QUANTUM COMPUTING

STATE OF THE NATION

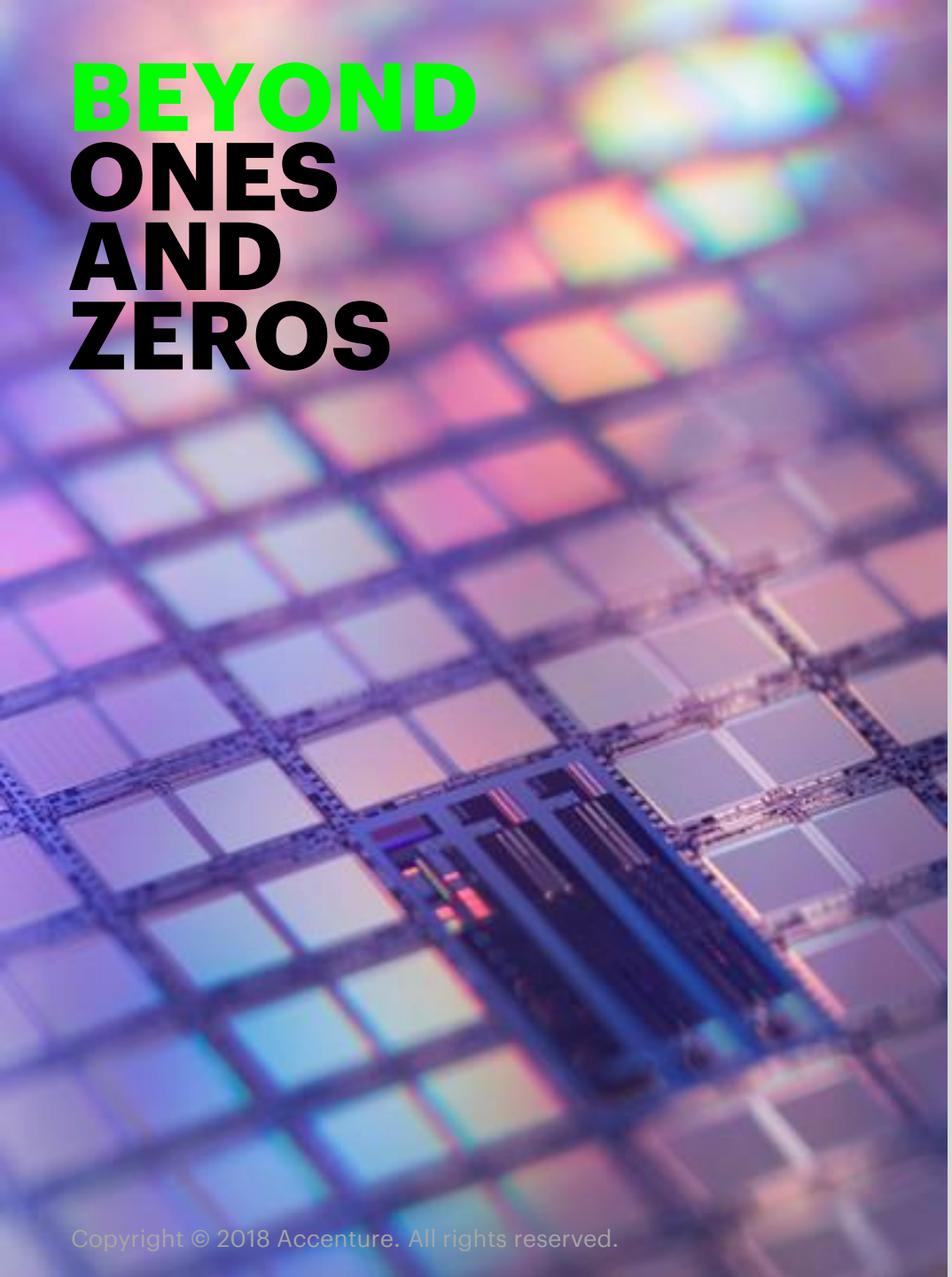
OPEN RHEIN MAIN 2019

MATTHIAS ZIEGLER

EMERGING & GROWTH ASGR AND TECHNOLOGY INCUBATION GLOBAL LEAD

SEPTEMBER, 2019

accenturetechnology



BEYOND ONES AND ZEROS

“WE ARE CURRENTLY IN THE MIDST OF A SECOND QUANTUM REVOLUTION:

THE FIRST GAVE US NEW RULES THAT GOVERN PHYSICAL REALITY.

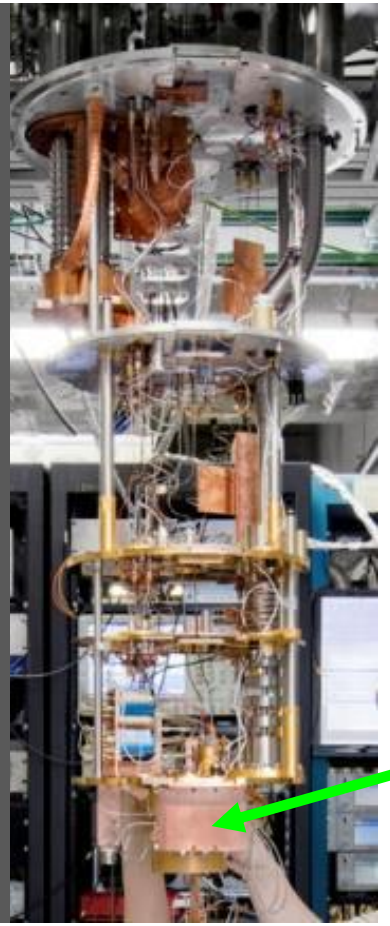
THE SECOND WILL TAKE THESE RULES AND USE THEM TO DEVELOP NEW TECHNOLOGIES.”

JONATHAN P. DOWLING

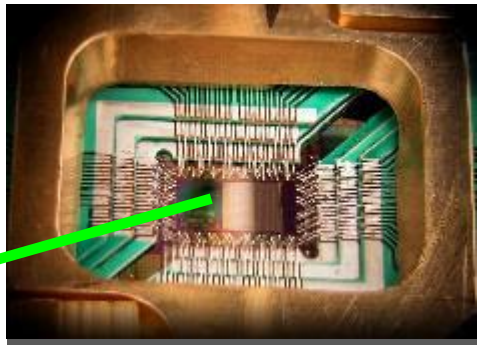
TAMING QUANTUM PHYSICS – APPLICATION:
QUANTUM COMPUTER ON PREMISE AND CLOUD

Dilution Refrigerator

Microwave Setup



Electronics



QPU

cooler than outer space (2.6 K ≈ -270°C): <0.1 K, fast electronics (GHz), the size modern transistors (10 nm)

Copyright © 2018 Accenture. All rights reserved.

TAMING QUANTUM PHYSICS – APPLICATION: FIRST COMMERCIAL QUANTUM COMPUTING SYSTEMS

IBM Q System One

Gate QC: 20 High Fidelity Qubits

D-Wave 2000Q

Annealer: 2000 Qubits

Copyright © 2018 Accenture. All rights reserved.

TAMING QUANTUM PHYSICS - VISION: CLASSICAL SHORTCUT BY A QUANTUM DETOUR

CLASSICAL

QUANTUM

CLASSICAL

PROBLEM

QUANTUM TRANSLATION

ALGORITHM AT WORK

QUANTUM SOLUTION

SOLUTION

PERSPECTIVES ON SOLVING PROBLEMS WITH QUANTUM ADVANCED ANALYTICS

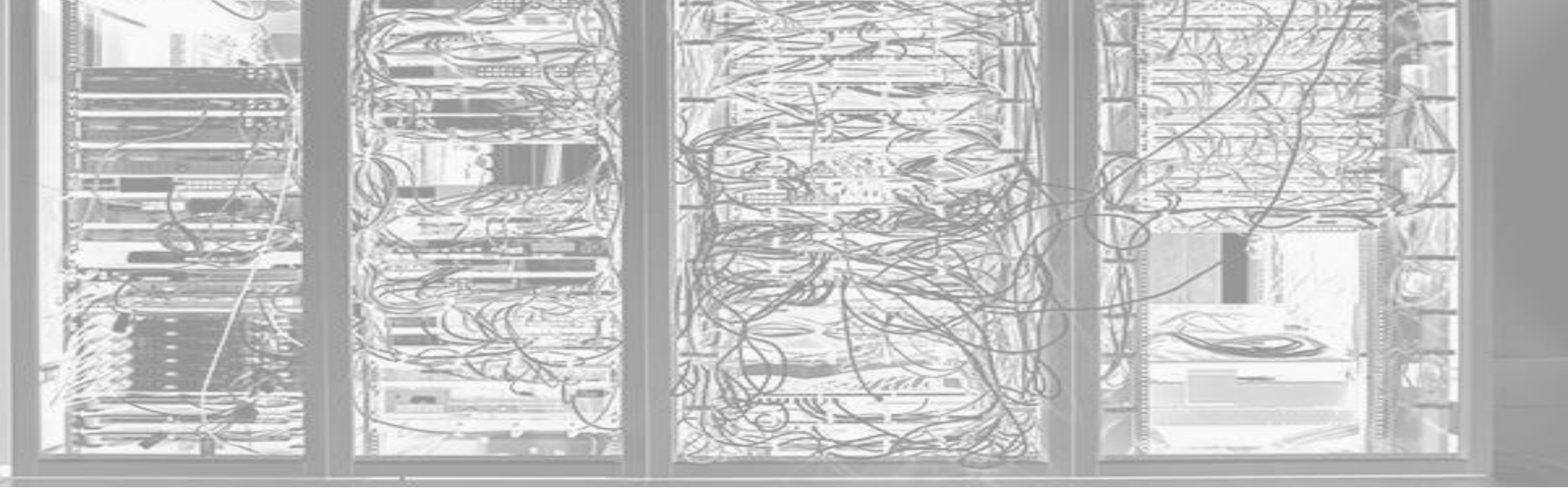
SIMULATION

OPTIMIZATION

CRYPTOGRAPHY

DATA ANALYSIS MACHINE LEARNING

THE FUTURE SCENARIO IS THAT QUANTUM COMPUTING WILL AUGMENT SUBROUTINES OF CLASSICAL ALGORITHMS THAT CAN BE EFFICIENTLY RUN ON QUANTUM COMPUTERS

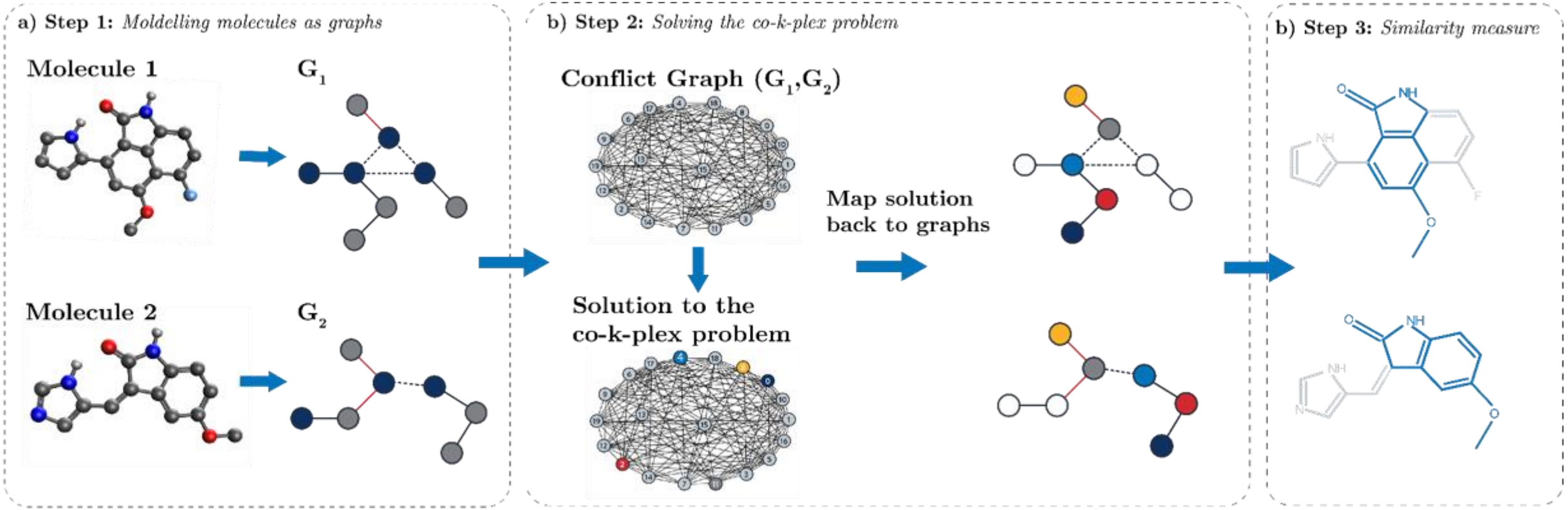


BIG RACKS IN THE BASEMENT?
SPINNING HEADS ON THE FLOORS ABOVE?
YOU FOUND A PLACE WITH QUANTUM COMPUTING POTENTIAL

Life Sciences

ACCELERATING DRUG DISCOVERY WITH QUANTUM COMPUTING

GRAPH BASED MOLECULAR SIMILARITY METHOD



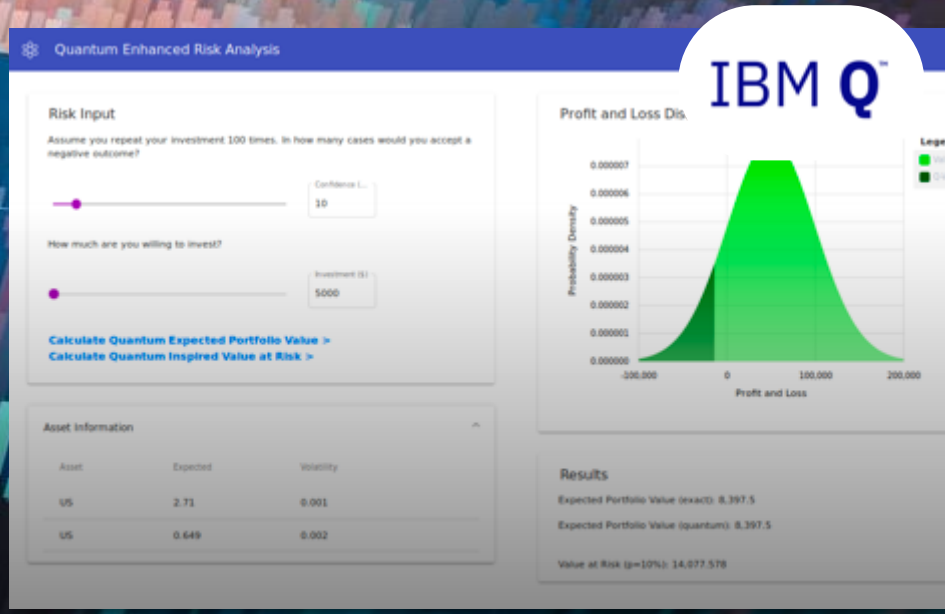
Financial Services

QUANTUM COMPUTING

MAKES FAST WORK OF ARBITRAGE OPPORTUNITIES

QUANTUM

PORTFOLIO RISK ANALYSIS



Risk analysis and it`s algorithms support the understanding and quantification of potential losses (or gains) e.g. to protect against default.

Discover the potential and current state of quantum risk analysis to support decision making for risk managers.

TOOLS

- Quantum
- Quantum Simulator
- Classical computer

RESULTS

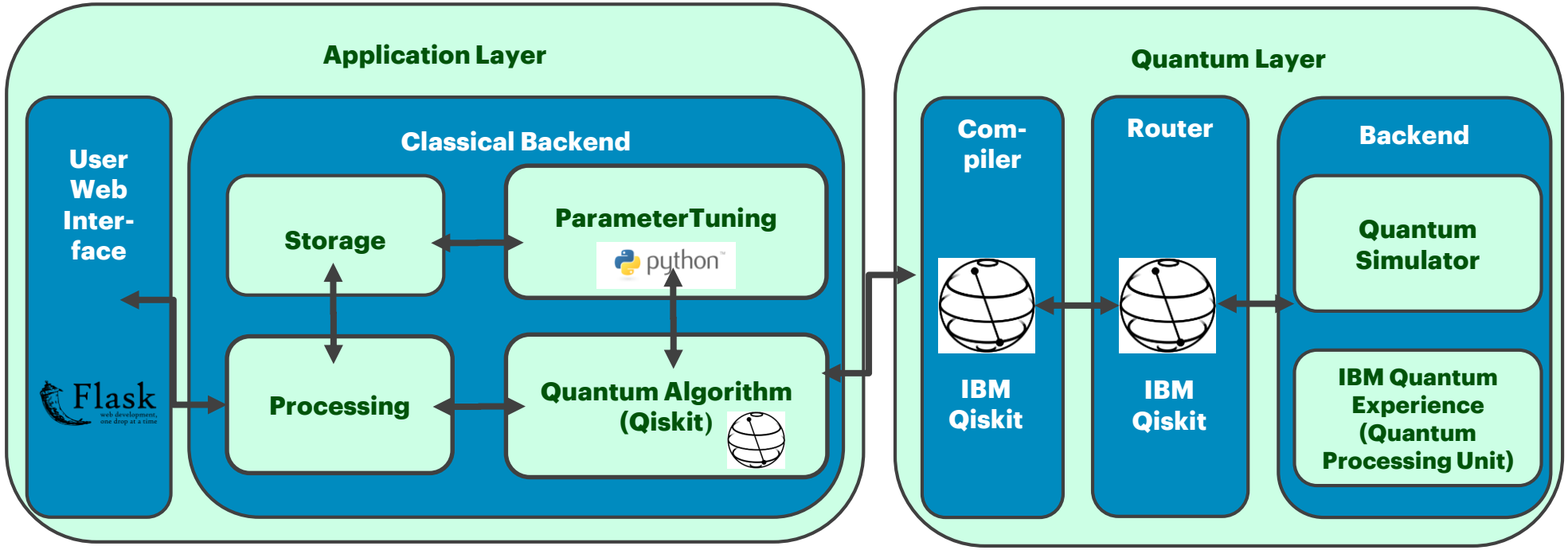
Experiment Data Set
Statistics of a set of financial assets, which are either randomly generated datasets or a collection of historical data*

Custom Enablement
Identify challenges along the quantum software stack from gate-level quantum back-end to web-application front-end

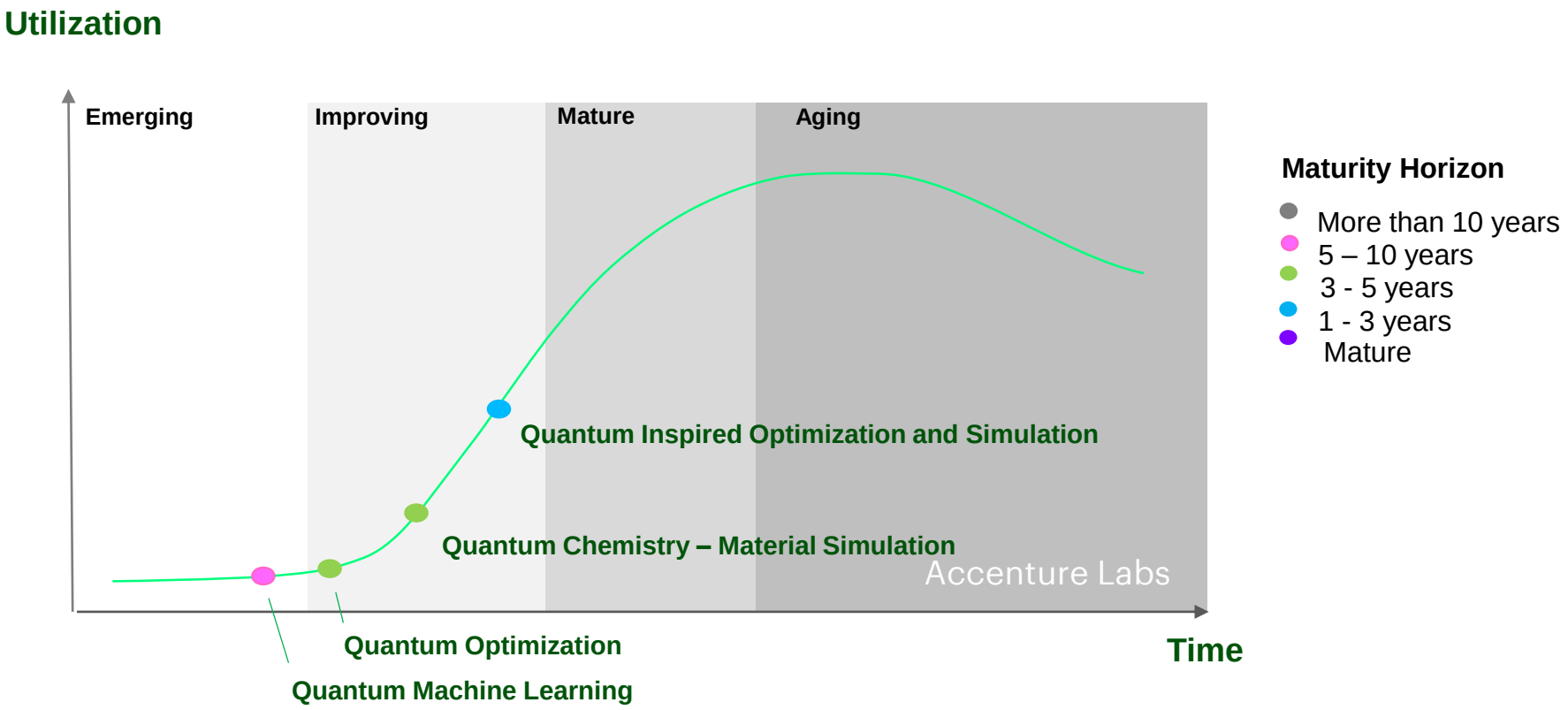
Problem specification
Quantifying portfolio investment risks to guide investment decisions depending on your risk threshold

*Historical data of government bond value development (https://www.investing.com/rates-bonds/germany-10-year-bond-yield-historical-data)

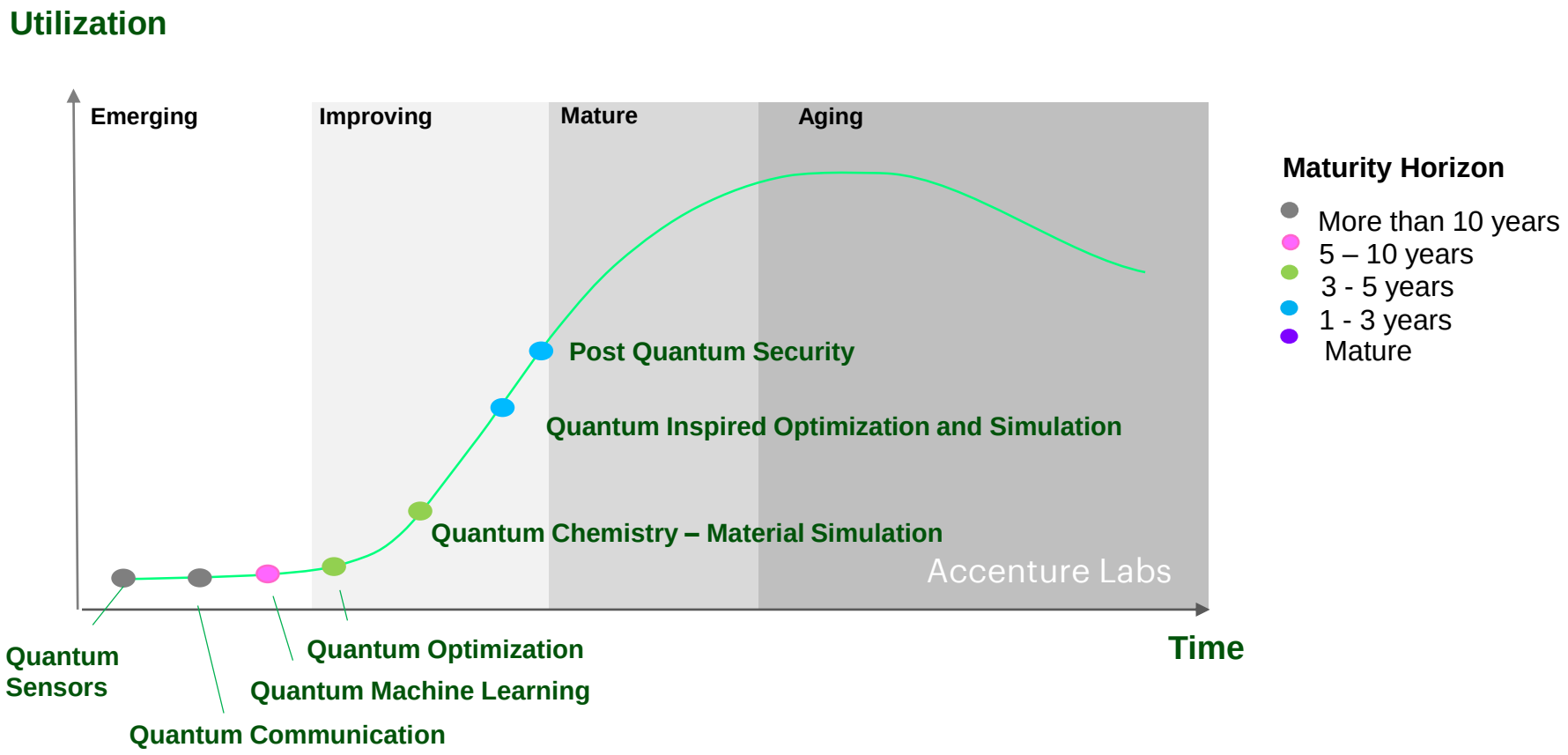
QUANTUM APPLICATION ARCHITECTURE GATE QUANTUM COMPUTING EXAMPLE



QUANTUM TECHNOLOGY INCUBATION



QUANTUM TECHNOLOGY INCUBATION



IMPLICATIONS ON SECURITY


WIRED

https://www.wired.co.uk/article/quantum-computers-quantum-security-encryption

The quantum clock is ticking on encryption – and your data is under threat

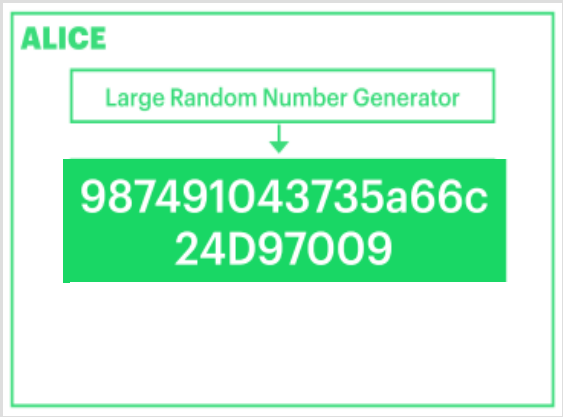
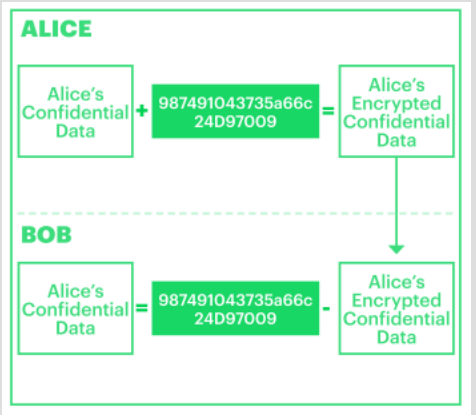
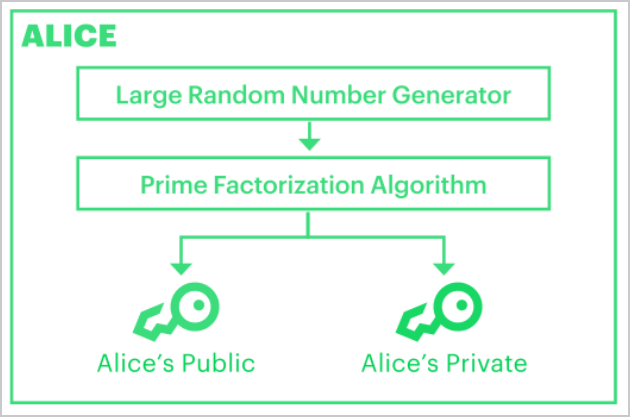
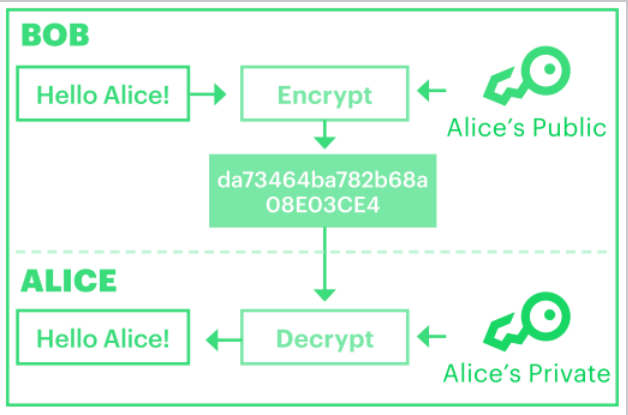
Quantum computers pose a major threat to the security of our data. So what can be done to keep it safe?

The Cryptography Stack by NIST

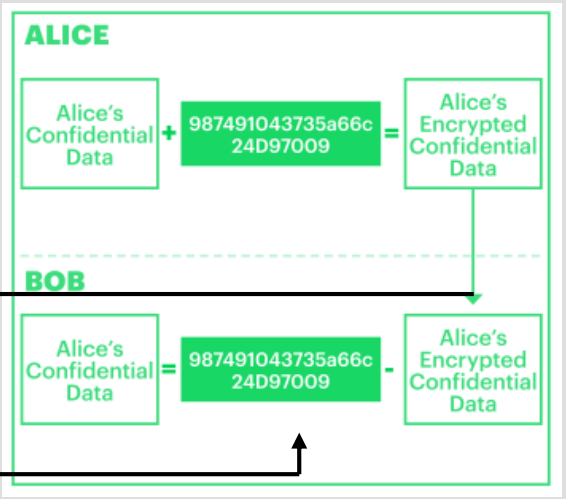
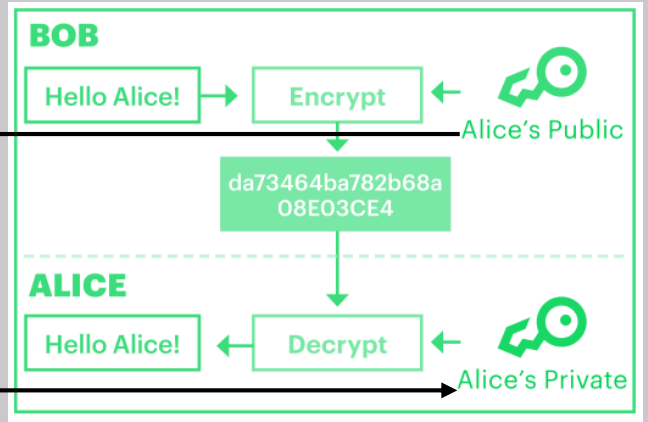
Applications	**web browsing, cloud services, e-mail, messaging, VOIP, storage encryption,**
Protocols (e.g. secure webserver-browser communication)	TLS, SSL, IPSec
Cryptography	Key exchange (RSA), encryption, authentication
Lower Level (Algorithms)	Libraries, block ciphers (AES, DES)

Is it time for a technology shift?

CLASSICAL CRYPTOGRAPHY

	Key Generation	En- & Decryption
Symmetric		
Asymmetric		

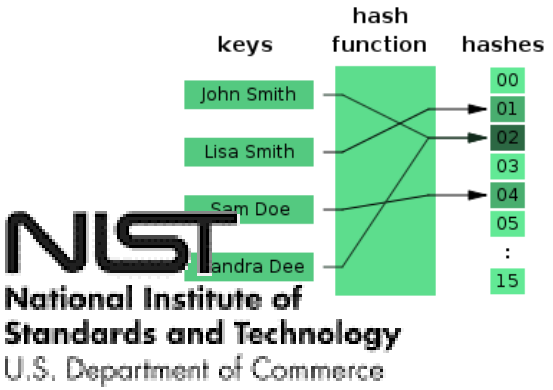
CLASSICAL CRYPTOGRAPHY - QUANTUM ATTACK CHANNELS

	Quantum Algorithm	Encryption & Decryption
Symmetric	**Grover Search** $\sqrt{N}$ speed-up for key search AES-128 – 64-80 bit security	
Asymmetric	**Shor Algorithm** exponential speed-up for prime factorization RSA – close to 0 bit security	

PHASE 1: POST QUANTUM CRYPTOGRAPHY

Theoretical Concept: e.g. Hash functions

Implementation: National Institute of Standards aims for draft standards between 2022-2024



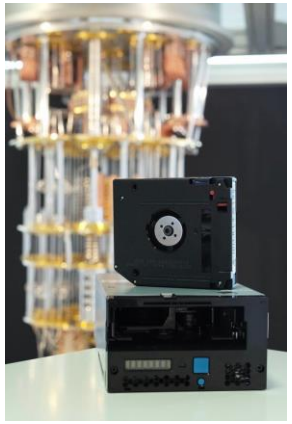
PHASE 2: QUANTUM COMMUNICATION

Proof-of-Concept

- 2700 km Sattelite transmision
- China trusted network
- 1.5 kbps 200 km optical cable

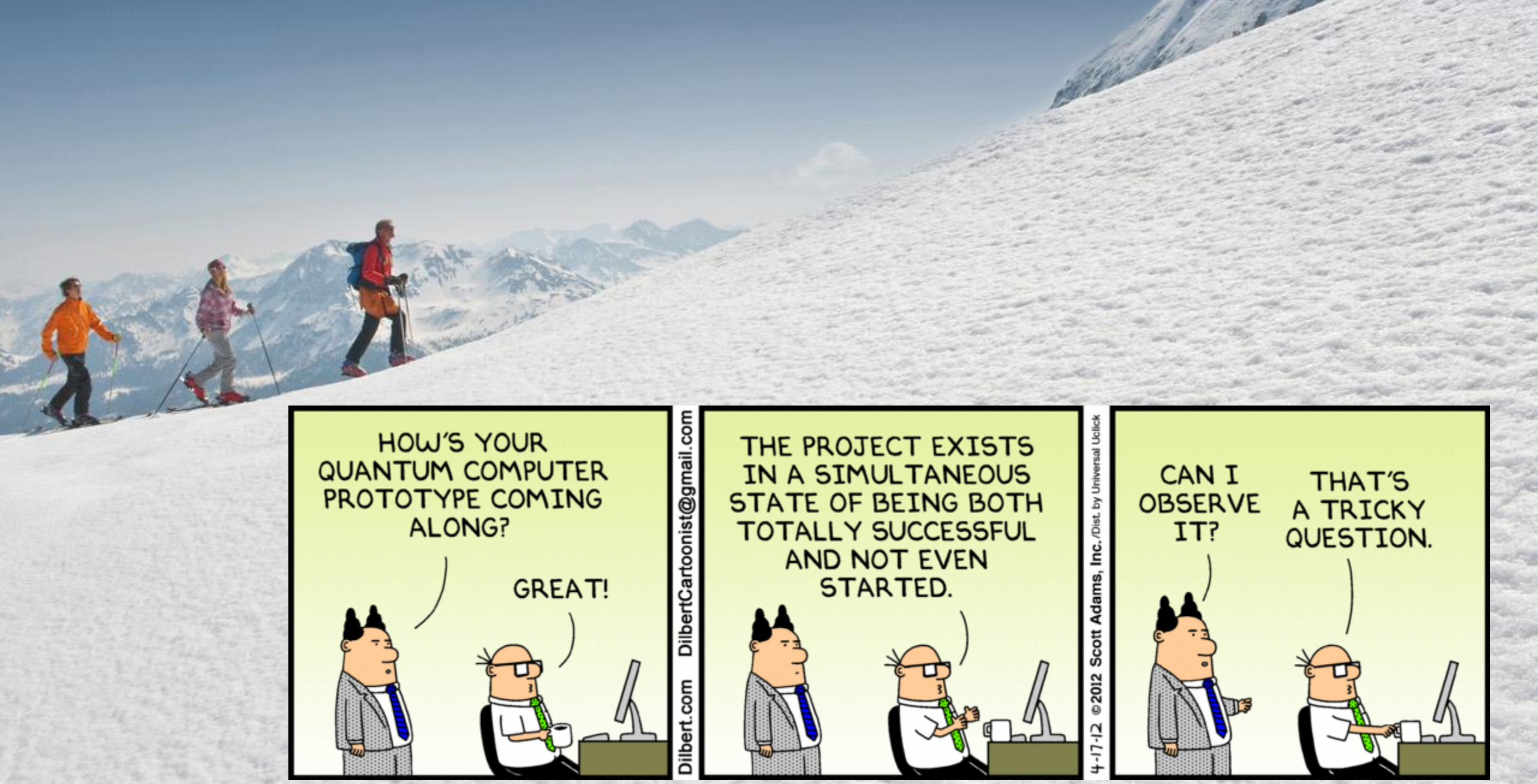
Industrial Implementation

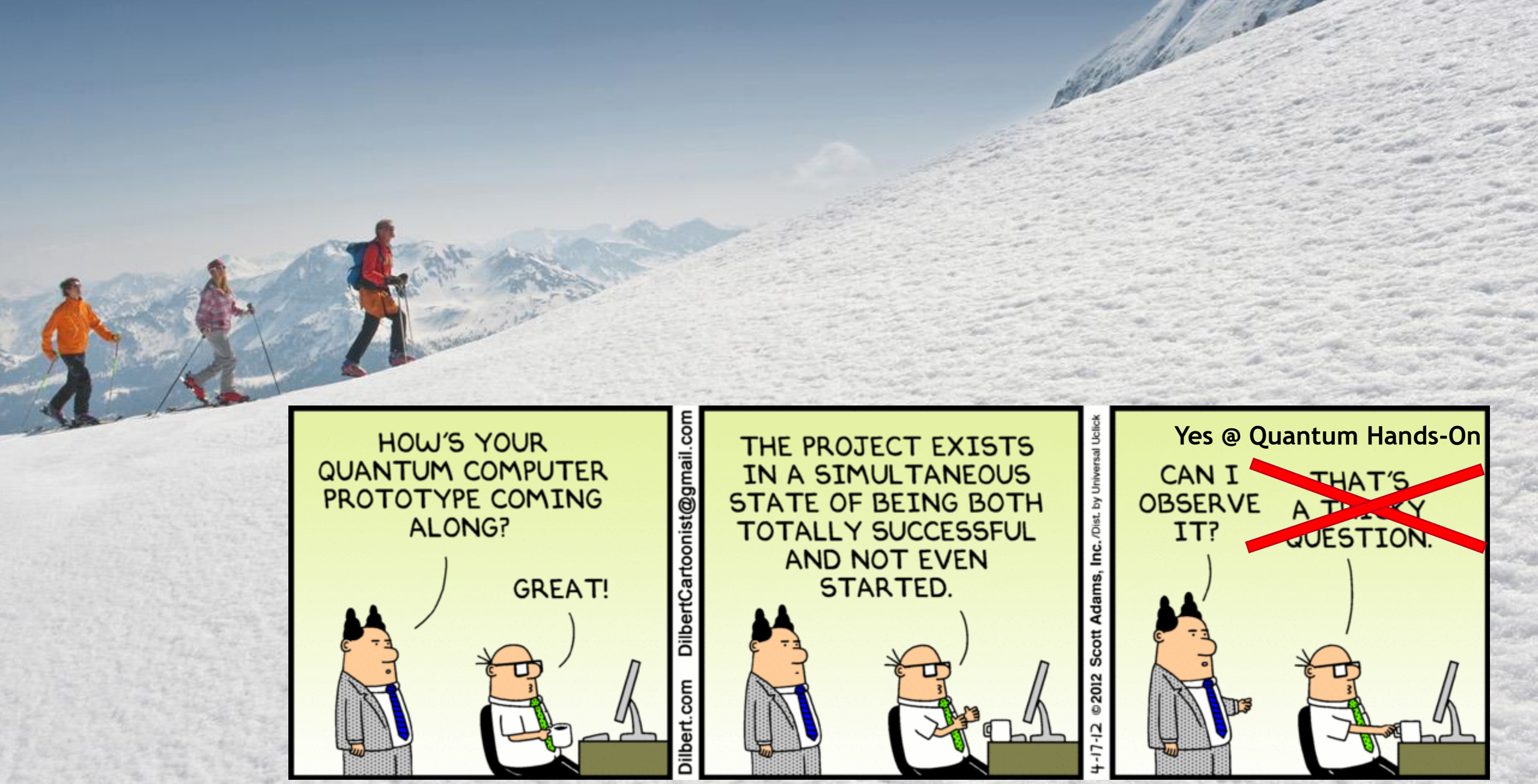
- **Transmision rates in optical fibre technology:**
  - 10 MBit/s for 10 km
  - 100 kBit/s for 100 km
- **Post-Quantum Encryption**
  - post quantum computing-safe tape drive prototype Credit: IBM



NEXT STEPS

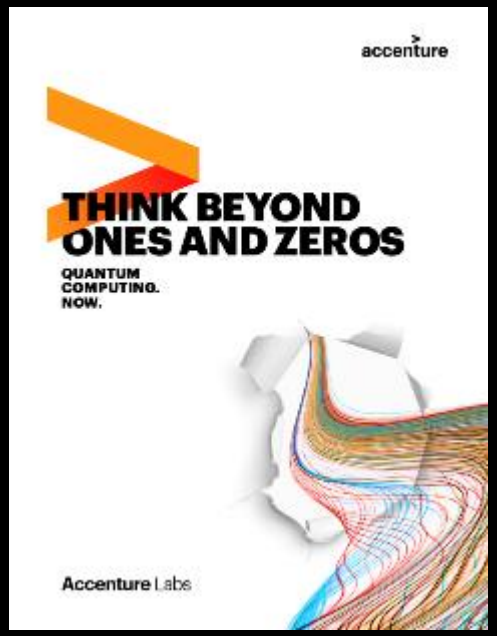
PREPARE FOR THE ARRIVAL OF MAINSTREAM QUANTUM COMPUTING BY CONDUCTING BUSINESS EXPERIMENTS USING QUANTUM COMPUTATION

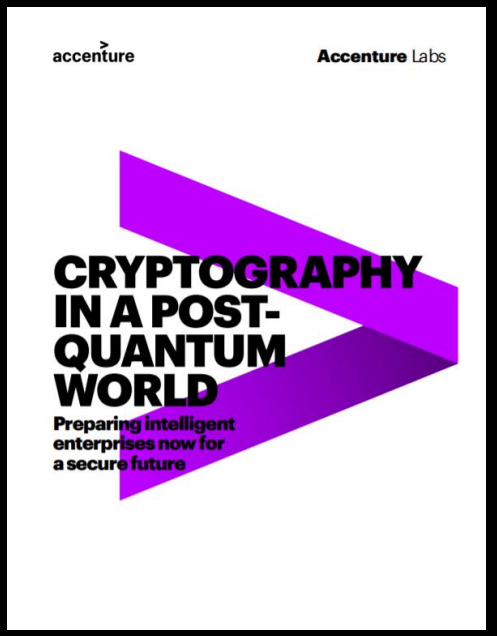




QUANTUM COMPUTING. APPLIED NOW.

LEARN MORE





www.accenture.com/quantum

@matthiasziegler

Matthias Ziegler

accenturetechnology