

# Blockchain Para Negocios

David E. Ammouial

# Agenda

- **Qué es una “blockchain”?**
  - Características y estructura
  - Cuentas vs. contratos inteligentes
- **Casos de uso**
- **Ventajas y costos de usar una blockchain**
- **Pistas de reflexión**

# ¿Qué es?

- En pocas palabras:
  - Base de datos
  - Peer-to-peer
  - Inmutable
  - Sin necesidad de confianza

# ¿Qué es?

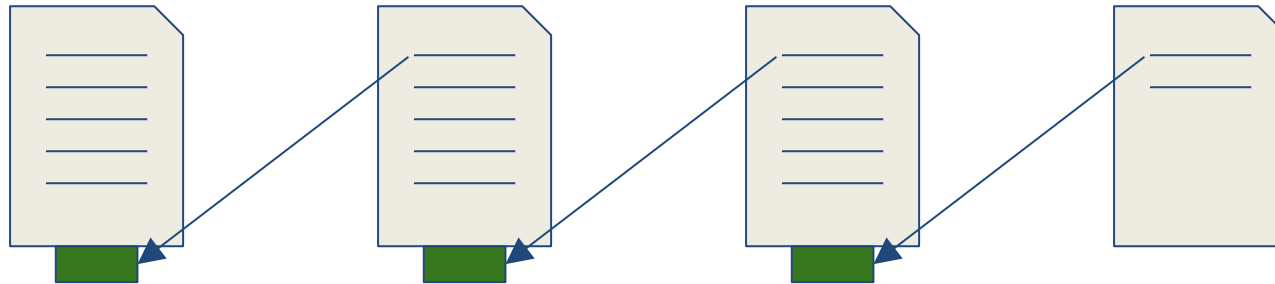
- Base de datos, red y framework
  - Estructura de datos
  - Una red de comunicación
  - Conjunto de herramientas y conceptos

# ¿Qué es?

- Estructura **distribuida**: red de malla
  - Ninguna entidad tiene autoridad
  - Comunicación entre pares (p2p)
  - Replicación del estado entre todos los participantes

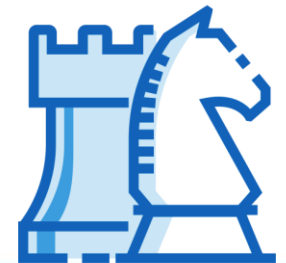
# ¿Qué es?

- Estructura de datos **inmutable**, “append-only”
  - Una transacción no se puede retractar



# ¿Qué es?

- **Consenso**, realidad compartida
  - Reglas deterministas
  - Estado único en todo momento

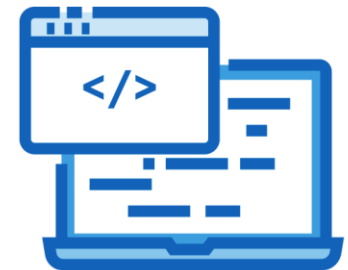


# Cuentas y contratos

- Transacción:
  - Origen, destino
    - Direcciones: 0x829BD824B016326A401d083B33D092293333A830
    - Basado en criptografía asimétrica (curvas elípticas), firmas
  - Ethers (“valor”) y/o datos
    - Permite describir cambios de estado con precisión

# Cuentas y contratos

- Humanos (cuentas)
  - Claves privadas/públicas
- Programas (contratos)
  - **Código** determinista en lugar de clave privada
  - Acepta **datos** además de valor
  - **Lenguaje** Turing-complete
  - Mantiene un **estado**



# Casos de Uso



- Caso de uso: control de asistencia
  - Asegura la integridad del registro

# Cadenas de suministro

- Seguimiento de cambios de estado
- Actores independientes, no se conocen
- Ejemplos:
  - Cadena de frío
  - Seguimiento de correos y paquetes
  - Aduanas...

08:03



08:41



15:26



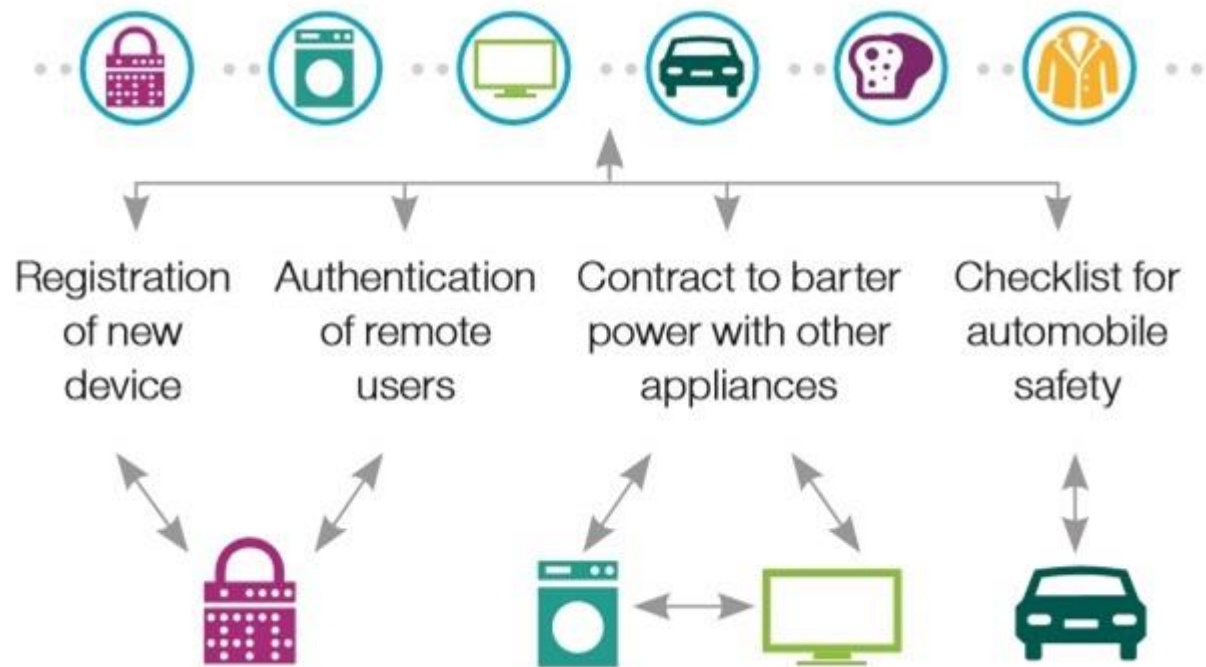
17:01



# Economías extendidas

- Dinero local
- Puntos de fidelidad compartidos entre empresas distintas

# Smart Property / IoT



# Blockchain:

## ¿Cuándo es apropiado?

- Costos asociados:
  - Cada transacción cuesta
    - Costo de las operaciones de acuerdo a la **complejidad**
    - Costo de **almacenamiento** en un contrato
  - **Límites** de tamaño por transacción, por bloque
  - **Lentitud**: comparar con ingestión Hadoop, Elasticsearch...
- **No llamaría a un notario para mi lista de supermercado**
- Soluciones mixtas, usar blockchain sólo cuando aporte valor:
  - Cálculos off-chain / resultados on-chain
  - Almacenar datos off-chain, hashes on-chain

# Y más...

- Existen diversas blockchains, y generalmente registros distribuidos
  - Ejemplo: Corda que no tiene ni bloques ni es una cadena!
- Cómo usar blockchain en temas ciudadanos?
  - Transparencia
  - Votaciones
  - Seguimiento de recursos y presupuestos públicos



Gracias  
por su atención



David E. Ammouial  
dammouia@everis.com

everis

an NTT DATA Company