

Un registro notarial de transacciones basado en blockchain para el *clearing house* de un marketplace de espacios de datos

Del prototipo sobre Hyperledger Besu a la infraestructura cualificada ISBE

Francisco Javier Jiménez Urbano

GrayHats S.L.U., Córdoba (España)

Proyecto *dataspace.es* — Convocatoria de Espacios de Datos

Resumen. El intercambio de datos en espacios de datos exige trazabilidad, integridad y no repudio de las transacciones realizadas en el marketplace. La arquitectura de referencia IDS-RAM prevé para ello un componente de *clearing house* que registre las operaciones de forma fiable. Este trabajo presenta un registro notarial de transacciones basado en blockchain que materializa dicho componente. Por cada transacción, el marketplace genera un registro en formato JSON; el registro se canonicaliza de forma determinista (JCS, RFC 8785) y se calcula su resumen SHA-256. Ese resumen actúa como identificador de contenido: indexa el registro completo en una base de datos documental MongoDB (fuera de cadena) y se ancla en una blockchain compatible con Ethereum mediante un contrato inteligente que almacena la pareja *hash*–marca de tiempo y emite un evento. El diseño aporta integridad, no repudio y un sello temporal verificable, manteniendo los datos —posiblemente personales— fuera de cadena y, por tanto, suprimibles conforme al RGPD. Se describe el prototipo sobre Hyperledger Besu (red *permissioned*, consenso QBFT) y el flujo de verificación, y se propone su despliegue en producción sobre la infraestructura cualificada española ISBE —basada en Besu—, con EBSI/EUROPEUM como horizonte de interoperabilidad europea.

Palabras clave. blockchain, notarización, *clearing house*, espacios de datos, IDS-RAM, Hyperledger Besu, ISBE, SHA-256, integridad, no repudio.

1. Introducción

Los espacios de datos europeos permiten a productores y consumidores compartir e intercambiar datos de forma soberana, segura e interoperable. Cuando ese intercambio se articula a través de un *marketplace* —con oferta, contratación y pago de acceso a conjuntos de datos—, surge la necesidad de dejar constancia fiable de cada transacción: quién adquirió qué, en qué condiciones y en qué instante. Esta constancia es la base de la facturación, la resolución de conflictos y, sobre todo, del no repudio entre las partes.

La arquitectura de referencia de espacios de datos IDS-RAM [1] prevé para esta función un componente de *clearing house*: un tercero de confianza que registra las operaciones del intercambio y proporciona servicios de *clearing*, facturación y prueba. El reto es dotar a ese registro de garantías técnicas fuertes de integridad e inmutabilidad, sin convertirlo en un punto único cuya manipulación comprometa la confianza de todo el marketplace.

Este trabajo propone materializar el *clearing house* mediante un *registro notarial de transacciones* anclado en una blockchain compatible con Ethereum. El fundamento —anclar un resumen criptográfico en un libro mayor inmutable— se instancia aquí para las transacciones de un marketplace de espacios de datos, alineado con la hoja de ruta de infraestructuras cualificadas europeas. Las contribuciones son:

- un modelo de notarización que combina

almacenamiento *fuera de cadena* (MongoDB) y anclaje *en cadena* del resumen, con direccionamiento por contenido;

- el uso de una *canonicalización* determinista del registro JSON (JCS, RFC 8785) previa al resumen SHA-256, condición necesaria para una verificación reproducible;
- un contrato inteligente notario que registra la pareja *hash*–marca de tiempo y un *flujo de verificación* de existencia e integridad;
- un análisis del cumplimiento del RGPD (datos fuera de cadena, suprimibles; solo el resumen es inmutable); y
- un prototipo sobre Hyperledger Besu y una propuesta de despliegue en producción sobre la infraestructura cualificada ISBE, con EBSI/EUROPEUM como horizonte de interoperabilidad.

El artículo se organiza así: la Sección 2 resume el funcionamiento de una blockchain basada en Ethereum; la Sección 3 sitúa el *clearing house* en IDS-RAM; la Sección 4 describe el modelo de notarización; la Sección 5 el flujo de verificación; la Sección 6 el prototipo sobre Besu; la Sección 7 el camino a ISBE y EBSI; y las Secciones 8 y 9 discuten limitaciones y conclusiones.

2. Fundamentos: blockchain basada en Ethereum

Una *blockchain* es un libro mayor distribuido y replicado en una red de nodos, organizado como una cadena de *bloques*. Cada bloque agrupa un conjunto de transacciones y contiene el resumen criptográfico (*hash*) del bloque anterior; como el *hash* depende de todo el contenido, alterar un bloque pasado obligaría a recalcular todos los bloques posteriores en todos los nodos, lo que hace la historia prácticamente *inmutable* y

Proyecto *Plataforma dataspace.es* (expediente TSI-100130-2024-31), beneficiario GrayHats S.L.U. Financiado por la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio para la Transformación Digital y de la Función Pública, y por la Unión Europea – NextGenerationEU a través del Plan de Recuperación, Transformación y Resiliencia. Véase la sección de *Financiación*. Correspondencia: GrayHats S.L.U., Córdoba, España.

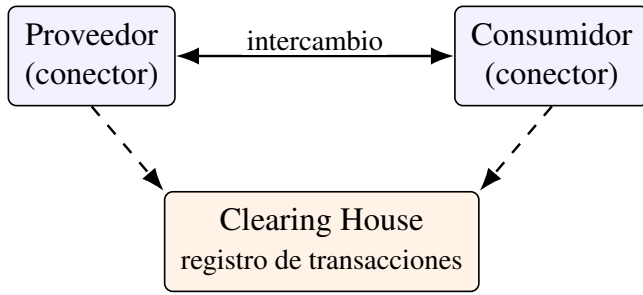


Figura 1. Posición del *clearing house* en IDS-RAM: registra las transacciones del intercambio entre conectores. Elaboración propia.

a prueba de manipulación [2]. Los nodos acuerdan el estado válido mediante un *mecanismo de consenso*.

Ethereum [3, 4] extiende este modelo con una *máquina virtual* (EVM) que ejecuta *contratos inteligentes*: programas desplegados en la cadena cuyo código y estado son públicos y cuya ejecución es determinista y verificable por todos los nodos. Un contrato expone funciones que los usuarios invocan mediante transacciones firmadas; la ejecución modifica el estado del contrato y puede emitir *eventos* (*logs*) que quedan registrados en la cadena y son consultables de forma eficiente. El coste de ejecución se mide en *gas*.

Según quién pueda participar, se distinguen redes *públicas* y *sin permiso* (cualquiera válida) y redes *permissioned* (un conjunto conocido de validadores), más apropiadas para entornos empresariales y regulados por su control de identidad, su rendimiento y su gobernanza. *Hyperledger Besu* [5] es un cliente de Ethereum de código abierto, compatible con la EVM, que puede operar tanto en la red pública como en redes *permissioned* con consensos de tolerancia a fallos bizantinos como QBFT. Esta compatibilidad EVM es relevante: un contrato desarrollado y probado sobre Besu puede desplegarse, sin reescritura, sobre otras redes EVM, incluidas las infraestructuras calificadas que se describen en la Sección 7.

3. El *clearing house* en IDS-RAM

En IDS-RAM [1], el intercambio de datos se produce entre conectores de un proveedor y un consumidor. El *clearing house* es el componente que registra las transacciones realizadas, de modo que las partes puedan posteriormente demostrar que una operación tuvo lugar (no repudio), liquidarla y resolver eventuales disputas. La Figura 1 sitúa ese componente.

El requisito esencial de ese registro es la *integridad verificable* y el *no repudio*: una vez anotada, una transacción no debe poder alterarse ni negarse. Una blockchain inmutable y con sello temporal es un sustrato natural para esta función, siempre que se resuelva la tensión con la protección de datos (Sección 8).

4. Modelo de notarización

Por cada operación de compra en el marketplace (véase el componente de cotización y pedido descrito en trabajos previos del proyecto), el sistema genera un *registro de transacción* r en formato JSON, con los datos relevantes de la operación: identificadores de las partes, referencia de la oferta y del conjunto de datos, cotización aplicada, token de acceso concedido e instante de la operación. El objetivo es notarizar r de forma que su integridad y su existencia en el

tiempo sean verificables por cualquiera.

4.1. Canonicalización y resumen

JSON admite múltiples serializaciones equivalentes del mismo contenido (orden de claves, espaciado, formato numérico). Para que el resumen sea reproducible, el registro se somete primero a una *canonicalización* determinista conforme al *JSON Canonicalization Scheme* (JCS, RFC 8785) [6], obteniendo una secuencia de bytes canónica $c = \text{JCS}(r)$. Sobre ella se calcula el resumen

$$h = \text{SHA-256}(c) \in \{0, 1\}^{256}. \quad (1)$$

Se emplea SHA-256 [7] —y no SHA-1— por ser resistente a colisiones: dado que la notarización persigue integridad y no repudio, el uso de una función con colisiones prácticas conocidas [8] invalidaría la garantía, al permitir construir dos registros distintos con el mismo resumen.

4.2. Almacenamiento fuera de cadena y anclaje en cadena

El resumen h se usa como *identificador de contenido* con doble papel (Figura 2):

- **Fuera de cadena:** el registro completo r se almacena en una base de datos documental MongoDB usando h como clave primaria ($_id = h$). La base de datos guarda el dato; la cadena no.
- **En cadena:** solo se ancla el resumen. Un contrato notario almacena la pareja (h, τ) —resumen y marca de tiempo del bloque— y emite un evento. Formalmente, mantiene una aplicación

$$A : \{0, 1\}^{256} \rightarrow \mathbb{N}, \quad A[h] = \tau, \quad (2)$$

donde τ es el instante (`block.timestamp`) en que se ancló h .

Este reparto es deliberado: la cadena aporta inmutabilidad y sello temporal *sin* contener los datos, y la base de datos aporta almacenamiento consultable y, en su caso, suprimible. El contrato notario se resume en la Figura 3.

4.3. Secuencia de registro y anclaje

La Figura 4 muestra el flujo completo. El servicio de notarización canonicaliza y resume el registro, lo persiste en MongoDB y envía una transacción `notarize(h)` al contrato; el bloque que la incluye fija el sello temporal τ y el contrato emite `Notarized`. El marketplace recibe un comprobante (h, τ) que puede entregar a las partes.

5. Flujo de verificación

El valor notarial reside en poder verificar, *a posteriori*, un registro r' que una parte presente. El procedimiento (Figura 5) canonicaliza r' y recalcula $h' = \text{SHA-256}(\text{JCS}(r'))$; consulta el ancla $A[h']$ en el contrato; y compara con la copia almacenada:

- si $A[h'] = 0$, el registro *no está notarizado*;
- si $A[h'] = \tau > 0$, existe prueba de existencia con sello temporal τ ; si además la copia en MongoDB para $_id = h'$ coincide con r' , la *integridad queda verificada*;
- cualquier alteración de r' produce un h' distinto, por lo que no encontrará ancla y será detectada.

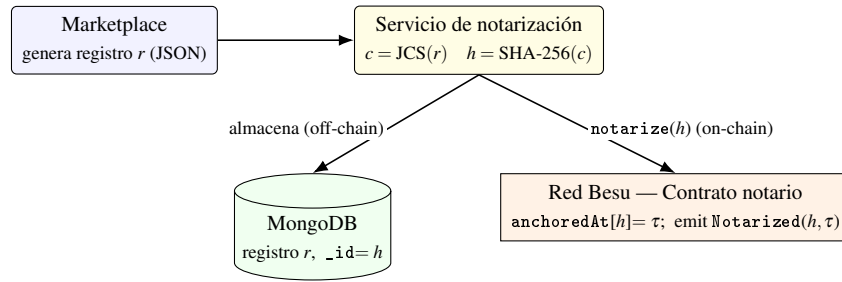


Figura 2. Arquitectura de notaría: el servicio canonicaliza y resume el registro; guarda el registro completo en MongoDB (fuera de cadena) y ancla solo el resumen en el contrato notario (en cadena). Elaboración propia.

```

pragma solidity ^0.8.0;
contract TransactionNotary {
    // resumen -> marca de tiempo del bloque
    mapping(bytes32 => uint256) public anchoredAt;
    event Notarized(bytes32 indexed hash,
        uint256 timestamp,
        address submitter);

    function notarize(bytes32 h) external {
        require(anchoredAt[h] == 0, "ya anclado");
        anchoredAt[h] = block.timestamp;
        emit Notarized(h, block.timestamp, msg.sender);
    }
    // 0 si no esta anclado
    function anchorOf(bytes32 h)
        external view returns (uint256) {
        return anchoredAt[h];
    }
}
  
```

Figura 3. Contrato notario (Solidity, simplificado): ancla el resumen con su sello temporal y emite un evento.

La verificación no requiere confianza en el servicio de notaría: se apoya en la función resumen y en el libro mayor inmutable.

6. Prototipo sobre Hyperledger Besu

El prototipo despliega una red *permissioned* con Hyperledger Besu y consenso QBFT (tolerancia a fallos bizantinos con un conjunto conocido de validadores), adecuada para un entorno controlado y de identidad gestionada. Sobre ella se despliega el contrato `TransactionNotary` (Figura 3). El *servicio de notaría* actúa como intermediario entre el marketplace y las dos persistencias: recibe el registro, lo canonicaliza (JCS) y resume (SHA-256), lo inserta en MongoDB con `_id=h` y envía la transacción `notarize(h)` al contrato mediante una biblioteca EVM estándar. El evento `Notarized` permite reconstruir el registro de anclajes a partir de los *logs*. Esta configuración valida el ciclo completo de notaría y verificación en un entorno de desarrollo controlado.

7. Camino a producción: ISBE y EBSI

El prototipo está pensado para migrar, sin reescritura del contrato, a una infraestructura cualificada de producción. La candidata natural es *ISBE* (Infraestructura de Servicios Blockchain de España), promovida por la Comunidad de Madrid y Alastria: una red nacional *public-permissioned* construida sobre *Hyperledger Besu*, diseñada para el cumplimiento normativo por diseño y con vocación de constituir una DLT cualificada (qDLT) con efecto legal en el mercado único digital, interoperable con EBSI [9, 10]. Al compartir ISBE el mismo sustrato EVM/Besu del prototipo,

la portabilidad del contrato notario es directa.

En el plano europeo, la *European Blockchain Services Infrastructure* (EBSI) [11] constituye el horizonte de interoperabilidad transfronteriza; su gobernanza está transitando al consorcio EUROPEUM-EDIC bajo control de los Estados miembros [12]. Dado que EBSI se ha orientado primordialmente a casos de uso del sector público, para un *clearing house* de un marketplace comercial el destino operativo es ISBE, con EBSI/EUROPEUM como capa de interoperabilidad. Este encaje alinea el registro notarial con la hoja de ruta de infraestructuras cualificadas europeas y con la identidad digital conforme a eIDAS 2.0 [13].

8. Discusión y limitaciones

Cumplimiento del RGPD. La inmutabilidad de la cadena es incompatible con el derecho de supresión si en ella se almacenan datos personales. El diseño lo evita: en cadena solo reside el resumen h , mientras el registro r —que puede contener datos personales— se almacena fuera de cadena en MongoDB, donde es suprimible. Conviene no obstante advertir que un resumen podría discutirse como seudónimo si el espacio de entradas fuera adivinable; el uso de SHA-256 sobre registros con suficiente entropía mitiga ese riesgo. Esta separación es coherente con el enfoque de inmutabilidad compatible con el RGPD que persiguen las infraestructuras cualificadas [10].

Escalabilidad y coste. El prototipo ancla un resumen por transacción. En producción, sobre una red cualificada con coste o cadencia de bloque acotados, el anclaje puede agregarse: calcular periódicamente la raíz de un árbol de Merkle de muchos resúmenes y anclar solo la raíz, conservando pruebas de inclusión individuales. Esta optimización se plantea como trabajo futuro.

Alcance de la garantía. La notaría prueba la *existencia* de un registro en un instante y su *integridad* frente a alteraciones, pero no la veracidad semántica de su contenido ni la correcta formación del registro por el marketplace; estas dependen de controles externos. Asimismo, la gestión de claves del servicio de notaría y de los validadores de la red es crítica y queda fuera del alcance de este trabajo.

Trabajo futuro. Agregación por Merkle, despliegue y evaluación sobre ISBE, integración del comprobante de notaría con las entidades de facturación e inventario del marketplace, y estudio de latencia y coste a escala real.

9. Conclusiones

Se ha presentado un registro notarial de transacciones basado en blockchain que materializa el componente

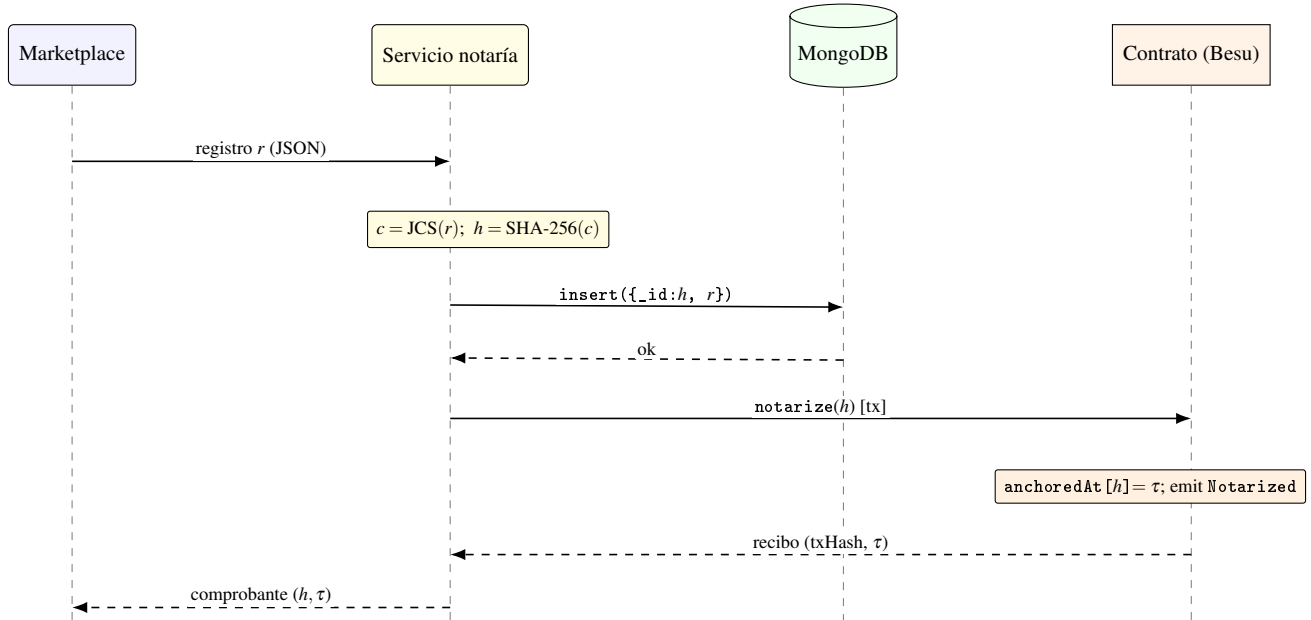


Figura 4. Secuencia de registro y anclaje de una transacción. El sello temporal τ procede del bloque que confirma la transacción. Elaboración propia.

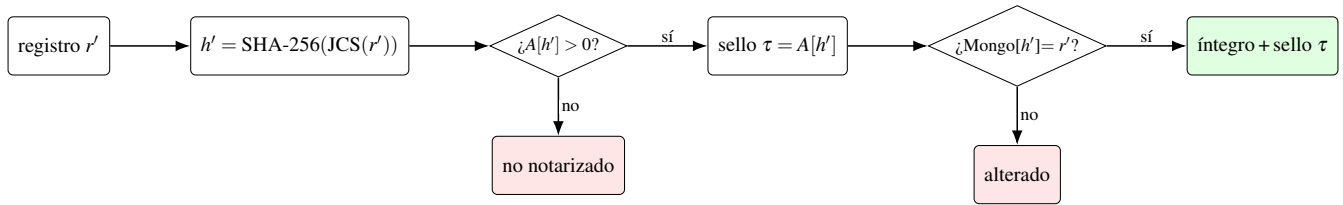


Figura 5. Flujo de verificación de existencia e integridad de un registro. Elaboración propia.

clearing house de IDS-RAM para un marketplace de espacios de datos. El diseño canonicaliza el registro JSON, lo resume con SHA-256 y reparte responsabilidades entre un almacén documental fuera de cadena (MongoDB) y un ancla inmutable con sello temporal en cadena, aportando integridad, no repudio y compatibilidad con el RGPD. El prototipo sobre Hyperledger Besu valida el ciclo de notarización y verificación, y su compatibilidad EVM habilita un despliegue directo en la infraestructura cualificada española ISBE, con EBSI/EUROPEUM como horizonte de interoperabilidad europea. El trabajo se ha desarrollado en el marco del proyecto *dataspace.es*.

Financiación

Este trabajo forma parte del proyecto «Plataforma *dataspace.es*» (expediente TSI-100130-2024-31), financiado por la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio para la Transformación Digital y de la Función Pública, en el marco del Programa de Productos y Servicios Tecnológicos para Espacios de Datos, y financiado por la Unión Europea – NextGenerationEU a través del Plan de Recuperación, Transformación y Resiliencia.

Financiado por la Unión Europea – NextGenerationEU. Sin embargo, los puntos de vista y las opiniones expresadas son únicamente los del autor o autores y no reflejan necesariamente los de la Unión Europea o la Comisión Europea. Ni la Unión Europea ni la Comisión Europea pueden ser consideradas responsables de las mismas.

Publicidad de la financiación:



Financiado por la
Unión Europea
NextGenerationEU



**Plan de Recuperación,
Transformación y Resiliencia**

Referencias

- [1] International Data Spaces Association, *IDS Reference Architecture Model (IDS-RAM)*, versión 4, 2023.
- [2] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008.
- [3] V. Buterin, *Ethereum White Paper*, 2014.
- [4] G. Wood, *Ethereum Yellow Paper*, 2014–.
- [5] Hyperledger Besu, *Documentación técnica*, LF Decentralized Trust, 2024.
- [6] E. Rundgren et al., *JSON Canonicalization Scheme (JCS)*, RFC 8785, 2020.
- [7] NIST, *Secure Hash Standard (SHS)*, FIPS PUB 180-4, 2015.
- [8] M. Stevens et al., *The First Collision for Full SHA-1*, CRYPTO, 2017.
- [9] Alastria y Comunidad de Madrid, *ISBE — Infraestructura de Servicios Blockchain de España*, 2025.
- [10] LF Decentralized Trust, *Building ISBE on Besu*, 2026.
- [11] Comisión Europea, *European Blockchain Services Infrastructure (EBSI)*, 2024.
- [12] Comisión Europea, *EBSI evolves with EUROPEUM-EDIC*, 2026.
- [13] Reglamento (UE) 2024/1183, *Marco Europeo de Identidad Digital (eIDAS 2.0)*, 2024.