Quantum Computing and Blockchain

What is the connection and why is it interesting?

Keisuke Fujii
Department of Physics, Graduate School of Science,
Kyoto University

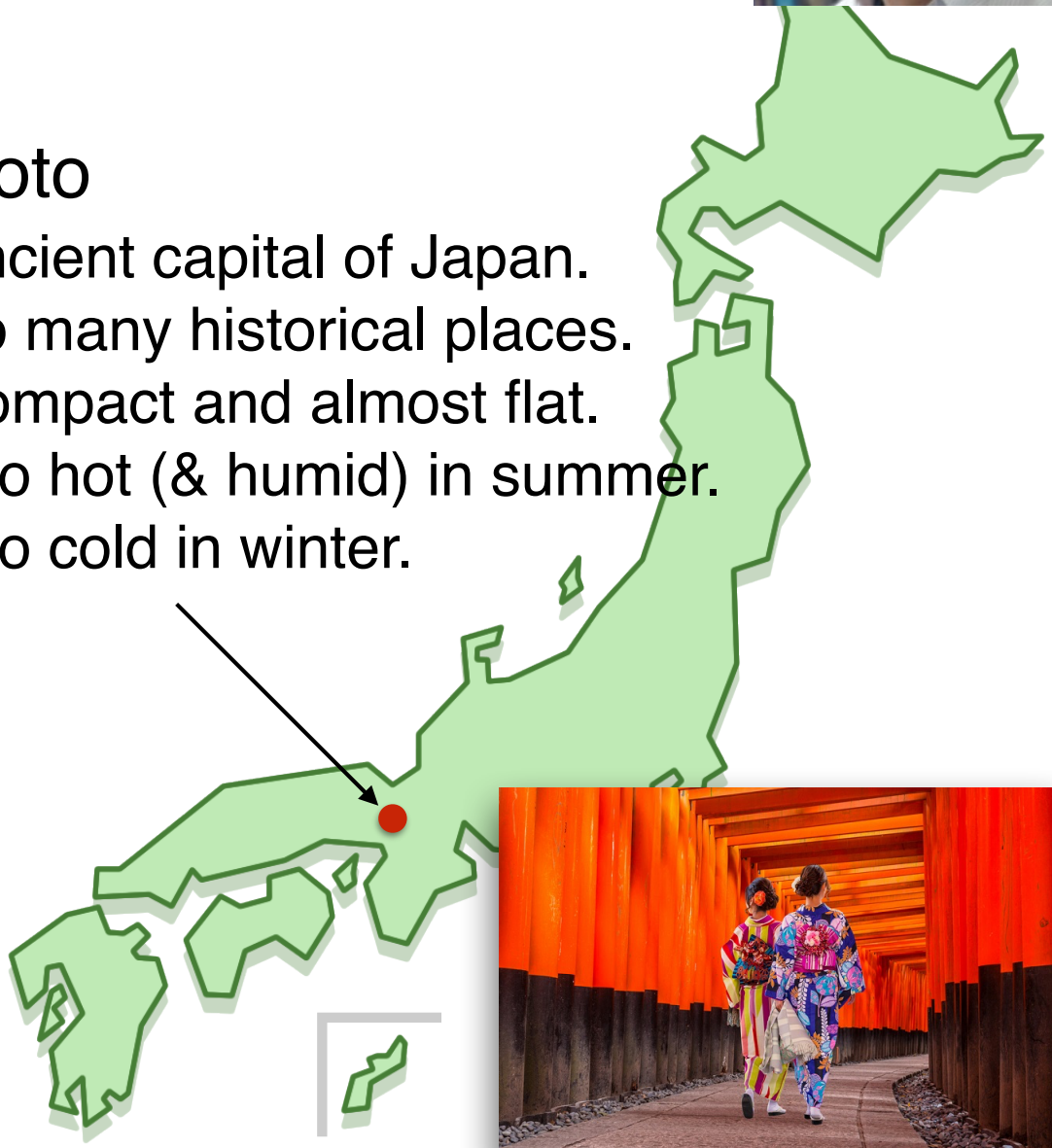
GRADUATE SCHOOL OF FACULTY OF SCIENCE
KYOTO UNIVERSITY

京都大学
KYOTO UNIVERSITY

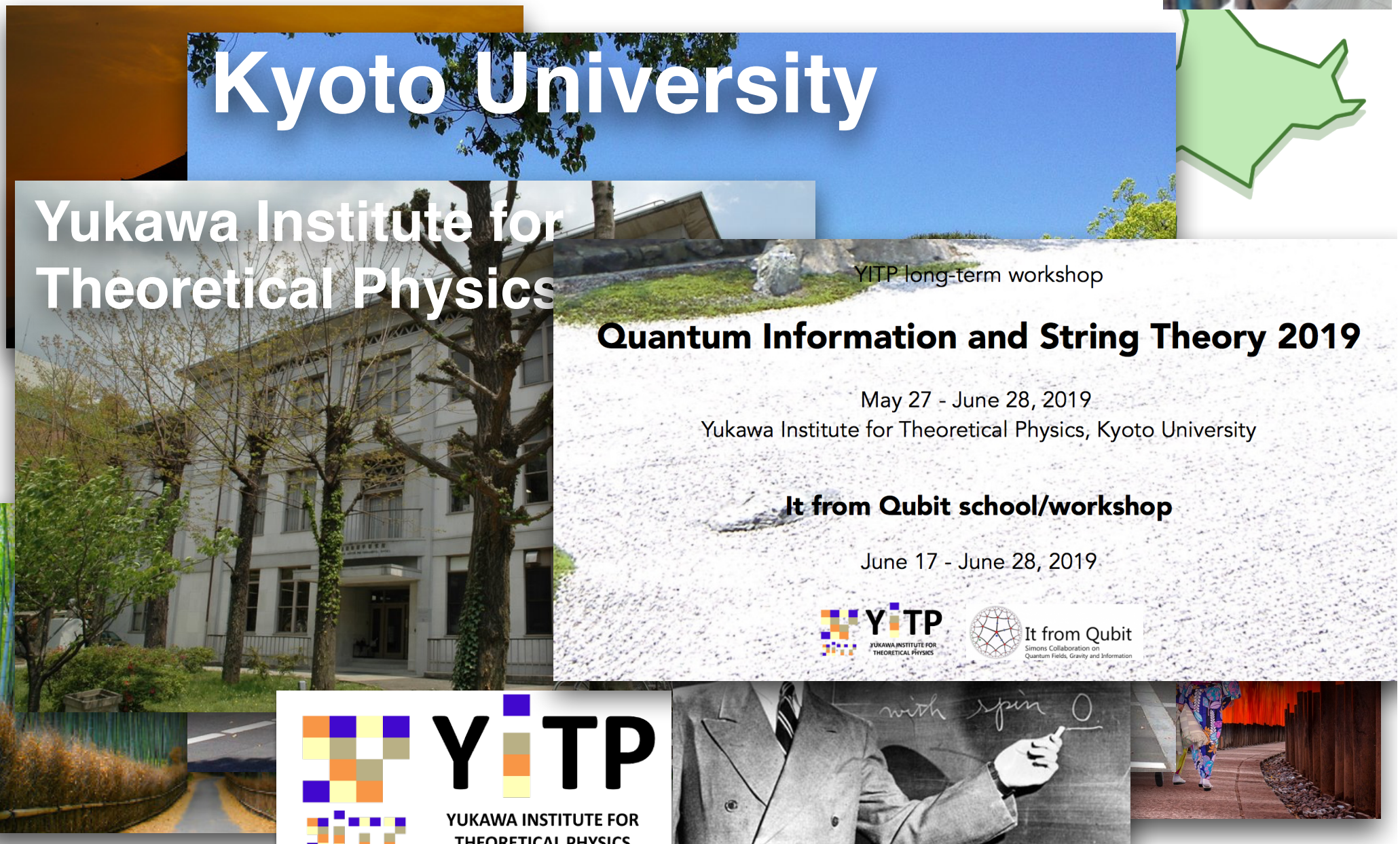
Keisuke Fujii@Kyoto University
Department of Physics,
Graduate school of Science

Kyoto

-Ancient capital of Japan.
-So many historical places.
-Compact and almost flat.
-Too hot (& humid) in summer.
-Too cold in winter.



Keisuke Fujii@Kyoto University
Department of Physics,
Graduate school of Science

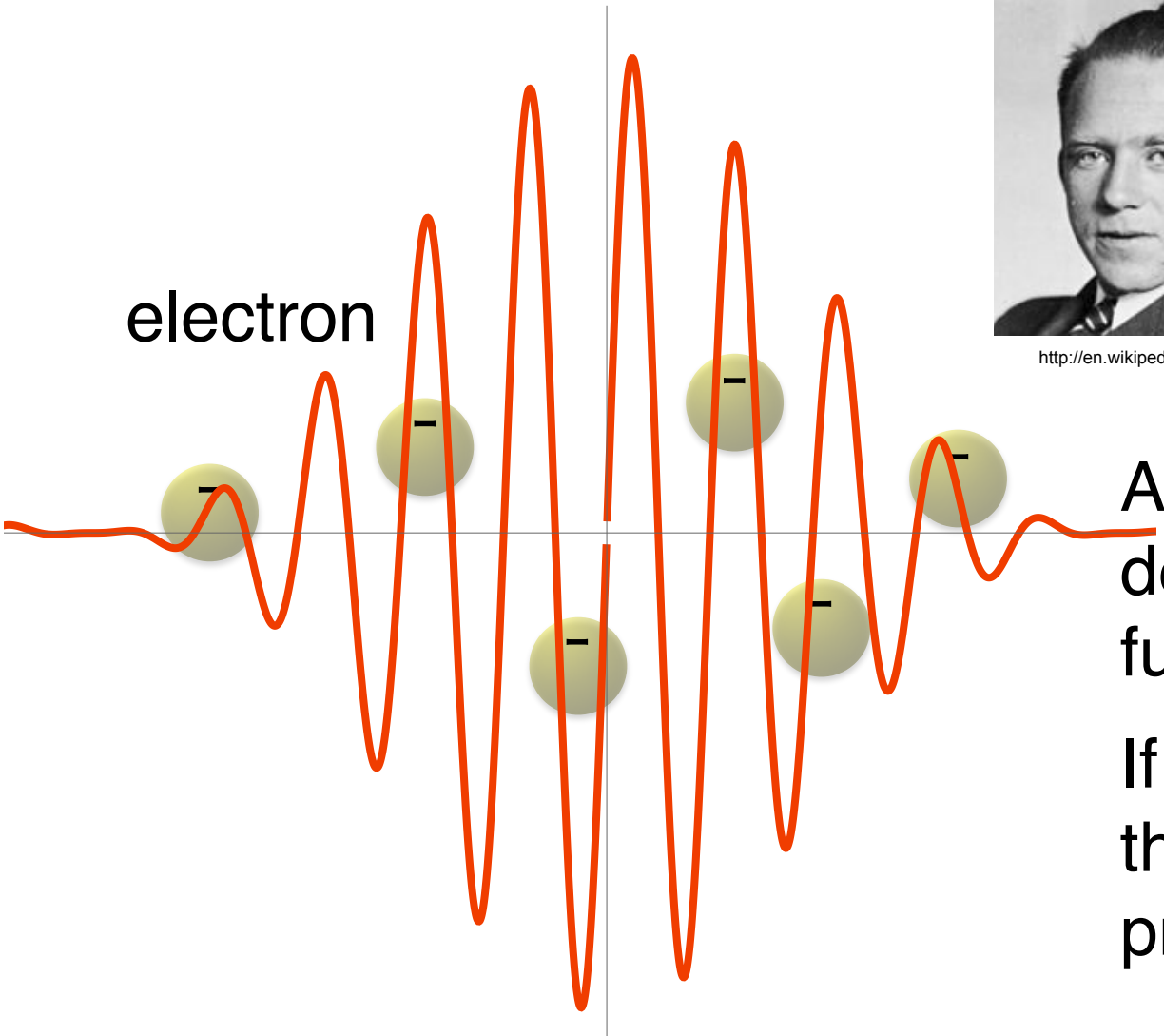


Outline

- Quantum physics and information
- How quantum computers work
- Industrial approaches to quantum computers
- Quantum computer and blockchain
- Summary

Quantum physics

Wave & particle duality



Werner K Heisenberg (1901-1976)

http://en.wikipedia.org/wiki/Werner_Heisenberg

Erwin Schrödinger (1887-1961)

http://www.owlnet.rice.edu/~mishat/1933-5.html

An electron is described by **wave**-function, and can interfere.

If we do a measurement, the **position** is determined probabilistically.

Quantum physics

Wave & particle duality

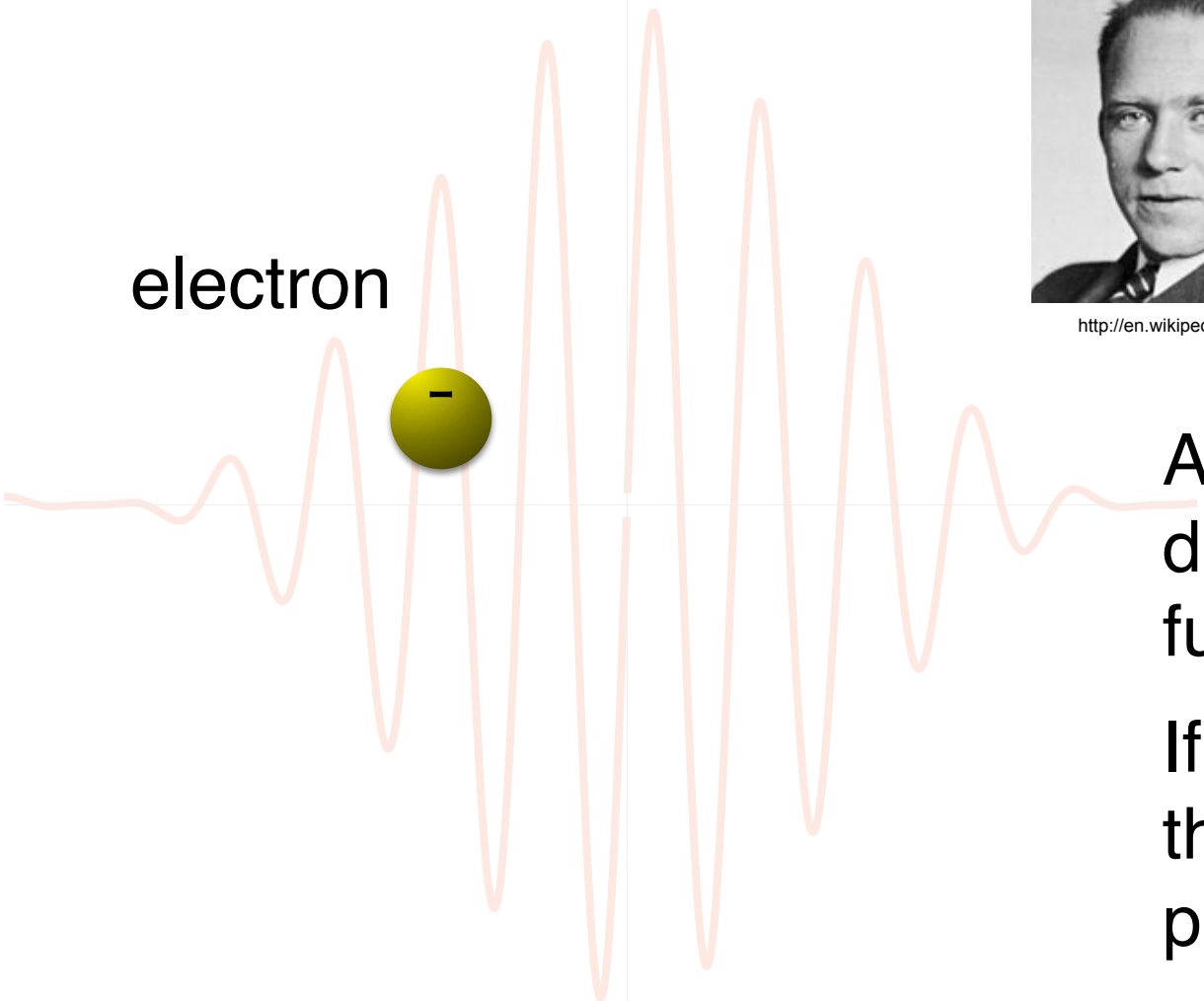
Werner K Heisenberg (1901-1976)

http://en.wikipedia.org/wiki/Werner_Heisenberg

Erwin Schrödinger (1887-1961)

http://www.owlnet.rice.edu/~mishat/1933-5.html

electron



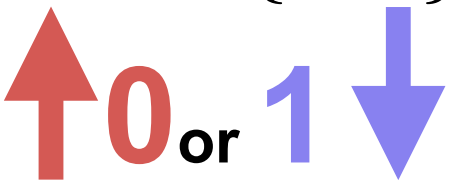
An electron is described by **wave**-function, and can interfere.

If we do a measurement, the **position** is determined probabilistically.

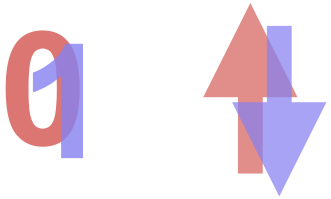
Quantum information

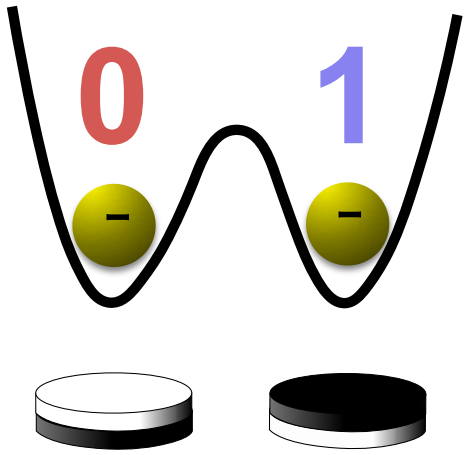
classical bit:

$$x \in \{0, 1\}$$

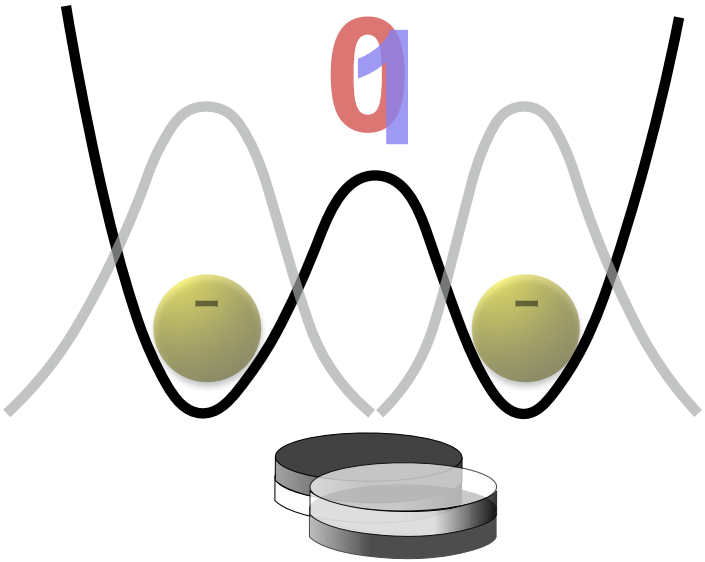


quantum bit:





superposition of 0 and 1



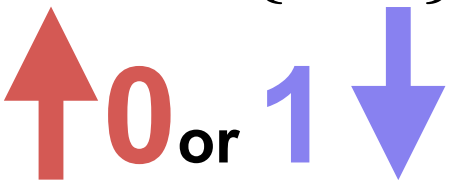
complex
vector space

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

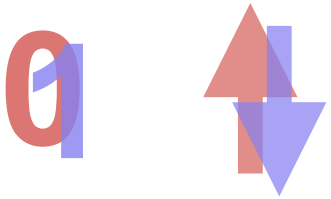
Quantum information

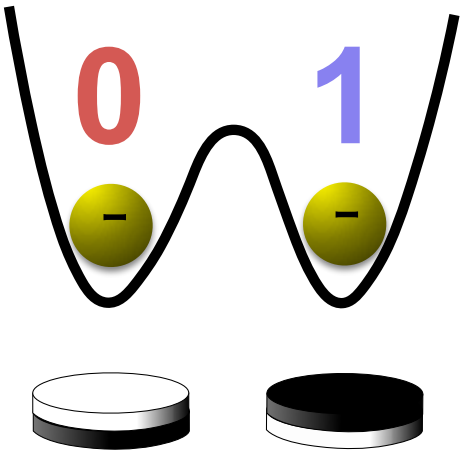
classical bit:

$x \in \{0, 1\}$

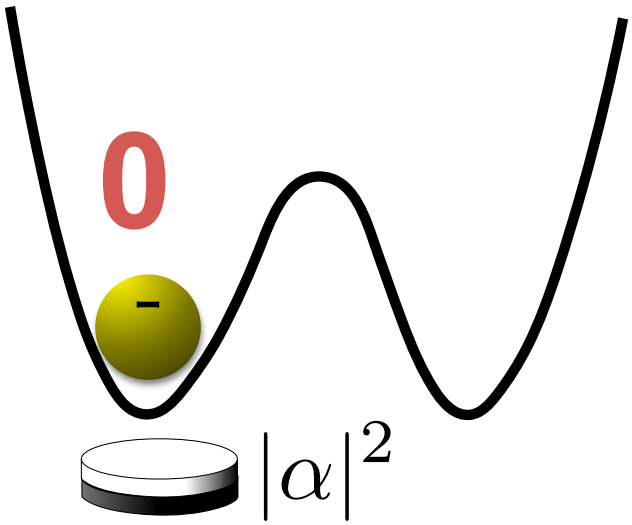


quantum bit:





superposition of 0 and 1



complex
vector space

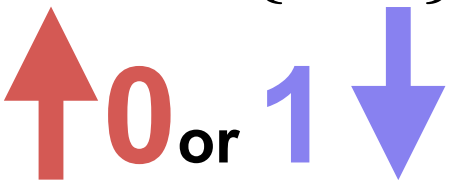
$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

If you do a measurement, 0 or 1 is determined probabilistically.

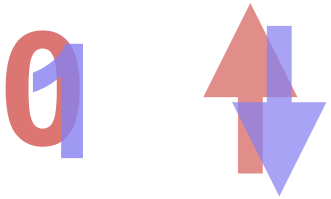
Quantum information

classical bit:

$x \in \{0, 1\}$

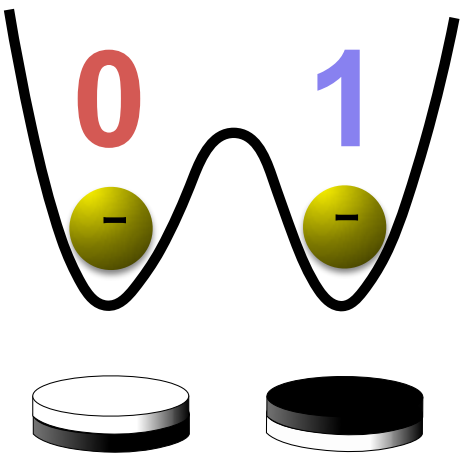


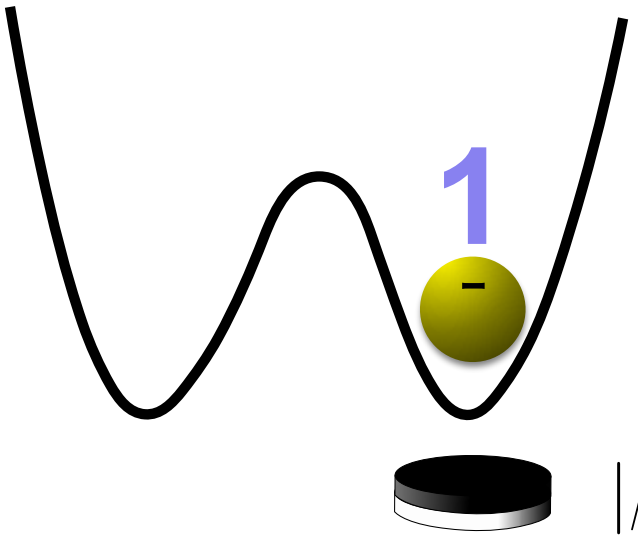
quantum bit:



superposition of 0 and 1

complex
vector space



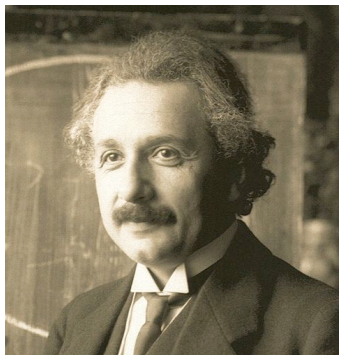


$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

If you do a measurement, 0 or 1 is determined probabilistically.

Bell's inequality

Einstein's letter to M. Born (1926):
"I, at any rate, am convinced that He (God) does not throw dice"



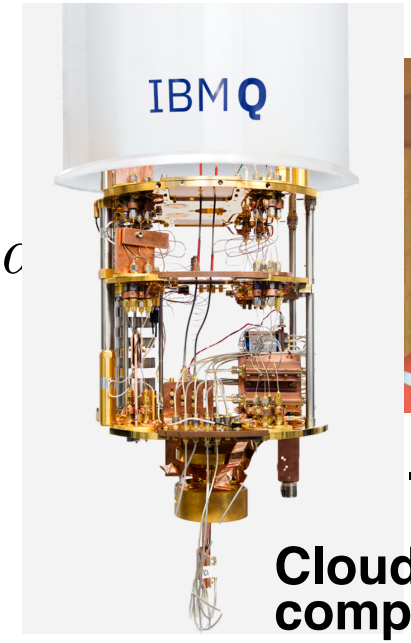
A. Einstein

In the Einstein-Podolsky-Rosen paper:
"elements of physical reality (= hidden variable) must be added to quantum mechanics to restore the theory causality and locality"

Bell's inequality (1964):
Any local hidden variable theory satisfies

$$E(a_x, b_x) + E(a_x, b_z) + E(a_z, b_x) + E(a_z, b_z) \leq 2$$

But quantum mechanics provides $2\sqrt{2}$!



Cloud quantum computer (IBM Q)

. S. Bell

Aspect's experiment (RPL 1981):

A. Aspect

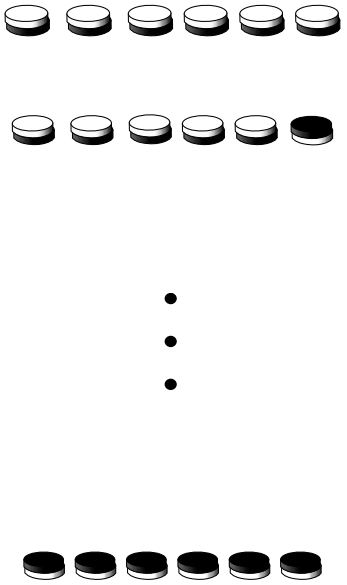
How quantum computer works

multiple classical bit (*n-dimensional vector space over GF(2)****):***

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (0,\quad 0,\quad 1,\quad 0,\quad 0,\quad 1)$$

multiple quantum bit:

$$|\psi\rangle = \begin{pmatrix} c_{00\ldots0} \\ c_{00\ldots1} \\ \vdots \\ c_{11\ldots1} \end{pmatrix} \begin{matrix} |00\ldots0\rangle \\ |00\ldots1\rangle \\ \vdots \\ |11\ldots1\rangle \end{matrix}$$



superposition of all possible patterns

2^n-dimensional complex vector space!

How quantum computer works

1981(MIT) "1st Symposium on Physics and Computation"

Richard P Feynman
(1918-1988)

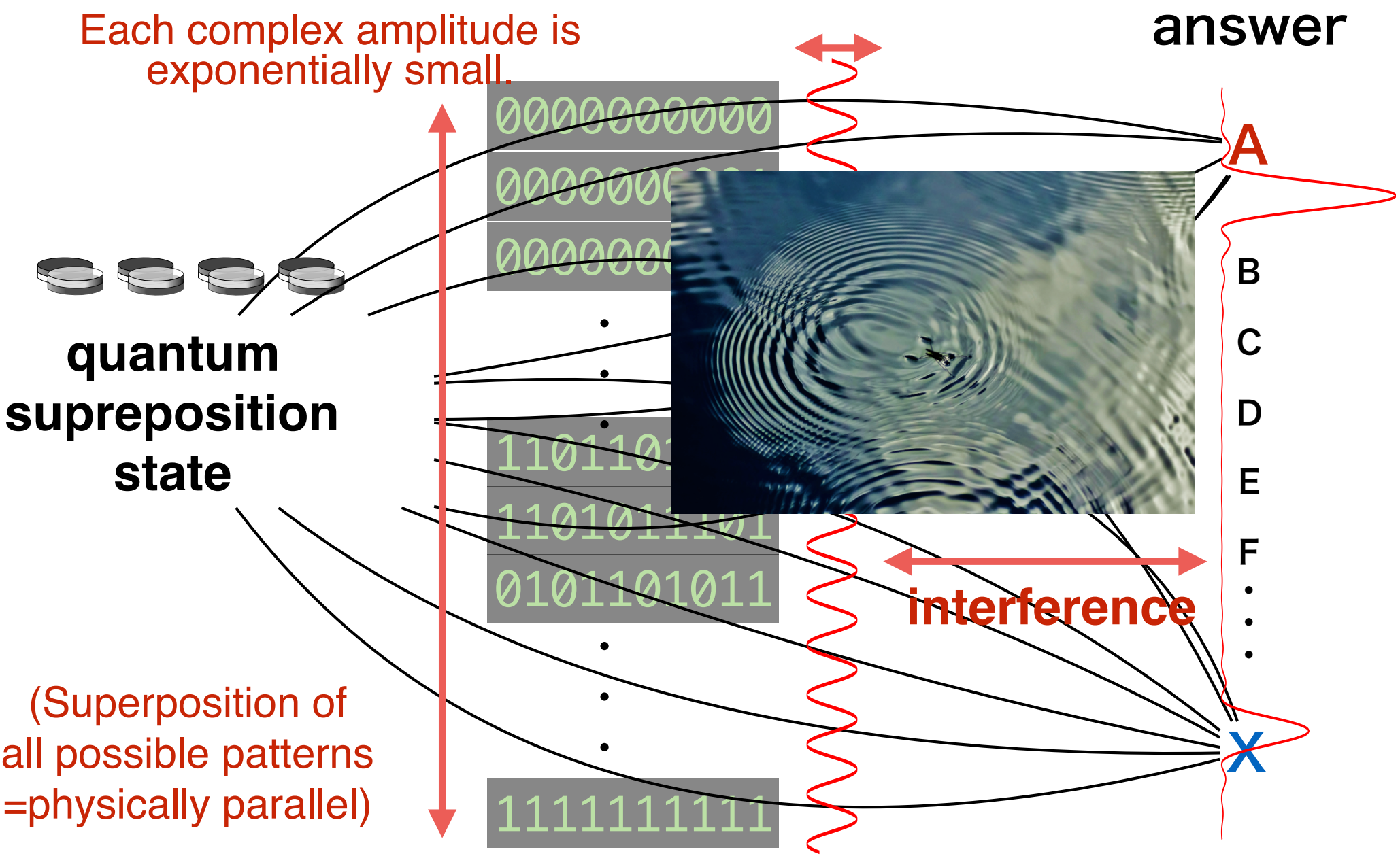
http://www.nobelprize.org/nobel_prizes/physics/laureates/1965/feynman-bio.html

*"I'm not happy with all the analyses that go with just the classical theory, **because nature isn't classical**. If you want to make a **simulation of nature** you'd better make it quantum mechanical"*

1981(Texas) "Physics and Computation"
Then you guys are using wrong physics….
*→**universal quantum computer 1985***

http://www.daviddeutsch.org.uk
David Deutsch (1953-)

How quantum computer works

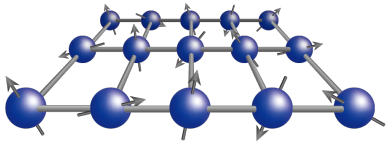


Quantum easy problems

- Intrinsically quantum related problems:

  Quantum chemistry · quantum material science

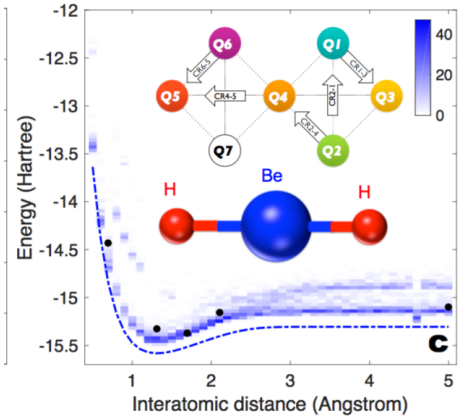
  → Quantum speedup is ubiquitous!



Nature **549**, 242–246 (14 September 2017) | doi:10.1038/nature23879

Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets

Abhinav Kandala , Antonio Mezzacapo , Kristan Temme , Maika Takita , Markus Brink , Jerry M. Chow & Jay M. Gambetta



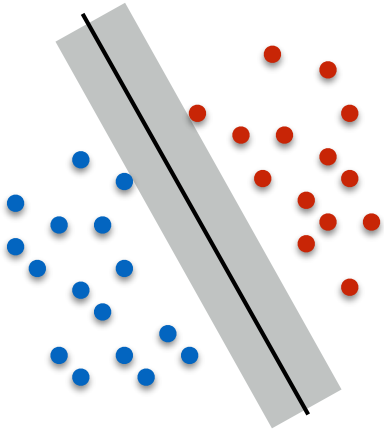
- Not intrinsically quantum but has a nice structure

  Factoring · PCA · SVM · Clustering ·

  (sparse, data encoded quantum state)

  recommendation system (Amazon, Netflix)

  → Calculation of eigenvalue & singular value using the linear algebraic structure of quantum systems.



QSVM

Rebentrost-Mohseni-Lloyd, PRL **113**, 130503 (2014)

Quantum industries

Microsoft

QuArC, StationQ etc…

豊田通商 DENSO Crafting the Core RECRUIT

1QBit QC WARE The Quantum Computing Company™ D-Wave

Quantum annealing（Ising problem）

IBM

intel

QUTech

QuTech@Delft

QuSoft

QuSoft@Delft

Google

+UCSB(Martinis)

qci

Quantum circuit inc.
@Yale University
(Schoelkopf, Devoret)

Quantum Native Systems QunaSys

IONQ

Univ. (Monroe)

20 qubits systems are already reached.
>**50 qubits** (1Peta dimensions) systems are already fabricated and would work in the near future.

NVIDIA

中国科学院 CHINESE ACADEMY OF SCIENCES

(A16Z: Andreessen Horowitz)

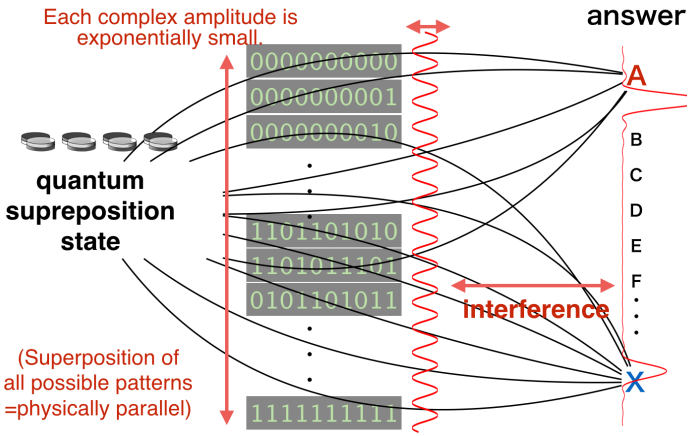
Silicon Quantum Computing Pty
(UNSW)

Quantum computer and blockchain

Proof of Work: computationally costly part

01011011 ⟵ h(?????) = 000101
preimage

→ *Grover's quantum search*
(only quadratic speedup, less impact)



Digital signature: Public-key cryptography, RSA, ECDSA ..

Sig(message, private_key) = signature

computationally hard

Verification(message, signature, public_key) = true/false

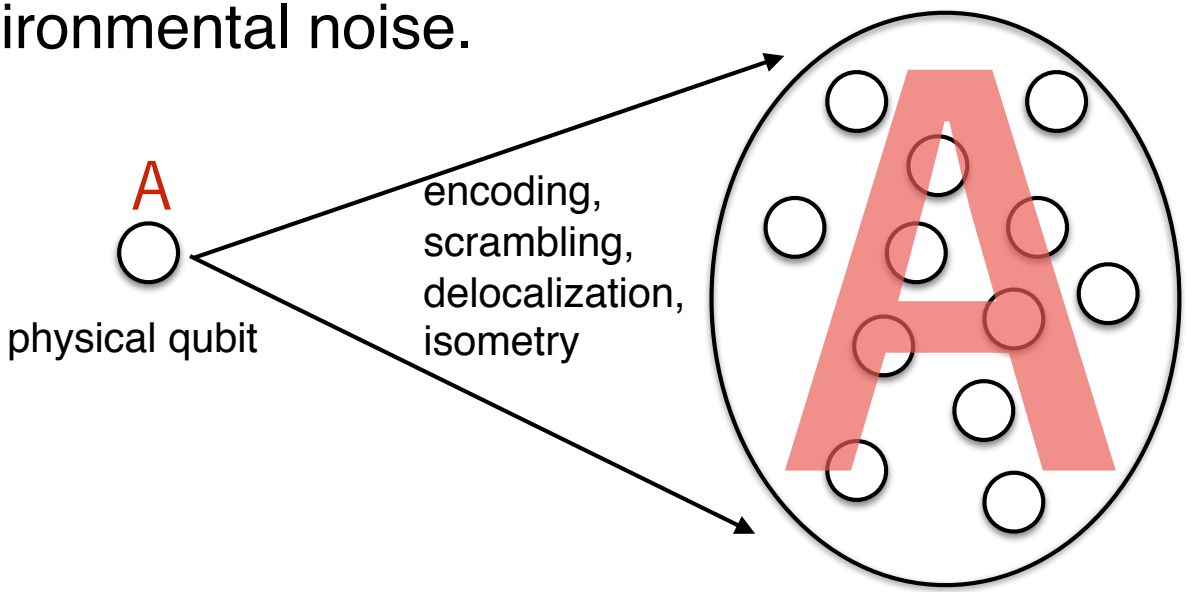
hardness of factoring, discrete logarithm → Shor's quantum algorithm

Summary

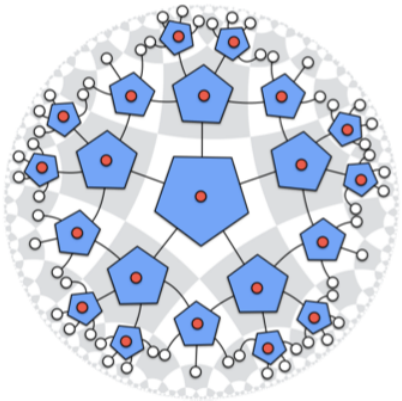
- Quantum computer: a computer that works under quantum mechanical law, and hence can efficiently simulate nature.
- IT giants are currently heavily engaged in developing quantum computers and exploring complex quantum frontier.
- Hacking a quantum computer provides us a deep insight about quantum physics, topological order, holographic principle, black hole etc…
- Potentially, quantum algorithms are effective on blockchain (PoW, DSA), but there would be no threat in a near feature.
- It would be interesting to explore blockchain for quantum computing and quantum computing for blockchain.

Quantum computer and high energy physics

Quantum error correction:
protection of quantum information from environmental noise.



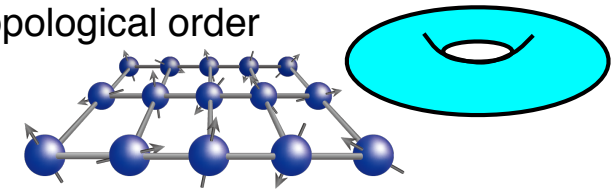
Holographic principle



(b) Holographic pentagon code

[Pastawski et al., JHEP '15]

Topological order



[Kitaev. Ann. Phys. '03]

Blackhole information paradox:
quantum information solution → fast scrambling: Blackhole is the fastest quantum computer in universe!