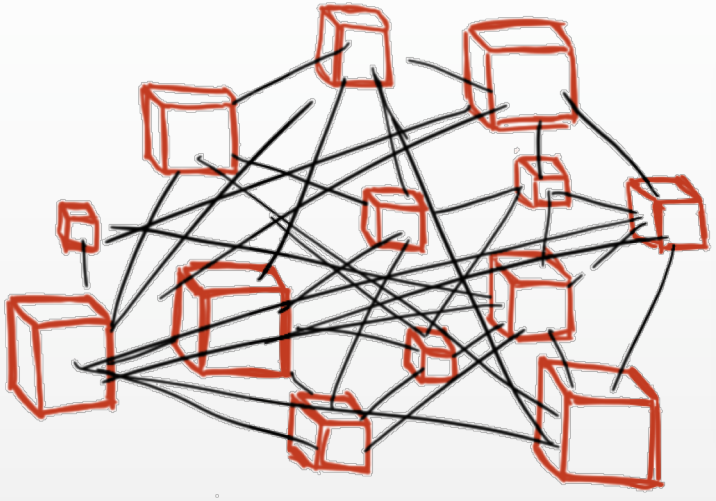
Santander

BLOCKCHAIN EN LOS SERVICIOS FINANCIEROS

Jornadas de Tecnología, Universidad de Cantabria, 5 April, 2019

SANTANDER BLOCKCHAIN CENTER OF EXCELLENCE

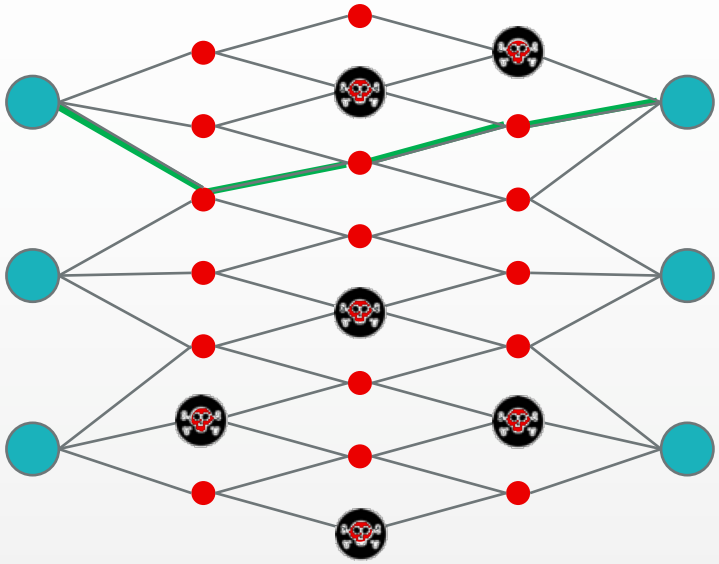


BLOCKCHAIN
EL INTERNET DEL VALOR

LA 4ª REVOLUCIÓN INDUSTRIAL

INTERNET: LA REVOLUCIÓN DE LAS COMUNICACIONES

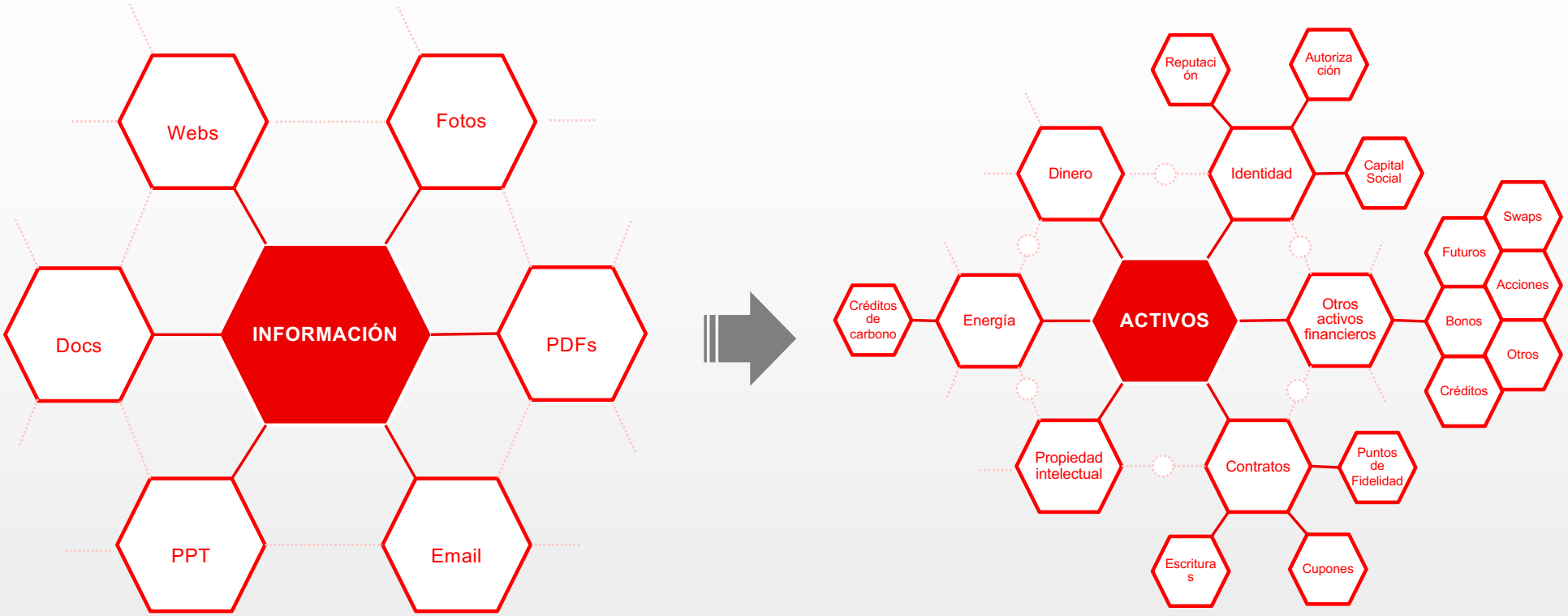
Red centralizada



Red distribuida

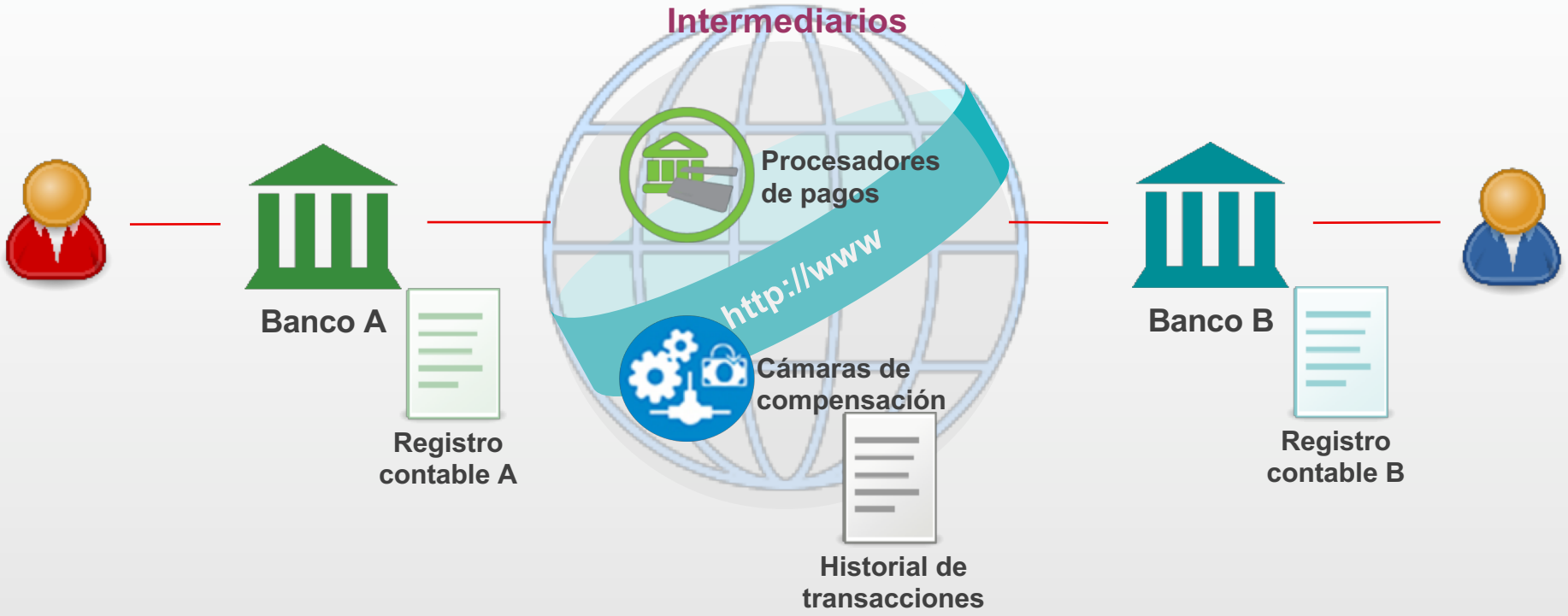
DEL INTERNET DE LA INFORMACIÓN

AL INTERNET DEL VALOR



EL VALOR VIVE EN LAS ENTIDADES DE CONFIANZA

- El **valor** (i.e. la propiedad de los activos) vive en **registros** (o bases de datos o *ledgers*)
- Las **entidades de confianza** (ej. bancos) operan dichos registros
- **Internet** es sólo la **capa de comunicación** entre dichas entidades



CON BLOCKCHAIN EL VALOR VIVE EN LA COMUNIDAD

- Registro único y compartido

  → única versión de la verdad

- Sin necesidad de confiar unos en otros
- Híper-replicado

  → resistente, inmutable y aún así barato

- En tiempo real

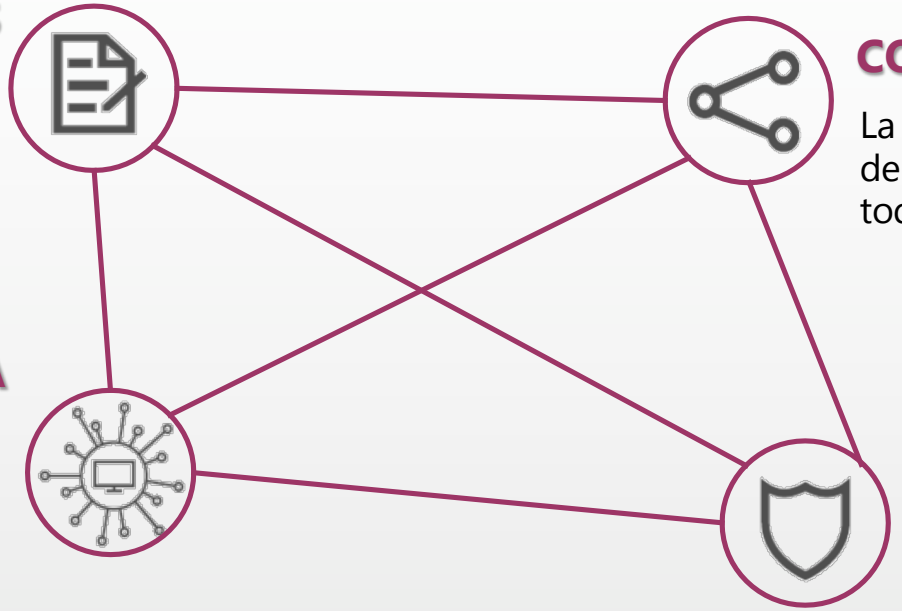
Rápido, barato, seguro e interoperable

ENTONCES, QUÉ ES EL BLOCKCHAIN?

- Es una base de datos segura, compartida y distribuida, que registra la propiedad de cualquier tipo de activo (no sólo financieros)

BASE DE DATOS

Esta base de datos sólo permite añadir transacciones, por lo que es un registro inmutable de todas las transacciones ocurridas.



COMPARTIDA

La misma copia de la base de datos se distribuye a todos los participantes.

DESCENTRALIZADA

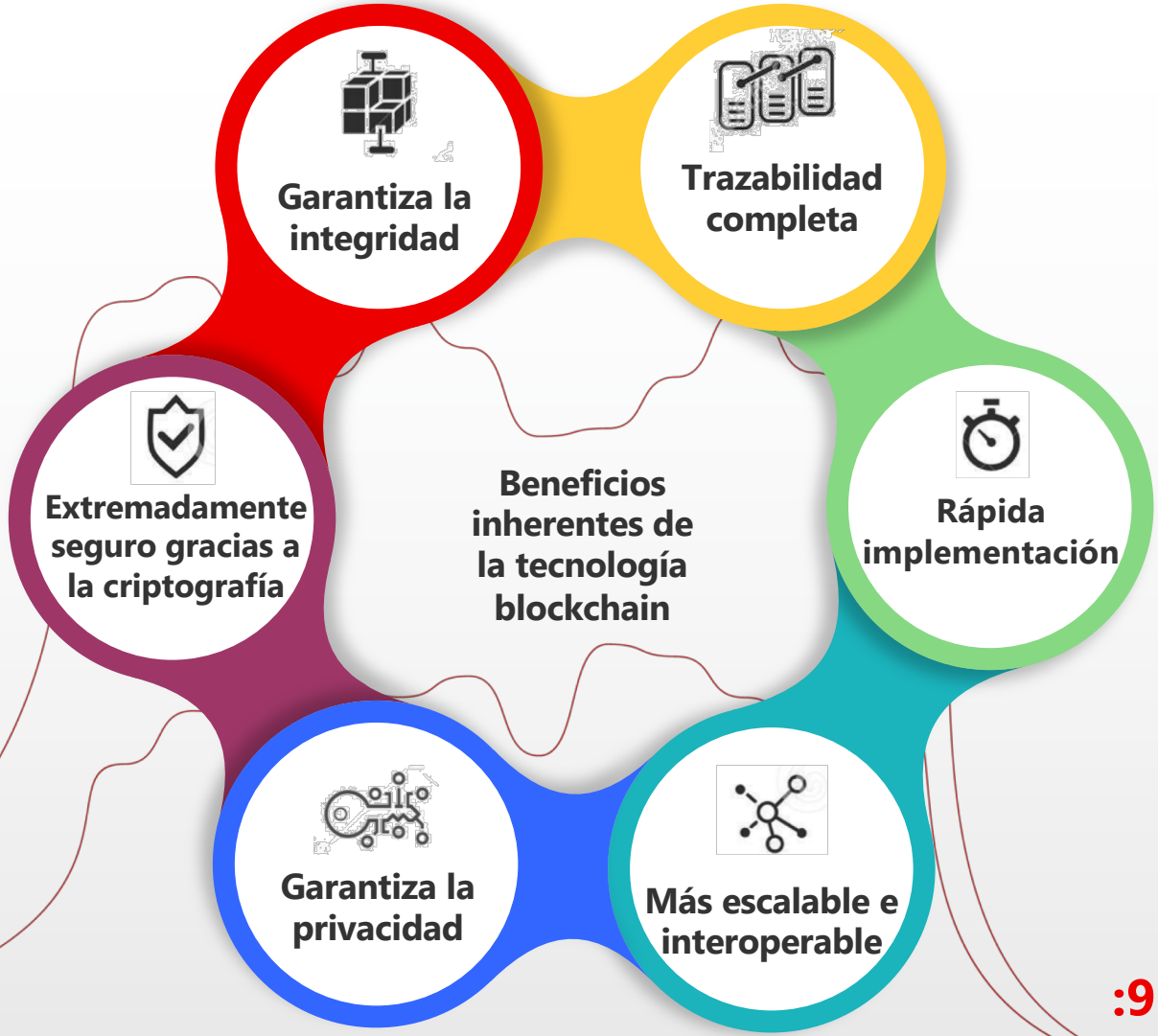
No existe un operador central. Los participantes llegan al consenso en cuál es el estado de la base de datos en cada momento.

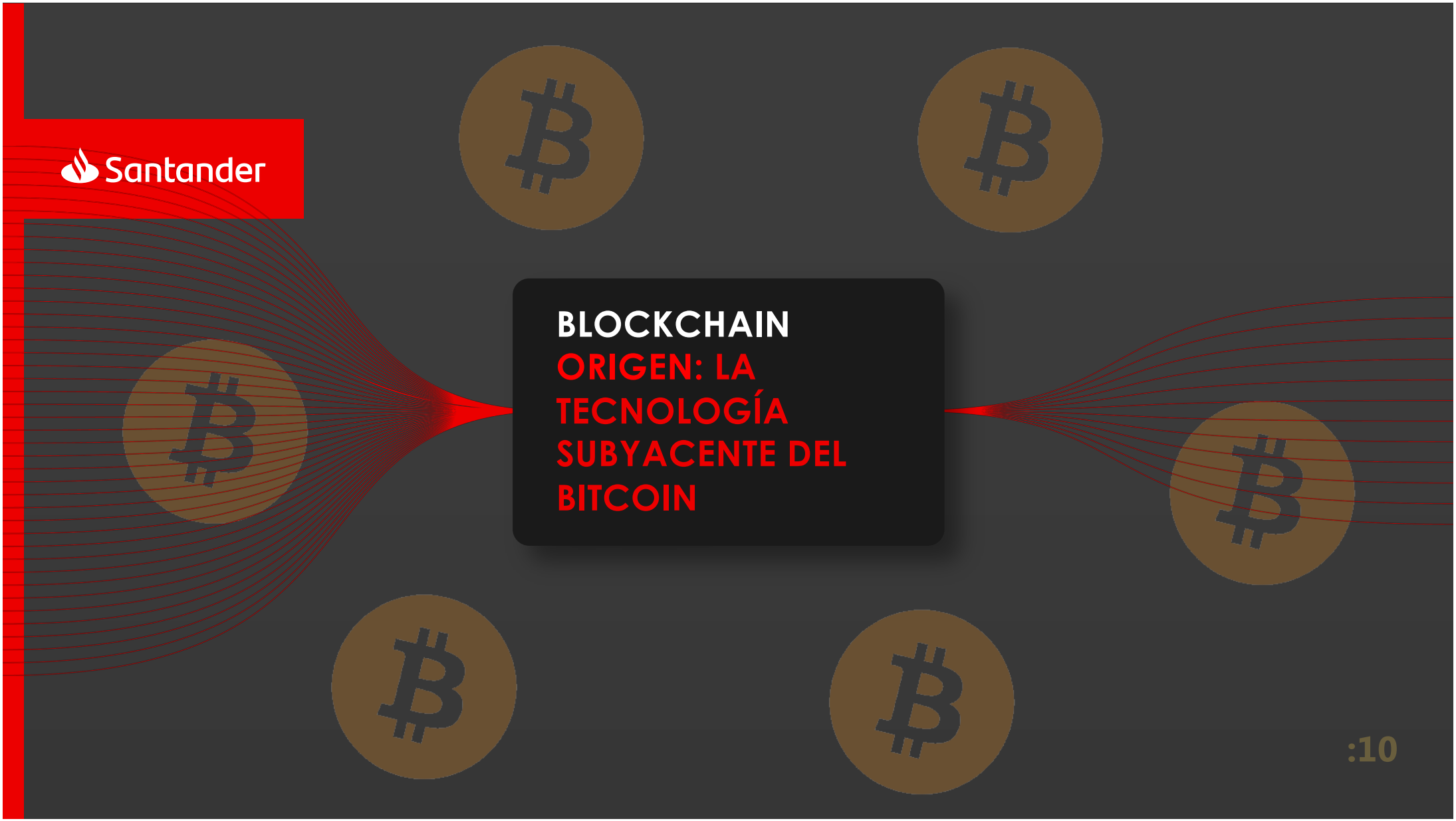
SEGURA

Usa la criptografía para crear transacciones que son inmunes al fraude.

POR QUÉ INTERESA TANTO ESTA TECNOLOGÍA?

- Altamente **resistente** a ataques externos.
- **Elimina reconciliaciones** y disputas.
- Simplifica mucho los **procesos** que implican **varios participantes** en localizaciones diferentes con diferentes intereses (evita canales paralelos).
- Permite crear **nuevos negocios** y servicios que actualmente no son posibles.




Santander
BLOCKCHAIN
ORIGEN: LA TECNOLOGÍA SUBYACENTE DEL BITCOIN
:10

BITCOIN: LA 1ª APLICACIÓN DE LA TECNOLOGÍA BLOCKCHAIN

BBDD segura y distribuida

Historial de transacciones completo e inmutable

Única versión de la verdad

Protocolo de comunicación

Los nodos llegan al consenso sobre el estado de la base de datos

Un token digital (o 'moneda') usada como

Incentivo para procesar transacciones

Mecanismo anti-spam

¿Cómo consigue Bitcoin establecer confianza en el envío de transacciones sin intermediarios?

:11

BITCOIN PERMITE TRANSACCIONES P2P SIN INTERMEDIARIOS ESTABLECIENDO CONFIANZA GRACIAS A:

CRIPTOGRAFÍA

- Los activos digitales quedan protegidos por **firmas digitales** y **hashes**.
- Garantiza la **integridad** del BBDD, la **autenticidad** de las transacciones y la **identidad** de los participantes.

GARANTIZA LA SEGURIDAD

COLABORACIÓN

- Red de **nodos interconectados** que comparten la **misma BBDD** distribuida.
- Solo aquellas transacciones **validadas por la mayoría** se incluyen en la base de datos.

SIN NECESIDAD DE UN CERTIFICADOR

CÓDIGO

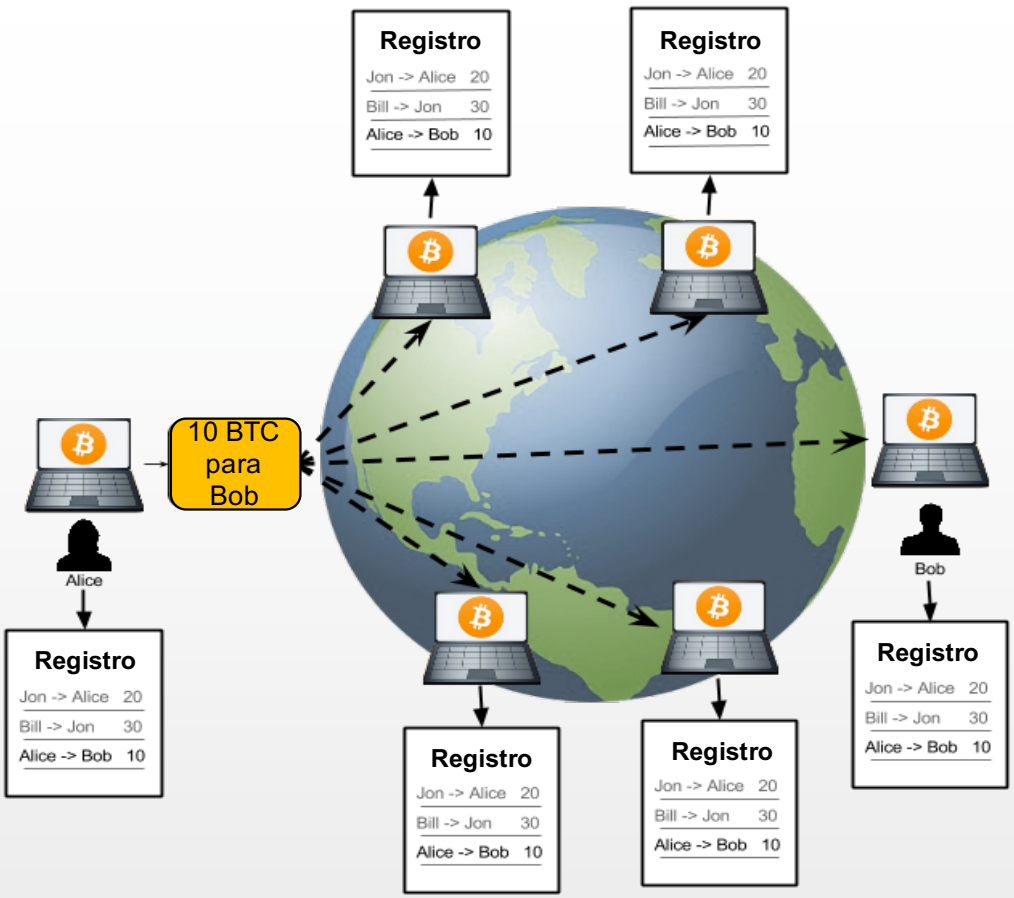
- **Distribuido** y **replicado**
- BBDD que **sólo** permite **agregar** transacciones, y contiene el historial inmutable de todas las transacciones: se detectan fácilmente las transacciones erróneas

IMPOSIBLE DE MANIPULAR

ÚNICA FUENTE DE LA VERDAD

TODOS LOS PARTICIPANTES MANTIENEN EL MISMO REGISTRO

- Red de participantes (“mineros”) interconectados que mantienen una **misma lista** de las transacciones que han sucedido hasta el momento.
- Sólo las **transacciones validadas por la mayoría** son registradas.
- De esta forma, el sistema **no depende de ningún participante en particular** sigue funcionando mientras la mayoría de los participantes sean honestos y sigan validando las transacciones.

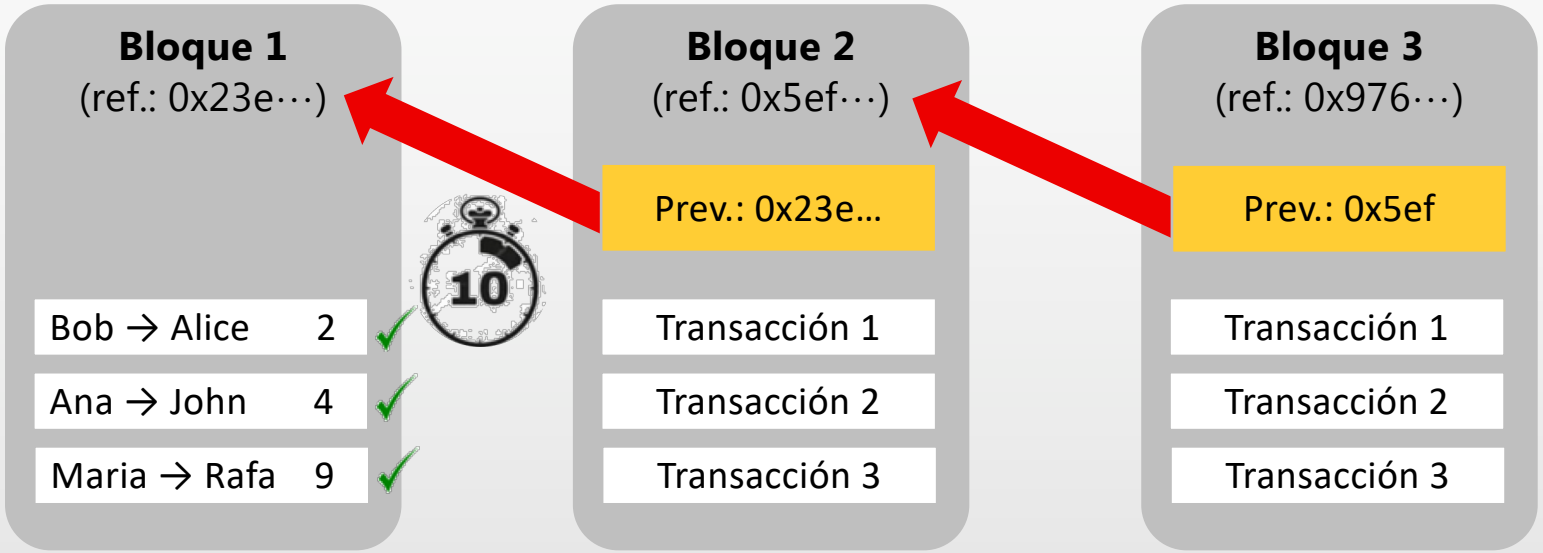


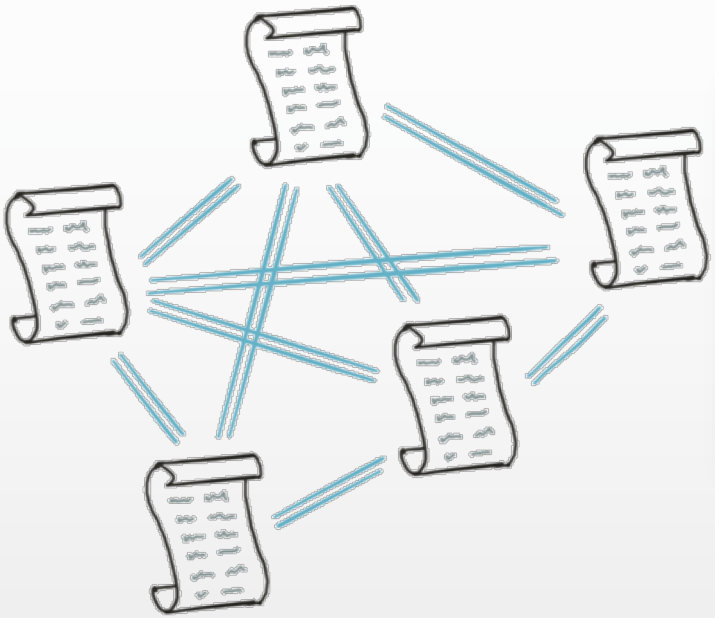
¿QUIÉNES SON LOS MINEROS?

- Los mineros son participantes de la red, que tienen un papel crucial en cualquier sistema de criptomonedas, pues son los **responsables de validar y agrupar** transacciones en **bloques**, **retransmitirlas** y **registrarlas**.
- Emplean un alto poder computacional necesario para **resolver un puzzle criptográfico** que se requiere al validar cada bloque. El primer minero en resolverlo, **recibe una recompensa**, que actualmente es de 12,5 BTC y que va disminuyendo a la mitad cada 4 años.
- Además, los mineros **reciben comisiones** de los usuarios por cada transacción ejecutada.

¿POR QUÉ SE LLAMA BLOCKCHAIN (CADENA DE BLOQUES)?

- Las nuevas transacciones se envían a la red de validadores ("mineros"), que las comprueban y descartan las incorrectas. **Las transacciones correctas son agrupadas en bloques**.
- Cada 10 minutos (aprox.) se genera un bloque nuevo.
- Y cada bloque contiene una **referencia al bloque anterior**, formando una "cadena de bloques" .
- Si se intentara cambiar una transacción pasada, la referencia de su bloque cambiaría y el resto de validadores lo detectaría inmediatamente. Por ello se dice que es un registro **INMUTABLE**.





UNA INNOVACIÓN ADICIONAL: LOS 'SMART CONTRACTS'

MÁS ALLÁ DE LAS CRIPTOMONEDAS: PROGRAMAS (Y DATOS) EN LA BASE DE DATOS COMPARTIDA

CRIPTOMONEDAS (EJ. BITCOIN)

Llave pública	Cantidad
Llave pública	Cantidad
Llave pública	Cantidad
Llave pública	Cantidad
…	…

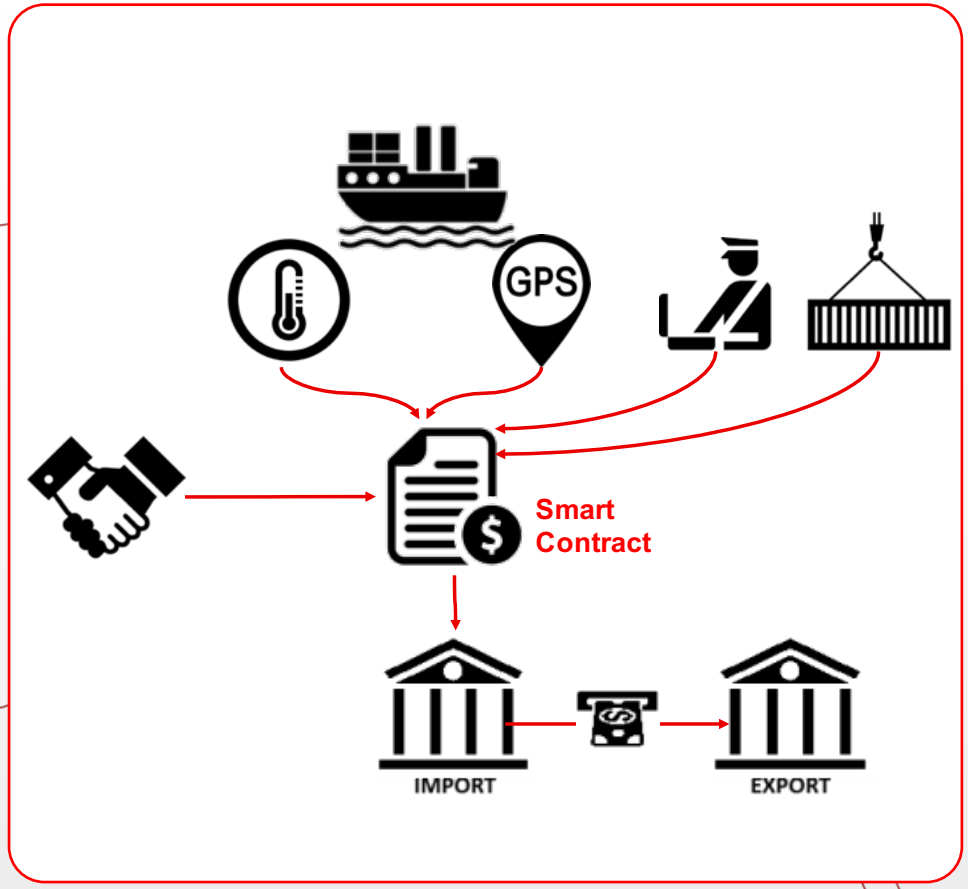
- La base de datos almacena cantidades de criptomoneda

SMART CONTRACTS (EJ. ETHEREUM)

```
contract cryptobank {
    mapping(address => uint) public balance;
    function transfer(uint amount, address receiver)
        if(balance[msg.sender] >= amount) {
            balance[msg.sender] -= amount;
            balance[receiver] += amount;
        } else {
            throw;
        }
    }
    ...
```

- La base de datos almacena programas y datos (que pueden representar cualquier cosa)
- Estos programas pueden interactuar unos con otros
- Pueden incluir criptomonedas, que suelen ser usadas para pagar a los nodos por el consumo computacional y energético

EJEMPLO



APLICACIONES DE BLOCKCHAIN EN LA EMPRESA

BLOCKCHAIN PARA USO EMPRESARIAL:
REDES PÚBLICAS VS. REDES PRIVADAS/PERMISIONADAS

REDES PÚBLICAS

1. Completamente **abiertas**. Cualquiera puede unirse y participar. No están controladas por nadie.
2. Todos los datos son **públicos**.
3. Tienen su **propio token o criptomoneda**, usado para pagar las comisiones de las transacciones y como incentivo a los participantes (Mineros)

bitcoin ethereum XRP

NO INTERESANTES PARA LOS BANCOS

REDES PRIVADAS/PERMISIONADAS

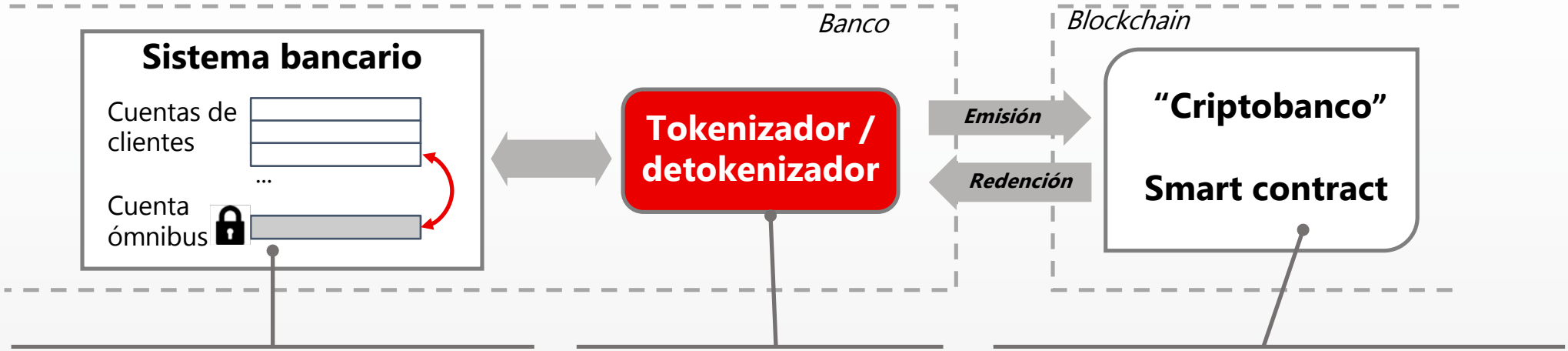
1. **Operadas por organizaciones** o consorcios de organizaciones. Son sólo accesibles con permiso.
2. Son esencialmente bases de datos **privadas** estructuradas como un registro distribuido. La información se mantiene **confidencial**.
3. **Pueden o no tener** asociado un **token**, pero no tiene valor intrínseco.

Quorum™ HYPERLEDGER c·rda Digital Asset

FOCO DEL BLOCKCHAIN LAB DEL SANTANDER

:20

TOKENIZACIÓN: BLOCKCHAIN ÚTIL EN EL MUNDO REAL



- Los activos reales a tokenizar se quedan bloqueados en una cuenta ómnibus
- Traduce los activos reales en tokens
- Mantiene los balances de los clientes, respaldados 1 a 1 con los fondos almacenados en el banco.
- Los activos son ahora digitales y se puede operar con ellos globalmente e interactuar con otros smart contracts.)

Cualquier activo (a parte del dinero) se puede tokenizar!!

MULTITUD DE CASOS DE USO EN TODOS LOS SECTORES

Identidad

Sistema de gestión de identidad seguro, donde la información personal es totalmente controlada por el propietario

Votaciones

Voto digital, permitiendo gestionar la identidad, mejorar la trazabilidad, menor fraude y recuento inmediato

Historial académico

Registro digital del historial académico, compartido entre instituciones académicas, seguro y portable.

Registro de la propiedad

Base de datos segura para el registro de la propiedad de: viviendas, arte, diamantes, coches, etc.

Música y medios

Los archivos de música, películas, etc. protegidos con criptografía, con sus derechos de autor y funcionalidad de pago integrados.

Micropagos

Actualmente los pagos de cantidades muy pequeñas no son posibles y son clave para el IoT y los servicios digitales.

• • •


Santander
APLICACIÓN REAL
DEL BLOCKCHAIN
(CASO SANTANDER)

Santander shows potential of blockchain in company votes

Spanish bank points to way to improving annual meetings

Santander's blockchain service challenges SWIFT's dominance

Santander Explores Blockchain's Potential Uses

Spanish bank aims to launch platform for international payments this year

Santander experimenta con una aplicación blockchain para micropagos

28-03-2018 El banco español está avanzando rápidamente con diversos proyectos relacionados con la digitalización y la utilización de criptomonedas

Santander launches blockchain-based foreign exchange service

Santander se une a cinco entidades para impulsar el dinero digital

Seis gigantes financieros promoverán sistemas de intercambio económico basados en la tecnología 'blockchain'

:24

¿POR QUÉ ES RELEVANTE PARA SANTANDER?

Nos proporciona la oportunidad de innovar eficientemente por fuera de la infraestructura core bancaria existente

Gracias al poder de la criptografía, es inherentemente seguro. Doblemente seguro cuando se combina con la seguridad bancaria existente.

Otros bancos están participando en los mismos ledgers distribuidos, promoviendo un entorno de colaboración y coopetición.

Multitud de casos de uso interesantes para aplicar esta tecnología, particularmente aquellos que son lentos, caros y propensos a errores.

La topología de la red de Santander es perfecta para la aplicación del blockchain

¿DÓNDE ESTAMOS?

Todo sobre Bitcoin (y la posible amenaza al sistema financiero)

Blockchain – no Bitcoin

Bancos (y no bancos)

PoCs en todos los sectores:

- Finanzas
- Supply chain
- Energía
- Salud
- …

Pilotos (a escala limitada, pero reales)

Necesidad de **blockchains adecuados al uso empresarial**

¡Camino de **Producción!**

Comercialización de las primeras aplicaciones

:26

MULTITUD DE CASOS DE USO BAJO ANÁLISIS…

*Oportunidades significativas de obtención de **eficiencias**, **reducción de consumo de capital** y creación de **nuevos productos y servicios***

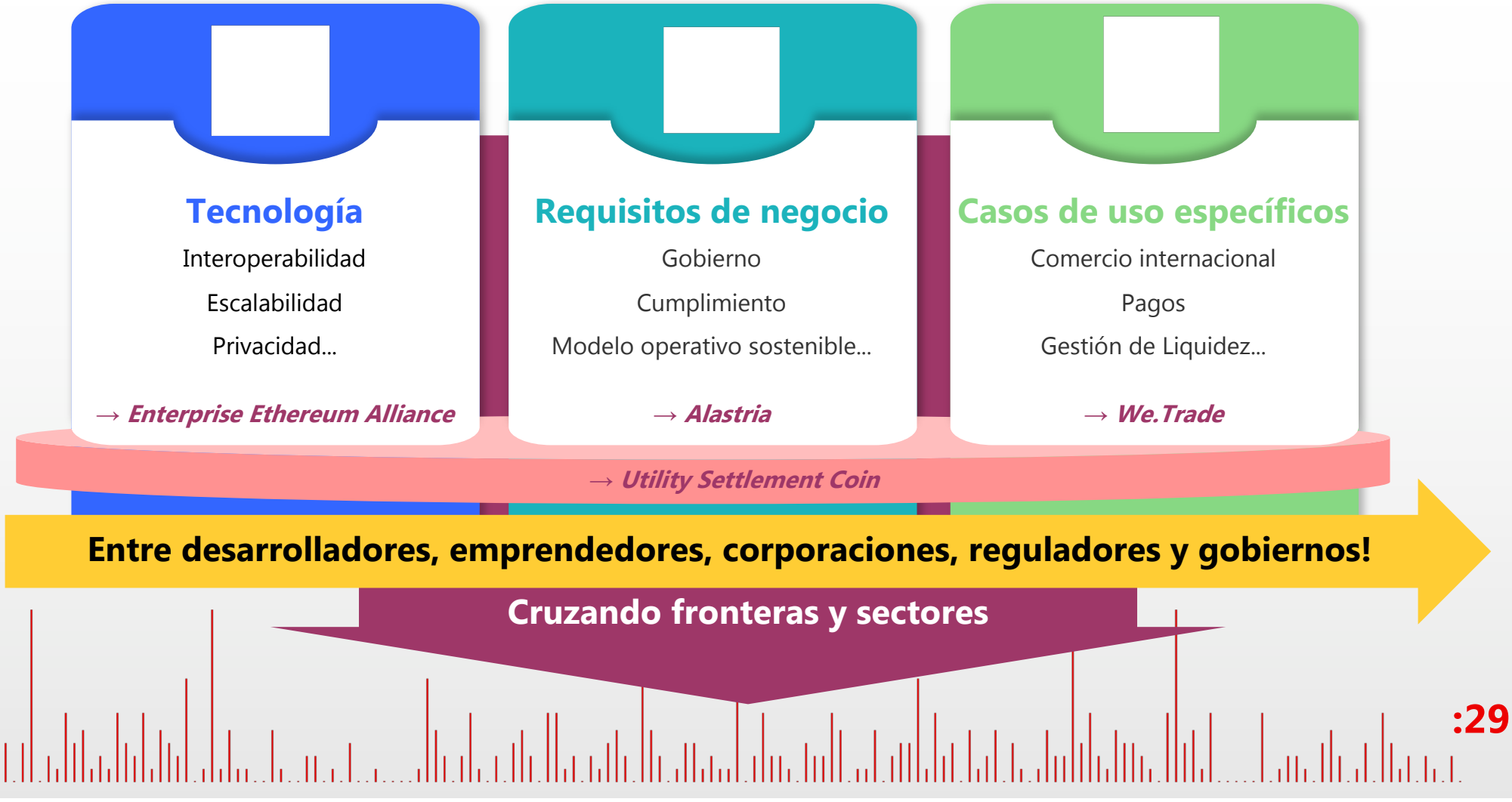
…PERO NO ES NECESARIO "BLOCKCHEINIZAR" EL MUNDO

Tres preguntas que contestar:

1. Es **lento**?
2. Es **caro**?
3. Es **propenso a errores**?

Cualquier proceso transaccional que es LENTO, CARO *y* PROPENSO A ERRORES *es potencialmente mejorable con la tecnología blockchain*

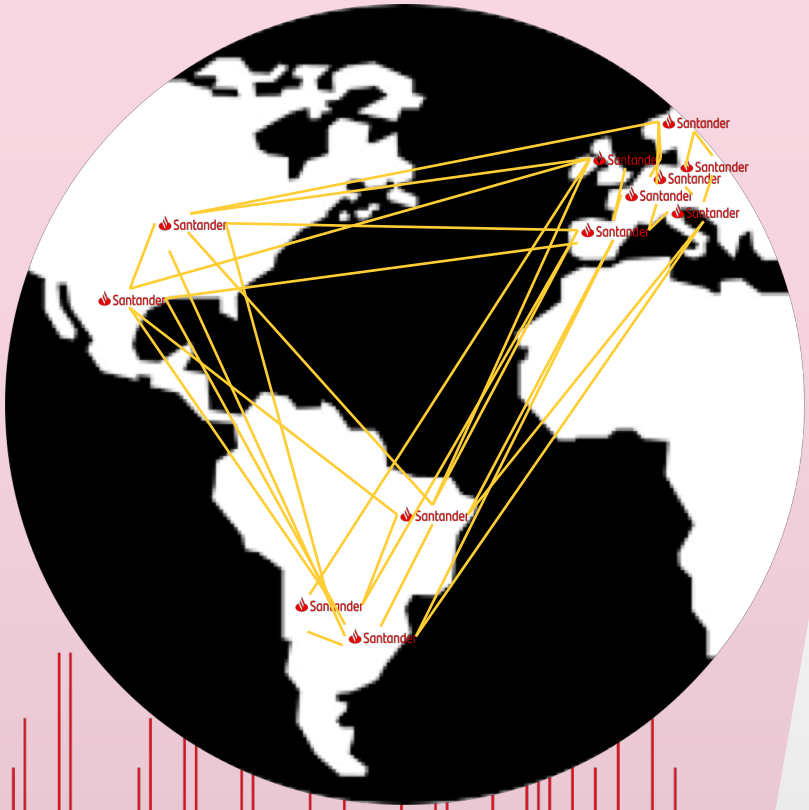
LA COOPETICIÓN ES CLAVE PARA EL ÉXITO



:29

EQUILIBRIO ENTRE PROYECTOS INTERNOS Y CONSORCIOS

Nuestra presencia geográfica y modelo de sucursales hace interesante la aplicación de blockchain



we.trade
more trust. more trade.

ALASTRIA

ENTERPRISE ETHEREUM ALLIANCE

USC
Utility Settlement Coin

FTL
Fast Track Listing

:30

GRACIAS!!

María de la Concepción de Monteverde

Santander Blockchain Center of Excellence

/cotymonteverde