Mika Ylianttila (M. Sc, Dr.Sc, eMBA) is a full-time associate professor (tenure track) at the Centre for Wireless Communications (CWC), at the Faculty of Information Technology and Electrical Engineering (ITEE), University of Oulu, Finland. He leads NetSEC (Network security, trust and privacy) research group at CWC Networks and Systems research unit, which studies and develops secure, scalable and resource-efficient techniques for 5G and beyond 5G systems.

Www:
https://www.oulu.fi/en/researchers/mika-ylianttila
https://www.oulu.fi/en/research-groups/network-security-trust-and-privacy

World's First 6G Research Program

6G Enabled Wireless Smart Society & Ecosystem

- National Flagship for **2018-2026**
- Volume **251 M€**
- Operated by **University of Oulu**
- Collaboration with **Nokia, VTT, Aalto University, BusinessOulu, OUAS.**

6G Flagship was elected as **Finland's high-tech Flagship,** by **Finnish Government** through **Academy of Finland**

1.
Wireless Connectivity
Ultra-reliable low-latency communications vs. 1 Tbps

Enabling **Unmanned Processes**
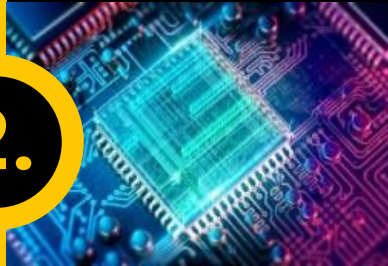
2.
Devices & Circuits
THz communications materials & circuits

Enabling **Unlimited Connectivity**

3.
Distributed Computing
Mobile edge intelligence

Enabling **Time Critical & Trusted Apps**

4.
Services & Applications
Multidisciplinary research accross verticals

Enabling **Disruptive Value Networks**

- To support companies in **finalisation of the 5G** standard by carrying out technology and system pilots.

- To develop/co-create the **fundamental technology components to enable 6G** systems.

- To speed up **dependable, robust and secure digitalisation of society** via 5G and 6G.

6GFLAGSHIP.COM, #6GFLAGSHIP

6G
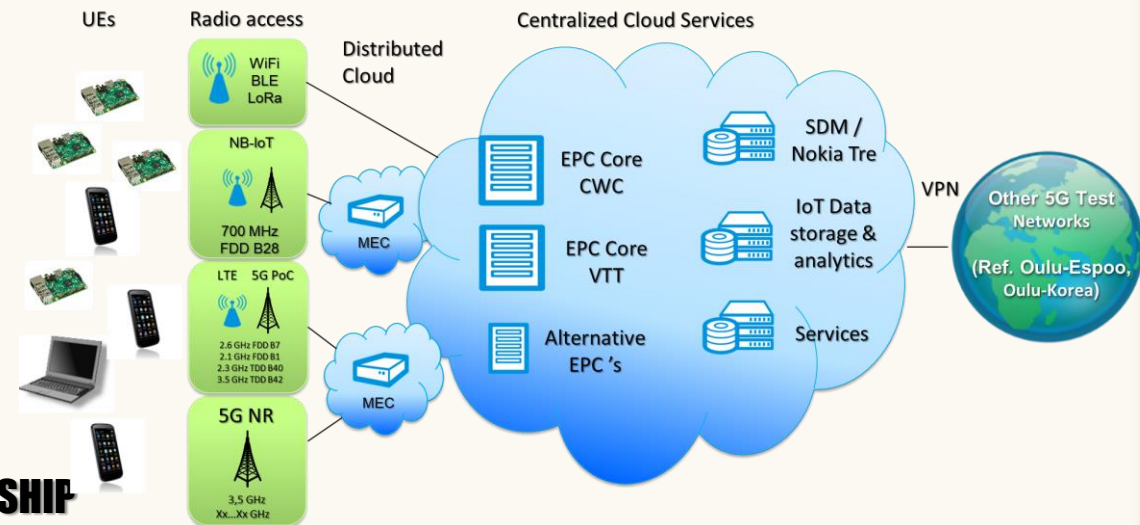
Vision for 2030

Our society is data-driven, enabled by near-instant, unlimited wireless connectivity.
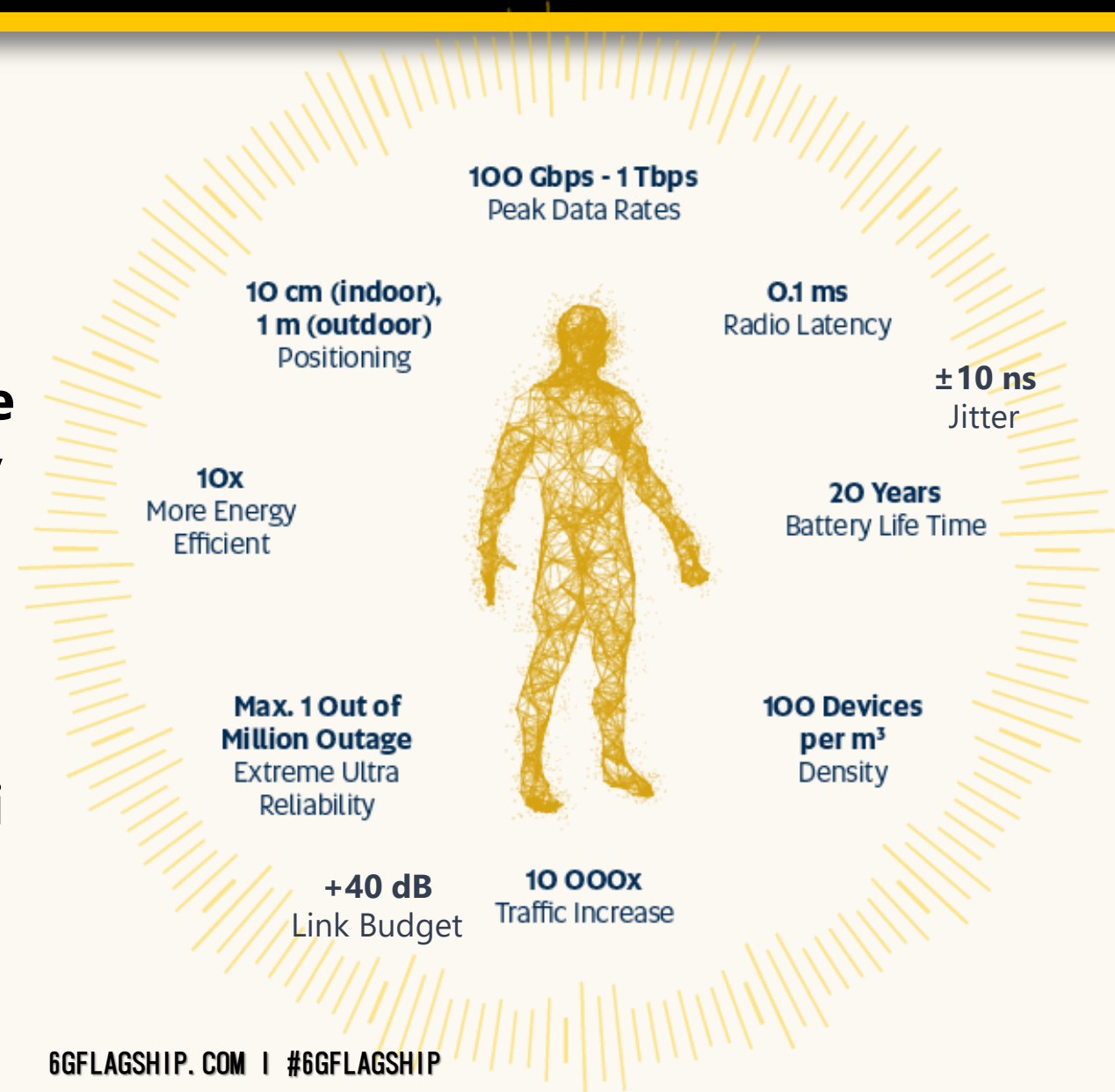
6G will emerge around 2030 to satisfy the expectations not met with 5G, as well as, the new ones fusing AI inspired applications in every field of society with ubiquitous wireless connectivity.

2030

- **Generic 6G targets presented by academia and industry in different fora.**

- **More dense networks -> more vulnerabilities and potentially malicious/compromised nodes**

- **More personal and sensitive IoT/measurements/confidential data moved in the network -> need for better privacy**

100 Gbps - 1 Tbps
Peak Data Rates

10 cm (indoor), 1 m (outdoor)
Positioning

0.1 ms
Radio Latency

±10 ns
Jitter

10x
More Energy Efficient

20 Years
Battery Life Time

Max. 1 Out of Million Outage
Extreme Ultra Reliability

100 Devices per m³
Density

+40 dB
Link Budget

10 000x
Traffic Increase

6G Merges Communications with New Applications

- **6G is not only about moving bits: it will become a framework of services, including communication service.**

- **In 6G, all user specific computation and intelligence may move to edge cloud.**

- **Integration of sensing, imaging and highly accurate positioning capabilities with mobility opens a myriad of new applications in 6G.**

- **Trust and privacy are key prerequisites for successful 6G service platform.**
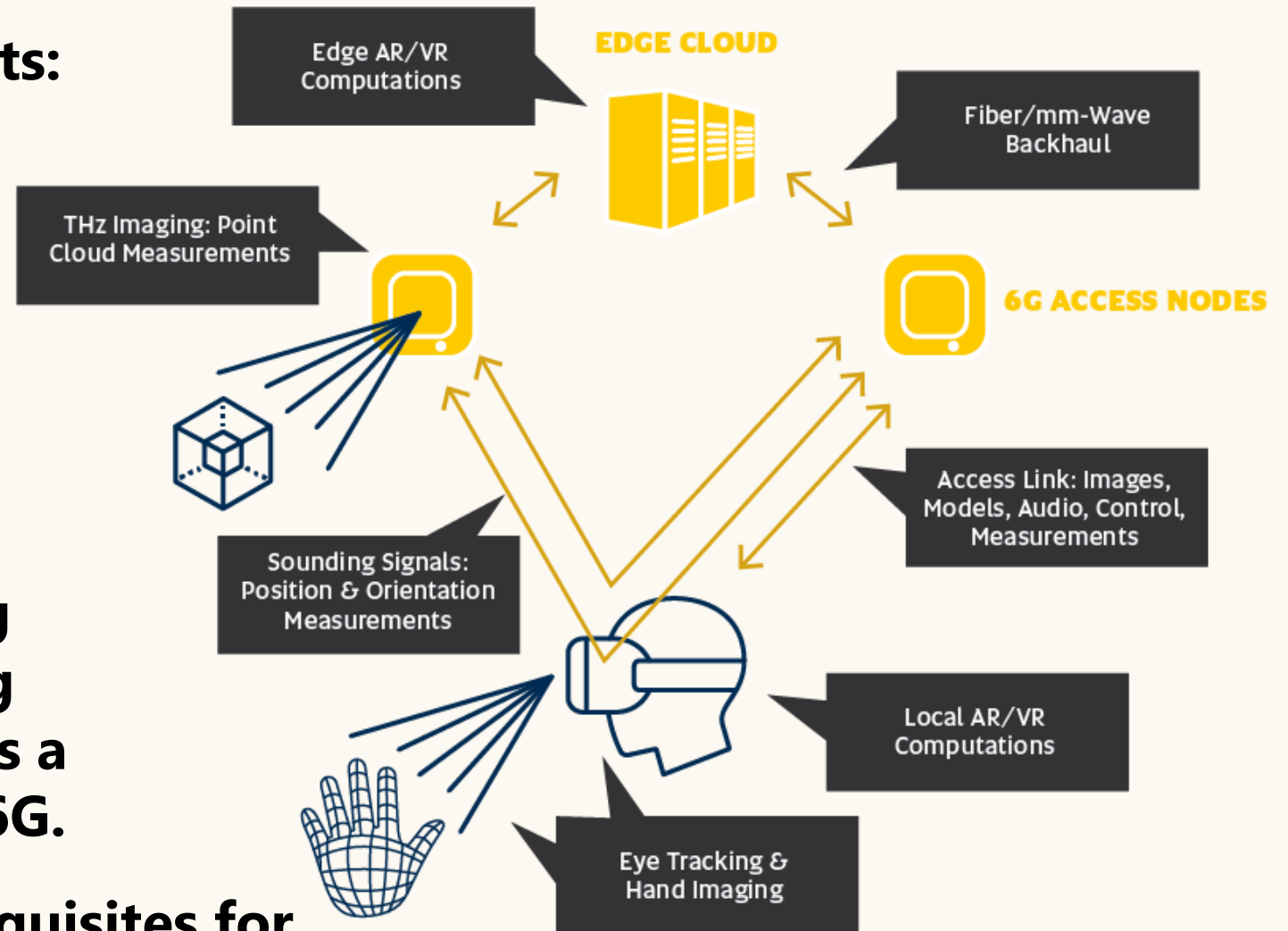
Nokia's view on 6G timeline

ACADEMY OF FINLAND

FLAGSHIP PROGRAMME

6G

FLAGSHIP

UNIVERSITY OF OULU

6G White Paper: Research Challenges For Trust, Security And Privacy.
http://urn.fi/urn:isbn:9789526226804

http://jultika.oulu.fi/files/isbn9789526223544.pdf

End-to-end trust networking for 6G

- **6G needs a network with embedded end-to-end trust, advanced security and privacy**

- **6G will create data markets – privacy protection will be a key enabler.**

- **Machine learning/AI and blockchain may play a major role in 6G networks.**

- **Post-quantum vs. architectural aspects of security**
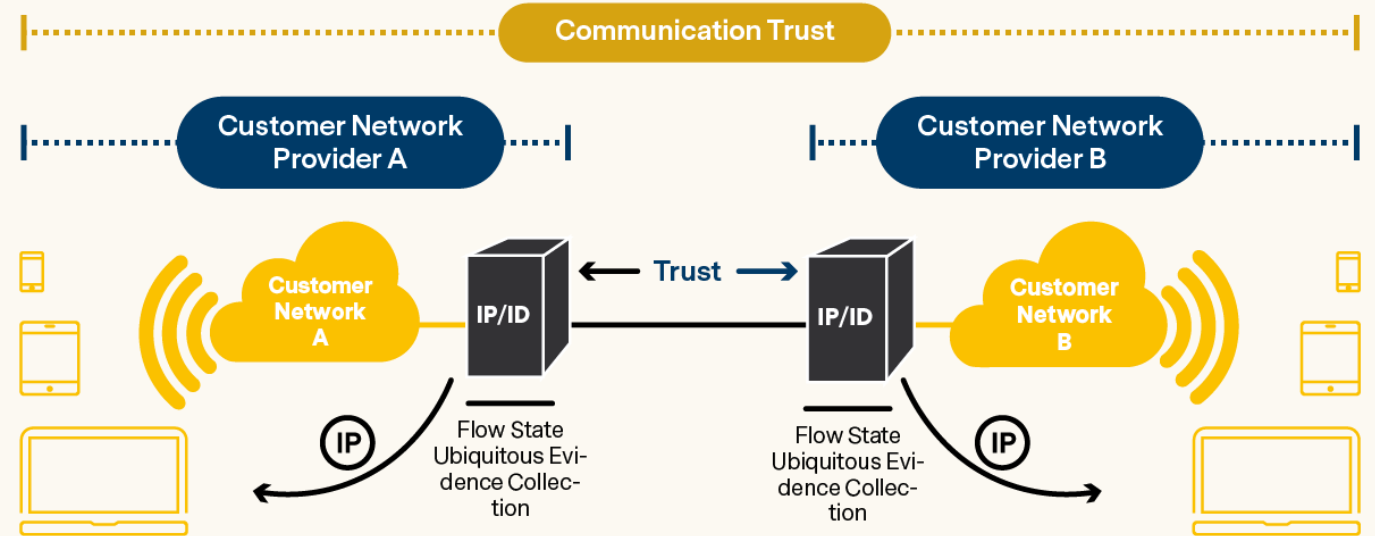
M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi & I Oppermann (Eds.). (2020). 6G White Paper: Research Challenges For Trust, Security And Privacy. (6G Research Visions, No. 9). University of Oulu. http://urn.fi/urn:isbn:9789526226804
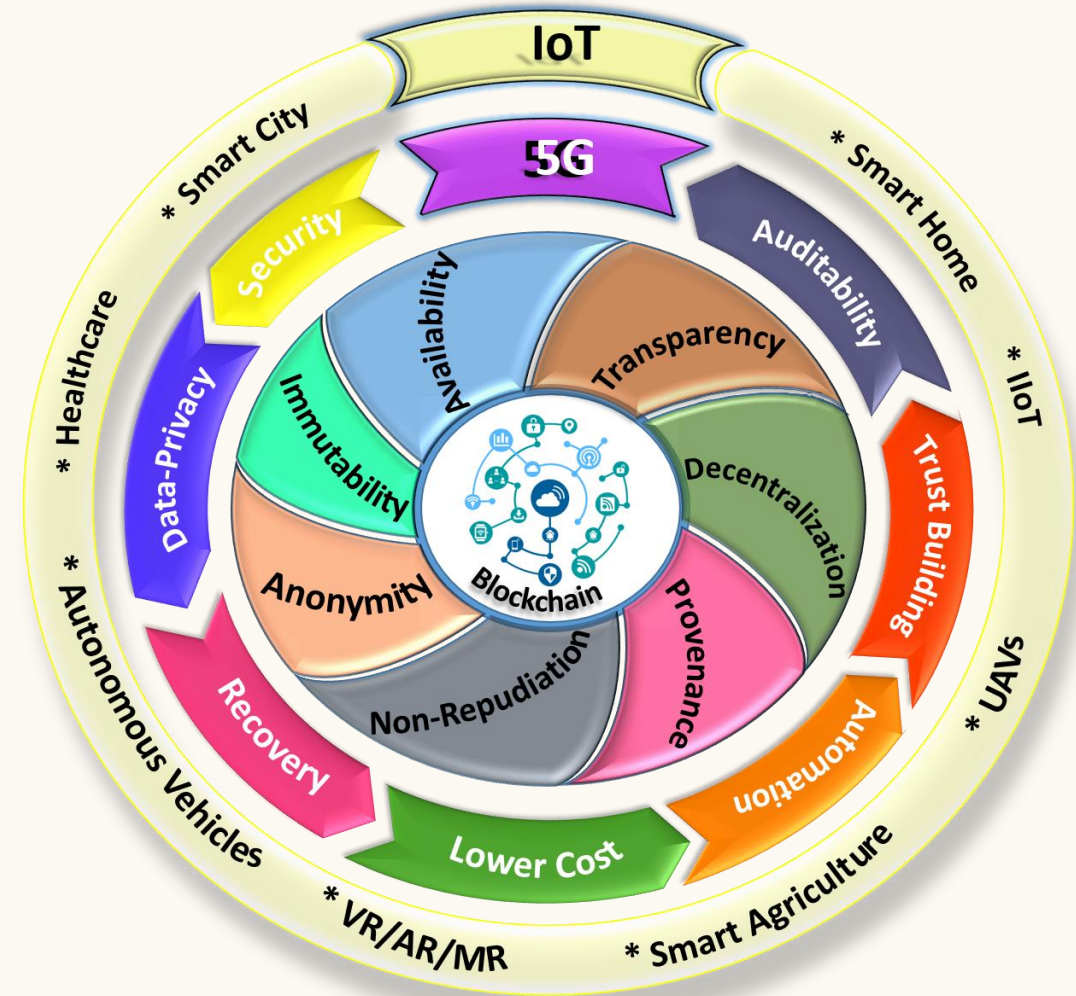
Youtube: 6G Flagship Webinar on Fundamental Research Challenges for Trust, Security and Privacy: https://www.youtube.com/watch?v=rcEvAOnzuhQ
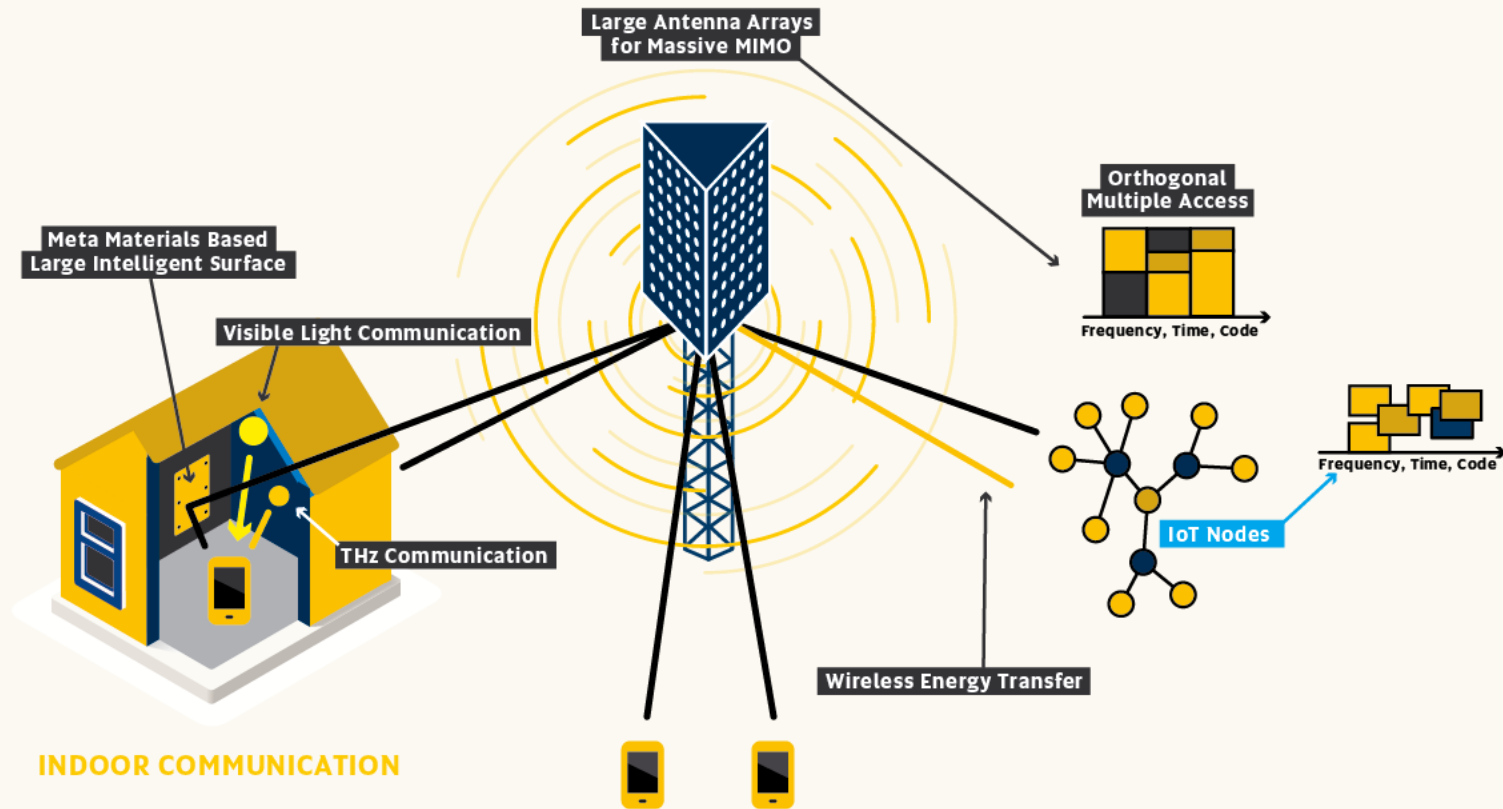
Post-Quantum Cryptography

- **Embedding intelligence and dynamicity to security**
  - **Multi-point threat detection, function migration**
  - **Software containers**
- **Autoconfiguring, zero-trust security**
- **Prevention of AI/ML based intelligent attacks**
  - **Example: poisoning and inference attacks to AI/ML models**

- **TelcoCloud is used for network functions and user data**
- **6G low latency**
  - **Offloading functions from connected IoT devices, vehicles**
- **How Confidentiality, Integrity, Privacy ensured for remote data?**
- **Remote attestation, platform synchronization, encrypted search**

Youtube: 6G Flagship Webinar on Fundamental Research Challenges for Trust, Security and Privacy: https://www.youtube.com/watch?v=rcEvAOnzuhQ

- **6G needs a network with embedded trust**

- **Blockchain technology has many potential use cases:**
  - Distributed trust management for across networks
  - Iot data management
  - Secure VNF migration
  - Automation using smart contract
  - Reliable service and QoS
  - Billing of IoT devices
  - Certification revocation

Tharaka Hewa, Anshuman Kalla, Avishek Nag, Mika Ylianttila, Madhusanka Liyanage, "**Blockchain for 5G and IoT: Opportunities and Challenges** ", in The 8th IEEE International Conference on Communications and Networking (IEEE ComNet'2020), Hammamet, Tunisia, March 2020

Physical Layer Security in 6G

- **Security protection at the physical layer.**

- **Platform/software/code security, inherited problems, will it be solved during 5G**

- **Intelligent reflective surface (eavesdropping), how to make it more secure**

- **AI/ML will play a major role both in link and system level optimisation of 6G wireless networks -> threat analysis, prevention, identification and mitigation**

Large Antenna Arrays for Massive MIMO

Meta Materials Based Large Intelligent Surface

Visible Light Communication

THz Communication

INDOOR COMMUNICATION

Orthogonal Multiple Access

Frequency, Time, Code

Frequency, Time, Code

IoT Nodes

Wireless Energy Transfer

6G and Post-Quantum Cryptography

Post-Quantum Cryptography

- **Quantum computer can become a reality**
  - **Symmetric crypto is OK**
  - **RSA is vulnerable to factorization**
- **NIST PQC standards competition -> standard will be ready in 2024**
  - **Implementing these in different systems will be a huge challenge for the latter half of 2020s**

- **Both encryption (through key exchange) and authentication (digital signatures) are in danger from quantum computers**
- **Currently quantum computers have some dozens of qubits and can not yet solve cryptographic problems**
- **To be effective in solving cryptography, quantum computers need qubits in the order of millions (based on current state of the art)**
- **When will we have such quantum computers?**

Further information in Youtube: 6G Flagship Webinar on Fundamental Research Challenges for Trust, Security and Privacy:
https://www.youtube.com/watch?v=rcEvAOnzuhQ

- **Analyzing 6G security threats, developing the use cases and security datasets for embedded security in 6G network.**

- **6G network security architecture models on the embedded trust for increased level of information security in 6G.**

- **Modeling trust network, analyzing the foundational technologies and requirements for enabling trustworthy networking in 6G.**

- **Privacy preservation and requirements in 6G networks. Collaboration on global standardization (e.g. ITU) for 6G security.**

- **Bilateral collaboration for sharing, promotion and dissemination of joint research project outcomes, information sharing on Korea-Finland 6G security trends and activities.**

Thank You!