



IV CONGRESO
SMART GRIDS
Madrid 23 Noviembre 2017

INTEGRACIÓN DE DISPOSITIVOS IOT EN REDES BLOCKCHAIN

Fernando Monzón

Gerente

everis



an NTT DATA Company

CONCEPTOS BÁSICOS DE BLOCKCHAIN

DESCENTRALIZACIÓN



Red Pública

Red Privado

Red Híbrida

Blockchain permite **compartir valor** de forma **digital y descentralizada**, **sin necesidad de una entidad central de confianza**.

CONSENSO

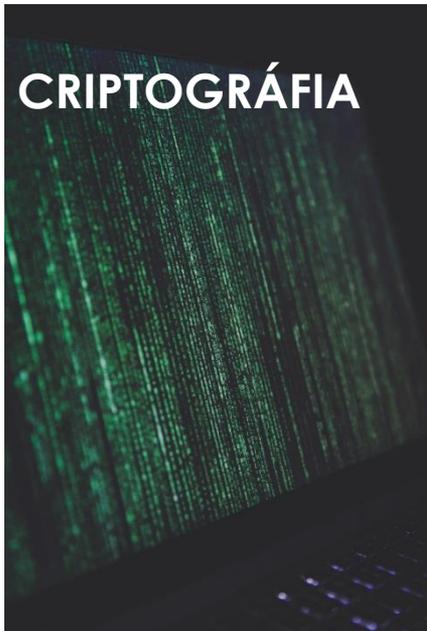


Blockchain original (Bitcoin) basado en un juego matemático.

En Blockchain privados, el nivel de consenso es modulable

El uso de unas **normas compartidas** en todos los nodos permite componer un nivel de consenso, adecuado a las necesidades, y al grado de descentralización que se quiera establecer.

CONCEPTOS BÁSICOS DE BLOCKCHAIN



Certificados digitales

Curvas elípticas

Claves

Hash

INMUTABILIDAD

Cada **nuevo registro** en el libro
Se **añade** a los anteriores.

No es posible borrar

Los nodos de lectura pueden ver
el ledger completo.



CONCEPTOS BÁSICOS DE BLOCKCHAIN

VIRTUALIZACIÓN



Blockchain permite **compartir valor....**

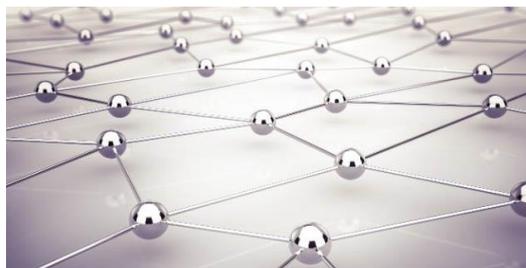
... y **no necesariamente**
Cripto-monedas

Tokenización

Kwh
Barriles de Petróleo
Inspecciones
Documentos
...

Cualquier Transacción

TIPOLOGÍA DE NODOS



Lectura

Escritura

Validación

DÓNDE ENCAJA BLOCKCHAIN?

Procesos **Complejos**

Múltiples actores implicados

Falta de confianza

Duplicidad de datos

Seguridad del dato



Proporcionando

Simplificación y Optimización

Confianza, a través del consenso

Unicidad e Inmutabilidad de datos

Seguridad y Criptografía: Integridad, Privacidad, Anonimidad

EVOLUCIÓN IOT



CARACTERÍSTICAS DE IOT



Dispositivos diferentes, **funcionalidad**, **protocolos** de datos y comunicación...

En cualquier lugar, instalaciones atendidas / desatendidas...



... y aún así generando datos constantemente

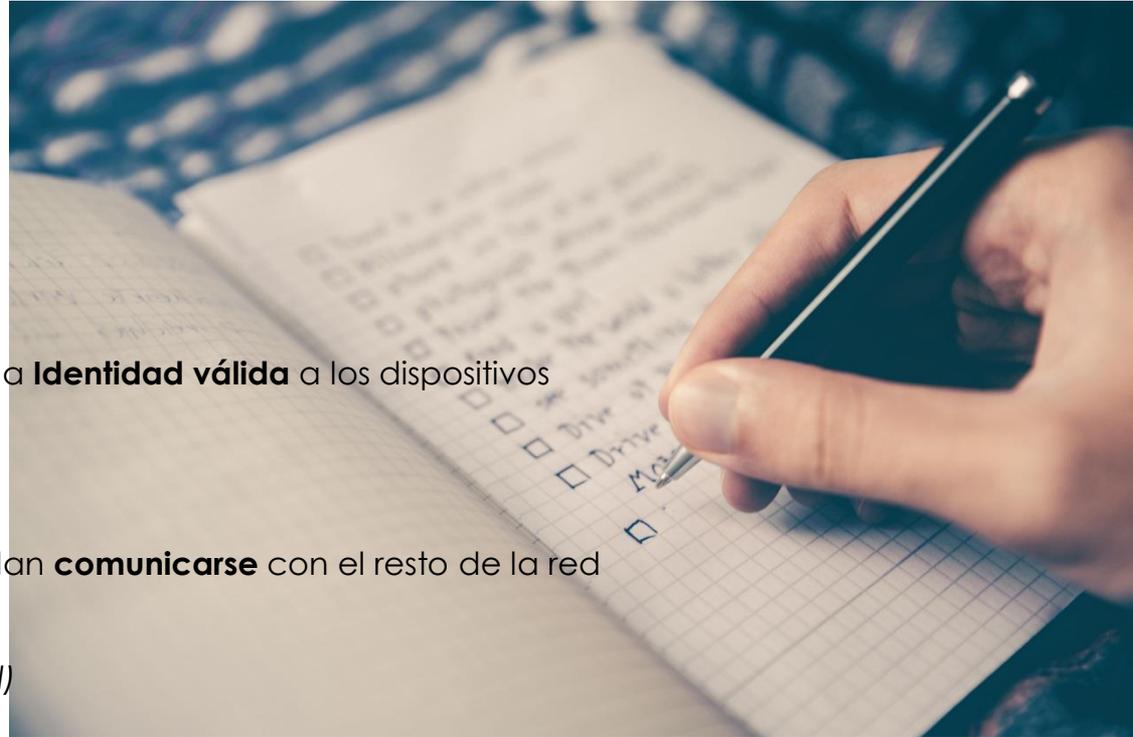


Baja capacidad de procesamiento & memoria,
Bajo nivel de **seguridad**

INTEGRACIÓN

Necesitamos:

- **SEGURIDAD:** Asegurar que podemos dar una **Identidad válida** a los dispositivos
 - Claves
 - Repositorio seguro
- **COMUNICACIÓN:** Que los dispositivos puedan **comunicarse** con el resto de la red
 - Compatibilidad Blockchain
 - Módulo de comunicación
 - Directo o a través de otro canal (app móvil)
- **INTELIGENCIA:** Proporcionar a los dispositivos capacidades mínimas de **inteligencia /validación**
 - Espacio mínimo de memoria
 - Capacidad de proceso



SOPORTE FÍSICO

Seguridad



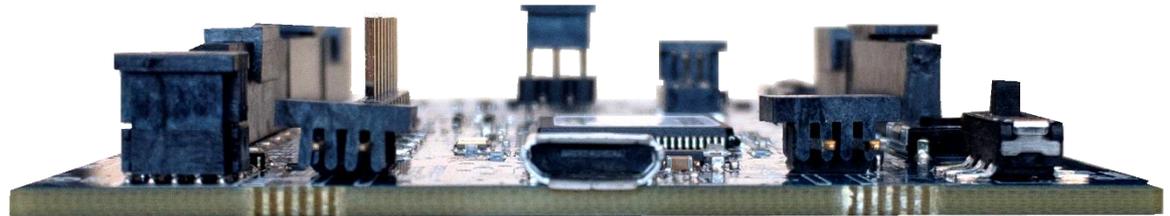
Espacio físico protegido de memoria para el almacenamiento de claves

Espacio de **almacenamiento** para **código** de validación Blockchain

Comunicación

PCB (Printed Circuit Board) incluyendo **módulo de comunicación**, que permita al dispositivo interactuar con el mundo exterior:

- BLE
- Wi-Fi
- NFC
-



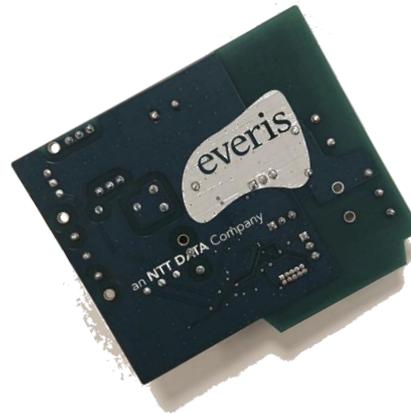
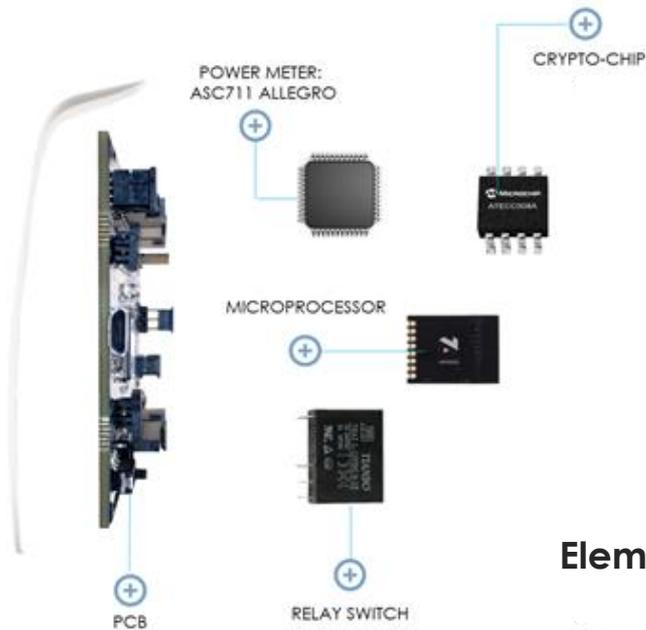
Inteligencia

Capacidad de **controlar comportamiento** del dispositivo

Firmware para gestionar la inteligencia asociada



EJEMPLO



Elementos físicos proporcionan funcionalidad **IoT**

Cripto chip proporciona la **identidad** del **dispositivo (activo asociado)**

Módulo radio del PCB proporciona la **comunicación**

Microprocesador proporciona la inteligencia necesaria

POSIBLES CASOS DE USO

Smart Grid- Distributed Energy



Gestión de transacciones
Carga Vehículo Eléctrico

Certificación parámetros
relevantes en activos críticos

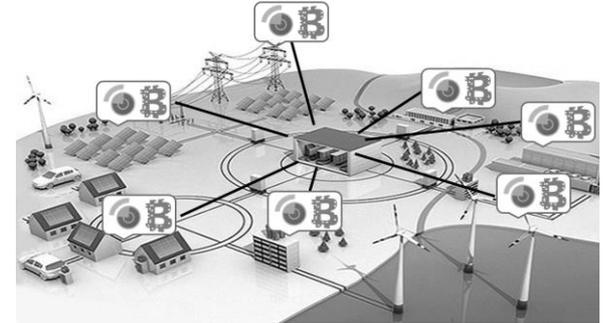


Gestión de transacciones
P2P Carga de Vehículos

Precinto Blockchain en
Smart Meters

Trazabilidad
Activos Singulares

Smart Grid- Digital Assets Management





IV CONGRESO **SMART GRIDS** Madrid 23 Noviembre 2017

DATOS DE CONTACTO:

Fernando Monzón
fmonzond@everis.com



an **NTT DATA** Company