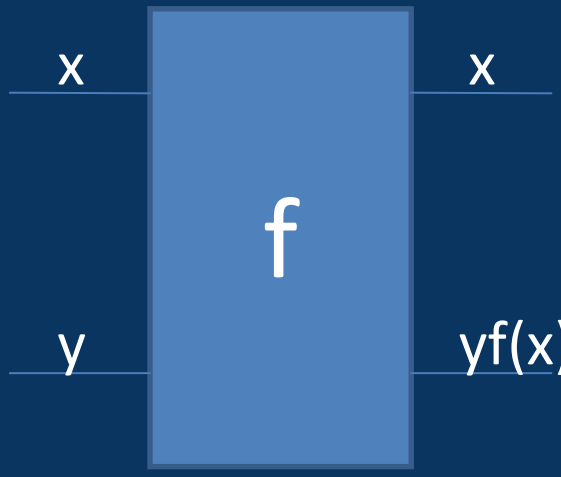
# A Basic Quantum Algorithm

# A Basic Quantum Algorithm

- A Program is a way of preparing a computer to carry out a Computation
- A Computation is a problem to which an Algorithm is a solution
- An Algorithm is a Hardware-independent specification of a Computation

# A Basic Quantum Algorithm

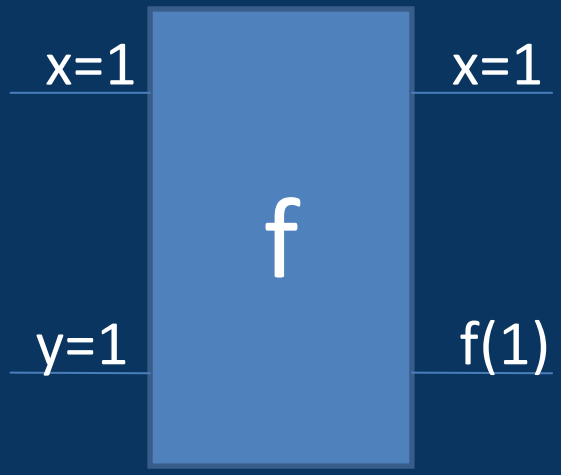
Question: Can we find out what the Boolean function f(x) is without looking inside the Black Box?

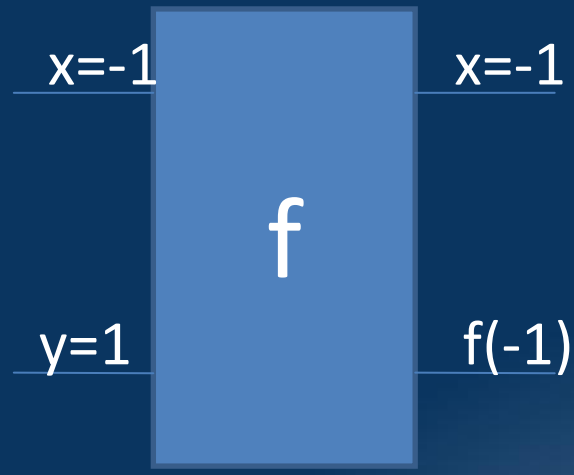



f(x) = 1 OR f(x) = -1

- Unit Operator
- NOT Operator
- Constant 1
- Constant -1

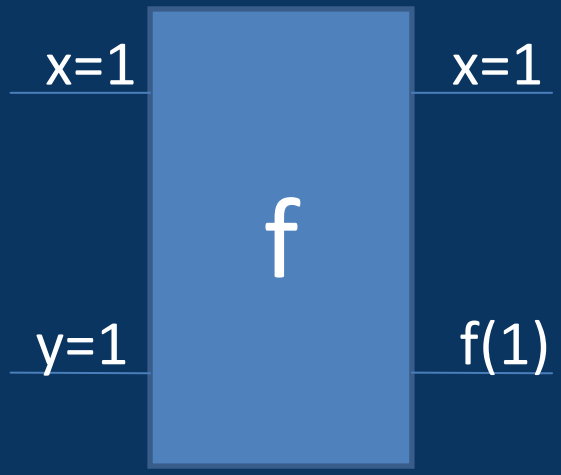
# A Basic Quantum Algorithm

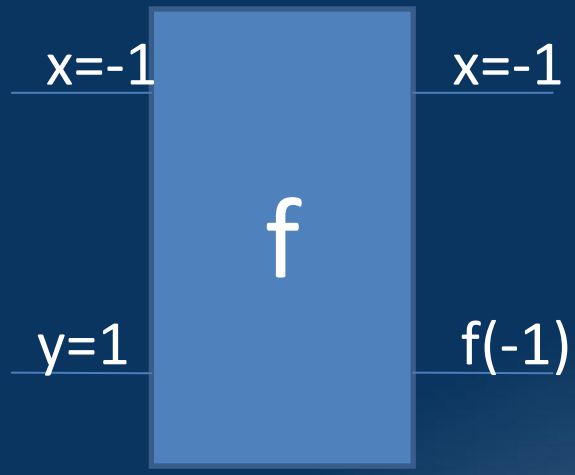



- Must Run System Twice
- True for both classical and quantum versions

# A Basic Quantum Algorithm




- What about does f(1) = f(-1)?
- Same as f(1)f(-1)
- Classically we must still run the system twice.

# A Basic Quantum Algorithm


- We prepare our two inputs using a NOT Gate
- We put our QuBit into a State of Superposition using Hadamard Gate (Superposition state represented by |1>|-1>)
- Run the Calculation f
- f(|1>)(f|-1>) appears in ONE run of the system
- Demonstrates *Quantum Parallelism*

# A Quantum Search Algorithm

# A Quantum Search Algorithm

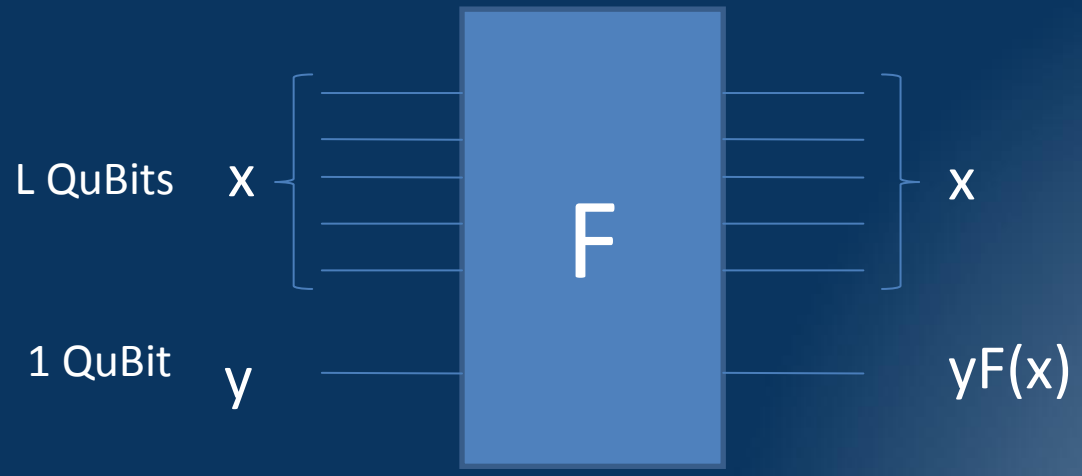
- Exhaustive Search Algorithm
- Example in C# Programming Language

```
public Boolean Is151InAList(Ilist<Int32> aList)
{
    for (Int32 i=0 ; i < aList.Count() ; i++)
    {
        if (aList[i] == 151) {return true;}
    }
    return false;
}
```

- Classically this would take on average half the number of items in the list i.e N/2. It could take N-1 times.

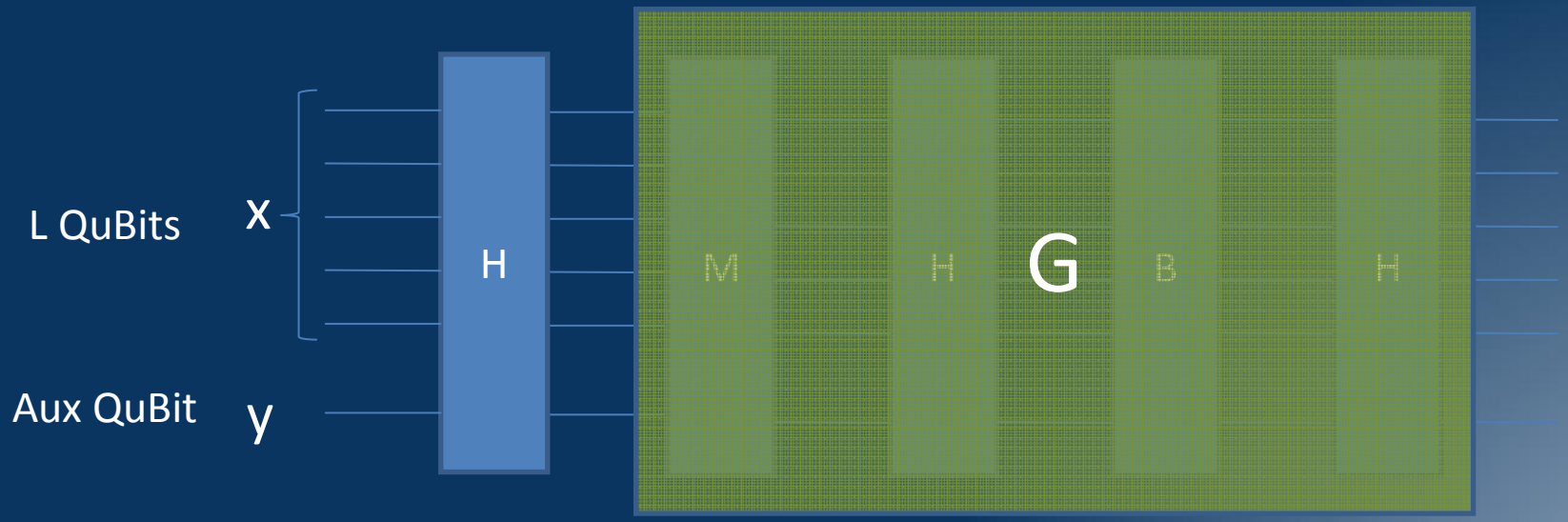
# A Quantum Search Algorithm

- F(x) is -1 when X is the searched for value
- F(X) is 1 when X is not the searched for value.
- X is in the range 0 -> N where $N = 2^L$



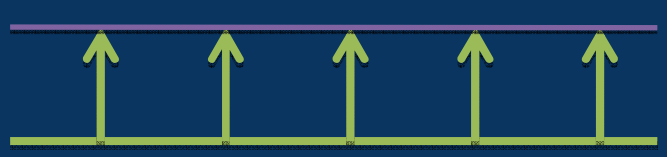
# A Quantum Search Algorithm

- H puts L QuBits in Superposition
- Place four Quantum Gates M H B H in succession
- MHBH is the Grover Operator



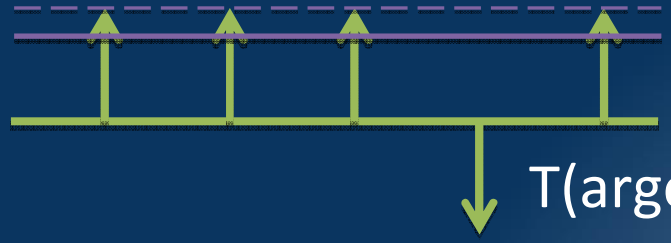
# A Quantum Search Algorithm

Superposition State (H)

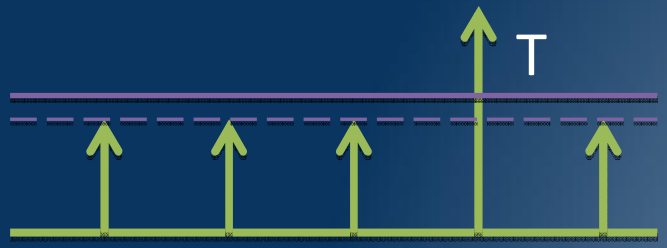



## The ‘Grover Operator’

Mark Target (M)

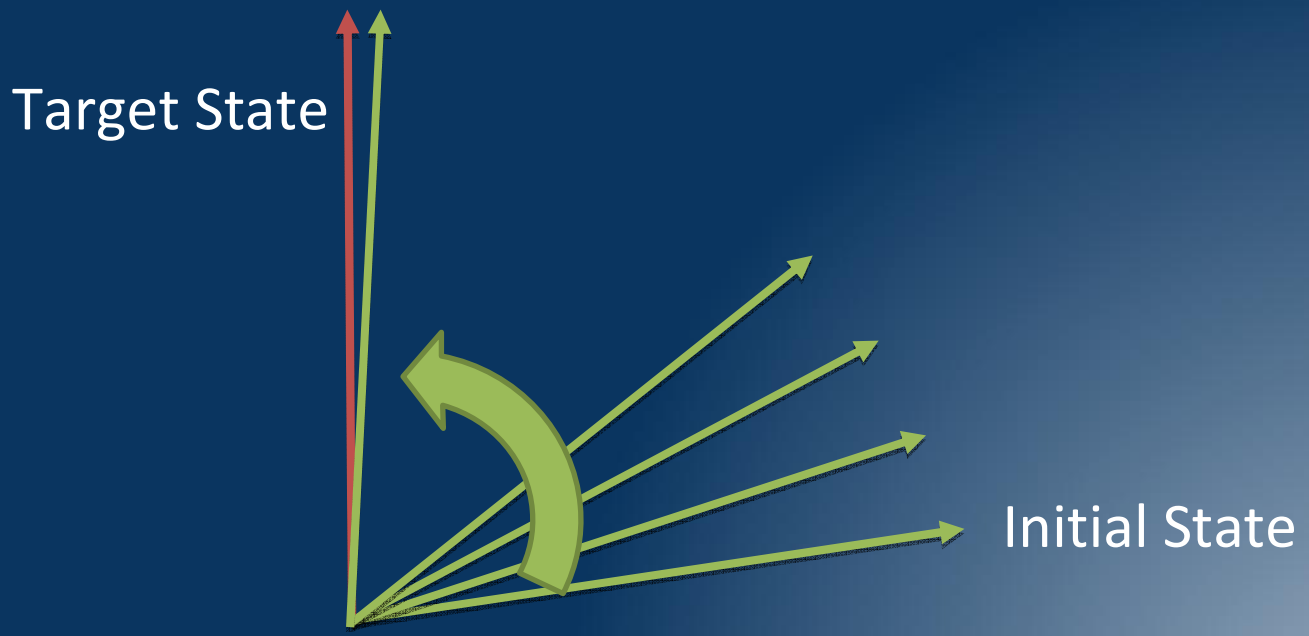



Grover
Diffusion Operator (HBH)
(Invert about Average)



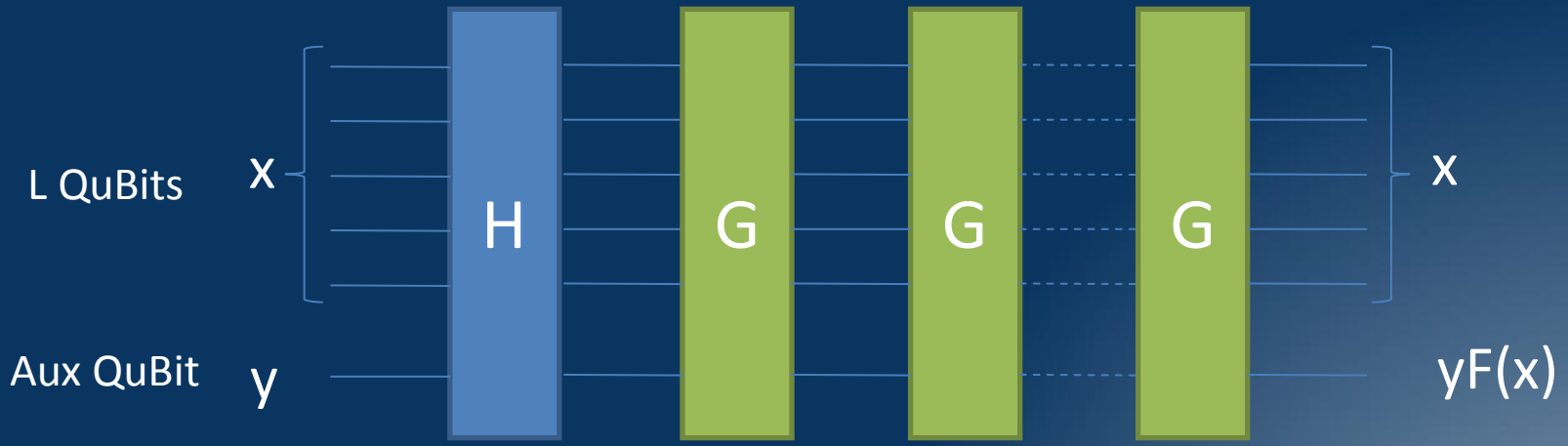
# A Quantum Search Algorithm

- Consider the combined QuBit states as a vector
- The Grover Operator rotates vector towards target



# A Quantum Search Algorithm

- Grover Search Algorithm = Hadamard Gate + Repeated Grover Operators.
- Maths shows ~ √N Grover Operations needed



# A Quantum Search Algorithm

At 100 million Grover operations per second

Searching $10^{30}$ items

~4 months

# A Quantum Search Algorithm

At 100 million Classical Operations per second

Searching $10^{30}$ items

~Age of Universe

# A Quantum Search Algorithm

Using a Quantum Computer you would be running $10^{30}$ operations in parallel.

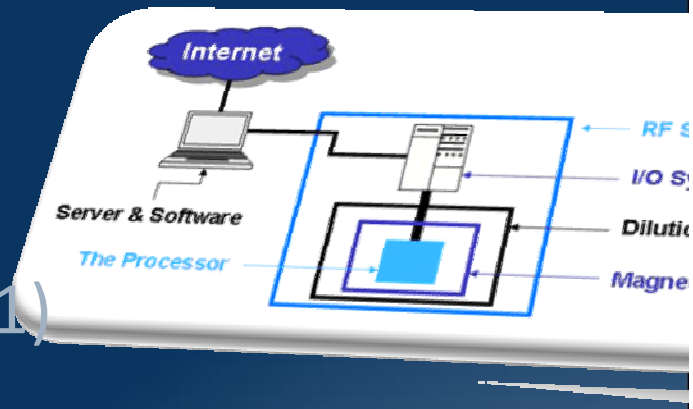
That's more operations than if you took all the Silicon on Earth and made it into transistors and ran them all in parallel!

# Finally …
# Quantum Computers Today

… back to reality …

# Quantum Computers Today

- Quantum Encryption Devices
  - http://www.magiqtech.com/
- University of Innsbruck
  - 14 Qubit Calculation (1 Apr 2011)
- D-Wave Machine
  - http://www.dwavesys.com
  - http://scottaaronson.com/blog
  - 128 Qubit calculation?



# Quantum Computers Today

# Summary

- We will reach a limit on current CMOS technology soon
- Quantum Computing makes use of the ‘Quantum  Multiverse’
- Trying to observe what happens destroys Quantum Interference
- Some known Quantum Algorithms will make certain intractable problems do-able
- A viable Universal Quantum Computer is yet to be built.

# A Quantum of Computing

## Qs & As

Thank You

Dave McMahon

dave@nxtgenug.net

@mcmahond

http://davemcmahon81.wordpress.com