Computer von morgen

Quanten-Informationsverarbeitung

Renato Renner (ETH Zurich)

created with DALL E

Quanten-Technologie …

□ … bedroht die Sicherheit unserer Daten

□ … erhöht die Sicherheit unserer Daten

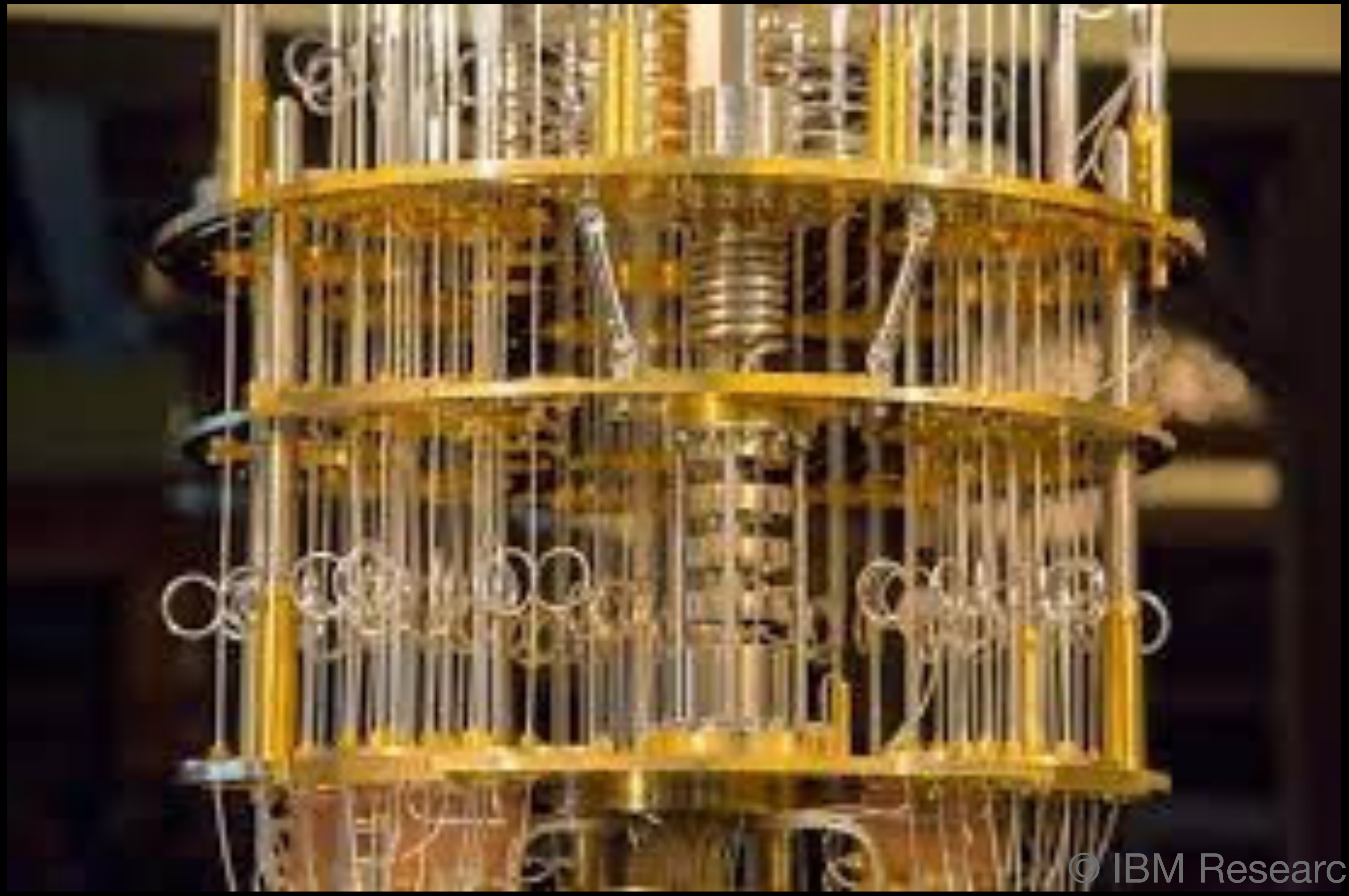
Quanten-Technologie …

☒ … bedroht die Sicherheit unserer Daten

☒ … erhöht die Sicherheit unserer Daten

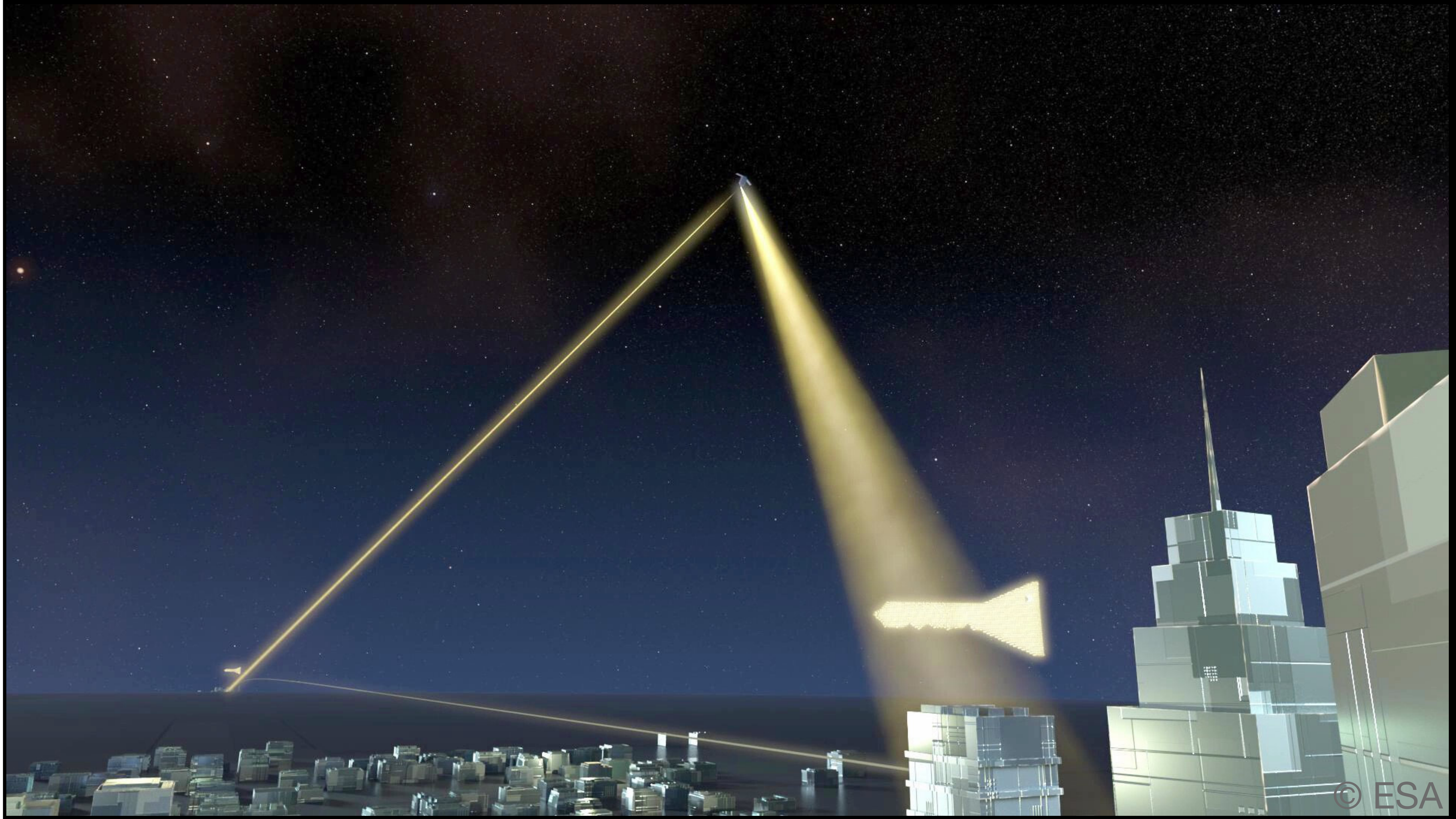
Doppelte Relevanz für Informationssicherheit

Quanten-Technologie
bricht herkömmliche Kryptographie



© IBM Research

Quanten-Technologie ermöglicht
absolut sichere Kommunikation



© ESA

Klassische Physik

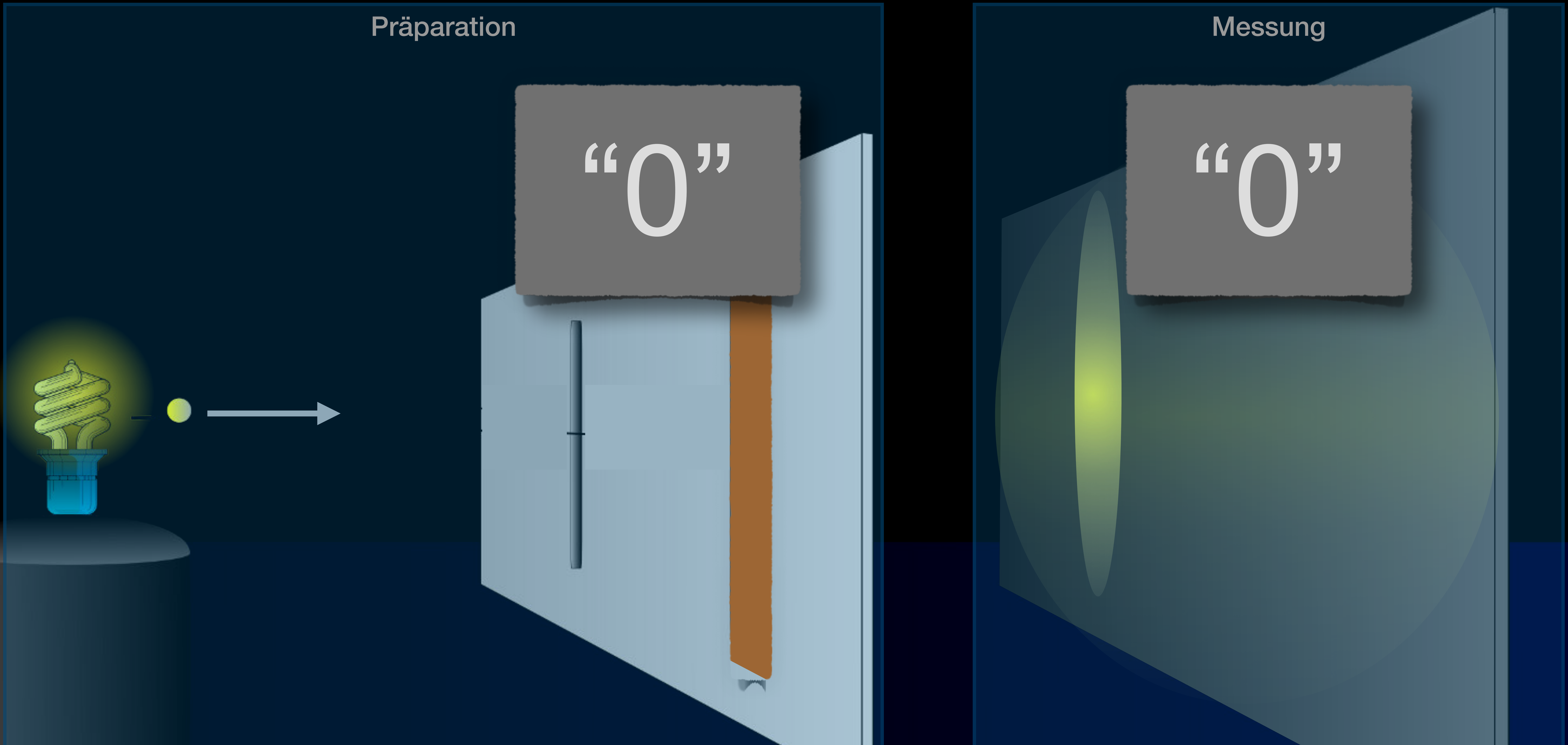
Klassische Physik

Klassische Physik

Klassische Information

Präparation
Messung

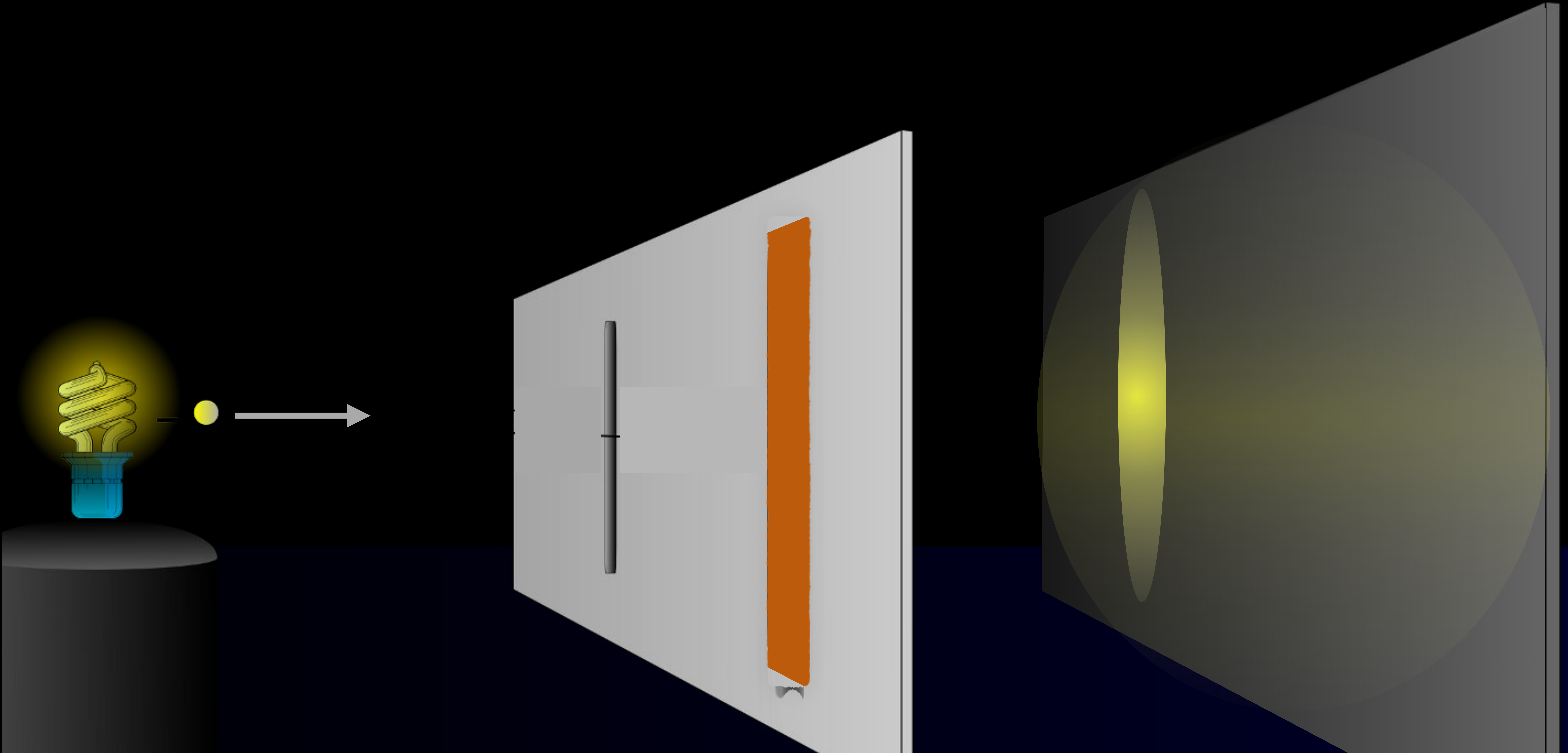
Klassisches Bit



Klassisches Bit

Präparation
“1”
Messung
“1”

Quantenphysik



Quantenphysik

Quantenphysik

Quantenphysik

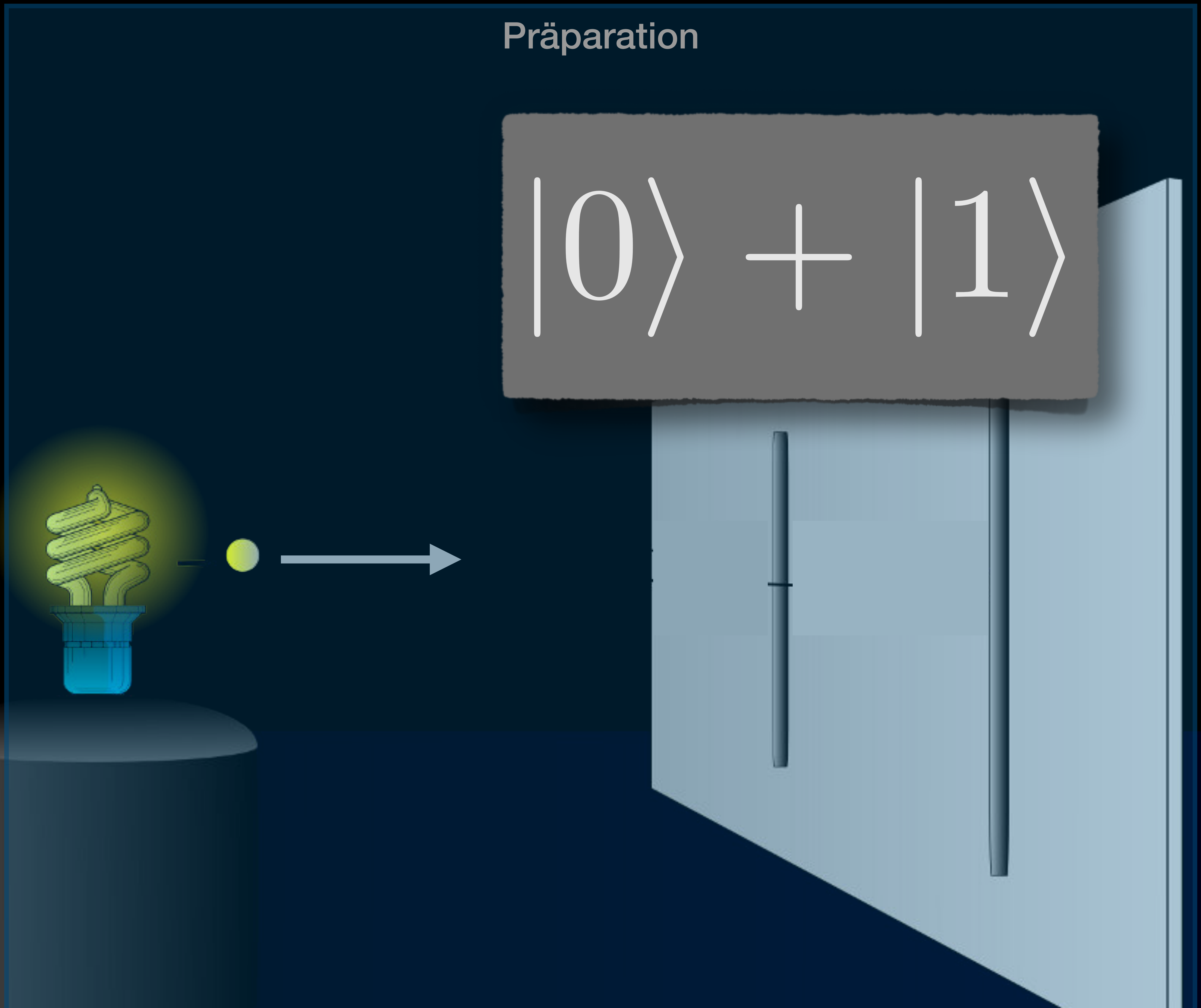
Qubit

Präparation
$|0\rangle$
Messung
$|0\rangle$

Qubit

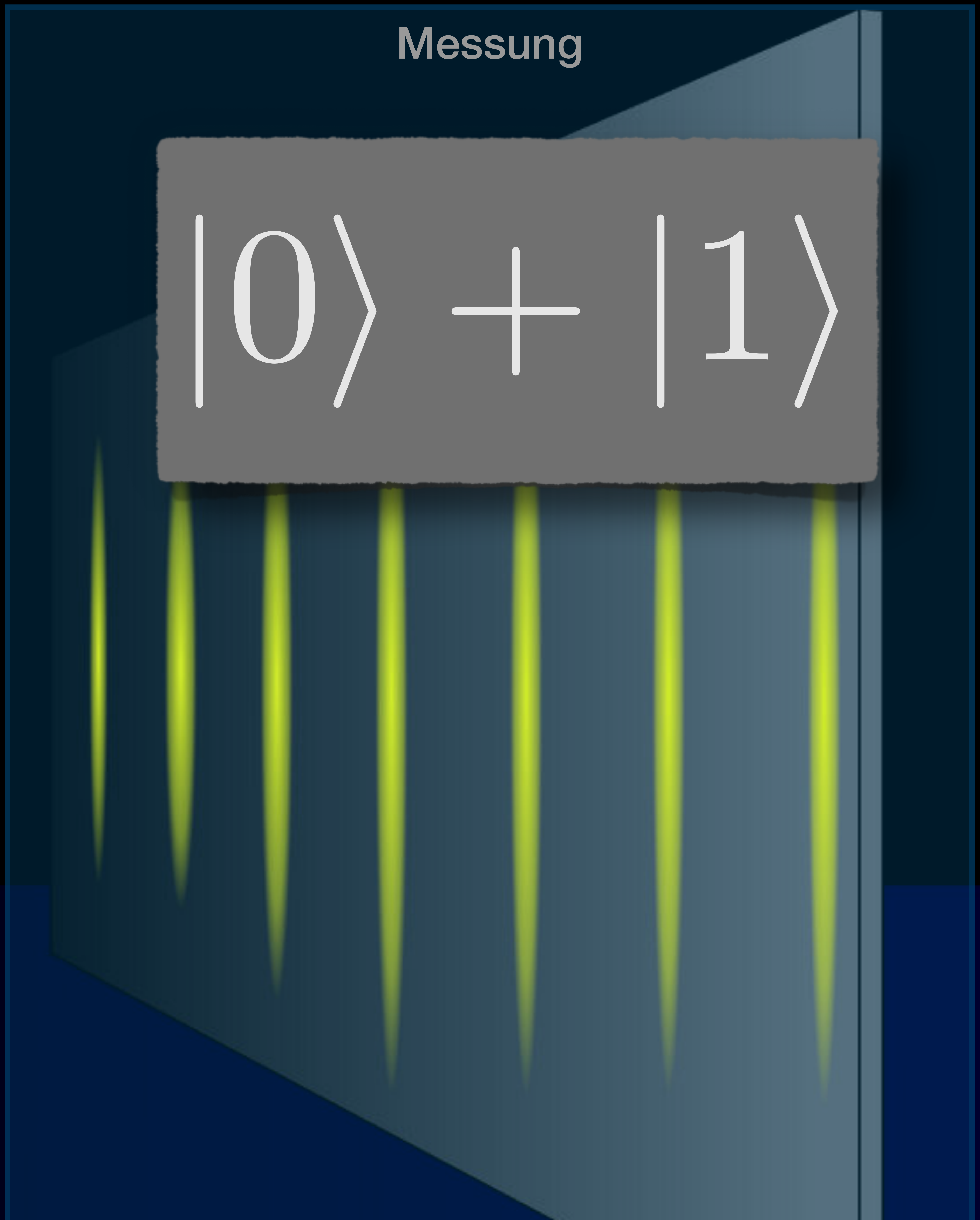
Präparation
$|1\rangle$
Messung
$|1\rangle$

Qubit



Präparation

$$|0\rangle + |1\rangle$$



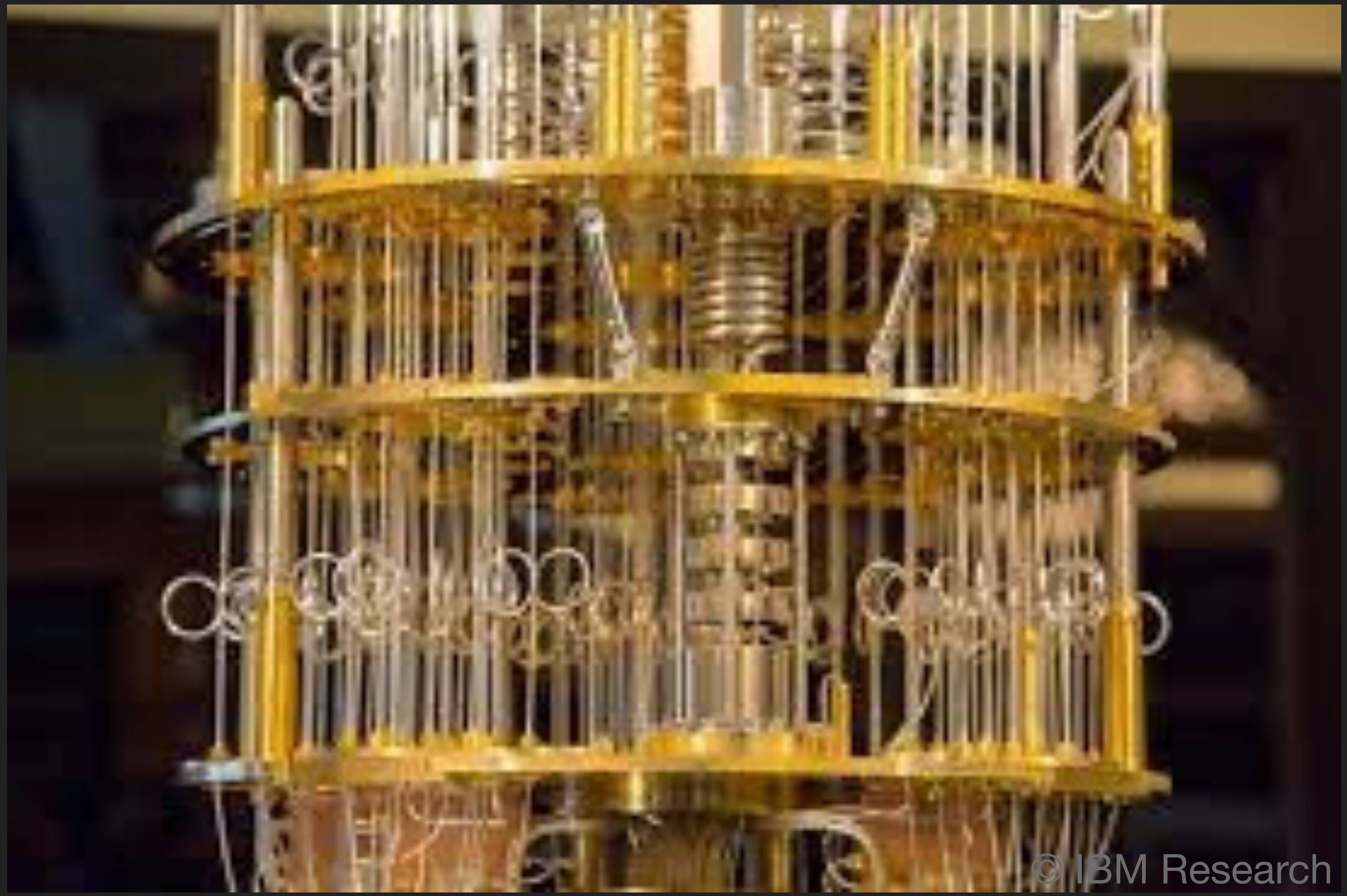
Messung

$$|0\rangle + |1\rangle$$

Qubits sind fragil

Präparation
$|0\rangle + |1\rangle$
Messung
$|0\rangle$
$|1\rangle$

Implementierung von Qubits

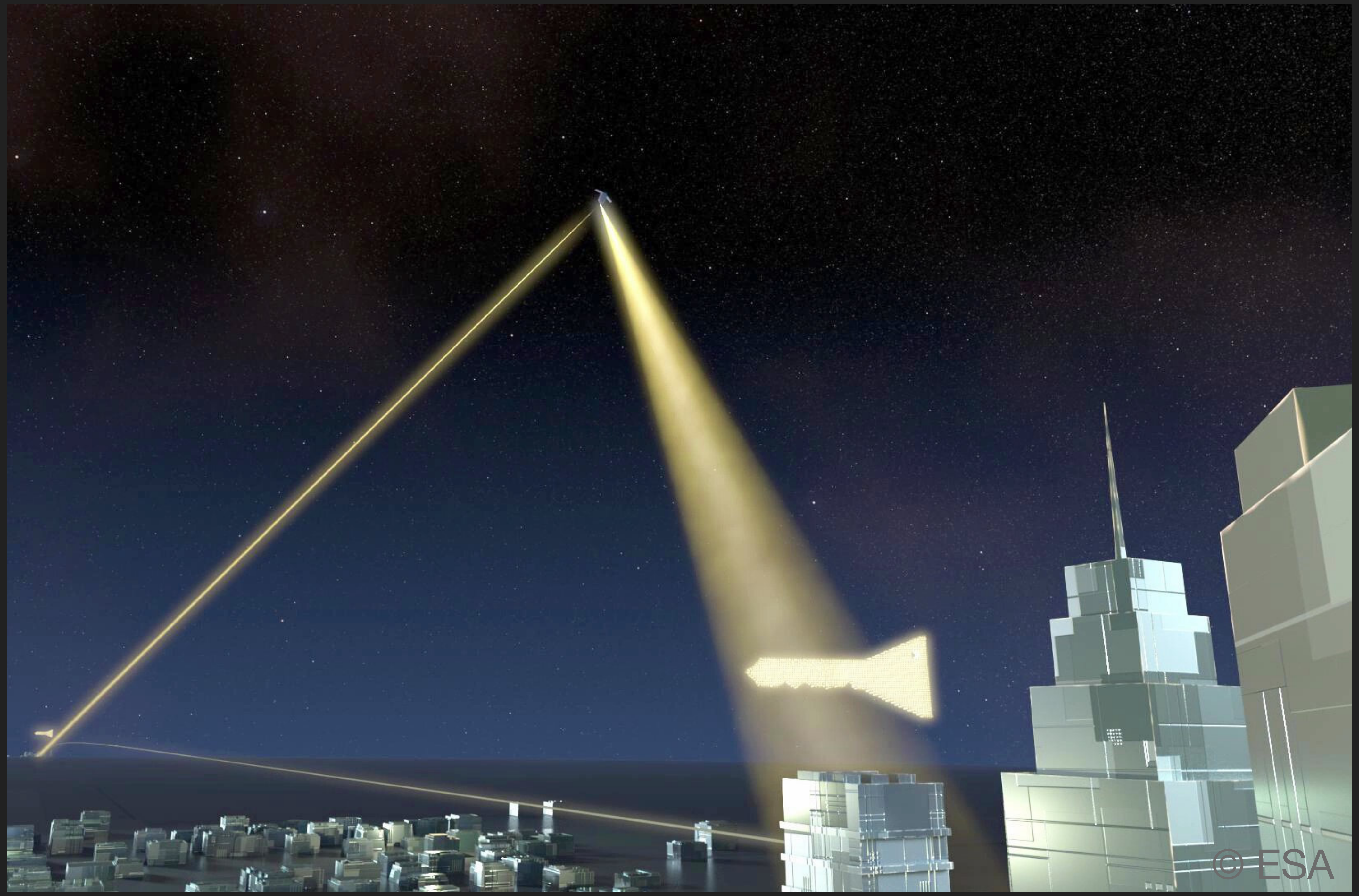


© IBM Research

Supraleitende Schaltkreise

oder

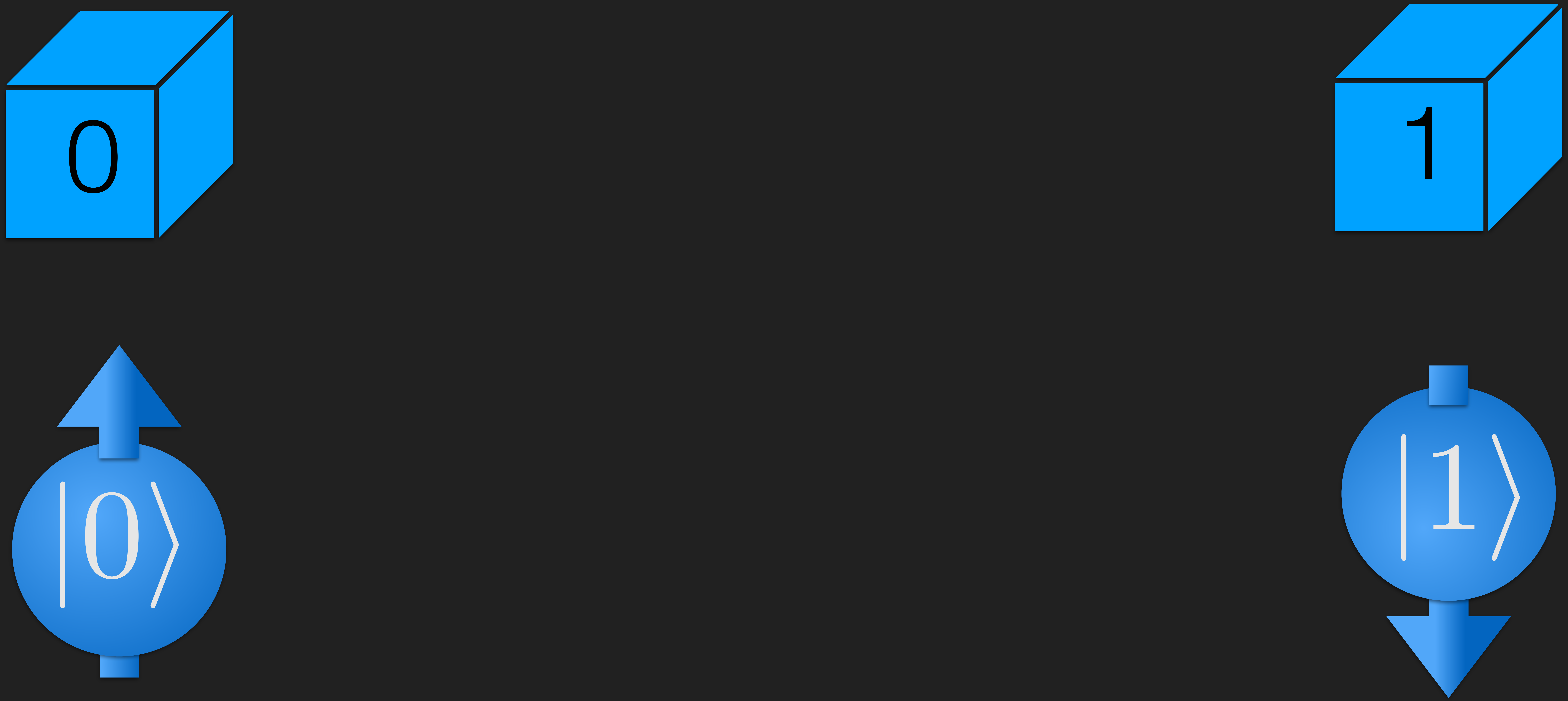
Ionen-Fallen



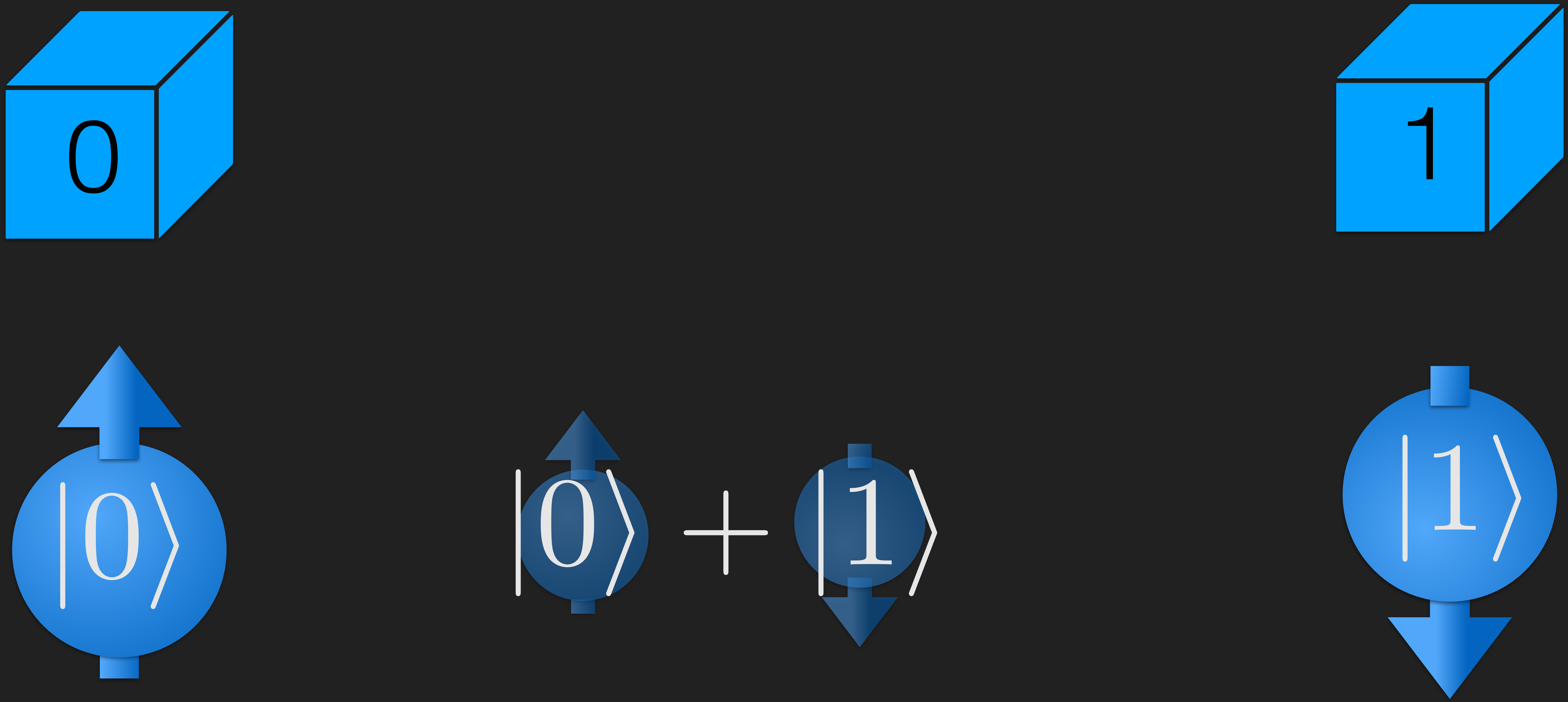
© ESA

Photonen

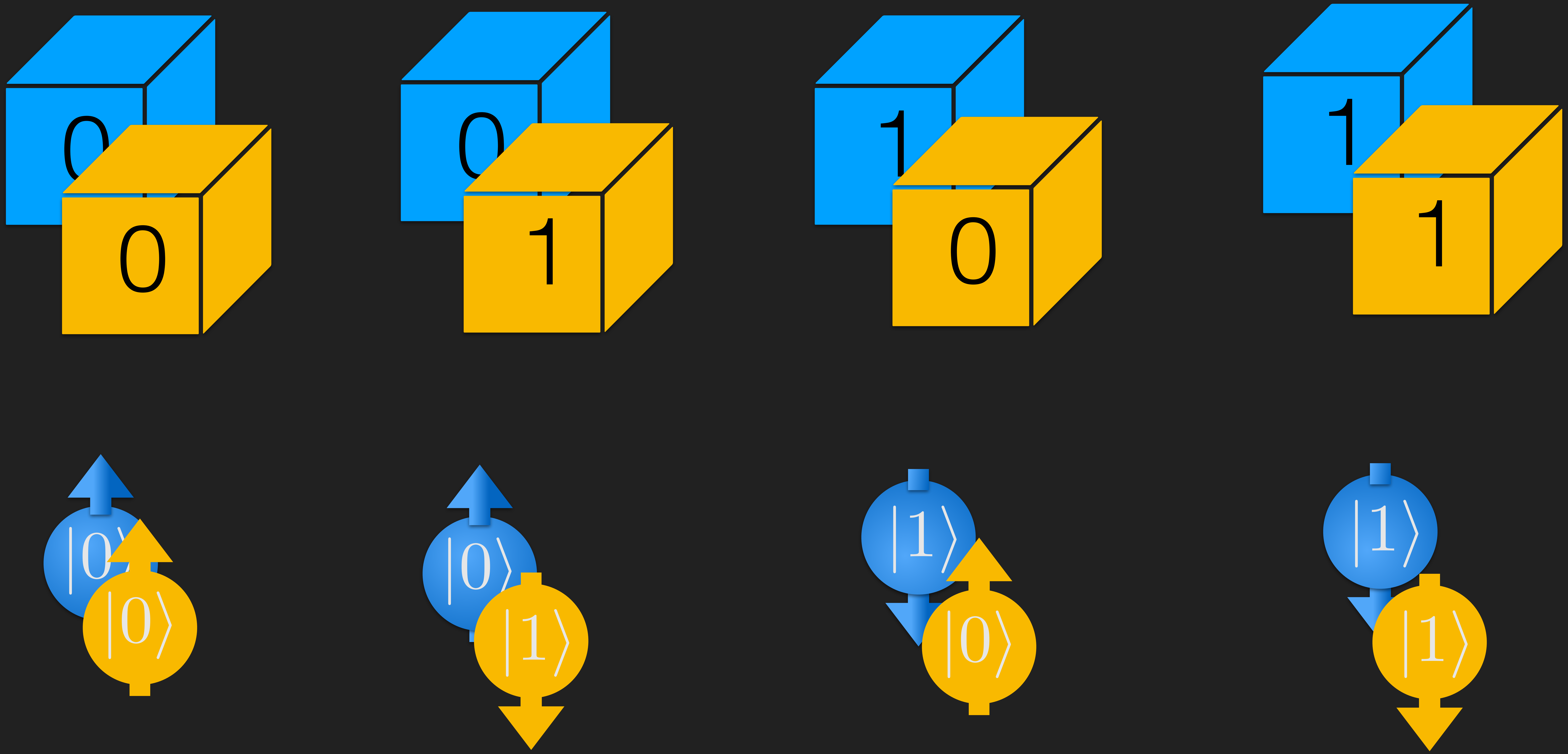
1 Bit versus 1 Qubit



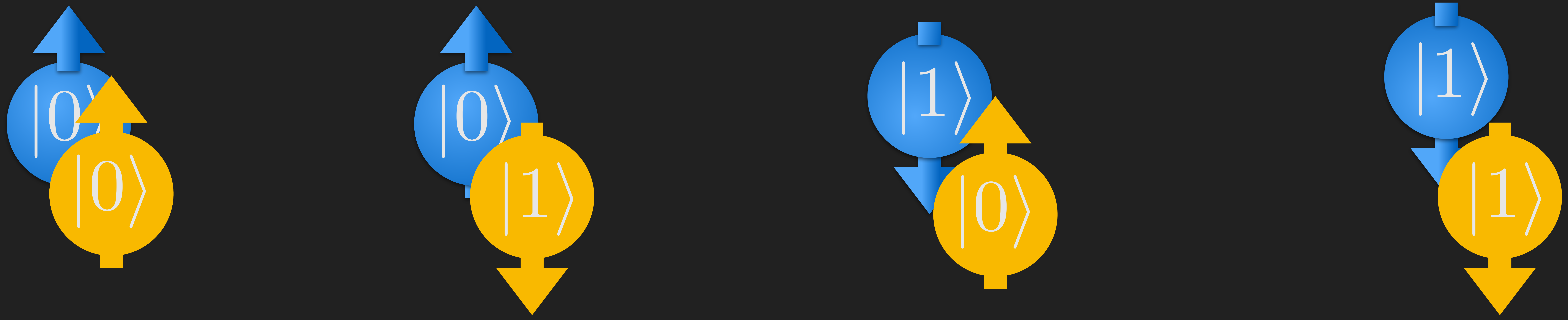
1 Bit versus 1 Qubit

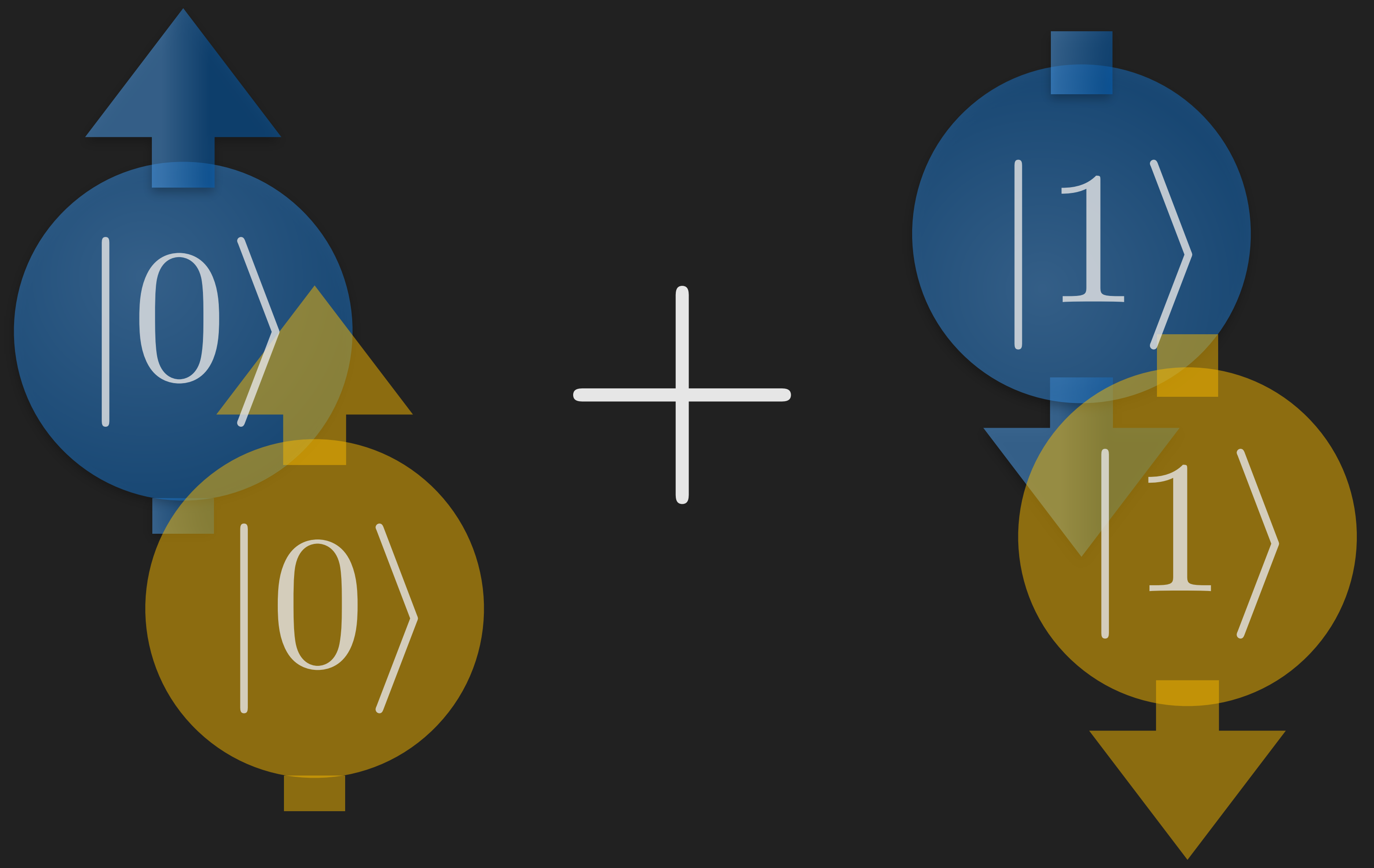


2 Bits versus 2 Qubits

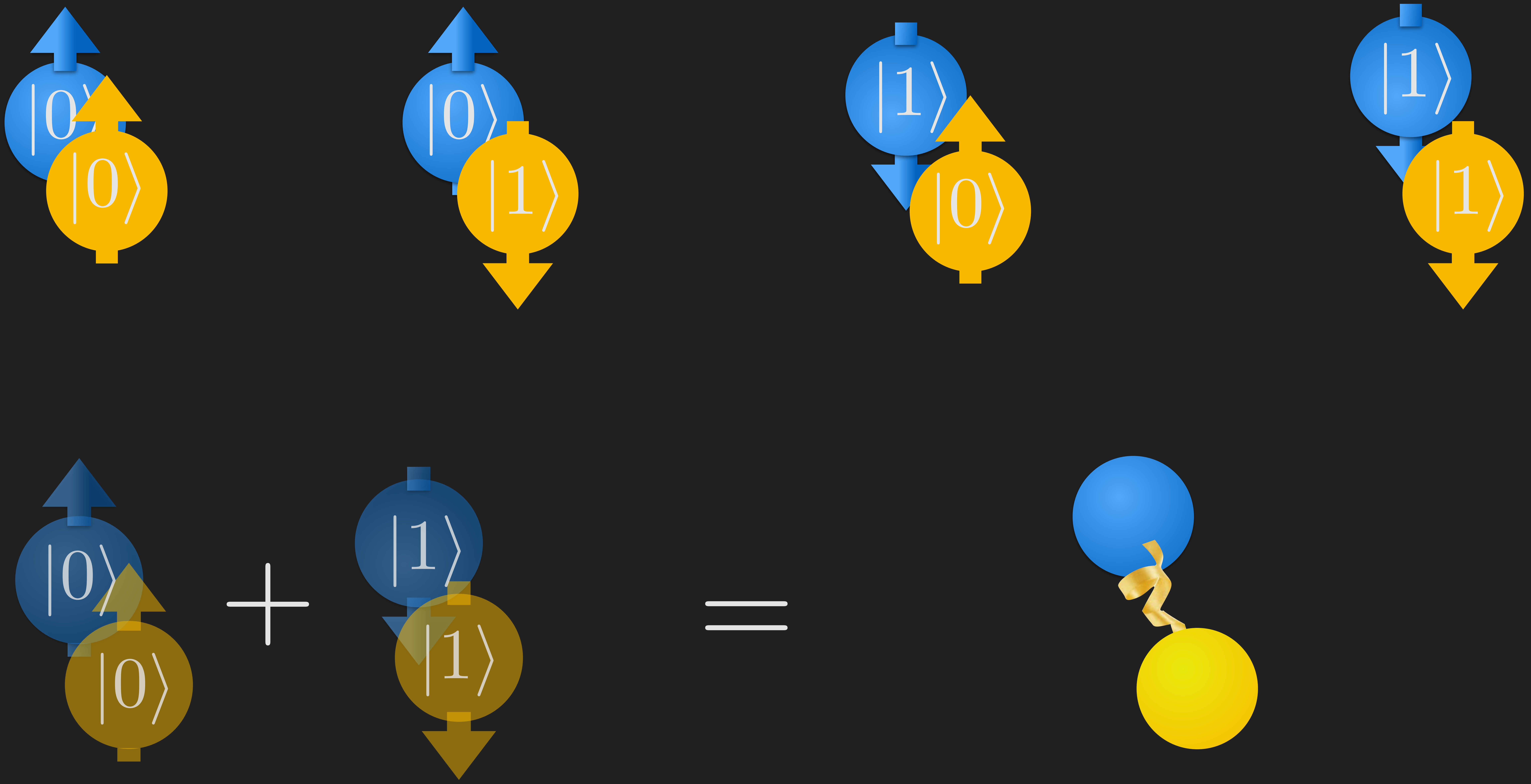


“Verschränkung”

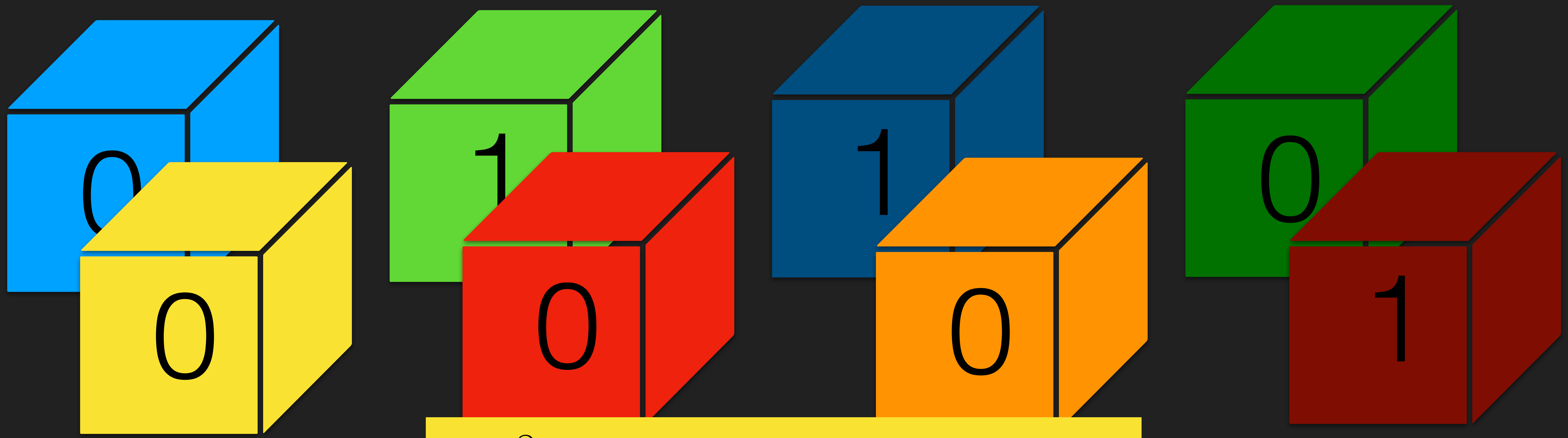




“Verschränkung”

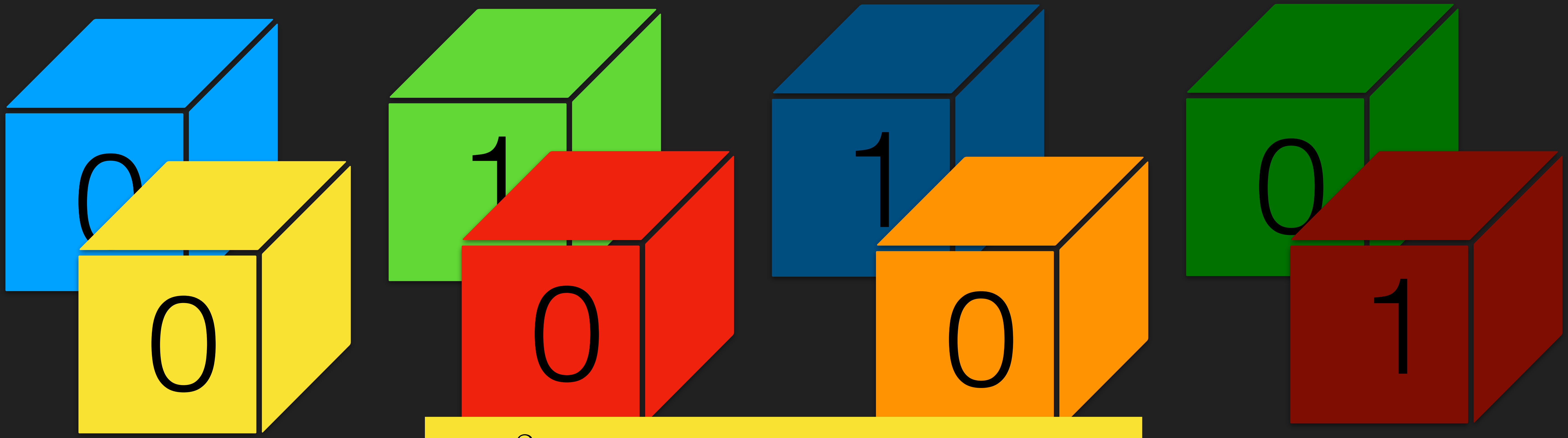


1 Byte versus 1 QByte

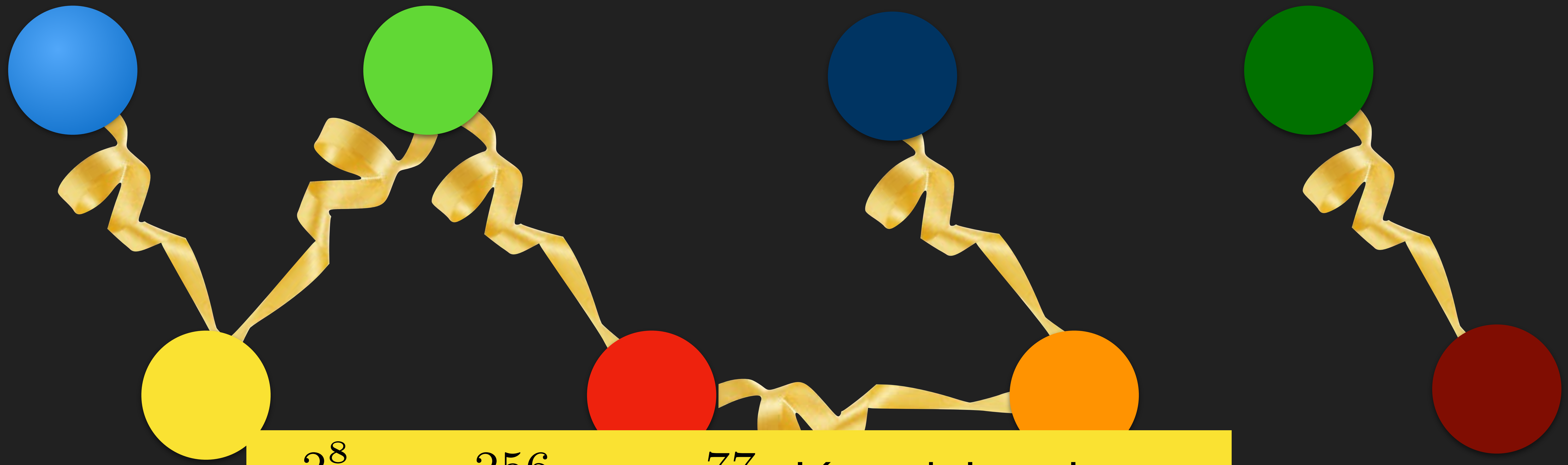


$2^8 = 256$ Kombinationen

1 Byte versus 1 QByte



$2^8 = 256$ Kombinationen



$2^{2^8} = 2^{256} \approx 10^{77}$ Kombinationen

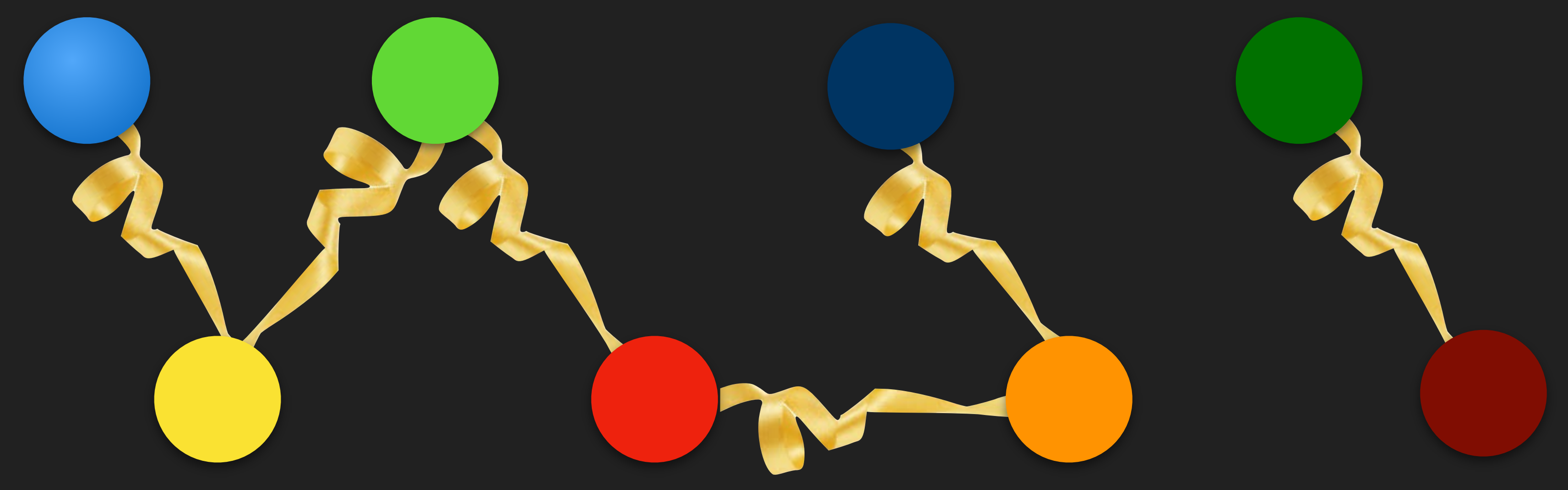
Quanten-Computing

Input
(Bits)

Verarbeitung
(Qubits)

Output
(Bits)

7663 →



→ 79×97

Qubits lassen sich nicht beobachten

Preparation

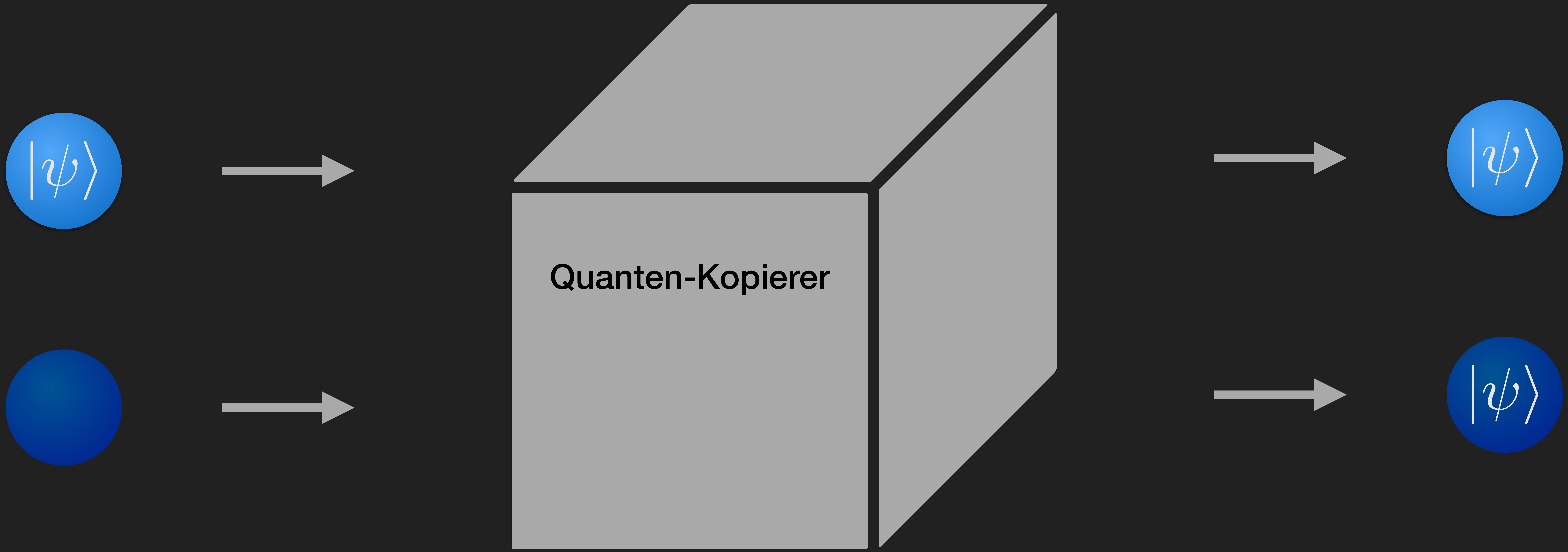
$|0\rangle + |1\rangle$

Messung

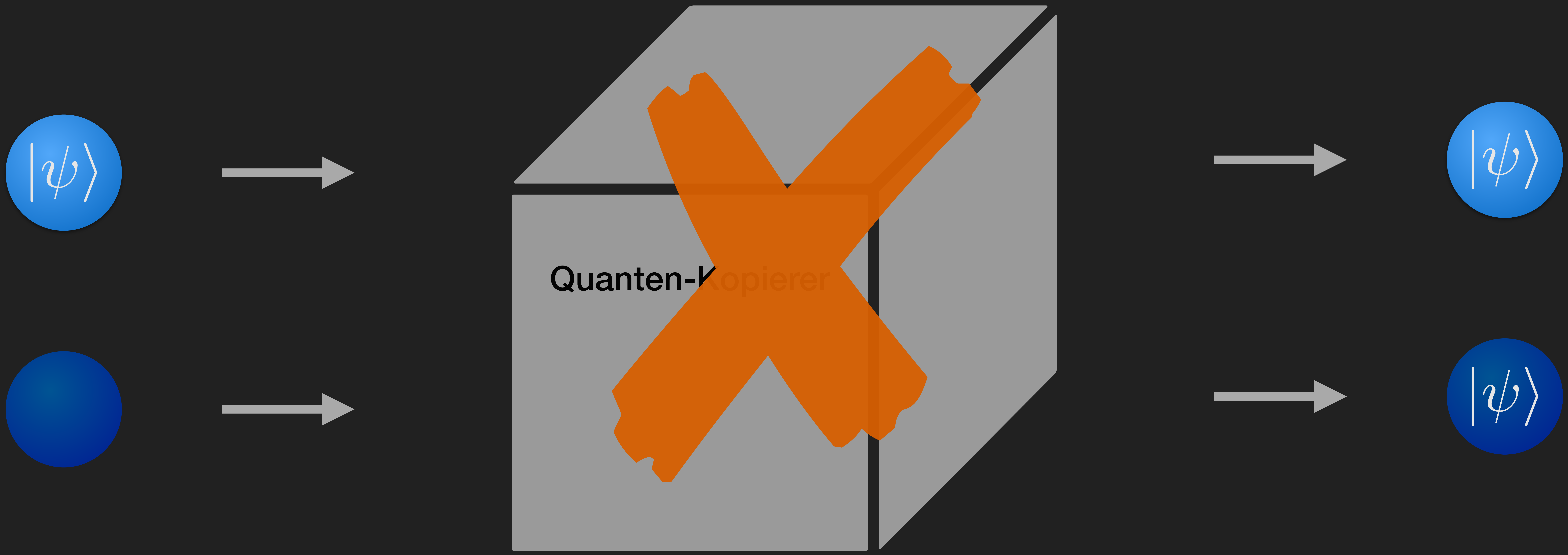
$|0\rangle$

$|1\rangle$

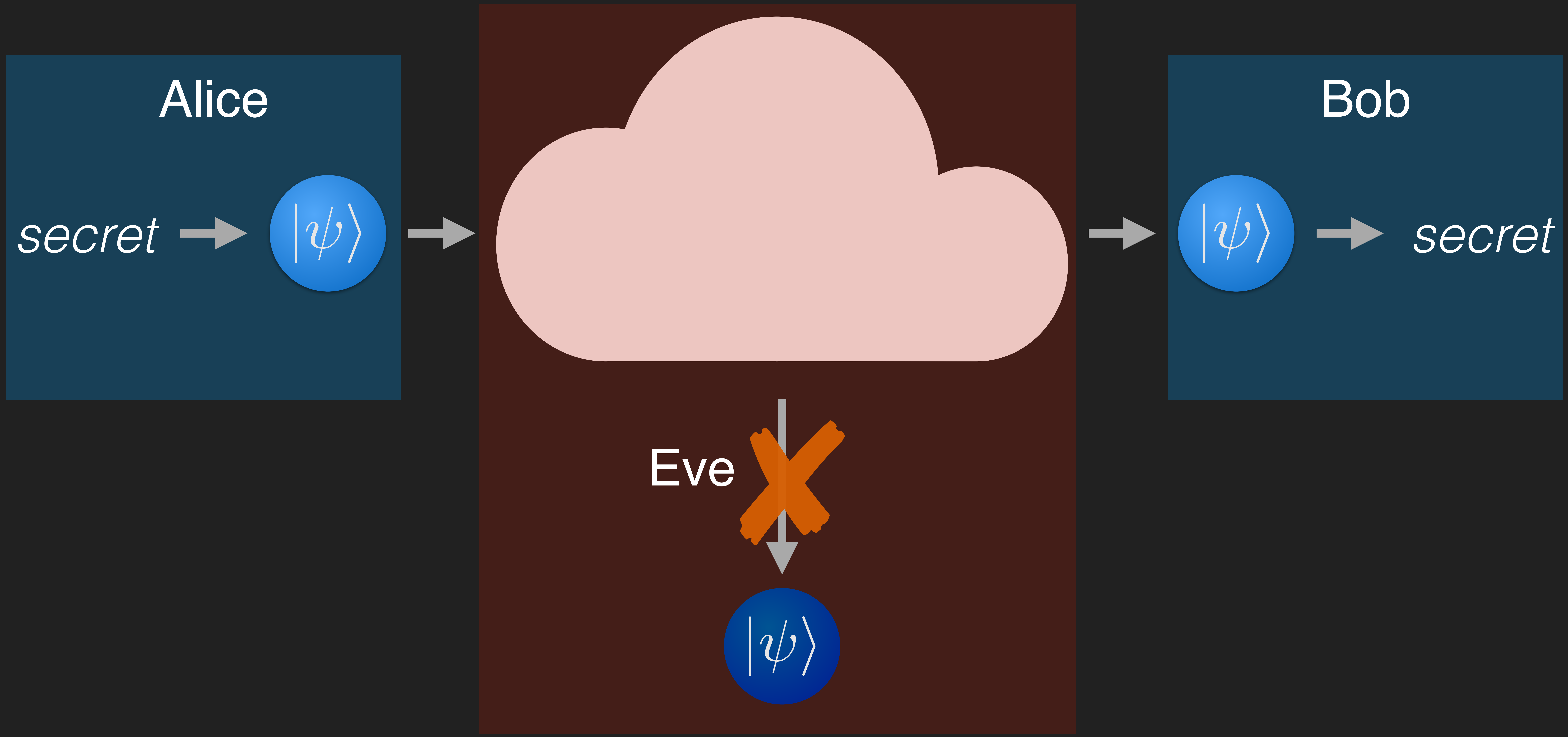
“No-Cloning”



“No-Cloning”

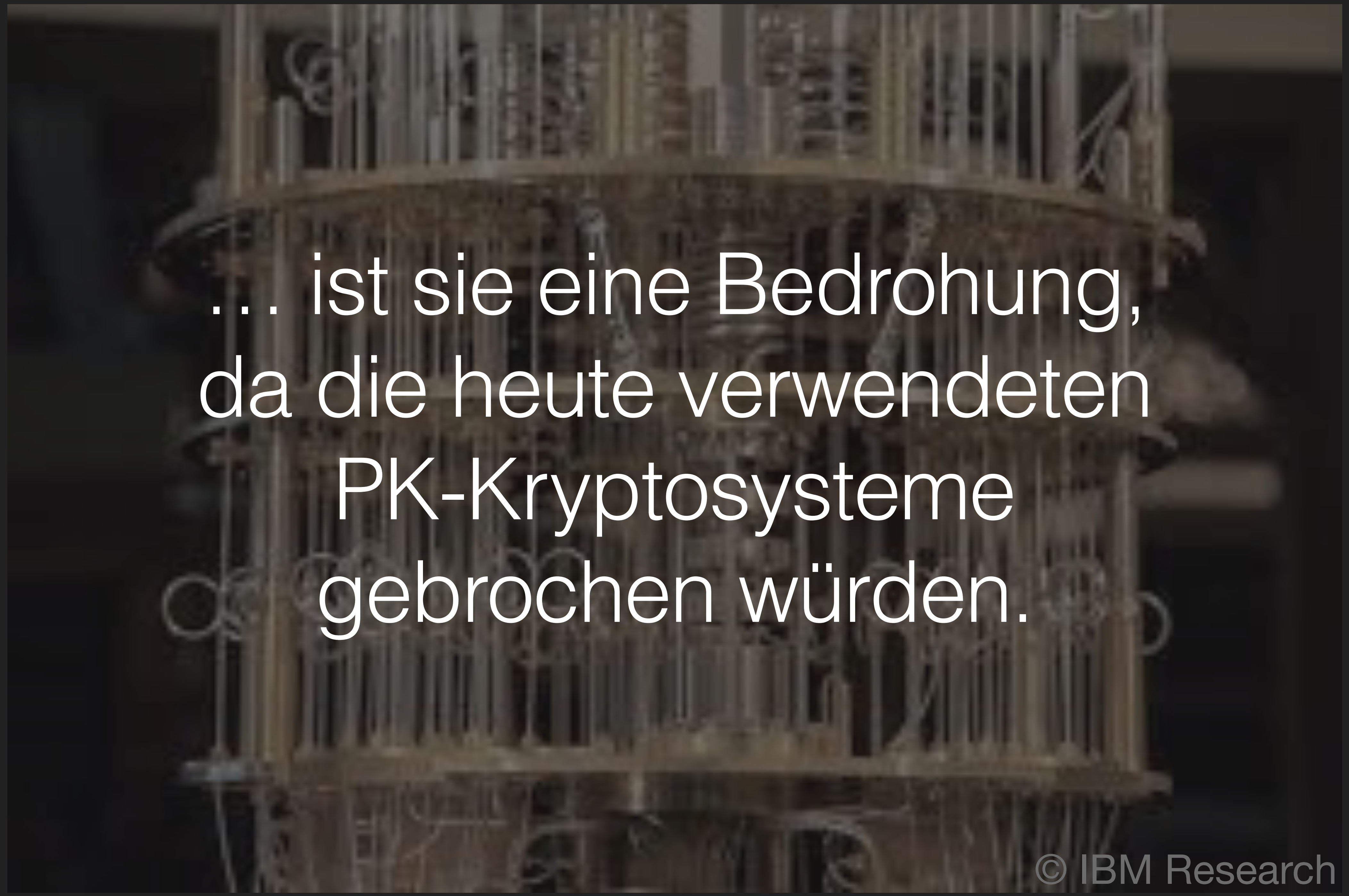


Quanten-Kryptographie



Die zwei Seiten der Quantentechnologie

In den Händen derjenigen, die unsere Geheimnisse lesen wollen …



… ist sie eine Bedrohung, da die heute verwendeten PK-Kryptosysteme gebrochen würden.

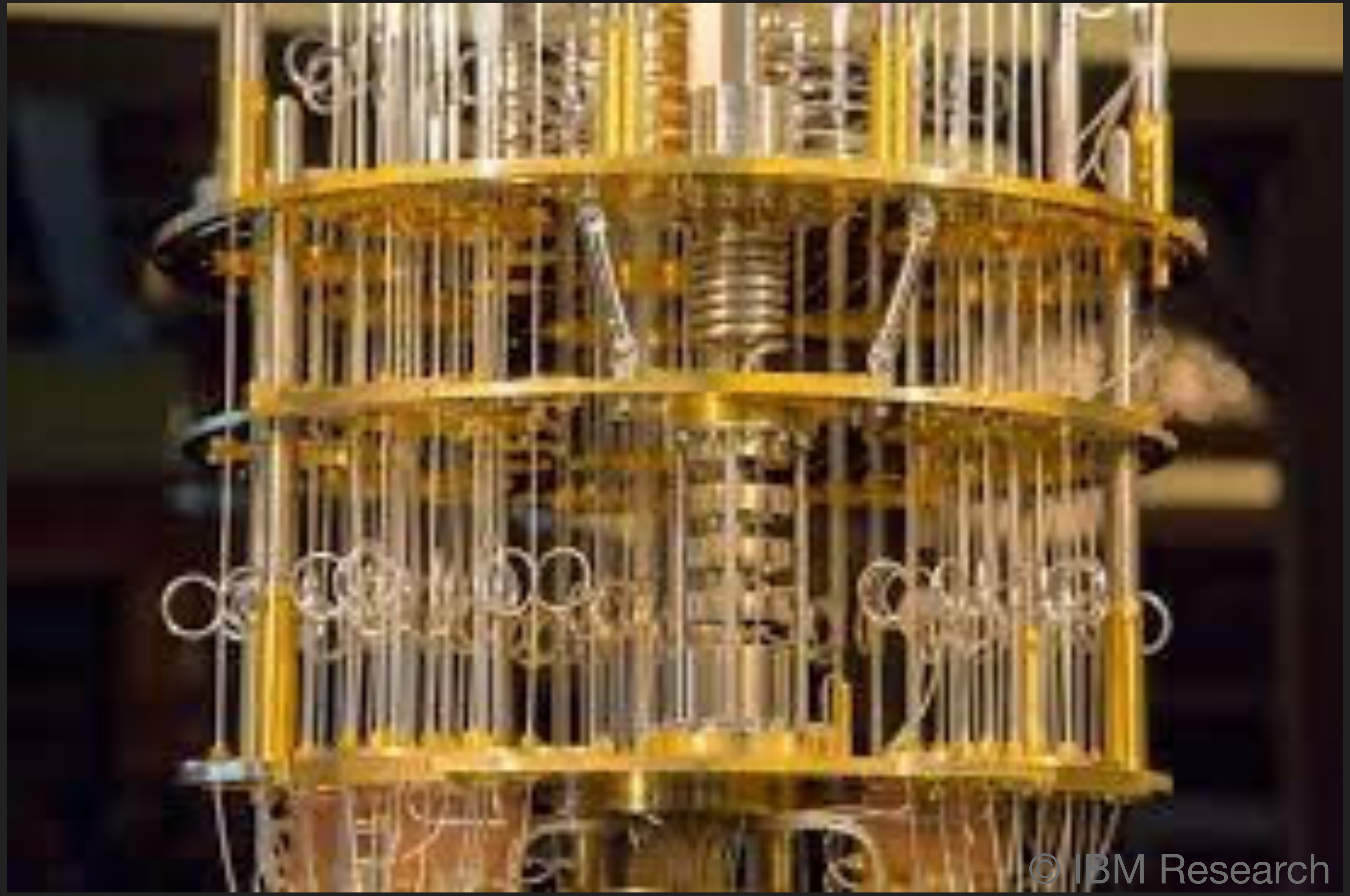
© IBM Research

In den Händen derjenigen, die unsere Geheimnisse schützen wollen …

… ermöglicht sie im Prinzip “everlasting Security”.

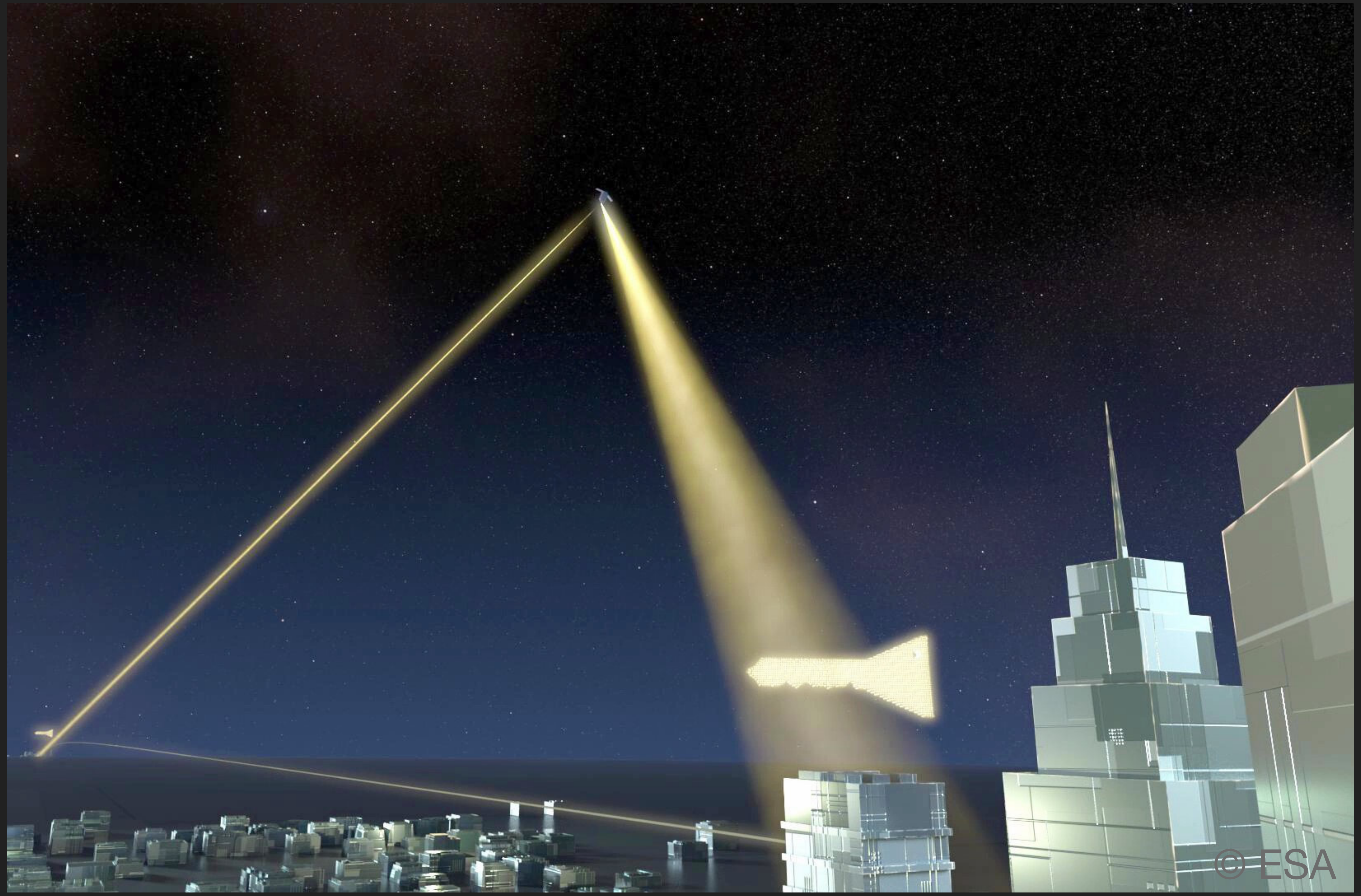
© ESA

Technologische Herausforderungen



Speicherung von Qubits

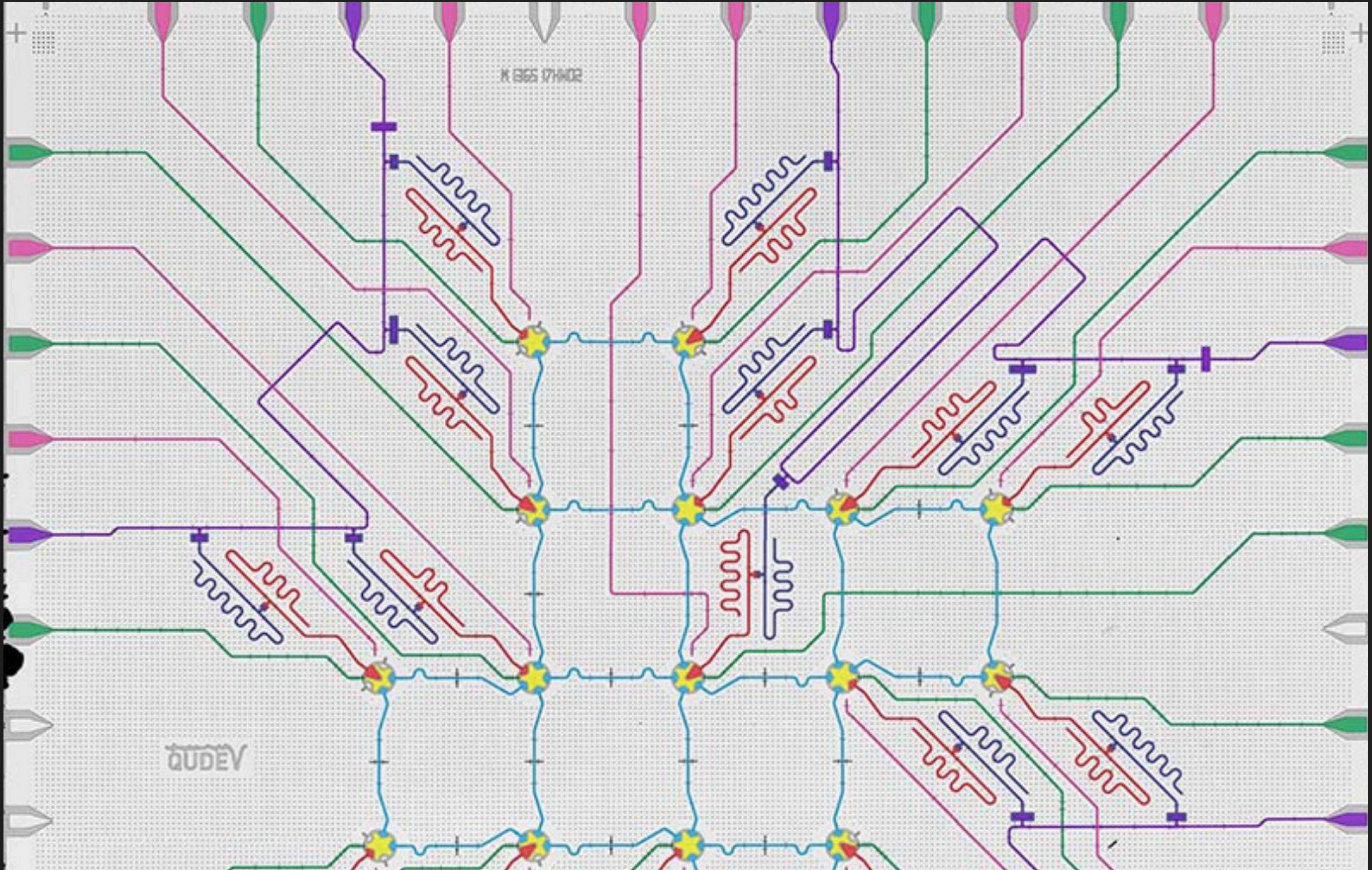
schwierig über mehr als
ein paar 100 Taktzyklen



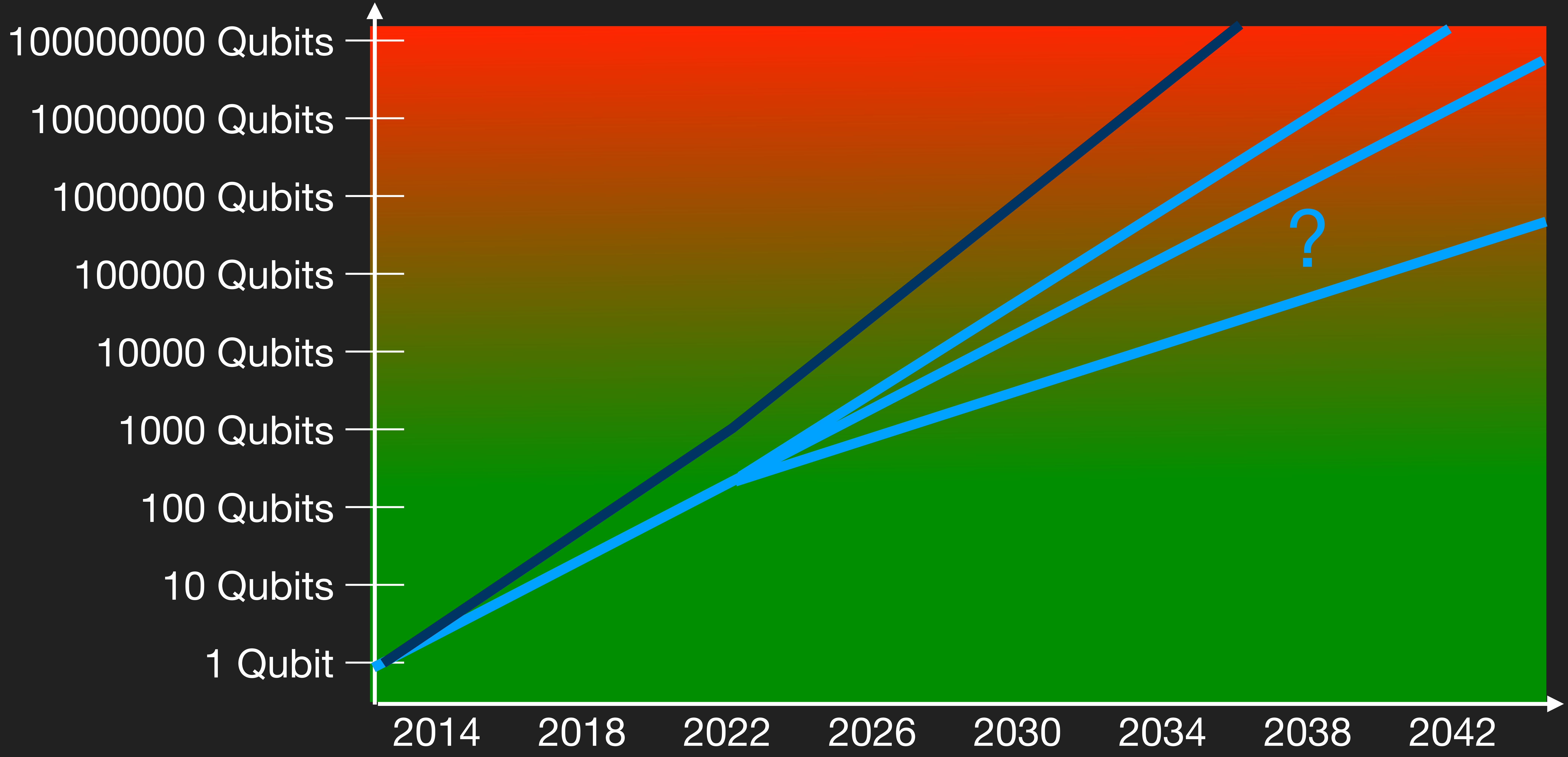
Übertragung von Qubits

einfach über Distanzen bis 100 km
schwierig über längere Distanzen

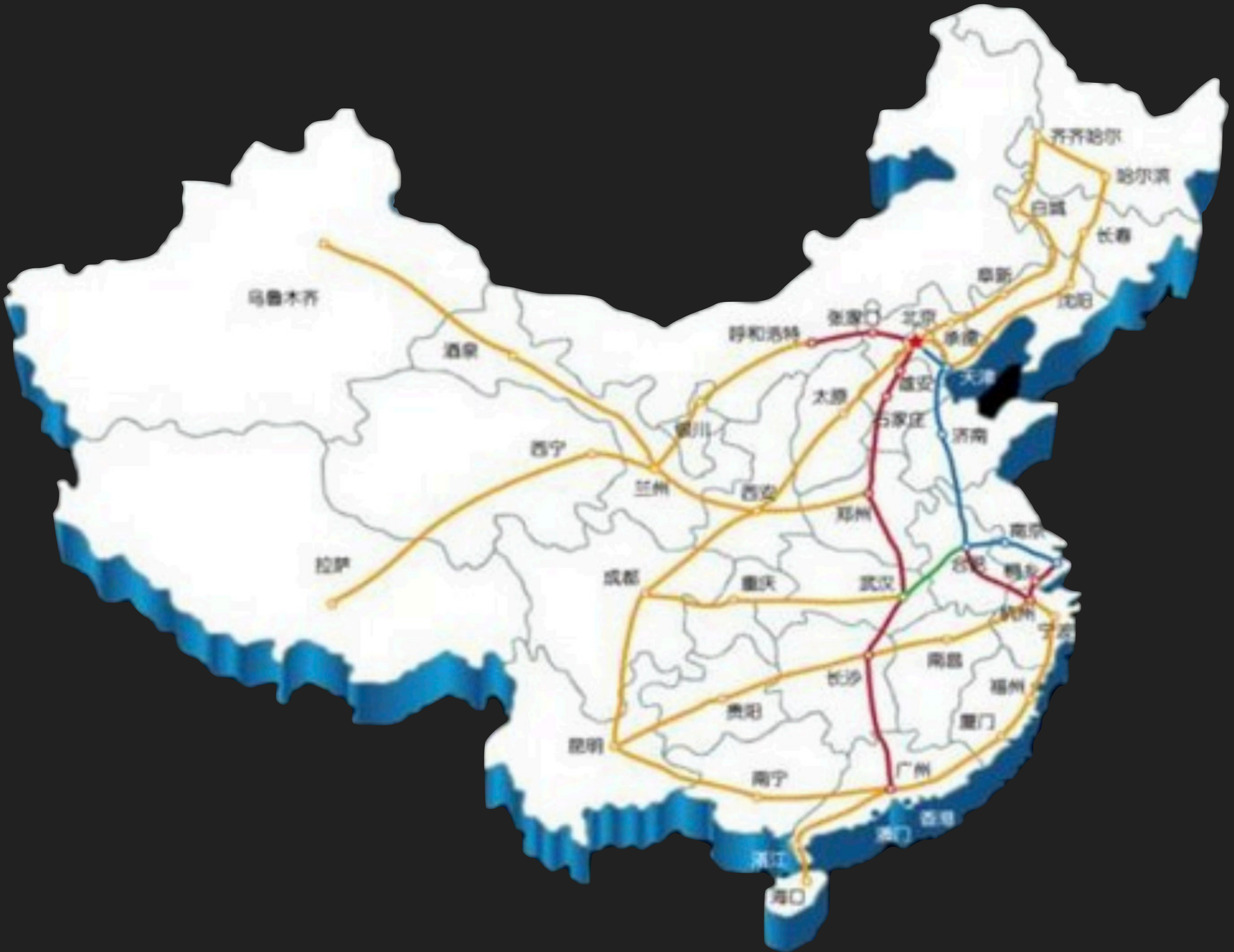
Fehler-Toleranz



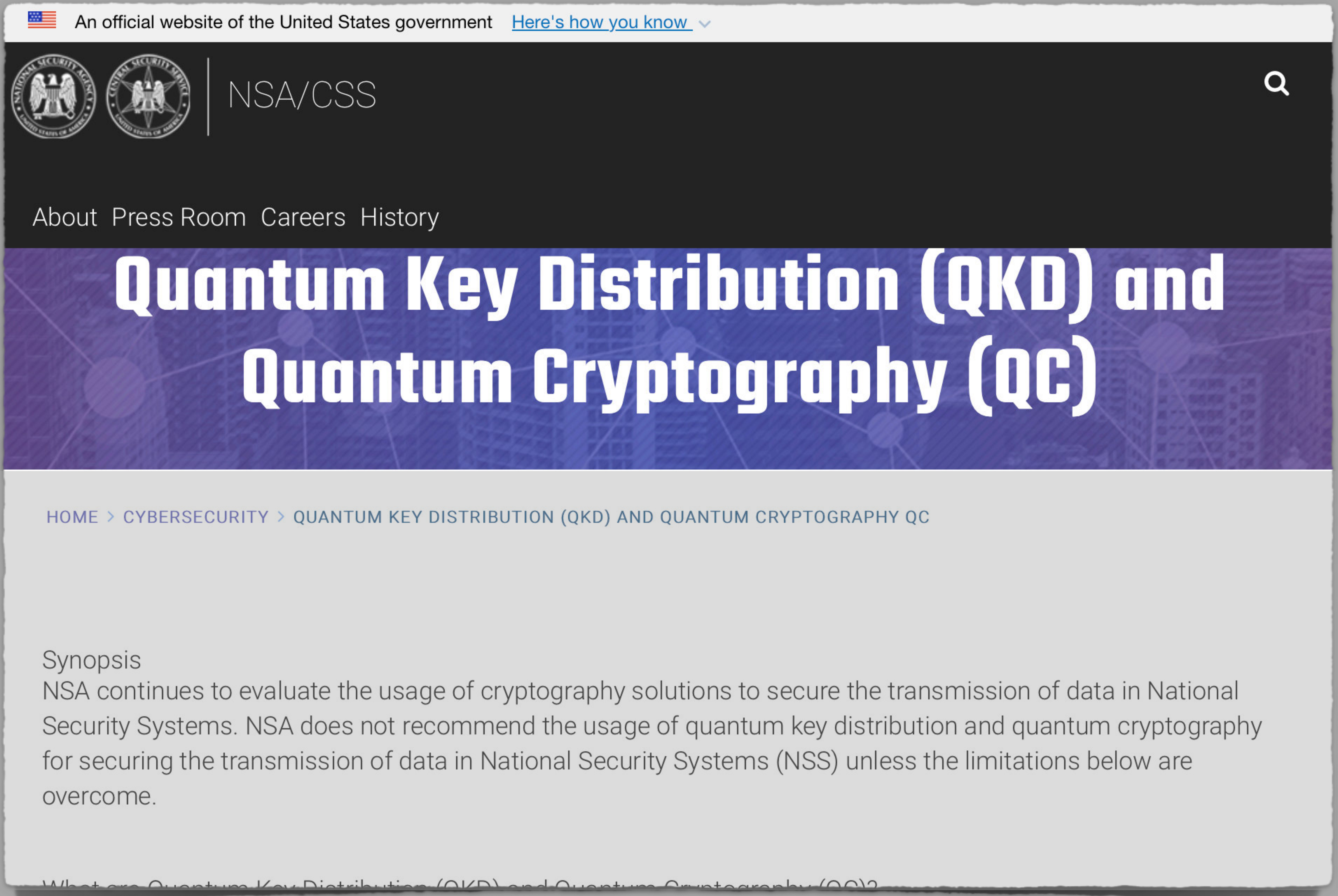
Stand der Technologie im Quanten-Computing



Stand der Technologie in der Quantenkommunikation



NSA White Paper



An official website of the United States government Here's how you know
NSA/CSS
About Press Room Careers History

Quantum Key Distribution (QKD) and Quantum Cryptography (QC)

HOME > CYBERSECURITY > QUANTUM KEY DISTRIBUTION (QKD) AND QUANTUM CRYPTOGRAPHY QC

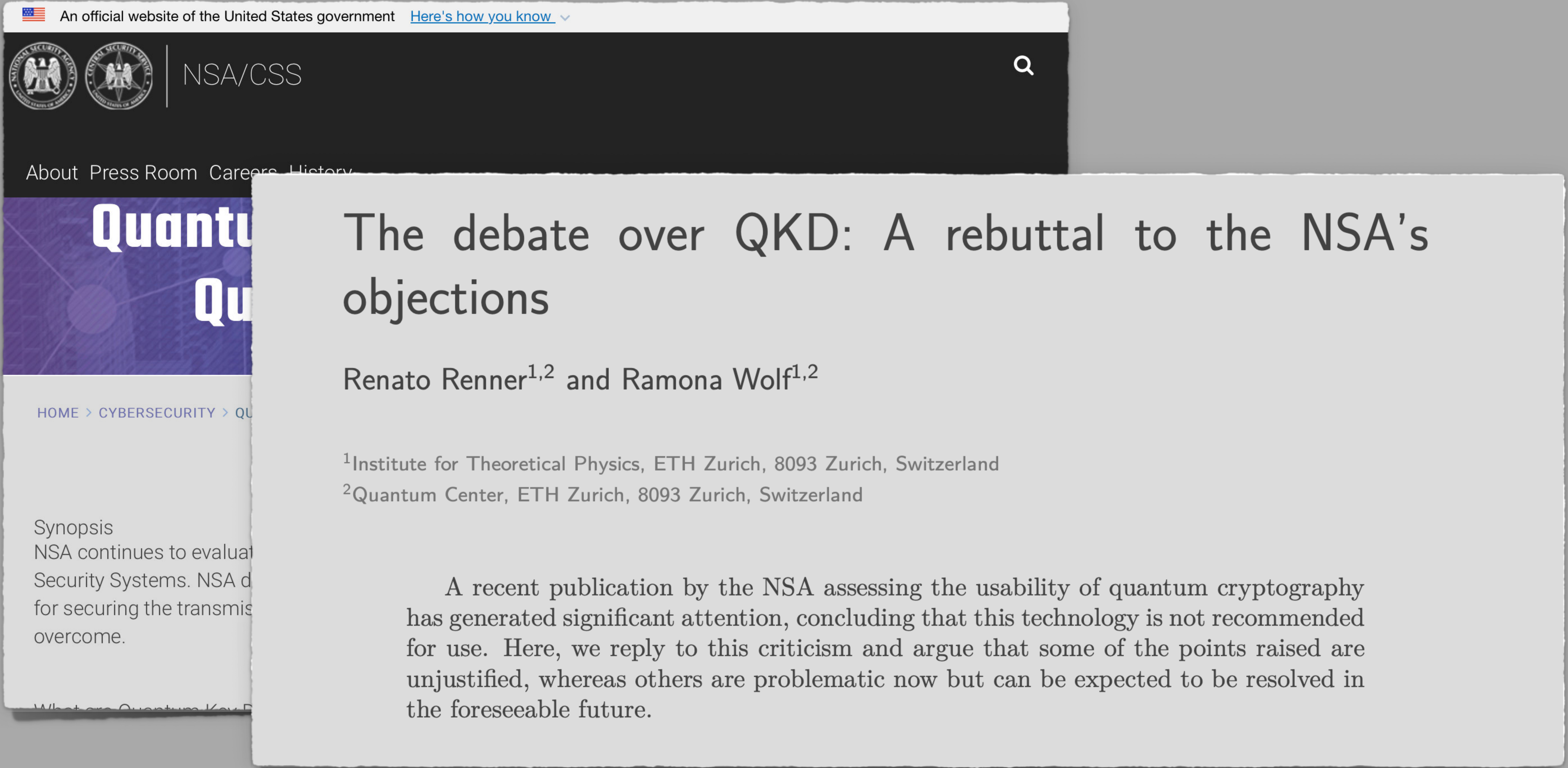
Synopsis

NSA continues to evaluate the usage of cryptography solutions to secure the transmission of data in National Security Systems. NSA does not recommend the usage of quantum key distribution and quantum cryptography for securing the transmission of data in National Security Systems (NSS) unless the limitations below are overcome.

What are Quantum Key Distribution (QKD) and Quantum Cryptography (QC)?

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

NSA White Paper



An official website of the United States government Here's how you know

NSA/CSS

About Press Room Careers History

Quantu

Qu

HOME > CYBERSECURITY > QU

Synopsis
NSA continues to evaluat
Security Systems. NSA d
for securing the transmis
overcome.

What are Quantum Key D

The debate over QKD: A rebuttal to the NSA's objections

Renato Renner[1,2] and Ramona Wolf[1,2]

[1] Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland
[2] Quantum Center, ETH Zurich, 8093 Zurich, Switzerland

A recent publication by the NSA assessing the usability of quantum cryptography has generated significant attention, concluding that this technology is not recommended for use. Here, we reply to this criticism and argue that some of the points raised are unjustified, whereas others are problematic now but can be expected to be resolved in the foreseeable future.

https://doi.org/10.48550/arXiv.2307.15116

Forschungsgruppe

Quanten-Technologie …

☒ … bedroht die Sicherheit unserer Daten

☒ … erhöht die Sicherheit unserer Daten

Quanten-Technologie …

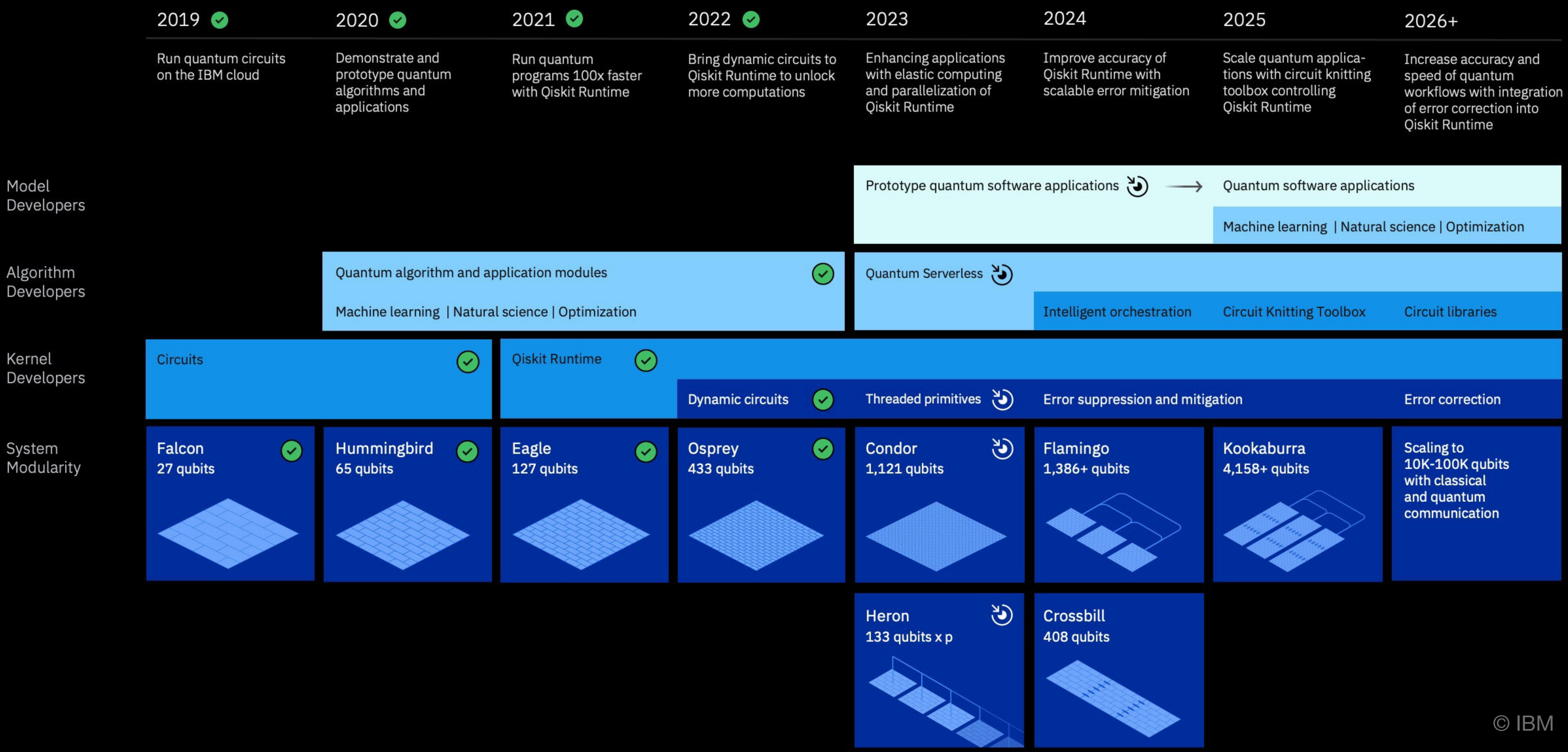
☒ … bedroht die Sicherheit unserer Daten

☒ … erhöht die Sicherheit unserer Daten

Fragen?

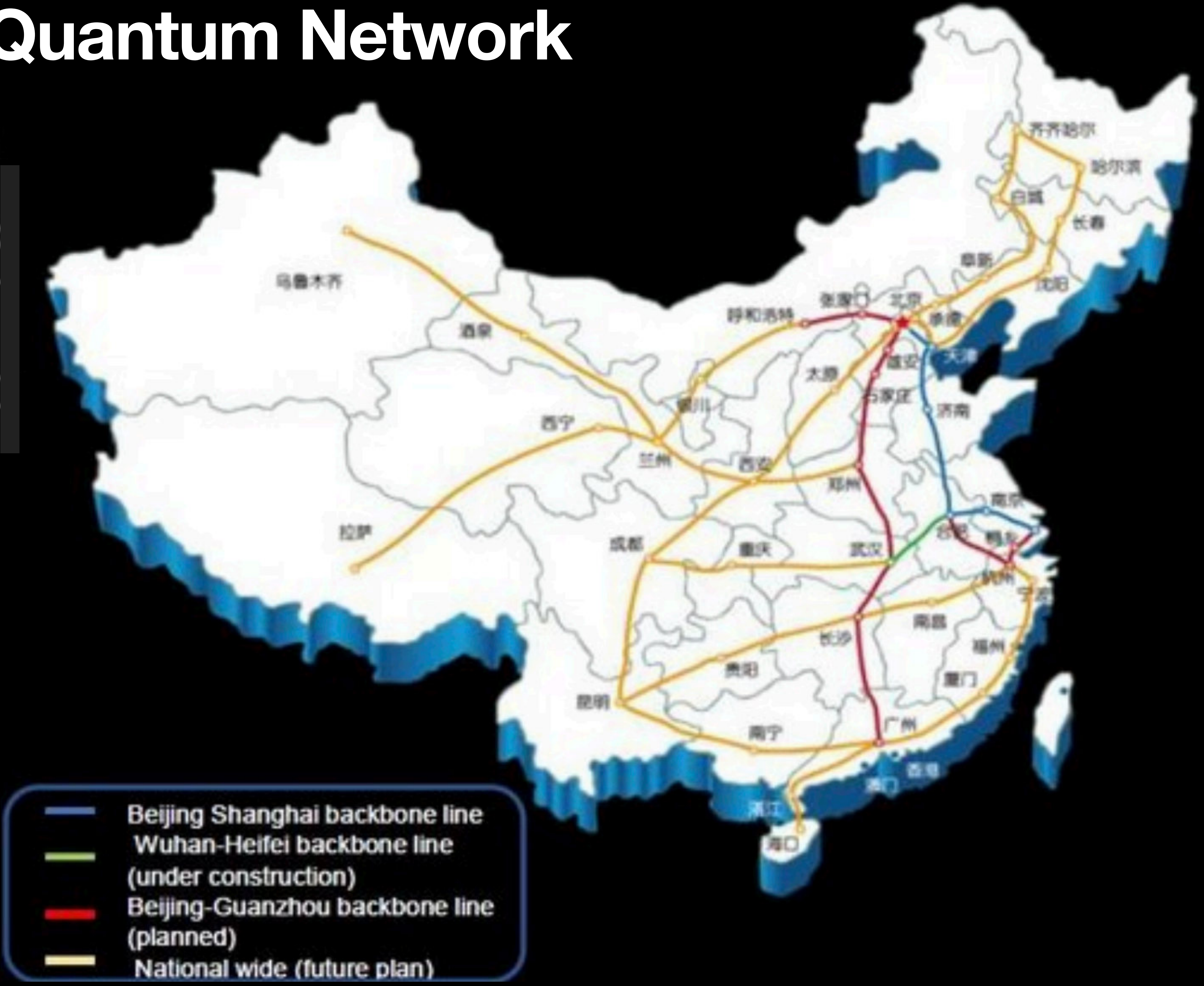
Extra-Slides

Example: IBM’s roadmap



	2019 ✓	2020 ✓	2021 ✓	2022 ✓	2023	2024	2025	2026+
	Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime	Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers					Prototype quantum software applications ↻ →		Quantum software applications Machine learning | Natural science | Optimization	
Algorithm Developers		Quantum algorithm and application modules ✓ Machine learning | Natural science | Optimization			Quantum Serverless ↻	Intelligent orchestration	Circuit Knitting Toolbox	Circuit libraries
Kernel Developers	Circuits ✓		Qiskit Runtime ✓	Dynamic circuits ✓	Threaded primitives ↻	Error suppression and mitigation		Error correction
System Modularity	Falcon ✓ 27 qubits	Hummingbird ✓ 65 qubits	Eagle ✓ 127 qubits	Osprey ✓ 433 qubits	Condor ↻ 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
					Heron ↻ 133 qubits x p	Crossbill 408 qubits		

China’s Quantum Network


乌鲁木齐
酒泉
西宁
拉萨
兰州
银川
呼和浩特
张家口
北京
承德
天津
雄安
太原
石家庄
济南
西安
郑州
成都
重庆
武汉
合肥
南京
杭州
宁波
南昌
长沙
福州
厦门
贵阳
昆明
南宁
广州
澳门
香港
湛江
海口
齐齐哈尔
哈尔滨
白城
长春
阜新
沈阳
Beijing Shanghai backbone line
Wuhan-Heifei backbone line (under construction)
Beijing-Guanzhou backbone line (planned)
National wide (future plan)