World Federation of Scientist'
Information Security Permanent Monitoring Panel (PMP)

# Plenary Session of the International Seminar on Planetary Emergencies: The Future of Cybersecurity

August 22rd 2019
Erice (Italy)

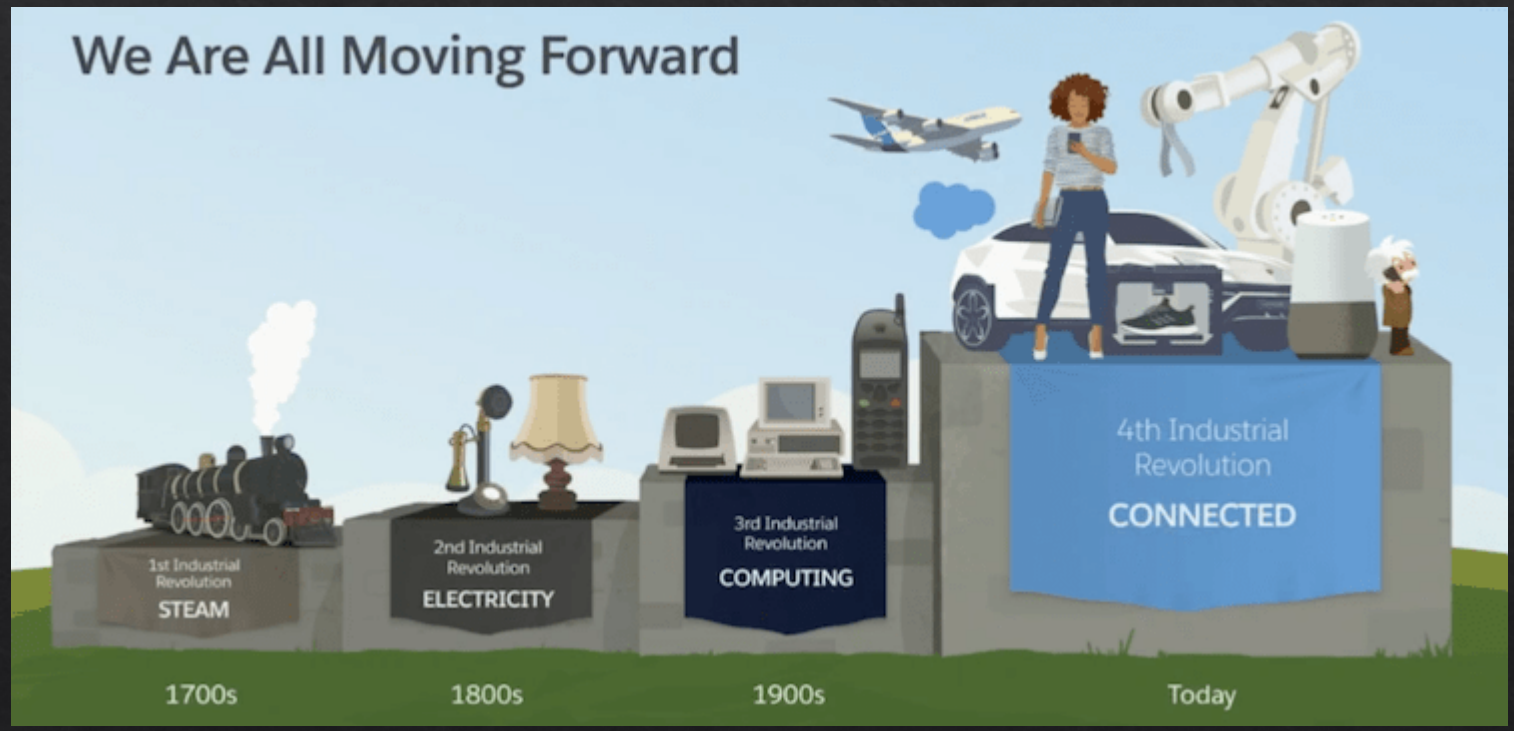
Alexander Ntoko
Chief, Operations & Planning Department
International Telecommunication Union (ITU)
Geneva, Switzerland

# Agenda

1. The 4th Industrial Revolution
2. Overview of Blockchain
3. Overview of Quantum Computing and Quantum Cryptography
4. Quantum Computing in the Blockchain Environment
5. Future of Quantum Computing
6. ITU's Contribution in the Field of Cybersecurity and Quantum Computing

# 4th Industrial Revolution

An Overview of the transition from 1st to 4th Industrial Revolution:




Source: Salesforce.com

The 4th Industrial Revolution (4IR) definition by Klaus Schwab

*"A technology revolution where the fusion of technologies blurs the lines between physical, digital and biological spheres"* - Klaus Schwab

The technologies of the 4IR include among others:

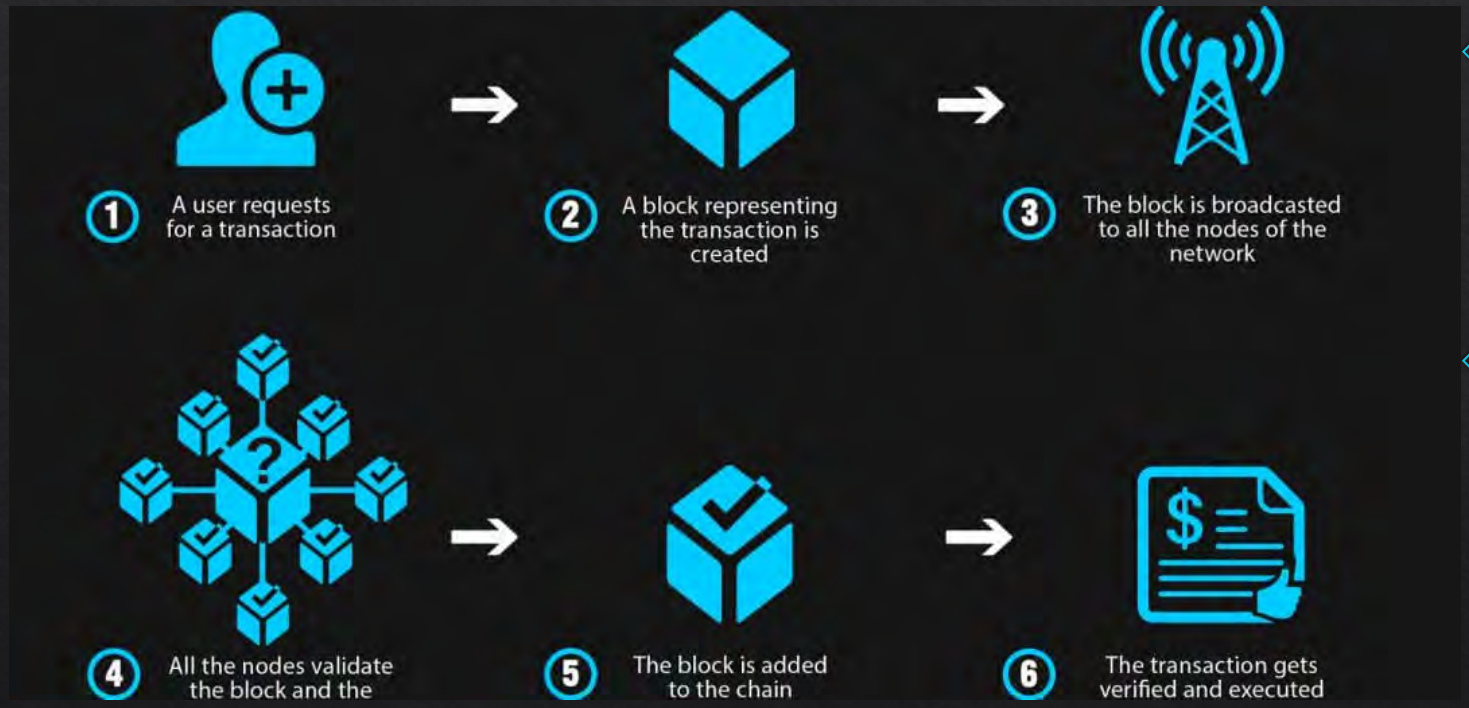
- Artificial Intelligence (AI)
- **Blockchain**
- Cloud Computing
- Nanotechnology
- **Quantum Computing**
- Virtual/Augmented Reality
- Biotechnology
- Robotics
- Autonomous vehicle
- 3D printing
- 5th Generation Cellular Network Technology (5G)
- Internet of Things
- Material Science
- Energy Storage

Source: World Economic Forum, Salesforce.com

# Overview of Blockchain - Features

- **No** official trusted third party
- In “permissionless” blockchains, parties to transactions can be pseudonymous and recognize each other via *public key cryptography*
- Pseudonymous blockchains are the basis of cryptocurrencies like Bitcoin where all money transfers are outside of any government oversight
- Platforms such as Ethereum permit self-executing (“smart”) contracts

# Overview of Blockchain - Features




Digital, decentralized, distributed ledger that can store any type of data

- Maintained collectively by users around the globe, rather than by one central administration
  - Transactions are grouped into a **block**
    - User computers are the "witnesses" of transaction
- Decisions to add an entry (**block**) are made by consensus
  - Once the solution is *approved by 51% of the members*, it is added to the communal ledger
    - If approved, blocks are "hashed"
  - Integrity of the ledger can be checked by anyone by running a hashing calculation
  - Content in recorded block can never be changed or hidden

# Overview of Quantum Computing and Quantum Cryptography

- Discipline that develops computer technologies based on quantum theory, where information is described in subatomic particles using (2) key properties (superposition and entanglement)

- **Key properties**
  - Superposition: particles can exist in **more than one state** at the same time
  - Entanglement: entangled **particles are correlated** to one another (mutual relationship or connected)such that **any action** performed **on one particle** will **affect the other**, **regardless of distance** separating them

- Quantum Computing performs computations in drastically less steps, stores a huge amount of information using less energy and provides secure communication

# Overview of Quantum Computing and Quantum Cryptography

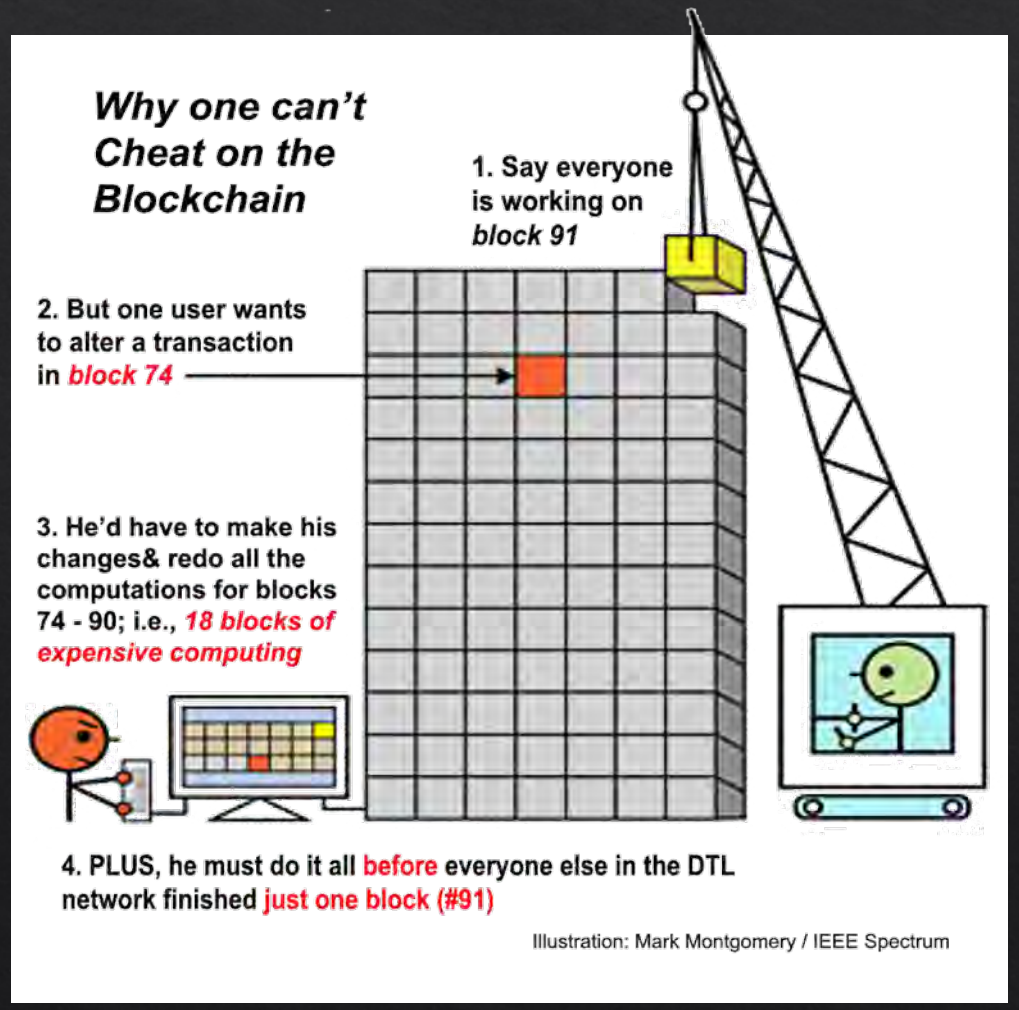
*Improving Data & Information Security*

- **Stronger Encryption**
  - quantum properties improve generation of random number used for encryption
  - snooping will invoke disturbance on particles state, changing the content of stored information
- **Eavesdropping Tamperproof**
  - no-cloning theorem states that it will be impossible for eavesdroppers to create a copy of the information sent using quantum computers if they don't know its content

# Quantum Computing Challenges to Blockchain

- **Security threats to blockchain applications**
  - private key in public key cryptography can be deduced
  - breaking of hash signatures using Shor's algorithm
  - speed of quantum computation could be used to take control of Blockchain network
- **Upgrading from Blockchain to quantum-resistant Blockchain**
  - updating from digital signature to a quantum-resistant scheme will need consensus
  - lost personal funds cannot be moved to quantum-resistant address & can be hacked

# Quantum Computing  Challenges to Blockchain




**Vulnerability in Digital Ledger Technology (DLT):**

A bad actor with a quantum supercomputer could engage in double spending (through ultra-fast transactions) of digital financial resources or block other transactions

# Blockchain *powered by* Quantum Computing

Improving Blockchain security using Quantum Cryptography

- Quantum Key Distribution (QKD) can be used instead of digital signatures to encrypt communication and make ledgers quantum-resistant
- QKD will be the first service used by the Quantum Communication Infrastructure in Europe

- **Quantum Blockchain** (by Ranjan & Visser)
  - **R**epresent transaction records in chronological order using Quantum particles
  - Quantum Internet would be required to run Quantum Blockchain
  - **Address scalability issues with current block chain:** bypasses some computationally intensive steps of verification and consensus, blockchain becomes invalidated as soon as hackers try to tamper with recorded blocks

# Future of Quantum Computing


- It is estimated that quantum computers will start going **mainstream in 5-10 years from now** [1]
- Pentagon sees quantum computing as the **next arms race**
- **Europe** had spent $1.2 Billion on Quantum Computing in 2016[2]
- **US** passed the National Quantum Initiative, which allocates $1.275 Billion to quantum research from 2019-2023[3]
- **China** is already working on building a $10 Billion quantum technology **lab**[4]

1) Source: IBM - https://www.research.ibm.com/5-in-5/quantum-computing/?source=post_page---------- ; Microsoft - https://www.barrons.com/articles/microsoft-we-have-the-qubits-you-want-1519434417?source=post_page----------
2) Source: https://www.nytimes.com/2018/10/21/technology/quantum-computing-jobs-immigration-visas.html?source=post_page----------
3) Source: https://www.forbes.com/sites/alexknapp/2018/12/20/congress-just-passed-a-bill-to-accelerate-quantum-computing-heres-what-it-does/?source=post_page----------#3706945c2ef8
4) Source: https://www.nextgov.com/emerging-tech/2018/07/pentagon-seeks-edge-quantum-computing/149718/
5) Source: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC110412/quantum_computing_report_v5.4.pdf

# Future of Quantum Computing

EU's future plan for a secure communication network:

- **EU Member States*** have signed a declaration agreeing on their **collaboration** to **explore, develop and deploy Quantum Communication Infrastructure (QCI)**** in Europe
- QCI will **integrate quantum technology** to:
  - secure critical infrastructure & encrypt systems against cyber threats
  - provide safe exchange of information & preserve privacy of government data
  - develop the future backbone of Europe's Quantum Internet

* As of July 2019, 10 countries have signed the declaration: Belgium, Germany, Italy, Luxembourg, Malta, Spain, Hungary, Portugal, Poland and the Netherlands

** QCI is part of the Quantum Technologies Flagship, a €1 billion, 10 year initiative launched by the European Commission in October 2018 pooling resources around a commonly agreed science and technology roadmap. Fields covered include quantum communication, quantum computing, quantum simulation, quantum metrology and sensing and the basic science behind quantum technologies

# Future of Quantum Computing

Future use of Quantum Computing & Blockchain by Department of Defense:

- July 2019, US Department of Defense (DOD) announced it is looking to develop **Blockchain cybersecurity shield** to:
  - enhance the authentication process of agents identity
  - enable secure messaging and process transactions between intelligence officers
  - create un-hackable codes that would secure internal databases
- **Quantum Computing** could be used to:
  - protect/encrypt critical DOD information and systems
  - provide competitive advantage over US adversaries

# Concluding remarks

- *One of the key mechanisms used to enhance online trust and security, is to rely on the current difficulties in breaking asymmetric cryptographic algorithms.*
- *This is mostly dependent on our knowledge of classical computing based on binary digits (bits).*
- *Quantum computing is still in its infancy and the quantum computing power needed to break current asymmetric algorithms might take some years to reach the general public.*
- *However, we have not always been very accurate in predictions especially in the domain of Computer Science.*
- *Developments in Quantum computing and Quantum cryptography need to be carefully monitored.*

# ITU's Contribution in the Field of Cybersecurity and Quantum Computing

ITU's work in Cybersecurity:

- **WSIS Action Line C5:** action plan aimed at building confidence & security in use of ICTs
- **ITU Plenipotentiary Conferences (2010, 2014, 2018):** strengthen the role of ITU in cybersecurity (use of ICTs, Global Cybersecurity Agenda…)
- **Global Cybersecurity Agenda (2007):** framework for international cooperation aimed at enhancing confidence and security in the information society
- **Global Cybersecurity Index (2018):** metric developed to measure cybersecurity capabilities of nation states
- **ITU-T Study Group 17 (SG17):** expert group coordinating security-related work

# ITU's Contribution in Cybersecurity and Quantum Computing

- **Quantum focused ITU technical report & standard (September 2018):**
  - 'Security framework for quantum key distribution in telecom network' (Report)
  - 'Quantum noise random number generator architecture' (Standard)
- **Quantum focused ITU standards with experts from ITU, ISO & ETSI (January 2019):**
  - 'Security Requirements for Quantum Key Distribution Networks – Overview'
  - 'Security Requirements for Quantum Key Distribution Networks – Key Management'
  - 'Use of cryptographic functions on a key generated in Quantum Key Distribution networks'
- ITU Workshops organized by SG13 and SG17 on Secure Quantum Communication nd Quantum IT for Networks
- Increase in quantum-specialized ITU members to 15 (currently: 7 companies and 2 universities are members)

# Thank You

alexander.ntoko@itu.int