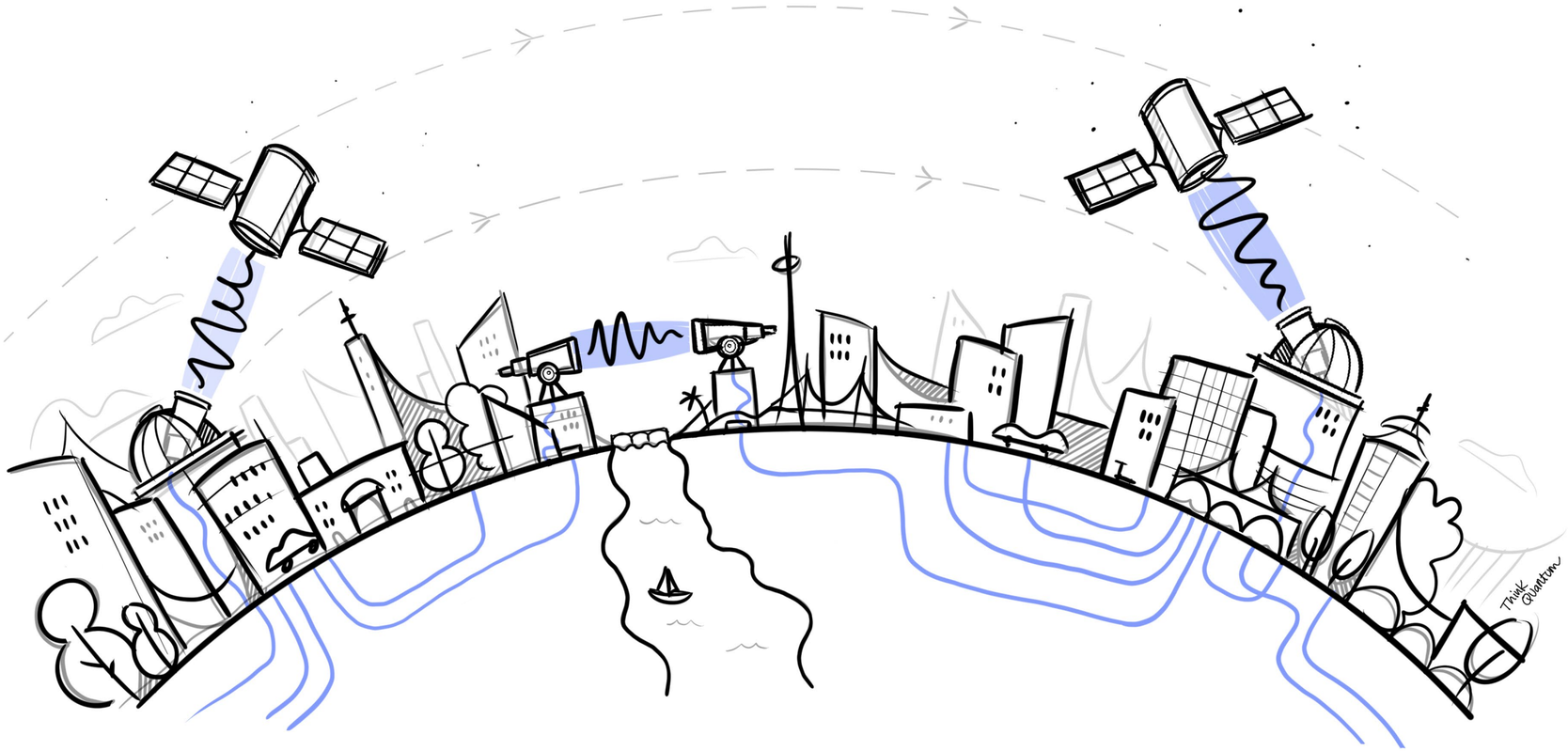
ThinKQUANTUM

OPTICAL AND QUANTUM TECHNOLOGIES FOR CYBER SECURITY

Piattaforme e tecnologie QKD per l'estensione della rete



Marco Avesani
Co-Founder & Lead System Engineer for Quantum Networking

marco.avesani@thinkquantum.com

VSIX – 26/11/2025

ThinkQUANTUM

ThinkQuantum è **nata** nel 2021 come **spin-off dell'UNIVERSITÀ DI PADOVA** offrendo **soluzioni complete per la sicurezza informatica basate su tecnologie quantistiche.**

800 1222·2022 ANNI

UNIVERSITÀ DEGLI STUDI DI PADOVA

Dal **2022, ThinkQuantum commercializza** soluzioni **QRNG** e **QKD** per la **fibra, lo spazio libero e scenari satellitari**.

ThinkQuantum, **ISO9001**, copre **l'intera value chain** dalla **progettazione e produzione fino alla messa in servizio dei sistemi**

ThinkQuantum, conuna **struttura azionaria italiana,** è un'azienda completamente italiana e offre una FILIERA EUROPEA AFFIDABILE a quei partner attivi in applicazioni geopoliticamente sensibili.

Background

ThinkQuantum è stata fondata grazie alla fusione delle competenze del gruppo di ricerca dell'università e delle capacità industriali di Officina Stellare.

Il **gruppo universitario** vanta **oltre 20 anni di esperienza** nel campo dell'informazione quantistica e delle comunicazioni quantistiche nelle fibre, nello spazio libero e con satelliti

Officina Stellare è **leader** nella **progettazione e sviluppo di telescopi** e sistemi optomeccanici per l'osservazione, la **comunicazione laser e applicazioni di difesa sia a terra che nello spazio**

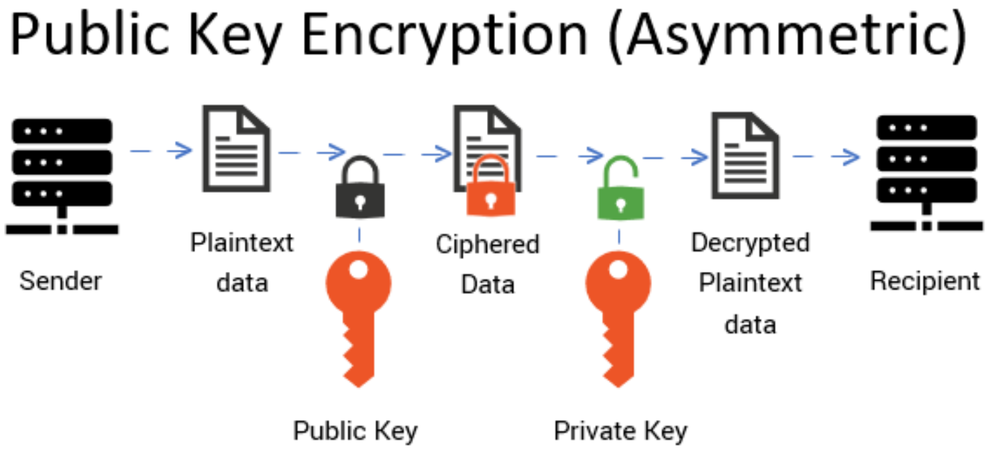
Coinvolta in diversi progetti ESA (Agenzia Spaziale Europea), ASI (Agenzia spaziale italiana) e UE EC (Commissione Europea). Installazioni in maggior parte di reti quantistiche europee:

Comunicazioni sicure

La **maggior parte** delle **informazioni** che **trasmettiamo** ogni giorno su **Internet è, e deve essere, crittografata.** Alcuni **esempi** sono: transazioni **finanziarie**, **messaggistica**, informazioni **sull'identità**

Fondamentale per infrastrutture critiche quali: comunicazioni, trasporti, difesa e medicale

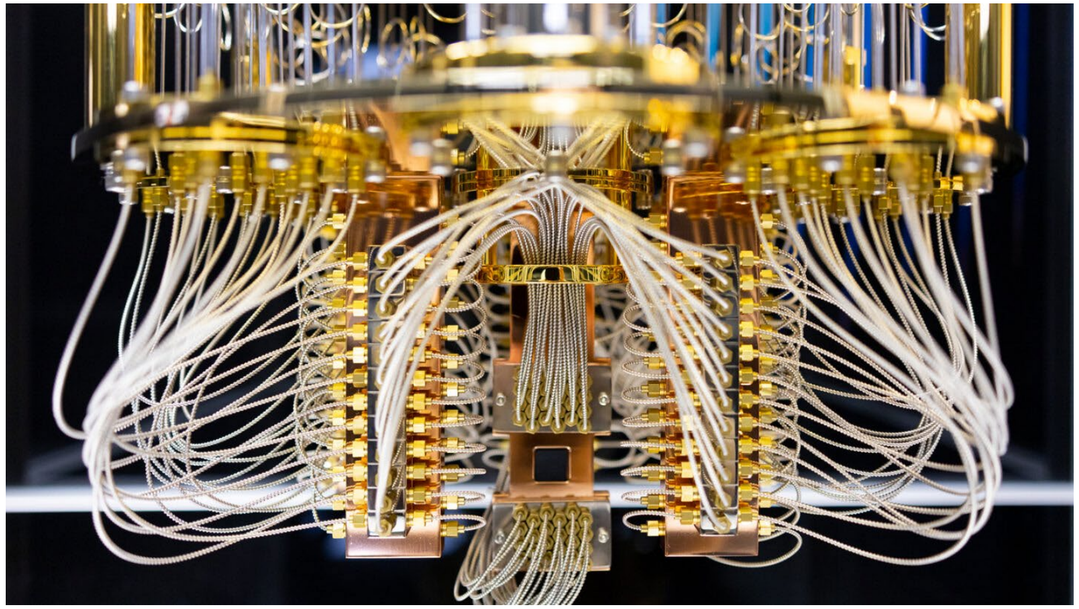
I sistemi di **crittografia** comunemente **utilizzati oggi** si basano sulla **crittografia a chiave pubblica**, come **RSA**, **curve ellittiche**, etc



Si basano su **problemi matematici**, come la fattorizzazione di grandi numeri, che sono **estremamente difficili** da risolvere da **computer**

Il pericolo dei computer quantistici

Questi **problemi** sono **facilmente risolvibili** dai **computer quantistici**



Tutta l'infrastruttura di sicurezza moderna è in pericolo.

Ci dobbiamo veramente preoccupare ora? C'è tempo?

COMPUTERS

IBM's new 53-qubit quantum computer is its biggest yet

The system will go online in October.

BY STEPHEN SHANKLAND | SEPTEMBER 18, 2019 5:00 AM PDT

POPULAR SCIENCE

WANT MORE?

Get Rogers Unison and stop paying for lines you don't use.

SCIENCE TECH DIY GOODS VIDEO ROLL THE DICE SUBSCRIBE

China is opening a new quantum research supercenter

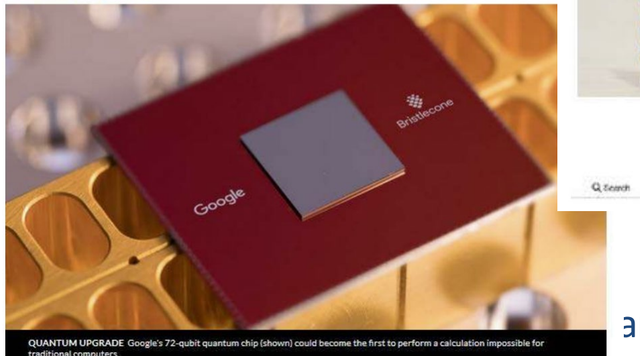
The country wants to build a quantum computer with a million times the computing power presently in the world.

By Jeffrey Lin and P.W. Singer October 10, 2017

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER 5:17PM, MARCH 5, 2018



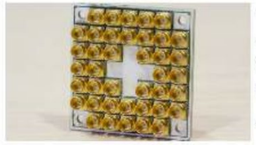
QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers

Intel brings Quantum computing a step closer to reality

BY ROHITH BHASKAR OCT. 12, 2017, 2:57 P.M.

Intel is betting on its fabrication expertise to push quantum computing into the mainstream

2 shares



A lot of companies are pushing to make quantum computing real. Google, IBM, Microsoft an... in the Indu... quantum ma... confines of ...

Search Bloomber...

Forbes

IBM Doubles Its Quantum Computing Power Again

FINANCIAL TIMES myFT

Quantum technologies + Add to myFT

Google claims breakthrough in quantum computer error correction

ThinKQUANTUM

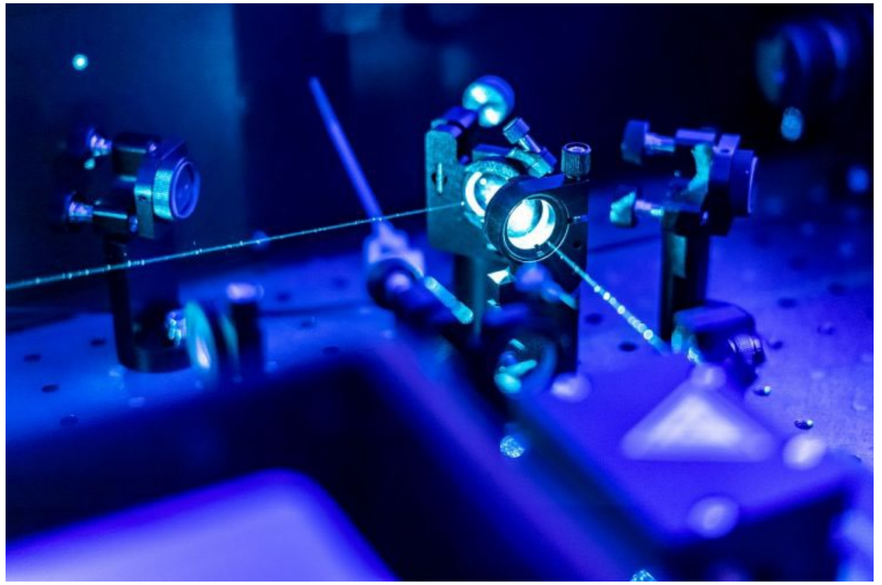
antum.com

La soluzione dalla meccanica quantistica: Quantum Key Distribution

Quantum Key Distribution (QKD) è un **protocollo** per generare **chiavi identiche perfettamente sicure** tra due utenti **distanti**

Funziona **scambiando singole particelle quantistiche** di luce tramite **fibra, spazio libero o canali satellitari**

Si basa sulle leggi della fisica e non su difficili problemi matematici

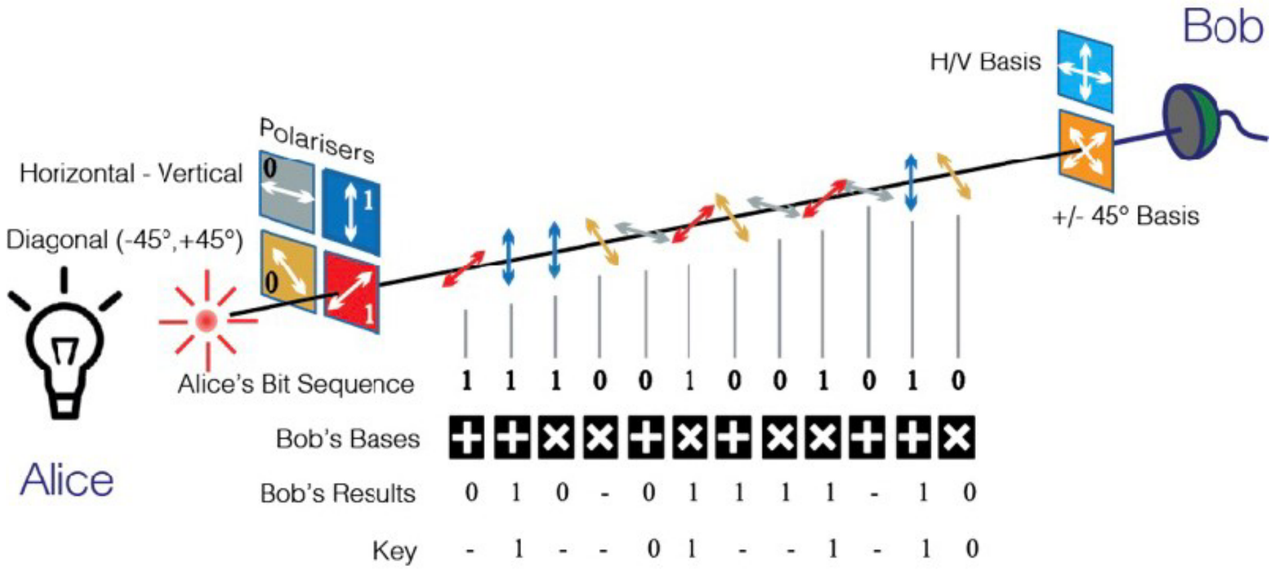


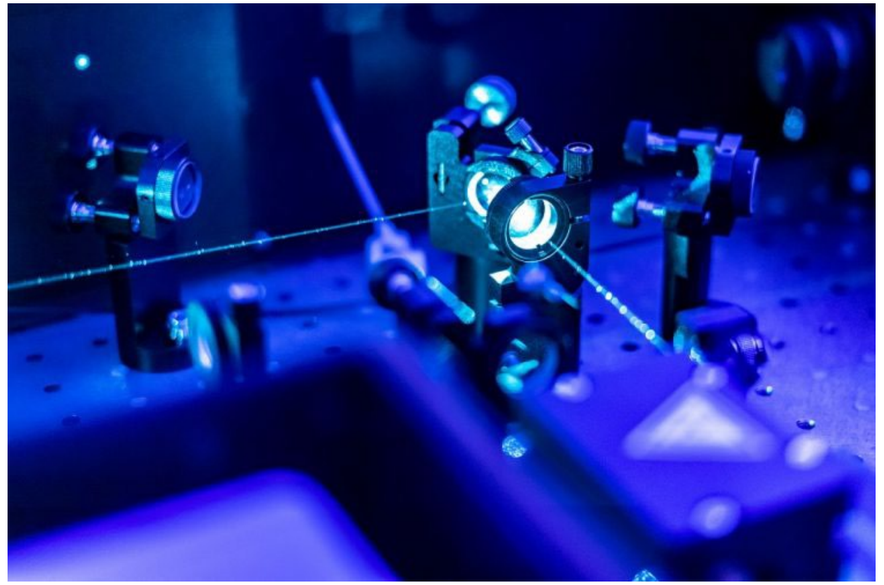
La soluzione dalla meccanica quantistica: Quantum Key Distribution

Quantum Key Distribution (QKD) è un **protocollo** per generare **chiavi identiche perfettamente sicure** tra due utenti **distanti**

Funziona **scambiando singole particelle quantistiche** di luce tramite **fibra, spazio libero o canali satellitari**

Si basa sulle leggi della fisica e non su difficili problemi matematici





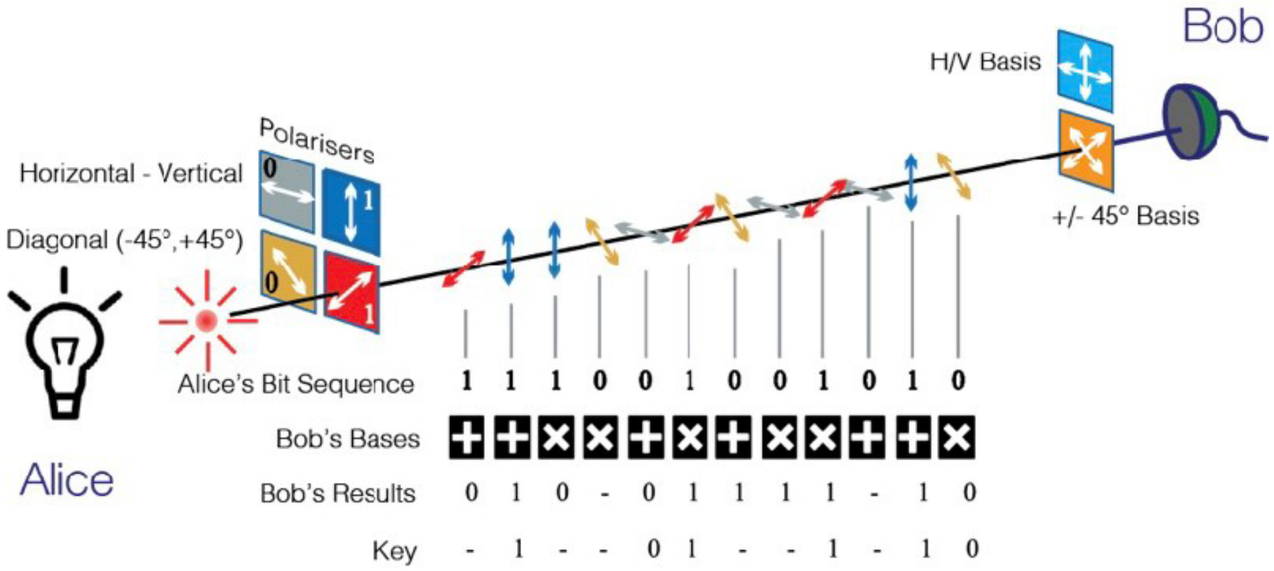
- In **comunicazioni classiche** i **dati** possono essere **letti e ritrasmessi senza essere alterati**. Gli **stati quantistici** (Qubit) **non sono clonabili**
- Ogni **interazione** dell'attaccante **introduce errori**, che posso misurare

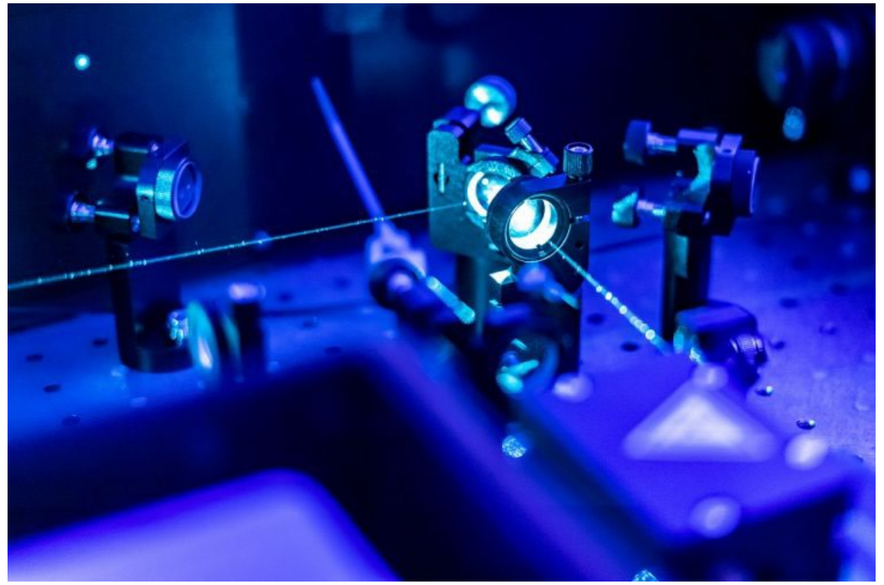
La soluzione dalla meccanica quantistica: Quantum Key Distribution

Quantum Key Distribution (QKD) è un **protocollo** per generare **chiavi identiche perfettamente sicure** tra due utenti **distanti**

Funziona **scambiando singole particelle quantistiche** di luce tramite **fibra, spazio libero o canali satellitari**

Si basa sulle leggi della fisica e non su difficili problemi matematici



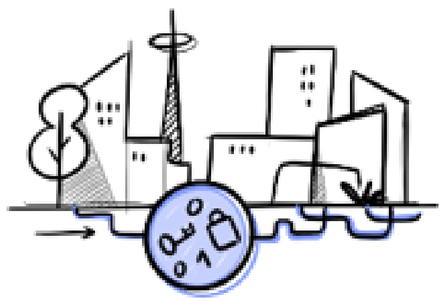


- In **comunicazioni classiche** i **dati** possono essere **letti e ritrasmessi senza essere alterati**. Gli **stati quantistici** (Qubit) **non sono clonabili**
- Ogni **interazione** dell'attaccante **introduce errori**, che posso misurare

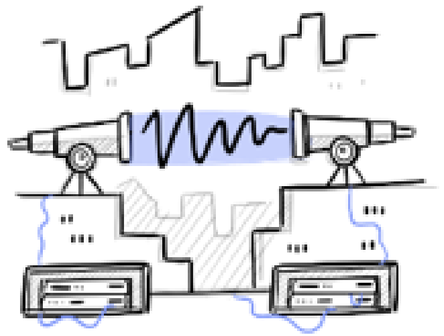
Sicuro da qualsiasi tipo di attacco, non solo dai computer quantistici

Prodotti per molti domini

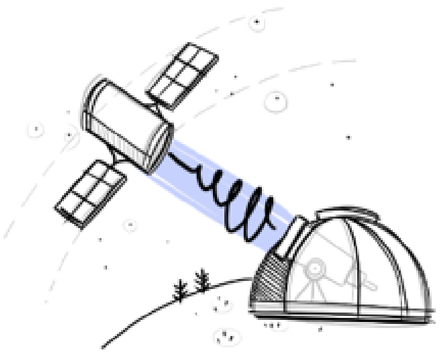
Fibra ottica



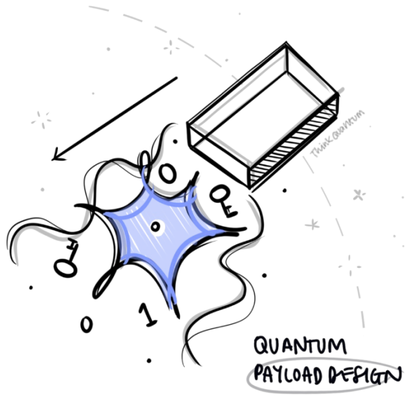
Spazio-libero



OGS & Ricevitori



Sorgenti satellitari



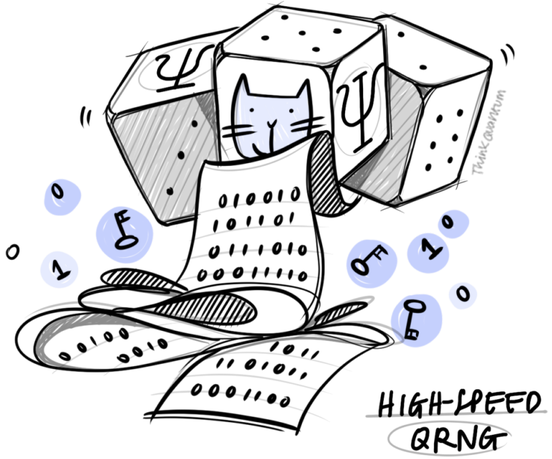
QRNG

Generazione quantistica di numeri casuali

La generazione di numeri casuali è di fondamentale importanza in molti settori industriali, oggi si utilizzano numeri pseudo-casuali (*'algoritmi deterministici su macchine deterministiche'*) con forti limitazioni di qualità e sicurezza

La maturità delle tecnologie quantistiche consente di **sfruttare la casualità intrinseca della fisica quantistica per generare numeri casuali**

Quantum Random Number Generation 'QRNG'

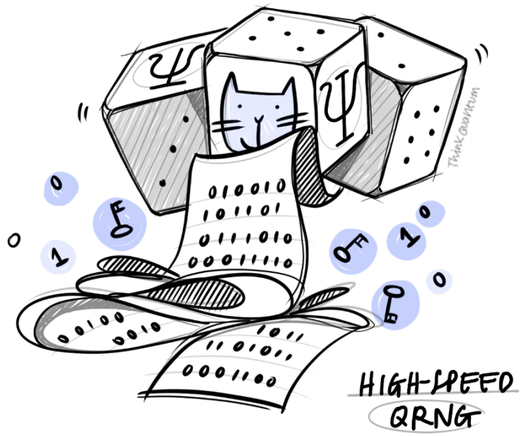


Prodotti QKD e QRNG

ThiKe

Piattaforma QRNG

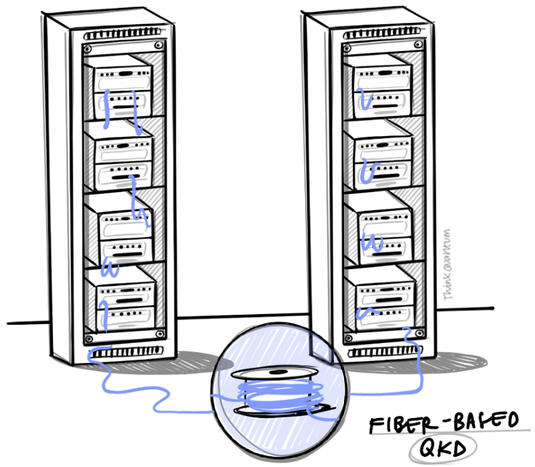
- *Source-device independent*
- *Secure random bit rate: 330 Mbps*
- *Versione OEM disponibile*



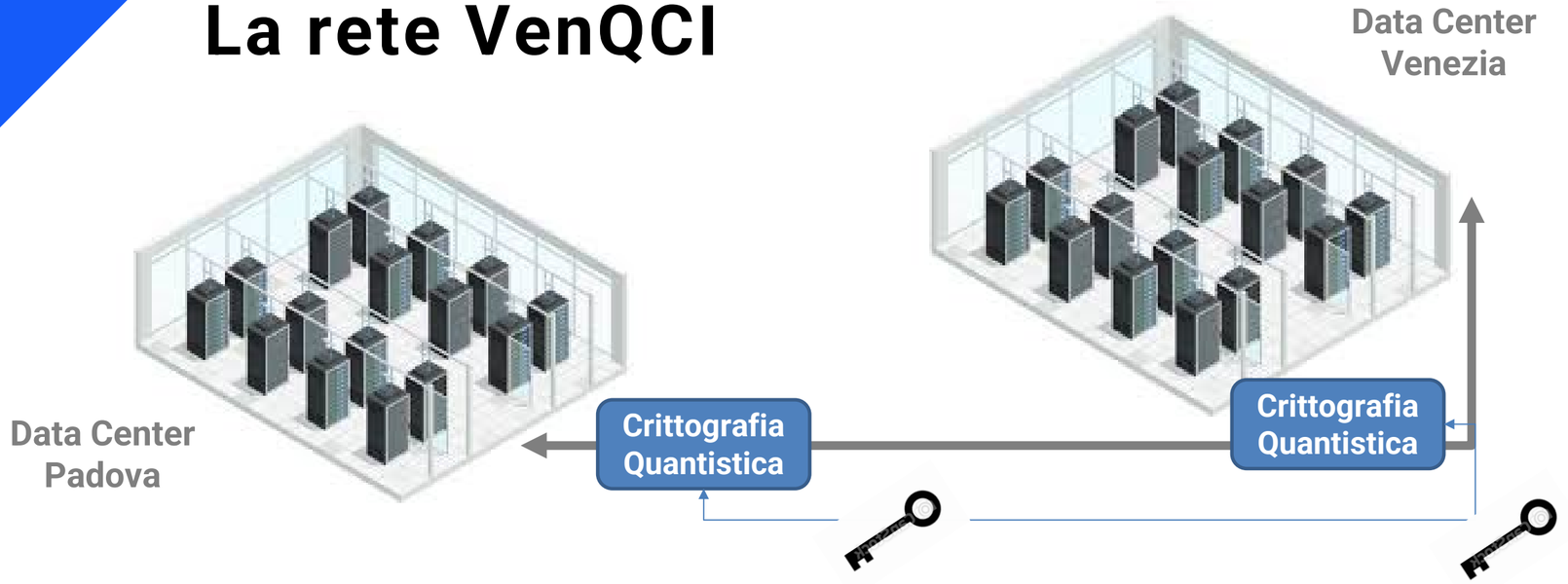
QuKy

QKD platform

- *1-decoy BB84*
- *Codifica della polarizzazione con lo schema iPognac*
- *“True” QRNG stream*
- *Key Management System*
- *SDN*
- *30dB di perdite di canale*



La rete VenQCI

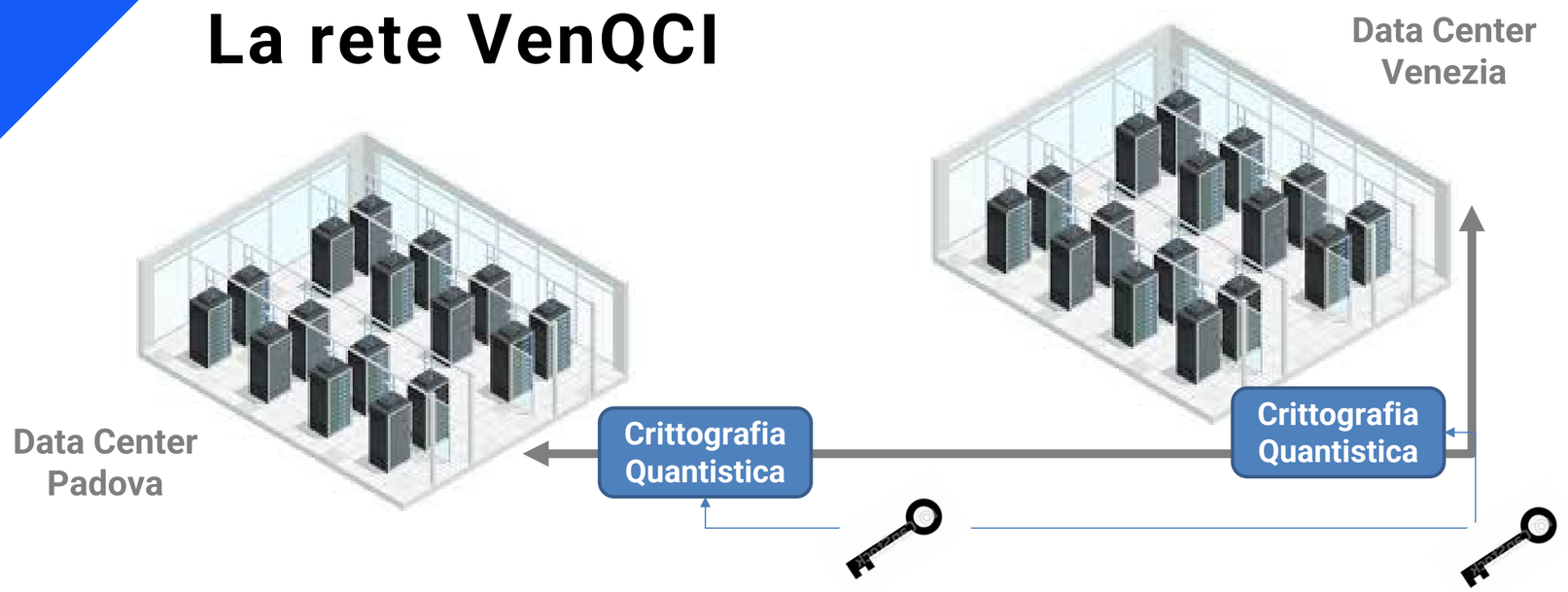


Tecnologie
Ciascun **nodo** della rete è dotato di:

- **dispositivi per lo scambio di chiavi quantistiche (QKD) ThinkQuantum**
- sistemi di **cifratura CISCO** del traffico a **layer 2 / 100GE** con chiavi quantistiche

- **I nodi**
- Regione Veneto (VEGA)
- CAV (Marghera)
- CAV (Padova Est)
- Vsix (Padova, zona Industriale)
- QuTech (Padova, centro)

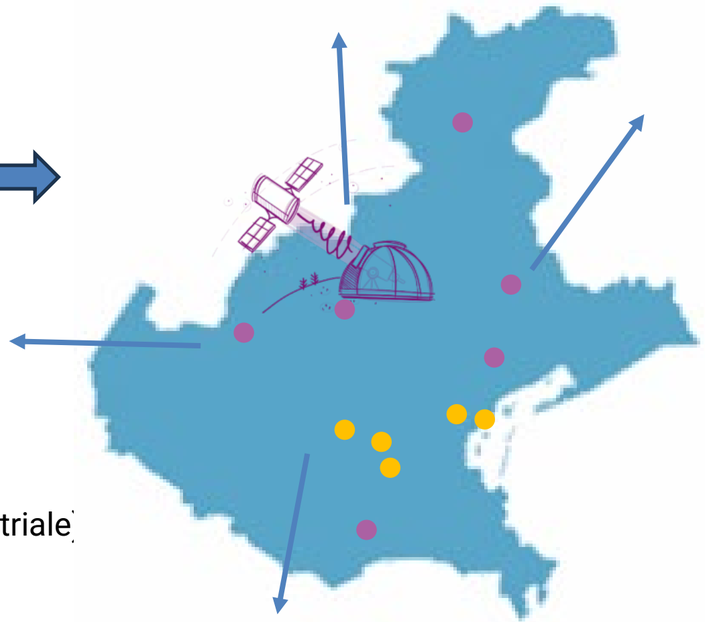
La rete VenQCI



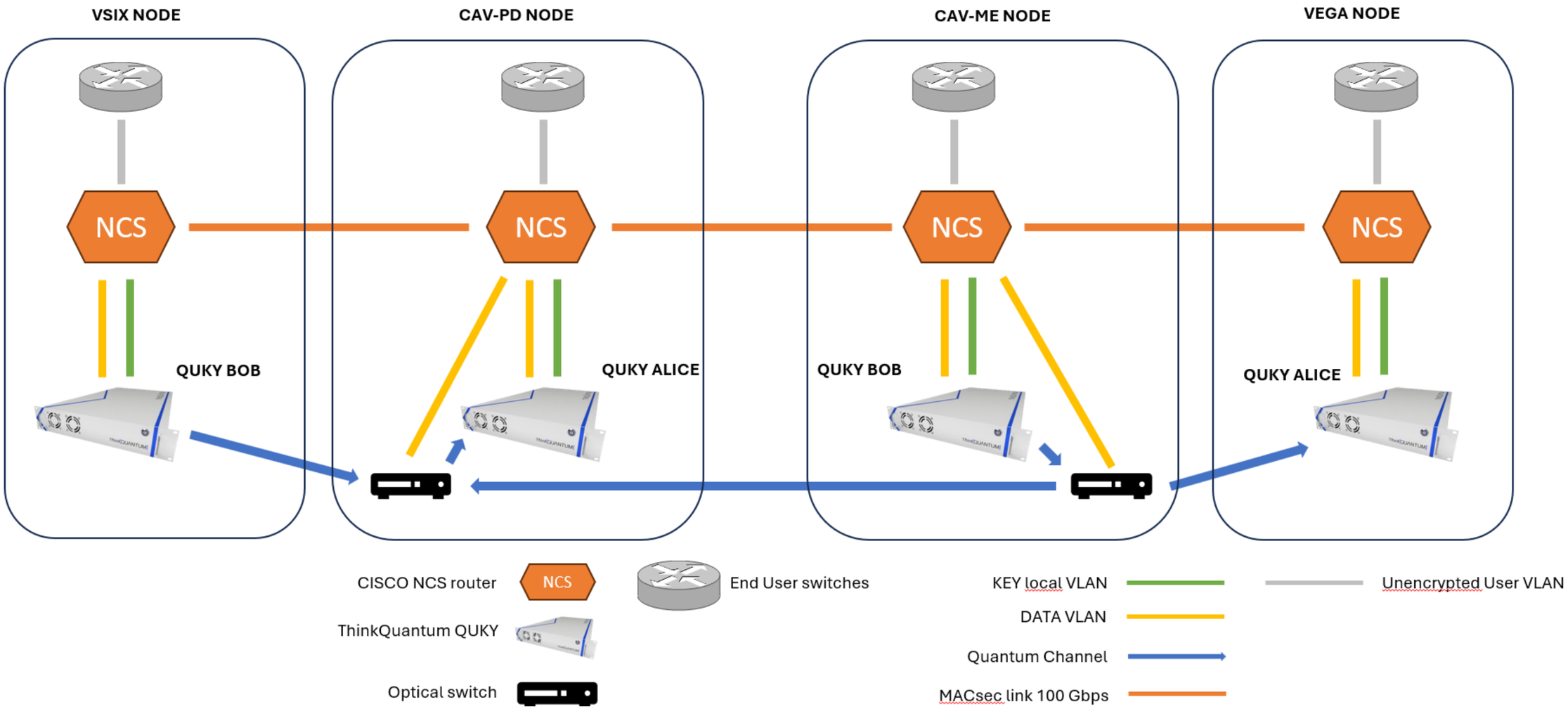
Tecnologie
Ciascun **nodo** della rete è dotato di:

- **dispositivi per lo scambio di chiavi quantistiche (QKD) ThinkQuantum**
- sistemi di **cifratura CISCO** del traffico a **layer 2 / 100GE** con chiavi quantistiche

- **I nodi**
- Regione Veneto (VEGA)
- CAV (Marghera)
- CAV (Padova Est)
- Vsix (Padova, zona Industriale)
- QuTech (Padova, centro)



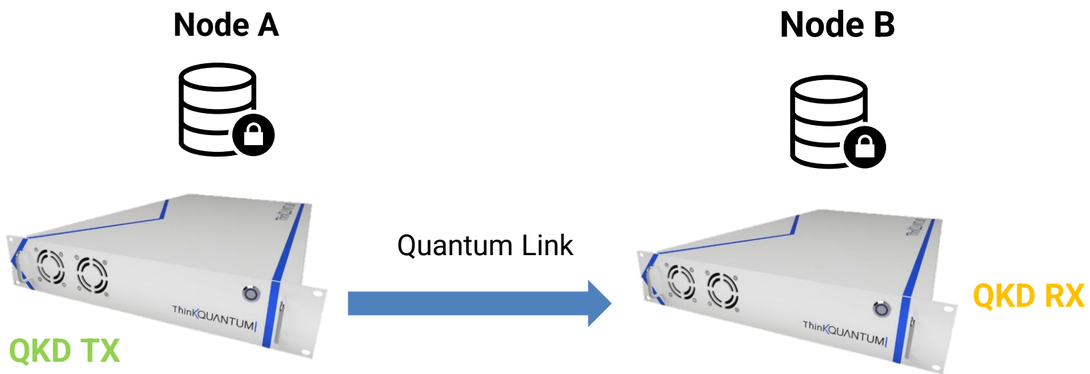
La rete VenQCI



L’innovazione della tecnologia QKD al centro di VenQCI: QKD switching

La tecnologia **QKD** offre il **più alto grado di sicurezza** per la **protezione dei dati**, ma presenta alcune importanti **sfide nell’integrazione** con **l’infrastruttura** di comunicazione classica.

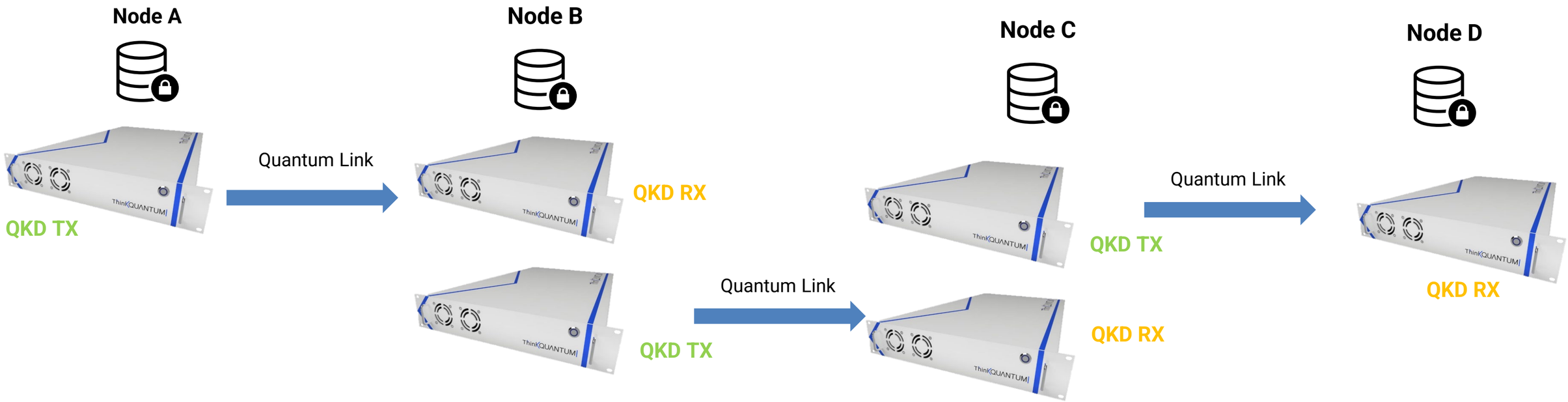
I **sistemi QKD standard** sono intrinsecamente **point-to-point**



L’innovazione della tecnologia QKD al centro di VenQCI: QKD switching

La tecnologia **QKD** offre il **più alto grado di sicurezza** per la **protezione dei dati**, ma presenta alcune importanti **sfide nell’integrazione** con **l’infrastruttura** di comunicazione classica.

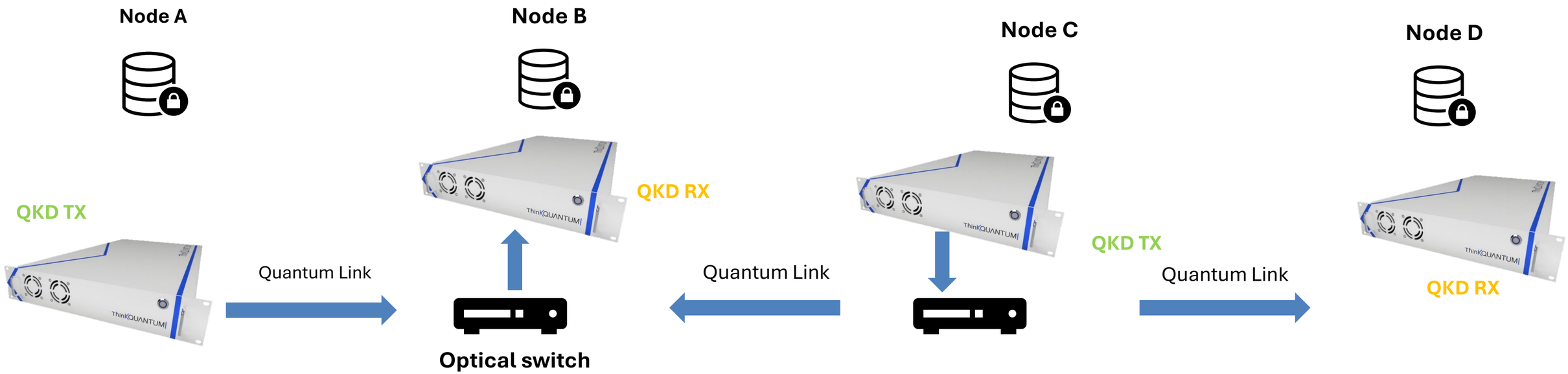
I **sistemi QKD standard** sono intrinsecamente **point-to-point**



Lo sviluppo di una **rete RELAY a 4 nodi** richiederebbe **3 link fisici** e **6 dispositivi QKD**

L’innovazione della tecnologia QKD al centro di VenQCI: QKD switching

La **tecnologia sviluppata in ThinkQuantum** ed **introdotta nella rete di VenQCI** realizza lo **switching ottico** dei terminali QKD, permettendo la connessione di un sistema QKD a più dispositivi.

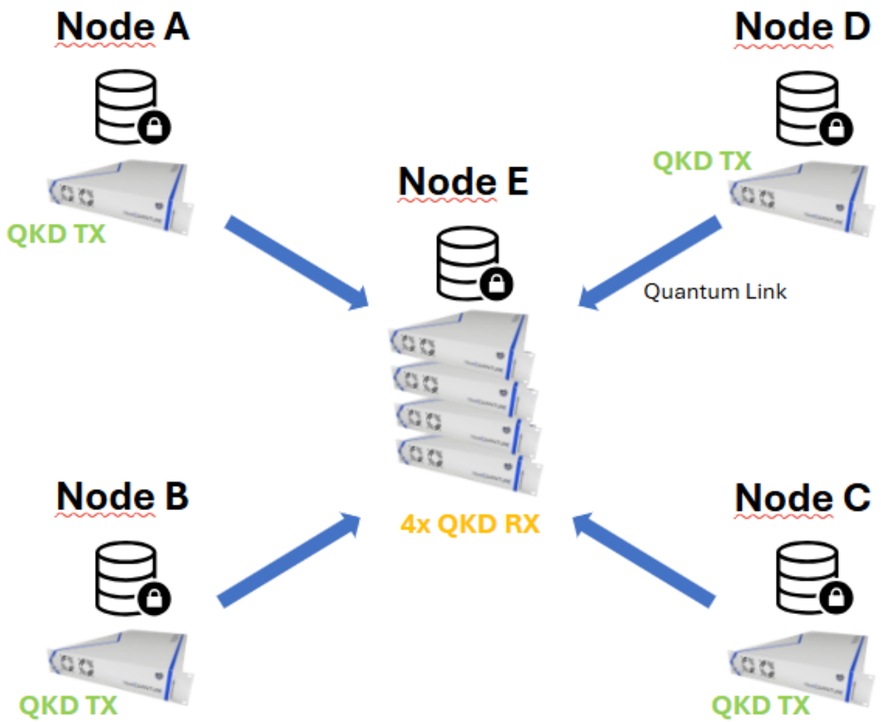


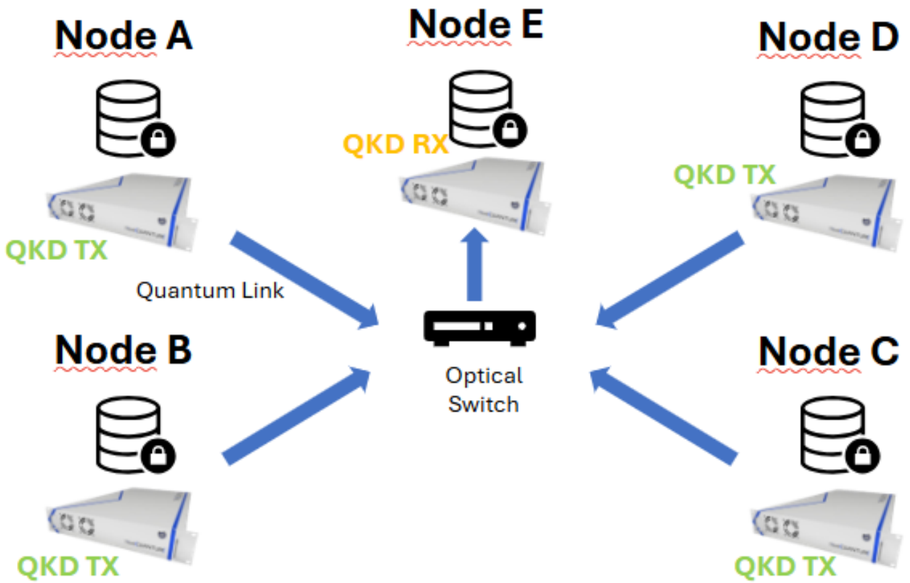
Questo sistema permette di **implementare topologie di reti complesse**, **diminuendo** il numero di **dispositivi** necessari e **semplificando l’espansione** futura della rete.

Per una rete di 4 nodi si risparmiano due dispositivi, mantenendo 3 link fisici

L’innovazione della tecnologia QKD al centro di VenQCI: QKD switching

In **una rete a stella** con **5 nodi** e **4 link fisici**, sarebbero necessari **8 dispositivi QKD**



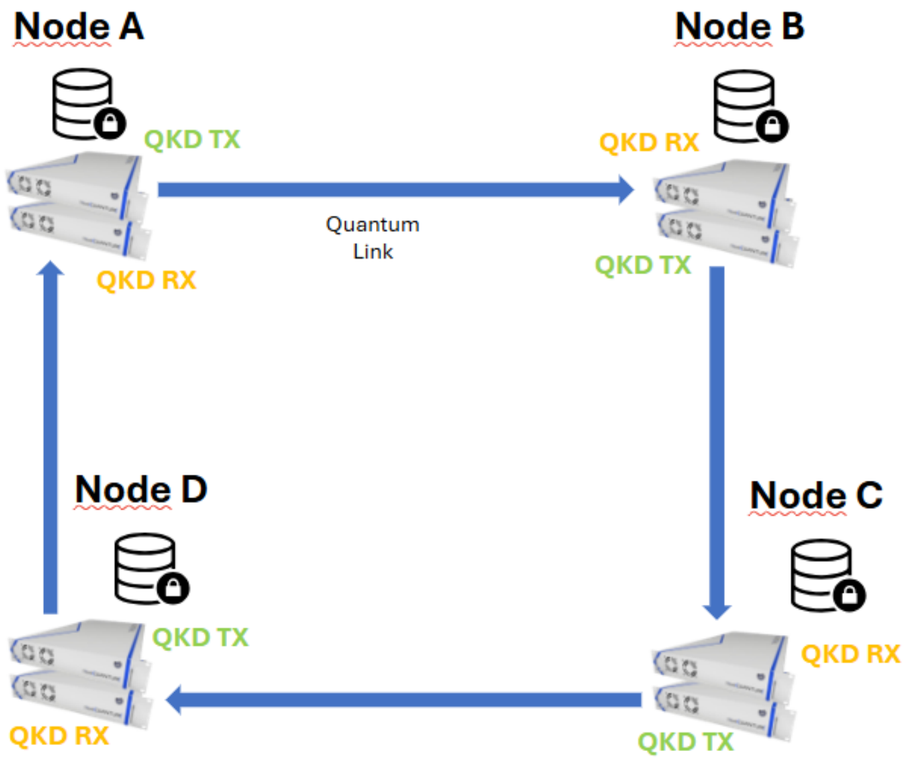


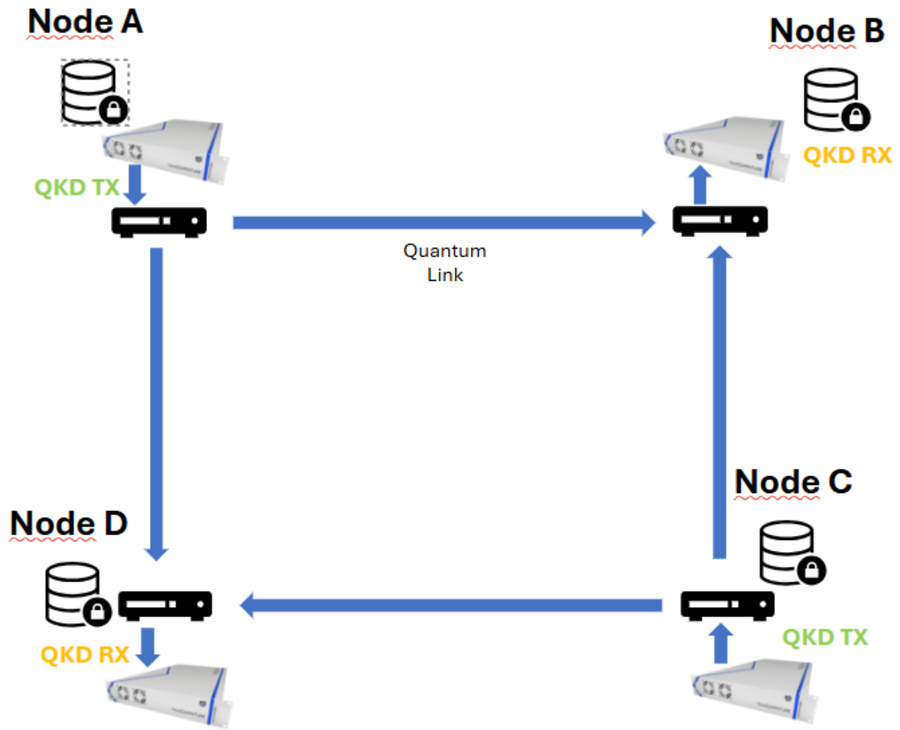
Con il sistema di **switching** è possibile **risparmiare 3 dispositivi QKD**

L’aggiunta di un nuovo nodo non richiede modifiche nell’hub centrale. Il key manager si occupa della gestione delle chiavi in tutti i nuovi nodi.

L’innovazione della tecnologia QKD al centro di VenQCI: QKD switching

In **una rete ad anello** con **4 nodi** e **4 link fisici**, sarebbero necessari **8 dispositivi QKD**

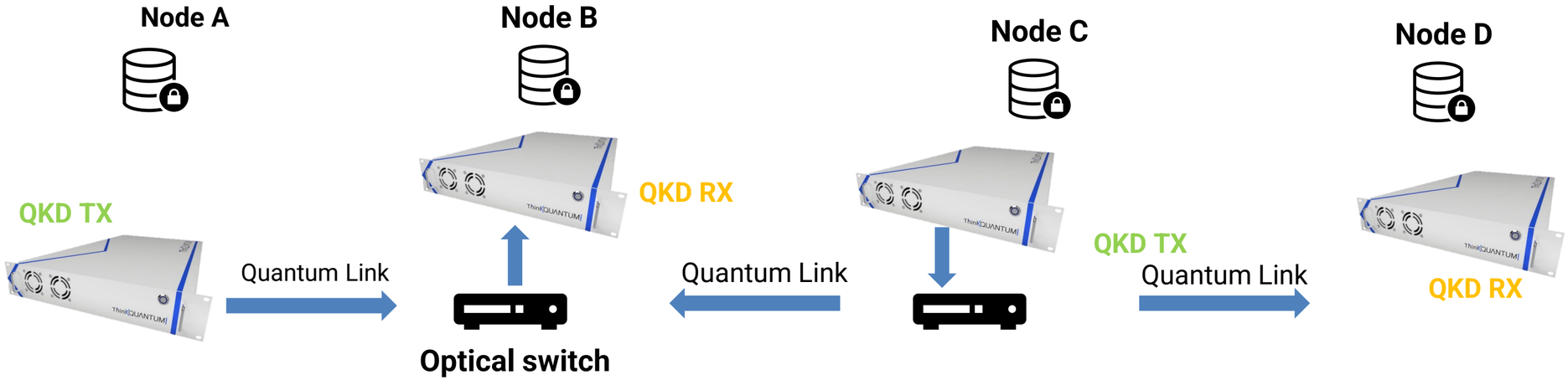




Con il sistema di **switching** è possibile **risparmiare 4 dispositivi QKD**

L’innovazione della tecnologia QKD al centro di VenQCI: QKD switching

Nella rete di **VenQCI** la tecnologia di **switching** è già stata **implementata** ed utilizzata in **produzione**



Un esempio il **network** composto dai nodi

- **VSIX**
- **CavPD**: Centro CAV casello di padova
- **CavVE**: Centro CAV casello di Mestre
- **VEGA**: Veneto technology park
-

QKD links:

- **VSIX - CavPD: ~5 km fibra**
- **CavPD - CavVE: ~20 km fibra**
- **CavVE - VEGA: ~5 km fibra**

L’innovazione della tecnologia QKD al centro di VenQCI: QKD switching

Il **network è oggetto anche di uno studio scientifico** recentemente condiviso con la comunità scientifica.

Presentato il sistema e discussi risultati di più di due mesi monitor continuo del network

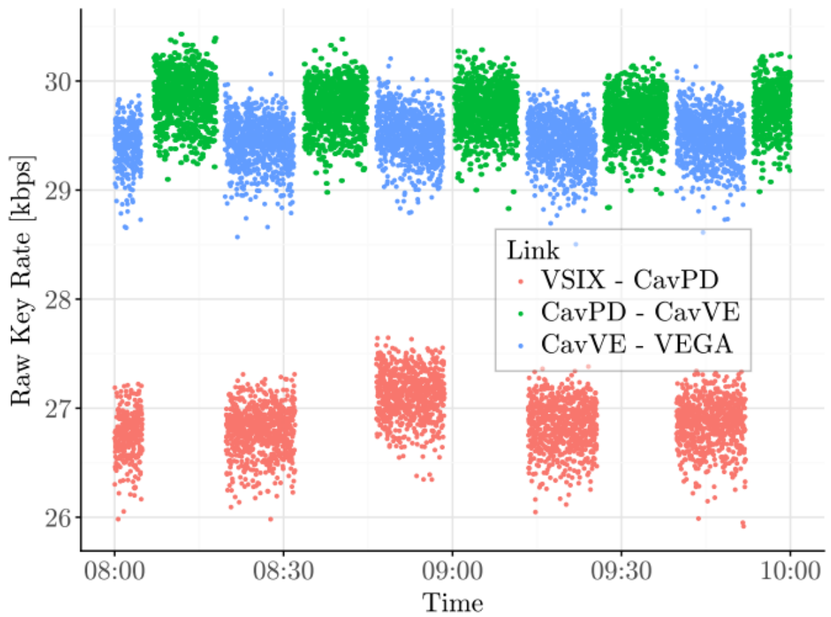
Long-term analysis of *efficient-BB84* 4-node network with optical switches in metropolitan environment

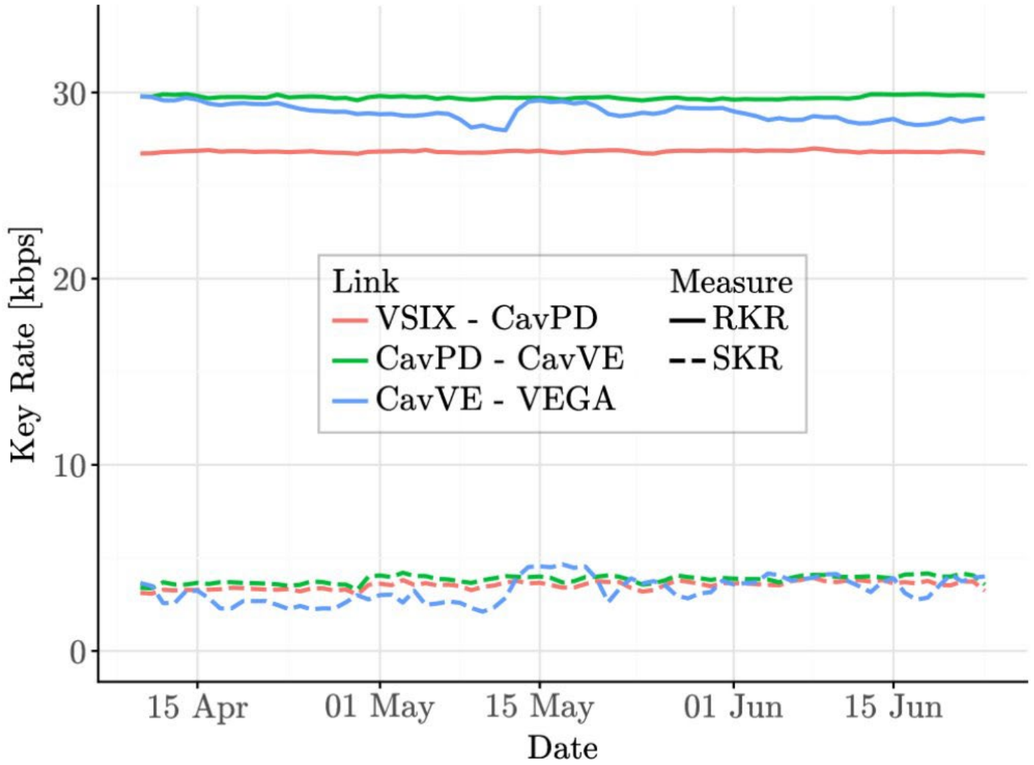
Alberto De Toni,[1] Edoardo Bortolozzo,[1,2] Alessandro Emanuele,[2] Marco Venturini,[2] Luca Calderaro,[2] Marco Avesani,[1,2] Giuseppe Vallone,[1,2,3] and Paolo Villoresi[1,2,3]

[1]*Dipartimento di Ingegneria dell’Informazione, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*

[2]*ThinkQuantum s.r.l., via della Tecnica 85, IT-36030 Sarcedo, Italy*

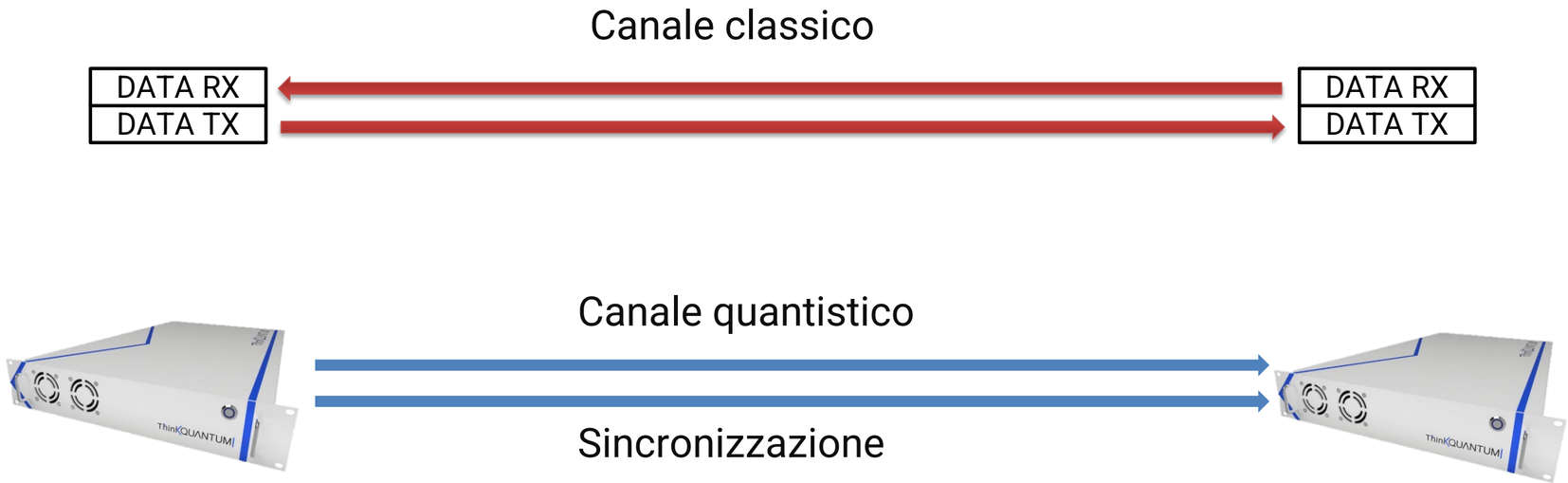
[3]*Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6A, IT-35131 Padova, Italy*





L’innovazione della tecnologia QKD al centro di VenQCI: sincronizzazione con I qubit, il Qubit4Sync

Un’altra **sfida** è legata al **numero di fibre** richieste dai sistemi di QKD. **Tipicamente** è richiesto **un canale classico per la comunicazione** (dedicato, multiplexed o addirittura internet) **e due fibre simplex dark per il canale quantistico (qubit) e per quello di sincronizzazione**



L’innovazione della tecnologia QKD al centro di VenQCI: sincronizzazione con I qubit, il Qubit4Sync

Un’altra **sfida** è legata al **numero di fibre** richieste dai sistemi di QKD. **Tipicamente** è richiesto **un canale classico per la comunicazione** (dedicato, multiplexed o addirittura internet) **e due fibre simplex dark per il canale quantistico (qubit) e per quello di sincronizzazione**

Nei sistemi ThinkQuantum viene utlizzato un sistema di sincronizzazione basato sui qubit stessi: Qubit4Syc. Questo permette di risparmiare 1 fibra per collegamento.

Semplificazione dell’installazione per i nuovi utenti

L’innovazione della tecnologia QKD al centro di VenQCI: multiplexing e coesistenza

Anche le dark fiber richiesto dal canale quantistico sono una risorsa preziosa: sono utilizzate per minimizzare il rumore aggiunto agli stati quantistici. Tuttavia non sempre sono disponibili:

L’innovazione della tecnologia QKD al centro di VenQCI: multiplexing e coesistenza

Anche le dark fiber richiesto dal canale quantistico sono una risorsa preziosa: sono utilizzate per minimizzare il rumore aggiunto agli stati quantistici. Tuttavia non sempre sono disponibili:

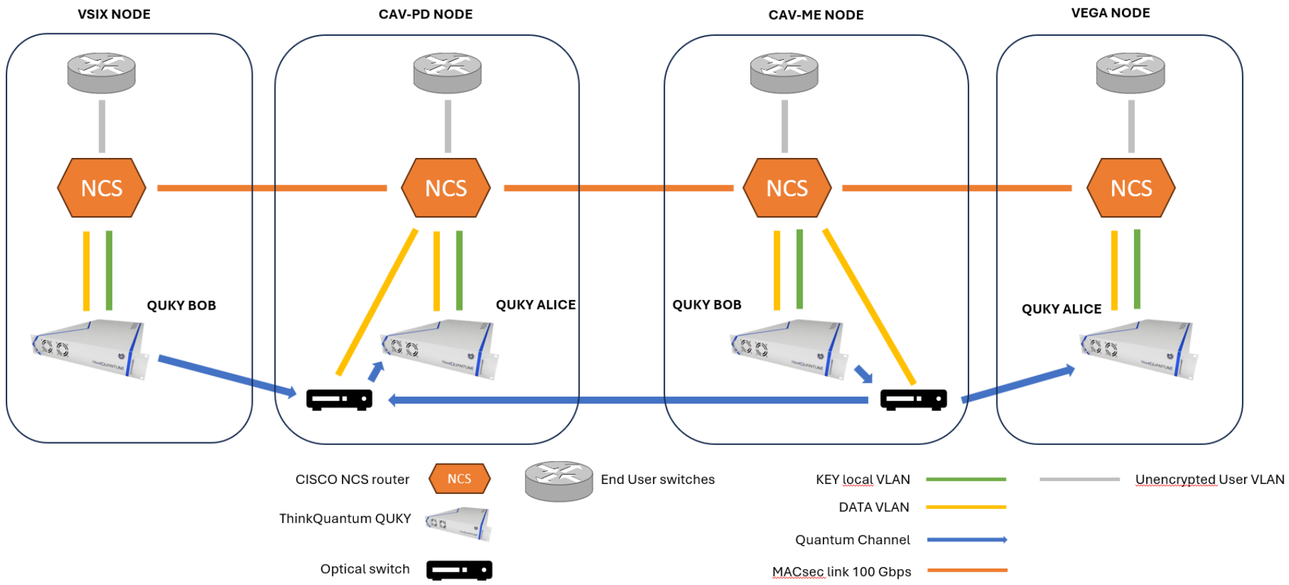
Utilizzando sistemi di **multiplexing** e de-multiplexing spettrale, abbinati a sistemi di **filtraggio avanzati** è possibile far **coesistere comunicazioni classiche con i sistemi QKD, in banda C (occupazione 1 canale DWDM) o O, sulla stessa fibra.**

Ulteriore riduzione di fibre necessarie

L’innovazione della tecnologia QKD al centro di VenQCI: KMS & encryptors

I sistemi di **KEY Management**, **installati** sui sistemi **QKD**, gestiscono **autonomamente ed automaticamente** la complessità **della gestione e distribuzione delle chiavi anche su reti mesh complesse**

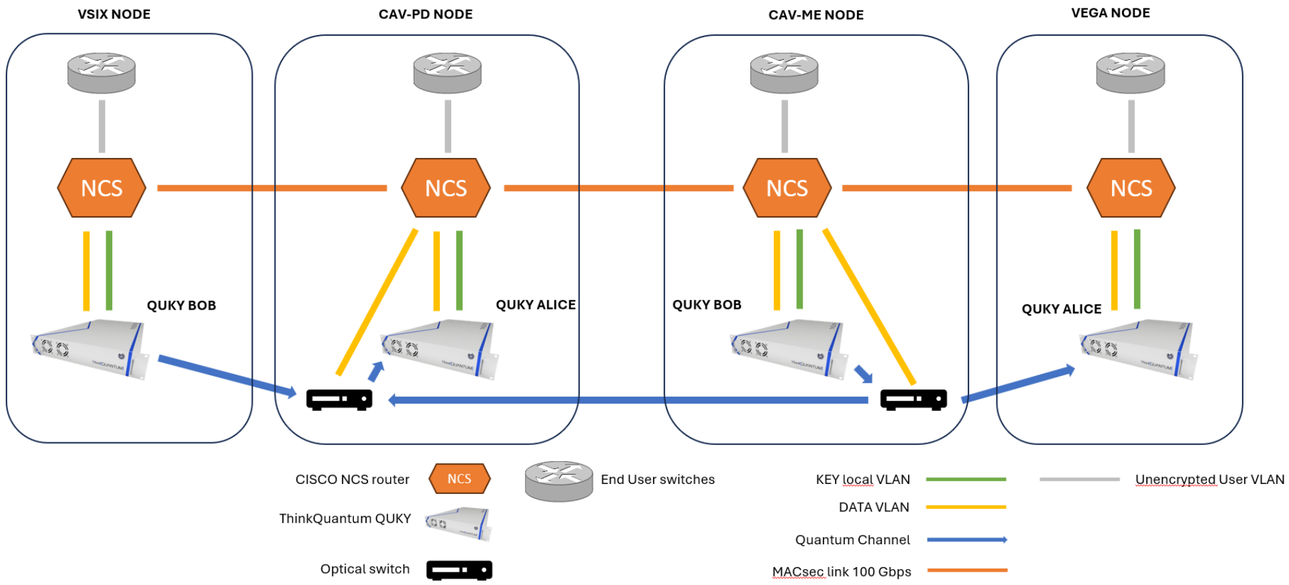
Supportano una configurazione statica della rete, a breve disponibile gestione dinamica tramite sistemi Software Defined Network e multi-dominio



L’innovazione della tecnologia QKD al centro di VenQCI: KMS & encryptors

I sistemi di **KEY Management**, **installati** sui sistemi **QKD**, gestiscono **autonomamente ed automaticamente** la complessità **della gestione e distribuzione delle chiavi anche su reti mesh complesse**

Supportano una configurazione statica della rete, a breve disponibile gestione dinamica tramite sistemi Software Defined Network e multi-dominio

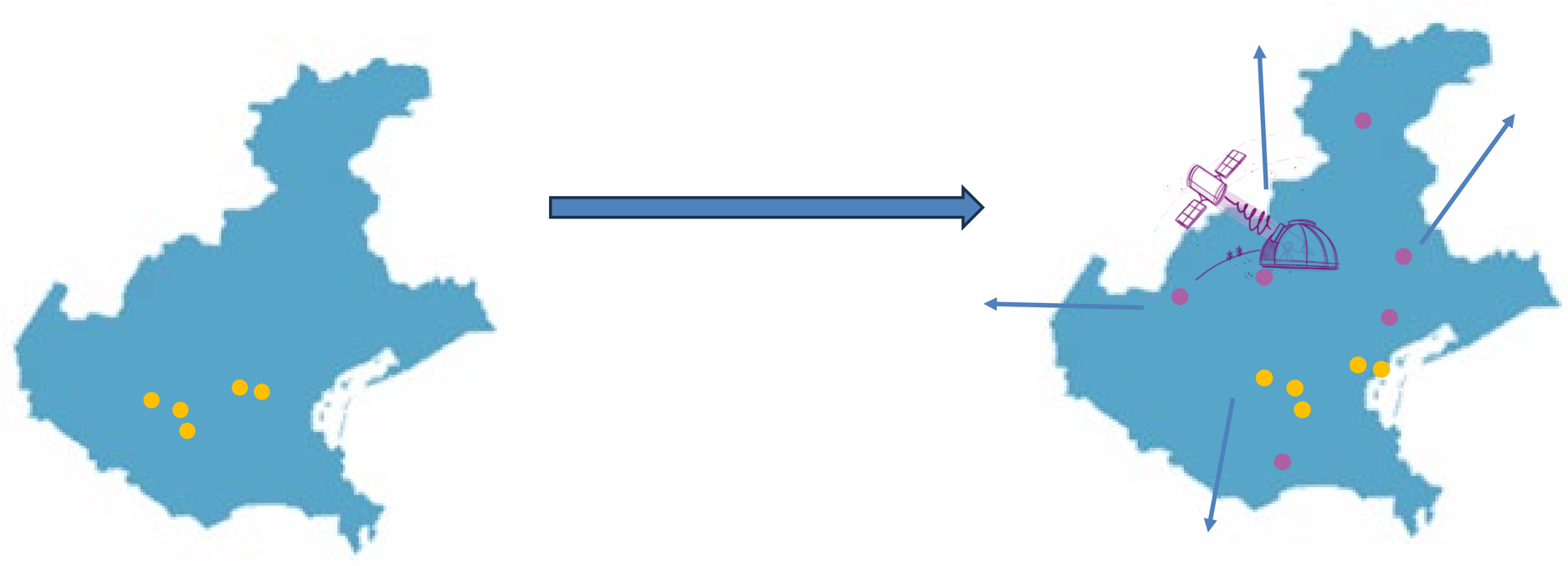


Il key manager permette di fornire chiavi per cifratura a qualsiasi layer, da layer 1 in su

Compatibile con standard ETSI (014, 04) e proprietari (CISCO SKIP) e con la maggior parte di encryptor hardware

La richiesta delle chiavi avviene tramite semplice REST API. Supporto per l’integrazione

Verso il futuro della rete



L’utilizzo di queste **tecnologie ed il design** della rete **VenQCI** la rende **facilmente espandibile** con **nuovi nodi e utenti**. Già avviato il processo di espansione.

La **rete guarda già al futuro**, con la possibilità di **collegamenti in spazio libero** dove la fibra non è presente e **satellitari** per una **connettività globale**

Non solo fibra ottica

Free-space channel

Single mode fiber

QUKY-TX

Single mode fiber

QUKY-RX

Node A
(trusted)

QKD TX

Fiber

FREE SPACE OPTICS

Free Space Quantum Link

Remote Site
(unstrusted)

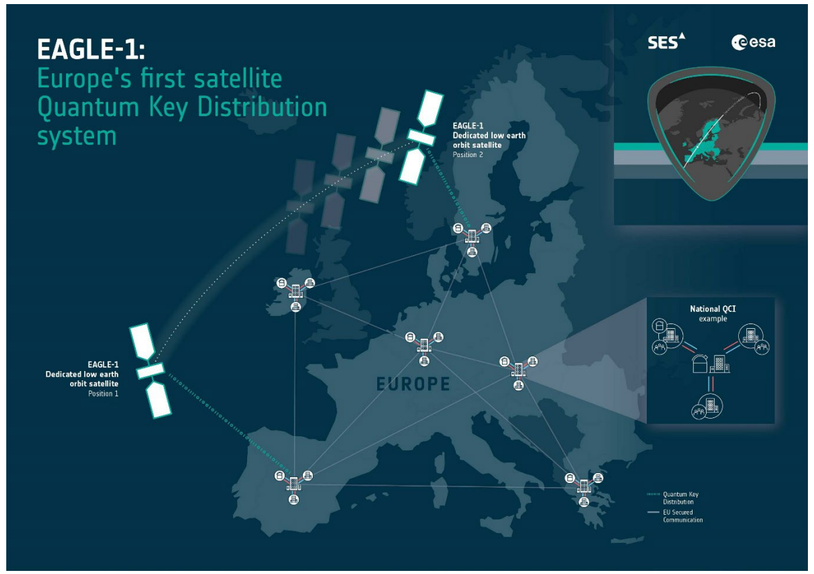
FREE SPACE OPTICS

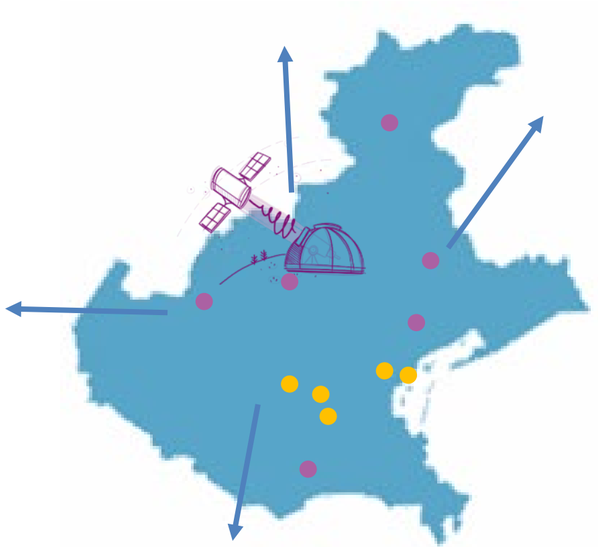
Fiber Quantum Link

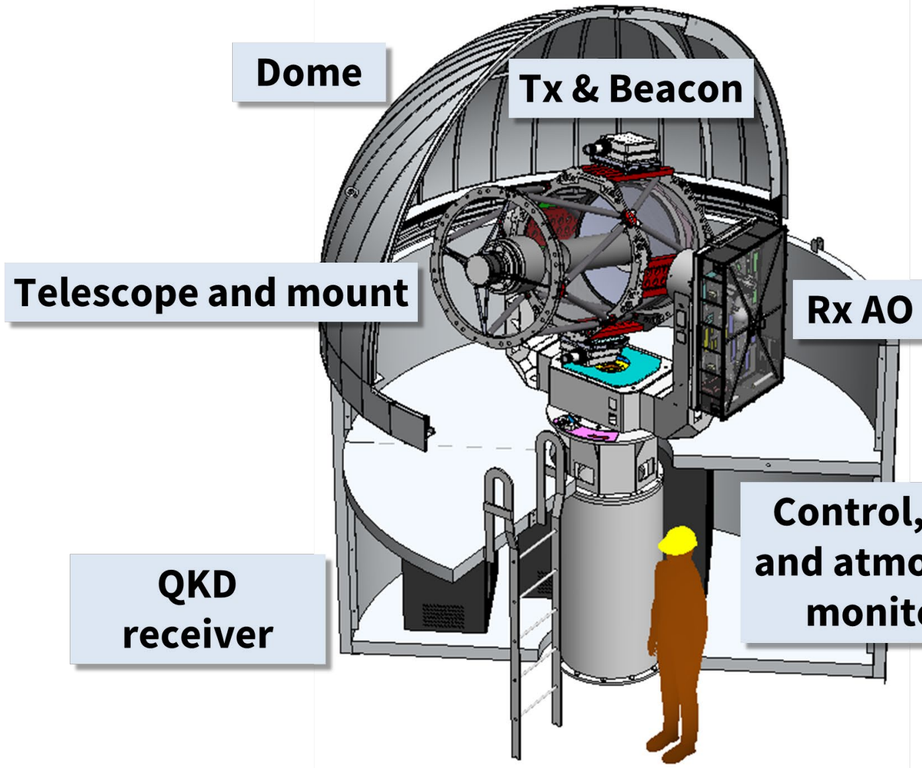
Node B
(trusted)

QKD RX

Collegamenti satellitari ottici: classici e quantum





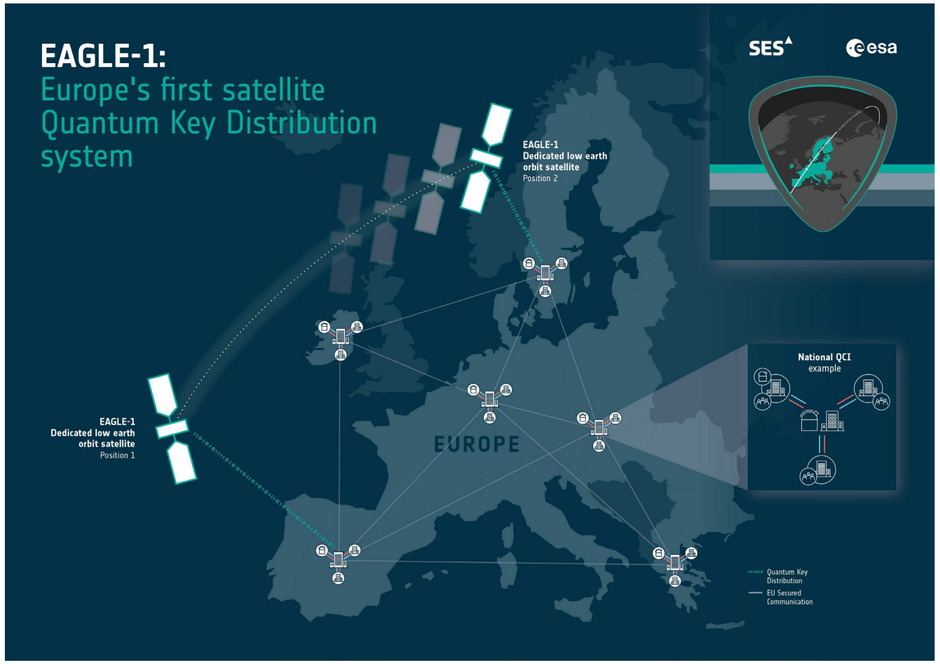


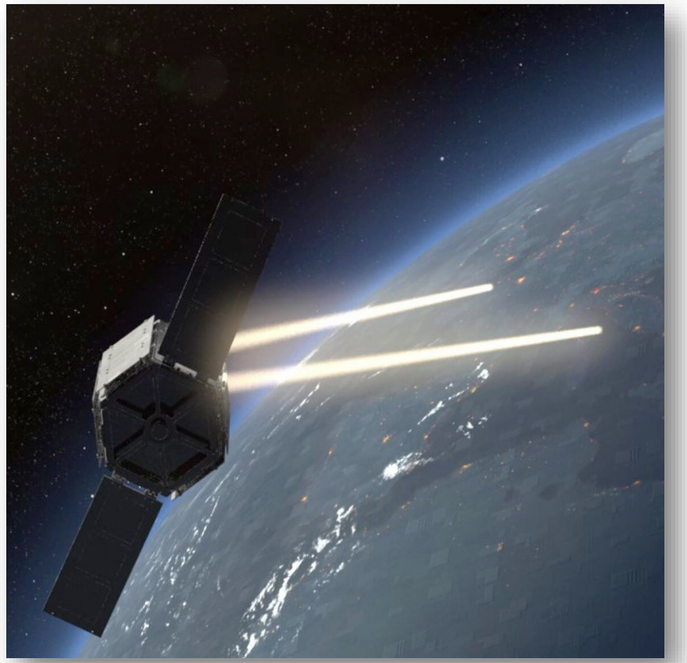
L'Europa ha diversi **programmi** per **connettere reti quantistiche europee tramite un network satellitare**

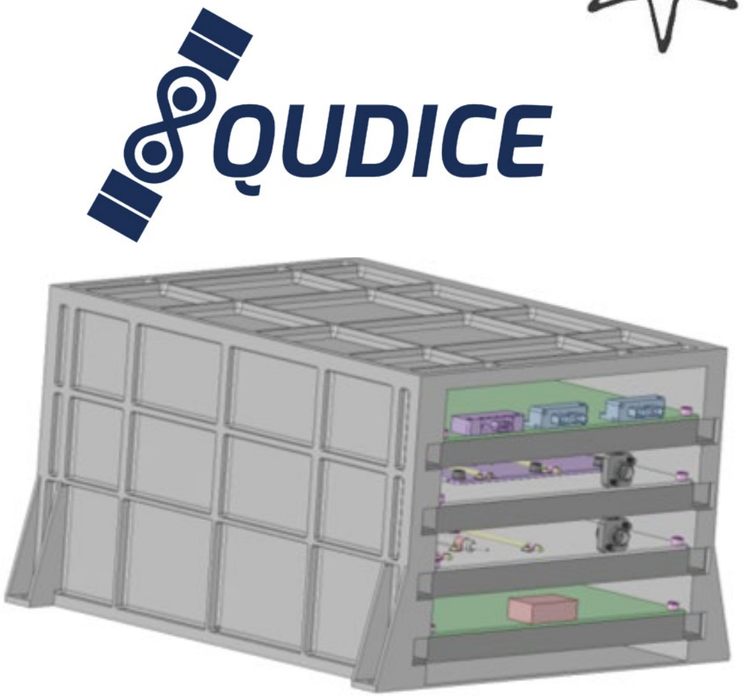
ThinkQuantum e OS stanno sviluppando **terminali a terra e nello spazio** per realizzare questa rete. I sistemi e la tecnologia sono **compatibili ed integrabili in VenQCI**

Collegamenti satellitari ottici: classici e quantum

Sorgenti spaziali







Eagle-1, primo satellite europeo dimostratore per la QKD

OS sta sviluppando l'Optical Ground Station per Eagle-1

OS e TQ fanno entrambi parte di un consorzio per una costellazione di satelliti QKD europei

OS coinvolto nello sviluppo dell'OGS

TQ coinvolta nello sviluppo del payload quantistico

TQ fa parte di QUDICE

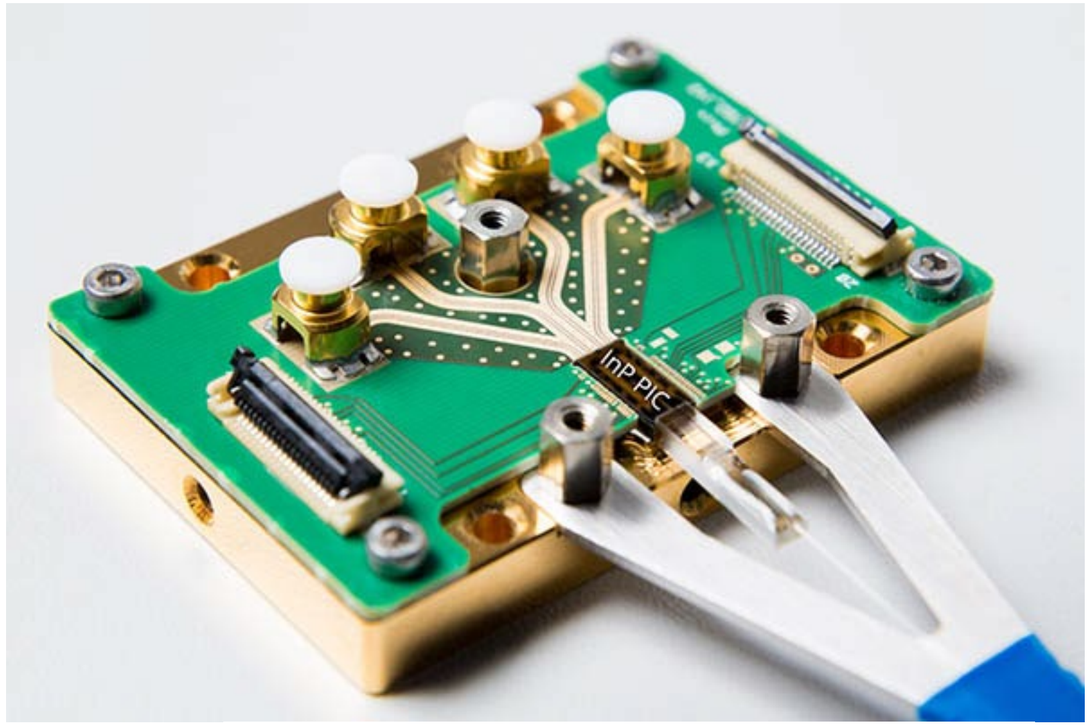
TQ Coinvolto nello sviluppo di una sorgente BB84 per cubesat

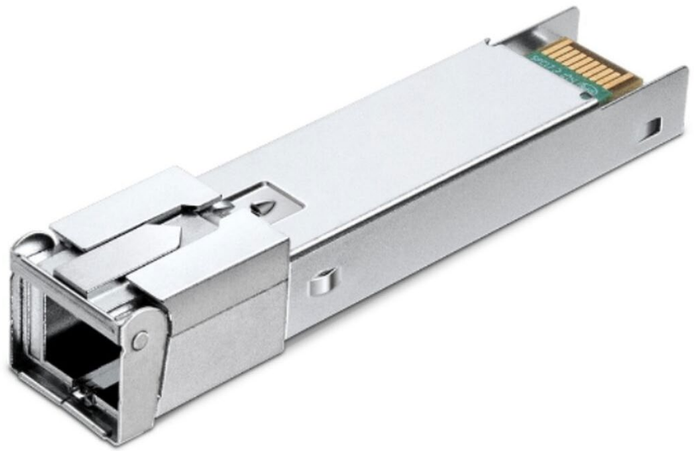
Sorgente ad alta velocità basata sull'encoder Ipognac brevettato da TQ

Circuiti fotonici integrati e sistemi pluggabili

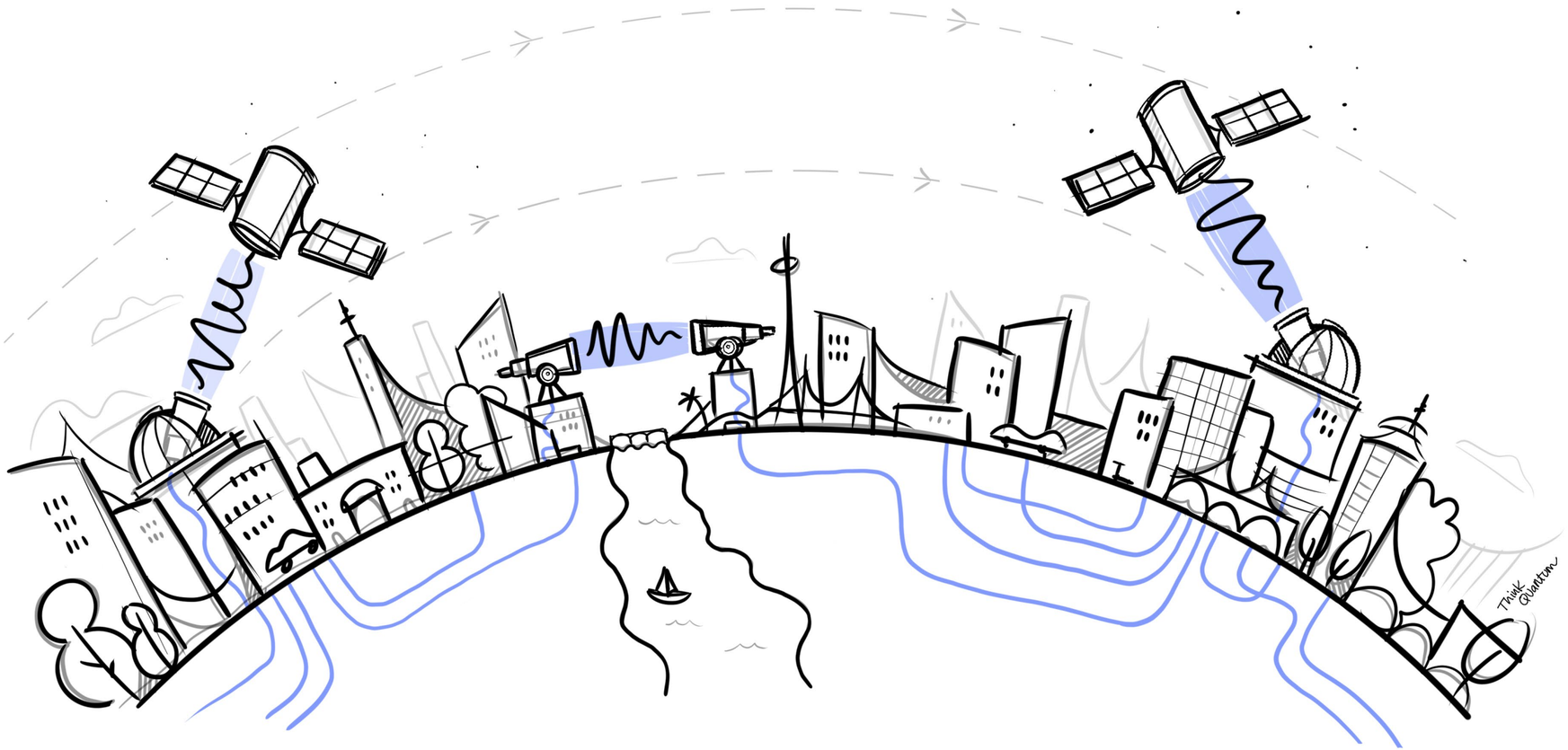
Sviluppo di circuiti integrati fotonici per QKD

- Fondamentale per la produzione di massa e la scalabilità della produzione
- Riduzione costi
- Massiccia riduzione delle dimensioni e del consumo energetico





Grazie per l'attenzione



marco.avesani@thinkquantum.com

venqci@vsix.it