Rövid bevezetés a kvantuminformatikába

Kozlovszky Miklós
m.kozlovszky@sztaki.hu
SZTAKI LPDS

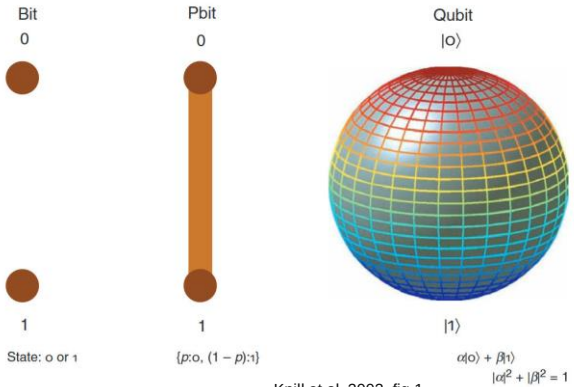
SZTAKI Wigner ELKH Eötvös Loránd Research Network

Bevezetés

- A kvantuminformatika napjainkban kezdi meghódítani a világot, ez a kvantum-érának is nevezhető időszak kezdete.
- A sok megválaszolatlan implementációs kérdés és korai stádiumban lévő fejlesztés további kutatásokat tesz szükségessé.
- Az alapismeretek és a technológia alapjait meghatározó kutatási eredmények már elérhetők.
- Ezek megismerése elengedhetetlen a kvantumtechnológia jövőbeli szakértőinek és felhasználóinak.
- A programozók akkor is tudnak a meglévő infrastruktúrán dolgozni, ha nem válnak előtte elméleti fizikussá!

Kvantuminformatika - kvantum számítástechnika

- A kvantuminformatika olyan problémák megoldását ígéri, amelyek a hagyományos számítógépekkel igen hosszú idő alatt lennének megoldhatók.
  - Ilyen problémák pl. a sok paraméteres szimulációk futtatása, széles körben használt kriptográfiai eljárások törése, stb.
- A kvantuminformatika egyszerre jelent fenyegetést a hagyományos kriptográfiát használó rendszereknek és ígér védelmet (egyfajta „lehallgathatatlanságot”) a felhasználók számára.
- A kvantumalapú számítástechnika lesz az első lépés a teljes kvantumrendszerek felé, és teljesen át fogja formálni a hagyományos hálózatok és titkosítási megoldások világát.

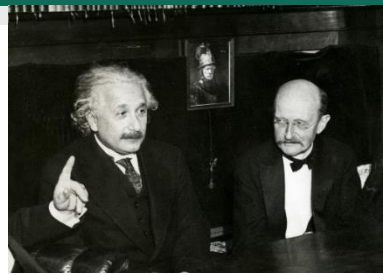


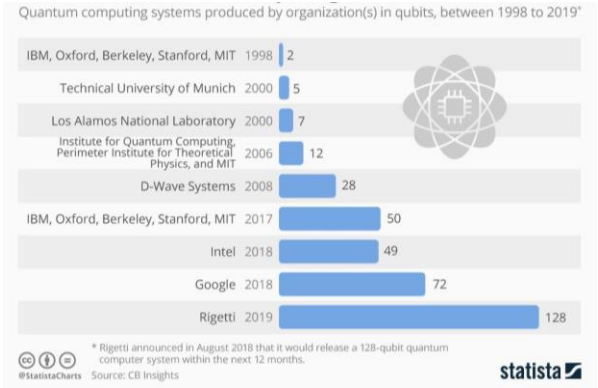
Knill et al. 2002, fig.1
https://devopedia.org/quantum-computing

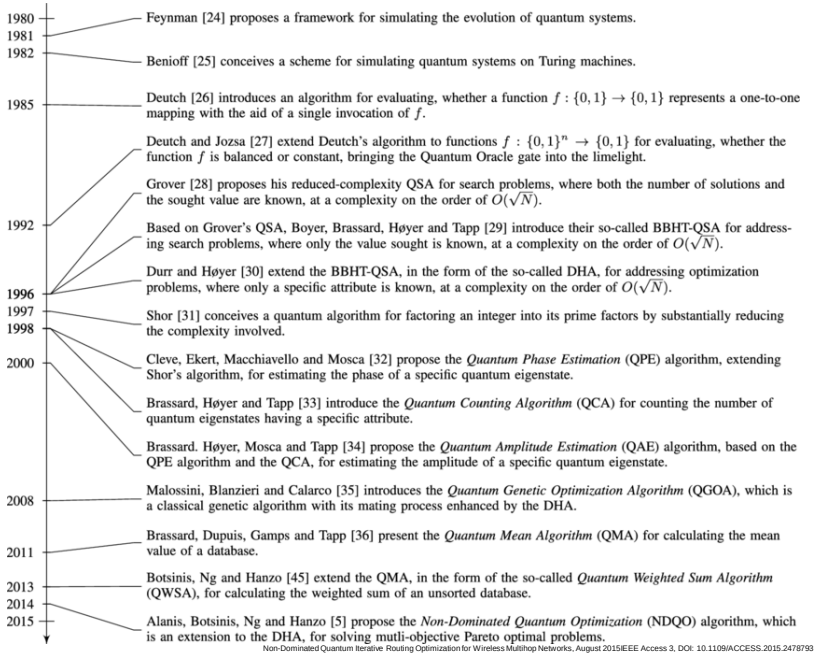
Egy csipetnyi történelem

ELKH Cloud | SZTAKI | Wigner | ELKH Eötvös Loránd Research Network

- Fizika
  - 1900 Max Planck - energia kvantálás
  - 1905 Einstein - fotoelektromos hatás, fény részecske, foton fogalma
  - 1924 Louis de Broglie - anyaghullám-elmélet
  - 1925 - A modern kvantummechanika születése
  - 1927 Heisenberg - határozatlansági relációja
- Számítástechnika – algoritmusok
- Számítástechnika - hardverek





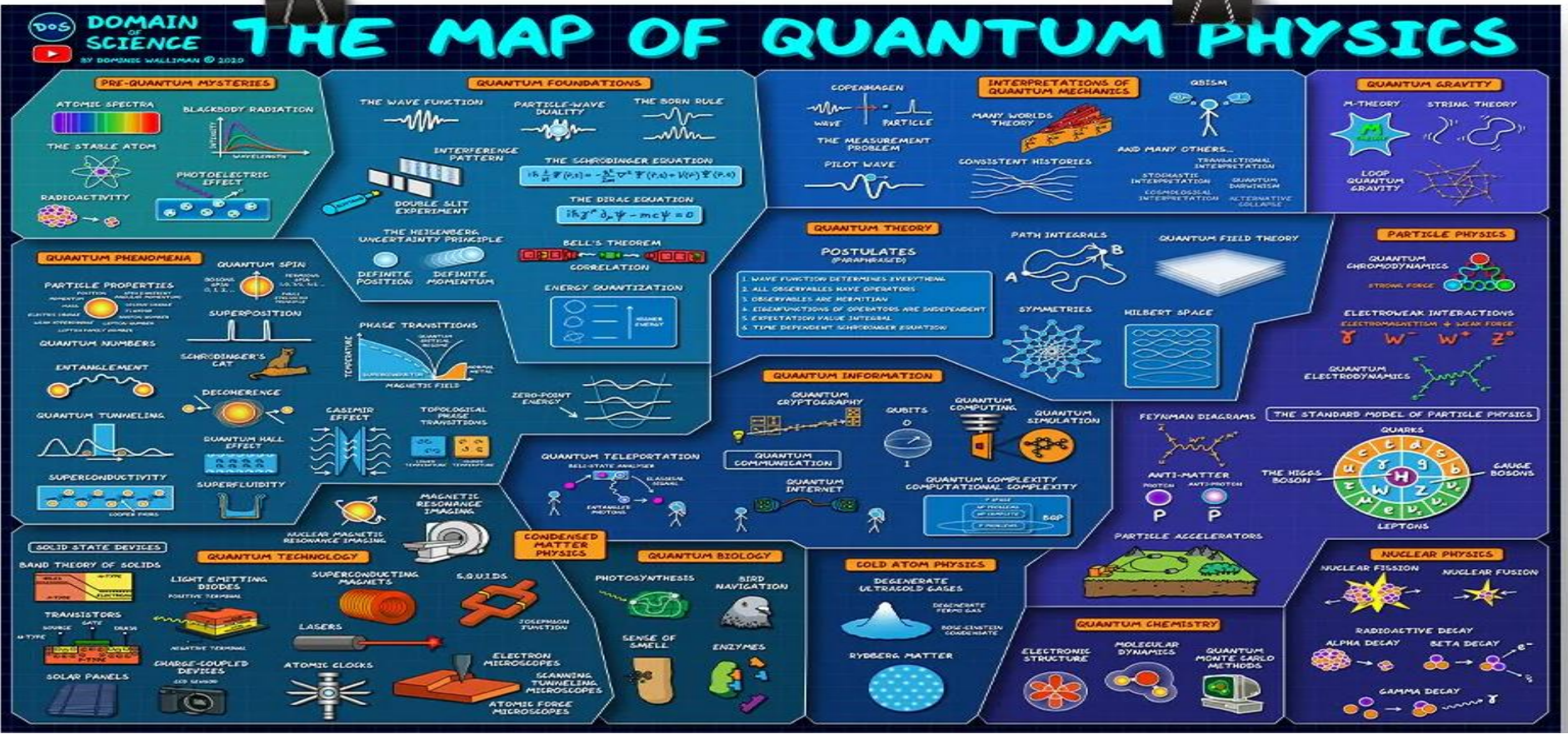


Non-Dominated Quantum Iterative Routing Optimization for Wireless Multihop Networks, August 2015IEEE Access 3, DOI: 10.1109/ACCESS.2015.2478793

Kvantum jelenségek

ELKH Cloud | SZTAKI | Wigner | ELKH Eötvös Loránd Research Network

https://www.flickr.com/photos/95869671@N08/50211268918



Kvantum számítástechnika

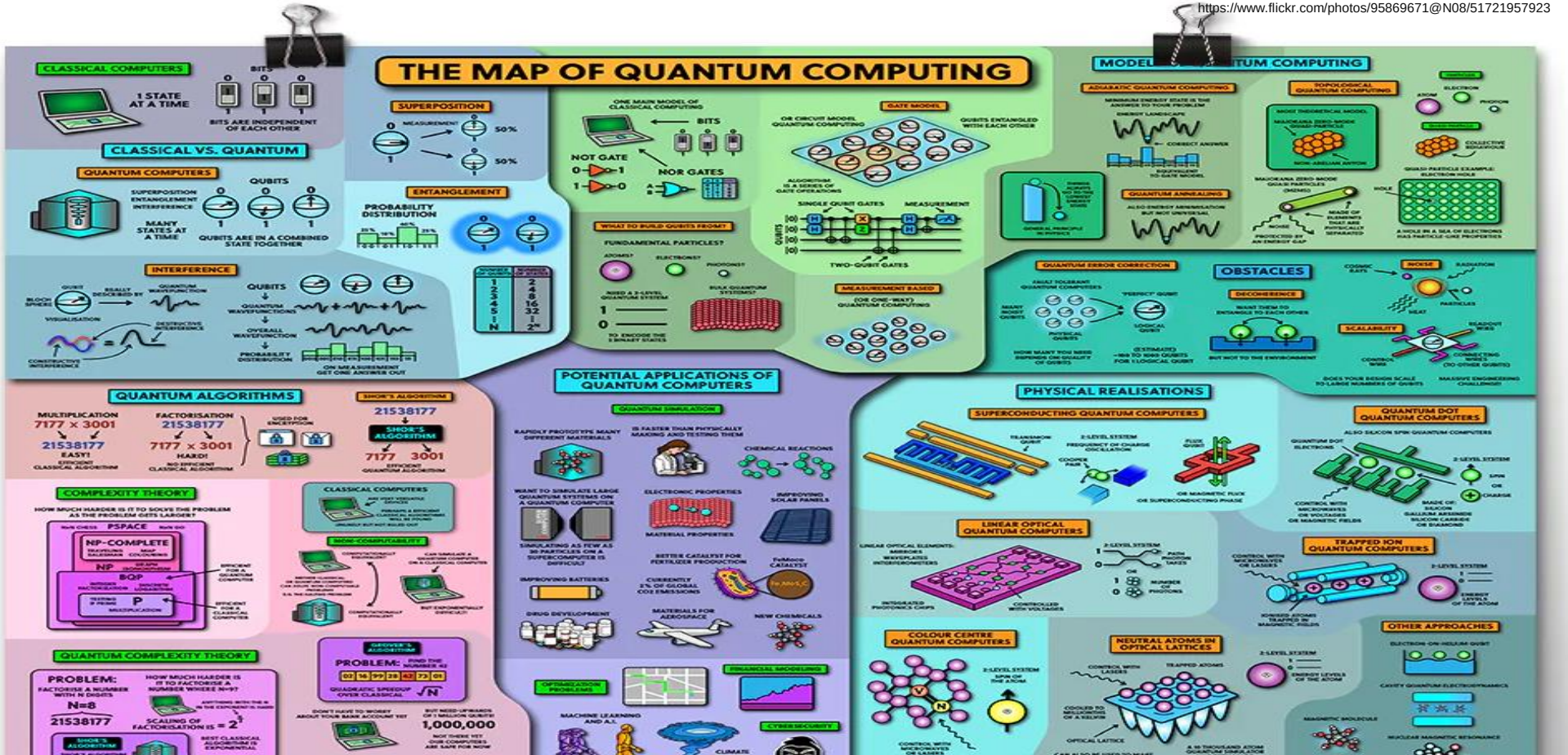
ELKH Cloud

SZTAKI

Wigner

ELKH Eötvös Loránd Research Network

https://www.flickr.com/photos/95869671@N08/51721957923



Gyakorlati példák: Kriptográfiai eljárások

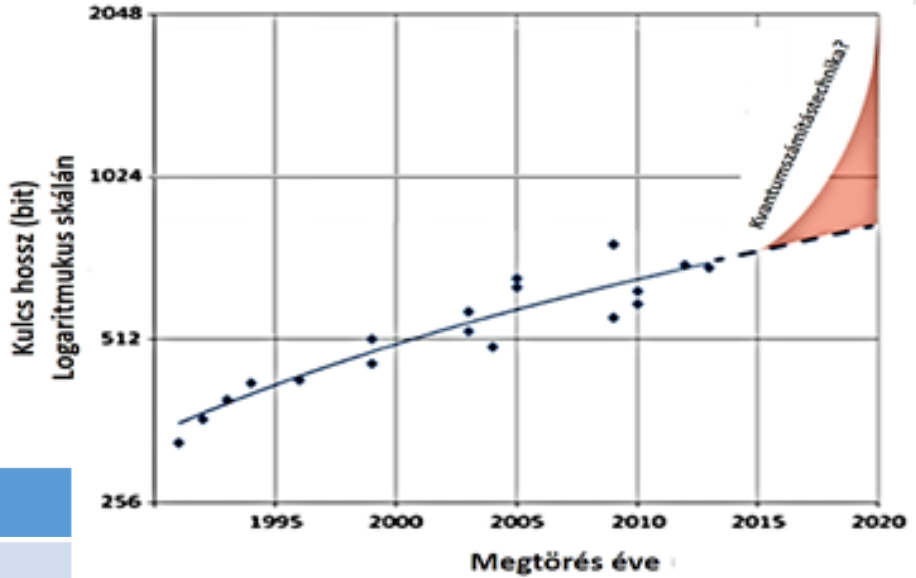
- Jelenleg a kommunikációhoz (pl.: Internetes, távközlés, elektronikus kereskedelem, stb.) leginkább három kriptográfiai eljárást alkalmazunk:
  - a nyilvános kulcsú titkosítás
  - a digitális aláírás
  - kulcscsere
- Ezekhez leggyakrabban alkalmazásra kerül:
  - **Diffie-Hellmann nyilvános kulcscsere**
    - *X9.42-es szabvány, amelynél a titkosításhoz nincs semmilyen előre megbeszélt információra szükség Whitfield Diffie és Martin Hellman (1976)*
  - **RSA titkosító rendszer**
    - *Ron Rivest, Adi Shamir és Leonard Adleman (1977)*
  - **elliptikus görbéken alapuló titkosítás (ECC)**
    - *A titkosítás az ECDLP (elliptic curve discrete logarithm problem) nevű matematikai problémára épülő kriptográfiai megoldások együttes elnevezése: aláírásra (pl. ECDSA), titkosításra (pl. EC ElGamal) és autentikációra (pl. ECDH) szolgáló algoritmusok*

Ezek mind bonyolult számelméleti problémákra (pl.: prímfaktorizáció vagy a diszkrét logaritmus probléma) vezethetők vissza.

Kulcsgenerálás problémája

- A klasszikus számítógépes architektúrák fejlődése folyamatosan növelte a számolási teljesítményt, a törési képességet és az ehhez kapcsolódó fenyegetettséget.
- Ezt a fejlődést folyamatos kulcsméret növeléssel lehetett kompenzálni.

Klasszikus számítógép	Kvantumszámítógép
Legjobb ismert algoritmussal	Shor kvantum algoritmussal
10^{34} lépés	10^{7} lépés
THz (szuper) számítógépen:317 *10^{12} év	MHz számítógépen:10 másodperc
	4000 qubit szükséges hozzá



Jelenleg az ún. **Noisy Intermediate-Scale Quantum** (NISQ) technológia korát éljük.

PQC - Poszt-kvantumkriptográfia
Túl a kvantumkriptográfián…

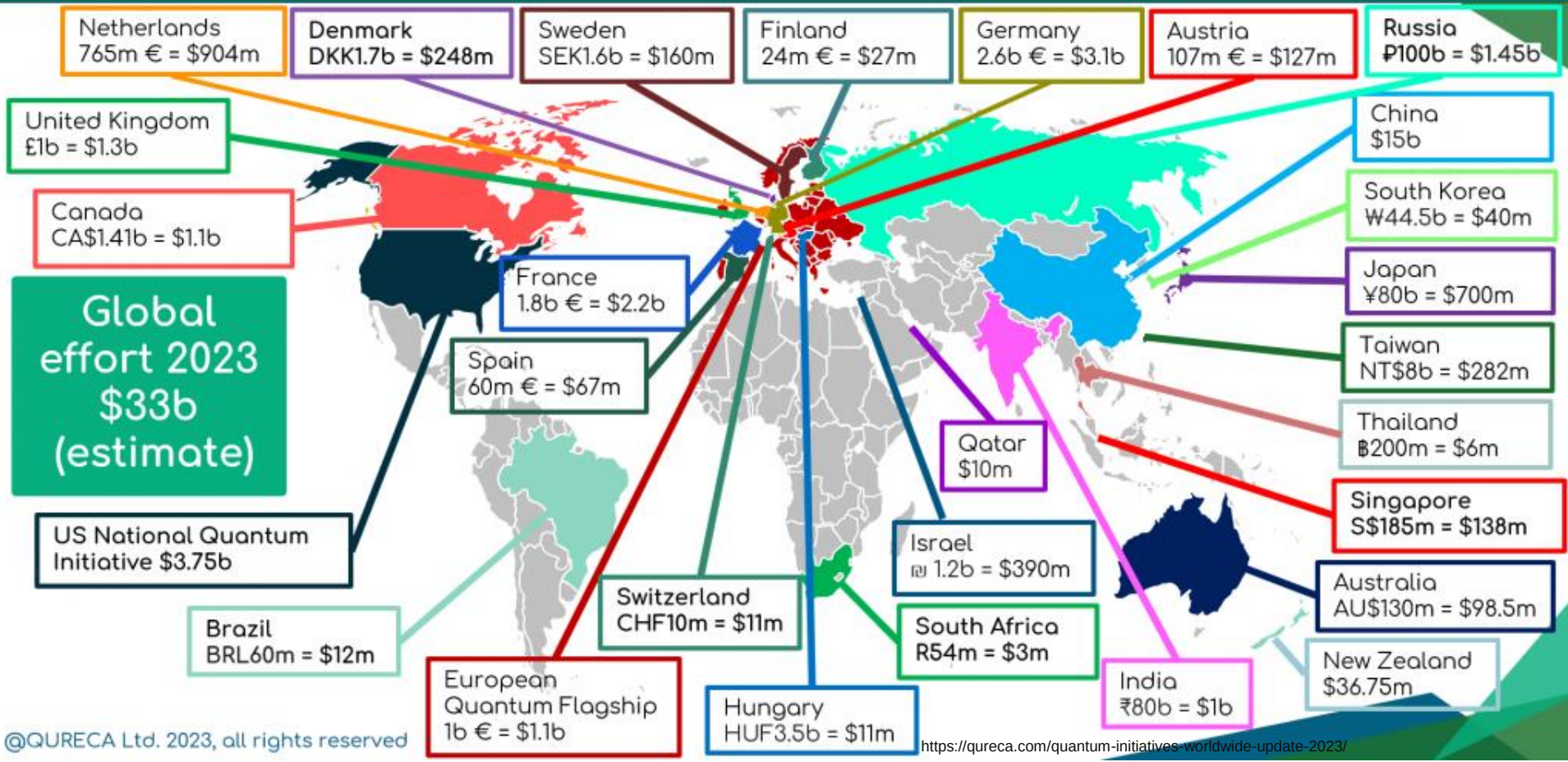
Kvantuminformatikai projekt befektetések jelenlegi helyzete a világban

ELKH Cloud

SZTAKI

Wigner

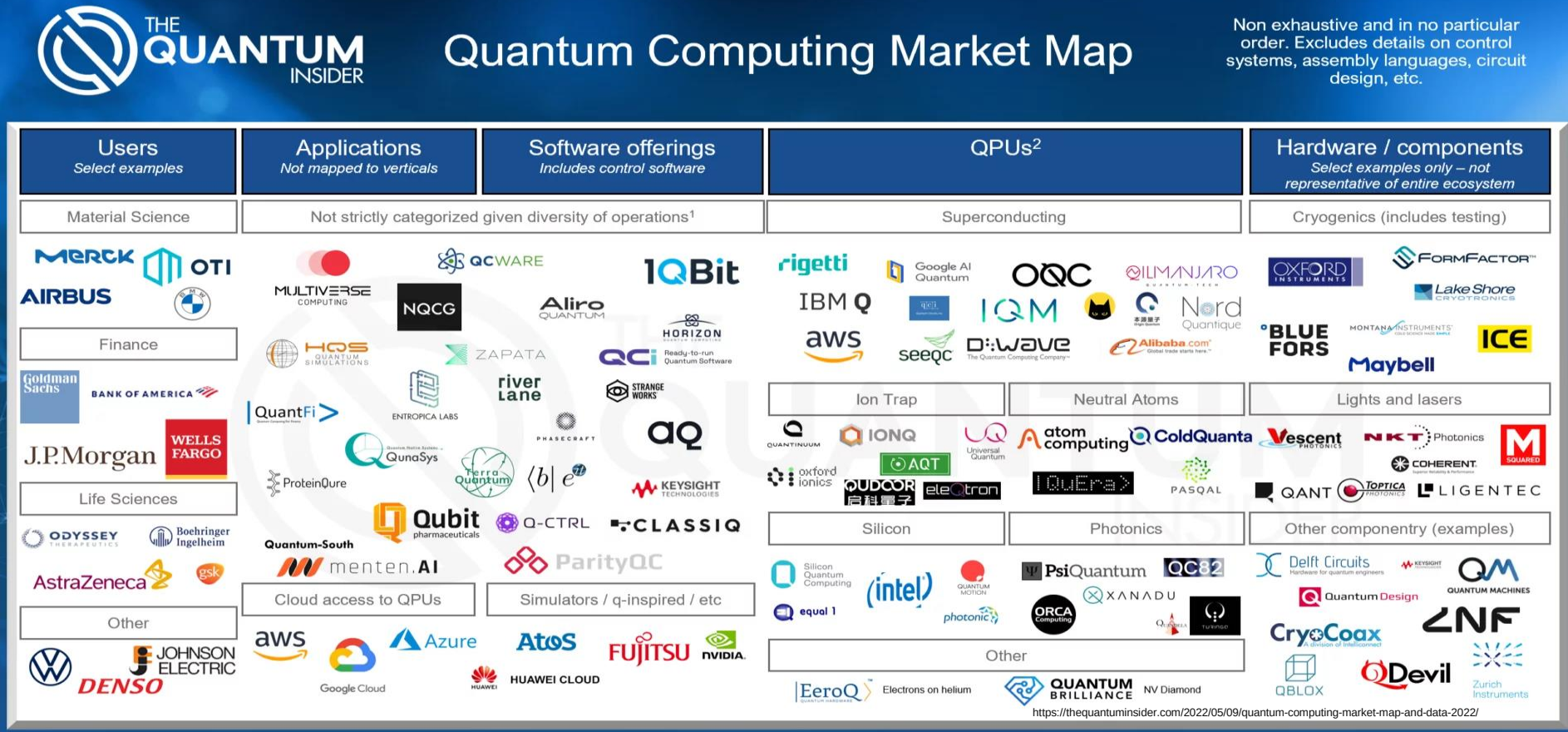
ELKH Eötvös Loránd Research Network



https://qureca.com/quantum-initiatives-worldwide-update-2023/

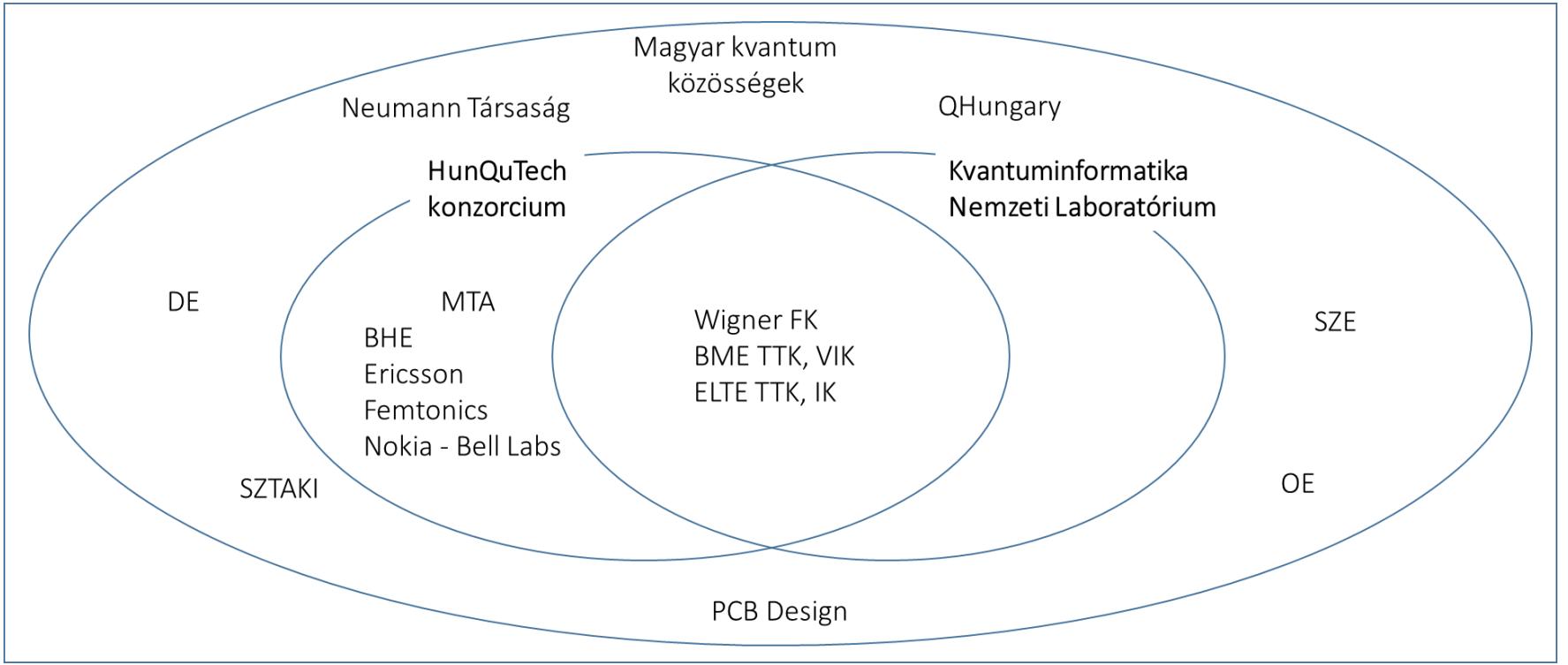
A kvantum számítástechnika piaci szereplői

ELKH Cloud · SZTAKI · Wigner · ELKH Eötvös Loránd Research Network



[1] Software offerings can be further classified into SDKs, firmware / enablers, algorithms / applications, simulators etc, but many companies are offering a mixture across the stack

Hazai helyzet



Összefoglalás

- A kvantum számítástechnika már nem a jövő, hanem a jelen
- Érdemes megismerni - jó hosszútávú befektetés
- Elérhető infrastruktúra
- Megtanulható használat

Sok örömöt és hasznos tudást kívánok a mai előadásokhoz!

ELKH Cloud

SZTAKI

ELKH | Eötvös Loránd Research Network

Wigner

www.elkh.org