Quantum Computers: Revolution or Apocalypse?

Hans Heum, NTNU

NDTV WORLD · Live TV · News · Video · Opinion · Diaspora · India Global · #USPolls · Asia · Australia

News > World News > 'Has Potential To Change Almost Everything': Scientists To Channel Quantum Power

'Has Potential To Change Almost Everything': Scientists To Channel Quantum Power

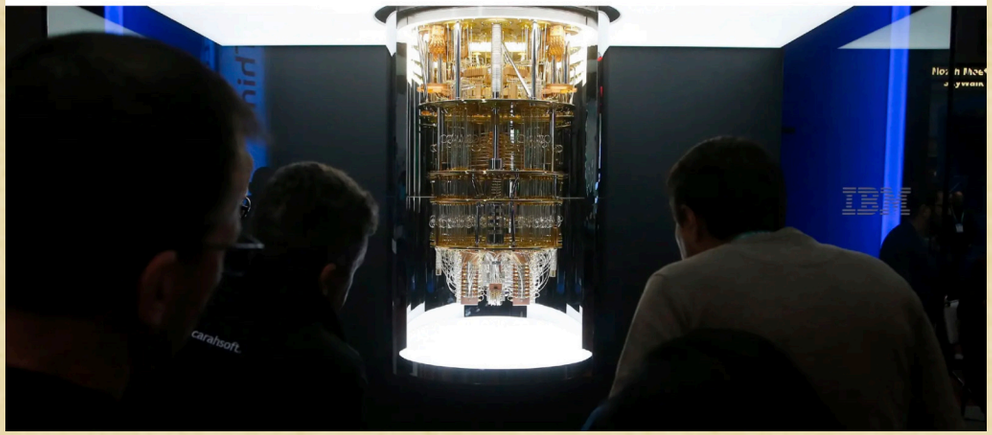
NewScientist · Sign in · Enter search keywords

Google launches $5m prize to find actual … m computers

Kultur | Teknologi

Maskiner som denne kan drepe internett

Men redningsplanen er klar.



"Machines that kill the internet."

Often Heard

1. "Now that Moore's Law is reaching its physical limit we need Quantum Computers to continue the trend."

2. "Quantum Computers can instantly solve hard problems by trying all solutions in parallel."

3. "Quantum Computers will accelerate the Green Energy Transition."

4. "Quantum Computers will revolutionize artificial intelligence."

5. "Quantum Computers can break any code."

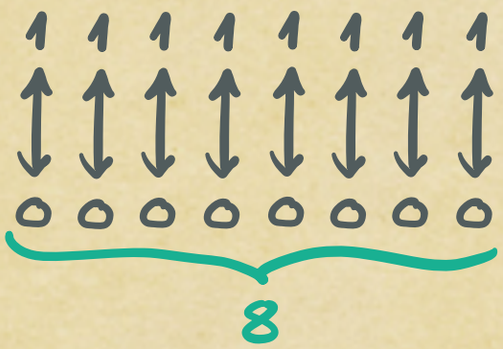
All false/unjustified statements!

... But each based on a grain of truth

The Quantum Computer

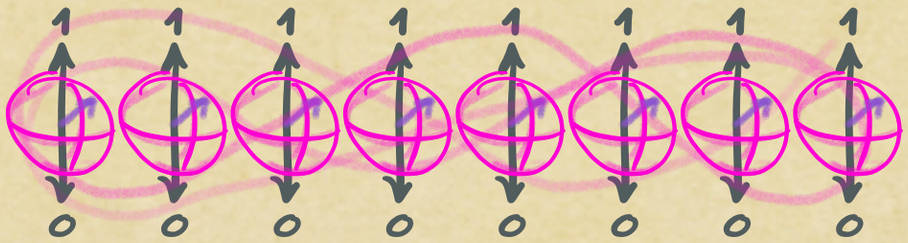
Bit :

Byte:



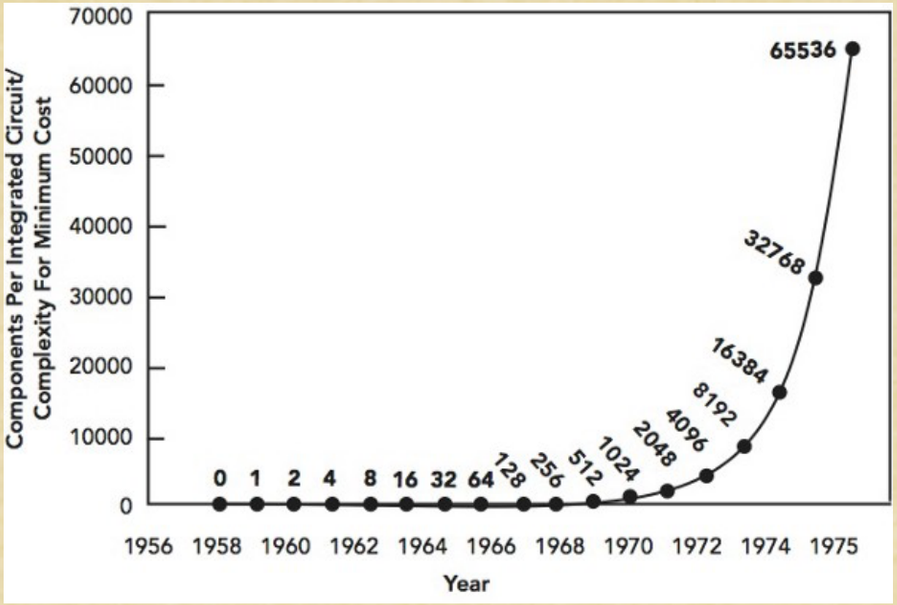
Qubit :

Qubyte ?



1. "NOW THAT MOORE'S LAW IS REACHING ITS PHYSICAL LIMIT WE NEED QUANTUM COMPUTERS TO CONTINUE THE TREND."

MOORE'S LAW:
COMPUTING POWER
(TRANSISTOR COUNT)
DOUBLES EVERY
2 YEARS.



GRAIN OF TRUTH: QUANTUM COMPUTERS DO NOT FACE THE SAME PHYSICAL LIMITS ...

PROBLEM: QUANTUM COMPUTERS ARE NOT JUST "BETTER COMPUTERS".

4. "Quantum Computers will Revolutionize Artificial Intelligence."

Grain of truth:

Many promising Quantum M.L. algorithms through the years!

Problem:

Every time, a classical algorithm was then found that does the same job.

4. "Quantum Computers will Revolutionize Artificial Intelligence."

Grain of truth:

Many promising Quantum M.L. algorithms through the years!

Problem:

Every time, a classical algorithm was then found that does the same job.

Silver lining:

Quantum Machine Learning on Quantum Data!

(A 19 y.o. BS student!)

5. "Quantum Computers can break any code."

Simply **False**.

But Big Grain of Truth:

Quantum Computers break **all** popular choices of Asymmetric Cryptography in use since the 80's!

(**Yes**, that includes Bitcoin/Ethereum)

SHOR'S ALGORITHM

- DISCOVERED IN 1994
- KICKSTARTED A RACE

$n \rightarrow p \cdot q$

BREAKS:

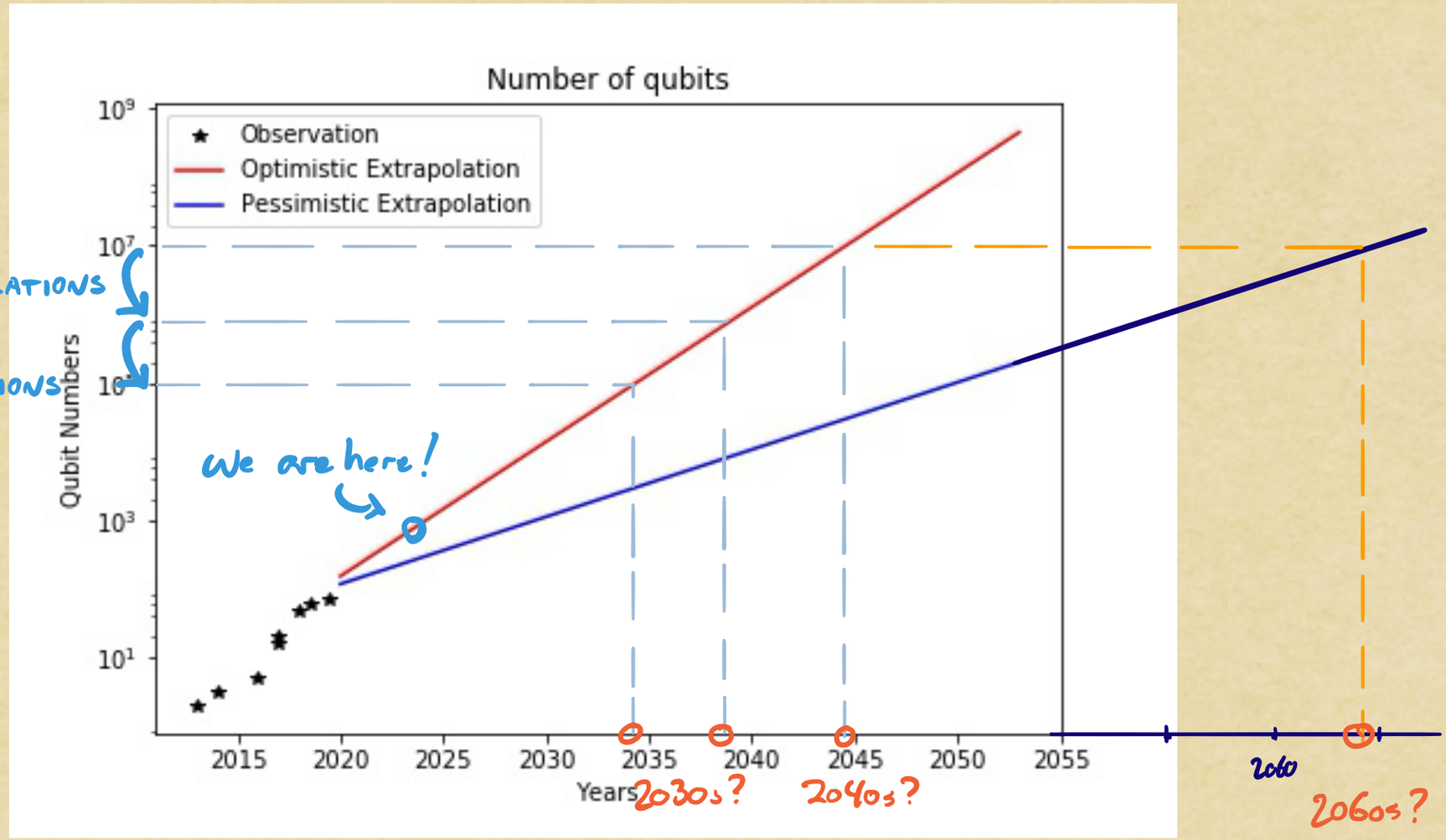
✗ RSA

✗ DIFFIE - HELLMAN

✗ EC-DSA

...AND MORE

So when is the Quantum Apocalypse?



~ Between 10 and 40 years from now?

TL;DR

As far as we know, Quantum Computers will be good for two things:

1. Simulating Quantum Nature
2. Breaking Asymmetric Crypto

Solution: Go back to only symmetric crypto?

No! New quantum-safe Asymmetric alternatives on the horizon:

Post-Quantum Cryptography

Questions? → hans.heum@ntnu.no