Flip Book

Quantum Computing and Communications

Is your industry ready?

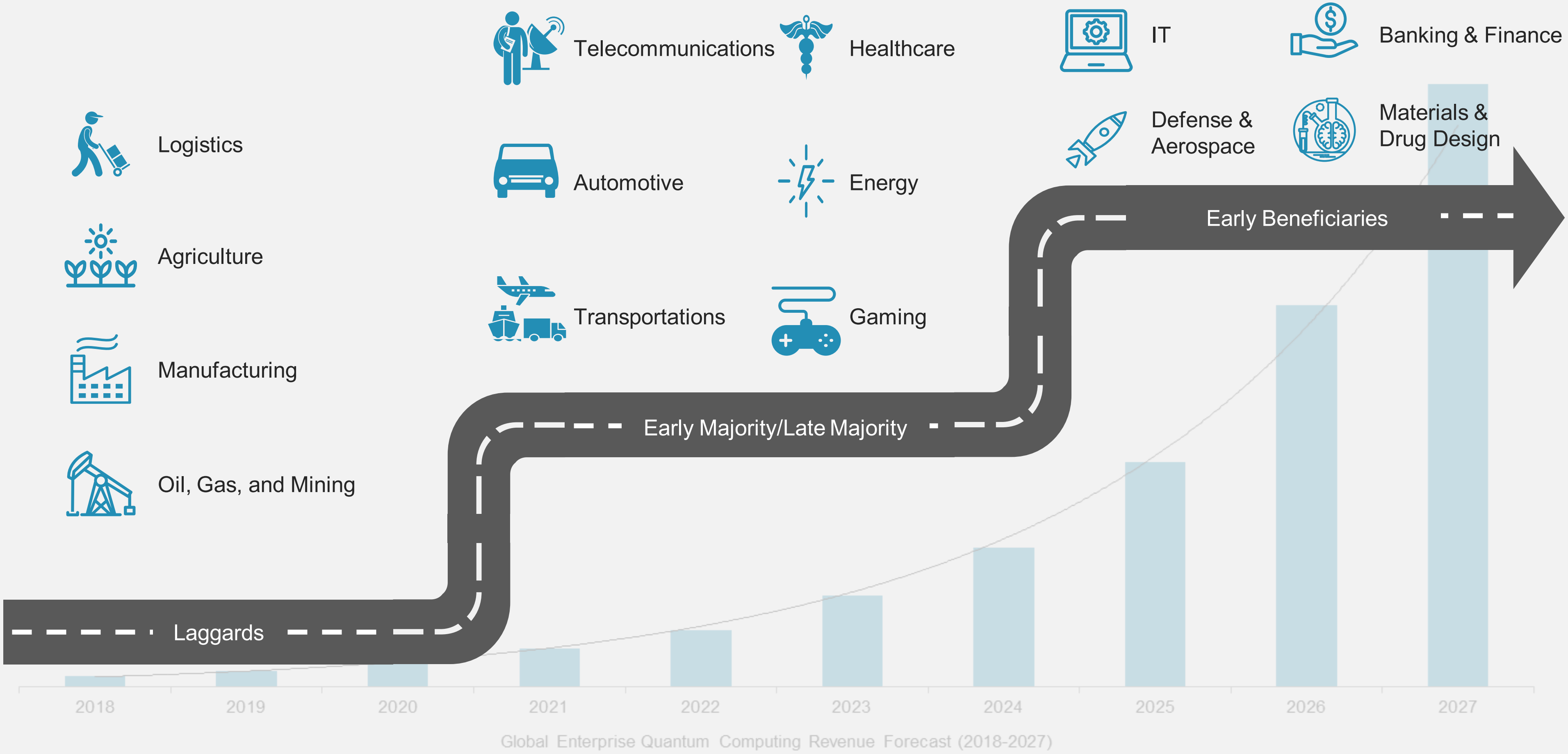
Are you ready?

2019

Quantum Computing Generating Buzz

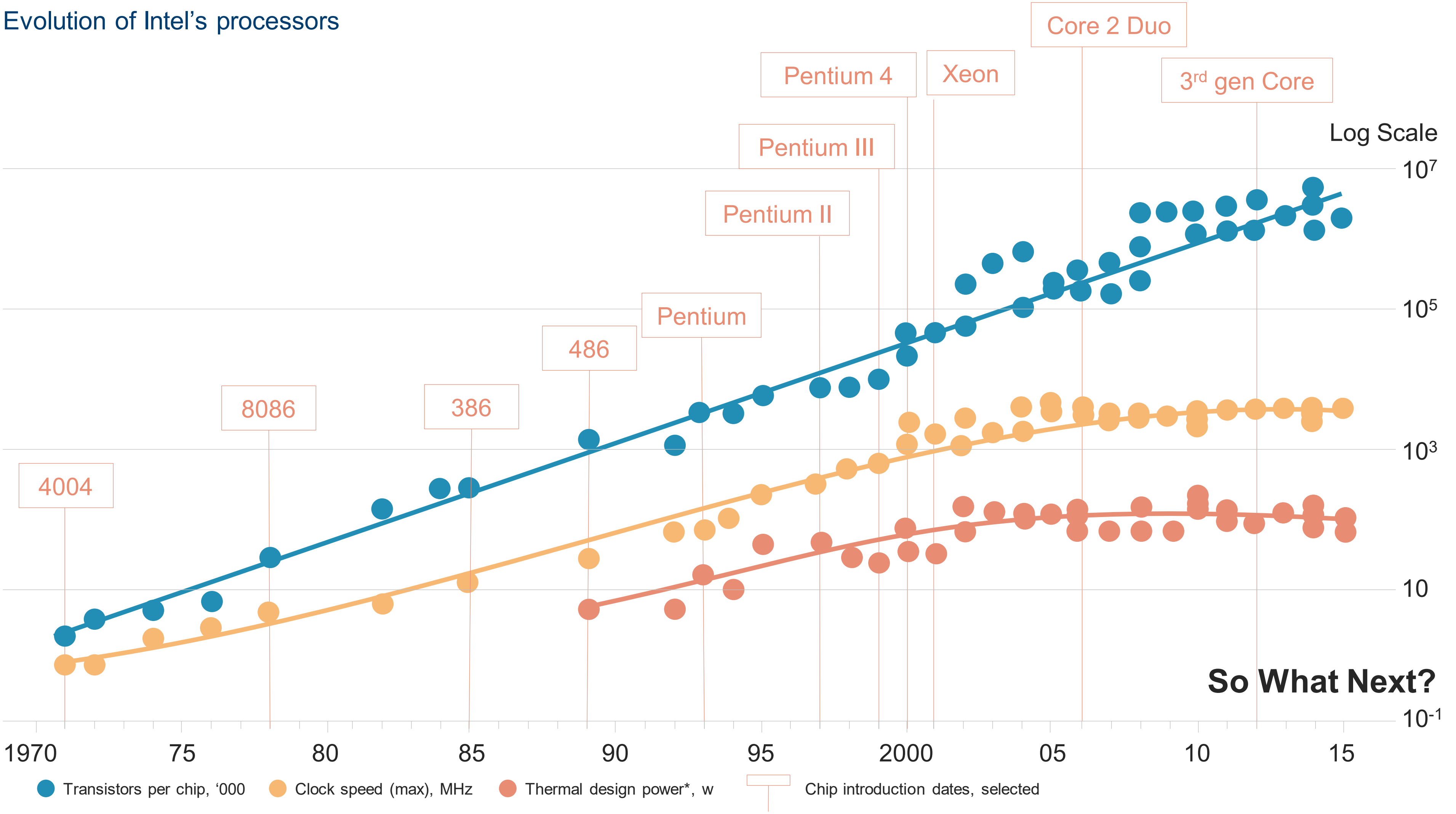
Quantum computing, the next big leap in computing power and communication security, set to push boundaries and trigger major disruption in operations, value chain and business models across industries

Quantum computing: Industry adoption trend (Illustrative)



Exponential increase in classical computational power over the past few decades; however, with Moore’s law nearing its end, **further increase in computational power at same aspect ratio seems uncertain**

Evolution of Intel’s processors



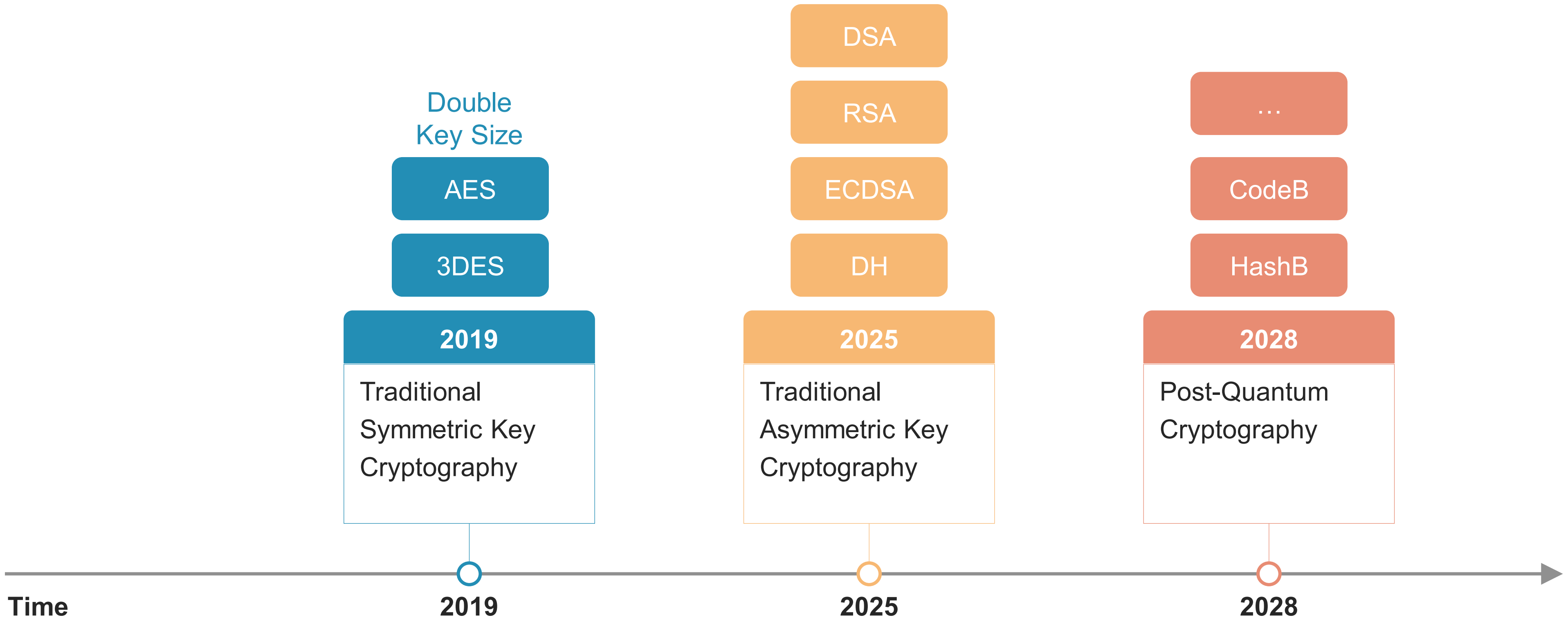
So What Next?

***Sources**: Intel; press reports; Bob Colwell; Linley Group; IB Consulting; The Economist*

**Maximum safe power consumption*

Strength of algorithms, underlying math and difficulty of calculation that form the basis of the best of classical cryptography schemes not enough to ensure absolute security

Timeline for future cryptography standardization events


Double Key Size
AES
3DES
2019
Traditional Symmetric Key Cryptography
DSA
RSA
ECDSA
DH
2025
Traditional Asymmetric Key Cryptography
…
CodeB
HashB
2028
Post-Quantum Cryptography
Time
2019
2025
2028

So What Next?

ADVANCES IN CRYPTOGRAPHY PROCESSING

Source: *Accenture*

Quantum computing: A robust solution to industry's demand for high computation power or better security

Quantum Computing

Physical space constraints and increasing real estate cost would make it difficult to meet future computation requirements, as data rates would increase exponentially with the successful implementation of IoT.

One way to increase computation power while keeping aspect ratio constant is to shift computing processes to a distant location (for example, cloud/edge computing). However, the speed of the communication channel could pose a challenge. The second solution would be to overcome the binary computation principle and switch to quantum computing.

Communication security and integrity is a primary requirement of any individual, business or government. Furthermore, security of communication is important to boost confidence in e-currency, and quantum cryptography or communication is a solution to this.

This white paper/report gives you relevant information on quantum computing.

Huge leap in quantum domain during the decade, from D-Wave's commercially available quantum computer (2011) to China's launch of quantum satellite (2016)

Todd Holmdahl, VP, Microsoft Quantum

"Five years from now, we will have a commercial quantum computer."

🙂

- February 23, 2018

Pan Jianwei, Quantum Experiments at Space Scale

How long before a mature global quantum network is possible? Pan believes that progress will be rapid. "Maybe it will take 10 years," he guesses.

🙂

- April 13, 2018

Mike Mayberry, Head of Intel Labs

Intel forecasts a ten-year wait until (quantum computing) companies progress beyond "toy systems".

🙂

- January 29, 2018

Talia Gershon, Thomas J. Watson Research Center

"Today, quantum computing is a researcher's playground. In five years, it will be mainstream."

🙂

- March 20, 2018

Gregoire Ribordy, CEO

"China will be able to connect its embassies and other government facilities around the world (via its quantum satellite within the next five years)."

🙂

- June 29, 2017

Mikhail Dyakonov, Theoretical Physicist, University of Montpellier

"When will useful quantum computers be constructed?... Not in the foreseeable future."

☹

- November 15, 2018

Gil Kalai, Mathematician at Hebrew University

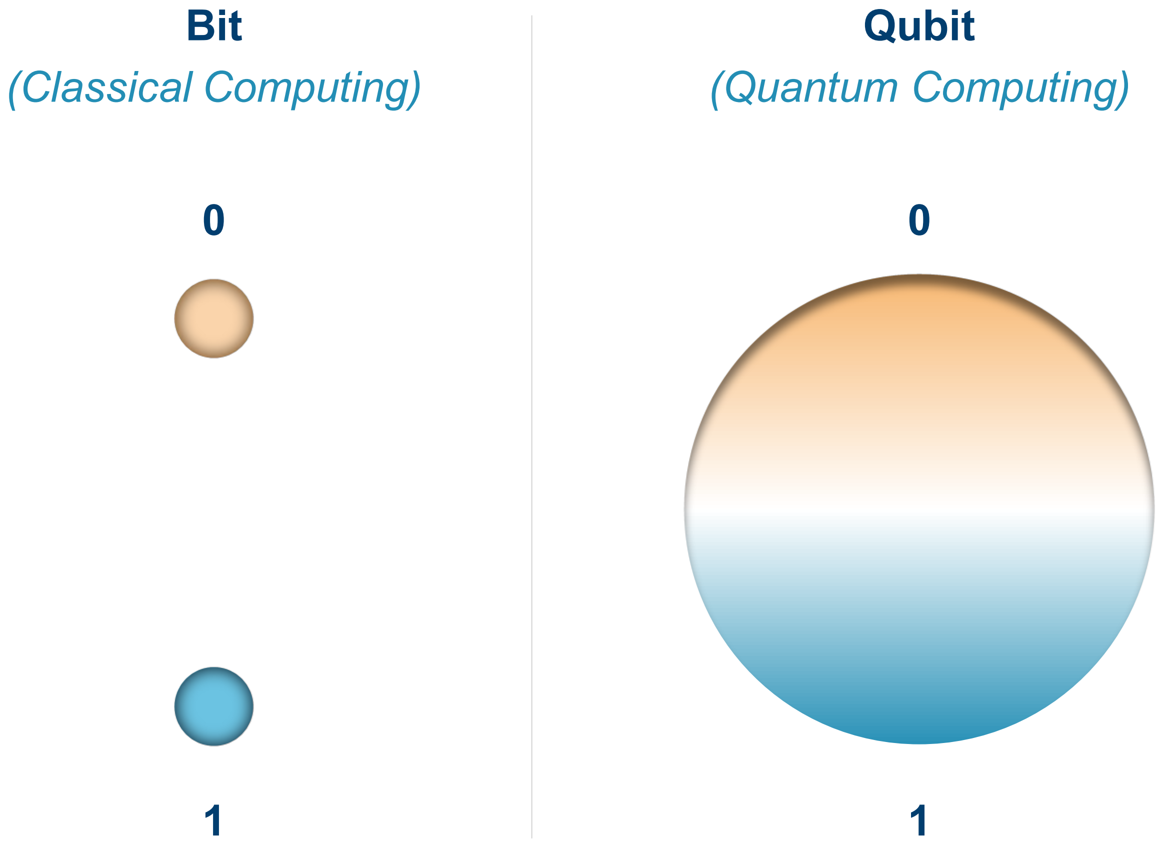
When did you first have doubts about quantum computers?... "At first, I was quite enthusiastic, like everybody else. But at a lecture in 2002 by Michel Devoret, called "Quantum Computer: Miracle or Mirage," I had a feeling that the sceptical direction was a little bit neglected…"

😐

- February 07, 2018

Quantum Computing Explained

Use of qubits, which allows two states (i.e., 0 and 1) to exist simultaneously, differentiating quantum computing from classical computing



Classical computing:
It functions using only two states; 0 and 1. These states are called bits. At a given time, only one state exists, not both.

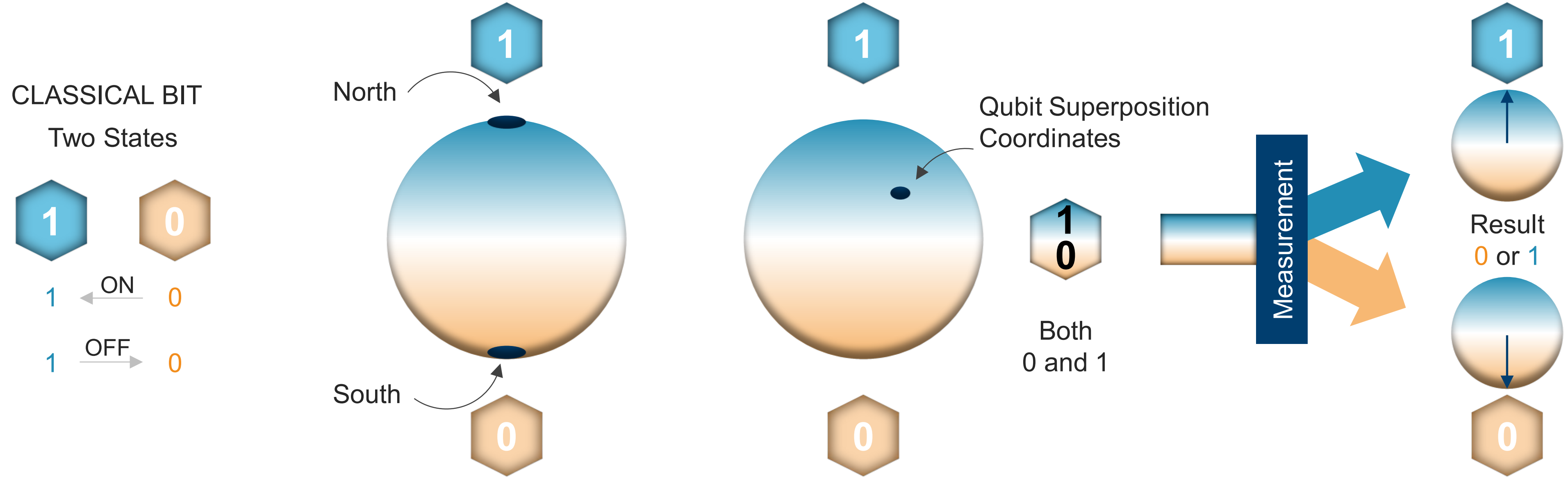
Quantum computing:
Quantum computers use qubits instead of bits. Unlike classical computers, quantum computers can run on both 0 and 1 at the same time.

As shown in the figure, bits exist either at the north pole or the south pole, not both. On the other hand, qubits can exist anywhere on the sphere. This is called superposition.

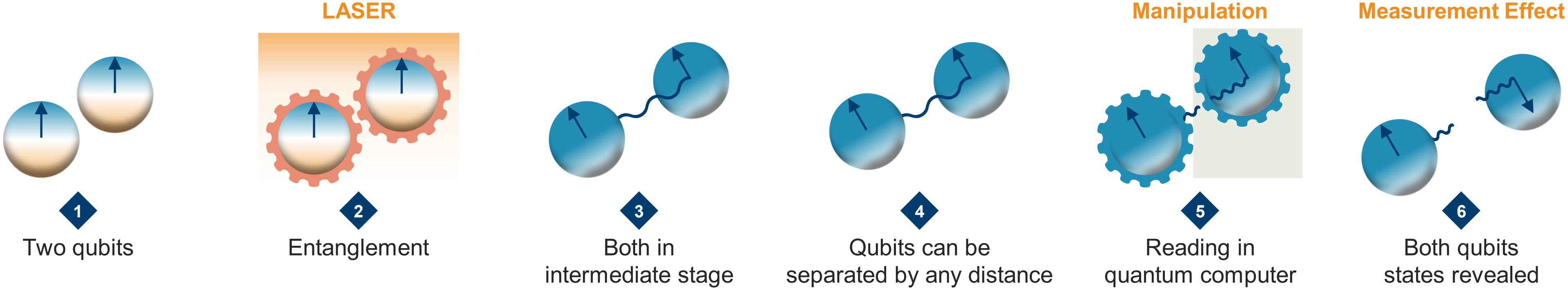
Superposition provides massive computation power; entanglement ensures unparalleled security

Superposition and Entanglement: Fundamental principles of quantum mechanics

Qubit Superposition

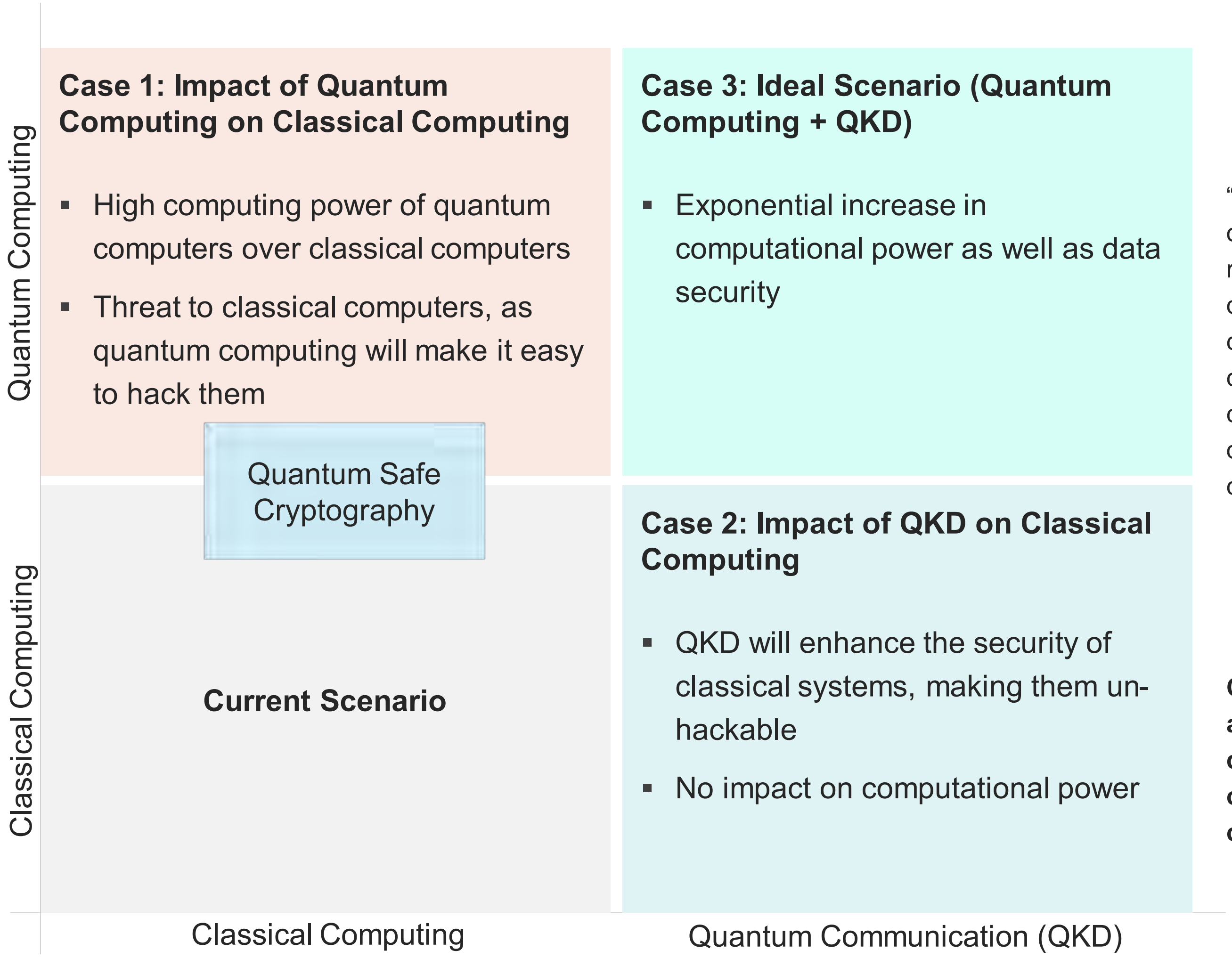


Qubit Entanglement


LASER
Manipulation
Measurement Effect
1
Two qubits
2
Entanglement
3
Both in intermediate stage
4
Qubits can be separated by any distance
5
Reading in quantum computer
6
Both qubits states revealed

What to Expect of Quantum Computers

“If the time for development and deployment of the quantum-resistant cryptography technology is longer than the quantum computer development period, it will make a big chaos.” – *Prof. Michele Mosca*



Case 1: Impact of Quantum Computing on Classical Computing

- High computing power of quantum computers over classical computers
- Threat to classical computers, as quantum computing will make it easy to hack them

Case 3: Ideal Scenario (Quantum Computing + QKD)

- Exponential increase in computational power as well as data security

Quantum Safe Cryptography

Current Scenario

Case 2: Impact of QKD on Classical Computing

- QKD will enhance the security of classical systems, making them un-hackable
- No impact on computational power

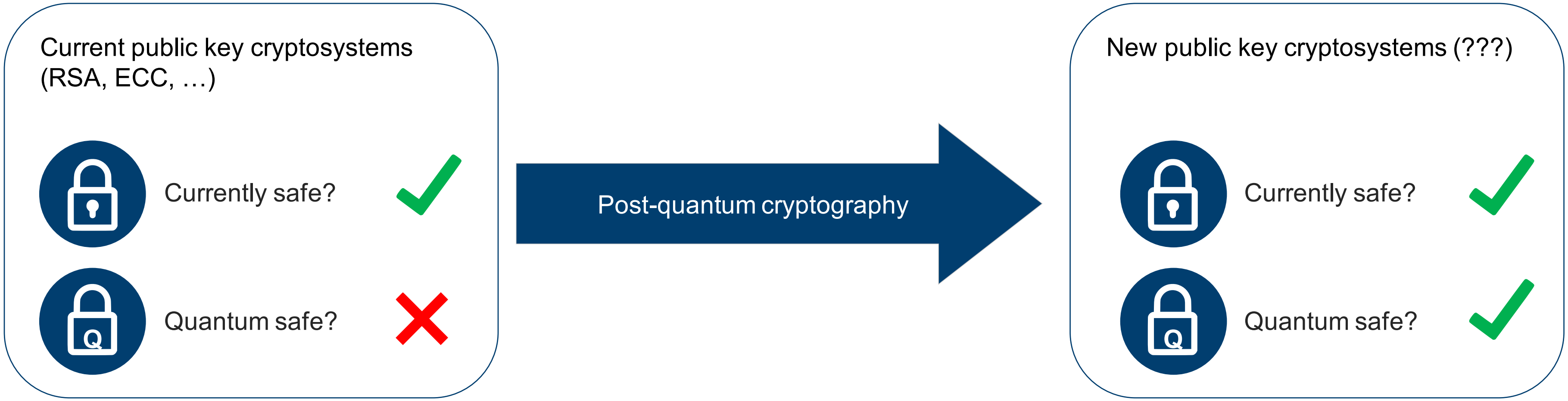
“If the sum of the time, which includes development and deployment of the quantum resistant cryptography technology against quantum computers, is longer than the quantum computer development period, it will make a big chaos. It is an urgent matter to develop cryptographic techniques that can counteract quantum computers in all cryptographic communication as well as military aspects.”

- Professor Michele Mosca, Waterloo University

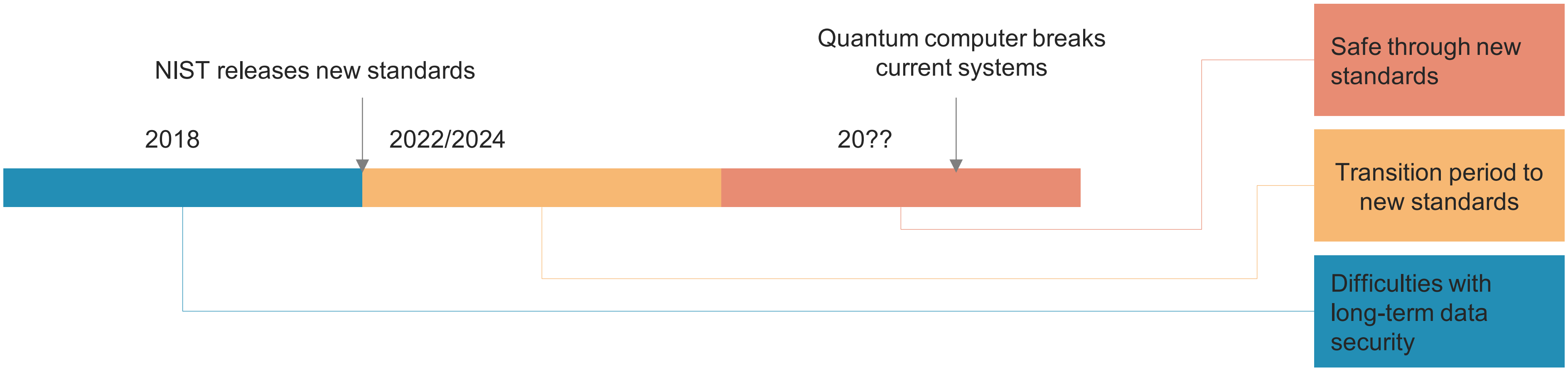
Cryptography technology that can resist attack from quantum computers is largely divided into quantum-based QKD and classical computing-based post-quantum cryptography.

Post-quantum cryptography: New classical computing-based public key cryptosystems being designed to secure classical computers from quantum threat; effectiveness of systems yet to be established

Every organization should work to achieve quantum-proof coverage by 2025.



Current public key cryptosystems (RSA, ECC, …)
Currently safe? ✓
Q
Quantum safe? ✗
Post-quantum cryptography
New public key cryptosystems (???)
Currently safe? ✓
Q
Quantum safe? ✓

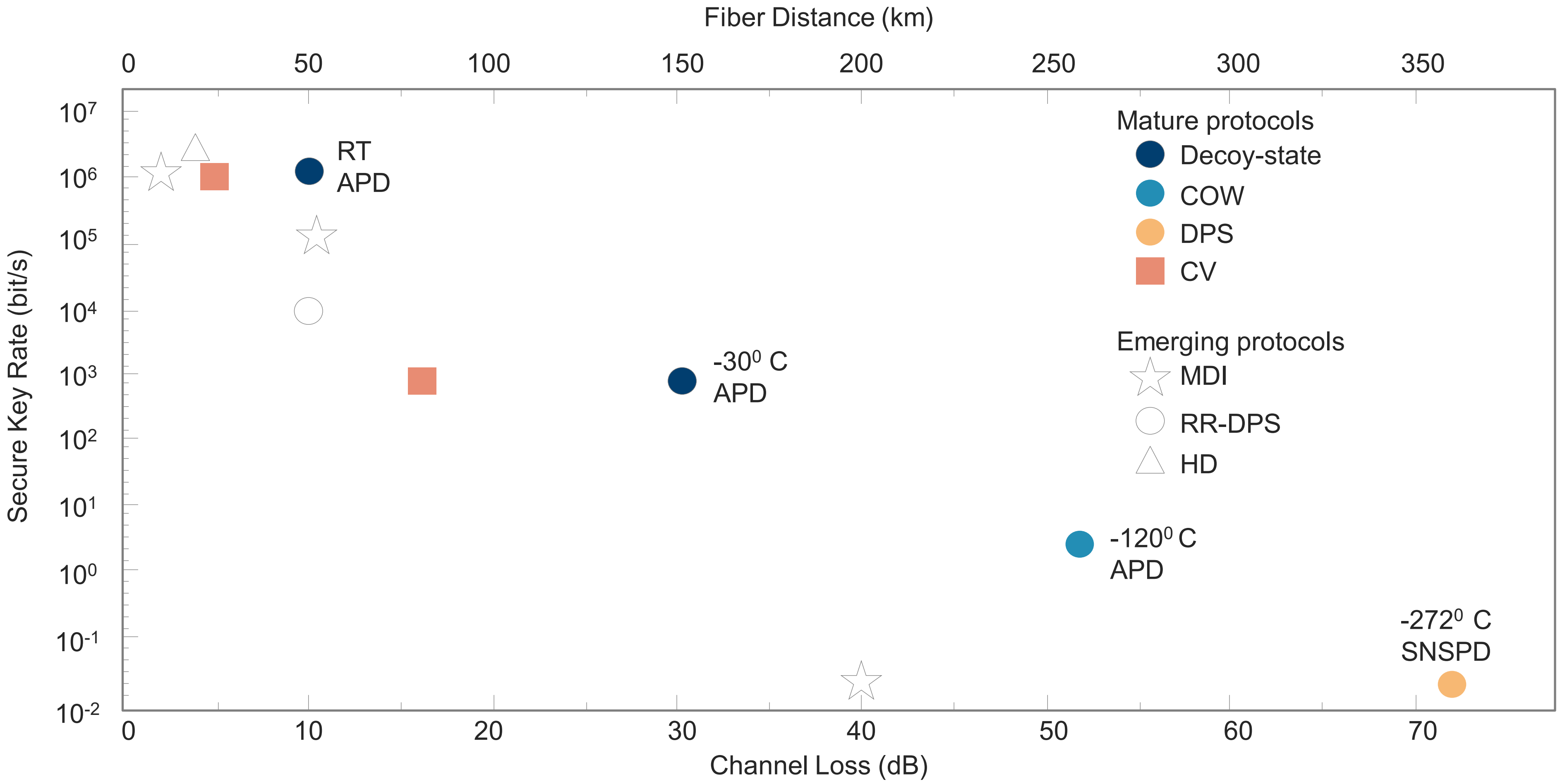


NIST releases new standards
Quantum computer breaks current systems
2018
2022/2024
20??
Safe through new standards
Transition period to new standards
Difficulties with long-term data security

Source: *Innopay*

Channel loss main challenge in implementing secure QKD system over fiber optics, the best bet for safe communication

QKD is a subject of active ongoing research, therefore, further developments are likely to occur in the near future.

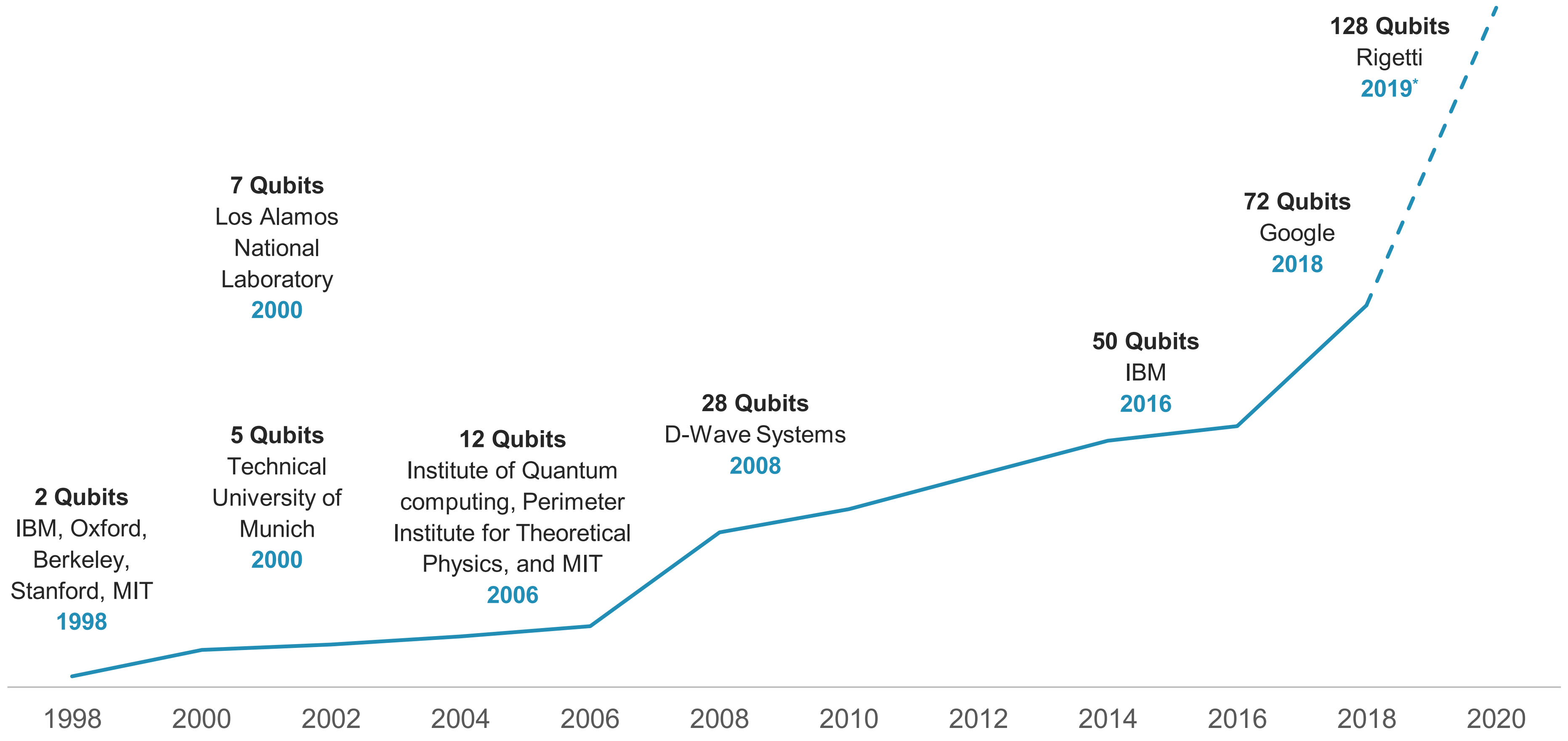


Secret key generation rates in recent QKD schemes (representative)

Qubits evolving gradually, hinting at quantum computing age on the horizon

Quantum computers are getting more powerful.

Number of qubits achieved by date and organization 1988 – 2020*



Source: *MIT, Qubit counter. *Rigetti quantum computer expected by late 2019.*

Companies Active in the Ecosystem

Organizations working to bring commercial quantum systems in the mainstream over the next 5–10 years

Quantum Computing Ecosystem

1QBit
D-Wave The Quantum Computing Company™
Qubitekk
IONQ
rigetti

Microsoft
Google
IBM
accenture High performance. Delivered.
Alibaba Cloud aliyun.com

RIVERLANE
QBITLOGIC
Q^x Branch
⟨InfiniQuant⟩
QC WARE

Q-CTRL
qci Quantum Circuits, Inc
Raytheon BBN Technologies
Chinese Academy of Sciences
RIKEN

NTT Communications
NOKIA Bell Labs
intel
hp

SIEMENS
imec
HITACHI
Honeywell

LOCKHEED MARTIN
AIRBUS
NORTHROP GRUMMAN
Booz | Allen | Hamilton®

Quantum Communications Ecosystem

SK telecom
BT
FUJITSU

HUAWEI
AT&T
NEC

Chinese Academy of Sciences
IDQ
asky

Quintessence Labs Data Uncompromised
CQC Cambridge Quantum Computing Limited
kpn

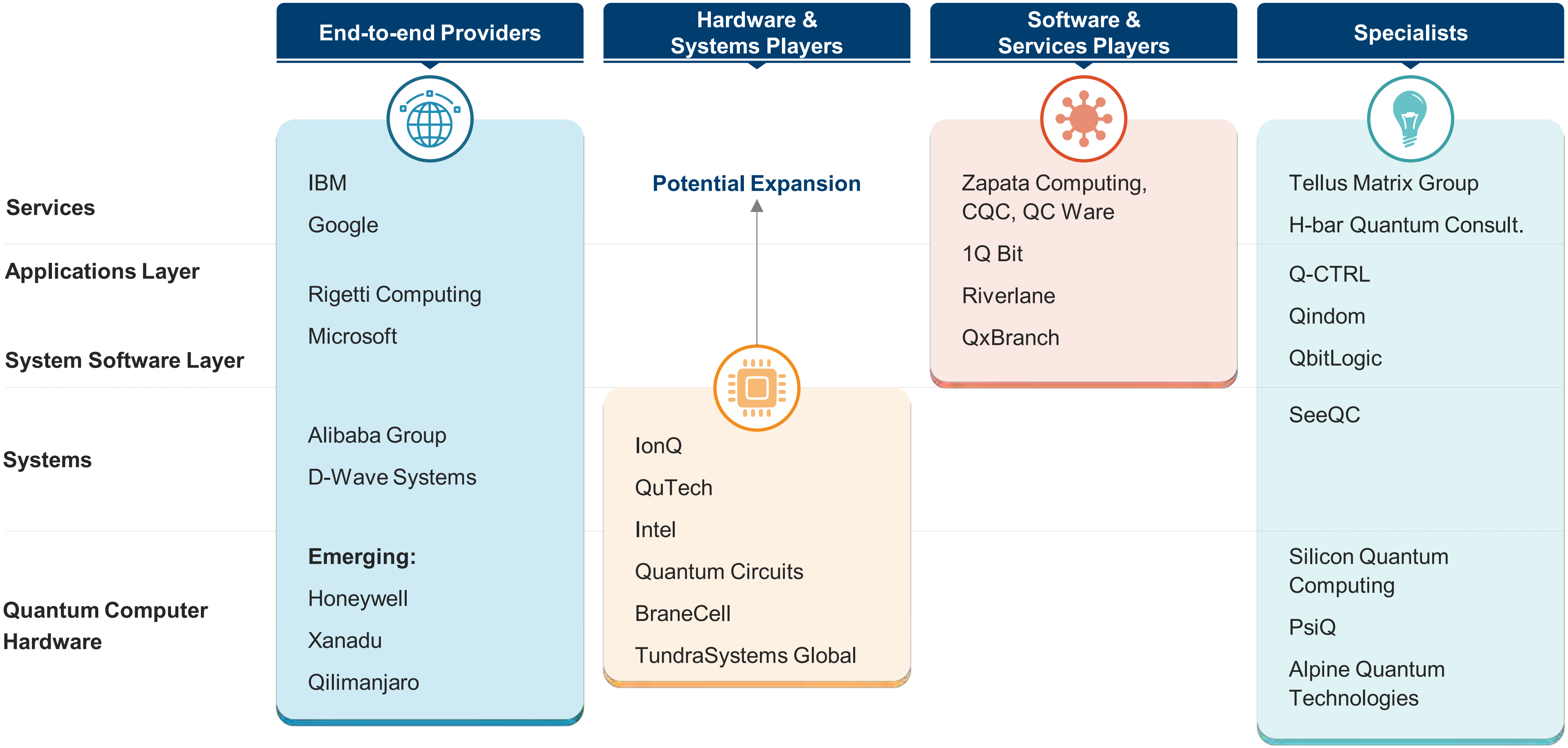
QUANTUM NUMBERS CORP
国盾量子 QuantumCTek
MagiQ

Alibaba Cloud aliyun.com
hp
MITSUBISHI ELECTRIC

Raytheon BBN Technologies
TOSHIBA

IBM, Google, Microsoft, Alibaba Group aiming at providing end-to-end solutions in quantum computing

There are four roles in the quantum computing ecosystem.



Services

Applications Layer

System Software Layer

Systems

Quantum Computer Hardware

End-to-end Providers

IBM

Google

Rigetti Computing

Microsoft

Alibaba Group

D-Wave Systems

Emerging:

Honeywell

Xanadu

Qilimanjaro

Hardware & Systems Players

Potential Expansion

IonQ

QuTech

Intel

Quantum Circuits

BraneCell

TundraSystems Global

Software & Services Players

Zapata Computing, CQC, QC Ware

1Q Bit

Riverlane

QxBranch

Specialists

Tellus Matrix Group

H-bar Quantum Consult.

Q-CTRL

Qindom

QbitLogic

SeeQC

Silicon Quantum Computing

PsiQ

Alpine Quantum Technologies

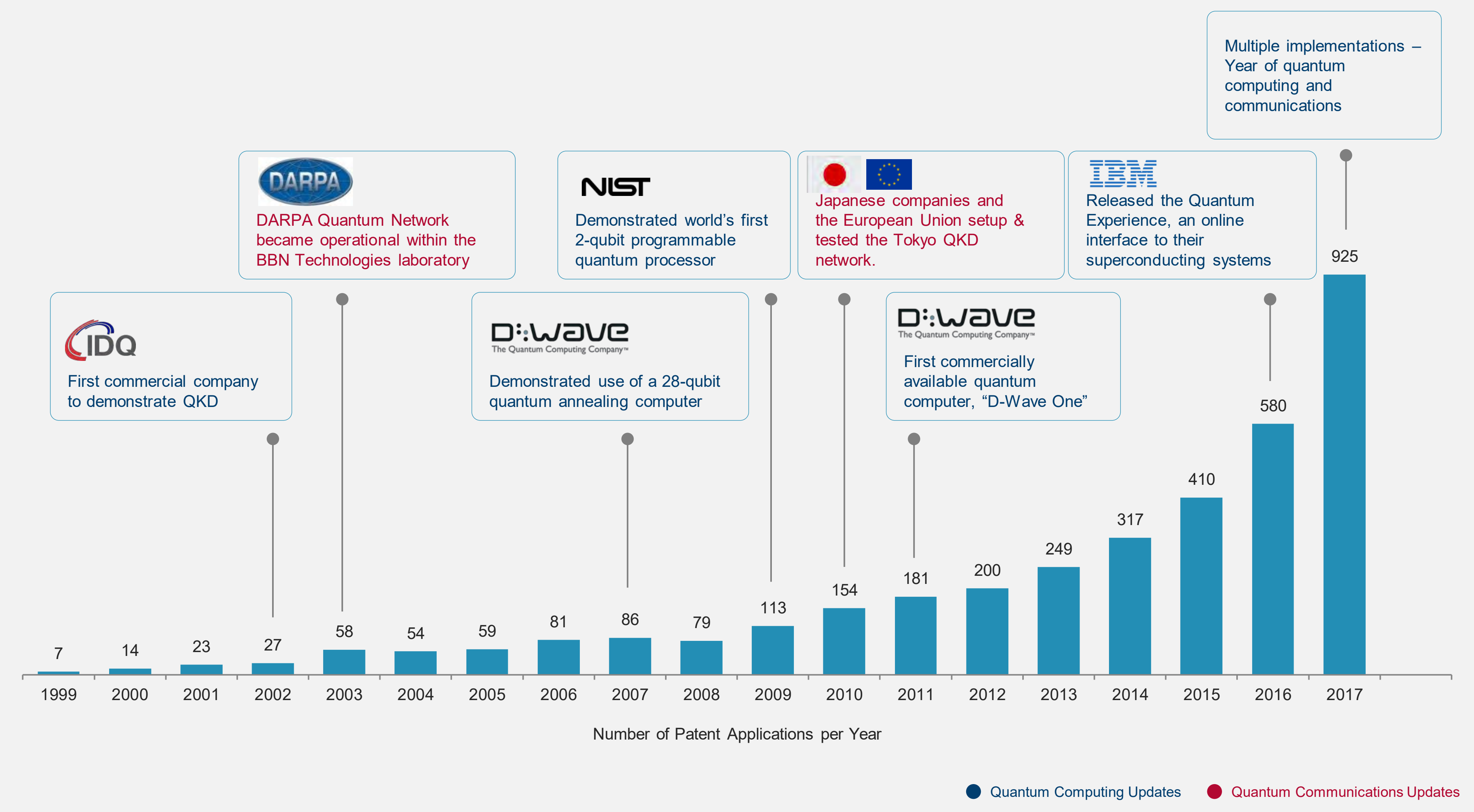
Source: *BCG Analysis*

DWave, Rigetti, Silicon Quantum Computing and CQC among quantum computing startups that have raised >= USD 50 Million

	D:Wave The Quantum Computing Company™	rigetti	Silicon Quantum Computing	CQC Cambridge Quantum Computing Limited	1QBit
Disclosed Funding	USD 210M	USD 119.5M	USD 66M	USD 50M	USD 45M
Headquarter	Canada	US	Australia	UK	Canada
Quantum Offerings	Quantum computers	Quil: Quantum instruction language Forest: An API for quantum computing in the cloud	Creating a silicon-based quantum computer	Proprietary OS for quantum computers	Software solution for classical & quantum computing architecture

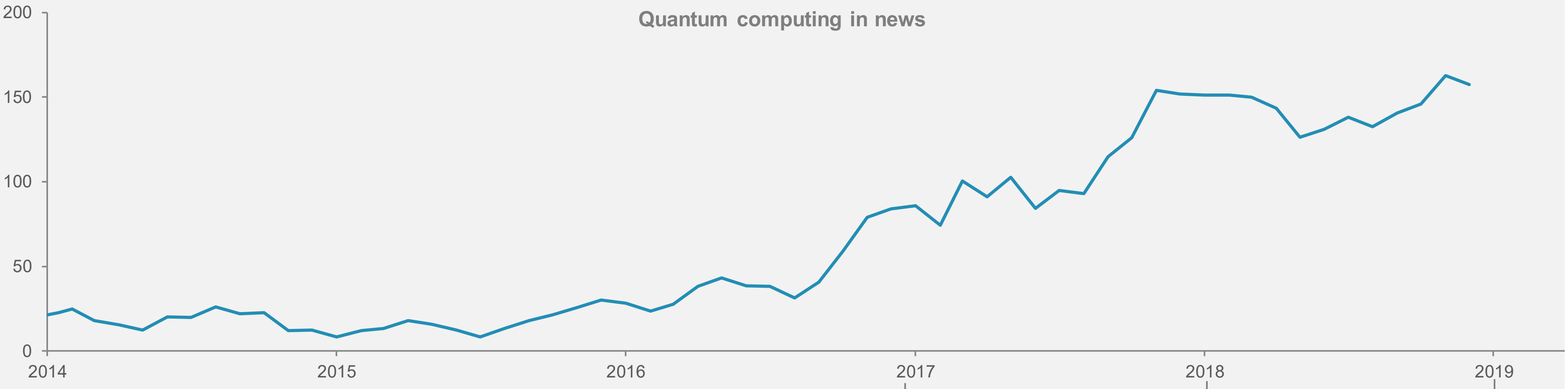
	IONQ	QC WARE	IDQ	asky	Qubitekk
Disclosed Funding	USD 20M	USD 6.5M	USD 5.6M	NA	USD 4.1M
Headquarter	US	US	Switzerland Acquired by SK Telecom	China	US
Quantum Offerings	Trapped-ion quantum processors Algorithms for quantum computers	Cloud-based quantum computing platform	Random number generator for cloud and distributed environments	Quantum gateway QKD terminal Photon detector	Quantum repeaters QKD systems

Development in line with research: Exponential rise in innovations in the domain since 2010; boom in products and implementation from 2017



Patent Data Source: Relecura

2017: The year of quantum computing in terms of number of achievements in the domain



D:WAVE The Quantum Computing Company™

General commercial availability of the D-Wave 2000Q quantum annealer

IBM

Built and tested an operational 50-qubit prototype processor
Plans to offer 20-qubit quantum computer as a cloud-based service

Microsoft

Revealed an unnamed quantum programming language, integrated with Visual Studio

intel

Confirmed the development of a 17-qubit superconducting test chip

Quantum satellite-based entangled distribution over 1200 km
Beijing-Shanghai 2000 km QKD Trunk Line opened
Quantum encrypted intercontinental video call over a record distance of 7,600 km

SK telecom

Developed a trusted repeater, achieving a distance record of 112 km for QKD

rigetti

Demonstrated unsupervised machine learning using 19Q, a 19-qubit general purpose superconducting quantum processor

Google

Announced the creation of a 72-qubit quantum chip Bristlecone

IBM

First experimental realization of a quantum artificial life algorithm in a quantum computer

The UK's first quantum network launched in Cambridge, facilitating unhackable communications

intel

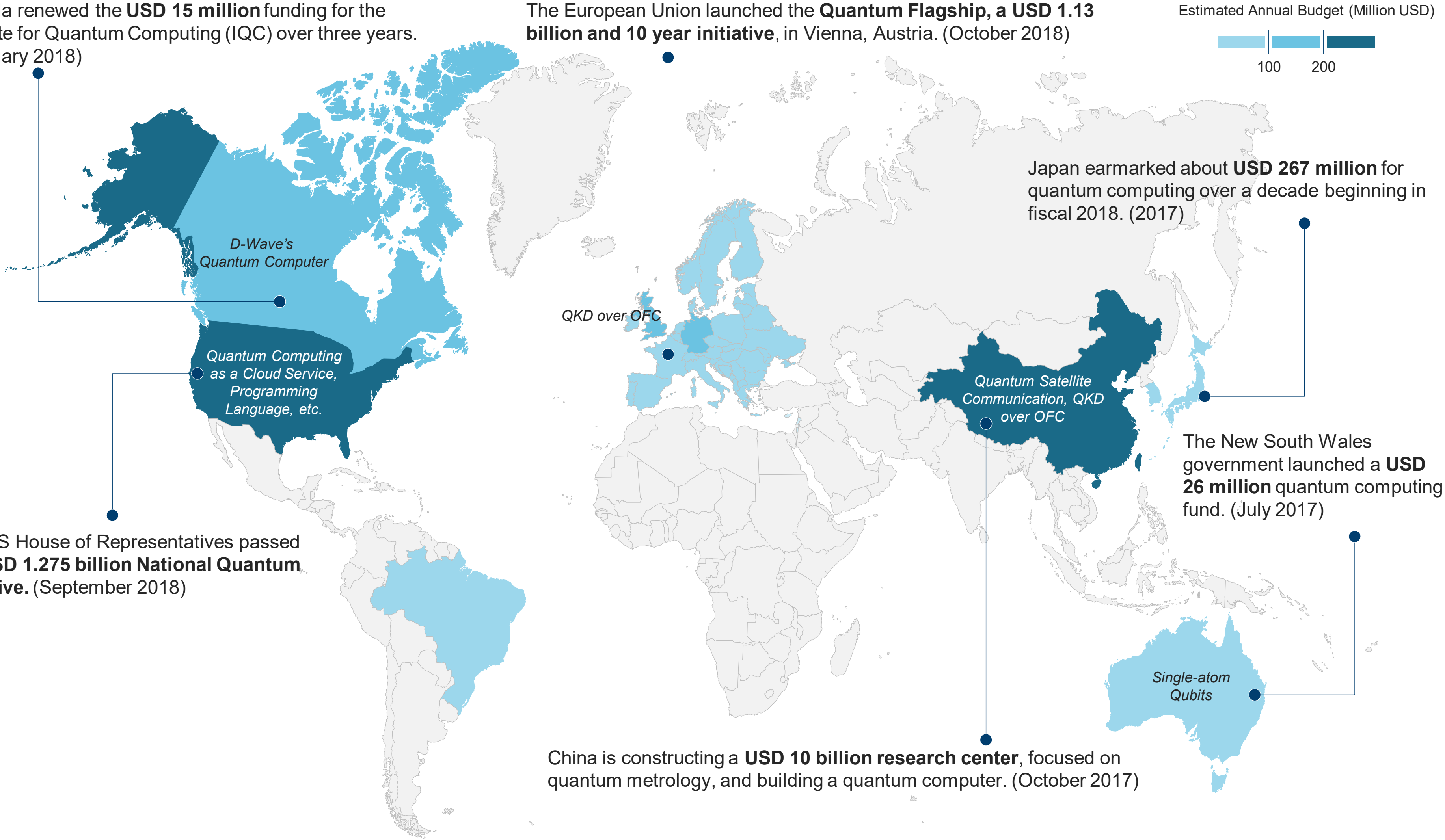
Began testing its silicon-based spin-qubit processor; confirmed the development of a 49-qubit super-conducting test chip Tangle Lake

Google

Claims to have achieved quantum supremacy. Their processor was able to perform a calculation in three minutes and 20 seconds that would take the most advanced classical computer (Summit), approximately 10,000 years.

● Quantum Computing Updates ● Quantum Communications Updates

Number of countries investing in the domain increasing year-on-year, with China at the top, followed by the US; East focusing on communication, West on computation


Estimated Annual Budget (Million USD)
100
200
D-Wave's Quantum Computer
Quantum Computing as a Cloud Service, Programming Language, etc.
QKD over OFC
Quantum Satellite Communication, QKD over OFC
Single-atom Qubits

Canada renewed the **USD 15 million** funding for the Institute for Quantum Computing (IQC) over three years. (February 2018)

The European Union launched the **Quantum Flagship, a USD 1.13 billion and 10 year initiative**, in Vienna, Austria. (October 2018)

Japan earmarked about **USD 267 million** for quantum computing over a decade beginning in fiscal 2018. (2017)

The New South Wales government launched a **USD 26 million** quantum computing fund. (July 2017)

The US House of Representatives passed the **USD 1.275 billion National Quantum Initiative.** (September 2018)

China is constructing a **USD 10 billion research center**, focused on quantum metrology, and building a quantum computer. (October 2017)

Source: *The Quantum Age: Technological Opportunities (2016)*

Use Cases

Cybersecurity, drug discovery, AI/ML and intensive simulations among the potential use cases for quantum computing

Quantum computing can be used in multiple applications across sectors.

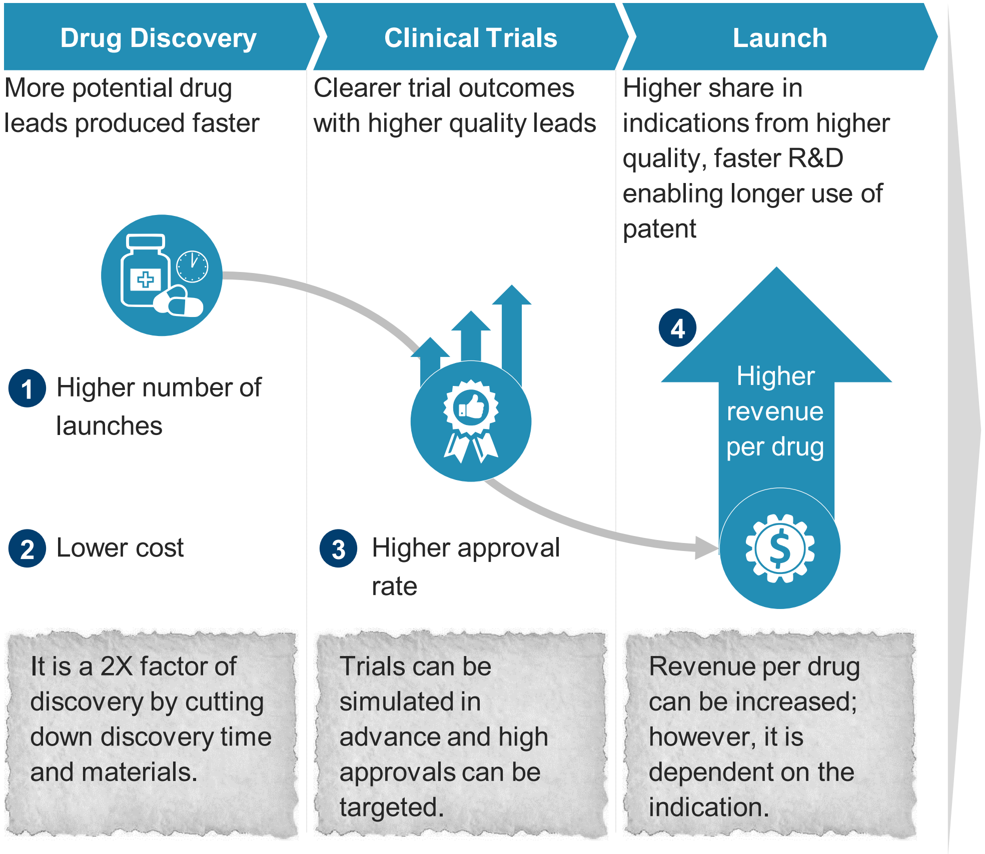
Industries	Selection of Use Cases	Enterprises (Examples)	
High-Tech	▪ Cybersecurity ▪ Machine learning and artificial intelligence, such as neural networks ▪ Search ▪ Bidding strategies for advertisements ▪ Online and product marketing	IBM Alibaba Google Microsoft	Telstra Baidu Samsung
Industrial Goods	▪ Automotive: Traffic simulation, e-charging station and parking search, autonomous driving ▪ Aerospace: R&D and manufacturing such as fault-analysis, turbulence simulation, stronger polymers for airplanes ▪ Material Science: More efficient materials for solar energy	Airbus NASA Northrop Grumman Raytheon	BMW Volkswagen Lockheed Martin Honeywell Bosch
Chemistry and Pharma	▪ Catalyst and enzyme design ▪ Pharmaceuticals R&D such as faster drug discovery ▪ Bioinformatics such as genomics ▪ Patient diagnosis for healthcare	BASF Biogen Dow Chemical	JRS DuPont Amgen
Finance	▪ Trading strategies ▪ Portfolio optimization ▪ Asset pricing ▪ Risk analysis ▪ Fraud detection	J P Morgan Commonwealth Bank	Barclays Goldman Sachs
Energy	▪ Network design ▪ Energy distribution ▪ Oil well optimization	Dubai Electricity and Water Authority	BP

Source: *BCG Analysis*

Complex molecule discovery in pharma R&D likely to be a USD 15–30 Billion market opportunity

At the atomic level, current high-performance computing cannot handle most simulations. Quantum computing can exponentially increase drug discovery.

Quantum computing applications throughout pharma value chain



Drug Discovery: More potential drug leads produced faster

Clinical Trials: Clearer trial outcomes with higher quality leads

Launch: Higher share in indications from higher quality, faster R&D enabling longer use of patent

1 Higher number of launches

2 Lower cost

3 Higher approval rate

It is a 2X factor of discovery by cutting down discovery time and materials.

Trials can be simulated in advance and high approvals can be targeted.

Revenue per drug can be increased; however, it is dependent on the indication.

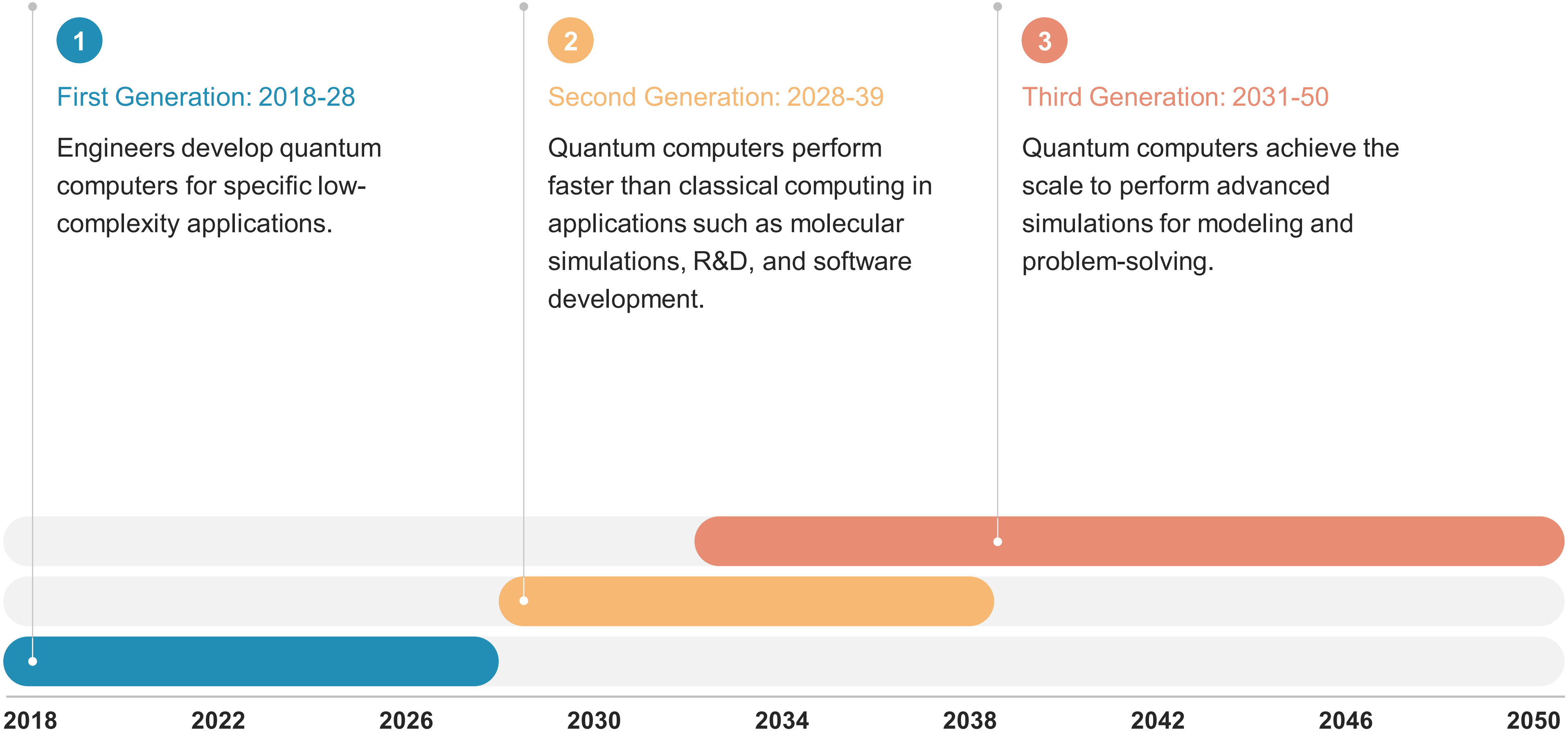
Higher molecular discovery and approval rates drive value proposition

	~USD 200 Billion	2027 branded pharma net income in the US
1	~USD 10 Billion – USD 20 Billion	~5-10% boost in potential drug opportunities from faster discovery
2	~USD 5 billion	Cost advantage from reduction in time for drug discovery (15% - 20% of R&D time)
3	~USD 100 Billion –- USD 200 Billion	~1.5–2x higher approval rate; low-weight molecules match current higher approval rates of biologics
4	~USD 20 Billion – USD 50 Billion	Increase in revenue per drug due to higher quality drugs gaining share (5-20%) and longer time in market (5%) with patent owing to faster R&D
	~USD 15 Billion – USD 30 Billion	Estimated opportunity size (Incremental value x 10% willingness to pay)

Source: *BCG Analysis*

Potential Market

Quantum computing market expected to evolve in three overlapping generations



1

First Generation: 2018-28

Engineers develop quantum computers for specific low-complexity applications.

2

Second Generation: 2028-39

Quantum computers perform faster than classical computing in applications such as molecular simulations, R&D, and software development.

3

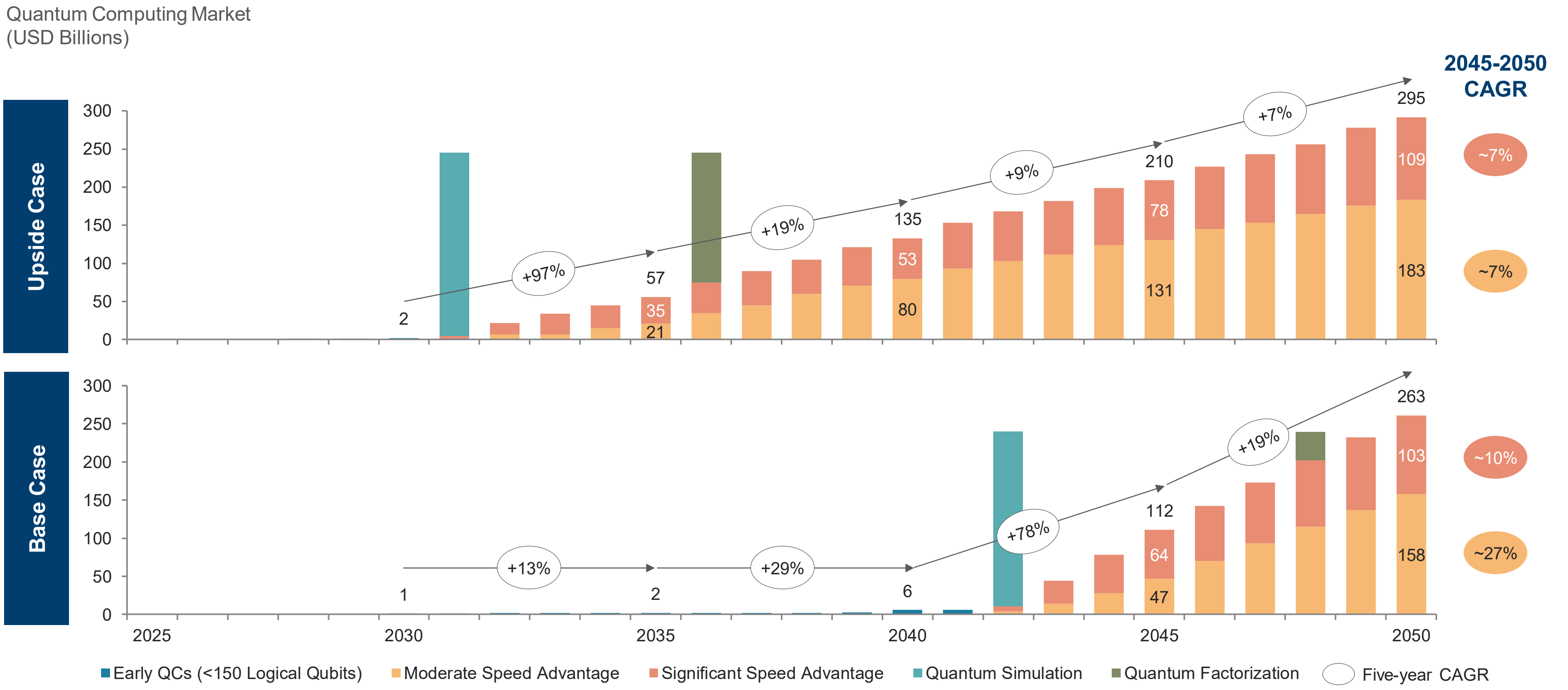
Third Generation: 2031-50

Quantum computers achieve the scale to perform advanced simulations for modeling and problem-solving.

Source: *BCG Analysis*

Base case predicts quantum computing market to reach USD 2 Billion by 2035; soar to more than USD 260 Billion by 2050 as adoption picks up

Base case scenario: Assuming Moore's law speed of qubit development with no improvement in error correction
Upside case scenario: Assuming Moore's law speed of qubit development with a significant reduction in need for error correction



Source: *BCG Analysis*

Ready?

Steps to take to get started

1 Analyze Potential

- Quantify the potential of quantum computing for businesses.
- Monitor the progress of the ecosystem.
- Assess where to develop or secure promising future IP that is relevant for a particular industry.

2 Gain Experience

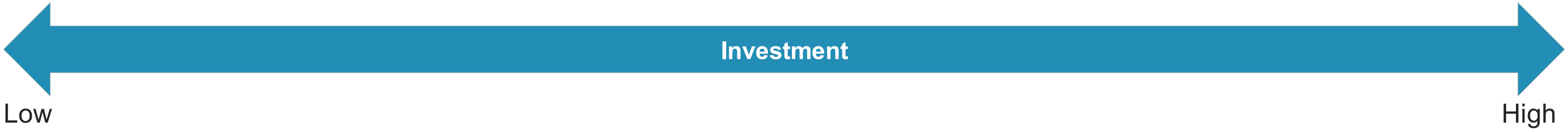
- Experiment with and assess quantum algorithms and their performance on current and upcoming quantum hardware using cloud-based access by investing in a small, possibly virtual, quantum group or lab.
- Build capabilities by collaborating with key software and service players.
- Scout for partnerships and potential acquisitions.

3 Lead Your Own Effort

- Build own quantum unit with dedicated resources to lead quantum pilots in collaboration with outside providers, this guarantees direct access to hardware and the latest technology developments.
- Leverage technology-specific speed-ups and take early advantage of rising technology maturity.
- Avoid locking in to a particular technology or approach before testing the performance on several technologies.

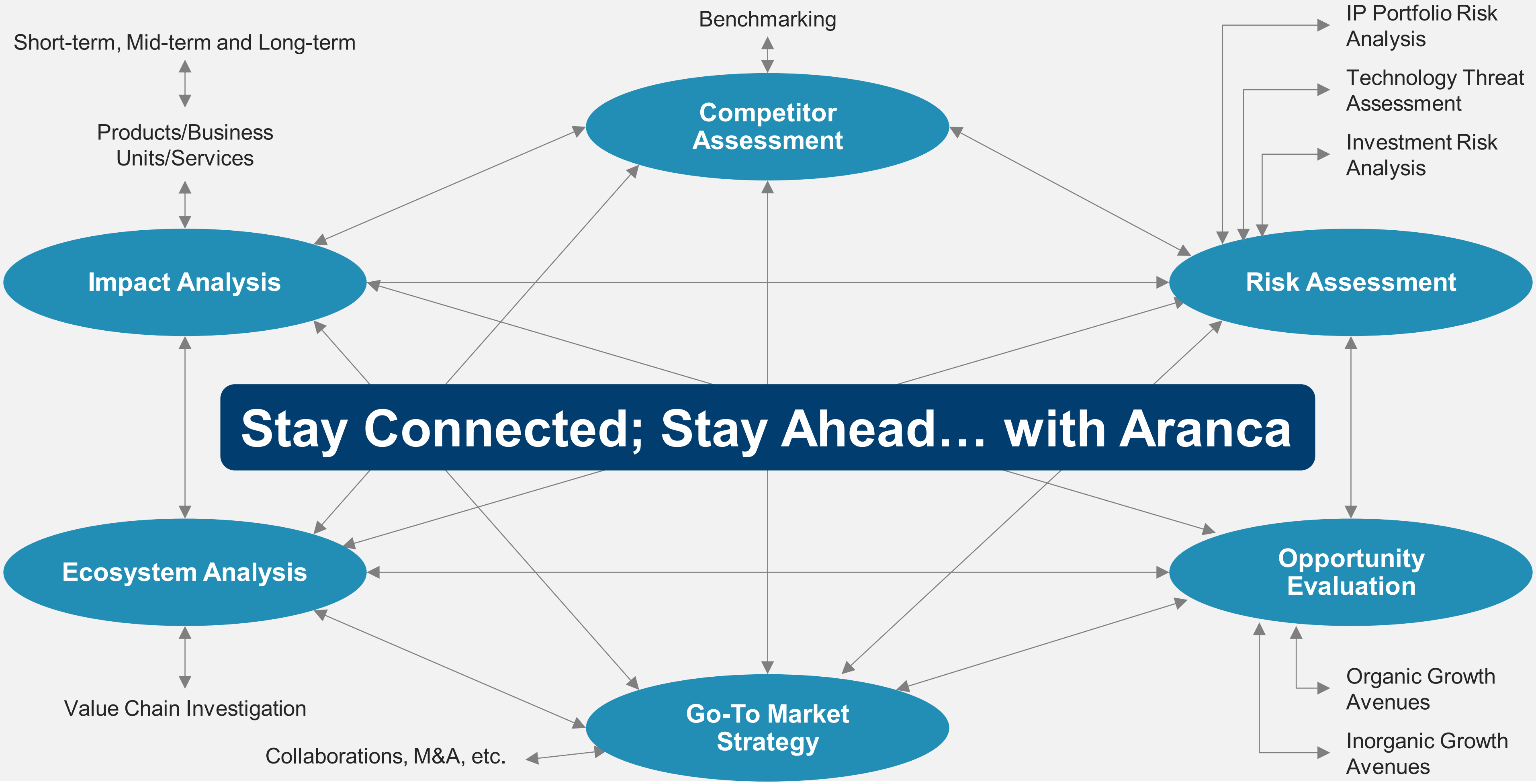
4 Launch New Offerings

- Invest in a cross-functional group of domain and quantum computing experts to assure frontline access to top-notch hardware or building own quantum computer.
- Realize the first-mover advantage of a new discovery or application.
- Become active drivers of the ecosystem.



How Aranca can help

A brief overview of Aranca's offerings


Benchmarking
Short-term, Mid-term and Long-term
Products/Business Units/Services
Competitor Assessment
IP Portfolio Risk Analysis
Technology Threat Assessment
Investment Risk Analysis
Impact Analysis
Risk Assessment
Stay Connected; Stay Ahead… with Aranca
Ecosystem Analysis
Opportunity Evaluation
Value Chain Investigation
Go-To Market Strategy
Organic Growth Avenues
Inorganic Growth Avenues
Collaborations, M&A, etc.

About Aranca

Founded in 2003, Aranca is a global research & advisory services firm working with clients worldwide across financial markets, industry sectors and technology domains. Aranca brings to play the strong combination of best data and best talent to empower decision makers with intelligence and insights, enabling them to reach better business decisions. Our multi-disciplinary expertise is designed to cater to clients of all sizes across a wide spectrum, from Fortune 500 companies and financial institutions to private equity and high potential startups. In the MENA region, Aranca works with some of the top family groups, private equity and investment management firms with strong focus on strategic corporate and financial advisory services.

Disclaimer

The information contained herein is believed to be obtained from the reliable sources and Aranca disclaims all warranties as to the accuracy, adequacy and completeness of such information.

Since Aranca is not a law firm, it (including its directors, employees and representatives) does not and cannot render legal services/advice to any individual or entity in any part of the world.

Author

Neha Tapase

Assistant Manager

Technology Research and Advisory

Aranca

Unit 201 & 301, Floor 2 & 3, B Wing, Supreme
Business Park, Hiranandani Gardens, Powai,
Mumbai – 400 076