The Quantum Blockchain Cloud

(or: buzzword compliance in the age of quantum computing)

Roland van Rijswijk-Deij

NLNETLABS

The H-word

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 Under Hype Cycle and Market Clock Scrutiny

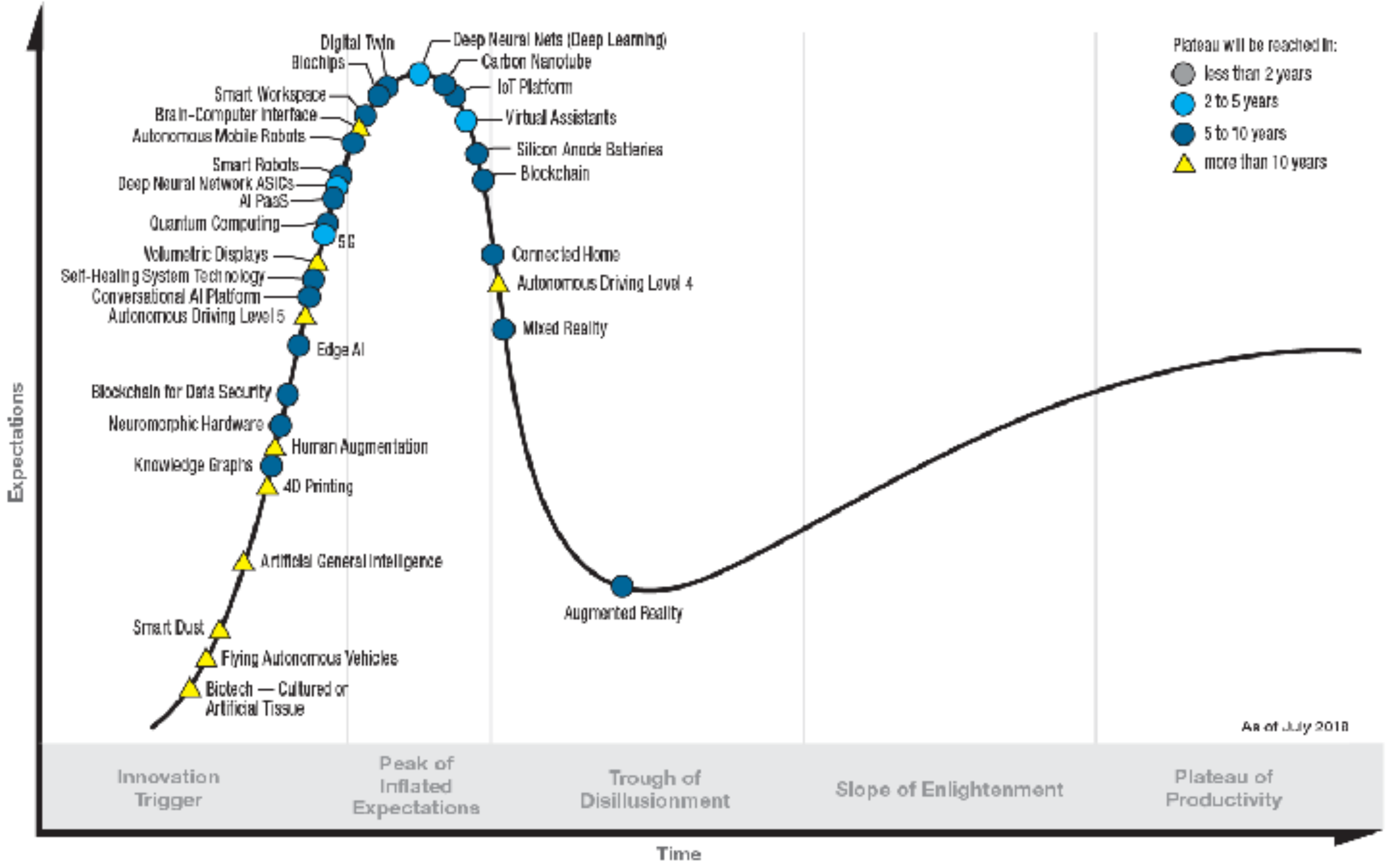
With new technology come the plaudits and the critics. Quantum computing is no different from any other sector

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

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



NLNETLABS

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

The hype isn't helpful!

- The **amount of hyperbole** is mind boggling
  - Google's "quantum supremacy" was compared to the Wright brothers' first flight moment
- **How can we know what is true or not?**
- Is quantum computing really happening? Is our public key cryptography really no longer safe? **Hopefully this talk will help.**

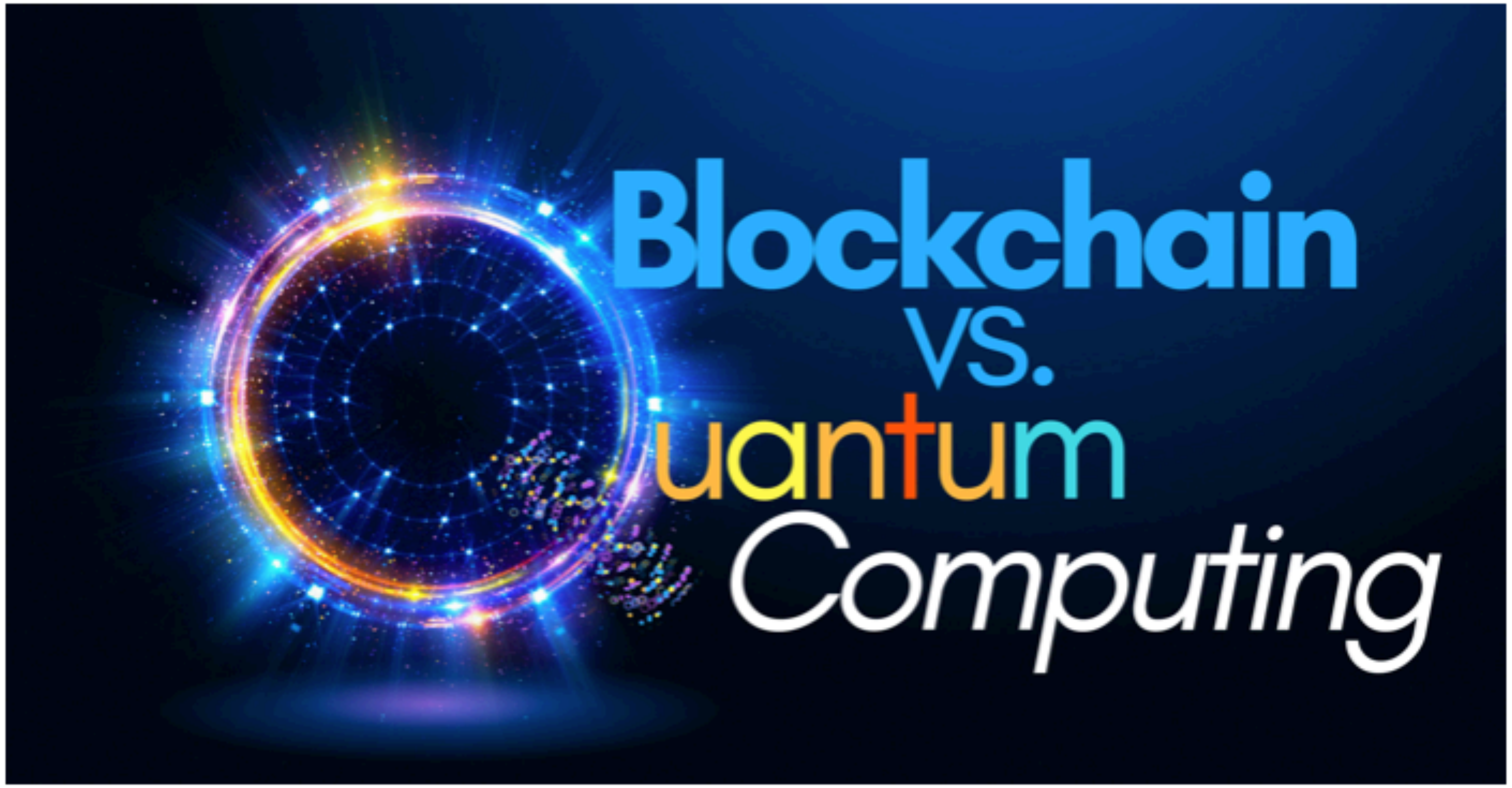
NLNETLABS

Hackernoon sez it better...

Quantum Computing: Is it the end of blockchain?

June 3rd 2018

TWEET THIS



Is this the end of blockchain?

Some facts

- Quantum computers have *qubits*, which - as many of you may already know - can simultaneously encode any value between 0 and 1 at the same time (in superposition)

- The trick with *qubits* is that they can be *entangled*, that is: their quantum states can be linked

    - This leads to some weird properties, such as "quantum teleportation"

    - It also plays a role in breaking classic public key cryptography

Building a qubit

- It turns out there are many ways in which qubits can be created
- Think of this as "hard drive" vs. "tape drive" vs. "flash drive"
- Many of these methods have some extreme requirements (very very cold environments, diamonds, powerful lasers, ...)
- The holy grail is keeping qubits stable; current records are in the order of a minute

Physical vs. logical qubit

- It turns out quantum computers are inherently noisy and unreliable; consequently, you need many *physical* qubits to create one *logical* qubit
- To perform error-free computations on a quantum computer, you need quantum error correction, to get from physical unreliable qubits to reliable logical qubits
- This can cause serious confusion; when the claims start flying that we need hundreds or millions or billions of qubits to break cryptography, **what type of qubits are they talking about?**

OK, but what about D-Wave?

- D-Wave regularly shows up in discussion about quantum computing
- Current model is claimed to have 2048 qubits, with a new model claiming 5000 qubits by mid-2020
- So are we done by mid-2020? No more RSA or Elliptic Curves? Some news outlets seem to think so (the picture on the right is from a scare-tactic Forbes article on quantum)

Not so fast (after all)

- D-Wave is not a general purpose QC, instead it does something called "adiabatic quantum computing"
- The jury is still out on whether this provides a real speed-up over classic computing, experts disagree
- The documentation is also unclear, but it appears that the 2048/5000 qubit claim talks about *physical* qubits
- Most importantly, though, D-Wave's systems cannot run Shor's algorithm (more about that in a minute)

Time for a quick summary

- Making stable qubits is really hard
- Qubits are highly unreliable
- You need orders more physical qubits to create logical qubits
- The state of the art are machines with some 50-ish logical qubits with limited stability

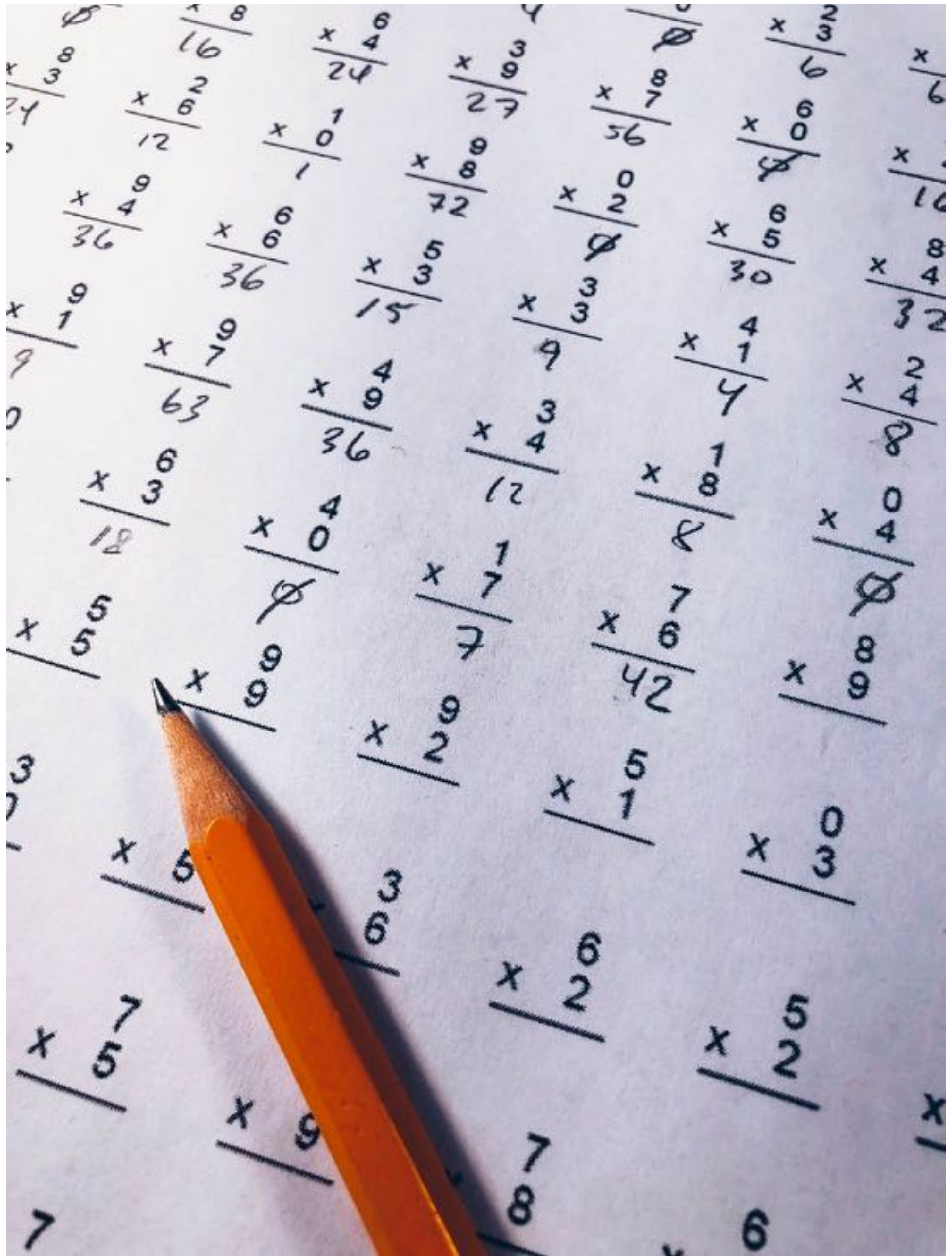


Photo by Chris Liverani on Unsplash

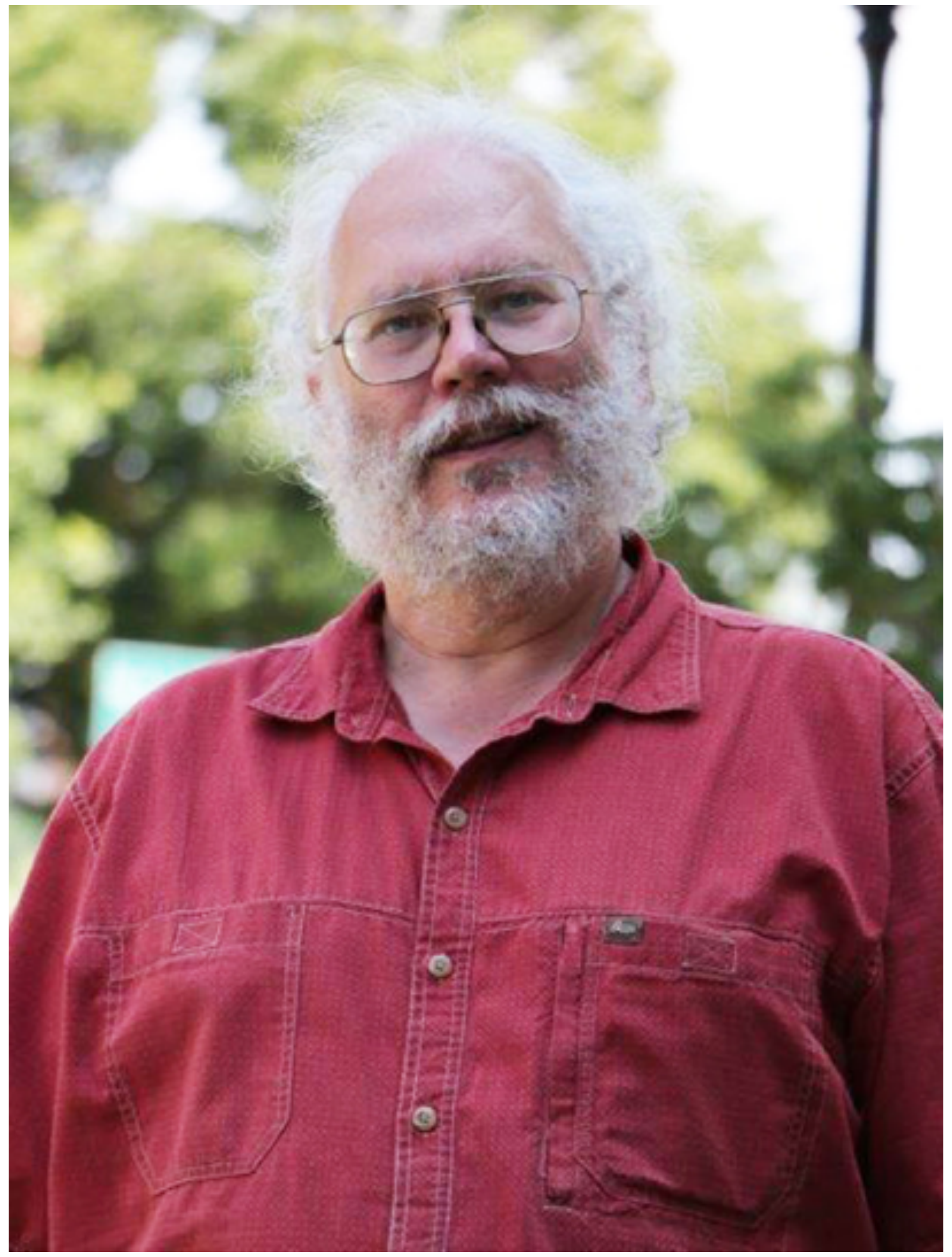
NLNETLABS

Shor's algorithm

- In 1994 prof. Peter Shor (see picture) devised an algorithm to factor very large numbers (think: RSA) much more efficiently on quantum computers

- This was touted as the "killer app" for quantum computers (which many claim had been a niche interest until then)

- His algorithm requires a stable general purpose quantum computer to execute; let's assume that exists for the sake of argument



Research to improve Shor

- Researchers are trying to improve Shor's algorithm
- To drive down the requirements to break common public key algorithms
- They do this without actual access to a working QC (awesome!)
- Take, for example, this table from [6] (references at end of deck):

	Physical assumptions				Approach		Estimated costs		
Historical cost estimate at $n = 2048$	Physical gate error rate	Cycle time (microseconds)	Reaction time (microseconds)	Physical connectivity	Distillation strategy	Execution strategy	Physical qubits (millions)	Expected runtime (days)	Expected volume (megaqubitdays)
Fowler et al. 2012 [9]	0.1%	1	0.1	planar	1200 T	single threaded	1000	1.1	1100
O'Gorman et al. 2017 [18]	0.1%	10	1	arbitrary	block CCZ	single threaded	230	3.7	850
Gheorghiu et al. 2019 [19]	0.1%	0.2	0.1	planar	1100 T	single threaded	170	1	170
(ours) 2019 (1 factory)	0.1%	1	10	planar	1 CCZ	serial distillation	16	6	90
(ours) 2019 (1 thread)	0.1%	1	10	planar	14 CCZ	single threaded	19	0.36	6.6
(ours) 2019 (parallel)	**0.1%**	**1**	**10**	**planar**	**28 CCZ**	**double threaded**	**20**	**0.31**	**5.9**

NLNETLABS

Research to improve QECC

- Researchers are not just trying to improve Shor
- More fundamentally (because it is required for other quantum algorithms) they are trying to improve error correction
- One of the latest developments is called "surface codes"; these purportedly work better on "noisy" qubits
- In the context of Shor: they require approximately 15,000 physical qubits per logical qubit for qubits with an error rate of 10^{-3} (state of the art)

NLNETLABS

So where are we with Shor?

Public Key System	Key size	Security	Logical qubits required	Physical qubits required	Running time
RSA	1024 bits	80 bits	2,050	8.05×10^6	3.58h
	2048 bits	**112 bits**	**4,098**	$\mathbf{8.56 \times 10^6}$	**28.63h**
	4096 bits	128 bits	8,194	1.12×10^7	229h
ECC	**256 bits**	**128 bits**	**2,330**	$\mathbf{8.56 \times 10^6}$	**10.5h**
	384 bits	192 bits	3,484	9.05×10^6	37.67h
	512 bits	256 bits	4,719	1.13×10^7	55h

Source: [2] -- terms and conditions apply 🤪

That previous slide...

- Has a *lot* of assumptions, none of which hold today
- So the $64 million question is: when, if ever, will these assumptions hold?
- An oft-quoted person is Michele Mosca, whose most recent prediction puts the likelihood of a quantum computer that can break RSA 2048 in the next decade at **one in six**

picture source: represent.com

So what do the experts agree on?

- **Nobody** really **knows if a quantum computer** good enough **to run Shor will ever be built**
- *Equally*, **nobody claims** that **it can never be built**
- There is **lots and lots of parallel research** going on, all of **which requires major breakthroughs** to get there
- *The best thing you can do*: **keep a keen eye on post-quantum crypto!**

NLNETLABS

Mosca's Inequality

- A handy way to reason about when you should really take action is what is often referred to as "*Mosca's Inequality*": **X + Y > Z**

  where: **X** = *the amount of time you want to keep your data secret*
  Y = *the amount of time you take to transition to PQC*
  Z = *when we expect QC's to be able to run Shor*

- The problem, again, here is that **nobody really knows a sensible value for Z** in this equation

The experts are on it

President Donald J. Trump signs the "National Quantum Initiative" into law

NLNETLABS

More hyperbowl...^H^H^H^H...bole

picture source: Wikipedia

Quantum Key Distribution

- I assume most (if not all?) of you are familiar with One-Time Pads?

From: A History of U.S. Communications Security (Vols. I and II);
the David G. Boak Lectures, National Security Agency, 1973
https://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf

NLNETLABS

QKD relies on the observer effect

- QKD is used to distribute a one-time pad from A to B
- Security relies on the fact that you can tell if the message was observed
- Common implementation: polarised light through a fibre-optic cable

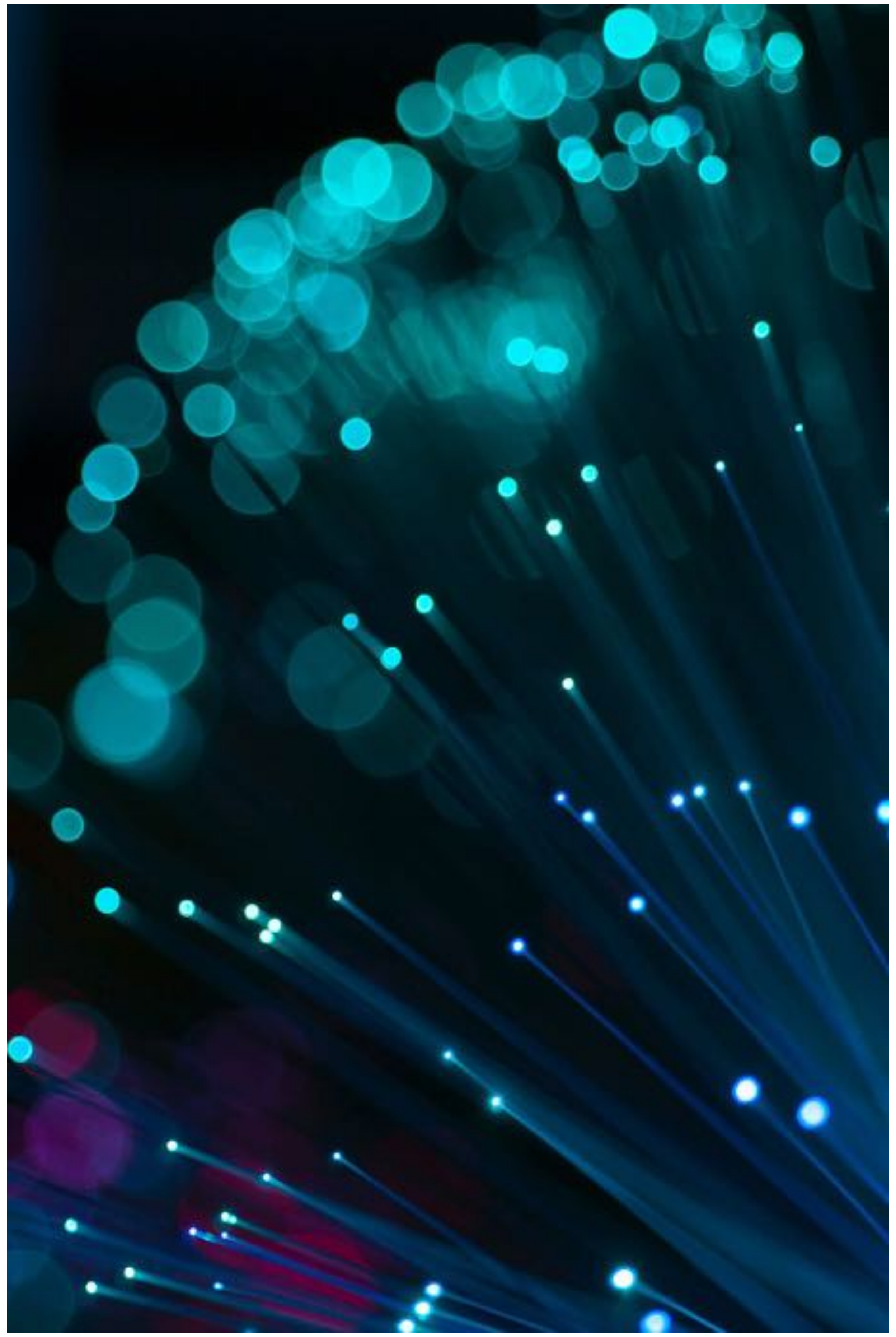
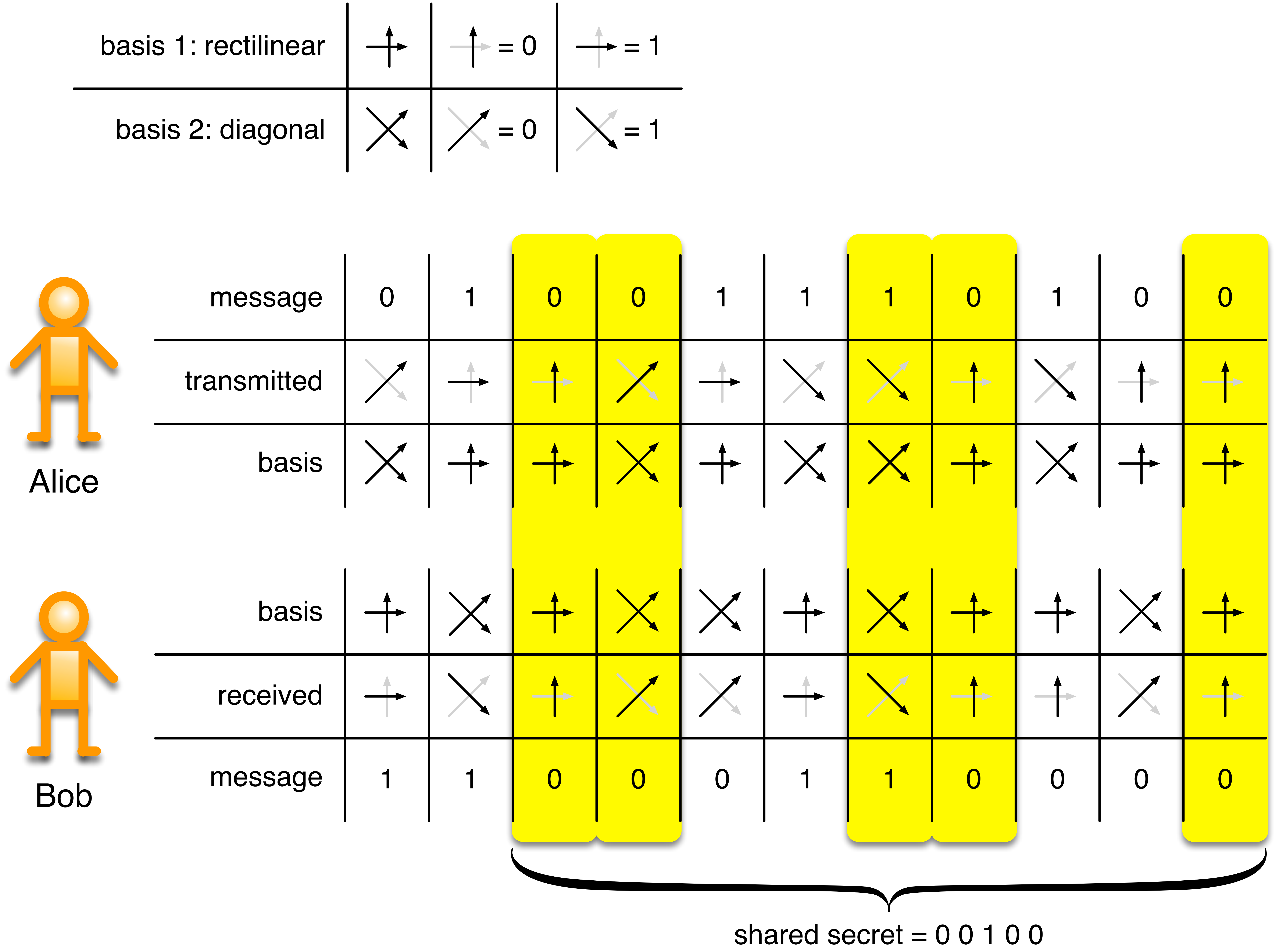


Photo by Umberto on Unsplash

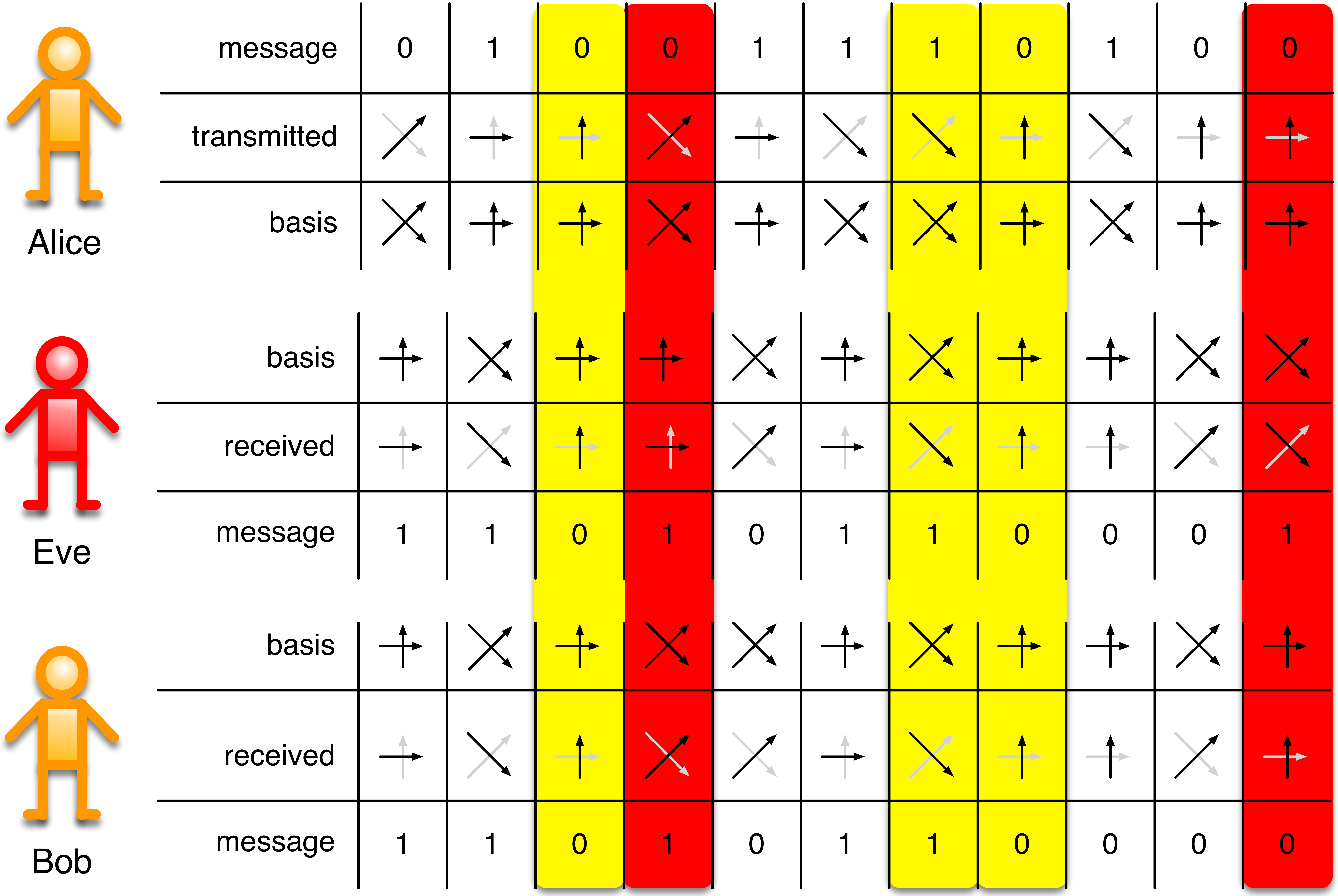
NLNETLABS

Conceptual QKD in two slides



NLNETLABS

Conceptual QKD in two slides



Issues with QKD

- It **requires "classic" cryptography** to authenticate the communicating parties (am I really sending something to Bob?)

- More importantly, though, **it is vulnerable to attacks**

  - **Photon-splitting attack** (*doesn't that sound awesome?!*)
    QKD relies on single photon emission, but that is actually impossible

  - **Trojan attack**
    Shining a very bright light at the message source, attack can infer chosen polarisation from reflection with 90% accuracy [7]

NLNETLABS

Do we really need QKD?

- It is expensive
  - order of €25K/device, you need two!
  - oh, and you need dark fibre
- It is inefficient (bit rate in the order of 1Mbit/s over 50km)
- And there are known attacks, how many are still to come?
- Never underestimate the bandwidth of a truck full of one-time pads 🤪

Photo by VanveenJF on Unsplash

Wrapping up

- There is a lot of hype and hyperbole about quantum computing
- Just as there is about blockchain (hence the title of this talk)
- So we have two takeaways for you:

NLNETLABS

Takeaway #1

DON'T PANIC

picture source: Wikimedia Commons

NLNETLABS

Takeaway #2

- **Pay attention to Post Quantum Cryptography**
- ...and **give people like Andreas more €€€ for** their **research!**

Photo by Марьян Блан | @marjanblan on Unsplash

So what is the QBC?

Well that, as they say, is simple:

It's a **computer system in someone else's data centre** that **you don't find out actually exists** until you **make a transaction that needs to be persisted on a ledger** after which it **sets fire to said data centre, belching out more pollutants than a brown coal fired power plant in Germany**

NLNETLABS

Thank you! Questions?

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

roland@nlnetlabs.nl

NLNETLABS

References

(1) Sattel, S., "The Future of Computing - Quantum & Qubits", Autodesk, https://www.autodesk.com/products/eagle/blog/future-computing-quantum-qubits/

(2) Grumbling, E. and Horowitz, M. (eds.), "Quantum Computing: Progress and Prospects", National Academy of Sciences, 2019, https://download.nap.edu/cart/download.cgi?record_id=25196

(3) Mosca, M., "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?", IACR Cryptology ePrint Archive, November 2015, https://eprint.iacr.org/2015/1075

(4) Vardi, M.Y., "Quantum Hype and Quantum Skepticism", editorial in Communications of the ACM, Vol. 62, Issue 5, May 2019, https://dl.acm.org/citation.cfm?id=3328504.3322092

(5) Monroe, D., "Closing in on Quantum Error Correction", in Communications of the ACM, Vol. 62, Issue 10, October 2019, https://dl.acm.org/citation.cfm?id=3363418.3355371

(6) Gidney, C. and Ekerå, M., "How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits", ArXiV, May 2019, https://arxiv.org/abs/1905.09749

(7) Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C. and Leuchs, G., "Trojan-horse attacks threaten the security of practical quantum cryptography", New Journal of Physics, Vol. 16, December 2014, https://iopscience.iop.org/article/10.1088/1367-2630/16/12/123030

(8) Hoffman, P., "The Transition from Classical to Post-Quantum Cryptography", IRTF, CFRG Working Group, draft-hoffman-c2pq-05, https://tools.ietf.org/html/draft-hoffman-c2pq-05

(9) Smolin, J., Smith, G. and Vargo, A., "Oversimplifying Quantum Factoring", Nature, Vol. 499, 2013, pp. 163-165, ArXiV PDF: https://arxiv.org/pdf/1301.7007.pdf