



**gtd**

# Quantum & Blockchain Crossroads

La Próxima Infraestructura de Seguridad Digital

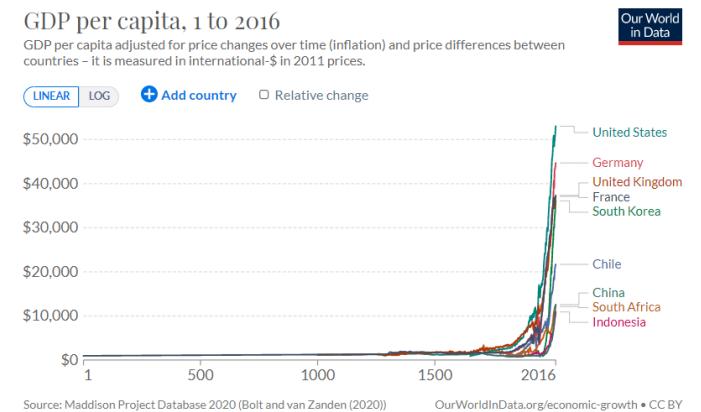
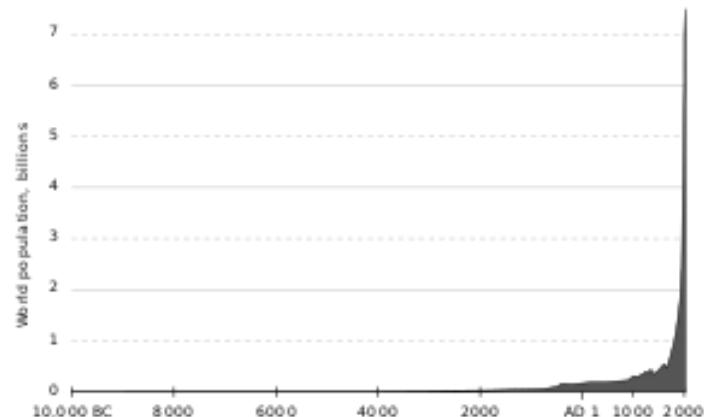
# Un mundo lineal ...



## Sources

Keidanren Sdgs  
<https://www.keidanrensdgs-world.com/society-5-0-jp>

Year	1400	1500	1600	1700	1800	1900	2000	2100
population (in billions)	0.35–0.40	0.43–0.50	0.50–0.58	0.60–0.68	0.89–0.98	1.56–1.71	6.06–6.15	10–13



United Nations  
<https://population.un.org/wpp/DataQuery/>

Maddison Project Database, version 2020  
<https://ourworldindata.org/grapher/maddison-data-gdp-per-capita-in-2011us-single-benchmark>



## Industria 1.0

- Mecanización
  - Motores  
(Vapor/Combustión)
- (1784)

## Industria 2.0

- Línea de Producción
- Producción en Masa
- Energía Eléctrica

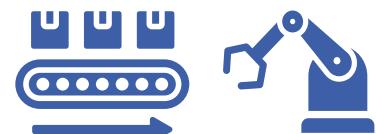


## Industria 3.0

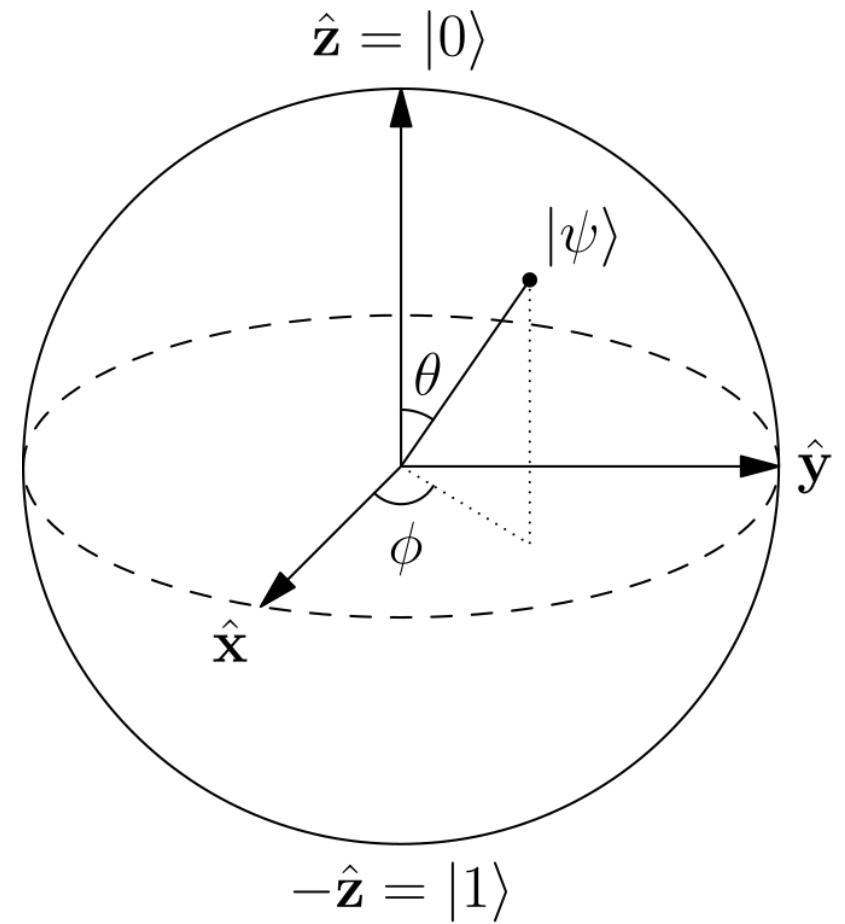
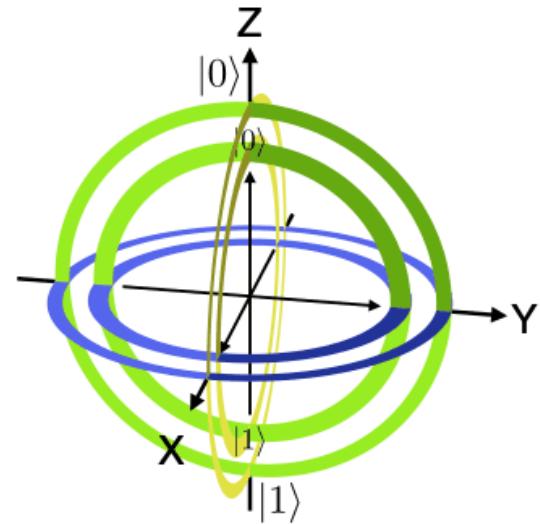
- Automatización
- Computadores  
y Electrónica

## Industria 4.0

- Sistemas ciber-físicos
- Internet de  
las cosas (IoT)
- Sistemas  
Autónomos



# Un tema de Escala ... y dimensiones

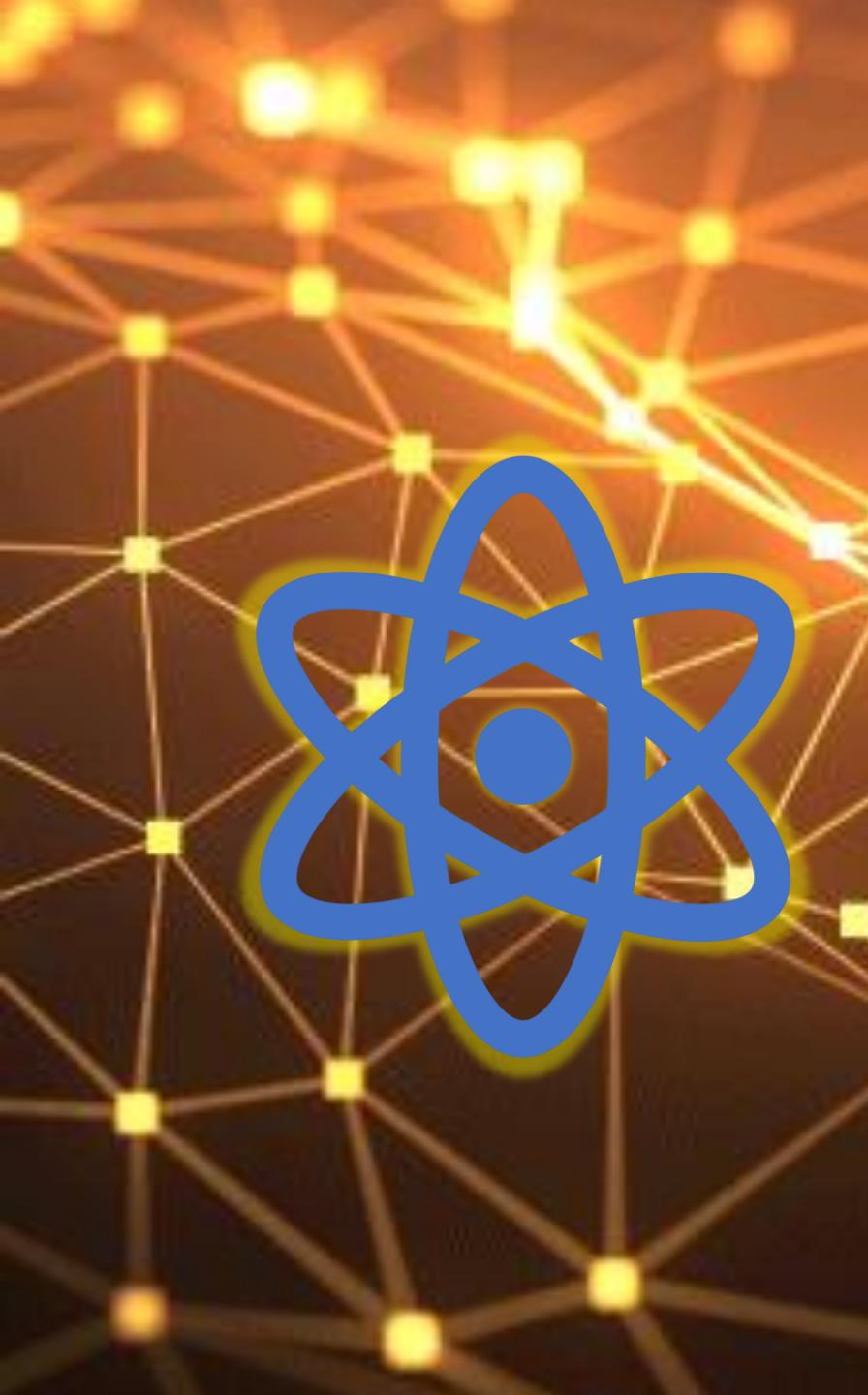


Bit :  $b \in \{0, 1\}$  and

Qubit :  $q \in \left\{ \alpha_0|0\rangle + \alpha_1|1\rangle \mid \alpha_0, \alpha_1 \in \mathbb{C} \text{ and } |\alpha_0|^2 + |\alpha_1|^2 = 1 \right\}.$



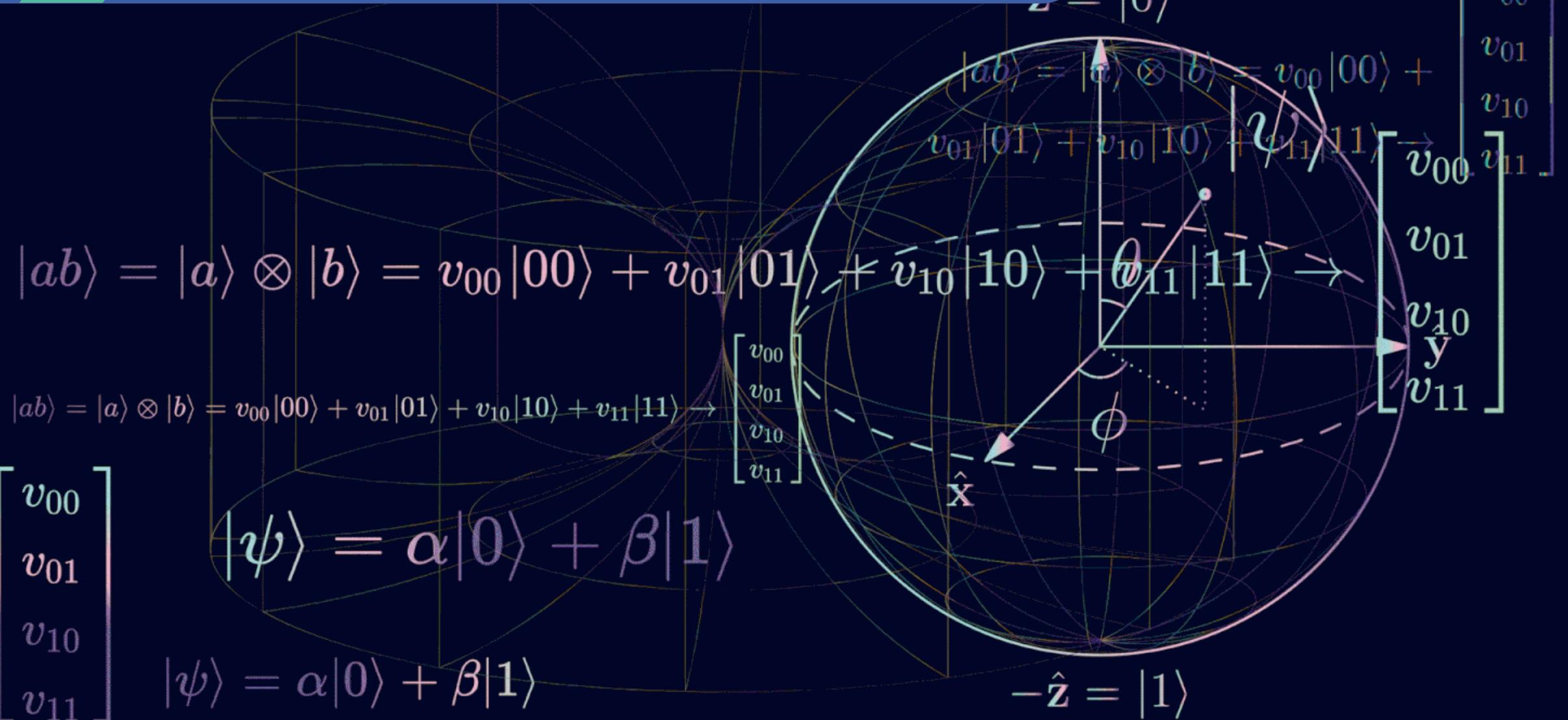
- DLT/Blockchain
- Inteligencia Artificial (AI)
- Metaverso (Augmented Reality)
- Quantum Technologies



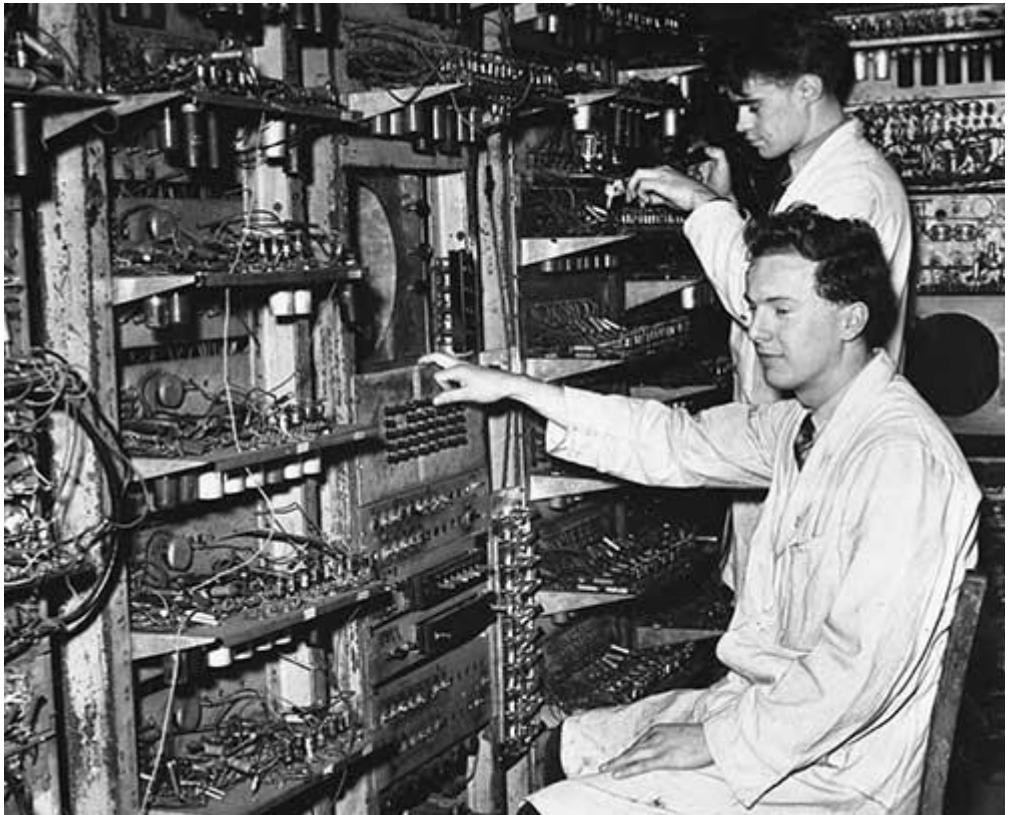
# Porqué Quantum Computing

- El 31% de los problemas complejos se abandonan debido al tiempo y los recursos necesarios para abordarlos
- El 81% de las empresas Fortune 500 tienen casos de uso para desarrollar en los próximos 3 años
- Tamaño del mercado de \$ 850 mil millones para 2040 (\* Investigación BCG)

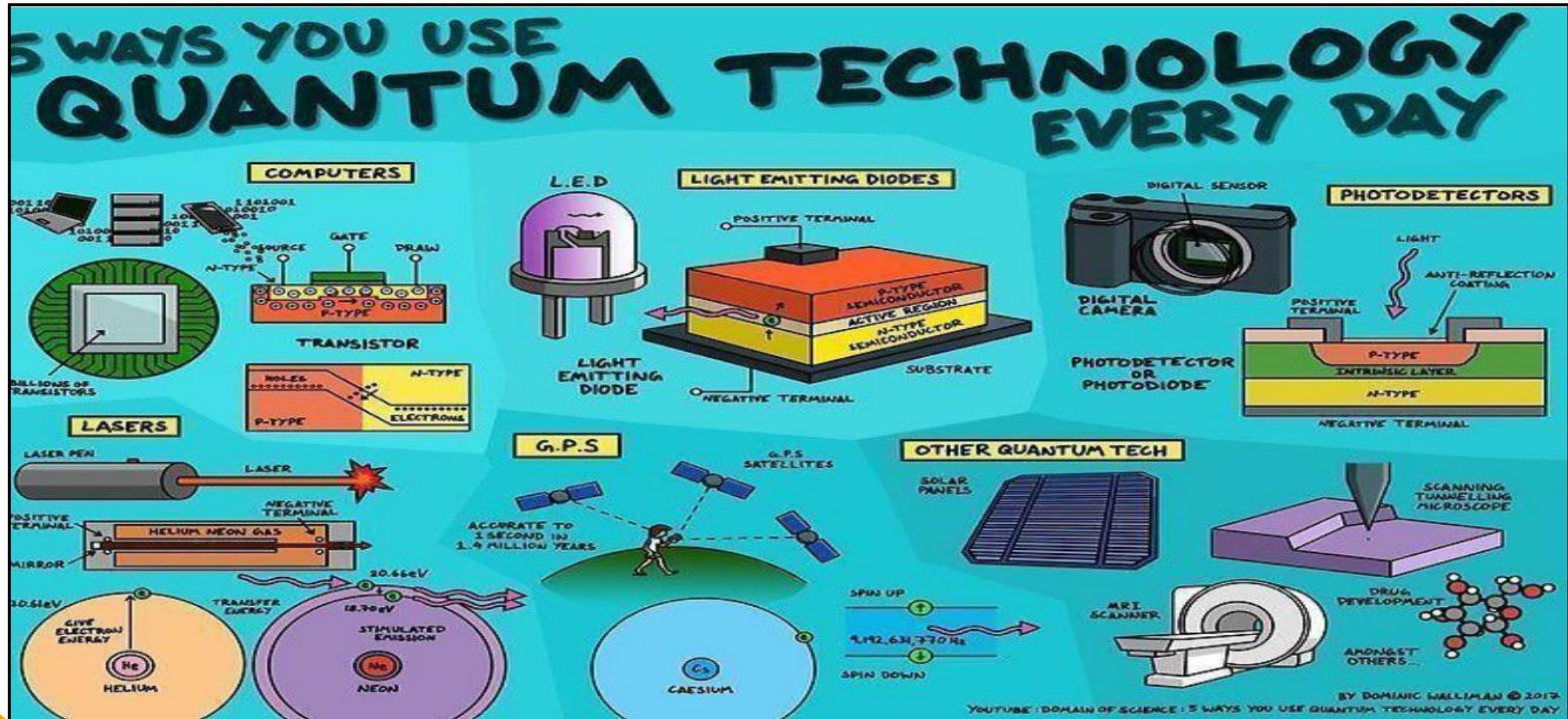
## La primera revolución cuántica cambió a la humanidad



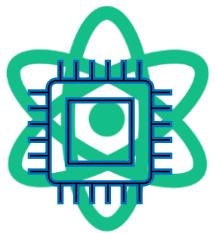
75 años de diferencia



# Tecnologías Cuánticas ya en uso

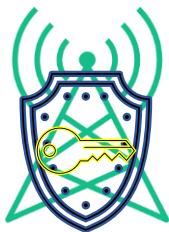


# Principales tecnologías cuánticas



## Quantum Computing

Provides computing power impossible and unimaginable for today's high-performance computers



## Quantum Communications

Ultra-secure communications, unhackable encryption mechanisms, known as post-quantum



## Quantum Sensing

High sensitivity and precision devices, taking advantage of the nature of subatomic particles

# Del laboratorio a Problemas reales



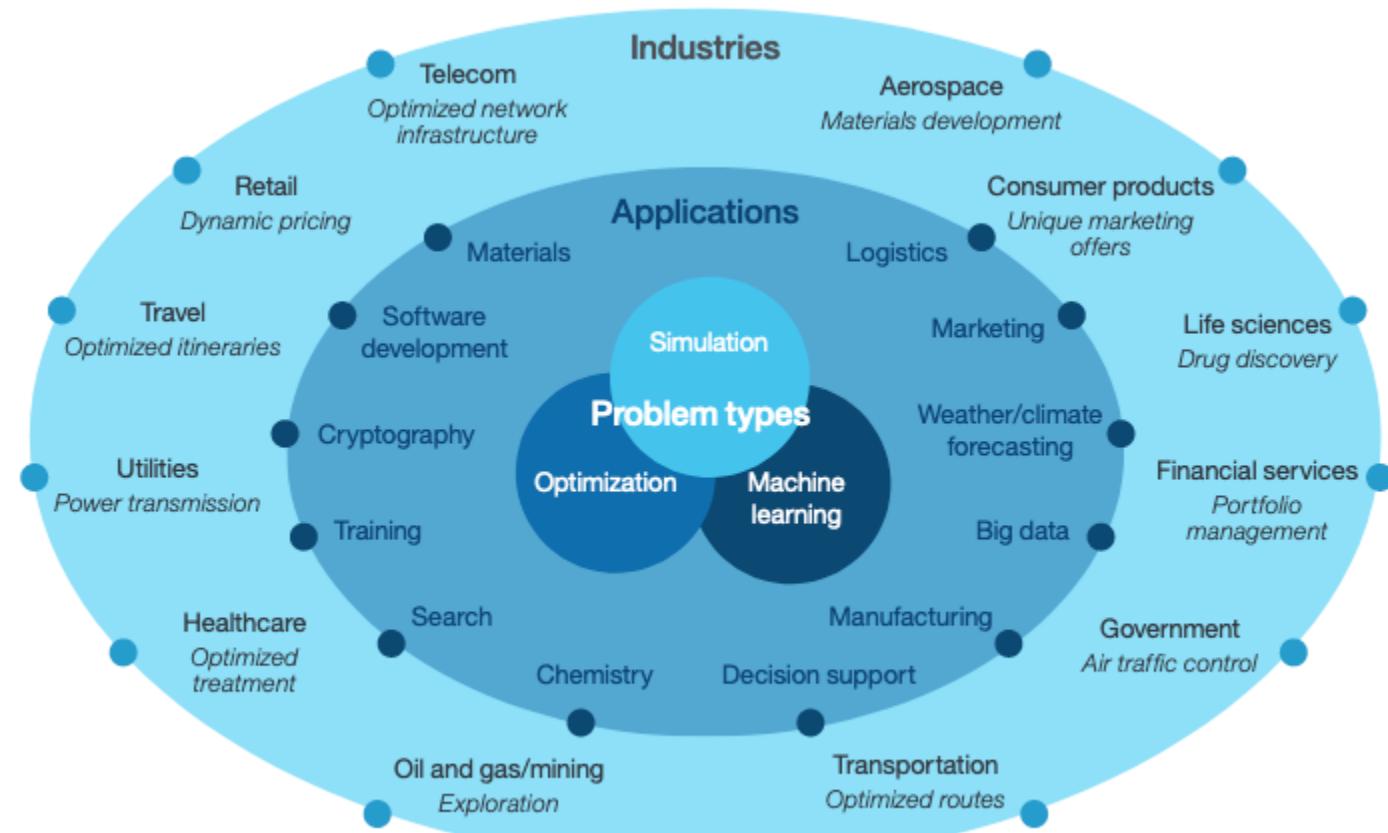
# Cómputo Clásico vs Cómputo Cuántico

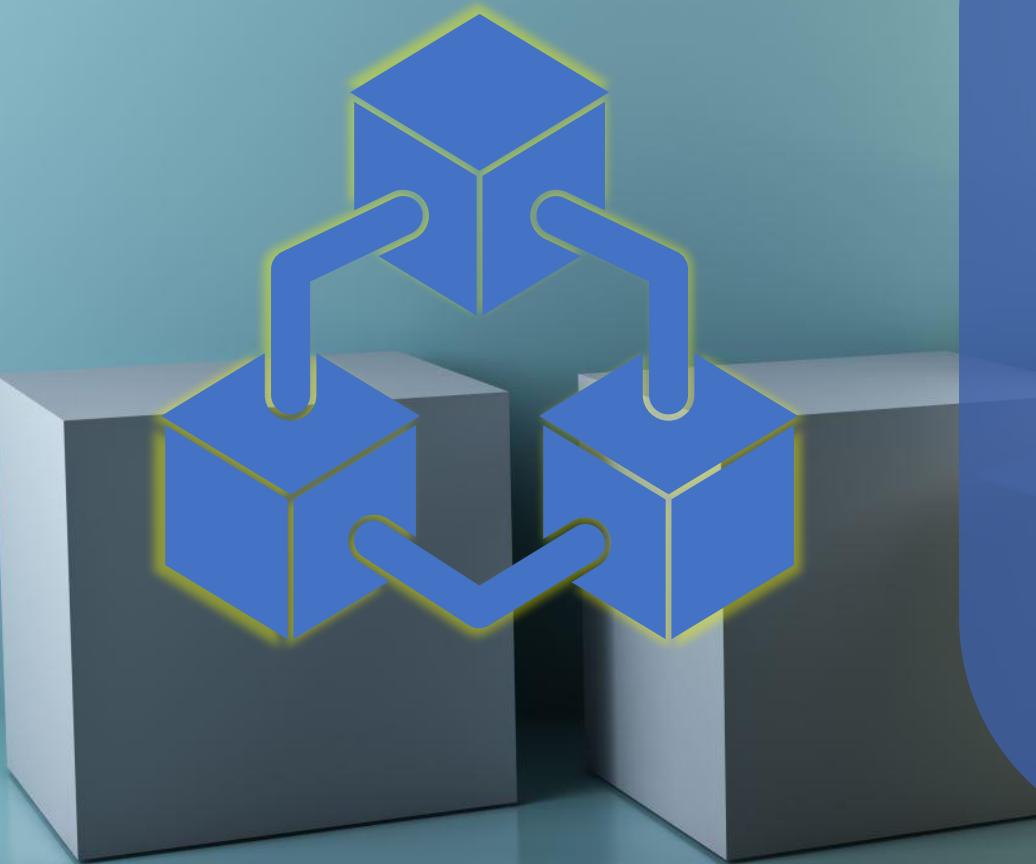
Clave de comparación	Computadora clásica	Computadora cuántica
Bases de la informática	Computadora multipropósito integrada a gran escala basada en física clásica	Computadora paralela de alta velocidad basada en mecánica cuántica
Almacenamiento de información	Almacenamiento de información basado en bits utilizando voltaje/ carga	Almacenamiento de información basado en Quantum Bit (QUBIT) utilizando giros de Electrones
Valores de bits	Los bits que tienen un valor de 0 o 1 y pueden tener un valor único en cualquier instante	Qubits que tienen un valor de 0 o 1, o pueden tener ambos valores al mismo tiempo
Número de estados posibles	El número de estados posibles es 2 que es 0 o 1	El número de estados posibles es infinito, ya que puede contener combinaciones de 0 o 1 junto con alguna información compleja

# Cómputo Clásico vs Cómputo Cuántico

Clave de comparación	Computadora clásica	Computadora cuántica
Producción	Determinista- (La repetición del cálculo en la misma entrada proporciona la misma salida)	Probabilístico- (La repetición del cálculo en estados superpuestos da respuestas probabilísticas)
Puertas utilizadas para procesar	Las puertas lógicas procesan la información secuencialmente, es decir, y, o no, etc.	<ul style="list-style-type: none"><li><b>Universal quantum gates:</b> IBM, Google, Intel, Rigetti Computing, D-Wave Systems</li><li><b>Adiabatic quantum computation (AQC):</b> D-Wave Systems, Fujitsu, IBM, Rigetti Computing</li><li><b>Quantum annealing:</b> D-Wave Systems, Fujitsu, Hitachi, IBM</li><li><b>Topological quantum computing (TQC):</b> Microsoft, IBM, Intel, Rigetti Computing, Xanadu</li></ul>
Alcance de posibles soluciones	Respuestas definidas y limitadas debido al diseño del algoritmo	Las respuestas probabilísticas y múltiples se consideran debido a las propiedades de superposición y enredos
Operaciones	Las operaciones usan álgebra booleana	Las operaciones usan álgebra lineal y se representan con matrices unitarias.
Implementación de circuito	Circuitos implementados en tecnologías macroscópicas (por ejemplo, CMO) que son rápidos y escalables	Circuitos implementados en tecnologías microscópicas (por ejemplo, resonancia magnética nuclear) que son lentas y delicadas

# Tipos de Problemas y Aplicaciones





# Porqué Blockchain

- Inmutabilidad, Trasparencia y Trazabilidad, como pilares de nuevos modelos de operación de la cadena de valor
- Creciente ritmo de adopción de la tecnología (las criptomonedas han acelerado el uso de las cadenas de bloques)
- Tamaño del mercado de \$ 220 mil millones para 2030 (\* globenewswire.com)

# Blockchain - Razones

Trust/Confianza

Estructura Descentralizada

Seguridad y Privacidad

Velocidad

Trazabilidad

Inmutabilidad



## The Properties of Distributed Ledger Technology (DLT)

### Programmable

A blockchain is programmable (i.e. Smart Contracts)

### Secure

All records are individually encrypted

### Anonymous

The identity of participants is either anonymous or pseudonymous



### Distributed

All network participants have a copy of the ledger for complete transparency

### Immutable

Any validated records are irreversible and cannot be changed

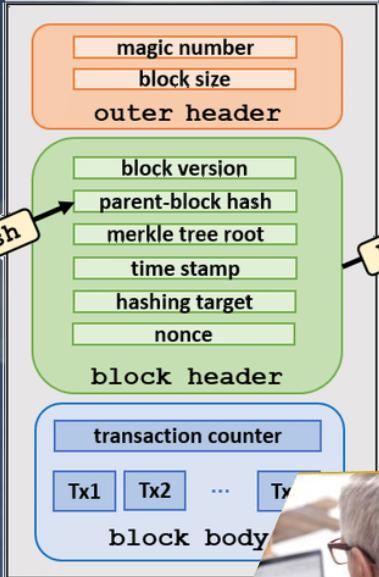
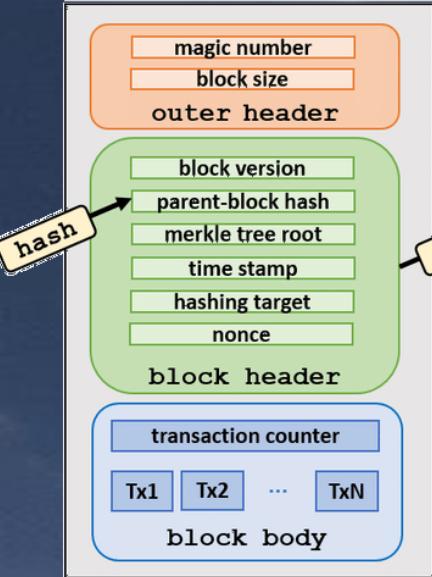
### Unanimous

All network participants agree to the validity of each of the records

### Time-stamped

A transaction timestamp is recorded on a block

# Blockchain (Cómo funciona)



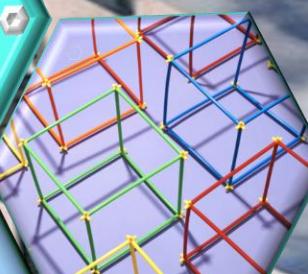
A quiere enviar un activo a B

El bloque se distribuye a toda la red

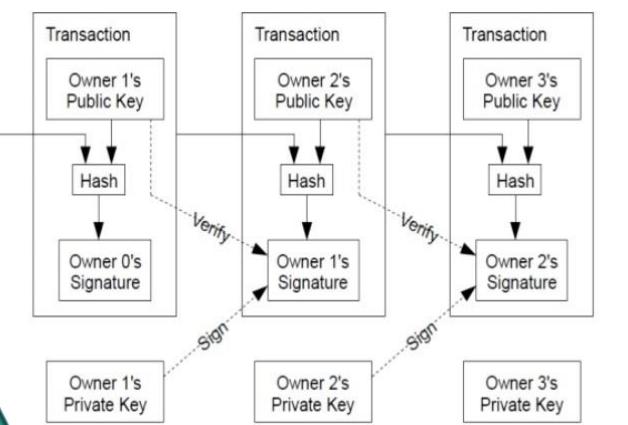
La transaccion se representa en linea como un bloque

La red aprueba la transaccion como valida

El bloque registra las validaciones y se agrega a la cadena de bloques



El activo se envía



# Tecnologías Blockchain ya en uso



Document properties

!invoice4.pdf

General Tags File properties

Document type

\* Document type  
INV Invoice

Documents in Egypt ACI envelopes are required to be tracked on blockchain.

Put document on blockchain (3.00 - v3)

Document properties

Document ID (optional)

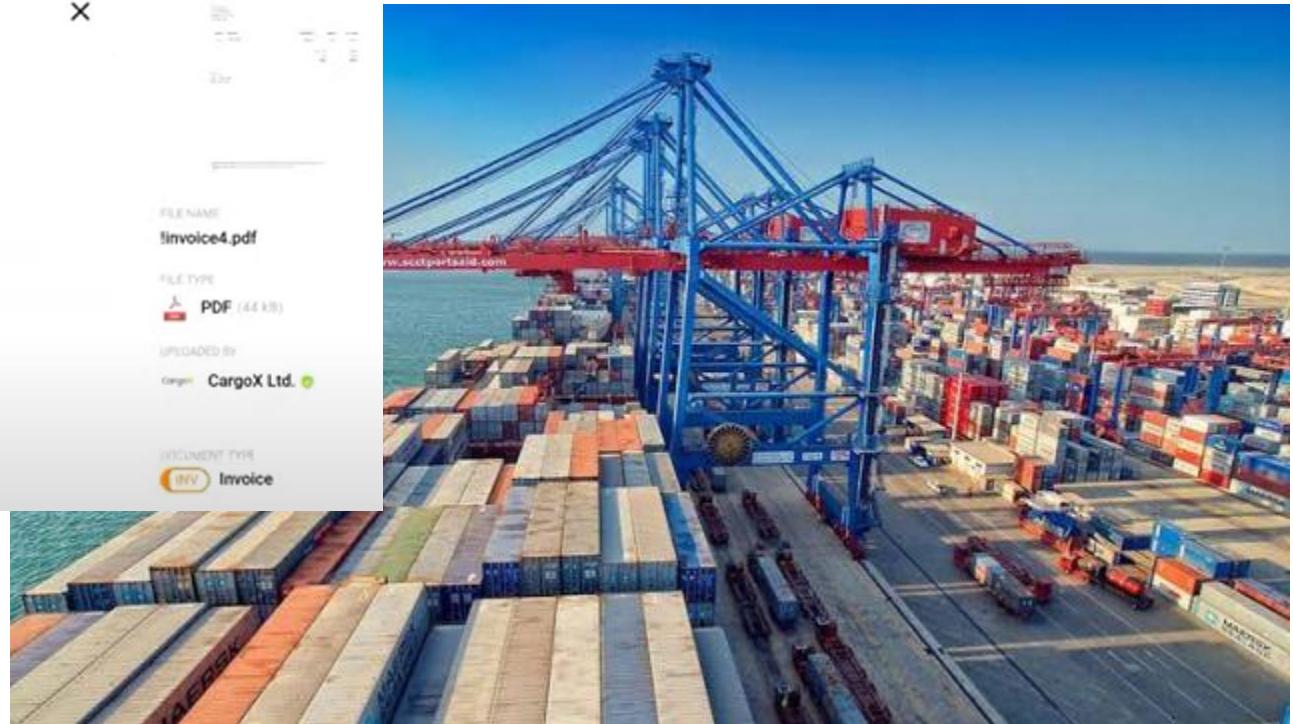
Document owner

FILE NAME !invoice4.pdf

FILE TYPE PDF (44 KB)

UPLOADED BY CargoX Ltd.

DOCUMENT TYPE INV Invoice

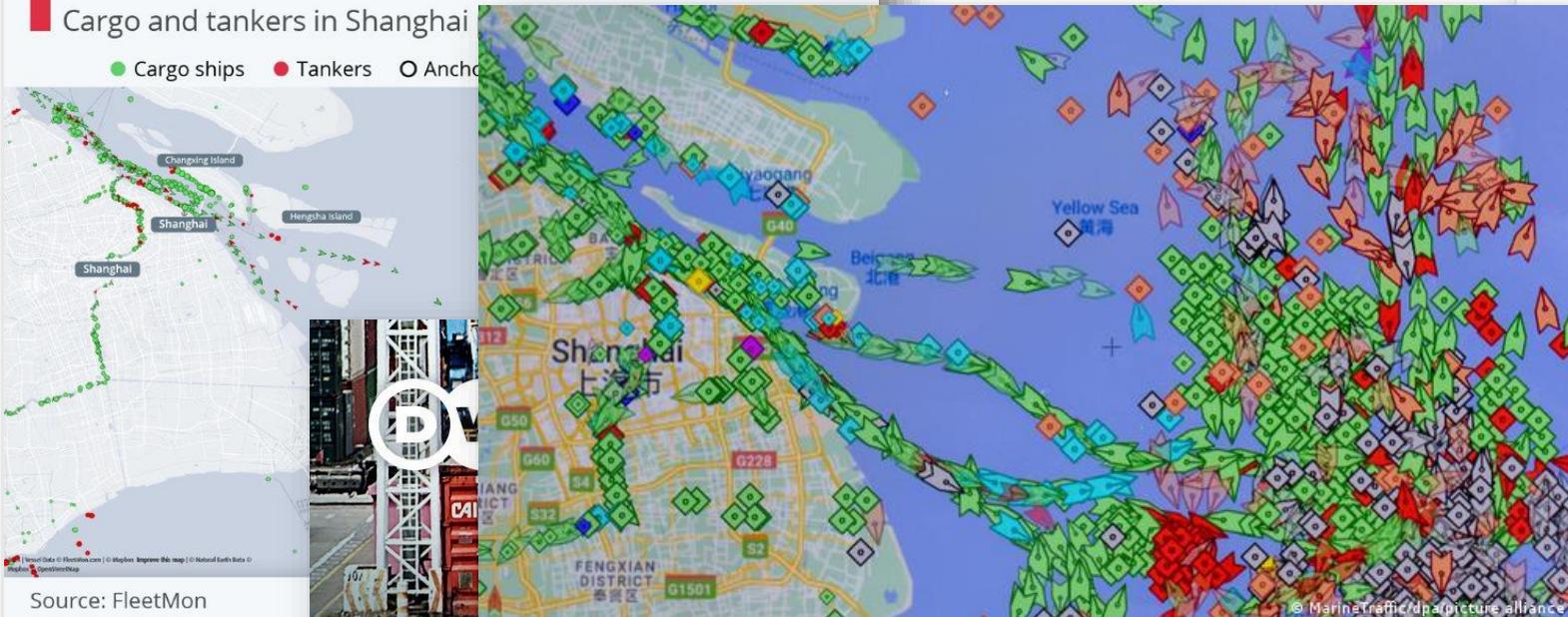


# Desafíos Actuales

## Shanghai Ship Jam Spells Supply Chain Trouble

Cargo and tankers in Shanghai

● Cargo ships ● Tankers ○ Anchored



Promedio de horas de espera en Shanghái para buques cisterna, graneleros y portacontenedores

2021 — 2022  
— Promedio de 2019 a 2022 ■ Rango de 2019 a 2022



China's lock shipping problems

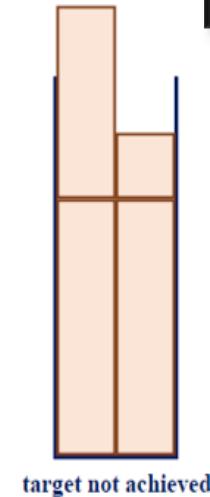
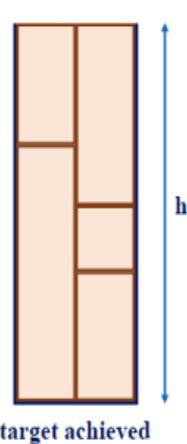
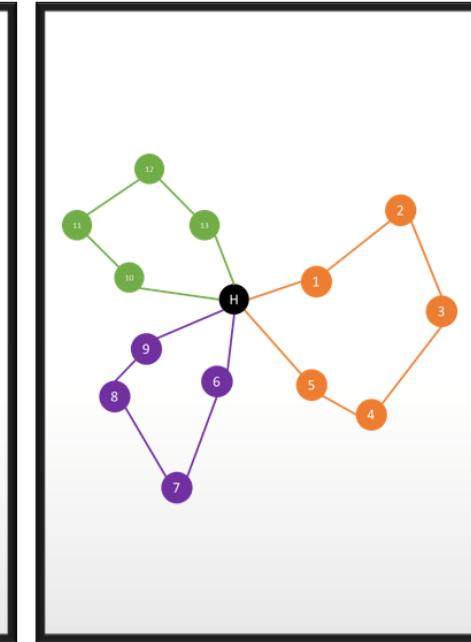
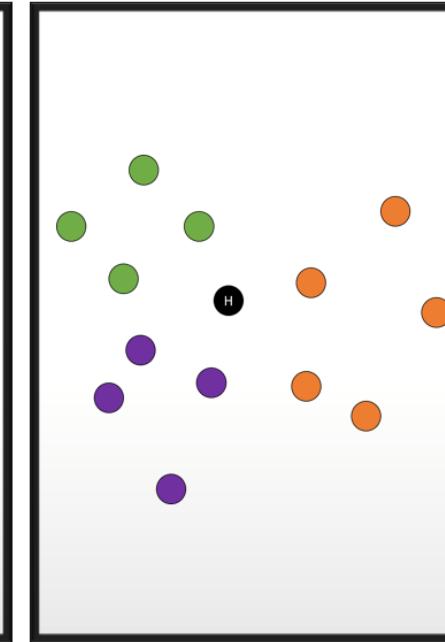
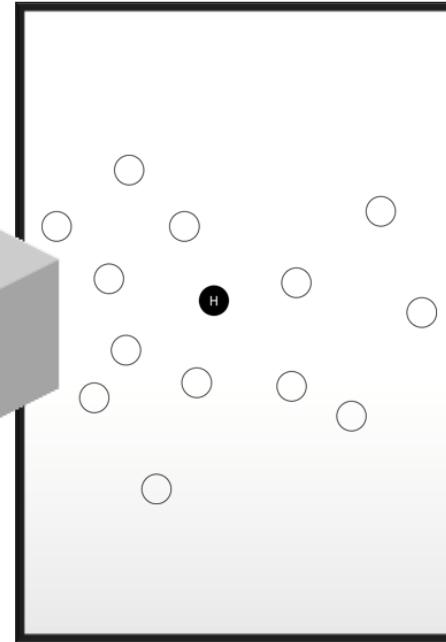
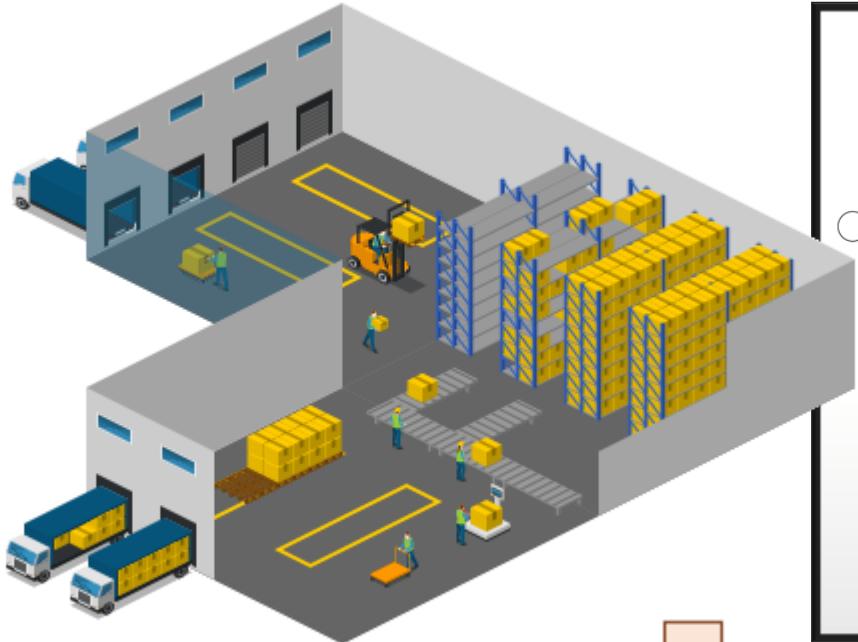
CIENTOS DE BUQUES A LA ESPERA DE CARGA Y DESCARGA EN EL PUERTO DE SHANGHÁI

# Tecnologías de la industria logística



- Logística/Flujo de materiales/Optimización de la línea de montaje
- Ciudades Sostenibles: Recolección de Residuos
- Enrutamiento de tráfico y optimización de señales de tráfico
- Programación/planificación de líneas aéreas, enrutamiento
- Problema de plataformas de trenes
- Planificación y Programación Portuaria
- Optimización de la cadena de suministro
- Optimización de Última Milla
- Programación del personal
- Optimización de la estación de carga de automóviles eléctricos

# Casos de Uso en Industria y Logística

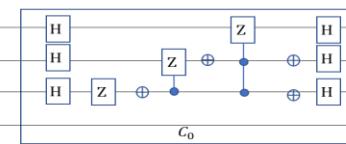
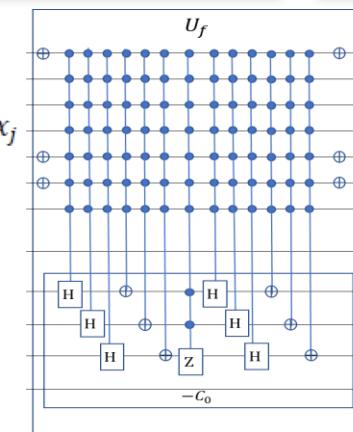


$$H_1 = \sum h(x)|x><x|$$

$$\text{where, } h(x) = n \sum_{u_j u_k \in \bar{E}} x_j x_k - \sum_{u_j \in V} x_j$$

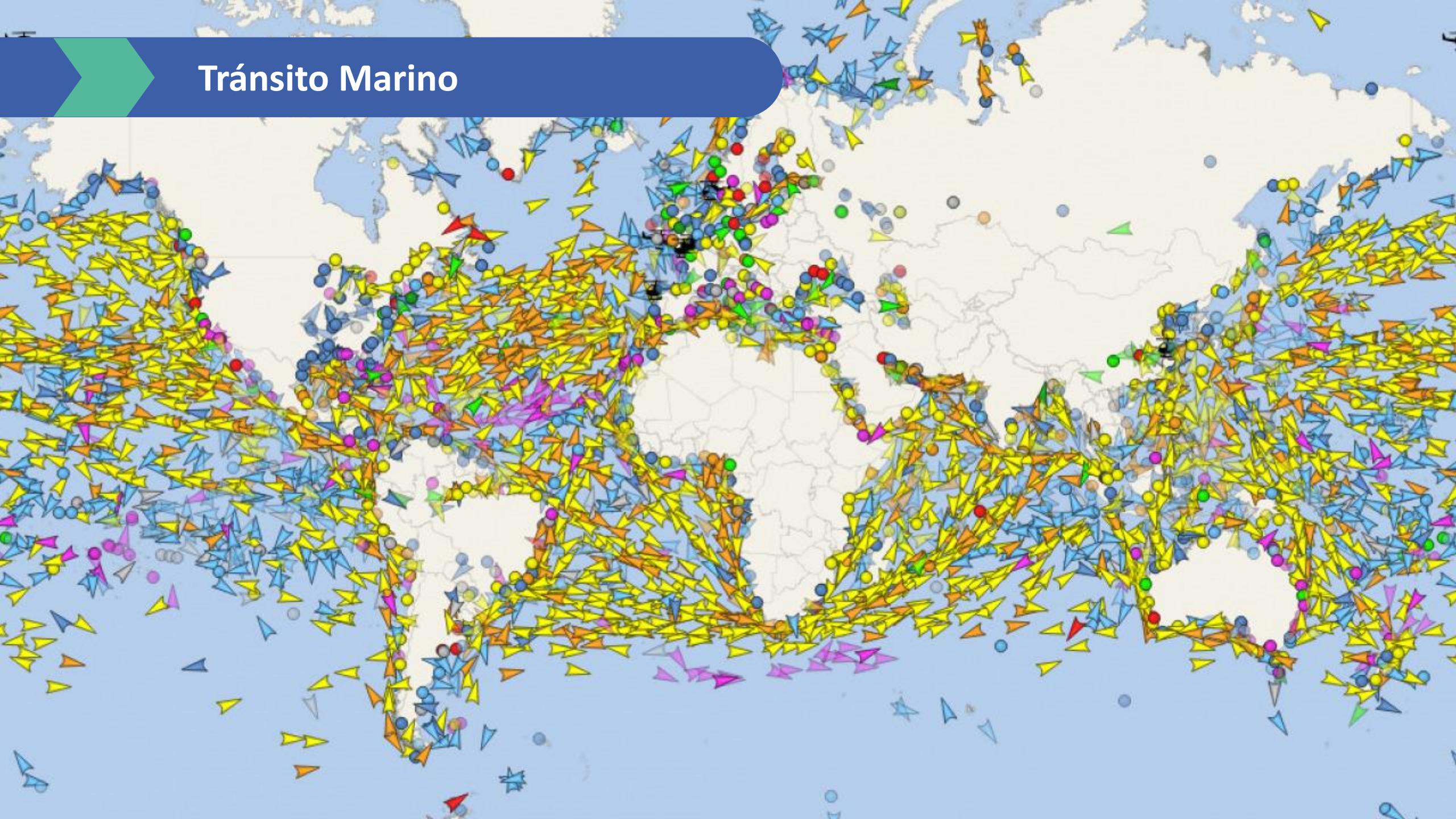
$$H_0 = I - |s\rangle\langle s|, \text{ being } |s\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$

$$H = (1-t)H_0 + tH_1$$



s  
|f(x)>  
c  
|0>

# Tránsito Marino



## Application and Presentation Layer

Smart Contract, Chaincode, DApps, UI

## Consensus Layer

PoW, PoS, DPoS, PoET, PBFT

## Network Layer

Peer-to-Peer

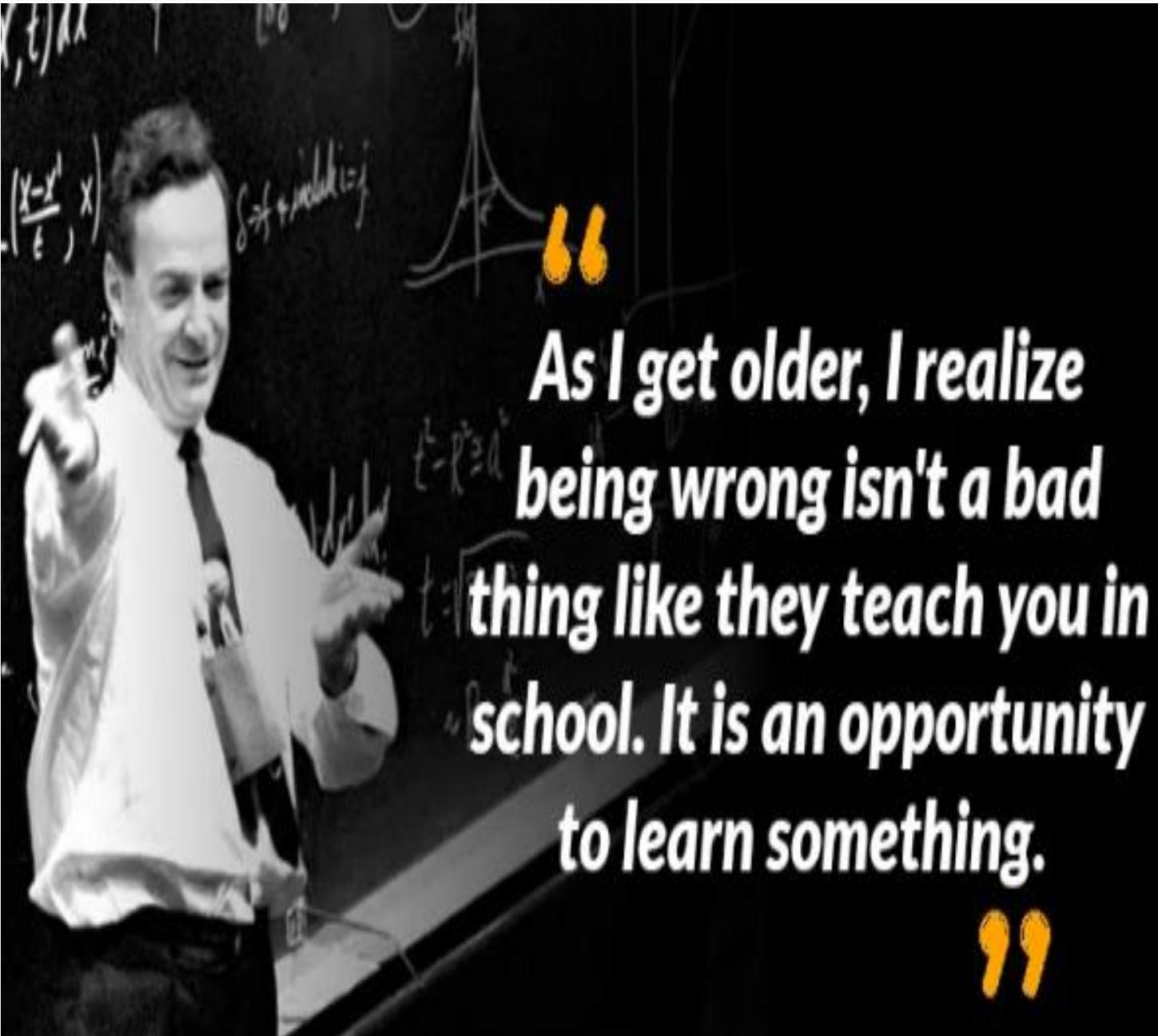
## Data Layer

Digital Signature, Hash, Merkle Tree, Transactions

## Hardware / Infrastructure Layer

Virtual Machine, Containers, Mining Rig

Crossing point	Blockchain impact	Quantum technology impact	Latest applications explored
Cryptography	Asegura las transacciones y protege los datos	Podría romper algunos algoritmos criptográficos existentes	nuevos algoritmos criptográficos resistentes a los cuánticos, como la criptografía basada en celosía y la criptografía poscuántica. Estos nuevos algoritmos podrían utilizarse para proteger las cadenas de bloques de ataques cuánticos..
Consensus mechanisms	Llega a un acuerdo sobre el estado del libro mayor	Podría hacer que algunos mecanismos de consenso sean vulnerables a ataques	nuevos mecanismos de consenso resistentes a los cuánticos, como la prueba de participación resistente a los cuánticos y la prueba de trabajo resistente a los cuánticos. Estos nuevos mecanismos de consenso podrían utilizarse para proteger las cadenas de bloques de ataques cuánticos.
Smart contracts	Contratos autoejecutables almacenados en una blockchain	Podría permitir nuevos tipos de contratos inteligentes, pero también explotar vulnerabilidades en los contratos inteligentes existentes.	nuevos contratos inteligentes resistentes a los cuánticos. Estos nuevos contratos inteligentes podrían utilizarse para crear nuevos tipos de aplicaciones, como instrumentos financieros cuánticos y sistemas de votación resistentes a los cuánticos..
Quantum key distribution (QKD)	Manera segura de distribuir claves de cifrado	Podría usarse para proteger redes y transacciones blockchain	QKD ya se está utilizando para proteger algunas redes blockchain, como Quantum Resistance Ledger (QRL).
Quantum random number generation (QRNG)	Manera segura de generar números aleatorios.	Podría usarse para mejorar la seguridad de los mecanismos de consenso de blockchain y los contratos inteligentes.	QRNG ya se está utilizando para mejorar la seguridad de algunas redes blockchain, como Algorand y Cardano.
Quantum-resistant cryptography	Nuevos algoritmos criptográficos resistentes a los ataques de ordenadores cuánticos	Podría usarse para proteger blockchains y otras aplicaciones de ataques cuánticos	Integración de la criptografía resistente a los cuánticos en las redes blockchain existentes. Por ejemplo, la Fundación Ethereum está trabajando para integrar la criptografía resistente a los cuánticos en Ethereum 2.0.



“  
*As I get older, I realize  
being wrong isn't a bad  
thing like they teach you in  
school. It is an opportunity  
to learn something.*  
”

**gtd**

CHILE • PERÚ • COLOMBIA • ECUADOR

ESPAÑA • ITALIA

