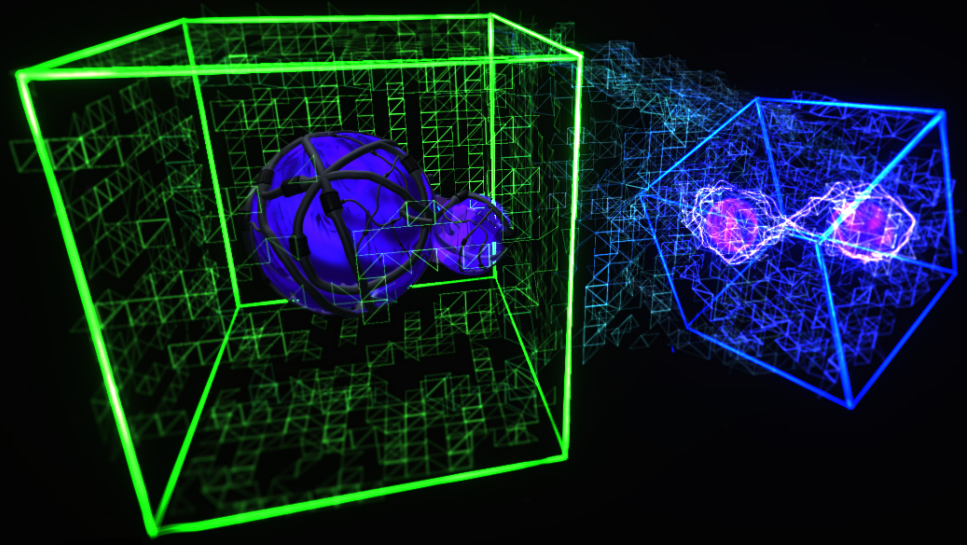
Welcoming a Quantum World

The Power of Quantum Information and Its Applications

Mile Gu



NANYANG TECHNOLOGICAL UNIVERSITY
Complexity Institute

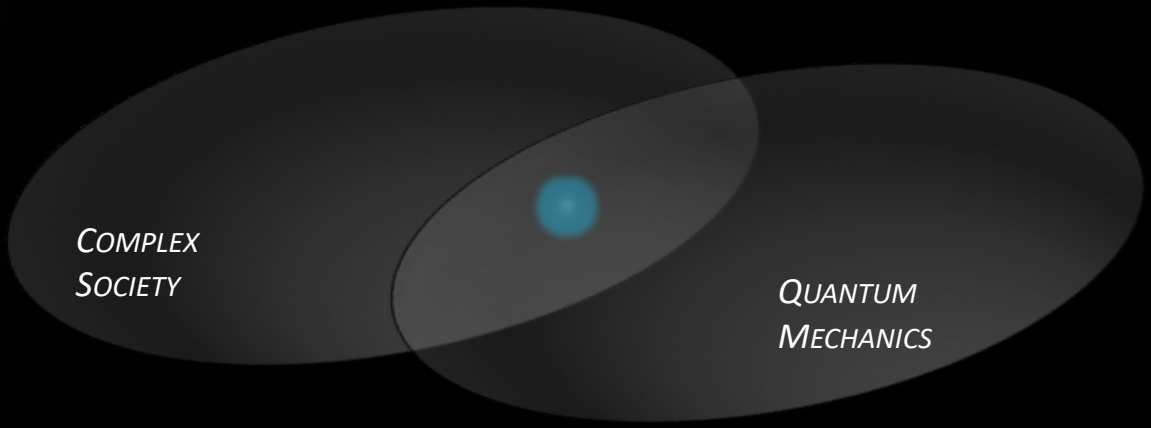
John Templeton Foundation

Centre for Quantum Technologies
National University of Singapore

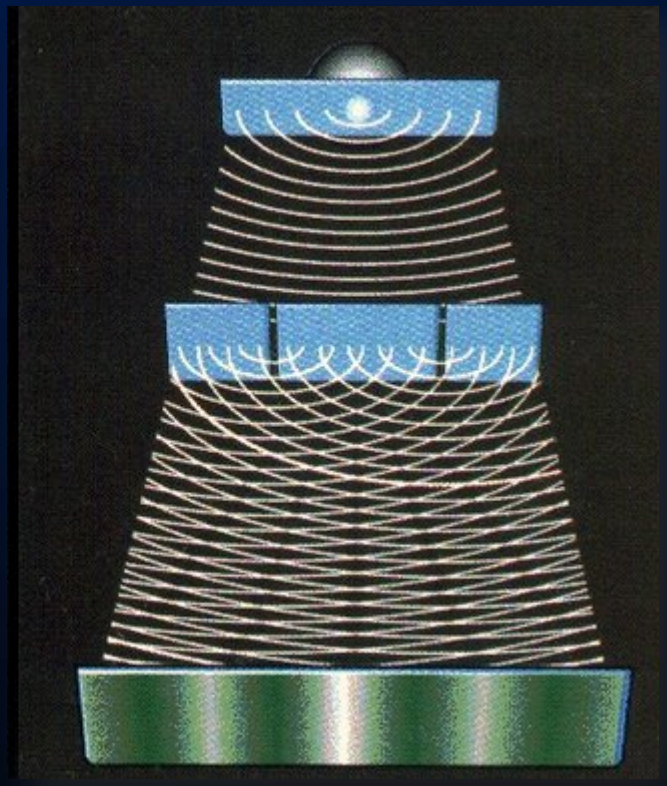
Welcoming a Quantum World

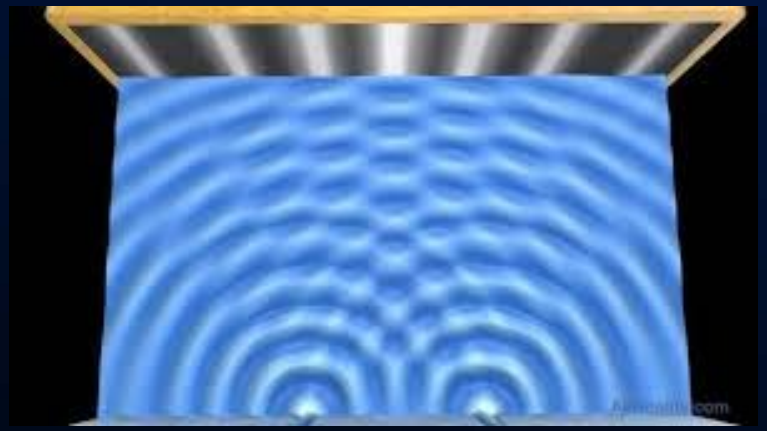
The Power of Quantum Information and Its Applications

Mile Gu

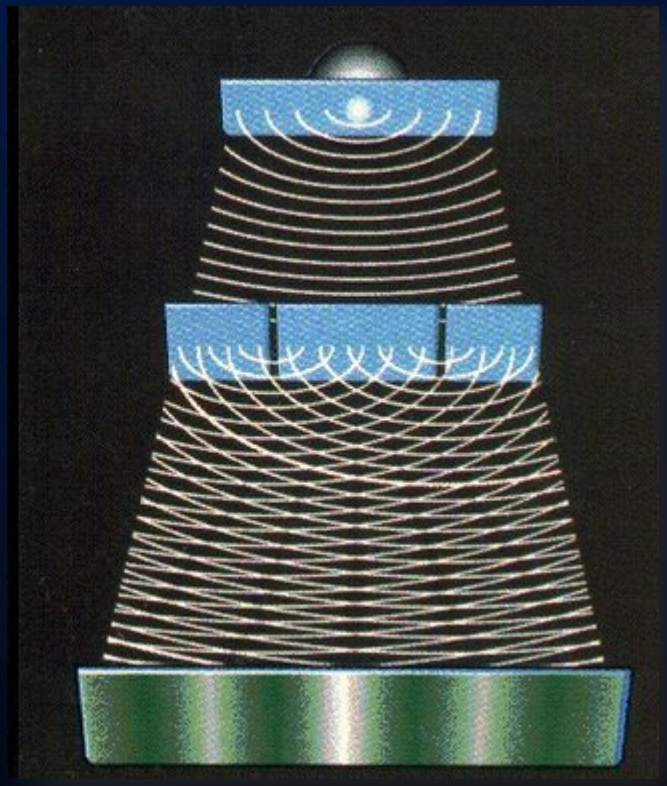


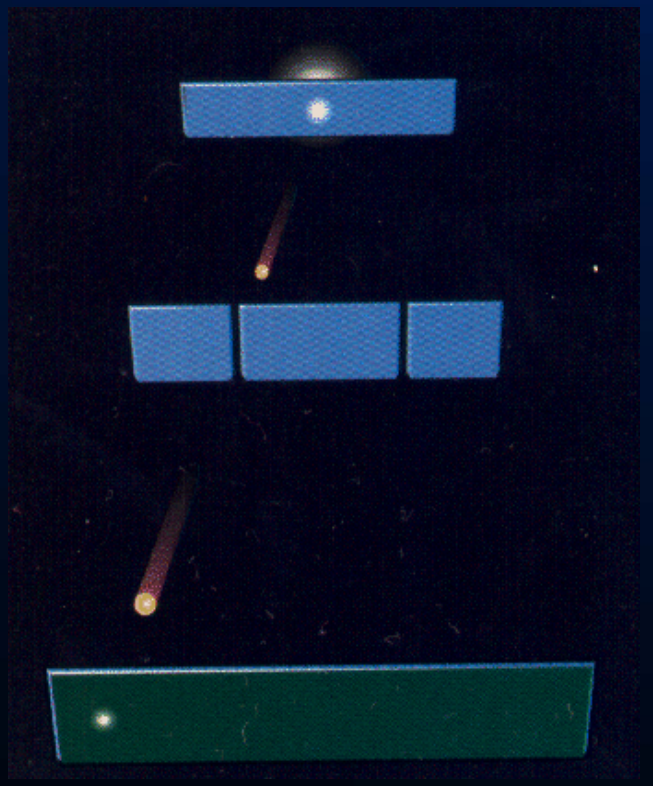
The Double Slit Experiment...



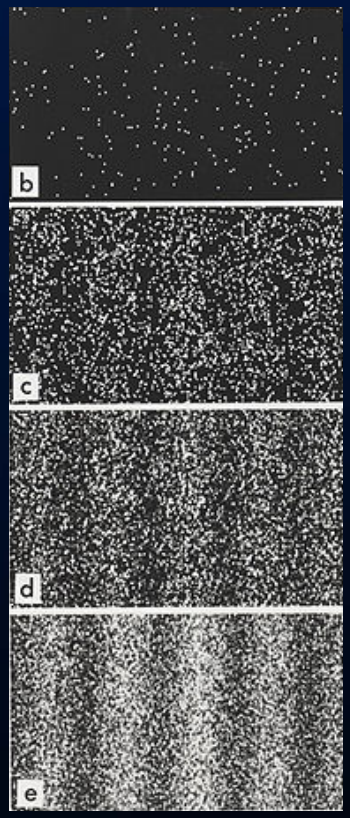


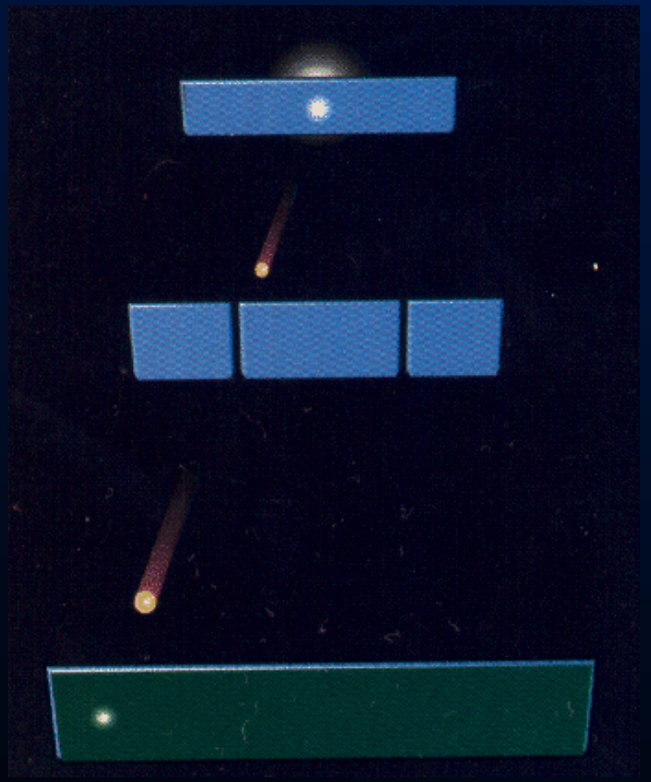
The Double Slit Experiment...





The Double Slit Experiment...





Davisson, C. J.; Germer, L. H. *Proceedings of the National Academy of Sciences, 1928*
Tonomura, Akira, et al. American Journal of Physics 57.2, 1989

In Quantum Science...

VOLUME 87, NUMBER 16 PHYSICAL REVIEW LETTERS 15 OCTOBER 2001

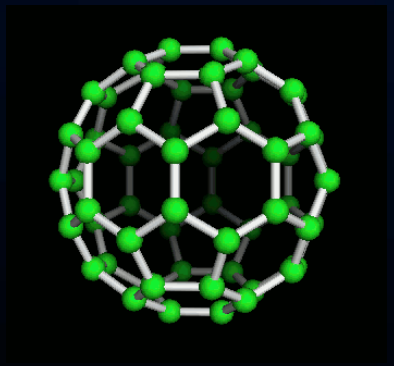
Diffraction of Complex Molecules by Structures Made of Light

Olaf Nairz, Björn Brezger, Markus Arndt, and Anton Zeilinger

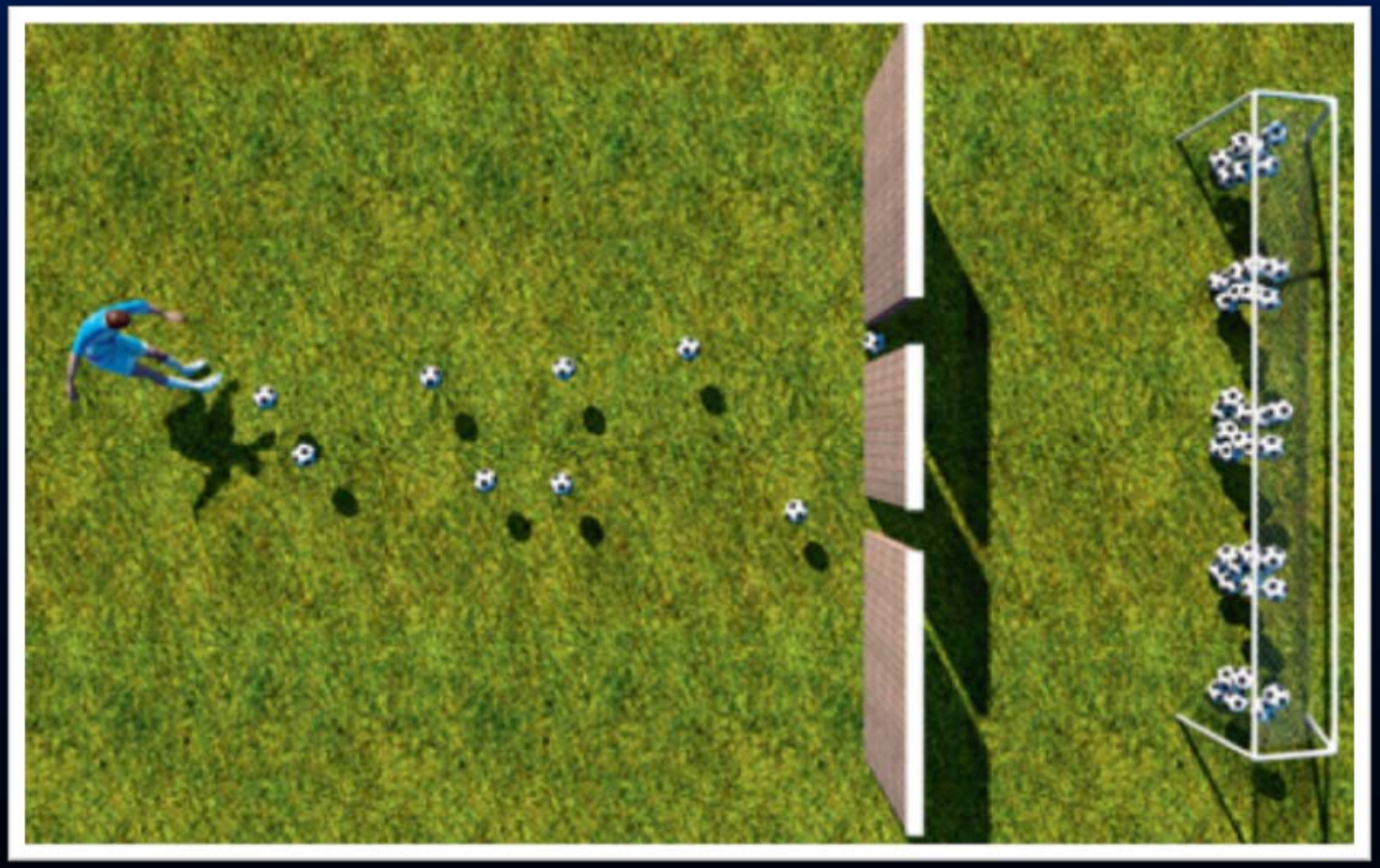
Universität Wien, Institut für Experimentalphysik, Boltzmanngasse 5, A-1090 Wien, Austria

(Received 1 June 2001; published 26 September 2001)

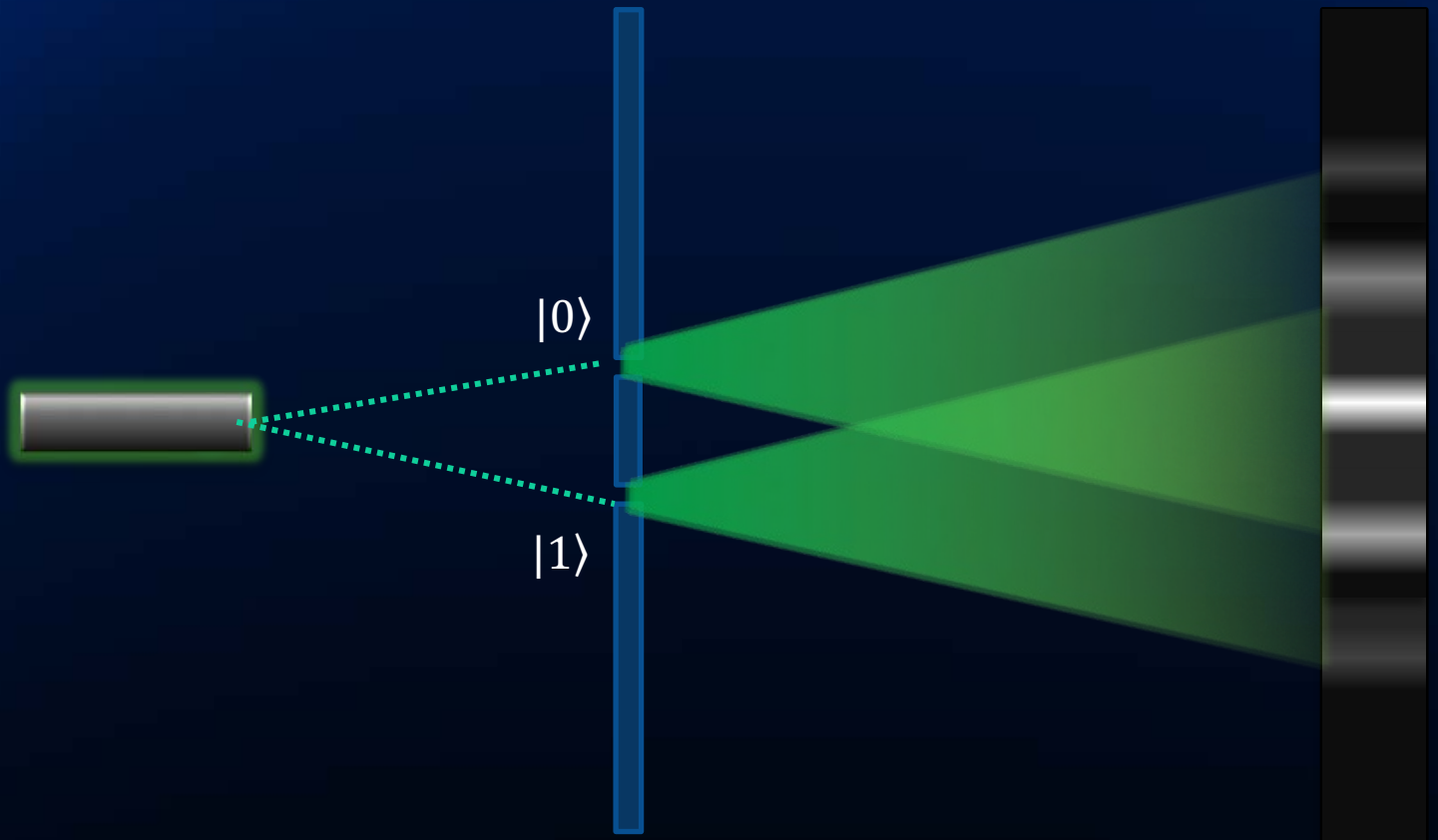
We demonstrate that structures made of light can be used to coherently control the motion of complex molecules. In particular, we show diffraction of the fullerenes C_{60} and C_{70} at a thin grating based on a standing light wave. We prove experimentally that the principles of this effect, well known from atom optics, can be successfully extended to massive and large molecules which are internally in a thermodynamic mixed state and which do not exhibit narrow optical resonances. Our results will be important for the observation of quantum interference with even larger and more complex objects.



The Double Slit Experiment...



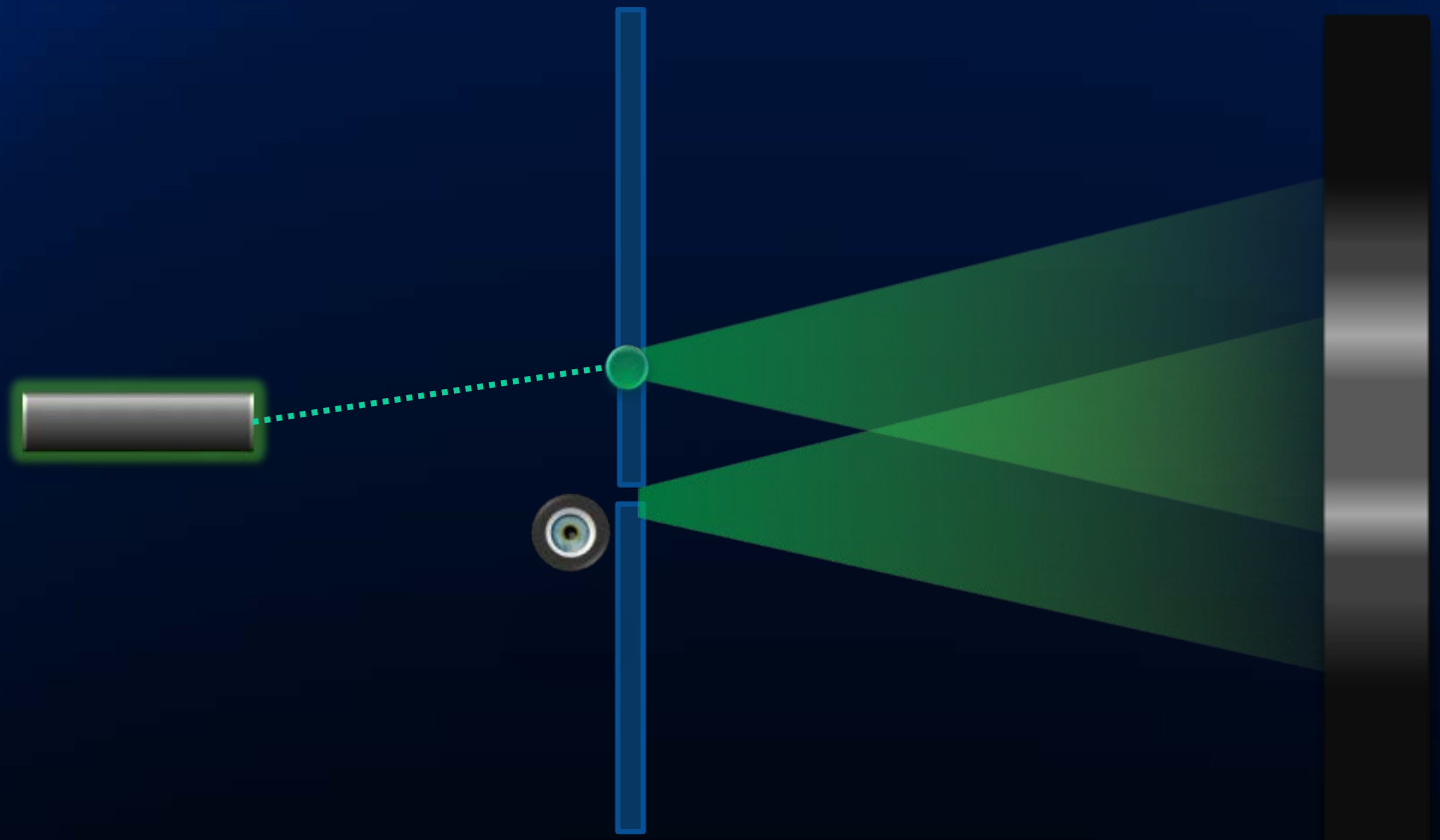
In Quantum Science...



$$|\varphi\rangle = |0\rangle + |1\rangle$$

A particle can go through a superposition of both slits!

In Quantum Science...



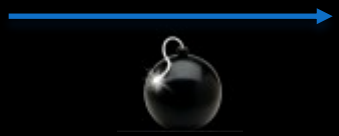
Measuring the particle position causes
Its quantum state to collapse

$$|0\rangle + |1\rangle \rightarrow |0\rangle$$

Quantum Bomb Detector:

We have a stockpile of Single-Photon activated bombs – but some of them are duds.

Good Bombs have photo-detectors that, when seeing a photon, explodes.



Bad bombs do not interact with photons

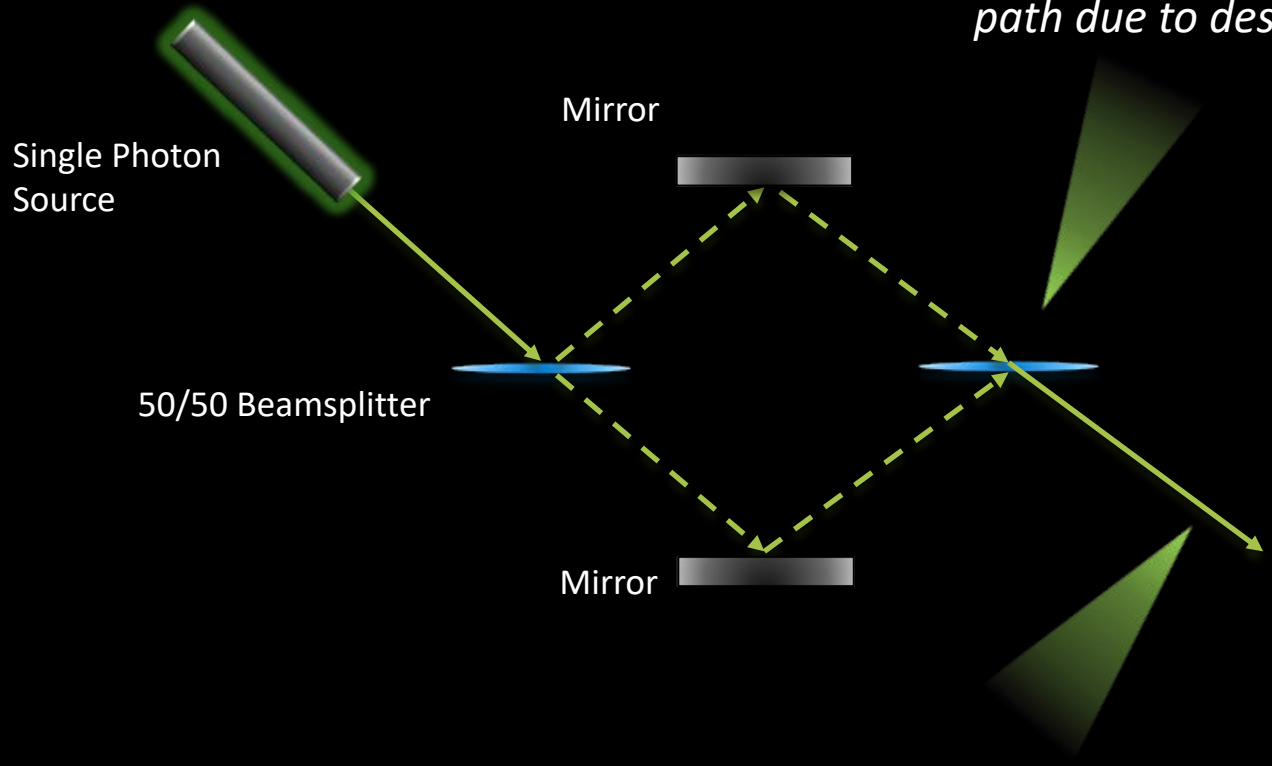
Elitzur, Avshalom C.; Lev Vaidman, *Foundations of Physics*. **23** (7): 987–997, 1993

Quantum Bomb Detector:

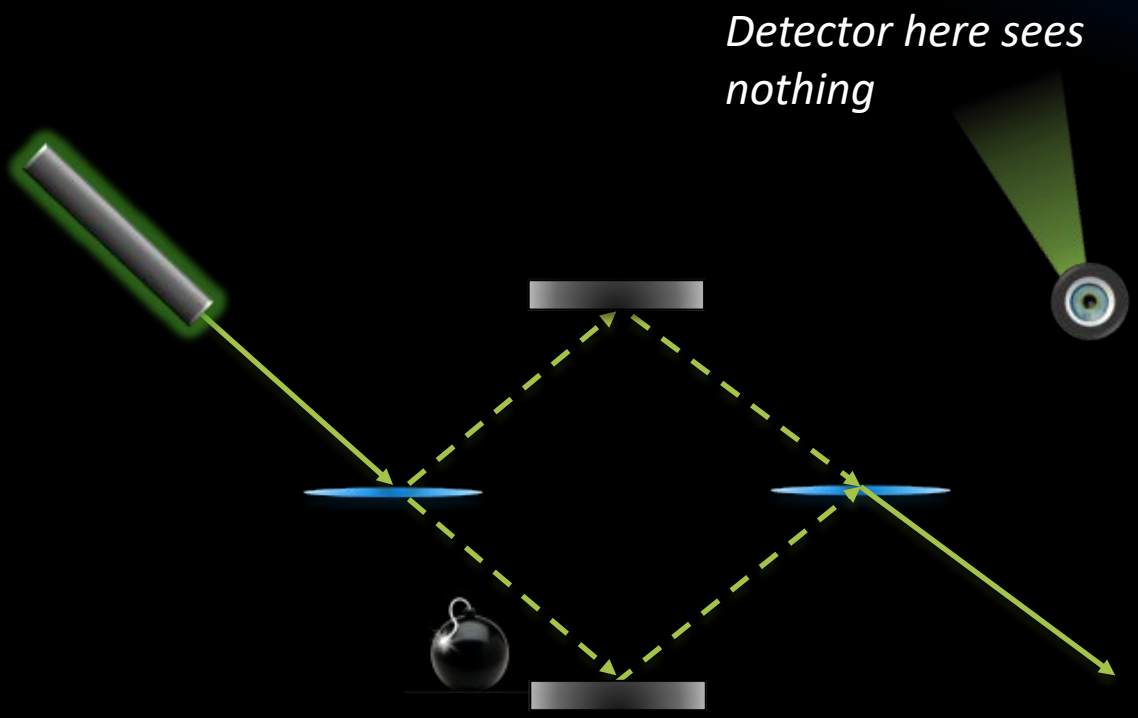
We have a stockpile of Single-Photon activated bombs – but some of them are duds.

How do we make sure every bomb works without blowing all of them in the process?

Quantum Bomb Detector:

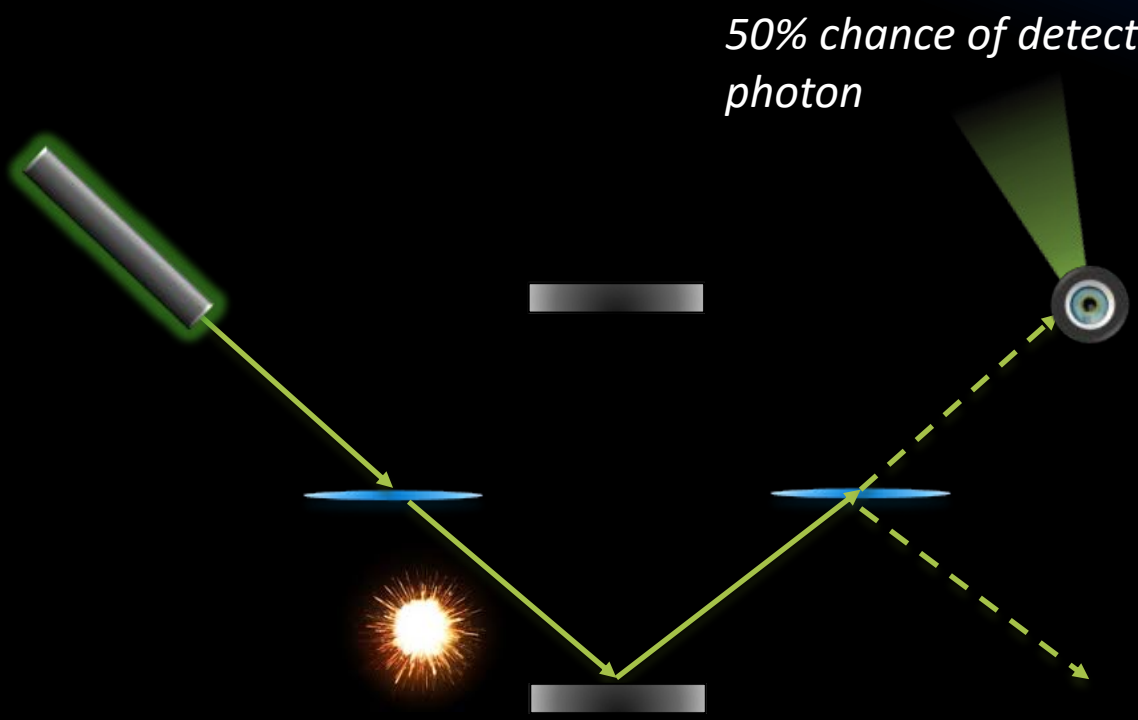


Quantum Bomb Detector:



A Dud will not affect this interference.

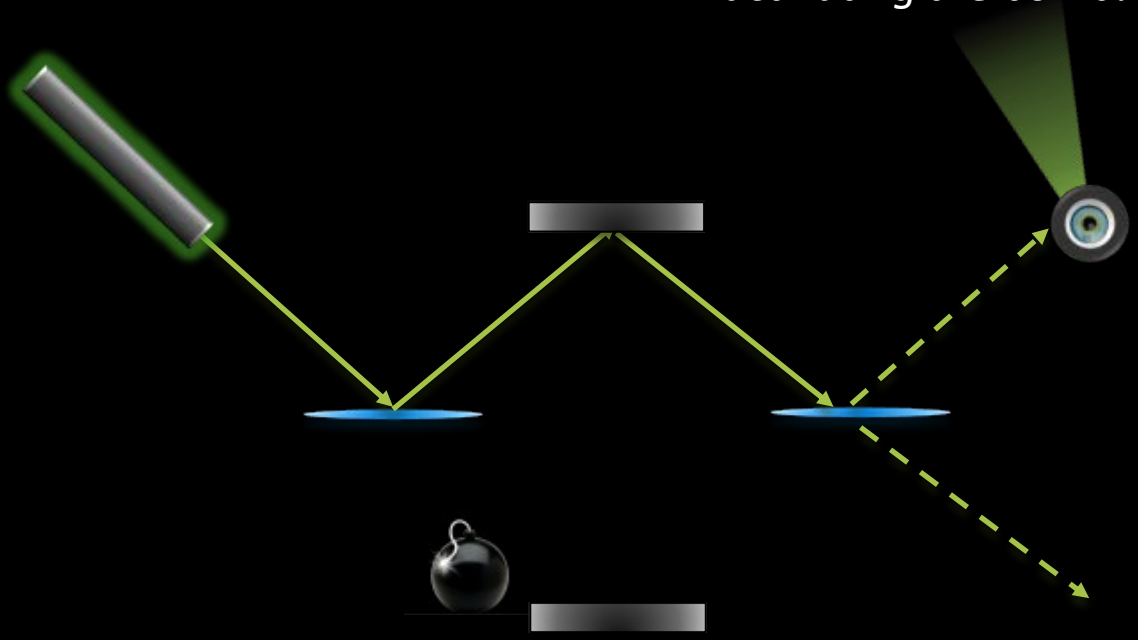
Quantum Bomb Detector:



A real bomb can detect photons, and thus destroys the interference pattern.

Quantum Bomb Detector:

Detecting a photon here will allow us to verify a Bomb works, without activating the bomb!



Seeing without Looking *- This interference pattern is still destroyed, even when the Bomb never interacts with the photon! (experimentally verified 1995)*

Kwiat, Paul, et al. *Annals of the New York Academy of Sciences* 383-393 (1995):

Abandoning Local Reality...

"Everything we call real is made of things that cannot be regarded as real. If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet."

- Niels Bohr

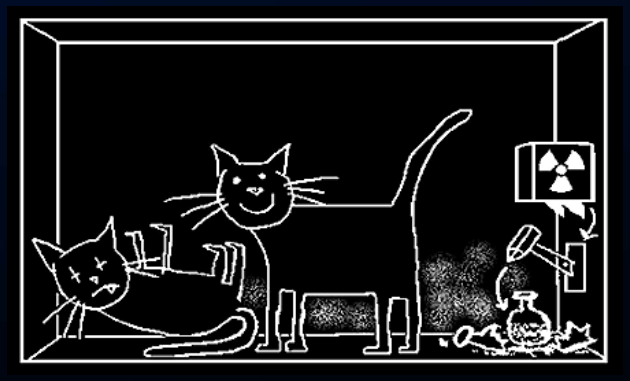
Quantum theory is not locally realistic

A system can exist in a superposition of different configurations.

Abandoning Local Reality...

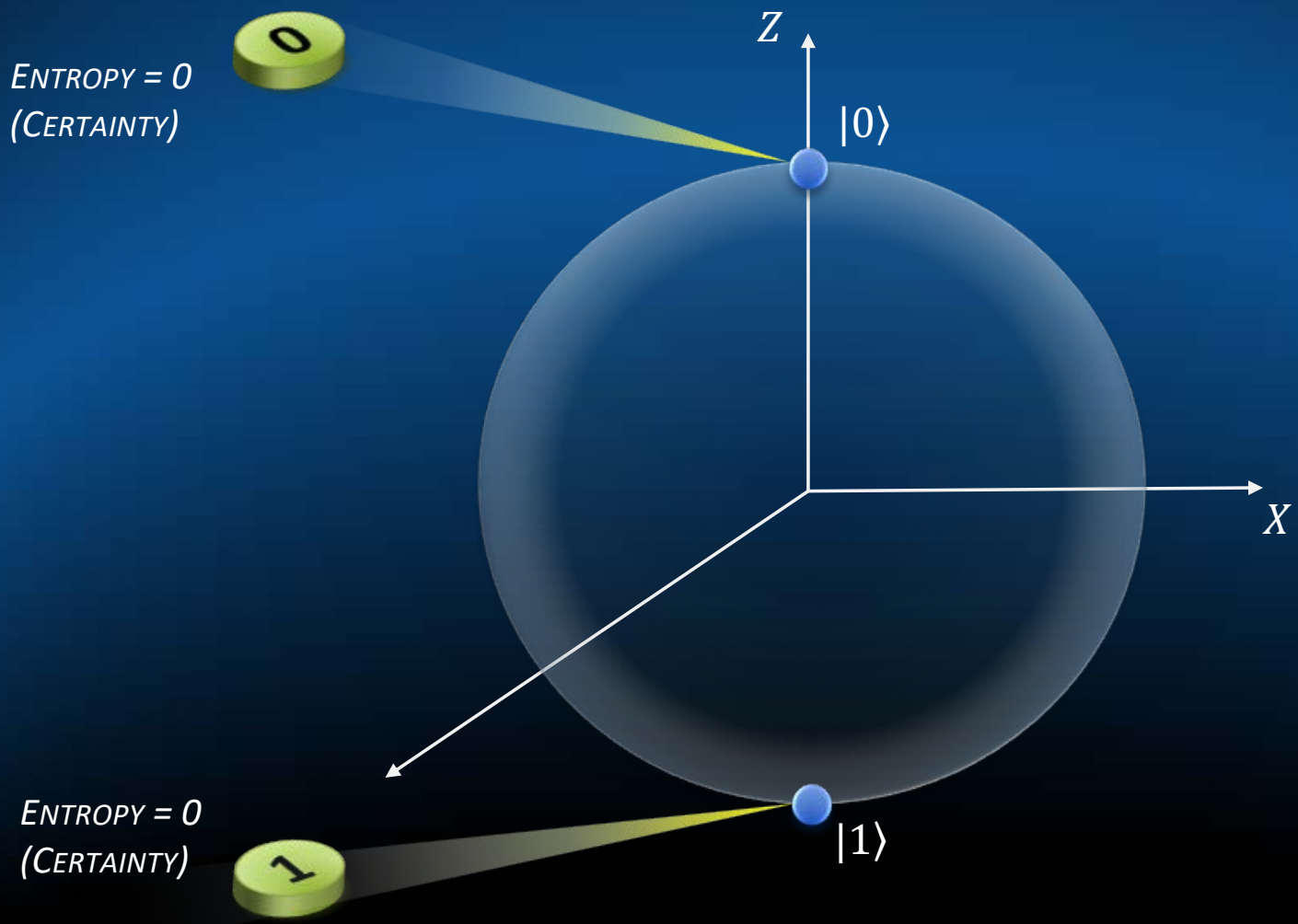
"Everything we call real is made of things that cannot be regarded as real. If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet."

- Niels Bohr

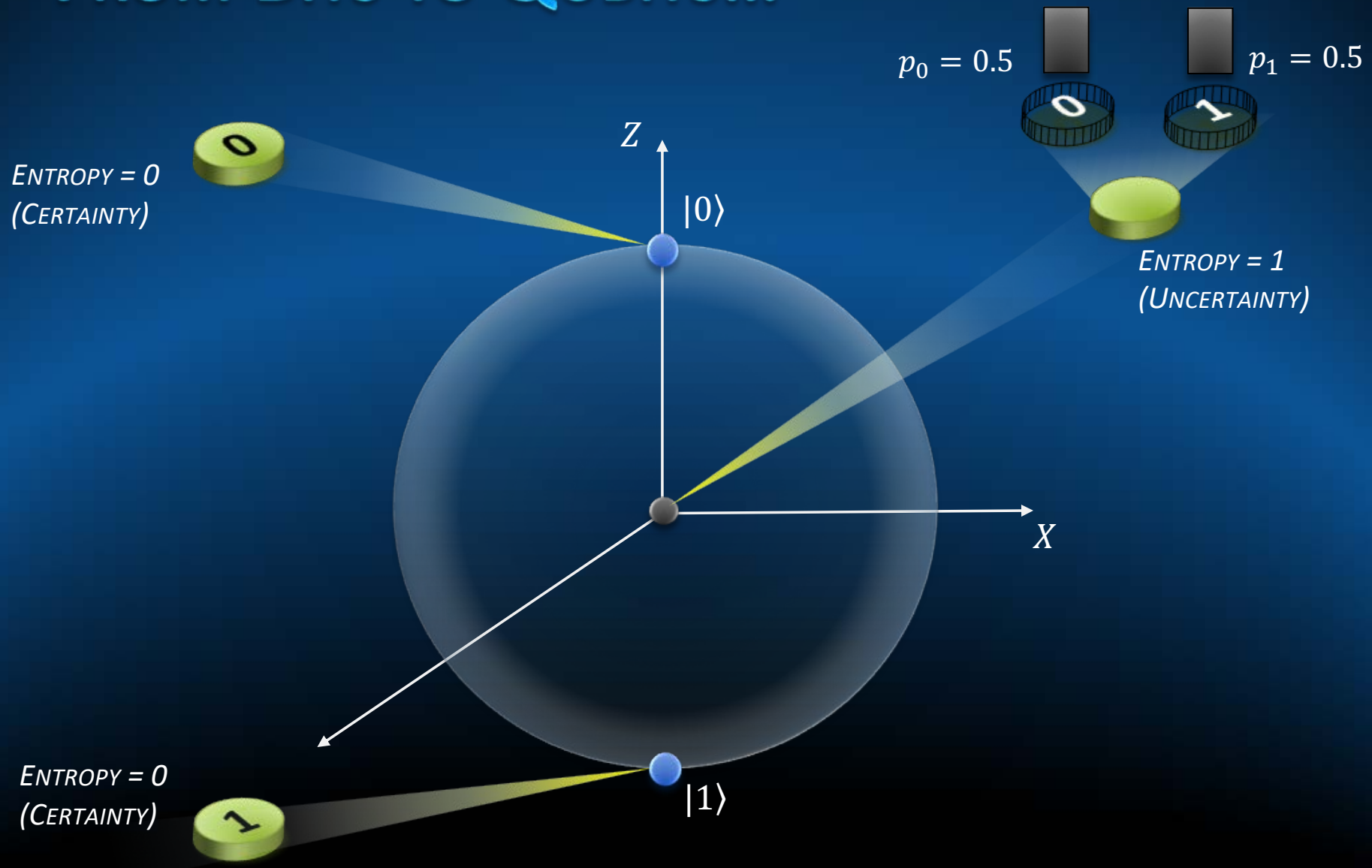


Schrodinger's Cat $|Dead\rangle + |Alive\rangle$

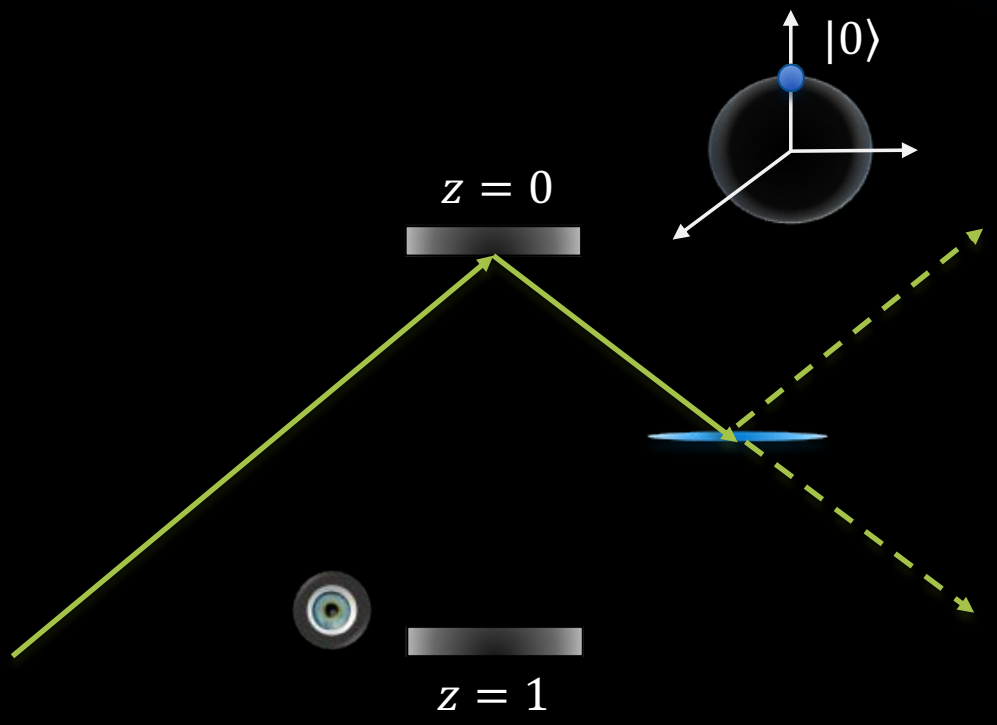
Anatomy of a bit



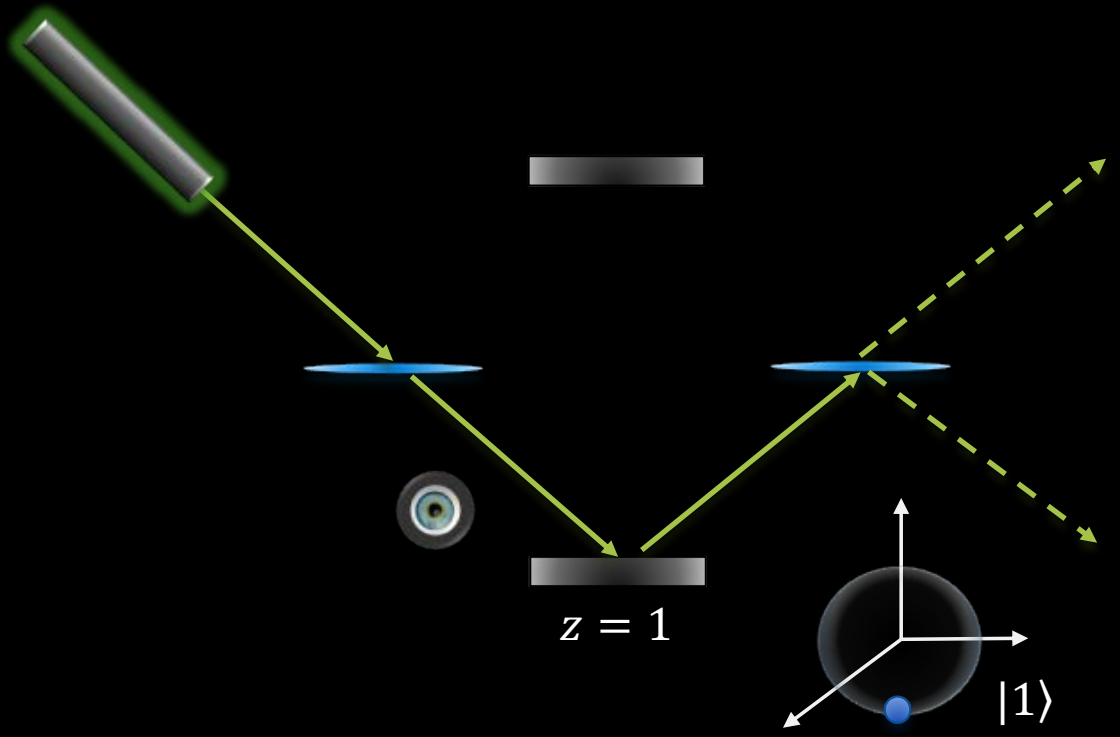
From Bits to Qubits…



BITS ILLUSTRATED

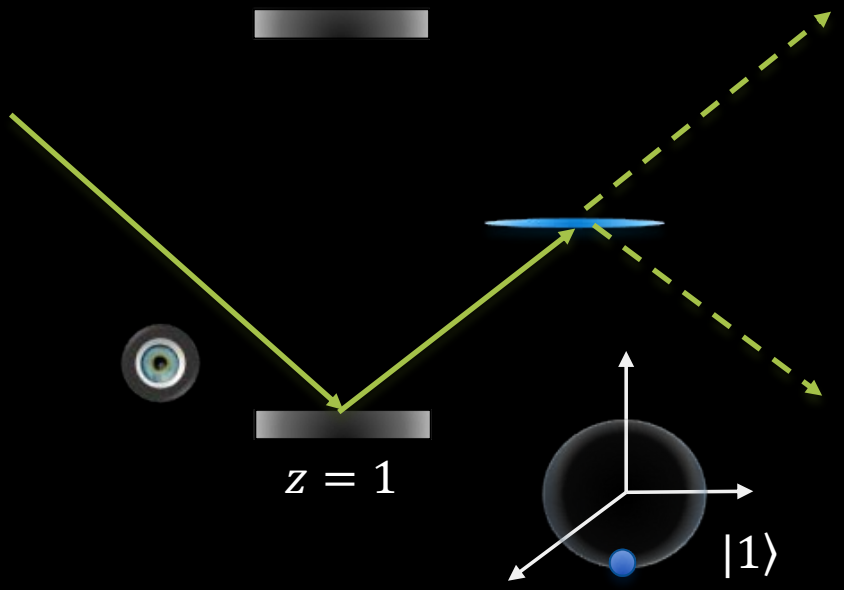


BITS ILLUSTRATED

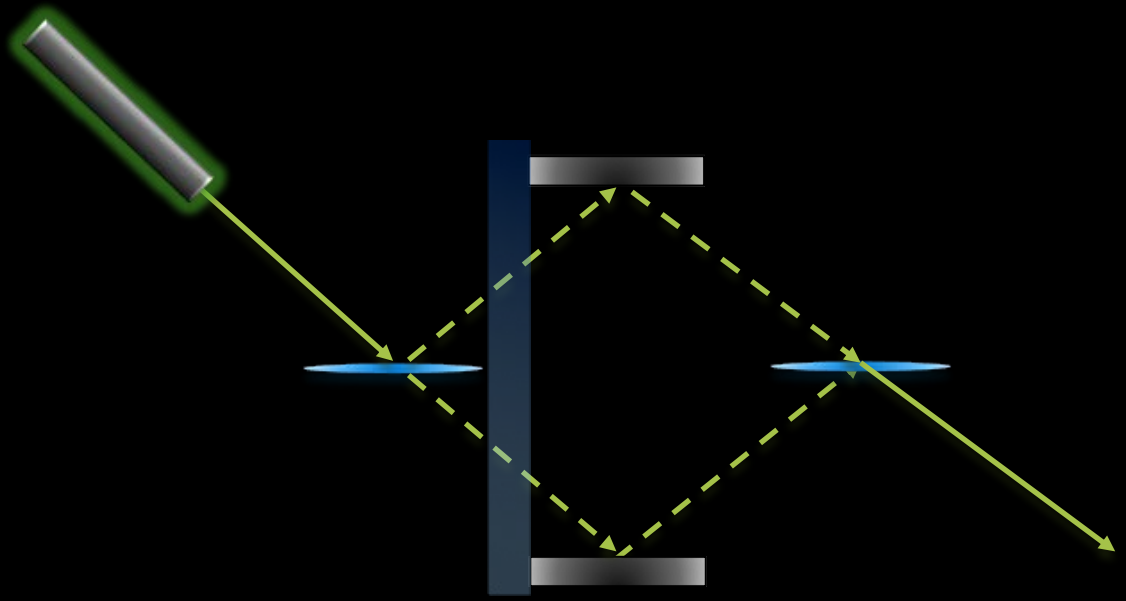


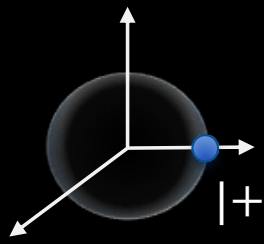
Bits Illustrated

We can reliably encode one bit of information (i.e., value of z), by setting our system in $|0\rangle$ or $|1\rangle$ state.



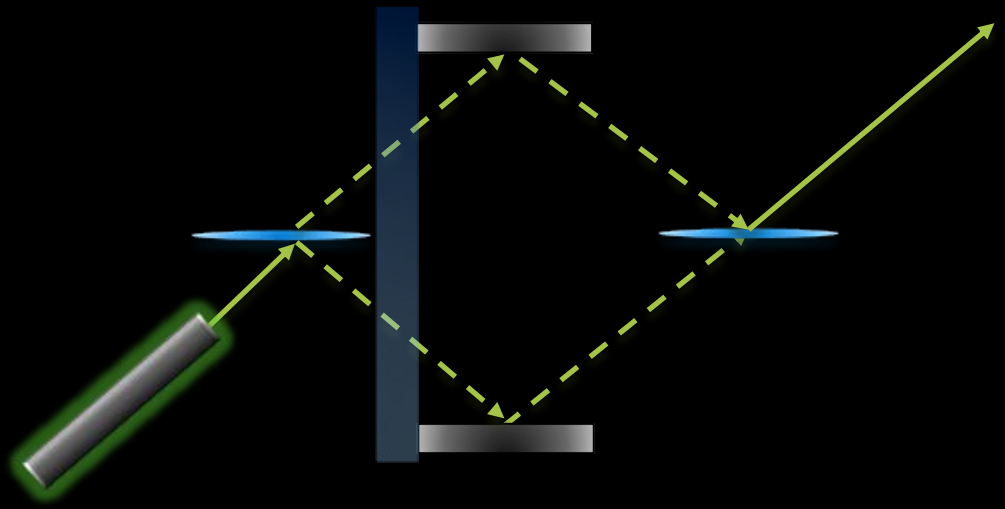
From bits to Qubits

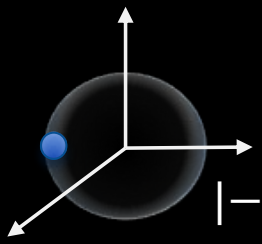




$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

From bits to Qubits

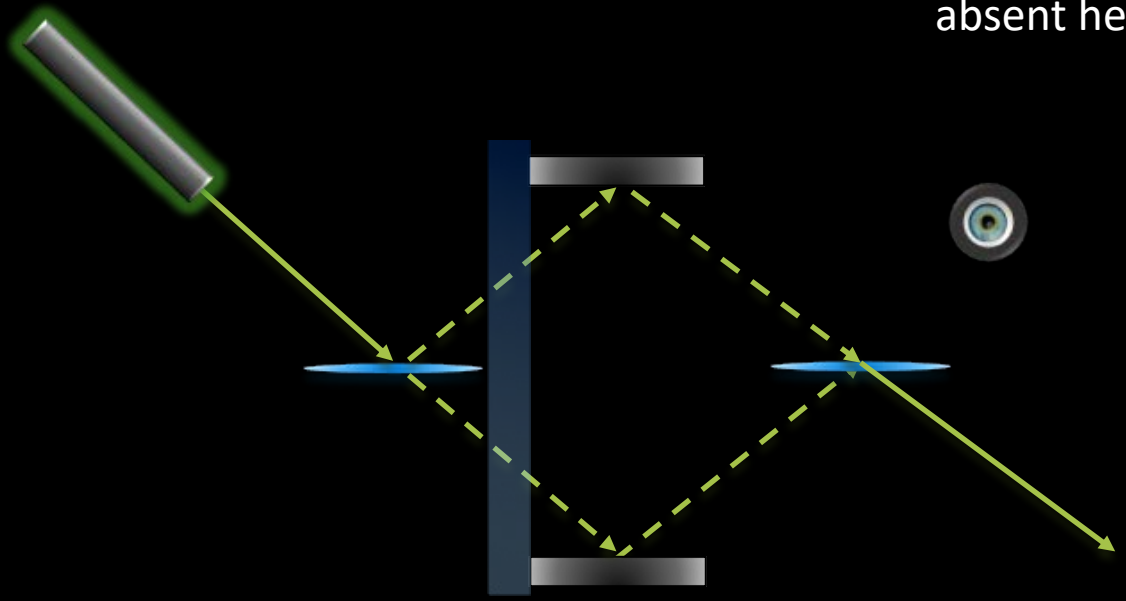


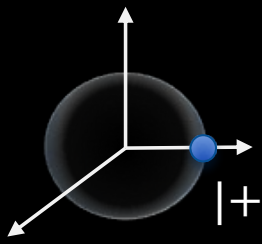


$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

From bits to Qubits

$|+\rangle$ state: Photon is always absent here.

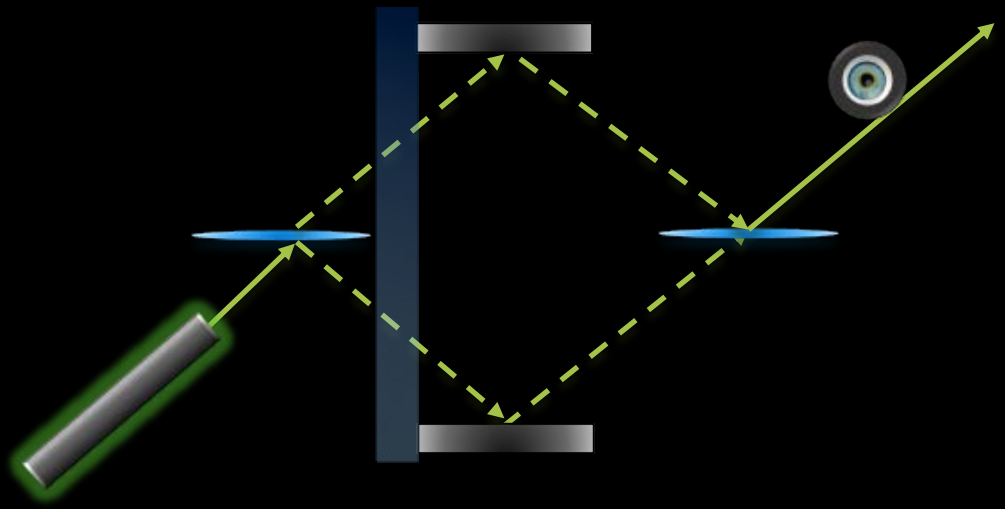


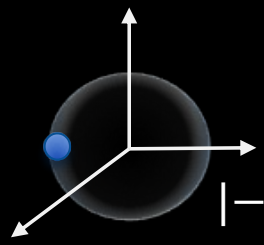


$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

From bits to Qubits

$|+\rangle$ state: Photon is always present

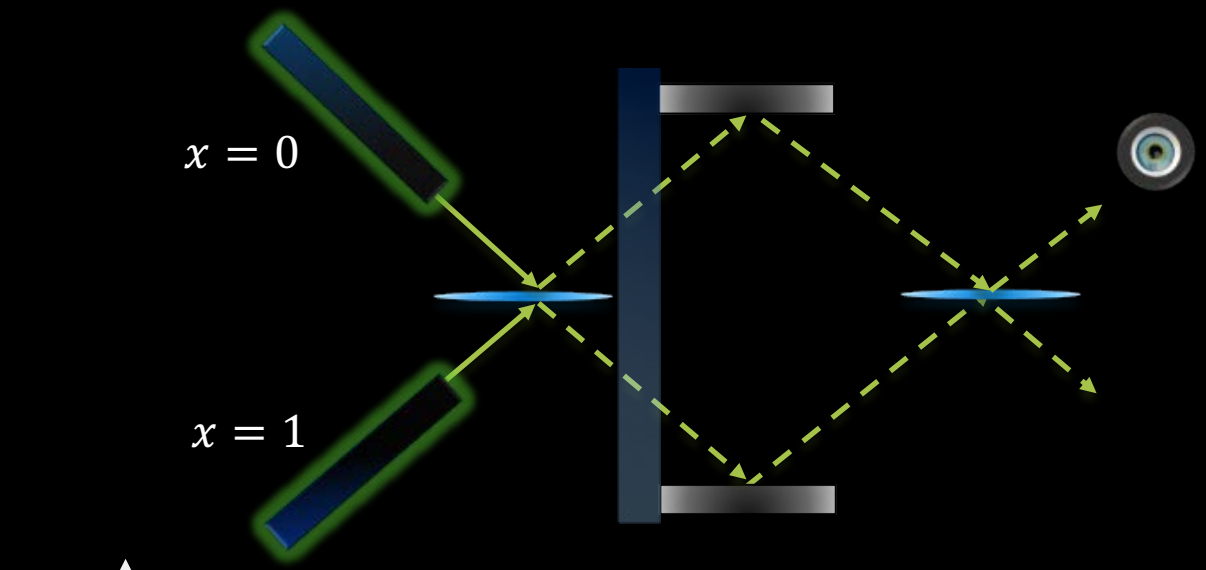


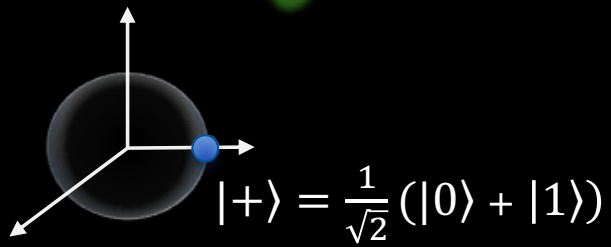


$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

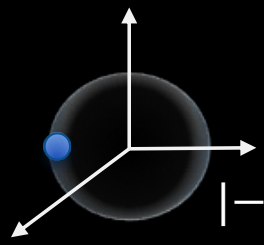
From bits to Qubits

We can also reliably encode and retrieve the a bit of information (i.e., value of x), by setting our system in $|+\rangle$ or $|-\rangle$ state.



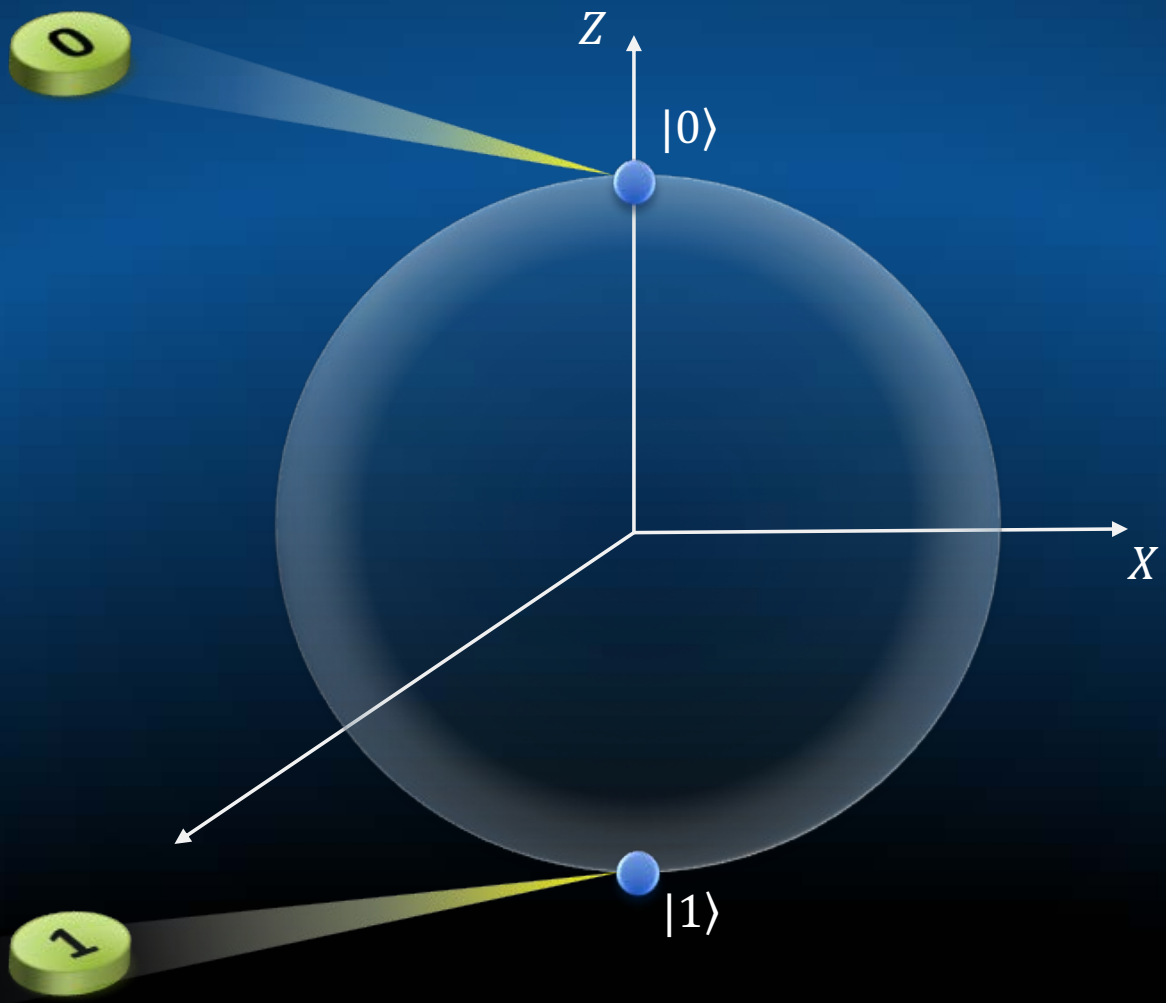


$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

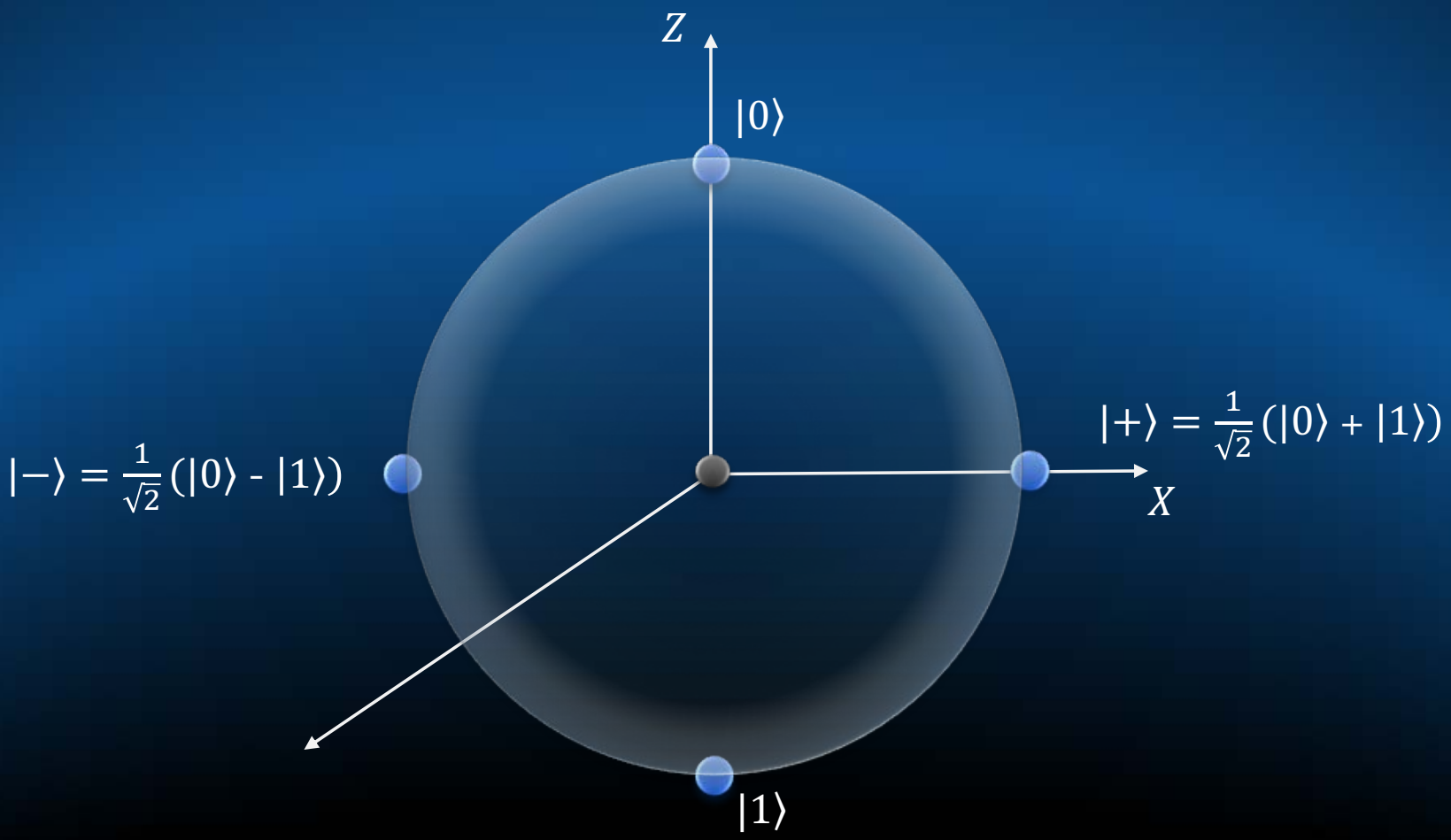


$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

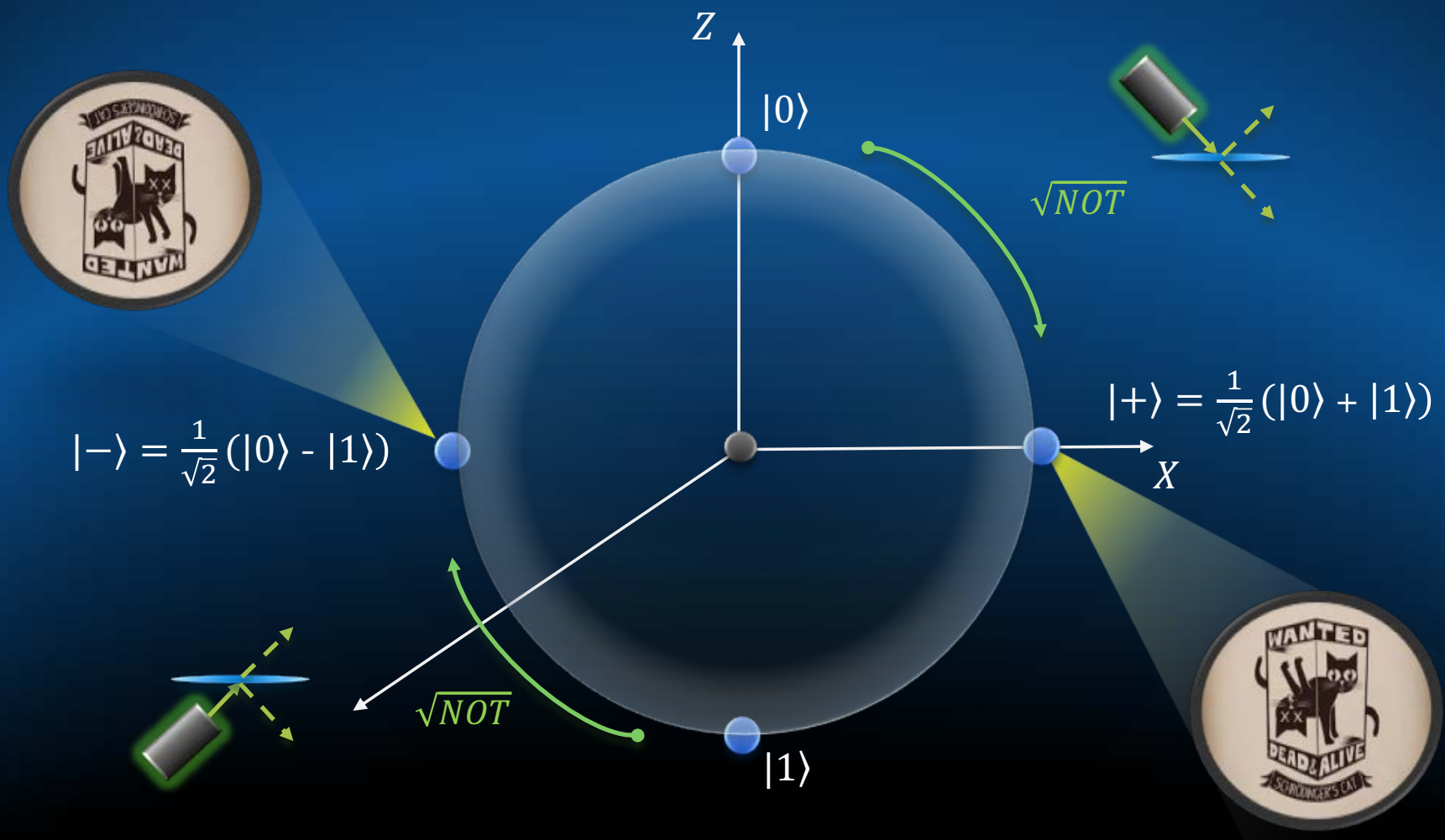
From Bits to Qubits...



From Bits to Qubits…



From Bits to Qubits...

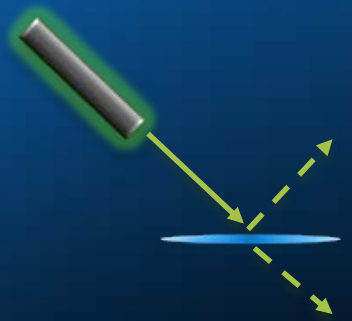


From Bits to Qubits...

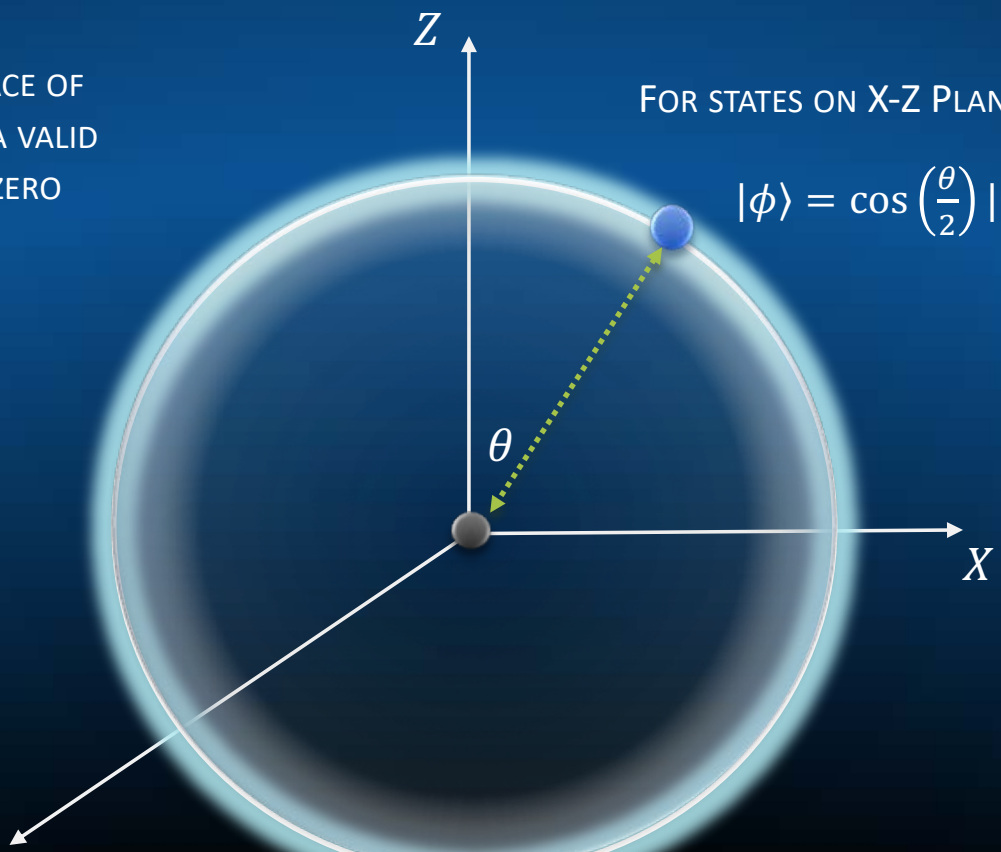
Any point on surface of sphere represents a valid quantum state of zero entropy.

For states on X-Z Plane:

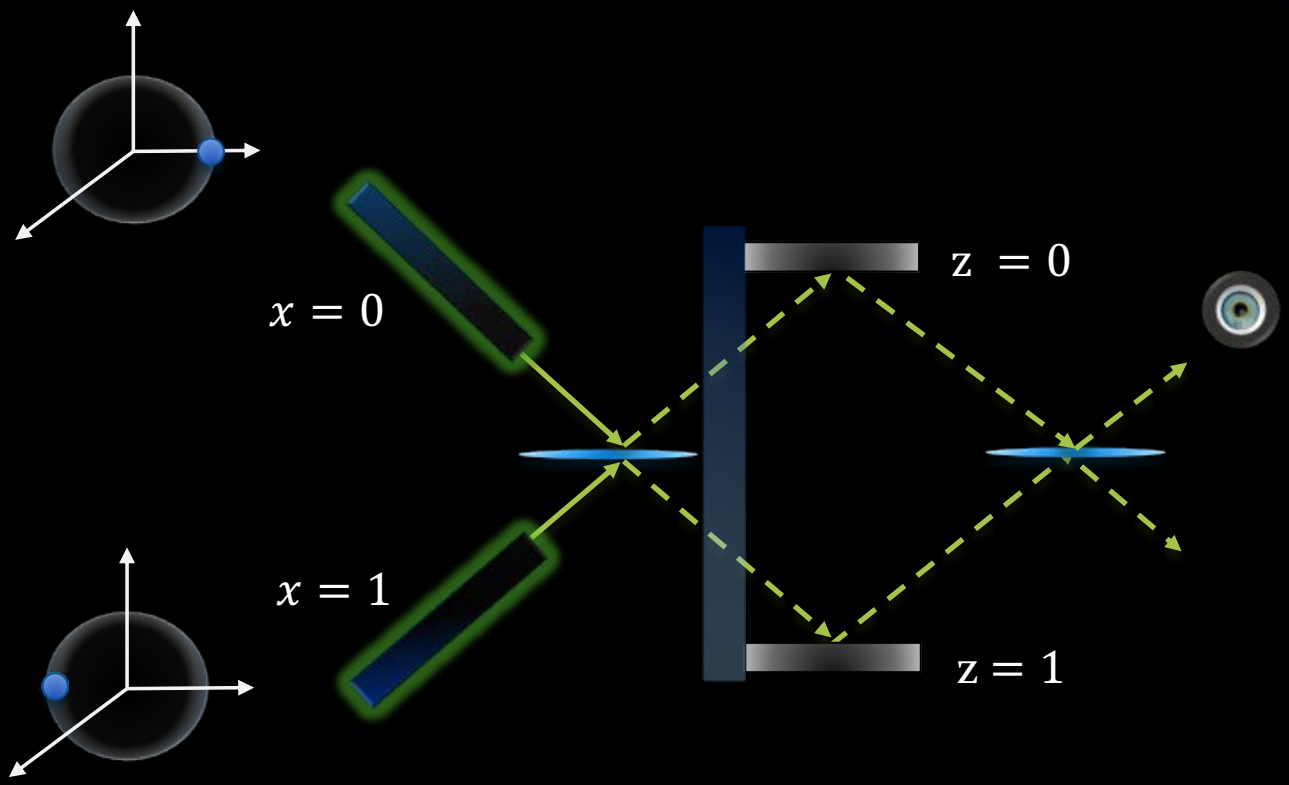
$$|\phi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle$$



Use a non 50/50 beamsplitter

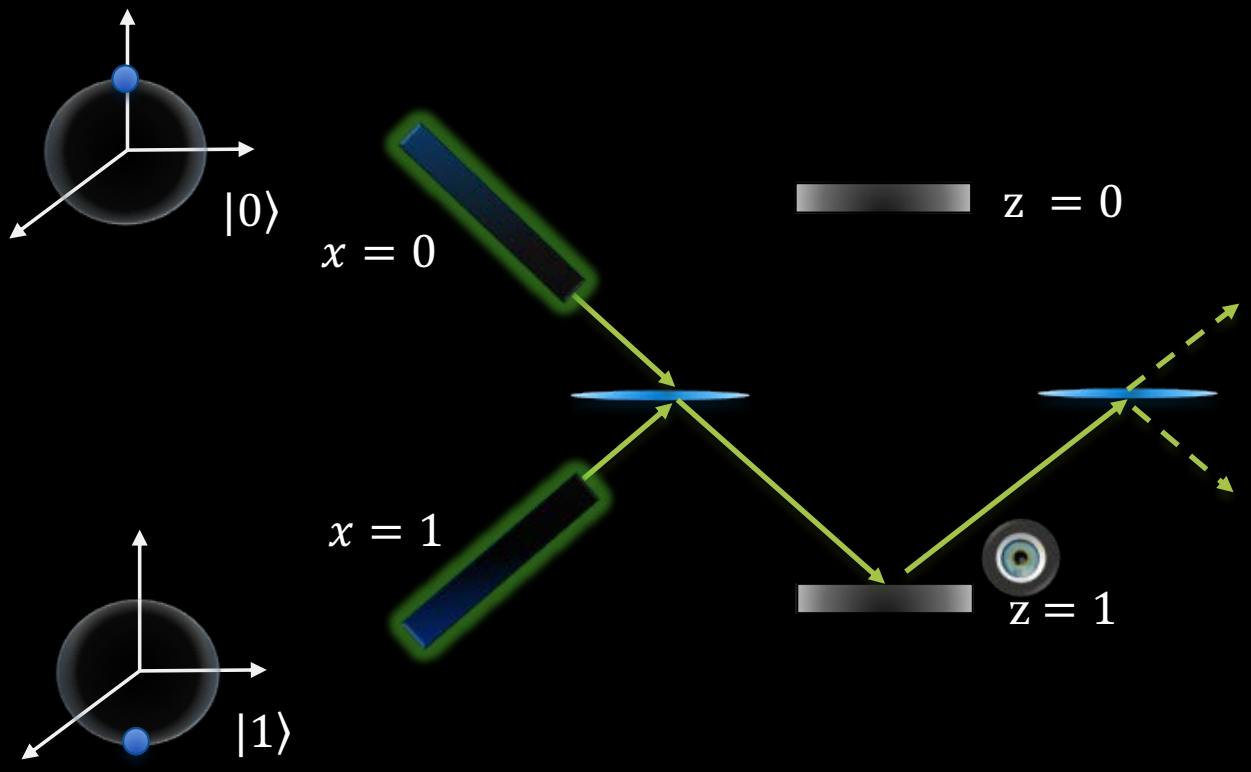


Uncertainty Principle



Measuring x requires we find out nothing about which arm the photon pass though

Uncertainty Principle

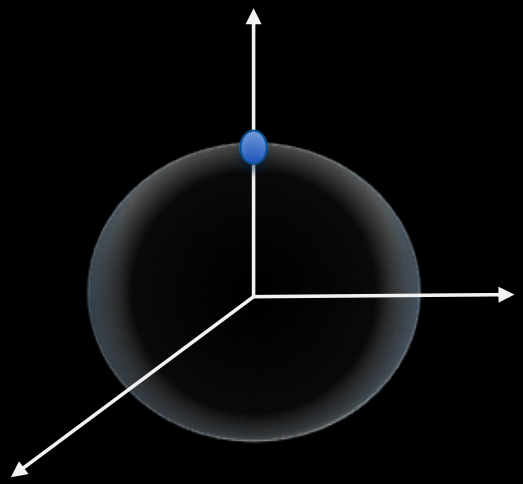


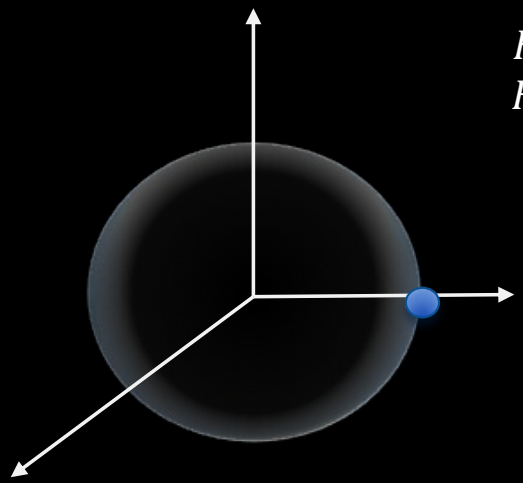
Measuring z would collapse the wave function and thus erase any Information we know about x

Uncertainty Principle

We cannot retrieve information about x and z at the same time!

$H(X) = 1$
$H(Z) = 0$



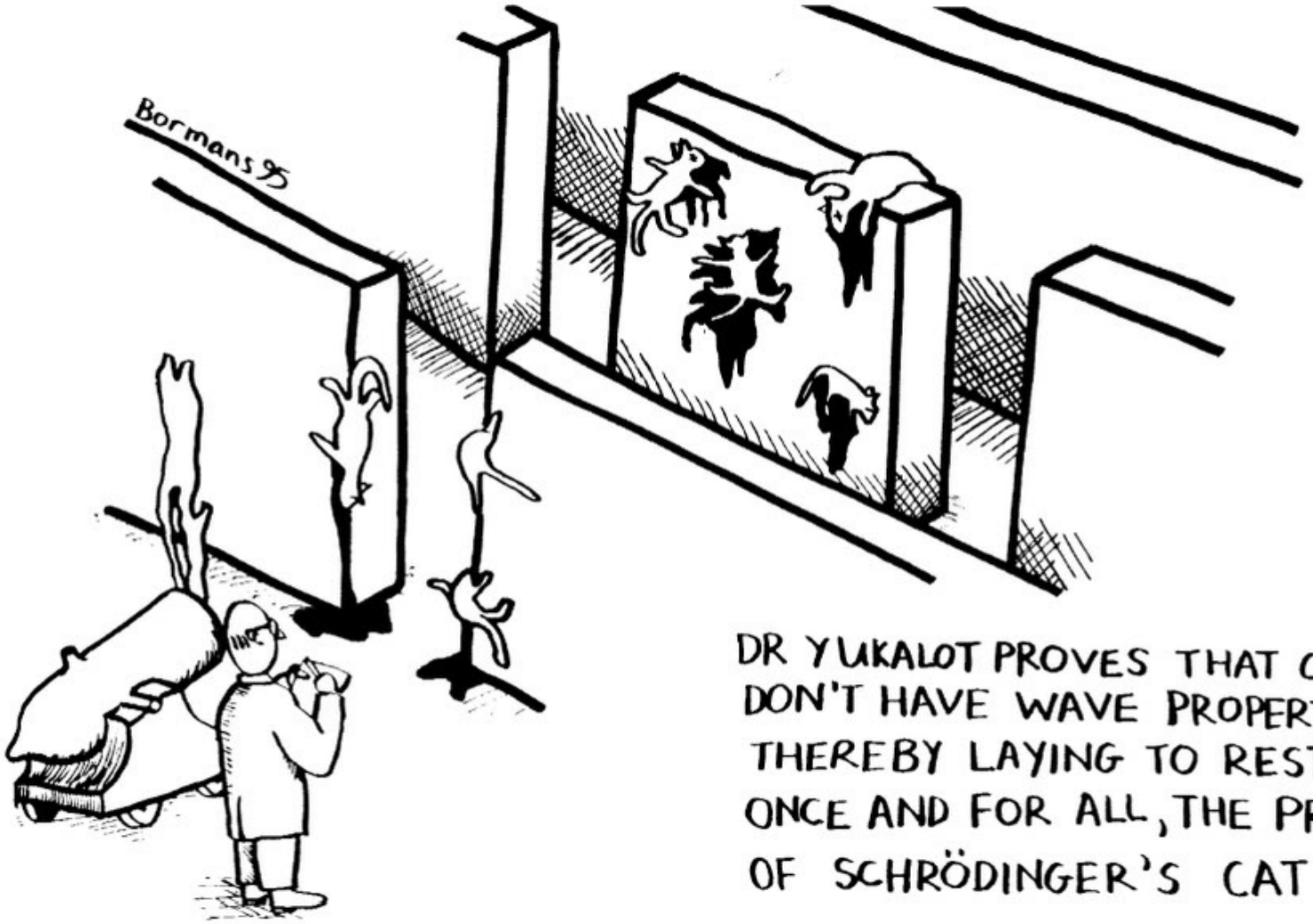


$H(Z) = 0$
$H(X) = 1$

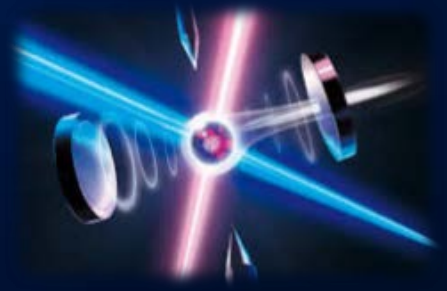
$$H(X) + H(Z) \geq 1$$

Uncertainty of *x*

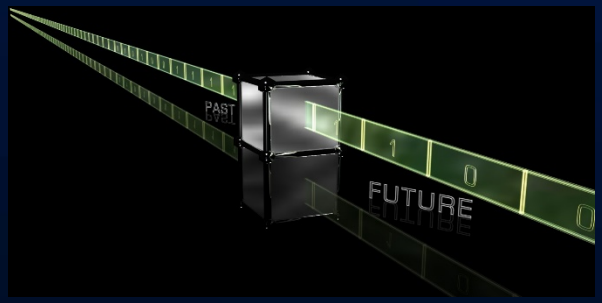
Uncertainty of *Z*


Bormans 95
DR YUKALOT PROVES THAT CATS DON'T HAVE WAVE PROPERTIES, THEREBY LAYING TO REST, ONCE AND FOR ALL, THE PROBLEM OF SCHRÖDINGER'S CAT.

The 2nd Quantum Revolution (1980 – present)



Quantum Sensing

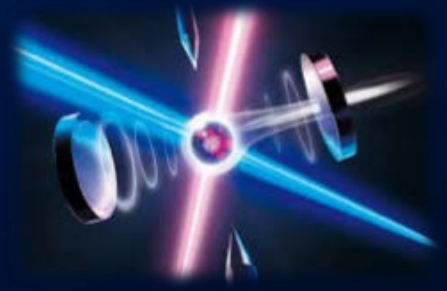


Quantum Modelling

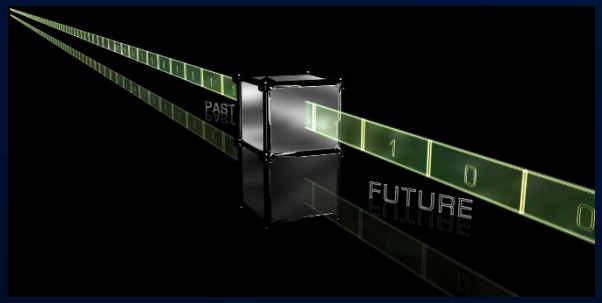
Quantum Cryptography

Quantum Computing

The 2nd Quantum Revolution (1980 – present)



Quantum Sensing



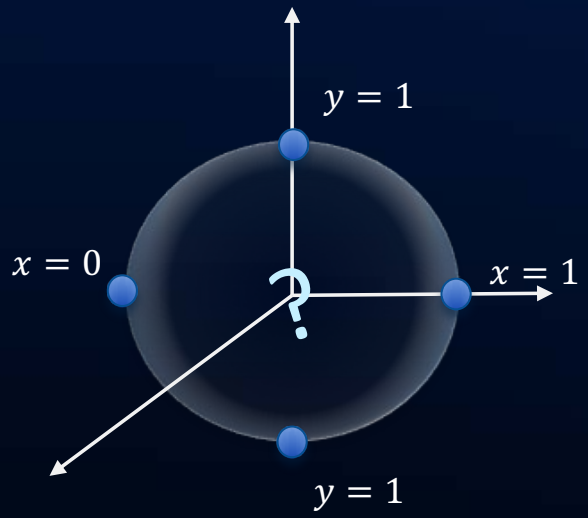
Quantum Modelling

Quantum Cryptography

Quantum Computing

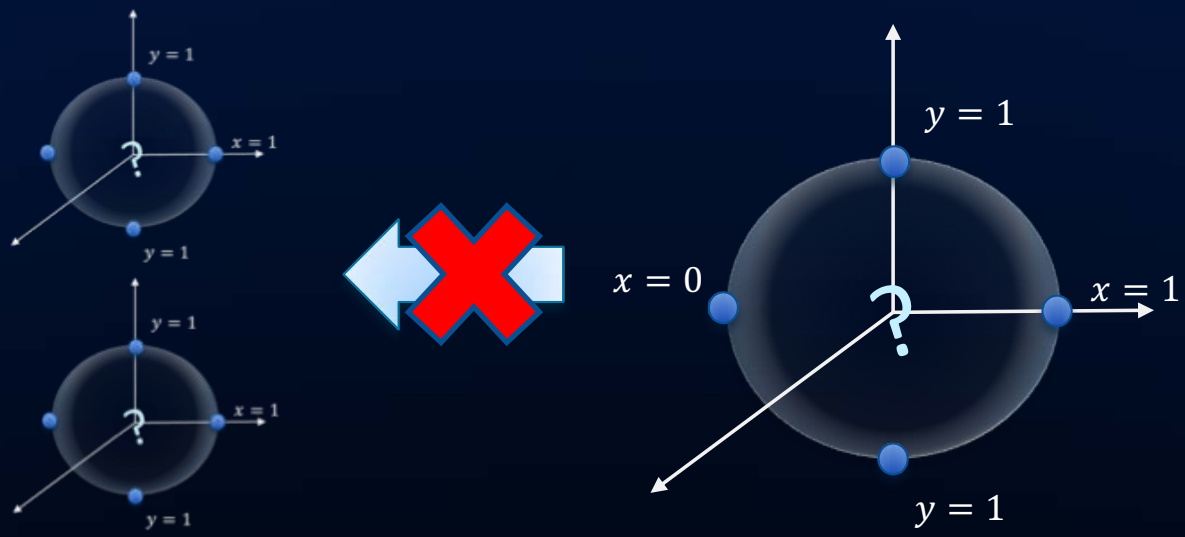
The 2nd Quantum Revolution (1980 – present)

Quantum Cryptography



The uncertainty principle implies that no one – no matter how powerful – can ever reliably know both x and z.

Quantum Cryptography

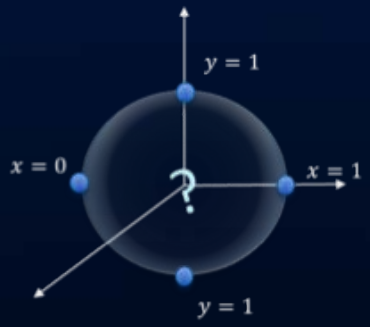


No-Cloning Theorem

An unknown quantum bit cannot be cloned.

Quantum Cryptography

Alice

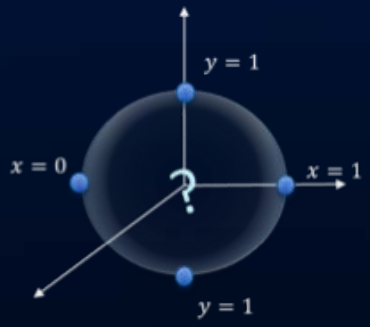


Quantum Channel

Bob

Quantum Cryptography

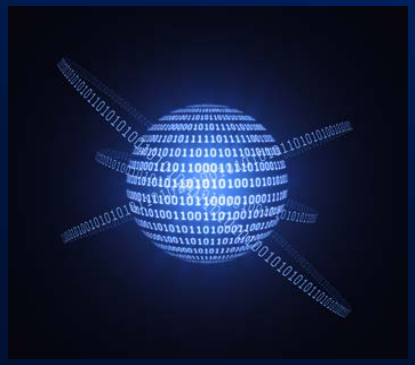
Alice



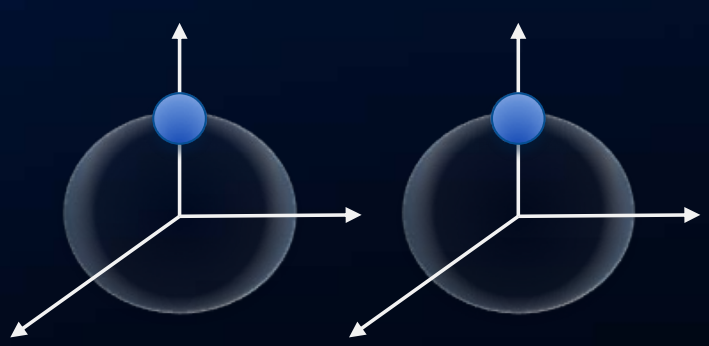
Quantum Channel

Bob

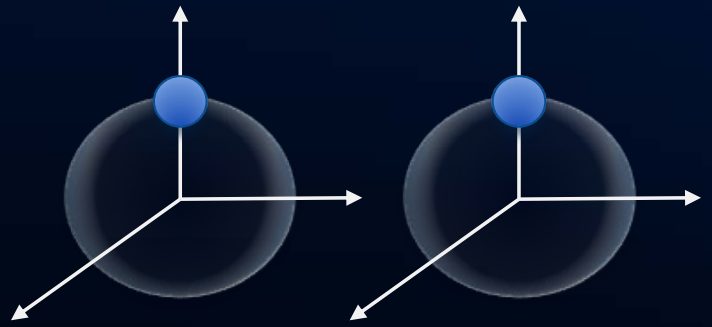
Quantum Computing



Quantum Computing

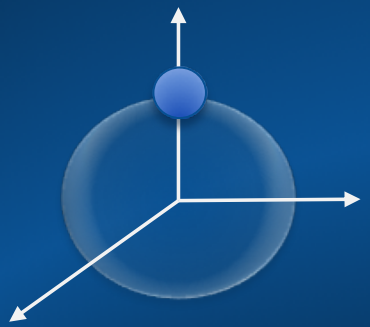


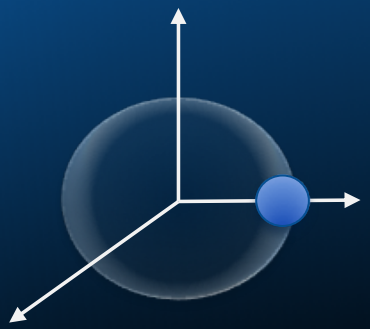
$|0\rangle|0\rangle$



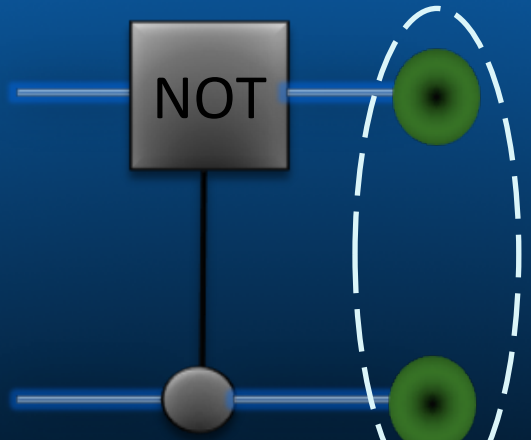
$|1\rangle|1\rangle$

Quantum Computing





$|0\rangle|+\rangle$

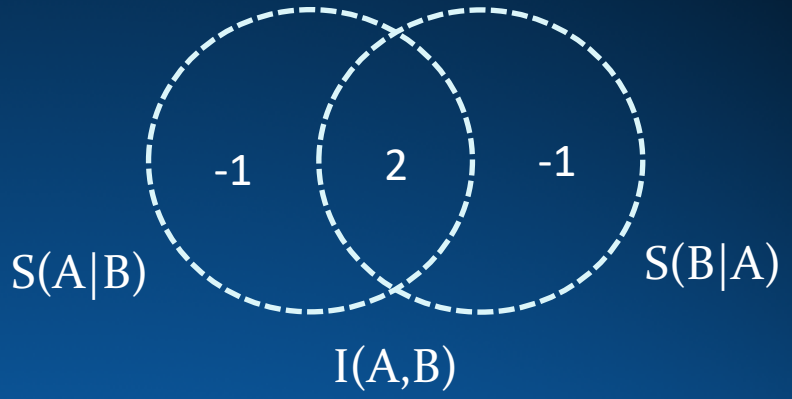


$|0\rangle|0\rangle + |1\rangle|1\rangle$

Entangled

A state with correlations that has zero entropy!

Quantum Computing

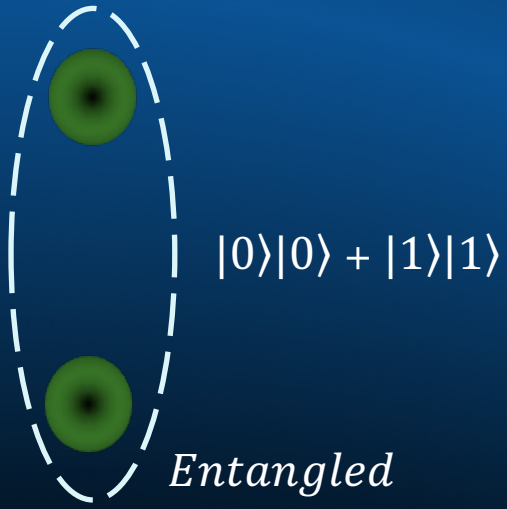


Mutual Information:

$$I(A,B) = S(A) + S(B) - S(A,B) = 2$$

Conditional Entropy:

$$S(A|B) = S(A) - I(A,B) = -1$$



A quantum system B can contain more information about a Quantum system A that what system A contains about itself

Quantum Computing

2 Parameters

$$a|0\rangle + b|1\rangle$$

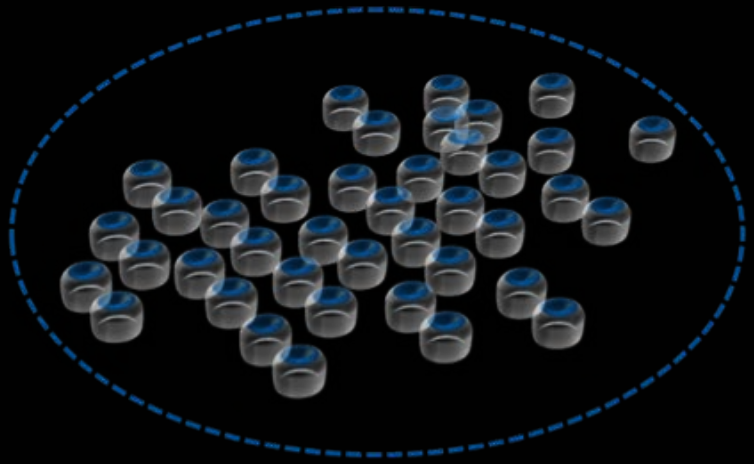
4 Parameters

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

8 Parameters

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

Quantum Computing



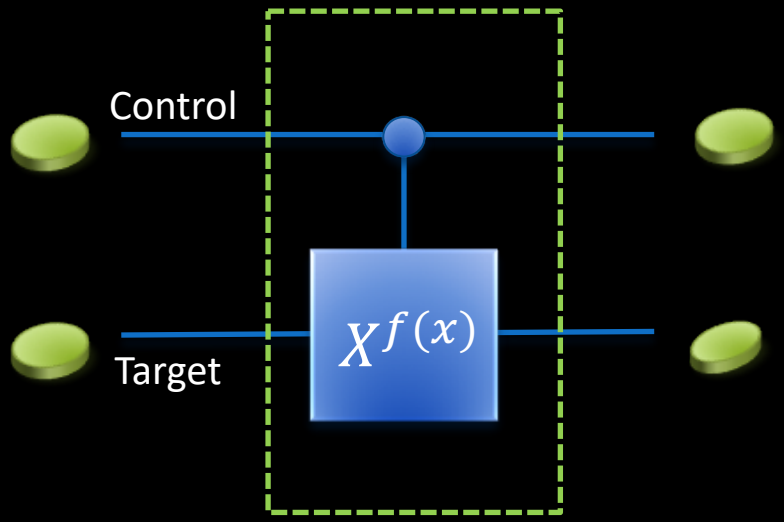
Parameters required to specify State of 300 Qubits

>

The Number of atoms in the Universe

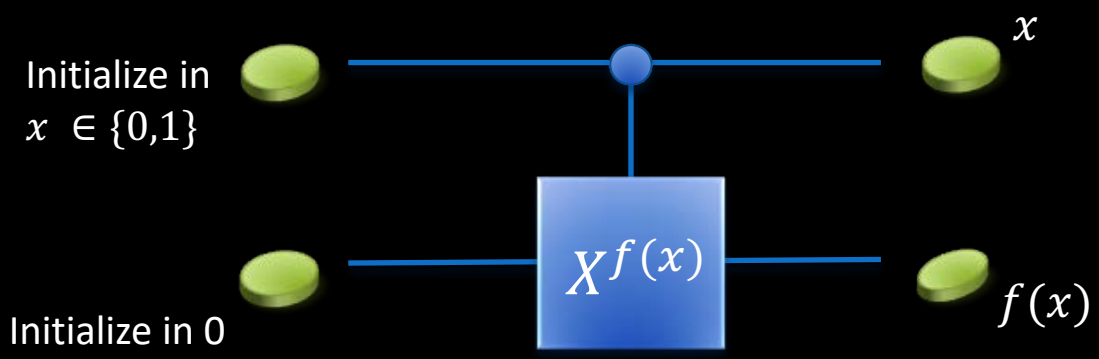
The Amount of Information Required to Track n Qubits grows exponentially with n!

Quantum Parallelism



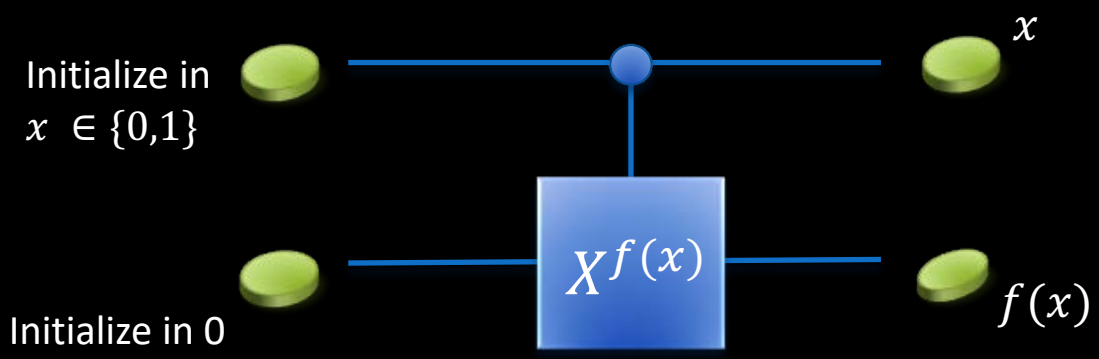
Flips target bit depending on the value of the control bit

Quantum Parallelism



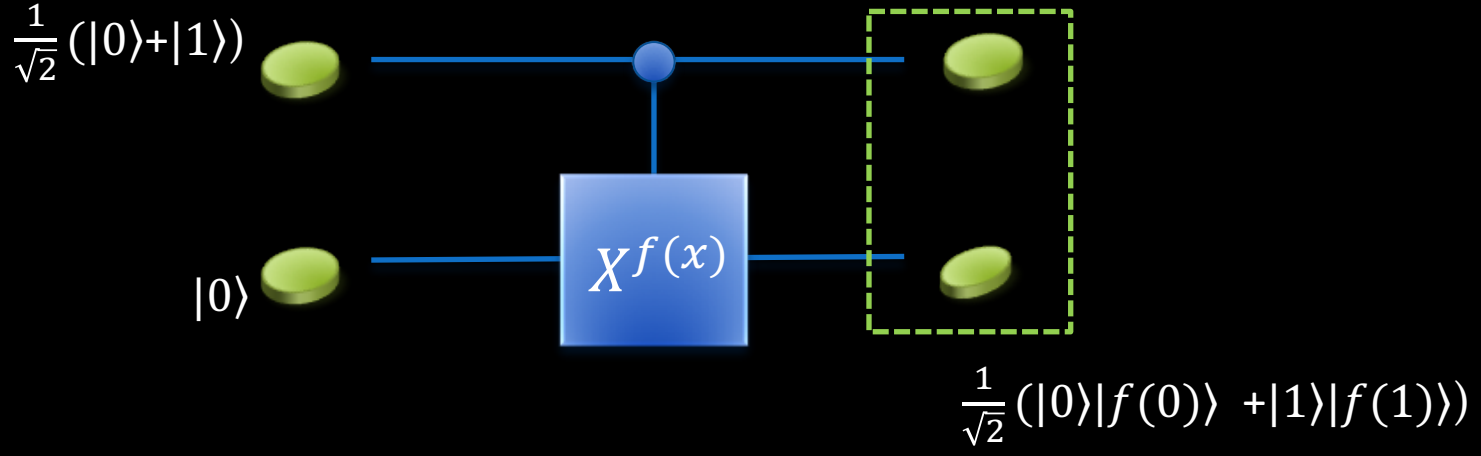
This logic circuit will write down answer to $f(x)$ on the target bit.

Quantum Parallelism



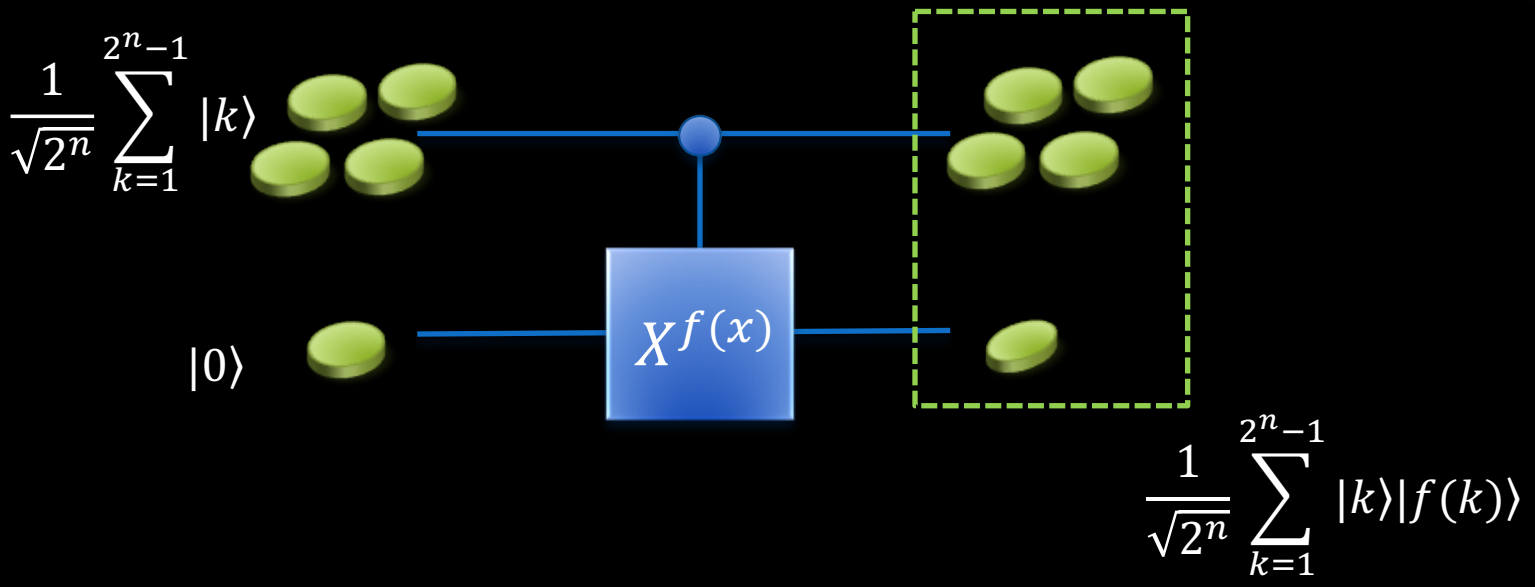
This logic circuit will write down answer to $f(x)$ on the target bit.

Quantum Parallelism



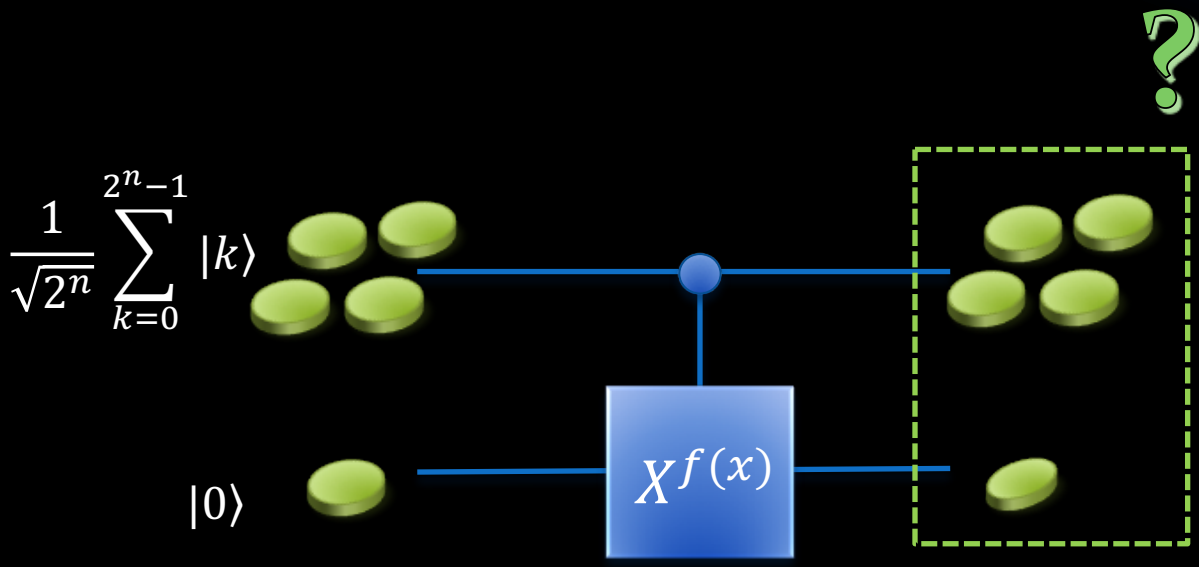
A quantum system can take a superposition of inputs and compute both answers simultaneously!

Quantum Parallelism



We can evaluate a superposition $f(x)$ on an exponential number of possible inputs using a polynomial number of qubits!

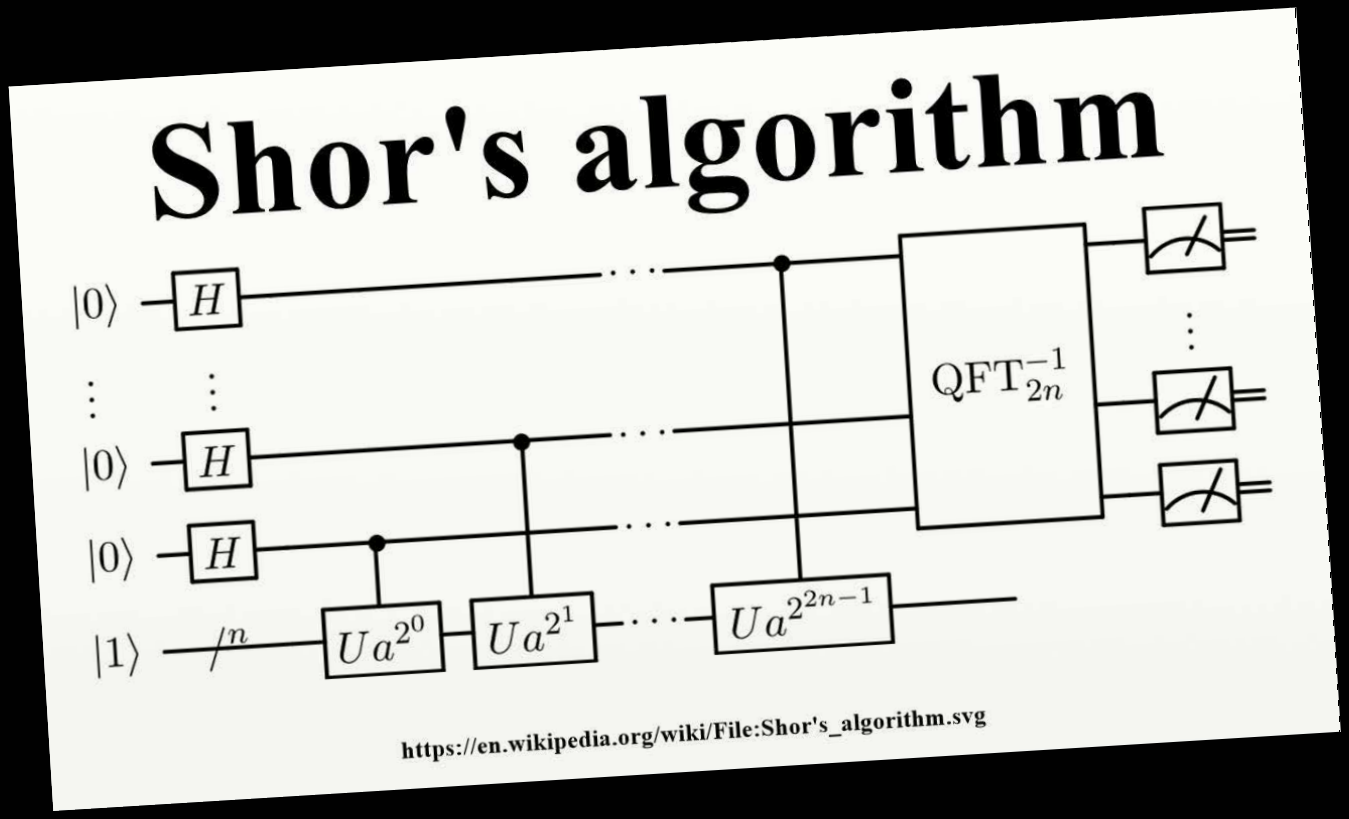
Quantum Parallelism



Can we actually access this information?

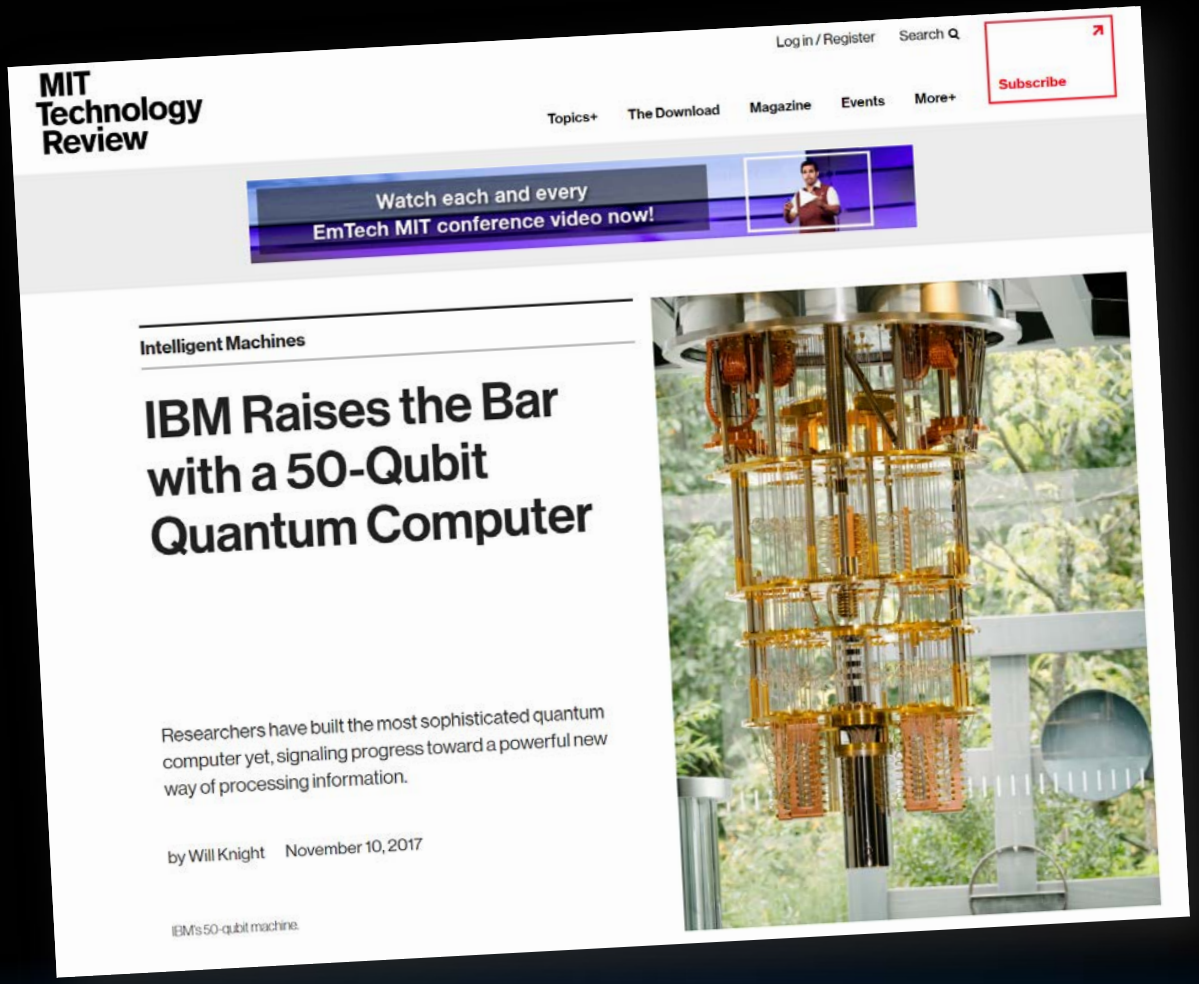
$$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle|f(k)\rangle$$

We can evaluate a superposition $f(x)$ on an exponential number of possible inputs using a polynomial number of qubits!



FACTORING CAN BE DONE IN POLYNOMIAL TIME USING QUANTUM COMPUTERS!- NO EFFICIENT CLASSICAL ALGORITHM KNOWN!

To present Day...



To present Day…

Michelle Simmons - Australian of the Year 2018
Director of the Centre for Quantum Computation and Communication Technology

To present Day...

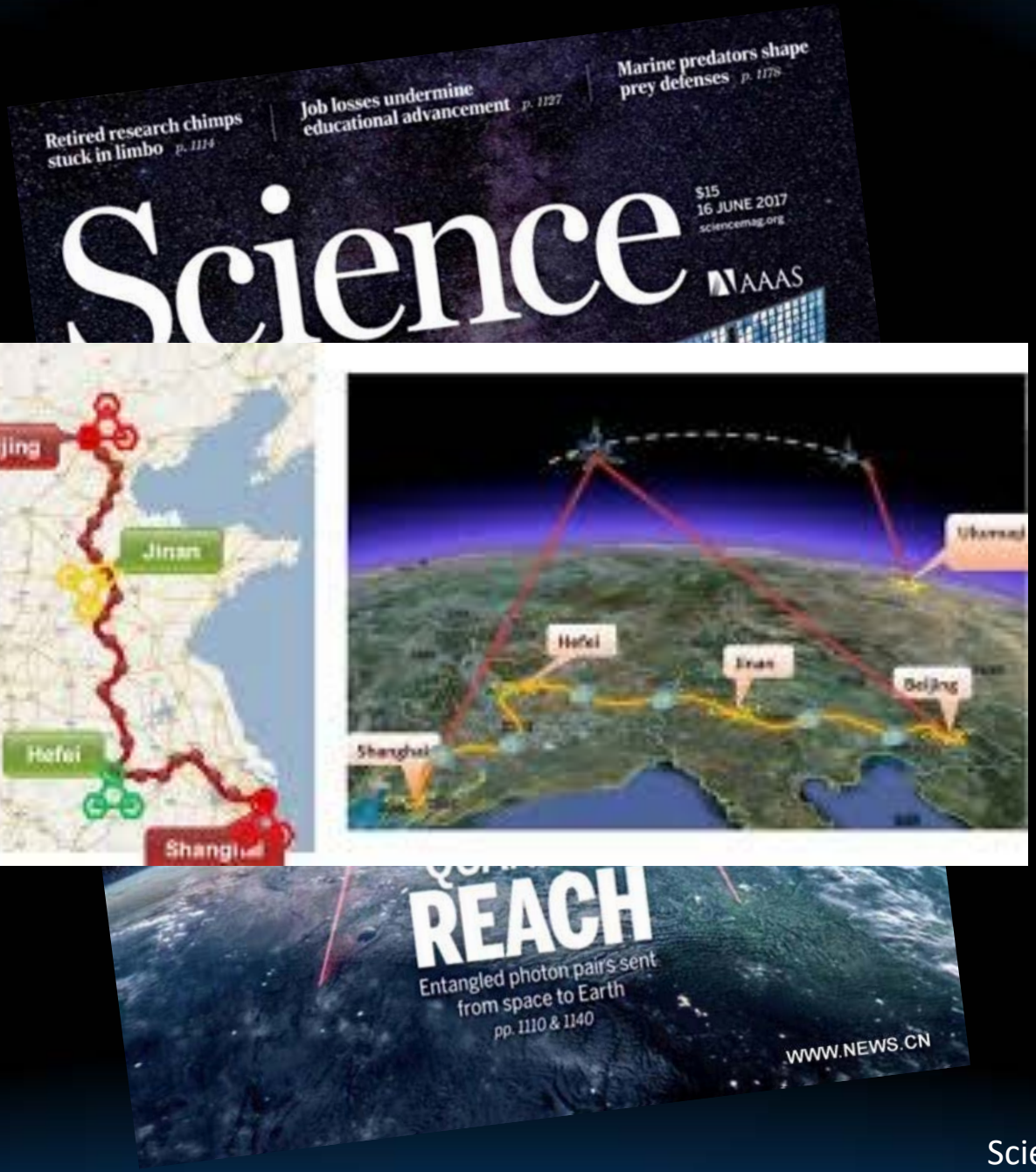
EASTERN ARSENAL POPSCI.COM/BLOGS

China is opening a new quantum research supercenter

The country wants to build a quantum computer with a million times the computing power of all others presently in the world.

By Jeffrey Lin and P.W. Singer *October 10, 2017*

NATIONAL LABORATORY FOR QUANTUM INFORMATION SCIENCES
The $10 billion National Laboratory for Quantum Information Sciences in Hefei will be the center of China's attempt to take the global lead in quantum computing and sensing.
CNTV



Science June 2018


量子通信技
荣获2015年度国家自然科学奖
一等奖
习近平总书记考察量子保密通信"京沪干线"和量子科学实验卫星总控中心
在国际上首次将MDIQKD的光纤传输距离突破到404公里
2015年12月
2016年1月
2016年4月
2016年8月
2016年11月
2016年11月
2016年12月
2017年9月
中国量子通信产业联盟成立
量子科学实验卫星"墨子"号成功发射，刘延东副总理通过视频全程观看发射过程
国科控股联合中科大成立国科量子通信网络有限公司
量子网络
Science
致知
非攻


北京
高村
王庆坨
天津
子牙
沧州北
东光
德州
庄里
徐州
薛城
滕州
曲阜
泰安
禹城

To present Day...

EUROPEAN RESEARCHERS PUBLISH QUANTUM SOFTWARE MANIFESTO

Publication date: 27-11-2017

Researchers and industry specialists across Europe, led by Harry Buhrman (director of QuSoft, group leader at CWI, and professor at the University of Amsterdam), have launched a Quantum Software Manifesto. With the Manifesto, the group aims to increase awareness of and support for quantum software research.

The group is asking the scientific community and quantum tech industry to endorse their initiative. They call for increased collaboration between academics and industrial partners, and encourage further collaboration between quantum hardware

Quantum Software Manifesto Cover

Big Open Question:
What can quantum technologies do?

To present Day...

Quantum Computers Are (Probably) Going To Steal Your Bitcoin

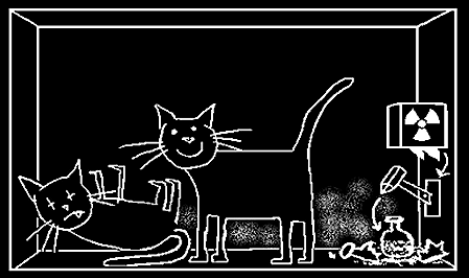
Rae Johnston
Nov 1, 2017, 9:15am· Filed to: Australian Stories

Share

Image: iStock

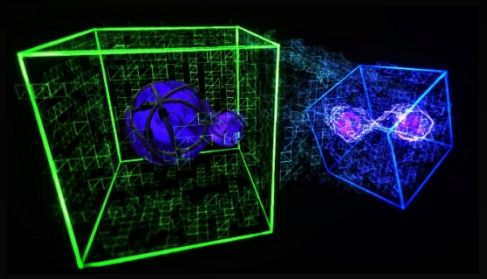
Aggarwal, Divesh, et al. "Quantum attacks on Bitcoin, and how to protect against them." *arXiv preprint arXiv:1710.10377*(2017).

Concluding Remarks



Quantum Systems are not Locally Realistic

A quantum system can be simultaneously in two different states at the same time.



This allows them to perform certain classical intractable of impossible tasks – *e.g. quantum cryptography, Shor's algorithm, simulating complex systems*

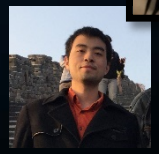
They are not that far away –

Some (e.g. quantum crypto) are already being commercially deployed. Others are developing quickly (e.g. IBM quantum experience)

We still have no idea what their full capabilities are!

The Quantum and Complexity Sciences Initiative

Jayne Thompson



Yang Chengran

NANYANG TECHNOLOGICAL UNIVERSITY
Complexity Institute

Centre for Quantum Technologies
National University of Singapore

Felix Binder

Sun Whei Yeap

Liu Qing

Carlo Di Franco

Mile Gu

Varun Narasimhachar

Andrew Garner

www.quantumcomplexity.org