



Módulo 1. Funcionamiento técnico de Blockchain

- ☰ Bloques, transacciones y estructura de la cadena
- ☰ Timestamp, orden temporal y validación de la información
- ☰ Referencias

Bloques, transacciones y estructura de la cadena

En los entornos donde circulan criptoactivos y aplicaciones basadas en *blockchain*, la confianza ya no se apoya en una autoridad central que valide la información, sino en un conjunto de mecanismos técnicos que permiten verificar, registrar y preservar datos de manera distribuida. En este marco, comprender cómo se organizan los datos dentro de la cadena resulta un punto de partida indispensable para interpretar el funcionamiento del sistema en su conjunto y para analizar con criterio técnico sus alcances y limitaciones.

En esta primera unidad abordaremos la lógica estructural de *blockchain* como sistema de registro distribuido. El análisis se centra en la forma en que las transacciones se agrupan, cómo se construyen los bloques y de qué manera estos se enlazan entre sí mediante mecanismos criptográficos. Esta arquitectura es la que permite garantizar la integridad de la información registrada, asegurar la trazabilidad de los eventos y sostener la coherencia del sistema sin depender de un ente central de control.

Desde una perspectiva profesional, estos conceptos aparecen de manera recurrente en tareas vinculadas al análisis de redes *blockchain*, la auditoría de transacciones, el diseño de soluciones descentralizadas y la evaluación de riesgos operativos. Comprender qué información contiene un bloque, cómo se relaciona con los bloques anteriores y por qué esa relación resulta resistente a modificaciones posteriores permite interpretar fenómenos como la inmutabilidad del registro y la confianza distribuida entre los participantes de la red.

A lo largo de la unidad, desarrollaremos la estructura interna de los bloques, la relación entre transacciones individuales y bloques agregados, el rol del *hash* en el encadenamiento criptográfico y las razones técnicas que explican por qué los registros almacenados en *blockchain* mantienen su consistencia a lo largo del tiempo. Este recorrido sienta las bases conceptuales necesarias para comprender, en las unidades siguientes, cómo intervienen el orden temporal, la validación distribuida y los mecanismos de consenso en la operación cotidiana de las redes *blockchain*.

Bloques, transacciones y estructura de la cadena

En los sistemas *blockchain*, el bloque constituye la unidad básica de almacenamiento y organización de la información. Cada bloque agrupa un conjunto de transacciones previamente validadas y las integra a la cadena mediante mecanismos criptográficos que aseguran coherencia, integridad y continuidad histórica del registro. Desde una perspectiva técnica, comprender la estructura interna de un bloque permite interpretar cómo se construye la confianza distribuida y por qué el sistema resulta resistente a modificaciones posteriores del contenido registrado.

Un bloque puede entenderse como un contenedor de datos con una estructura definida por el protocolo de la red. Esta estructura responde a reglas comunes que todos los nodos respetan para aceptar un bloque como válido. En redes públicas como Bitcoin, dicha estandarización resulta indispensable para que nodos distribuidos geográficamente puedan verificar, almacenar y replicar la información sin necesidad de coordinación centralizada (Ministerio Público Fiscal, 2023).

Desde el punto de vista funcional, la información de un bloque se organiza en dos grandes componentes: el encabezado (*block header*) y el cuerpo del bloque. El encabezado concentra los metadatos necesarios para identificar el bloque dentro de la cadena y vincularlo criptográficamente con los bloques anteriores. El cuerpo, en cambio, contiene el conjunto de transacciones que justifican la existencia del bloque y constituyen

el registro contable propiamente dicho (Medranda Morales & Arcos Agudo, 2023).

El encabezado del bloque cumple un rol estructural y de verificación. Allí se almacenan datos como el *hash* del bloque anterior, la marca temporal de inclusión, el nivel de dificultad, el *nonce* utilizado en el proceso de validación y el *hash* raíz del árbol de Merkle. Estos elementos permiten que cualquier nodo compruebe que el bloque se encuentra correctamente enlazado a la cadena y que su contenido no ha sido alterado desde el momento de su incorporación (Ministerio Público Fiscal, 2023).

El cuerpo del bloque, por su parte, agrupa las transacciones validadas que se incorporan de manera conjunta. Cada transacción contiene información sobre los orígenes y destinos de los activos, firmas criptográficas y datos asociados a su ejecución. El bloque no almacena las transacciones de forma aislada, sino que las organiza de manera que su integridad pueda ser verificada de forma eficiente mediante estructuras criptográficas específicas, como el árbol de Merkle.

El árbol de Merkle permite resumir el conjunto de transacciones en un único valor criptográfico, denominado raíz de Merkle. Este valor se incluye en el encabezado del bloque y actúa como un identificador global del contenido del cuerpo. A partir de este mecanismo, cualquier modificación en una transacción altera la

raíz de Merkle y, en consecuencia, invalida el bloque completo. Esta relación refuerza la integridad del registro y facilita procesos de auditoría y verificación parcial de datos (Ministerio Público Fiscal, 2023).

El vínculo entre bloques se establece a través del hash del bloque anterior, que se incorpora explícitamente en el encabezado del bloque siguiente. De este modo, cada bloque referencia de manera directa al anterior, conformando una secuencia encadenada. Esta dependencia estructural explica por qué una alteración en un bloque previo impacta en todos los bloques posteriores, ya que modifica los valores criptográficos que sostienen la continuidad de la cadena.

A nivel operativo, esta estructura posibilita que los nodos validen los bloques sin necesidad de confiar en el emisor. Cada nodo puede recalcular los *hashes*, verificar la correspondencia entre encabezado y contenido, y comprobar que las reglas del protocolo fueron respetadas. La estructura del bloque, por lo tanto, materializa el principio de verificación distribuida que

caracteriza a *blockchain* como tecnología de registro (Medranda Morales & Arcos Agudo, 2023).

Desde el ejercicio profesional, esta comprensión resulta central en tareas de análisis forense, auditoría de transacciones y seguimiento de flujos de criptoactivos. Identificar los campos de un bloque y su función permite interpretar exploradores de bloques, reconstruir recorridos transaccionales y evaluar la consistencia de la información registrada, aspectos habituales en contextos de investigación técnica y regulatoria.

Asimismo, la estructura del bloque condiciona el rendimiento y las capacidades de la red. El tamaño del bloque, la cantidad de transacciones incluidas y los datos del encabezado influyen directamente en la velocidad de propagación, en los costos operativos y en la escalabilidad del sistema. Estas variables son objeto de debate y ajuste permanente en distintas redes *blockchain*, lo que refuerza la necesidad de comprender su base estructural.

En síntesis, el bloque no es únicamente un contenedor de transacciones, sino una unidad técnica compleja que articula datos, criptografía y reglas de validación. Su estructura permite que la cadena funcione como un registro coherente, verificable y resistente a alteraciones, sentando las bases para la

inmutabilidad y la trazabilidad que caracterizan a los sistemas *blockchain*.

Figura 1. Estructura de un bloque



Made with  Napkin

Fuente: elaboración propia a partir de Ministerio Público Fiscal (2023).

Tabla 1. Componentes principales de un bloque y su función

Componente	Ubicación	Función principal	técnica
Hash del bloque anterior	Encabezado	Vincula el bloque con la cadena previa	
<i>Timestamp</i>	Encabezado	Registra el momento de incorporación	
Raíz de Merkle	Encabezado	Resume criptográficamente las transacciones	
<i>Nonce</i>	Encabezado	Permite cumplir las condiciones de validación	
Transacciones	Cuerpo	Registros de transferencias de activos	
Tamaño del bloque	Metadato	Determina capacidad y propagación	

Fuente: elaboración propia con base en Ministerio Público Fiscal (2023).

Relación entre transacciones y bloques

En una red *blockchain*, las transacciones y los bloques mantienen una relación estructural y funcional que resulta central para el funcionamiento del sistema como registro distribuido. Las transacciones constituyen los eventos elementales que reflejan transferencias de valor o cambios de estado, mientras que los bloques actúan como unidades de agregación que permiten organizar, validar y registrar esos eventos dentro de la cadena. Analizar esta relación permite comprender cómo se pasa de operaciones individuales a un registro colectivo coherente y verificable.

Una transacción puede definirse como una instrucción firmada criptográficamente que expresa la voluntad de transferir un activo o ejecutar una acción válida según las reglas del protocolo. Cada transacción es generada por un usuario, difundida a la red y sometida a procesos de verificación antes de ser incorporada de manera definitiva al registro. En este punto, la transacción existe como un dato independiente, aún no consolidado en la cadena (Ministerio Público Fiscal, 2023).

El bloque cumple la función de agrupar un conjunto de transacciones previamente verificadas. Esta agrupación no es arbitraria, sino que responde a criterios técnicos definidos por el

protocolo de la red, como el tamaño máximo del bloque, las comisiones asociadas a cada transacción y las condiciones de validación vigentes. De este modo, el bloque actúa como un contenedor estructurado que transforma transacciones aisladas en un registro colectivo con validez histórica.

Desde una perspectiva operativa, la relación entre transacciones y bloques se materializa en un proceso secuencial. Las transacciones se generan y se difunden en la red, donde son verificadas de manera preliminar por los nodos. Aquellas que cumplen con las reglas del sistema quedan disponibles para ser incluidas en un bloque. La construcción del bloque implica seleccionar un subconjunto de transacciones y organizarlas de manera coherente dentro de su estructura interna (Medranda Morales & Arcos Agudo, 2023).

Una vez que las transacciones son incluidas en un bloque y este bloque es validado por la red, dichas transacciones adquieren un nuevo estatus. Dejan de ser eventos pendientes y pasan a formar parte del registro permanente de la cadena. Esta transición marca el punto en el que la transacción se integra al consenso distribuido y se vuelve verificable por cualquier nodo de la red a partir del bloque que la contiene.

La dependencia entre transacciones y bloques también se expresa en términos de integridad. Las transacciones no se

almacenan de forma independiente dentro de la cadena, sino como parte de un bloque cuyo encabezado resume criptográficamente su contenido. A través de mecanismos como el árbol de Merkle, todas las transacciones del bloque quedan vinculadas a un único identificador. Esto implica que una modificación en una transacción alteraría el identificador del bloque y rompería la coherencia de la cadena, reforzando la inmutabilidad del registro (Ministerio Público Fiscal, 2023).

Desde el punto de vista del registro contable, el bloque funciona como una «fotografía» del estado de la red en un momento determinado. Las transacciones incluidas reflejan cambios acumulados que, una vez confirmados, actualizan el estado global del sistema. La cadena de bloques, entonces, puede entenderse como una sucesión ordenada de bloques, cada uno de los cuales consolida un conjunto de transacciones y deja constancia de su validez en el tiempo.

Esta relación tiene implicancias directas en tareas de análisis técnico y forense. Para reconstruir el recorrido de un criptoactivo, no alcanza con observar una transacción aislada; resulta necesario identificar el bloque que la contiene, su posición dentro de la cadena y los bloques posteriores que consolidan su validez. La lectura conjunta

de transacciones y bloques permite evaluar confirmaciones, profundidad en la cadena y grado de irreversibilidad del registro.

Asimismo, la relación entre transacciones y bloques introduce límites operativos al sistema. Dado que cada bloque posee una capacidad finita, no todas las transacciones generadas pueden ser incluidas de manera inmediata. Esto genera dinámicas de selección y priorización que impactan en tiempos de confirmación y costos operativos. Aunque estos aspectos se desarrollarán en otras unidades, su base se encuentra en la forma en que las transacciones se agrupan en bloques.

En términos conceptuales, puede afirmarse que la transacción representa la unidad mínima de significado económico o funcional, mientras que el bloque representa la unidad mínima de registro histórico dentro de *blockchain*. La interacción entre ambas es la que permite pasar de acciones individuales a un sistema de registro colectivo distribuido, sin necesidad de intermediarios centrales (Medranda Morales & Arcos Agudo, 2023).

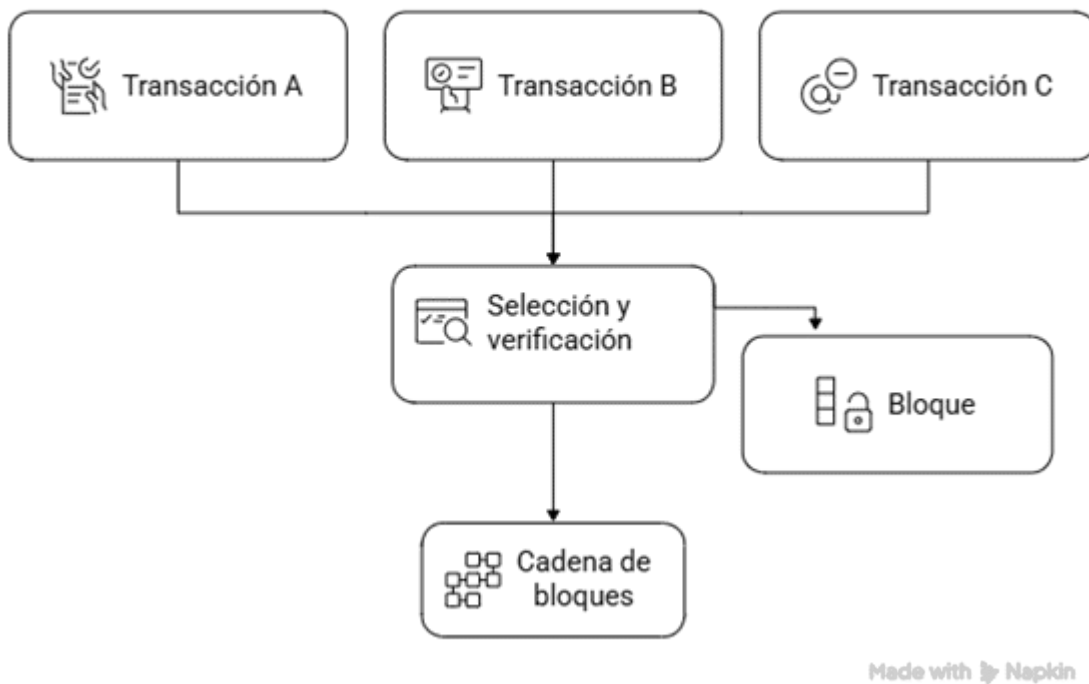
La relación entre transacciones y bloques articula el funcionamiento técnico de la cadena. Las transacciones aportan

el contenido dinámico del sistema, y los bloques proporcionan la estructura que permite validarlo, ordenarlo y preservarlo en el tiempo. Comprender esta relación resulta indispensable para interpretar cómo *blockchain* transforma operaciones individuales en un registro confiable, trazable y compartido.

Para visualizar de manera integrada la relación operativa entre transacciones y bloques, resulta útil representar el flujo que siguen las operaciones desde su generación individual hasta su incorporación definitiva en la cadena. Este recorrido permite identificar el pasaje desde eventos aislados, producidos por usuarios distribuidos, hacia unidades estructuradas que consolidan información validada por la red. La siguiente figura sintetiza este proceso, destacando el rol del bloque como instancia intermedia entre la transacción individual y el registro histórico de la cadena.

Figura 2. Relación entre transacciones y bloques

Proceso de creación de bloques en una cadena de bloques



Fuente: elaboración propia a partir de Ministerio Público Fiscal (2023).

Si bien transacciones y bloques se encuentran estrechamente vinculados, cumplen funciones diferenciadas dentro del funcionamiento técnico de *blockchain*. Distinguir sus características permite comprender con mayor precisión qué tipo de información aporta cada uno y cómo se articulan dentro del sistema de registro distribuido. La tabla que se presenta a continuación resume estas diferencias desde una perspectiva funcional, facilitando la comparación entre ambos conceptos en términos de rol, validación y persistencia del registro.

Tabla 2. Diferencias funcionales entre transacción y bloque

Dimensión	Transacción	Bloque
Unidad básica	Evento individual	Conjunto de transacciones
Función principal	Transferir valor o ejecutar una operación	Registrar y consolidar transacciones
Estado inicial	Pendiente de inclusión	Parte validada de la cadena
Validación	Criptográfica y de reglas	Consenso distribuido
Persistencia	No permanente por sí sola	Permanente dentro de la cadena

Fuente: elaboración propia con base en Ministerio Público Fiscal (2023).

Encadenamiento y hash

El encadenamiento de bloques constituye uno de los rasgos técnicos que distingue a *blockchain* de otros sistemas de registro

digital. A través de este mecanismo, cada bloque queda vinculado de manera directa con el anterior, formando una secuencia continua que preserva el orden histórico de los registros. Esta relación no se establece mediante referencias simples, sino a partir de funciones criptográficas que generan identificadores únicos para cada bloque, conocidos como *hash*.

El *hash* puede entenderse como una huella digital del contenido de un bloque. Se trata del resultado de aplicar una función criptográfica a los datos que conforman el bloque, produciendo una cadena alfanumérica de longitud fija. Este valor resume la información completa del bloque y presenta la particularidad de modificarse ante cualquier alteración mínima de los datos de entrada. De este modo, el *hash* permite verificar la integridad del bloque de forma inmediata y objetiva (Ministerio Público Fiscal, 2023).

El encadenamiento se produce cuando el *hash* de un bloque es incorporado explícitamente en el encabezado del bloque siguiente. Esta inclusión genera una dependencia estructural entre ambos bloques: el bloque nuevo reconoce y valida al anterior como su antecedente legítimo. A partir de esta lógica, la cadena se construye como una sucesión ordenada de bloques interrelacionados, donde cada uno aporta continuidad y coherencia al registro global.

Esta relación criptográfica tiene consecuencias directas sobre la seguridad del sistema. Si se modificara el contenido de un bloque ya incorporado a la cadena, su *hash* dejaría de coincidir con el valor almacenado en el bloque siguiente. Esta incongruencia se propagaría hacia adelante, invalidando todos los bloques posteriores. En términos operativos, esto implica que alterar un registro histórico exige rehacer criptográficamente toda la cadena a partir del punto modificado, lo que vuelve el proceso inviable en redes distribuidas de gran escala (Medranda Morales & Arcos Agudo, 2023).

Para clarificar la función del *hash* dentro del encadenamiento, resulta pertinente detenernos en los principales elementos que intervienen en este vínculo criptográfico y en los efectos que generan sobre la cadena. La siguiente tabla resume estas relaciones desde una perspectiva funcional.

Tabla 3. Relación entre *hash*, bloque y encadenamiento

Elemento involucrado	Función dentro del bloque	Impacto sobre la cadena
<i>Hash</i> del bloque	Identificador único del contenido	Permite verificar integridad

<i>Hash</i> del bloque anterior	Referencia criptográfica al bloque previo	Garantiza continuidad histórica
Modificación del contenido	Altera el hash generado	Rompe la coherencia del encadenamiento
Inclusión en bloque siguiente	Vincula bloques consecutivos	Consolida la secuencia de la cadena

Fuente: elaboración propia con base en Ministerio Público Fiscal (2023).

Desde una perspectiva de funcionamiento distribuido, el *hash* cumple además un rol central en la verificación entre nodos. Cada nodo de la red puede recalcular los *hashes* de los bloques y comprobar que coincidan con los valores registrados. Esta posibilidad elimina la necesidad de confiar en un intermediario y traslada la validación al propio diseño del sistema, apoyado en reglas matemáticas compartidas.

El encadenamiento basado en *hash* también explica por qué la cadena se comporta como un registro acumulativo. Cada bloque nuevo no solo agrega información, sino que reafirma la validez de todos los bloques anteriores al referenciarlos indirectamente. En este sentido, el crecimiento de la cadena refuerza la estabilidad

del registro histórico, ya que cada nuevo bloque aumenta el costo computacional de cualquier intento de alteración retrospectiva.

En contextos profesionales vinculados al análisis técnico, la auditoría o la investigación de criptoactivos, comprender este mecanismo resulta indispensable. La lectura del *hash* de un bloque, su relación con los bloques adyacentes y su posición dentro de la cadena permiten evaluar la integridad de los datos, detectar inconsistencias y reconstruir la secuencia temporal de los registros con precisión técnica.

Entonces, el encadenamiento y el hash operan de manera conjunta como el núcleo de la seguridad estructural de blockchain. El hash asegura la identidad e integridad de cada bloque, mientras que el encadenamiento transforma a los bloques individuales en una cadena coherente, resistente a alteraciones y verificable de forma distribuida. Este mecanismo sienta las bases técnicas de la inmutabilidad del registro, eje que será desarrollado con mayor profundidad en el siguiente subtema.

Inmutabilidad del registro

La inmutabilidad del registro constituye una propiedad operativa que emerge del diseño técnico de *blockchain* y de la forma en que se articulan bloques, transacciones y mecanismos criptográficos. En términos funcionales, esta característica refiere a la capacidad del sistema para conservar los registros una vez incorporados a la cadena, preservando su contenido a lo largo del tiempo y garantizando que los datos reflejen de manera consistente los eventos que efectivamente ocurrieron en la red.

Esta propiedad no responde a una decisión normativa ni a una restricción externa, sino que se deriva directamente de la arquitectura del sistema. Cada transacción validada queda integrada en un bloque, y cada bloque se incorpora a la cadena mediante un encadenamiento criptográfico que refuerza la coherencia del conjunto. A medida que nuevos bloques se agregan, el registro histórico se consolida y se vuelve progresivamente más resistente a modificaciones retrospectivas (Ministerio Público Fiscal, 2023).

Desde una perspectiva técnica, la inmutabilidad se explica por la dependencia estructural entre los bloques. El contenido de cada bloque influye en su identificador criptográfico, y este identificador es retomado por el bloque siguiente. Como consecuencia, cualquier alteración sobre un bloque ya

incorporado genera una ruptura en la cadena que resulta inmediatamente detectable por los nodos de la red. Esta lógica convierte a la modificación de registros en un proceso computacionalmente inviable en redes distribuidas de gran escala.

La inmutabilidad tampoco implica ausencia de control o verificación. Por el contrario, el diseño del sistema permite que cualquier nodo pueda auditar el historial completo de la cadena y comprobar que los registros se mantienen consistentes con las reglas del protocolo. De este modo, la confianza en la información almacenada se apoya en la posibilidad de verificación distribuida y no en la autoridad de un actor central (Medranda Morales & Arcos Agudo, 2023).

En el plano operativo, esta propiedad tiene implicancias directas sobre el uso profesional de blockchain. En contextos de análisis técnico, auditoría o investigación, la inmutabilidad del registro permite trabajar sobre datos cuya integridad se encuentra garantizada por el propio funcionamiento del sistema. La información registrada puede ser consultada, rastreada y analizada sin que exista incertidumbre sobre su alteración posterior.

Para comprender con mayor claridad cómo se materializa esta propiedad en la práctica, resulta útil sintetizar los factores técnicos que la sostienen:

- el encadenamiento criptográfico entre bloques, que vincula cada registro con los anteriores;
- el uso de funciones *hash* que reaccionan ante cualquier modificación del contenido;
- la replicación del registro completo en múltiples nodos distribuidos;
- la validación colectiva de los bloques antes de su incorporación a la cadena;
- el aumento progresivo del costo computacional asociado a la alteración de registros históricos.

Estos elementos operan de manera conjunta y refuerzan la estabilidad del registro a medida que la cadena crece. La inmutabilidad, entonces, no debe entenderse como una característica absoluta e instantánea, sino como una propiedad que se consolida con el tiempo y con la acumulación de bloques validados sobre un mismo historial.

Desde el punto de vista conceptual, la inmutabilidad transforma a *blockchain* en un sistema de memoria técnica compartida. Cada

bloque agregado no solo incorpora nueva información, sino que reafirma la validez de los registros previos, generando un historial acumulativo que puede ser consultado y verificado por cualquier participante de la red. Esta lógica resulta especialmente relevante en escenarios donde la trazabilidad y la persistencia de los datos constituyen requisitos operativos centrales.

En conclusión, la inmutabilidad del registro surge como consecuencia directa del diseño estructural de *blockchain*. A partir de la combinación entre criptografía, encadenamiento de bloques y validación distribuida, el sistema produce un registro resistente a alteraciones, verificable de manera colectiva y estable en el tiempo. Este rasgo completa el análisis de la lógica técnica fundamental de la cadena y sienta las bases para abordar, en la unidad siguiente, el rol del tiempo y del orden cronológico en la validación de la información.

CONTINUAR

Timestamp, orden temporal y validación de la información

En los sistemas blockchain, la validez de la información registrada no depende únicamente de su integridad estructural, sino también de su correcta ubicación en el tiempo. Una vez comprendida la lógica de bloques, transacciones, encadenamiento e inmutabilidad desarrollada en la unidad anterior, resulta necesario avanzar hacia el análisis del orden temporal que organiza los eventos dentro de la cadena y que permite establecer con precisión cuándo ocurrió cada operación.

En esta segunda unidad abordaremos el rol del tiempo como componente técnico del funcionamiento de blockchain. La incorporación de marcas temporales (timestamp) en los bloques permite ordenar las transacciones de manera cronológica y construir un historial coherente de eventos compartido por todos los nodos de la red. Este ordenamiento resulta indispensable para resolver situaciones en las que múltiples operaciones compiten por ser registradas y para sostener acuerdos distribuidos sobre la secuencia válida de los hechos.

Desde una perspectiva operativa, el tiempo en blockchain no cumple una función meramente descriptiva. La marca temporal se integra al proceso de validación de los bloques y contribuye a prevenir problemas estructurales como el doble gasto, al permitir que la red determine qué transacción fue aceptada primero dentro del registro común. De este modo, el orden temporal se convierte en un insumo técnico para la toma de decisiones distribuidas.

Asimismo, la unidad profundiza en los mecanismos de validación colectiva que garantizan que la información registrada sea aceptada como válida por la red. Estos mecanismos articulan el tiempo, el consenso y la verificación entre nodos, diferenciando a blockchain de los sistemas tradicionales de bases de datos, donde el orden y la validación dependen de una autoridad central.

A lo largo de esta unidad analizaremos cómo se construye el orden temporal en la cadena, qué función cumple el timestamp en la validación de la información y por qué estos elementos resultan centrales para comprender el funcionamiento técnico y la confiabilidad de las redes blockchain en contextos profesionales reales.

Timestamp como prueba temporal

En las redes *blockchain*, el tiempo se incorpora al sistema como un dato técnico verificable que permite ordenar los eventos registrados y construir un historial compartido de transacciones. A diferencia de otros entornos digitales donde la marca temporal depende de un servidor central o de una autoridad única, en *blockchain* el *timestamp* se integra al proceso de validación distribuida y forma parte de la estructura del bloque. Esta integración convierte al tiempo en un componente operativo del consenso y no en un simple dato descriptivo.

El *timestamp* puede definirse como una marca temporal asociada a un bloque que indica el momento aproximado en el que dicho bloque fue incorporado a la cadena. Esta marca se expresa como un valor numérico y se incluye dentro del encabezado del bloque, quedando protegida por los mismos mecanismos criptográficos que resguardan el resto de la información. De este modo, el tiempo registrado hereda las propiedades de integridad e inmutabilidad propias de la estructura de la cadena.

Desde el punto de vista funcional, el *timestamp* cumple el rol de prueba temporal. Esto implica que permite demostrar que un

conjunto de transacciones existía en un momento determinado y que fue aceptado por la red en ese orden específico. En contextos distribuidos, donde múltiples nodos generan y reciben transacciones de manera simultánea, esta prueba temporal resulta necesaria para establecer una secuencia común de eventos aceptada colectivamente.

El vínculo entre *timestamp* y validación se vuelve evidente cuando se analiza el proceso de incorporación de un bloque. Para que un bloque sea considerado válido, su marca temporal debe respetar determinadas condiciones establecidas por el protocolo, como encontrarse dentro de un rango coherente respecto de los bloques anteriores. Esta restricción contribuye a evitar inconsistencias temporales y refuerza la coherencia cronológica de la cadena.

A nivel operativo, el *timestamp* permite resolver conflictos vinculados al orden de las transacciones. Cuando dos operaciones intentan gastar el mismo recurso o modificar un mismo estado, la red necesita un criterio objetivo para determinar cuál ocurrió primero. La inclusión de las transacciones en bloques con marcas temporales consensuadas habilita esta resolución sin recurrir a intermediarios centrales, reforzando la lógica descentralizada del sistema.

Para comprender cómo se articula el *timestamp* dentro del funcionamiento general de *blockchain*, resulta útil observar el flujo simplificado que sigue la información temporal desde la transacción hasta el bloque validado.

Figura 3. Proceso de creación de bloque de *blockchain*.

Proceso de creación



Made with  Napkin

Fuente: elaboración propia.

Este esquema permite visualizar que la marca temporal no se añade de manera externa o posterior, sino que se integra al bloque en el momento mismo de su construcción. A partir de ese instante, el *timestamp* queda fijado y protegido por el encadenamiento criptográfico.

En términos prácticos, el uso del *timestamp* como prueba temporal tiene múltiples implicancias profesionales. En el análisis de transacciones, permite reconstruir secuencias de eventos y verificar la prioridad temporal de determinadas operaciones. En contextos regulatorios o forenses, posibilita demostrar que una transacción existía en un momento específico y que no fue alterada con posterioridad. En aplicaciones más amplias, como contratos inteligentes o registros distribuidos, el tiempo registrado condiciona la ejecución de reglas y la validez de acciones automatizadas.

El carácter distribuido del *timestamp* también introduce ciertas particularidades. La marca temporal no representa una hora absoluta universal, sino un valor aceptado por consenso dentro de la red. Esta característica resulta coherente con el diseño descentralizado del sistema y permite que el orden temporal sea funcional al acuerdo colectivo, más que a la precisión cronológica de un reloj central.

El timestamp actúa como un mecanismo técnico que incorpora el tiempo al núcleo operativo de blockchain. Su función como prueba temporal permite ordenar eventos, sostener el consenso distribuido y prevenir conflictos derivados de la simultaneidad de transacciones. Este análisis sienta las bases para profundizar, en el próximo subtema, en el ordenamiento de transacciones y su impacto en la validación de la información dentro de la cadena.

Ordenamiento de transacciones

En las redes *blockchain*, el ordenamiento de las transacciones constituye un proceso técnico indispensable para sostener la coherencia del registro distribuido. Dado que las transacciones se generan de manera simultánea y desde múltiples nodos, el sistema debe establecer un criterio común que permita organizarlas en una secuencia aceptada colectivamente. Este orden no surge de manera espontánea, sino que se construye a partir de reglas de validación, marcas temporales y procesos de consenso.

En un primer momento, las transacciones circulan por la red sin un orden definitivo. Cada nodo recibe, verifica y almacena transacciones de forma local, lo que implica que distintas copias del sistema pueden percibir las en secuencias diferentes. Esta situación es inherente a los sistemas distribuidos y no representa un problema en sí misma, siempre que exista un mecanismo posterior que permita unificar el orden aceptado por la red.

El ordenamiento definitivo de las transacciones se produce cuando estas son incluidas en un bloque validado. El bloque actúa como una unidad de cierre temporal y lógico, ya que consolida un conjunto de transacciones en una secuencia determinada y la integra a la cadena. A partir de ese momento, el orden relativo entre las transacciones incluidas queda fijado y pasa a formar parte del historial compartido del sistema.

Este proceso cumple una función central en la prevención de conflictos operativos, como el doble gasto. Cuando dos transacciones intentan utilizar los mismos recursos, el orden en el que son incorporadas a la cadena determina cuál resulta válida y cuál queda descartada. El sistema no evalúa únicamente la existencia de las transacciones, sino su posición relativa dentro de la secuencia aceptada por la red.

El ordenamiento de transacciones también se vincula con criterios económicos y técnicos. En muchas redes, los nodos que

proponen bloques priorizan transacciones según determinados parámetros, como las comisiones asociadas o el tamaño de los datos. Esta priorización influye en el momento en que una transacción es incluida en un bloque y, por lo tanto, en su posición dentro de la cadena. El orden temporal, en este sentido, se construye a partir de decisiones técnicas reguladas por el protocolo.

Para comprender con mayor claridad este proceso, resulta útil distinguir las distintas etapas por las que atraviesa una transacción hasta adquirir un orden definitivo dentro del registro distribuido.

Tabla 4. Etapas del ordenamiento de transacciones en *blockchain*

Etapas del proceso	Situación de la transacción	Tipo de orden
Difusión en la red	Transacción propagada entre nodos	Orden variable y local
Verificación preliminar	Transacción validada según reglas básicas	Sin orden global

Inclusión en un bloque	Transacción seleccionada por un nodo validador	Orden definido dentro del bloque
Validación del bloque	Bloque aceptado por consenso	Orden fijado en la cadena
Bloques posteriores	Confirmaciones adicionales	Orden reforzado en el tiempo

Fuente: elaboración propia.

Una vez que el bloque es validado y se agregan bloques posteriores sobre él, el orden de las transacciones se consolida progresivamente. Cada nuevo bloque refuerza la secuencia establecida, incrementando la estabilidad del registro y reduciendo la probabilidad de reorganizaciones. Este fenómeno explica por qué, en la práctica, se suele hablar de «confirmaciones» como medida de seguridad temporal.

Desde una perspectiva profesional, comprender el ordenamiento de transacciones resulta fundamental para el análisis de redes *blockchain*. Permite interpretar tiempos de confirmación, evaluar prioridades operativas y reconstruir secuencias de eventos en investigaciones técnicas o regulatorias. Asimismo, habilita la

lectura crítica de métricas como congestión de red, costos de transacción y comportamiento de los validadores.

En síntesis, el ordenamiento de transacciones transforma un conjunto de operaciones dispersas en un registro secuencial coherente. A través de la inclusión en bloques y la validación distribuida, blockchain establece un criterio común de «qué ocurrió primero», resolviendo conflictos y sosteniendo la consistencia del sistema sin recurrir a una autoridad central. Este análisis prepara el terreno para abordar, en el próximo subtema, los mecanismos de validación distribuida que hacen posible este acuerdo colectivo.

Validación distribuida

La validación distribuida constituye el mecanismo mediante el cual una red *blockchain* acepta colectivamente la información que se incorpora al registro. A diferencia de los sistemas centralizados, donde una autoridad única verifica y aprueba los datos, en *blockchain* esta función se reparte entre múltiples nodos que operan bajo reglas comunes. Este diseño permite

sostener la coherencia del sistema aun cuando los participantes no se conocen entre sí ni confían de manera directa unos en otros.

El proceso de validación se activa cuando un conjunto de transacciones es propuesto para formar parte de un bloque. En ese momento, los nodos verifican que las transacciones cumplan con las reglas del protocolo, como la correcta firma criptográfica, la disponibilidad de los recursos involucrados y la consistencia con el estado previo de la cadena. Esta verificación no se apoya en decisiones discrecionales, sino en criterios técnicos previamente definidos y compartidos por toda la red.

La validación distribuida se articula con el orden temporal desarrollado en los subtemas anteriores. El *timestamp* del bloque y la posición que ocupa dentro de la cadena resultan determinantes para que los nodos acepten su validez. Un bloque con una marca temporal incoherente o que contradiga el orden establecido por la cadena es rechazado por la red, lo que refuerza la estabilidad del registro común.

Desde el punto de vista operativo, este mecanismo permite resolver desacuerdos sin recurrir a una instancia central de arbitraje. Cada nodo realiza su propia verificación y compara el resultado con el de otros nodos. Cuando una mayoría converge en la aceptación de un bloque, este se integra a la cadena y se

replica en todas las copias del registro. El consenso surge, entonces, de la coincidencia entre verificaciones independientes y no de una orden externa.

La validación distribuida también cumple un **rol preventivo** frente a intentos de manipulación. Para que un bloque inválido sea aceptado, sería necesario que una porción significativa de los nodos actúe de manera coordinada en contra de las reglas del protocolo. En redes amplias y descentralizadas, este escenario resulta operativamente inviable, lo que refuerza la confianza en la información registrada sin necesidad de controles jerárquicos.

En términos profesionales, comprender este mecanismo resulta central para analizar el funcionamiento real de una red *blockchain*. La validación distribuida explica por qué los datos registrados mantienen coherencia a pesar de la ausencia de una autoridad central, y permite interpretar fenómenos como bifurcaciones temporales, reorganizaciones de bloques o discrepancias transitorias entre nodos.

Asimismo, este modelo introduce una diferencia sustantiva respecto de los sistemas tradicionales. En bases de datos centralizadas, la validación y el orden dependen de un único sistema administrador. En *blockchain*, en cambio, la validación se produce como resultado de un acuerdo técnico distribuido, lo

que modifica las lógicas de control, auditoría y responsabilidad sobre los datos.

La validación distribuida transforma el registro de información en un proceso colectivo basado en reglas técnicas compartidas. A través de la verificación independiente de los nodos, el sistema establece qué información resulta válida, en qué orden se incorpora y bajo qué condiciones se mantiene en el tiempo. Este mecanismo completa el análisis del rol del tiempo y del orden cronológico en *blockchain* y prepara el terreno para abordar, en el subtema siguiente, las diferencias con los sistemas de bases de datos tradicionales.

Diferencias con bases de datos tradicionales

El análisis del *timestamp*, del ordenamiento de transacciones y de la validación distribuida permite establecer una comparación fundada entre *blockchain* y las bases de datos tradicionales. Si bien ambos sistemas comparten la función general de almacenar información, difieren de manera sustantiva en su arquitectura, en sus mecanismos de control y en la forma en que garantizan la validez y coherencia de los datos registrados.

En los sistemas tradicionales, el orden temporal de la información y su validación dependen de una autoridad central que administra la base de datos. Este administrador define qué operaciones se aceptan, en qué secuencia se registran y bajo qué condiciones pueden modificarse. En *blockchain*, en cambio, estas funciones se distribuyen entre los nodos de la red y se sostienen mediante reglas técnicas compartidas, sin intervención de una instancia jerárquica única.

Desde una perspectiva funcional, las principales diferencias pueden sintetizarse en los siguientes aspectos:

- **Modelo de control:** las bases de datos tradicionales operan bajo un esquema centralizado, mientras que *blockchain* distribuye el control entre múltiples participantes.
- **Orden temporal:** en sistemas tradicionales, el tiempo se gestiona a partir del reloj del servidor; en *blockchain*, el orden se construye mediante *timestamps* incorporados a bloques validados por consenso.
- **Validación de la información:** las bases de datos confían en permisos y roles definidos por la administración; *blockchain* utiliza validación distribuida basada en reglas criptográficas.
- **Modificación de registros:** los sistemas tradicionales permiten la edición o eliminación de datos según políticas

internas; en *blockchain*, los registros se preservan como historial acumulativo.

- **Confianza en el sistema:** en bases de datos centralizadas, la confianza se deposita en la entidad administradora; en *blockchain*, se apoya en el diseño técnico del sistema.

Estas diferencias no implican que un modelo reemplace al otro, sino que responden a necesidades operativas distintas. Mientras que las bases de datos tradicionales resultan adecuadas para entornos cerrados y altamente controlados, blockchain se orienta a escenarios donde múltiples actores requieren compartir un registro común sin delegar el control en una autoridad central.

Para clarificar esta comparación desde una perspectiva técnica, la siguiente tabla resume las principales diferencias entre ambos enfoques de gestión de la información.

Tabla 5. Comparación entre *blockchain* y bases de datos tradicionales

Dimensión	Blockchain	Base de datos tradicional
Arquitectura	Distribuida	Centralizada
Orden temporal	Construido por <i>timestamp</i> y consenso	Determinado por el servidor
Validación	Distribuida entre nodos	Centralizada
Modificación de datos	Registro acumulativo	Edición directa posible
Confianza	Basada en el diseño técnico	Basada en la autoridad administradora

Fuente: elaboración propia.

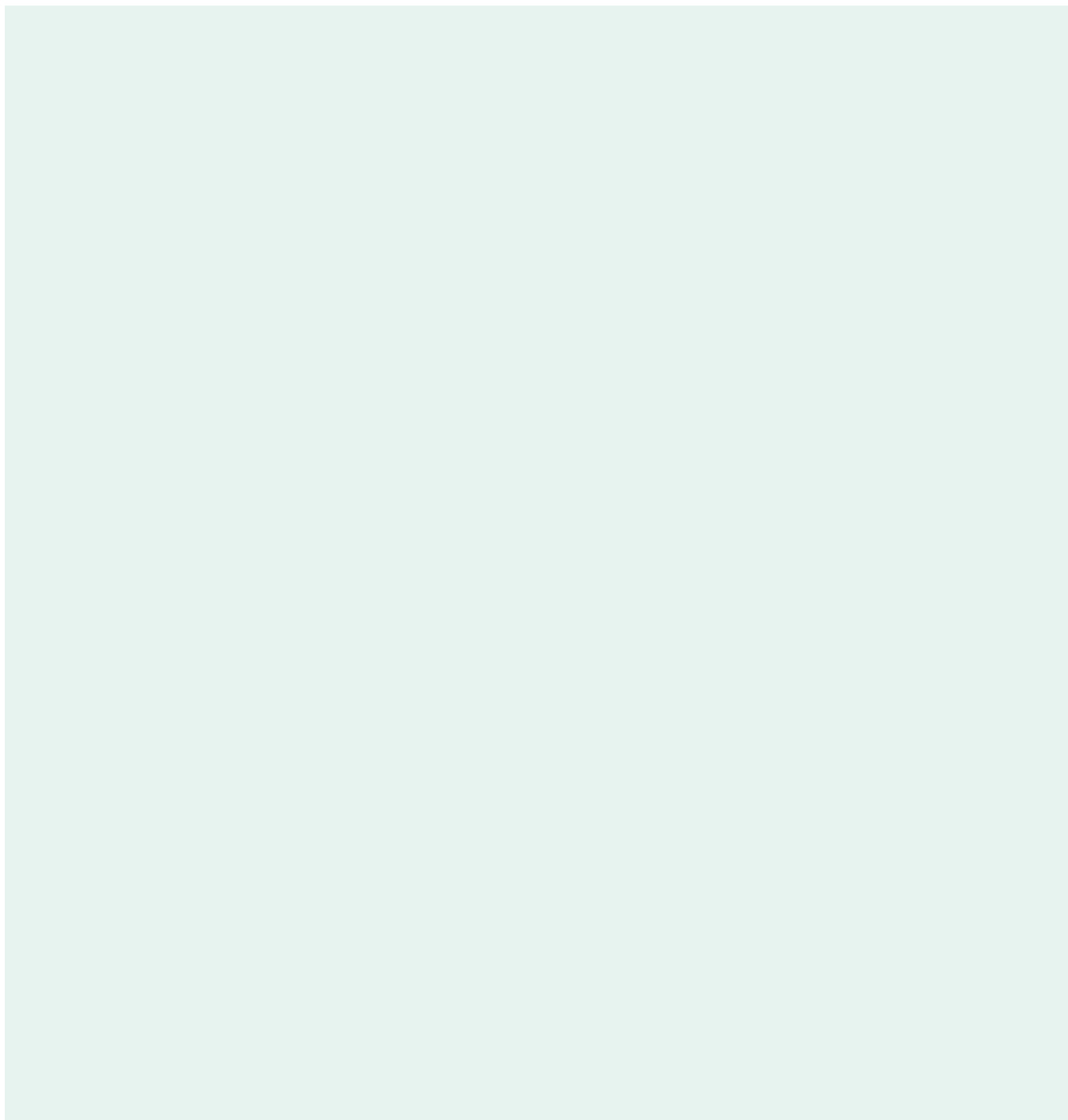
Desde el ejercicio profesional, esta comparación resulta relevante para la toma de decisiones tecnológicas. Comprender cómo se valida la información, cómo se establece el orden temporal y quién controla el registro permite seleccionar el sistema más

adecuado según el contexto operativo, regulatorio o institucional en el que se deba trabajar.

En síntesis, *blockchain* y las bases de datos tradicionales responden a lógicas distintas de gestión de la información. Mientras unas priorizan el control centralizado y la flexibilidad operativa, *blockchain* privilegia la validación distribuida, el orden temporal consensuado y la preservación del historial. Este contraste cierra el desarrollo de la Unidad 2 y permite integrar el rol del tiempo, el orden y la validación como elementos centrales del funcionamiento técnico de *blockchain*.

CONTINUAR

Referencias



Medranda Morales, N., & Arcos Agudo, M. (2023). *Blockchain*. En *Blockchain, criptoactivos y metaverso. Una aproximación teórica* (pp. 13–40). Editorial Abya-Yala. <https://doi.org/10.17163/abyaups.6>

Ministerio Público Fiscal de la Nación. (2023). *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos. Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal*. https://www.mpf.gob.ar/ufeci/files/2023/05/Informe_Criptoactivos.pdf

PortaSigma. (s. f.). *Timestamp en la firma electrónica: ¿Qué es un sello de tiempo?* <https://www.portasigma.com/timestamp-sello-tiempo/>

Skiller Academy. (2024, 20 de marzo). *Timestamp: Clave para la precisión en la gestión de datos*. <https://skiller.education/timestamp/?srsltid=AfmBOopL64phDmw7YRBK51SkwnrqtSVDEvOojrpgTbMkKsfq458qL-xq>

CONTINUAR