Blockchain

Se trata de una de las tecnologías emergentes qué debemos tener en cuenta por su impacto en el sistema probatorio español. Es la tecnología subyacente del bitcoin, pero tiene un potencial sentido práctico único, mucho más allá del económico.

SUG/00239 - Consultas y Sugerencias en Materia de Juego
Si bien el bitcoin no puede ser considerado como una moneda de curso legal o dinero electrónico oficial, tampoco puede considerarse como un mero objeto económicamente evaluable toda vez que el bitcoin o moneda virtual es un medio de cambio virtual o electrónico, reuniendo las características propias de aquéllos, entre ellas el pago electrónico de bienes o servicios (informe del Instituto Español de Estudios Estratégicos de 19 de marzo de 2014)

A nuestros efectos, definiremos «blockchain» como una estructura de datos distribuida, pública y de carácter contable, formada por cadenas de bloques o cadenas articuladas, compuesta por nodos y diseñada para evitar eventuales modificaciones, de tal forma que información contenida en la cadena de bloques solo podrá ser modificada o eliminada si los bloques posteriores son modificados, lo que provoca que para nosotros sea una base de datos histórica de carácter irrefutable, ya que de ser eliminada o modificada, quedaría perfectamente registrado puesto que se añadirían nuevos registros a la cadena, algo que será aprobado por acuerdo de la mayoría de los participantes de la cadena[1]. Al depender blockchain del P2P está sometida a la descentralización, no dependiendo ni de intermediarios ni de ninguna institución gubernamental o financiera.

Hash

Otra definición que nos va a servir para el tema es la de «hash», como algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Destacaremos que, de forma independiente a la longitud de los datos de entrada, el valor del hash de salida tendrá siempre la misma longitud[2].

Blockchain utiliza un sellado de tiempo confiable, que funciona como el hash: vincula el bloque recién creado con el inmediatamente anterior. El empleo de una autoridad de sellado de tiempo emitido por un prestador de servicios de certificación donde ni siquiera el propietario de un dato puede cambiarlo sin que tales modificaciones se hagan públicas (y por tanto aprobadas por los participantes de blockchain) le da una calidad óptima de cara a periciales informáticas.

---

[1] Resulta imposible manipular la cadena de bloques. Podemos modificar uno o dos bloques de datos, pero ni hablar de modificar decenas o centenares de ellos de forma simultánea, lo que provoca a nuestros efectos que funcione como un libro contable dónde se almacena información codificada y certificada.

[2] Los códigos hash son obtenidos mediante la aplicación de un algoritmo que convierte una gran cantidad de datos de un tamaño variable en un valor pequeño de tamaño uniforme (por eso los valores hash son también conocidos como números resúmenes). Esto implica que un conjunto de datos tales como una conversación por correo electrónico, un conjunto de ficheros o un disco duro entero, a través de una función matemática nos producen un valor alfanumérico, el código hash, y si se modifica un solo bit de ese extenso conjunto de datos, cambiará el valor del hash.

Hashparagraph

Introduzcamos otro término: «hashgraph»: con un funcionamiento parecido a blockchain, cada nodo puede difundir información sellada formando eventos (ya no hablamos de bloques) sobre transacciones creadas y recibidas de otros, a otros nodos elegidos al azar. Después estos nodos agregarán los eventos recibidos con la información recibida de otros nodos en un nuevo evento, y lo enviarán a otros nodos elegidos al azar. Esto continúa hasta que todos los nodos conocen la información creada o recibida al principio, provocando que la información llegue a cada nodo de la red muy rápidamente[3]. Es también más segura pues es una tecnología asincrona (nadie puede evitar que se llegue a un consenso o interrumpir uno que ya ha sido alcanzado) empleando para ello el sellado de tiempo confiable.

Prueba

Prueba sería aquella razón, argumento, instrumento u otro medio con el que se pretende mostrar y hacer patente la verdad o falsedad de una cosa.
Prueba también sería el instrumento conducente a demostrar la certeza de los hechos controvertidos en el proceso.

Con estas definiciones de partida, la cadena bloques tiene una perfecta cabida en nuestro ordenamiento jurídico como medio de prueba, a pesar de que ni blockchain ni hashgraph se encuentran en las cláusulas del artículo 1º, apartado primero del artículo 299 de la LEC son legítimos medios de prueba, apoyándonos en artículo 352.

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

Artículo 299. Medios de prueba.
1. Los medios de prueba de que se podrá hacer uso en juicio son:

1.º Interrogatorio de las partes.
2.º Documentos públicos.
3.º Documentos privados.
4.º Dictamen de peritos.
5.º Reconocimiento judicial.
6.º Interrogatorio de testigos.

Artículo 352. Otros dictámenes periciales instrumentales de pruebas distintas.
Cuando sea necesario o conveniente para conocer el contenido o sentido de una prueba o para proceder a su más acertada valoración, podrán las partes aportar o proponer dictámenes periciales sobre otros medios de prueba admitidos por el tribunal al amparo de lo previsto en los apartados 2 y 3 del artículo 299.

Advirtamos que si revisamos el reglamento eIDAS[4], podemos constatar que ni blockchain ni hashgraph son prestadores de servicios de certificación de confianza. Esto significa que son confiables, pero no cualificados, pues no son verificados por un prestador de servicios de confianza. No gozan pues de presunción de exactitud, por lo que habría que acreditar ésta en cada caso concreto demostrando que la información contenida no fue manipulada o eliminada.

[3] 250.000 transacciones por segundo frente a las 7 de blockchain.
[4] REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

Cadena de custodia y prueba electrónica

Es incontestable que cada vez se aportan más pruebas a los procesos obtenidas a través de las TIC, pero antes de confiar en la veracidad del contenido de una prueba electrónica hay que adoptar numerosas cautelas, pues éstas son fácilmente manipulables. Eso nos lleva a poner acento en la llamada cadena de custodia haciendo especial referencia al ámbito digital. Podríamos definir a la cadena de custodia como: conjunto de procedimientos de seguridad destinados a garantizar la integridad e ausencia de menoscabo en el elemento probatorio desde el momento de su obtención, hasta la práctica de la prueba en juicio oral. Esta necesaria conservación de ciertas fuentes de prueba viene justificada por la necesidad de asegurar que puedan emplearse como pruebas en el juicio. Deben pues ser protegidas contra contaminación, sustracción, intercambio o destrucción, de tal modo que su principal objetivo sea asegurar que provenga de fuente original y auténtica y si no es así, que quede constancia de esa falta de autenticidad.

Debemos resaltar que prácticamente todo proceso con las pruebas que conlleven la manipulación provocan la alteración de las mismas[5], de ahí lo importante del concepto de Cadena de Custodia, que no hay que confundir con la gestión de muestras. Ésta responde a un concepto más amplio que incluye todo procesamiento de pruebas, desde la toma de vestigios, de datos hasta su destrucción o devolución a los propietarios una vez finalizado el juicio, con un control que proteja su integridad. La cadena de custodia, que podemos ver como algo embebido en este concepto más grande, por otra parte, se refleja en un conjunto de documentos que dan detalle de toda la gestión de muestras, incluyendo que manipulaciones se hacen y por quien se hacen.

Esta distinción que acabamos de hacer entre la gestión de muestras y la cadena de custodia nos dirigen directamente a otro concepto: la prueba sobre la prueba. Con él, hablamos de establecer un control sobre la fiabilidad de la prueba que se aportó al inicio, de tal forma que la autenticidad del resultado probatorio, de los estudios que hagamos sobre la misma, quedes confirmados o refutados. No es algo que aparezca con la informática, en los tribunales la prueba sobre la prueba ha consistido desde antiguo en actuaciones tales como el careo entre testigos que realizan declaraciones contradictorias, en el peritaje psicológico sobre testigos o sobre la víctima de un delito e incluso periciales tan particulares como o la prueba caligráfica para verificar la autenticidad de una firma. Desde que la informática invadió la vida de la sociedad, la práctica de la prueba sobre la prueba se ha incrementado, sin duda por la elevada volatilidad y facilidad de modificación de las fuentes de prueba que la conforman[6].

---

[5] Tengamos en cuenta que el mero hecho de introducir un pendrive en un puerto USB ya puede llevar a su contaminación. Si sucede esto en una actuación tan simple, y es capaz de alterar la autenticidad de la prueba, se ve mucho mejor la necesidad de articular un modo de demostrar la integridad de la prueba para que sea fiable en sede judicial.

[6] Podemos ver un ejemplo con la sentencia Tribunal Supremo 300/2015 de 19 de mayo que alude a la queja sobre la falta de autenticidad de un diálogo mantenido. En este caso se consideró un pantallazo como prueba sin realizar sobre el mismo estudio pericial alguno, pues los participantes en la conversación la reconocieron como auténtica y fiel a la original, lo que por otra parte nos lleva a deducir que la pericial solo es obligatoria si la contraparte ha sido quién ha mantenido que la conversación que se aporta y la impugna. De otra forma, si quien la impugna no ha participado en la conversación o, siendo parte de la misma, no niega su fidelidad, no es preciso realizar prueba pericial informática alguna.
De la sentencia STS 300/2015, 19 de Mayo de 2015:

Añadamos otro aspecto de interés, el que nos habla de la inversión de la carga de la prueba pericial sobre la prueba electrónica. Esto es: se trata de lo que sucede cuando para impugnar la autenticidad de la prueba electrónica, se ha de practicar otra prueba que determine si existe o no alteración de la misma. Lo que es importante en este momento para nosotros es determinar a quién le corresponde hacer frente a esta carga probatoria.

En una nota al pie aludimos a la sentencia del Supremo 300/2015 de 19 mayo, de ella observamos que quien pretenda ser favorecido por la protección de cualquier tipo de comunicación establecida mediante el soporte de las TIC es quien debe demostrar tanto su idoneidad, así como la veracidad sobre su origen, mediante una pericial. Esto, en pocas palabras, es un desplazamiento de la carga de la prueba, un giro de la práctica habitual de la prueba sobre la prueba, pero no en extremo novedoso pues sigue la línea de lo ya establecido respecto a la autenticidad de los documentos aportados a la causa.

Y es en este punto donde entra en juego la garantía de autenticidad en el campo de informática con el ya aludido código hash. Cuando tratamos de determinar si estamos ante un mismo archivo que se captó en su día, un anuncio publicado en un foro, una web, una conversación por mensajería que se aporta como original o cualquier elemento similar, como debemos comprobar si se ha dado o no una ruptura de la cadena de custodia, una herramienta estupenda son los códigos hash. Estos serán elementos clave para demostrar la indemnidad de una evidencia digital. Si no se da la coincidencia del hash original con el final, eso basta para desvirtuar el resultado probatorio en el juicio oral. Recordemos que es la parte que aporta la evidencia electrónica la que debe demostrar su autenticidad, por lo que lo lógico es que de forma previa se realice una copia exacta del contenido de la misma (un clonado[7]). Así, el trabajo del perito informático no será tan solo calcular el hash, pues habrá así mismo de preservar la fuente de la prueba (el contenido electrónico que se pretende aportar a la causa).

Otro elemento complementario al anterior, que aquí tan solo apuntamos, sería el llamado haking legal. Por emplear una definición extendida[8] podríamos definirlo como la intromisión en sistemas, programas o datos informáticos ajenos con la finalidad de investigar los delitos que se hayan podido cometer. Esto debe hacerse, como es obvio,

---

Respecto a la queja sobre la falta de autenticidad del diálogo mantenido por Ana María con Constancio a través del Tuenti, la Sala quiere puntualizar una idea básica. Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.

[7] Es aconsejable que el clonado se haga por duplicado de forma que podamos depositar una de ellas ante fedatario y empleando la otra para el análisis técnico.

[8] Kerr, Orin S., Digital Evidence and the New Criminal Procedure. 105 Columbia Law Review 279 (2005). Available at SSRN: https://ssrn.com/abstract=594101

con instrumentos no invasivos, que nos permitan acceder a toda la información sin provocar en ella ningún tipo de daño o alteración[9].

[9] Muy utilizado al respecto de mantener esa aspecto “no invasivo” es el llamado «bit stream image»: se trata de una copia sector a sector / bit a bit de un disco duro. Sería en realidad un conjunto de archivos que se pueden usar para crear una copia exacta de un disco duro, preservando todos los datos latentes además de los archivos y las estructuras de directorios.