DIGITAL SOVEREIGNTY AND QUANTUM COMMUNICATION

from the perspective of a company

Table of Contents

What Is Digital Sovereignty?

- Control over your actions and data
- Direct and indirect independence of outside influence over your actions and data
- This includes:
  - Governments
  - Companies
  - People

Why Do We Need It?

Examples

- Through the CLOUD Act all US companies must give the government access to all data, even if they are stored outside of the US
  - This includes European subsidiaries
- What if a government just pressures a company into complying?
- What would many companies do if AWS suddenly stops working tomorrow?
- What if Microsoft increases the costs of Office 365 50% year to year?
- What if SAP increase costs of some of their main products 50% year to year?

How To Get Sovereign?

From the perspective of a company

- Critical data should be on systems only in your political reach
- Don’t just look at the companies headquarters, but their owner structure and revenue stream as well
  - Are companies safe that are 100% European, but gain e.g. 70%+ of revenue in the US?
- Used solutions should be part of an open ecosystem to have competition
- Keep critical knowledge in-house
- Be flexible in migrating to different solutions

qonduit

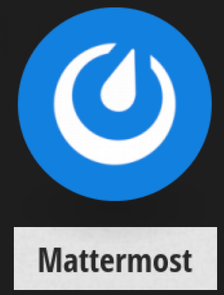
What Should I Do?

Concrete Tips

- Don’t outsource everything
- Keep enough knowledge of the general problem space in-house
- Use products with a possible way of migrating if possible
- Don’t focus on a product by a company, but on the overall aspects and problem space
  - Don’t have Azure Cloud Admins, but Cloud Engineers
- Have modular tools and don’t always buy everything from one supplier
- Don’t just look at the costs of the product today, but also also think about the future (total cost of ownership)
  - Keep the business model of you supplier in mind. Is it sustainable, or maybe just a promotion with big price increases in the future?
- Figure out a critical path for your work, you don’t need to be perfect at day one

Example for Modularity

qonduits internal office stack



HETZNER

Wolkesicher

salmacis

peaknetworks

HETZNER

Example for Modularity

qonduits internal office stack - digitally sovereign?

- All involved companies or products are either in the EU or open-source, so no direct foreign influence
- Each component could be switched independently, so no real single-point of failure
- Leverage of each company is small., there are many similar providers available
- Example: Collabora Online could be migrated to a different datacenter besides Hetzner, to a different managing company besides Wolkesicher or be migrated to a different tool as it uses the Open Document Format.

Example for Critical Path

qonduits internal office stack

We use MacBooks, but they are not in the critical path

I could destroy my MacBook now and could work fine with a new Linux notebook tomorrow

Nextcloud

Collabora Online

Mattermost

Jitsi Meet

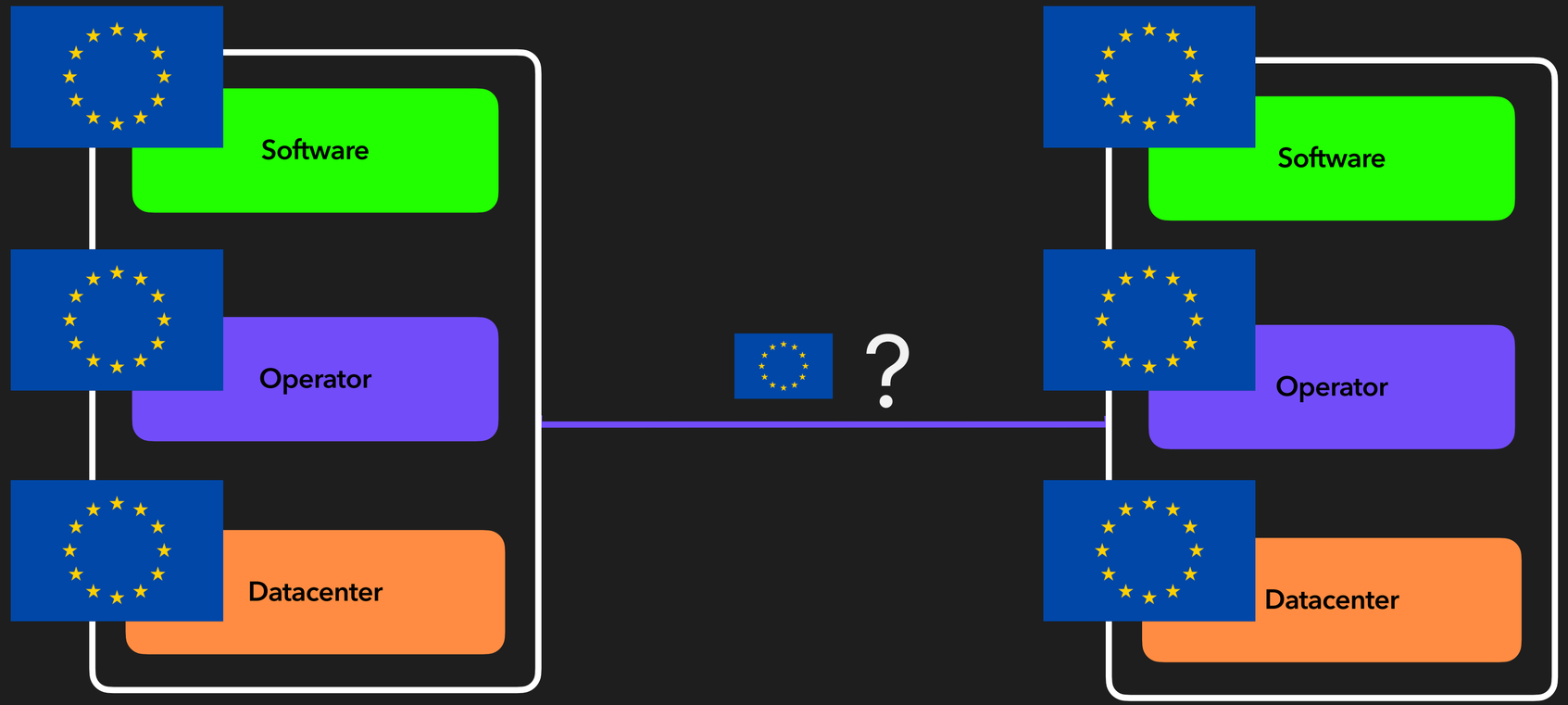
Critical path

ENCRYPTED TODAY.
UNBREAKABLE TOMORROW.

QKDN and Digital Sovereignty

Digital Sovereignty

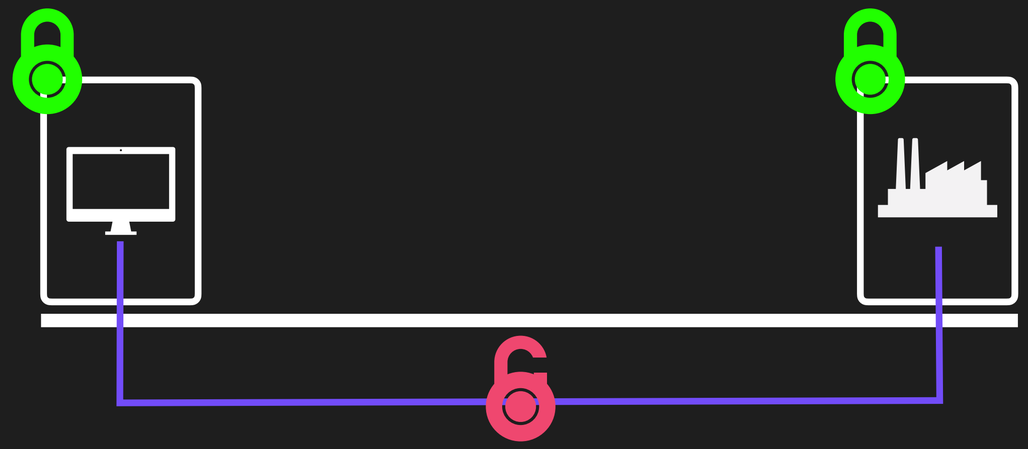
The whole stack



Digital Sovereignty

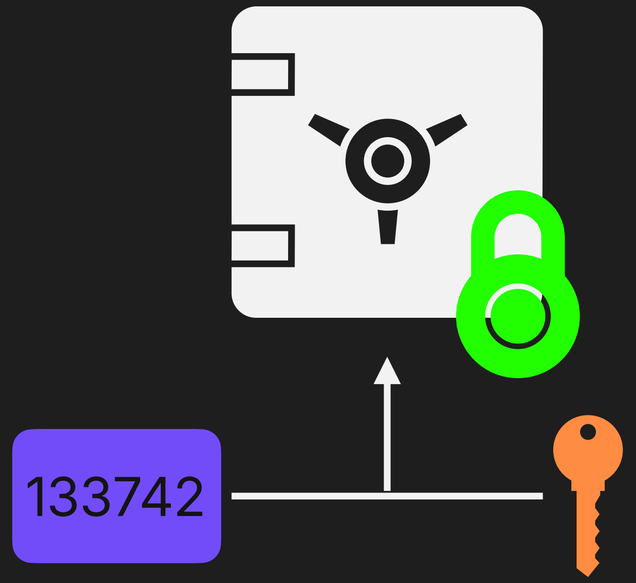
Networks

- Connection points can be secured, but fiber in the ground is vulnerable
- Reading data out of a fiber in the ground is a real threat
- It is proven that Intelligence Agencies do it
- As you secure the fiber, you secure all layers above as well



qonduit

How would you secure your vault?



Secure your vault

- Use different methods with different attack vectors:
  - Send the key as a letter
  - Tell the passcode in person
  - Attacker has to get the letter AND hear the conversation
- Two methods have to **fail** before the **vault** is in **danger**!

qonduit

You would not trust a single procedure for your top secret vault.

Then why do you trust a single procedure for your communication?

Modern vaults are **datacenters** and you access them **remotely**.

qonduit

Current Problem and Situation

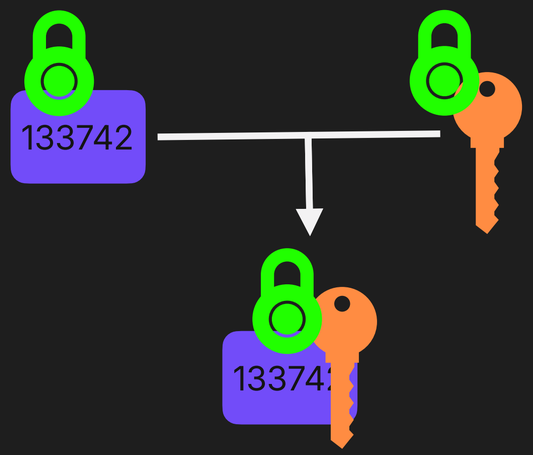
Encrypted communication

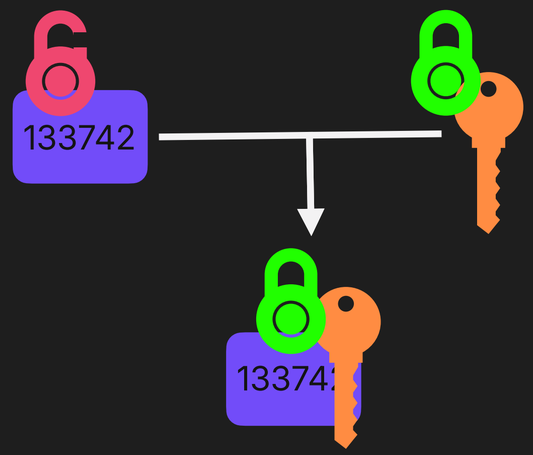
- **Encrypted communication** is based on one type of procedure for key exchange
- The most common procedures are also vulnerable to **quantum computers**
- Communication can be stored now, and decrypted later, so all past communication can be decrypted in the next years!
- But even new algorithms for **Post-Quantum Cryptography** (**PQC**) only reset the security to the old level, at best!
- The question still remains: How long is my data secure?

Its time for the **next level of** secure communication!

Hybridisation

The next level

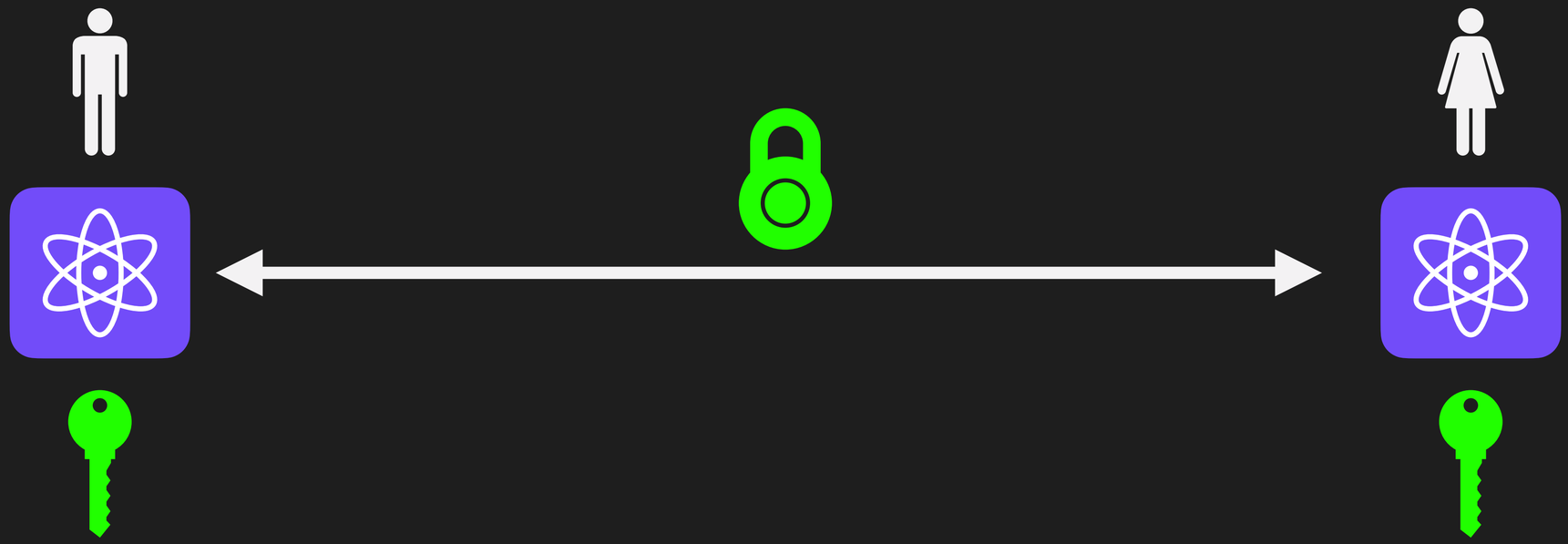




- We combine PQC algorithms with pre-shared keys into a hybrid approach.
- Even if one of the components is not secure, the **resulting encryption** is still secure!
- But how do we exchange this pre-shared key to both entities?

qonduit

Quantum Key Distribution



- Quantum Key Distribution (QKD) enables the secure exchange of a key
- A key transmitted over QKD is physically not tappable!
- But: QKD is peer-to-peer (not scalable) and has a limited range

QKDN

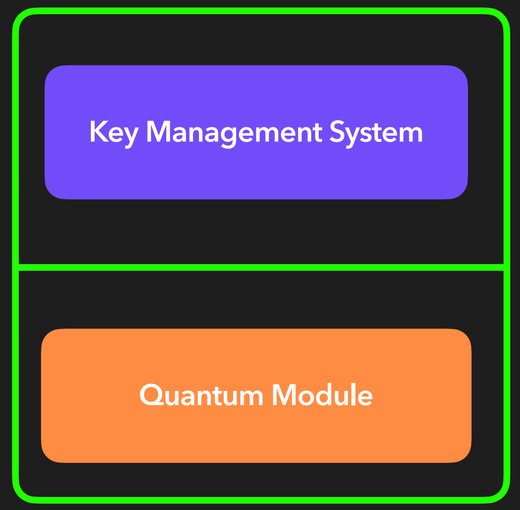
QKD as a network

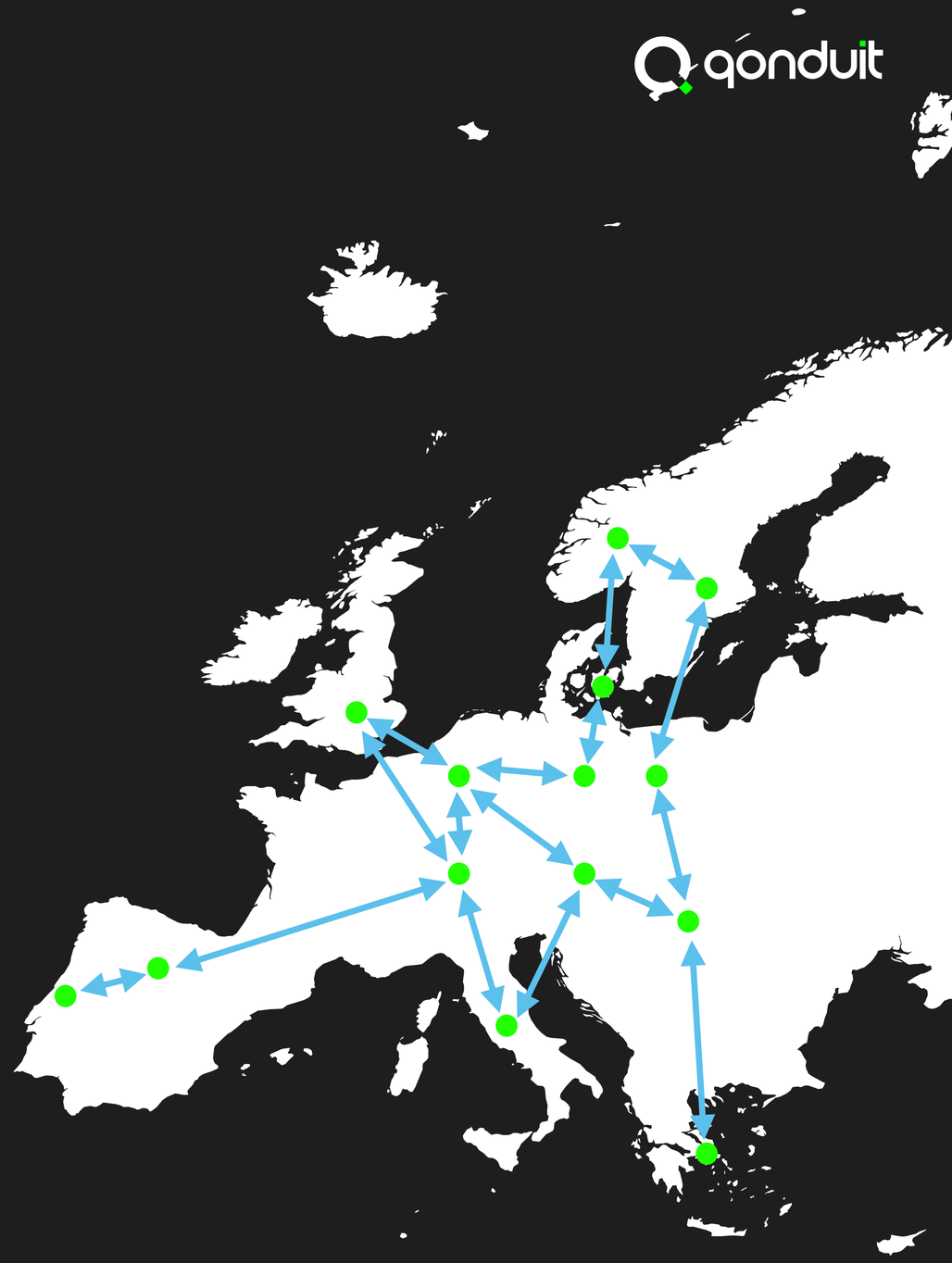
QKDN

QKD as a network

For the networking functionality →

For the peer to peer communication →

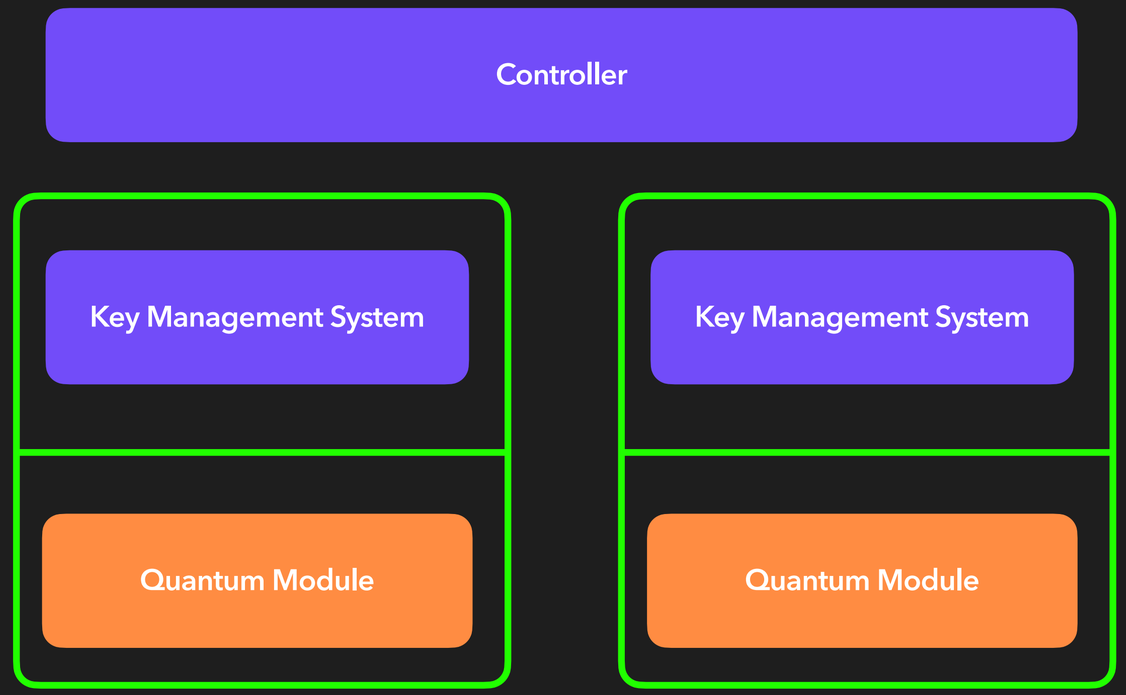


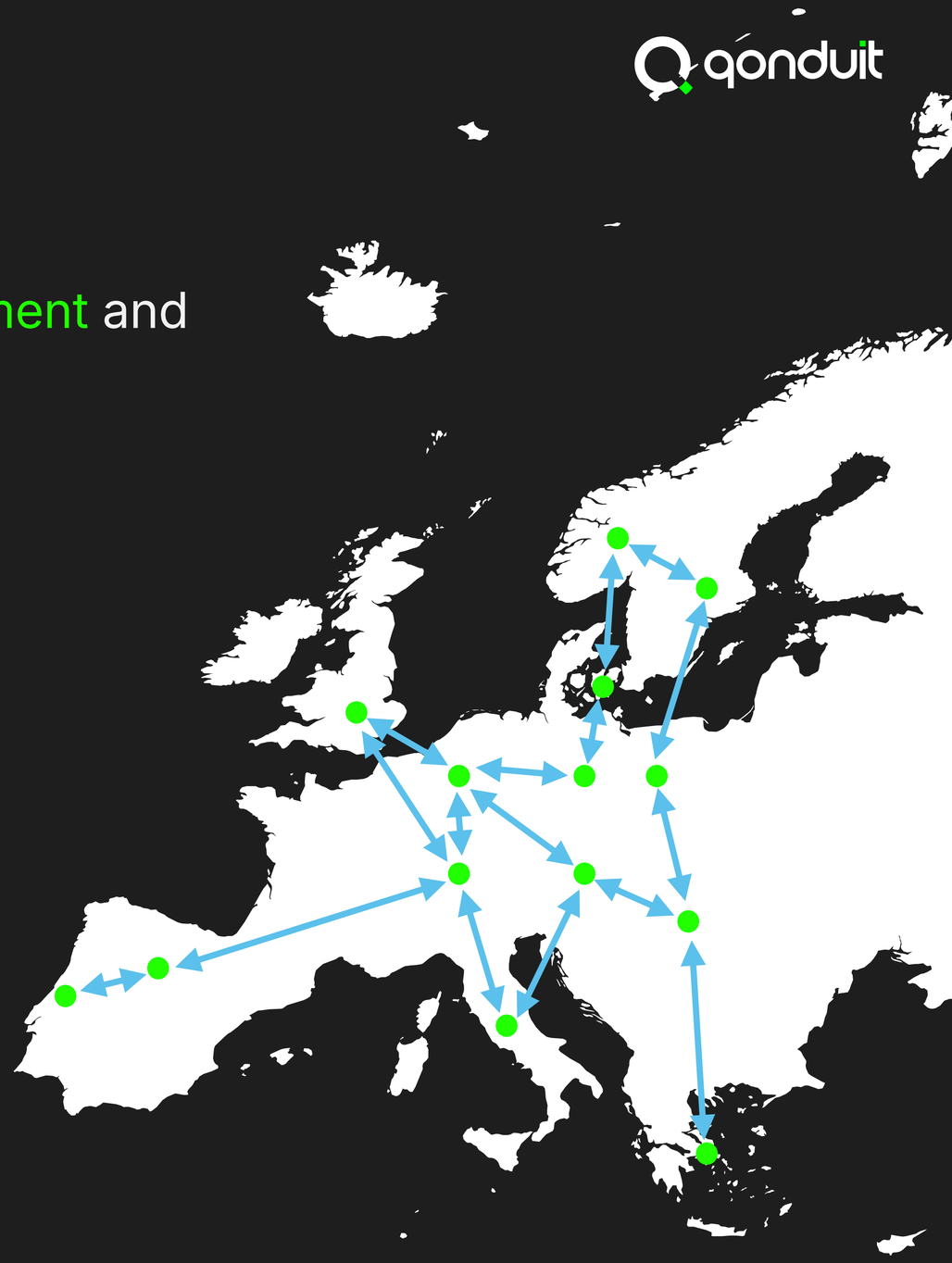


QKDN

QKD as a network

For management and operations

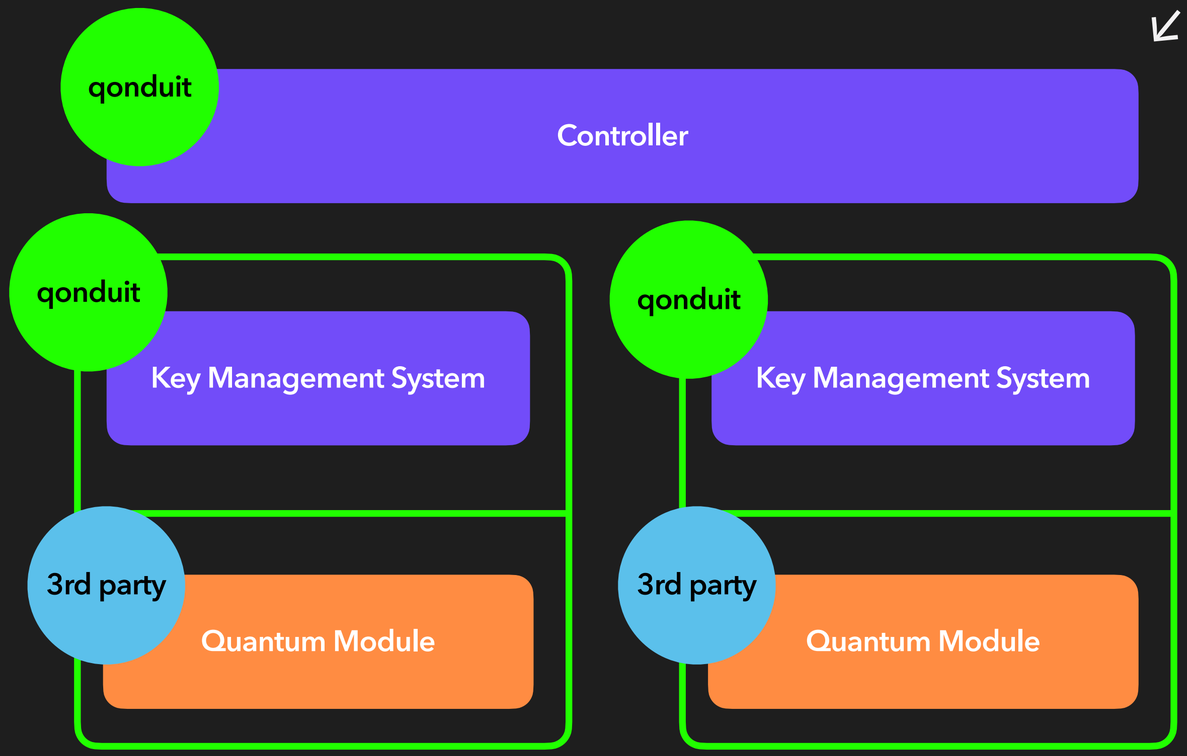


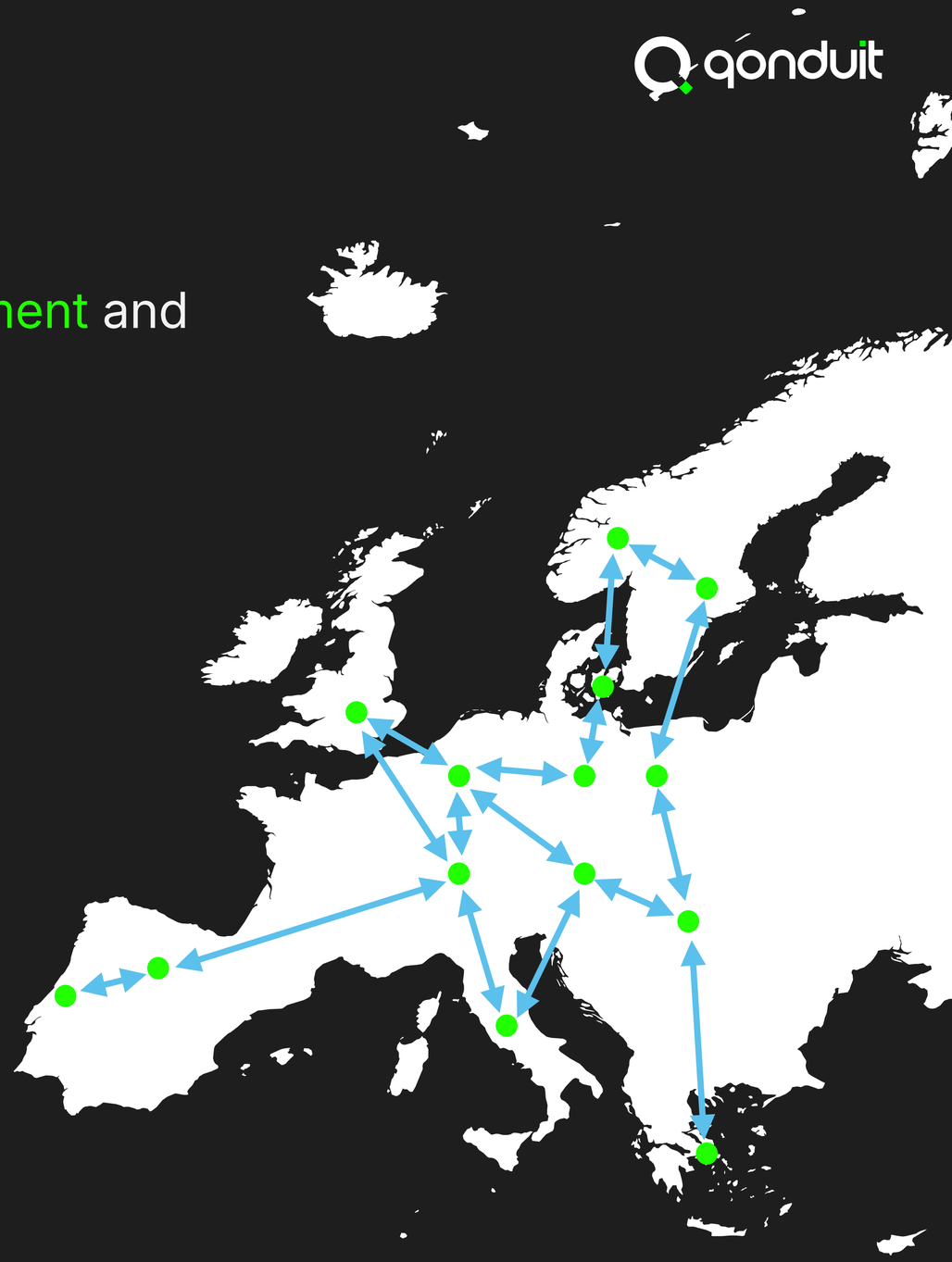


QKDN

QKD as a network

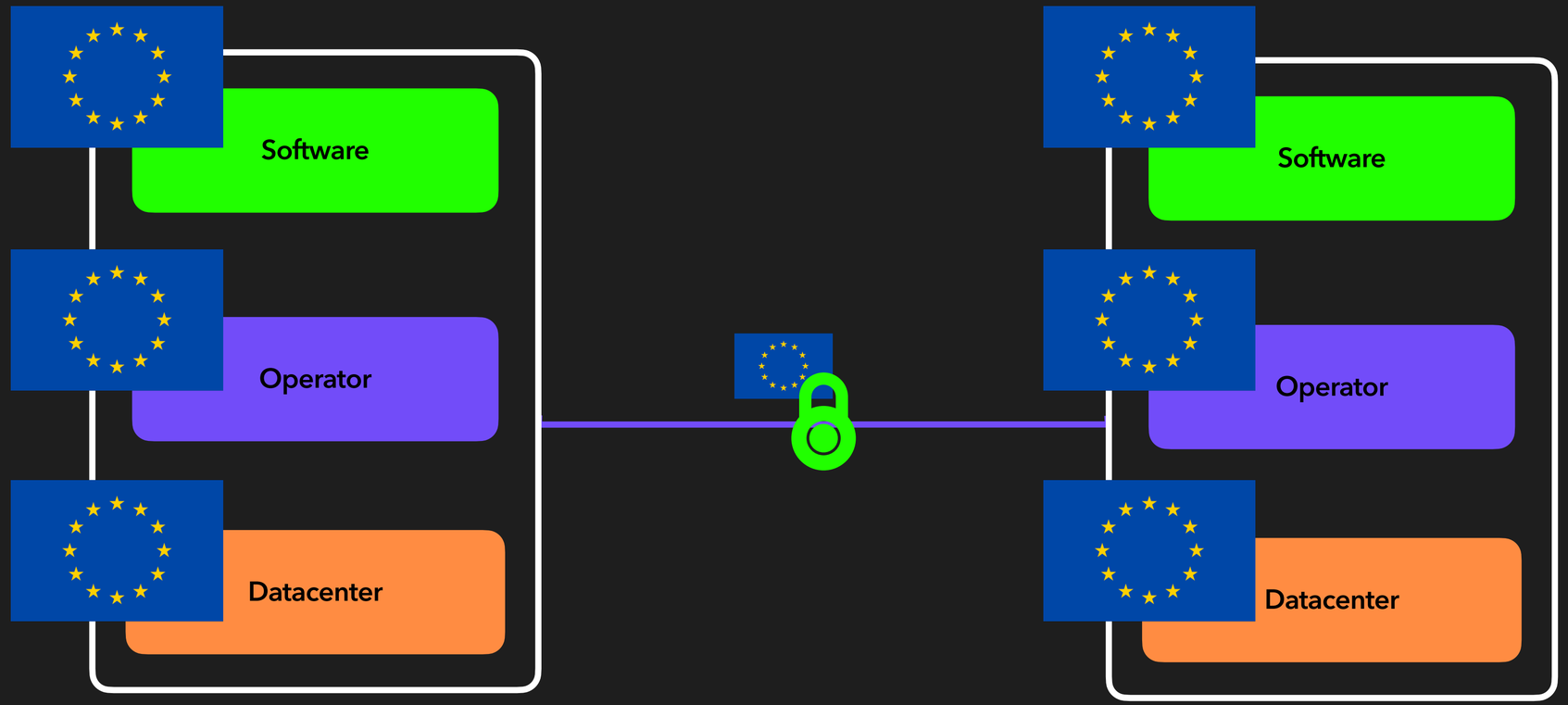
For management and operations





QKDN

Part of Europes Digital Sovereignty



How It Fits Together

qonduit as part of Europes Digital Sovereignty

- qonduit...
  - ...builds encryption for Europes **data security**
  - ...follows **European Digital Sovereignty** for tools and internal culture
  - ...supports an **ecosystem** of other QKDN components
  - ...uses **open-source** APIs and cryptography libraries
  - ...builds the **important know-how in-house**
  - ...leverages **source available licenses** to enable the customer to gain the **critical knowledge required**
  - ...encourages other companies to support European Digital Sovereignty.

Any questions?

Anything you want to know more about?

Contact us: neil.schark@qonduit.eu