



HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

Tudomány és technológia a smart ökoszisztémák szolgálatában

20 percben

A teljesség igényével és józan ész szubjektivitásával.

Dr. Imre Sándor

imre@hit.bme.hu



TOP 10 STRATÉGIAI TECHNOLÓGIA 2018-2019

Gartner

Intelligent



Autonomous Things



Augmented Analytics



AI-Driven Development

Digital



Digital Twin



Empowered Edge



Immersive Experience

Mesh



Blockchain



Smart Spaces



Privacy and Ethics



Quantum Computing

People-centric



Hyperautomation



Multiexperience



Democratization



Human Augmentation



Transparency and Traceability

Smart spaces



Empowered Edge



Distributed Cloud



Autonomous Things



Practical Blockchain



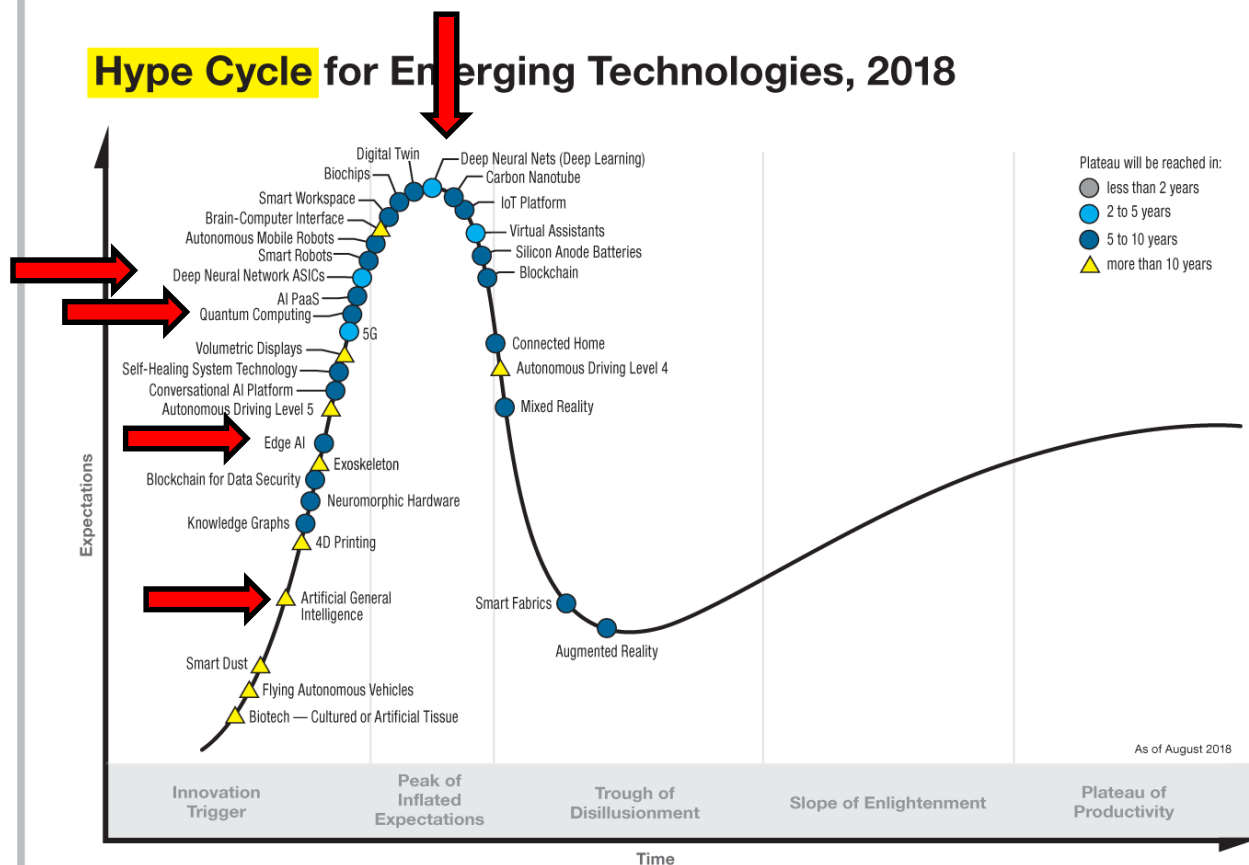
AI Security

-
- This conceptual illustration depicts a human head in profile, filled with glowing neural activity and digital elements. From the top of the head, a network of blue lines branches out like a tree, supporting various circular icons representing modern technology: a keyboard, Wi-Fi signal, gear, smartphone, bar chart, hard drive, folder, laptop, cloud storage, document, monitor, mouse cursor, wrench and screwdriver, and a magnifying glass over a pie chart. The entire composition is set against a dark background with a grid pattern and vibrant light effects emanating from the brain area. Two large, curved arrows, one blue and one orange, frame the central image, suggesting a cyclical or interconnected process.



© Hálózati Rendszerek és Szolgáltatások Tanszék

Hype Cycle for Emerging Technologies, 2018



gartner.com/SmarterWithGartner

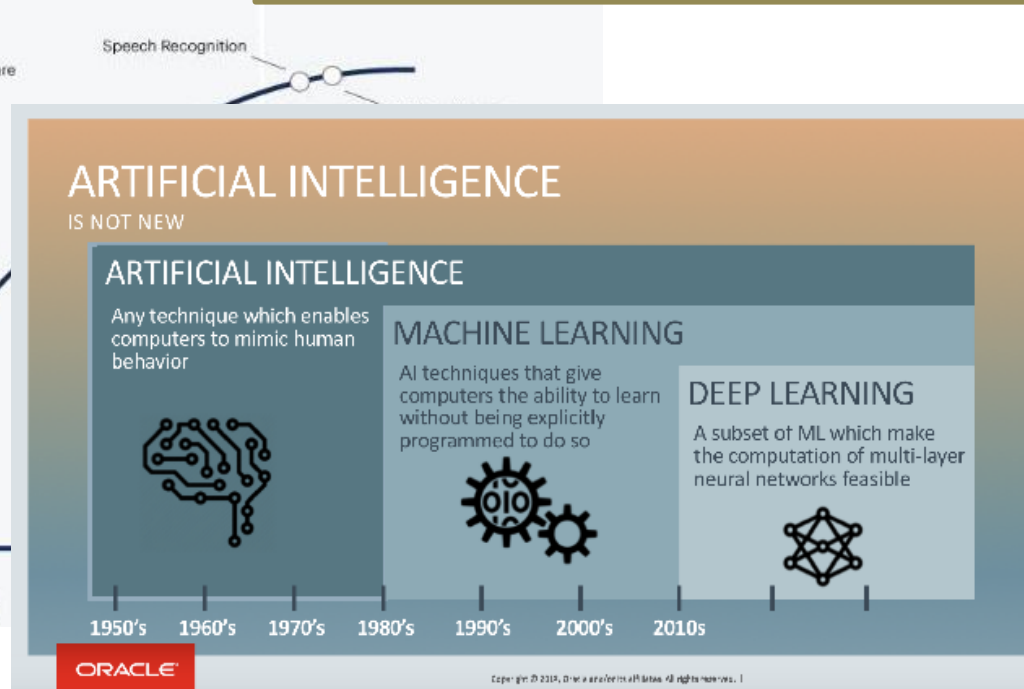
Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

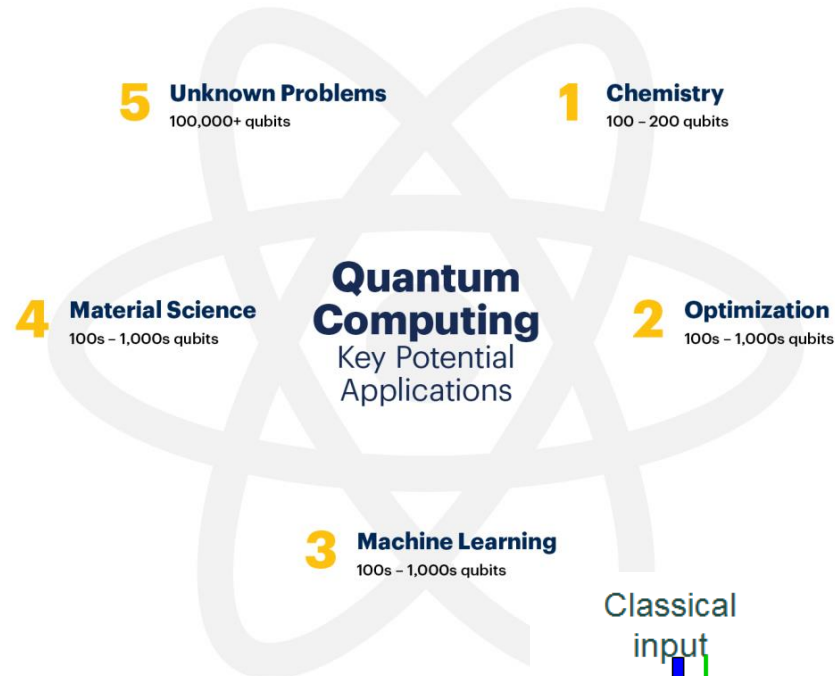
Gartner

FELDOLGOZÁS - MESTERSÉGES INTELLIGENCIA

- Problémamegoldás
 - analitikus
 - próbálgatás alapú
 - tanulás alapú
- ❖ Itt már a tanulást modellezzük!

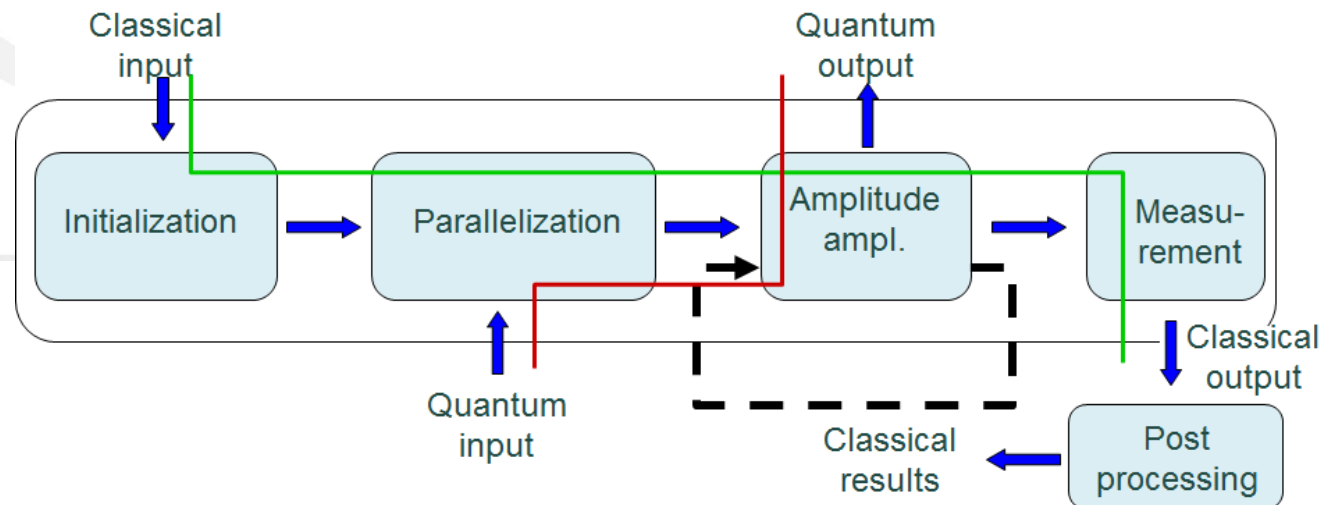
MESTERSÉGES INTELLIGENCIA HYPE GÖRBE 2019



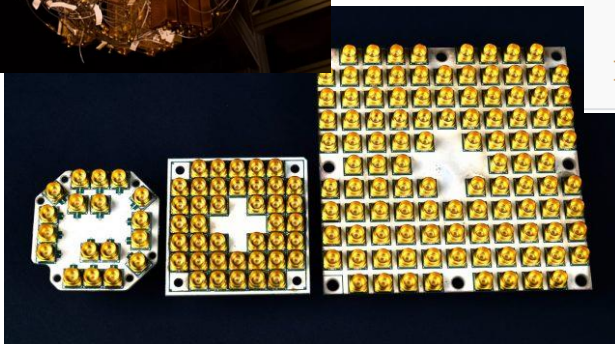


gartner.com/SmarterWithGartner

Source: "Nature," Wikipedia
© 2019 Gartner, Inc. All rights reserved.



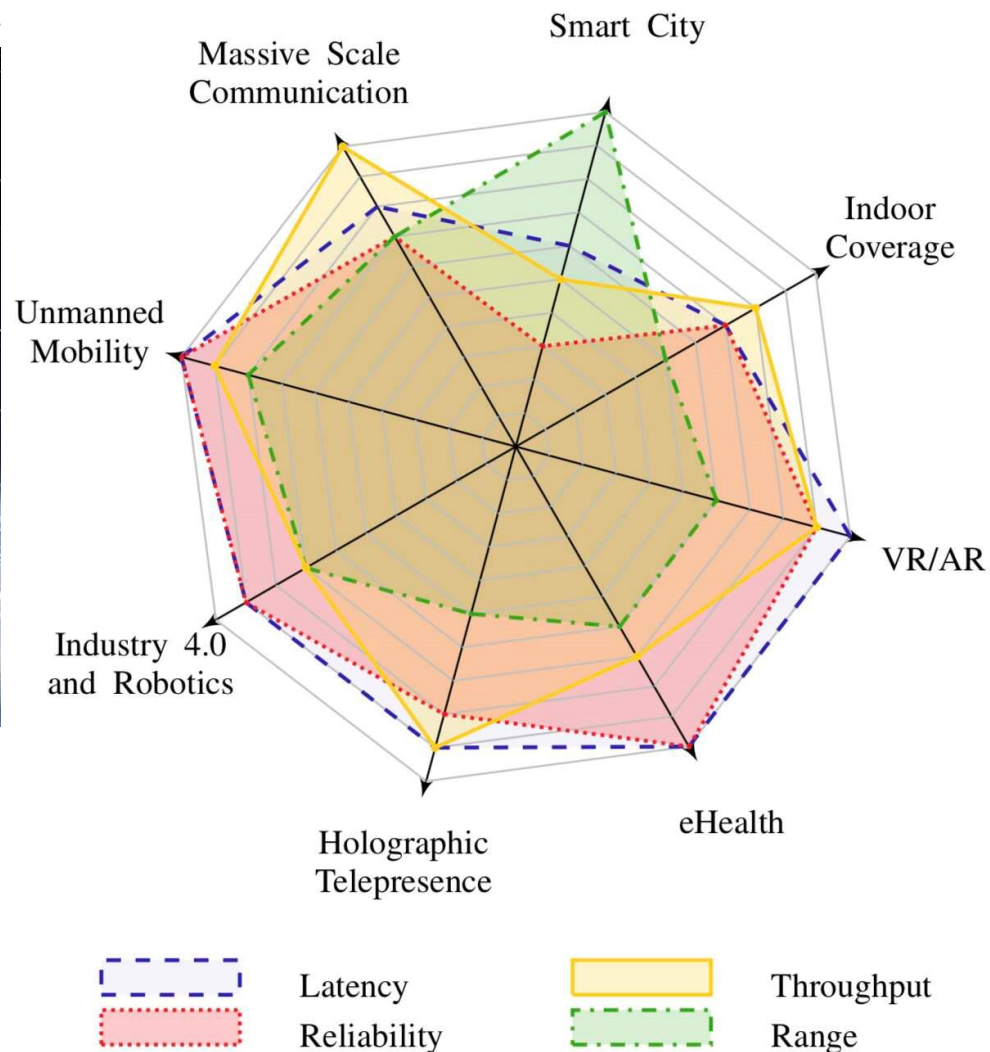
- Kvantum informatika
 - Hardver
 - Szoftver
 - ❖ Módszertan!
 - ❖ Programnyelvek



```
operation BellTest (count : Int, initial: Result) : (Int,Int)
{
  body
  {
    mutable numOnes = 0;
    using (qubits = Qubit[1])
    {
      for (test in 1..count)
      {
        Set (initial, qubits[0]);

        let res = M (qubits[0]);

        // Count the number of ones we saw:
        if (res == One)
        {
          set numOnes = numOnes + 1;
        }
      }
      Set(Zero, qubits[0]);
    }
    // Return number of times we saw a |0> and number of times we saw a |1>
    return (count-numOnes, numOnes);
  }
}
```

Density of connections: 10^6 devices/km² → 10^8 devices/km² Latency: 10ms → 0.1ms Frequency bandwidth: 20GHz → 3THz Data rate: 10Gbps → 1Tbps Mobility: 500km/h → 1000km/h Network energy efficiency: 100x

A 6G-HEZ VEZETŐ ÚT

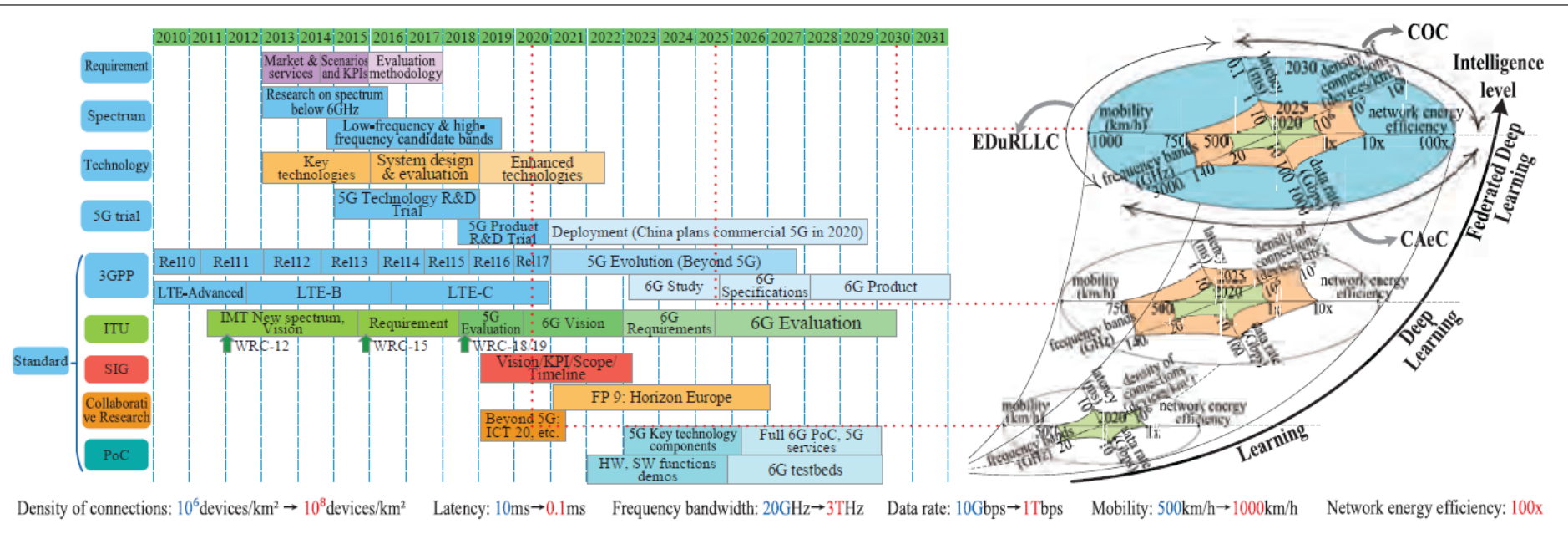


Figure 1. The roadmap of 6G. Explicit performance comparisons between 5G and 6G requirements are listed. IEEE ComMag 08/2019

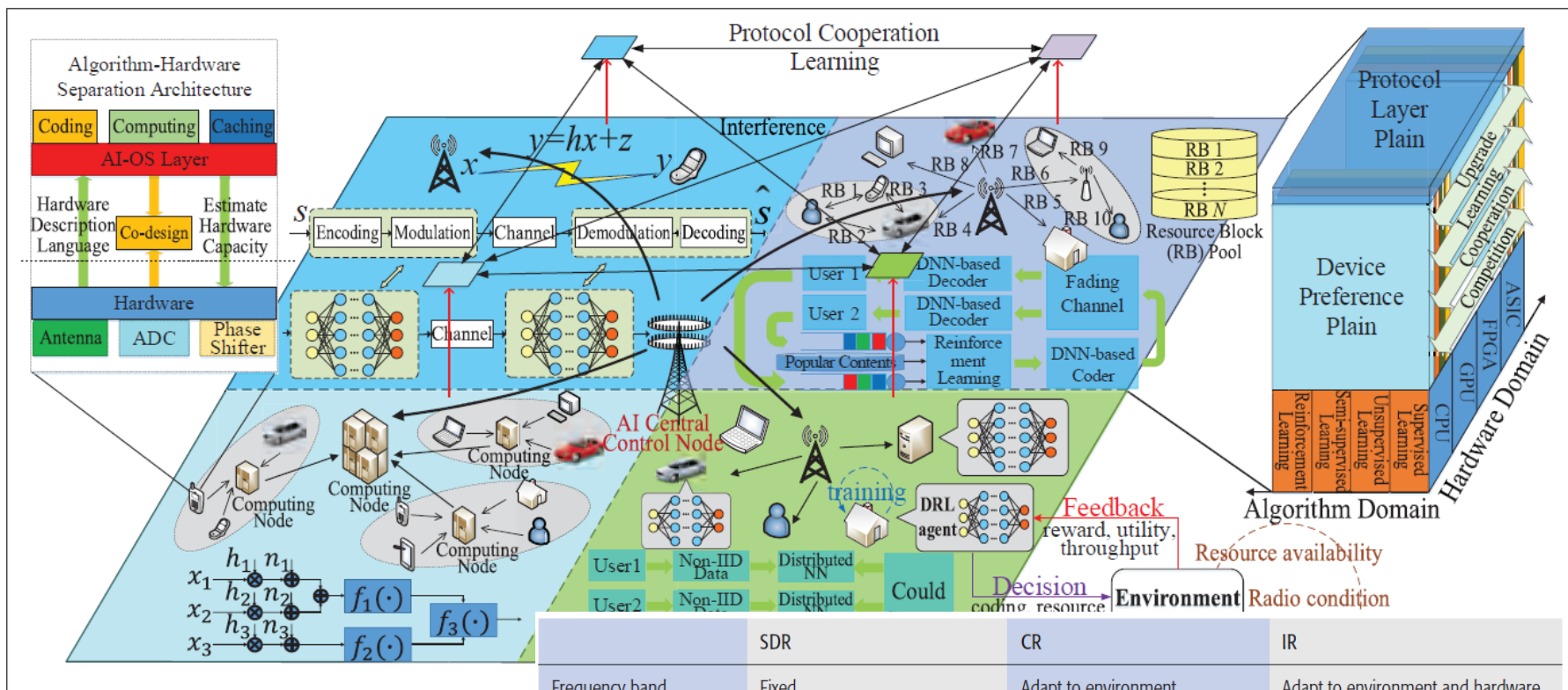


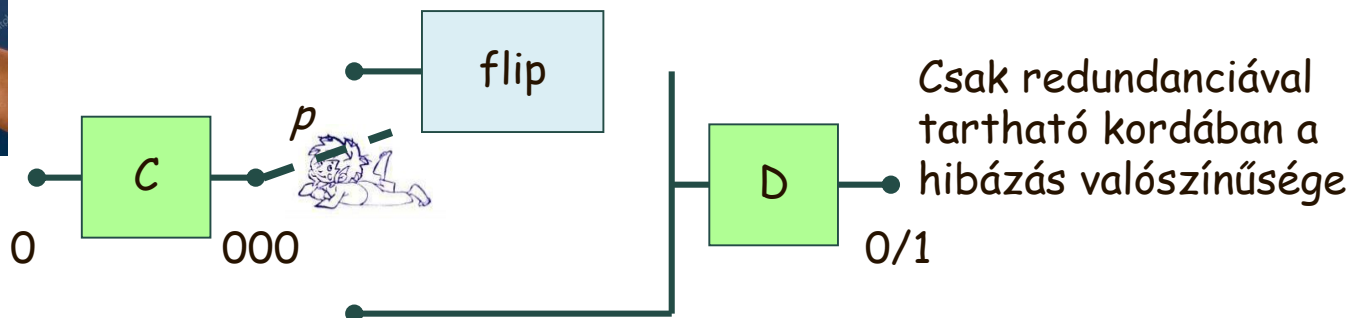
Figure 2. The architecture of 6G.

	SDR	CR	IR
Frequency band	Fixed	Adapt to environment	Adapt to environment and hardware
Spectrum sharing	Fixed	Opportunistic	AI-enabled
Hardware capability	Pre-claimed	Pre-claimed	Online estimated
Hardware upgradability	No	No	Yes
PHY Tx/Rx module	Modulation/coding/detection/estimation	Modulation/coding/detection/estimation	Deep neural networks
Multiple access	Predetermined	Sensing based	Distributed ML based
Protocols over Layer 3	Fixed	Fixed	Self-upgradable
Main steam apps	Voice, data	Multimedia, data	AI, in-network computation

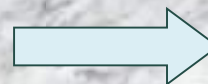
Table 1. Comparison of SDR, CR, and IR.



Klasszikus csatorna

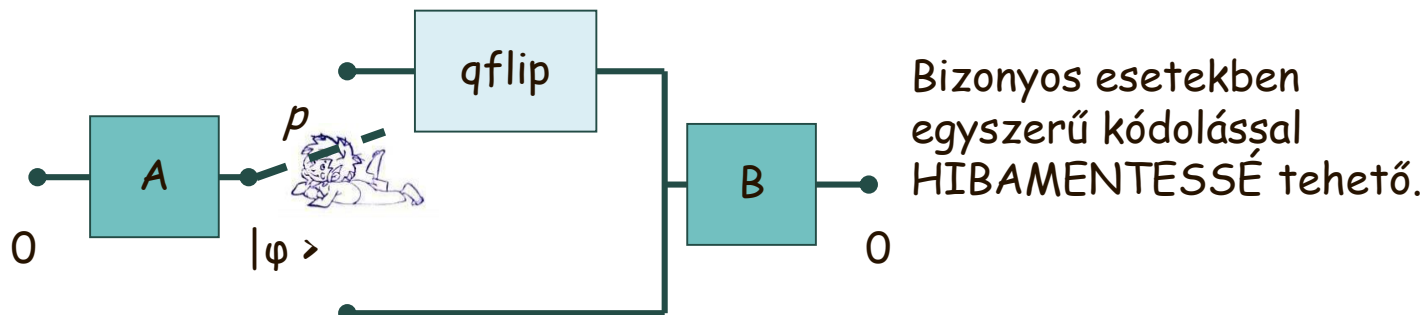


$$p_{ij} = \frac{1}{2}$$

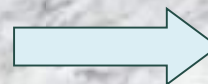


$$C = 1 - H(p) = 0$$

Kvantum csatorna



$$p_{ij} = \frac{1}{2}$$

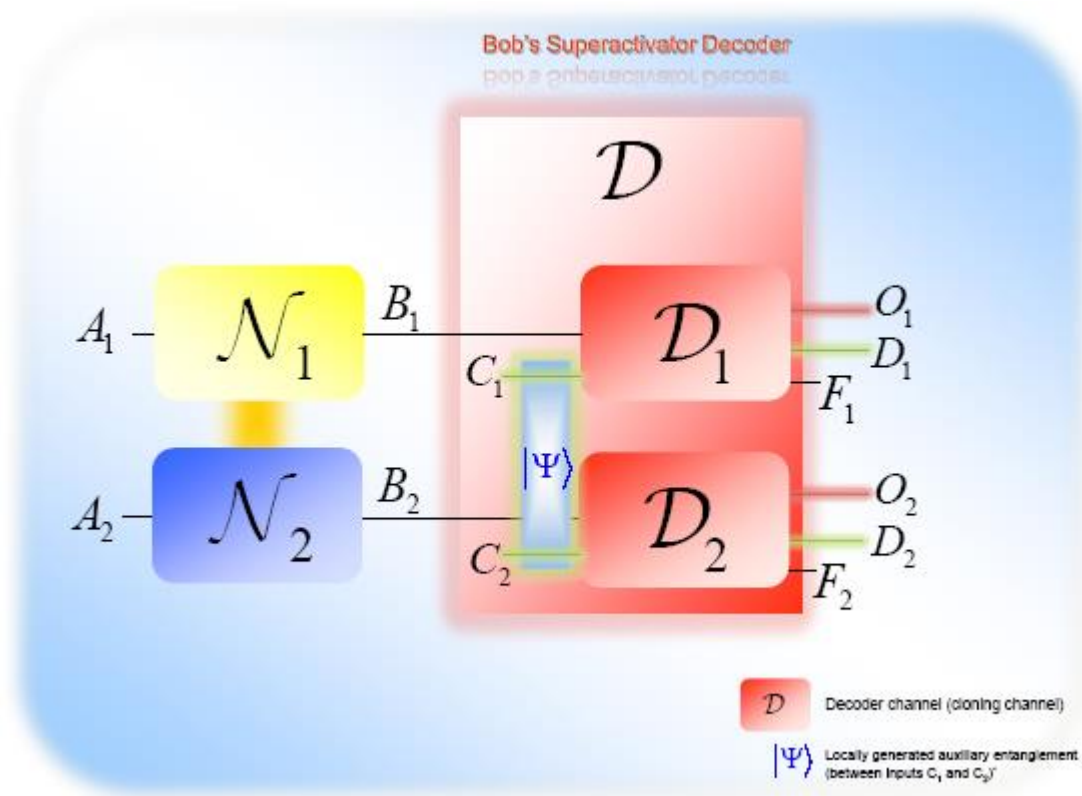


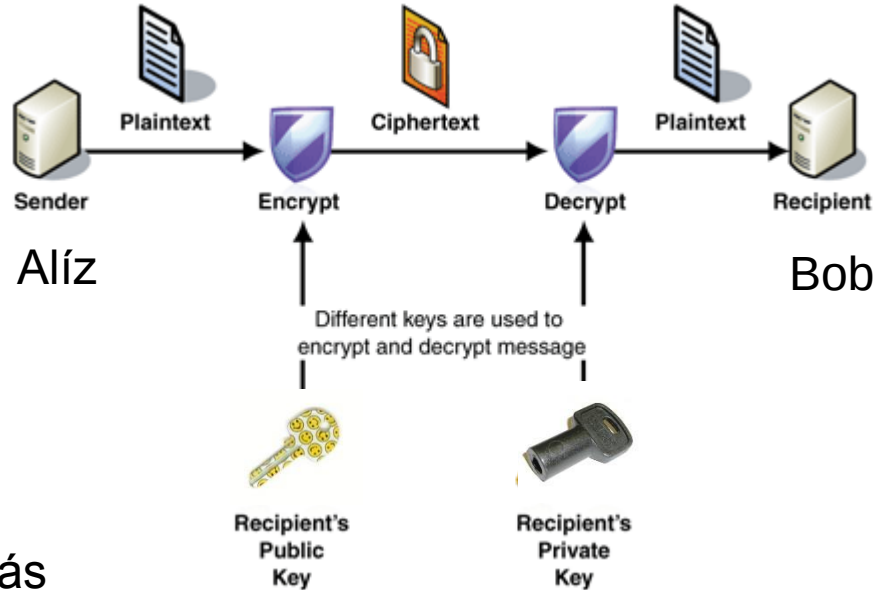
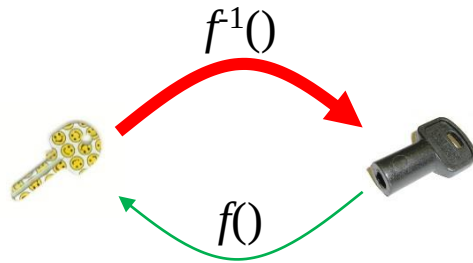
$$C = 1$$

SZUPERAKTIVÁLÁS



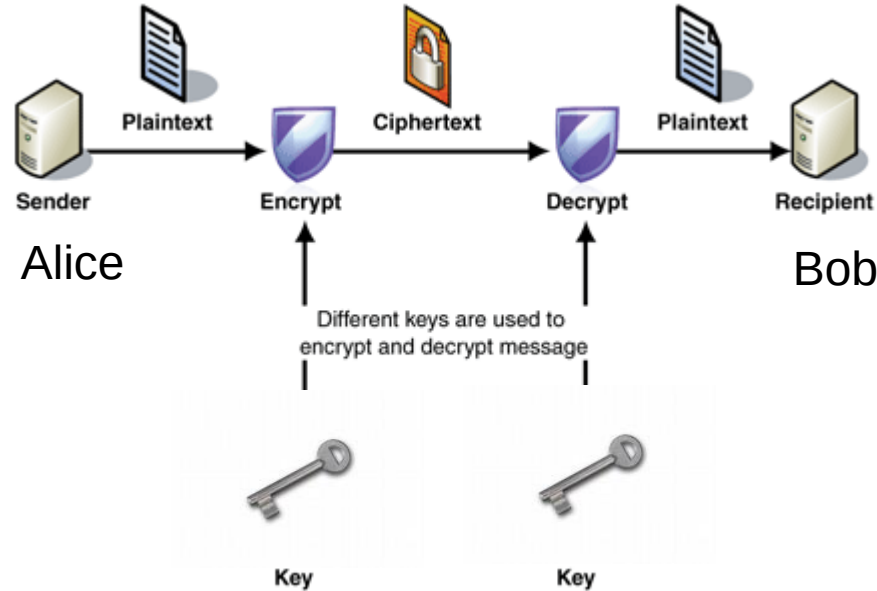
- 2 db. külön-külön $C = 0$ kapacitású csatorna
ügyesen
összekapcsolva mégis
képes információt
átvinni!



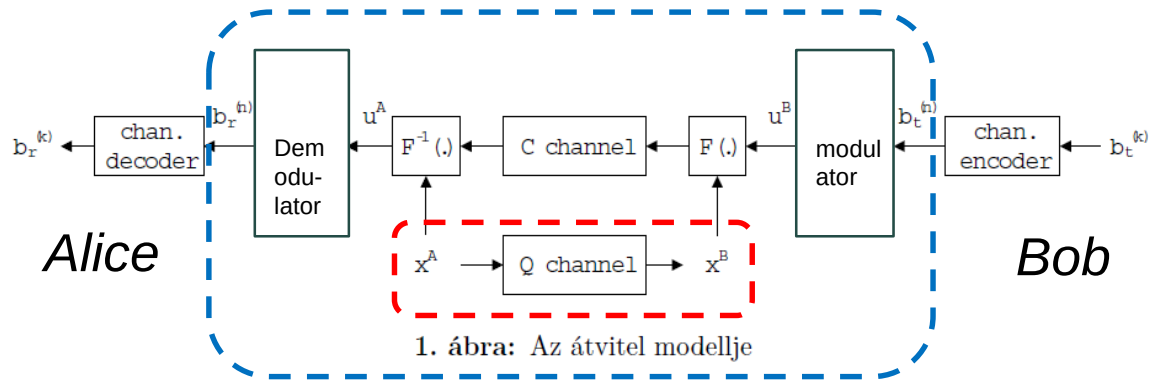
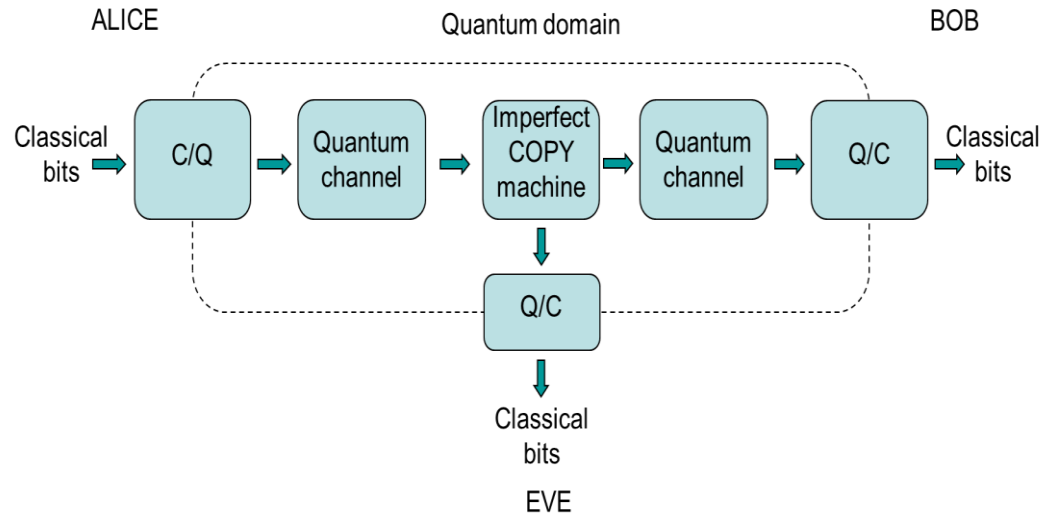


- Nyilvános kulcsú titkosítás
 - nyilvános titkosító kulcs, titkos fejtőkulcs
 - kulcsok előállítása: két nagy prímszám szorzatát felhasználva
 - feltörés: a törzstényezők meghatározása
- A mai napig nem sikerült bizonyítani, hogy nincs hatékony algoritmus a feltörésre. Mindenesetre eddig nem sikerült ilyen klasszikus algoritmust találni.
- **De kvantumosat IGEN!**

- Post-quantum/Quantum-safe
 - Új klasszikus nyilvános kulcsú eljárások (pl. **OPEN QUANTUM SAFE**)
 - hash functions
 - error correcting codes
 - lattices (including the learning with errors (LWE) and related problems)
 - multivariate equations
 - supersingular elliptic curve isogenie
 - Nehézség: még nem ismerjük a kvantum számítógépek határait
- Kvantum kulcsszétosztás
 - A fizikai réteg védelme: szimmetrikus kulcsú megoldásokhoz a kulcsok biztonságos megoldása.



- Szimmetrikus kulcsú titkosítás
 - Egyforma kulcsok mindkét oldalon
- Abszolút biztonságos, ha bizonyos előírásokat betartunk
- Gond, hogy a kulcsot miként juttassuk el a túloldalra????



- Paradigmaváltás a tudományban!
A tudományos kutatás alapelvei örökök, de változnak
 - a kihívások
 - az eszközök
 - a módszertanok
 - és remélhetőleg a tudósok is!



Az új polihisztor a (kvantum) AI?