ISARA

A QUANTUM OF SAFETY

ROOTING TRUST IN A QUANTUM WORLD

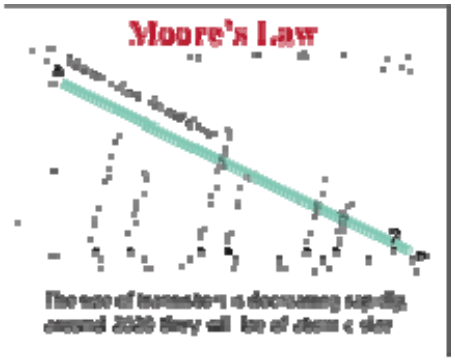
Mark Pecen, COO

June 12, 2018

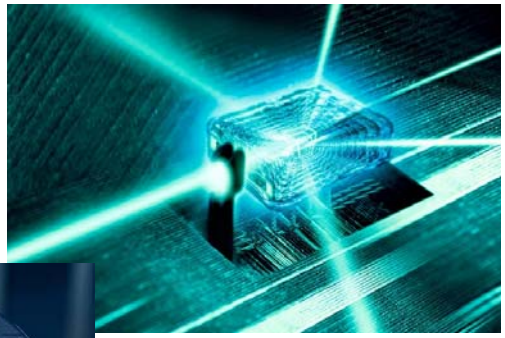
Agenda

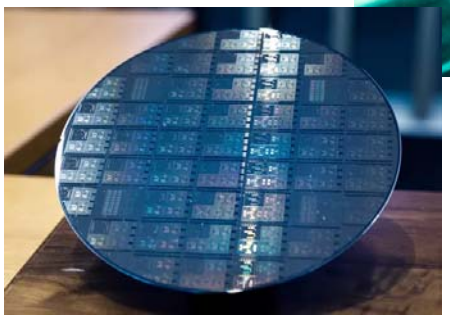
1. About quantum computing
2. The impact of quantum computing on security
3. Industry response to roots of trust issues

Quantum computing is the marriage of...

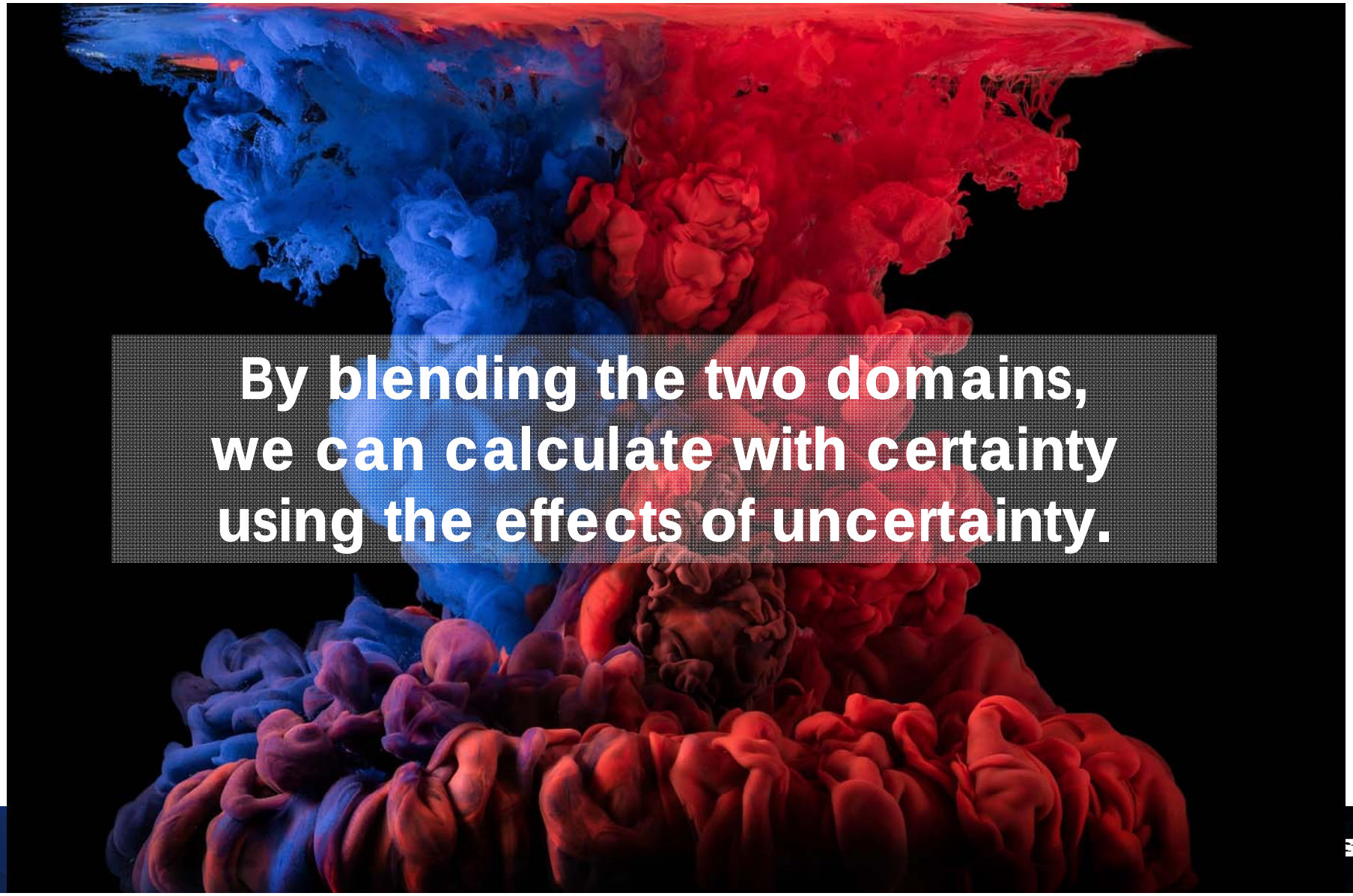


INFORMATION THEORY





QUANTUM MECHANICS


By blending the two domains,
we can calculate with certainty
using the effects of uncertainty.

A classical bit is either 1 or 0

- A classical bit is like a light bulb that's either on or off
- In a standard Von Neumann processor, we get one set of states per clock tick

0

"Off"

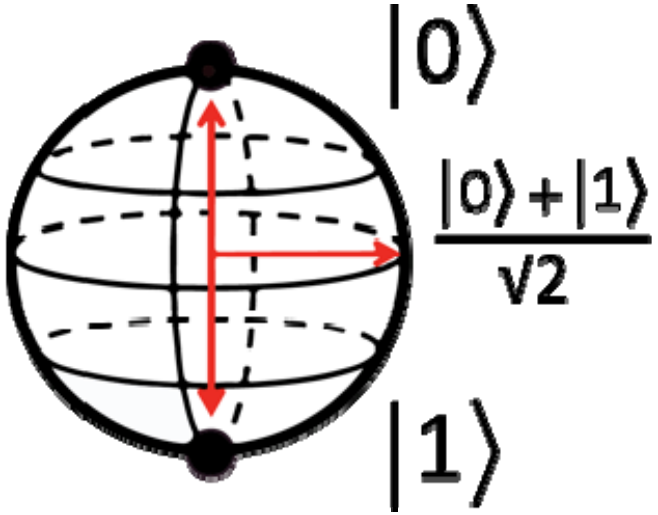
or

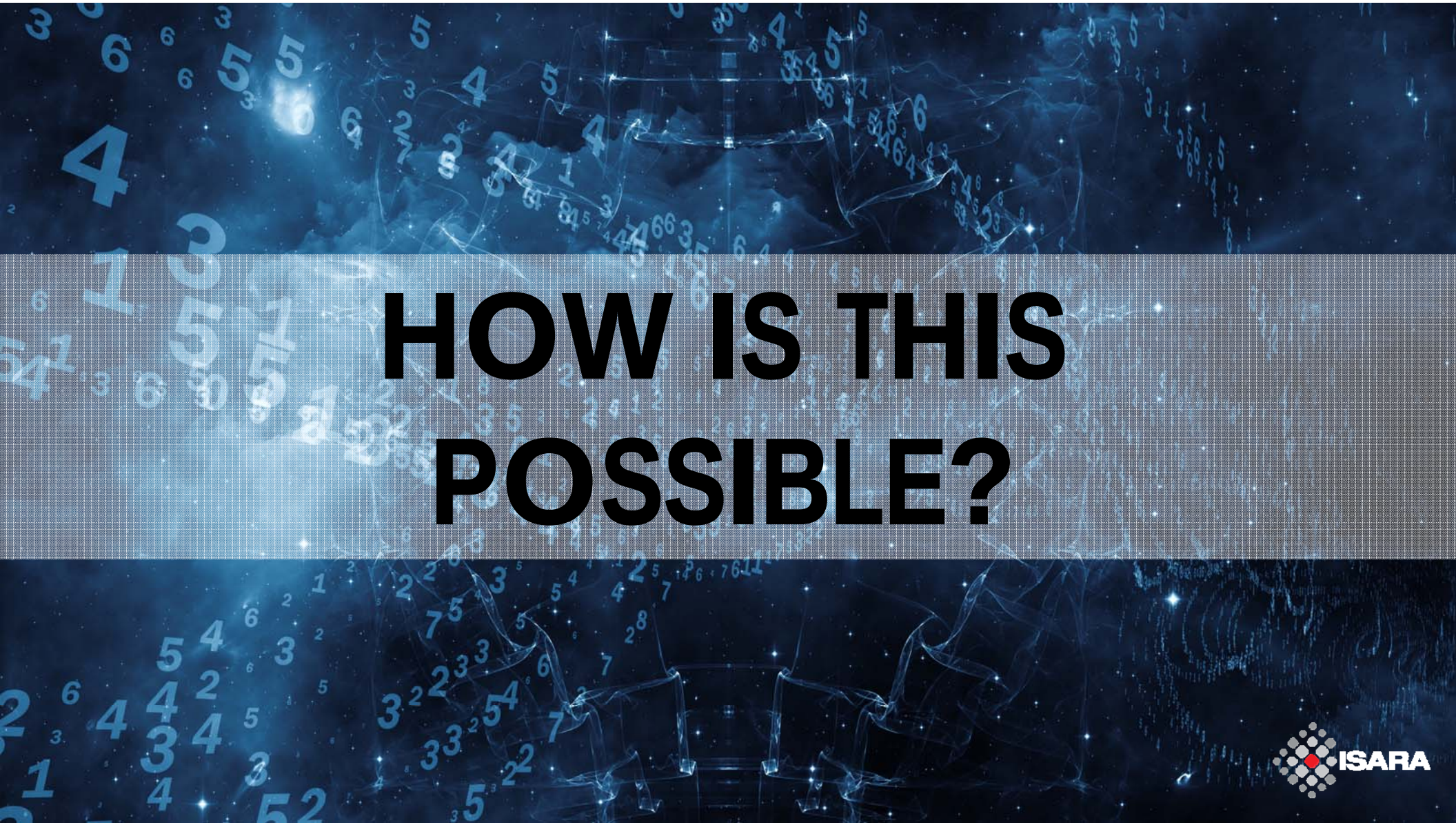
1

"On"

A quantum bit (qubit) is different

- A quantum bit can exist in **multiple states simultaneously**, like a light bulb that's on and off at the same time
- Number of states = 2^N, where N = number of qubits
- Example: A system with 16 qubits can be in 2^{16} = **65,536** states at once!

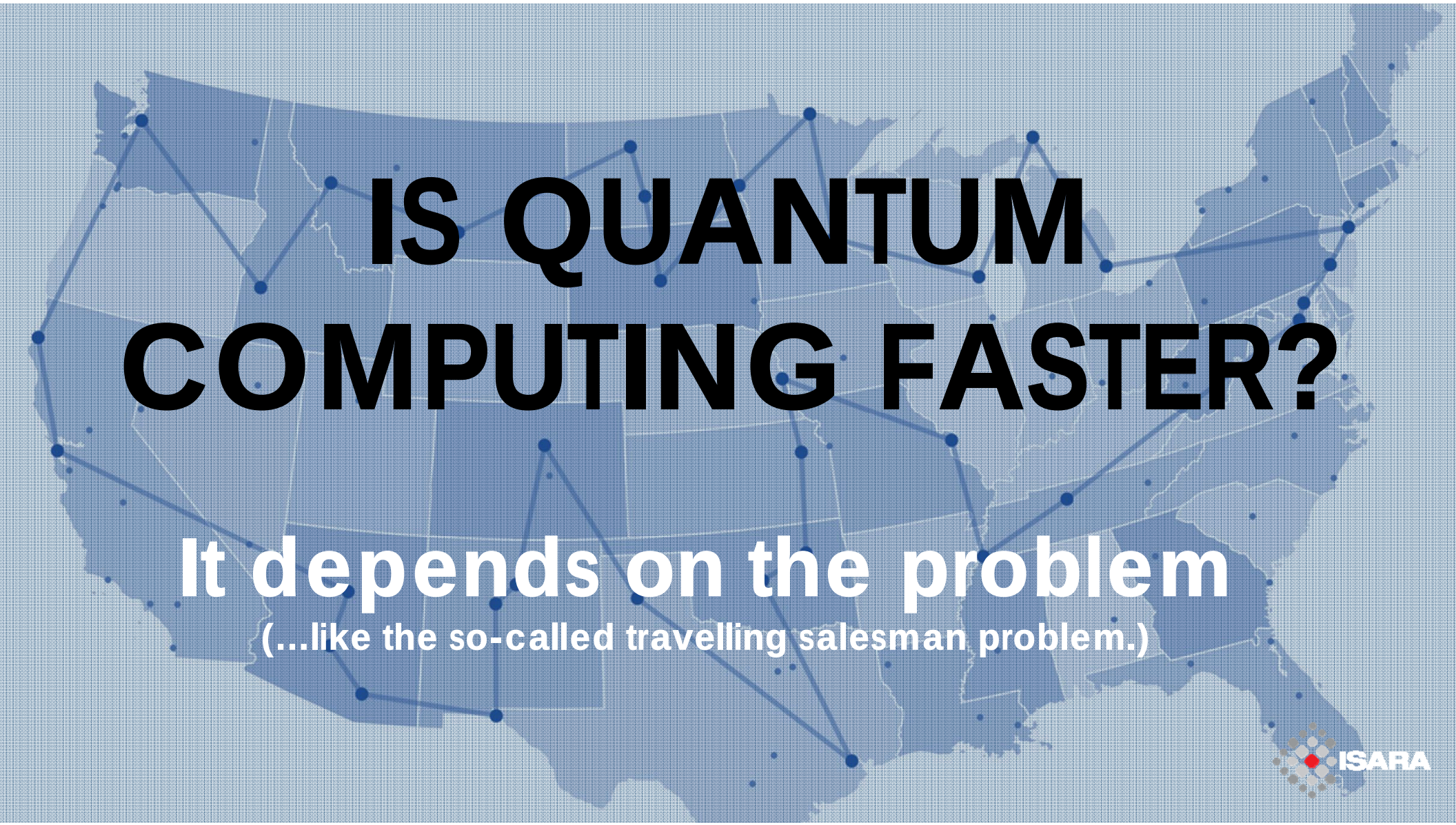



HOW IS THIS POSSIBLE?
ISARA

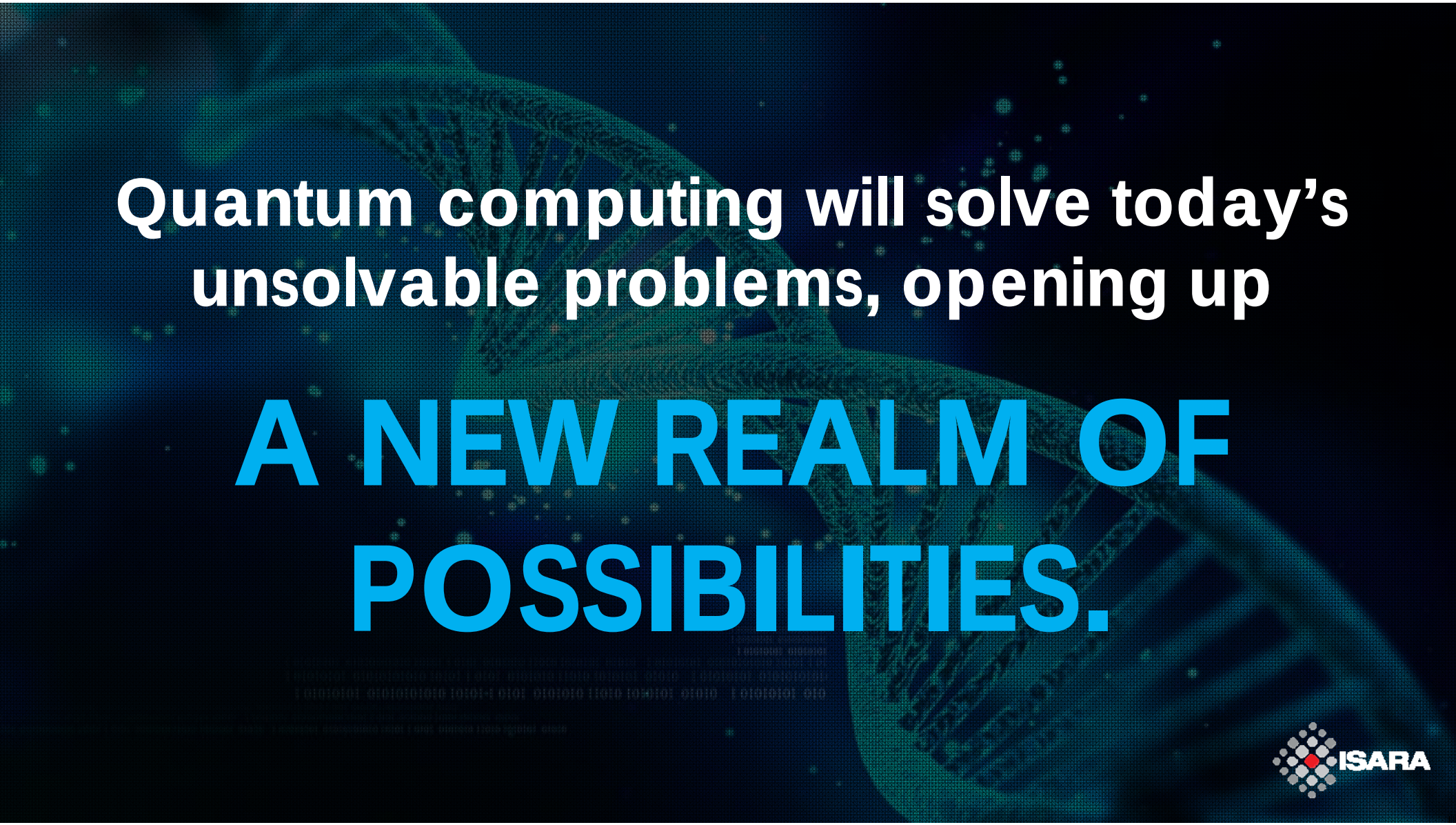
There's a better question…

How can we use this interesting property of being in many states at once to solve important problems ?

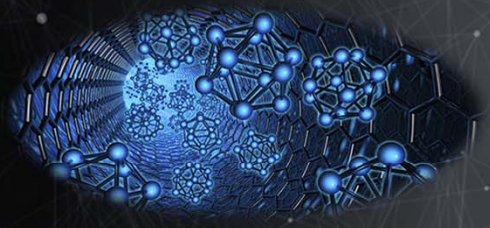
Because the quantum computer lends itself to solving certain types of problems extremely easily.


IS QUANTUM
COMPUTING FASTER?
It depends on the problem
(…like the so-called travelling salesman problem.)
ISARA


THE QUANTUM
RACE IS ON
Microsoft
Google
rigetti
D-Wave
The Quantum Computing Company™
IBM
intel
ISARA


Quantum computing will solve today's unsolvable problems, opening up
A NEW REALM OF POSSIBILITIES.
ISARA

QUANTUM COMPUTING
WILL REVOLUTIONIZE MANY INDUSTRIES



MATERIAL DESIGN

CRYPTOGRAPHY

BIG DATA

WEATHER SERVICES

CHEMISTRY

MACHINE LEARNING

ISARA


THE CHALLENGE
Quantum computing will break today's public key encryption standards.
ISARA

EFFECT ON TODAY'S CRYPTOGRAPHY

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

ISARA

IMPACT ON SECURE COMMINICATIONS

Secure Communication Protocol

Handshake | **Data Exchange**

Shor's algorithm **breaks** current public-key algorithms

Authentication
Key Establishment

Symmetric Encryption

AES 256 → AES 128

Grover's algorithm **reduces** the effective symmetric key size to half

IMPACT ON SOFTWARE UPDATES

Embed a Root of Trust at Manufacture

- Create software update
- Digitally sign the update

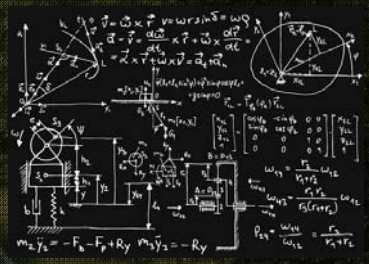
Digital Signature | **Software Update**

- Receive software update
- Verify ECDSA or RSA digital signature → **broken using Shor's algorithm**
- Apply software update

ISARA

PATHWAYS TO QUANTUM SAFETY

Quantum Key Distribution



Quantum-Safe Cryptography

ISARA

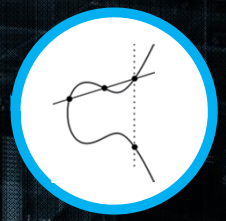
THE "NEW" MATH

Hash-based

Code-based

Lattice-based

Multivariate-based

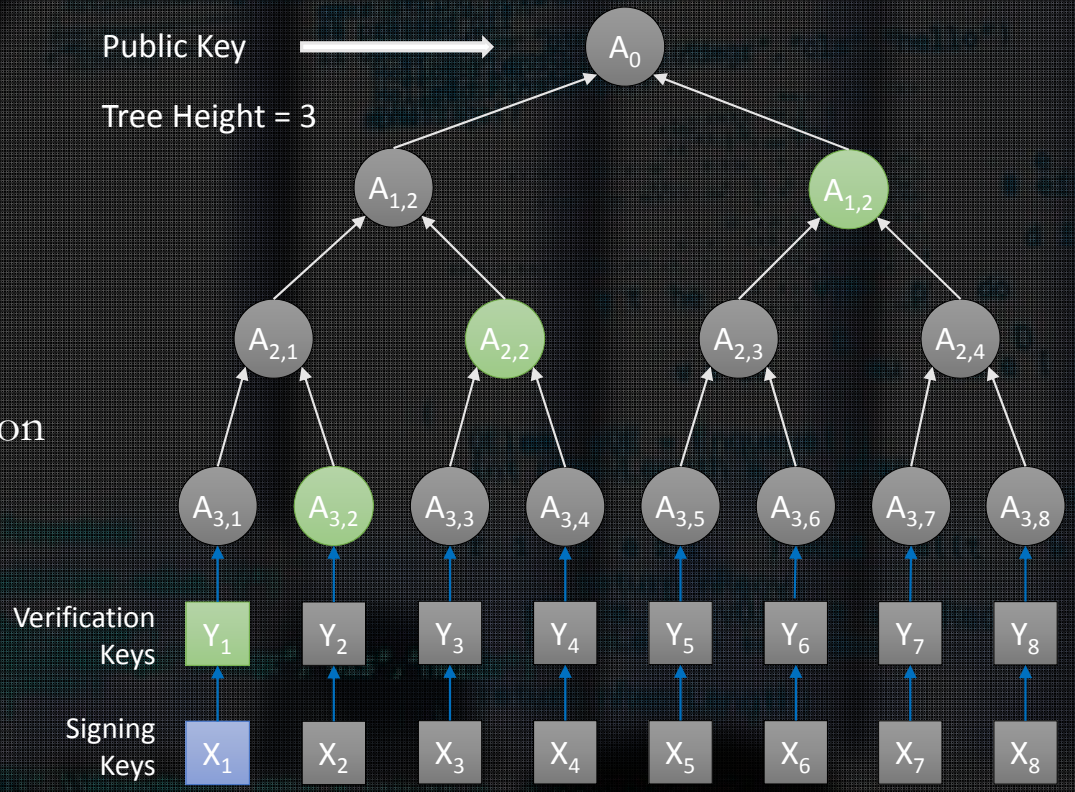


Isogeny-based

ISARA

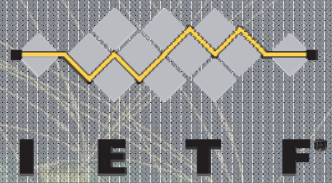
Example Signature Solution: Quantum-Safe Hash-Based Signatures

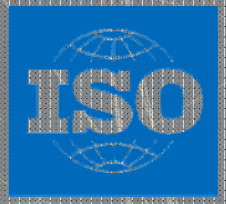
- Introduced by Merkle in 1979
- "One-Time Signatures"
- Small public key but very large private key
- Fast signing & verifying & stateful
- Became practical by combining all verification keys into a single Public Key
- And it happens to be quantum-safe
- Candidates:
  - Leighton-Micali Signatures (LMS)
  - eXtended Merkle Signature Scheme (XMSS)



SUCCESS REQUIRES

STANDARDS





ISARA

USING STATEFUL HASH-BASED SIGNATURES

- The math is mature to be used
- ETSI Working Group QSC was first to characterize these signatures
- IETF is in the final stages of specification
- NIST will standardize stateful hashes for code signing
- ISARA successfully impended LMS and XMSS on an HSM
- The implementation uses tree reduction and state management
- Trees of height 20 provide million+ signatures

CLEARING THE PATH TO QUANTUM-SAFE SECURITY

www.isara.com
quantumsafe@isara.com

Join us on social

@ISARACorp @ISARACorp @ISARA Corporation

ISARA

Mark Pecen

- **Mark Pecen, Chief Operating Officer of ISARA Corporation, which develops security libraries for next-generation networks and computing platforms.**
- **Chairman of the European Telecommunication Standards Institute (ETSI) TC Cyber Working Group for Quantum Safe Cryptography (QSC), in Sophia Antipolis, FRANCE**
- Former senior executive for BlackBerry, Ltd. where he founded the Advanced Technology Research Centre and developed a significant portion of BlackBerry's wireless and networking patent portfolio

- Awarded the title of Motorola Distinguished Innovator and Science Advisory Board member for developing valuable intellectual property for cellular wireless communication – managed professional services for clients in Europe and North America
- Inventor on over 100 patents of technologies adopted globally and used in everyday wireless services, including for the Global System for Mobile Telecommunication (GSM), Universal Mobile Telecommunication System (UMTS), High-Speed Packet Access (HSPA+), Long-Term Evolution (LTE) for 4G wireless and others
- Serves on boards of Mobiquity, Safeguard Scientifics, Rocket Wagon, Swift Labs, Ontario Centres of Excellence, University of Waterloo Institute for Quantum Computing, Wilfred Laurier University School of Business
- Graduate of the University of Pennsylvania, Wharton School of Business and School of Engineering and Applied Sciences