

CRIPTO · SERIE 2 · PARTE 04 / 04

BLOCKCHAIN PARA LA TRAZABILIDAD

Registros compartidos entre empresas que no se fían.
Arquitectura de Hyperledger Fabric, el caso de los mangos de Walmart con sus cifras, el problema del oráculo, el papel de los sensores IoT y un criterio formal para decidir si hace falta una blockchain.

Complemento técnico de la guía «Blockchain sin monedas»
<https://amstech.dev/guias/bitcoin-s2/04-blockchain-sin-monedas/>

@ams_tech

ÍNDICE

1	Resumen
2	Blockchains públicas y con permisos
3	Hyperledger Fabric: ejecutar, ordenar, validar
4	Walmart: los mangos
5	El problema del oráculo
6	Sensores con identidad criptográfica
7	¿Hace falta una blockchain? El criterio de Wüst y Gervais
8	Lo que el vídeo simplifica
9	Referencias

1. RESUMEN

La blockchain no necesita una criptomoneda: su propiedad útil es ser un **registro compartido, ordenado y a prueba de manipulaciones** entre partes que no se fían entre sí. En la cadena alimentaria se usa para la **trazabilidad**: reconstruir el recorrido de un lote, desde la granja hasta la tienda, en segundos en lugar de días.

Este dossier:

- describe las blockchains con permisos y la arquitectura de **Hyperledger Fabric**, la base de IBM Food Trust (§2–§3);
- analiza el piloto de Walmart con mangos, que redujo el rastreo de 6 días, 18 horas y 26 minutos a 2,2 segundos, unas 265.800 veces más rápido, y explica de dónde sale realmente esa mejora (§4);
- formaliza el **problema del oráculo**, el límite fundamental del sistema (§5), y el papel de los sensores IoT con identidad criptográfica (§6);
- aplica el criterio de decisión de Wüst y Gervais (§7).

2. BLOCKCHAINS PÚBLICAS Y CON PERMISOS

	PÚBLICA (BITCOIN, ETHEREUM)	CON PERMISOS (FABRIC)
Quién escribe	cualquiera	participantes autorizados e identificados
Quién lee	cualquiera	según la política del consorcio
Defensa frente a identidades falsas	trabajo o depósito (serie 2)	identidad con certificados (PKI)
Consenso	probabilístico (PoW) o con finalidad (PoS)	servicio de ordenación tolerante a fallos
Rendimiento	limitado (dossier 3)	de miles de transacciones por segundo [1]
Moneda	necesaria (paga la seguridad)	innecesaria

En un consorcio de empresas, los participantes **se conocen y responden legalmente** de sus actos. El problema de las identidades falsas (dossier 2) desaparece, y con él la necesidad de minería o depósitos. Lo que queda es el problema de fondo: ponerse de acuerdo en un registro que **ninguno controla en solitario**.

3. HYPERLEDGER FABRIC: EJECUTAR, ORDENAR, VALIDAR

Fabric [1] separa en tres fases lo que en Ethereum ocurre a la vez:

1. **Ejecutar (avalar).** El cliente envía la transacción a los nodos **avaladores** que exige la **política de aval** (por ejemplo, «la granja y el matadero»). Cada uno la ejecuta en simulación sobre su copia del estado, sin modificarla, y firma el resultado: qué claves leyó (con su versión) y qué escribiría.
2. **Ordenar.** El **servicio de ordenación** recibe transacciones avaladas de todos los clientes, fija un **orden total** y las agrupa en bloques encadenados por huellas. No ejecuta nada y no necesita ver el contenido.
3. **Validar.** Cada nodo recibe los bloques y, para cada transacción, comprueba que cumple la política de aval y que las versiones de lo que se leyó no han cambiado desde la simulación. Si han cambiado, la transacción queda marcada como inválida (un control de concurrencia optimista). Solo entonces se aplica.

Separar las fases tiene dos ventajas: la ejecución se paraleliza entre avaladores y los programas (*chaincode*) pueden escribirse en lenguajes generales sin que todos los nodos tengan que ejecutarlos.

El orden lo decide un protocolo de consenso clásico. **Raft** tolera caídas de nodos, pero no nodos maliciosos; desde Fabric 3.0 hay también un ordenador **BFT** (tolerante a fallos bizantinos), que funciona mientras menos de un tercio de los nodos de ordenación mientan. La elección refleja la confianza del consorcio en quienes mantienen ese servicio.

4. WALMART: LOS MANGOS

4.1 EL EXPERIMENTO

En 2016–2017, Walmart e IBM hicieron dos pilotos de trazabilidad sobre Fabric: carne de cerdo en China y mangos cortados para el mercado norteamericano [2]. Según los responsables de seguridad alimentaria de Walmart, rastrear un paquete de mangos hasta su granja de origen con el método tradicional llevó **6 días, 18 horas y 26 minutos** [7][8]; con el sistema, **2,2 segundos** [2]:

$$\frac{6 \text{ d } 18 \text{ h } 26 \text{ min}}{2,2 \text{ s}} = \frac{584.760 \text{ s}}{2,2 \text{ s}} \approx 265.800. \quad (1)$$

4.2 DE DÓNDE SALE LA MEJORA

La aceleración no viene de la criptografía, sino de la **integración de datos**. El método antiguo consistía en llamar a cada eslabón (tienda, centro de distribución, procesador, importador, productor) y que cada uno buscara en su propio sistema, a menudo en papel. Con el registro compartido, cada eslabón anota su paso **en el momento** y en un formato común. La consulta recorre una estructura ya enlazada.

Una base de datos central compartida habría logrado una aceleración parecida. Lo que aporta la blockchain es que **ninguna empresa controla esa base de datos**: proveedores competidores aceptan escribir en ella porque nadie puede reescribir los apuntes de los demás sin que se note. La mejora técnica viene de los datos; la blockchain resuelve el problema **organizativo**.

4.3 CARREFOUR

Carrefour lanzó en España en 2018 su primera cadena alimentaria con blockchain, sobre IBM Food Trust, con un pollo con código QR en la etiqueta [3]. El esquema es el mismo: los eslabones anotan, y el consumidor consulta una vista de lectura.

5. EL PROBLEMA DEL ORÁCULO

Una blockchain garantiza la **integridad** de lo que se anota, no su **veracidad**. Si un operario anota «lote mantenido a 4 °C» y no fue así, el registro conserva una mentira, eso sí, perfectamente íntegra y firmada. Conectar el registro con el mundo físico es el **problema del oráculo** [4]: la confianza del sistema no puede superar la de sus fuentes de datos.

Formalmente, si un dato pasa por una cadena de k eslabones independientes, cada uno fiable con probabilidad r_i , la fiabilidad del dato final es como mucho

$$R \leq \prod_{i=1}^k r_i, \quad (2)$$

y la blockchain solo protege el último eslabón: el almacenamiento. Si el sensor, el operario o la integración fallan, el registro inmutable conserva el error.

6. SENSORES CON IDENTIDAD CRIPTOGRÁFICA

Para reducir el factor humano en (2), el dato debe generarse y **firmarse** en origen:

1. Un sensor (por ejemplo, de temperatura en un camión frigorífico) tiene una **clave privada** guardada en un **elemento seguro**: un chip que firma pero no permite extraer la clave.

2. Cada medida se envía con su firma digital (por ejemplo, ECDSA sobre la curva P-256) y una marca de tiempo.
3. Al anotarla, cualquiera puede verificar que la medida procede de **ese** sensor y no se ha alterado.

Esto acota el oráculo, pero no lo elimina. Garantiza **qué dispositivo** midió, no **qué** midió. Un sensor bien firmado junto a una bolsa de hielo mide hielo. Por eso estos sistemas se combinan con auditorías físicas, sensores redundantes y detección de anomalías (por ejemplo, temperaturas imposibles para un trayecto).

7. ¿HACE FALTA UNA BLOCKCHAIN? EL CRITERIO DE WÜST Y GERVAIS

Wüst y Gervais [5] propusieron un árbol de decisión con seis preguntas:

```

¿Hay que guardar un estado? — no → no hace falta blockchain
    | sí
¿Hay varios escritores? — no → no hace falta blockchain
    | sí
¿Se puede usar un tercero de confianza siempre disponible? — sí → no hace falta blockchain
    | no
¿Se conocen todos los escritores? — no → blockchain sin permisos (pública)
    | sí
¿Se fían todos los escritores entre sí? — sí → no hace falta blockchain
    | no
¿Hace falta verificabilidad pública? — sí → blockchain pública con permisos
    | no → blockchain privada con permisos
  
```

Aplicado a la trazabilidad alimentaria:

PREGUNTA	RESPUESTA	COMENTARIO
¿Estado?	sí	el historial de cada lote
¿Varios escritores?	sí	granja, procesador, transportista, tienda
¿Tercero de confianza?	discutible	si lo hubiera (un regulador con una base de datos), bastaría
¿Escritores conocidos?	sí	empresas identificadas
¿Se fían entre sí?	no del todo	competidores y proveedores con intereses distintos
¿Verificación pública?	parcial	el consumidor solo lee una vista

El resultado es una **blockchain con permisos**, que es exactamente lo que se usó. El mismo árbol explica por qué **la mayoría** de los proyectos «blockchain» no la necesitan: o hay un solo escritor, o existe un tercero de confianza.

8. LO QUE EL VÍDEO SIMPLIFICA

EN EL VÍDEO	CON PRECISIÓN
«Un registro que nadie puede cambiar a escondidas»	En una blockchain con permisos, los participantes del consorcio podrían reescribirlo de común acuerdo; lo que impide es el cambio unilateral sin que se note
«De casi 7 días a 2 segundos»	584.760 s frente a 2,2 s en un piloto; la mejora viene sobre todo de integrar los datos
«Garantiza que el dato no cambia, no que sea verdad»	Es el problema del oráculo (§5)
«Se conectan sensores»	Sensores con claves en un elemento seguro; acotan, no eliminan, el problema
«Compensa cuando hay varias partes que no se fían»	Es la rama central del árbol de Wüst y Gervais (§7)

9. REFERENCIAS

- [1] E. Androulaki et al. «Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains». *EuroSys '18*, ACM, 2018. arXiv:1801.10228.
- [2] R. Kamath. «Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM». *The Journal of the British Blockchain Association*, 1(1), 2018.
- [3] IBM Newsroom. *Carrefour lanza el primer blockchain alimentario en España*. 20/11/2018. <https://es.newsroom.ibm.com>
- [4] G. Caldarelli. «Understanding the Blockchain Oracle Problem: A Call for Action». *Information*, 11(11), 509, 2020.
- [5] K. Wüst, A. Gervais. «Do you need a Blockchain?». *Crypto Valley Conference on Blockchain Technology (CVCBT)*, IEEE, 2018. <https://eprint.iacr.org/2017/375>
- [6] Hyperledger Foundation. *Hyperledger Fabric documentation (v3): ordering service, Raft y BFT*. <https://hyperledger-fabric.readthedocs.io>
- [7] LF Decentralized Trust. *Walmart case study*. <https://lfdcentralizedtrust.org/case-studies/walmart-case-study>
- [8] Global Trade Review. «Food companies unite to advance blockchain for supply chain traceability». 2017. <https://www.gtreview.com>

El cálculo de (1) se ha hecho con un script propio a partir de las cifras publicadas [2][7][8]. Kamath [2] redondea el tiempo inicial a «siete días».