Moving the Goal to Post Quantum

Prof. dr. ir. Roland van Rijswijk-Deij
University of Twente, The Netherlands

Photo by My Profit Tutor on Unsplash

WHO HERE HAS NOT HEARD OF QUANTUM COMPUTING?

Photo by Camylla Battani on Unsplash

HYPER HYPER

Quantum Computing Hype Cycle Just Getting Started

Quantum computing could be to the 2020s what cloud computing was to the 2010s

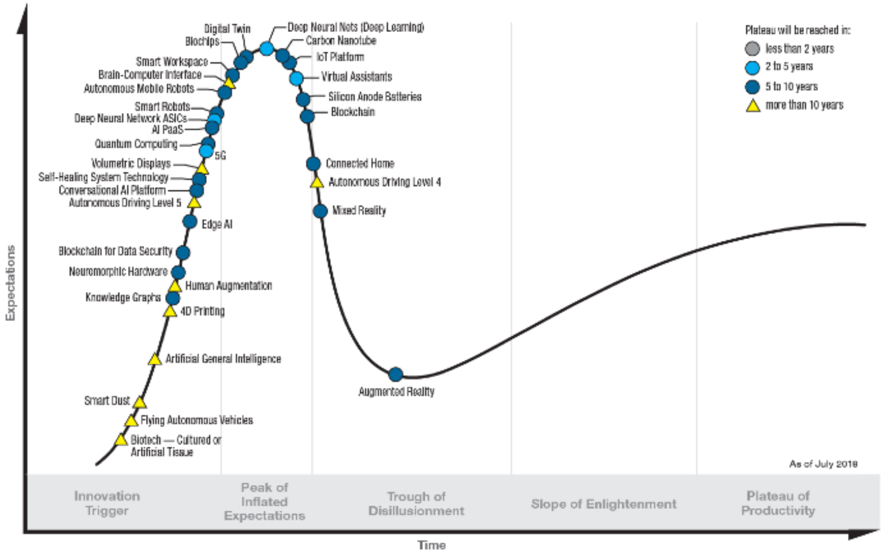
By **Dana Blankenhorn, InvestorPlace Contributor** Jul 25, 2018, 1:24 pm EST

April 18, 2019 | Contributor: Kasey Panetta

Quantum computing is not a cure-all for business computing challenges

by **James Sanders** in **Innovation** on May 16, 2019, 11:05 AM PST

Hype Cycle for Emerging Technologies, 2018



Quantum Computing Under Hype Cycle and Market Clock Scrutiny

With new technology come the plaudits and the critics. Quantum computing is no different from any other sector

By **James Dargan** - August 1, 2019 46 0

The hype around quantum computing: it's not too early to get in

by Jurgita Lapienytė 15 February 2021

TUCCR.

Twente University Centre for Cybersecurity Research

HYPE ➡️ PRESSURE ➡️ MISTAKES

HYPE ➡️ PRESSURE ➡️ MISTAKES

NOS Nieuws • Maandag 8 maart 2021, 17:00 •
Aangepast maandag 8 maart 2021, 22:18

Onderzoeker Kouwenhoven erkent fout: deeltje voor quantumcomputer niet gevonden

HYPE ➡️ PRESSURE ➡️ MISTAKES

NOS Nieuws • Maandag 8 maart 2021, 17:00 •
Aangepast maandag 8 maart 2021, 22:18

Onderzoeker Kouwenhoven erkent fout: deeltje voor quantumcomputer niet gevonden

SCIENCE

17 maart 2022 - 11:05 door Jos Wassink

Kouwenhoven departs, Microsoft presents Majoranas

In a strange combination of events, Microsoft announced both the departure of Leo Kouwenhoven this week ánd the discovery of scalable Majoranas – developed in Denmark.

HYPE ➡️ PRESSURE ➡️ MISTAKES

NOS Nieuws • Maandag 8 maart 2021, 17:00 •
Aangepast maandag 8 maart 2021, 22:18

Onderzoeker Kouwenhoven erkent fout: deeltje voor quantumcomputer niet gevonden

SCIENCE

17 maart 2022 - 11:05 door Jos Wassink

Kouwenhoven departs, Microsoft presents Majoranas

In a strange combination of events, Microsoft announced both the departure of Leo Kouwenhoven this week ánd the discovery of scalable Majoranas – developed in Denmark.

Delftse onderzoekers kwantumcomputers 'verwijtbaar onzorgvuldig'

Geen schending wetenschappelijke integriteit.

Het College van Bestuur van de TU Delft oordeelt dat Leo Kouwenhoven en Hao Zhang 'onzorgvuldig' hebben gehandeld en dat er deels ook sprake is van 'verwijtbare onzorgvuldigheid' bij de publicatie van hun werk over Majoranadeeltjes. Deze deeltjes zijn veelbelovend als basis voor een stabiele kwantumcomputer.

Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*

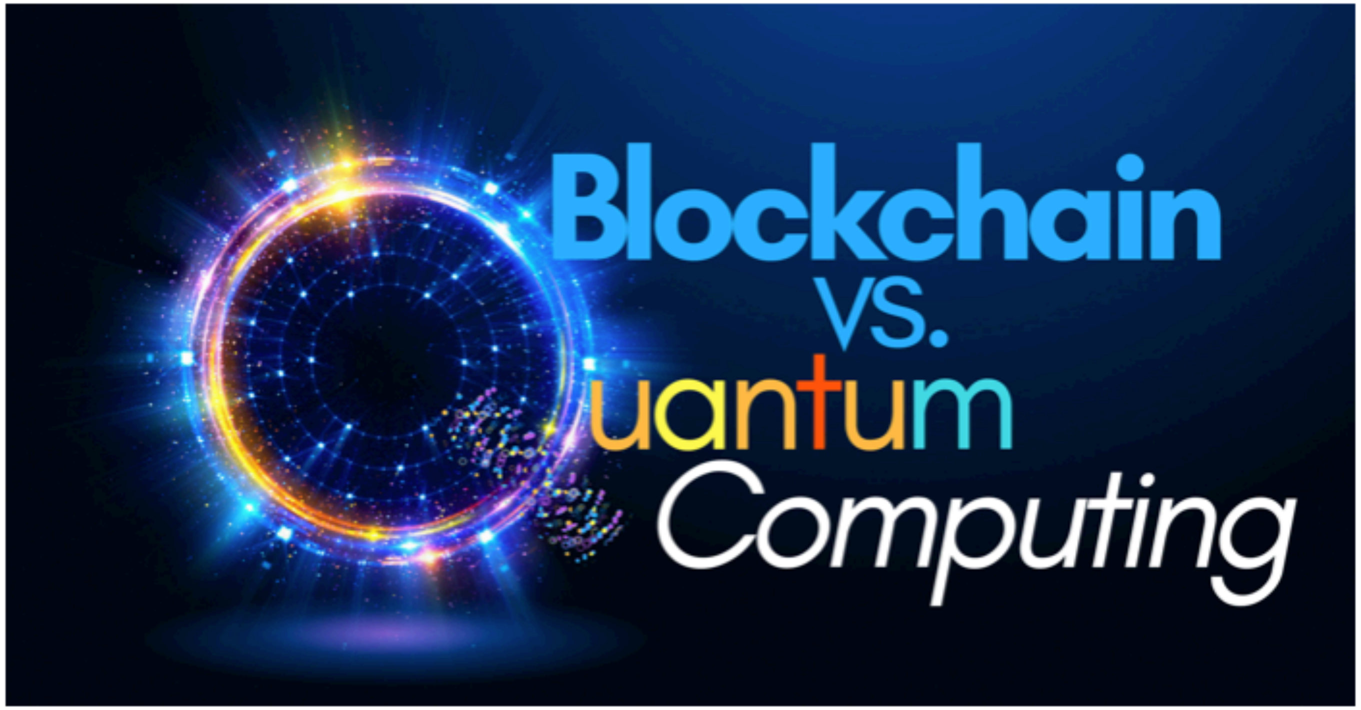

QUANTUMSUPREMACY
10.23.19

OK, ONE MORE 'CAUSE I CAN'T RESIST...

Quantum Computing: Is it the end of blockchain?

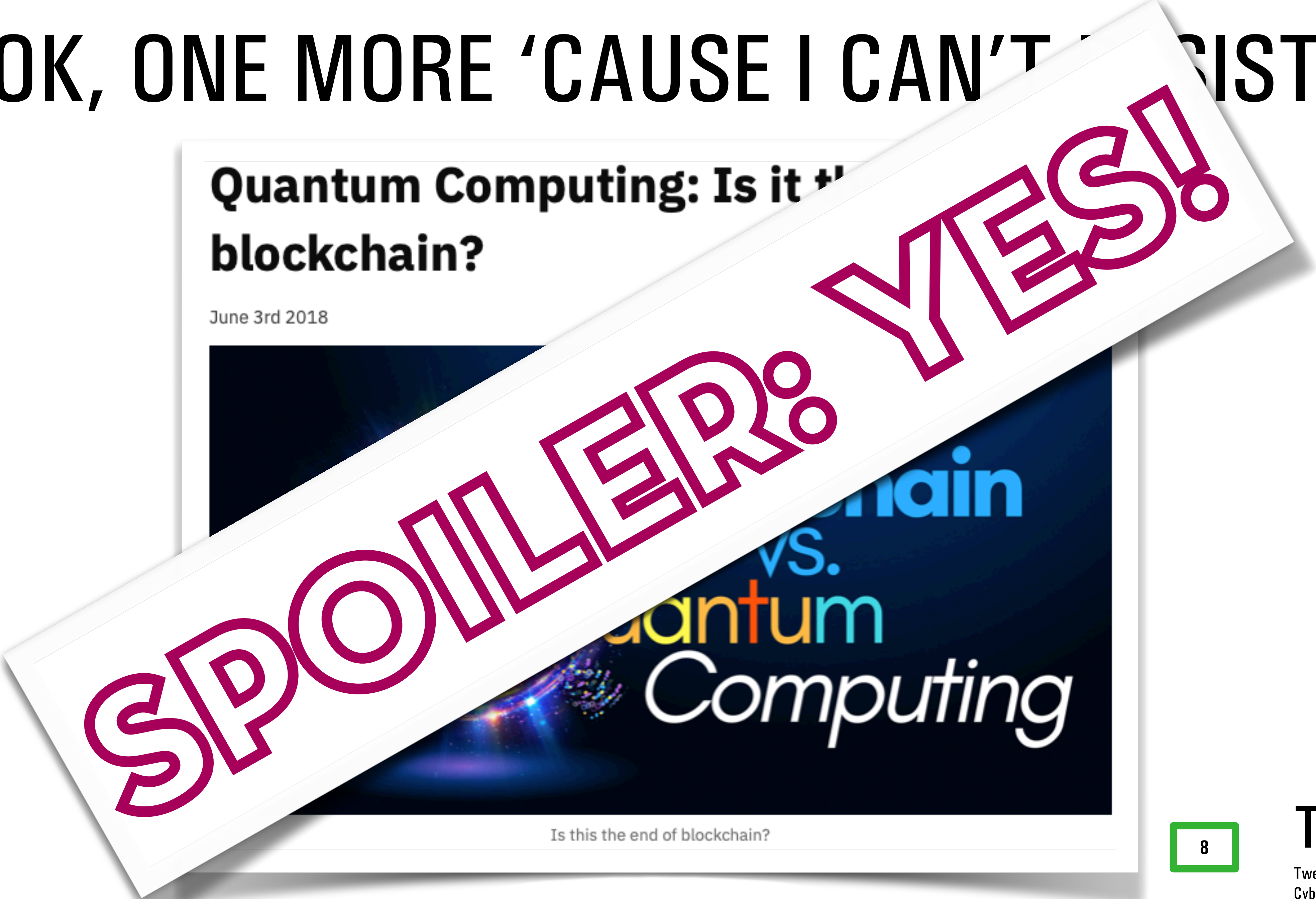
June 3rd 2018

TWEET THIS



Is this the end of blockchain?

OK, ONE MORE ‘CAUSE I CAN’T [illegible]SIST...



THE HYPE ISN'T HELPFUL

- The tech **news sites are abuzz with quantum**
- It may seem like **quantum computing is just around the corner**
- And that **it's going to change the world** (it is)
- Some **quick facts**:
  - Practical quantum computers require **1,000s of** so-called *logical qubits* (which consist of **10,000s of** *physical qubits*)
  - Google's **quantum supremacy machine had 53 physical qubits** — how supreme is that?

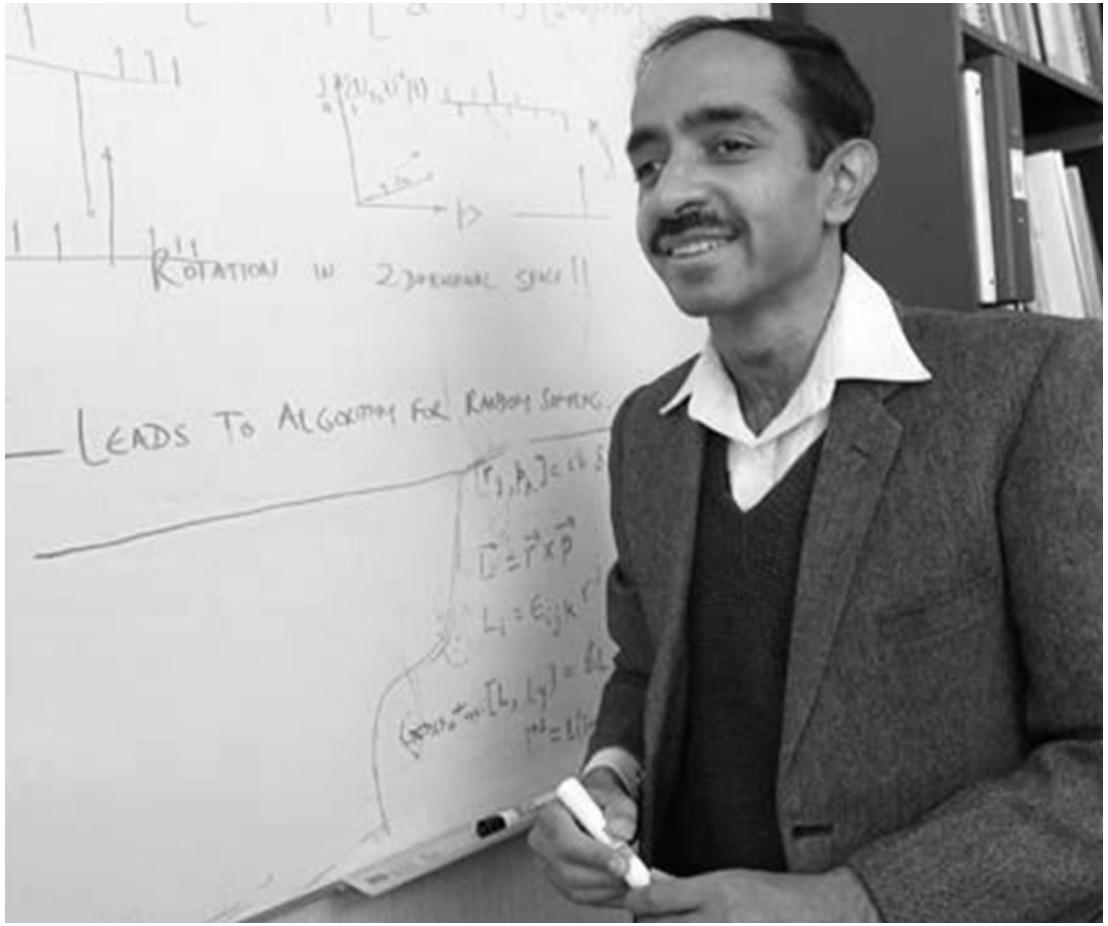
TUCCR.
Twente University Centre for Cybersecurity Research

THE HYPE ISN'T HELPFUL

Goal of this talk:
Poke through the hype and tell you *why you should care* about quantum computing and *what challenges we face* when *deploying quantum-resistant cryptography*

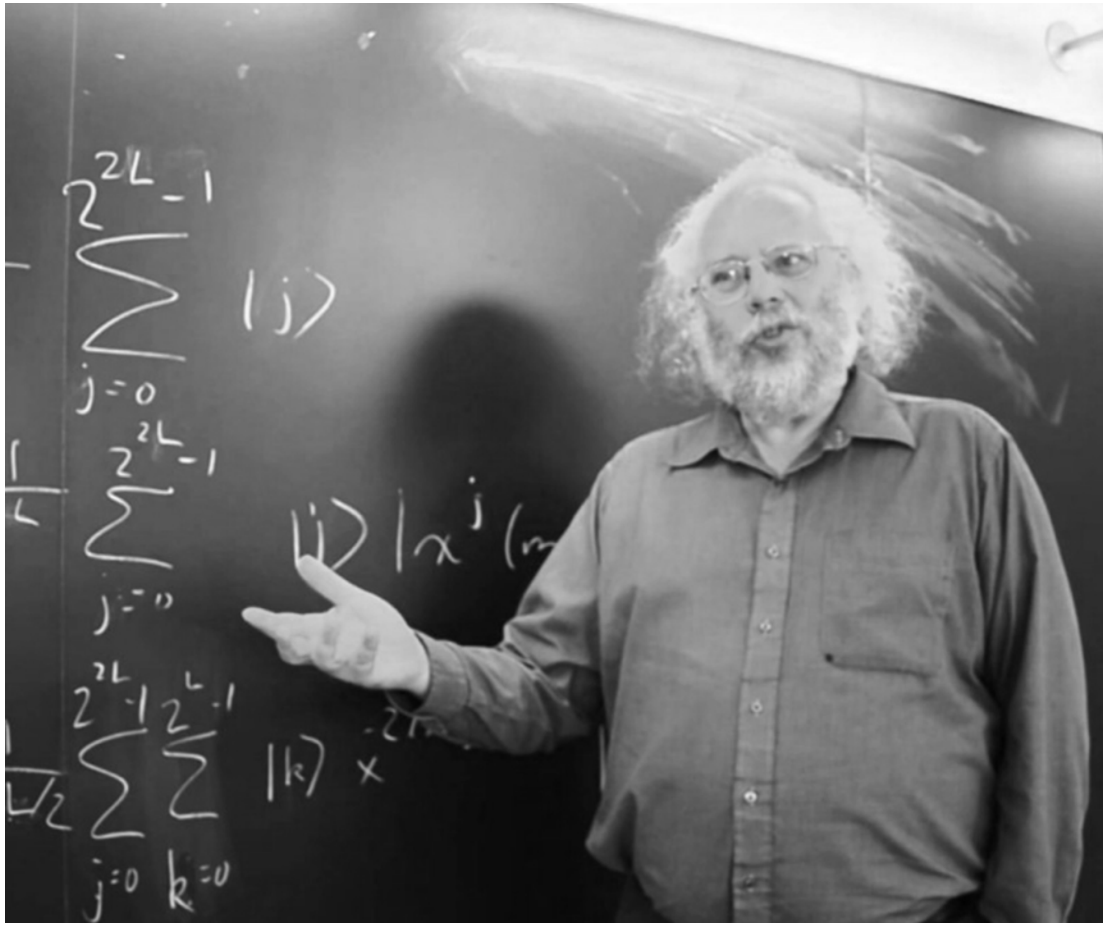
- The
- It ma **the corner**
- And
- Som
  - Pr o-called *lo al qubits*)
  - G **hysical qubits** — how supreme is that?

WHY, THEN, WORRY ABOUT QUANTUM?



Lov Grover

(image: dotquantum.io)



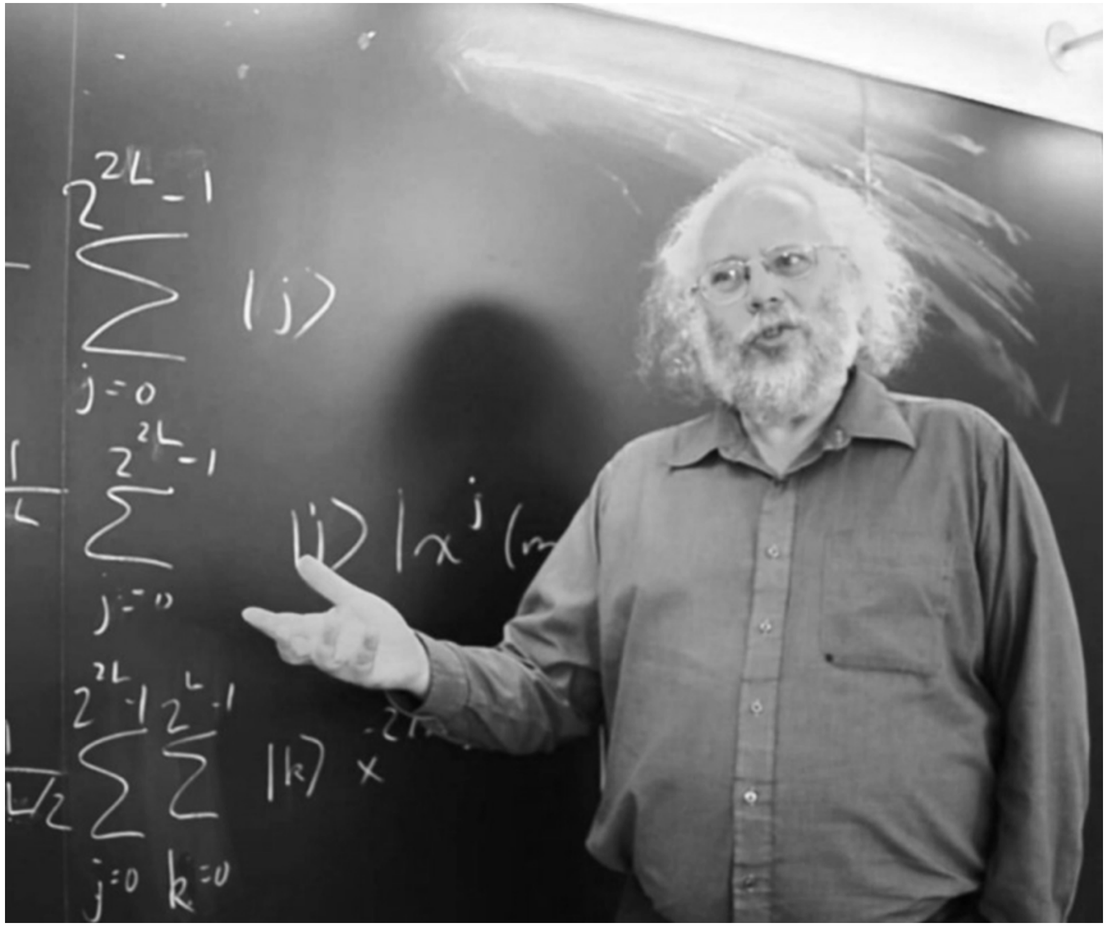
Peter Shor

(image: dotquantum.io)

WHY, THEN, WORRY ABOUT QUANTUM?

Great theory, but
no relevant **impact**
on cryptography

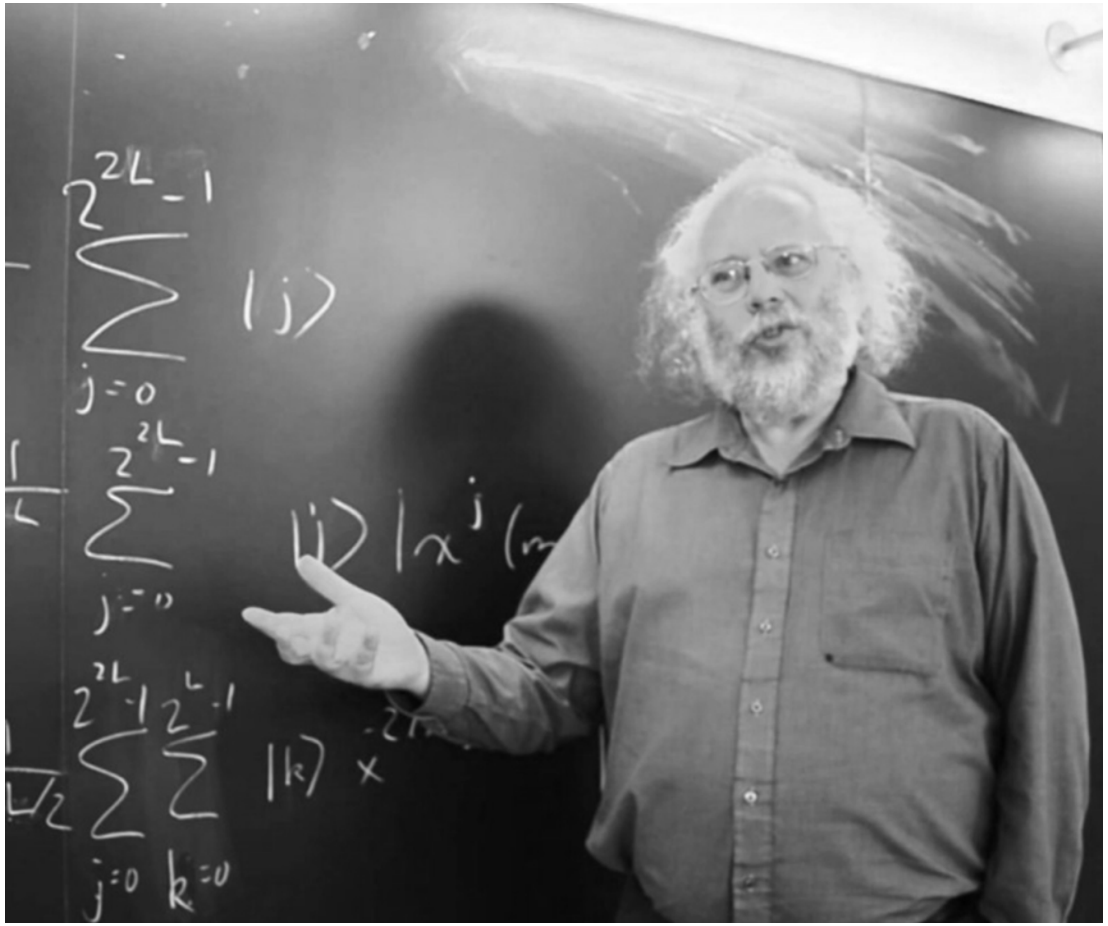
Lov Grover
(image: dotquantum.io)



Peter Shor
(image: dotquantum.io)

SHOR'S ALGORITHM

- Reduces effort of factoring integers and solving discrete logarithms to **polynomial time**
- This is a **big deal** - a sufficiently powerful quantum computer **could break all current public key crypto**
- E.g. break RSA 2048 **in hours**

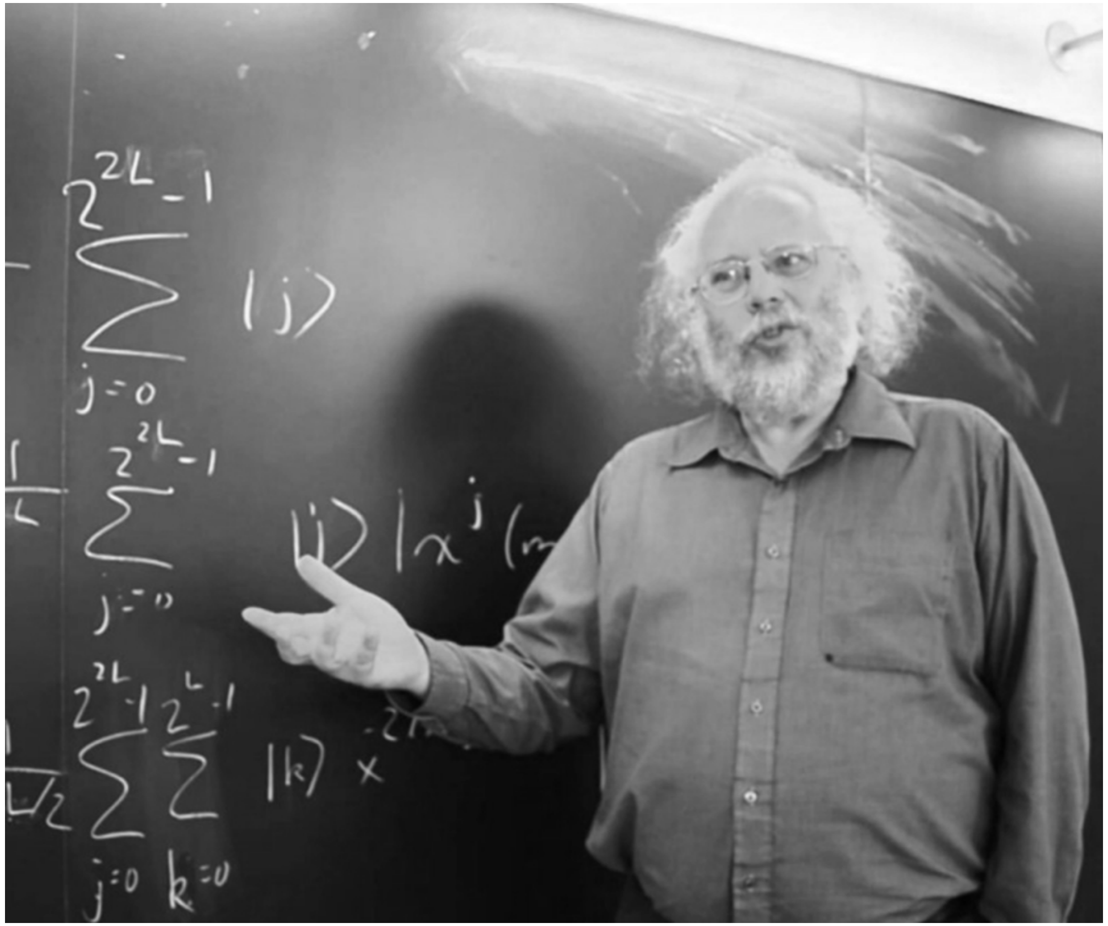


Peter Shor

(image: dotquantum.io)

SHOR'S ALGORITHM: IMPACT

- **Asymmetric crypto** is used for many purposes: **key negotiation and authentication for HTTPS, legally binding digital signatures, …, …, …**
- A sufficiently powerful **quantum computer would cause major problems for all** of **the Internet**



Peter Shor

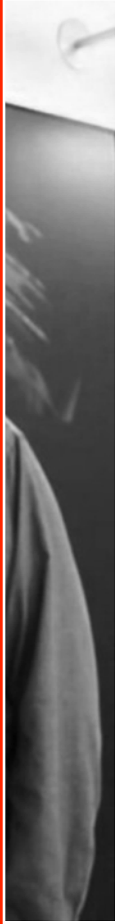
(image: dotquantum.io)

SHOR'S ALGORITHM: IMPACT

In normal user terms,
we go from this:

to this:

For **all of the Internet**



(image: dotquantum.io)

TUCCR.
Twente University Centre for
Cybersecurity Research

WHEN WILL SHOR BE A PROBLEM?

Public Key System	Key Size	Security	Logical qubits	Physical qubits	Running time
RSA	1024 bits	80 bits	2,050	8.05×10^6	4 hours
	2048 bits	**112 bits**	**4,098**	**8.56×10^6**	**29 hours**
	4096 bits	128 bits	8,194	1.12×10^7	~10 days
ECC	**256 bits**	**128 bits**	**2,330**	**8.56×10^6**	**11 hours**
	384 bits	192 bits	3,484	9.05×10^6	38 hours
	512 bits	256 bits	4,719	1.13×10^7	~2 days

Source: Grumbling, E. and Horowitz, M. (eds.), "Quantum Computing: Progress and Prospects", National Academy of Sciences, 2019

IBM unveils its 433 qubit Osprey quantum computer

Frederic Lardinois @fredericl 3:00 PM GMT+1 • November 9, 2022

Comment

Image Credits: Amardeep Singh / 500px / Getty Images

IBM unveils its 433 qubit Osprey quantum computer

Frederic Lardinois @fredericl 3:00 PM GMT+1 • November 9, 2022

Comment

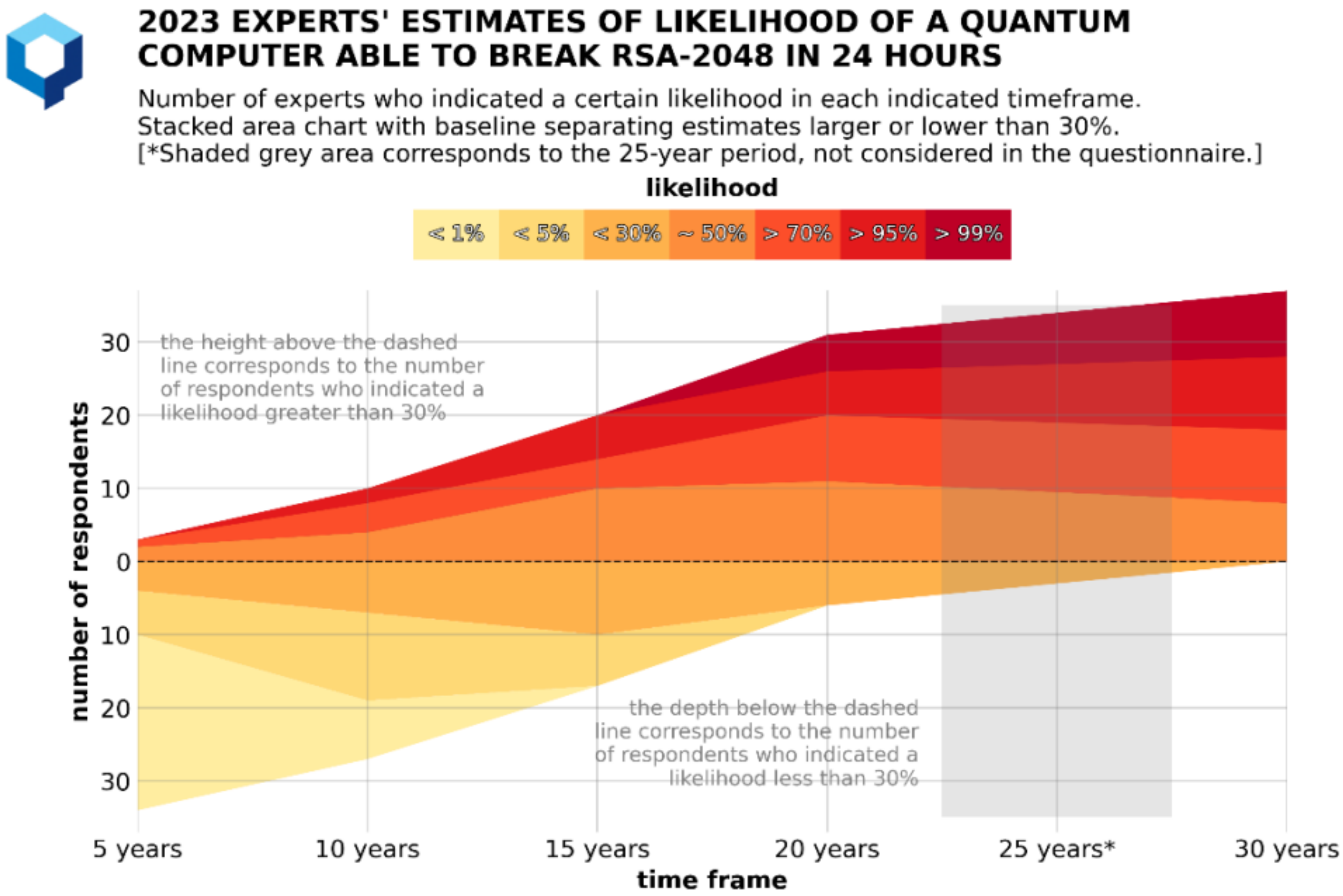
Image Credits: Amardeep Singh / 500px / Getty Images

WHEN WILL SHOR BE A PROBLEM?

Public Key System	Key Size	Security	Logical qubits	Physical qubits	Running time
RSA	1024 bits	80 bits	2,050	8.05×10^6	4 hours
	2048 bits	**112 bits**	**4,098**	$\mathbf{8.56 \times 10^6}$	**29 hours**
	4096 bits	128 bits	8,194	1.12×10^7	~10 days
ECC	**256 bits**	**128 bits**	**2,330**	$\mathbf{8.56 \times 10^6}$	**11 hours**
	384 bits	192 bits	3,484	9.05×10^6	38 hours
	512 bits	256 bits	4,719	1.13×10^7	~2 days

Source: Grumbling, E. and Horowitz, M. (eds.), "Quantum Computing: Progress and Prospects", National Academy of Sciences, 2019

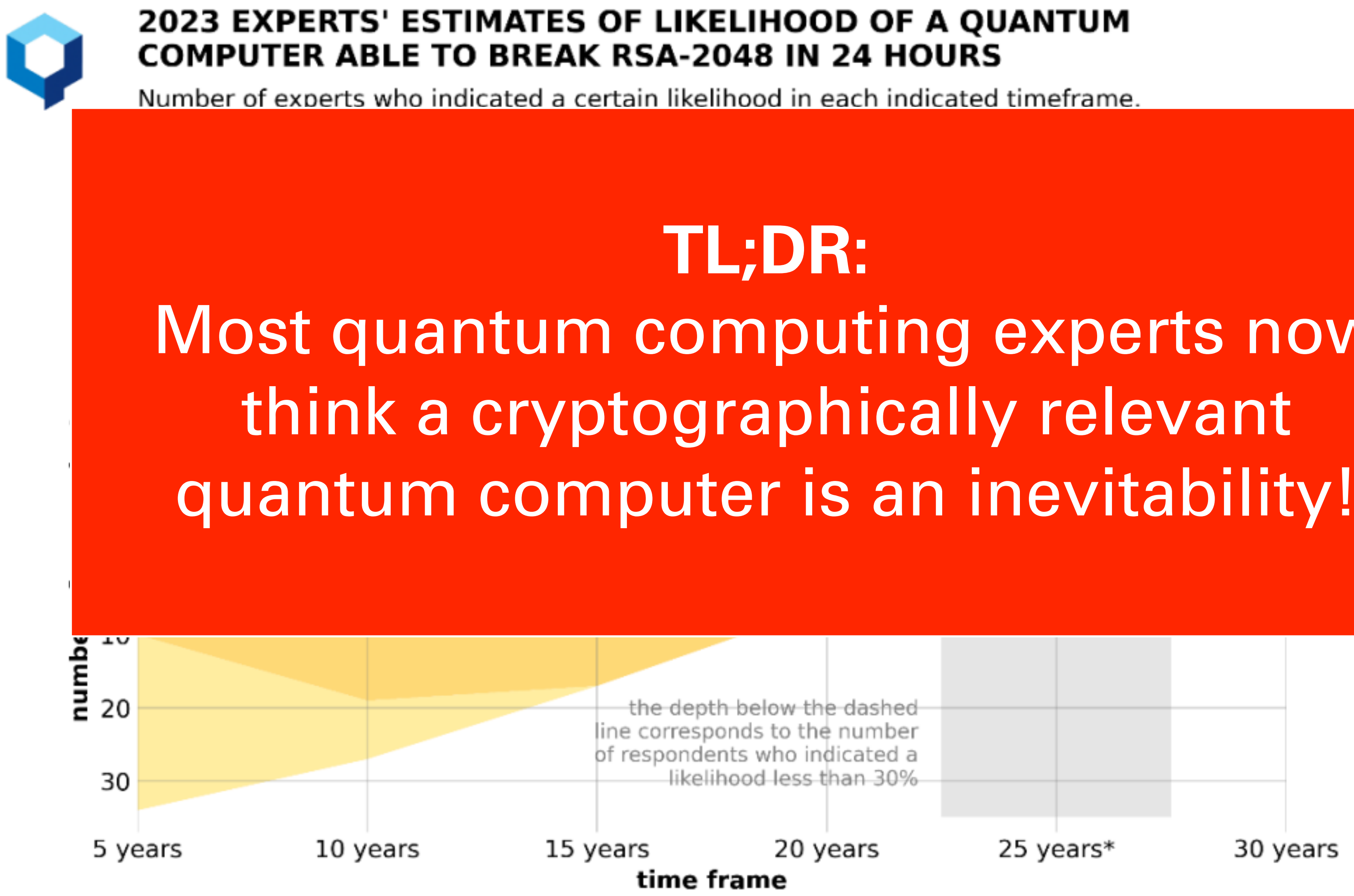
WHAT QUANTUM EXPERTS THINK



source: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

TUCCR.
Twente University Centre for Cybersecurity Research

WHAT QUANTUM EXPERTS THINK



TL;DR:

Most quantum computing experts now think a cryptographically relevant quantum computer is an inevitability!

source: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

TUCCR.

Twente University Centre for Cybersecurity Research

TIME OF USE

- Whether we are safe **depends on how long** cryptographic **data is used**
- Rule of thumb:
  - **Short-term use**: no need to worry and **no need for immediate action**
  - **Long(er)-term use**: need to start **think**ing **about transitioning now**

Photo by Abdul A on Unsplash

TIME OF USE EXAMPLES

- **Short-term use:**
  (Two-factor) authentication, short-lived digital signatures (e.g. website certificates), online authentication protocols such as OpenID connect, SAML, … (essentially **anything where the result of the cryptographic operation loses relevance quickly**)

- **Long-term use:**
  Encrypted long-term archives, legally binding digital signatures, ephemeral key exchange, … (essentially **anything where the result of the cryptographic operation should be safe for decades**)

POST QUANTUM CRYPTOGRAPHY

- Cryptographers are working on **new public key algorithms** that are “**quantum safe**”
- That is: they **remain secure**, even **after a** sufficiently powerful **quantum computer comes to be**
- Development states of algorithms range **from ripe to green**

post- /pəʊst/ a prefix, meaning “behind,” “after,” “later,” “subsequent to,” “posterior to,” occurring originally in loanwords from Latin (postscript), but now used freely in the formation of compound words (*post-Elizabethan; postfix; postgraduate; postorbital*).

RADICALLY DIFFERENT

- For some algorithms, every key can **only** be **used once**
- Some require much **more CPU** power **or memory**
- Some algorithms have much **larger keys** (100s of KBs) **or signatures** (1,000s of bytes)
- Has **consequences for applications!**

Photo by Varvara Grabova on Unsplash

NIST COMPETITION

- Competition to select **secure quantum safe algorithms** for **different applications** (encryption, key exchange, signatures)
- End goal: **standardise secure and suitable algorithms**
- Current status: **first algorithms selected for standardisation**

National Institute of Standards and Technology
U.S. Department of Commerce

WHEN, NOT IF

- It is now a matter of **when, not if post quantum** algorithms **will be adopted**
- **Once** NIST **standards exist**, the US and other **governments** will start **requiring their use in tenders**
- This will **likely** take **years**, and **impact** many **Internet industries**

Photo by Martin Sanchez on Unsplash

ROCKY ROAD

- There is a **rocky road ahead**
- **PQC** has really **only** been **tested in** mainstream **Web** applications
- Yet the **Internet is** much **more than** just **the Web**
- The **$1B question: how do we transition the entire Internet to PQC?**
- This is the **main research question for** our **SHARQS** project

Photo by John Salzarulo on Unsplash

ROCKY ROAD

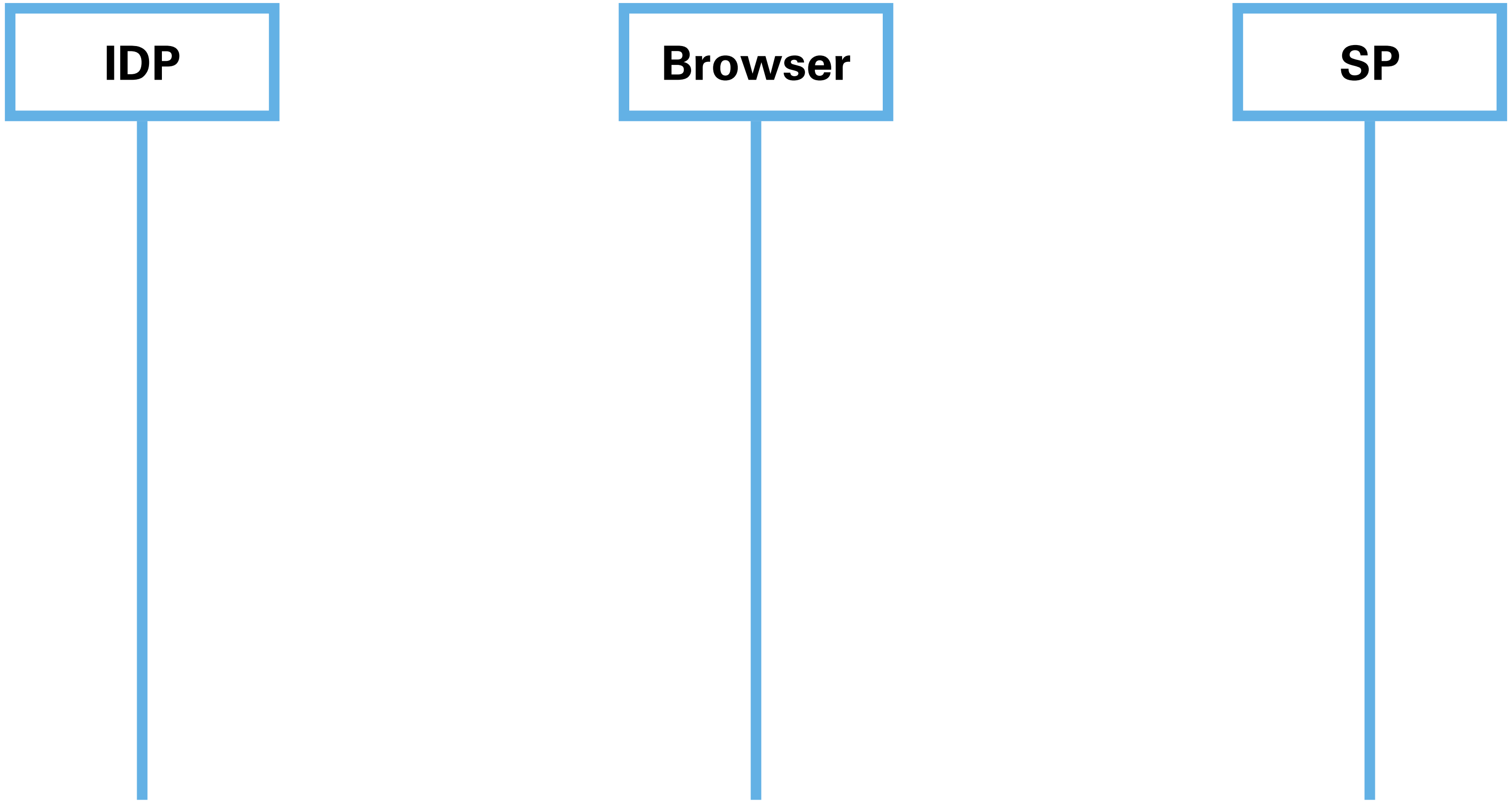
- Th
- **PQ**
  m
- Ye
  ju
- Th
  tra
  PQ
- Th
  for our SHARQS project

My esteemed academic colleagues working on post-quantum crypto think that **now we have algorithms we are** (almost) **done…**

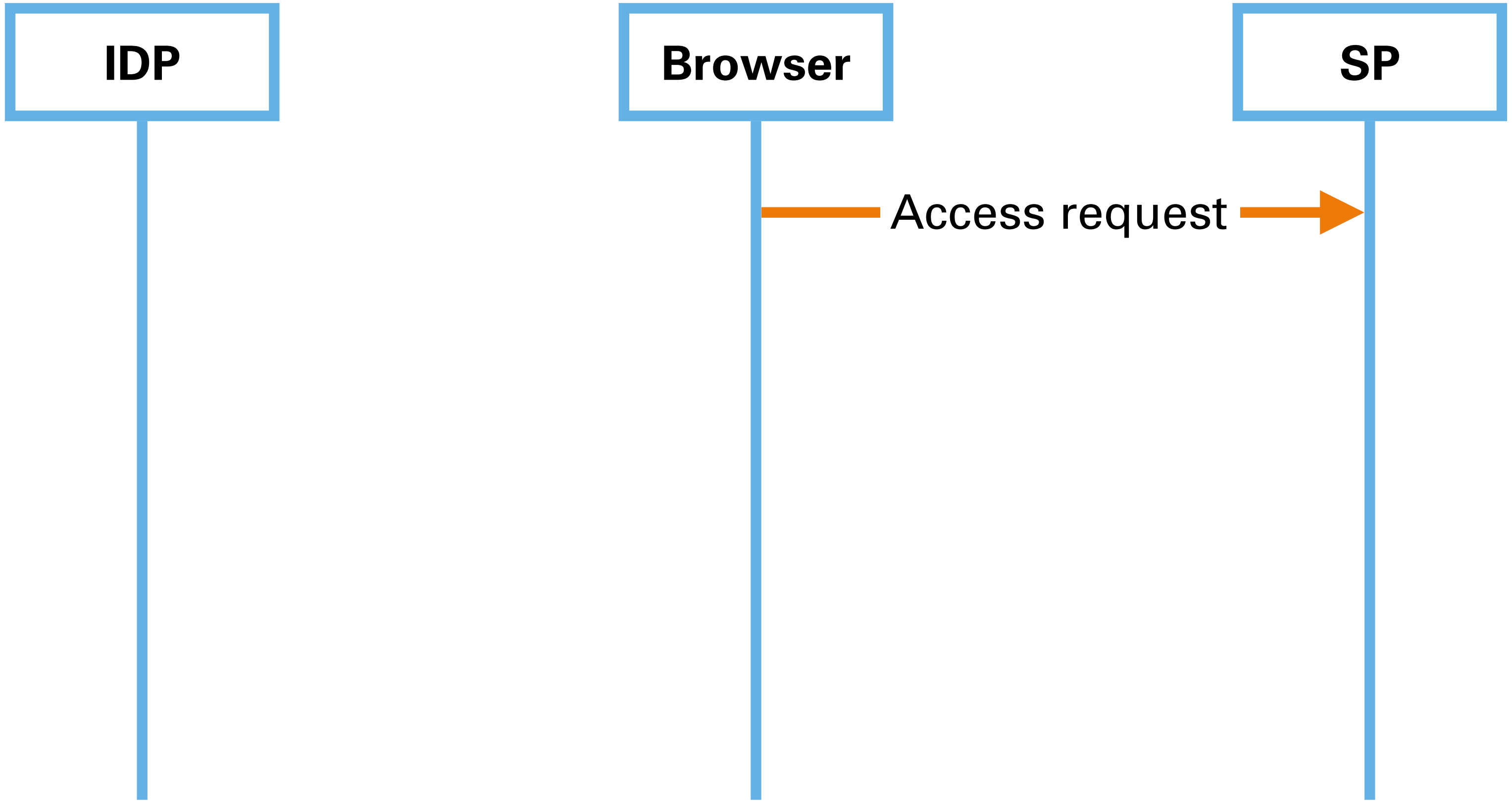
I think **they are wrong** 😁

Photo by John Salzarulo on Unsplash

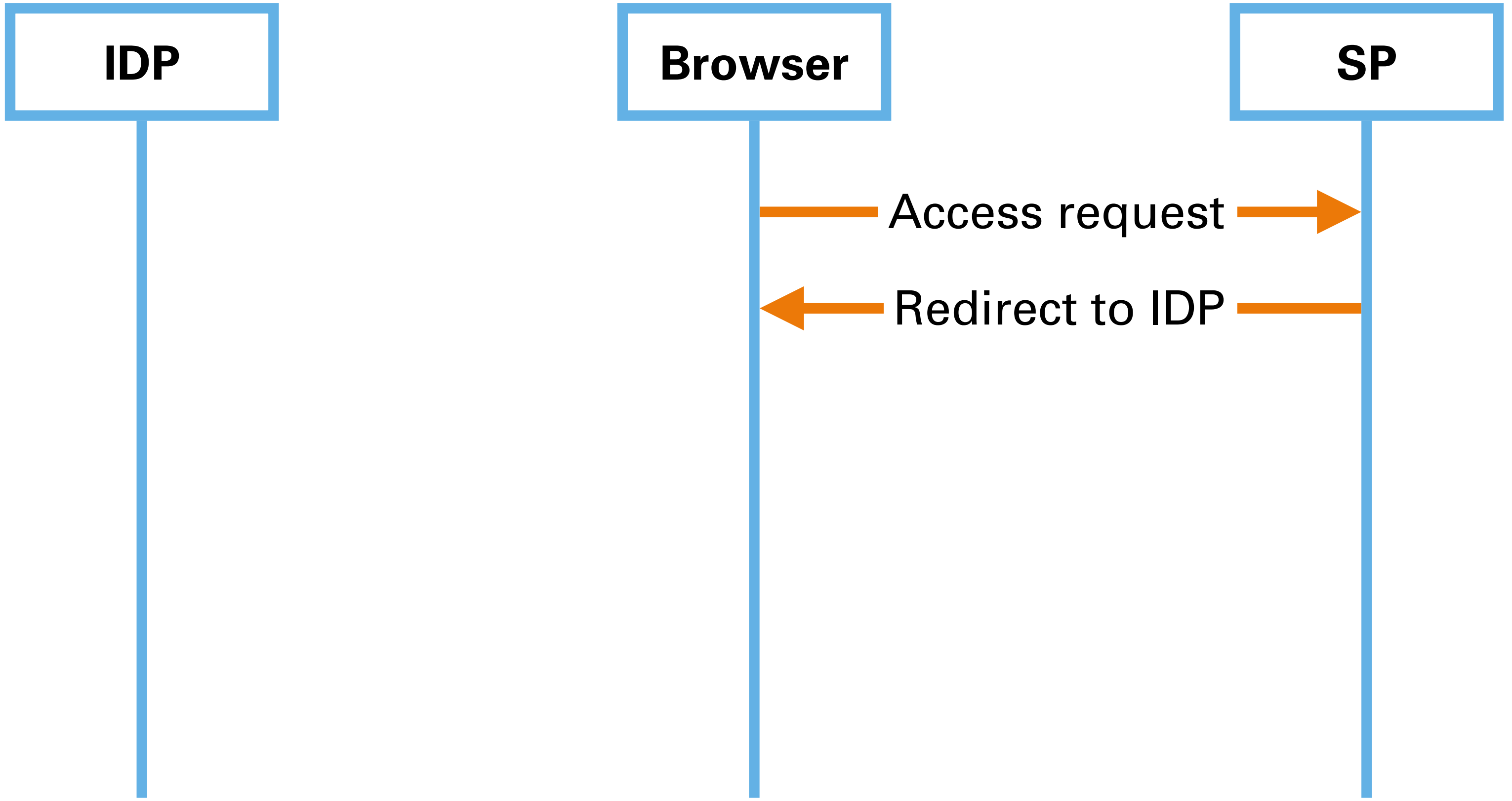
AN NREN EXAMPLE: FEDERATED IDENTITY



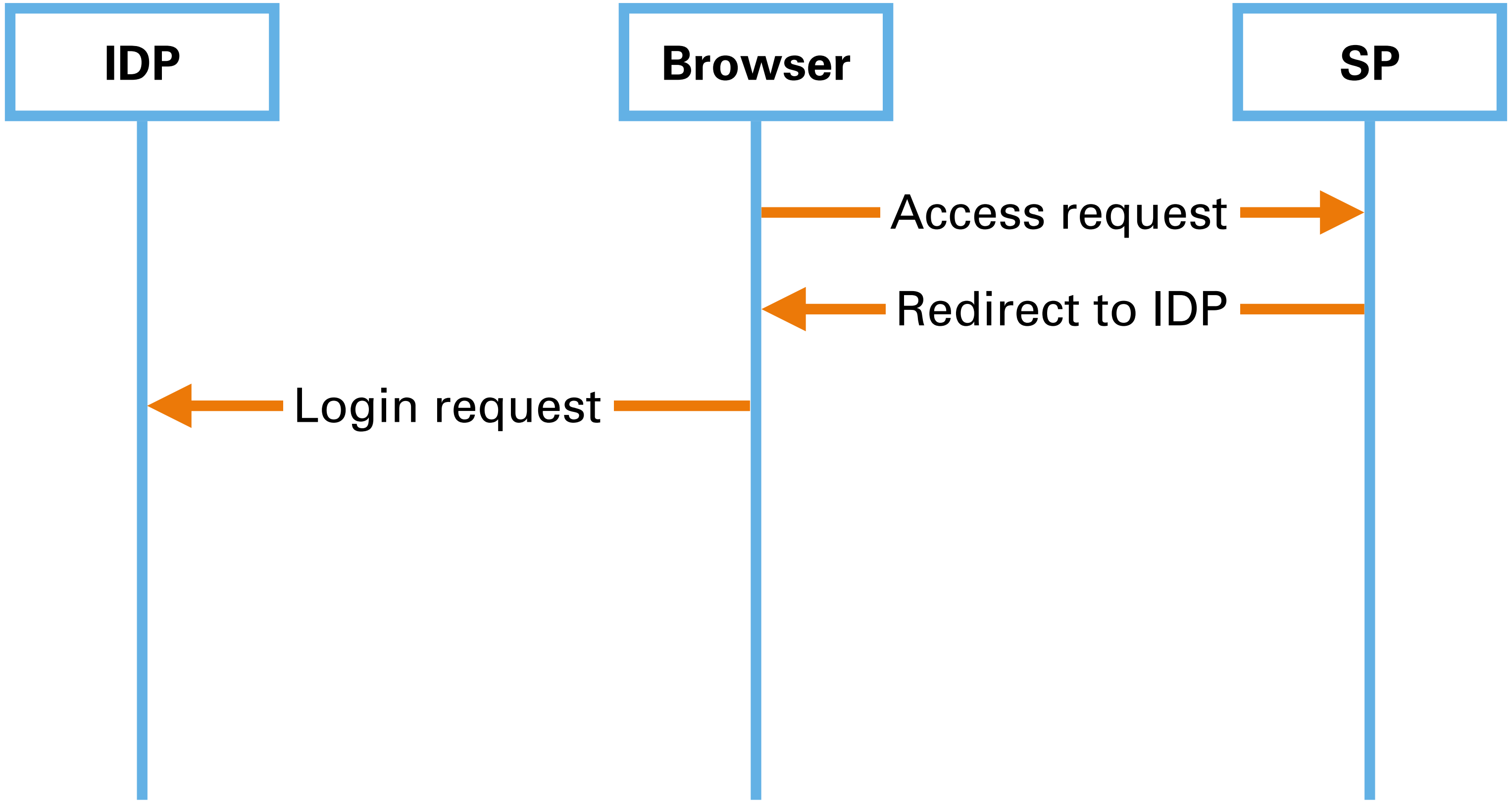
AN NREN EXAMPLE: FEDERATED IDENTITY



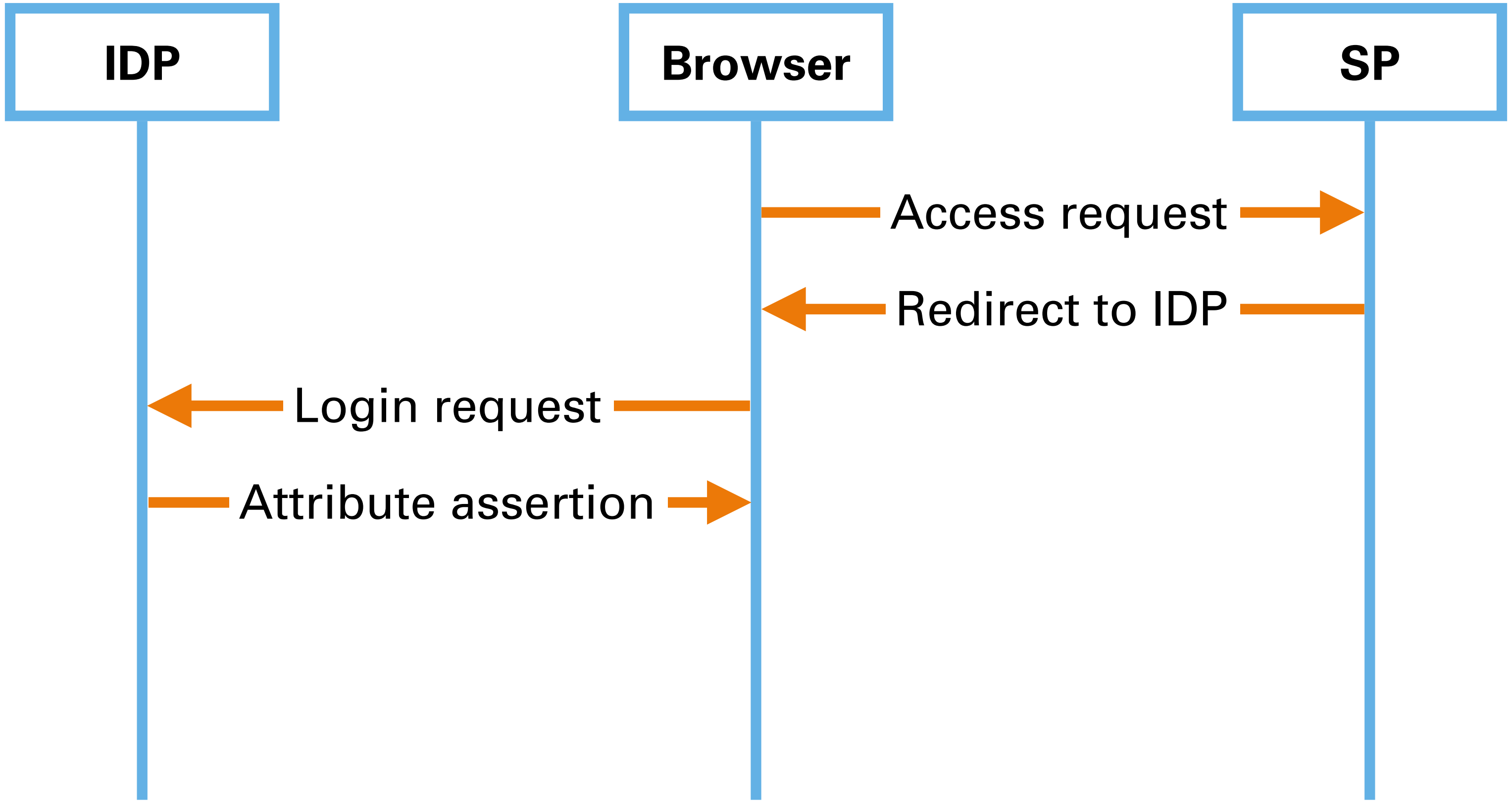
AN NREN EXAMPLE: FEDERATED IDENTITY



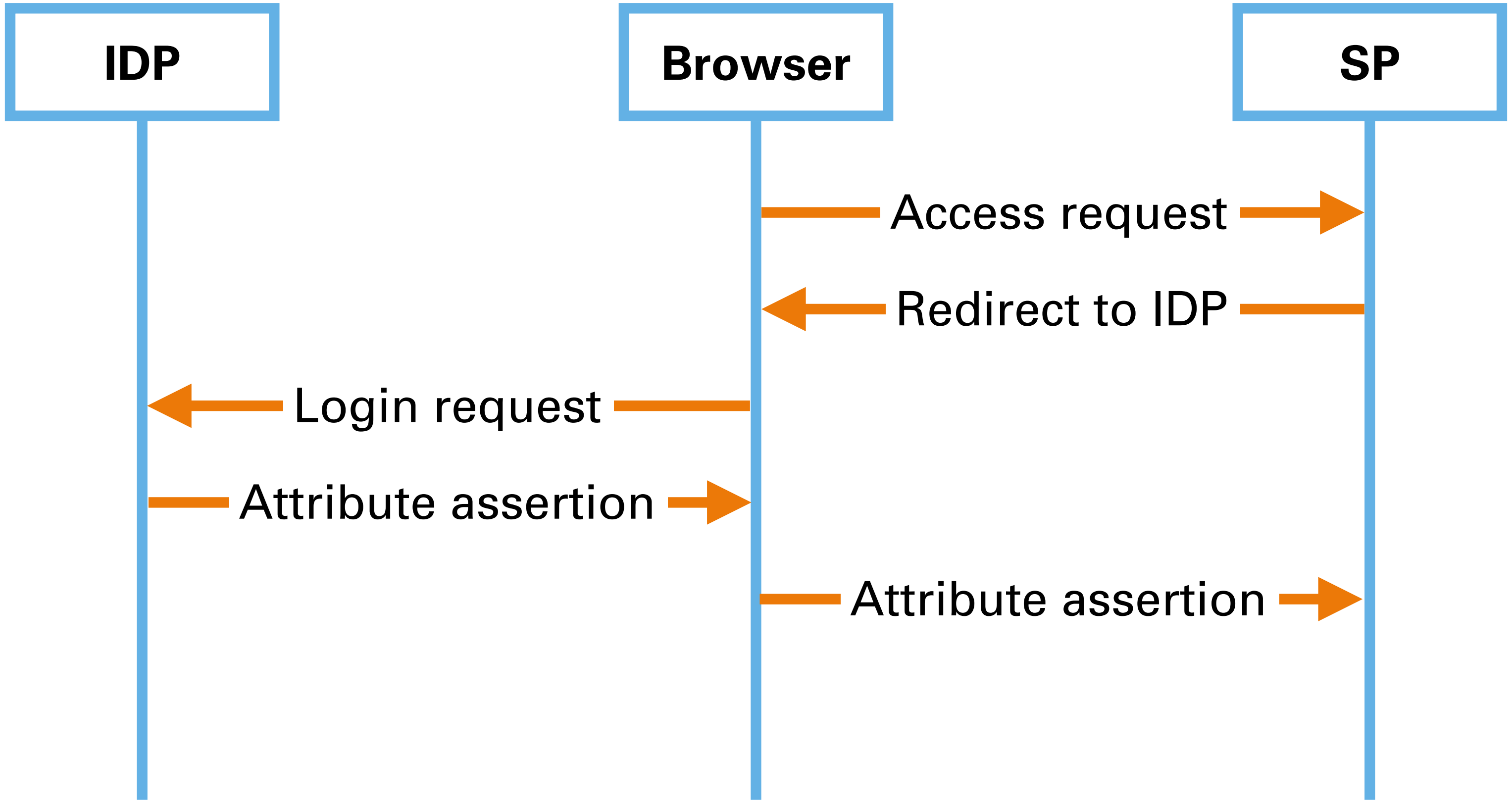
AN NREN EXAMPLE: FEDERATED IDENTITY



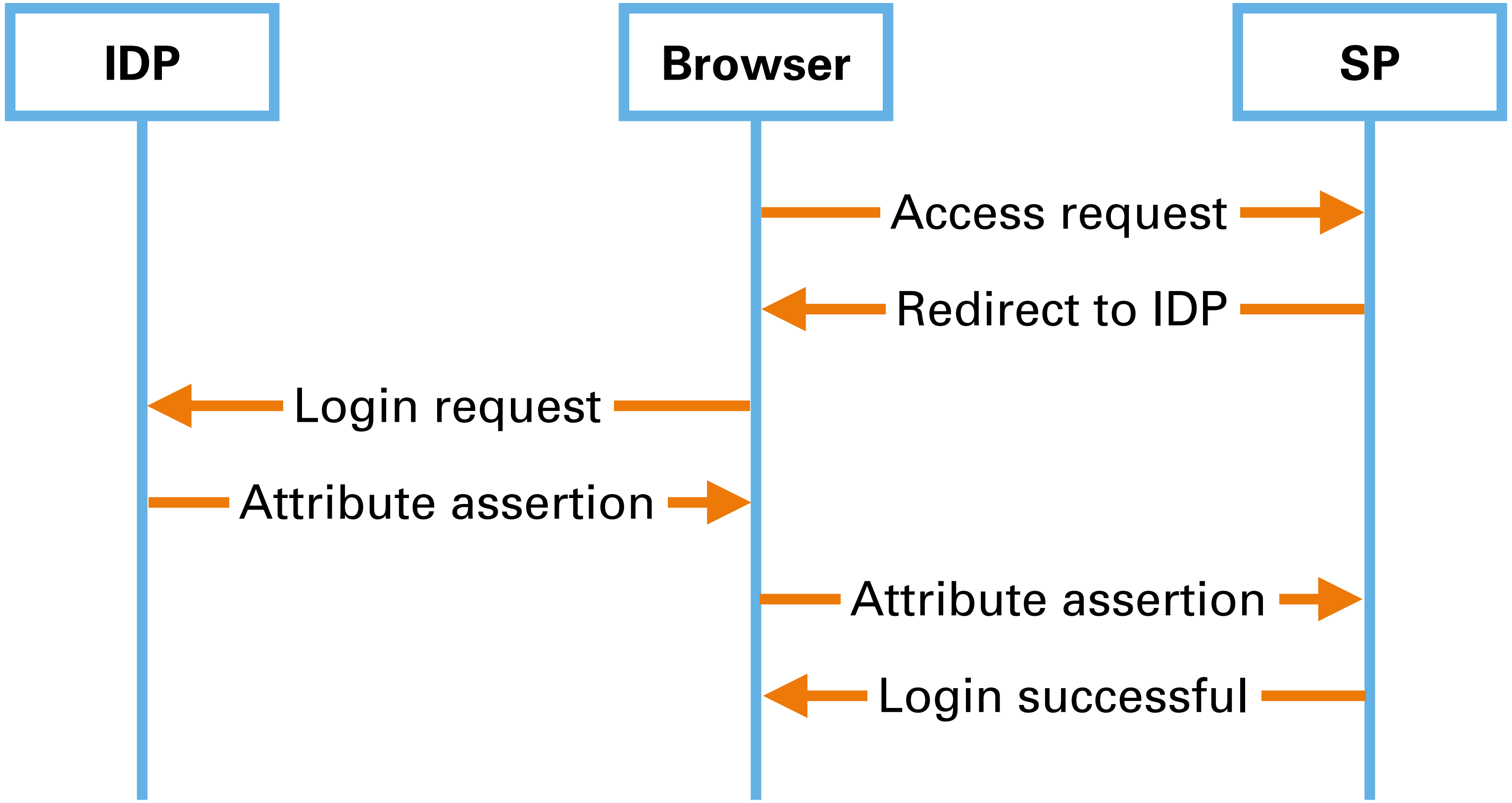
AN NREN EXAMPLE: FEDERATED IDENTITY



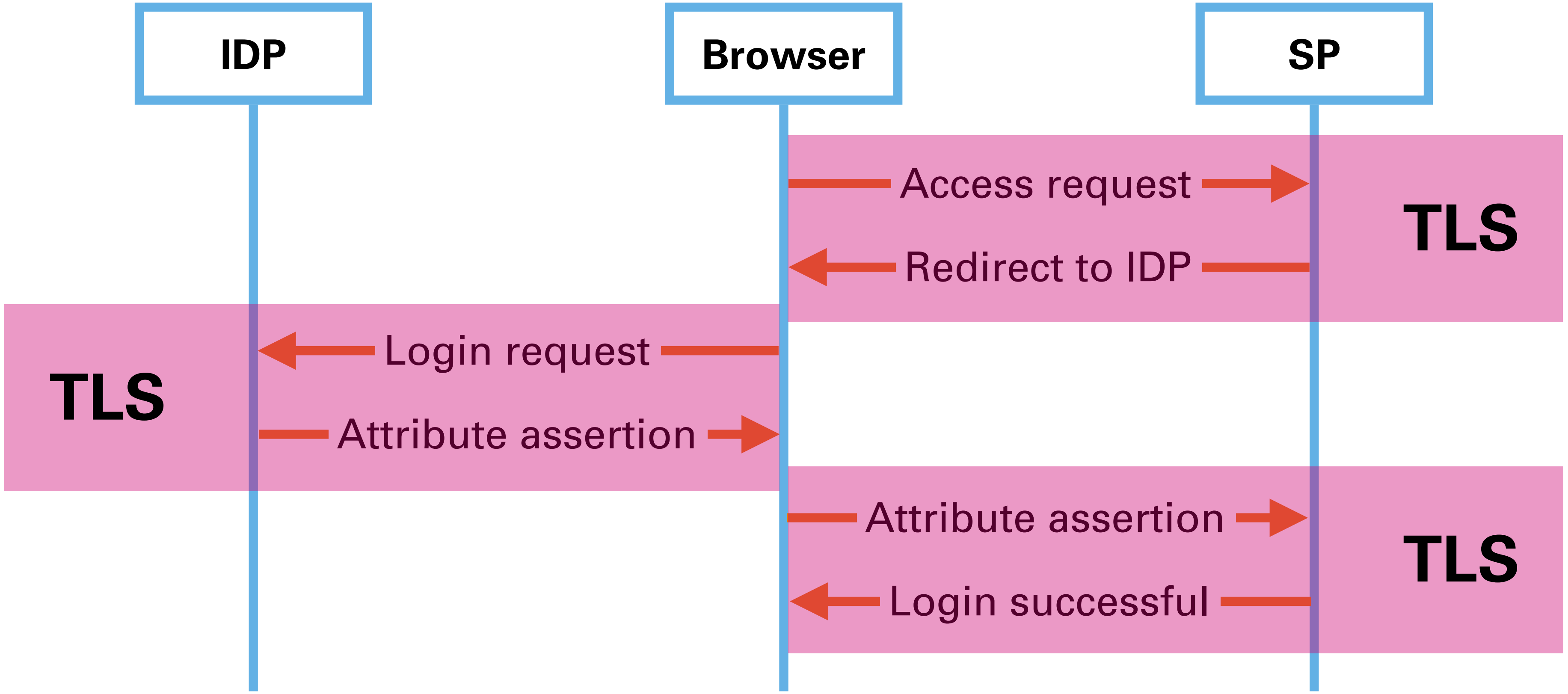
AN NREN EXAMPLE: FEDERATED IDENTITY



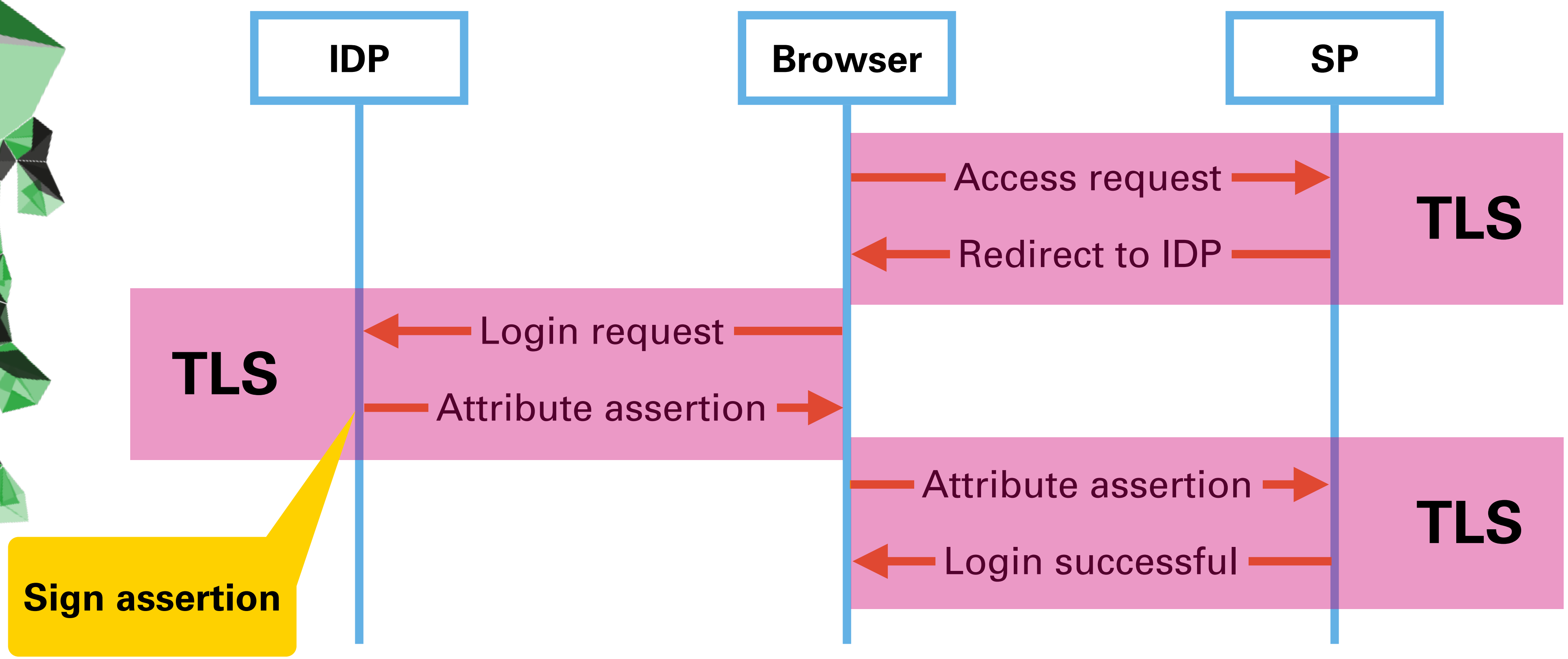
AN NREN EXAMPLE: FEDERATED IDENTITY



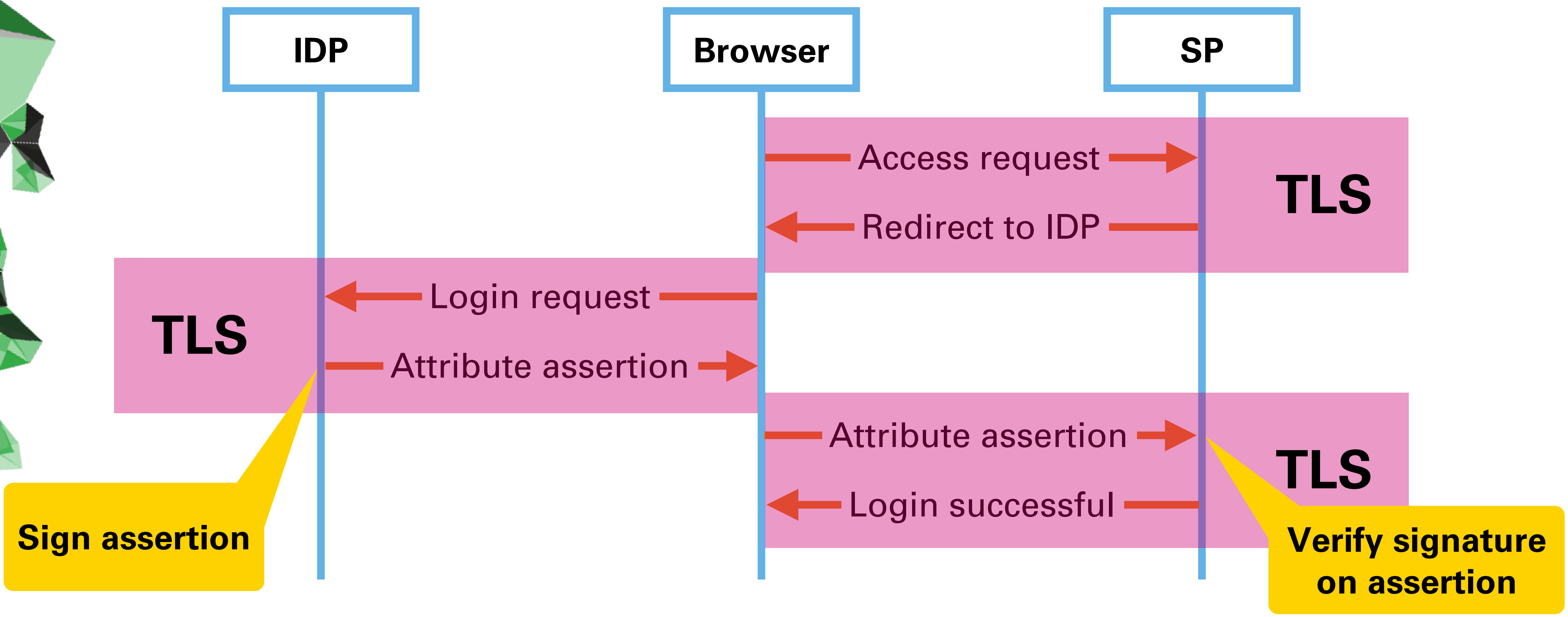
AN NREN EXAMPLE: FEDERATED IDENTITY



AN NREN EXAMPLE: FEDERATED IDENTITY

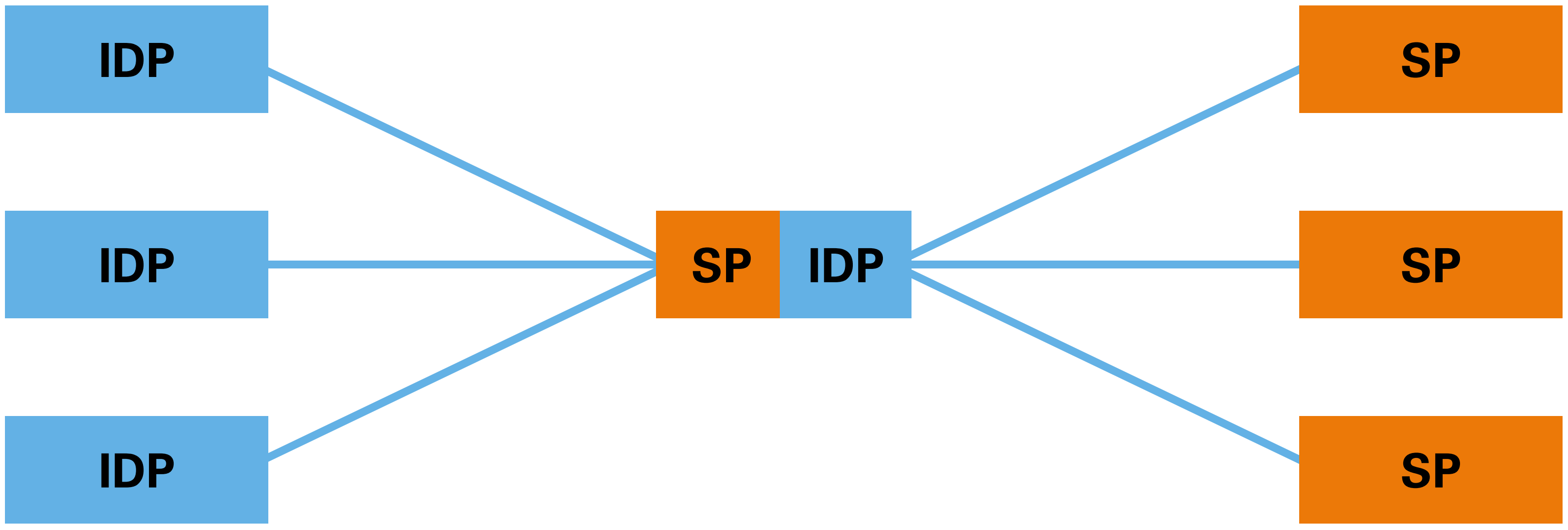


AN NREN EXAMPLE: FEDERATED IDENTITY

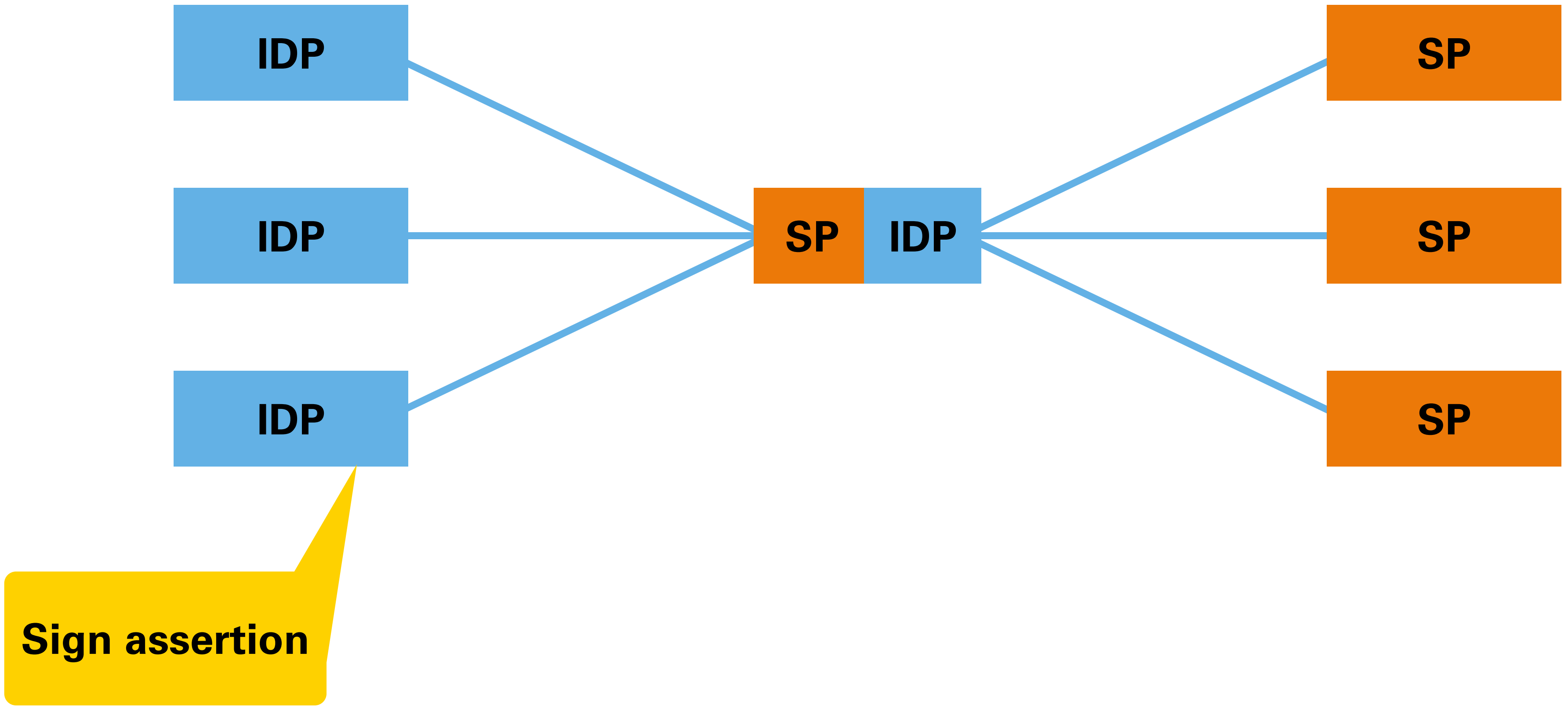


TUCCR.
Twente University Centre for Cybersecurity Research

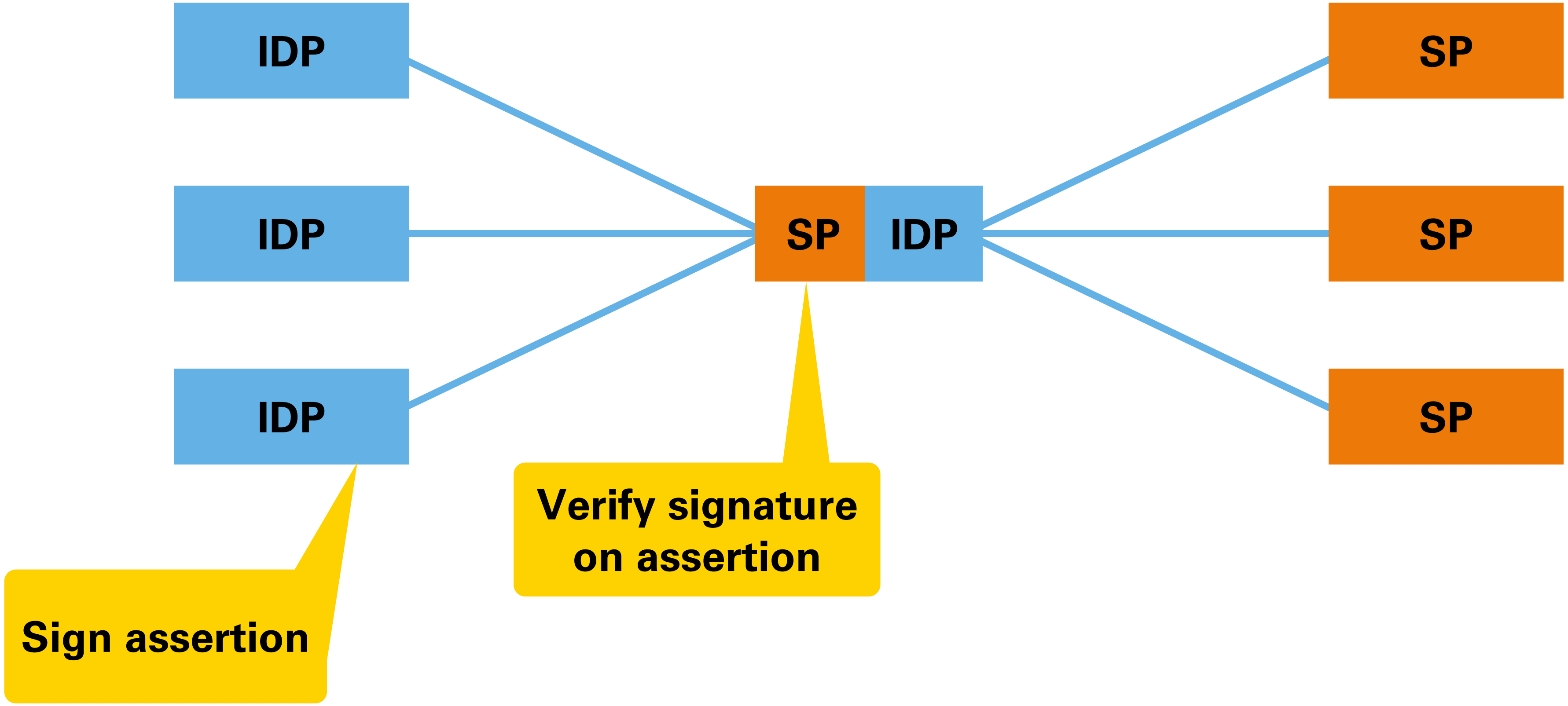
WELL ACTUALLY...



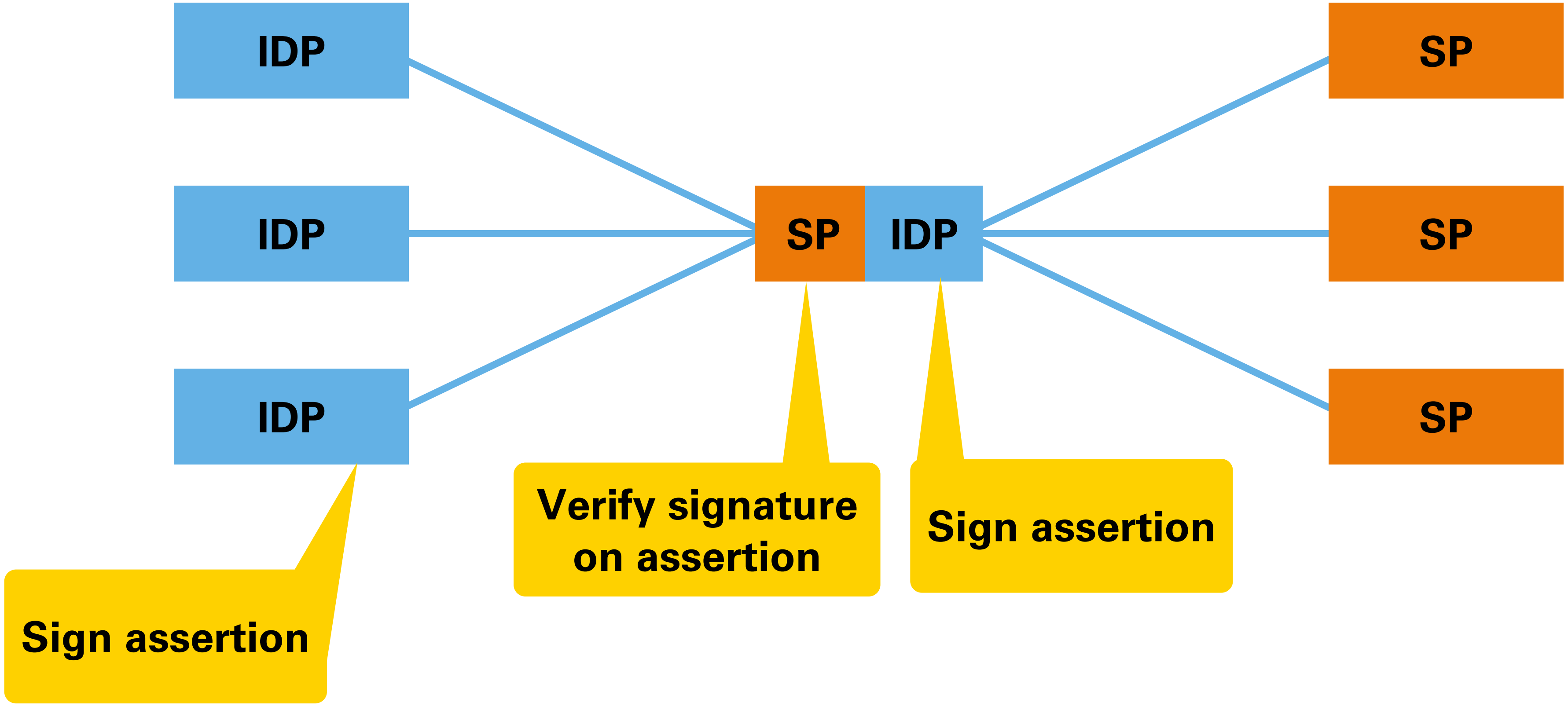
WELL ACTUALLY...



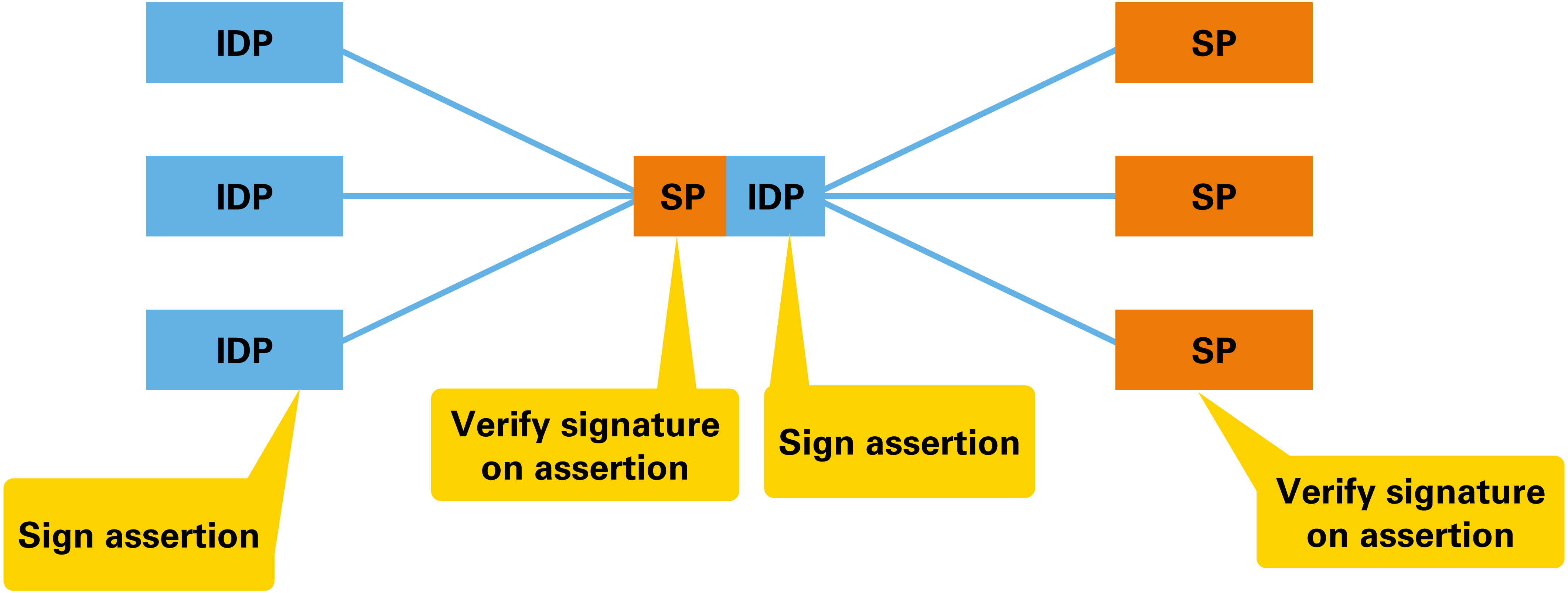
WELL ACTUALLY...



WELL ACTUALLY...



WELL ACTUALLY...



Some **more** missing **details:**

- Hub-n-spoke —> **more TLS** connections
- Where-Are-You-From (WAYF), **even more TLS** connections
- **Signing (and verifying)** federation **metadata**

All in all (in hub-n-spoke + WAYF):

- 6 TLS connections
- 2 signatures, 2 verifications

GOAL OF THIS ONE EXAMPLE

GOAL OF THIS ONE EXAMPLE

- There is potentially even **more complexity just in the web identity federation case**

GOAL OF THIS ONE EXAMPLE

- There is potentially even **more complexity just in the web identity federation case**
- This is just one example, we have **other federations**

GOAL OF THIS ONE EXAMPLE

- There is potentially even **more complexity just in the web identity federation case**
- This is just one example, we have **other federations**
- These are just examples for "mainstream computing"; **what about HPC? IoT? ICS?**

GOAL OF THIS ONE EXAMPLE

I have left out even more detail 😜

I hope I convinced you **were are only just starting the transition** to post-quantum cryptography

TUCCR.
Twente University Centre for Cybersecurity Research

WHAT TO DO?...

- Powerful **quantum computers are years, if not decades away**
- **Treat any** vendor **claim** that **you need to act NOW**, or hype-panic **with suspicion**
- Do **take** the **PQC** transition **seriously**, it is the **biggest change** to the Internet **in decades**

Photo by Tonik on Unsplash

COMMUNITY

- We have our **work** cut out **for** us **the coming years**
- The **NREN community can take** up **a pioneering role**
- **Close ties with academia** mean **we can work together**
- **Our research needs** your help and **your input** (and data)!

Photo by Hannah Busing on Unsplash

THANK YOU! QUESTIONS?