

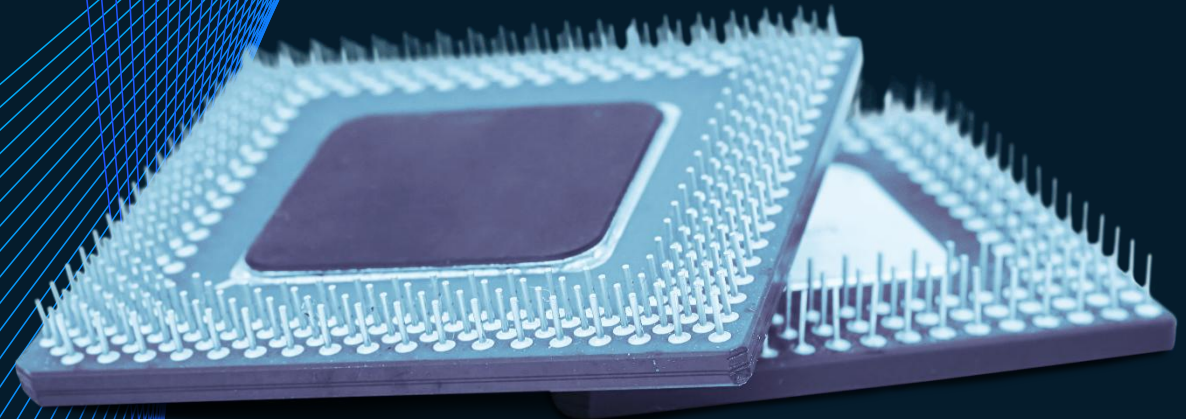
McKinsey
& Company

Quantum Technologies – the next GenAI in Finance?

Talk at Fields Institute

October 2025

CONFIDENTIAL AND PROPRIETARY
Any use of this material without specific permission
of McKinsey & Company is strictly prohibited



Contents

Market and investment perspective

Value at stake in finance

Quantum use cases in finance

Outlook

Breakthroughs in qubit stability are fuel for use case development in finance...

What's New? (Key Breakthroughs)



Qubit stability in focus

System-wide efforts on quantum control & stabilization



Big tech pushing forward

Continued progress in performance & scalability



Error correction goes mainstream

Now essential for system accuracy – no longer optional

What's the Momentum? (Patents & Publications)



+13% growth in quantum tech (QT) granted patents – US leads

+7% growth in publications (vs. 2023)
China contributes **~42%** of all global publications

Patent application leaders

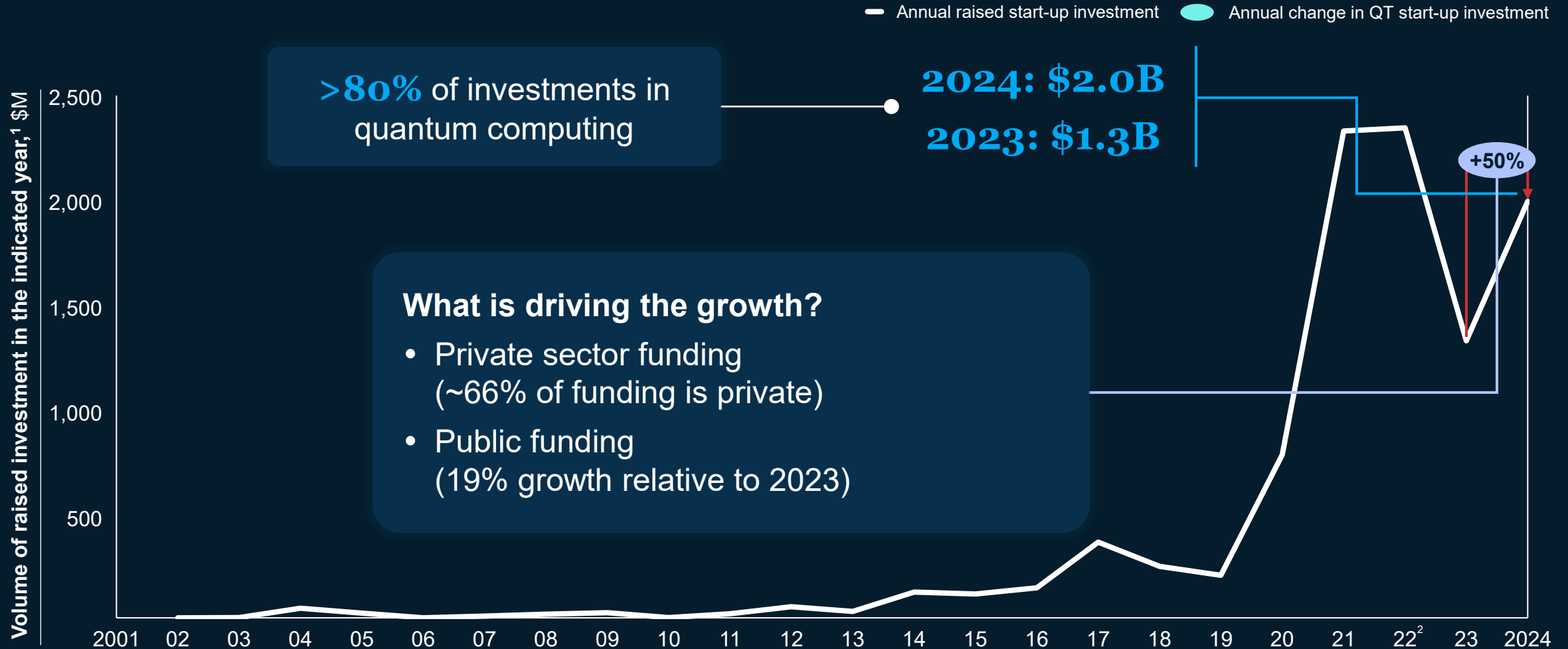
Quantum communication: US **~43%**

Quantum sensing: US **~45%**

Quantum computing: China **~32%**, US **~22%**



...accompanied by a growth in Quantum Tech funding increasing 50% in 2024 to \$2B

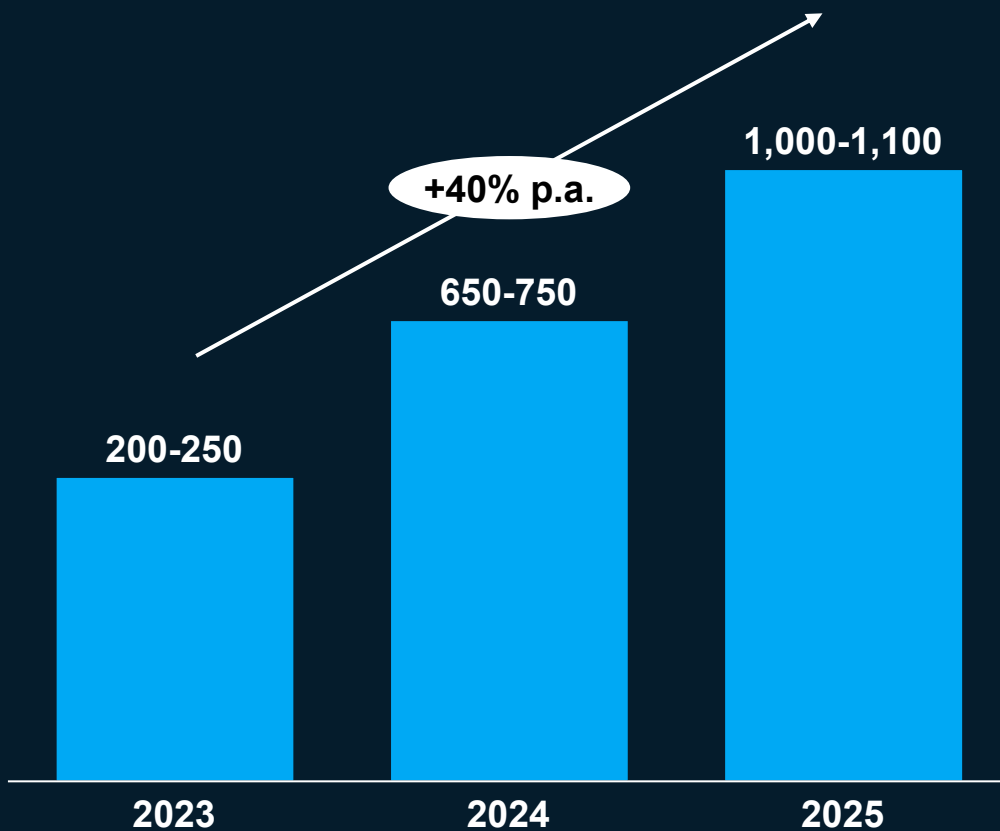


1. Based on investment data recorded in PitchBook; actual investment likely higher (excl. investments with missing details on investment types); data availability on start-up investment in China is limited

2. Excludes other uncategorized funding data

QC companies began a shift towards co-development of use cases yielding revenue generation, expected to surpass \$1B by 2025

Revenue estimates of QC companies, \$M



Quantum technology market size scenarios in 2035/2040

Based on existing development roadmaps and assumed adoption curve

	Quantum computing	Quantum communication	Quantum sensing ¹
2035	\$28B-\$72B	\$11B-\$15B	\$7B-\$10B

Potential economic value² from quantum computing in 2035:

~\$1-2T

potential economic value driven by four industries

1. Approach for quantum sensing updated through clusters of use cases based on recent development, announcements, and breakthroughs

2. Economic value is defined as the additional revenue and saved costs that the application of quantum computing can unlock

Contents

Market and investment perspective

Value at stake in finance

Quantum use cases in finance

Outlook

QC presents a \$1T to \$2T opportunity, with ~\$600B in Finance and rapid acceleration expected in the coming five to ten years

Preliminary

Economic value¹

Focus Economic value: + Low ++ Medium +++ High

Industry	Key segment for QC	~2025-2030	~2030-2035	Value at stake with incremental impact of QC by 2035 (billion USD)
Financial industry ¹	Financial services	++	+++	400-600
Global Energy & Materials	Oil & gas	+	++	200-500
	Sustainable energy ¹	+	+++	
	Chemicals	++	+++	
Travel, Transport & Logistics	Travel, transport, and logistics	+	+++	200-500
Pharmaceuticals & Medical Products	Pharmaceuticals	++	+++	200-500
Advanced Industries	Automotive	+	++	70-400
	Aerospace & defense	+	++	
	Advanced electronics	+	++	
	Semiconductors	+	++	
Insurance	Insurance	+	++	50-100
Telecom, Media & Technology	Telecom	+	++	50-100
	Media	+	+	
Total				900-2000

1. Quantum computing technologies and industry is immature and has high uncertainty for viability and value of use cases. Business value estimates are preliminary and intended to guide research towards high-value potential areas, not as definitive projections for business value.

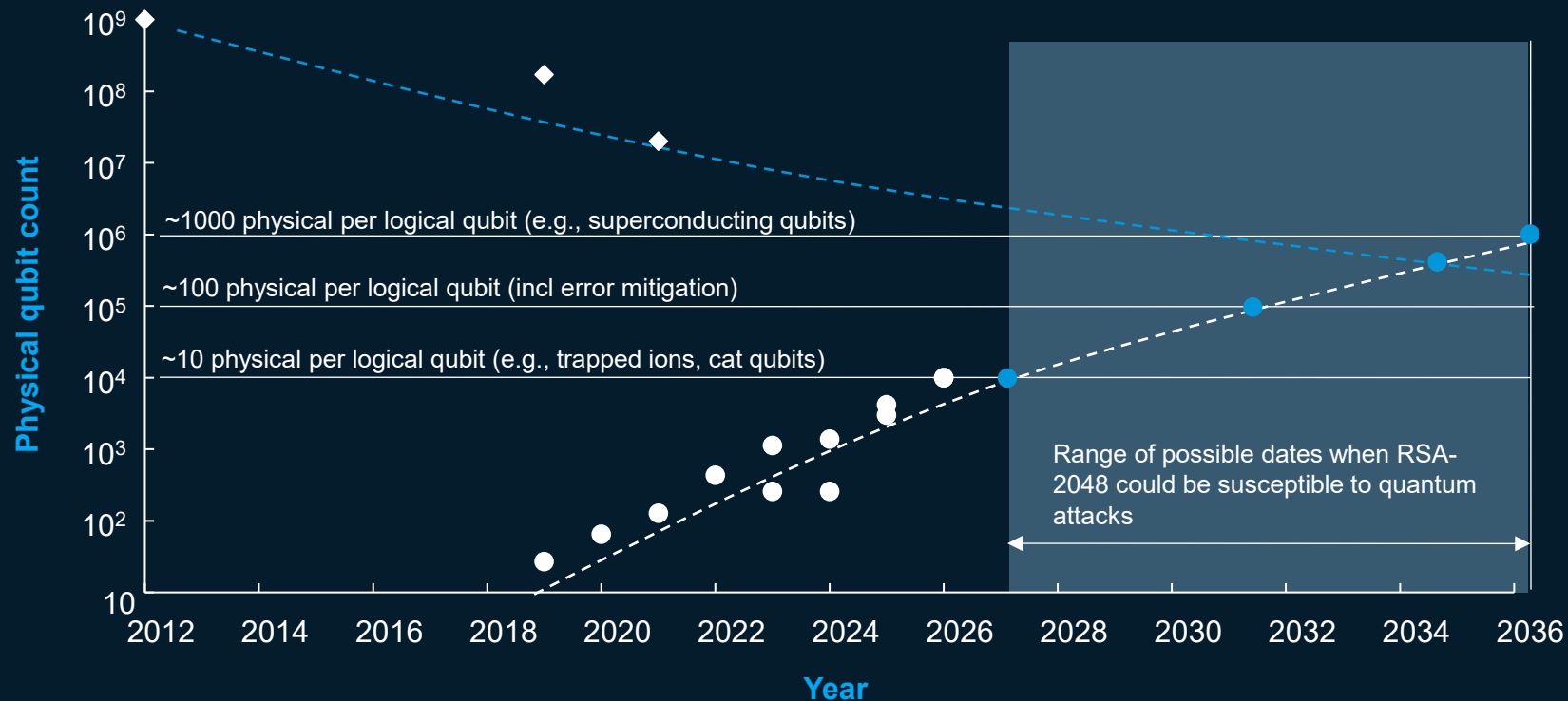
2. Sustainable energy market is expected to grow rapidly from 2022-2035. However, the 2035 market size is influenced by numerous factors and challenging to predict

Classical security protocols could be susceptible to quantum attacks; financial institutions need to prepare for Q-Day

Illustrative

Quantum resource availability and requirements by year (illustrative), 2012–'36

- Industry road maps ◆ Proposed resource requirements to break RSA-2048¹
- When number of available physical qubits meets resource requirements to break RSA-2048 (approx projections)
- Trend for physical qubit count required to break RSA-2048 --- Availability of physical qubits (incl projected)²



Key insights



- Once RSA-2048 is susceptible to quantum attacks (potentially happening once ~1,000 logical qubits are reached) the first signs of Q-Day may show
- However, the timelines do not solely depend on number of qubits, but also on the algorithms developed (i.e., proposed resource requirement to break RSA-2048¹)
- Business leaders may need to prepare for Q-Day before RSA-2048 is susceptible to quantum attacks, e.g., through post-quantum cryptography

1. Craig Gidney and Martin Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, Quantum, April 2021
 2. Historical for pre-2024, projected for post-2024

Q-Day is expected to have a strong impact on the financial industry which is highly reliant on cryptography and has high crypto-agility

Selected industries

+ Low ++ Medium +++ High

Industry	Key segment	Cryptographic requirements ¹	Crypto-agility ²	Q-Day impact ³	Rationale	QKD adoption likelihood
Finance	Financial services	+++	+++	+++	High demand for secure communication and long-term storage, IT modernization efforts help provide crypto-agility, high Q-Day impact due to diverse, highly distributed infrastructure	+++
	Oil and gas	++	+	+	Limited secure communication requirements, low IT maturity, limited Q-Day impact	+
Global energy and materials	Sustainable energy	++	+	++	Critical infrastructure has high security requirements, other parts of segment have lower security requirements	++
	Chemicals	+	+	+	Limited secure communication requirements, lower IT maturity, limited Q-Day impact	+
Travel, transport, and logistics	Travel, transport, and logistics	++	++	++	Medium demand for secure communication and storage, digitalization efforts to enhance IT modernization improve crypto agility, medium Q-Day impact due to highly distributed infrastructure	++
Pharma and medical products	Healthcare	++	++	+++	IP and health records require secure communication and storage, some crypto agility from digital technology influx, high Q-Day impact	++

Likely QKD adopters include industries with high Q-Day impact and low crypto-agility

1. "Cryptographic requirements" refers to degree of need for strict cryptographic standards
2. High crypto-agility if software and hardware infrastructure are amenable to rapid updates of cryptographic systems
3. Estimated degree to which Q-Day—when commonly used cryptosystems (e.g., RSA, ECC) are susceptible to quantum attack—will affect operations

Meaningful use cases for quantum finance result in three types of impact



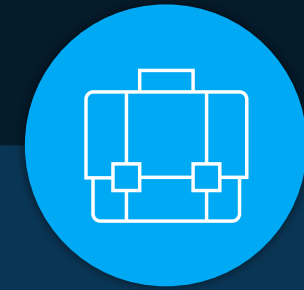
Cost reduction

Quantum computers enhance the accuracy of the underlying model by handling more variables and underlying data with less aggregation yielding cost savings



Acceleration

Quantum computers can operate more efficiently resulting in a speed-up in compute time



New business opportunities

Quantum computers can unlock new use cases that classical computers are not able to calculate

A Quantum Computer can solve particular types of problems in Finance

Which problems can a Quantum Computer solve?

- **Linear algebra (Machine Learning/ AI)** for, e.g., reduction of large data for better decisions, predictions and automation
- **Stochastic modelling and simulation** of quantum systems and processes, e.g., to model credit risk
- **Mathematical optimization** with algorithms that can enable near real-time optimization for, e.g., financial modelling
- **Factorization (Security)** of large numbers with exponential speedup to break, e.g., main-stream encryption protocols

How do potential use cases for these types of problems in Finance look like?



Linear algebra

Identify anomalous entities and transactions in payment and customer networks for fraud detection



Risk modelling

Simulate risks across portfolios, including credit and liquidity, to understand exposures and stress factors



Optimization

being able to optimize matching of collaterals considering more collaterals and solving with higher accuracy

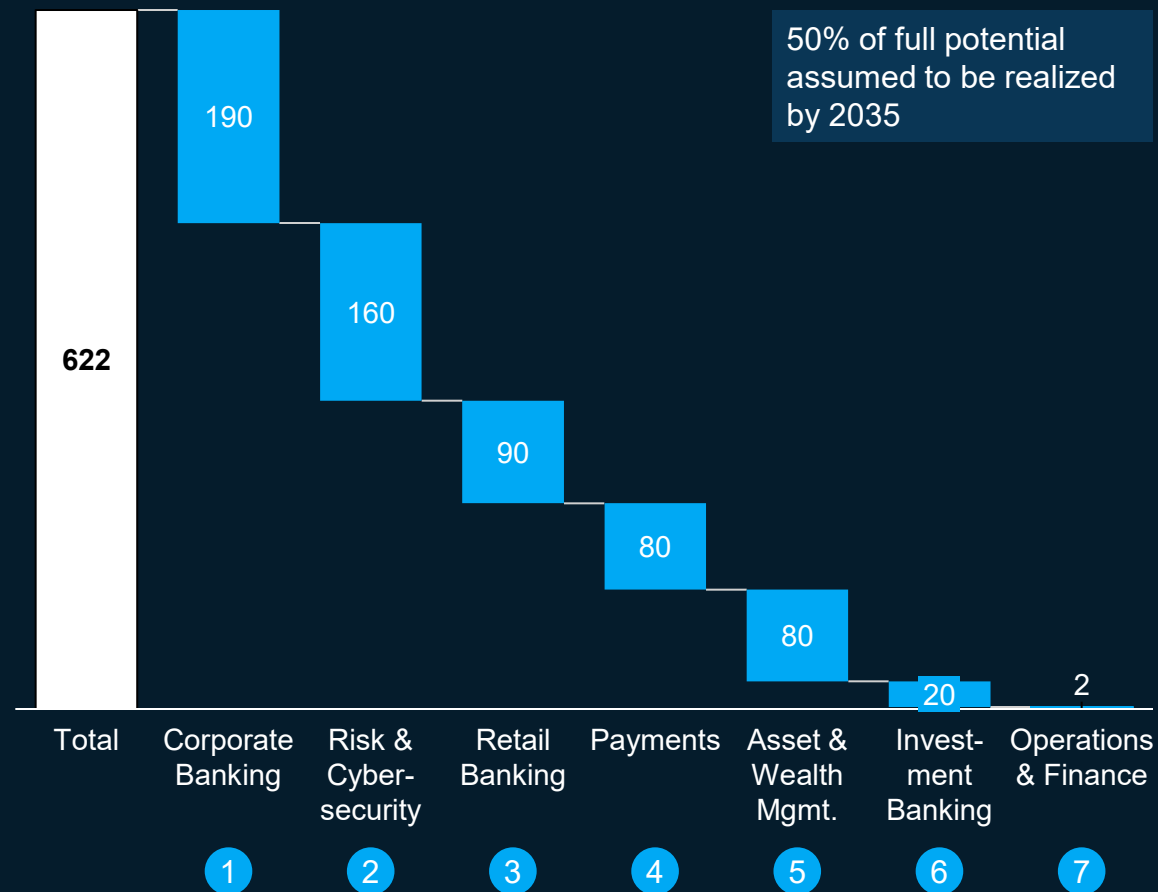


Factorization

using quantum random number generators to enhance security

The potential value at stake of quantum finance use cases is estimated to be USD 600 billion in 2035

Estimated value at stake of quantum finance globally per business unit in 2035, USD billion



Example use cases

- 1 Probability of default
Collateral optimization
- 2 Risk modelling
Fraud detection
- 3 Probability of default
Collateral optimization
- 4 Quantum blockchain
Quantum money
- 5 Non-physical assets
Portfolio optimization
- 6 Derivative pricing
Portfolio optimization
- 7 Customer service (QML)
Tax exposure optimization

Key assumptions

Assume full-scale fault-tolerant QC to be realized by 2035

Risk across all business units included under “Risk & Cybersecurity”

Includes both near-term and revolutionary next generation quantum use cases

PQC provides a near-term algorithm-based solution; fault-tolerant quantum computer requires QKD for quantum security

Preliminary



Vertical	Security	Performance ¹	Time to deployment	Total cost of ownership (TCO)	Infrastructure requirements ²	Market maturity	Example companies
PQC	<p>Heuristically secure (may be vulnerable against future attack leveraging quantum or classical algorithms unknown today)</p>	<p>Key rates on order of Gb/s Can be distributed over global networks</p>	<p>Primarily implemented as software update on existing hardware (which may require hardware upgrades)</p>	<p>Low TCO when only software update required High TCO if new hardware required to replace legacy systems</p>	<p>Low infrastructure requirements if only software update required May require substantial replacement of legacy hardware</p>	<p>Relatively new technology, poised to become more widely adopted</p>	
QKD	<p>Provably secure (with e.g., entanglement-based QKD)</p>	<p>Key rates on order of kb/s to Mb/s Max network lengths on order of 100 km</p>	<p>Requires installation of quantum technologies (incl. hardware infra.)</p>	<p>High initial infrastructure and hardware investments Additional hardware maintenance costs</p>	<p>Requires hardware for key distribution and potentially quantum repeaters May require dedicated quantum channels</p>	<p>Commercially available but technology not mature</p>	

While regulators still focus on near-term PQC, QKD is needed for full quantum security, the industry is preparing for

1. Measured by key rates and max deployment distances. 2. Includes specialized hardware required, classical infrastructure that must be replaced versus adjusted

Contents

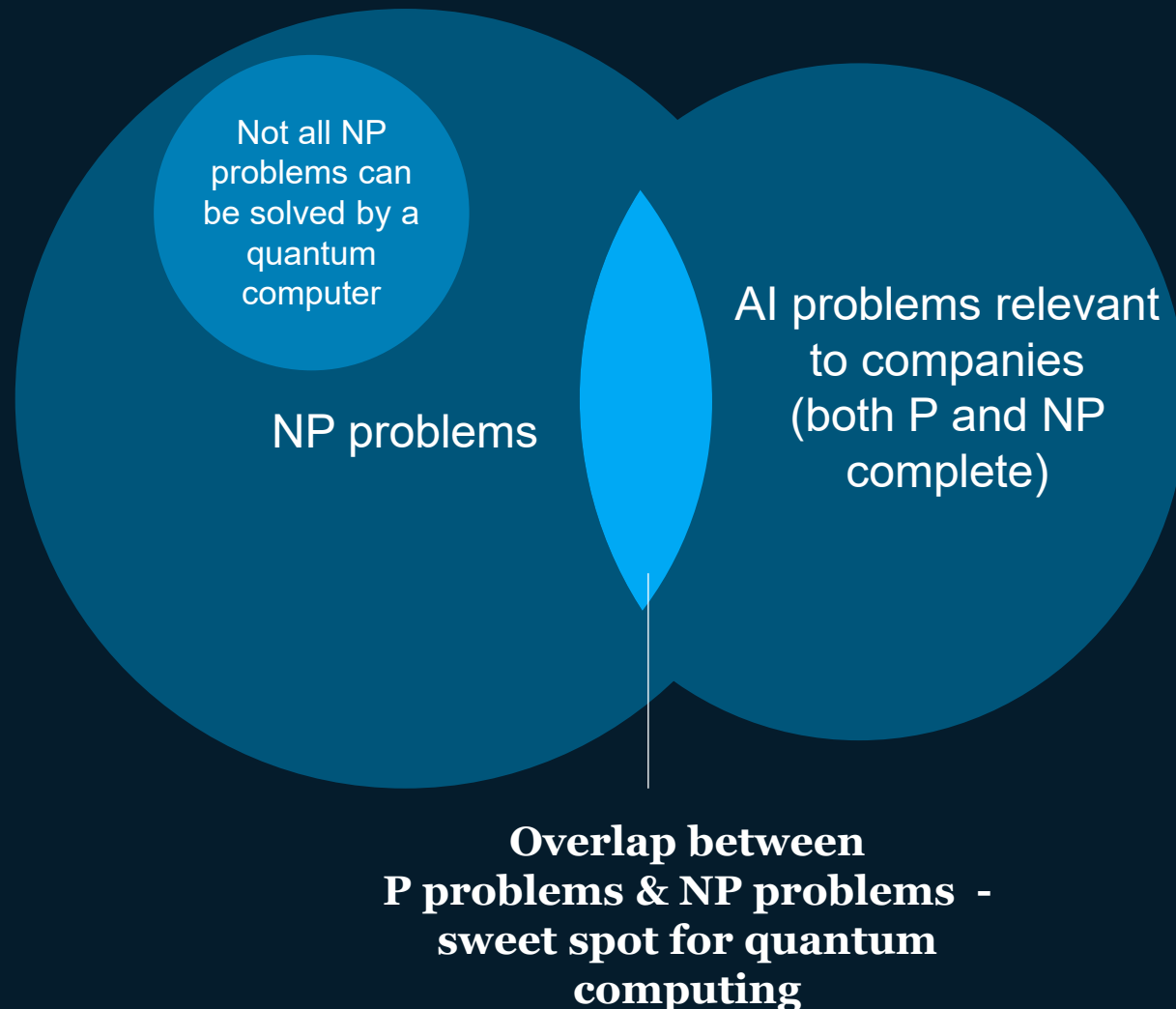
Market and investment perspective

Value at stake in finance

Quantum use cases in finance

Outlook

Most problems that are of practical nature for companies to date can find a solution through quantum computing



Key questions



Are there relevant NP problems for industry that cannot be efficiently solved on a quantum computer?

Are there NP problems that can be used for cryptography that would allow for PQC that cannot be broken?

When will a quantum computer also be relevant for P problems that can be solved efficiently today?

Collateral optimization is a major challenge both for corporates and banks

Banks can accept numerous types of collateral...

Sites
Aircraft
Shares of capital
Rolling stock
Residential property
Land
Property complex (plant, enterprise, etc.)
Com. property
Sea and river transport
Equipment
Construction-in-progress
Contractual claims
Livestock, poultry, fish
Self-propelled vehicles and other machinery
Goods in circulation
Transportation vehicles
Securities

- Cash
- Gold
- ...

... and corporates have typically numerous needs for



Typically, it is a complicated matching problem between the needs and available collateral

Enterprises usually have a large number of different loans for which a collateral is required...



... and they usually have many different options for assets that can be used as collateral

The many ways in which loan types and collaterals can be combined with the regulations and the pros and cons of each type make this a highly complex optimization problem

Contents

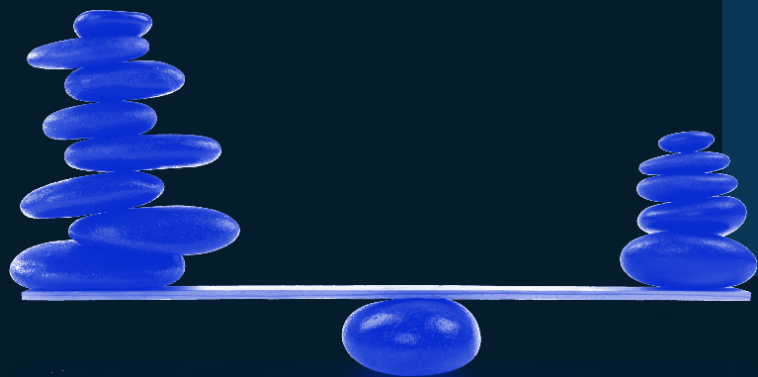
Market and investment perspective

Value at stake in finance

Quantum use cases in finance

Outlook

Three key success factors to sustainably leverage quantum technologies in the upcoming years



1



Take action now

Build quantum capabilities

Identify relevant use cases

Work closely with senior executives to generate sponsorship and consistent funding for a long development period

2



Capture Value

Start experimenting with quantum use cases now

Improve existing classical solutions through working on quantum

Leverage first mover advantage

3



Include all business units

Encounter all business units for potential use cases

Include business leaders into the progress

Value at stake might come from unexpected business units