



How I Learned to Stop Worrying and Love the Quantumpocalypse

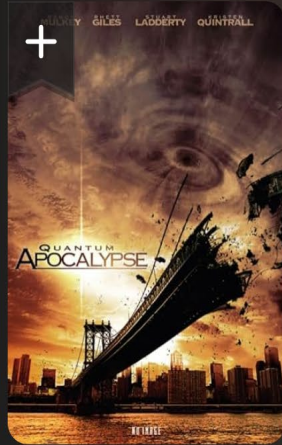
**An exemplary tale with thoughts
on change and opportunity**

Adam Firestone



Quantum Apocalypse

TV Movie · 2010 · Unrated · 1h 35m



Action

Adventure

Drama

A group of talented but rebellious 'rock-star scientists' find themselves in a race against time to save Earth when a comet makes an unexpected turn towards our blue planet where all life may cease to exist within days if our small town heroes fail to find a solution.

Director [Justin Jones](#)

Writer [Leigh Scott](#)

Stars [Rhett Giles](#) · [Stephany Jacobsen](#) · [Stuart Lafferty](#)

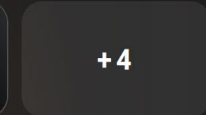
[IMDbPro](#) [See production info at IMDbPro](#)



IMDb RATING
★ 3.1 /10
2.3K

YOUR RATING
☆ Rate

STREAMING



+ Add to Watchlist
Added by 1.7K users

54 User reviews 9 Critic reviews

Two things up front:

**First: Credit where due – title art is from
a usefully named **bad** 2010 TV movie**

Next: I will **not be discussing this movie today, sorry!**

**Instead, I'll be
discussing the
intersection of
quantum computing
and cryptography...**



**...and maybe how
to avoid ending up
like this.**



Specifically:

The rationale behind quantum computing

Why quantum computing impacts you today

The intersection of quantum and cryptography

The intersection of cryptography and business

Basic cryptographic concepts

Mitigating quantum computing's impacts

What you can do today to quantum-proof your organization

Memorize that. There's a quiz later.





Let's start here:

Why should you care about quantum computing?



Because quantum computing can turn your organization's future from this...



To this.



No joke.

We call this “the coming
Quantumpocalypse.”

TEOTWAWKI

**And it has the potential to be the end of
the world as we know it.**

**...or at least the connected world that
enables business, government,
academia, and society.**

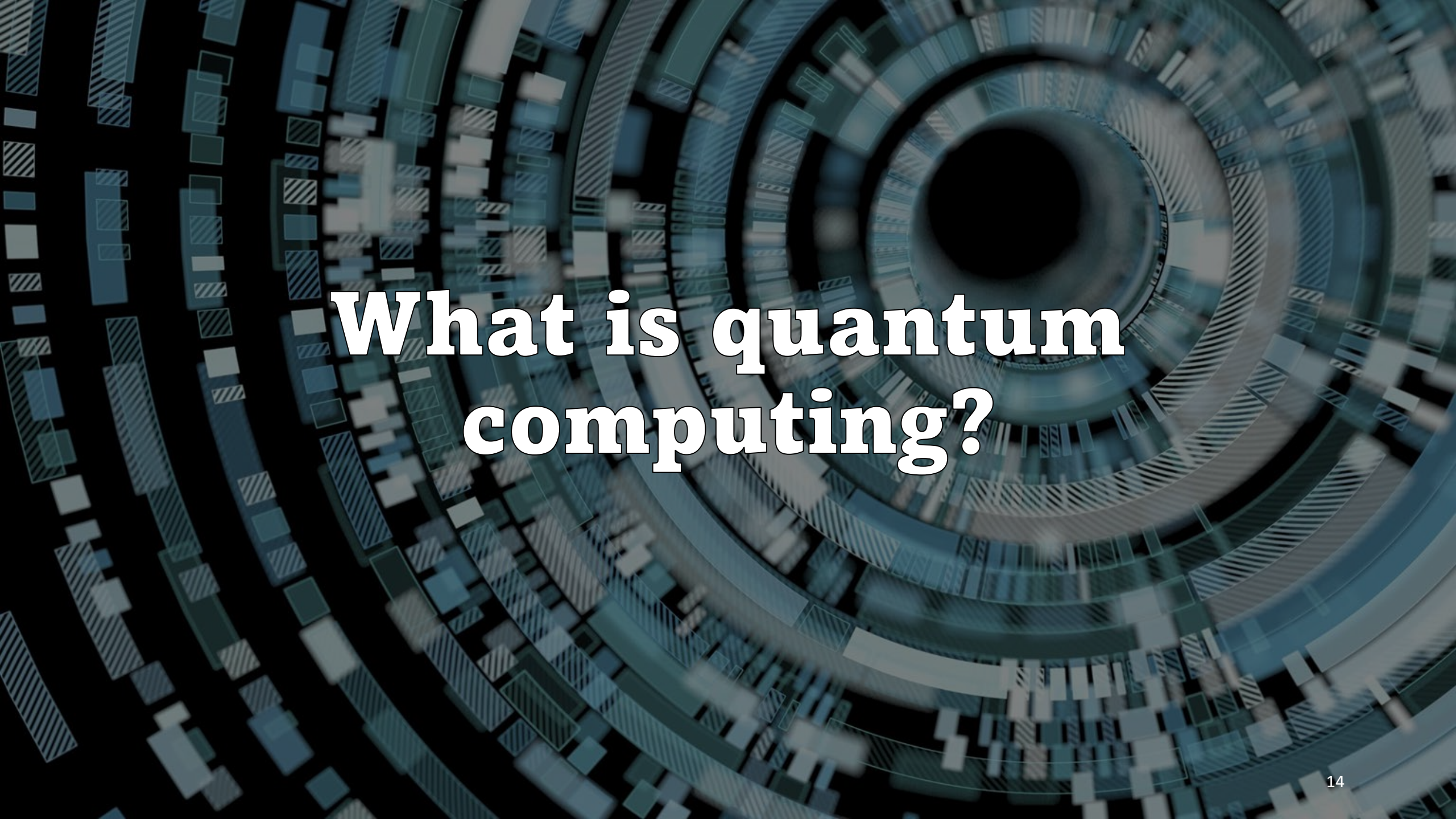
Now that I have your attention...





**Note that the
Quantumpocalypse is
one possible future.**

**We'll explore what
leads to that, and
other, better futures.**



What is quantum computing?

Quantum computing uses the ability of subatomic particles to exist in more than one state at a time.

- ▼ **This allows operations to be done more quickly, and with less energy than classical computers.**

(Example of a classical computer → your smartphone.)

In classical computers, a binary digit (bit) stores a single piece of information

- ▼ **that can exist in one of two states:**

1 or 0.

**Quantum computers use
Quantum Bits - or Qubits.**

- ▼ **Qubits are kind of like
bits in that there are two
possible outcomes -
a 0 or a 1....**

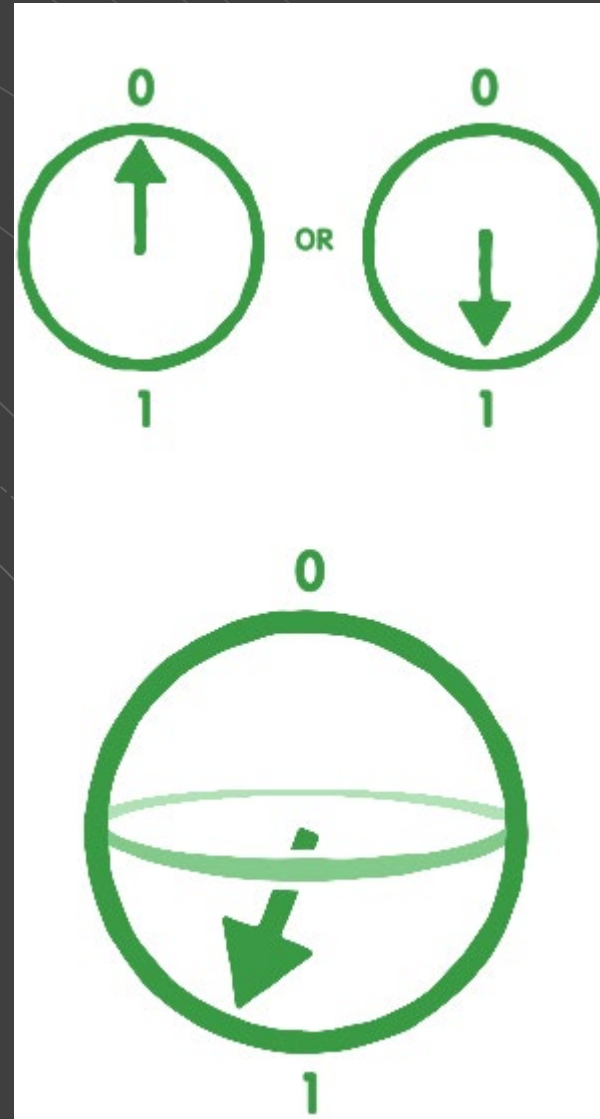
But also, not at all like bits, because the state of a Qubit can also be a **superposition of both possible states.**



Maybe it's a 1, or maybe it's a 0, or maybe it's **some combination of both at the same time.**

▼ **Something
like this:**

BIT



QUBIT

Example:

In classical computing, three bits can represent **any one of 8 values at a time:**
000, 001, 010, 011, 100, 101, 110, 111.

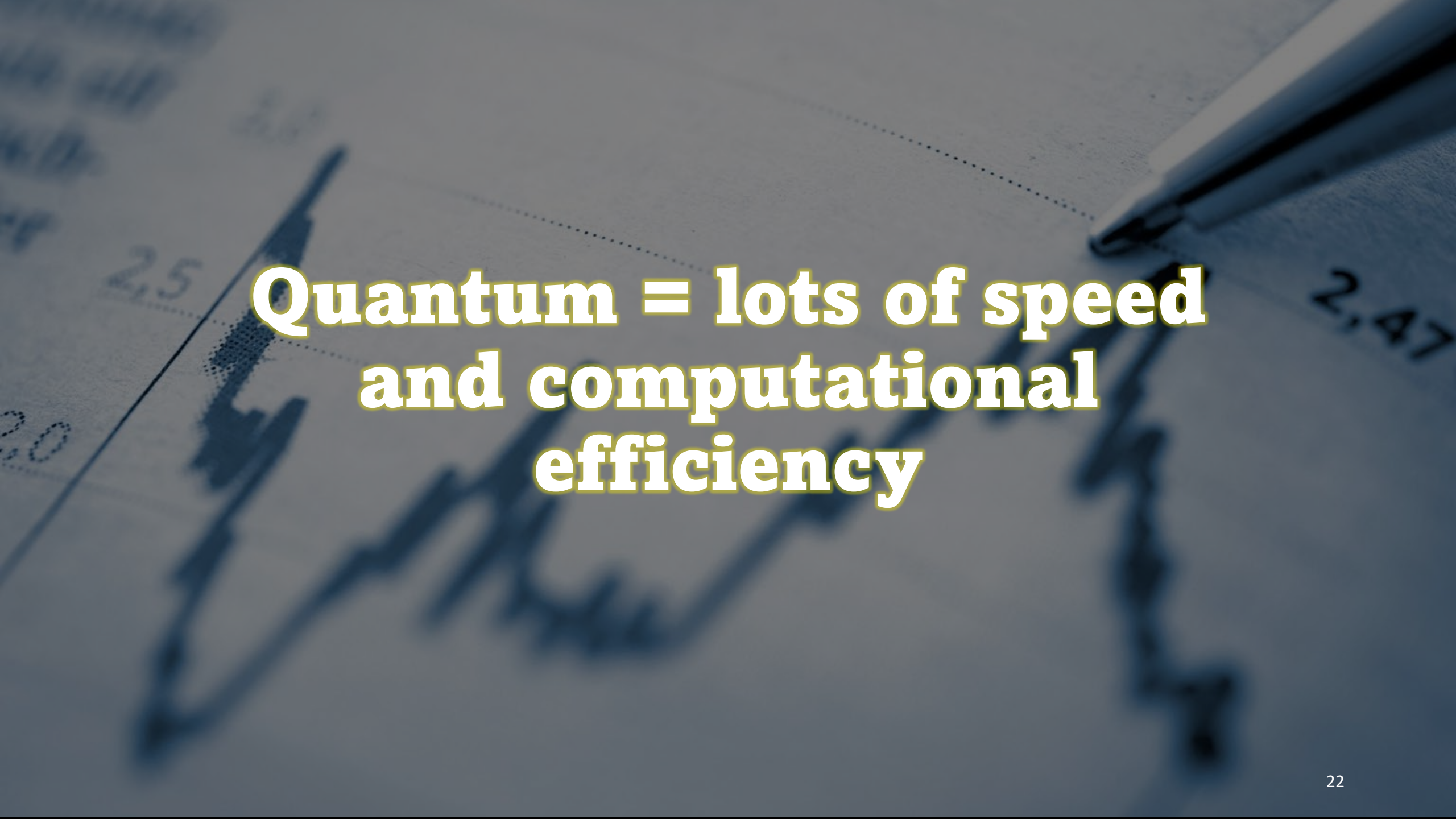


In Quantum computing, three Qubits can represent **all 8 values at once.**


Takeaways:

- ▼ **A qubit stores much more information than a classical bit**

Quantum computers can perform operations much faster than a classic computer.

The background of the slide is a blurred image of a pen writing on a document. A line graph is visible, with a dotted line and a solid line. The numbers '2.5' and '2.47' are visible on the graph. The text 'Quantum = lots of speed and computational efficiency' is overlaid in the center in a bold, yellow font with a black outline.

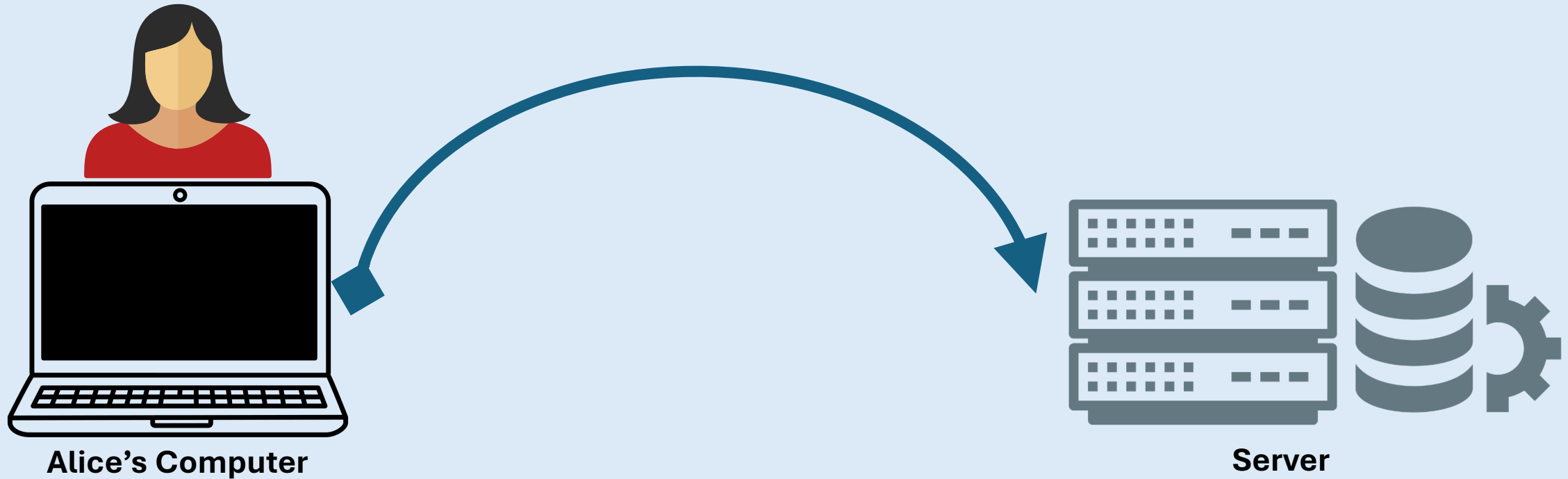
**Quantum = lots of speed
and computational
efficiency**



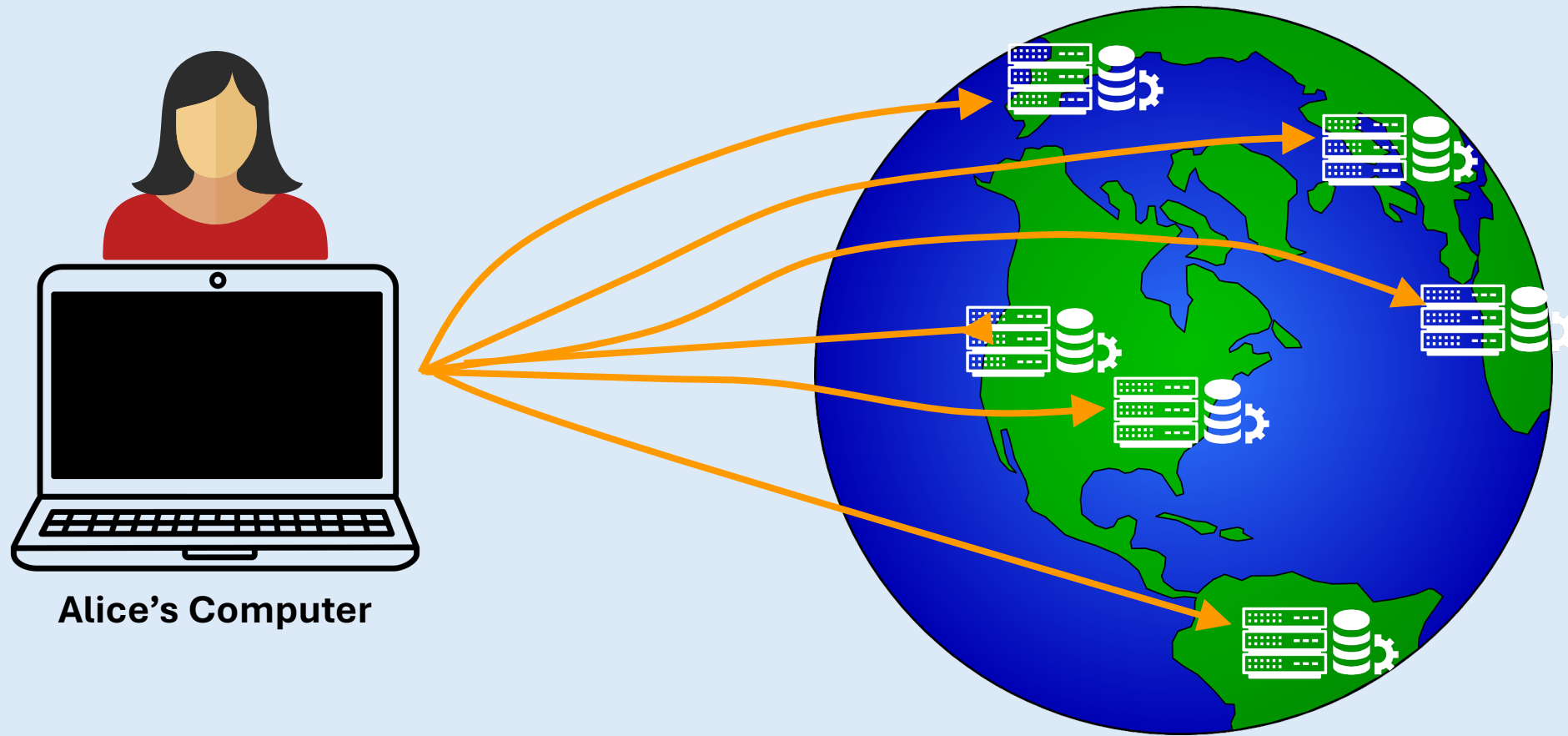
**Next, let's talk about
where the real world and
cryptography meet**



**Alice is a banker at a
global commercial bank**



As part of her job, Alice connects to servers and databases containing sensitive information.



**Sometimes the servers containing information
Alice needs are located far away.**



**This geographical distribution
causes *business* problems.**



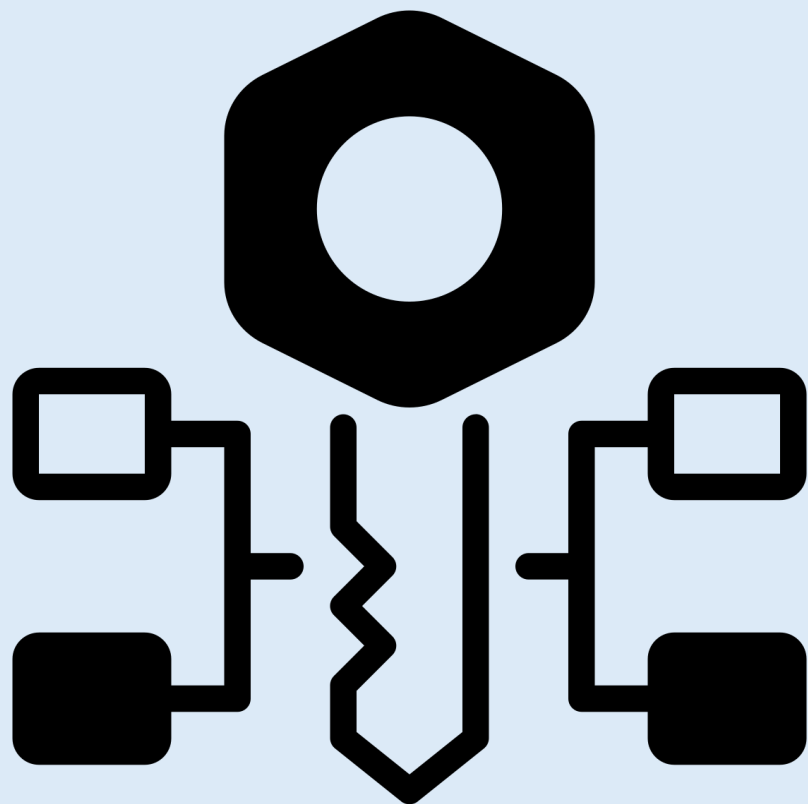
How do I know that the information I'm sending or receiving isn't being intercepted between the server and my computer?

How do I know that the server I'm connected to isn't a bad server pretending to be the server I want?

How do I know that I can trust the information I'm receiving from the server?



**Fortunately, since around 1978,
there's been a technical solution
for Alice's business problems.**



It's called classical asymmetric cryptography.

Asymmetric crypto enables us to:

- **Securely share secrets to establish confidential communications**
- **Establish the other party's identity**
- **Ensure the integrity of shared or retrieved information**

**To create these benefits,
asymmetric crypto relies
on a type of math called
a **one-way function****



A Function is One-Way if:

- **Calculating the output of the function is computationally easy, but:**
- **Back-calculating the inputs based on the output is computationally infeasible**
- **Computationally infeasible = 10,000 – 100,000 years**

**One-way functions typically
used in asymmetric crypto
include:**

*Integer
factorization
(RSA)*

*Discrete
Logarithm
(DHKE)*

*Elliptic Curve
(ECDH)*

THIS IS NOW

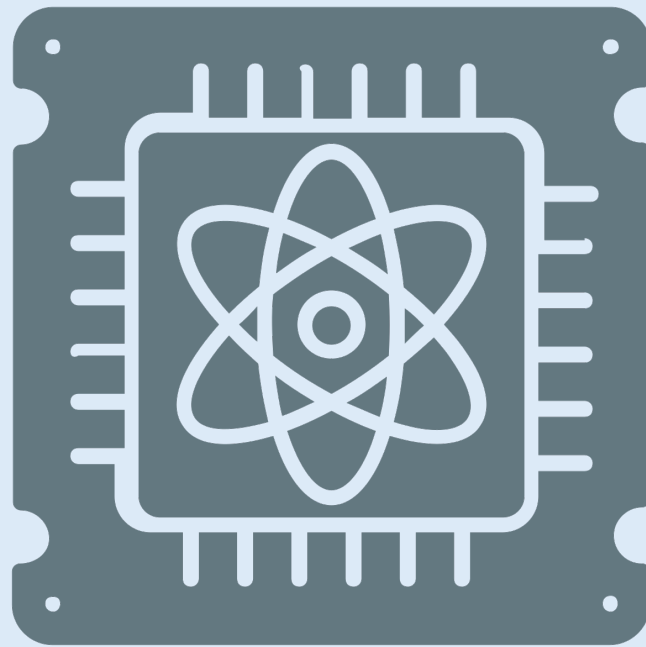
But, let's go
< Back to the > Future
Five years or so into the future, to be precise...



© 2023 Universal Studios. All Rights Reserved.



That's when the USG predicts that cryptographically relevant quantum computers (CRQC) will be available.





60 MINUTES

**It's not just the USG.
On July 28, 2024,
Google and IBM
engineers went on
60 Minutes...**

**...and said that they
expected viable
quantum computers
by the end of the
decade.**



**Guess which types of
math problems quantum
computing solves
exponentially faster...**

**Quantum computing rapidly
solves:**
(via Shor's algorithm)

~~Integer
factorization
(RSA)~~

~~Discrete
Logarithm
(DHKE)~~

~~Elliptic Curve
(ECDH)~~

They're the ones that asymmetric crypto uses.

As a result, quantum computing renders current asymmetric crypto **obsolete. Overnight.**



**Establish and verify
an unknown remote
party's identity**

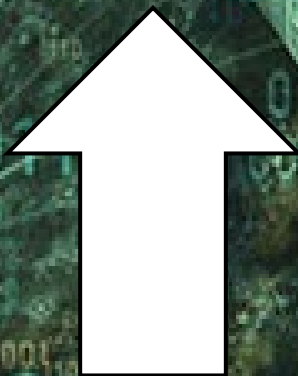
**Securely share secrets
or have confidential
communications**

This means that...

Post-quantum, we will no longer be able to...

**Ensure the
trustworthiness of
shared information**

TEOTWAWKI



Remember this?

Right now, nation-states and criminals are capturing copies of **all encrypted Internet communications and storing them to decrypt once quantum computers are available.**

**This is called a
Harvest Now,
Decrypt Later
(HNDL) attack.**





**And it means no
more secure
communications.
Ever.**

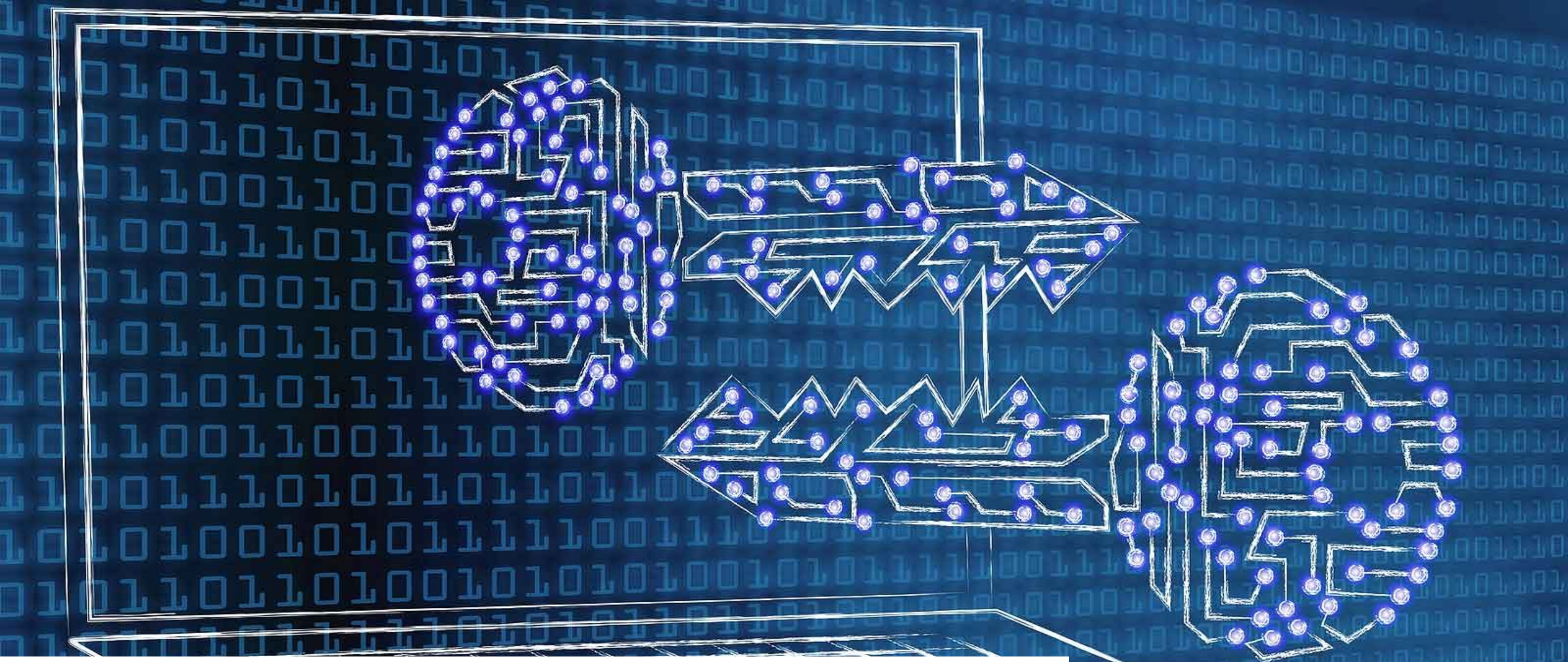
**The clock on Harvest attacks has
already started.**

The background image is a cinematic, apocalyptic scene. The sky is a deep, fiery orange and red, with dark, swirling clouds. In the distance, a city skyline is visible, with several tall, dark, jagged structures that appear to be ruins or remnants of a once-great city. The foreground is a desolate, rocky landscape with a lone figure in a dark, hooded cloak standing with their back to the viewer, looking out over the ruins. The overall mood is one of devastation and the end of an era.

**And that is why we call it the
Quantumpocalypse**

BUT...

**DON'T
PANIC**



First, the main symmetric crypto algorithm in use today is not becoming obsolete.

That algorithm, AES-256, is part of the post-quantum Commercial National Security Algorithm Suite defined by the NSA



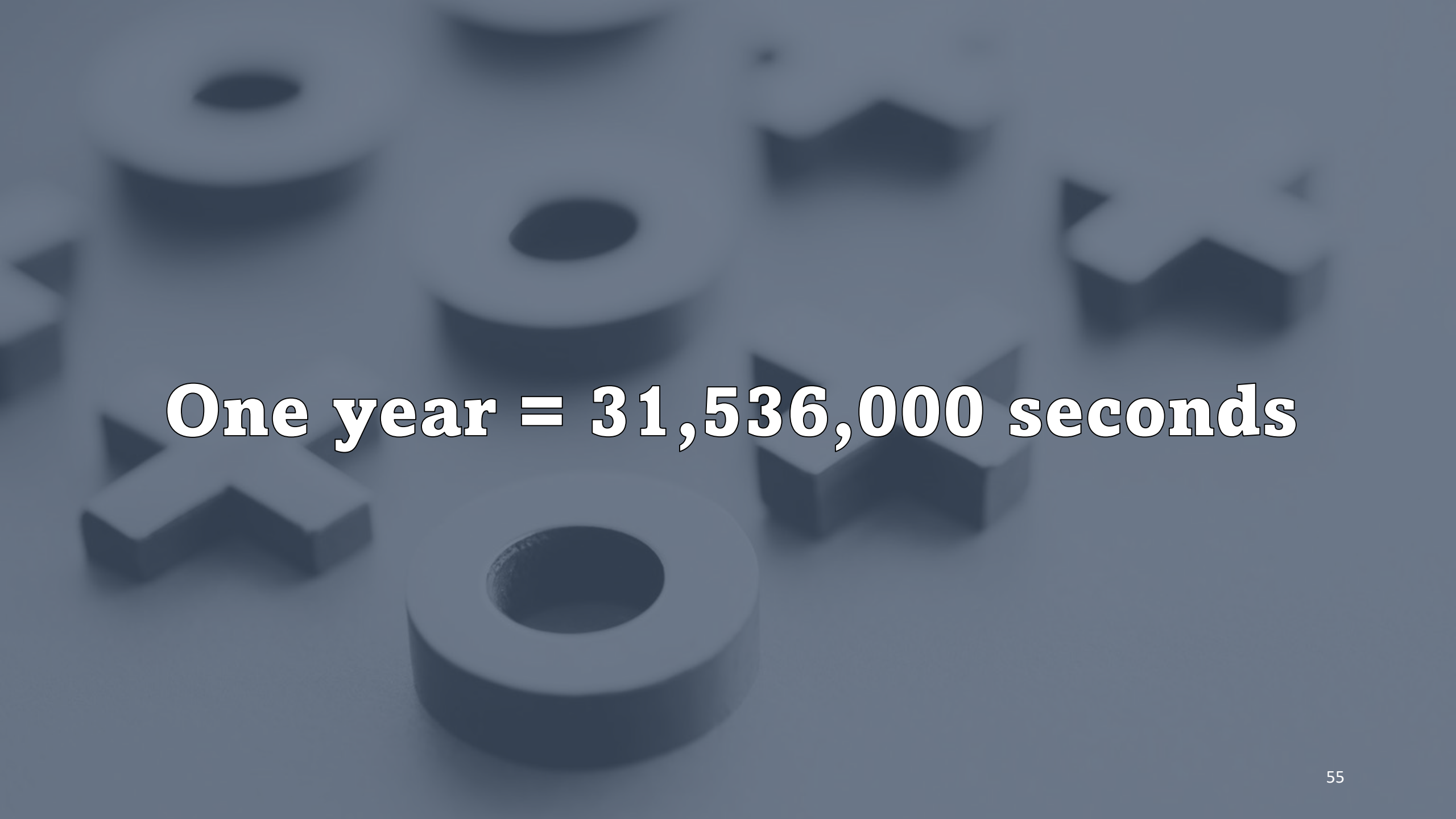
Under quantum attack, a 256-bit key would be as resistant (as per Grover's Algorithm) as a 128-bit key is today under classical computing attack.

A dark, textured padlock with a heart-shaped cutout in the center is shown in the foreground. A key is inserted into the top of the padlock. In the background, another key is visible, slightly out of focus. The entire image has a dark, blue-grey tint.

How secure is that?

The background of the slide features a close-up, slightly blurred image of several interlocking metal gears. The gears are a dark, metallic grey color and are arranged in a way that creates a sense of depth and mechanical complexity. The lighting is soft, highlighting the teeth of the gears and casting gentle shadows.

**A supercomputer that performs
 10.51×10^{15} operations/ second...**

The background of the slide features a collection of interlocking mechanical parts, including gears and star-shaped components, rendered in a monochromatic blue-grey color. These elements are scattered across the frame, with some in sharp focus and others blurred, creating a sense of depth and mechanical complexity.

One year = 31,536,000 seconds

**It would take
1 billion billion years
to crack a 128-bit key**


**The second use of the
word billion was not
a typo.**

**P.S. The universe is
only about 13.75
billion years old.**



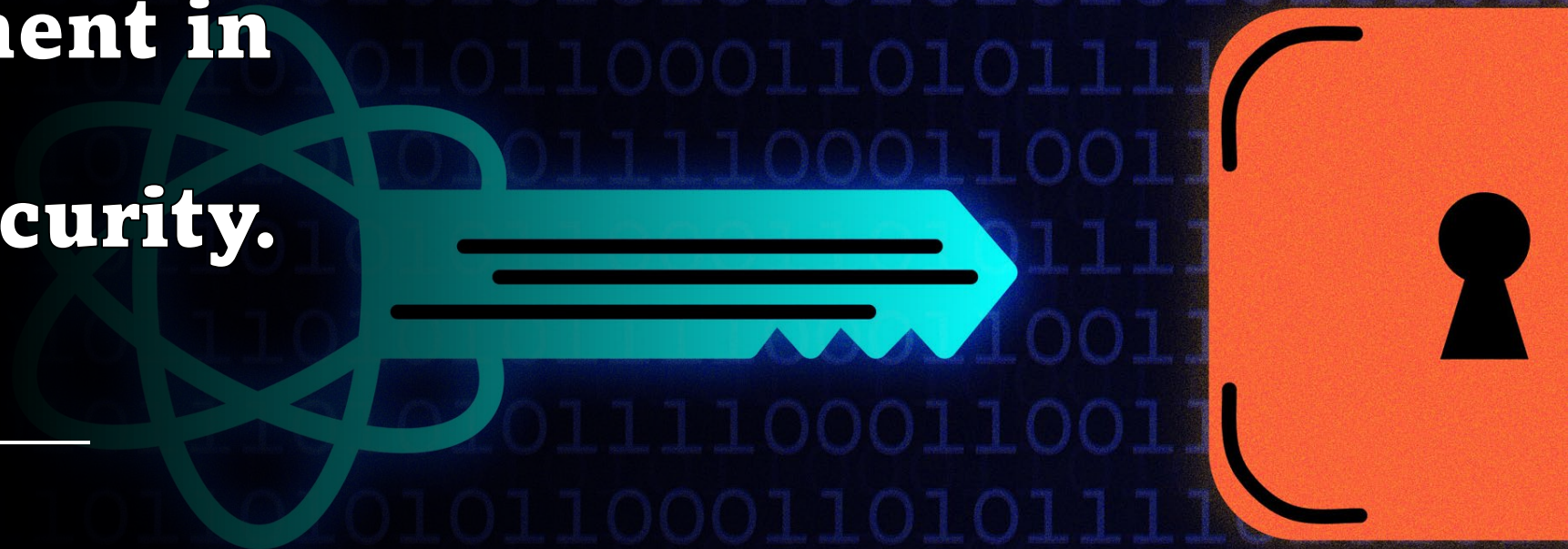
YayCat says:

**Yay!
Symmetric
Crypto!**



**For asymmetric
crypto, there's been
a huge investment in
post-quantum
information security.**

**This has resulted in technology called
“Post-Quantum Cryptography” (PQC).**



The US National Institute of Standards and Technology (NIST) has begun publishing PQC standards, such as ML-KEM (FIPS 203).

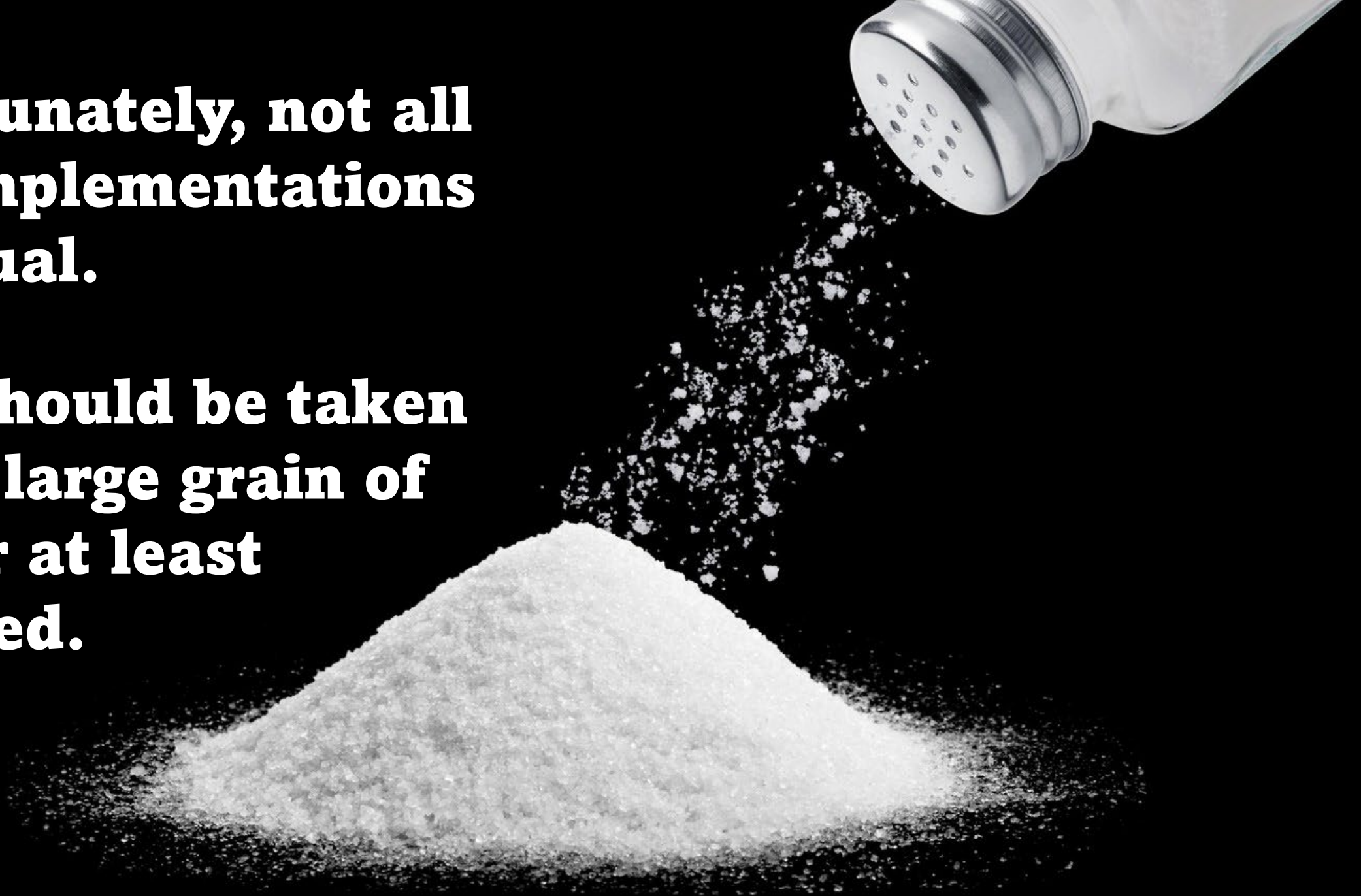
The National Security Agency (NSA) has reflected PQC in its Commercial National Security Algorithm Suite version 2.0 (CNSA 2.0) standard.

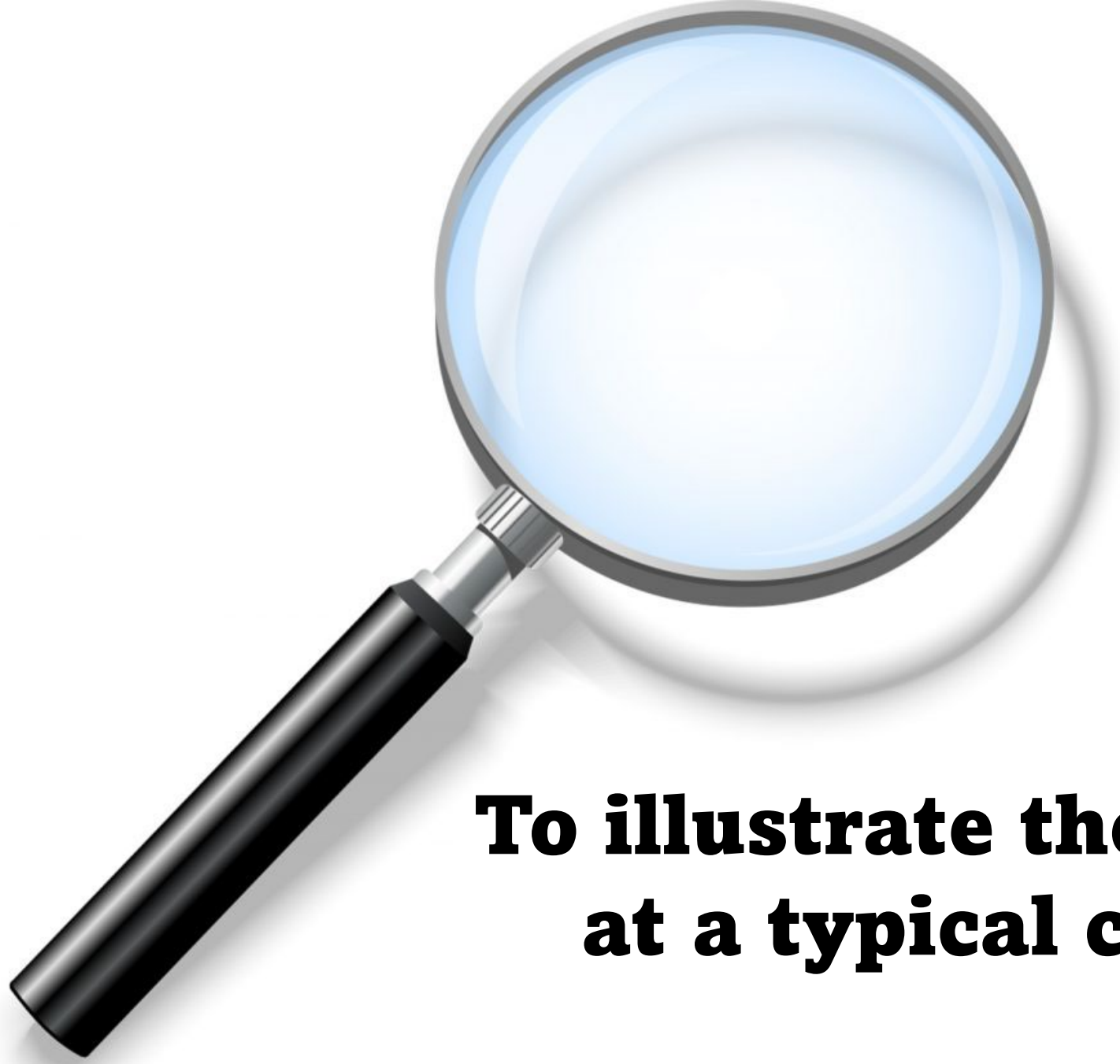
The best news?

- ▼ **PQC is now a matter of productization and adoption, not fundamental research and development.**

**Unfortunately, not all
PQC implementations
are equal.**

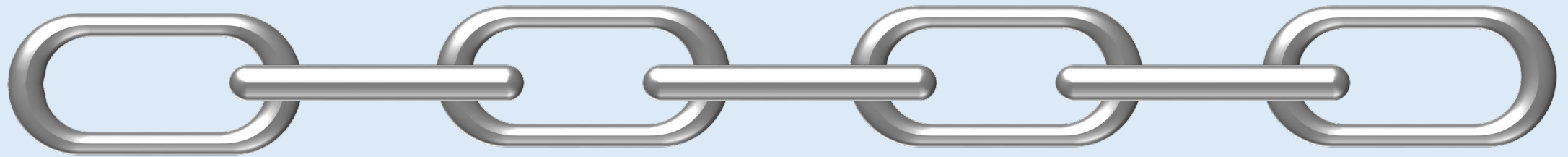
**Most should be taken
with a large grain of
salt, or at least
caveated.**





**To illustrate the issue, let's look
at a typical crypto process.**

Applying cryptographic security to internet communication isn't a discrete event.

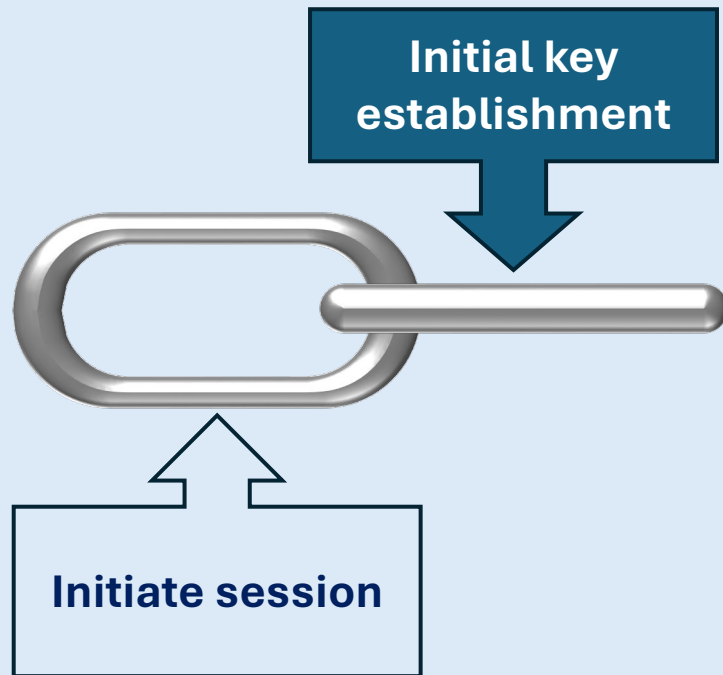


It's a **chain of carefully choreographed events.
Let's look at a typical internet communication scenario.**

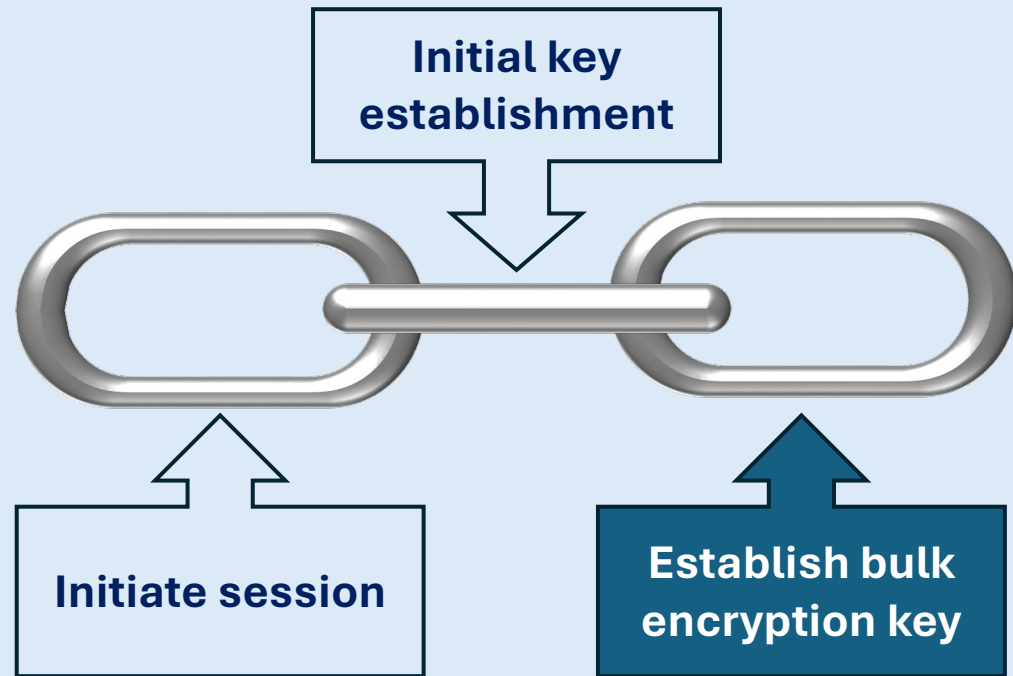
First, parties initiate a communication session



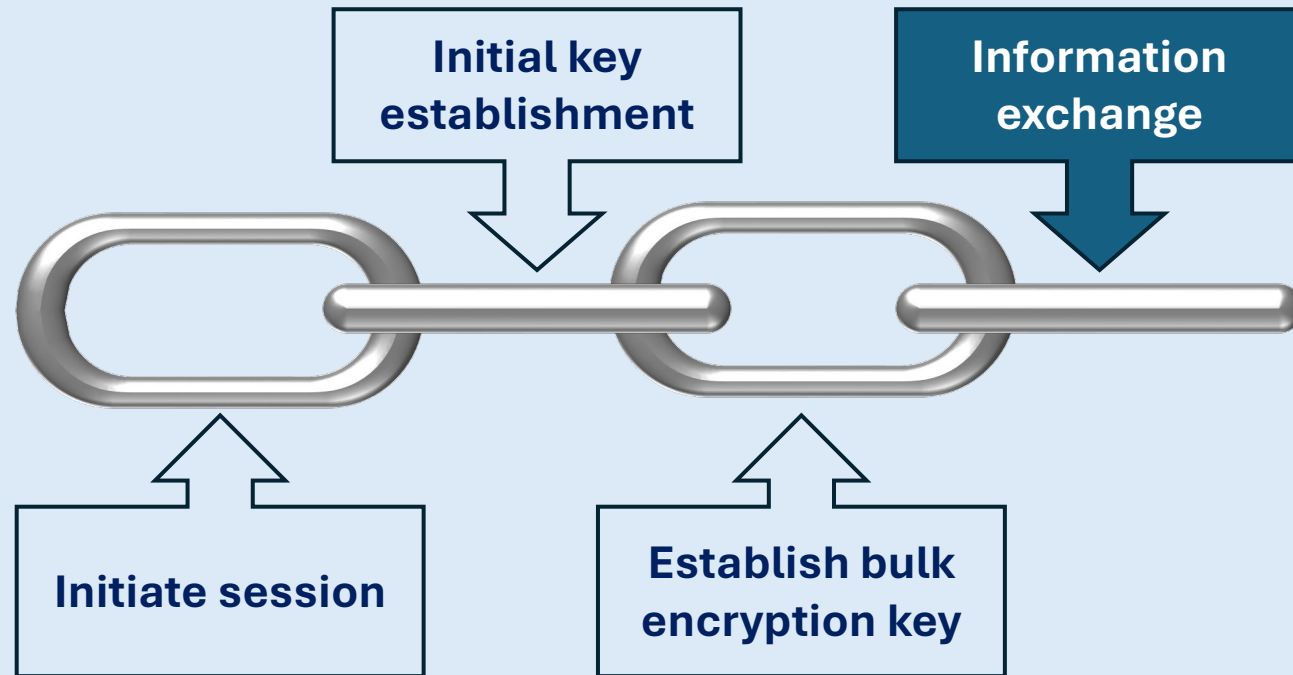
Then they establish an initial shared key



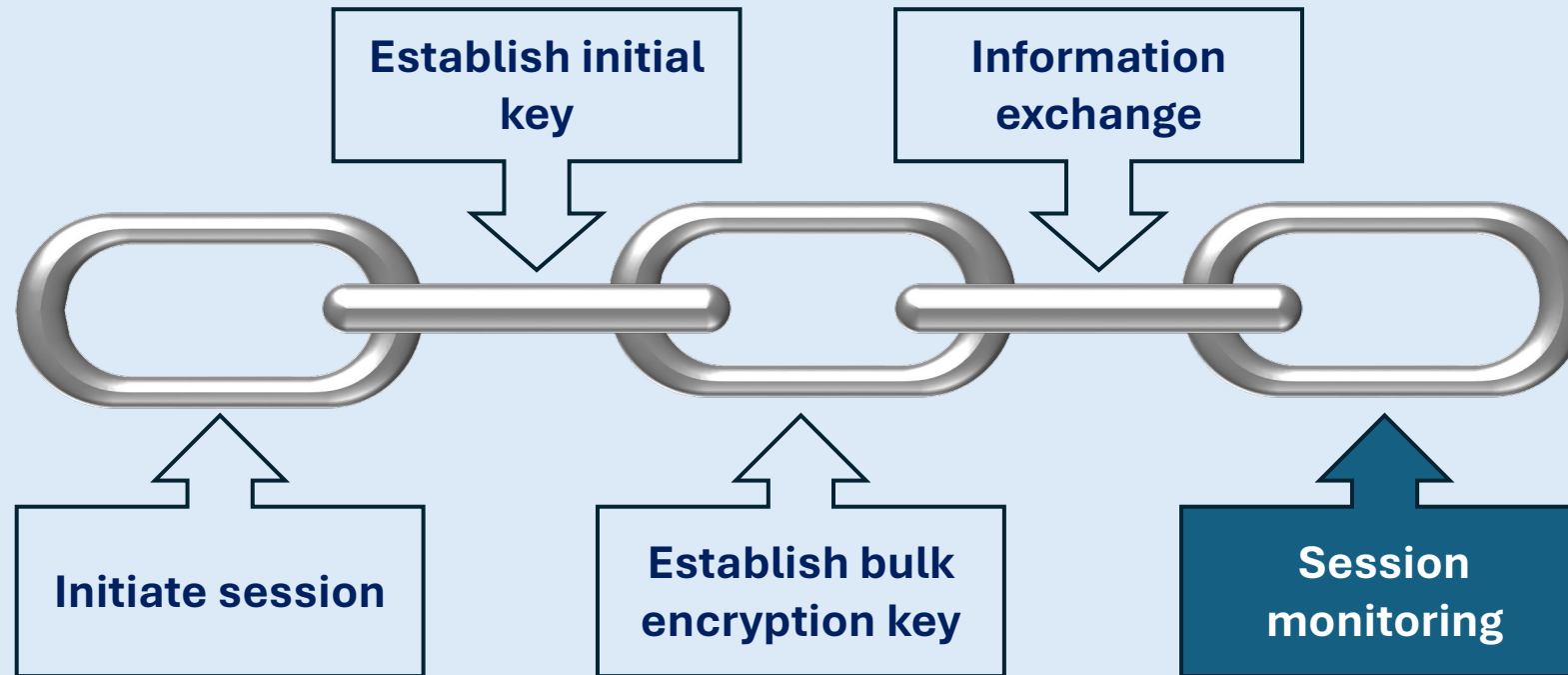
Next, a bulk encryption key is established



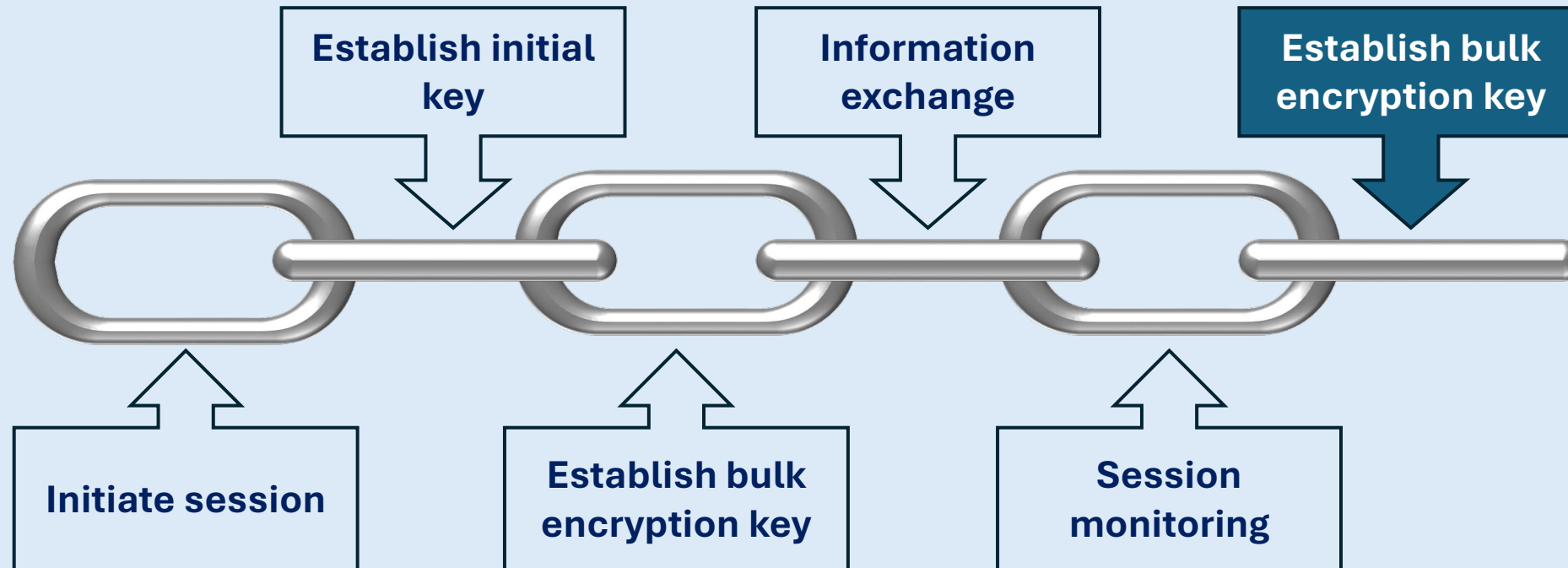
Information exchange begins



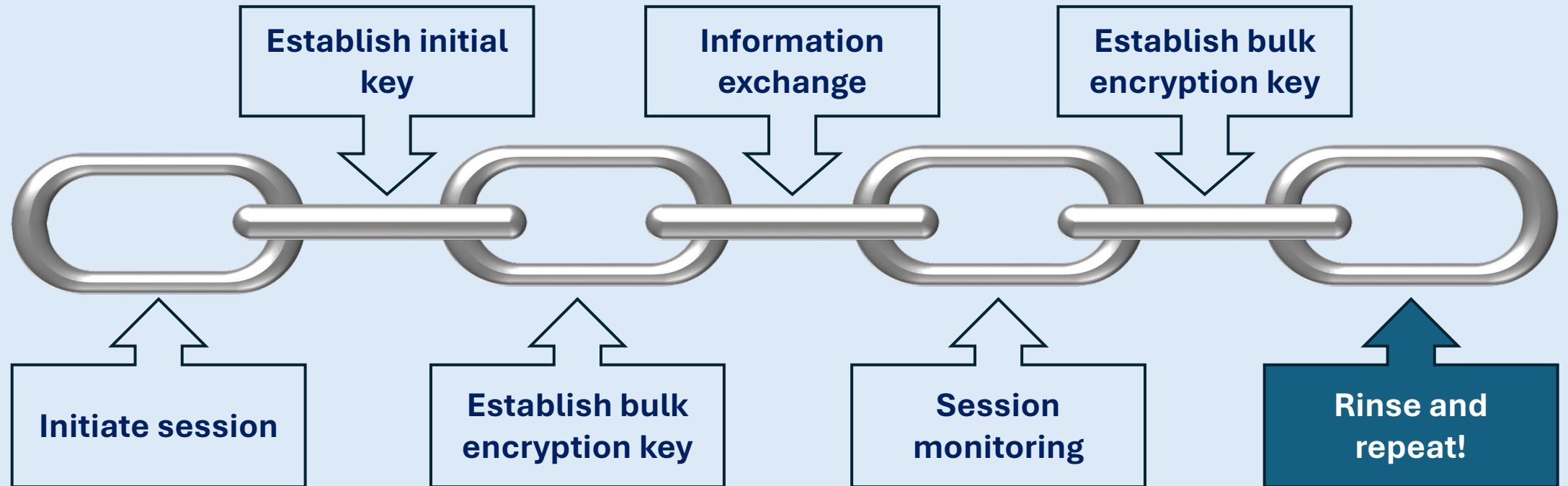
The parties monitor the session



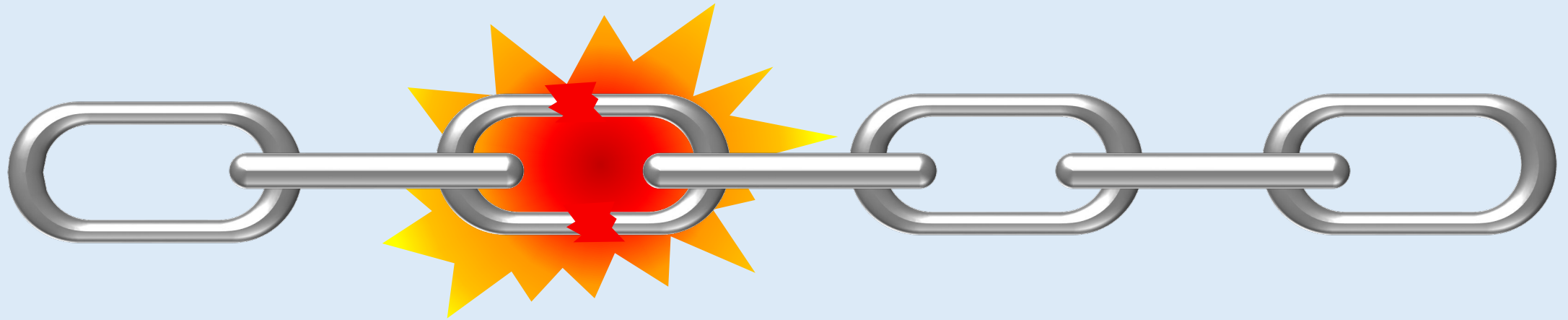
After a threshold (age, amount of data) has been reached, new bulk encryption keys are created

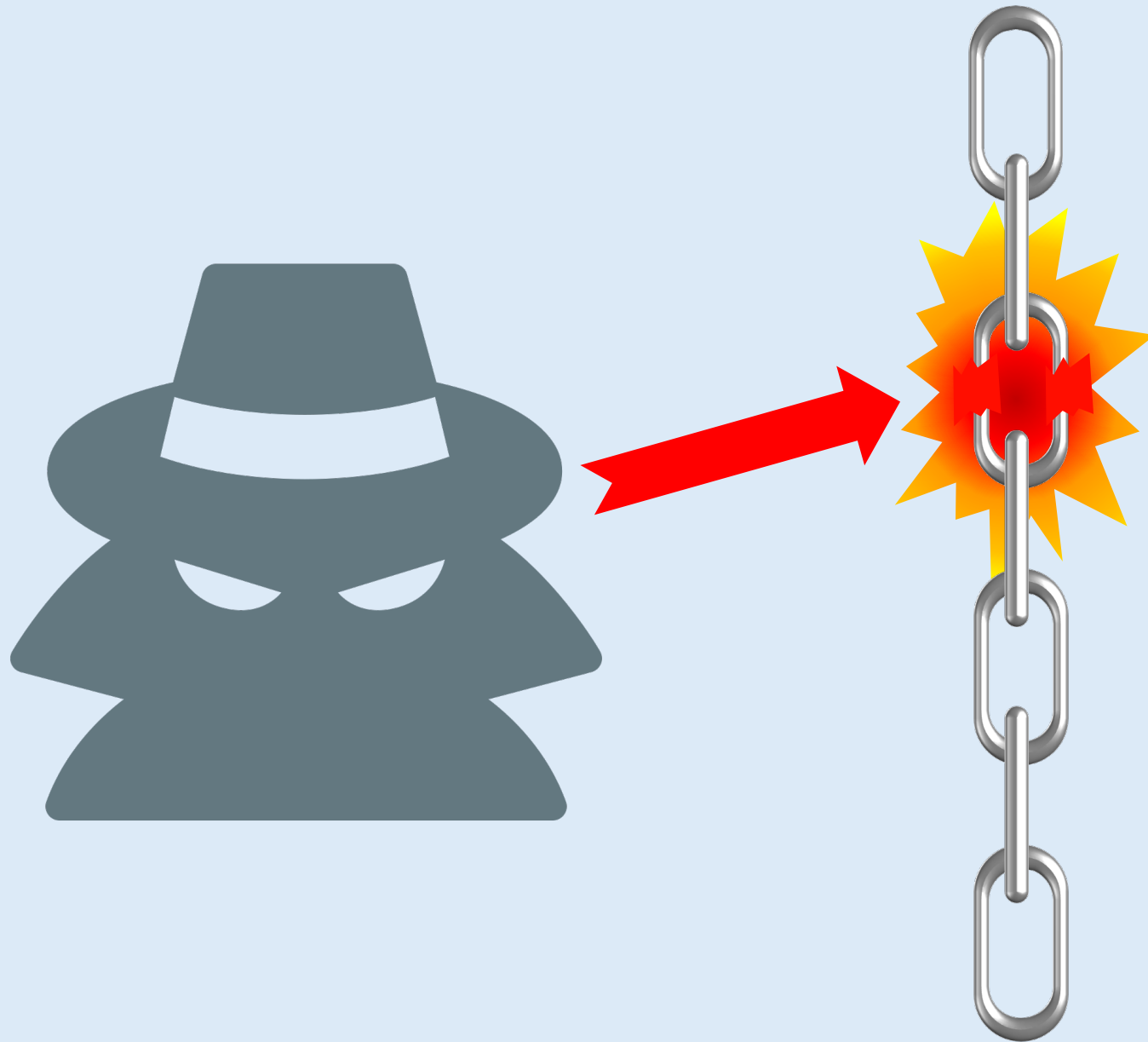


The cycle then repeats



If any link is broken, the entire chain fails.

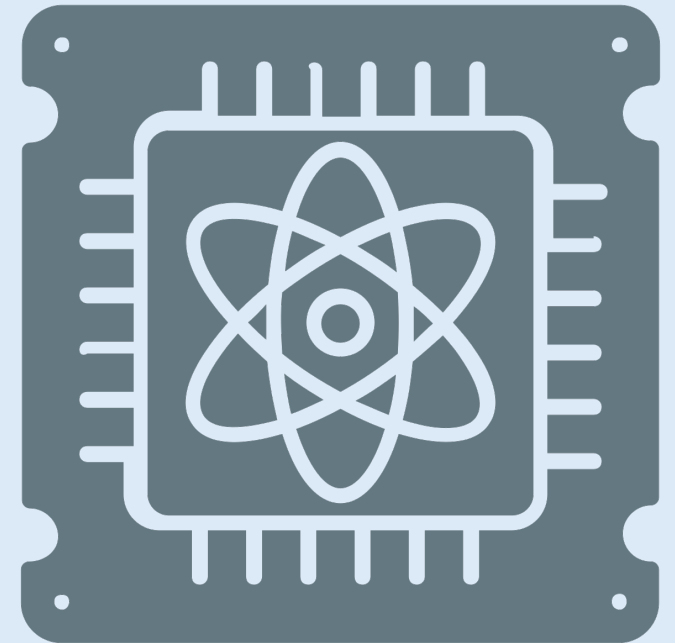


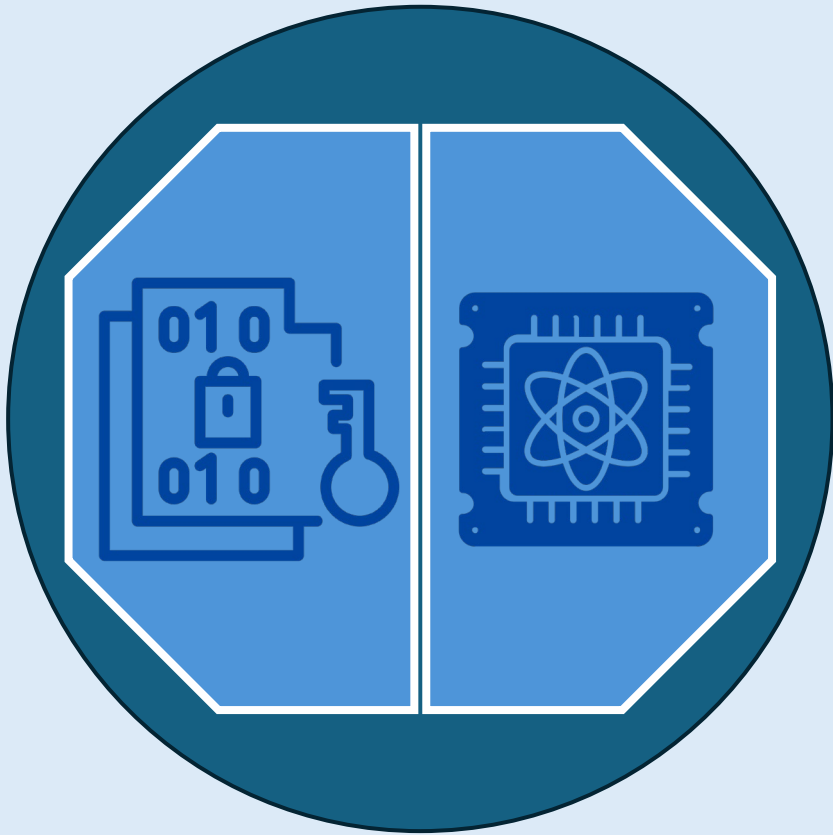


**Because of this,
malicious actors
don't attack the
entire chain.**

**They go after the
weakest link.**

Post-quantum, the weakest link is any part of the process that uses classical (pre-quantum) crypto.

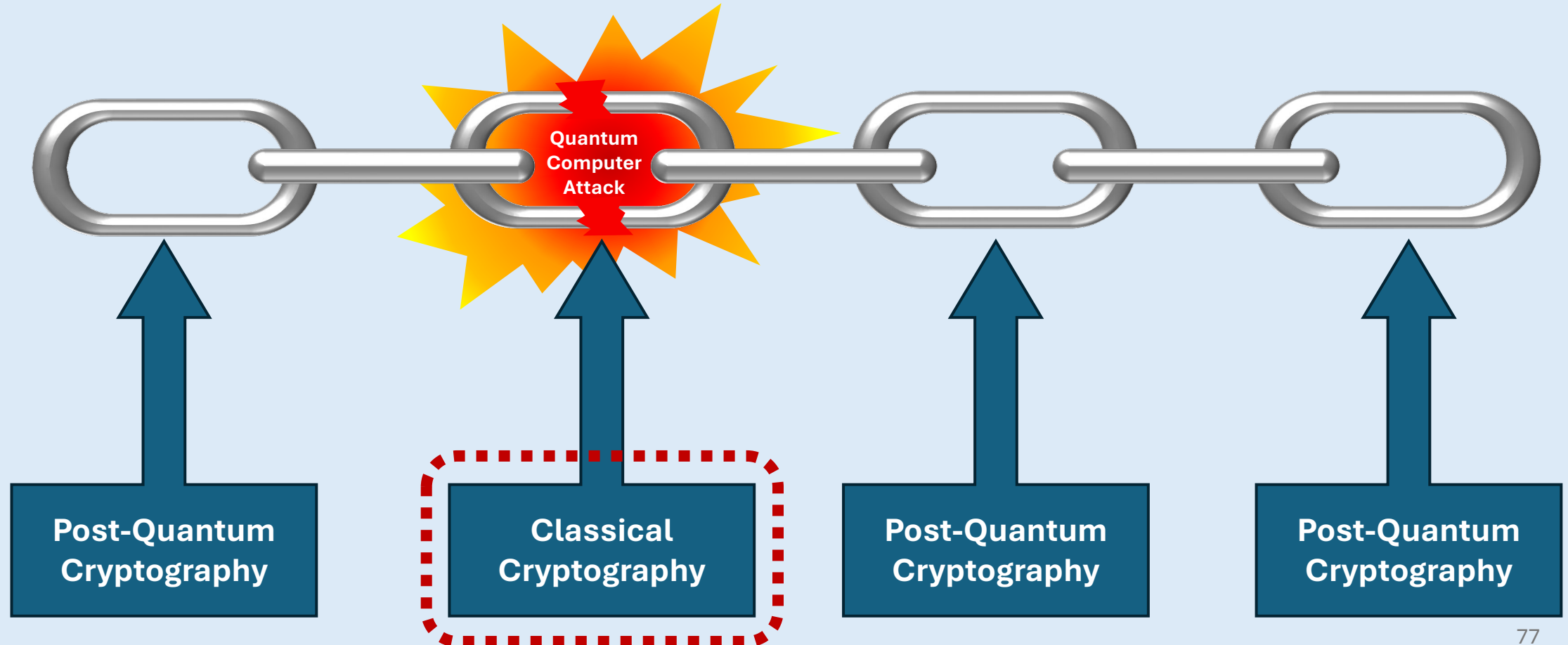




This is where concerns about **hybrid PQC arise.**

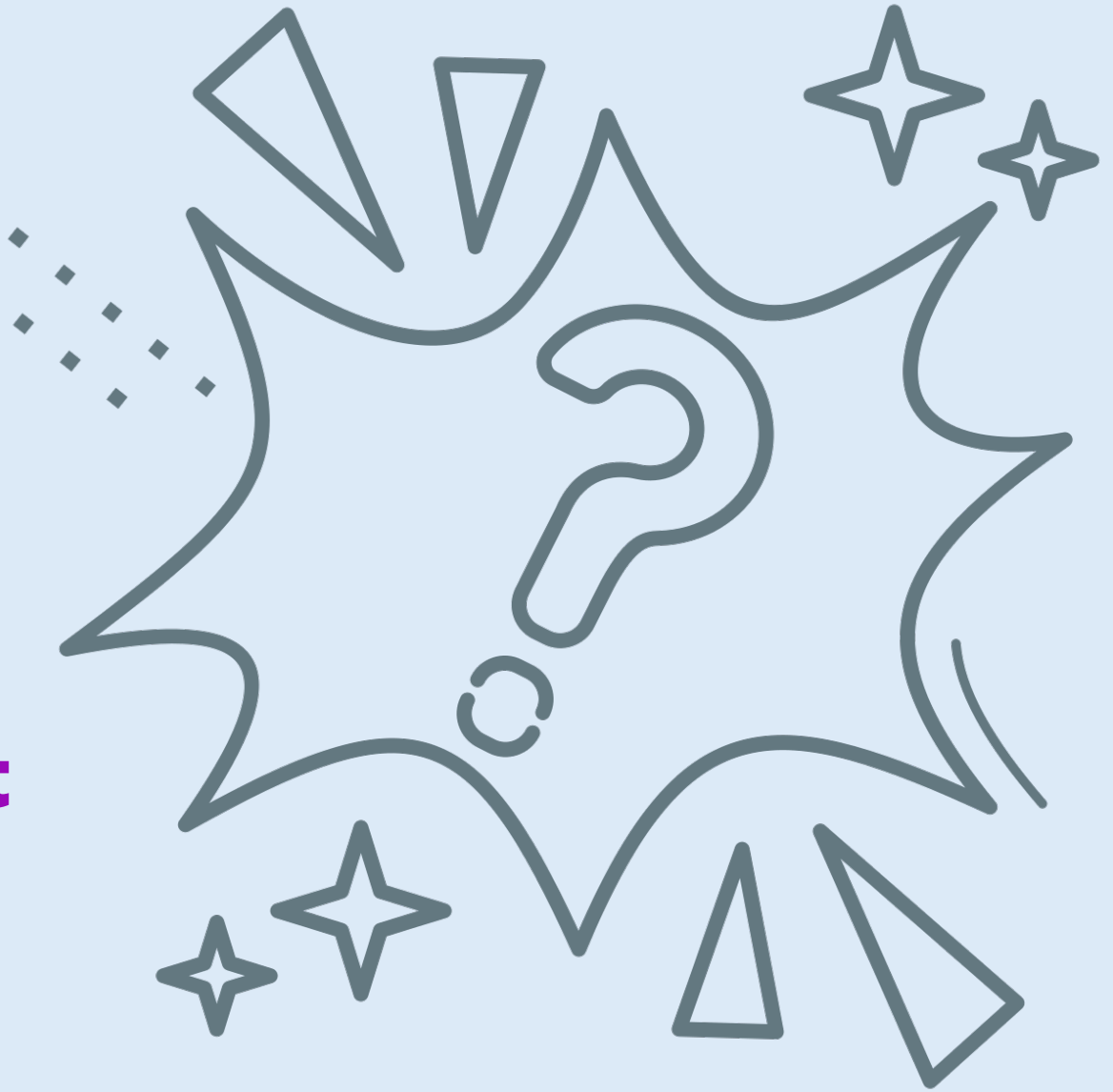
Hybrid post-quantum cryptography pairs PQC with classical crypto for elements of the chain like key establishment.

This creates weak links in the chain that are vulnerable to attack by a quantum computer.



This begs the question...

**If hybrid post-quantum
cryptography creates, or
at least doesn't mitigate,
vulnerabilities, why do it
in the first place?**

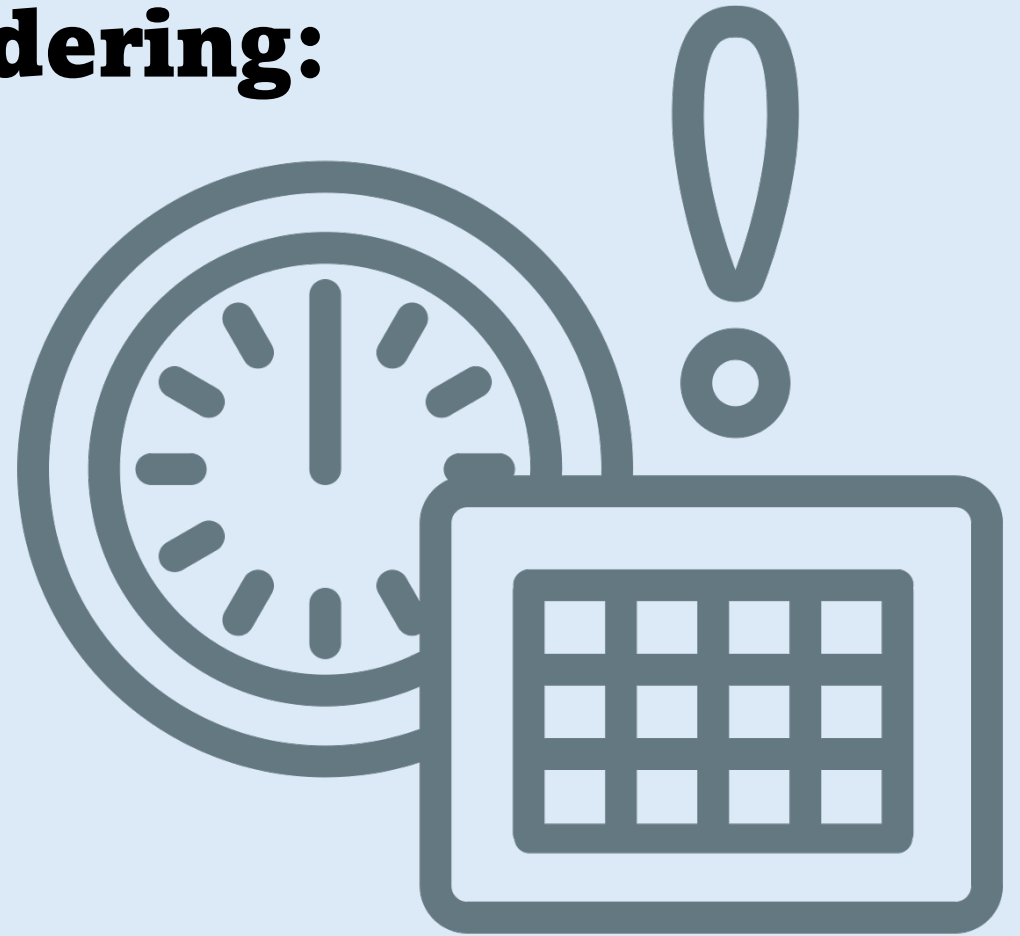




At the risk of opening a can of worms, there are a number of factors that contribute to the answer...

First, there's temporal ordering:

**Many hybrid PQC
predate development of
PQC best practices...**



Then, there's business logic...



**Technology solutions
represent investment;
organizations want to
protect that investment.**

Standards are playing catch-up:

Example, the Commercial National Security Algorithm Suite (CNSA) 2.0 was published in September 2022...

...and clarifying guidance came out in April 2024.

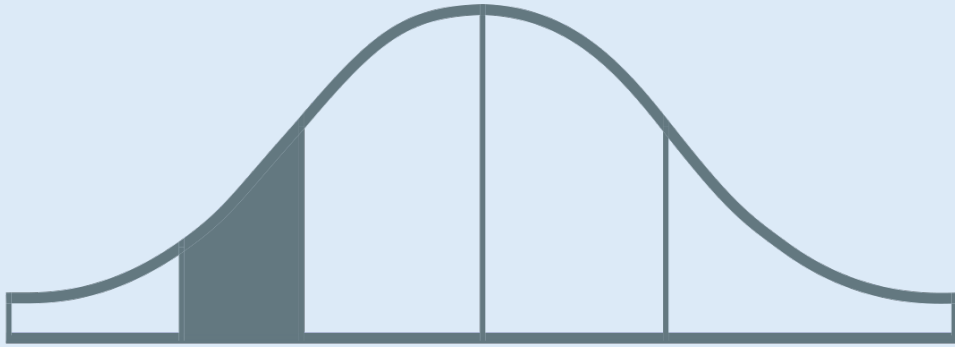




**The clarification specifically
disallows the use of hybrid
PQC:**

“Web browsers/servers and cloud services: support and prefer CNSA 2.0 by 2025, exclusively use CNSA 2.0 by 2033.” CNSA 2.0 FAQ

Also, there's the early-adopter penalty:



Early investors in hybrid PQC may not have the financial will or ability to **re-spend to comply with changing technology...**

...even if that leads to suboptimal outcomes.



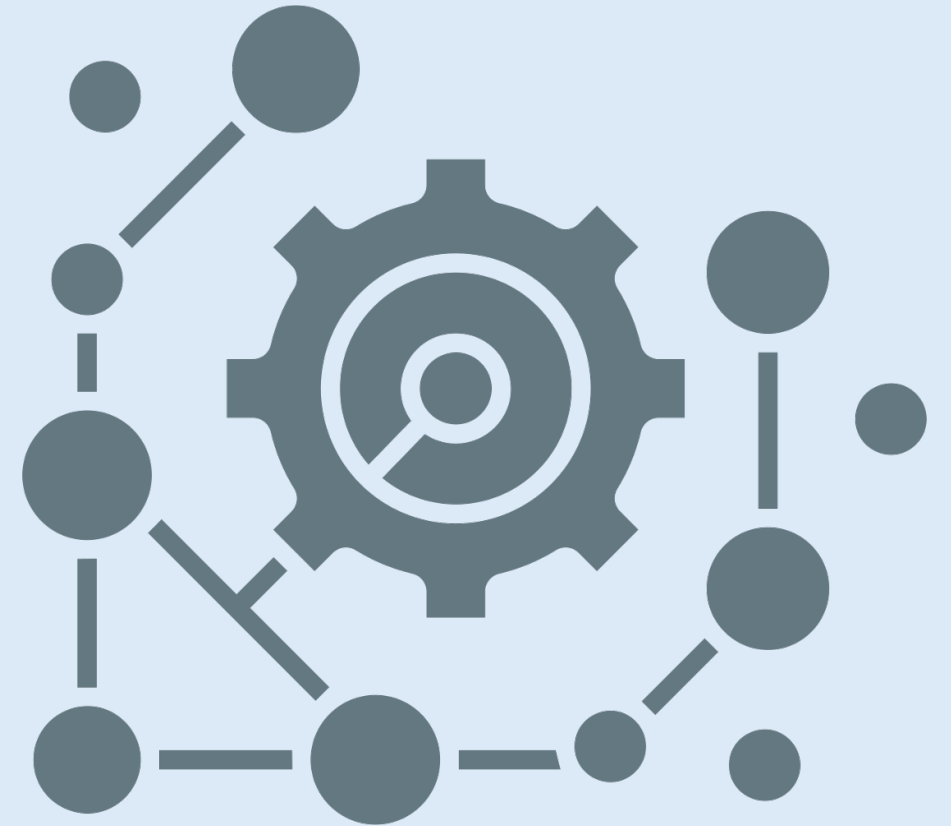
**The graveyards of history are
littered with early technology
adopter penalties.**

Finally, there's technical complexity

Changing an entire crypto protocol is more challenging than an algorithm swap...

...using a hybrid solution enables organizations to say they're doing something...

...while waiting for someone to do the right thing.



**To be clear, this is not a
cryptography problem.**

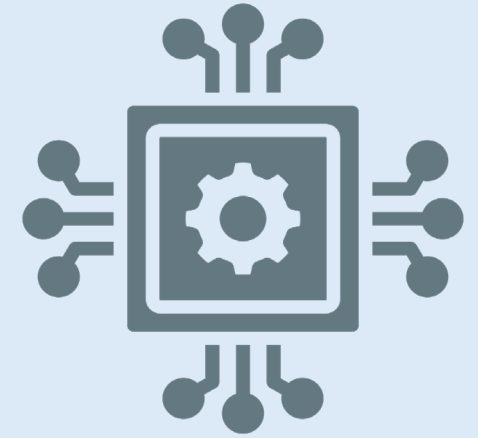
This is a **business problem.**

Because cryptography is...

Everywhere.



It's built into your hardware.



**It's in all software that moves
or manages information.**

**The ability to do business is
directly threatened by
quantum computing.**



WHAT



NOW



"ALL THE NEWS
YOU NEED TO KNOW"

News·Today

FOUNDED 1851

MONDAY, OCTOBER 2012
Vol. MCMXX, No. 144672

BAD NEWS!!

sa l'ouppapi

NON-COMPLIANCE

COMPLIANCE

NON-COMPLIANCE

**There aren't many
fully PQC products
available today.**



**Right now, spending our way
out isn't a viable solution**



**You can start making
the software
development
ecosystem quantum
resistant immediately**



CNSA 2.0: Your new best friend

Names 6 PQC algorithms:

- **Software/firmware signing**
 - **Leighton-Micali Signature**
 - **Xtended Merkle Signature Scheme**
- **Symmetric-key algorithms**
 - **AES-256**
 - **SHA-384/SHA-512**
- **Public-key algorithms**
 - **CRYSTALS-Kyber (ML-KEM) – Key establishment**
 - **CRYSTALS-Dilithium (ML-DSA) – Digital signatures**



Things to do today

- **Ensure that code at rest is protected with AES-256**
- **Ensure that hashing schemes use only SHA-384 or SHA-512**
- **Develop organizational PQC roadmap**



SHORT-TERM

Within six months:

- **Adopt post-quantum data-in-transit solution that does not use hybrid PQC**
- **Examples:**
 - **PQC enterprise VPN**
 - **PQC enterprise datacenter/SDN solution**
 - **PQC managed file transfer/data room**

Down the road: 18 months +

Note: Timeline driven by industry/vendor adoption of PQC standards

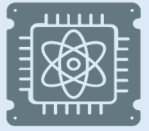
Retooling of internal IT to use PQC-enabled network infrastructure

Revise IT policies for compliance with PQC standards

PQC policies for vendors and partners

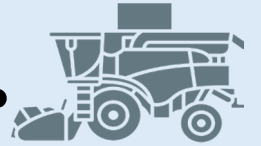
Recap!





Quantum computers are ~5 years away, but...

...the threat they create is happening now.



PQC can help mitigate that threat...

...but some PQC really isn't PQC.



The only way to be sure that PQC is PQC...

...is to verify that PQC products comply with PQC standards.



NIST

Thank you!