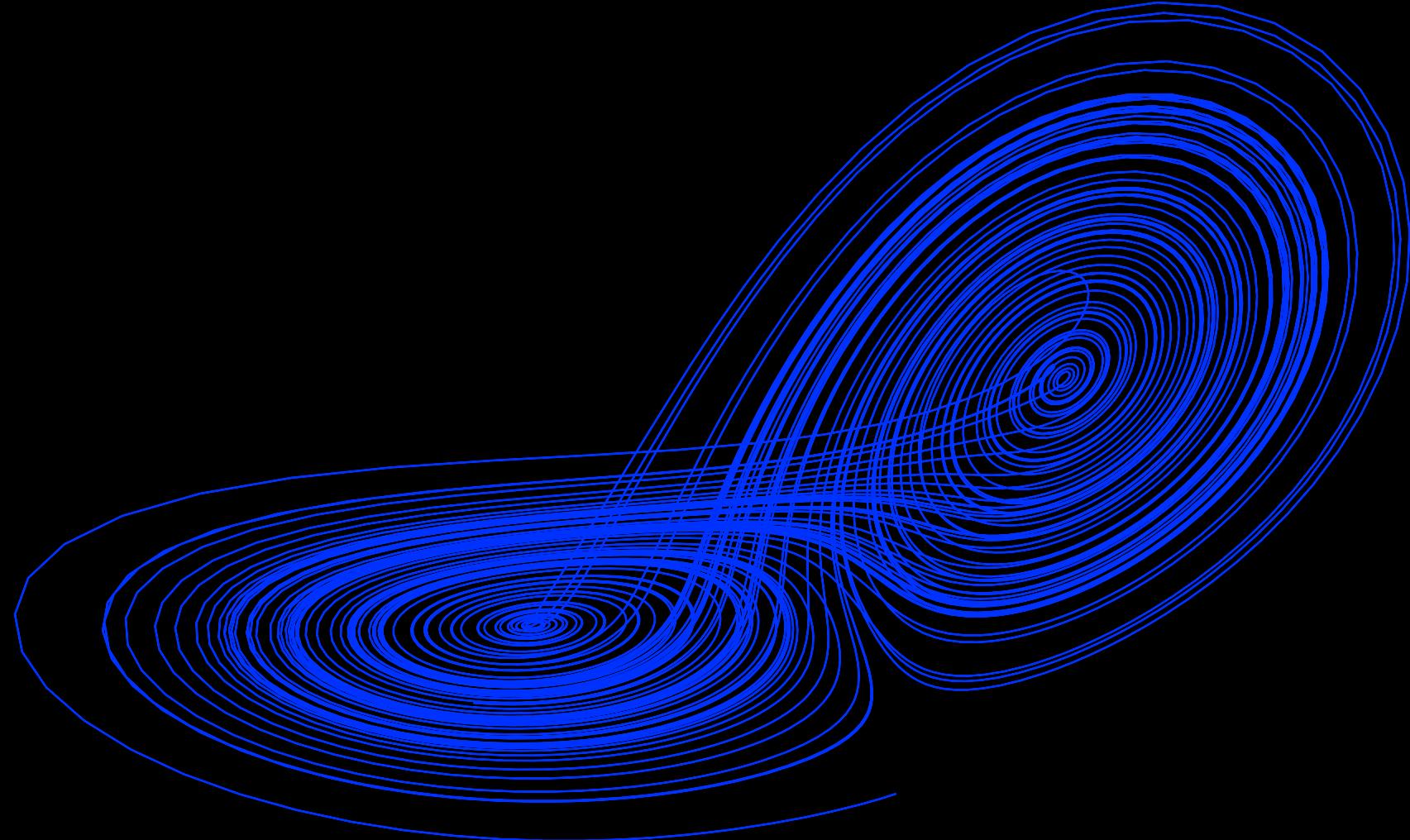


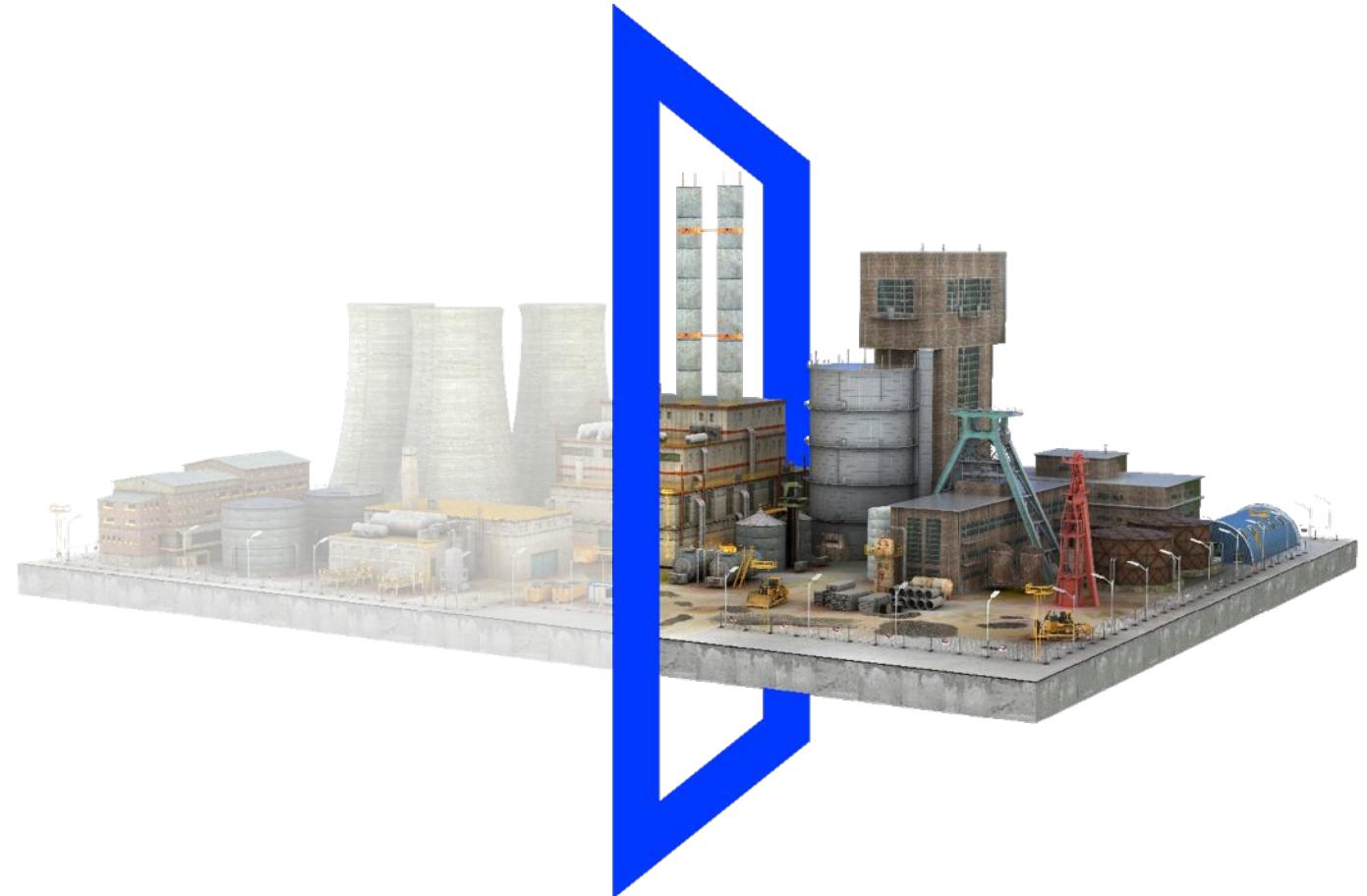
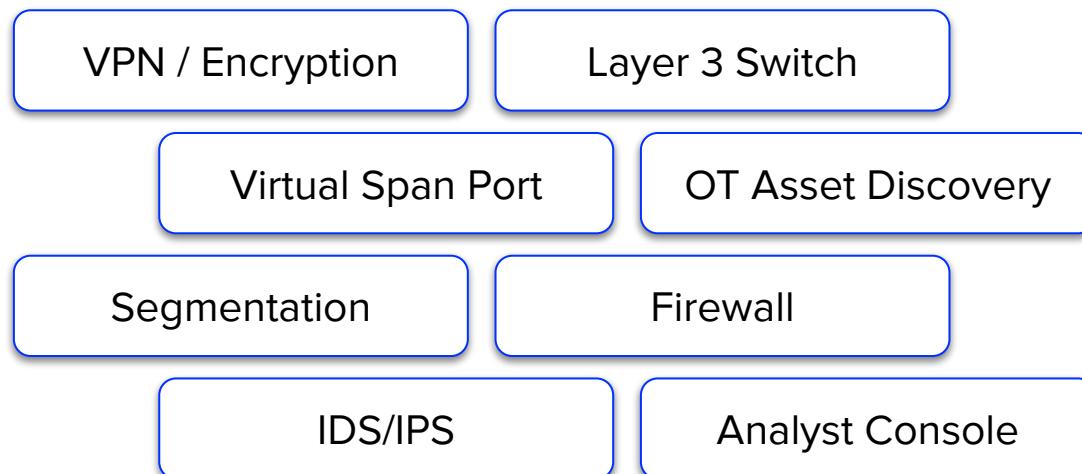
Carlos Tomás Moro | [carlos@opscura.io](mailto:carlos@opscura.io)  
Co-Founder & VP Engineering



Get Cloaked. Frictionless Protection for Industrial Networks.

# Opscura Solutions: Frictionless Security Overlay

- ↳ Secures all network communication, including legacy devices
- ↳ Includes full-stack of protection capabilities
- ↳ Deploys in minutes with negligible downtime



# OT Cybersecurity & Network problems we solve

Opscura **protects** industrial networks by isolating, cloaking and authenticating sensitive assets and data deep in the OT network

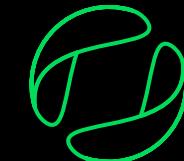
We **connect** security teams across OT, IT and partners with safe data sharing, streaming and notifications



Virtual Span Port

## Visibility

Getting Deep-Level Ot Data  
To Threat Monitoring Tools



Data Cloaking

## Segmentation

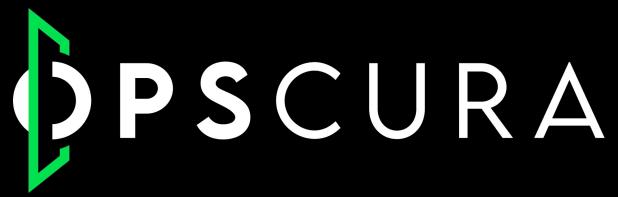
Controlling Access  
Between Networks



OT Access Control

## Threat Prevention

Reducing The Ot Attack  
Surface & Protecting  
Legacy Critical Endpoints



# Introducción a la criptografía y retos futuros

1. Criptografía Digital
2. Criptografía de bajo consumo
3. Blockchain
4. Criptografía post-cuántica o “quantum-safe”



# Criptografía digital

# ¿Para qué se puede usar la criptografía?

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican.

La criptografía se ocupa de dotar a la información de las siguientes propiedades:

- **Confidencialidad:** La información es accesible sólo para personas autorizadas
- **Integridad:** El mensaje recibido es el original
- **Autenticación:** El emisor y el receptor son quienes dicen ser
- **No-repudio:** El emisor puede demostrar que ha enviado el mensaje y el receptor que lo ha recibido

# Desiderata de Kerckhoffs (1883)

1. El sistema tiene que ser indescifrable en la práctica, si no lo es matemáticamente.
2. **El método de cifrado no debería requerir ser secreto y no debería ser un problema que cayese en manos del enemigo.**
3. Debe ser posible comunicarse y recordar la clave sin usar notas escritas. Los usuarios deben poder cambiar la clave a voluntad.
4. Debe ser aplicable a las comunicaciones telegráficas.
5. Debe ser portable y no tiene que requerir a muchas personas para operarlo.
6. El sistema debe ser fácil de usar y no debe requerir que los usuarios sepan una larga lista de reglas.

Criptografía Militar, Journal des sciences militaires, 1883

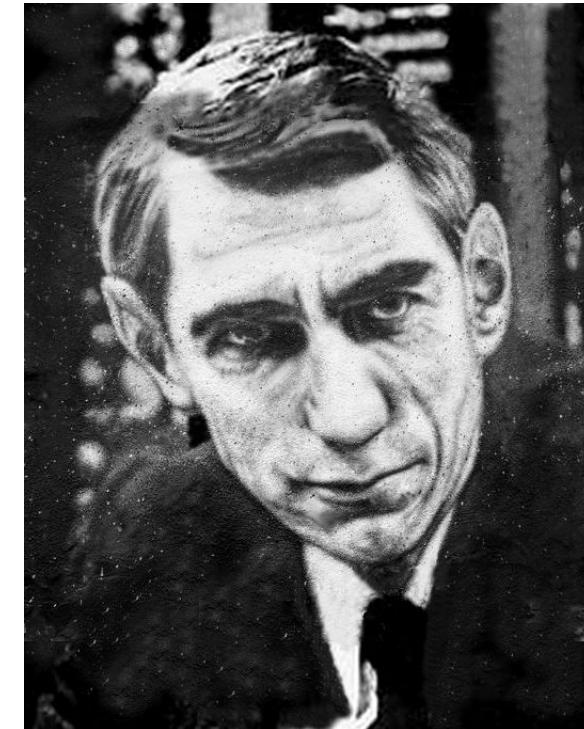
# Teoría de la Información de Shannon

Durante la 2a Guerra Mundial Shannon creó las bases para los sistemas de comunicaciones actuales.

Se publicaron al acabar la Guerra.

A Mathematical Theory of **Communication**, Bell System Technical Journal 27, **1948**

Communication Theory of **Secrecy Systems**, Bell System Technical Journal 28, **1949**



Claude E. Shannon  
1916 - 2001

# Primeros estándares en criptografía

Hasta los años 70, el cifrado era un asunto prácticamente exclusivo de gobiernos. Con el avance de las telecomunicaciones y la globalización, las grandes corporaciones comienzan a necesitar también cifrado.

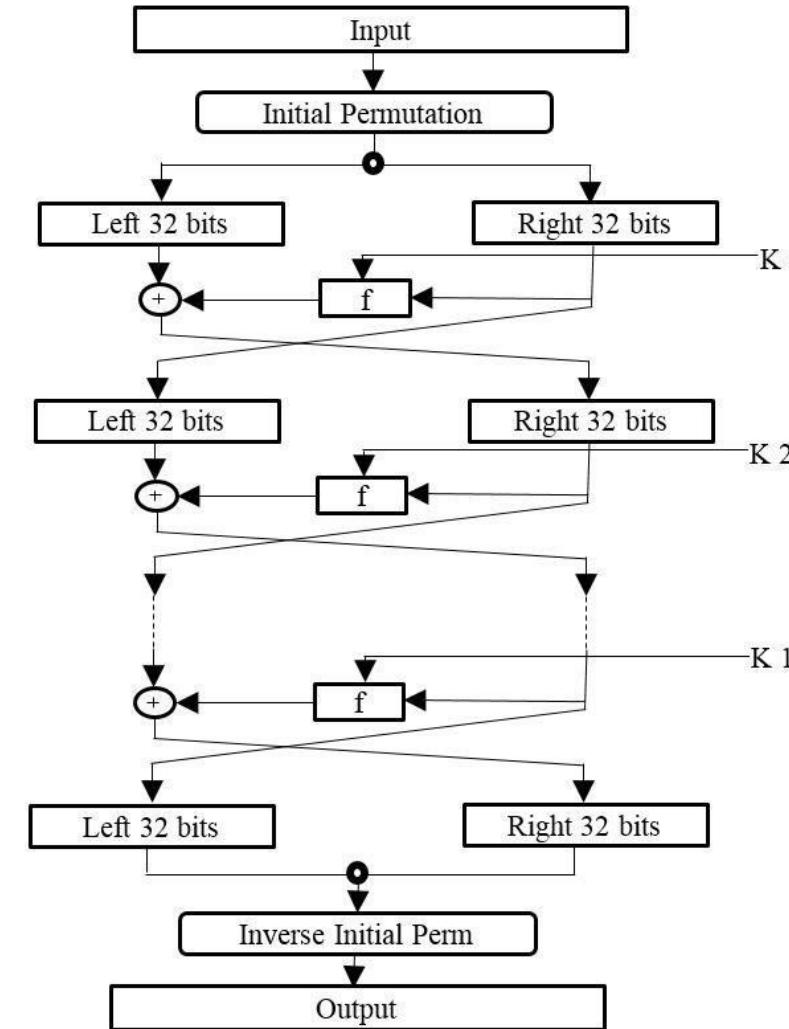
Para dar solución a este problema, en 1972 el US National Bureau of Standards empieza una convocatoria para definir un nuevo cifrado abierto.

En el 1973 se selecciona la propuesta de IBM y la NSA aconseja hacer unas mejoras.

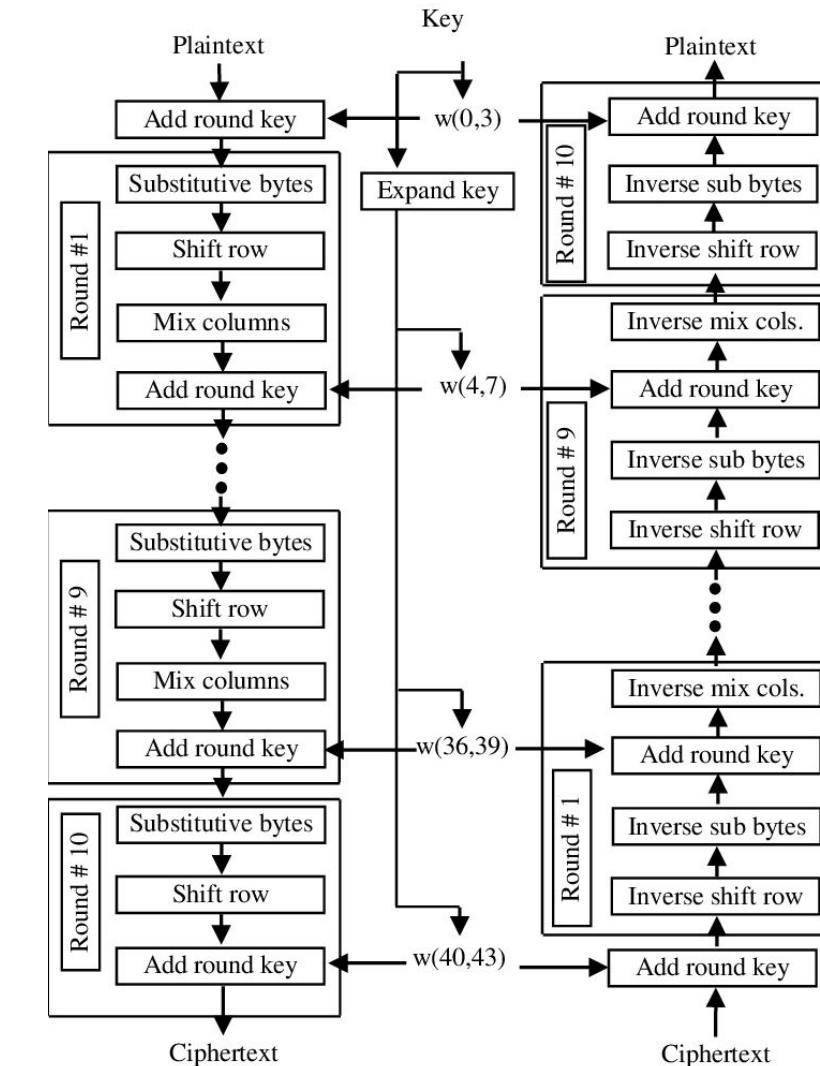
En 1977 se declara estándar el cifrado DES - Data Encryption Standard

Se mantiene hasta el 2000, con la llegada del AES – Advanced Encryption Standard

# Permutaciones: DES & AES



DES



AES

La seguridad del cifrado es adaptable mediante el aumento de la longitud de clave y el número de rondas

# Nuevos problemas: la gestión de claves

La Desiderata de Kerckhoffs planteaba que debería ser posible comunicarse y recordar la clave sin usar notas escritas.

Sin embargo la mejora de la computación hace que sea posible el uso de todas las contraseñas como se hizo con las bombas contra Enigma

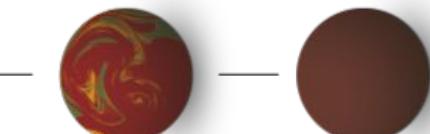
En el momento que tenemos cifrados robustos y abiertos, la seguridad de nuestras comunicaciones depende exclusivamente de cómo de secretas son nuestras claves.

Cuando la criptografía era de uso exclusivamente militar, la gestión de estas contraseñas se hacía mediante libros de claves. Pero las organizaciones civiles no tienen los protocolos para custodiar de forma efectiva este tipo de información

# Función trampa



muy fácil



muy difícil



# Uso de números primos

Multiplicar dos números primos es una operación sencilla  $7 \times 11 = 77$   
Descomponer un número en primos requiere muchas operaciones:

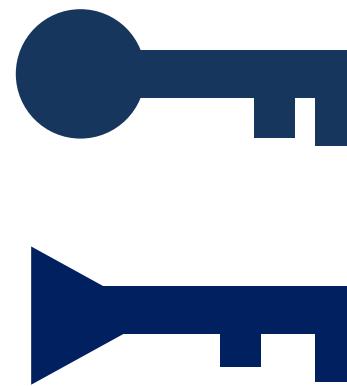
$$77 \div 2 = \text{no} \quad 77 \div 3 = \text{no} \quad 77 \div 4 = \text{no} \quad 77 \div 5 = \text{no}$$

$$77 \div 6 = \text{no} \quad 77 \div 7 = \text{sí}$$

$$11 \div 8 = \text{no} \quad 11 \div 9 = \text{no} \quad 11 \div 10 = \text{no} \quad 11 \div 11 = \text{sí}$$

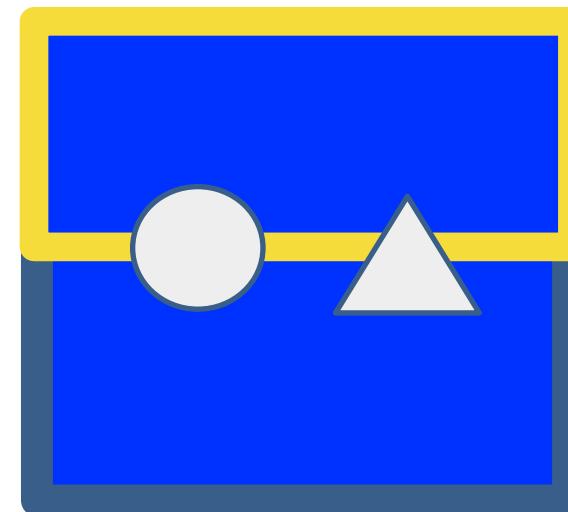
Se usa el algoritmo de Euclides

# Criptografía asimétrica o criptografía de clave pública



Clave  
Pública

Clave  
privada



La información que se cifra con la clave pública se descifra con la clave privada

La información que se cifra con la clave privada se descifra con la clave pública

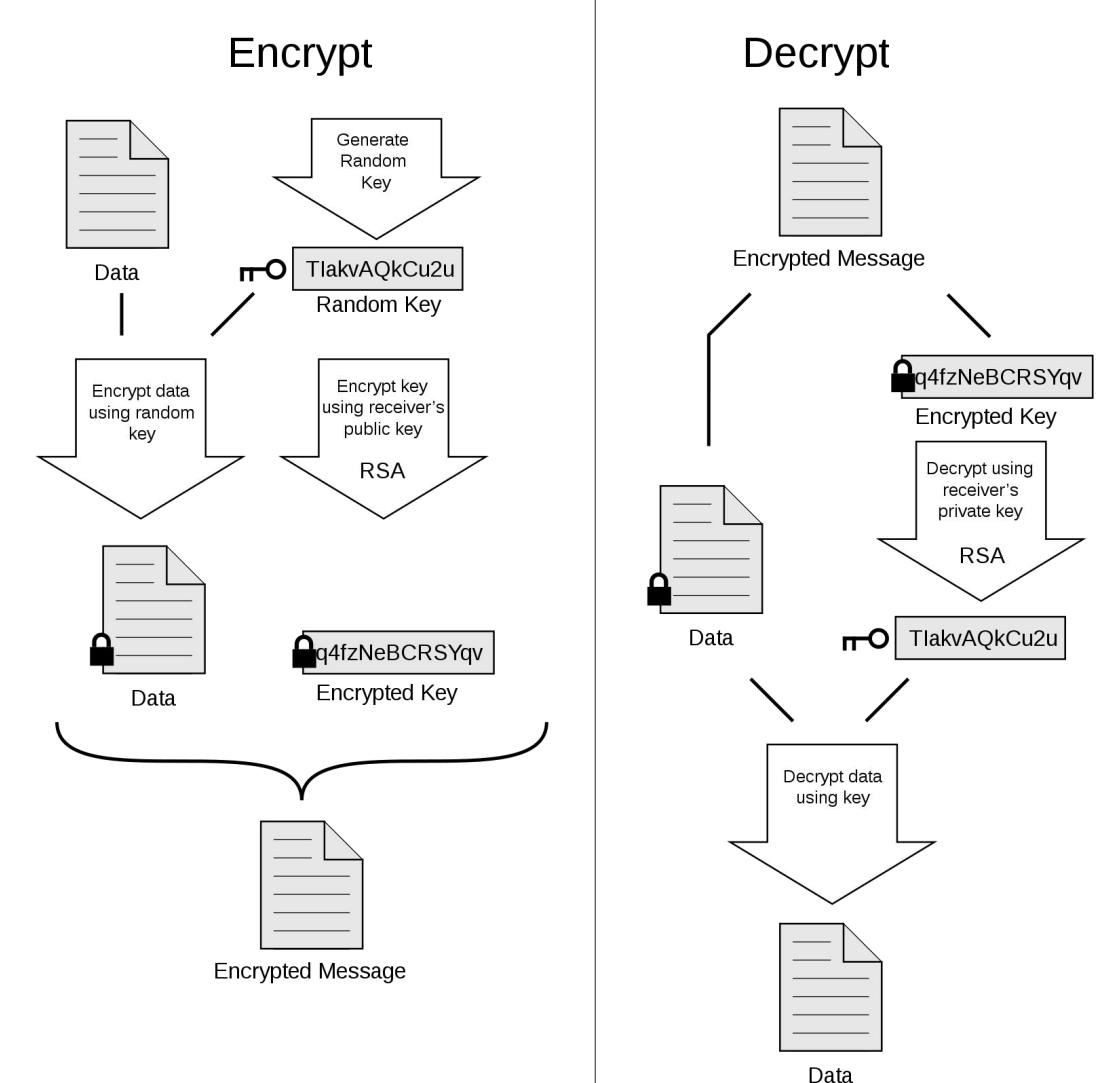
Rivest, Shamir, Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 1978

# Criptografía híbrida

La criptografía de clave pública o asimétrica es mucho menos eficiente (por el tipo de operaciones matemáticas que lleva a cabo) que la criptografía simétrica.

Para poder usar criptografía asimétrica de forma eficiente, puedo cifrar mi mensaje con una clave simétrica aleatoria y usar criptografía asimétrica para proteger la clave aleatoria

PGP: Pretty Good Privacy. Zimmermann, 1991



# Autenticación y firmas digitales

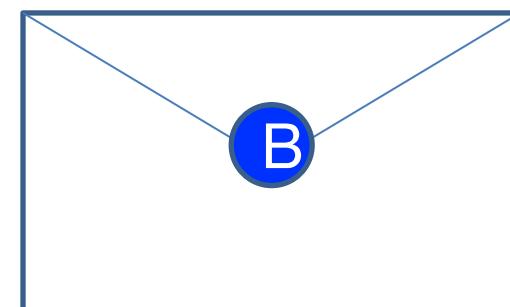
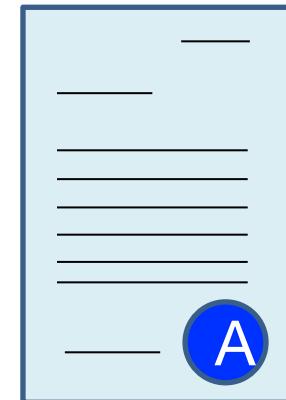
A quiere mandar un mensaje firmado a B

$$F = E(p_a(m))$$

Solo se puede descifrar usando la clave Pública de A. Solamente puede haberlo cifrado A.

Luego cifra con la Pública de B.  
Solamente B puede leer.

$$C^* = E(P_b(F)) = E(P_b(E(p_a(m))))$$



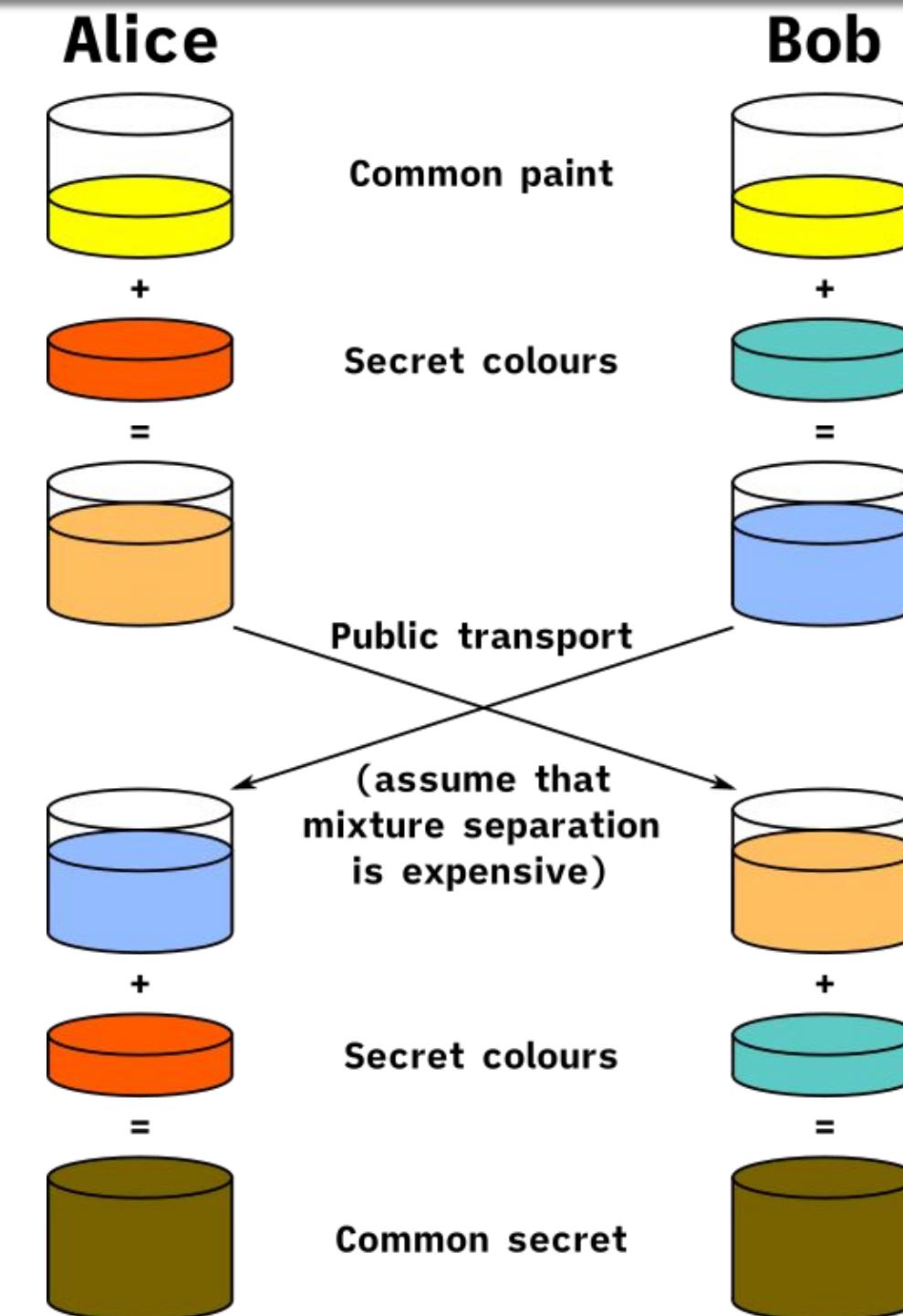
Mensaje claro = m firmado = F cifrado y autenticado =  $C^*$   
Pública =  $P_a, P_b$  Privada =  $p_a, p_b$

# Diffie-Hellman: claves efímeras de sesión

Podemos usar criptografía de clave pública para poder intercambiar claves simétricas. Sin embargo si en algún momento se filtrase la clave privada, se podría recuperar la clave simétrica utilizada en todas mis comunicaciones pasadas.

Para evitar este riesgo existen los esquemas *Perfect Forward Secrecy* en la que la clave simétrica se establece mediante un método de claves asimétricas temporales.

W. Diffie, M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory 22 (1976)

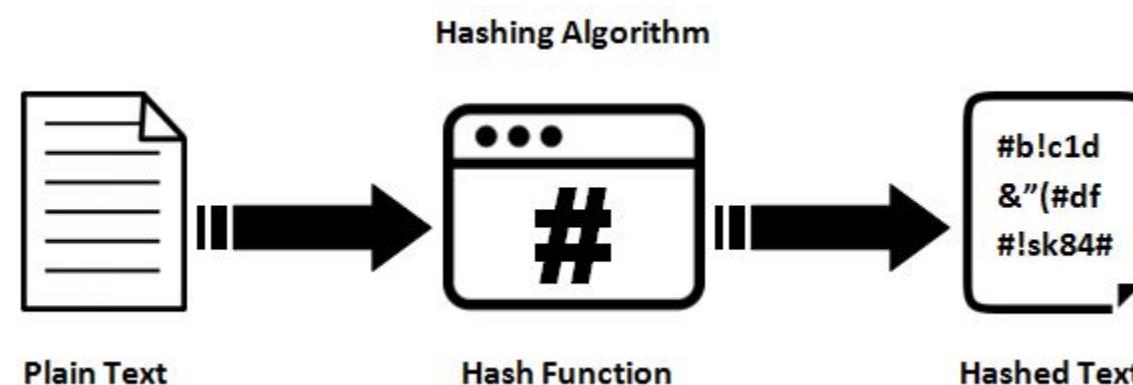


# Funciones resúmenes o hashes

Las funciones hash o funciones resumen sirven para resumir un texto indefinidamente largo en un número fijo de letras.

Actualmente las funciones más seguras son las SHA (Secure Hash Algorithm)

Tienen que tener ciertas propiedades para que sean útiles. Como son funciones resumen, pueden tener colisiones donde diferentes textos pueden tener el mismo resultado.

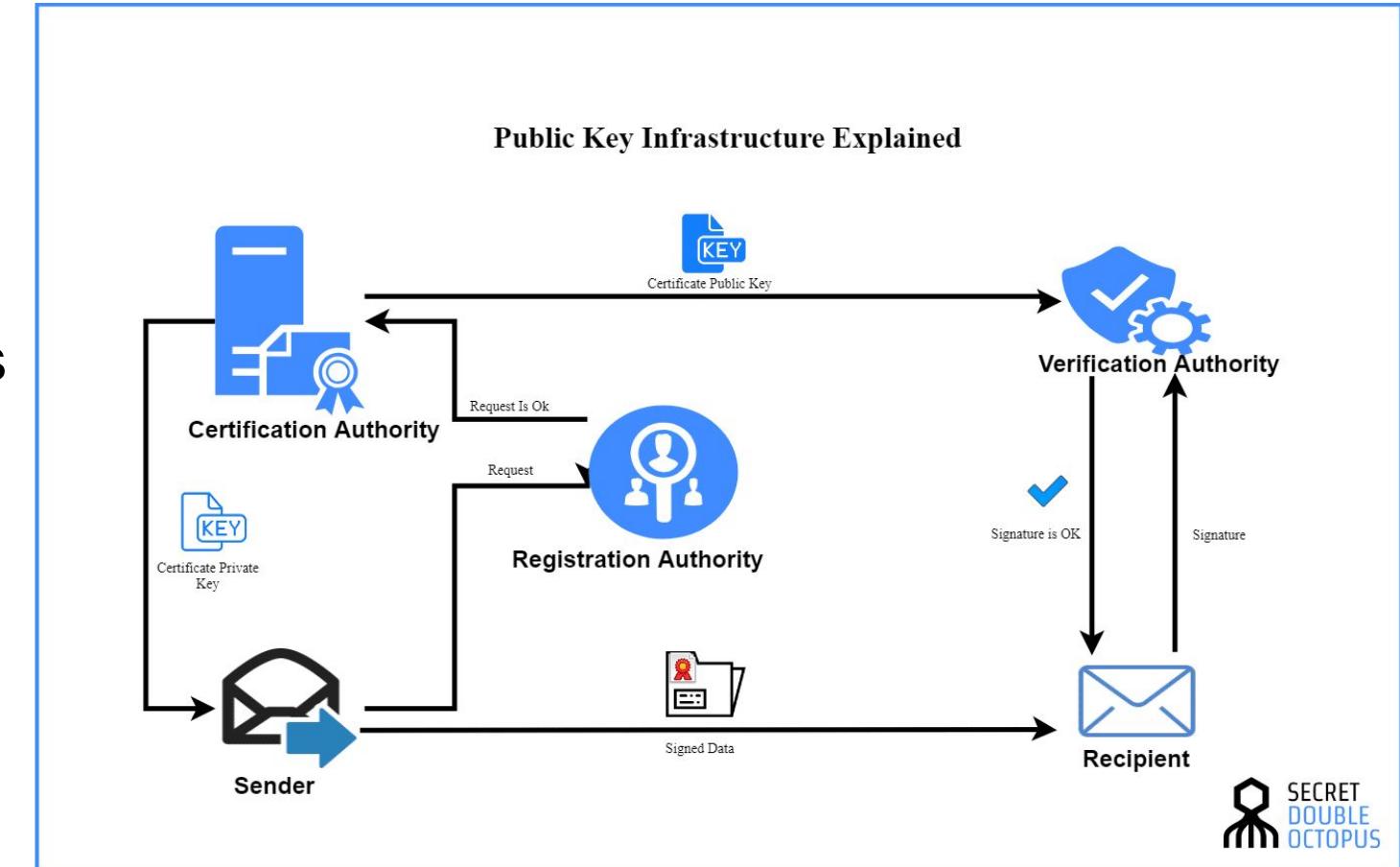


# Infraestructura de claves públicas

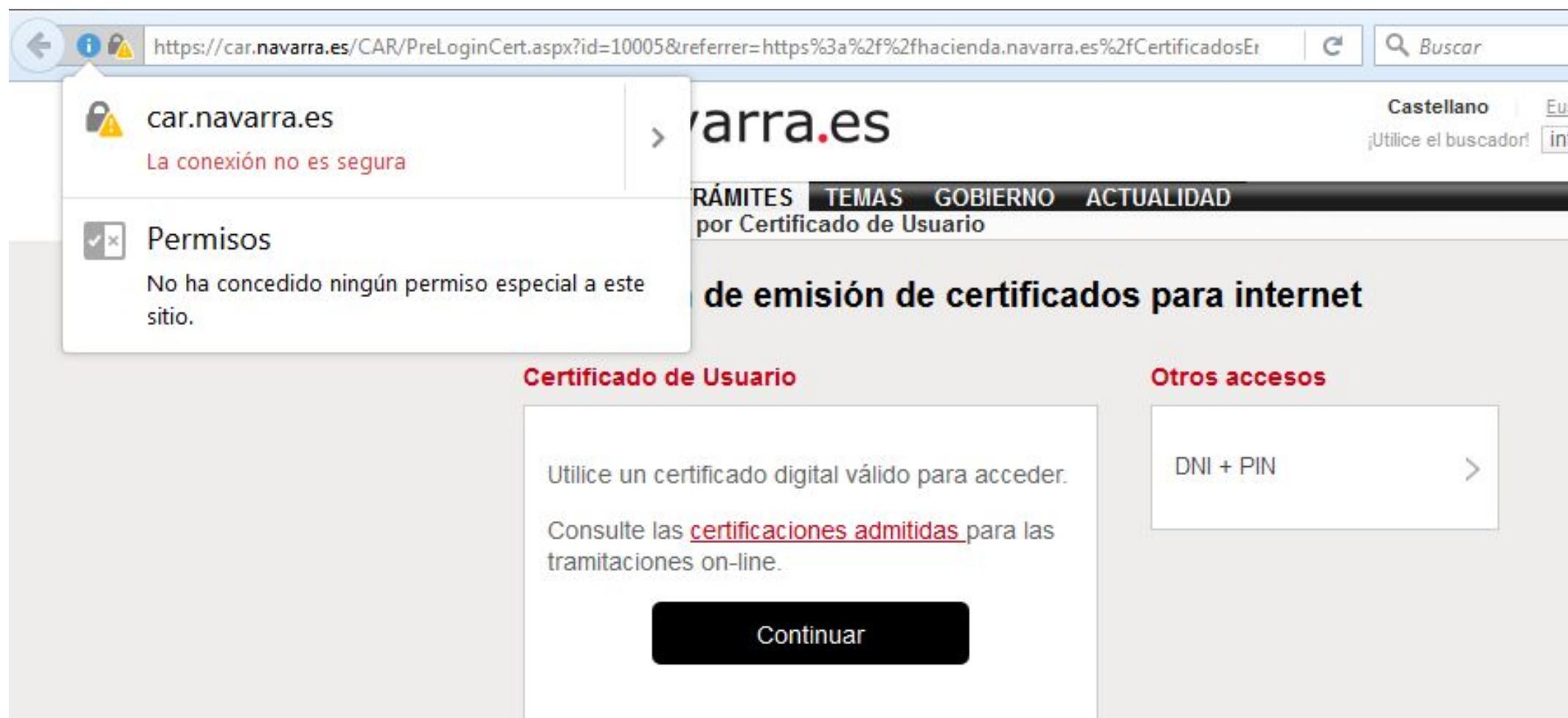
Hasta ahora hemos hablado de confianza entre pares, pero ¿cómo podemos gestionar organizaciones?

La clave es que podemos usar claves públicas para firmar otras claves públicas y establecer niveles de confianza

La forma de almacenar esos conjuntos de firmas es lo que llamamos **certificados digitales**



Para que un certificado sea confiable debe estar firmado por una Root of trust de confianza para el usuario



# ¿Podemos confiar en las Root of trust?

Security

## French gov used fake Google certificate to read its workers' traffic

Liberté, égalité ... invisibilité: Homme-dans-l'intermédiaire snooping at treasury dept

By John Leyden 10 Dec 2013 at 16:55

49

SHARE ▾



A French government agency has been caught signing SSL certificates and impersonating Google.

SC Media US > News > Gogo caught using fake Google SSL certificates



by Teri Robinson, Executive Editor

[Follow @TeriRnNY](#)

January 06, 2015

## Gogo caught using fake Google SSL certificates



Fliers who don't want their data intercepted by Gogo LLC, or unnecessarily fall into the hands of law enforcement, might want to reconsider using the inflight WiFi service after it was found to be using fake Google SSL certificates.

The practice, which essentially sets up a **man-in-the-middle** (MitM) attack of sorts, was discovered by Google engineer Adrienne Porter Felt, who logged into Gogo WiFi during a recent flight.

After seeing a telltale red "x" in her address bar, warning that the certificate for a site "was signed by an untrusted issuer," Felt realized that Gogo, not Google, had signed it.



Gogo caught using fake Google SSL certificates

Por eso también debemos fijar que cadena de validación es la correcta ("pinnear")

Actualmente consideramos que un sistema de comunicaciones en internet es seguro si se combinan estas tecnologías criptográficas:

- La autenticación del servidor se realiza mediante certificados de clave pública de tamaño suficiente firmados por una fuente de confianza
- La clave de sesión se establece en el inicio mediante un sistema de tipo Diffie-Hellman o equivalente
- La clave de sesión pactada se utiliza para cifrar la información con un cifrado robusto como AES
- A los mensajes se les añade una capa de verificación de integridad basada en funciones hash (HMAC) para evitar que sean manipulados durante el tránsito



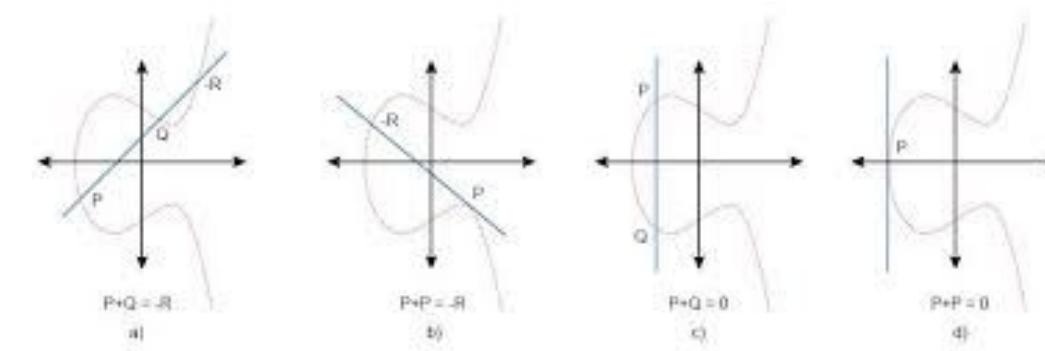
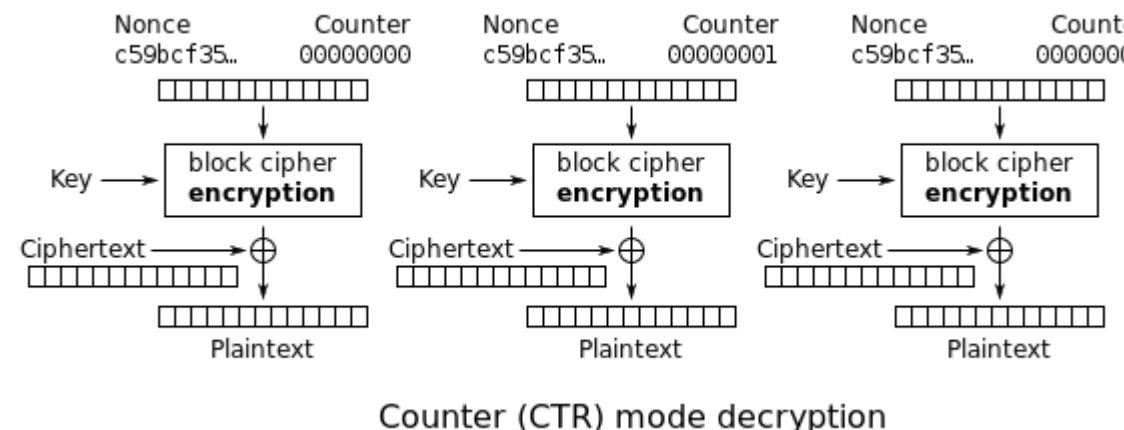
# Criptografía de bajo consumo

# Reduciendo costes: Cifrados de flujo y curvas elípticas

El esquema TLS es robusto pero tiene el problema de que tiene un coste computacional alto que crece al aumentar el volumen de información.

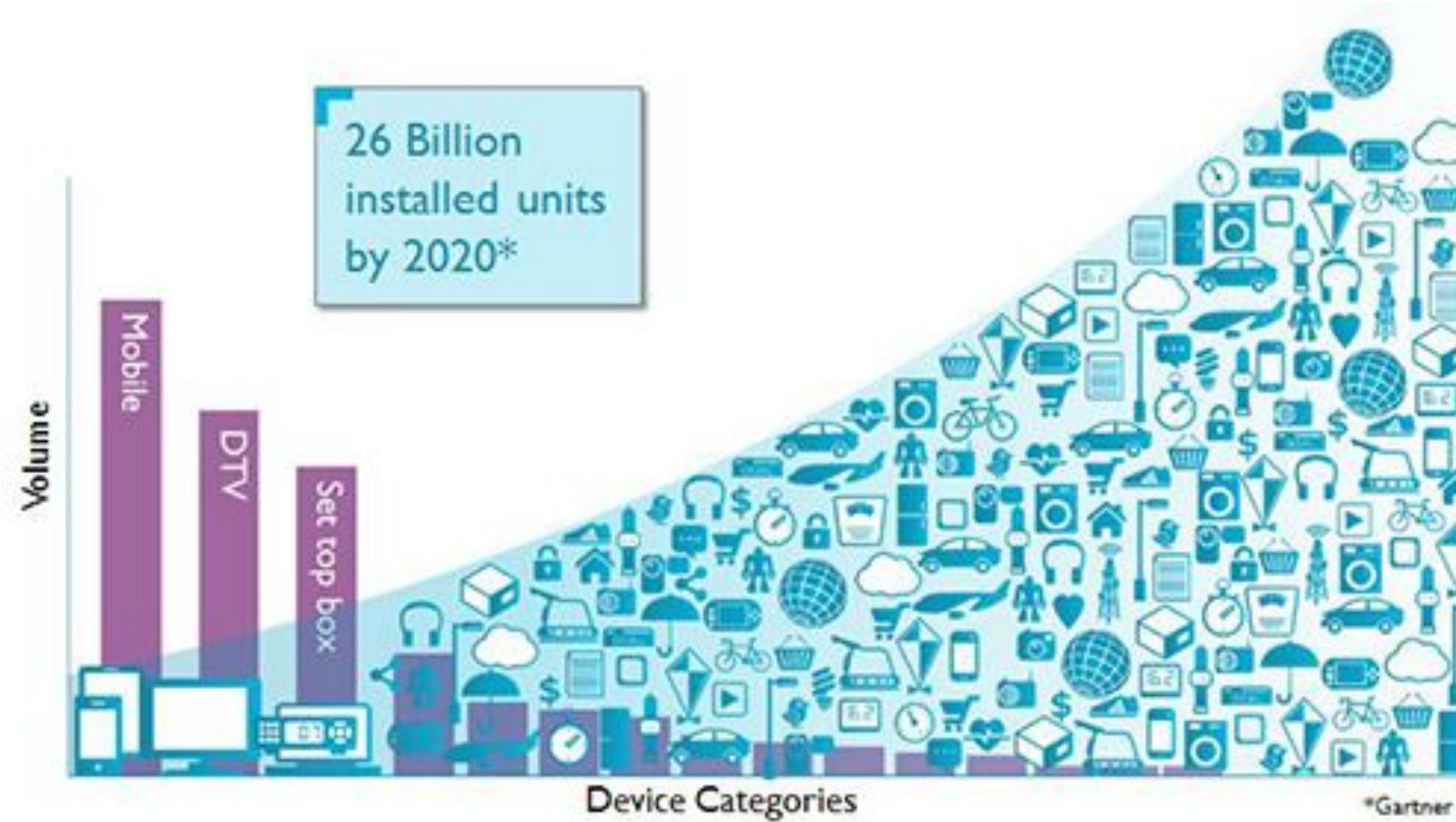
Para el cifrado simétrico de grandes volúmenes de información como voz o vídeo, se pueden usar **cifrados de flujo**, que a menudo son menos robustos pero con menor coste computacional

Para reducir el consumo de la criptografía asimétrica podemos usar **curvas elípticas**, que ofrecen un sistema casi igual de robusto por una fracción del coste computacional



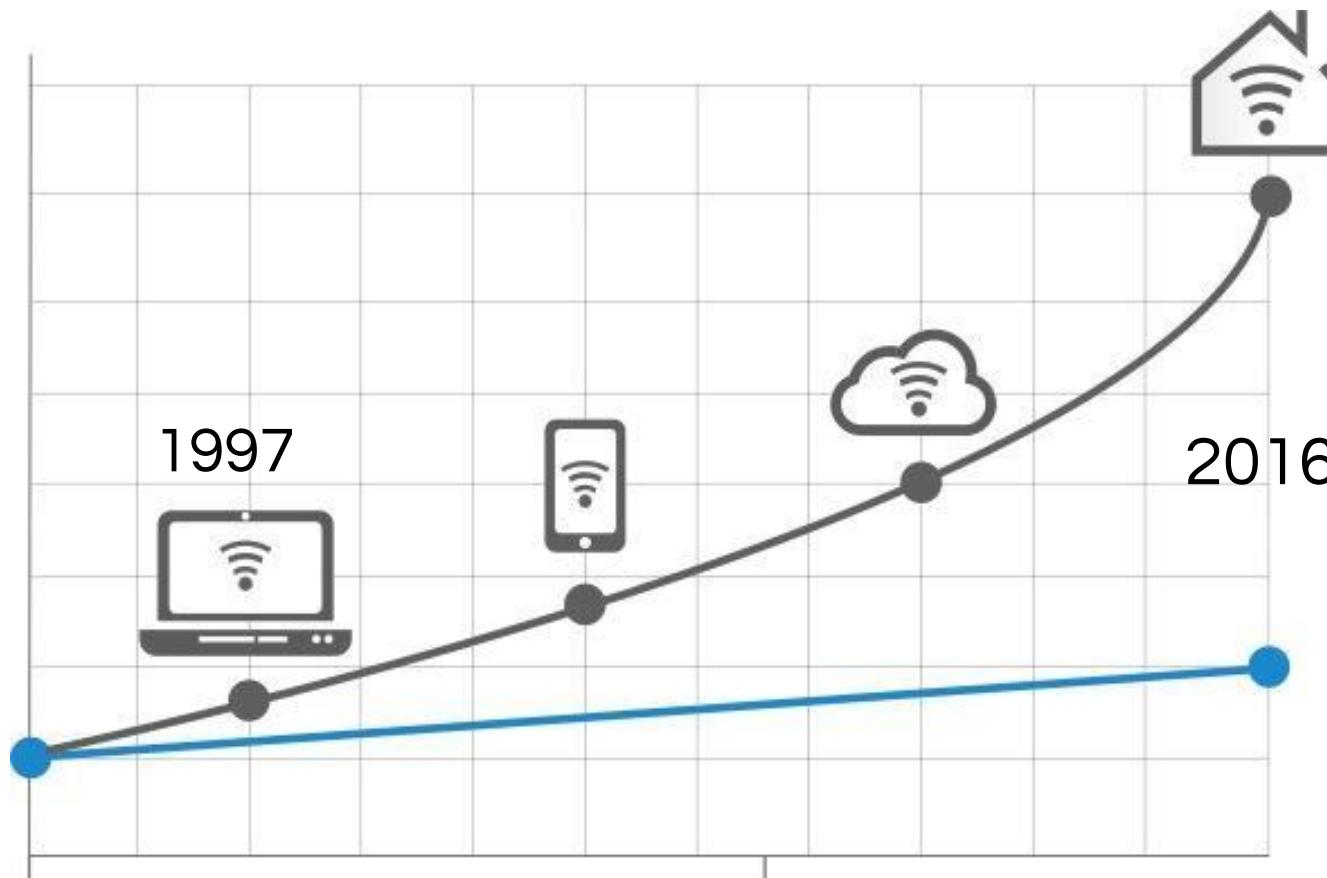
# Internet of things

Más y más datos están siendo enviados...



...y algunos canales de datos no son fáciles de proteger.

# Efectos colaterales de la adopción del IoT



- Tecnologías de la información
- Tecnologías de cifrado

Over 90% of data transactions on IoT devices are unencrypted

News

May 22, 2019 • 4 mins

Internet of Things Network Security Security

**Unsecured IoT Devices Give Hackers a Backdoor Into Your Network – Get Protected Now**



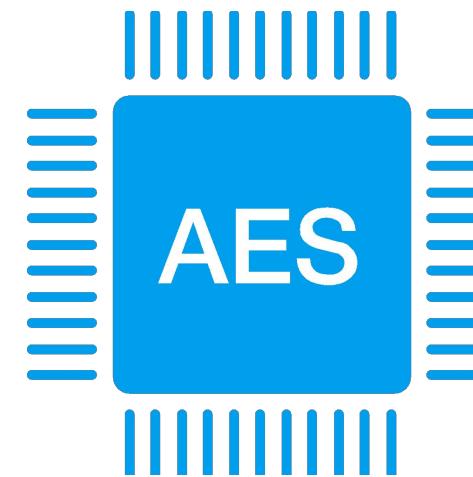
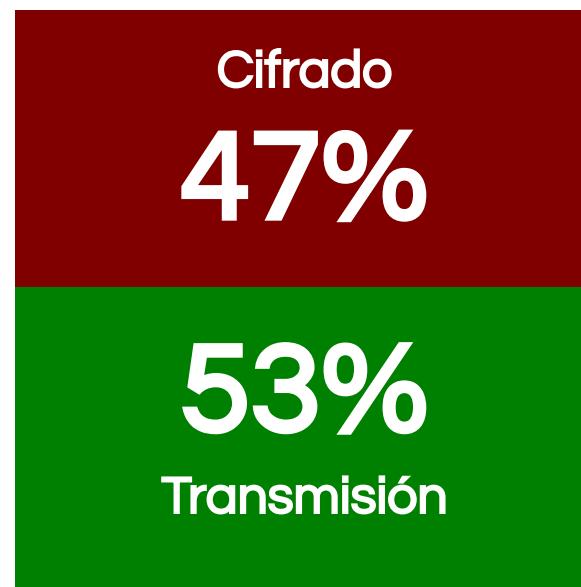
Emily Newton - January 12, 2023

**More Than Half of IoT Devices Vulnerable to Severe Attacks**



# Criptografía vs autonomía

## CONSUMO DE ENERGÍA



- AUMENTA EL TAMAÑO
- COSTE ADICIONAL

**Aceleradores AES mediante HW dedicado**  
son usados para garantizar la seguridad de  
los dispositivos IoT

# Autenticación de IoT

¿Cómo sabes quién es quién?

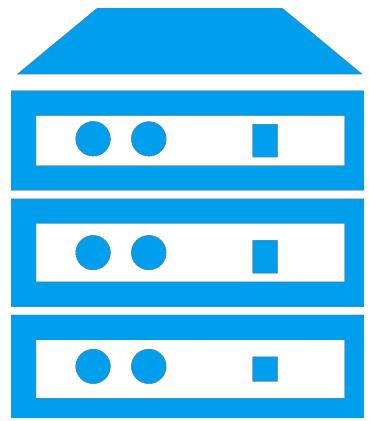


Imagina una llave maestra para 30 mil millones de dispositivos

Además, muchos de estos sistemas no tiene capacidad computacional para usar criptografía de clave pública

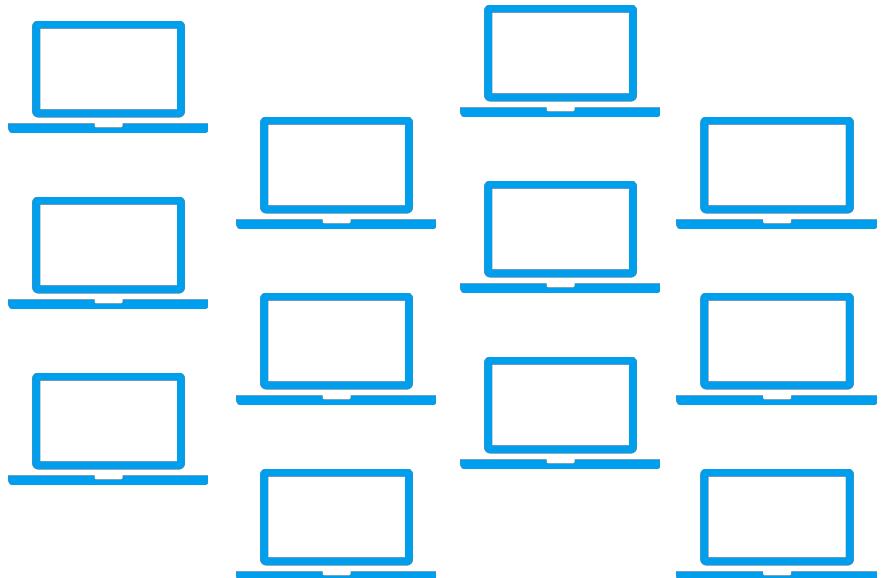
# Escalabilidad

1x



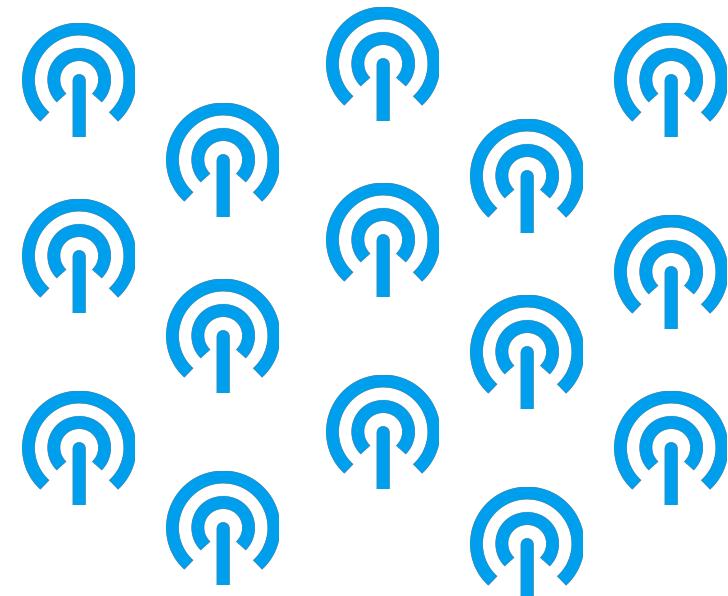
Servidor

100x



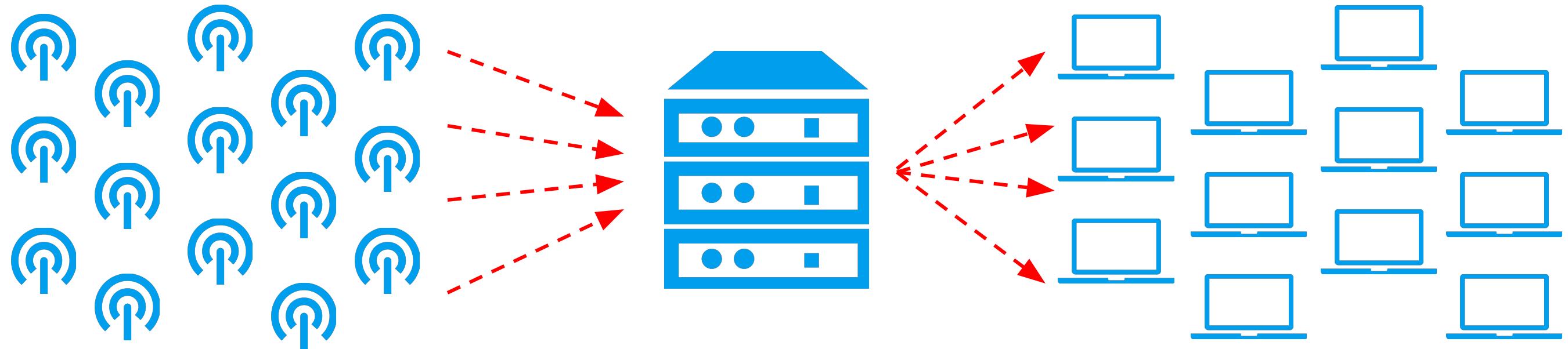
Centro de control

10,000x



Sensores

# Desafíos criptográficos del IoT



- Capacidad del sensor
- Propiedad
- Autentificación
- Escalabilidad

# Propuesta Opcura para IoT

## KEYLENGTH



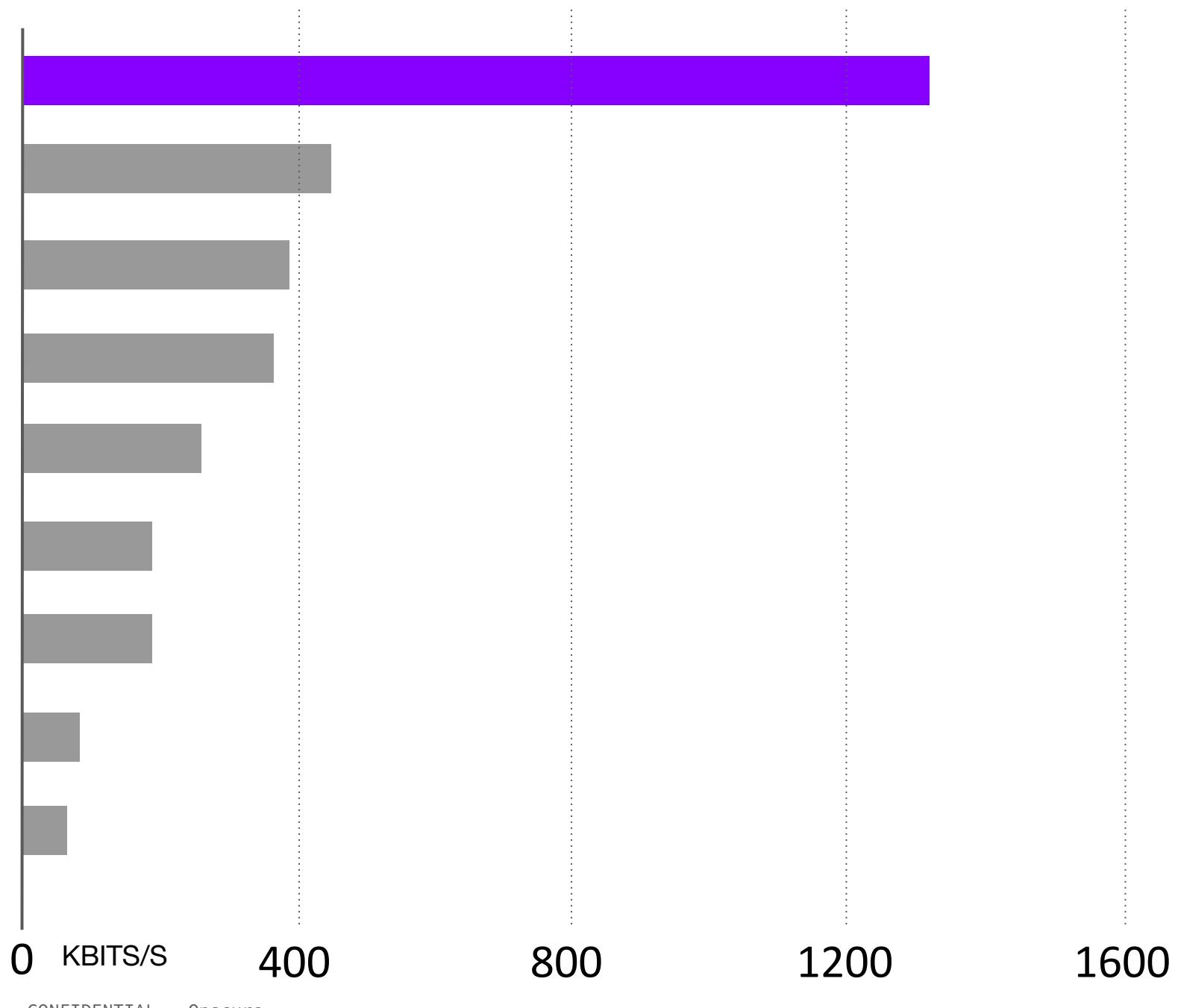
## CIPHER

- Opcura CHAOS
- SPECK-128
- HC-128
- SOSEMANUK
- AES
- SIMON-128
- WG8
- SALSA20
- PRESENT

The greener the better.  
% over 256 bits key length.

Ciphers with security  
issues are marked in red.

## PERFORMANCE



# Propuesta Opscura para IoT



**ID 11051      Session 2022**

D2 – Information systems and telecommunication

Information security techniques, technologies, and applications for securing  
critical utility assets

**Analysis of the impact of cryptography in the GOOSE communications**

**Miguel Á. SÁNCHEZ**

Arteche

Spain

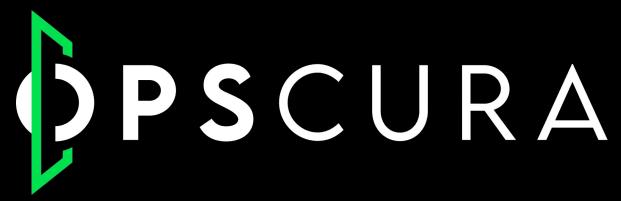
[miguel.sanchez@arteche.com](mailto:miguel.sanchez@arteche.com)

**Gerard VIDAL**

Enigmedia

Spain

[gerard@enigmediasecurity.com](mailto:gerard@enigmediasecurity.com)



# Blockchain

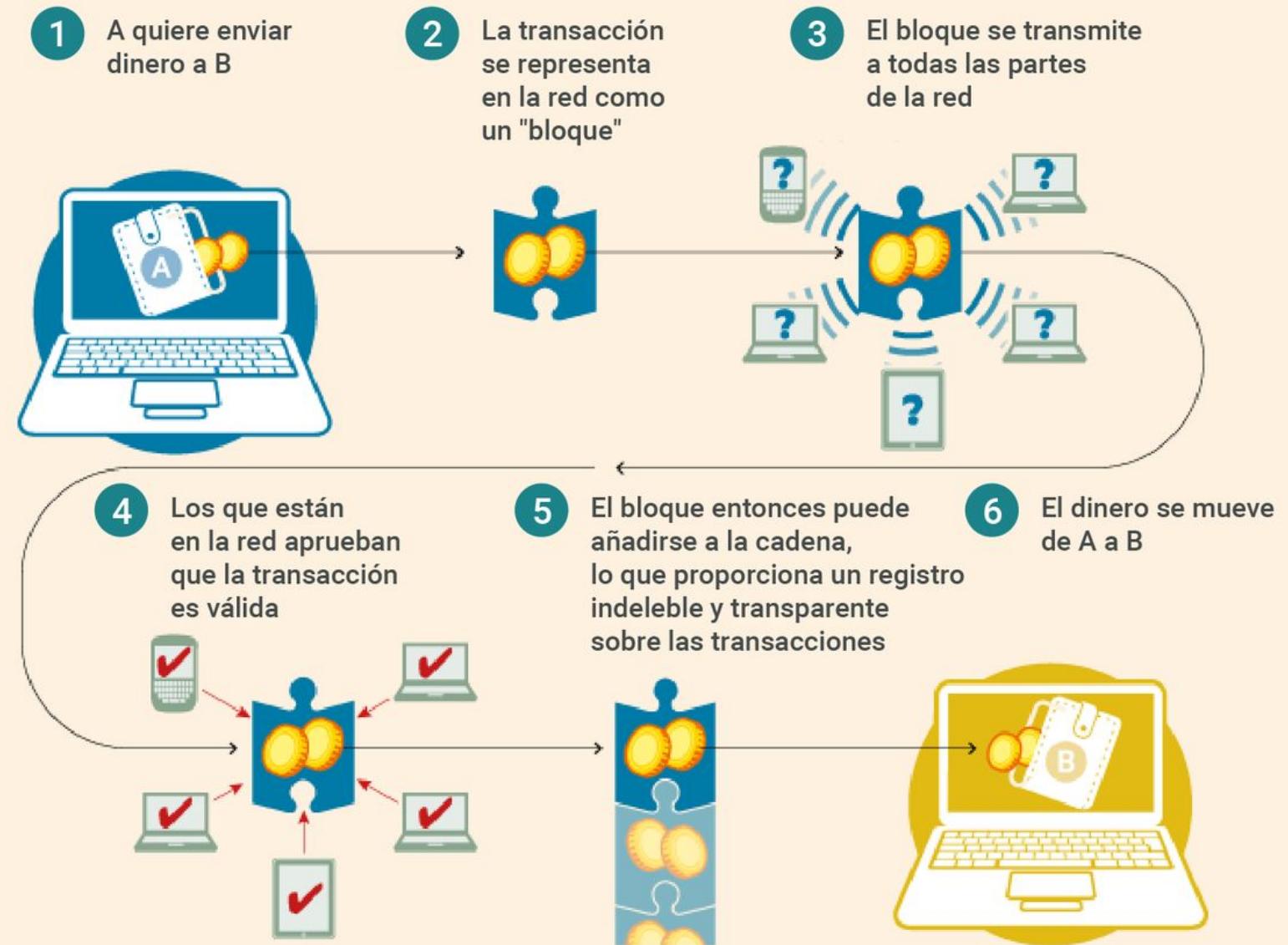
# Que promete blockchain

En 2008, una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto publican en internet un sistema de pago basado en una moneda digital que promete ser:

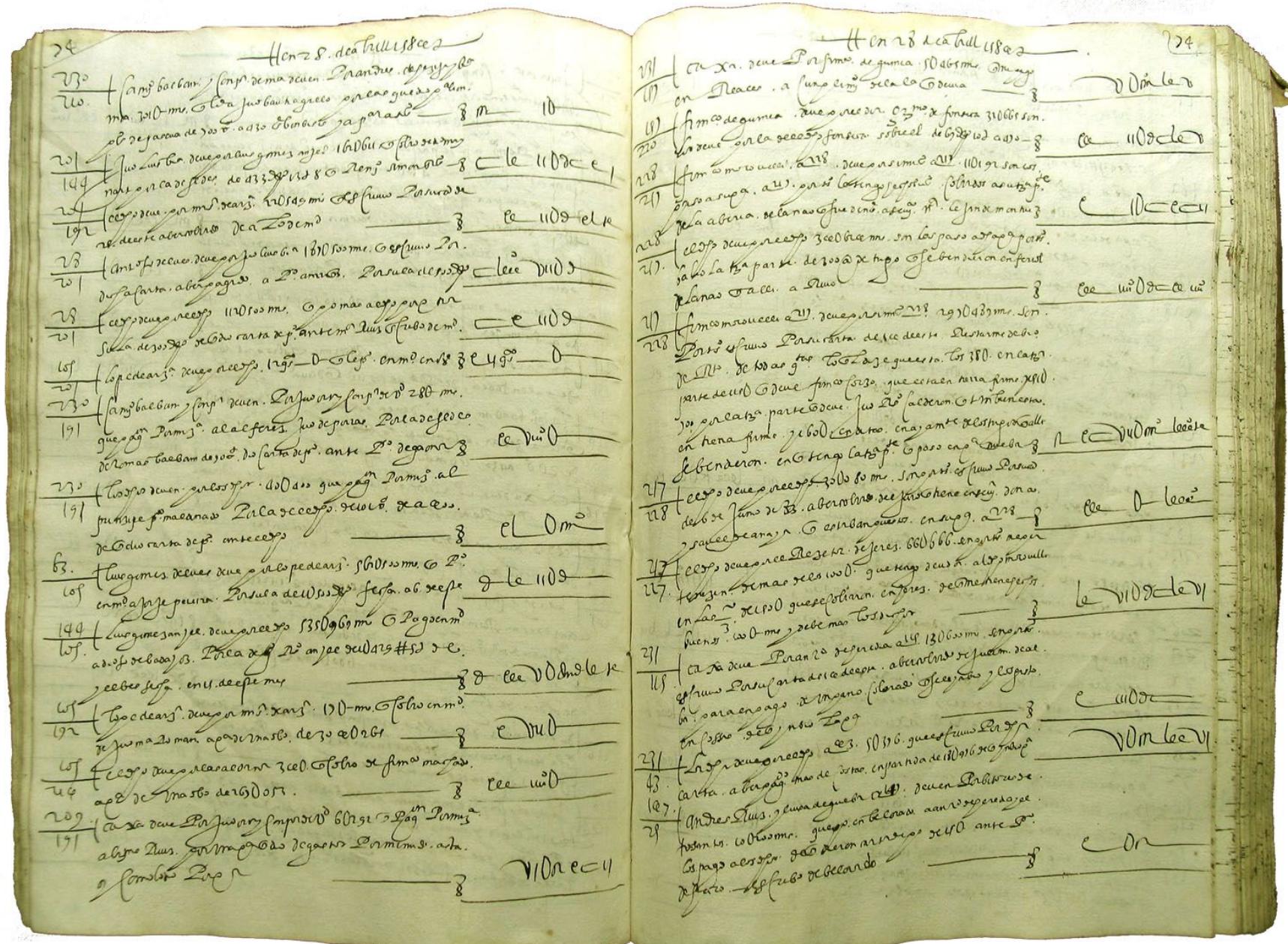
- Descentralizado
- Transparente
- Anónimo
- Seguro

Denominan Bitcoin a la moneda y blockchain al sistema de pagos

## Cómo funciona blockchain



# Base de Datos Contable: Ledger

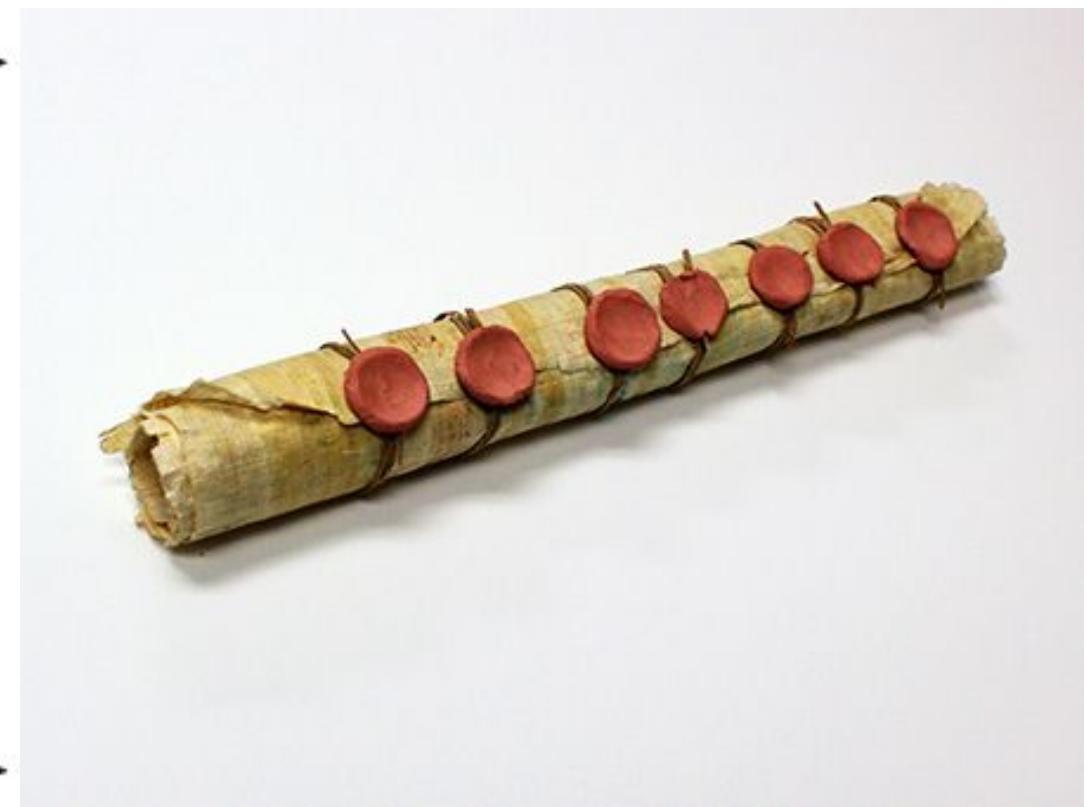
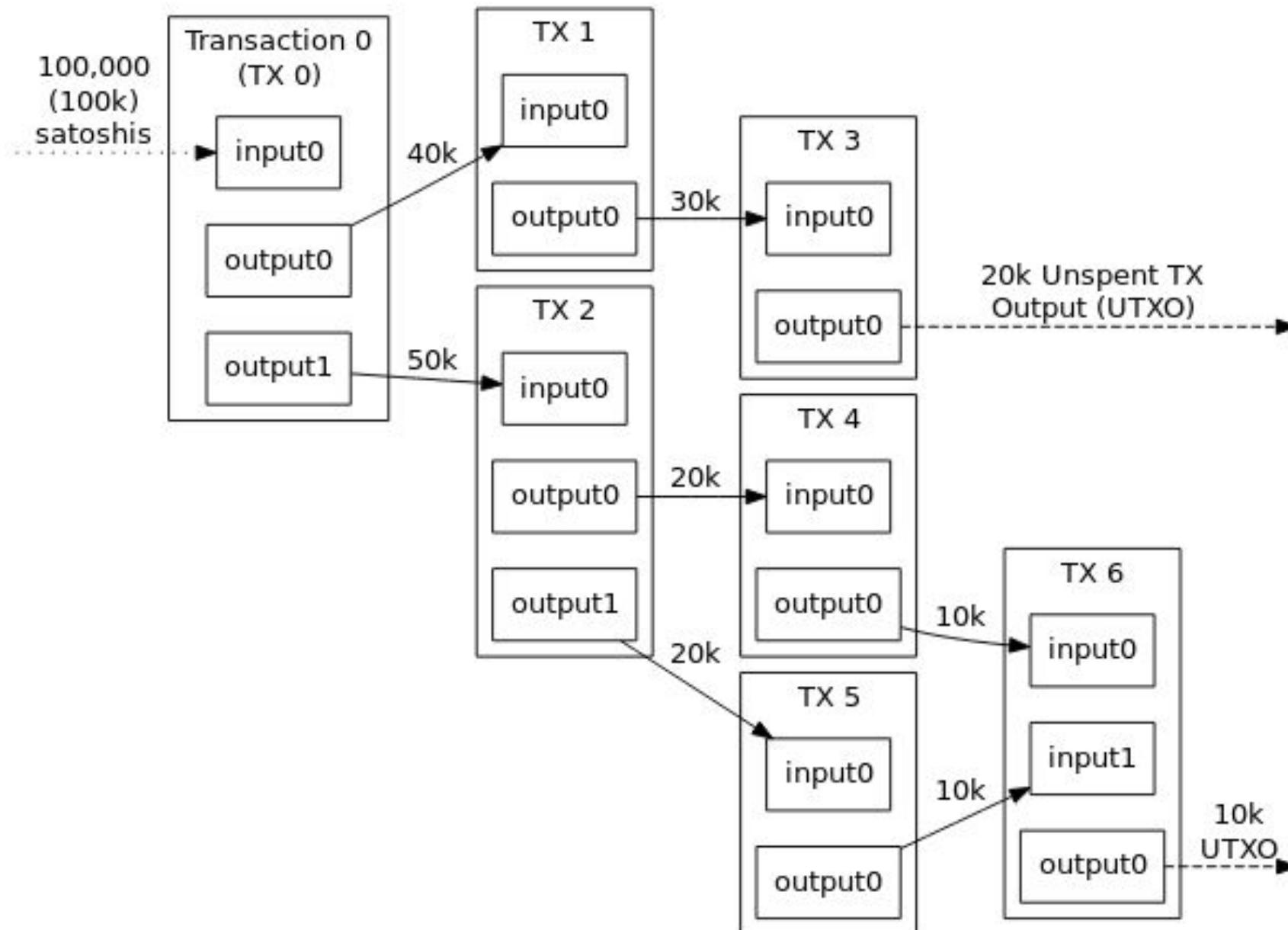


El ***ledger*** o **libro contable**, es un registro de todas las transacciones realizadas hasta la fecha.

Deben existir maneras de resumir este libro para que pueda ser factible no tener que revisar todas las transacciones pasadas.

Deben existir métodos para que haya consenso sobre el estado del libro contable

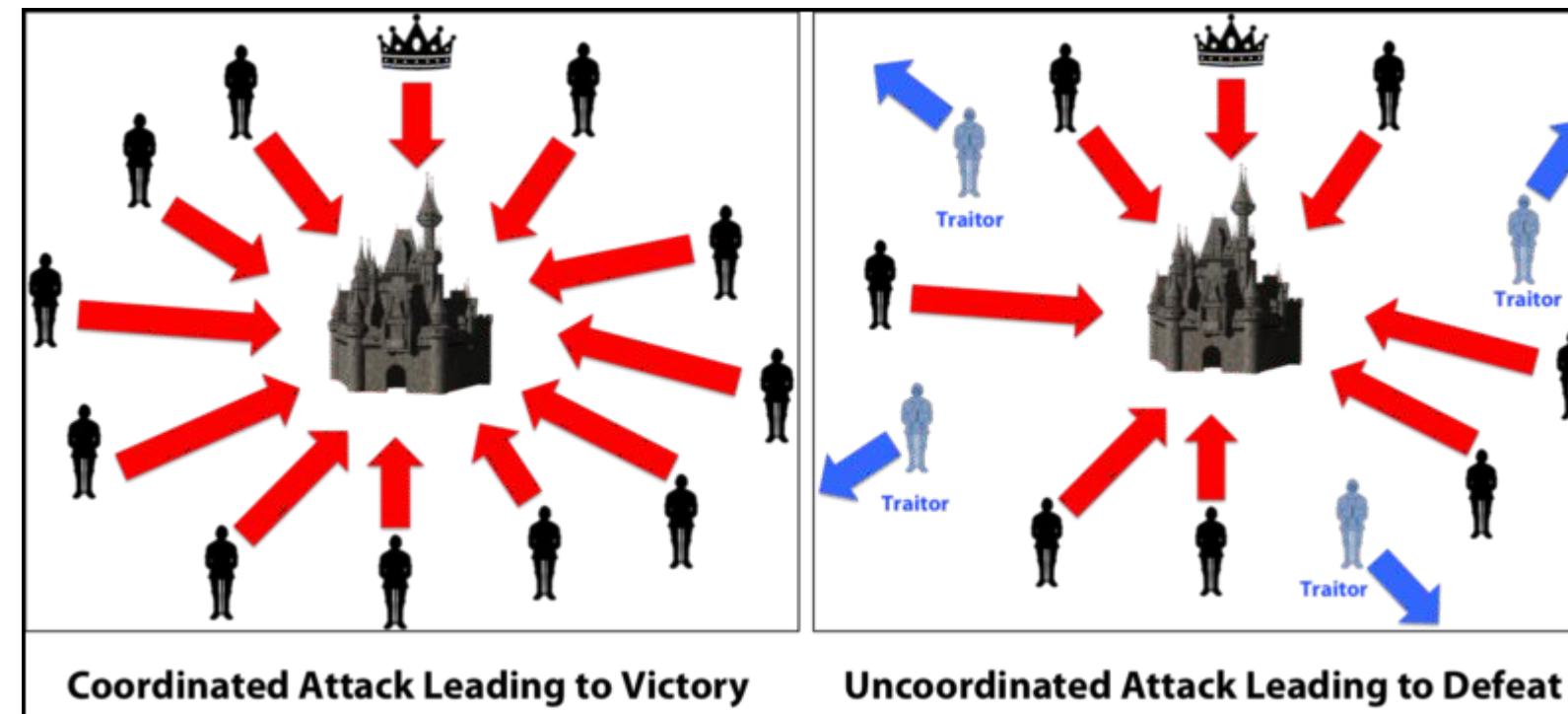
# ¿Cómo validamos una página del Ledger?



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

# Consenso en sistemas distribuidos

El problema del consenso distribuido se conoce como el Problema de los generales bizantinos



Imaginemos un conjunto de generales que quieren tomar una ciudad que tienen rodeada. La única forma de conseguirlo es que la mayoría ataquen a la vez, pero tampoco se pueden fiar de que no sea una trampa

**Hay que ponerse de acuerdo incluso sabiendo que puede haber traidores**

# Dos mecanismos de consenso

Para resolver el problema de consenso se han implementado dos mecanismos

- En los sistemas Proof of Work se busca encontrar una firma que haga cuadrar el Ledger por fuerza y error. El primero que lo consigue es premiado por ese esfuerzo
- En los sistemas Proof of Stake, el siguiente bloque del Ledger es determinístico pero se hace que tenga que ser aprobado por varios actores simultáneamente

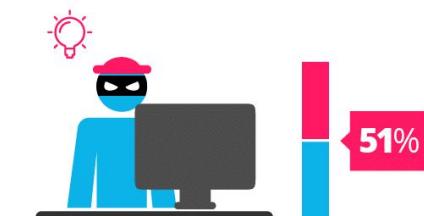
En cualquier caso, una mayoría de participantes podría alterar la cadena



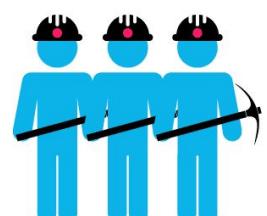
## Proof of Work



*proof of work is a requirement to define an expensive computer calculation, also called mining*

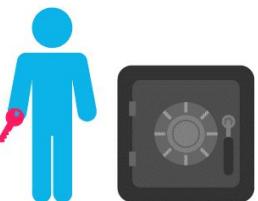


*A reward is given to the first miner who solves each blocks problem.*



*Network miners compete to be the first to find a solution for the mathematical problem*

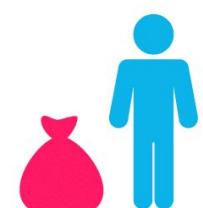
## vs Proof of Stake



*Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.*



*The PoS system there is no block reward, so, the miners take the transaction fees.*



*Proof of Stake currencies can be several thousand times more cost effective.*

**Se usan funciones hash como mecanismo de Proof-of-Work a la hora de crear nuevos bloques**

**Se utilizan firmas digitales y hashes para resumir la cadena anterior**

**Los monederos se gestionan mediante criptografía de clave pública.**

**El identificador de un monedero es un hash de la clave pública del monedero**

**Se utilizan sistemas criptográficos de no repudio para establecer consenso**

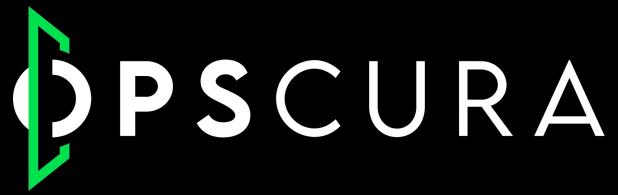


**Ninguno de los elementos técnicos son nuevos, pero la combinación de todos ellos sí lo es.**

# Dos mecanismos de consenso

- No es escalable (aunque se está trabajando en mejorarla)
- Gran coste energético (PoS más eficiente que PoW)
- Baja velocidad de verificación
- Inmutable: no compatible con derecho al olvido
- No hay un marco regulatorio (hay algún avance en este sentido)
- Brechas de seguridad en los smart contracts (peligroso por inmutabilidad)
- Permite transacciones con desconfianza mutua pero hay pocos mercados que funcionen con desconfianza mutua (pocos casos de uso en los que se usen como método de pago)





# Criptografía post-cuántica o “quantum-safe”

# Que es la computación cuántica

A diferencia de los ordenadores clásicos que se basan en transistores, los ordenadores cuánticos se basan en Qubits

Los qubits se basan en el principio de superposición, una partícula puede estar en varios estados “a la vez”. Hasta que no haga una medida, no me quedará con un único estado.

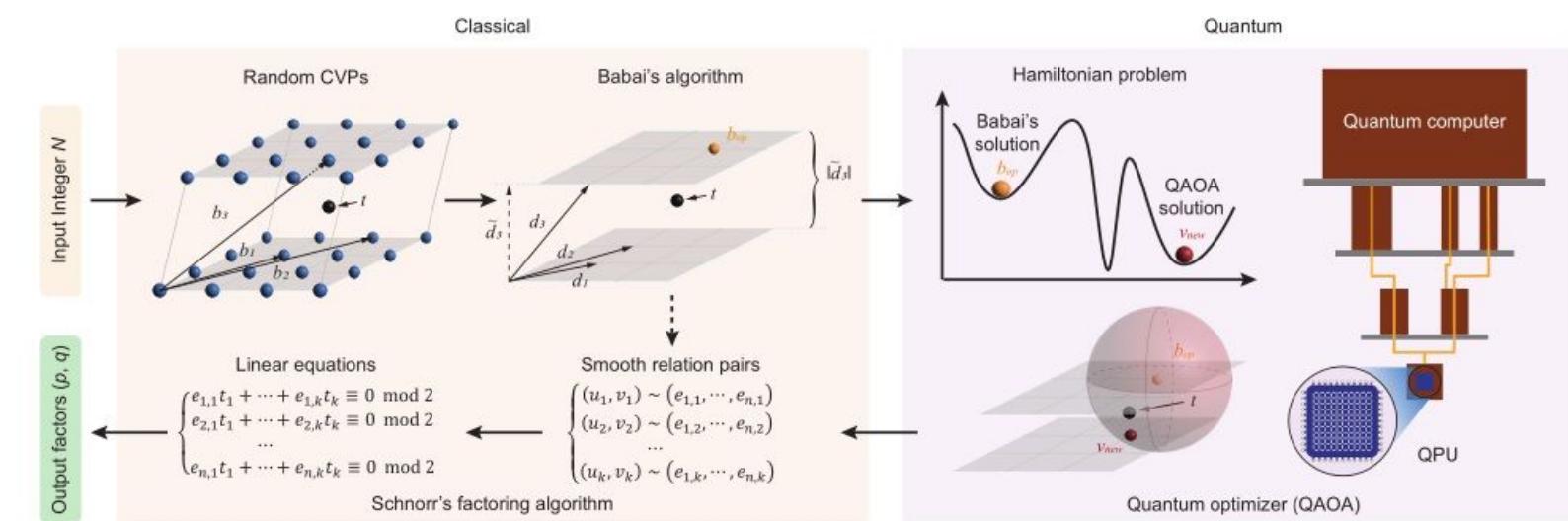
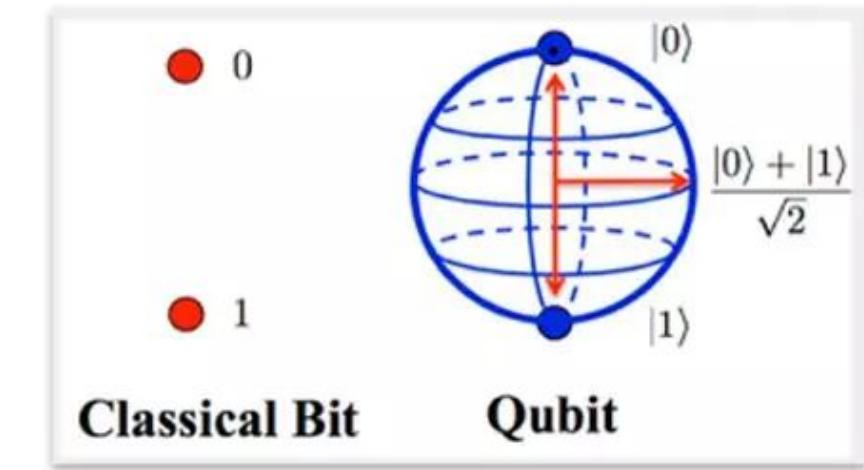
¡Las operaciones se convierten en probabilísticas!

# Qubits

Operadores de Pauli - son características de un sistema cuántico.

Puedo definir estados “a discreción”.

Para representar esa información se usa la Esfera de Bloch

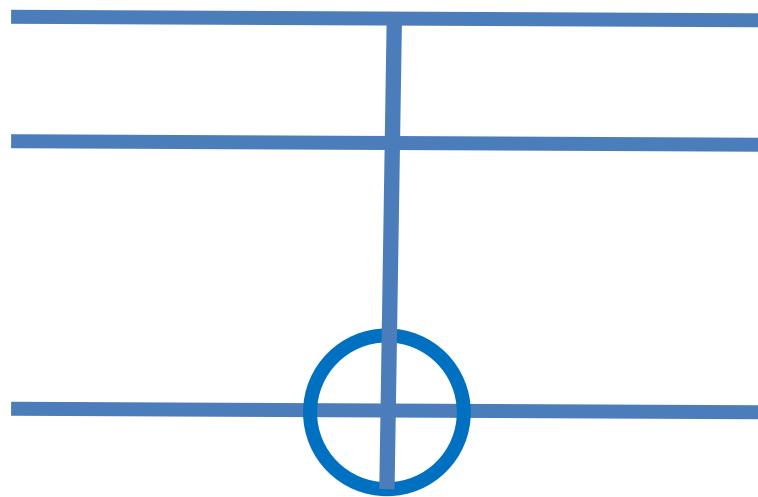


# Puertas lógicas cuánticas

Permiten hacer operaciones con qubits.

Son análogas a las puertas lógicas clásicas.

A diferencia de las clásicas, permiten operaciones con estados indeterminados.



Puerta de Toffoli  
CCNOT

# ¿En qué afecta la computación cuántica a la criptografía?

- La criptografía de clave pública se basa en números primos
- Para romper la criptografía de clave pública necesito factorizar la clave en los números primos que he usado para crearla (Shor)
- ¿Que necesitaría para factorizar una clave pública RSA de 2048 bits usando un ordenador cuántico?
  - Se creía que serían necesarios al menos 10.000 Qbits
  - Investigadores chinos en cambio publicaron en diciembre de 2022 que sería suficiente con 372 Qbits.
  - En 2025 se comercializará el primer ordenador cuántico de 4158 Qbits

**¡La computación cuántica tiene sobre la criptografía actual el mismo efecto que tuvo la computación clásica sobre los cífrados de sustitución!**

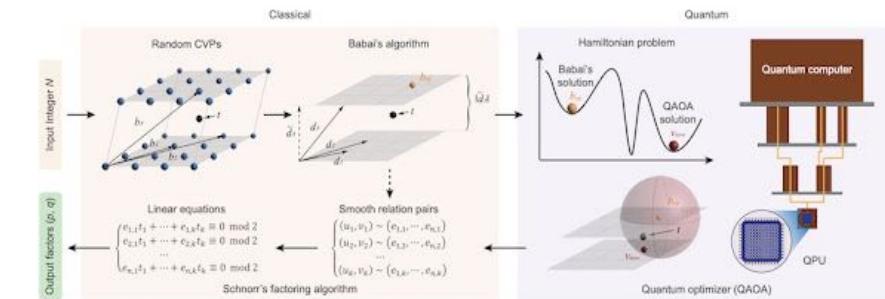


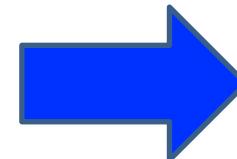
FIG. 1. Workflow of the sublinear-resource quantum integer factorization (SQIF) algorithm. The algorithm adopts a “classical+quantum” hybrid framework where a quantum optimizer QAOA is used to optimize the classical Schnorr’s factoring algorithm. First, the problem is preprocessed as a closest vector problem (CVP) on a lattice. Then, the quantum computer works as an optimizer to refine the classical vectors computed by Babai’s algorithm, and this step can find a higher quality (closer) solution of CVP. The optimized results will feedback to the procedure in Schnorr’s algorithm. After post-processing, finally output the factors  $p$  and  $q$ .

RSA number	Qubits	Kn-depth	2DSL-depth	LNN-depth
RSA-128	37	113	121	150
RSA-256	64	194	204	258
RSA-512	114	344	357	458
RSA-1024	205	617	633	822
RSA-2048	372	1118	1139	1490

# Recomendaciones

Asimétrica - FIPS 186-4, SP 800-56A/56B

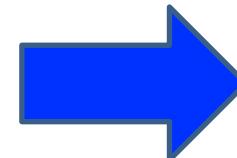
- RSA
- Elliptic Curve Cryptography (ECDSA)
- Finite Field Cryptography (DSA)
- Diffie-Hellman key Exchange



ROTO

Simétrico - FIPS 197, SP 800-57

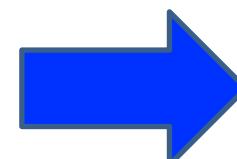
- AES
- Triple DES



X2 CLAVE

Hash - FIPS 180-4, FIPS 202

- SHA-1, SHA-2 and SHA-3

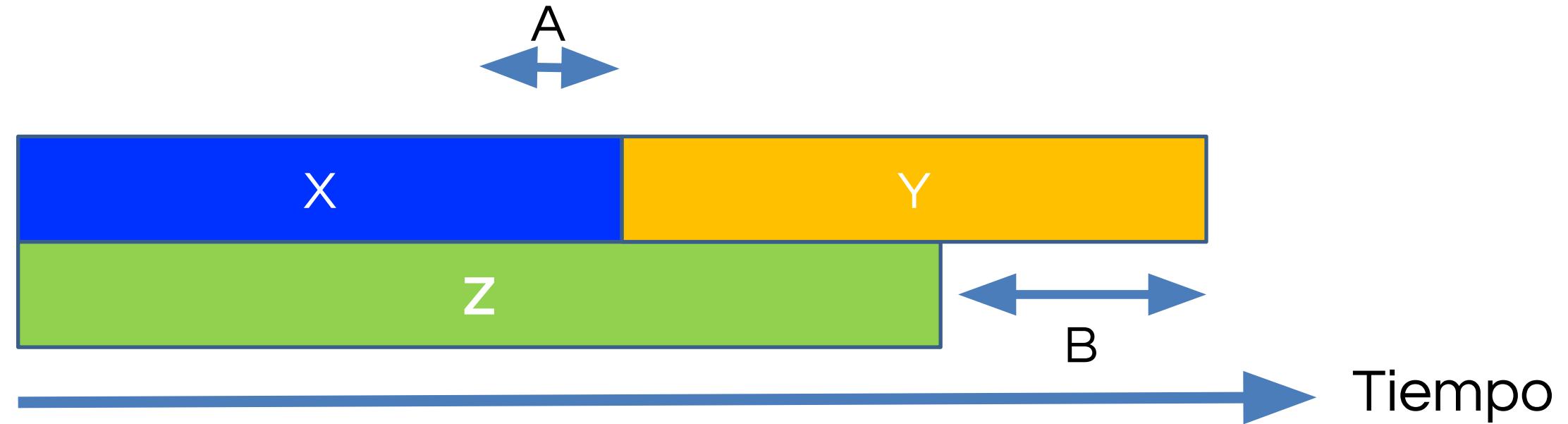


AUMENTAR  
CLAVE

# Teorema de Michele Mosca

A = ¿Qué hacemos ahora?

B = Cuánto tiempo estamos al descubierto?



X = sustituir infraestructura

Y = necesidad de seguridad

Z = ordenador cuántico

# Iniciativas quantum-safe

NSA > nuevos programas e iniciativas

<https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm>

Europa > PQCrypto Project - WITDOM

ETSI > Nuevas iniciativas y workshops – Junio 2016

IETF > Preparando RFC sobre firmas basadas en funciones hash

ISO > Nueva iniciativa

NIST > report y nueva call para cifrados post-cuánticos

# Sistemas Clave Pública “quantum safe”

Funciones Hash > Sistemas de clave pública basados en firma – Merkel, 1979

Aleatorización > Códigos de Goppa binarios – McEliece, 1978

Lattices > NTRU – Hoffstein, Pipher, Silverman, 1998

Ecuaciones Cuadráticas Multivariadas > HFEv – Patarin, 1996

# ¿Por qué la matemática caótica es “quantum-safe”?

**Opscura ha desarrollado y patentado un sistema de criptografía basado en matemática caótica 20 veces más eficiente que los estándares actuales**

Sensitividad a las condiciones iniciales:

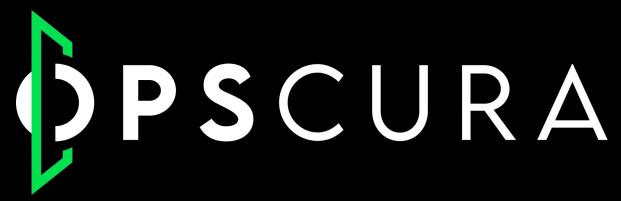
- Una pequeña variación en las condiciones iniciales implica grandes cambios.

Impredicibilidad:

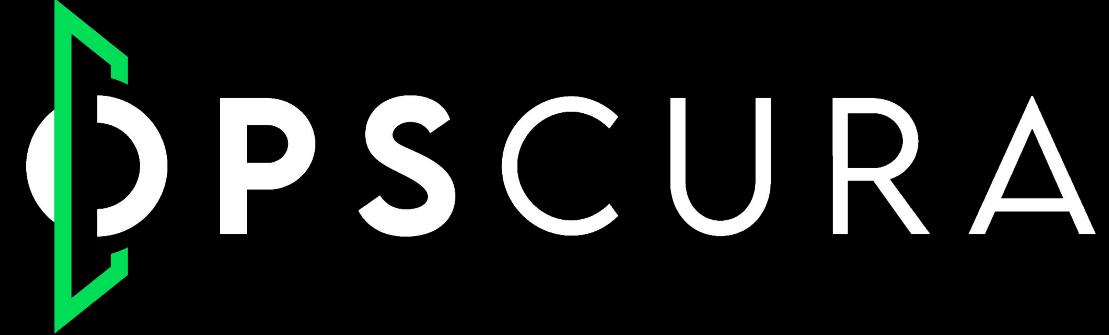
- Es imposible de predecir el Sistema con precisión infinita.

Propagación del error:

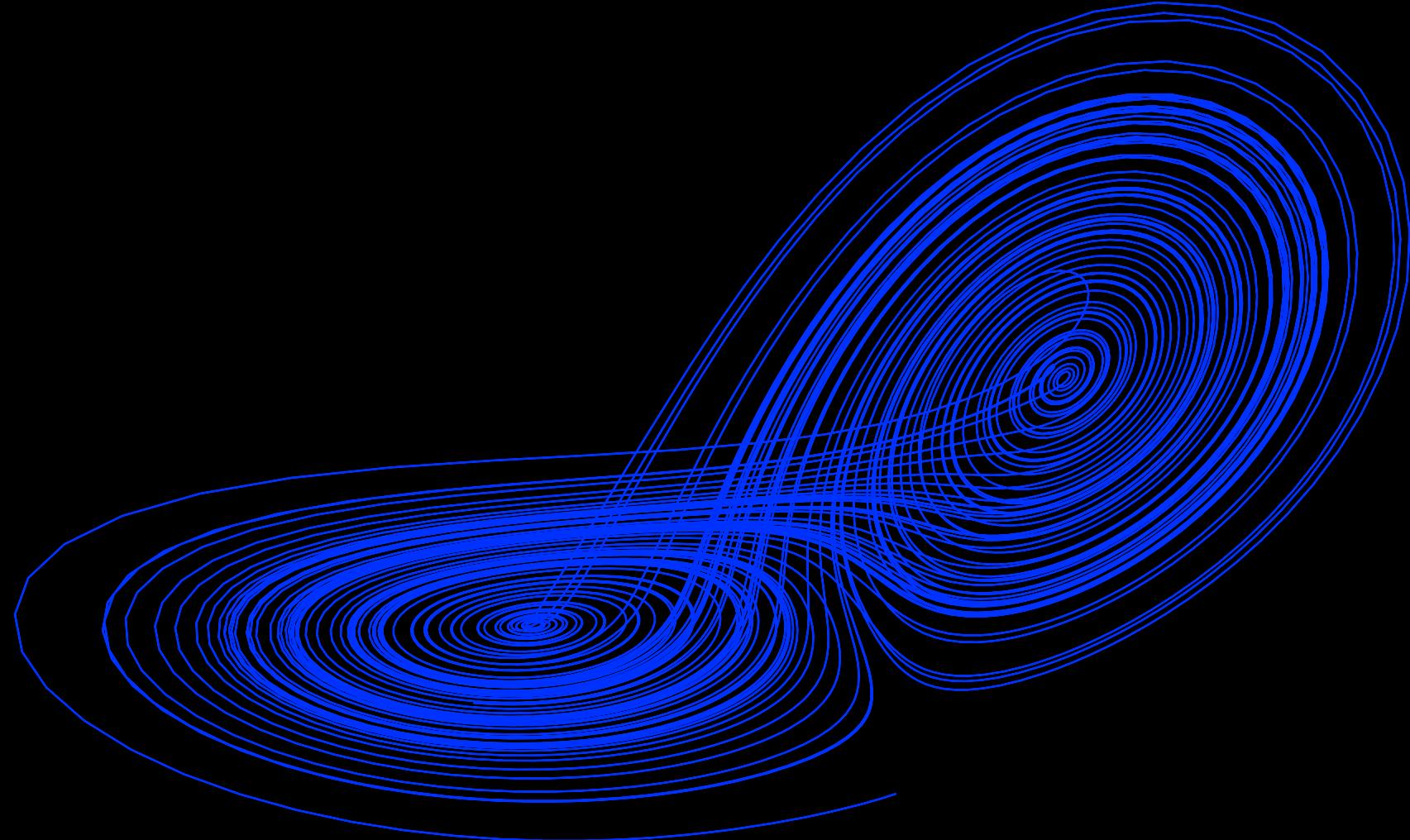
- Un pequeño error aumenta de forma exponencial.



# Preguntas



Carlos Tomás Moro | [carlos@opscura.io](mailto:carlos@opscura.io)  
Co-Founder & VP Engineering



Get Cloaked. Frictionless Protection for Industrial Networks.