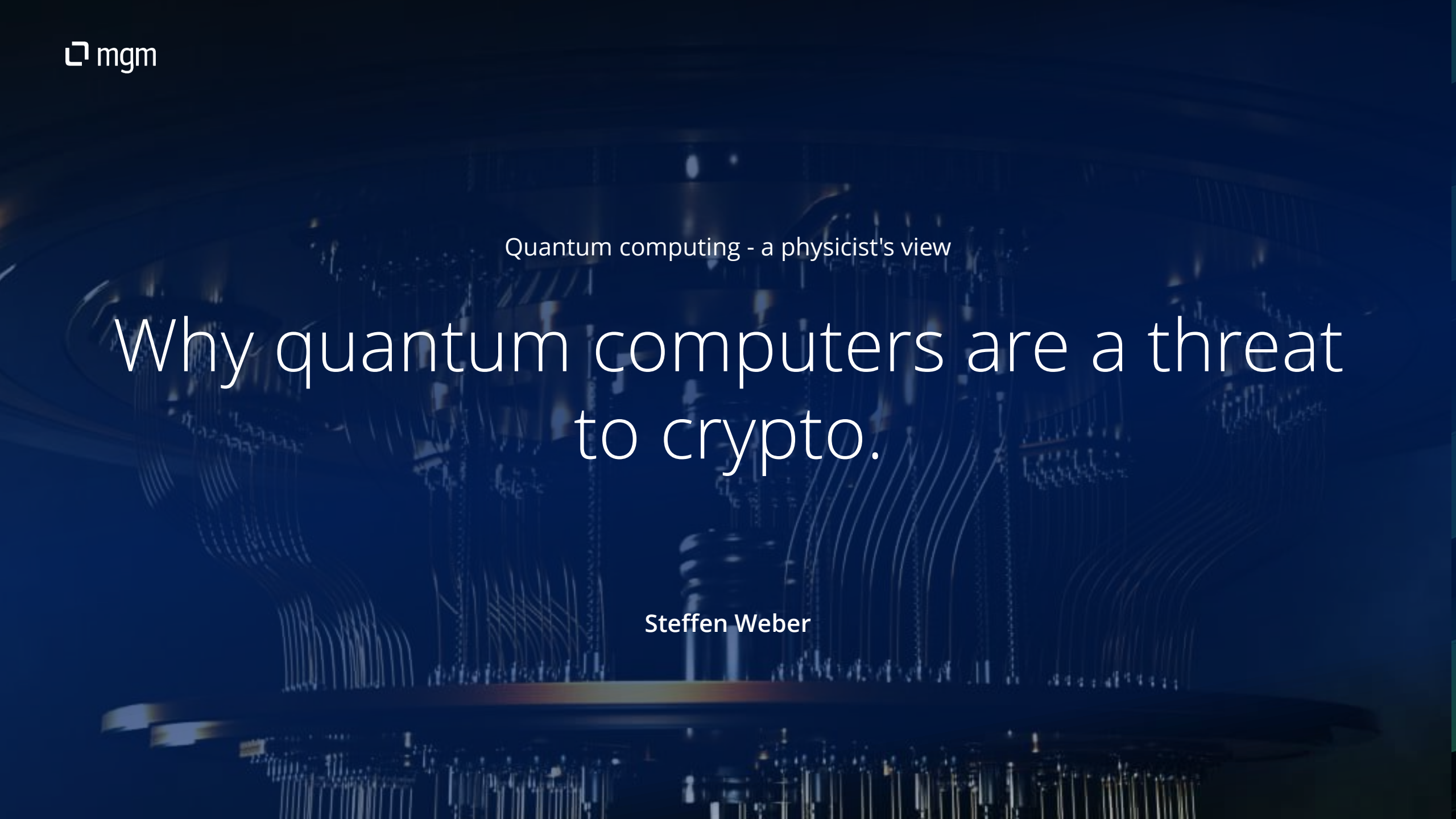
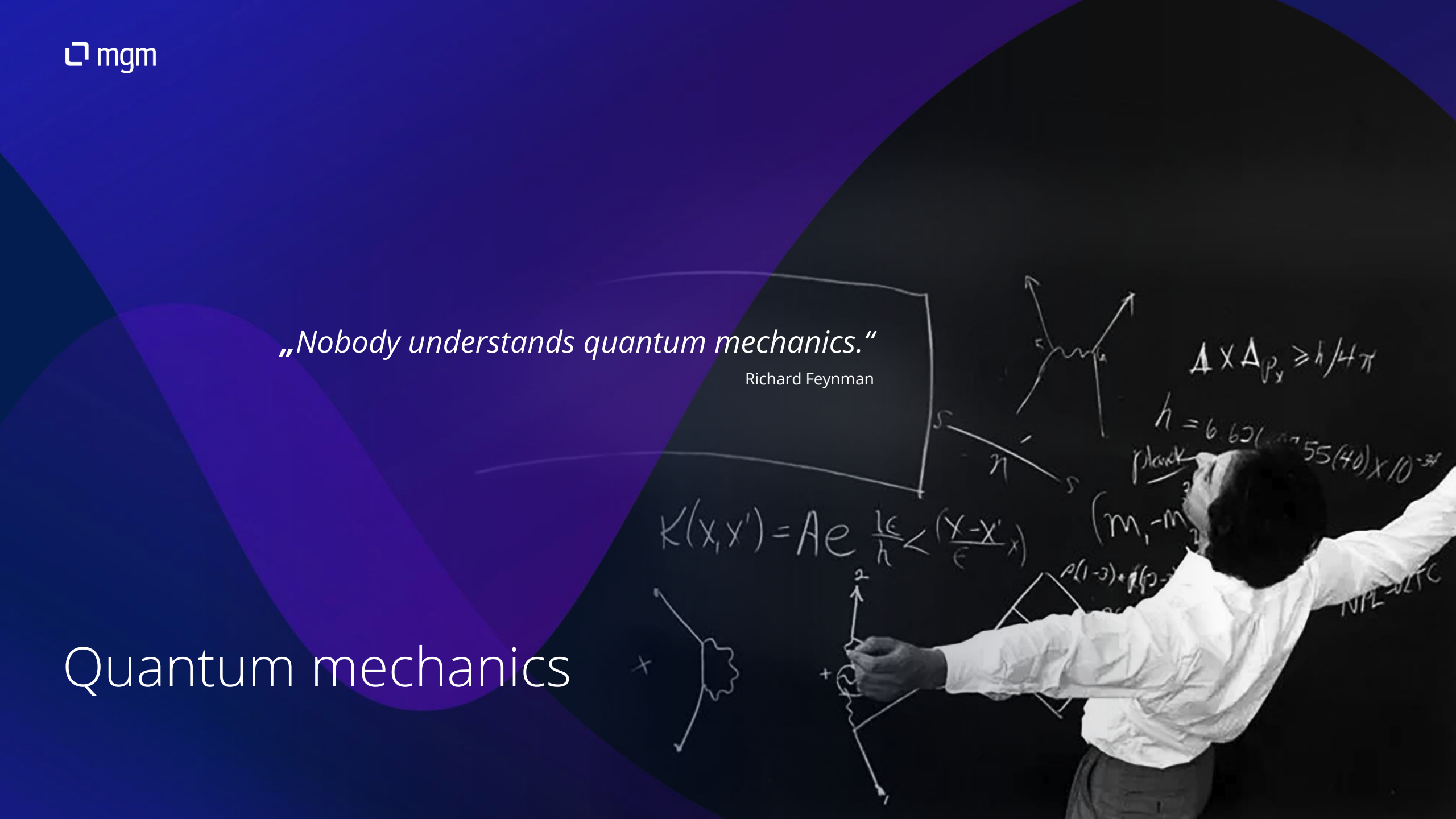

mgm
Quantum computing - a physicist's view
Why quantum computers are a threat to crypto.
Steffen Weber

mgm

„Nobody understands quantum mechanics.“

Richard Feynman



Quantum mechanics

World of particles

How the world works in microcode.

Strange properties

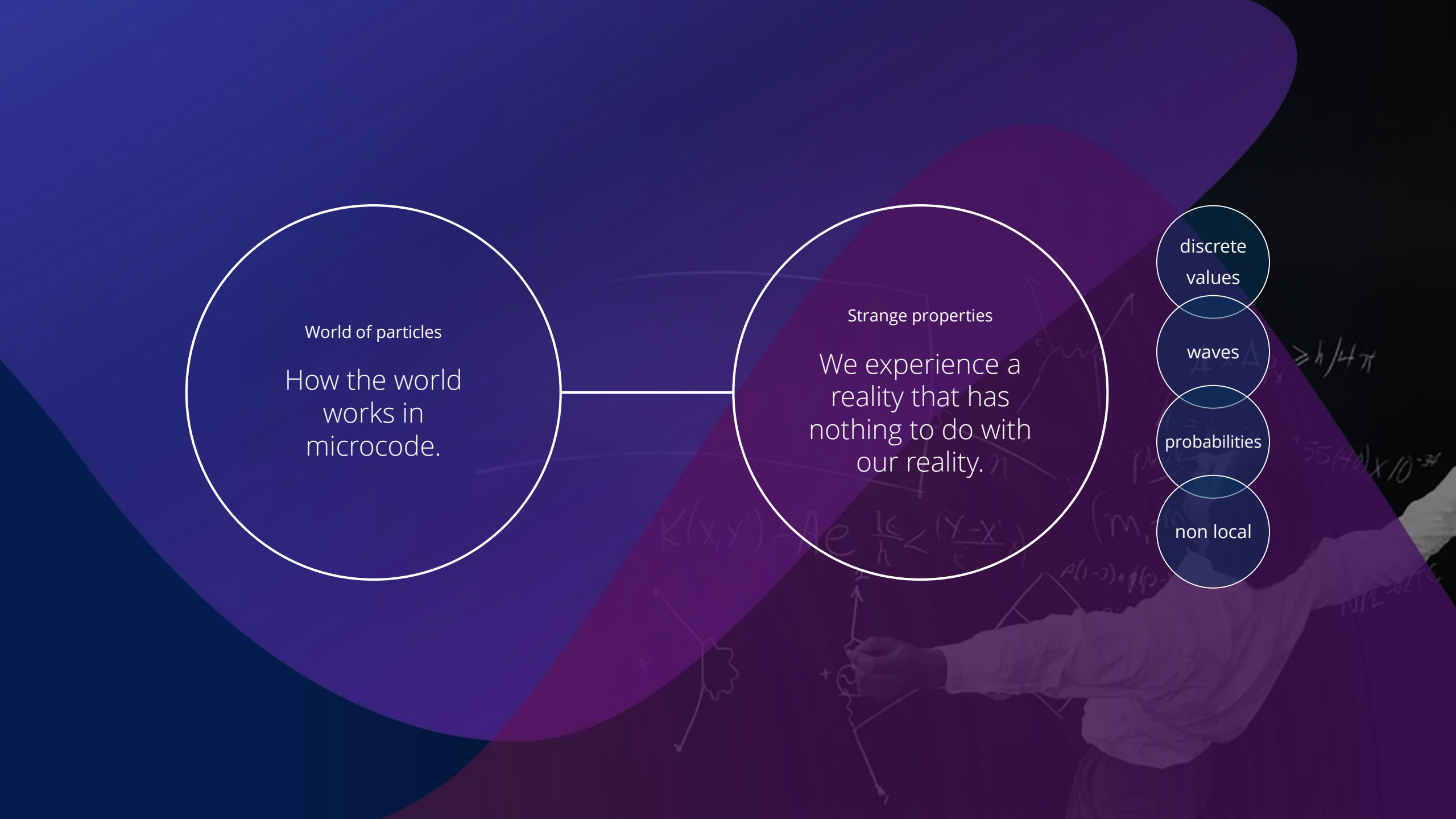
We experience a reality that has nothing to do with our reality.

discrete values

waves

probabilities

non local



Quantum mechanics

STRANGE PROPERTIES

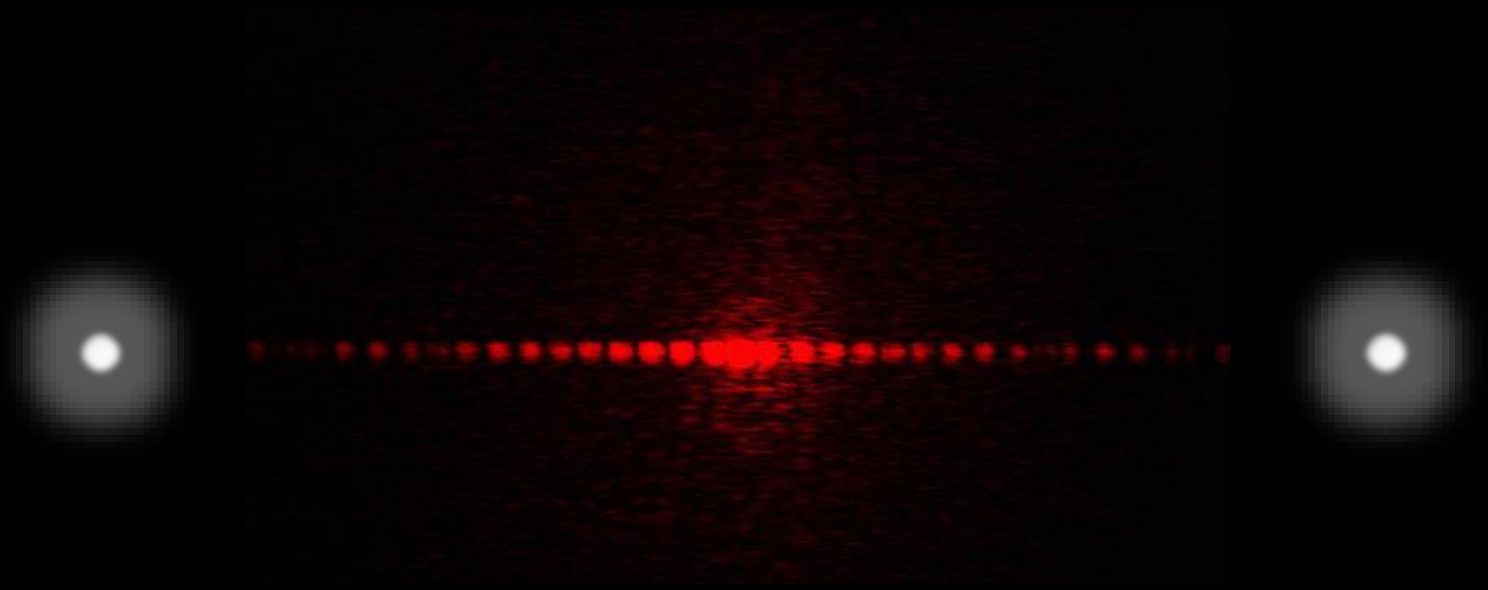
discrete values

waves

probabilities

non local

Quantum mechanics



The interference pattern shows part of the hidden information.

Interference is a result of the superposition of two or more waves according to the superposition principle.

STRANGE PROPERTIES

discrete values

waves

probabilities

non local

Quantum mechanics

ball
experienced reality

Ball
Quantum mechanics

Highest probability

Very low probability

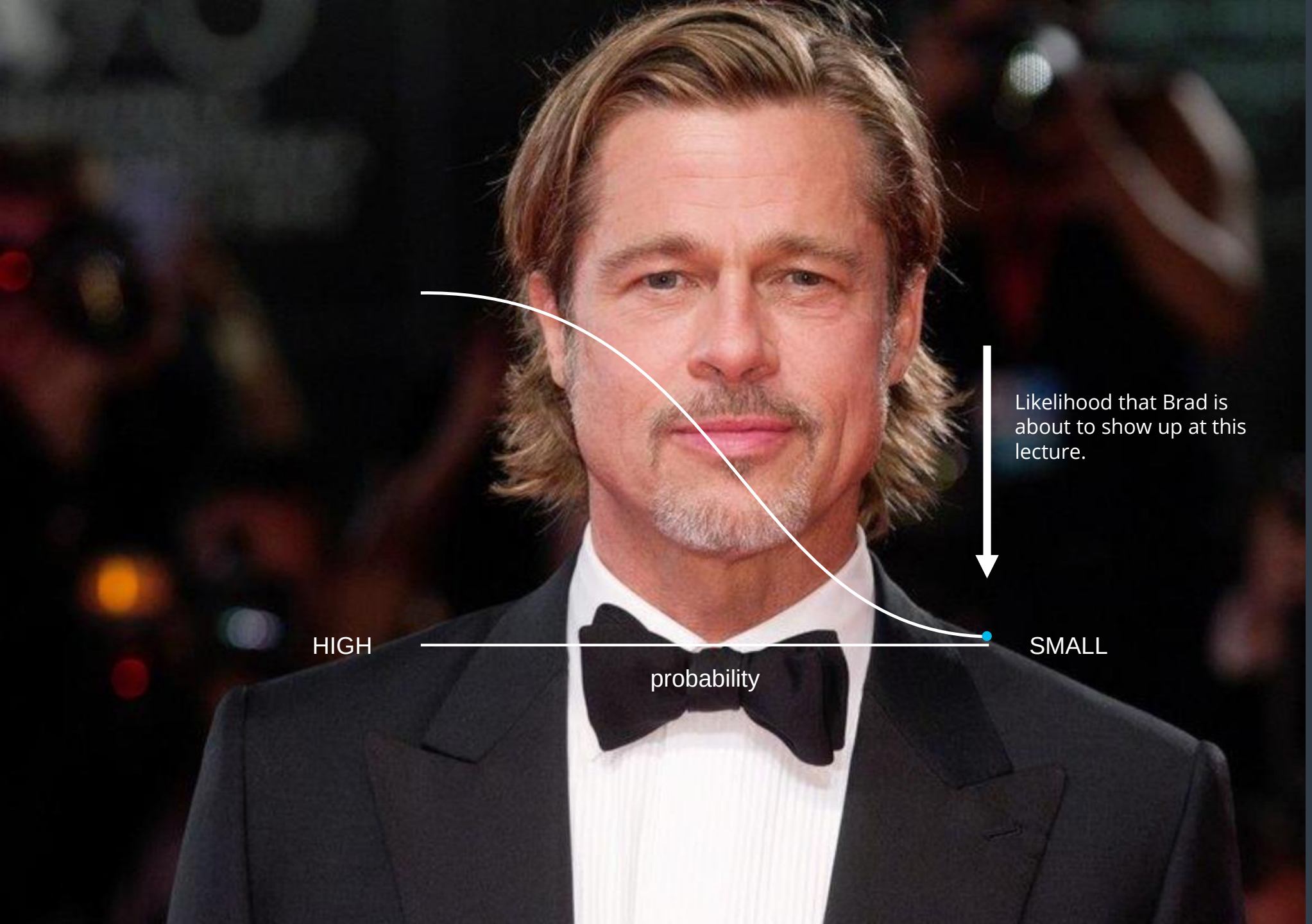
STRANGE PROPERTIES

discrete values

waves

probabilities

non local



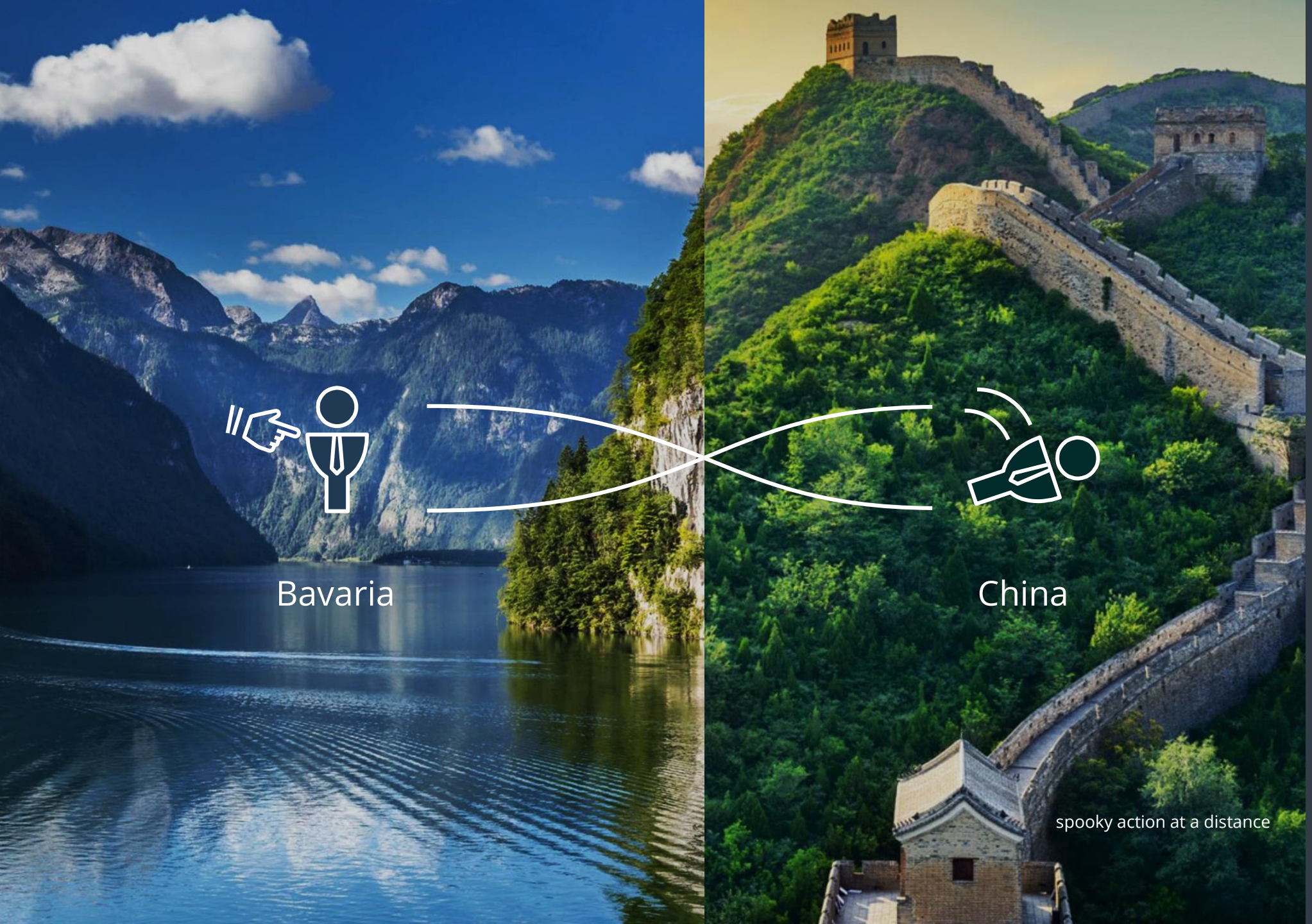
STRANGE PROPERTIES

discrete values

waves

probabilities

Nichtlokal



Quantum mechanics

STRANGE PROPERTIES

discrete values

waves

probabilities

non local

Quantum mechanics

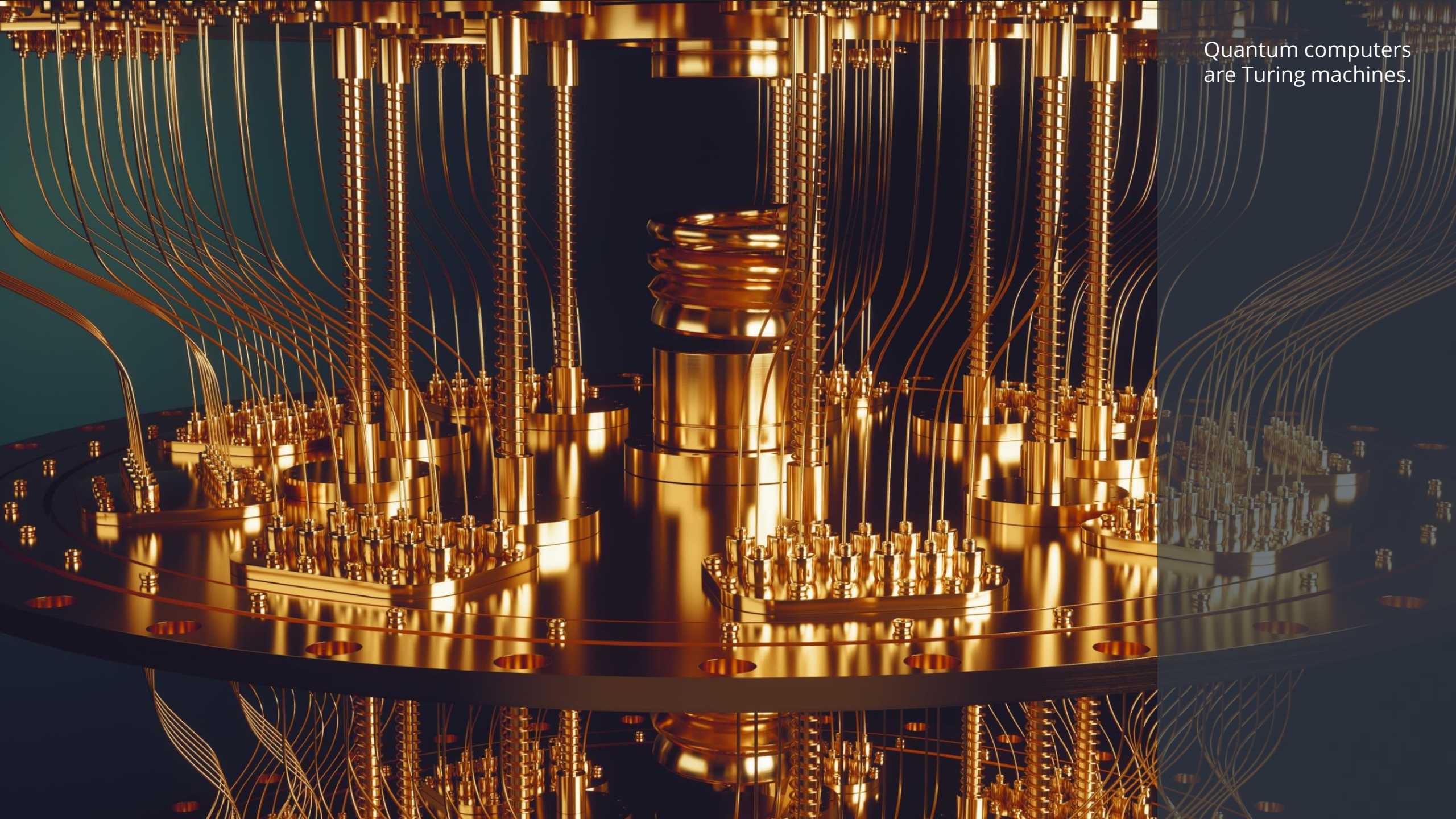
Every little particle

Experienced reality

Big numbers - Statistics

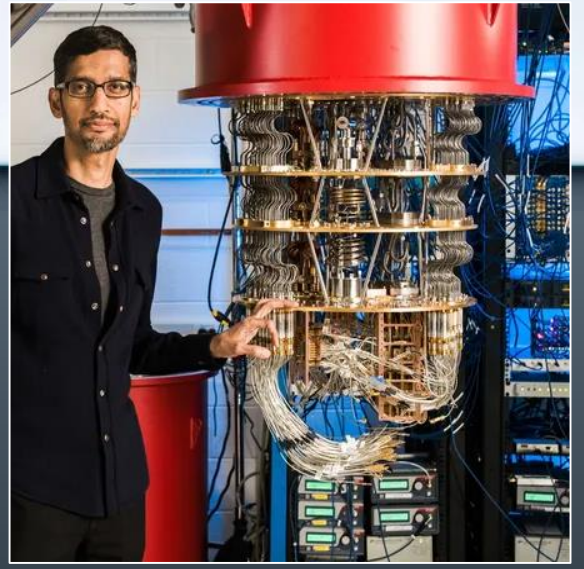
mgm

Quantum computers

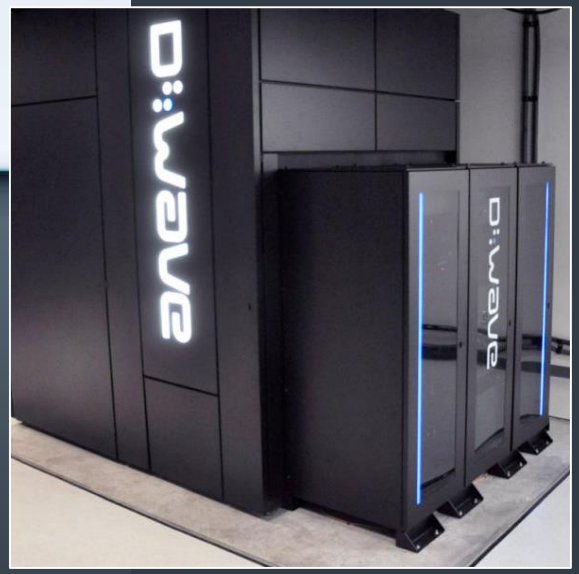

Quantum computers
are Turing machines.

Quantum computer

source: IBM



source: Google



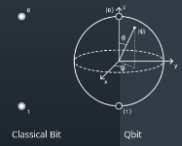
source: D-WAVE

BIG

FOR SALE

SPECIAL PROPERTIES

GOOD FOR NOTHING



Physical arrangements to manipulate quanta

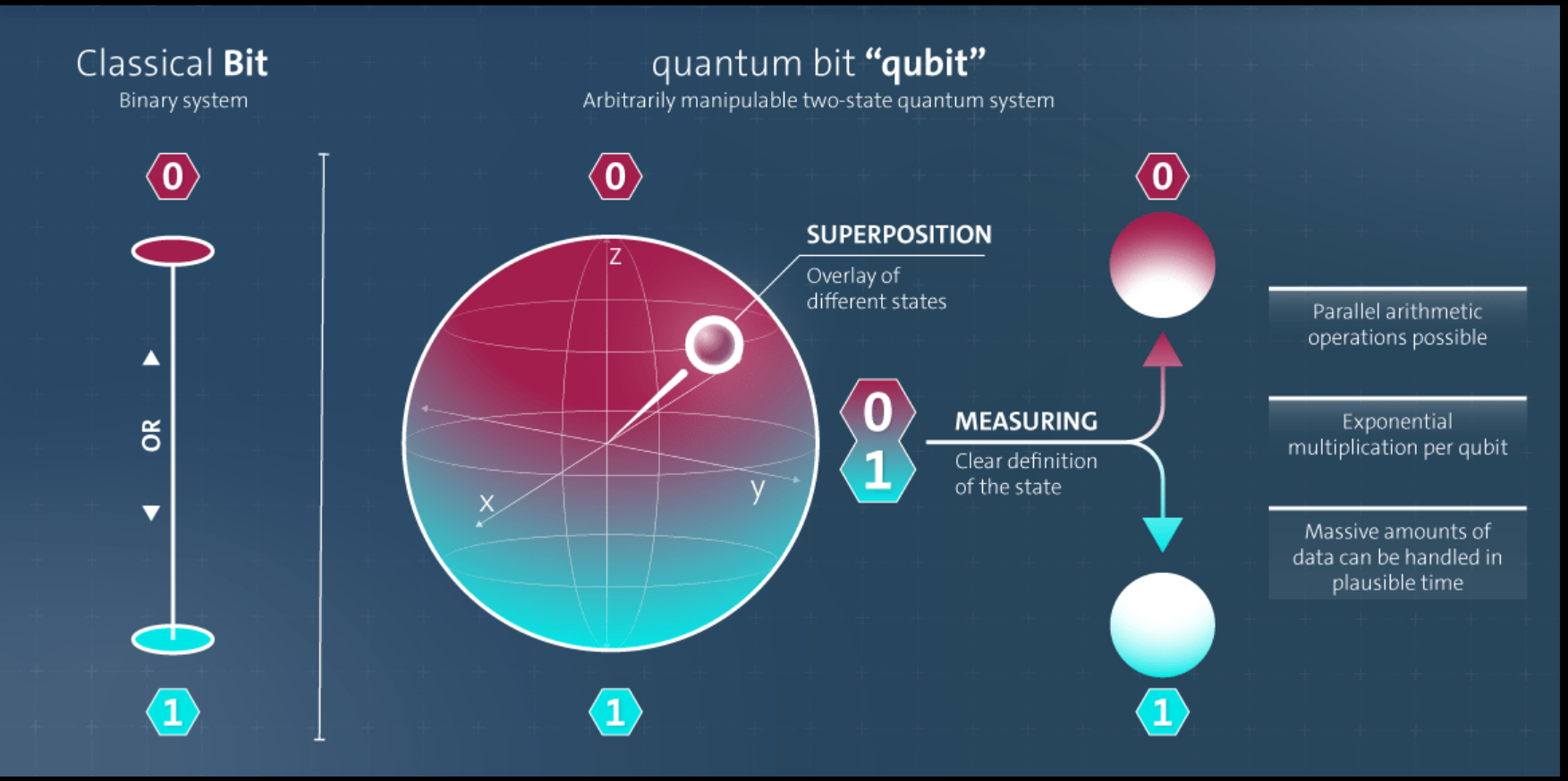
Qubits, Quantum gates

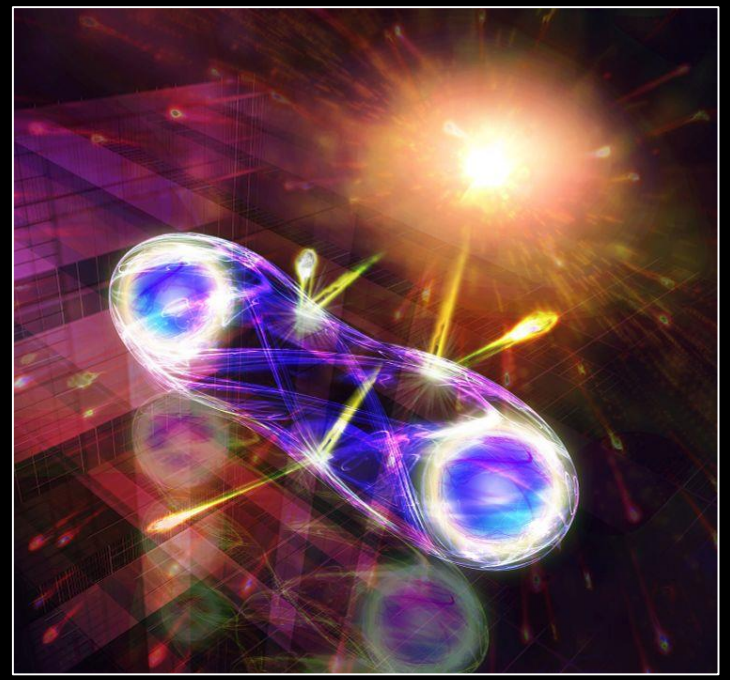
Universal gates

Similar challenges as for classic computer

Not to be confused with adiabatic QC

Qubits – a lot of information and a lot of parallel computing power





1-Qubit State $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

mgm

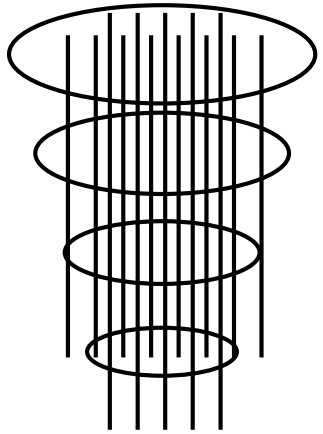
Next milestone of computer technology ?

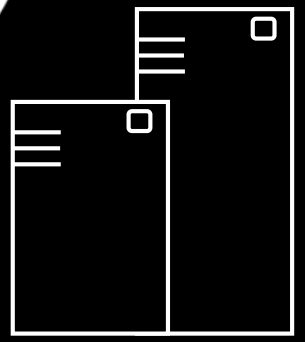
Quantum computing and Hollywood

Next milestone of computer technology ?
Yes, but...

STRENGTHS OF THE COMPUTERS LIE OPPOSITE

QUANTUM COMPUTER





CLASSICAL COMPUTER

COMPLEMENT INSTEAD OF REPLACEMENT

Functional: Simulation in both directions

Non-functional: degrees of complexity

- polynomial
- supra-polynomial "difficult problems“

Simulation quantum computer <-> classical computer:

-> difficult problem

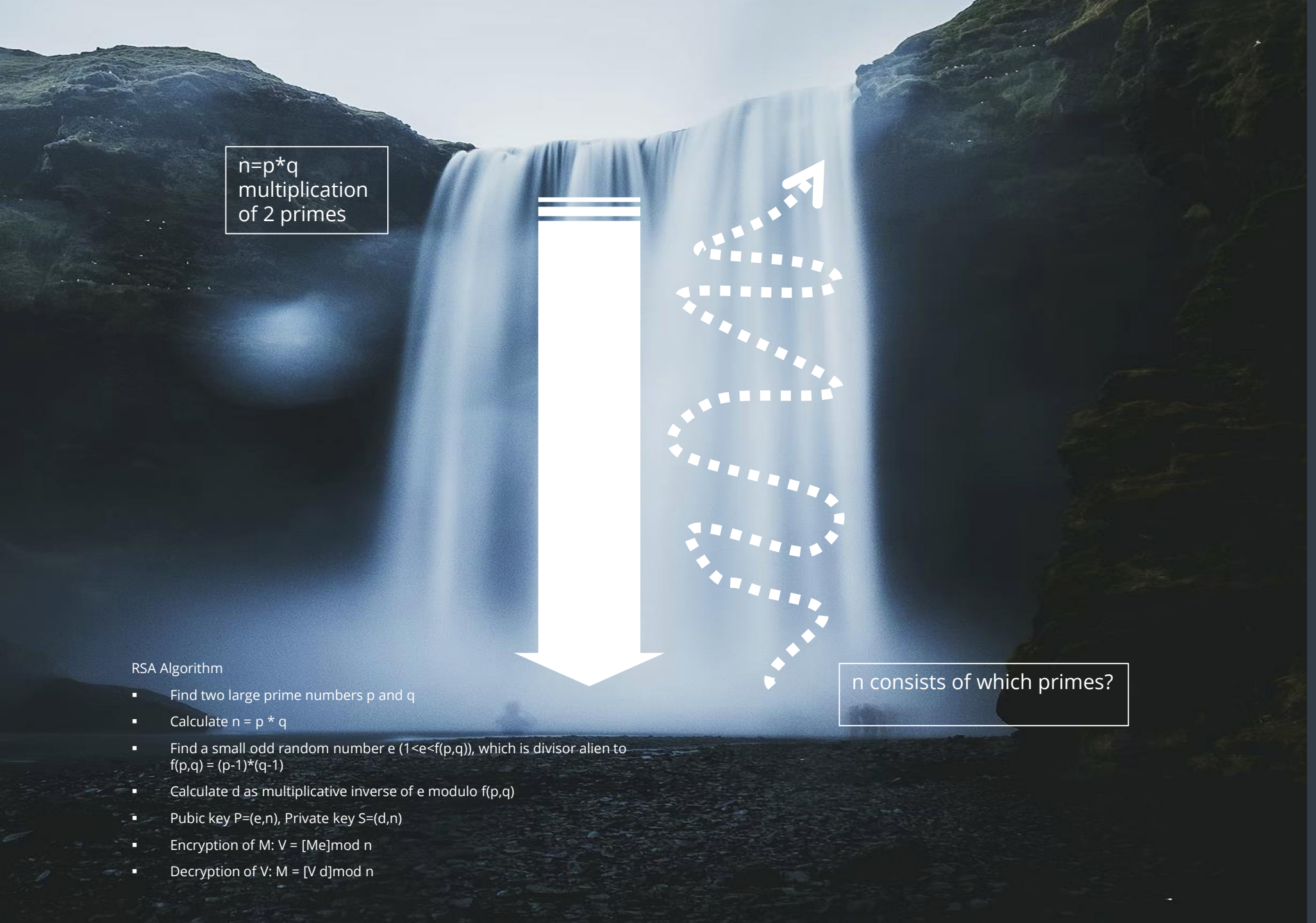
If the physics of the computer matches the problem, then a computer is efficient.

mgm

Cryptographic methods

Cryptographic methods

Attack vectors using RSA as an example



RSA Algorithm

- Find two large prime numbers p and q
- Calculate n = p * q
- Find a small odd random number e (1<e<f(p,q)), which is divisor alien to f(p,q) = (p-1)*(q-1)
- Calculate d as multiplicative inverse of e modulo f(p,q)
- Pubic key P=(e,n), Private key S=(d,n)
- Encryption of M: V = [Me]mod n
- Decryption of V: M = [V d]mod n

Challenge

What are p and q when n is known?

Encryption is based on the fact that it takes a lot of effort to calculate them.

Reversal: If an algorithm is found that quickly manages the prime number factorization and thus calculates p and q, then the encryption method is moot.

Cryptographic methods

Basic idea

- Mathematical mapping that quickly encrypts and decrypts when the key is known.
- whose inversion is a "difficult" problem if the key is unknown

Process classes

- Symmetric procedures (sender and receiver use the same key).
- Asymmetric methods (e.g. public and private key)
- and of course mixture of the two methods (because symmetric is much faster)

RSA, Diffie Hellman and Others

- Prime factorization seems to be a "difficult" problem

mgm

So what?

If the asymmetric procedure (including prime number factorization) could be computed quickly, all mixed procedures currently in use would lose out - including the ones used by our customers.

and

The decomposition of large prime numbers is the physics of quantum computing (as well as finding the discrete logarithm).

Attack vectors & quantum computing

Quantum Mechanics: Wave functions and discrete states

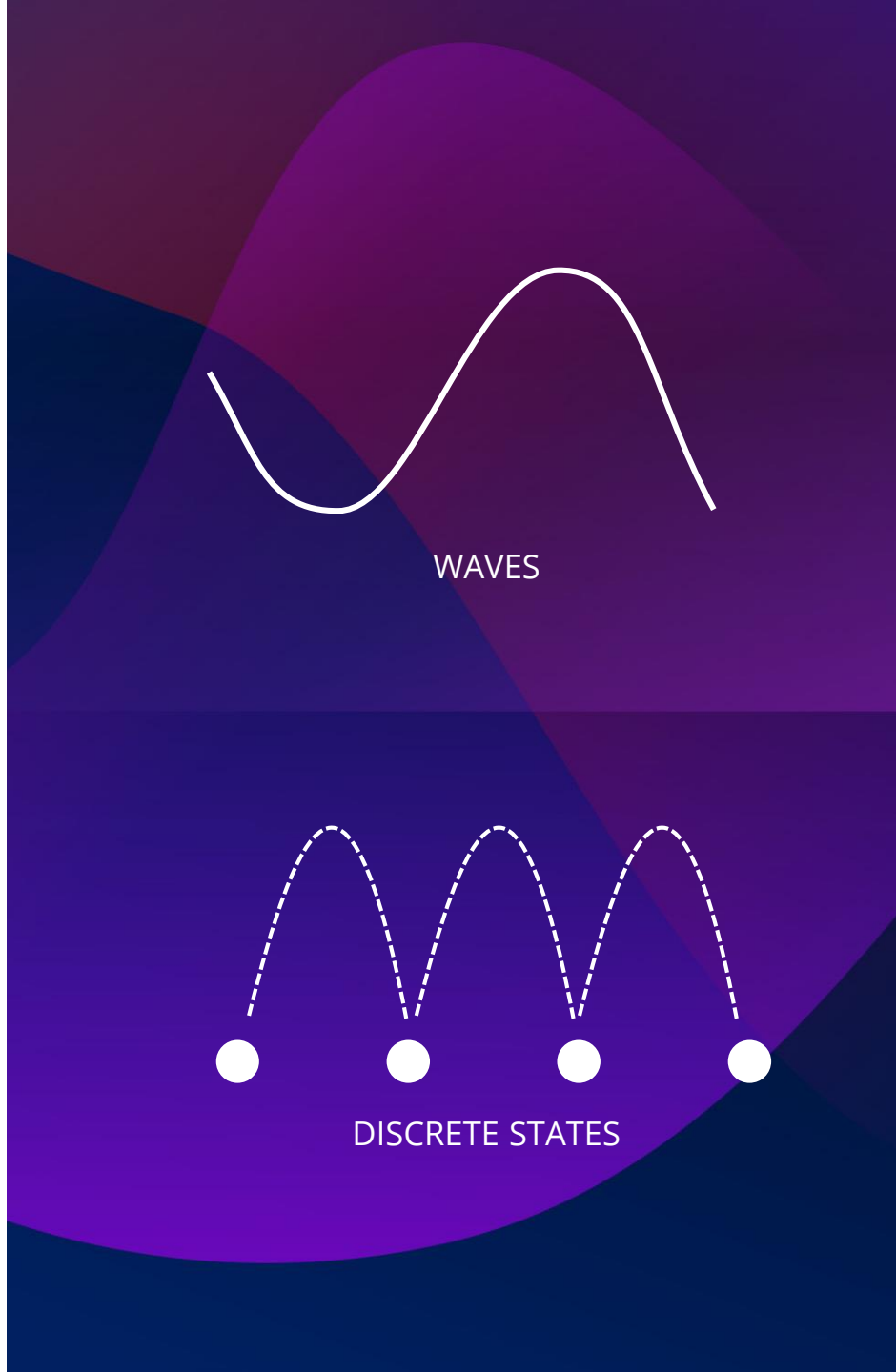
- → discrete Fourier transformation elementary part of the physics of these systems

discrete Fourier transformation & Peter Shor 1994

- algorithm for prime factorization
- algorithm for discrete logarithm

search in an unsorted list with n elements -> Grover algorithm

- worst case n comparisons in classical case
- Quantum computer does it with root (n) steps in a probability procedure (sharp boundary - can't do better)
- Can attack symmetric methods; however, this can be easily compensated by increasing the key length



mgm

Where do we currently stand (2022)?

Hardware
Quantum computers at the level of the first tube computers

Algorithms
Few available. Grover algorithm, prime factorization...

Symmetric ciphers
Probably safe for a long time

Asymmetric ciphers
At risc, but not for a while

PQ encryption
First candidates in research

Research & Development

5-10 years
1 Mio Qubits
(IBM)

Mature technology for practical use

Result: Don't Panic

And now for something completely different

Quantum Cryptography

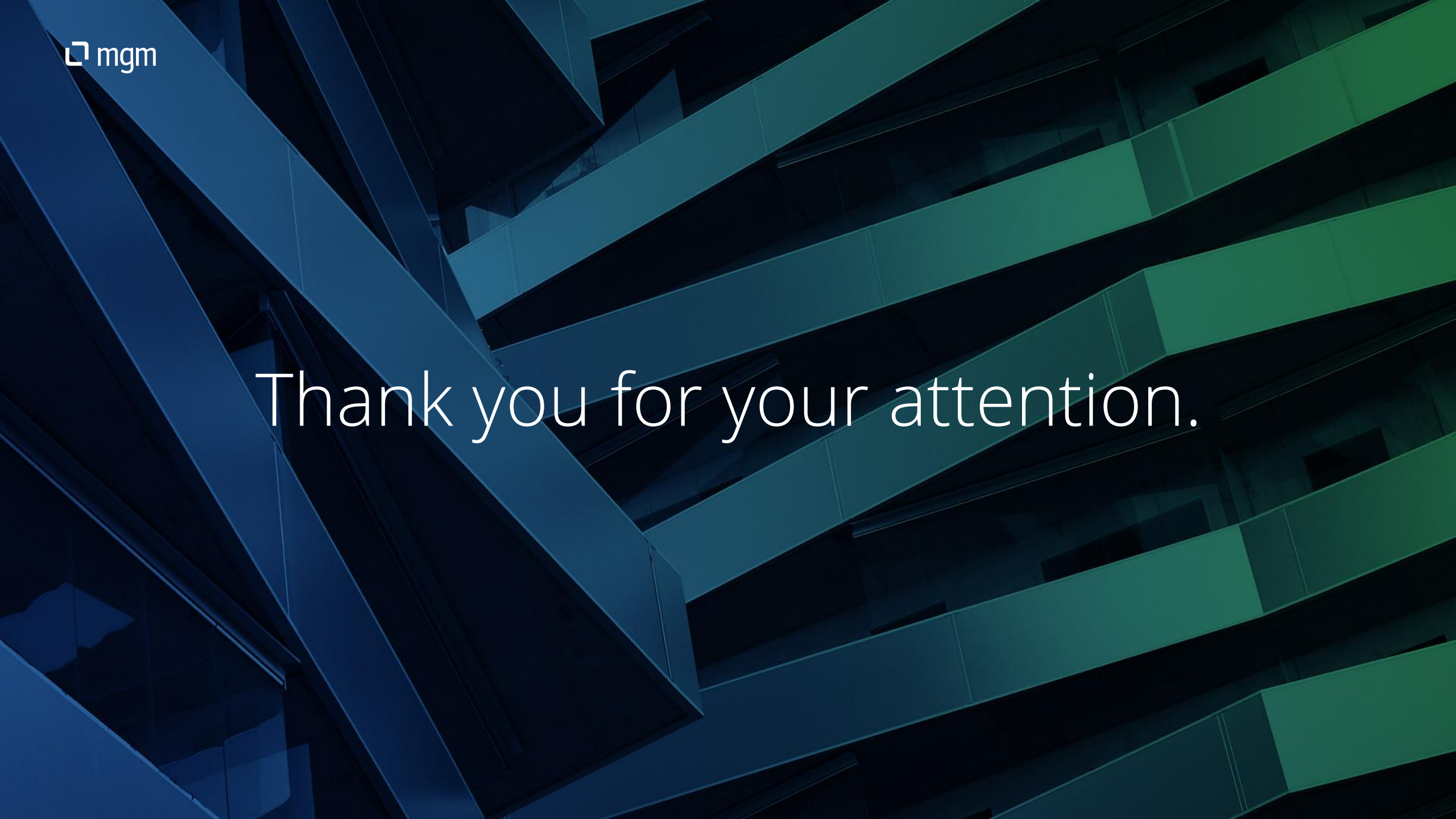
Often equated with quantum key exchange (has been implemented several times).

- The security of the various methods of quantum key exchange arises from the fact that an attacker who eavesdrops on the key transmission is noticed. If it is detected that the transmission has been eavesdropped, the transmitted key is discarded (in practice, if an error tolerance value is exceeded) and the key generation and transmission is restarted.

Underlying physics:

- Measurements change quantum states
- Information can be transmitted via entangled states

mgm


mgm
Thank you for your attention.