Quantum Computing from Optimization to Artificial Intelligence

Effects on Business, Software and Security

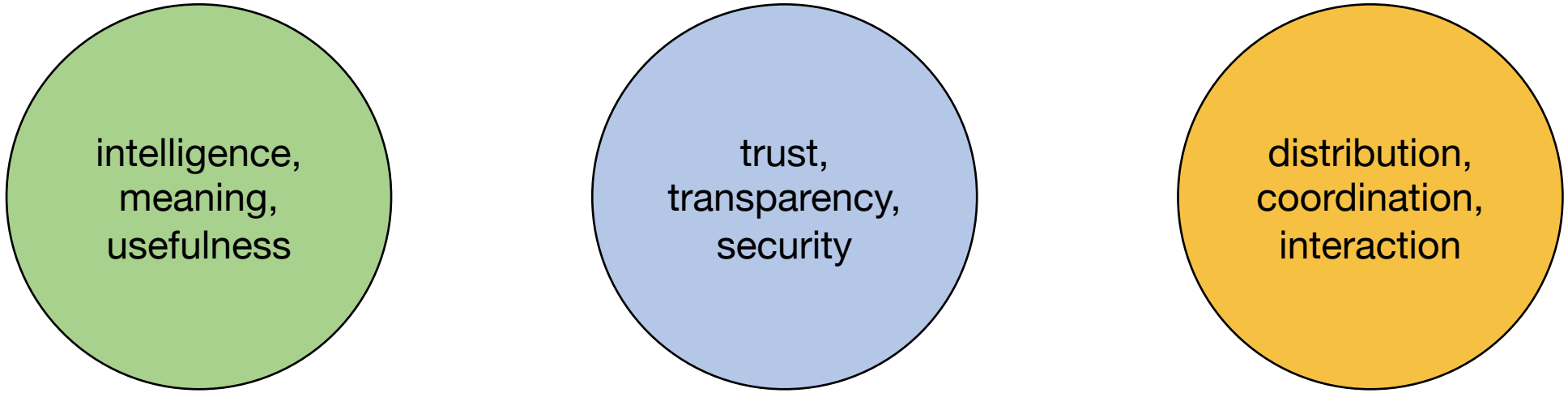
Thomas Gabor

Quantum Applications and Research Laboratory

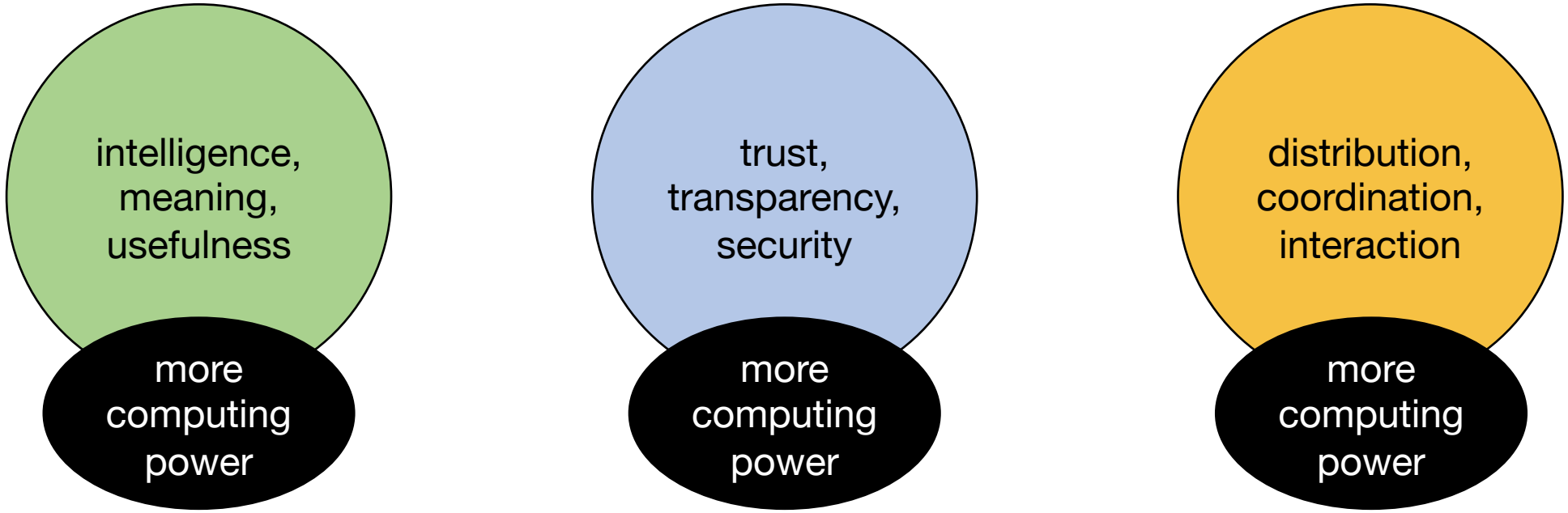
Mobile and Distributed Systems Group

LMU Munich

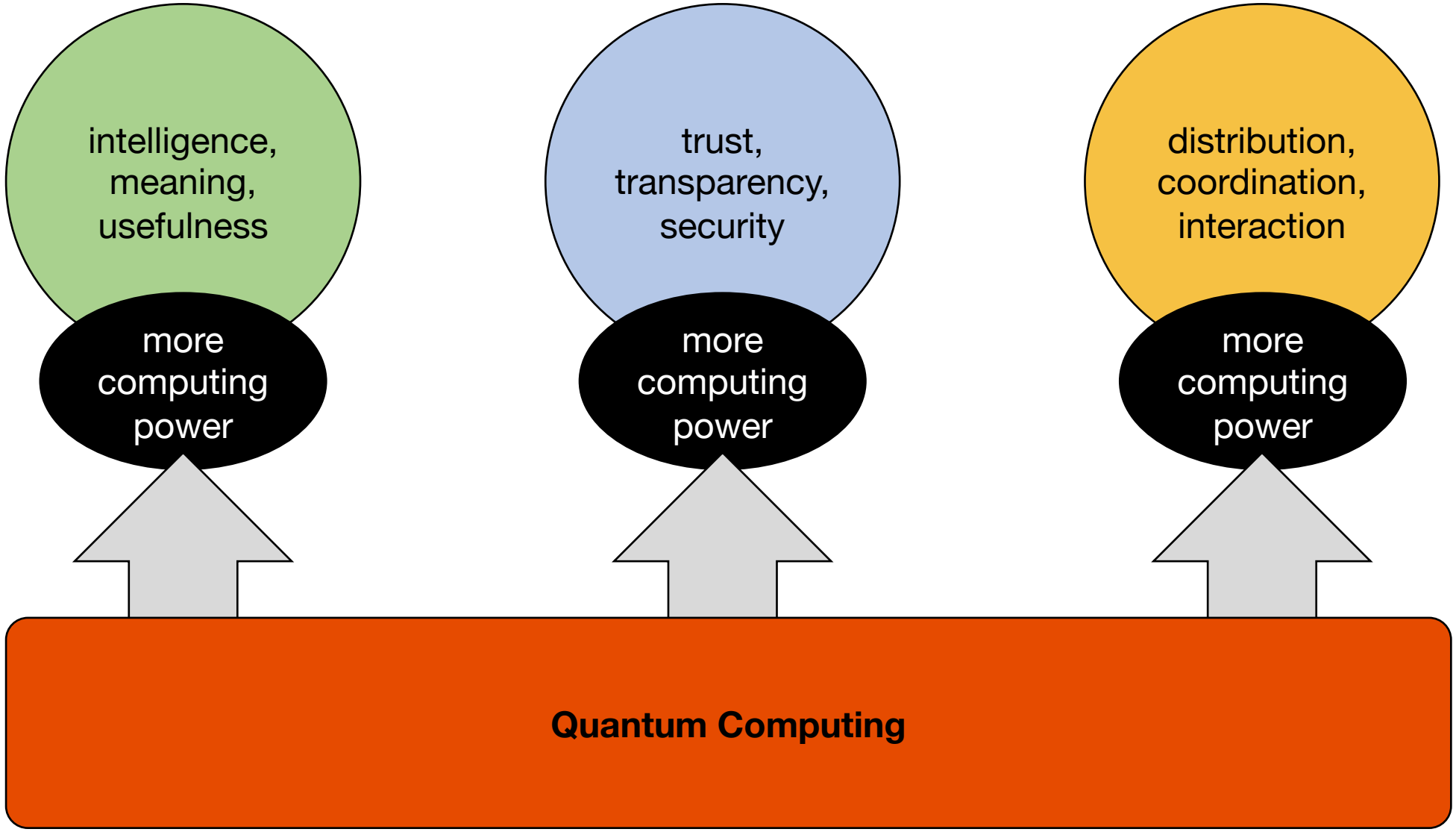
Future of Systems



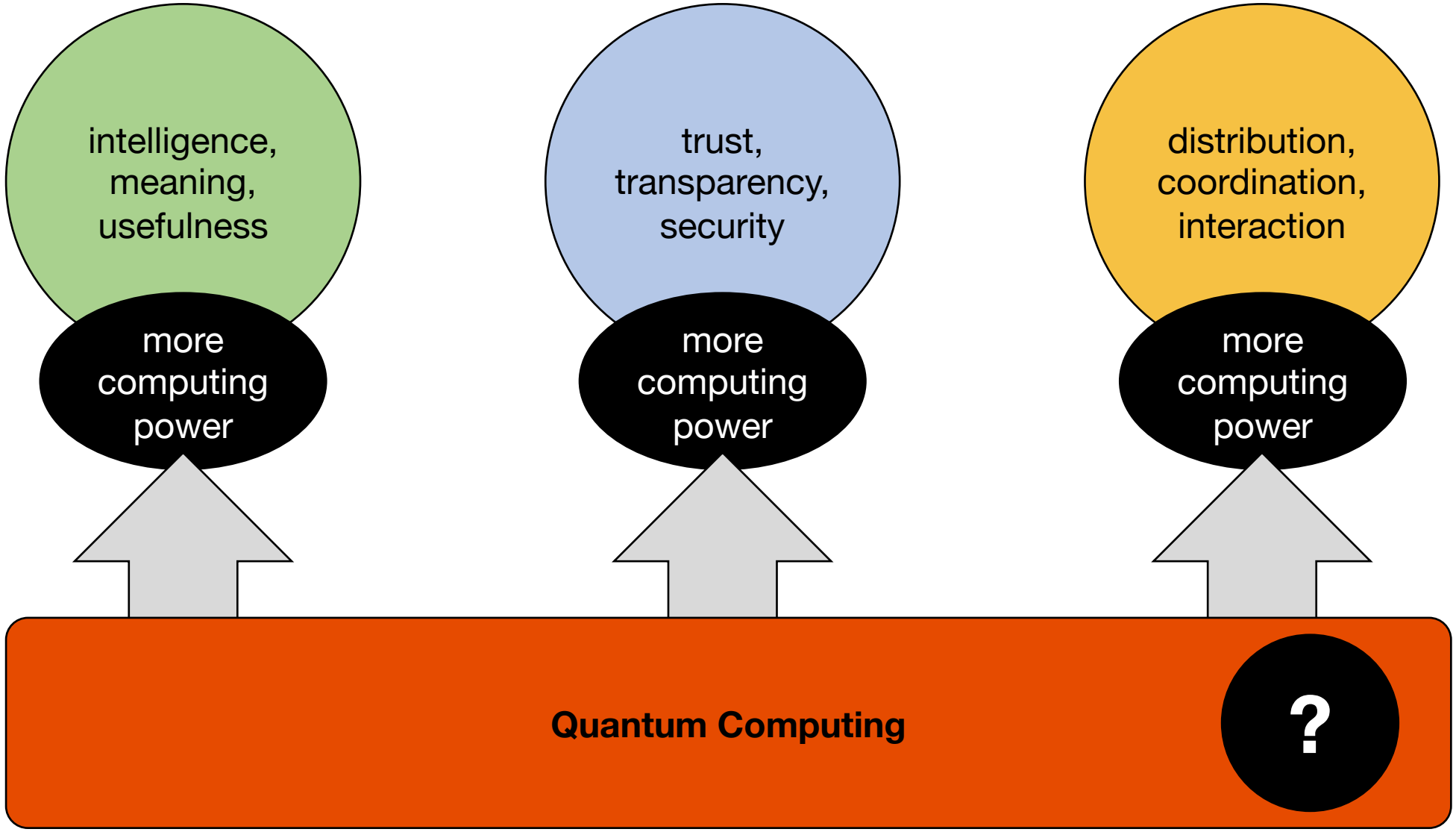
Future of Systems



Future of Systems



Future of Systems

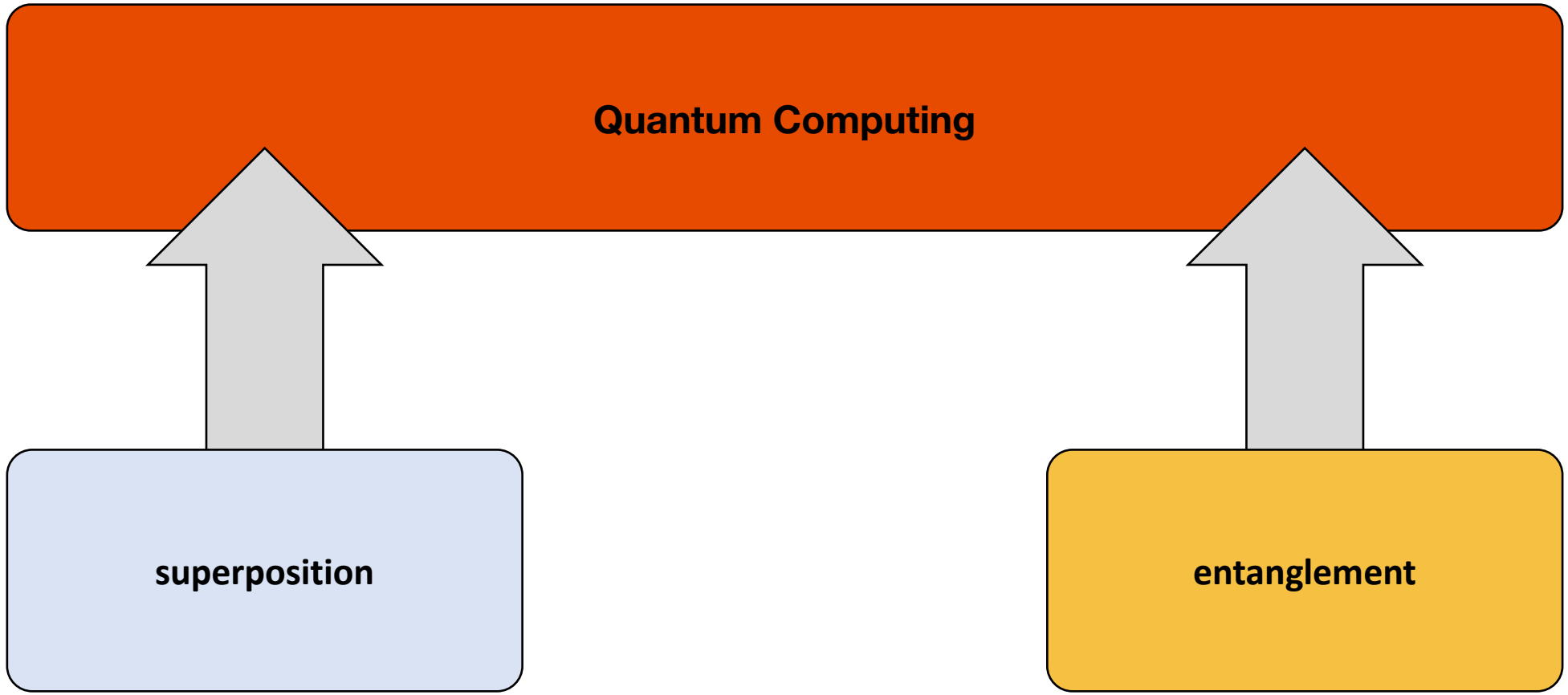


Agenda

1. Quantum Physics
2. Quantum Computing
3. Optimization Business
4. Opportunities

❶ Quantum Physics

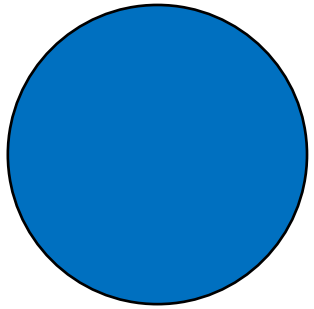
What‘s new?



Superposition

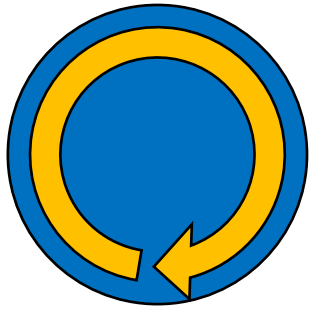
classical physics

particle



Superposition

classical physics



particle

spin

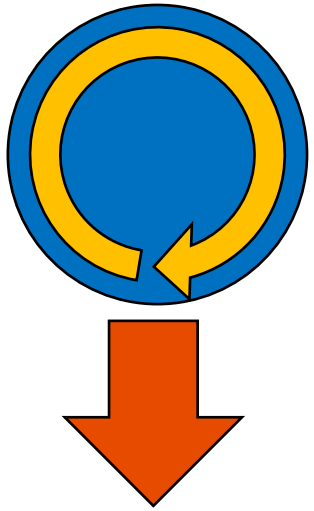
Superposition

classical physics

particle

spin

measure spin



Superposition

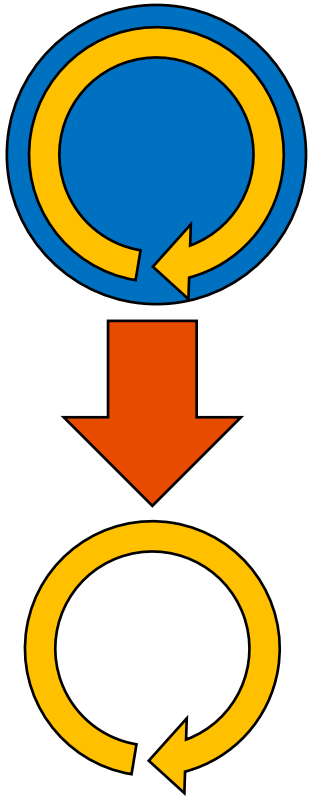
classical physics

particle

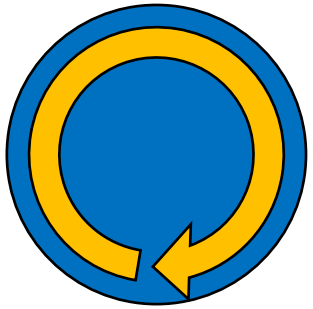
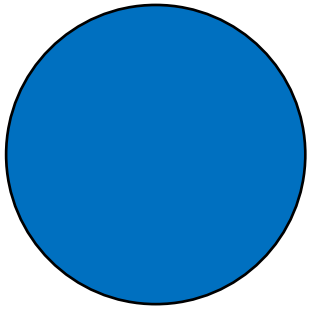
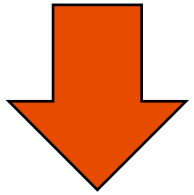
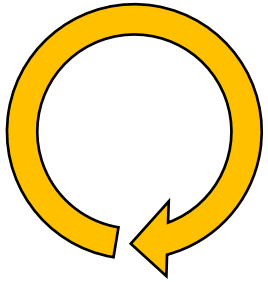
spin

measure spin

measured spin



Superposition

	classical physics	quantum physics
particle		
spin		
measure spin		
measured spin		

Superposition

classical physics

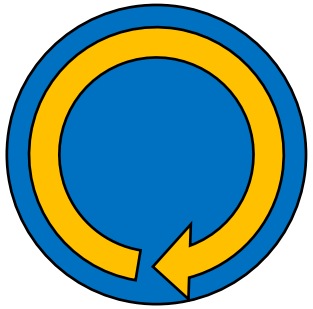
quantum physics

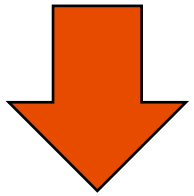
particle

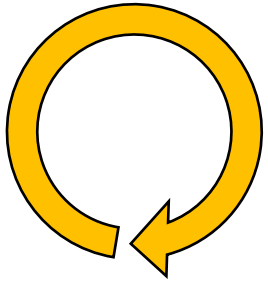
spin

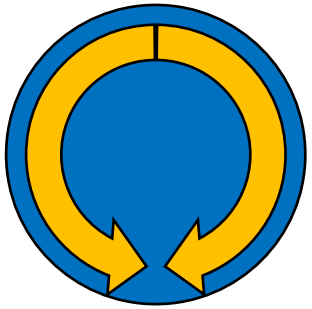
measure spin

measured spin









Superposition

classical physics

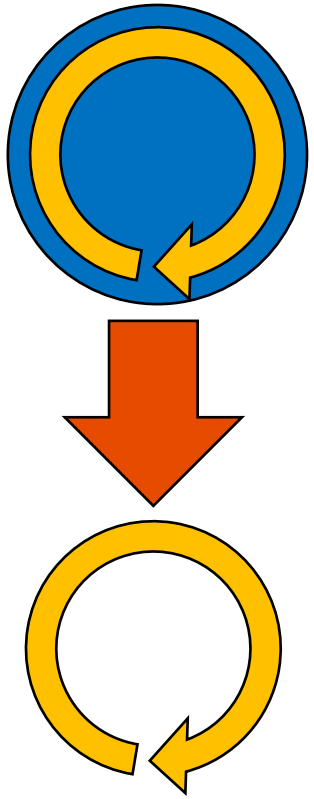
quantum physics

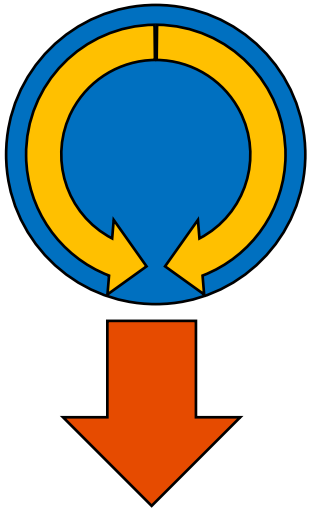
particle

spin

measure spin

measured spin





Superposition

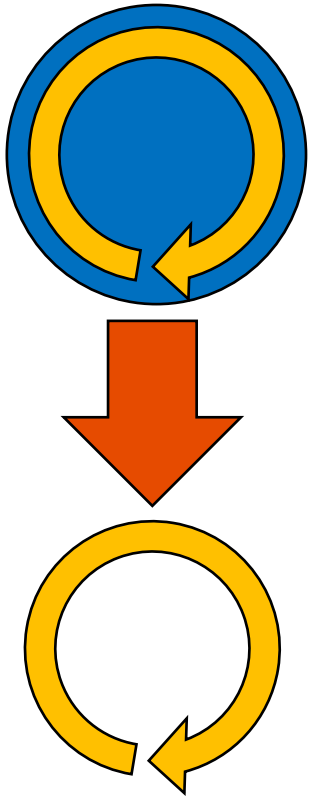
particle

spin

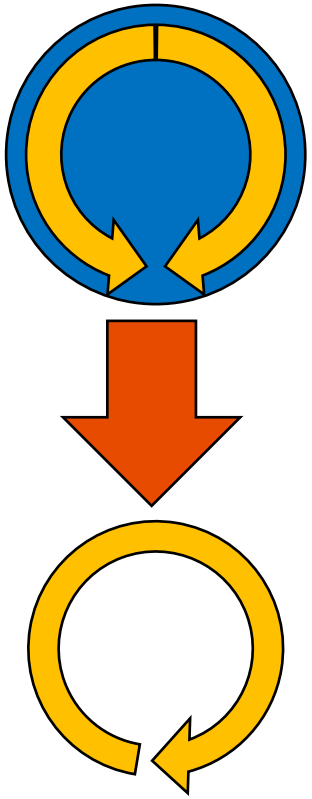
measure spin

measured spin

classical physics



quantum physics



Superposition

classical physics

quantum physics

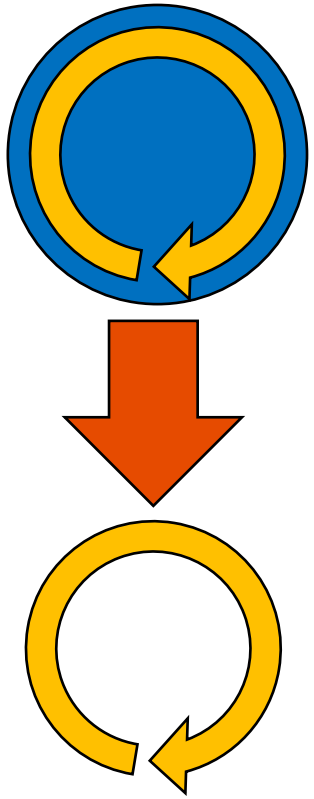
particle

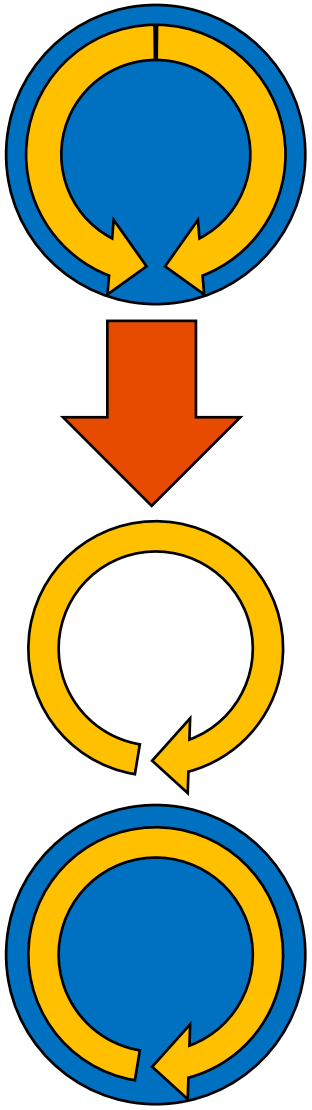
spin

measure spin

measured spin

changed particle

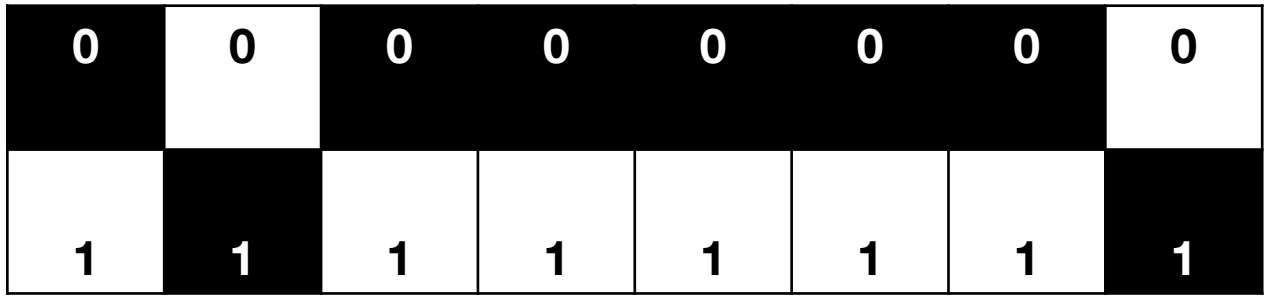




Registers

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1

Registers



ASCII letter A

Superposition on Registers

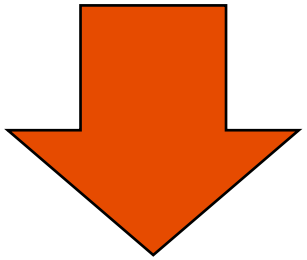
0 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%
50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**

all ASCII letters

at the same time

Superposition on Registers

0 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%
50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**



all ASCII letters

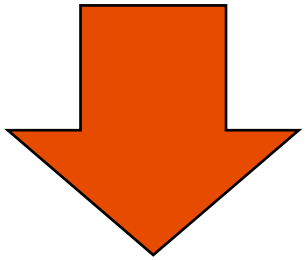
at the same time

measuring

Superposition on Registers

0 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%
50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**

all ASCII letters
at the same time



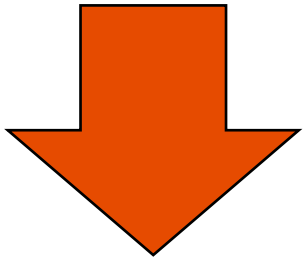
measuring

0	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**

ASCII letter E
with probability 1/256

Superposition on Registers

0 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%
50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**



0	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**

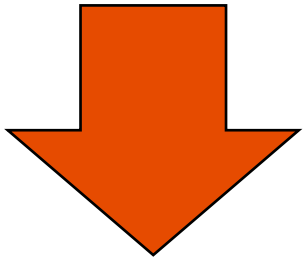
all ASCII letters
at the same time

measuring

ASCII letter &
with probability 1/256

Superposition on Registers

0 90%	**0** 10%	**0** 90%	**0** 90%	**0** 90%	**0** 10%	**0** 90%	**0** 10%
10% **1**	90% **1**	10% **1**	10% **1**	10% **1**	90% **1**	10% **1**	90% **1**



0	**0**	**0**	**0**	**0**	**0**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**

all ASCII letters
at the same time
(but probably E)

measuring

ASCII letter E
with probability 0.43

Entanglement

multiple quantum particles

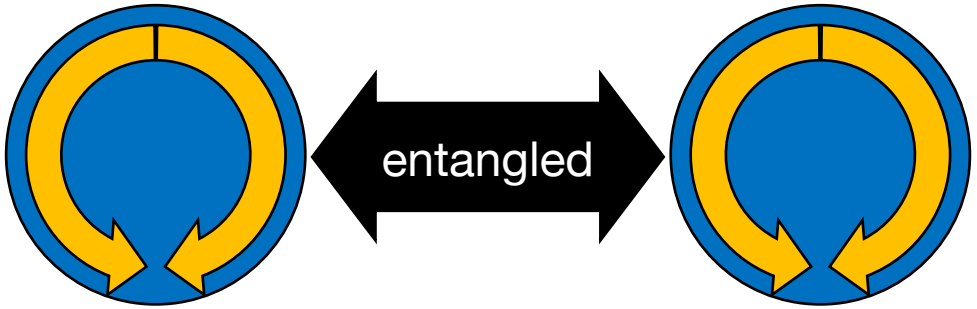
measure single spin

measured spin

changed particles

Entanglement

multiple quantum particles



measure single spin

measured spin

changed particles

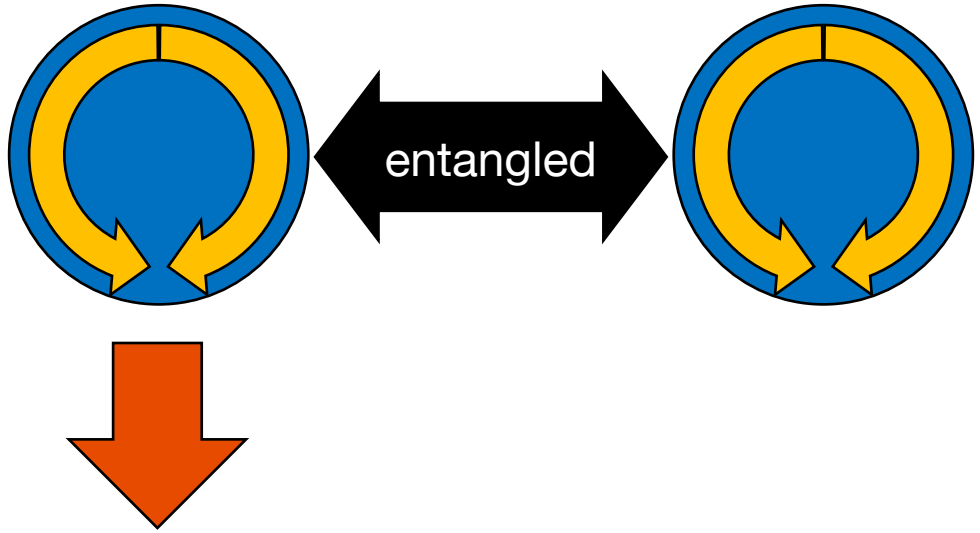
Entanglement

multiple quantum particles

measure single spin

measured spin

changed particles



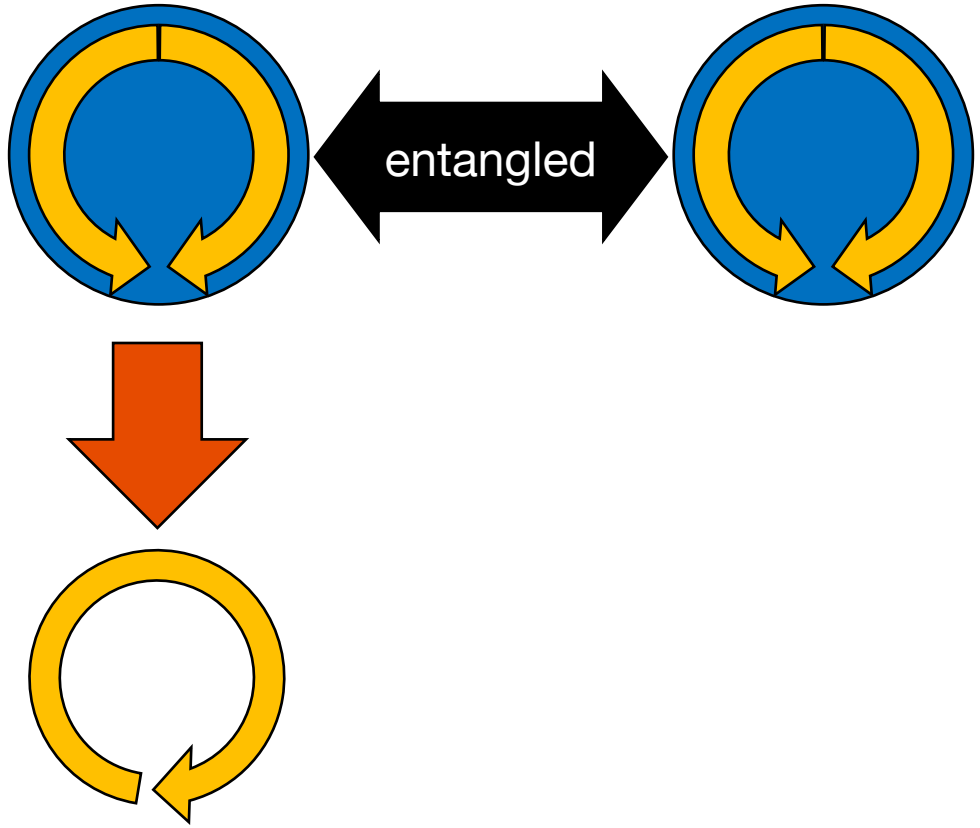
Entanglement

multiple quantum particles

measure single spin

measured spin

changed particles



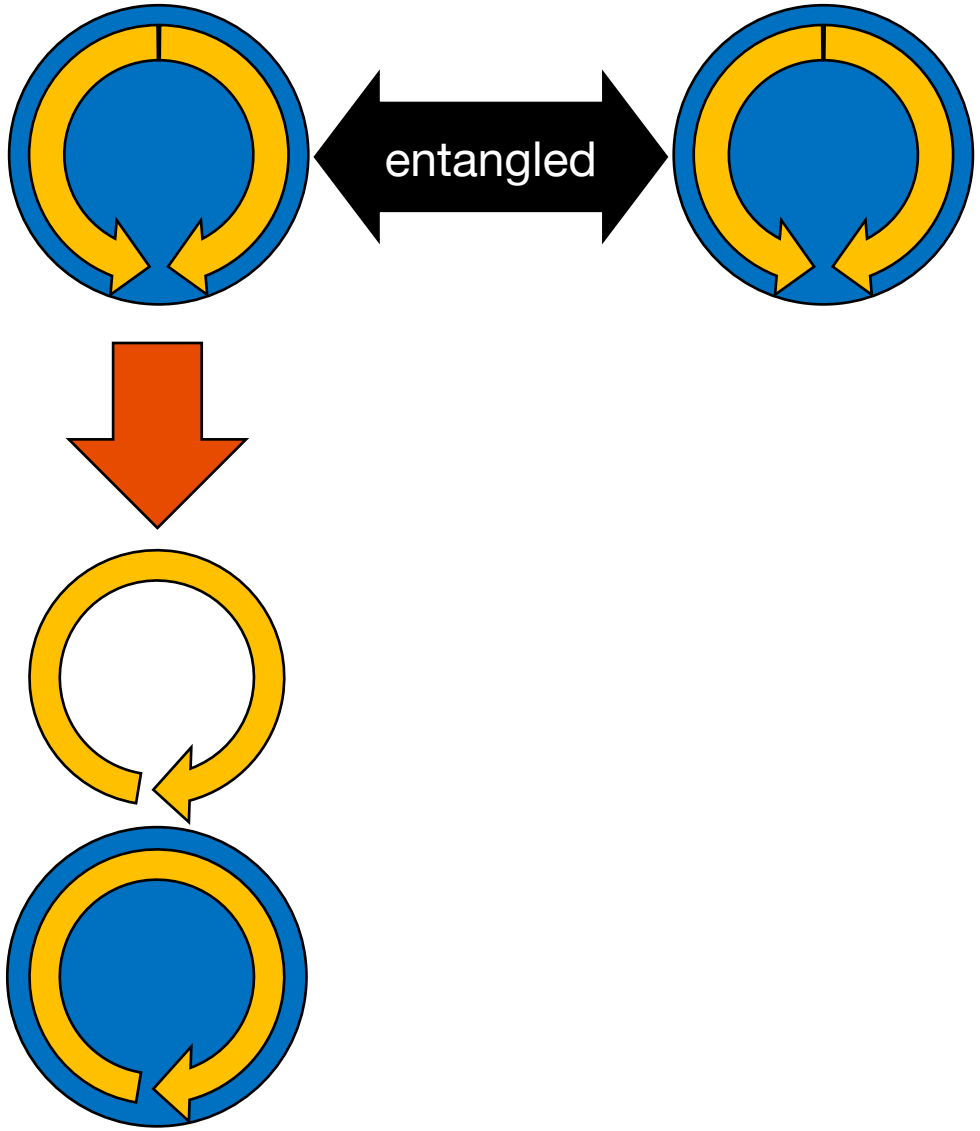
Entanglement

multiple quantum particles

measure single spin

measured spin

changed particles



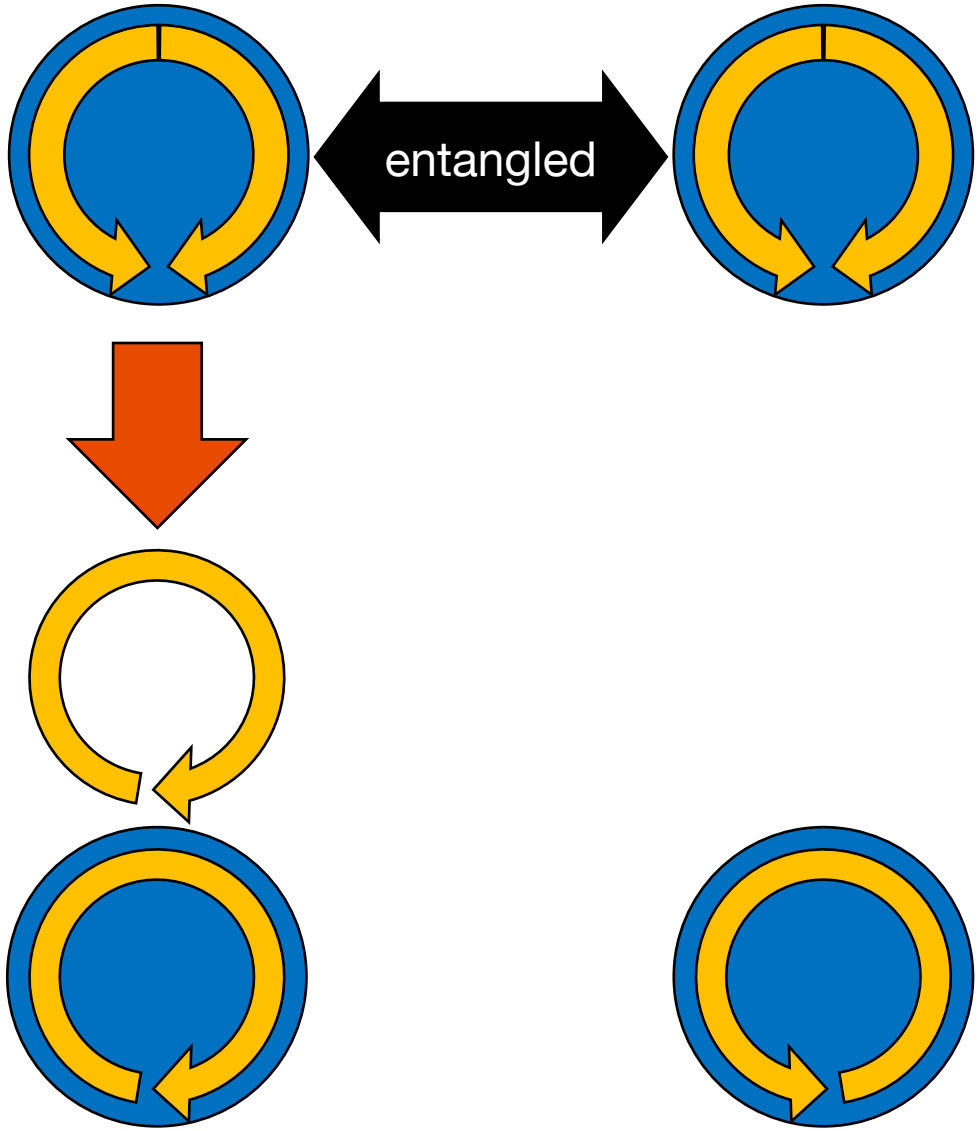
Entanglement

multiple quantum particles

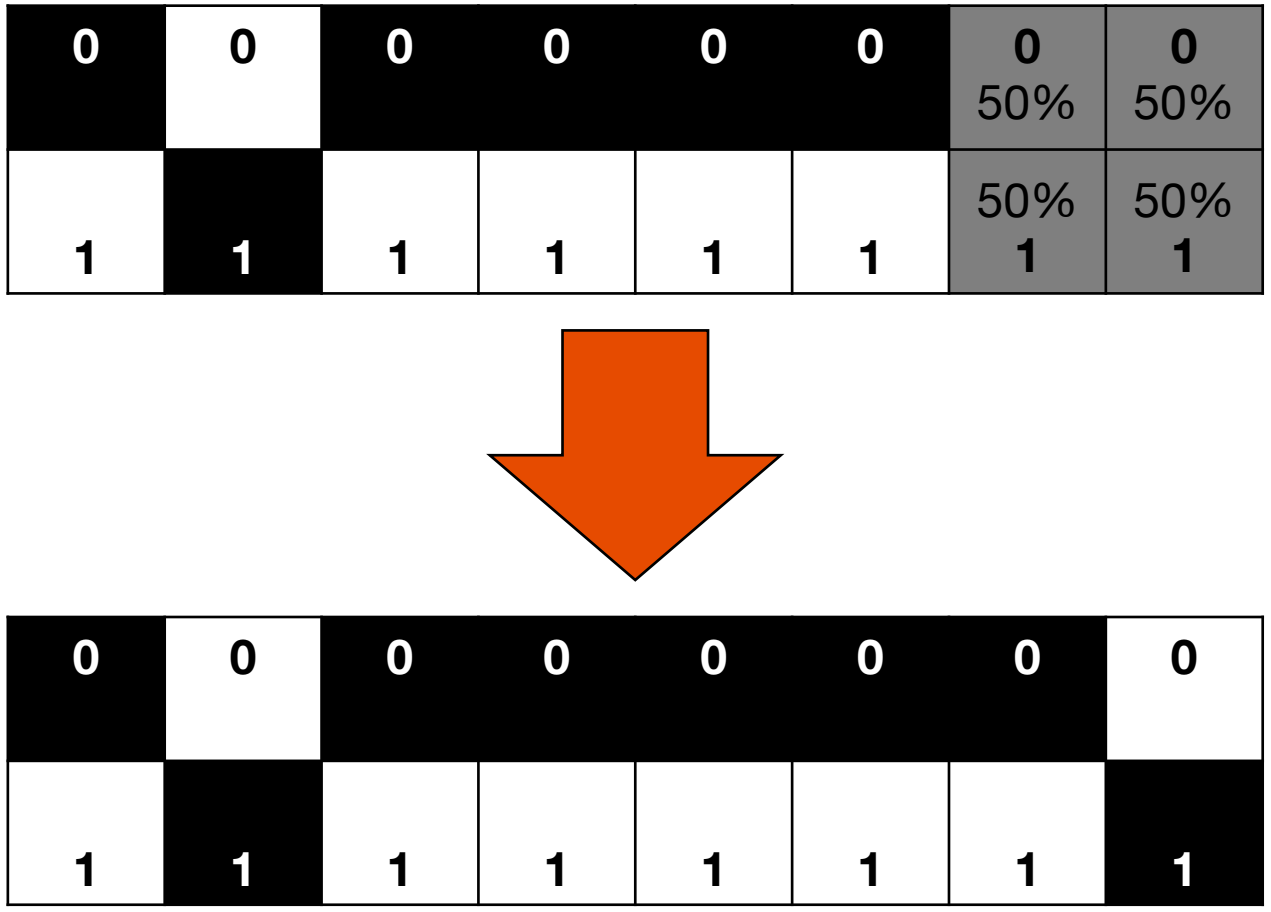
measure single spin

measured spin

changed particles



Entanglement on Registers

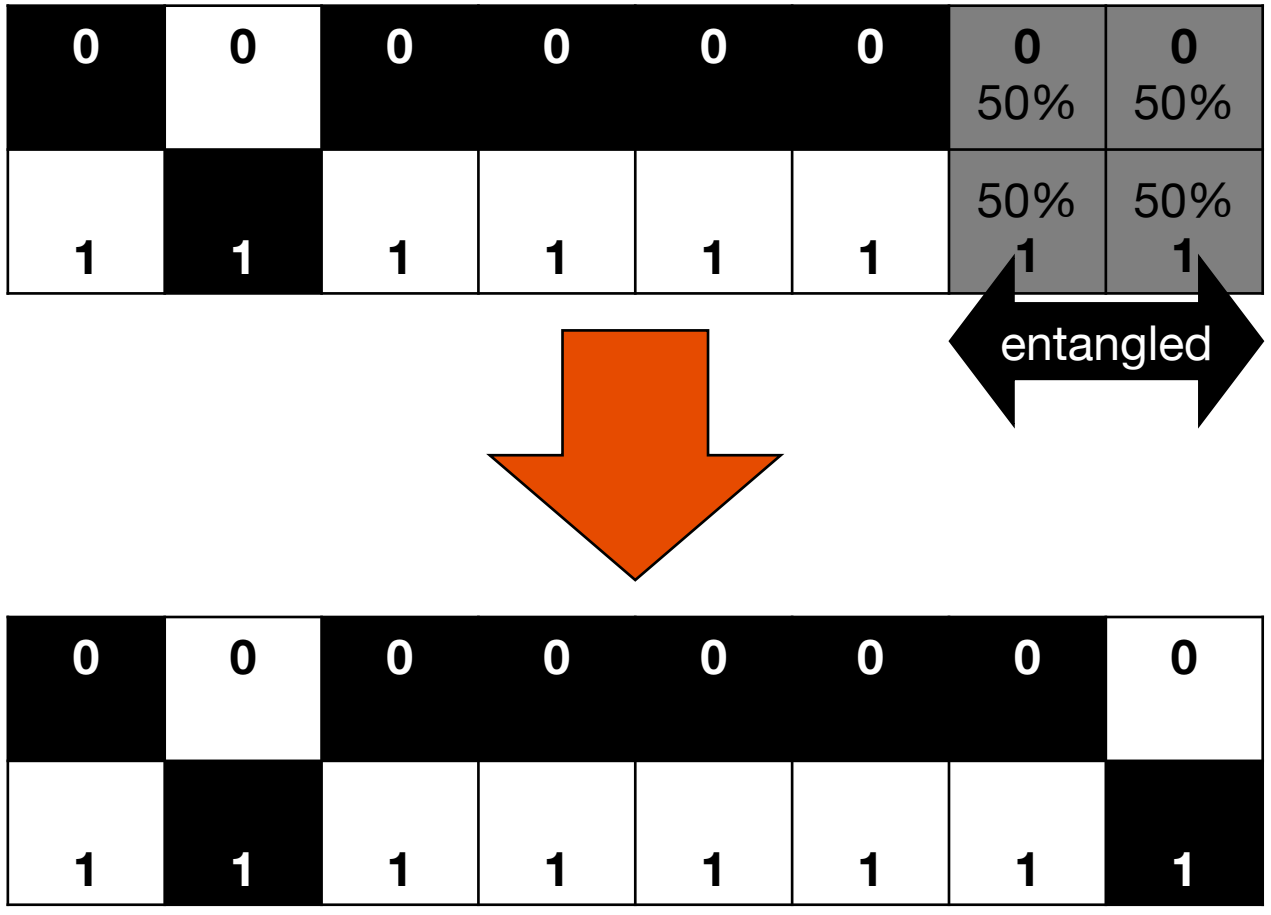


ASCII letters @ A B C
at the same time

measuring

ASCII letter A
with probability 1/4

Entanglement on Registers



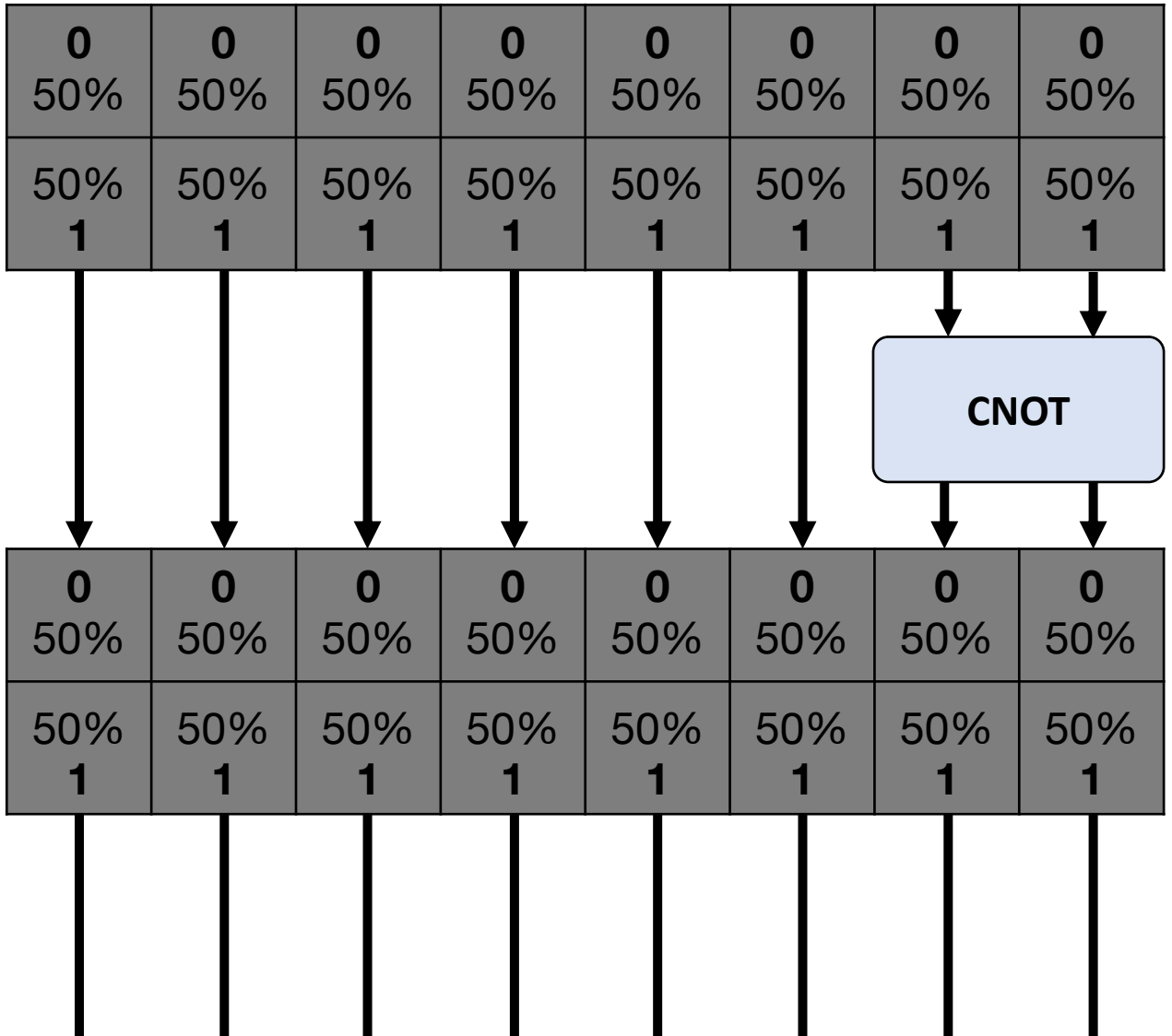
ASCII letters A B
at the same time

measuring

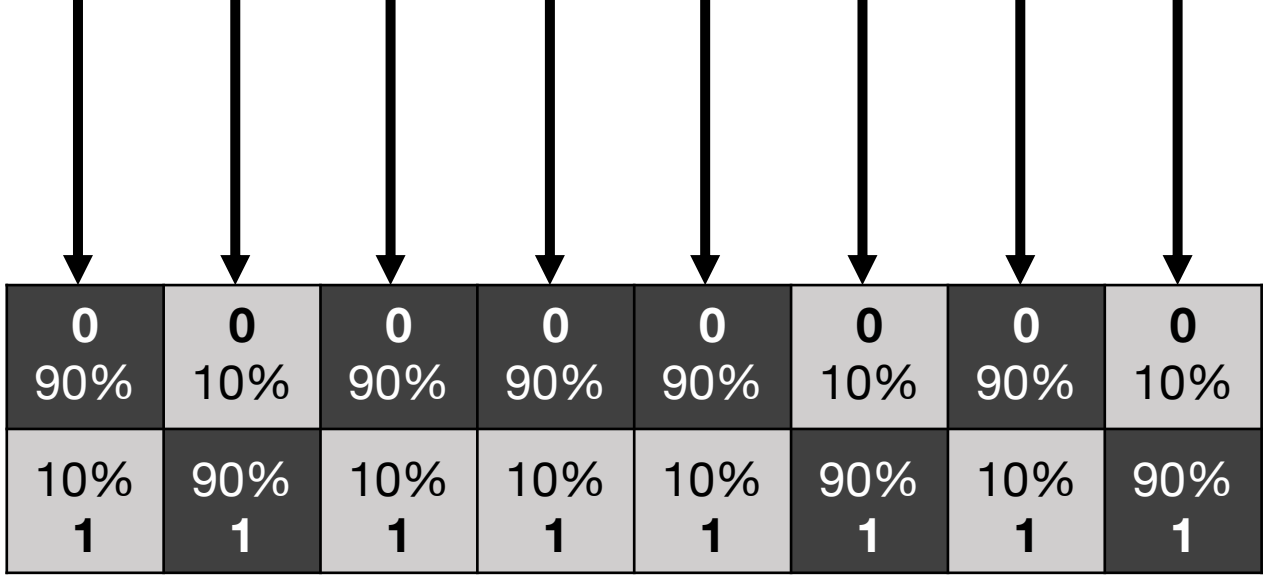
ASCII letter A
with probability 1/2

❷ Quantum Computing

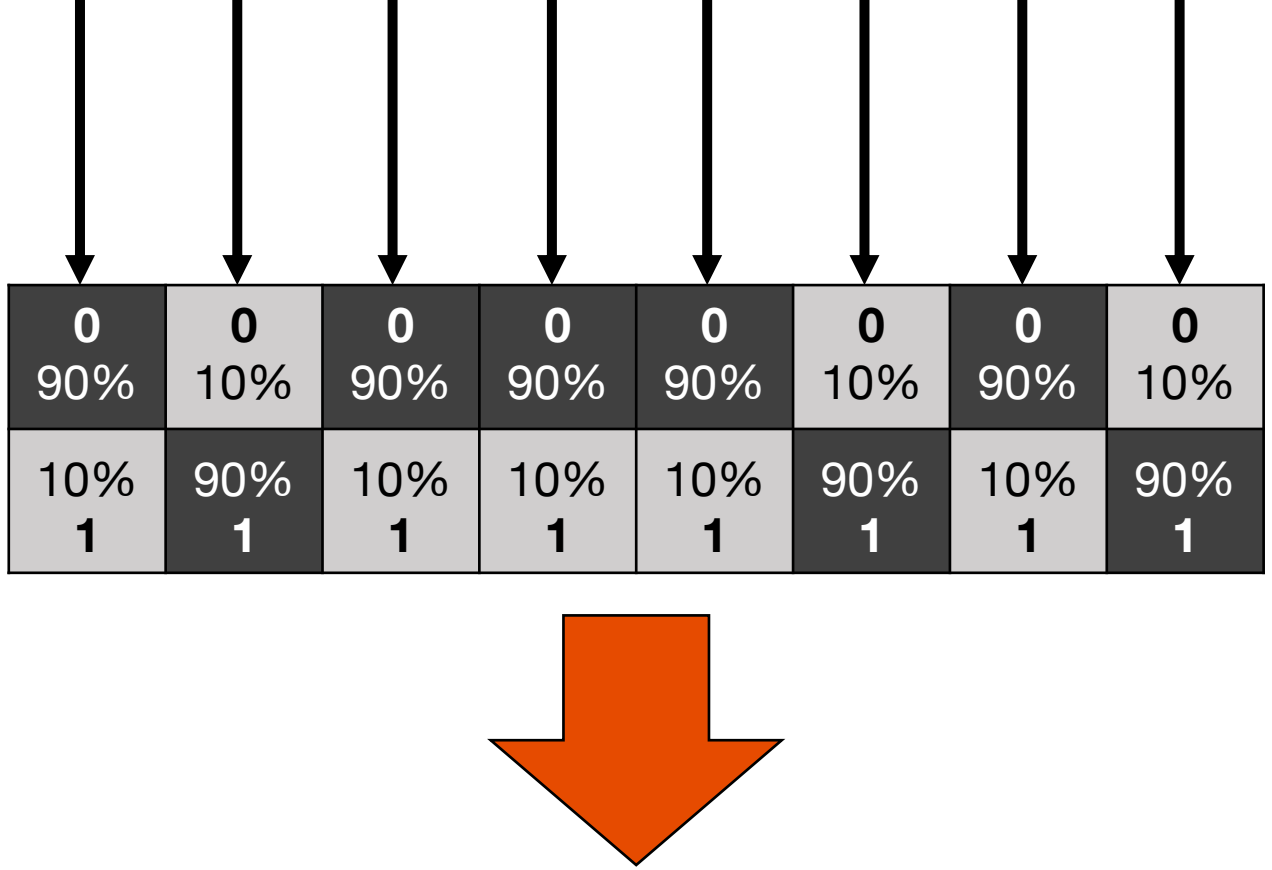
Gate Model



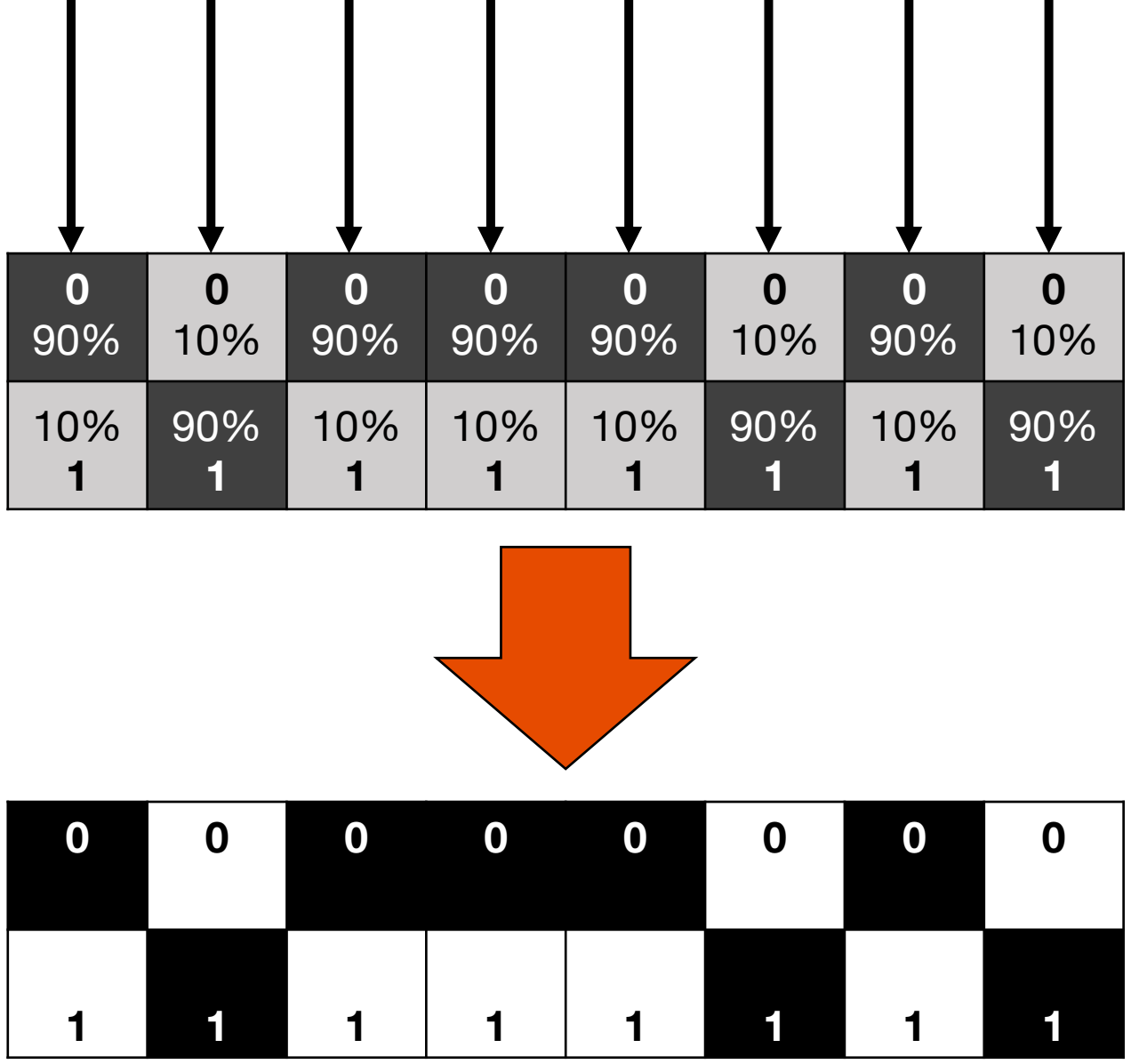
Gate Model



Gate Model



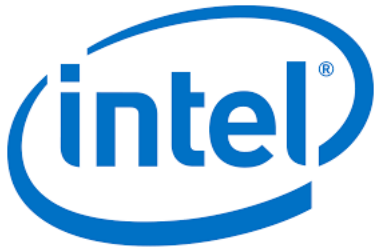
Gate Model



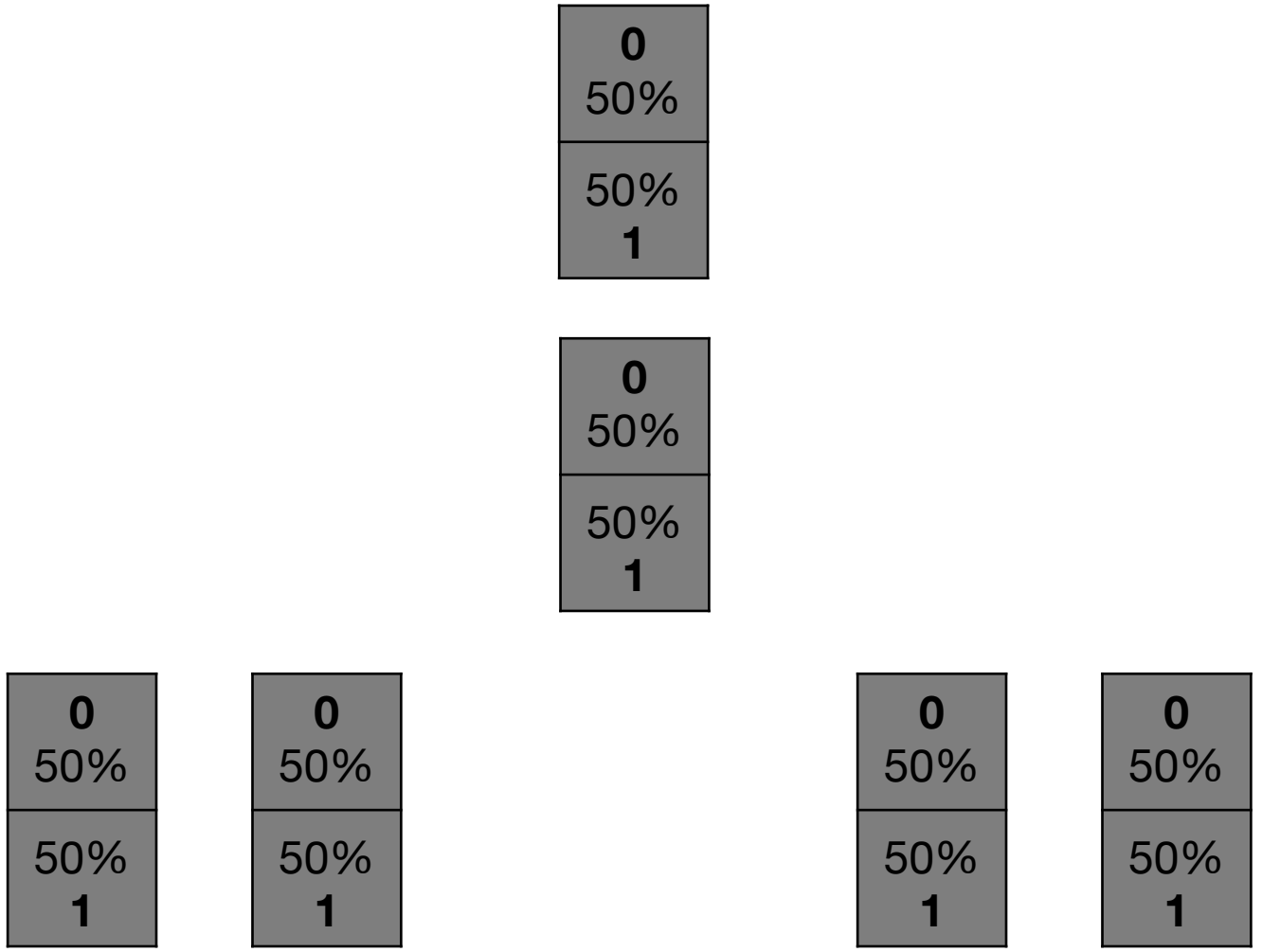
at the end
measure qubits

Gate Model

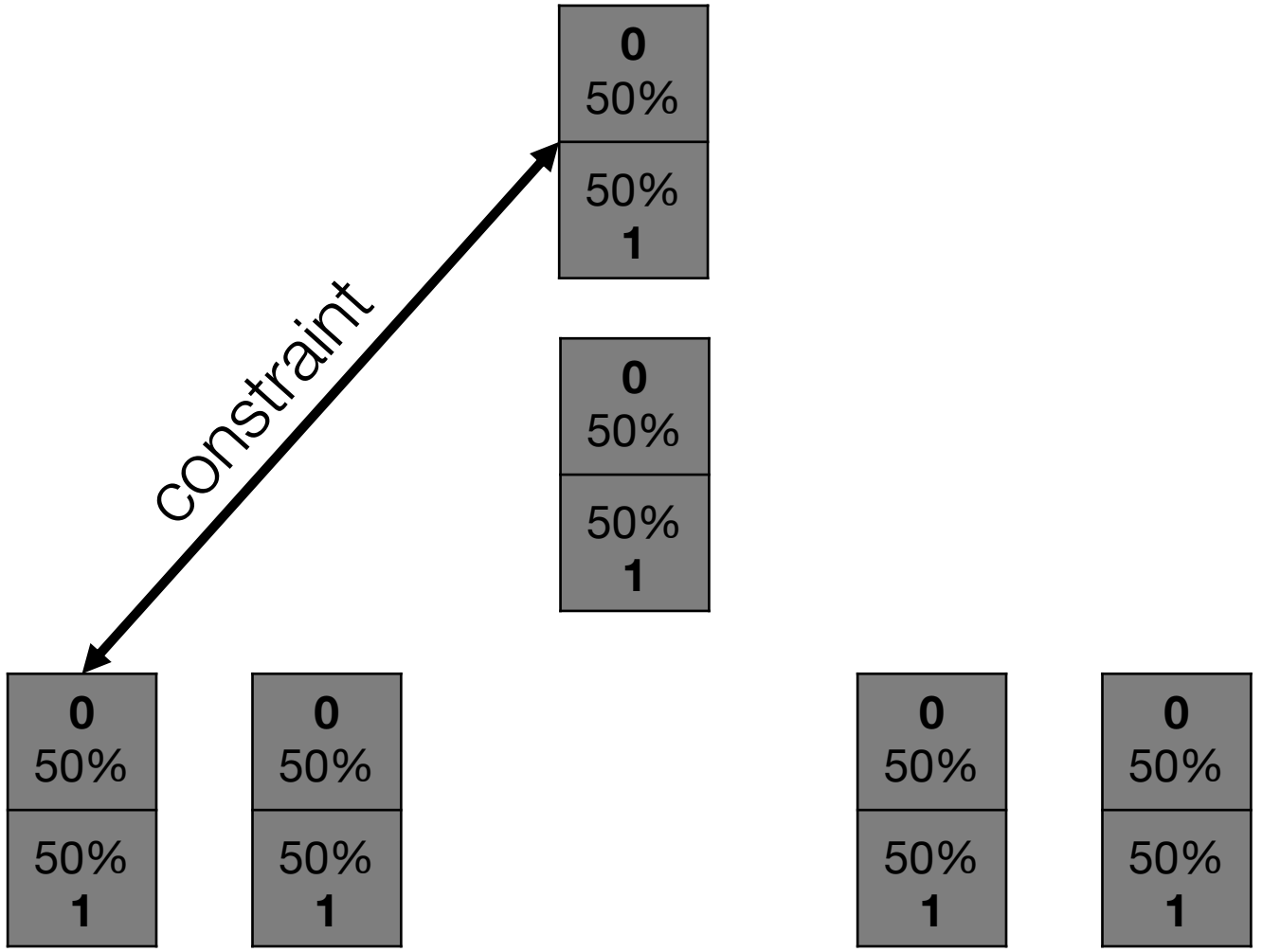
- direct pathway to universal quantum computer
- similar architecture to classical computers
- only protoypes in laboratories
- currently < 100 qubits



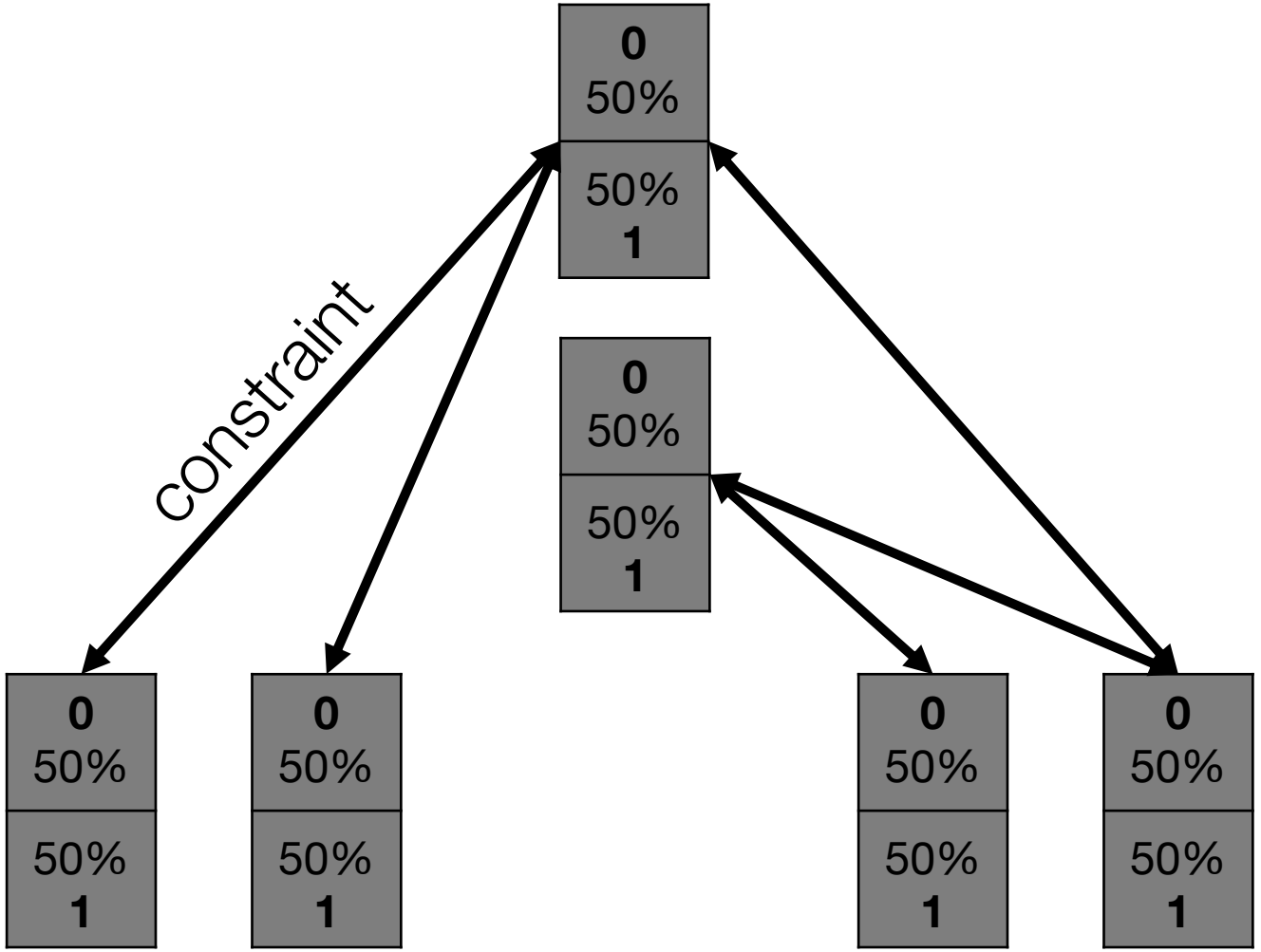
Annealing



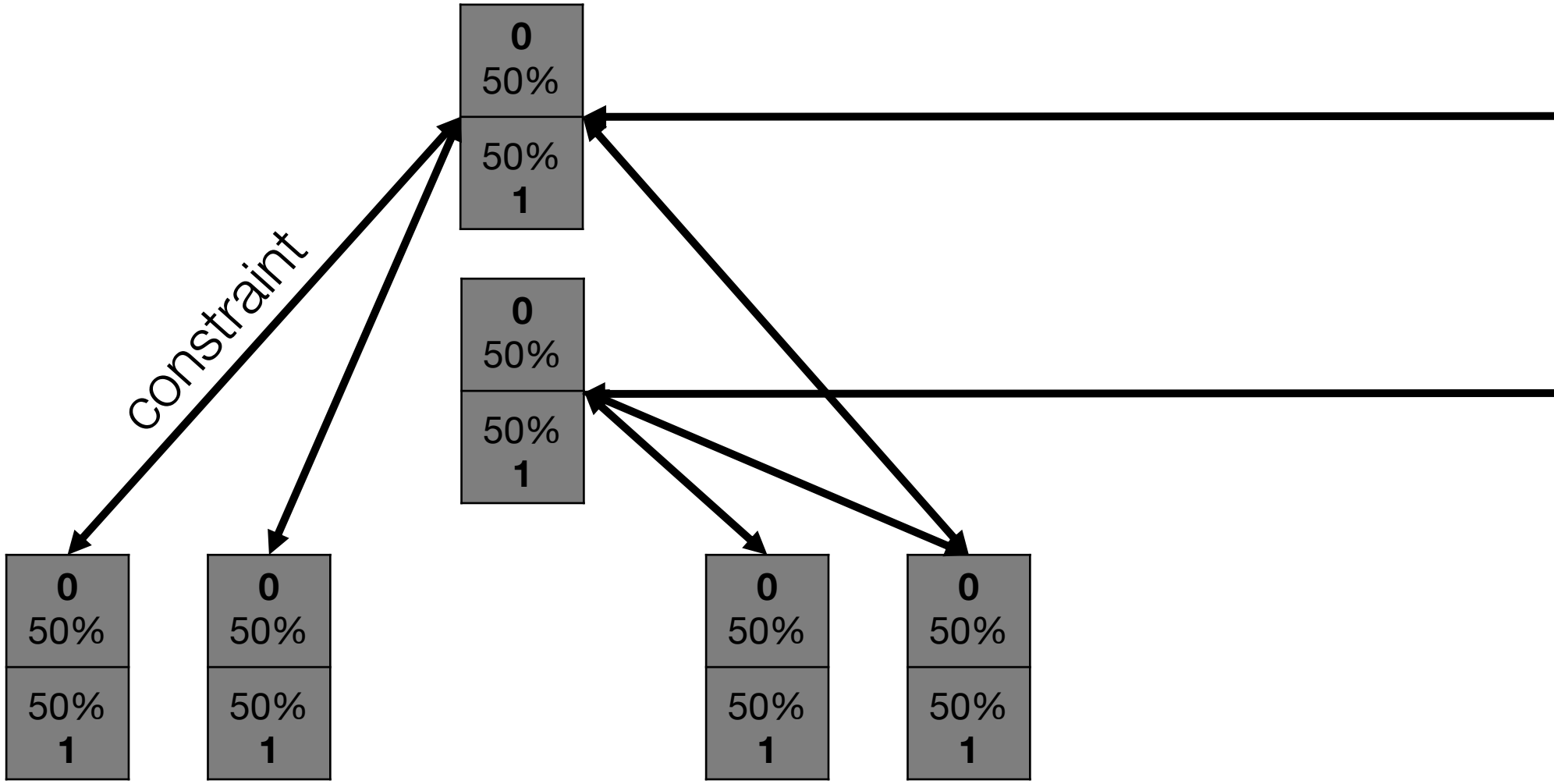
Annealing



Annealing



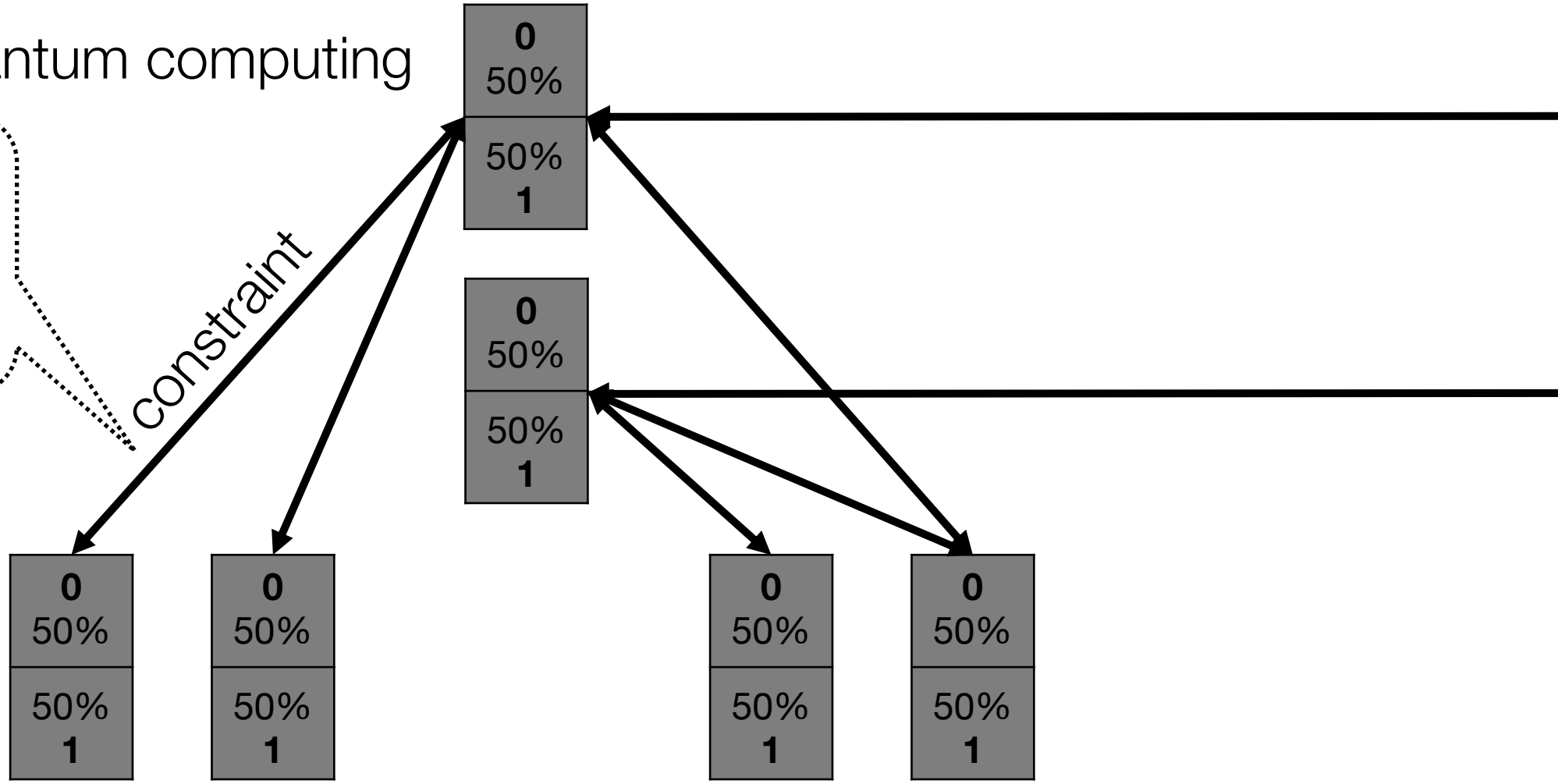
Annealing



Annealing

adiabatic quantum computing

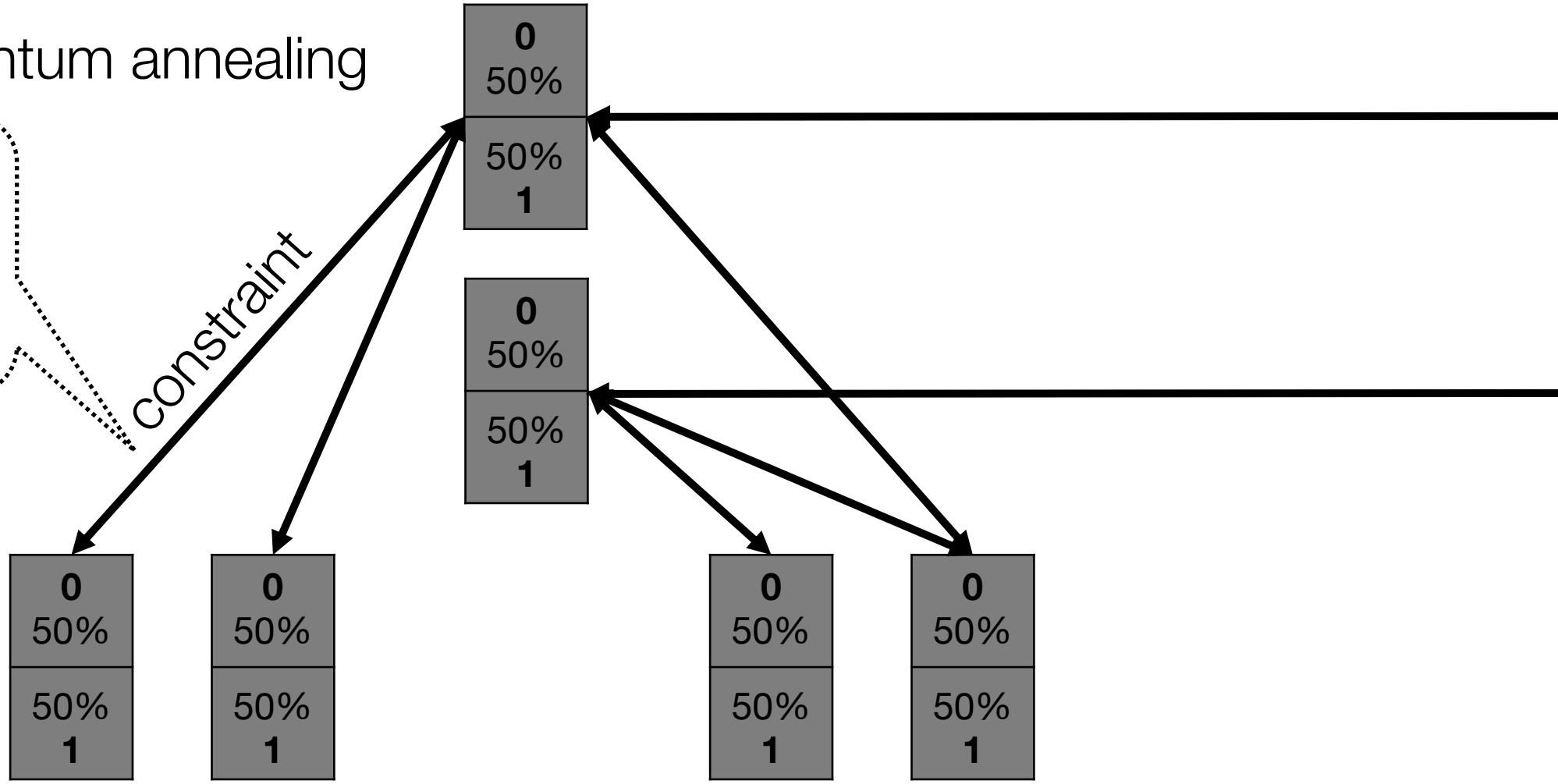
add constraints
infinitely slowly
while adding
no energy



Annealing

practical quantum annealing

add constraints
quite slowly
while adding
almost no energy

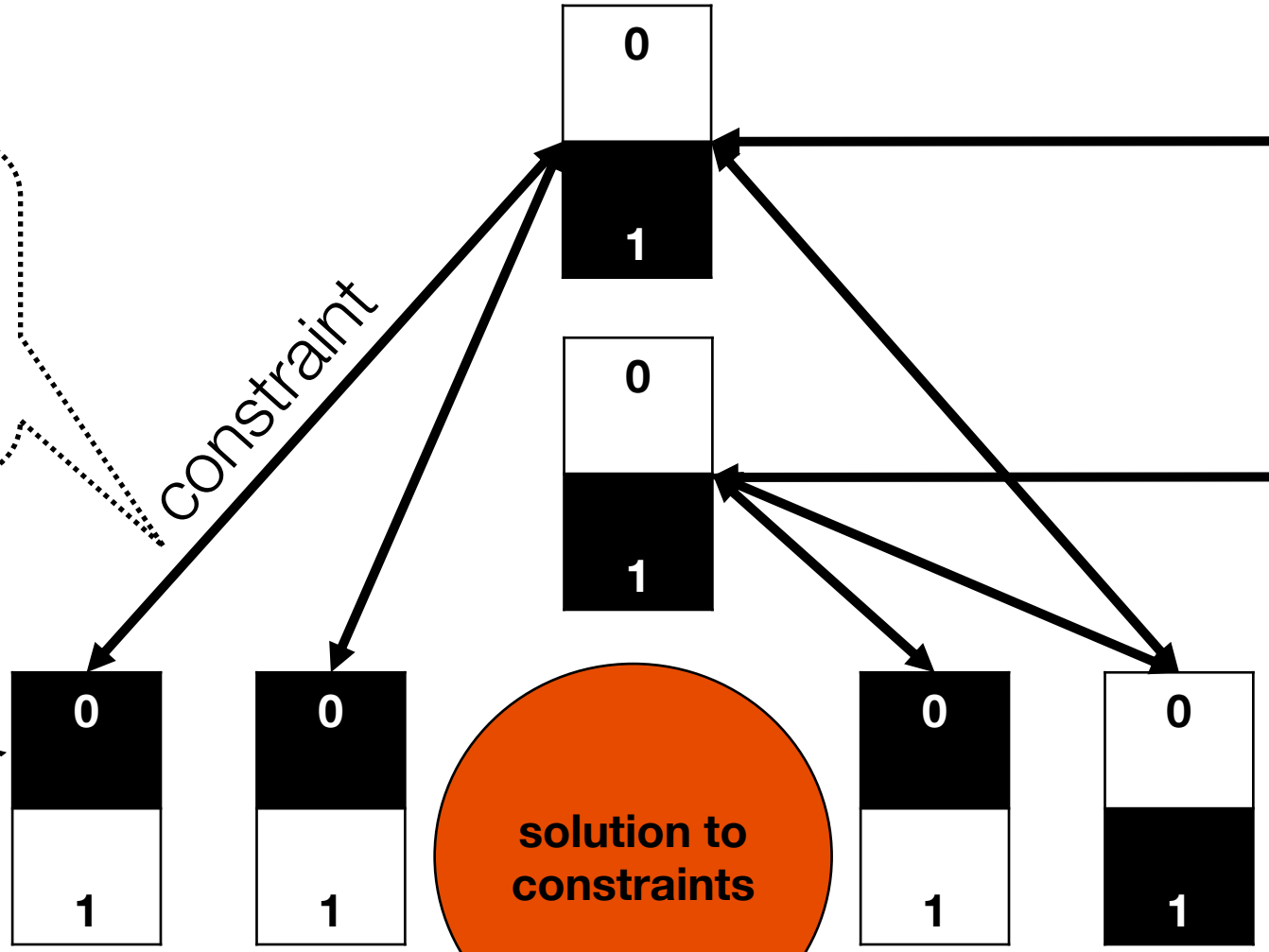


Annealing

add constraints
quite slowly
while adding
almost no energy

constraint

at the end
measure qubits



Annealing

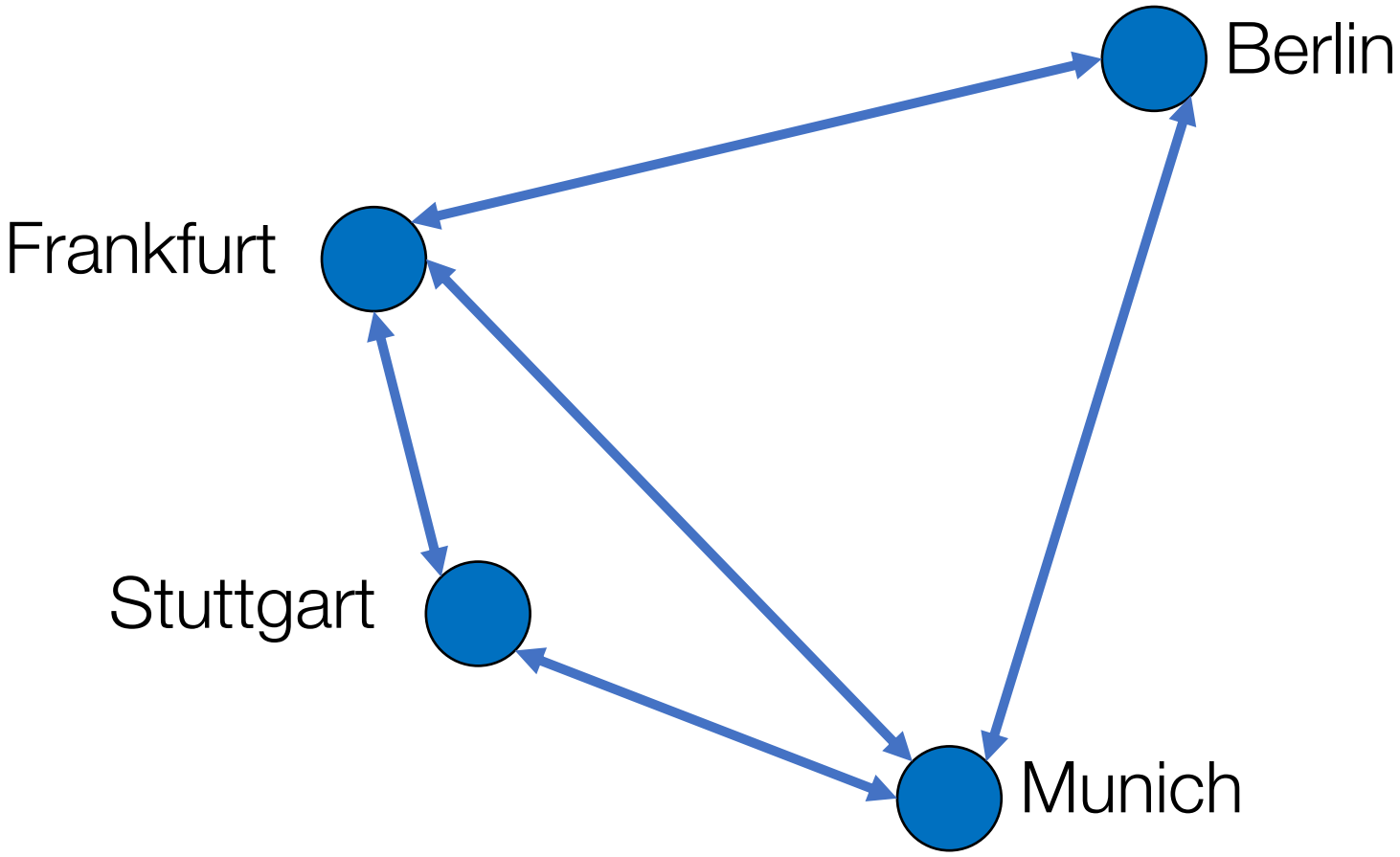
- potentially equally powerful
- archcitecture built for optimization
- available commercially
- currently > 2000 qubits

D:wave
The Quantum Computing Company™

FUJITSU

❸ Optimization Business

Travelling Salesman Problem



Travelling Salesman Problem

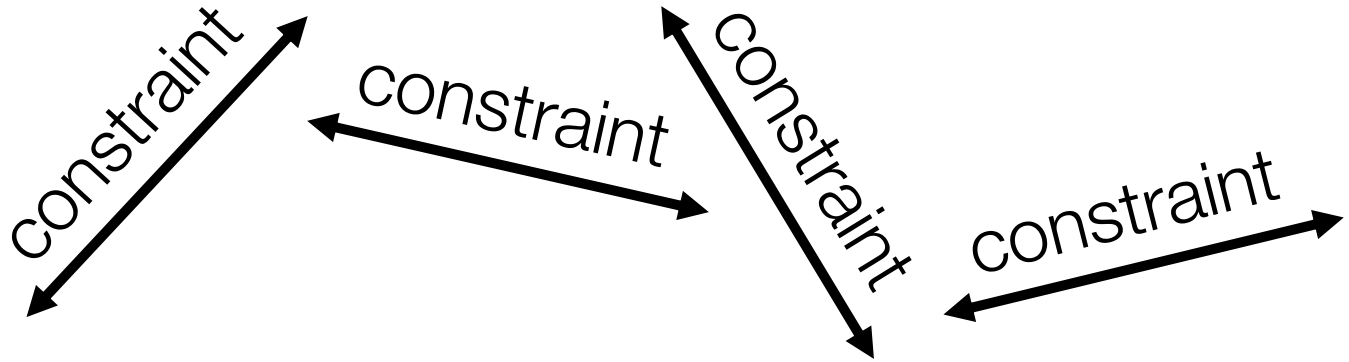
visit Munich first	visit Munich second	visit Munich third	visit Munich fourth	visit Stuttgart first	visit Stuttgart second	visit Stuttgart third	visit Stuttgart fourth	visit Frankfurt first	visit Frankfurt second	visit Frankfurt third	visit Frankfurt fourth	visit Berlin first	visit Berlin second	visit Berlin third	visit Berlin fourth
0 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%	**0** 50%
50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**	50% **1**

Travelling Salesman Problem

visit Munich first	visit Munich second	visit Munich third	visit Munich fourth	visit Stuttgart first	visit Stuttgart second	visit Stuttgart third	visit Stuttgart fourth	visit Frankfurt first	visit Frankfurt second	visit Frankfurt third	visit Frankfurt fourth	visit Berlin first	visit Berlin second	visit Berlin third	visit Berlin fourth
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

How to Optimize on a Quantum Annealer

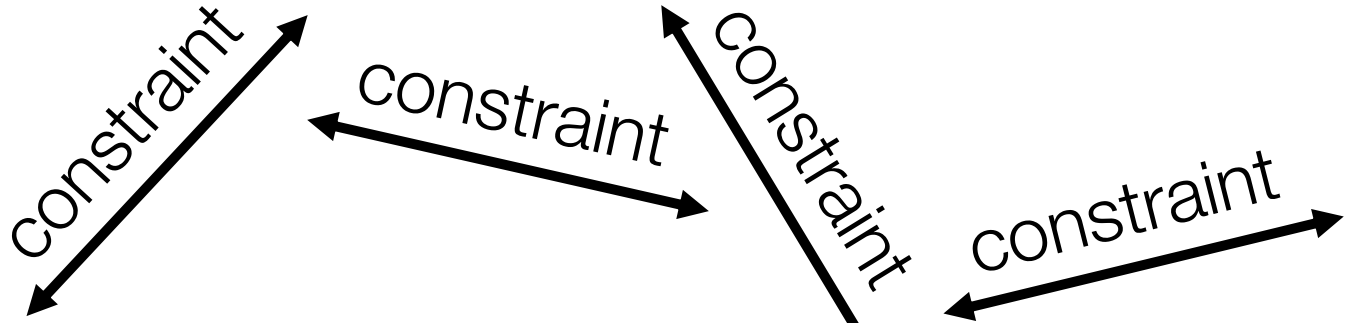
- translate problem into a set of suitable constraints



= QUBO

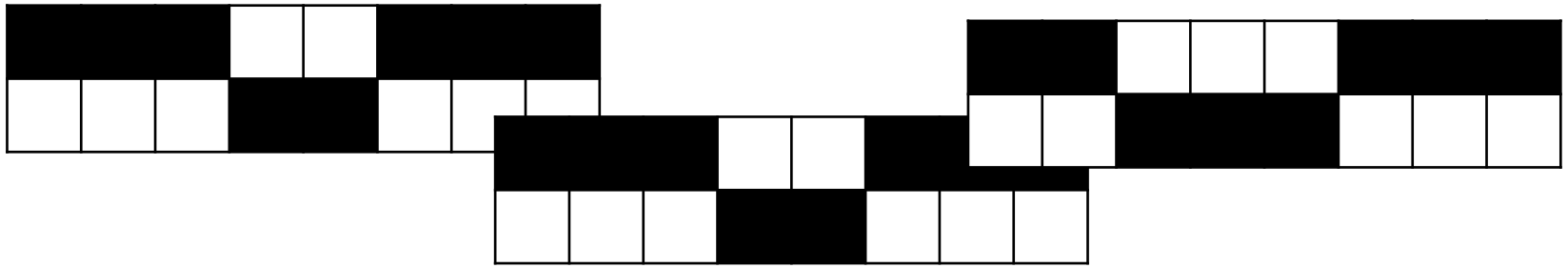
How to Optimize on a Quantum Annealer

- translate problem into a set of suitable constraints



= QUBO

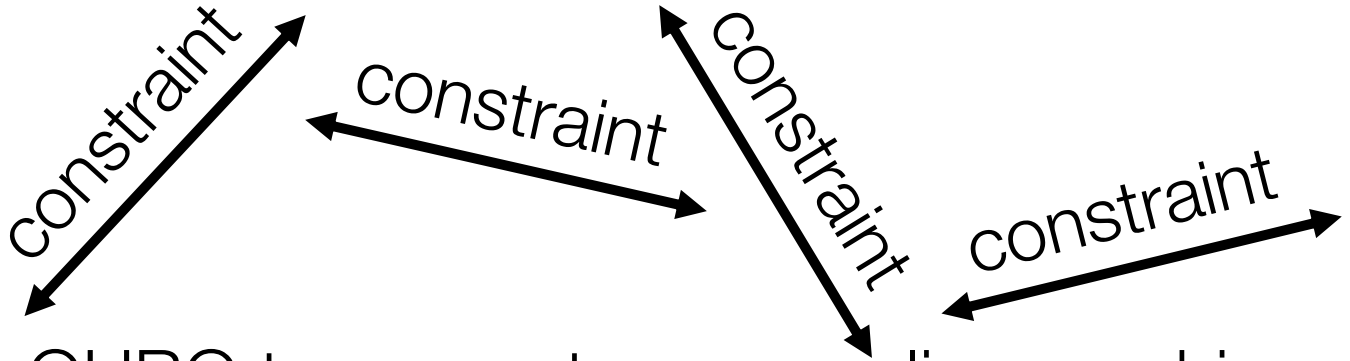
- transfer QUBO to a quantum annealing machine



= prob. results

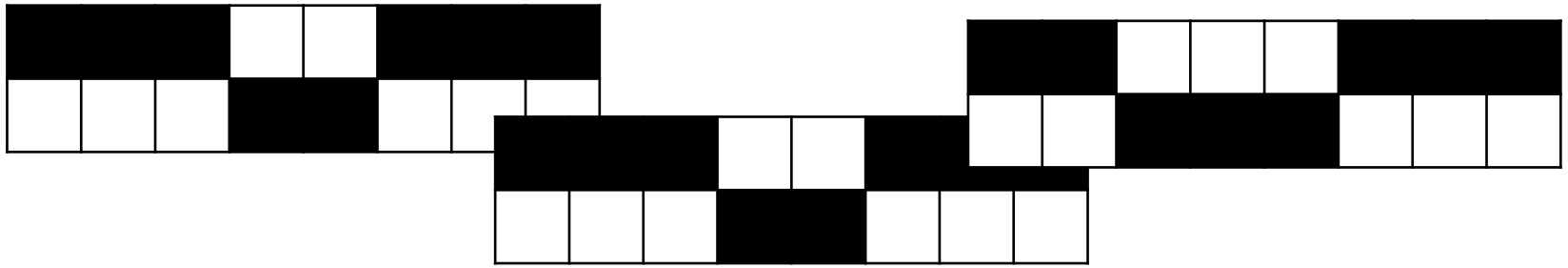
How to Optimize on a Quantum Annealer

- translate problem into a set of suitable constraints



= QUBO

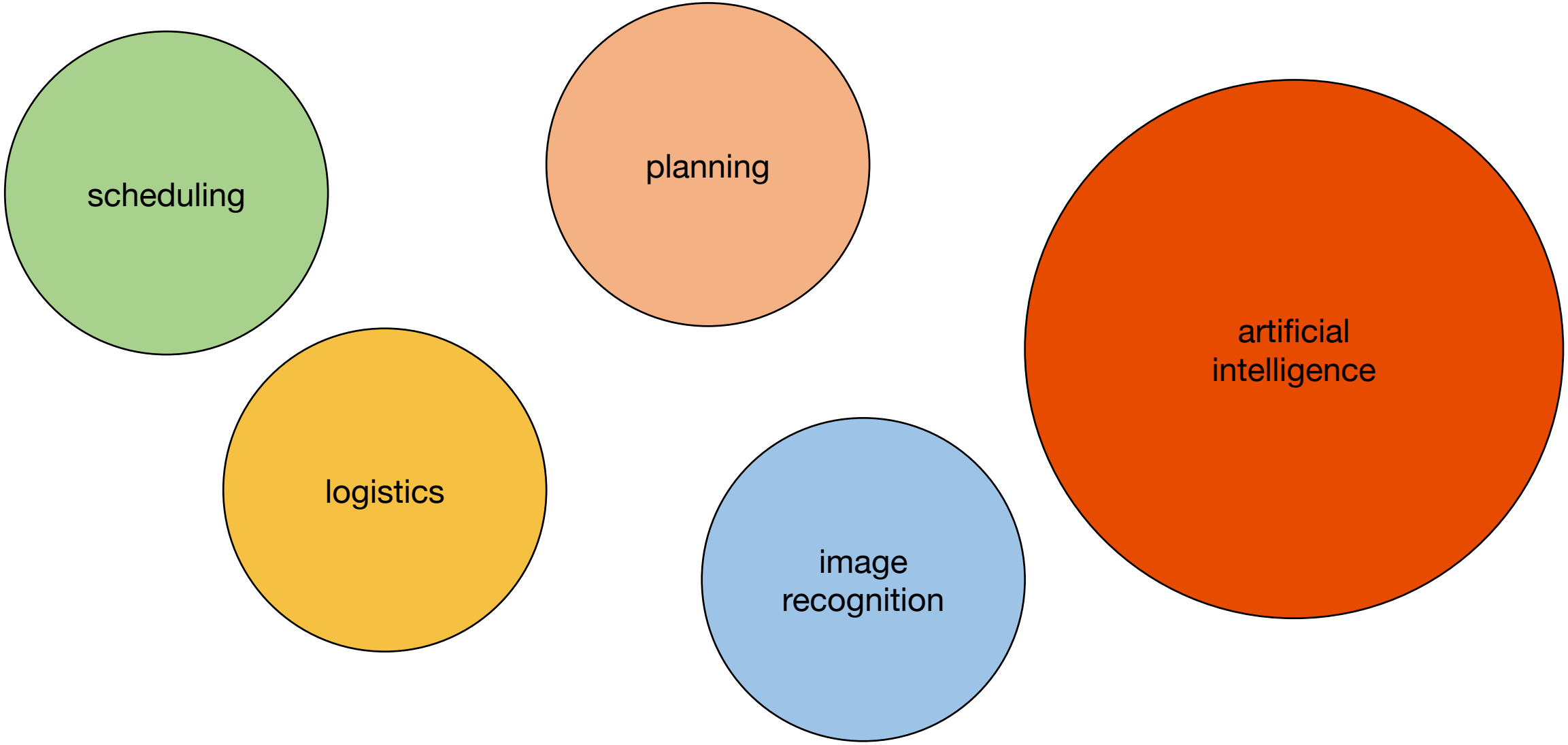
- transfer QUBO to a quantum annealing machine



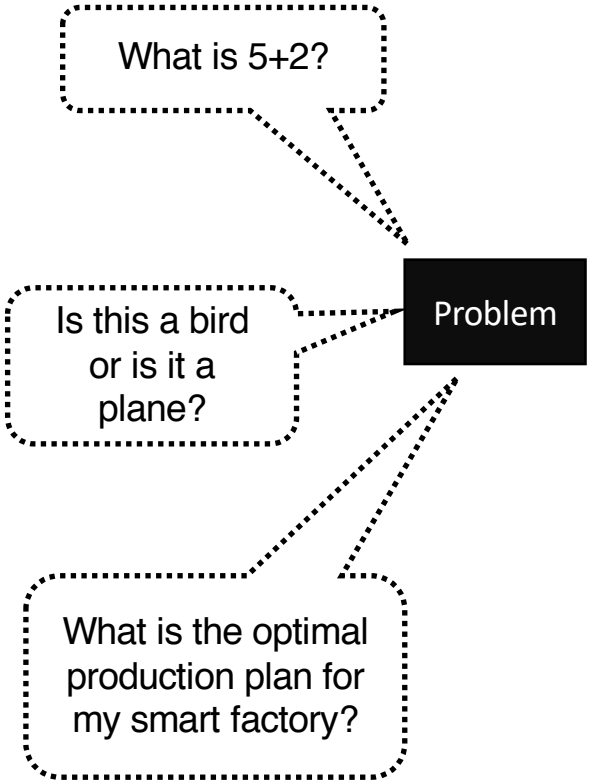
= prob. results

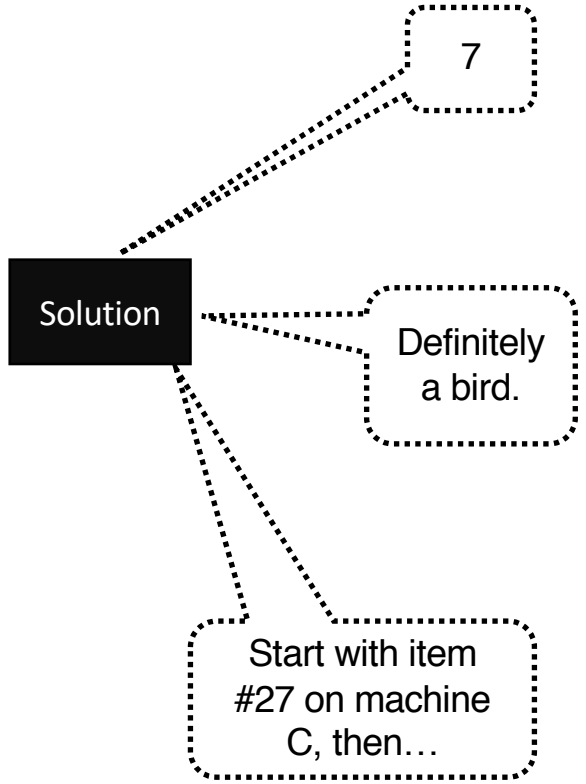
- analyze probabilistic results to make informed decision

Optimization Problems

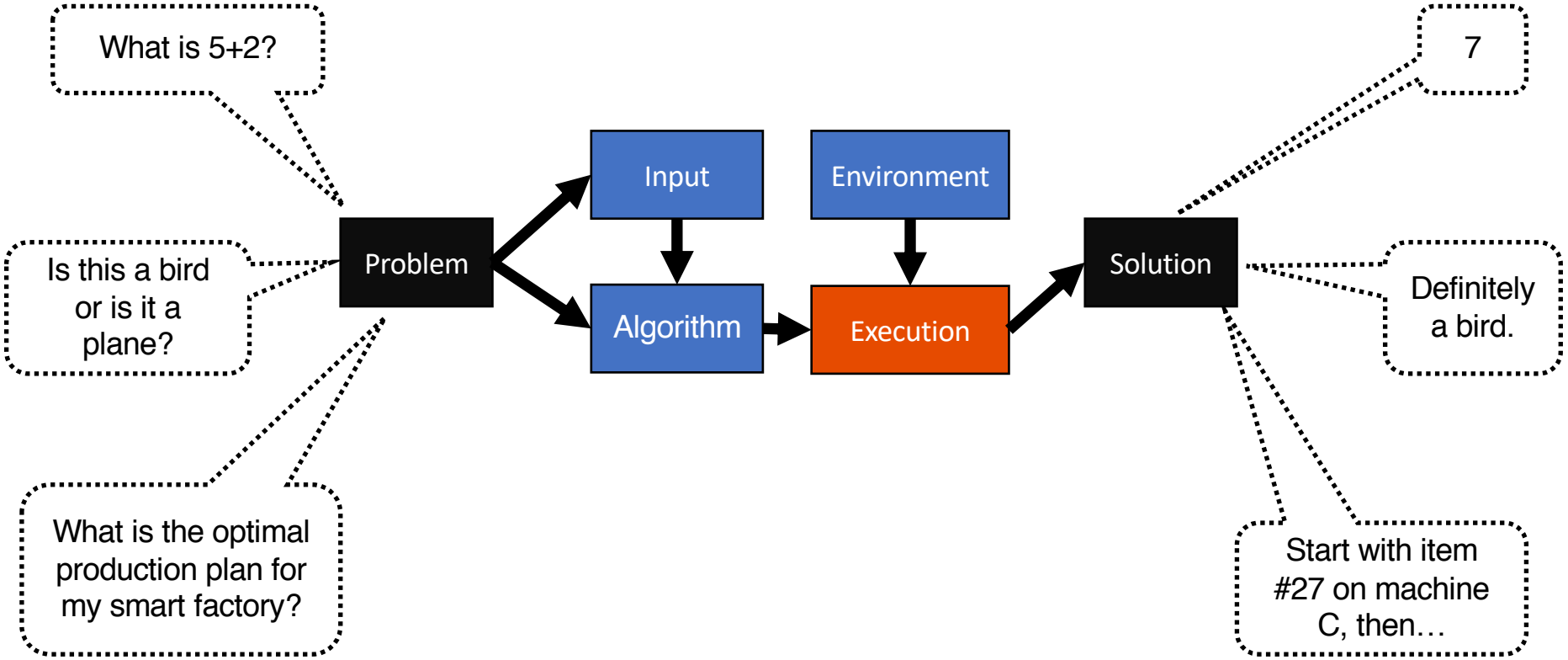


What does AI do?

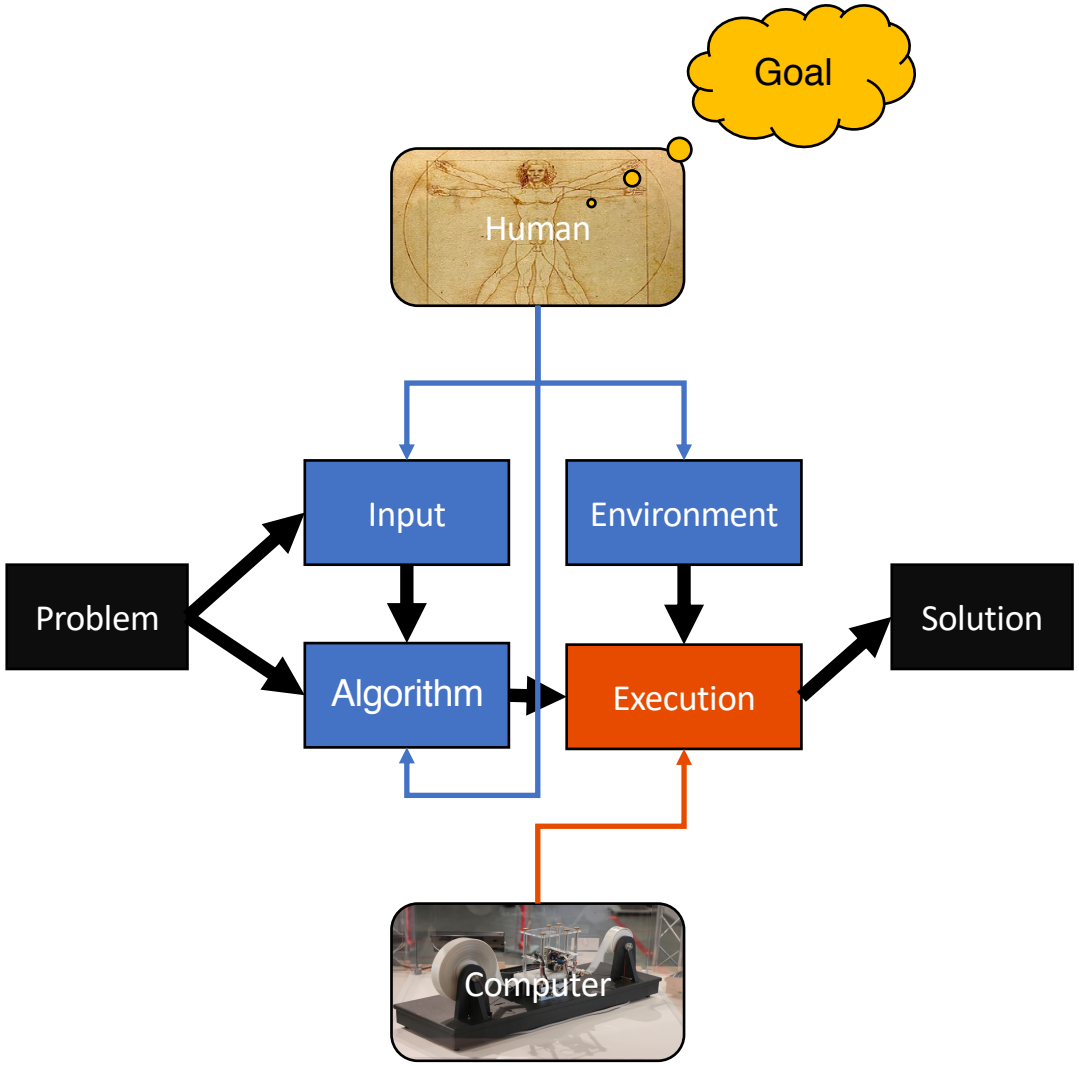




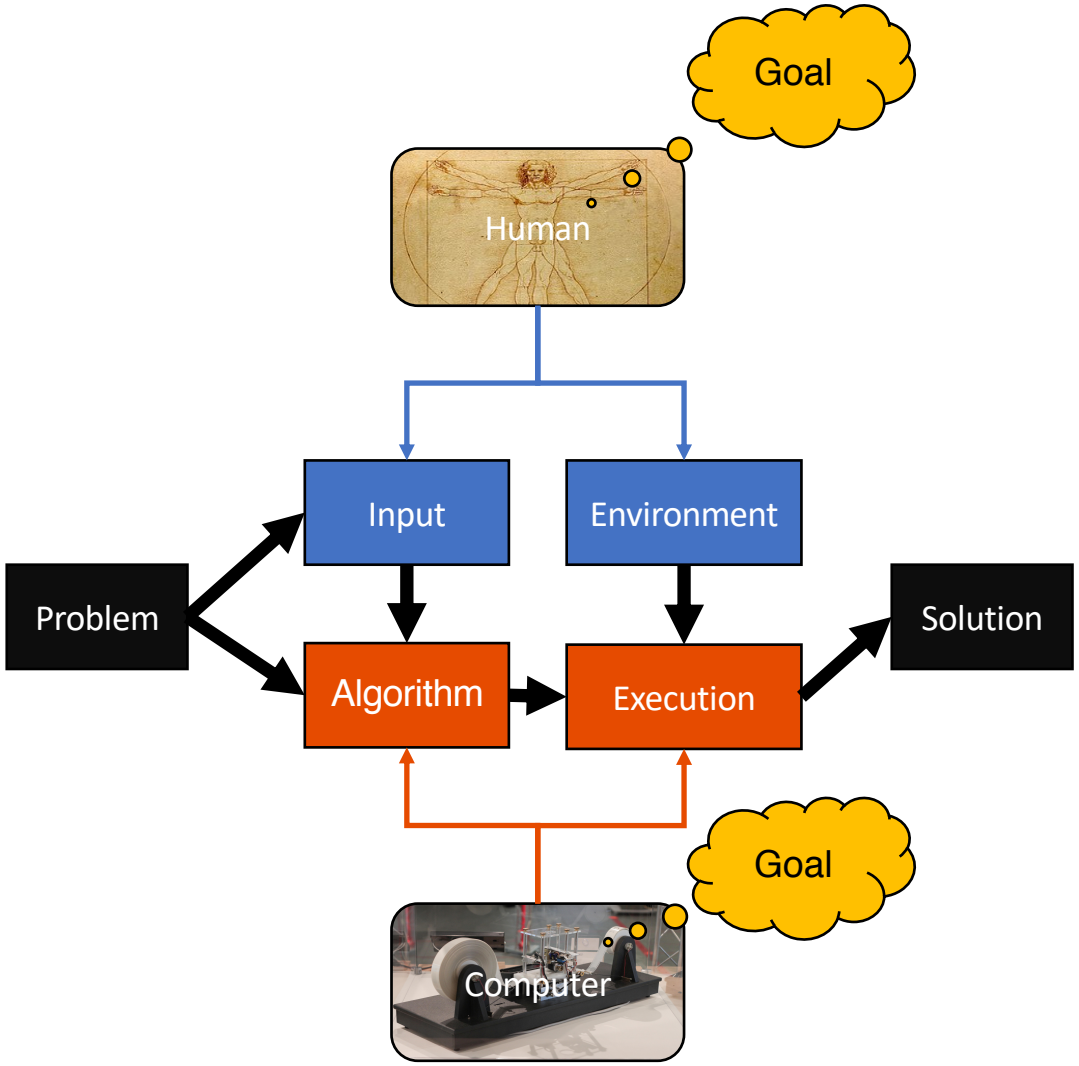
What does AI do?



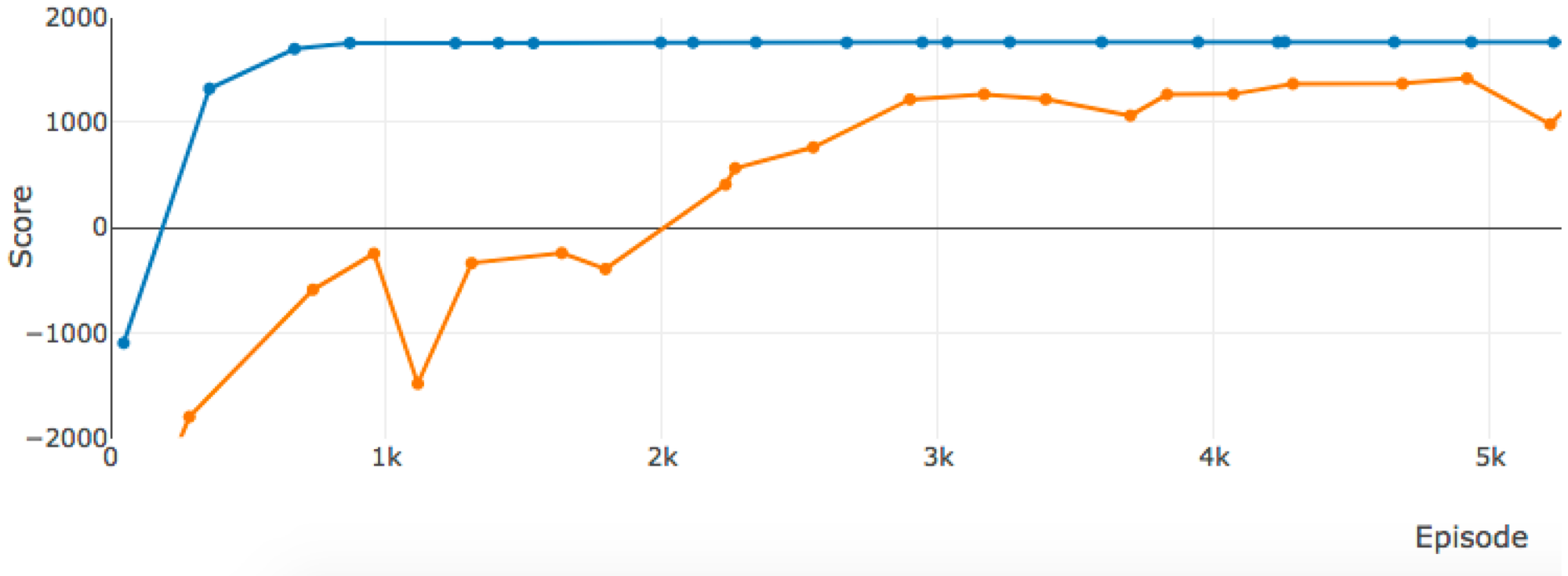
What does AI do?



What does AI do?



Training as Optimization



AI and Quantum Computing

- starts from random sample
- probabilistic processes, statistical evaluation
- computationally expensive, already running specialized hardware

AI: The Major Challenges

- Multi-Agent Coordination

  Systems are open, not closed.

- Mission Criticality

  Systems are made out of processes, not results.

- Migration and Change

  System development is eternal, never finished.

AI: The Major Challenges

- Multi-Agent Coordination

Systems are open, not closed.

more computing power

- Mission Criticality

Systems are made out of processes, not results.

more computing power

- Migration and Change

System development is eternal, never finished.

more computing power

❹ Opportunities

Asymmetric Cryptography

Shor‘s Algorithm

- runs on gate model quantum computer
- prime factorization in polynomial time
- would break RSA

Peter Shor

www-math.mit.edu/~shor

Asymmetric Cryptography

Shor‘s Algorithm

- runs on gate model quantum computer
- prime factorization in polynomial time
- would break RSA

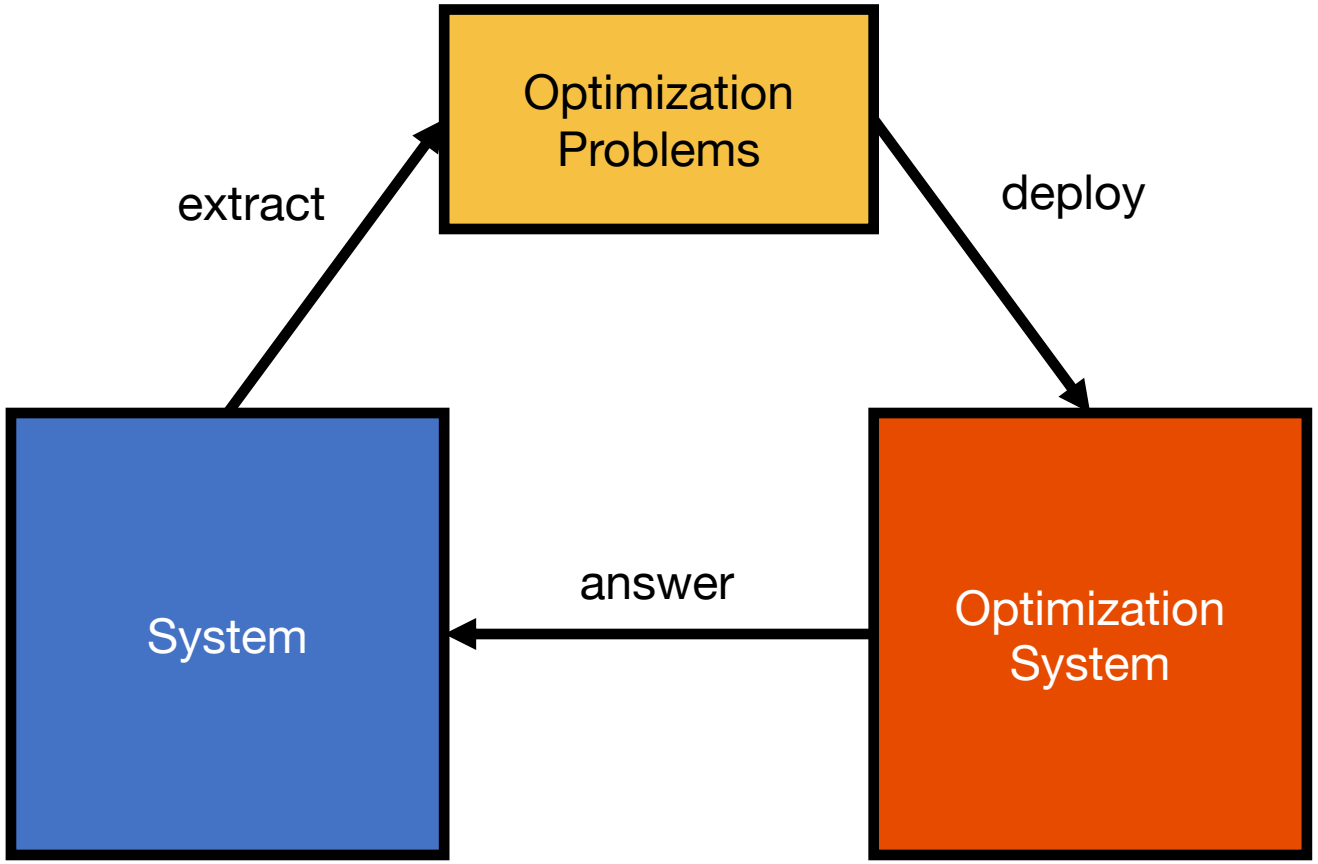
Pointers

- given unresolved scalability issues, larger keys might buy us time
- post-quantum cryptography

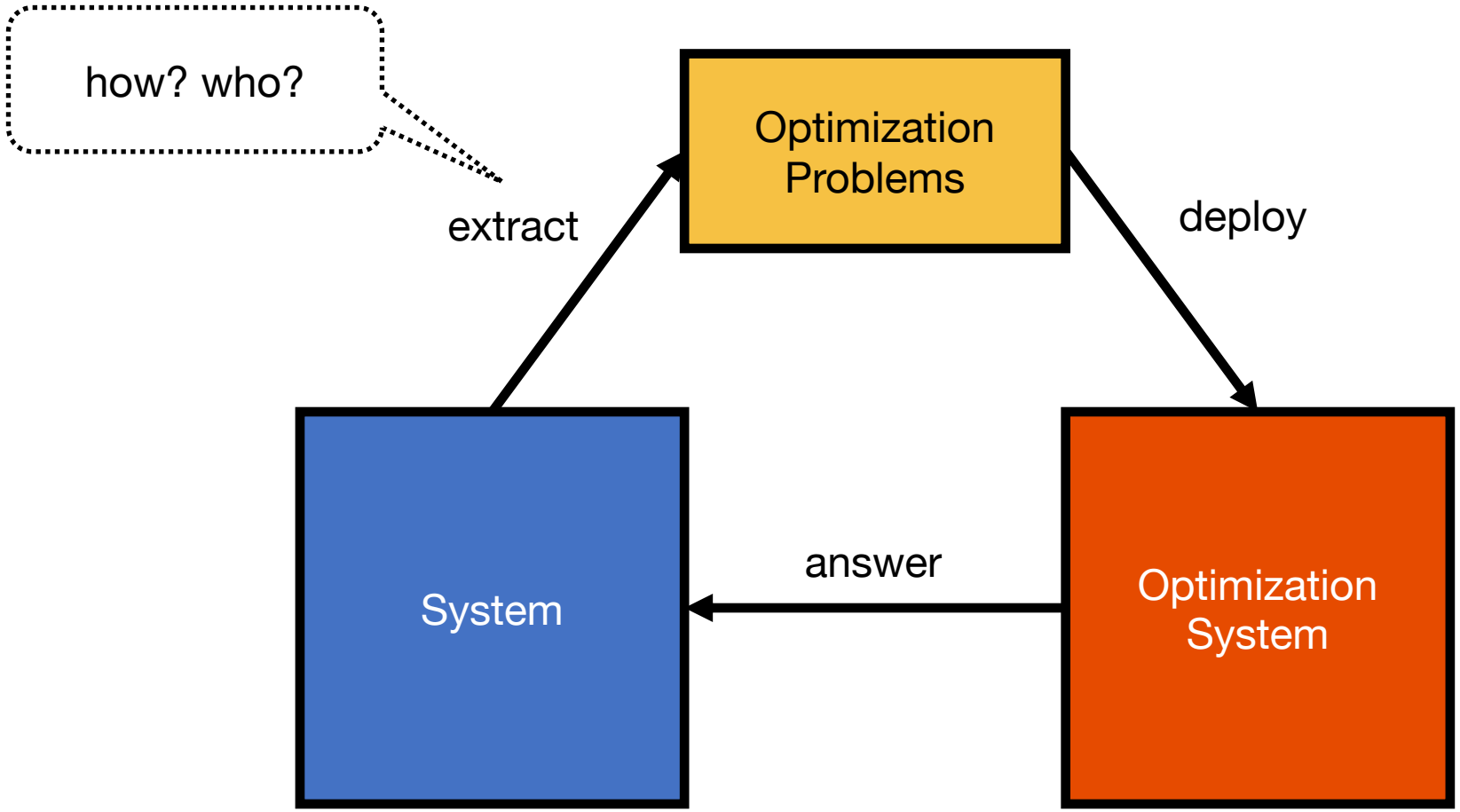
Peter Shor

www-math.mit.edu/~shor

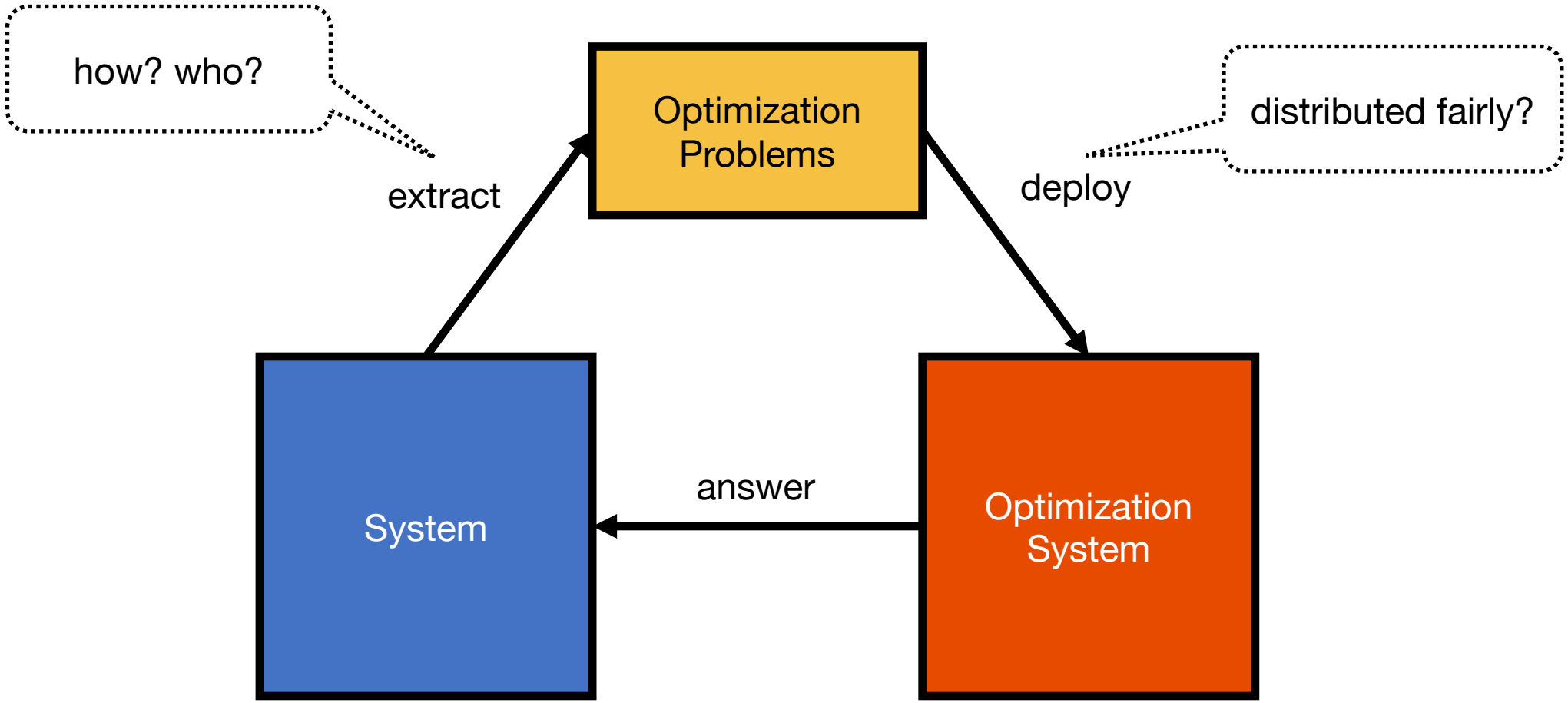
Distributed Infrastructure



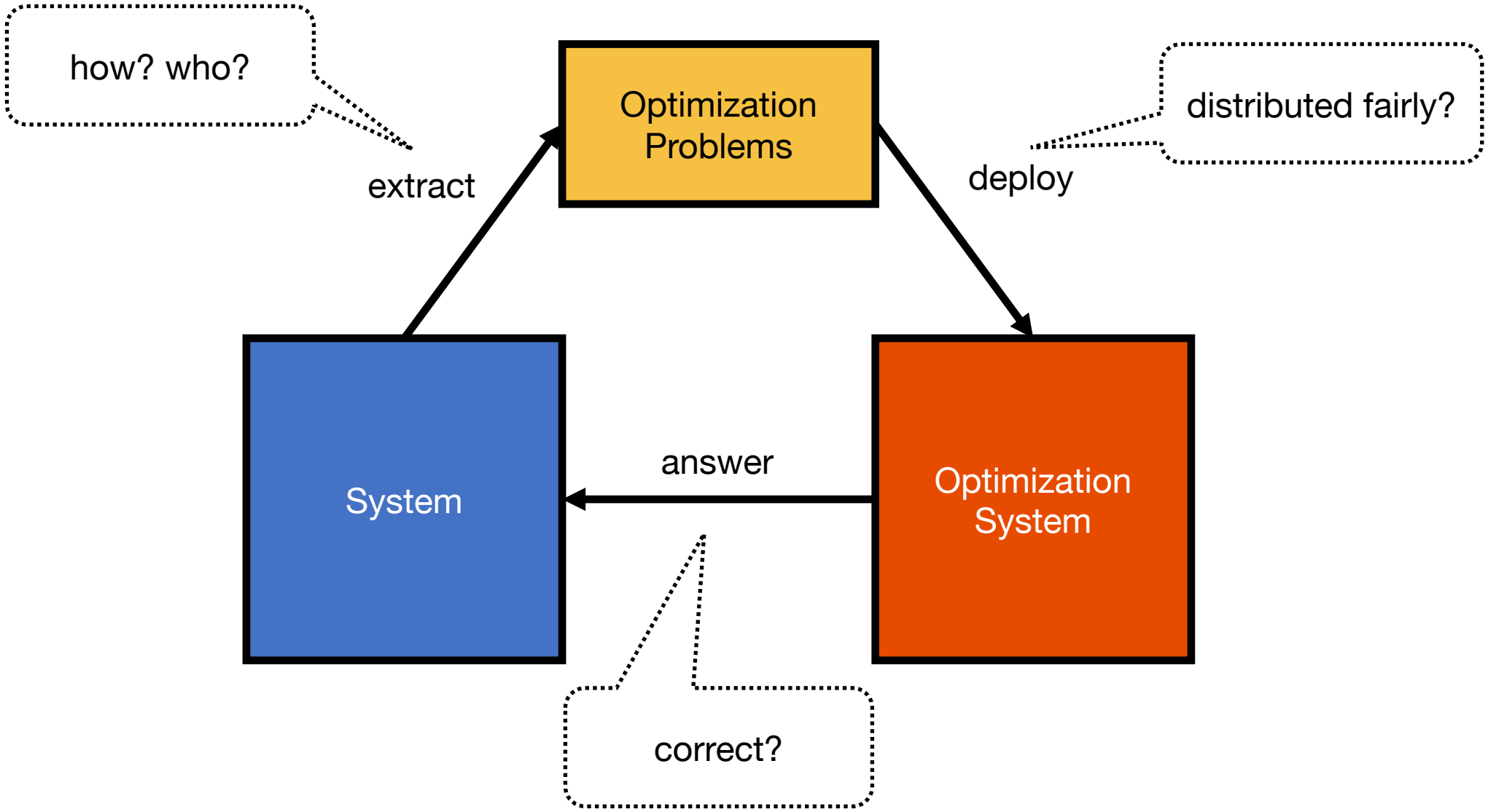
Distributed Infrastructure



Distributed Infrastructure



Distributed Infrastructure



A Quick Quantum Conclusion

- Quantum Computing promises new computing power when exposing central (optimization) tasks of your business.

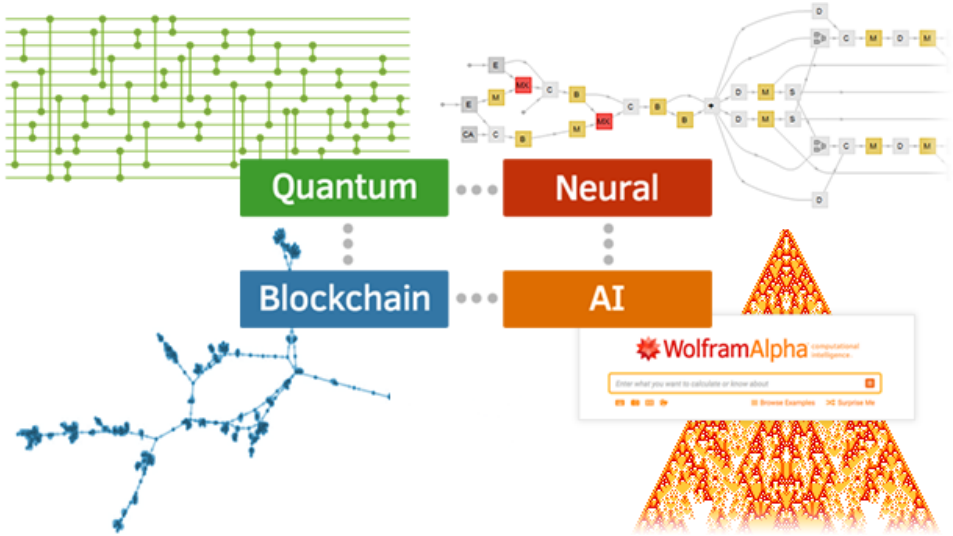
- Exposing your business‘s optimization problems may require a new approach to security.

- Artificial Intelligence itself may lend itself to improve the results of certain security tasks.

Link: Quantum Neural Blockchain AI

all these currently relevant *buzzwords* are…

- derived from irreversible computation
- based on probabilistic processes
- to some extent compatible…?



Stephen Wolfram

www.stephenwolfram.com

http://blog.stephenwolfram.com/2018/04/buzzword-convergence-making-sense-of-quantum-neural-blockchain-ai/

Thank You!

Thomas Gabor
Quantum Applications and Research Laboratory
Mobile and Distributed Systems Group
LMU Munich