



# QUANTUM ADVANTAGE WITHOUT QUANTUM MEMORIES

Wojciech Kozlowski

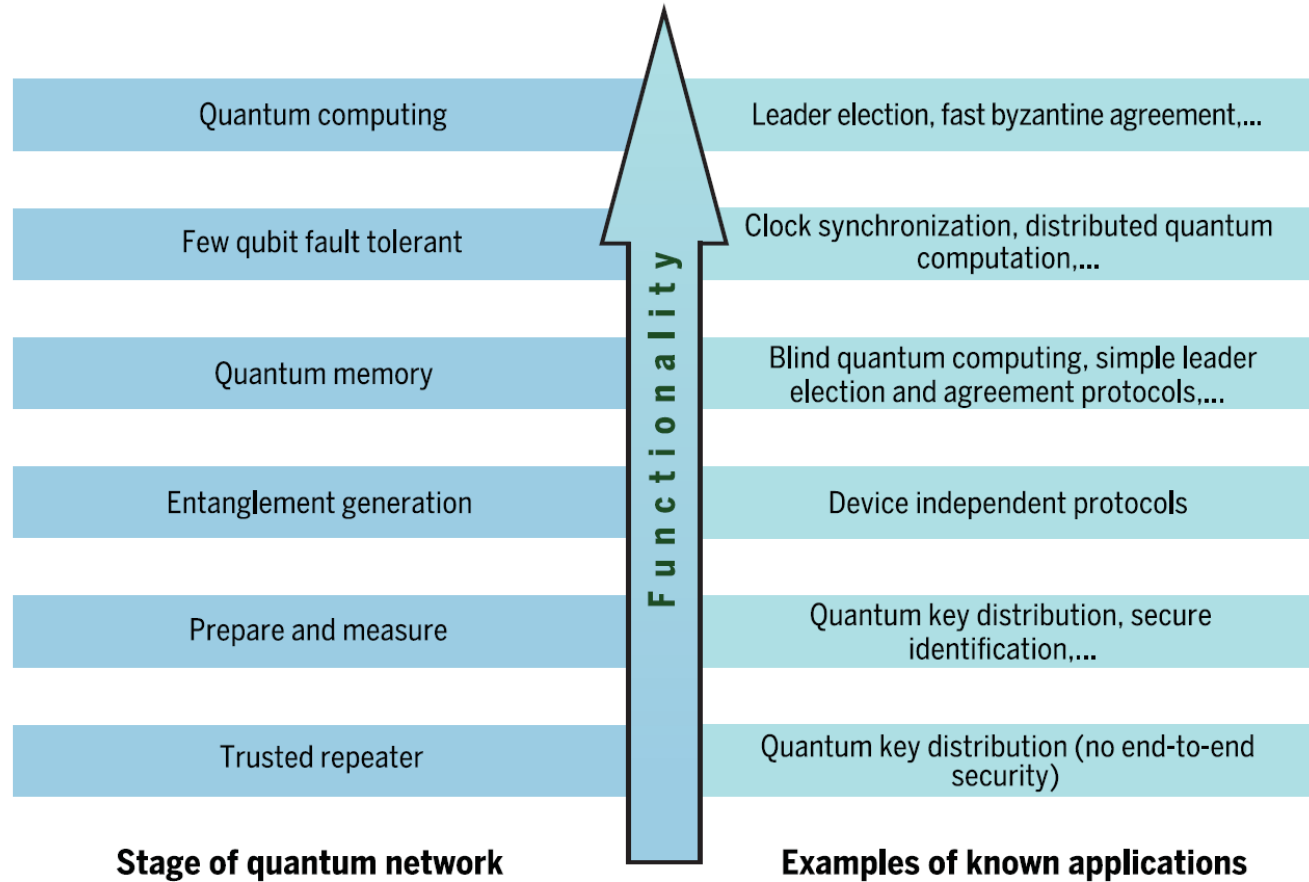
SURF

# Motivation

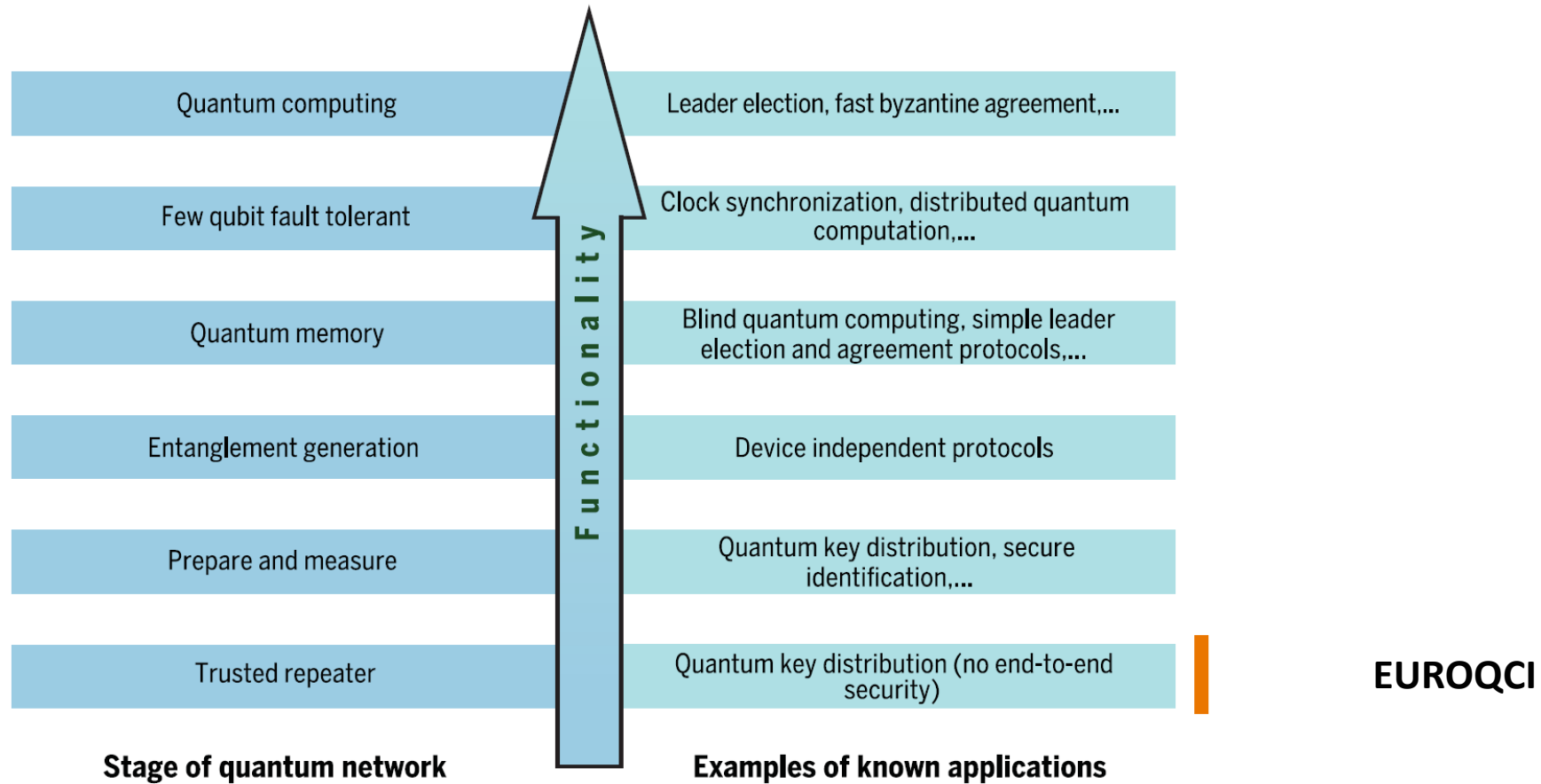
# Motivation

- **Quantum advantage** (in quantum communication) occurs when a quantum network can solve a real-world problem better in some way, e.g., faster, more securely, more efficiently, more effectively, etc.
- **Quantum memory** is storage for quantum states, entangled or otherwise.
- **Quantum advantage without quantum memories** occurs when a quantum network can solve a real-world problem better in some way without storing any quantum states in a quantum memory.

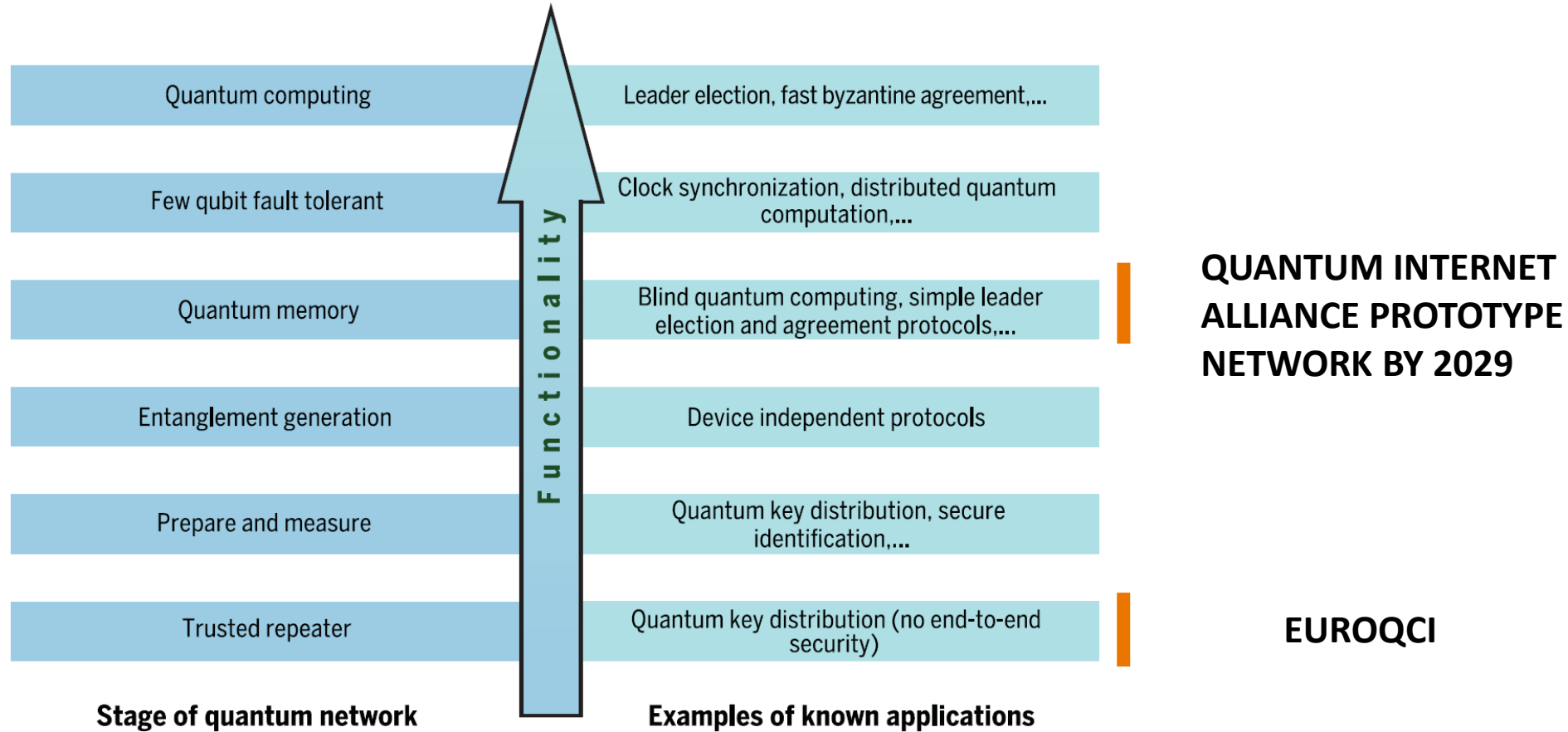
# Motivation



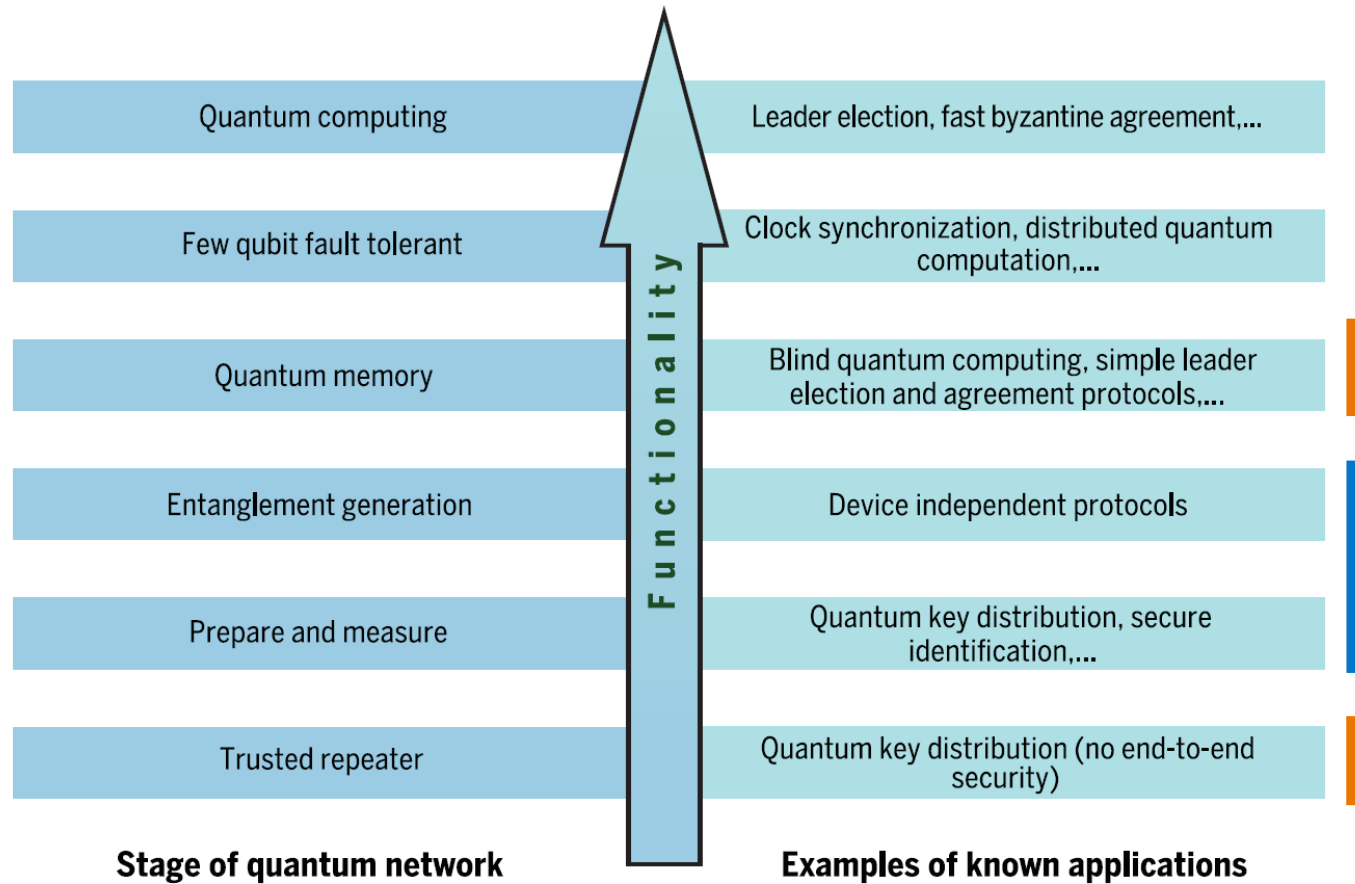
# Motivation



# Motivation



# Motivation



**QUANTUM INTERNET  
ALLIANCE PROTOTYPE  
NETWORK BY 2029**



**EUROQCI**

# Motivation

- Europe is deploying an extensive quantum communication infrastructure as part of EuroQCI.
- This will include cross-border extensions starting ca. next year.
- The focus is QKD, but almost every QKD device is also capable of prepare-and-measure or even entanglement stage applications.
- This means that the infrastructure for prepare-and-measure and entanglement stage applications is there.



# Motivation



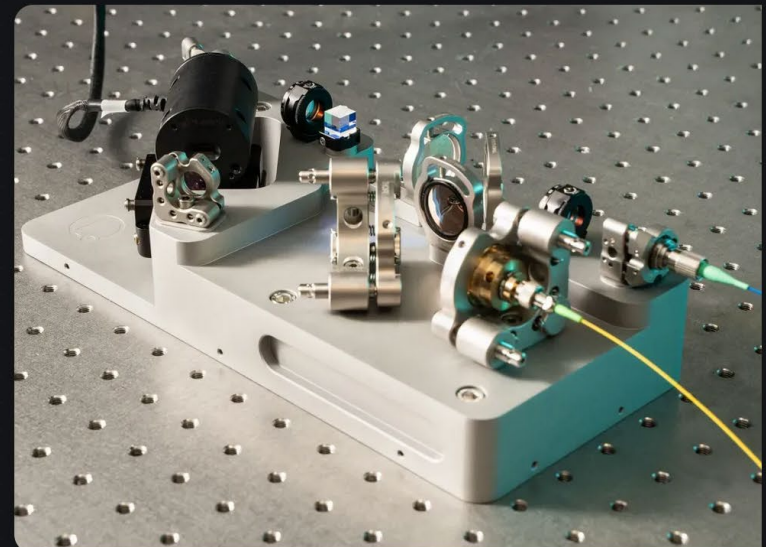
## Qu-SRC

The characteristics of the entangled photons define how widespread a quantum network can be used. Our unique quantum sources are designed to interface with vast majority of quantum computing and sensing platforms.

[VIEW DETAILS](#)

## Polarization Entangled Photon Pair Source

High rate and high heralding Sagnac-interferometer source of polarization-entangled photon pairs, based on spontaneous parametric down-conversion (SPDC) within a periodically poled Lithium Niobate crystal (type 0). Access to all mechanical and electrical parameters, ideal platform for Research & Development teams.



SURF

# Inventory of applications

# Inventories of applications

- Already exist:
  - Quantum Protocol Zoo (<https://wiki.veriqloud.fr/>),
  - Quantum cryptography beyond key distribution: theory and experiment (<https://arxiv.org/abs/2411.08877>),
  - RFC 9583 Application Scenarios for the Quantum Internet.
- Dive deep into the technical, mathematical, and theoretical background.
  - Very important but makes it difficult to figure out if it is interesting.
- Include applications from all stages of quantum network development.
  - Can be distracting since most powerful applications are from later stages.
- Create an inventory which focuses on functionality provided over mathematical detail and limited to memory-less stages.

# Relevance to QIRG

- It's a question many people have – “what are quantum networks for?” Here, I focus on the near-term – applications that, in principle, could be realized today. At the cost of considering the most powerful, but also most demanding applications.
- Understanding the use cases will help in understanding how to build the networks – they're not all built the same.
- Quantum entanglement networks will not come out of a vacuum – they will likely evolve from the previous QKD and prepare-and-measure networks.

# Applications

# Applications

1. Security
2. Position Verification
3. Unforgeable Tokens
4. Tacit Coordination

# Security

# Security

- More than just Quantum Key Distribution (often can be done with same hardware):
  - Fingerprinting, digital signatures, bit commitment, oblivious transfer, strong coin flipping, weak coin flipping, one-time programs.
  - Building blocks for secure multi-party computation and consensus protocols.
- In general, all of these can be done classically.
- Quantum provides some increase in security, sometimes it can be information-theoretic security, sometimes just weaker assumptions, generally secure against quantum computing attacks.
- Sometimes the security comes with deployment/implementation drawbacks.
- ITS possible for (possibly under special conditions): QKD, digital signatures, bit commitment, one-time programs.

# Security

- Key question: where is this increased level of security useful?
- For most cases, post-quantum cryptography is easier and sufficiently secure.
- High-security domains that already rely on additional security measures.
  - Can ITS enabled by quantum automate security tasks that are delegated to people? E.g., in government, military, finance.
- Security for data subject to stringent regulations: medical and other personal data.
  - A common problem nowadays is that the compute resource (datacenter / supercomputer) and the data source are in different locations, but regulations prohibit the transfer of data between the locations.
  - Can ITS enabled by quantum help create secure virtual research and compute environments?

# Position Verification

# Position Verification

- Verifies that a given message originates from a specific geographical position.
- Not possible classically – vulnerable to collusion attacks.
- Possible with quantum – secure assuming a bound on how much quantum information an adversary can store.
- In current stage of network development verification is limited to location of quantum nodes (i.e., static deployed locations).
- Intuitively useful in military and other high-security domains.
- Is it useful in other domains?
  - Networking: to verify the location of a node (peer/server/router)? DNS, BGP? Network attestation?
  - Authentication: in addition to typical 2FA for some applications?
  - Gaming: can increase security enable new, higher value, location-based games?

# Unforgeable Tokens

# Unforgeable Tokens

- Central authority releases tokens that cannot be forged.
- Most common schemes, e.g., quantum money require quantum memories.
- Possible to implement without memories by using a network of trusted agents.
- Classically can only have two out of the three properties: token unforgeability, instant validation and user privacy.
- Quantum advantage allows for all three properties. Therefore, applications that need all three simultaneously can benefit from quantum networks.
- Example provided in the academic papers was High-Frequency Trading.
- Where does the combination of all three unforgeability, user privacy, and instant validation bring value?

# Tacit Coordination

# Tacit coordination

- Tacit coordination is the ability to coordinate decisions between non-communicating parties.
- The idea is to have multiple non-communicating parties who each make a local observation and a local decision. The aim is then to optimize a global “utility” of their collective decisions based on their collective observations.
- Quantum mechanics allows to achieve better results than the best classical strategies.
- Can benefit coordinated decision-making where decision speed matters and there is no time to communicate.
- Possible to achieve without quantum memories (use entanglement source to provide entanglement at regular intervals) but can be difficult to achieve due to photon losses – thus in practice limiting practical distance.

# Interaction with the QIRG

- Ideally the inventory is a living document rather than a static RFC. The field is very dynamic – hardware capabilities and theoretical understanding change very rapidly.
- Problem domain and network experts are needed to help build the use cases in more detail – e.g., where to integrate quantum position verification?
- Quantum information experts are needed to ensure rigor, correctness, and security.
- Seeking interested people to just brainstorm applications or work together.
- Ideal outcome: find applications worth investigating, construct more elaborate use case, create prototype and test on the Dutch (or some other) research and education quantum network (part of EuroQCI).



**THANK YOU FOR  
YOUR ATTENTION**

 **Wojciech Kozlowski**

 **E-mail: [wojciech.kozlowski@surf.nl](mailto:wojciech.kozlowski@surf.nl)**

 **[www.surf.nl](http://www.surf.nl)**

**Driving innovation together**

**SURF**