Quantum Computing

Hendrik Santoso Sugiarto

TECH

Alphabet shares jump 6% after Google touts ‘breakthrough’ quantum chip

PUBLISHED TUE, DEC 10 2024•2:22 PM EST | UPDATED TUE, DEC 10 2024•4:58 PM EST

Kif Leswing
@KIFLESWING

Google 'Willow' quantum chip has solved a problem the best supercomputer would have taken a quadrillion times the age of the universe to crack

News By Keumars Afifi-Sabet published December 9, 2024

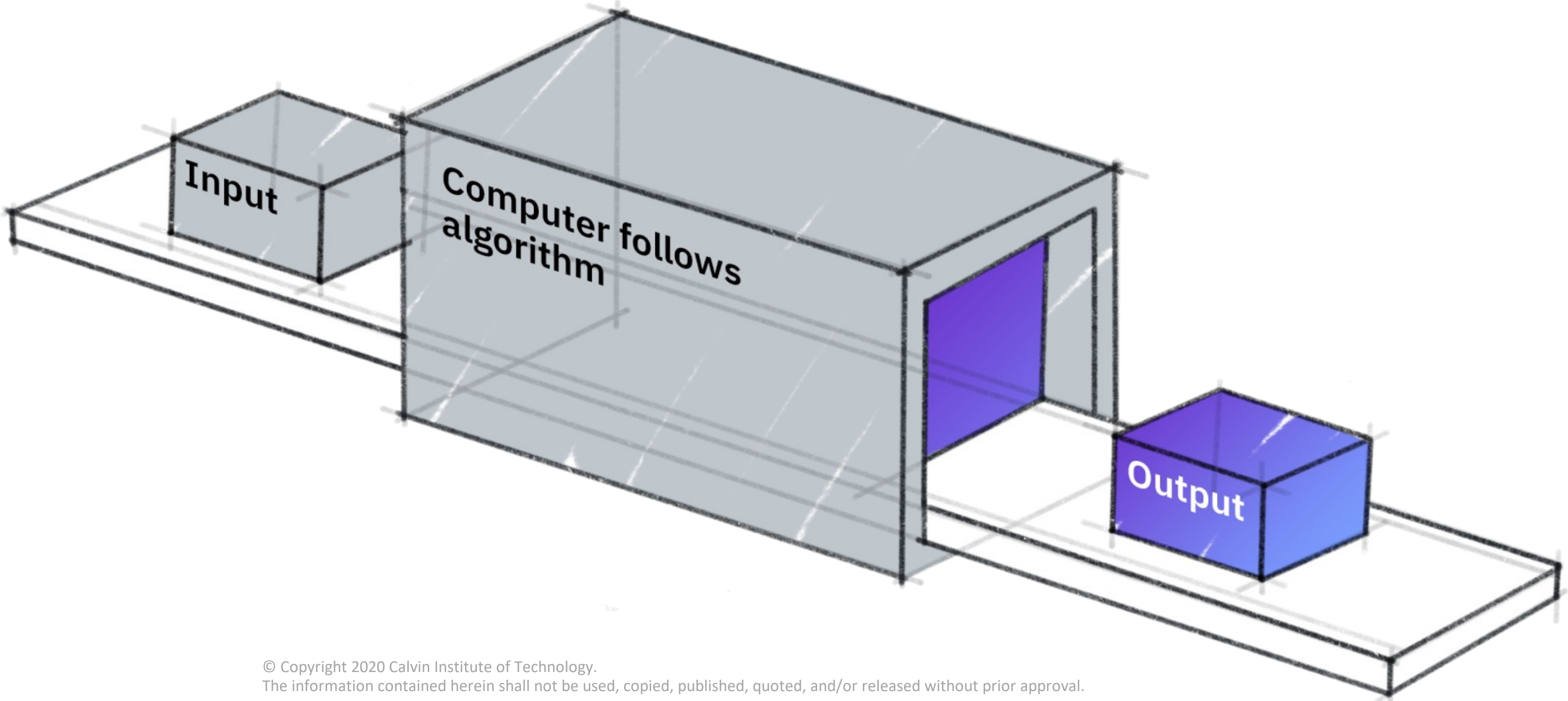
Google's new 105-qubit "Willow" quantum processor has surpassed a key milestone first proposed in 1995 — with errors now reducing exponentially as you scale up quantum computers.

CALVIN INSTITUTE OF TECHNOLOGY

Quantum Computer

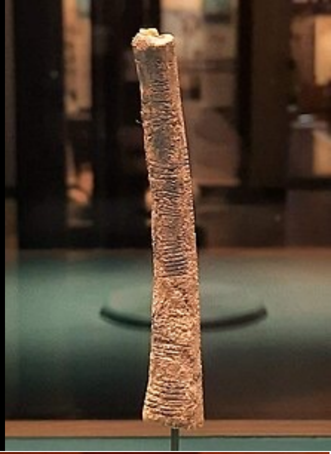
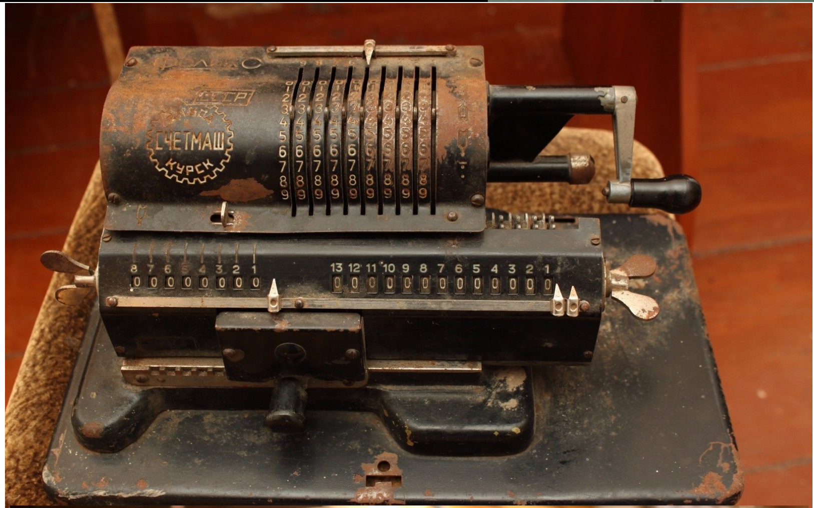
Apa itu Komputer?

- Komputer mempunyai beragam bentuk: cloud, laptop, smartphone, sistem logistik, dll
- Semuanya memiliki kesamaan: proses pengolahan dari input informasi menjadi output informasi dengan menggunakan himpunan instruksi (algoritma).



Computer Evolution

- Hunter-gatherer: Tally Sticks
- Agricultural (neolithic) revolution: Abacus
- 1^{st} Industrial (mechanical) revolution: Mechanical Calculator
- 2^{nd} Industrial (electrical) revolution: Electronic Calculator
- 3^{rd} Industrial (digital) revolution: Personal Computer
- 4^{th} Industrial (internet) revolution: Cloud Computer
- 5^{th} Industrial (quantum) revolution: Quantum Computer

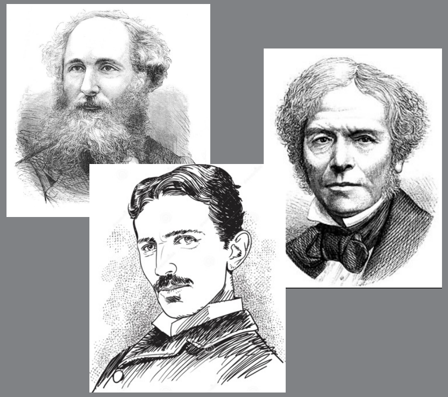


Development of Information Technology

Abad 19	Abad 20	Abad 21	Abad 22
Electromagnetism	Information Theory	IT Industry	
	Quantum Theory	Quantum Information	Quantum IT Industry

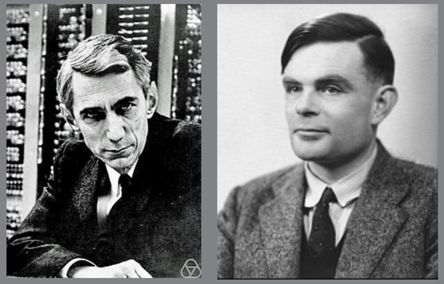
Abad 19

Electromagnetism



Abad 20

Information Theory



Quantum Theory

Abad 21

IT Industry

Google, Facebook, amazon, IBM, Microsoft, ORACLE

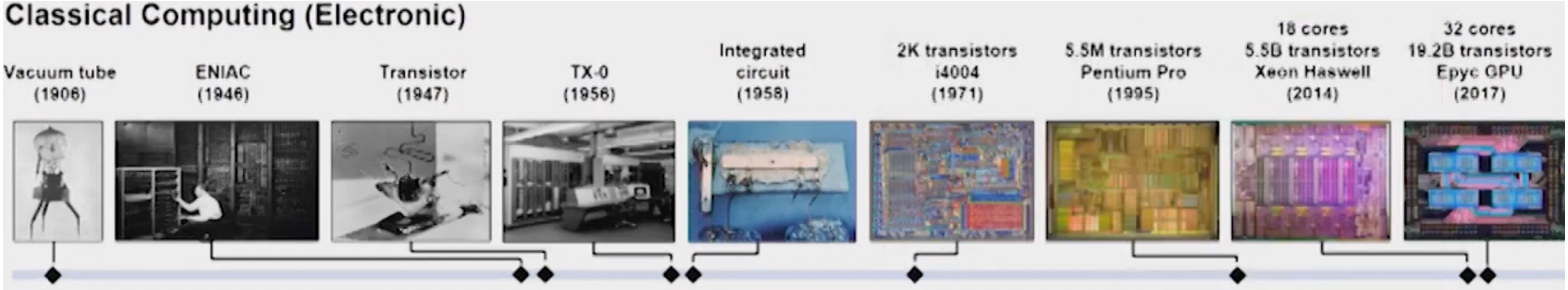
Quantum Information

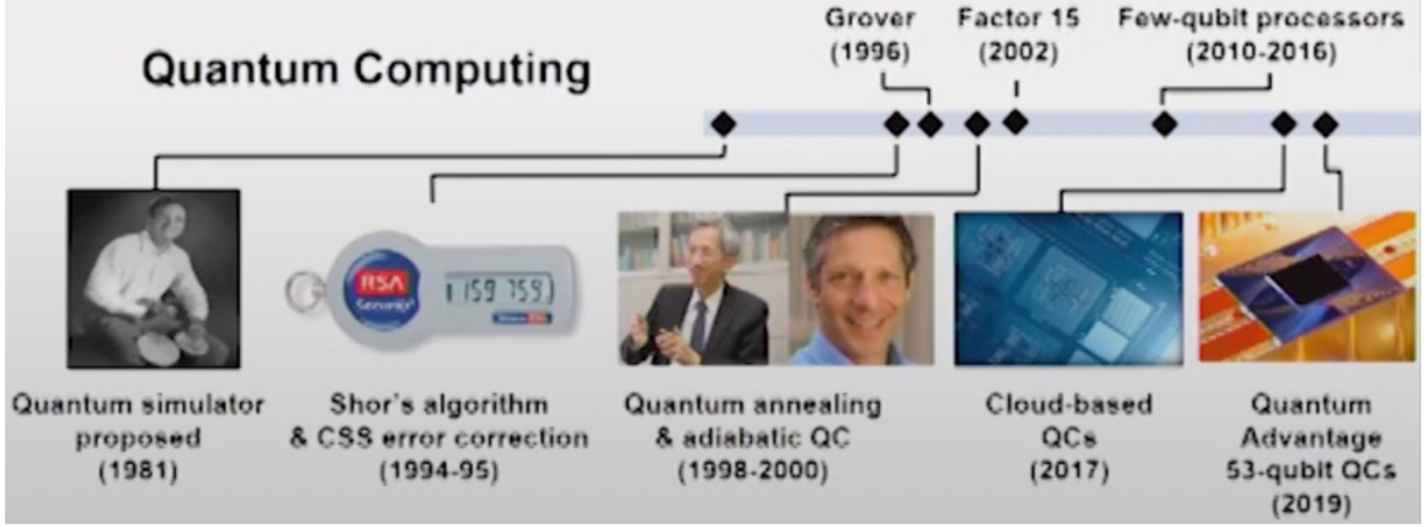
Abad 22

Quantum IT Industry

CALVIN INSTITUTE OF TECHNOLOGY

Computing Timeline

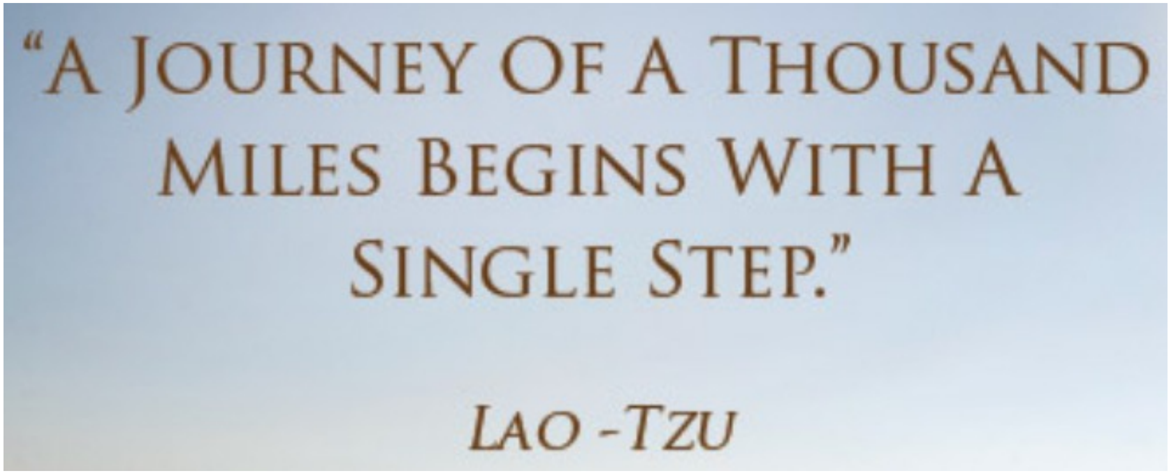


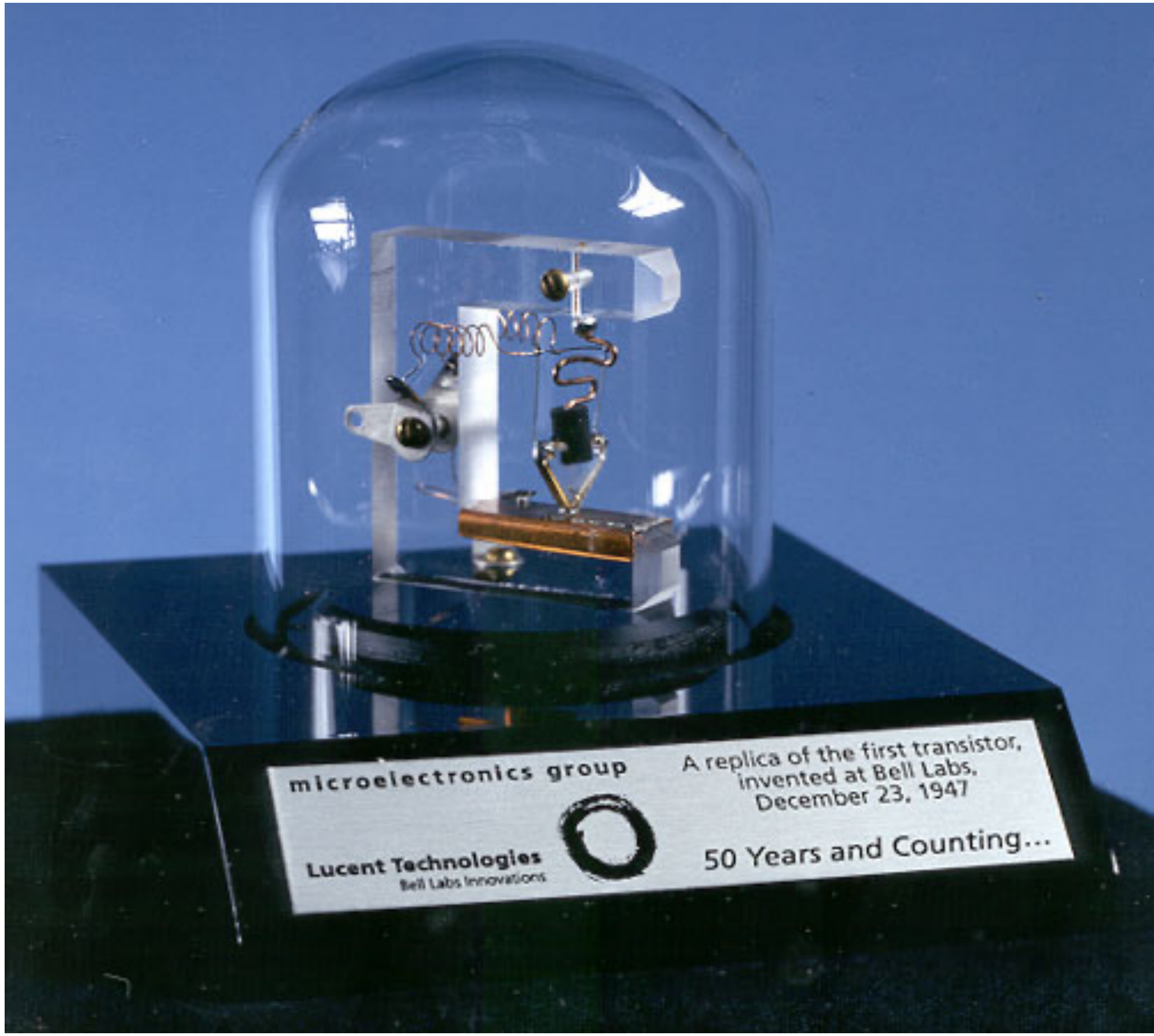


https://extremecomputingtraining.anl.gov/wp-content/uploads/sites/96/2022/11/ATPESC-2022-Track-1-Talk-11-Alexeev-Quantum-Computing-Trends.pdf

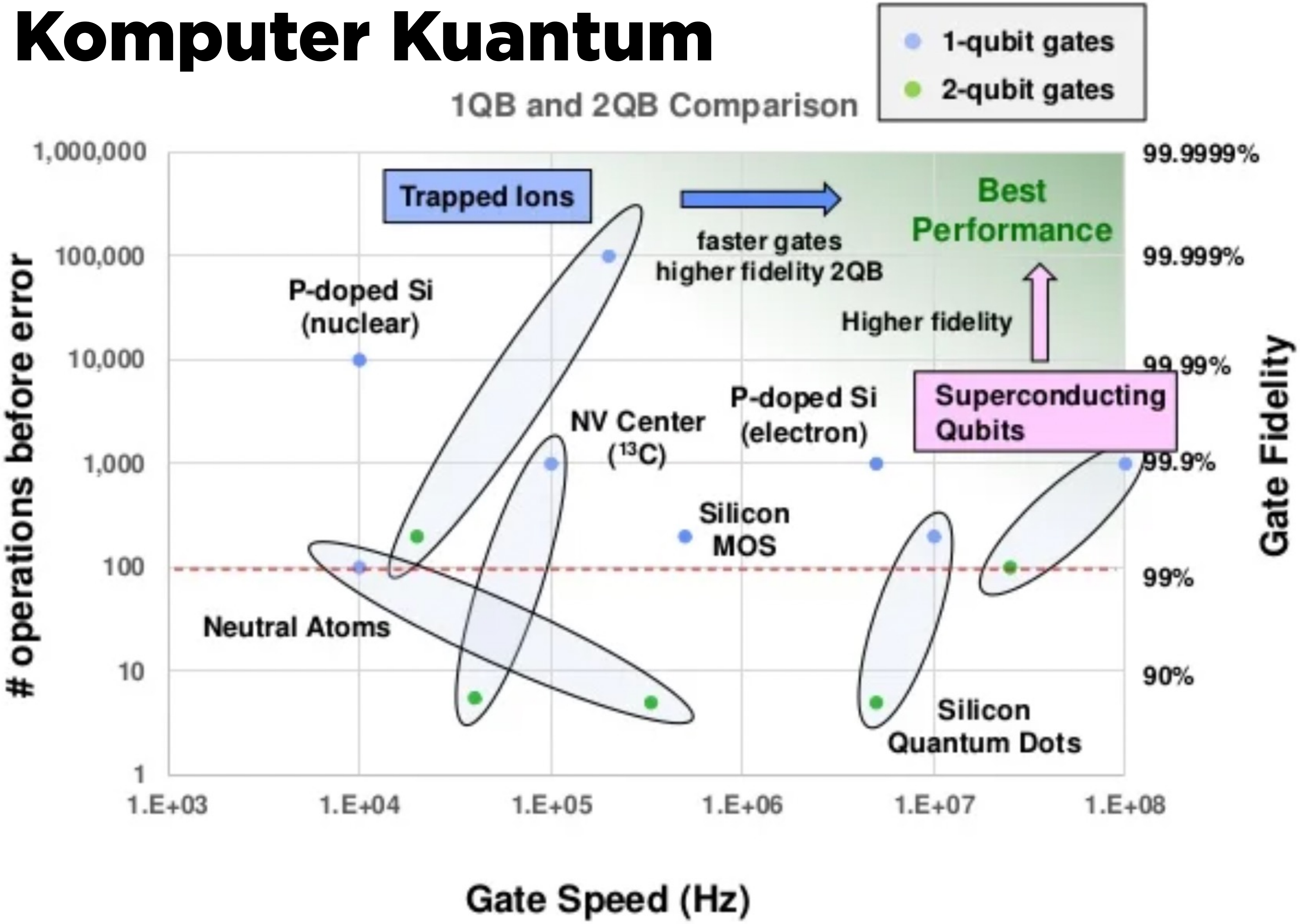
Small Steps in Technology

- Transistor pertama (1947)
- 70 tahun kemudian:
  - 1 prosesor memiliki miliaran transistor





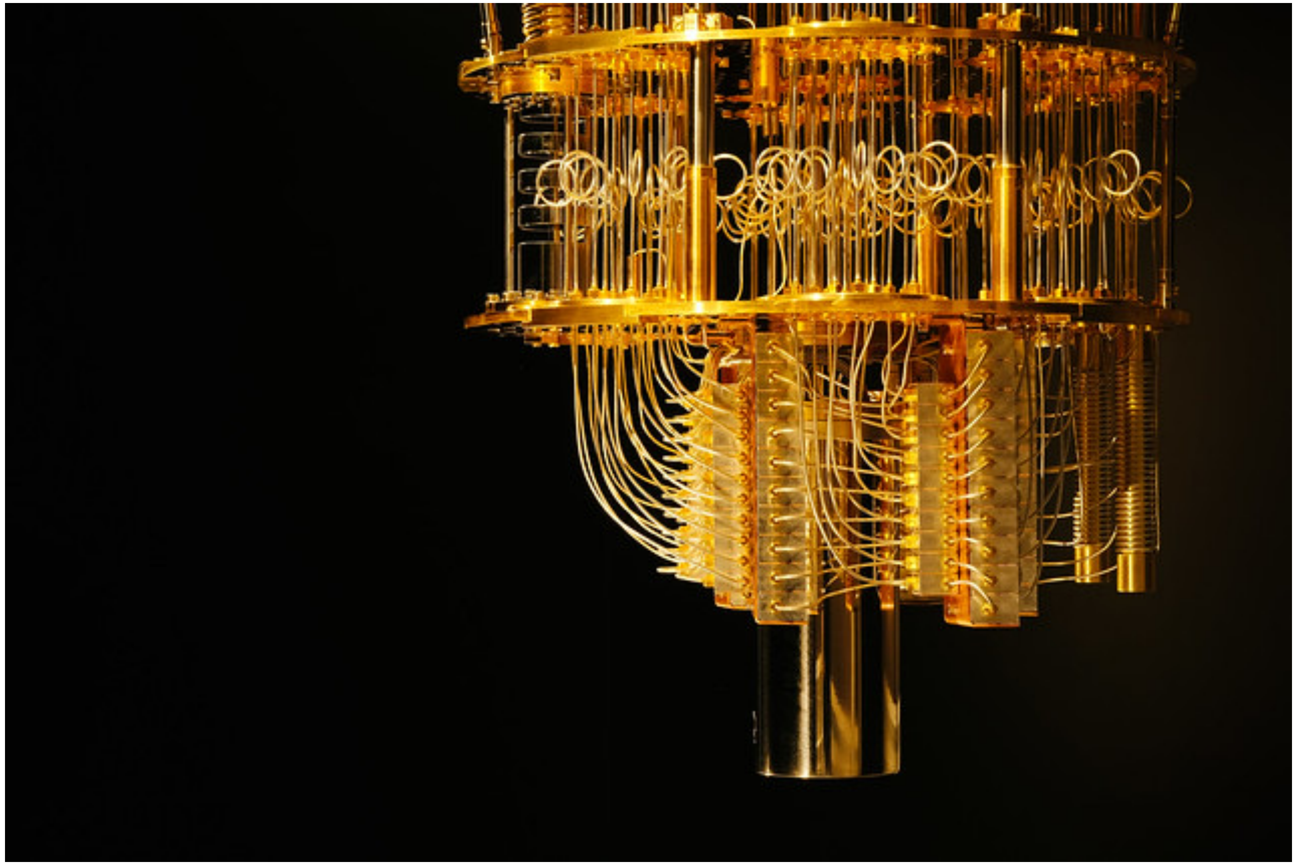
Kandidat Komputer Kuantum

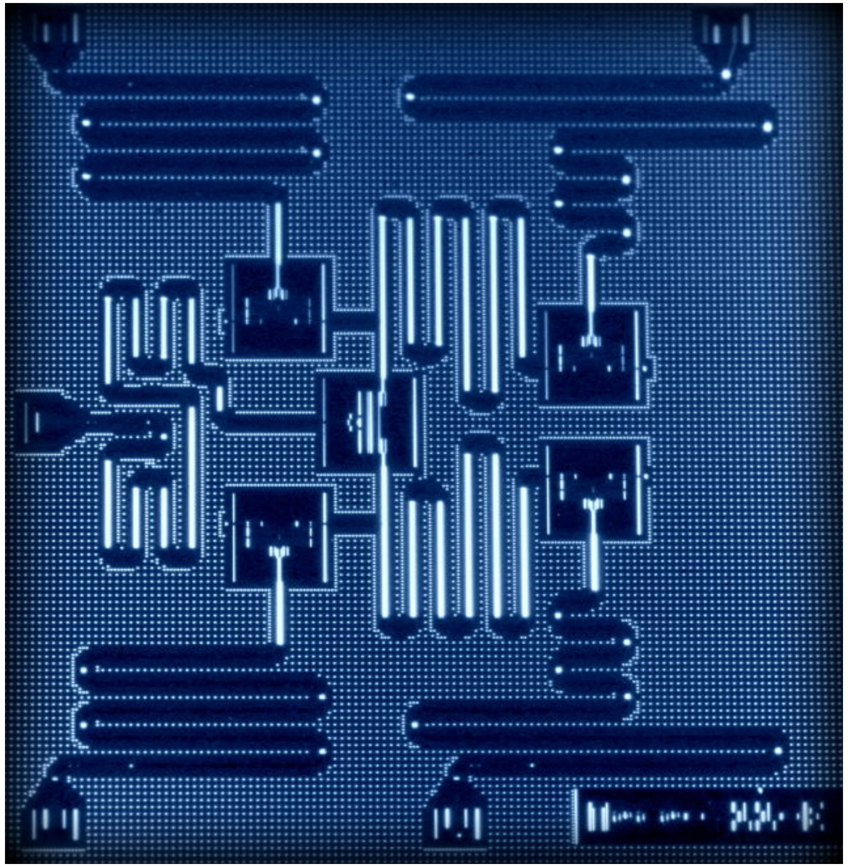


CALVIN INSTITUTE OF TECHNOLOGY

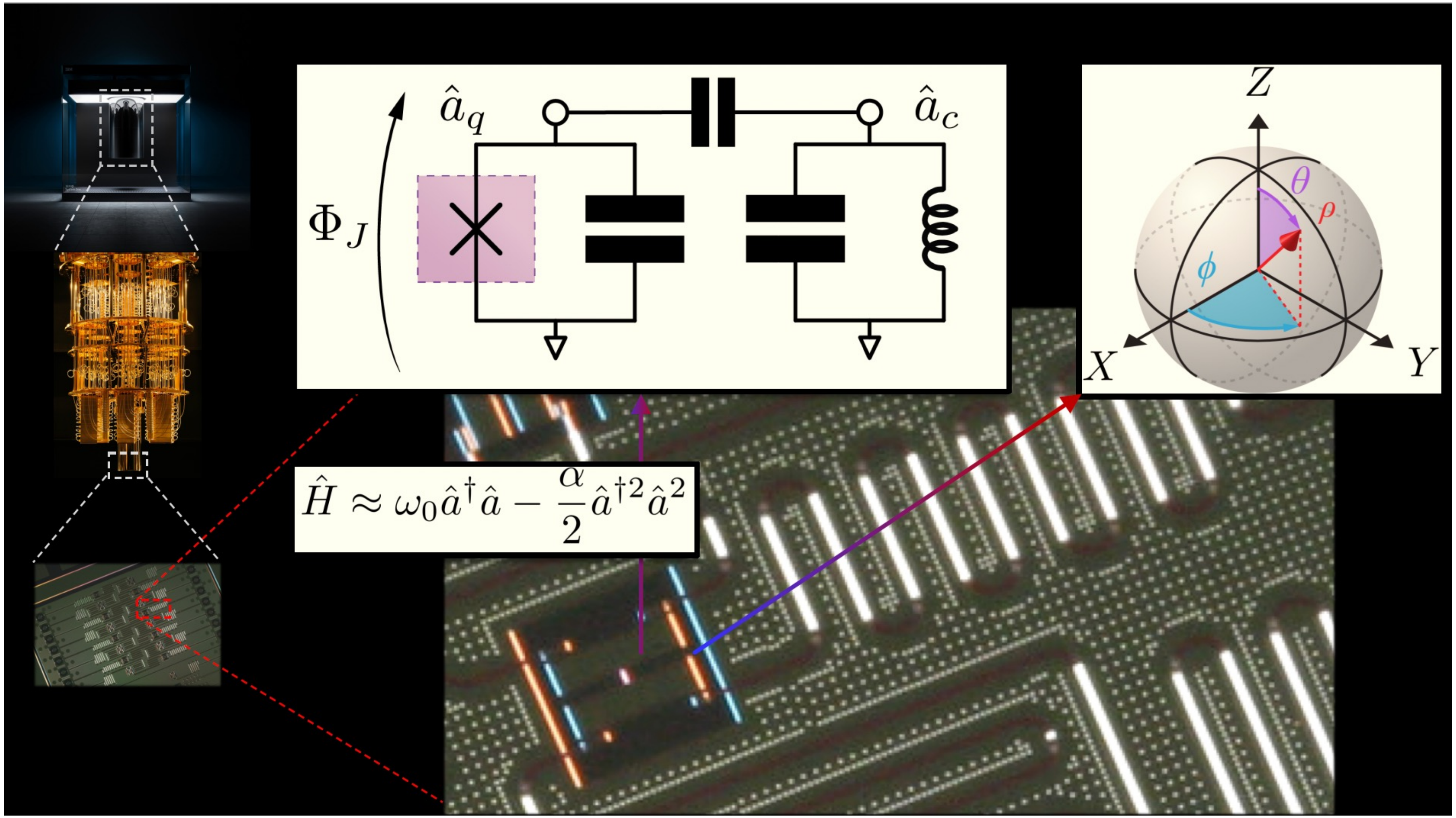
Quantum Processor

- IBM Superconducting Transmons (5-qubits Falcon)





Quantum Oscillator



Perbandingan Paradigma

Paradigma	Kubit	Entanglement	Gate	Skalabilitas	Pemeliharaan	Pengembang
Superconducting	Fluks kubit	Mudah	- Kecepatan Tinggi - Fidelitas Tinggi - Waktu Koherensi	Cukup mudah	- Temperatur 10mK	IBM, Google, rigetti
Photonics	Polaritas foton	Sulit	- Cepat - Fidelitas baik yang menjanjikan - Waktu Koherensi	Sulit	- Temperatur ruang	Xanadu
Trapped Ions	Level energi dari ion yang terperangkap.	Mudah	- Pelan - Fidelitas Tinggi	Agak sulit	- Medan Listrik yang berosilasi (perangkap ion).	IonQ, MIT, Oxford
Neutral Atoms	Energi level atom.	Mudah	- Waktu koherensi yang lama	Sulit	- Vakum temperatur ruang. - Laser sebagai "penjepit" optikal.	Pasqal
Quantum Dots	Putaran Elektron	Cukup mudah	- Fidelitas tinggi	Sulit namun berpotensi semakin mudah	- Kotak Kuantum - Ruang gelap pada suhu 4° Celsius.	Intel
Diamond Vacancies	Level energi elektron	Sulit	- Waktu Koherensi yang baik - Gerbang 2 kubit memiliki fidelitas rendah	Cukup sulit	- Tempratur ruang - vakum Tingkat tinggi.	Briliance
NMR	Putaran Nuklei	Mudah	- Efisien - Waktu Koherensi yang baik. - fidelitas yang menjanjikan (jumlah kubit kecil)	Sulit	- Temperatur ruang	SpinQ
Topological	Arah anyon	Mudah	- Tahan terhadap gangguan	Cukup mudah	- Medan magnet yang kuat. - Topologi superkonduktor, superkonduktor-isolator topologi/semikonduktor	Microsoft
Bosonic	Superposition of energy levels	Mudah	- Tahan terhadap gangguan	Cukup mudah	- Perlindungan QEC. - Arsitektur QED.	Delft, Tsinghua

Quantum Computing

Klasik vs Kuantum

Komputer Klasik

state (θ) → dynamics ($\theta' = A(\theta)$) → measurement ($\Delta\theta$’) → observables ($\langle\theta'\rangle$)
input → algorithm → classical noise + output → interpretation

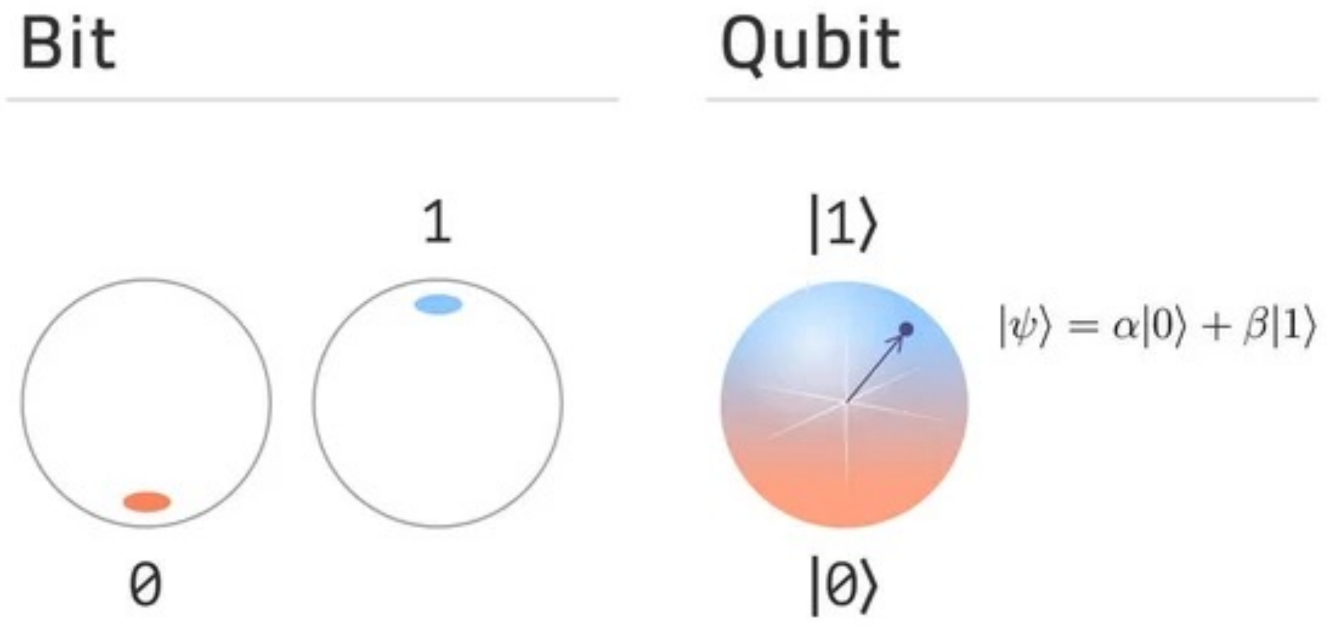
Komputer Kuantum

state ($|\psi\rangle$) → dynamics ($|\psi'\rangle = A|\psi\rangle$) → measurement ($|\psi'_i\rangle$) → observables ($\langle A\rangle$)
encoding → quantum algorithm → collapse to classical bit → interpretation

CALVIN INSTITUTE OF TECHNOLOGY

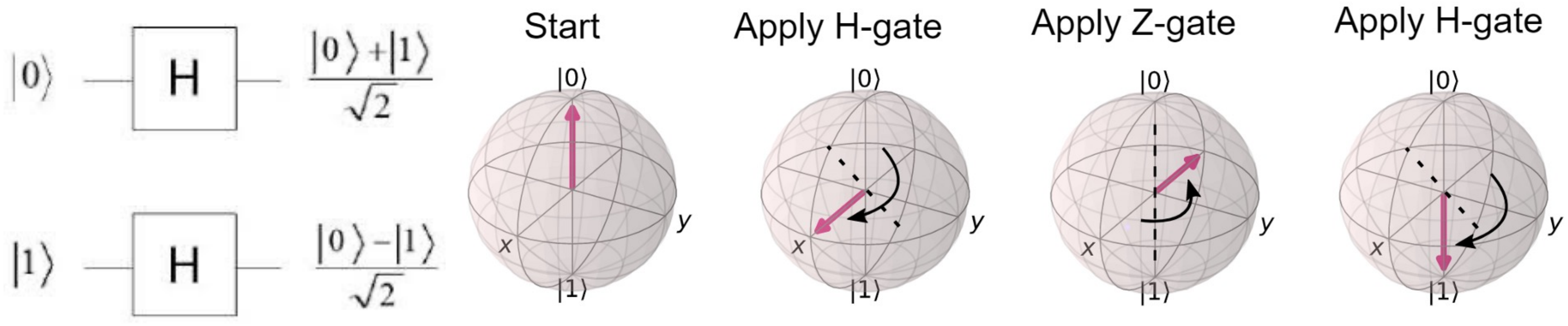
Superposition

- Qubit adalah kombinasi linear dari semua possible states (1 dan 0)



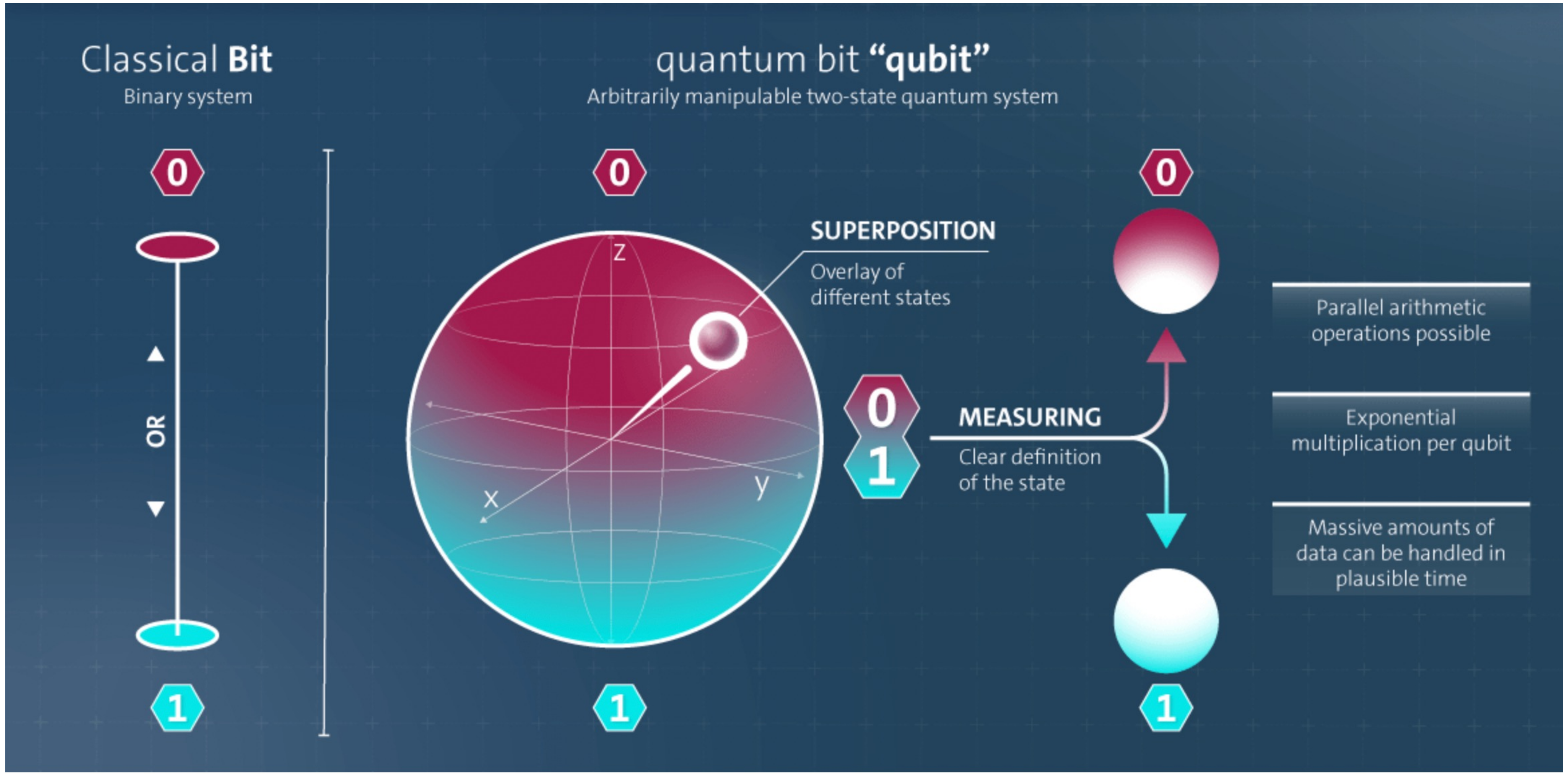
Gates

- Gates adalah operasi yang dapat merubah state qubit
- Beberapa kombinasi gates akan membentuk circuit



Measurement

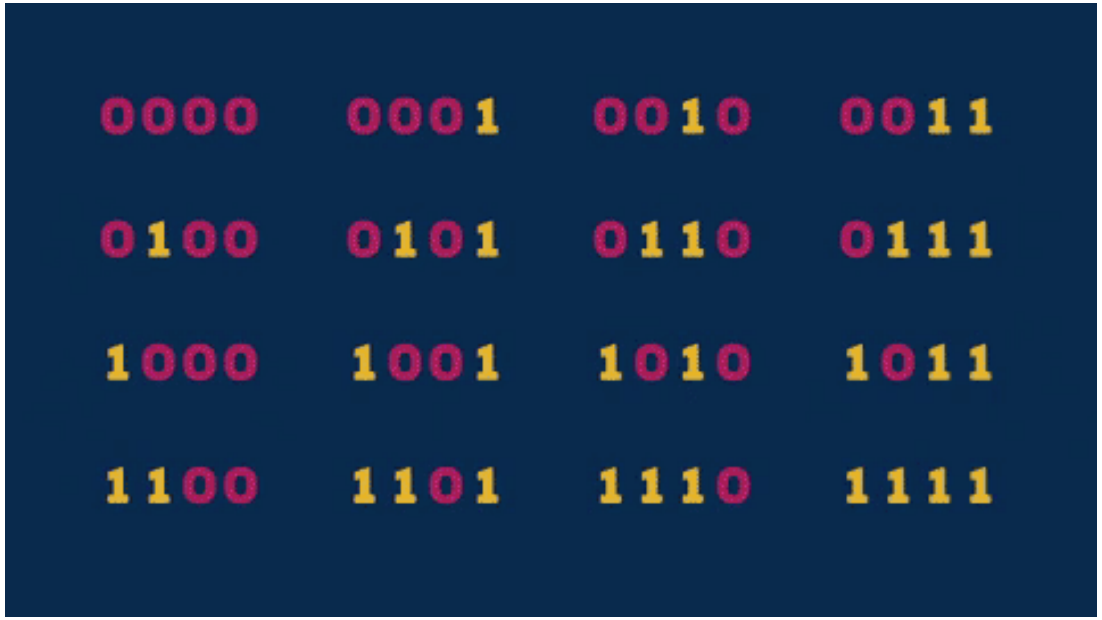
- Collapse of state, $|\psi\rangle\ = \alpha|0\rangle + \beta|1\rangle$
- Antara menangkap sinyal $|0\rangle$ dengan peluang α^2 atau $|1\rangle$ dengan peluang β^2

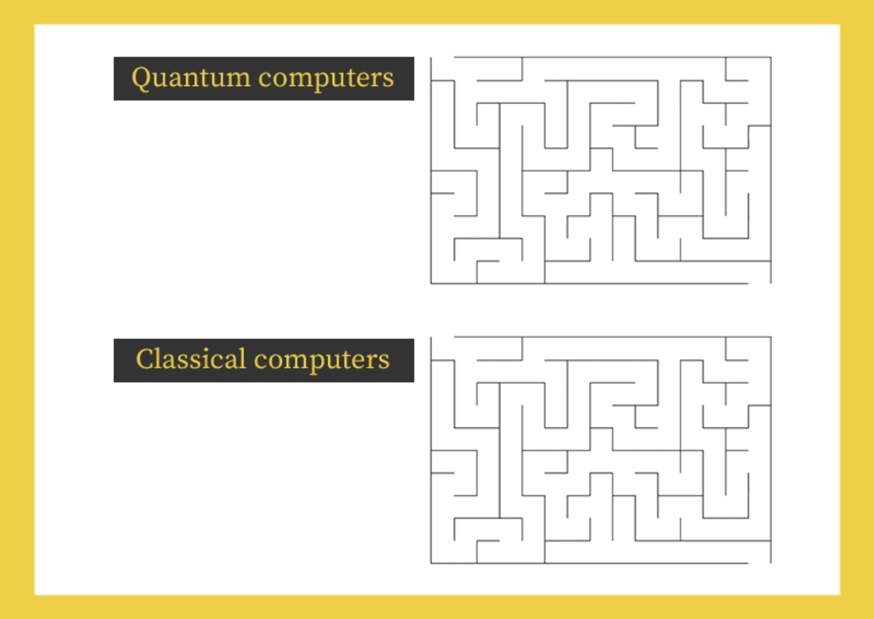


Multiqubit System

- Tensor Product

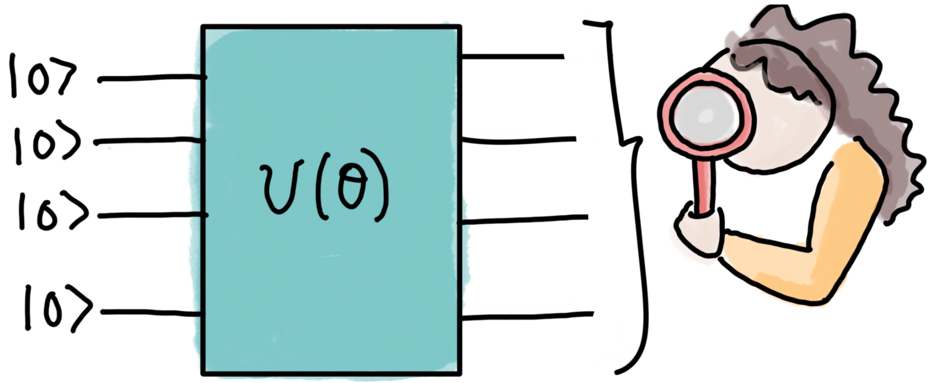
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

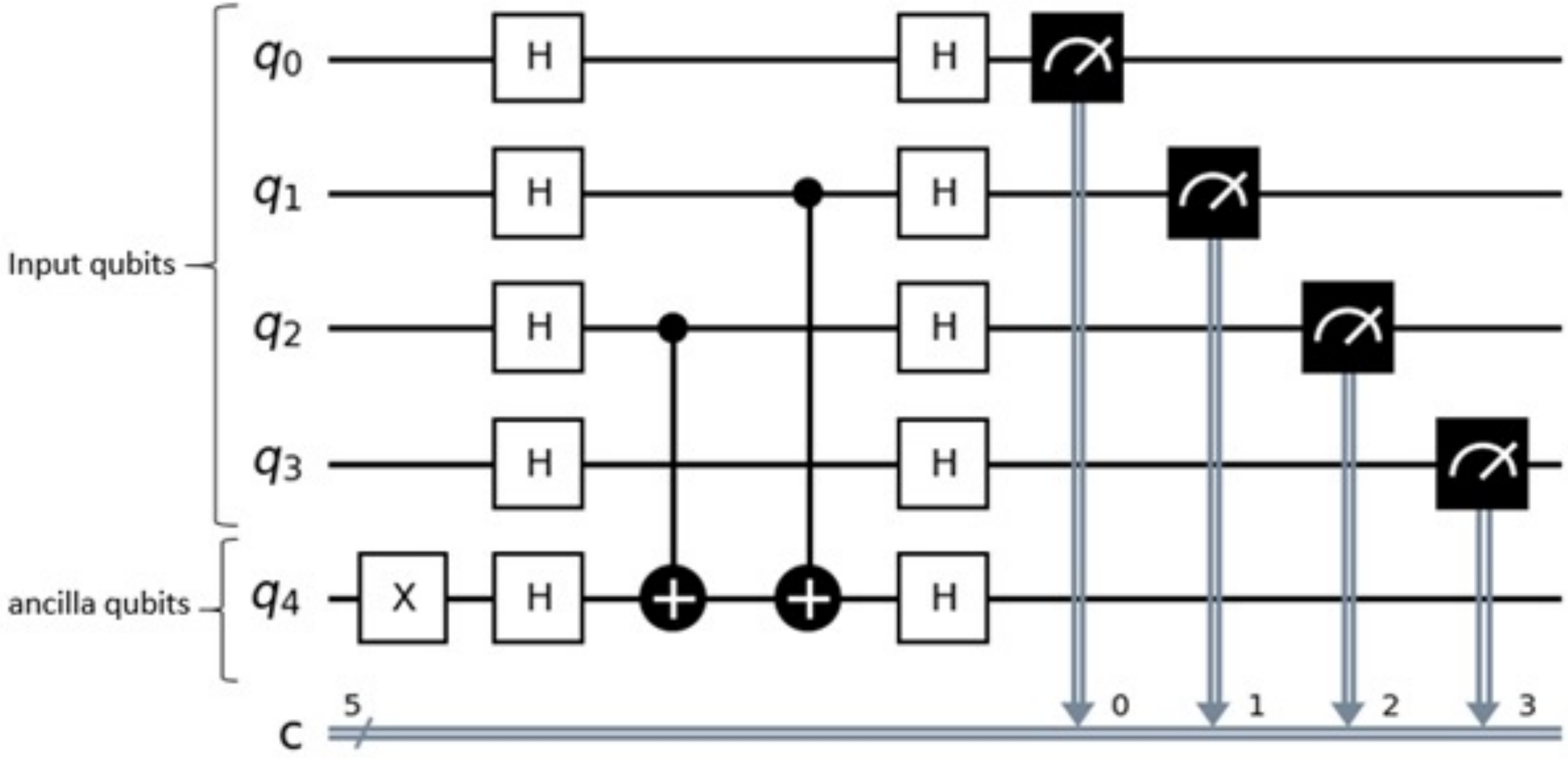




Quantum Algorithm

- $|\psi'\rangle = U|0\rangle^{\otimes n}$





Quantum Computing

Quantum Supremacy

God's People for God's Glory
CALVIN
INSTITUTE OF TECHNOLOGY

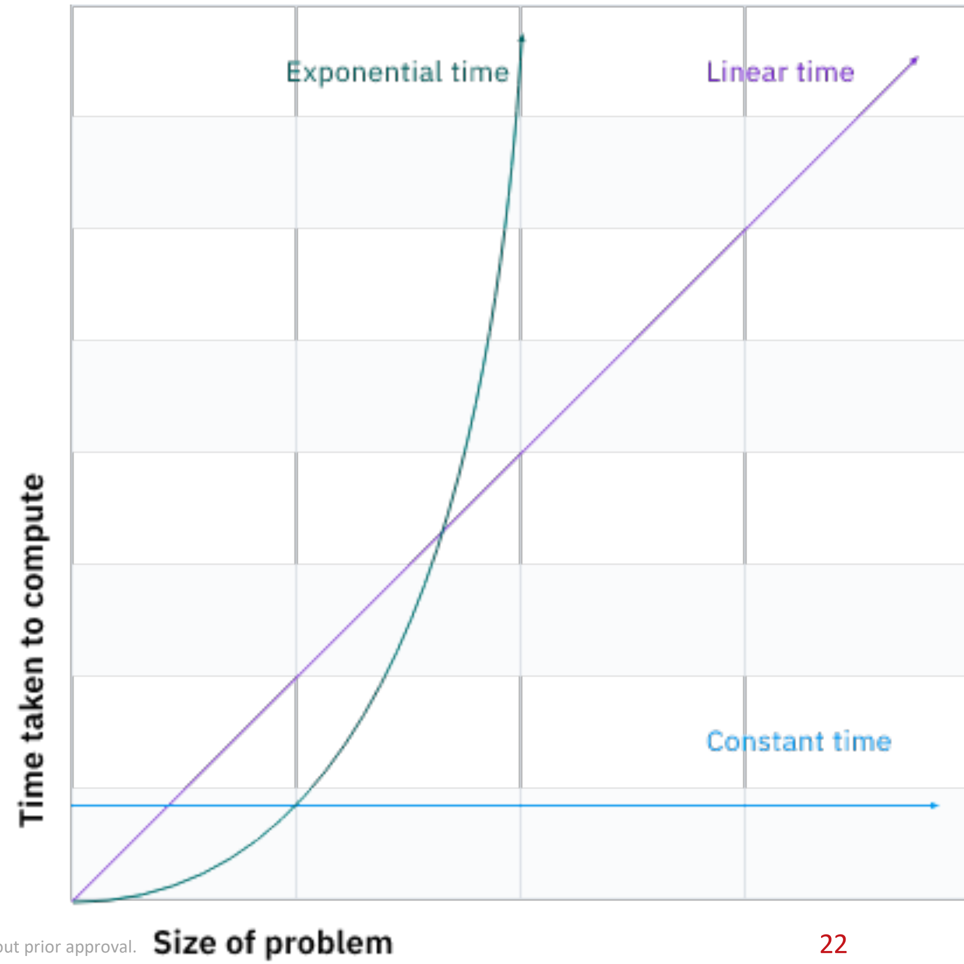
Algoritma untuk Menebak PIN

- Misalkan kita mempunyai angka rahasia (PIN) dan menebaknya dengan menggunakan cara brute-force (mencoba semua kemungkinan). Berapa lama waktu yang diperlukan?

Input	Computer follows algorithm	Output

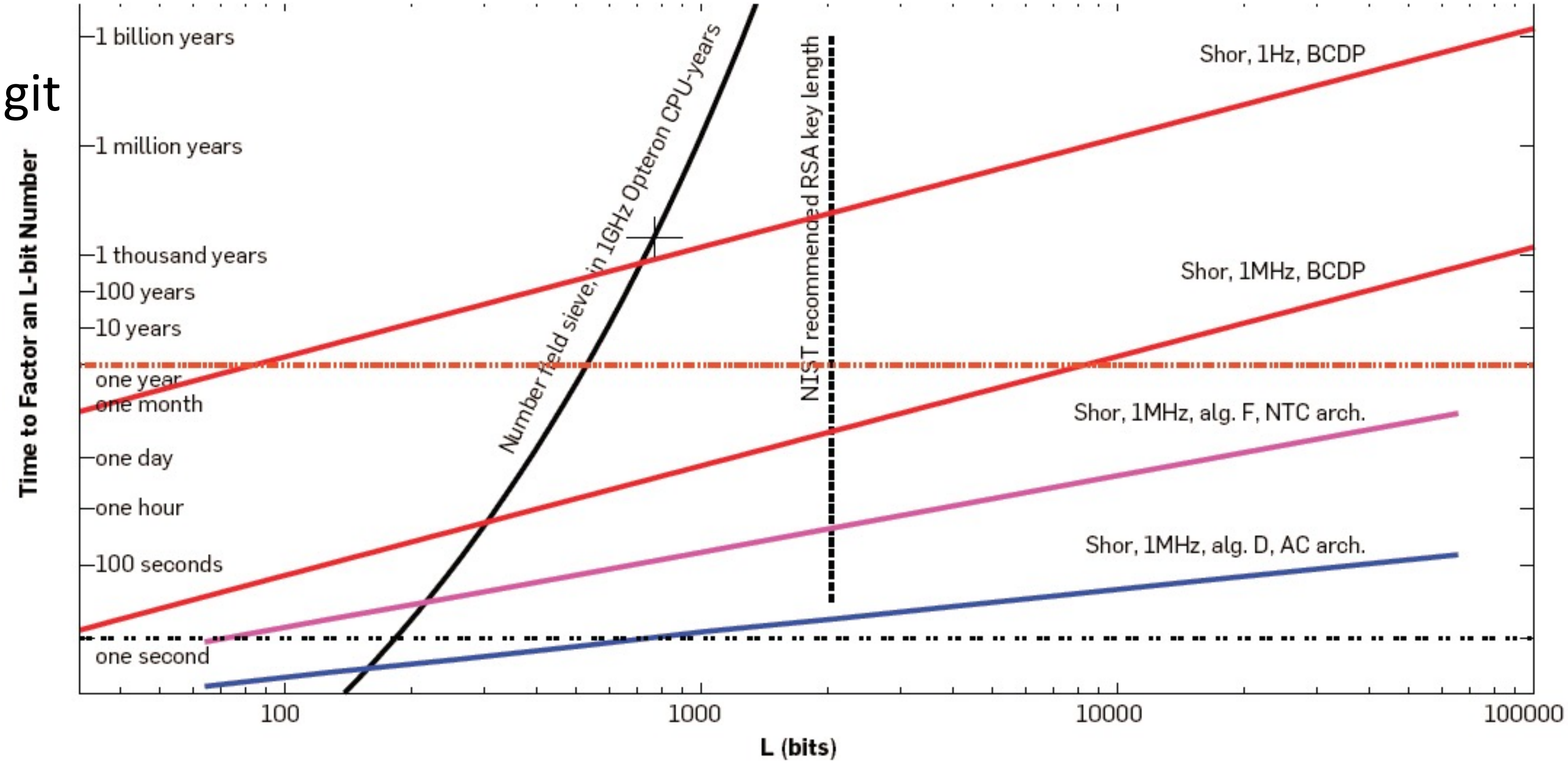
5672	`choose random x between 0 & 9999`
	`if x matches secret number`
	`  output x`
	`else:`
	`  go to start`
		5672

- 1-digit memiliki 10 pilihan (0, 1, 2, 3, 4, 5, 6, 7, 8, 9)
- 2-digit memiliki 100 pilihan ($T \propto 10^d$)
- Misalkan 1 detik untuk 10-digit (5 miliar kombinasi/detik)
- Maka kita membutuhkan:
  - ~150 tahun untuk 20-digit PIN
  - ~150 miliar tahun (120x umur alam semesta) untuk 30-digit PIN



Algoritma Keamanan RSA

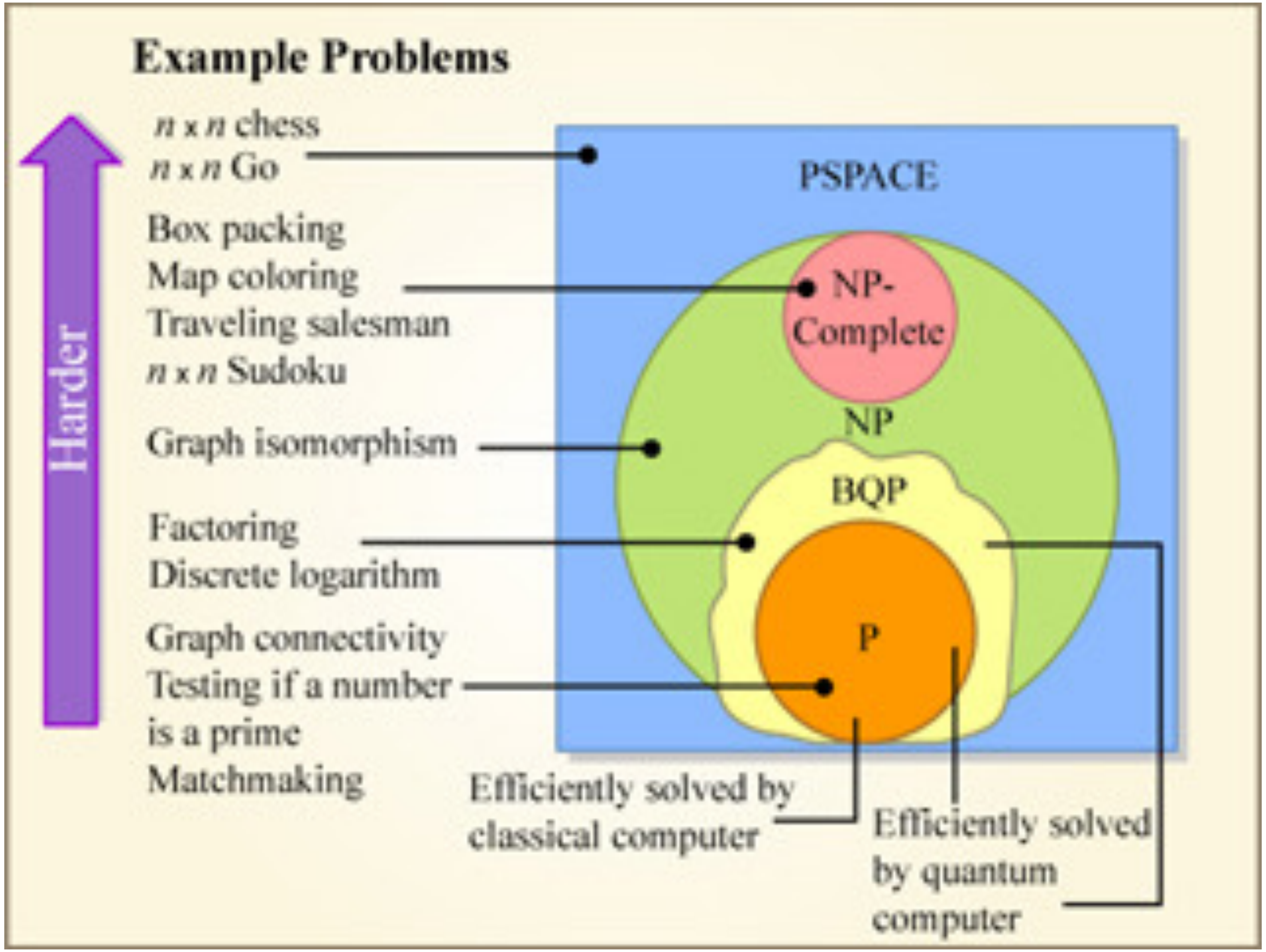
- Integer Factorization
- $p \times q = x$
- Contoh: $13 \times 7 = 91$
- 2700 core year: 250-digit



Quantum Supremacy

Algorithm	Classical Time	Quantum Time	Speedup	Limitation
Factoring[1] (+ related number theoretic)	2^N (for N digits)	N^3	Exponential	Classical runtime limit unproven
Simulation[2] (quantum chemistry)	2^N (for N atoms)	N^c	Exp. in space, polynomial in time	Mapping problem to qubits
Linear systems[3] (Ax=b)	2^N (for N digits)	~N	Exponential	Strict conditions, e.g. sparse matrix
Optimization[4]	2^N	?	?	Empirical
Search[5] (unsorted / unstructured data)	N	$\sqrt{N}$	Polynomial ($\sqrt{N}$)	Data loading

Complexity Space



Keunggulan Komputer Kuantum

- Superposisi
- Non-local (spooky action at distant)
- Kapasitas (peningkatan kompleksitas eksponensial):
  - 20 qubits $= 2^{20} > 1$ juta kemungkinan
  - 100 qubits > semua bits pada hard-drive dari seluruh dunia
  - 300 qubits > seluruh partikel dalam alam semesta
- Performa (bahkan sanggup menembus enkripsi terkuat di dunia)
- Efisiensi (kalor yang dikeluarkan untuk tiap komputasi hampir nol)

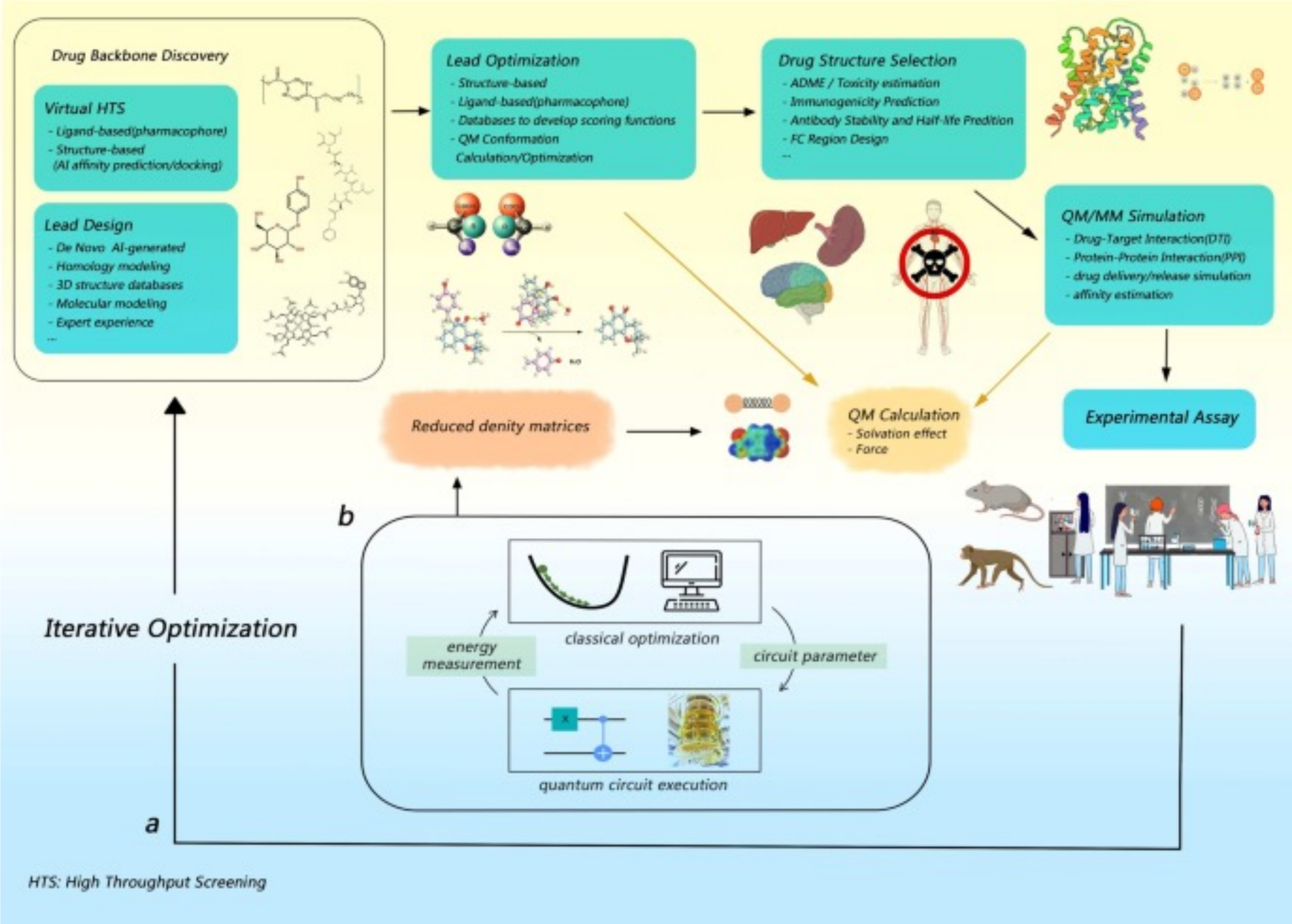
Application of Quantum Computing

God's People for God's Glory
CALVIN
INSTITUTE OF TECHNOLOGY

Aplikasi Komputasi Kuantum

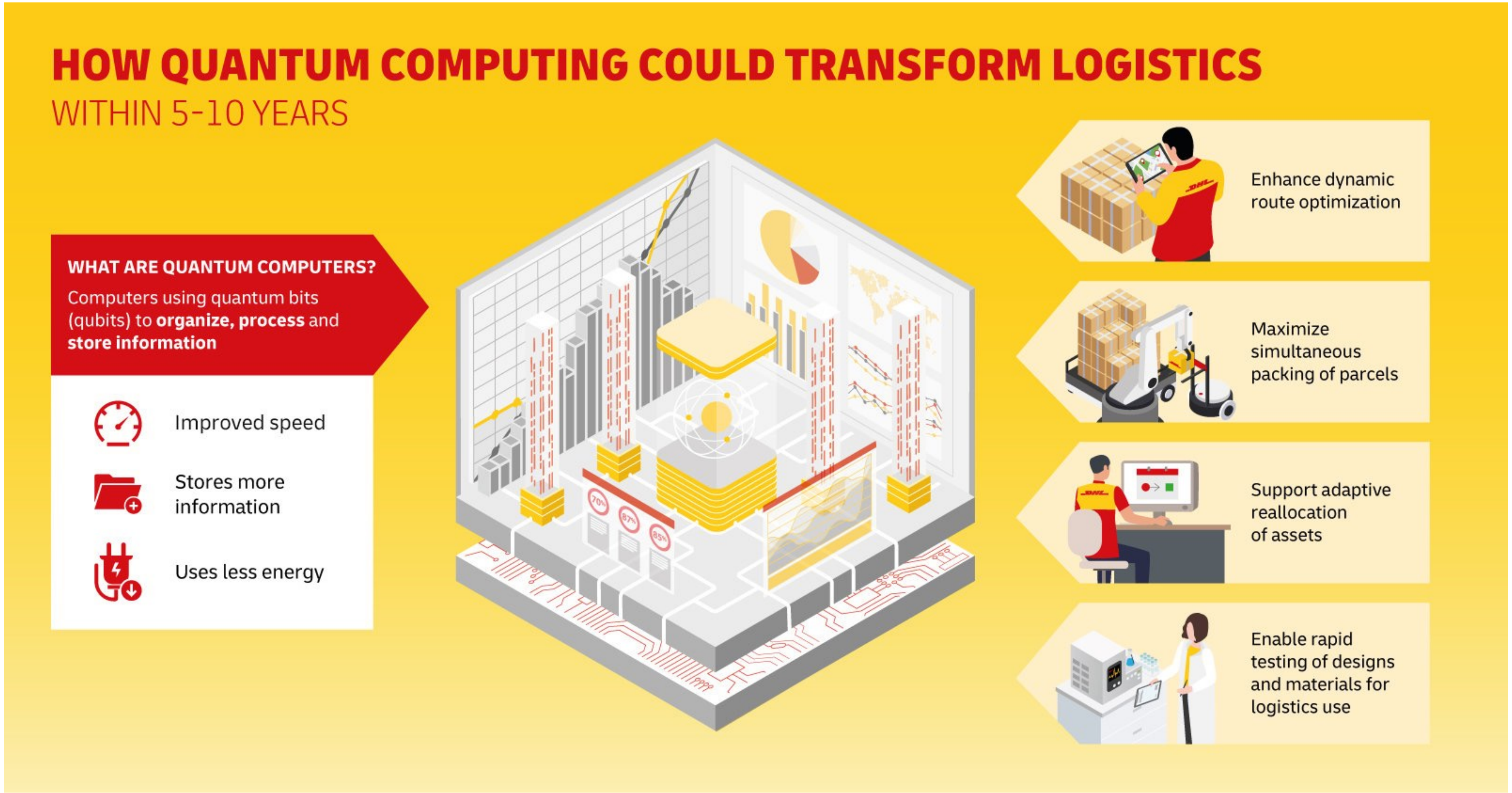
- Quantum Simulation (drug discovery, protein folding, chemical bonding, solid state properties, neuroscience)
- Quantum Optimization (quantum finance, logistic optimization, forecasting)
- Quantum Communication (quantum teleportation, quantum network, quantum internet)
- Quantum Security (quantum cryptography, quantum encryption)
- Quantum Data Management (quantum database, quantum data center)
- Quantum AI (quantum machine learning, quantum neural network)

Drug Discovery



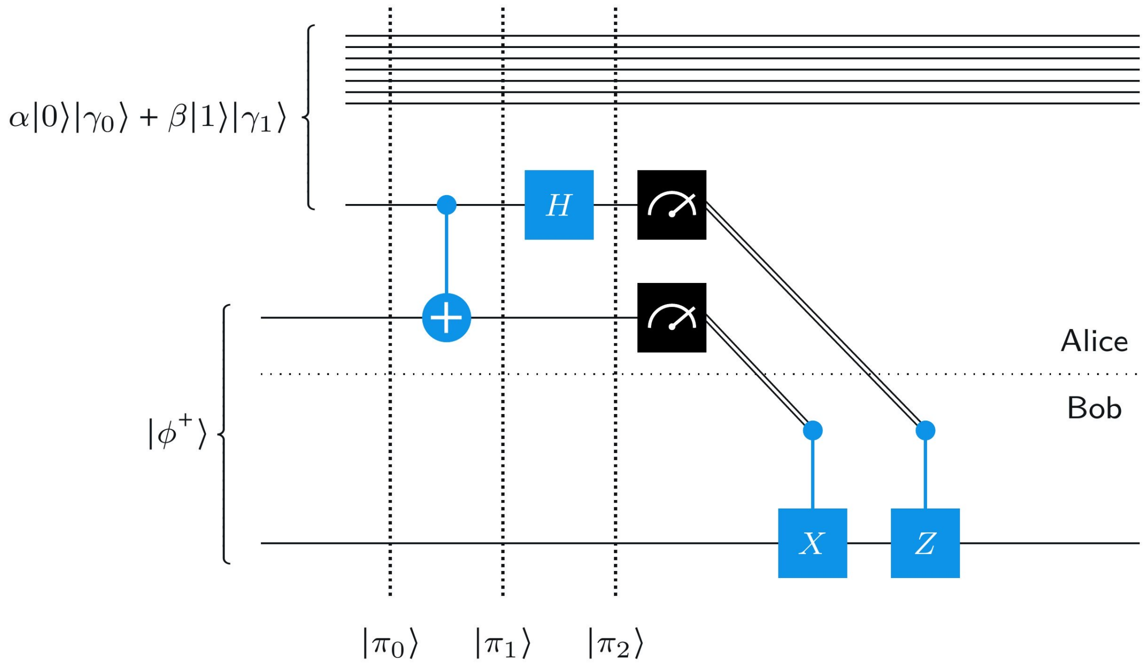
Logistics Optimization

- https://www.youtube.com/watch?v=SC5CX8drAtU



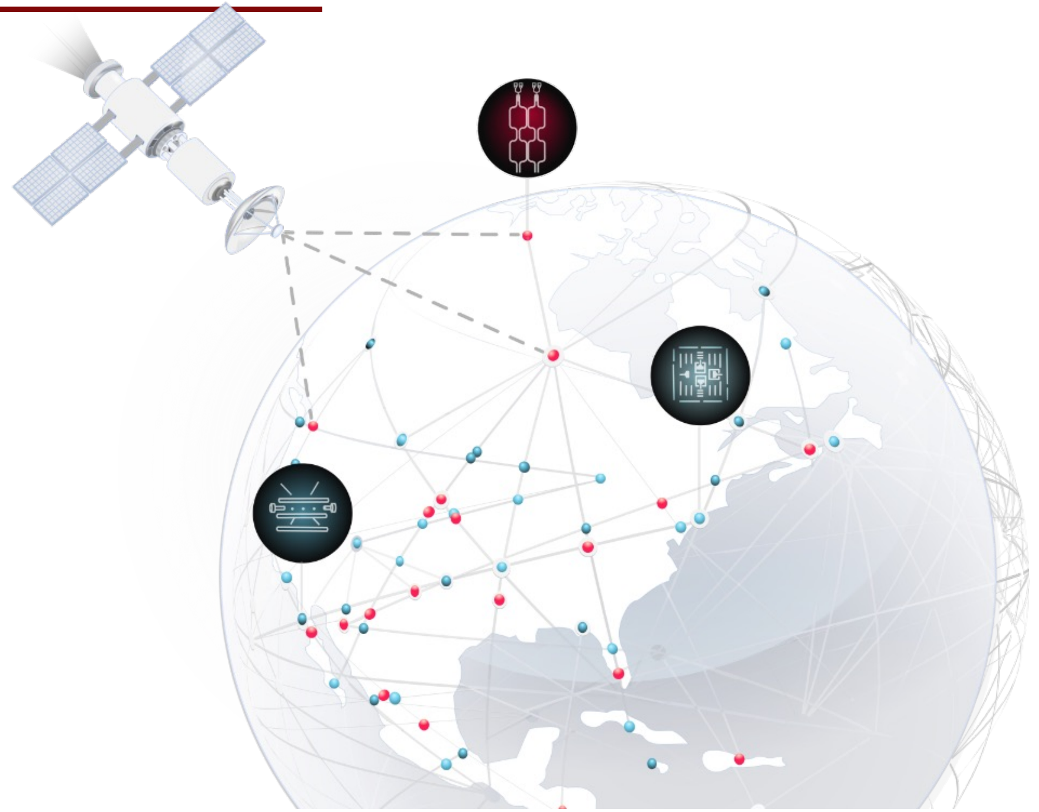
Quantum Teleportation

- Alice ingin mengirim qubit ke Bob dalam state: $|s\rangle = \alpha|0\rangle + \beta|1\rangle$
- Teleportasi: Bob memperoleh $|s\rangle$ sedang milik Alice menghilang
- Protokol: Untuk mentransfer qubit, Alice dan Bob harus menggunakan pihak ketiga untuk mengirim entangled qubit pair. Sehingga ketika Alice dan Bob melakukan operasi pada qubit masing-masing, maka qubit Alice akan berpindah ke Bob



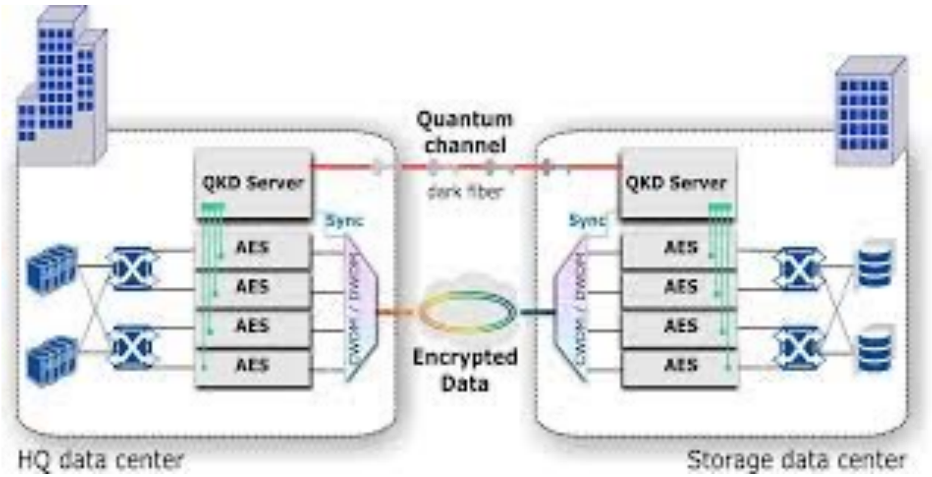
Quantum Internet

- Internet kuantum memungkinkan system komunikasi global yang terhubung secara kuantum sehingga memungkinkan data diolah secara algoritma kuantum dan diproteksi secara kriptografi kuantum
- www.aliroquantum.com/blog/what-is-a-quantum-network



Quantum Cryptography

- https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/
- Kriptografi kuantum pernah digunakan untuk mengamankan proses pemilu di swiss



Quantum Data Center

- Hardware kuantum akan menjadi bagian dari general-purpose datacenters
- Put the QC where the data is, not the data where the QC is
- Dapat mempercepat semua proses database untuk data jenis apapun (multimodal)

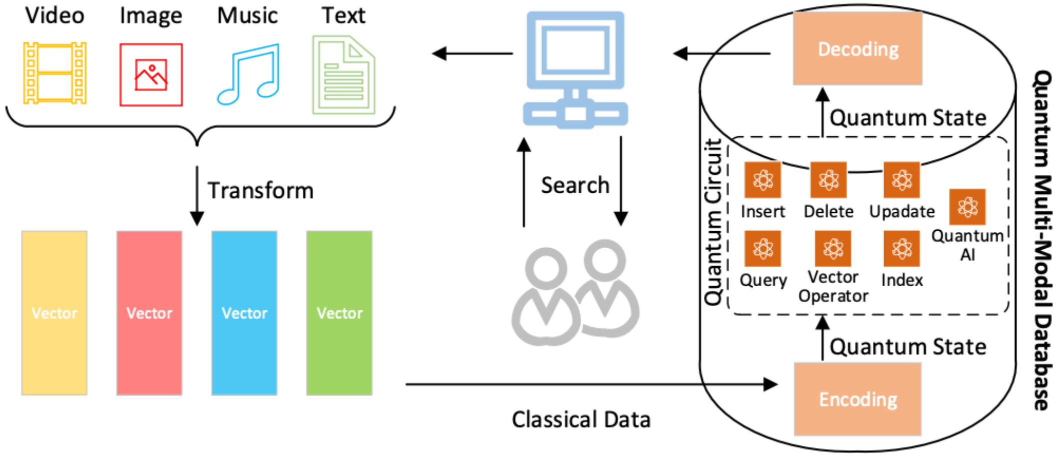
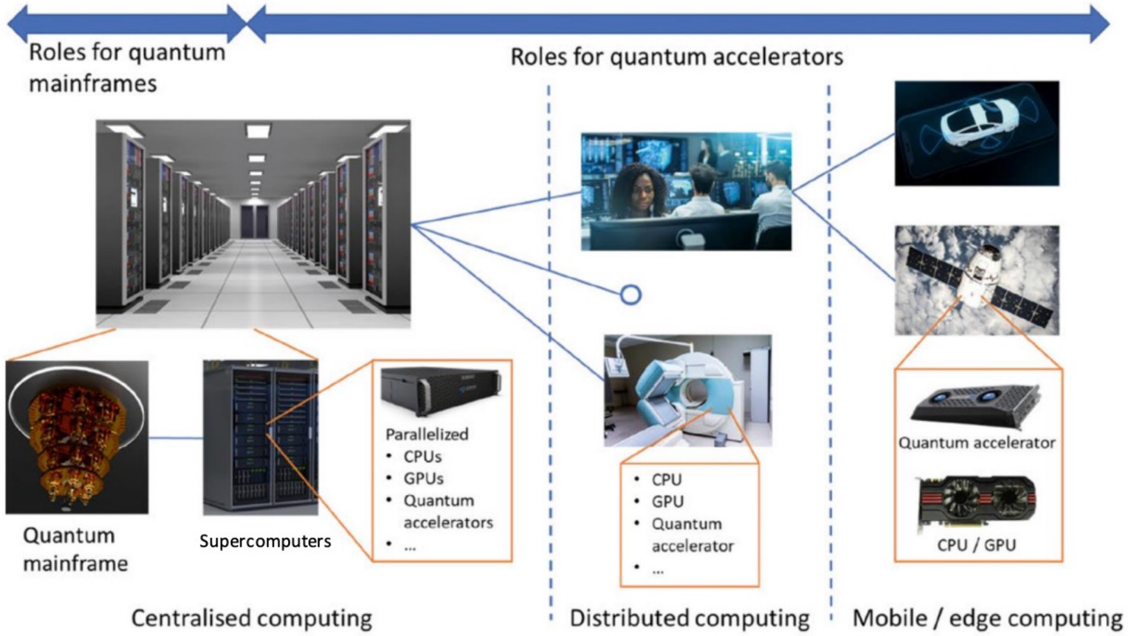


Figure 1: A Vision of Quantum Multi-Modal Databases

[Pawsey Installs First Room-Temperature On-Premises Quantum Computer in a Supercomputing Centre]



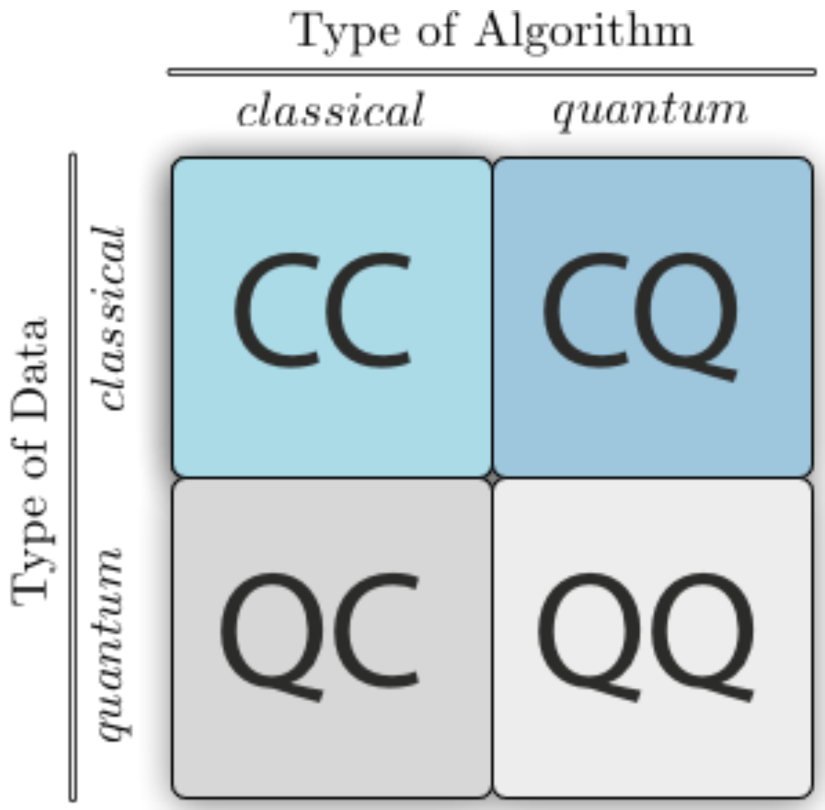
CALVIN INSTITUTE OF TECHNOLOGY

Quantum Machine Learning

- Machine learning dengan komputasi kuantum:
  - Quantum Data: $\vec{x} \to |\phi(\vec{x})\rangle$
  - Quantum Algorithm: $\hat{y} = A\vec{x} \to |\psi(\hat{y})\rangle = A|\phi(\vec{x})\rangle$

- Cara:
  - Encoding
  - Ansatz (quantum circuit)

- Potensi:
  - Efisiensi
  - Performa



Quantum Deep Learning

- Perhitungan inner/dot product banyak muncul di AI kontemporer, misalnya mekanisme attention: $(QK^T)V$
- Attention mechanism dengan kalimat sepanjang L memakan L^2 waktu dan memori:
  - $L = 1K \rightarrow L^2 = 1M \rightarrow 0.1s\ (10M\ ops/s)$
  - $L = 100K \rightarrow L^2 = 10B \rightarrow 1000s\ (10M\ ops/s)$
- N layers memakan N kali lebih banyak memori:
  - GPT-3 memiliki 96 layers
  - GPT-4 memiliki 120 layers
- Inner product antara banyak embedding dapat dilakukan secara kuantum dalam sekali proses $\langle\psi(Q)|\phi(K)\rangle$
- Caveat: tapi tetap diperlukan proses lain untuk mengkonversi menjadi data klasik

Tuhan Memberkati

God's People for God's Glory
CALVIN
INSTITUTE OF TECHNOLOGY