Post-Quantum

Cryptography Conference

Challenges for the Post-Quantum Transition of Mobile Ecosystems

Gustavo Banegas
Cryptographer at Qualcomm

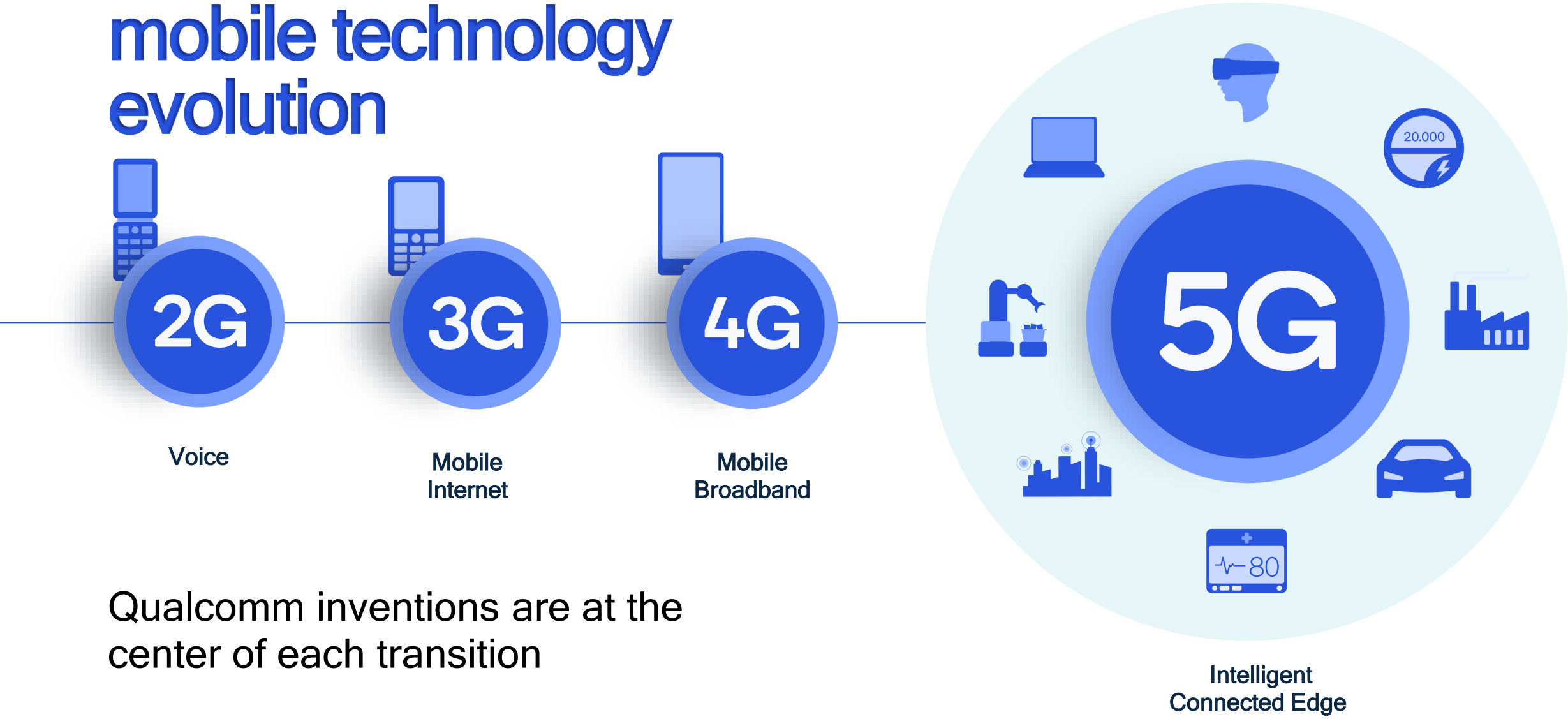
Qualcomm

Challenges for the post-quantum transition of mobile ecosystems

Gustavo Banegas - gsouzaba@qti.qualcomm.com
Florian Caullery - fcauller@qti.qualcomm.com

1. Introduction
2. SoC basics
3. Implication of the transition on chip architecture
4. Solution exploration
5. Conclusion

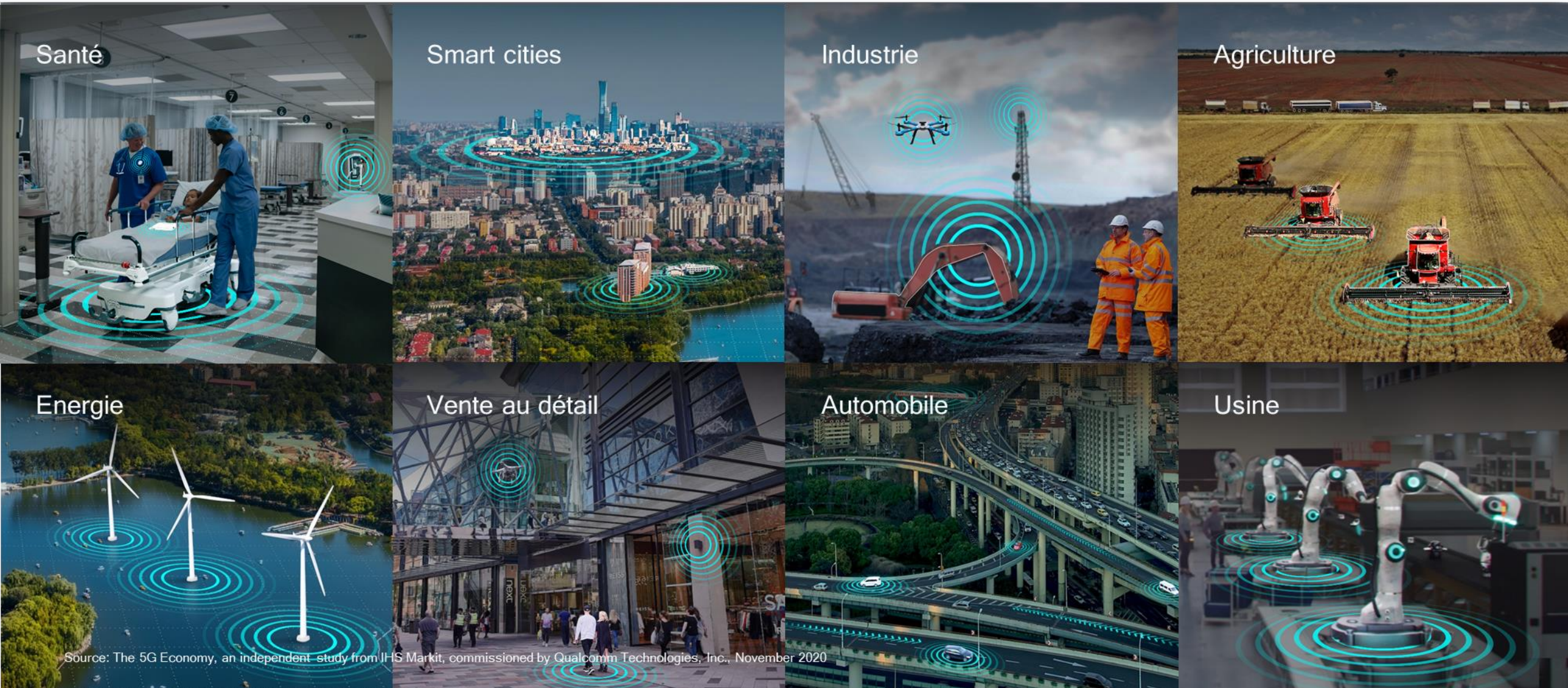
We drive mobile technology evolution



Qualcomm inventions are at the center of each transition

Driving digital transformation across industries

5G will enable approximately €10 trillion of global sales activity in 2035



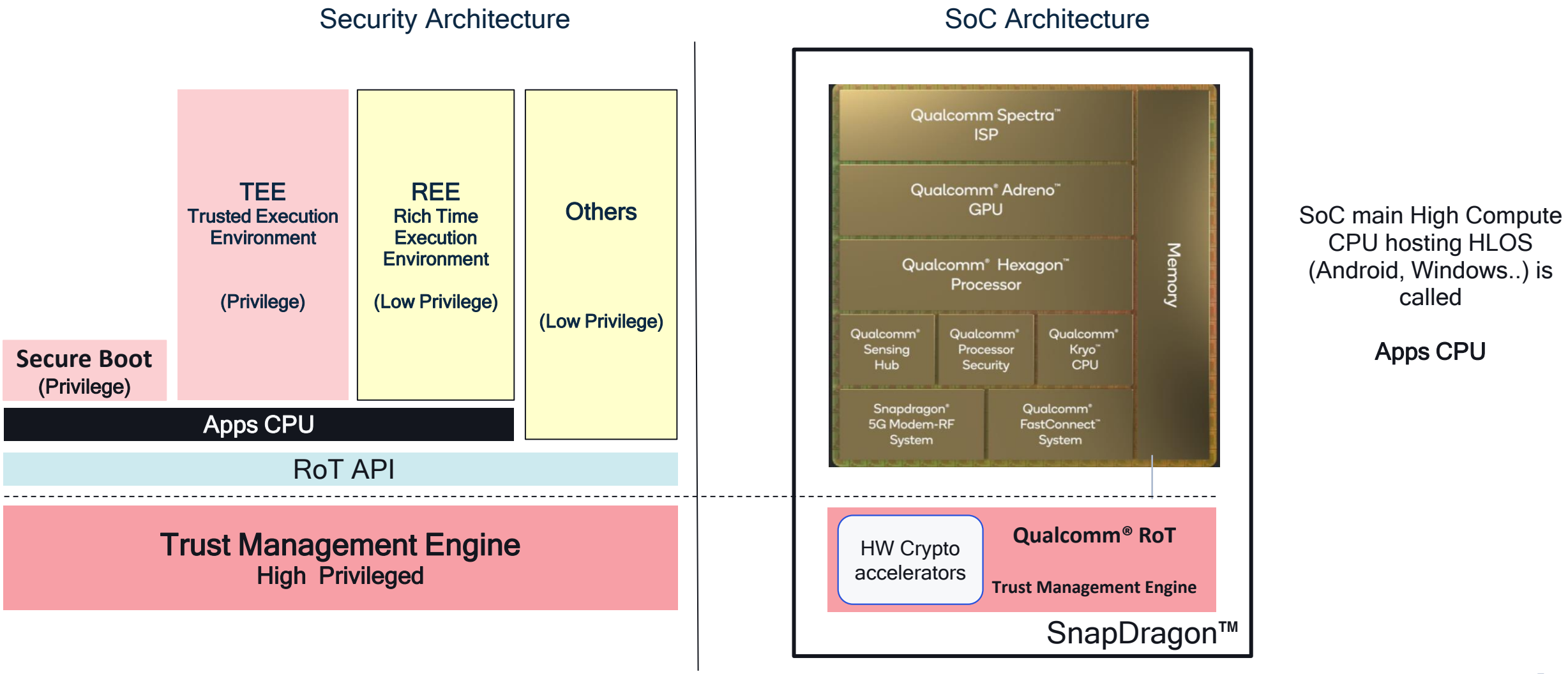
Source: The 5G Economy, an independent study from IHS Markit, commissioned by Qualcomm Technologies, Inc., November 2020

Qualcomm and the transition to post-quantum cryptography

- Snapdragon™ Qualcomm® flagship System on Chip (SoC) is deployed in a broad range of products across multiple markets (Mobile, Compute, Automotive, IoT…)
- Fast progress on Quantum Computing will jeopardize most of public key cryptography based systems pushing the world to organize the transition to Quantum-resistant algorithms
- Current consensus is that standard public key cryptography could become vulnerable in early 2030
- Device with long lifecycle are at particular risk so Governments and Industries are now organizing the transition to Post Quantum Cryptography (PQC)
- Qualcomm® is devoting significant resources to address this problem as it has the potential to negatively impact the chip market
- Our goal today is to highlight challenges on mobile environment that we need to address and give new insights on PQC transition

Qualcomm and the transition to post-quantum cryptography

The anatomy of a System on Chip

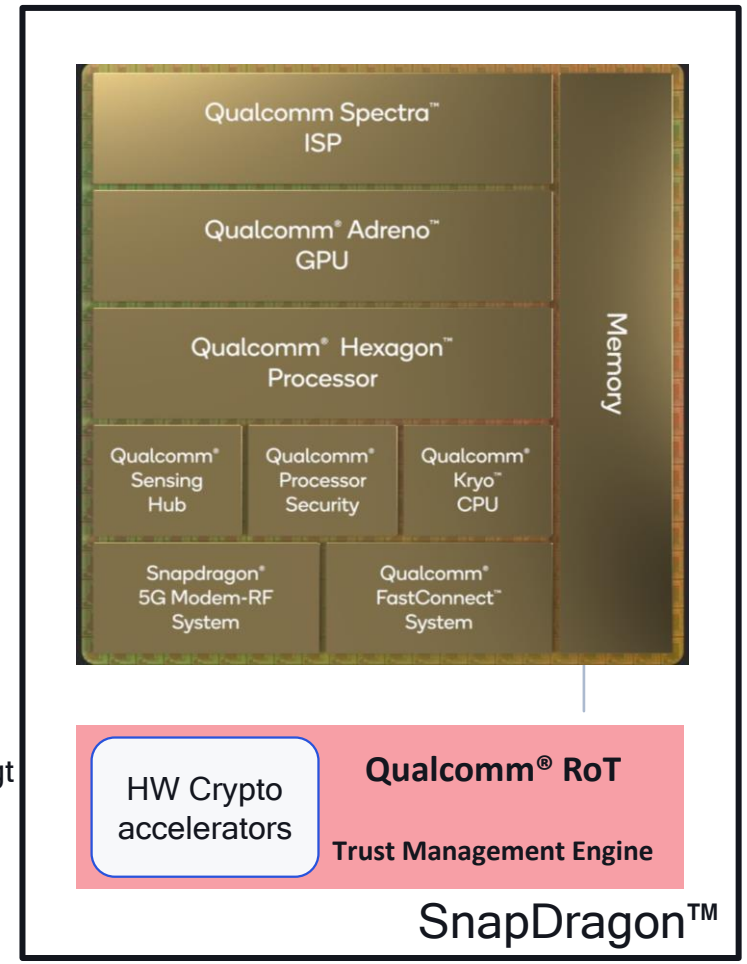


SoC main High Compute CPU hosting HLOS (Android, Windows..) is called

Apps CPU

Qualcomm and the transition to post-quantum cryptography

The anatomy of a System on Chip



RoT functions

- Lifecycle Mgt
- Key Mgt
- Crypto

Criteria / Crypto Processing	Performance / Cost	CPU Offload/Power	Security and Integrity	Agility
App CPU based	Yes	No	No: Key exposure	Yes
HW Crypto Accelerators /Co-processor	Implementation Dependant	Yes	Enabled	Limited

Security Mandate dedicated HW Crypto Accelerator / coprocessor approach

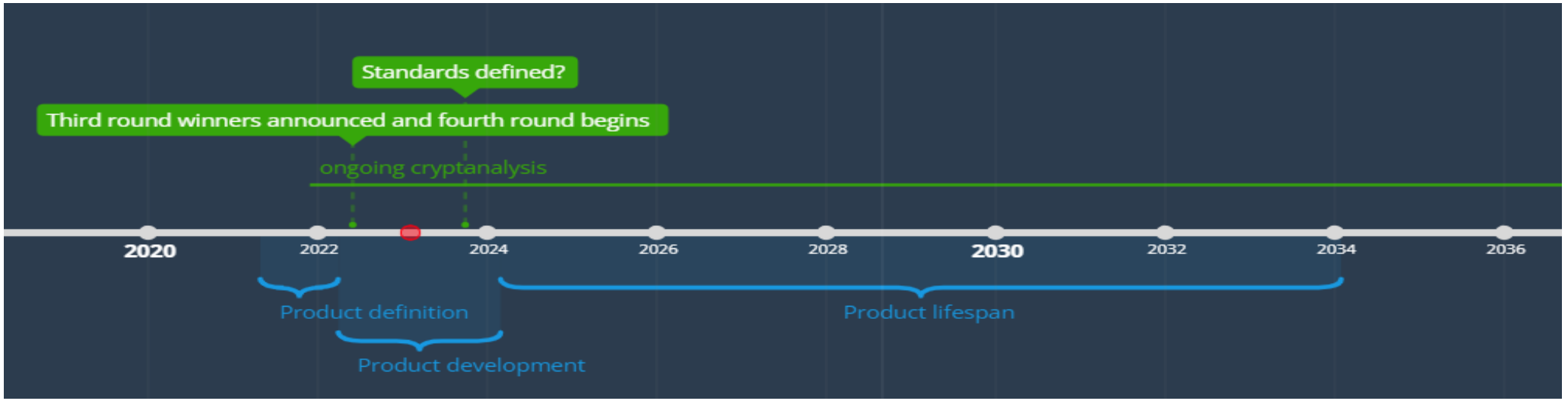
What are the PQC standards and candidates?

- Officially we have:
  - From Lattice-based:
    - Kyber (KEM)
    - Dilithium (Signature)
    - Falcon (Signature)
  - From Hash-based:
    - SPHINCS+

- For the next round:
  - Classic McEliece
  - Bike
  - HQC
- The new call for signatures (2023)

Qualcomm and the transition to post-quantum cryptography

How do we build a quantum resistant crypto accelerator ?



Crypto-agility is not an option, it is a requirement

Other principal differences:

- Public keys are at least 3 times bigger
- RAM requirement is higher
- Hybrid mode

Qualcomm and the transition to post-quantum cryptography

Implications on architecture

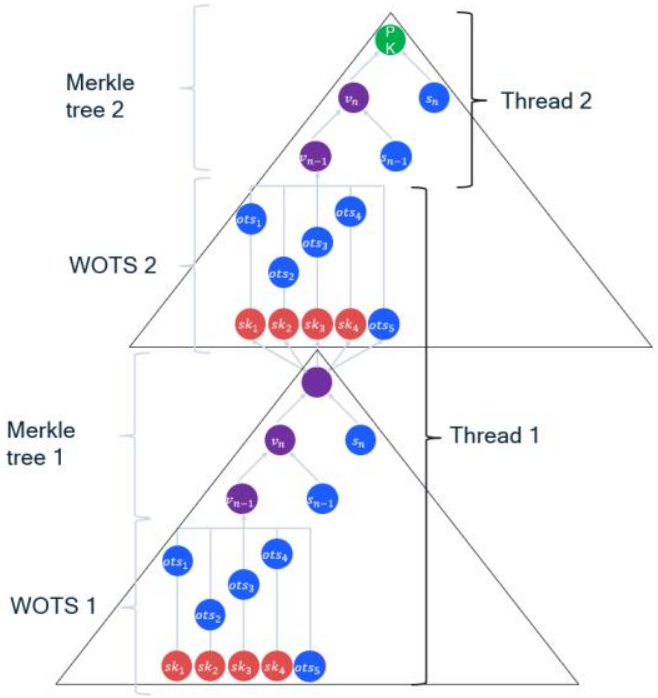
Properties / Crypto Processing	Agility	Performance / Cost	CPU Offload / Power	Security and Integrity
HW Crypto Accelerators /Co-processor	Limited	Implementation Dependant	Yes	Enabled: Key storage + SCA protection
PQC requirements	Mandatory	• High RAM • High throughput	CPU based	• SCA not well understood • Big keys
Implication on Architecture	Needs CPU	Needs a dedicated CPU architecture	Needs separation from Apps CPU	Needs: • Key isolation • SCA protection

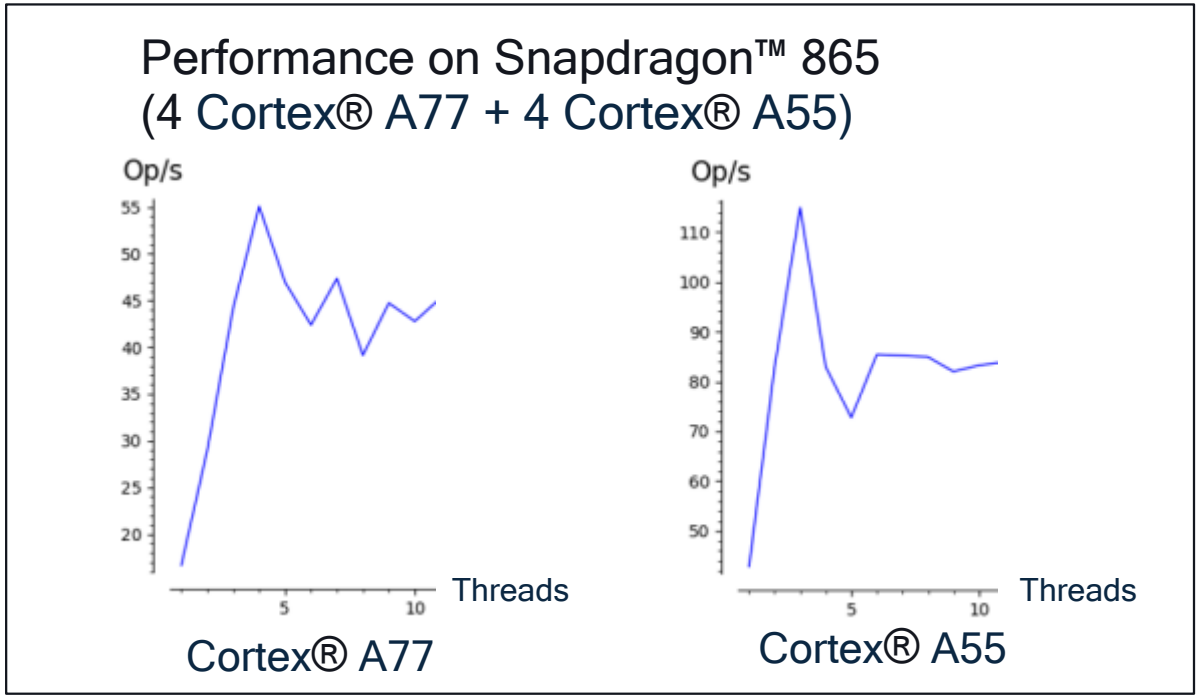
Solution exploration: Multithreading

Using multiple cores

Agility	Performance / Cost	CPU Offload / Power	Security and Integrity

- **Addressing performance issues by leveraging multiple cores available in the Apps CPU**
- We implemented **SPHINCS+** with a multithreaded version that uses all available CPU cores and obtained a speed-up of up to 3 times compared to single-threaded
- SPHINCS+ is easily parallelizable but other schemes could benefit from the approach



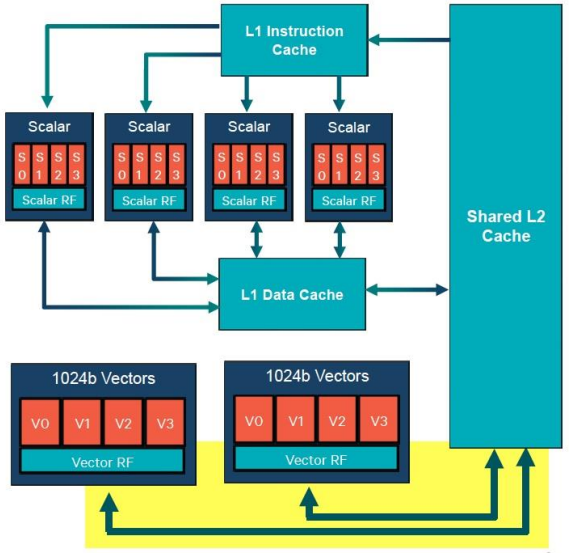


Solution exploration: DSPs

Using DSPs

Agility	Performance / Cost	CPU Offload / Power	Security and Integrity

- **Addressing CPU offload and power efficiency by leveraging other processing units in the SoC**
- **DSPs** seem to be ideal target for lattice-based schemes as the **NTT** is a variant of the **FFT** and it operates over 1024b long vectors



- The high level of parallelism can also be used in HBS and CBC

- We implemented **Dilithium** on our Qualcomm® Hexagon™ DSPs using HVX intrinsics in C

```
HVX_Vector butterfly4a;
HVX_Vector butterfly4b;
HVX_Vector zetas_rd4a;
HVX_Vector zetas_rd4b;

//Shuffling vectors
butterfly4a  = Q6_V_vdelta_VV(*a, controls_v[0]);
butterfly4b  = Q6_V_vdelta_VV(*b, controls_v[0]);

//Perform multiplication
*a = Q6_Vw_vadd_VwVw(montgommery_vector_multiplication(butterfly4a, zetas_rd4a), *a);
*b = Q6_Vw_vadd_VwVw(montgommery_vector_multiplication(butterfly4b, zetas_rd4b), *b);
```

- We were able to reach the same performance than on an ARM Cortex® A-77 on Snapdragon™ 865 for the NTT
- **Several academic articles also have explored the usage of GPUs**

Conclusion

- This presentation intends to emphasize:
  - The need to offload PQC computation from the application high performance CPU unit for security reasons
  - The need for crypto agility in the design of any PQC co processor

- Consequently, PQC is opening a wide range of options for co-processor designs, making it hard to select the best solution

- Ensuring Confidentiality and Integrity of the key materials against SW and Physical Attacks is the biggest challenge

- Qualcomm® is also involved in creation of new PQC standards: one of our member is one of the co-authors of the *Wave* signature scheme that will be proposed in the new NIST signature call.

Thank you

Qualcomm

Follow us on:

For more information, visit us at:

qualcomm.com & qualcomm.com/blog

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia