
IEBS
Innovación & Emprendedores

Blockchain para dummies

Charla: Logistics 2018

Director del Master en Blockchain y Fintech en IEBS Business School

Twitter: @ruljaimemaestre

Linkedin: https://es.linkedin.com/in/rauljaimemaestre

¿Cómo funciona Blockchain?

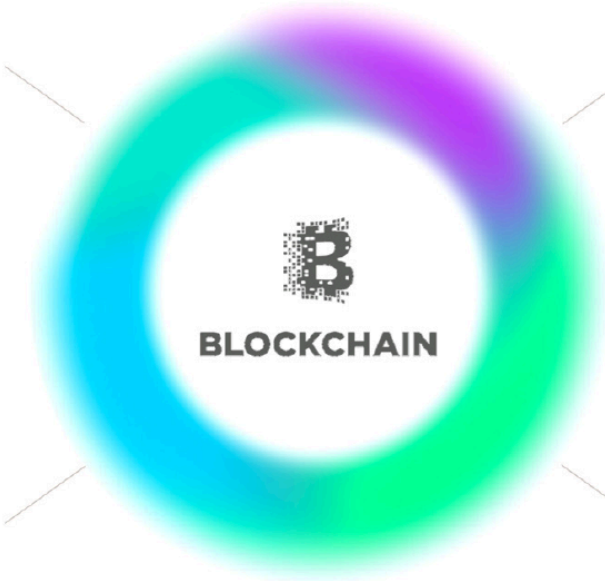
¿Qué es Blockchain?

Es un ledger distribuido

Blockchain es una base de datos descentralizada, protegida criptográficamente, en la que cada nodo tiene una copia de toda la información almacenada.

Es un paradigma de colaboración

Se reduce la fricción entre los distintos participantes en base a unas reglas bien definidas y de fácil adopción, sin necesidad de un gran nivel de acuerdo.



Es un sistema transparente

Todas las transacciones son registradas y se podrían consultar públicamente, pudiendo hacer un seguimiento del funcionamiento de la plataforma. El nivel de transparencia es modulable, pudiendo ir desde esquemas de uso anónimos, como Bitcoin, a niveles de trazabilidad alineados con la transparencia total.

Es una red de confianza

La confianza reside en el consenso entre los participantes, sin que exista la figura de un tercero.

Es un sistema inmutable

Una vez introducida, la información, no se puede modificar por parte de ningún actor implicado ni ningún administrador.

IEBS

Registro de cuentas

Registro de cuentas

- Blockchain registra y valida cada transferencia.
- Dividido por bloques las operaciones y el bloque original se denomina “bloque génesis”.
- Los mineros la mantienen vigente y coherente.
- Transacciones en tiempo real.

Registro de cuentas: descentralizado

- Blockchain es una red de libros de cuentas y cada monedero está obligado a escribir allí.
- Para validar una operación se necesita la validar por al menos el 50% de la red y se realiza la operación cuando se genera el sexto bloque.
- Los mineros reciben bitcoins por este trabajo.

Blockchain como sistema

Blockchain como sistema

- Blockchain es un sistema de confianza sin intermediarios.
- Blockchain puede gestionar cualquier tipo de valor o propiedad.

Blockchain: público

- Se elimina toda la burocracia de las operaciones.
- Blockchain elimina el control administrativo de los intermediarios.

Blockchain: Smart Property

Pasar cualquier transacción de propiedad sobre Blockchain (Ethereum - 2015)

Desde contratos, obras de arte, datos de salud, votos, propiedad intelectual, deudas, toda propiedad concebible…

Blockchain: Smart Contract

Es un contrato ejecutable por sí mismo

Blockchain permite almacenar contratos autoejecutables ajenos al control de nadie, que funcionan de manera autónoma y automática.

Es un elemento inmutable

El contrato se almacena en la cadena de bloques y se distribuye entre todos los nodos de la red, sin que pueda ser alterado por alguno de ellos.

Es un software que se ejecuta en Blockchain

Es un programa que se ejecuta en cada uno de los nodos de una red de Blockchain, de modo que el contrato se verifica dentro de un modelo de confianza distribuida, sin un tercero.

Es un código de programación

Mediante lenguaje de programación, las partes definirían el objeto del contrato, las acciones que se pueden realizar sobre él y las clausulas de aplicación.

Los siete princios esenciales de la Blockchain

Los sietes principios esenciales del Blockchain

Integridad en la red

Principio: La integridad está cifrada en todas las etapas del proceso, y no depende de cada miembro individualmente.

Problema: En Internet la gente no ha podido hacer transacciones o negocios directamente.

Posible solución: Red distribuida entre iguales y un poco de criptografía.

Poder distribuido

Principio: El sistema distribuye poder por una red de iguales sin que haya ningún punto de control.

Problema: En la primera era de Internet todas las grandes instituciones se preocuparon poco por su contrato social.

Posible solución: Cualquiera puede descargarse gratis el protocolo y tener una copia de Blockchain.

El valor como incentivo

Principio: El sistema hace coincidir los incentivos de todos los participantes.

Problema: Concentración poder de las empresas, combinado, complejidad y opacidad.

Posible solución: Participantes actúen en interés propio (teoría de los juegos).

Seguridad

Principio: Las medidas de seguridad están integradas en la red sin puntos flacos y garantiza confidencialidad y autenticidad de las actividades.

Problema: Pirateo, robo de identidad o información, fraude, ciberacoso, correo basura, programas maliciosos...

Posible solución: Participantes usen infraestructuras de clave (PKI).

Los sietes principios esenciales del Blockchain

Privacidad

Principio: Control de los propios datos.

Problema: La privacidad es un derecho humano fundamental en una sociedad libre.

Posible solución: No incorporar ningún requisito de identidad en la capa de red.

Derechos preservados

Principio: Los derechos de propiedad son trasparentes y legítimos.

Problema: Buscar maneras de ejercer los derechos más eficazmente.

Posible solución: Blockchain impide el doble gasto, confirma la propiedad de datos y cada transacción.

Inclusión

Principio: La economía funciona mejor cuando funciona para todos.

Problema: Mayoría de población sigue excluida de Internet.

Posible Solución: Solución con protocolos elementales de Internet, pero puede funcionar sin Internet.

¿Una o varias Blockchains?

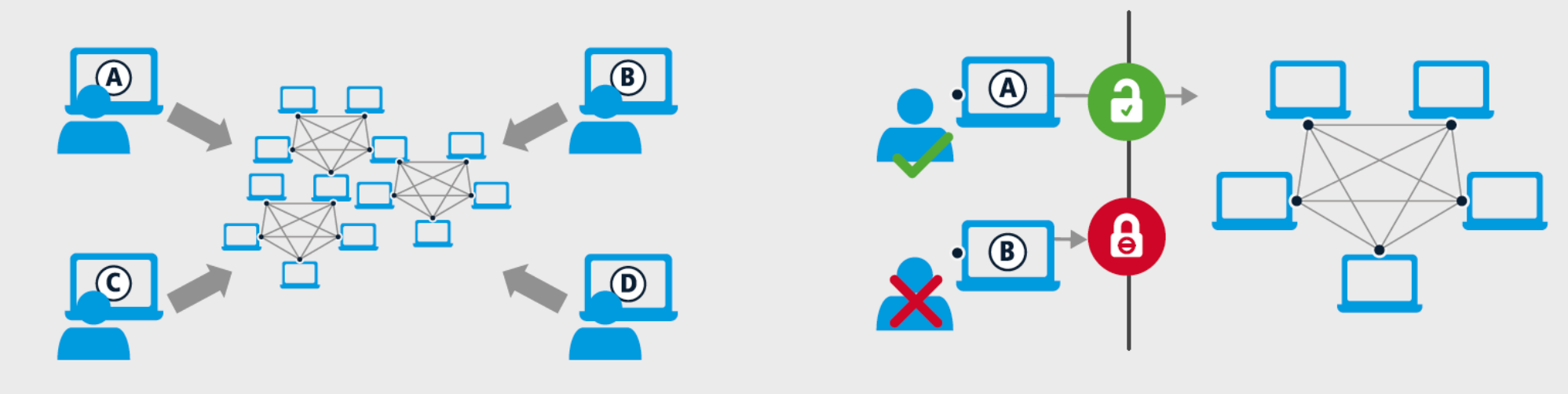
Diferentes tipos de blockchain

La tecnología blockchain existe un tipo, pero de blockchains existen varias.

Diferentes tipos de blockchain

La diferencia radica en las funcionalidades, protocolos de consenso, flexibilidad de administración de la red o las reglas para validar las transacciones.

Diferentes tipos de blockchain



Blockchain Pública

Blockchain Privada

Principales plataformas blockchain

Pública

- Global y permanente
- Formadas por un número muy elevado de nodos
- Funciona como un registro común, facilitando la construcción de servicios de valor añadido
- Potencia la transparencia y la confianza

Ethereum

Privada

- Mayor rendimiento
- Mayor confidencialidad
- Orientado al intercambio de información y la colaboración entre pares en escenarios complejos
- Mayor control sobre el comportamiento de la red

MultiChain

Ethereum

HYPERLEDGER

Analizando el documento de Satoshi Nakamoto

Analizando el documento de Sathoshi Nakamoto

Documento de Satoshi Nakamoto de 2008: “Bitcoin: Un Sistema de Dinero Efectivo Electrónico Peer-to-Peer”.

Analizando el documento de Sathoshi Nakamoto

Es la raíz de la moderna innovación: la criptodivisa o criptomoneda basada en tecnología blockchain.

Fundamentos del Bitcoin y sus principios

Dinero en efectivo electrónico

Proceso puramente peer-to-peer permite enviar pagos online.

Directamente entre las partes y sin pasar a través de una institución financiera.

Doble gasto

Un tercero de confianza no es imprescindible para prevenir el doble gasto.

Problema del doble gasto

Propone una solución para el problema del doble gasto usando una red peer-to-peer.

Fundamentos del Bitcoin y sus principios

Prueba de trabajo

La red confirma las transacciones en el tiempo.

En una cadena continua de prueba de trabajo, estableciendo un registro que no se puede modificar sin rehacer.

La cadena más larga

Demuestra también que procedo del conjunto de CPUs más potentes.

La mayoría de la potencia CPU esté controlada por nodos que no cooperen para atacar a la red.

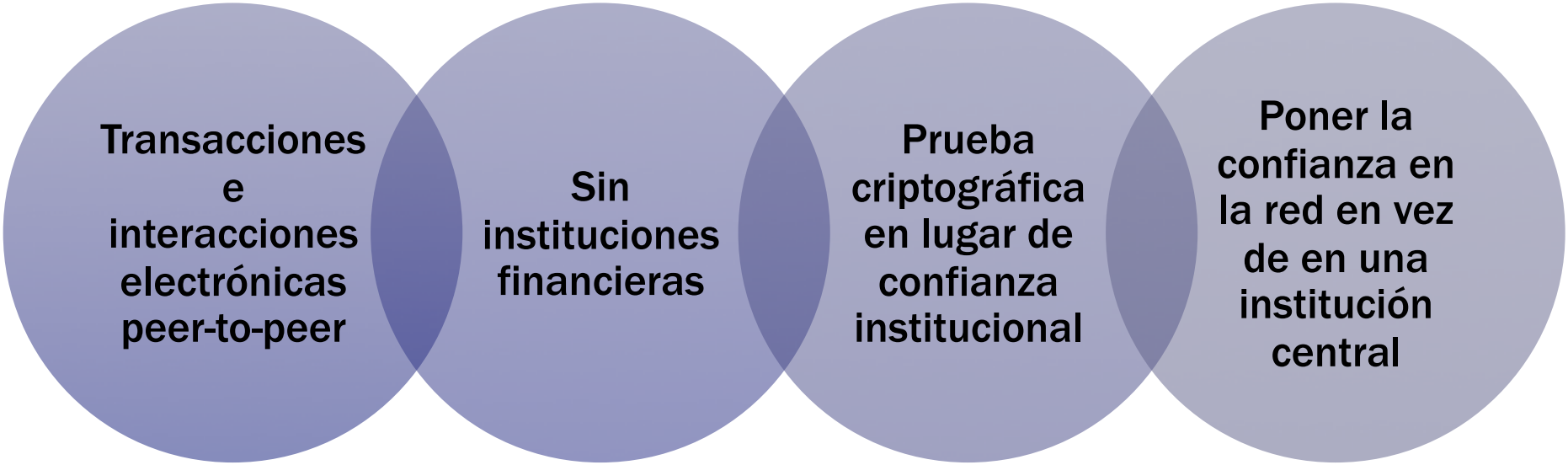
Se segura la cadena más largas y se aventaja a los atacantes.

Estructura mínima

La red en sí misma precisa de una estructura mínima.

Los mensajes se transmiten en base al mejor esfuerzo y los nodos pueden abandonar la red y regresar a ella a voluntad, aceptando la cadena de trabajo más larga como prueba de lo que ha sucedido.

Puntos esenciales del documento de Nakamoto



Definiciones de la Blockchain según Nakamoto

Definición técnica

Base de datos back-end que mantiene un libro mayor distribuido abiertamente.

Definición empresarial

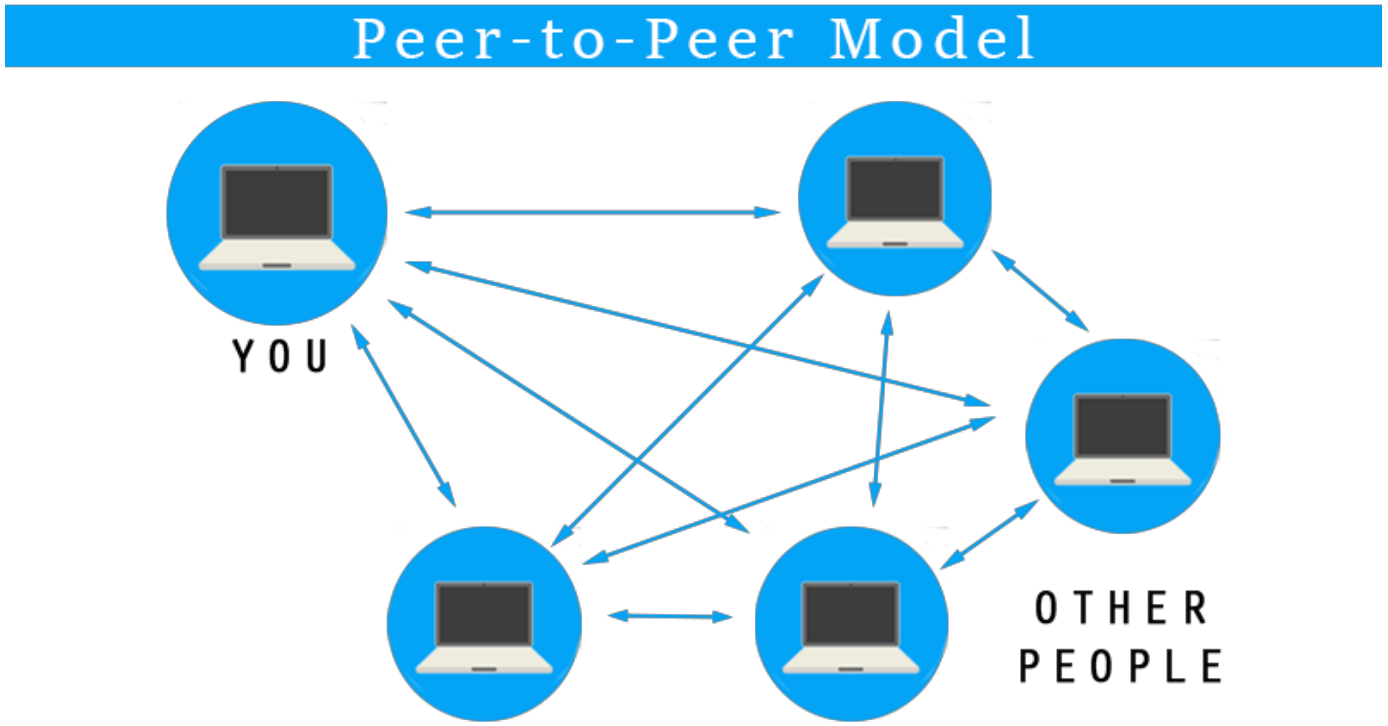
Red de intercambio para mover valores entre iguales.

Definición legal

Mecanismo de validación de transacciones que no requiere asistencia de intermediarios.

Sistema descentralizado basado en tecnología Peer to Peer

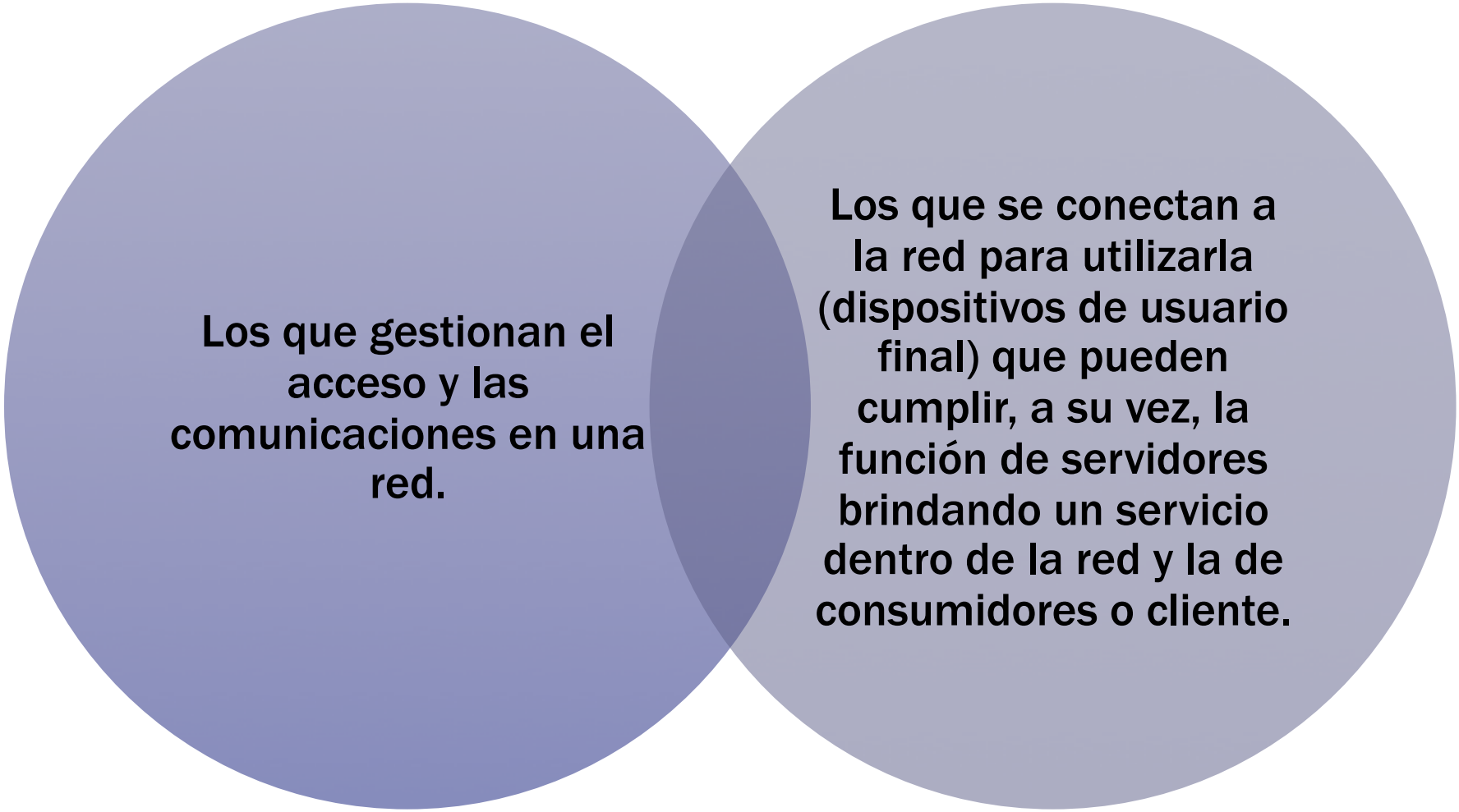
El protocolo de red blockchain se basa en una tecnología peer to peer.



Sistema descentralizado basado en tecnología Peer to Peer

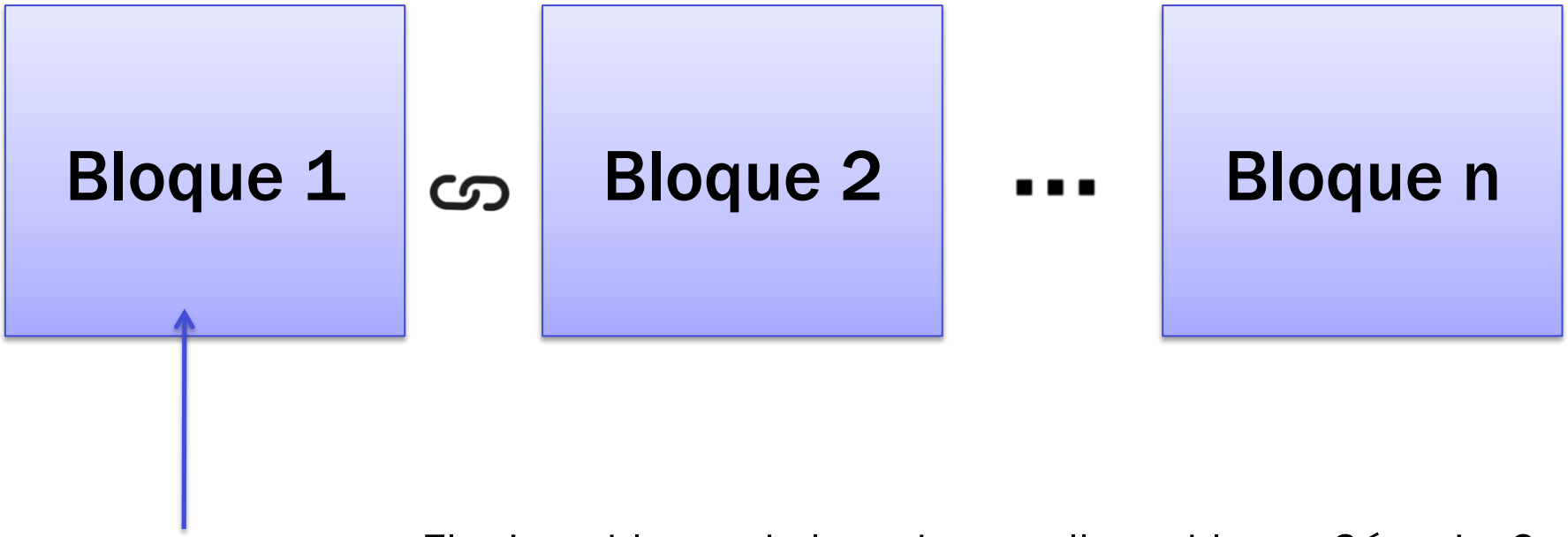
Las redes pueden clasificarse por las funciones que cumplen los dispositivos (nodos) en la transmisión de información.

Sistema descentralizado basado en tecnología Peer to Peer (categorías)



¿Qué es un bloque?

Blockchain es una cadena de bloques que contiene información. Los datos que se almacenan dentro de un bloque dependen del tipo de blockchain.



El primer bloque de la cadena se llama bloque Génesis. Cada nuevo bloque en la cadena está vinculado al bloque anterior.

Comprender SHA256 - Hash

Cada bloque tiene un hash. Es una huella digital que es única para cada bloque. Identifica un bloque y todos sus contenidos, y siempre es único, como una huella dactilar. Una vez que se crea un bloque, cualquier cambio dentro del bloque causará que el hash cambie.

HASH:

7E0CE566ED2900D81
508C7768A05A4A50C
CBC3632E72EE8D32D
E69636B663362

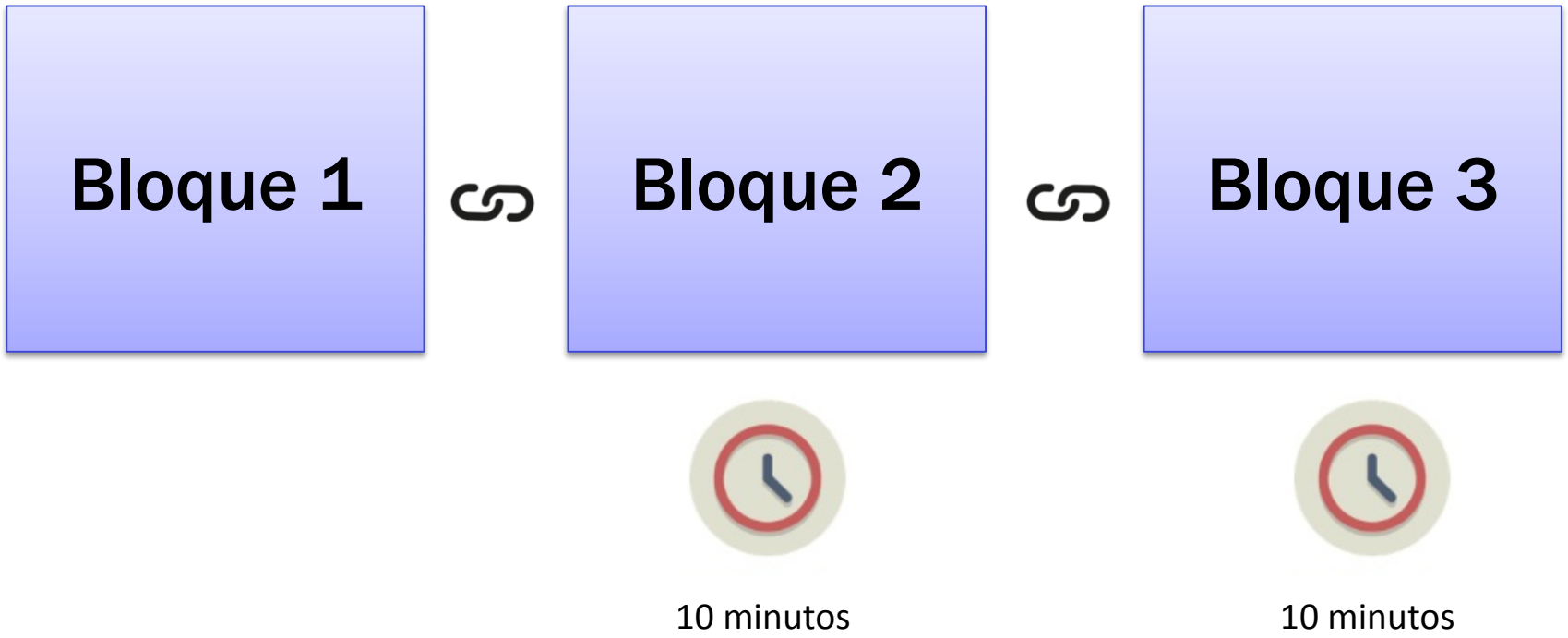
Hash actúa como una huella digital única del bloque

Comprender SHA256 - Hash

Hash es útil cuando queremos detectar cambios en las intersecciones. Si el hash de un bloque cambia, no permanece en el mismo bloque.

Prueba de trabajo

Problema computacional que requiere cierto esfuerzo para resolverlo.

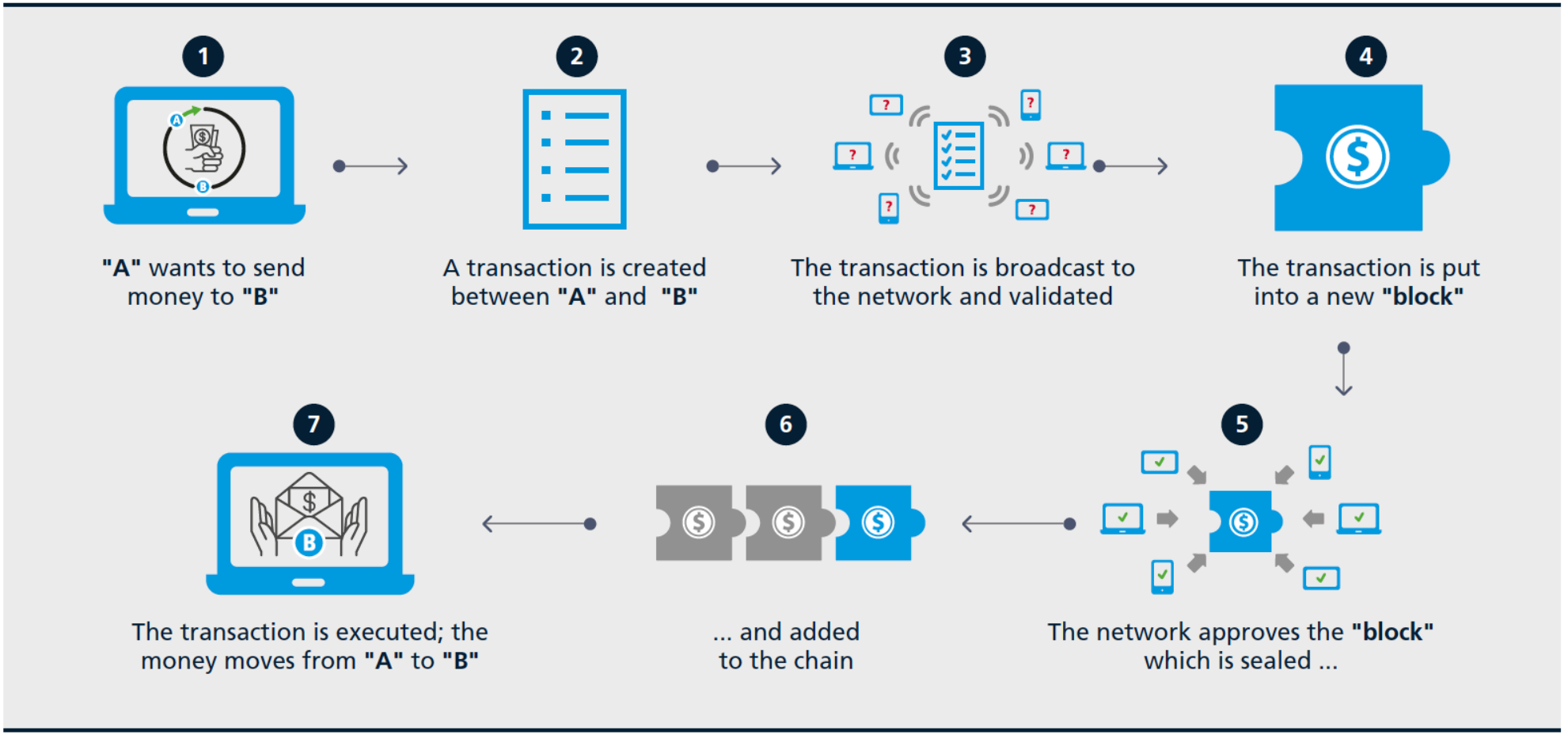


Prueba de trabajo

Este mecanismo hace que sea difícil manipular los bloques, por lo que incluso si se manipula uno sólo, se debe volver a calcular la prueba de trabajo para todos los bloque siguientes.

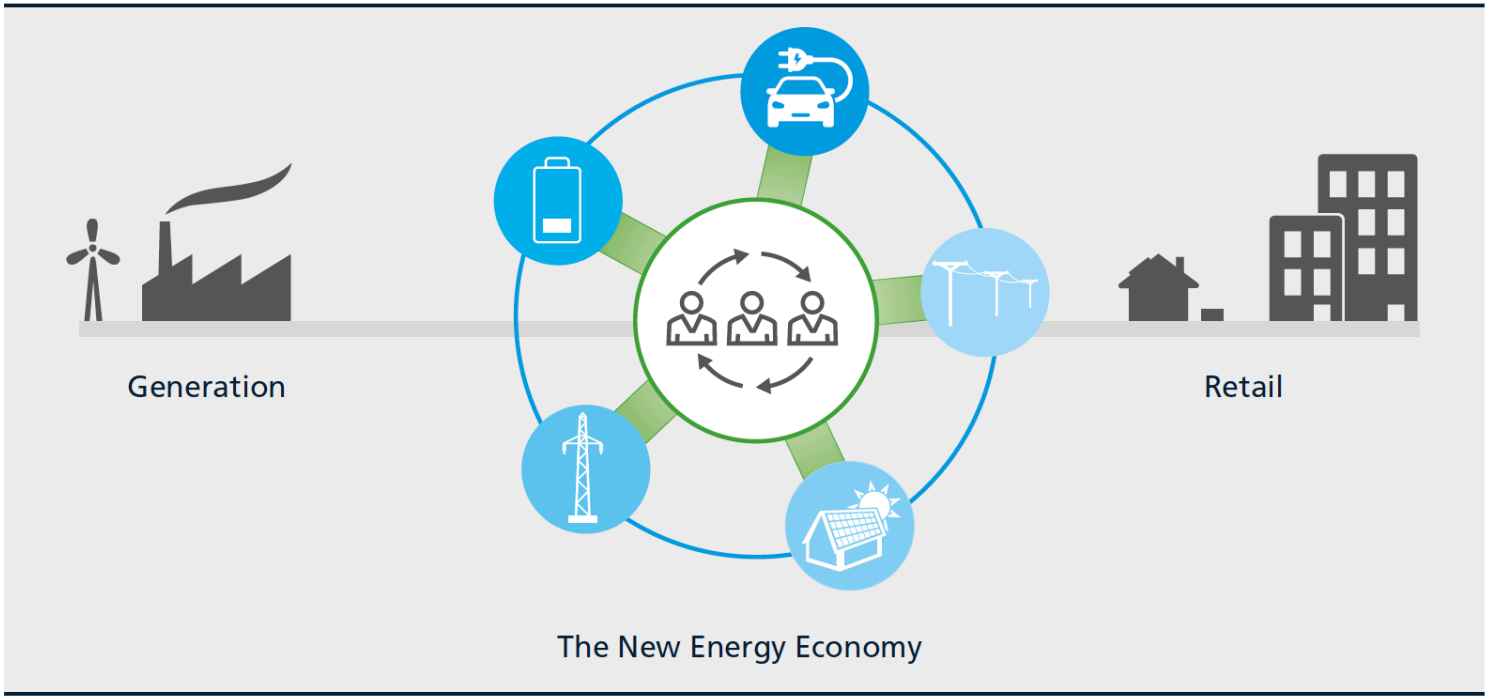
Por tanto, el hash y la prueba de trabajo aseguran una cadena de bloques.

Método Operativo en Blockchain



Ejemplos de Blockchain en Logística

Energía - Eliminando las ineficiencias del mercado (Electricidad P2P)

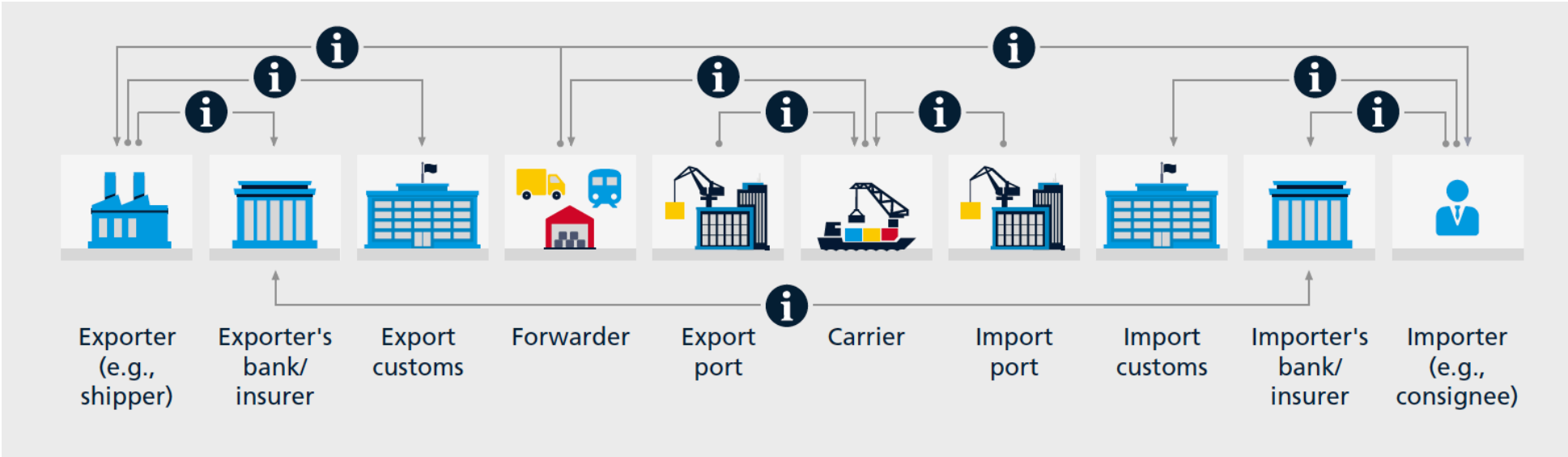


Power Ledger

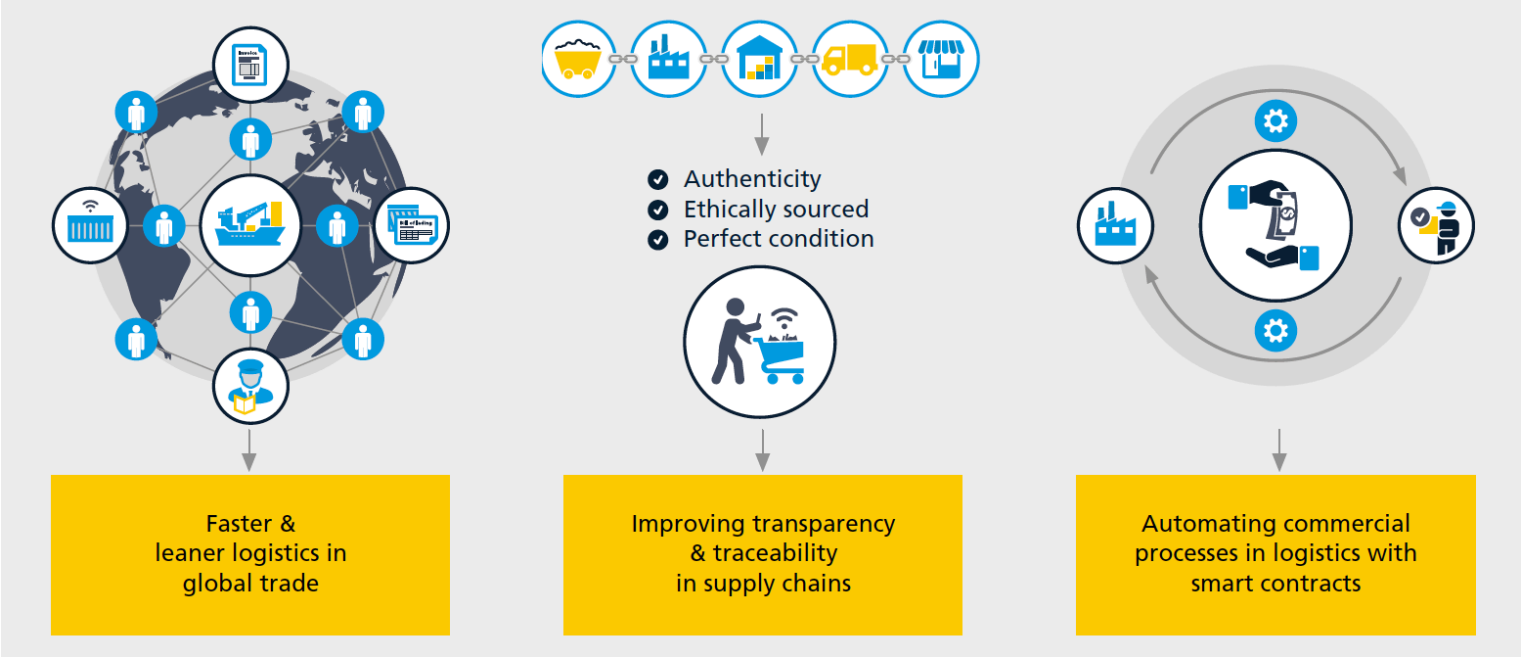
Ha desarrollado un mercado de energía peer-to-peer en una cadena de bloques, para comprar y vender electricidad proveniente de la energía solar.

IEBS

Desbloquear el valor en logística: flujo información en el comercio internacional



Desbloquear el valor en logística: Blockchain en logística

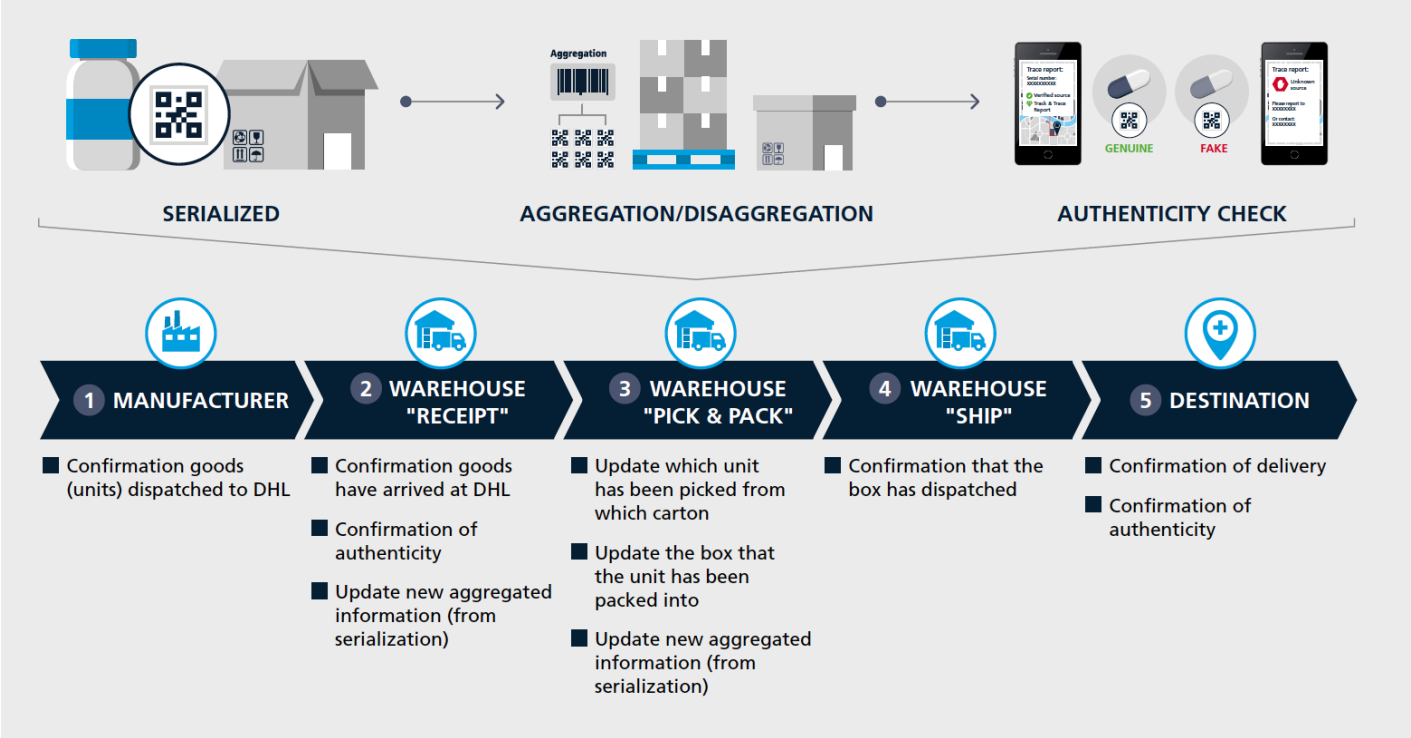


MAERSK

Transporte internacional de mercancías: objetivo mejorar la administración y trazabilidad de contenedores marítimos mediante la digitalización extremo a extremo de la cadena de suministro (incrementar la transparencia y conseguir intercambio seguro y confiable de información.

IEBS

Mejora de transparencia y trazabilidad en las cadenas de suministro

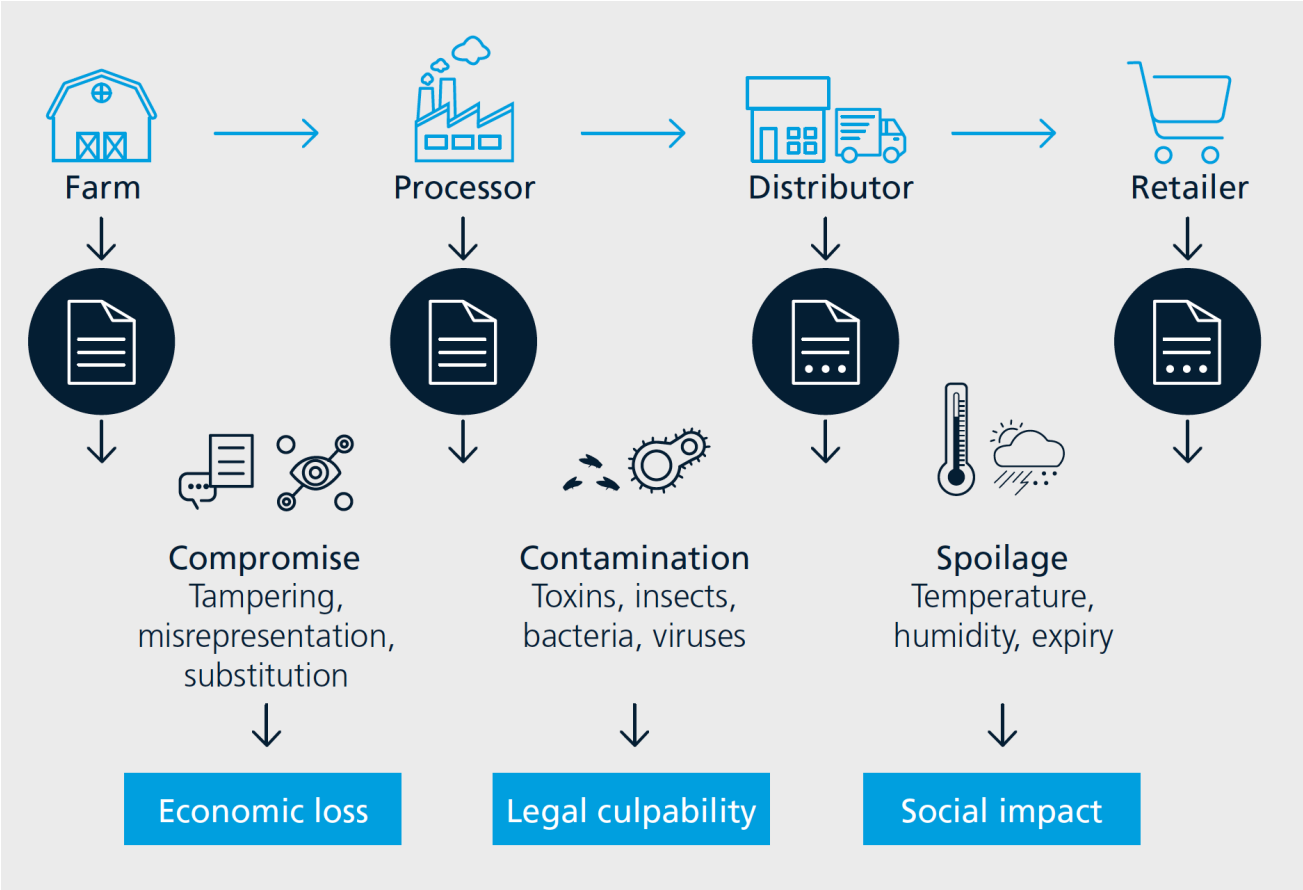


Ejemplo de sistema de seguimiento y rastreo en blockchain (monitorizar productos farmacéuticos desde fabricante al usuario final).

Capacidades de blockchain para la trazabilidad y la autenticidad de producto en la cadena de suministro de medicinas.

IEBS

Mejora de transparencia y trazabilidad en las cadenas de suministro



Ejemplo de uso la Blockchain para aumentar la seguridad y hacer seguimiento de la procedencia del producto en las cadenas de suministro de alimentos.

PROVENANCE

Desarrollo de sistema de trazabilidad para materiales y productos utilizando blockchain, con el objetivo de garantizar que la información que se almacena de manera segura, auditable, inmutable y accesible.

IEBS
Innovación & Emprendedores