Mi az a „kvantumapokalipszis?” – Lépések a kvantum kommmunikáció felé: QCIHungary project

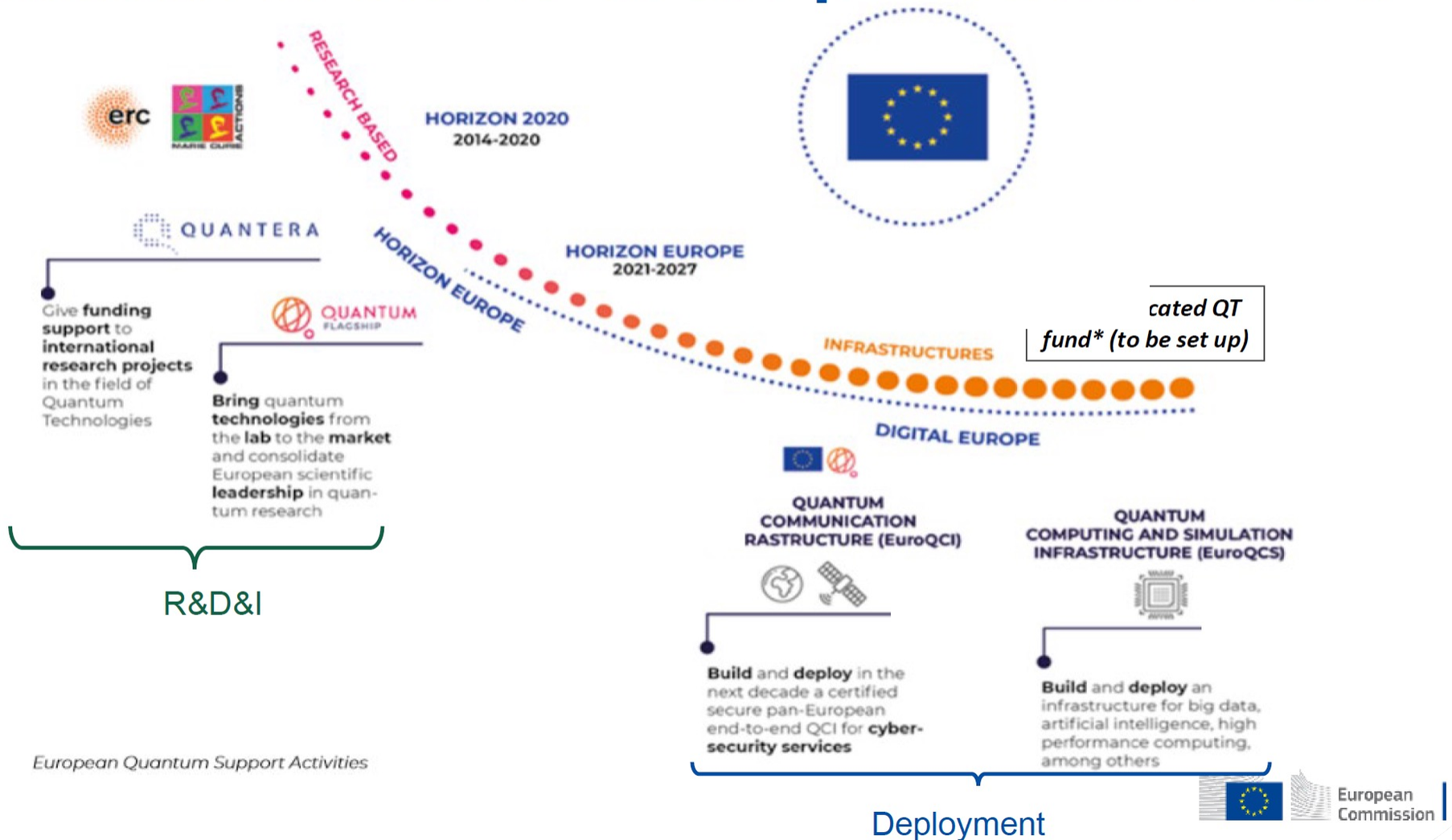
János Mohácsi, Nemzetközi K+F vezető, T&I szolgáltatás felelős

KIFÜ

23 March 2023

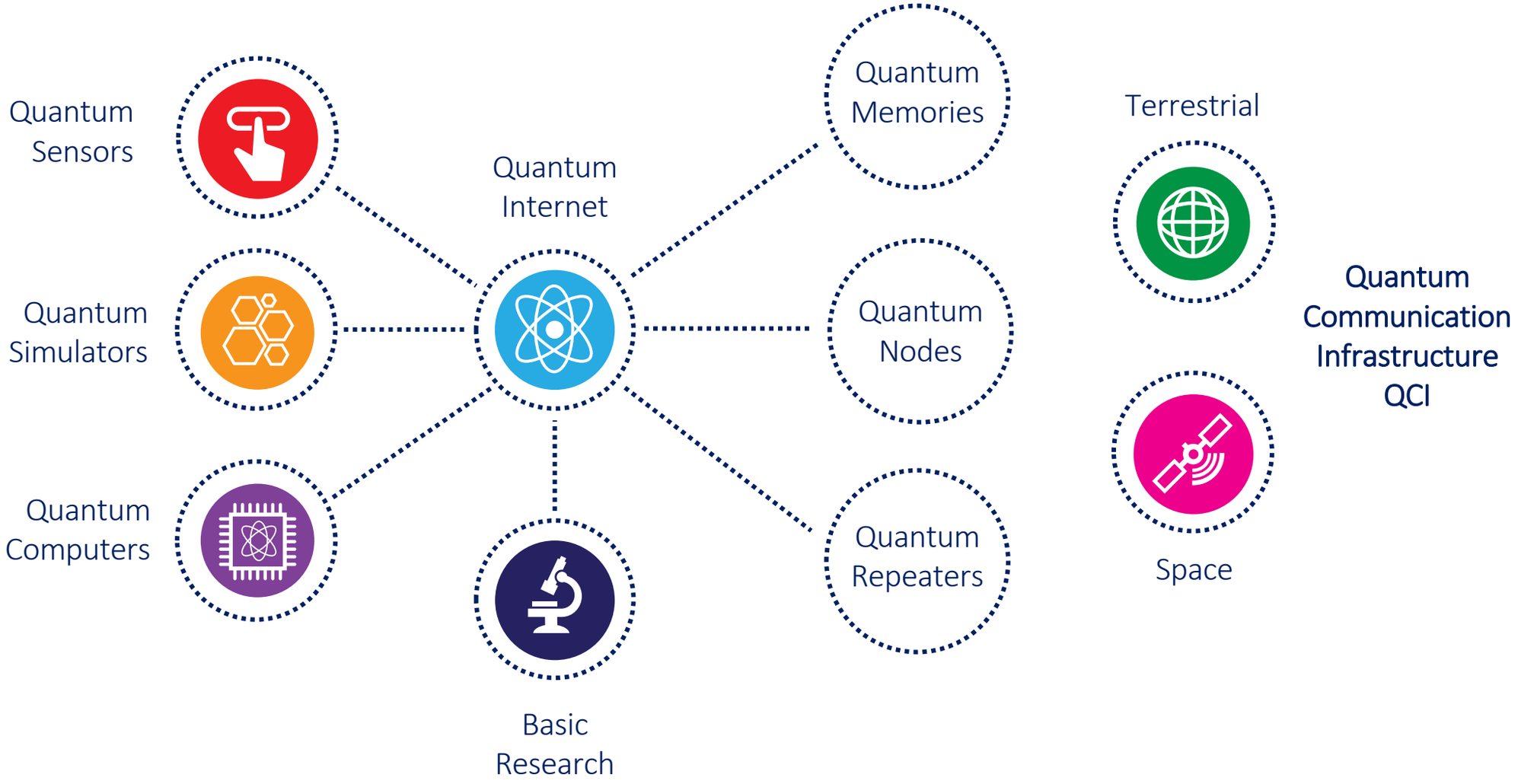
Kvantum az EU-ban: ökoszisztémák létrehozása

Quantum in the EU in the period 2021-2027

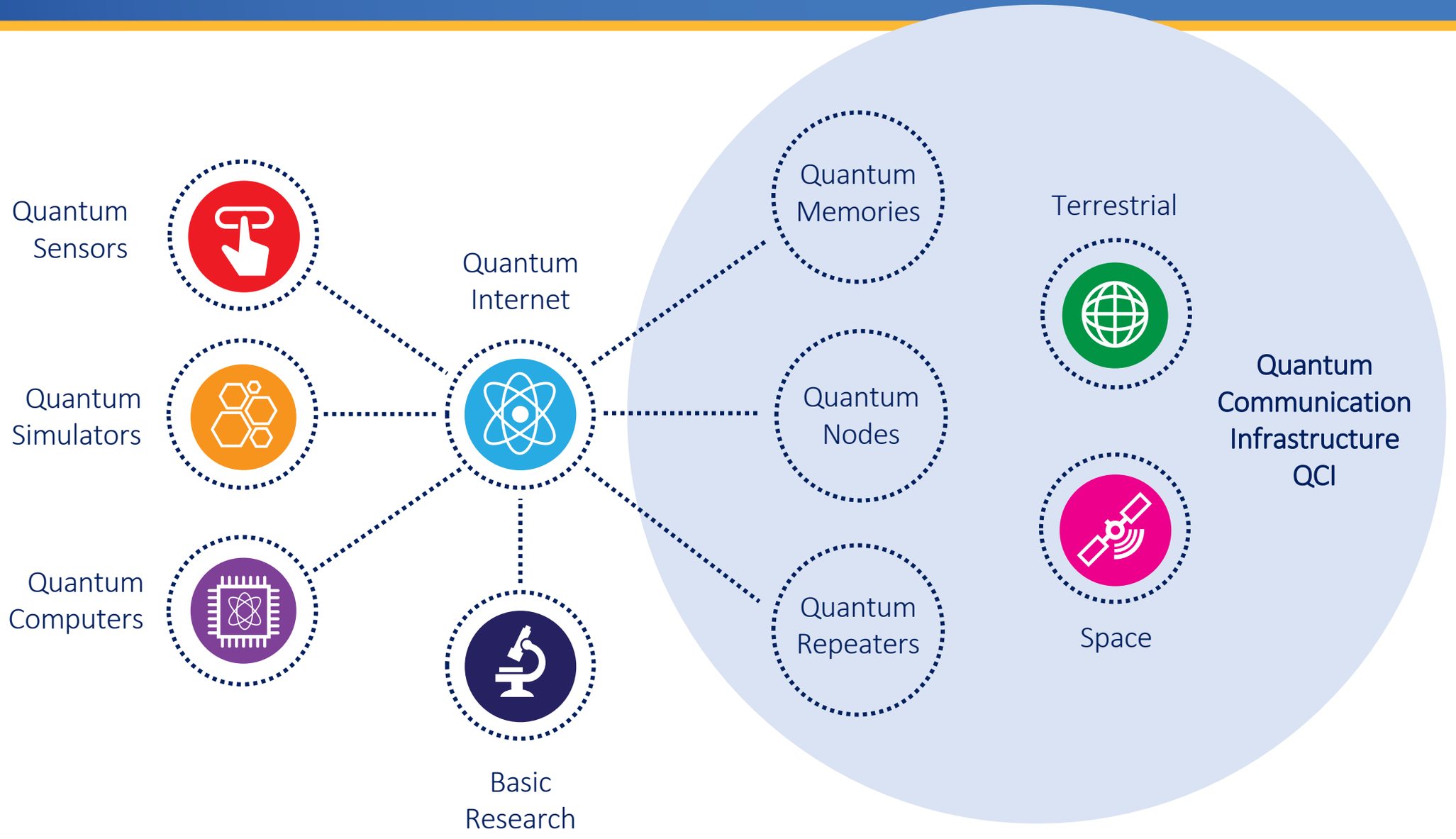


European Quantum Support Activities

Kvantum zászlóshajó kezdeményezés: Mi micsoda? /1



Kvantum zászlóshajó kezdeményezés: Mi micsoda? /1

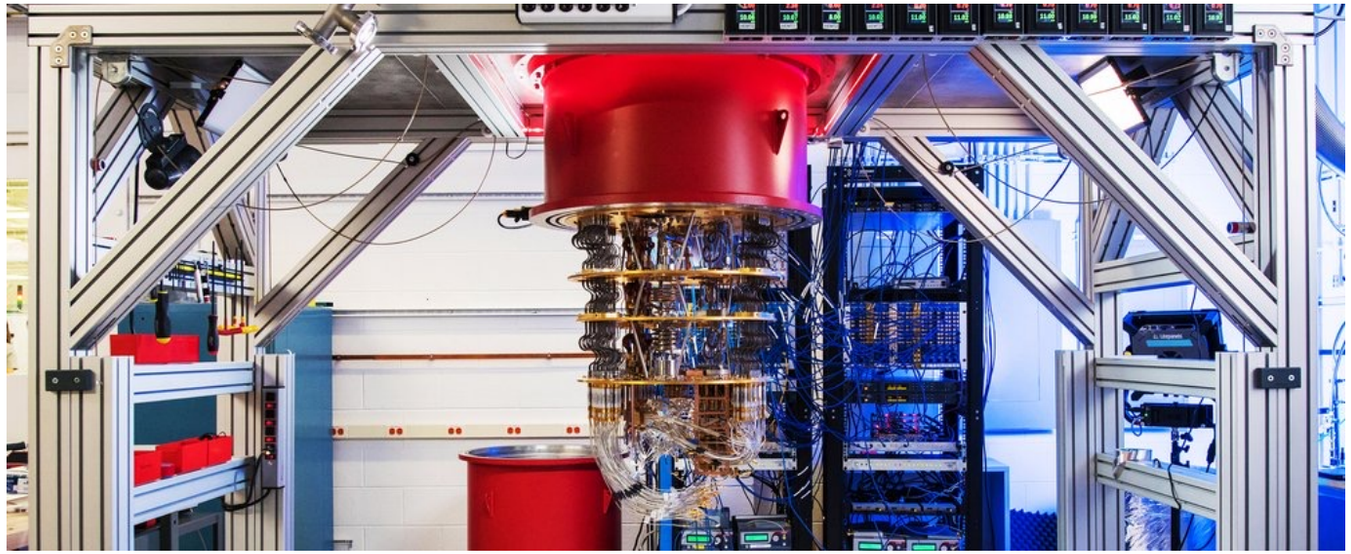


QKD (Quantum Key Distribution) - Mi micsoda? /2

- A QKD a fotonokat használó kulcselosztási sémák gyűjtő neve, NEM a kvantumkulcsok elosztása.
- A Post-Quantum Cryptography (PQC) nem a Quantum Cryptography vagy a QKD utódja. Csak azt mondja el, hogy a titkosítási algoritmusokat a kvantumszámítógépek lehetőségeinek figyelembevételével dolgozták ki.
- A Quantum Secure nem azt jelenti, hogy a kvantumok (QKD) védik a hálózatot. Ez azt jelenti, hogy a hálózat biztonságos a Quantum Computer egyes algoritmusaival történő támadásokkal szemben
- A QKD használatához 0 db kvantum számítógép szükséges. A kulcsokat kvantummechanikai hatások generálják szobahőmérsékleten, nincsen szükség kvantum algoritmusokra.
- Következtetés: A QKD a kvantum probléma kis szeletével és lehetőségeivel foglalkozik.

Kvantum?

- “Kvantum” több (hálózattal kapcsolatos) területre vonatkozik
  - Idő- és fekkvenci elosztás (T&F – Clonets)
  - Kvantumkulcs-elosztás (QKD / QCI)
  - Kvantum Internet
- Kvantum számítógép - Minden számítás három eleme: adatok, műveletek, eredmények
  - Adat = qubit
  - Művelet = kvantumkapu
  - Eredmények = mérések

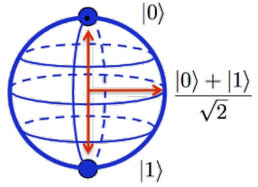


Qubit

- A qubit (vagy kvantumbit) a klasszikus bit kvantummechanikai analógja.
- Egy klasszikus bit értéke nulla vagy egyes lehet.
- A kvantum számítástechnikában az információ qubitben van kódolva.
- Egy qubit lehet $|0\rangle$, $|1\rangle$ állapotban vagy (a klasszikus bittel ellentétben) mindkét állapot lineáris kombinációjában. Ennek a jelenségnek a neve szuperpozíció.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

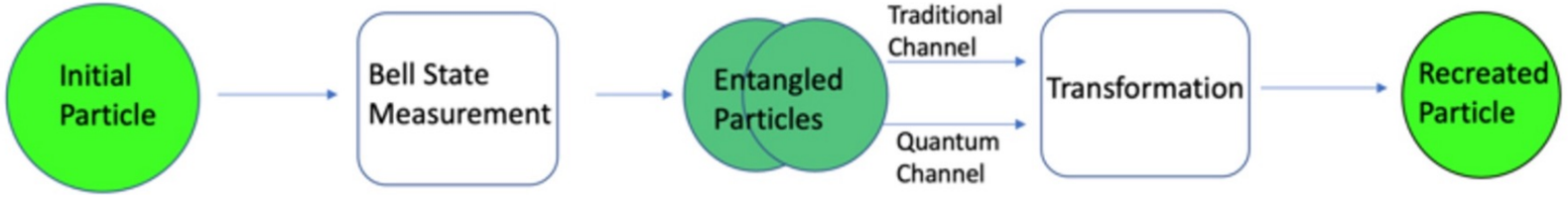
- De soha nem figyelhetjük meg α és β közvetlenül!



- Meg kell mérni $|\psi\rangle$ az érték meghatározásához $\Longrightarrow$ állapot véletlenszerűen omlik össze vagy $|0\rangle$ vagy $|1\rangle$
- Mekkora a valószínűsége a $|0\rangle$ vagy $|1\rangle$ megfigyelésének?
- A Qubit legkülönlegesebb tulajdonsága, hogy nem másolható és nem mérhető közvetlenül
- További információ: https://en.wikipedia.org/wiki/Qubit
- Kvantum összefonódás – információpár együtt tartja az értékét

Kvantum összefonódás és teleportáció

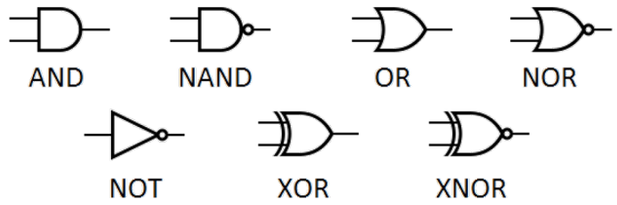
- A kvantumteleportáció egy olyan technika, amellyel kvantuminformációt (állapotot) továbbítanak az egyik helyen lévő feladótól a távolabbi vevőhöz.
- Míg a sci-fi a teleportációt általában fizikai objektumok egyik helyről a másikra való átvitelének eszközeként ábrázolja, a kvantumteleportáció csak kvantuminformációkat továbbít.
- Az Alice által birtokolt qubit lehet 0 és 1 is. Ha Alice a standard alapon mérné a qubitjét, az eredmény teljesen véletlenszerű lenne ha megfelelő kvantum forrást használ.
- De ha Bob megmérné a qubitjét, az eredmény ugyanaz lenne, mint amit Alice kapott. Tehát, ha Bob mér, első látásra véletlenszerű eredményt is kapna, de ha Alice és Bob kommunikálnának, rájönnének, hogy bár eredményeik véletlenszerűnek tűntek, tökéletesen korrelálnak egymással.



https://en.wikipedia.org/wiki/Bell_state

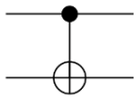
Kvantum számítógép – kvantum kapuk

A klasszikus biteket logikai kapuk segítségével alakítjuk át

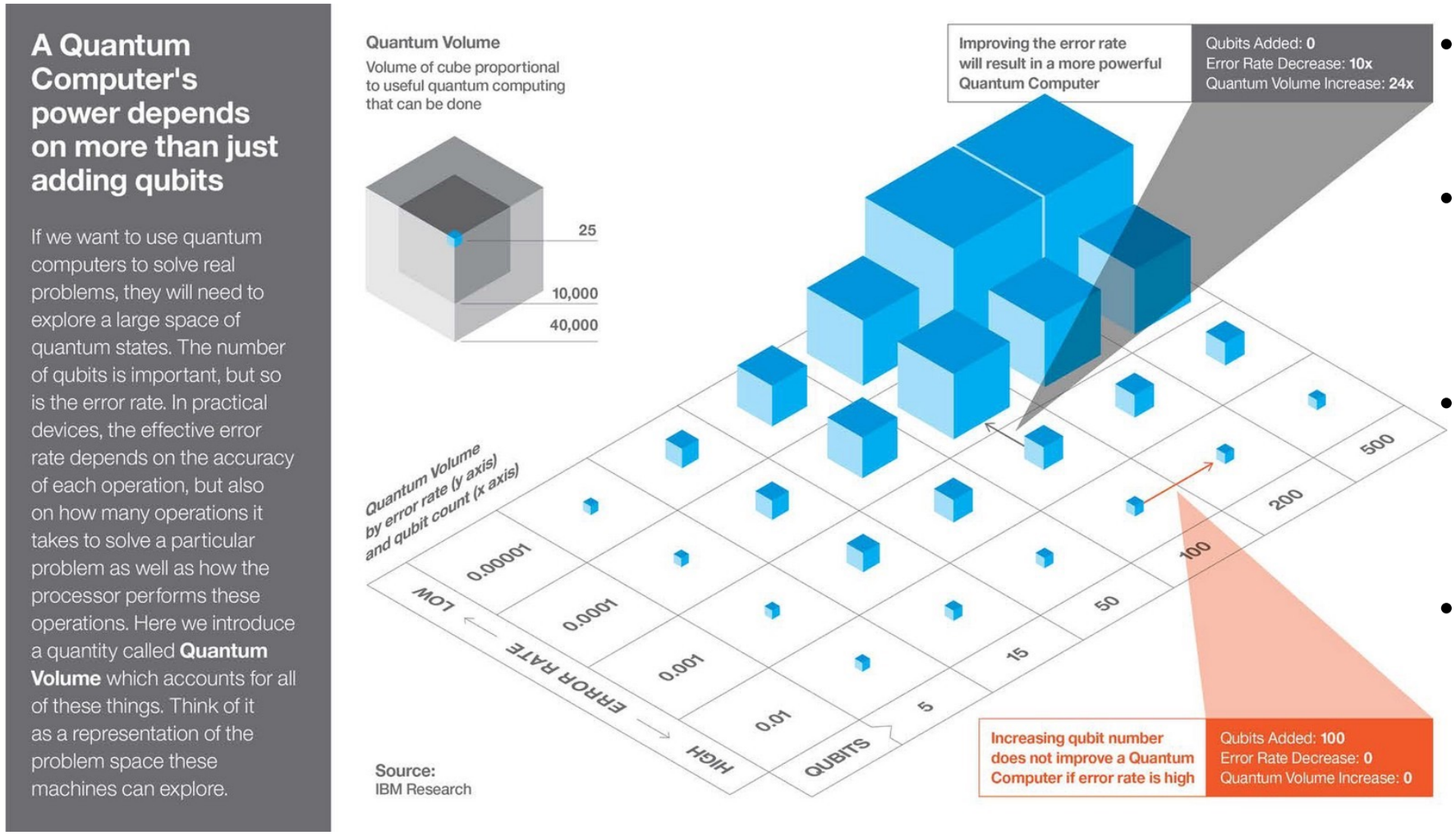


A qubiteket kvantumkapuk segítségével alakítják át

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \;\mapsto\; |\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$$

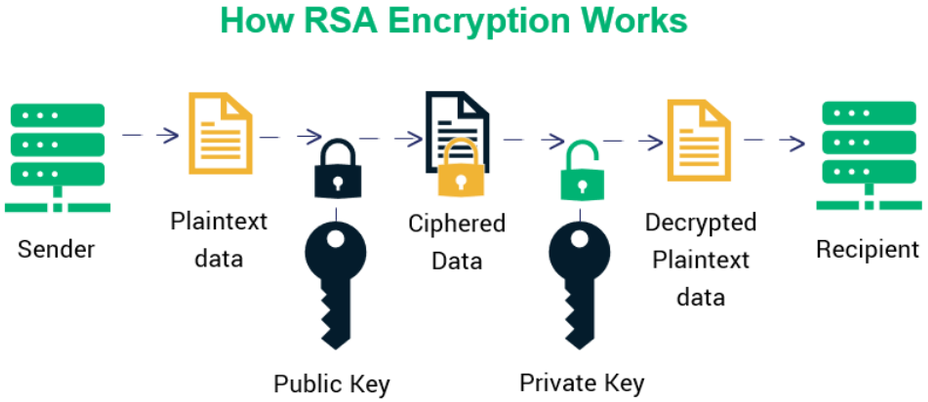
Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Kvantum számítógép ereje



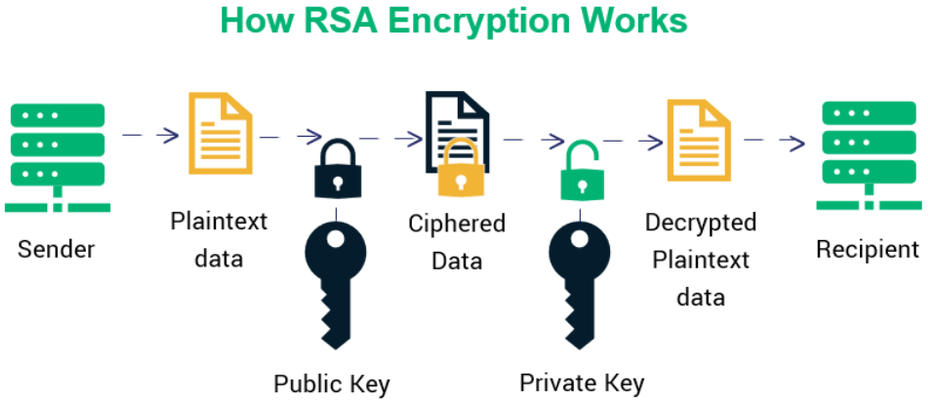
- A klasszikus kapuk (ha működnek) pontos eredményt adnak
- a kvantumkapuk olyan állapotok szuperpozícióit adják, amelyeket valószínűségekkel jellemeznek –> több mérés szükséges
- A felhalmozott mérések mérséklése érdekében „hibajavító kódokat” kell bevezetni
- Ez azt jelenti, hogy van „rezsiköltség”, azaz N működő qubit létrehozásához sokkal több fizikai qubitre lehet szükség --- ez a rezsi a rendszertől függ, de 10-1000-szeres is lehet

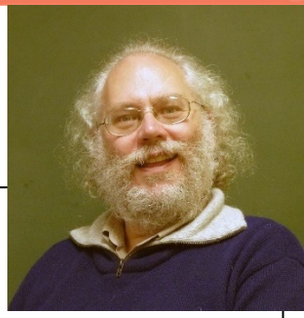
Shor algoritmus – kvantum apokalipszis?



Publikus kulcsos titkosítások:
RSA, elliptikus görbe, DL

Shor algoritmus – kvantum apokalipszis?





1994

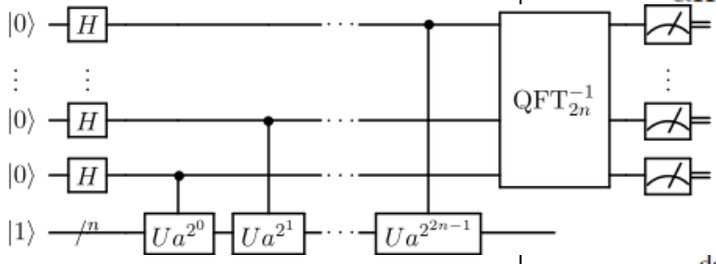
Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms



Publikus kulcsos titkosítások:
RSA, elliptikus görbe, DL

A Shor-algoritmus egy polinomiális idejű kvantumszámítógépes algoritmus egész számok faktorizálására, és diszkrét logaritmus megoldására
Ha egy elegendő számú qubittel rendelkező kvantumszámítógép működni tudna ... , akkor Shor algoritmusa használható lenne a nyilvános kulcsú kriptográfiai sémák feltörésére....

Kvantum előnyök és kihívások

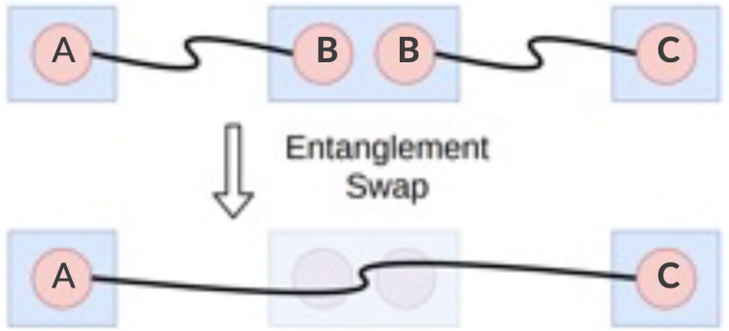
	Leírás
Előnyök és alkalmazhatóságuk	• **Nincs klónozás**: a qubitek nem másolhatók, így tökéletesek a titkosításhoz • **Szuperpozíció összeomlik**: ha egy qubitet mérünk, a szuperpozíció összeomlik így a lehallgatás nem maradhat felfedezése nélkül. • **Fizika a matematika helyett**: A kvantumbiztonság a fizikai jelenségre támaszkodik a matematika helyett – feltörés sokkal nehezebb (lehetetlen). • **Kvantum összefonódás**: együtt változik és semmisül meg a kvantum információ
Kihívások	• **Dekoherencia:** A qubit koherenciája az, hogy képes fenntartani a szuperpozíciót az idő múlásával. A környezet, a külvilággal való interakciók a rendszer dekoherenciáját okozzák. • **Qubit minőség (hűség)**: a mai kvantumszámítógépek qubitjei nem elég jók nagyméretű rendszerek számára. Bizonyos esetekben a kapott eredmény megkülönböztethetetlen lehet a zajtól. • **Skálázhatóság**: Új megoldások szükségesek qubitek létrehozásához, újításokra van szükség az átvitel technikában vagy lézerek vezérlésének jelenlegi módjaiban.

Mi az a Kvantum Hálózat ?

- A kvantumhálózatok lehetővé teszik az információk qubitek formájában történő továbbítását a fizikailag elkülönített kvantum csomópontok (pl. kvantumszámítógépek) között.
  - Fizikai (távközlési) optikai vagy szabad téri rendszer. Jelenleg csak részben képes használni az xWDM-et a kvantumállapot (dekoherencia) elvesztése miatt.
- Az alapvető hálózati struktúra a klasszikus p2p hálózathoz hasonló, amely végpontokat köt össze, amikor a helyinél több qubit szükséges vagy ha tárolásra van szükség.
  - Jelenleg csak direkt sötétszál kapcsolat 2 végcsomópont között olyan, amelyek megőrzi a kvantumkoherenciát.
- A jelerősítés és az optikai átjátszók használata nem lehetséges, mivel a kvantumállapot elveszik, és a qubitek nem másolhatók. Ezért a közvetlenül összekapcsolt kvantumcsomópontok közötti távolság jelenleg körülbelül maximum120 km.
- A Quantum Repeater használata lehetővé teszi a nagyobb távolságok használatát, de elég komplex berendezés az összefonódás tovább küldője (entaglement swap) és a teleportálója.
- Réteges szerkezet - több modell – alkalmazástól függően (mint OSI modell):

Application	
Transport	Qubit transmission
Network	Long distance entanglement
Link	Robust entanglement generation
Physical	Attempt entanglement generation

Werher at al



Kvantum hálózat alkalmazása?

- Kvantum összefonódáson alapuló alkalmazások támogatása
- Általánosságban elmondható, hogy a kvantum összefonódás kiválóan alkalmas olyan feladatokhoz, amelyek koordinációt, szinkronizálást vagy nagy biztonságot igényelnek:
  - Óra szinkronizálása
  - Választás – konszenzus kereső algoritmusok (lásd csütörtök 12:00 D szekció)
  - Biztonságos hozzáférés az erőforrásokhoz (például banki alkalmazás)
  - Teleszkóp/mérőberendezés alapbeállítás vagy más Földrajzilag szétszórt, nagy pontosságú berendezések kalibrációja
  - Kommunikáció kvantumszámítógépek között
  - Memória megosztása kvantumszámítógépek között
  - Kvantum alapú kulcscsere/kulcselosztás - **Quantum Key Distribution**
- További alkalmazása a Kvantum jelenségeknek – eddig ismert legjobb véletlen szám generátor

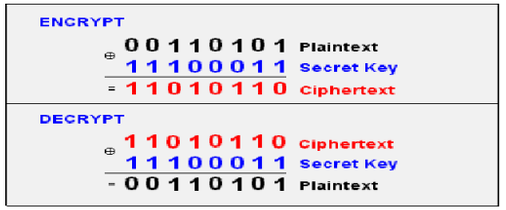
- **A hagyományos Internetre továbbra is szükség van az adatok és információk cseréjéhez**

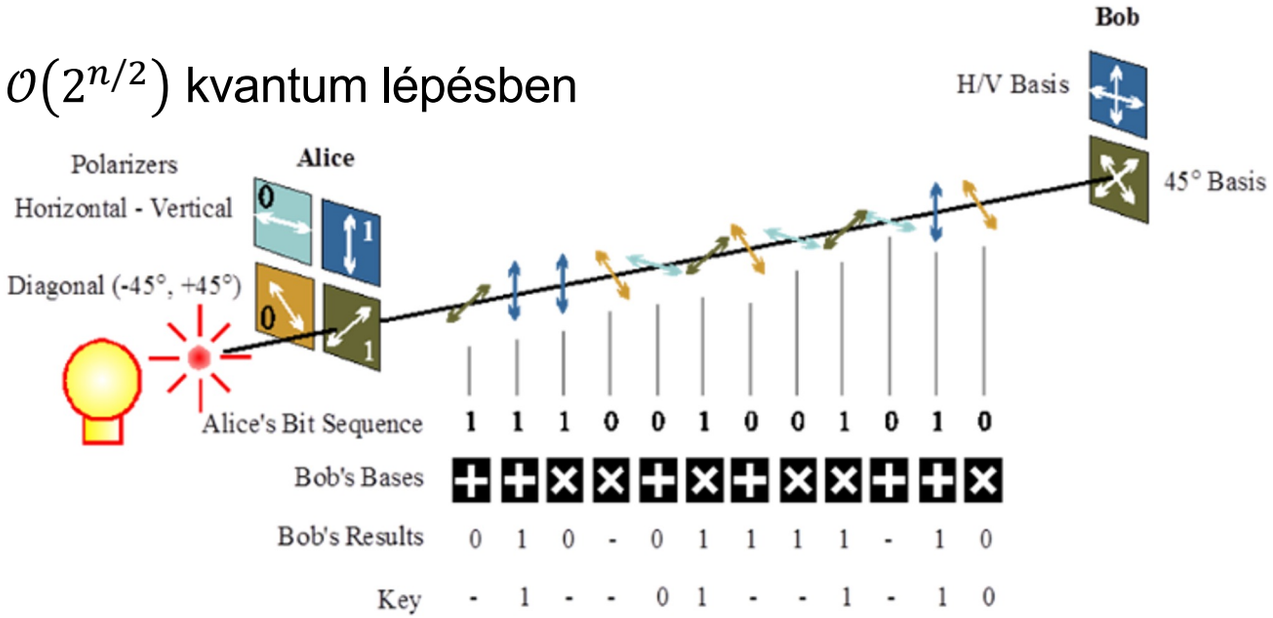
Hogy kezeljük a “kvantum apokalipszist”?

- Szimmetrikus kulcsú titkosítás
  - Grover's algorithmus: $\mathcal{O}(2^n)$ probléma megoldása $\mathcal{O}\left(2^{n/2}\right)$ kvantum lépésben
  - Javaslat: kulcs méret duplázás $(128 \rightarrow 256)$

Hogy kezeljük a “kvantum apokalipszist”?

- Szimmetrikus kulcsú titkosítás
  - Grover's algorithmus: $\mathcal{O}(2^n)$ probléma megoldása $\mathcal{O}(2^{n/2})$ kvantum lépésben
  - Javaslat: kulcs méret duplázás $(128 \rightarrow 256)$

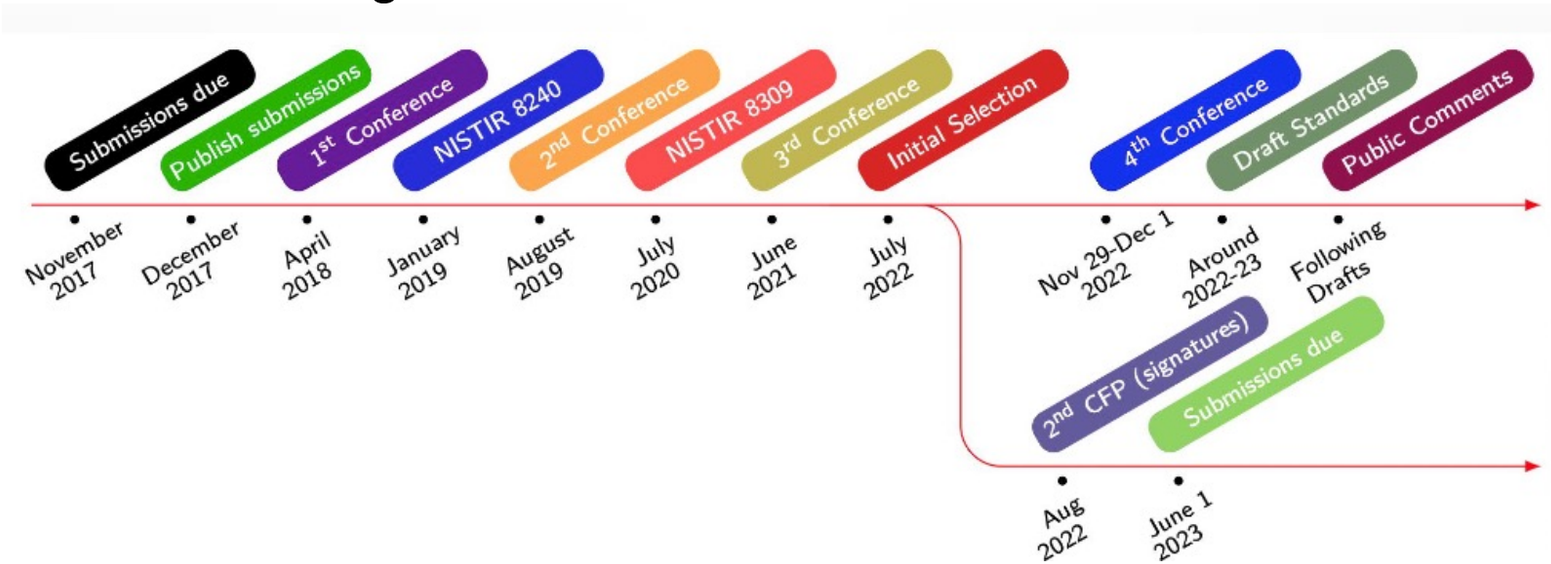




- Kvantum kriptográfia alkalmazása
  - Használjunk kvantum effektust a kriptográfiához - BB84 – one time pad
    - cv-qkd – több koherens fotonnal - polarizációt használva – nagy kulcs szükséges
    - dv-qkd – erősen csillapított keskeny sávú lézer, amely adott eloszlású fotonokat küld statisztikai módon.
    - entangled qkd - összefonódott foton pár – valódi quantum repeater szükséges
- Posztkvantum kriptográfia
  - A klasszikus algoritmusok amelyekről úgy gondolják, hogy ellenállnak a kvantumtámadásoknak

Post-quantum cryptography (PQC)

- Nyilvános kulcsú kriptográfia, amely a faktoráláson és a diszkrét logaritmuson kívül más problémákon alapul – amelyek jelenlegi tudásunk szerint kvantum számítógépen is nehéz megoldani
- Nyilvános kulcsú titkosítási és Digitális aláírási algoritmusok
- **Jelöltek:**
  - Lattice-based cryptography
  - Code-based cryptography
  - Multivariate cryptography
  - Hash-based cryptography
  - Isogeny-based cryptography
- 2017-ben kezdődött
  - 1. forduló: 69 pályamű
  - 2. forduló: 26 jelöltet választottak ki
  - 3. forduló: 15 jelöltet választottak ki
    - Kiválasztottak
      - KEM: CRYSTALS-Kyber
      - Signature: CRYSTALS-Dilithium, Falcon, SPHINCS+
  - 4. forduló: 4 jelöltet választottak ki (2022)
    - Kiválasztottak (2022.11)
      - KEM: Classic McEliece, BIKE, HQC
      - Signature: új javaslatokat várnak 2023 június 1-ig
- A nyertes(ek) szabványosítása körülbelül egy év múlva várhatóak



QCIHungary projekt javaslat

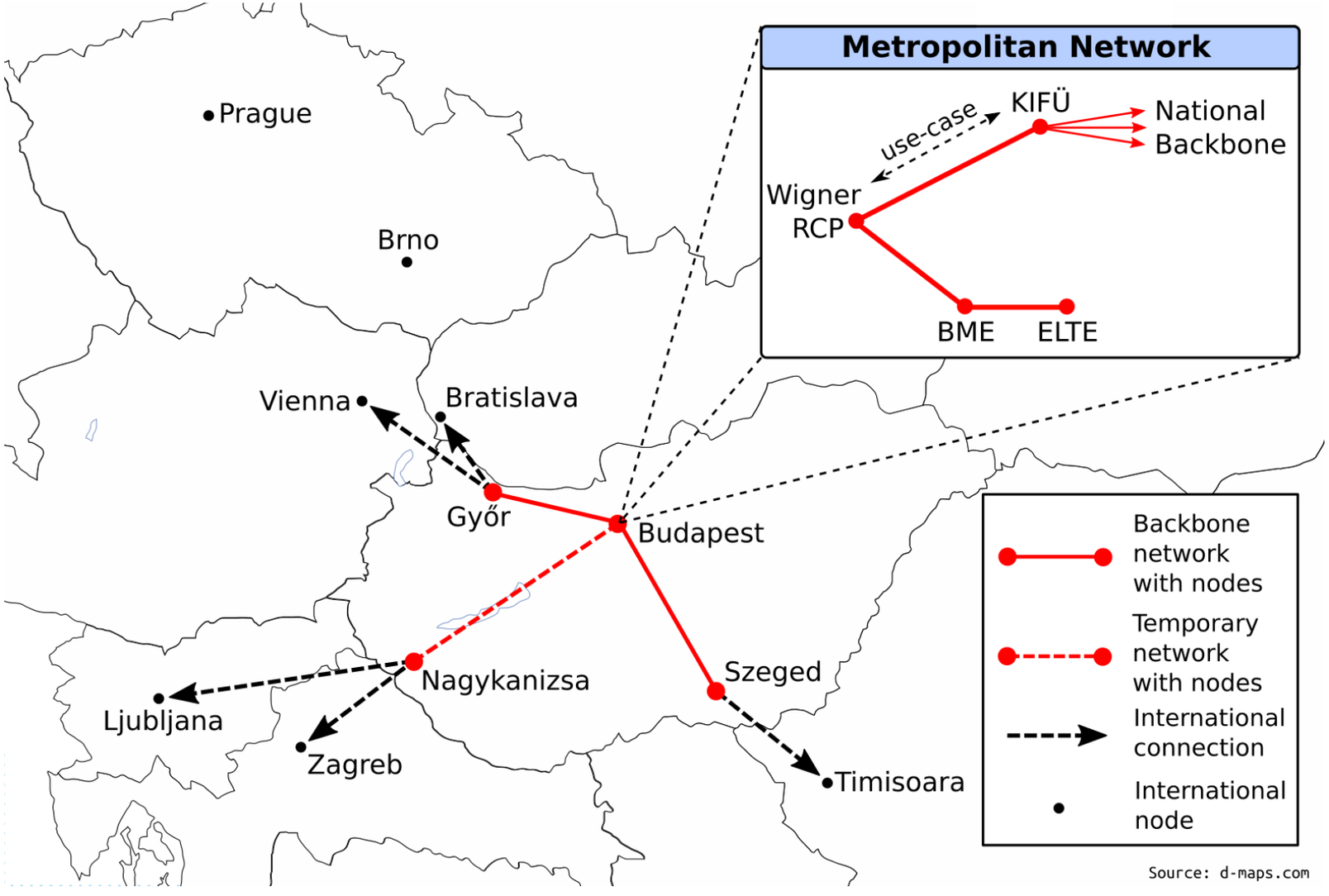
A QCI Hungary pályázat fő célja egy **leendő magyar QKD kommunikációs hálózat** alapelemeinek **kiépítése**. A részcélok közé tartozik a **hálózat tesztelése** egy valós **közhasználati** eseten keresztül, a **magyar QKD rendszerek működésének továbbfejlesztése**, szakértők és jövő nemzedékek **képzése és oktatása**, valamint **nemzetközi együttműködés** az EU kvantumkommunikációs ökoszisztémájában való sikeres részvétel érdekében. A pályázat részét képezik a későbbi, **műhold** által közvetített **kvantumkommunikáció** felé megtett lépések valamint a QKD-vel kapcsolatos szoftverek fejlesztése.

QCIHungary projekt javaslat– Általános információk

- **Projekt név:** QCIHungary
- **Partnerek:** KIFÜ – konzorciumvezető, koordinátor: Mohácsi János, tagok: Kvantuminformatikai Nemzeti Laboratórium tagjai: Wigner FK, BME HIT (Hálózati Rendszerek és Szolgáltatások Tanszék), ELTE Informatikai Kar. Társult partner(ek): Magyar Telekom Nyrt. (és Vodafone Zrt – újra csatlakozás folyamatban).
- **Projekt javaslat tervezett időtartama**: 2023.01-2025.07
- **Teljes tervezett költségvetés:** ~ 10 MEuro (50% hazai forrás) – EC döntés 2022 nyár

This work is part of a project that has received funding from the European Union's Digital Europe Programme under Grant Agreement No 101081247

Tervezett QCIHungary hálózat



QCI Hungary projekt javaslat tervezett felépítése

WP1 Project management, communication, and dissemination

Project administrative and financial management

Project technological coordination

Quality assurance

Communication and Dissemination

WP2

Establish national Quantum communication network using commercial off-the-shelf QKD devices and key management systems

WP3

Testing the operational aspects of a QKD link in a real use cases

WP4

Free-space and metropolitan telecom fiber-based QKD developments

WP5

International cooperation, preparation for the large-scale European QCI deployment

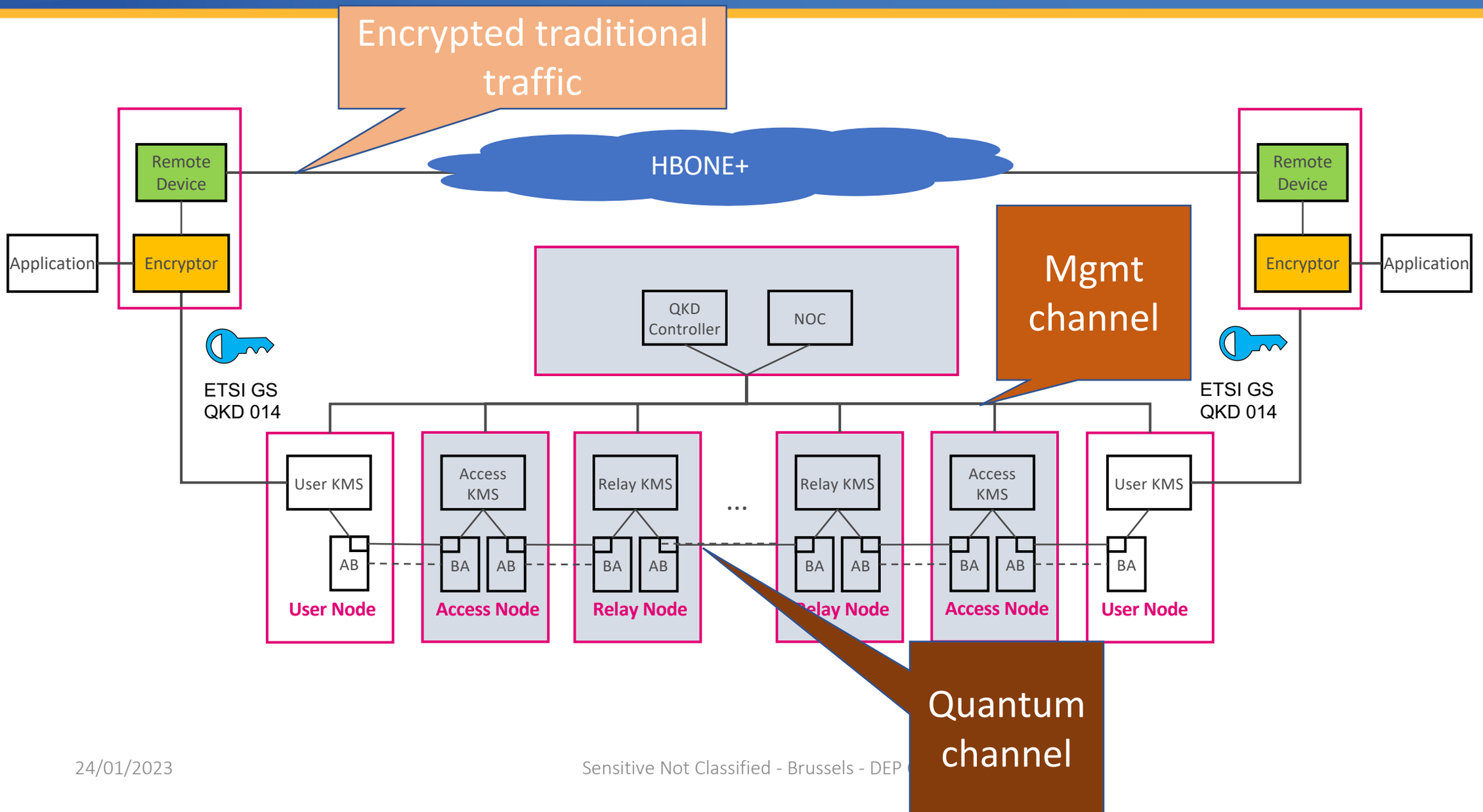
WP6

Quantum communication education and training

WP7

Software stack over a quantum communication channel

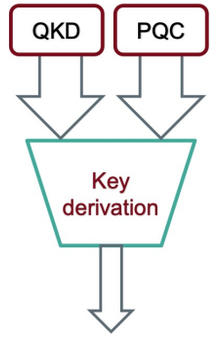
QCIHungary tervezett magas szintű architektúra



QKD összefoglalás és jövő

Diigital Sicher BSI (2021) „Quantum cryptography is a complement to post-quantum cryptography that should be researched and tested further, but it is not yet ready for widespread use.”

NSA (2022) álláspont



PQC és QKD egymást kiegészítő megoldások- Muckle(+) séma

QKD megoldandó feladatok

- 100-120 km-nél nagyobb távolság a QKD dobozok között?
- Kulcsok elosztása olyan helyeken, ahol nincsenek QKD dobozok a „kvantumbiztonság” megtartásával?
- VPN szerű működés ? – Távol/mobil felhasználók
- Többpontos QKD?
- Biztonságos kulcscsere a QKD dobozok és a felhasználók között?
- Szabványosság -minden szinten?

Kérdések?

Mohácsi János
mohacsi.janos@kifu.gov.hu