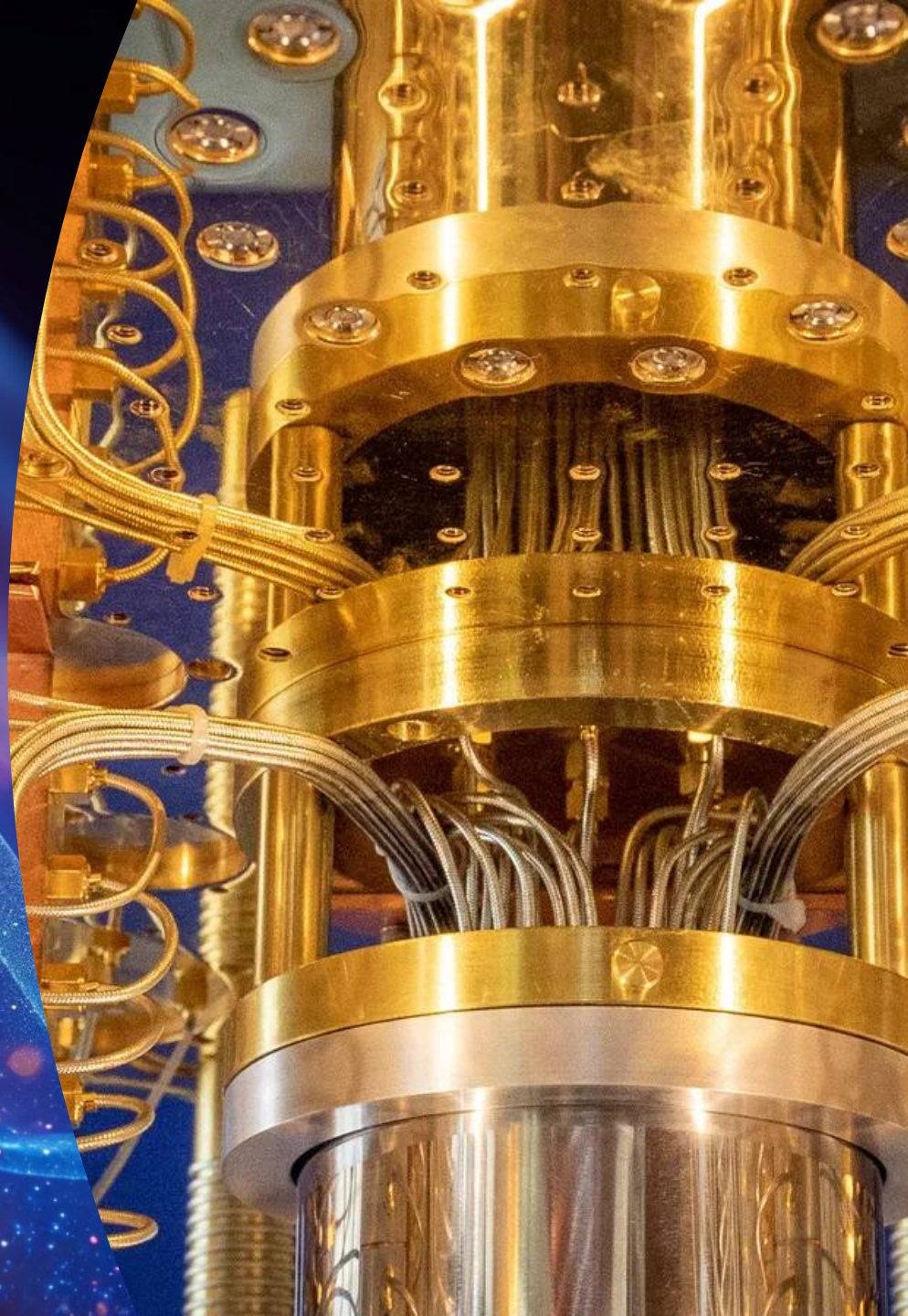
quantum circle

Accelerating Quantum

In Belgium & the EU



Sarah Ampe

Sarah Ampe

Manager Digital Risk at EY and core member of the Quantum Circle

- Masters in Mathematics at KU Leuven
- Working on digital trust:
  - Cryptography (PQC, crypto-agility)
  - eIDAS
  - PKI – Public CAs

quantum circle

quantum circle

We saw a growing need for exploration, collaboration and investment.

Back in 2024 ...

- Quantum was practiced at all Belgian universities and most research institutes, with proven research track records and international reputation.
- Large corporations just entered the awareness phase, a quantum startup scene was and is virtually nonexistent.
- The EU and +10 member states already had a National Strategy, while Belgium was lacking.
- Neighboring countries were developing strong quantum ecosystems, a route we decided to follow!

Quantum Circle
Sense of purpose

Our day-1 idea

We unite quantum explorers and experts to champion revolutionary technology, collaborate on ground- breaking applications, and drive market adoption, shaping a visionary investment landscape with societal and economic impact.

quantum circle

Quantum Circle
This is what we stand for

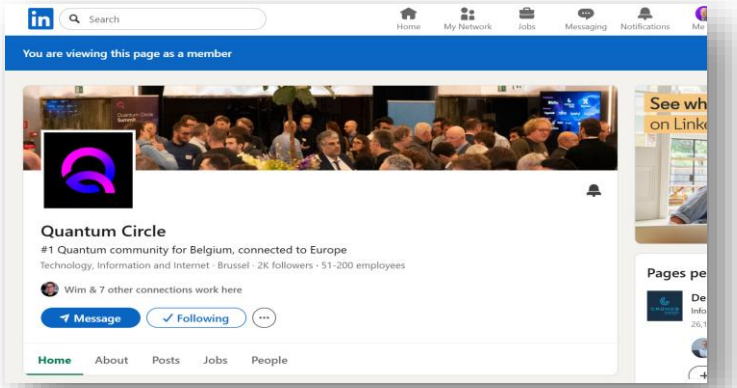
3 goals to deliver on our purpose, in sequence:

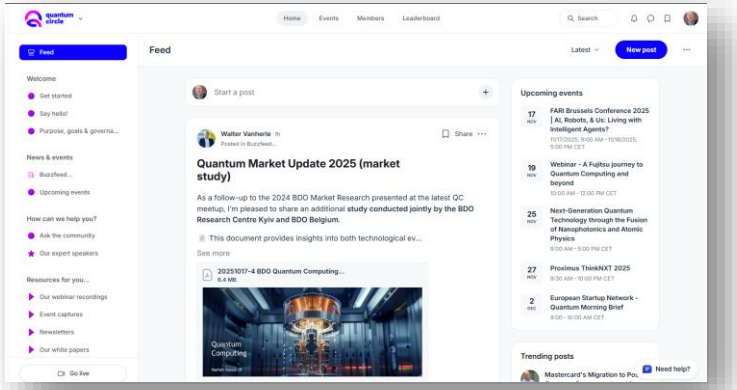
1. **We engage with all stakeholders in quantum computing, communication and sensing via all kinds of activities.**
2. **We advocate the game-changing potential of quantum technologies, collaborate on concrete industry use cases, exchange expertise and facilitate market adoption.**
3. **We establish foundations for a responsible investment climate with tangible economical and societal impact.**

quantum circle

How we communicate with members and stakeholders
Digital enablers, sharing relevance with the business

- **Website**
  Monthly update with news, activities, events, …
- **CRM contact management**
  800+ contacts and growing
- **Newsletter**
  600+ monthly readers = good reach: less technical content & more business usage focus, with local contributions
- **LinkedIn**
  2.200+ followers, content: news, events, member spotlights
- **Circle platform & app**
  250+ users registered
- **Meetups**
  Regular digital and live member sessions

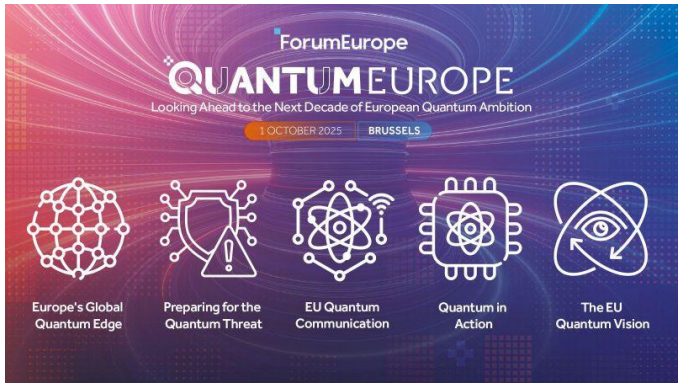


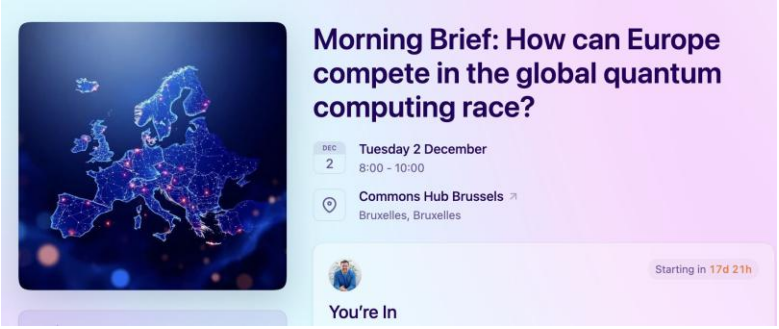


quantum circle

How we create impact through academic, policy and industry events

From 2 to 40+ initiatives in 2 years

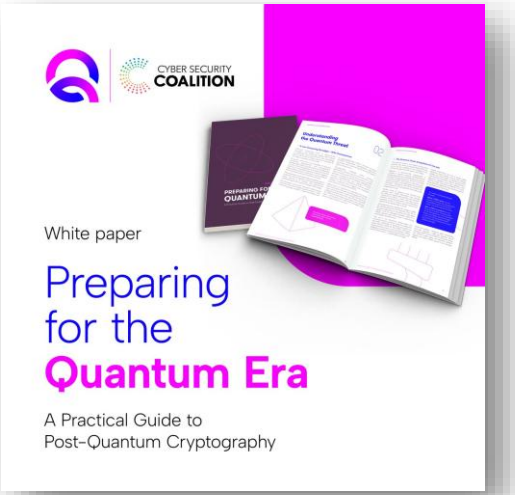




quantum circle

Where things get very tangible
From co-creation to white papers & playbooks

- **Co-creation activities**
  Energy grid balancing optimization research
  Transport & Logistics route optimization algorithm design
- **Our white papers**
  Engage on Quantum Technology, a starter guide
  Accelerating Quantum in Belgium, a positioning paper
  Quantum Readiness in Belgium, a market survey
  Post-Quantum Cryptography, a practical guide
- **Playbooks**
  Industry use case cases for business leaders
  Quantum for dummies playbook for decision makers
- **Summer Lab**
  2- day hands-on quantum computing training



quantum circle

What we learned over the past 2 years?
Belgium has loads of things in hands

- Our community of 250+ stakeholders channels knowledge transfer between, corporates, startups, tech providers and academics.
- Awareness level-up will take 2 to 3 more years, while collaboration around industry use-cases is they way towards business adoption.
- We can build on large pools of Data, AI and Cybersecurity businesses and public institutions, already federated via peer user groups.
- Belgium has unique capabilities in Cryptography, Nanotech, Photonics and Chip research as enablers for quantum stack development.
- Chemical, Pharmaceutical, Biotech, Energy, Logistics and Finance sectors are good candidates for early quantum adoption.
- A Federal Quantum Strategy is in the making, while a complementary Action Plan for Flanders should be ready by the summer.

quantum circle

Quantum in the regulatory landscape
Opportunity

EU Quantum Act (forthcoming)

What is it?
Announced EU legislative initiative in the Commission Work Program 2026
Aims to position Europe as a **global leader** in quantum technologies

Expected focus (3 pillars)
Coordination of R&I **investments** across Member States
Scaling industrial capacity (from research to production)
Security and resilience of quantum supply chains

Status
Preparatory phase; timing has shifted and remains indicative

Key message
Industrial policy & technological sovereignty — building and securing the European quantum ecosystem.

quantum circle

Quantum in the regulatory landscape
Risk

NIS2

"The use of any innovative technology, including artificial intelligence, should comply with Union data protection law, including the data protection principles of data accuracy, data minimisation, fairness and transparency, and data security, such as state-of-the-art encryption."

EU Digital Omnibus: Suggested to amend NIS2, to include the migration of high risk use-cases by 2030.

DORA

"In view of the rapid technological developments in the field of cryptographic techniques [...] financial companies should keep pace with the relevant developments in cryptanalysis and consider leading practices and standards, and therefore adopt a flexible approach based on defense and monitoring to deal with the dynamic landscape of cryptographic threats, including those arising from quantum technology."

CRA

"It is therefore important that the products with digital elements necessary for digital infrastructure providers to ensure the functioning of the internet are developed in a secure manner and that they comply with well-established internet security standards."

EU Commission Recommendation

The future potential development of quantum computers capable of breaking today's encryption makes it necessary for Europe to look for stronger safeguards, ensuring the protection of sensitive communications and the long-term integrity of confidential information, i.e., by switching to Post-Quantum Cryptography as swiftly as possible. This new type of cryptography will remove the known vulnerabilities of current asymmetric cryptography and enhance the robustness against the threats posed by the malicious use of quantum computers.

quantum circle

Why does this matter?

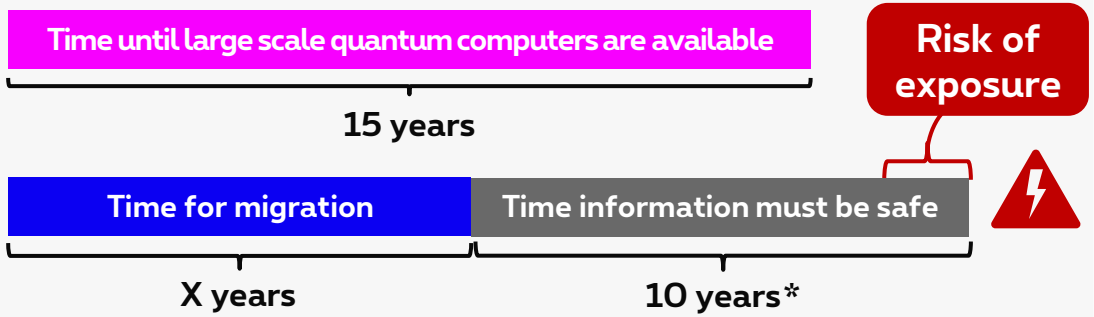
Data Confidentiality

Need: Protect data from unauthorized access

Cryptographic principle: You lock the data and only those with the key can access it

Example: Encrypted communication over a public network

Impact of quantum: Anyone intercepting the traffic could decrypt it and read the exchanged information



Hence, it is required that X < 5 years!

Malicious parties are already storing encrypted data today, to be able to decrypt it when a full quantum computer becomes available

Data Authentication

Need: Protect data from unauthorized changes

Cryptographic principle: You sign the data and everyone can validate that the data is authentic from you

Example: Digitally signing software packages

Impact of quantum: A third party could make malicious changes whilst pretending to be you

Two scenarios:

Risk of exposure

Hardware in production sites has a long lifetime and often can't be updated quickly so the same signature might be used for 20 years.

No immediate risk of exposure

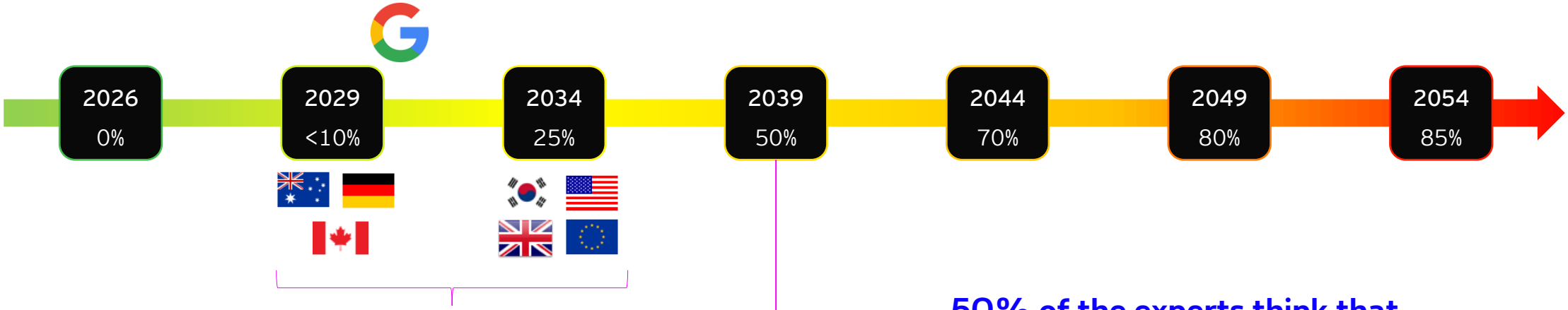
Software can be updated rapidly, allowing for adjustments to be made later.

quantum circle

* Many organizations hold critical data that must remain secure for 10 years. Depending on the organization, the retention period might differ.

But when?
Timelines

When will Quantum Computing be able to break currently used cryptography?



Many countries plan to prepare themselves by 2035

50% of the experts think that currently used cryptography can be broken by 2039

quantum circle


quantum
circle
Questions?
Sarah Ampe
Sarah.ampe@be.ey.com