Kevin Leonel Young

Incidencias de la *blockchain* sobre la autoría e integridad de los documentos electrónicos desde una doble perspectiva española-argentina

TRABAJO FINAL DE MÁSTER

Tutora: Dra. Roser Casanova Martí

Tarragona

2021

Este TFM se ha realizado en la modalidad:

□ **Artículo científico**

☑ **Trabajo de investigación**

RESUMEN:

La *blockchain* o cadena de bloques supone una de las innovaciones más disruptivas de los últimos tiempos. Su creciente implementación en diversos ámbitos implica una potencial relevancia para el derecho que es necesario profundizar. Específicamente dentro del ámbito probatorio, esta tecnología puede tener especial incidencia en dos de los atributos que hacen a la eficacia probatoria de los documentos electrónicos: la autoría y la integridad. A través de un análisis doctrinario, jurisprudencial y de la normativa civil, puestos en relación con algunos aspectos técnicos de la *blockchain* se procura determinar la efectiva incidencia de esta tecnología sobre esos dos elementos. Ello se hará desde una doble perspectiva española-argentina, esta última enfocada en la regulación procesal de la provincia de Córdoba. Determinada la naturaleza documental de las transacciones de la cadena de bloques, se propone su ingreso al proceso civil mediante el medio de prueba documental. La autoría podrá ser argumentada con base al uso de firmas electrónicas por parte de esta tecnología. No obstante, se encontrarán barreras que dificultan la atribución de efectos jurídicos sobre un individuo en concreto, sobre todo ante la ausencia de procesos que identifiquen correctamente a los participantes de la cadena de bloques. En lo que hace a la integridad, el uso de sellos de tiempo permitirá afirmar que un documento electrónico existió en un momento determinado, lo que sumado a la garantía de inmutabilidad que proporciona la *blockchain*, nos sitúa frente a una prueba sólida que respalda la inmutabilidad del contenido de dicho documento.

Palabras clave: *blockchain* – cadena de bloques – prueba electrónica – prueba en el proceso civil – documentos electrónicos – autoría – integridad.

***ABSTRACT*:**

The blockchain is one of the most disruptive innovations of recent times. Its growing implementation in various fields has a potential relevance for the law that needs to be studied. Specifically, within the evidentiary field, this technology may have a special impact on two of the attributes that make the evidentiary effectiveness of electronic documents: authorship and integrity. Through a doctrinal, jurisprudential, and civil law analysis, in relation to some technical aspects of the blockchain, we will try to determine the effective impact of this technology on these two elements. This will be done from a dual Spanish Argentine perspective, the latter focused on the procedural regulation of the

province of Córdoba. Having determined the documentary nature of blockchain transactions, its entry into the civil process is proposed by means of documentary evidence. Authorship may be argued based on the use of electronic signatures by this technology. However, barriers will be encountered that make it difficult to attribute legal effects on a specific individual, especially in the absence of processes that correctly identify blockchain participants. In terms of integrity, the use of time stamps will make it possible to affirm that an electronic document existed at a given time, which, added to the guarantee of immutability provided by the blockchain, places us in front of a solid proof that supports the immutability of the content of said document.

Key words: blockchain – electronic evidence – evidence in civil proceedings – electronic documents – authorship –integrity.

ÍNDICE

ABREVIATURAS

AST	Autoridad de Sello de Tiempo
BFA	Blockchain Federal Argentina
BOE	Boletín Oficial del Estado
BOEC	Boletín Oficial Electrónico de la Provincia de Córdoba
BORA	Boletín Oficial de la República Argentina
CCCN	Código Civil y Comercial de la Nación
CPCC	Código Procesal Civil y Comercial de la Provincia de Córdoba
DLT	Distributed Ledger Technology
LEC	Ley de Enjuiciamiento Civil
LFD	Ley de Firma Digital
LFE	Ley de Firma Electrónica
LSEC	Ley reguladora de determinados aspectos de los servicios electrónicos de confianza

I. INTRODUCCIÓN

La revolución tecnológica supone nuevos retos para el derecho y una de las innovaciones que muchos califican de disruptiva es la denominada *blockchain* o cadena de bloques. Si bien su aparición se remonta a 1991, su "salto a la fama" se produjo con la irrupción de las llamadas criptomonedas, aunque en realidad su uso no se limita solo a ellas, sino que trasciende diversos ámbitos, con potencial relevancia en el derecho. Es así como debido a las garantías de seguridad que esta tecnología supone, en los últimos tiempos su adopción se ha acelerado tanto por parte de empresas y particulares como por las mismas Administraciones públicas. Todo ello determina la necesidad del estudio de la *blockchain* y su implicación para el derecho, ya que en un futuro próximo no serán pocas las cuestiones que se suscitarán en los tribunales de justicia referidas a su utilización.

En este sentido, mucho se discute sobre las bondades de esta tecnología, sin embargo, la mayoría de los trabajos de la doctrina científica se centran particularmente en los aspectos relacionados con los criptoactivos, siendo más bien pocos los que indagan con algún grado de minuciosidad en cómo esta tecnología puede realizar un aporte útil y eficaz al derecho. Es por esta razón que dedicaremos nuestro trabajo de investigación a esta temática. Centrándonos en el ámbito probatorio se suele afirmar constantemente que la cadena de bloques otorga "plena validez legal" o hace "plena prueba" respecto a los datos a ella vinculados, pese a ello, contamos con escasos estudios específicos que justifiquen el fundamento de tales afirmaciones. Por ello resulta necesario profundizar en esta cuestión e indagar cómo esta tecnología aporta un mayor valor sobre la información contenida, que pueda ser útil en el marco de un proceso judicial.

En primer lugar, debemos señalar que la eficacia probatoria de los documentos electrónicos gira principalmente en base a tres ejes: autoría (o autenticidad), integridad y licitud. Por nuestra parte consideramos que la *blockchain* tiene una potencial incidencia sobre los dos primeros ejes. Por ello, la investigación se orientará en dos aspectos: por un lado, determinar si esta tecnología es útil para demostrar quien realizó una determinada transacción o documento a ella asociado, garantizando la fuente de la que proceden tales datos. Y por el otro, analizar si puede garantizar su integridad, esto es, que los datos no hayan sido modificados desde su creación o desde una determinada fecha.

De esto se deriva que el objetivo general de la presente investigación gire en torno a determinar cómo incide la *blockchain* en la prueba de la autoría e integridad de los documentos electrónicos y establecer si hace una aportación útil y eficaz sobre estos aspectos, que contribuya a la eficacia probatoria de los datos vinculados a ella.

Consideramos que este tema tiene especial relevancia para los operadores jurídicos en general, tanto desde el punto de vista del juzgador como desde la perspectiva de los abogados independientes, como a continuación se detalla. Desde la óptica del juzgador, si bien no se le requieren conocimientos técnicos en su labor, sí es necesario una mínima comprensión del tema para impartir justicia de manera eficiente, máxime cuando esta tecnología puede tener importantes incidencias en materia probatoria e incluso, aunque pueda valerse de dictámenes periciales o de otros medios de prueba, debe contar con los elementos necesarios que le permitan incluso apartarse de ellos de manera justificada. Y, del lado de la profesión legal independiente, los tiempos que corren exigen además de multidisciplinariedad en su labor, una constante adaptación a los cambios que permita adoptar estrategias legales acordes para garantizar la defensa de los intereses del cliente. Siendo que cada vez más sectores están implementando soluciones basadas en *blockchain*, resulta imperioso comprender su impacto legal, para así asegurar un adecuado asesoramiento, proposición de prueba y defensa, más teniendo en cuenta la naturaleza dispositiva del proceso civil que pone en cabeza de las partes la labor investigativa.

El análisis de todo lo mencionado se realizará conforme los presupuestos metodológicos de la dogmática jurídica. A tal fin partiremos de una tarea sistematizadora, que pretende dar cuenta del conjunto de normas con las que se va a trabajar. Asimismo, nos abocaremos a la labor descriptiva, identificando los problemas interpretativos que se presenten, especialmente en lo que refiere a la noción de prueba electrónica o documento electrónico. Se hará una valoración de la legislación vigente, constituyendo un análisis de *lege lata*. Por otro lado, se seguirá la metodología comparada desde un punto de vista externo, al relevar tanto el ordenamiento jurídico español como el argentino (este último delimitado a la provincia de Córdoba), tomando como base aquellas normas que tienen incidencia en la determinación de la autoría e integridad de la prueba. El estudio estará delimitado además solo para el caso de documentos electrónicos privados y circunscripto al ámbito del proceso civil. Asimismo, el principio rector que guiará el análisis e incidirá transversalmente en esta investigación, será el principio de libertad de prueba.

En cuanto a la estructura del trabajo, este se divide en diferentes apartados. En primer lugar, se delinean las bases teóricas respecto a algunos puntos vinculados a la prueba electrónica. Dado que son analizados dos ordenamientos jurídicos diferentes, consideramos útil y necesario dedicar un apartado a plasmar algunas cuestiones vinculadas a posiciones doctrinarias y regulación legal de la prueba electrónica en general y del documento electrónico en particular, que serán aplicadas posteriormente. En el apartado siguiente se explicará la denominada cadena de bloques o *blockchain*. Luego de conceptualizarla, se explicará sucintamente su funcionamiento, sus clases y la relevancia que reviste en el contexto actual. Asimismo, se hará un breve repaso por algunos casos puntuales en que esta tecnología es aplicada tanto en España como en Argentina. También se procurará dilucidar la existencia o no de normativa aplicable que incida en nuestro estudio y su consideración como fuente o medio de prueba. Finalmente, las nociones de los apartados anteriores se conjugarán para dar lugar a un análisis específico sobre los aspectos objeto de esta investigación: de la autoría y la integridad en la *blockchain*, en el cuarto y quinto apartado respectivamente.

Por último, anticipamos ya desde el inicio que la casuística a la que abre las puertas la cadena de bloques resulta inagotable. Si bien muchos de los apartados analizados podrían ser merecedores de un extenso tratamiento individualizado, intentaremos abordar el tema de una manera global para dar una respuesta concreta al problema planteado. Por ese motivo no se entrará en detalle sobre otros temas que, si bien están íntimamente vinculados con esta tecnología (como los contratos inteligentes o *smart contracts*), exceden el objetivo de estudio de esta investigación y que por su complejidad son merecedores de otro estudio diferenciado, aunque los resultados obtenidos en la presente también le podrán resultar aplicables.

II. LA PRUEBA FRENTE A LAS NUEVAS TECNOLOGÍAS

1. LA PRUEBA ELECTRÓNICA

1.1. PLANTEAMIENTO

Tradicionalmente el derecho ha sido reacio a la modernización y a su adaptación a las tecnologías de la información, produciéndose una constante tensión entre las regulaciones legales, normalmente desactualizadas, y los avances tecnológicos. No obstante, debemos recordar que uno de los principios que rige transversalmente todo el ámbito probatorio, es el principio de libertad de prueba. Tal como refiere Picó i Junoy[1], este principio implica el derecho que poseen las partes de un proceso para utilizar todos los medios de prueba que resulten necesarios para que el juzgador forme convicción suficiente sobre el objeto de litigio, lo que deriva en que toda prueba ofrecida en cumplimiento de los requisitos legales debe ser necesariamente admitida y practicada.

A tenor de lo antes mencionado, los avances tecnológicos nunca pueden suponer un impedimento a la concreción de este derecho fundamental, consagrado en el art. 24.2 de la Constitución española y art. 18 de la Constitución argentina. No obstante, las nuevas tecnologías, dieron y continúan dando lugar a innumerables fuentes de prueba, que generan diversos problemas a la hora de determinar su ingreso y valoración en un proceso judicial.

Para comenzar este trabajo debemos analizar qué se entiende por prueba electrónica, para continuar luego por describir su marco jurídico. Si bien existen numerosas expresiones equivalentes, tales como "prueba digital" o "prueba de las nuevas tecnologías" usaremos la expresión "prueba electrónica" para referirnos a este fenómeno, y cuyo contenido precisaremos a continuación.

1.2. CONCEPTO

En primer término, debemos delimitar el concepto de prueba electrónica. Para ello conviene hacer un repaso sobre algunas definiciones construidas por la doctrina.

[1] Joan Picó i Junoy, *Las garantías constitucionales del proceso*, 2ª ed. (Barcelona: J.M. Bosch Editor, 2012), 177.

Según Abel Lluch[2], la prueba electrónica es toda aquella "información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para formar la convicción en torno a una afirmación relevante para el proceso". La prueba electrónica tal como la describe este autor puede constituirse tanto como objeto o medio de prueba, e incluso ambos simultáneamente. Se dice que es objeto de prueba cuando debe probarse un hecho electrónico; o medio de prueba cuando debe probarse electrónicamente un hecho. Y en los casos que deba probarse electrónicamente un hecho electrónico, estaremos frente a la prueba electrónica como objeto y medio de prueba.

Por su parte, Delgado Martín[3] entiende por prueba digital o electrónica "toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio".

En el caso de Sanchís Crespo[4], la autora la define como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, o bien al fijar este hecho como cierto atendiendo una norma legal". Sin embargo, al momento de dar dicha definición, en el año 2012, la propia autora reconoció que este concepto variaría en el momento en que fuese implantado de manera completa el expediente judicial electrónico, tornándose más amplia. Siendo que ese hecho es una realidad tanto en España como en varias provincias de Argentina (incluyendo Córdoba) debemos tener en cuenta entonces el nuevo concepto que la autora propone. Así, la prueba electrónica sería todo "documento en soporte informático relativo a los medios de prueba". De esta manera, la autora sostiene que, si el documento representa el hecho controvertido, hablaremos de prueba electrónica documental, caso contario será prueba electrónica según el medio de prueba frente al que estemos.

En la doctrina argentina, la prueba electrónica se ha definido como "aquella prueba cimentada en la información o datos, con valor probatorio, que se encuentran insertos dentro de un dispositivo electrónico o que hubiera sido transmitida por un medio

[2] Xavier Abel Lluch, «Prueba electrónica», en *La prueba electrónica*, dir. Xavier Abel Lluch y Joan Picó i Junoy (Barcelona: J.M. Bosch Editor, 2011), 23-26.
[3] Joaquin Delgado Martín, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 2ª ed. (Madrid: Wolters Kluwer, 2018), 40.
[4] Carolina Sanchís Crespo, «La prueba en soporte electrónico», en *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio*, coord. Eduardo Gamero Casado y Julián Valero Torrijos (Navarra: Aranzadi, 2012), 713.

afín, a través del cual se adquiere el conocimiento sobre la ocurrencia o no de hechos que las partes hayan afirmado como fundamento de sus derechos, o cuestionados, y que deban ser invocados dentro de un proceso judicial"[5].

Vemos así que, aún con diferentes matices, la prueba electrónica es concebida ampliamente como aquella prueba que se asienta en dispositivos electrónicos o medios digitales y que resulta útil para probar hechos o afirmaciones en el proceso. Esto debe coligarse con la constatación de que en los tiempos que corren la prueba electrónica dejó de ser la excepción para comenzar a convertirse en la regla. Es así como, con el advenimiento constante de nuevas tecnologías y su acelerada adopción, sobre todo en los últimos tiempos, la prueba electrónica ya está presente en una gran cantidad de procesos judiciales. Como consecuencia y si bien se trata de una especie dentro del género de la prueba, sus especiales características la convierten en un desafío para muchos operadores jurídicos.

1.3. Desafíos y tensiones actuales

Como consecuencia de la creciente difusión de los aportes tecnológicos, la prueba electrónica ha supuesto desde un principio un desafío para gran parte de los abogados y jueces. Si bien podríamos hacer un extenso listado de ventajas y desventajas de la prueba electrónica[6], no es la finalidad del presente trabajo de investigación, sino que nos centraremos en algunas problemáticas puntuales, que a continuación desarrollaremos.

Los avances tecnológicos implican el nacimiento constante de nuevas fuentes de prueba electrónica, por lo que su enumeración se hace prácticamente imposible, no resultando factible una regulación legal que pueda preverlas a todas. De esta manera nos encontramos frente a fuentes probatorias ilimitadas, en contraposición a los medios de prueba que están desarrollados en los códigos procesales, que son esencialmente limitados.

Esta tensión generada entre medios de prueba limitados, frente a fuentes ilimitadas, genera la doble tarea de identificar cuáles son estas nuevas fuentes de prueba

[5] Gastón Enrique Bielli y Carlos Jonathan Ordoñez, *La prueba electrónica: teoría y práctica* (Buenos Aires: La Ley, 2019), 7.
[6] Para un mayor abundamiento recomendamos la lectura del resumen efectuado en Fernando Pinto Palacios y Purificación Pujol Capilla, *La prueba en la era digital* (Madrid: Wolters Kluwer, 2017), 29-31.

y cómo va a operar su ingreso al proceso mediante alguno de los medios de prueba previstos por la legislación procesal[7].

Otra de las principales dificultades de la prueba electrónica −tal como reitera Abel Lluch[8]− radica en las garantías de autenticidad, integridad y licitud para superar el denominado *test* de admisibilidad y desplegar en el proceso toda su eficacia probatoria.

En cuanto a la autenticidad, y a diferencia de los medios tradicionales, el carácter electrónico dificulta la prueba acerca de quien creó ese contenido. Este punto será ampliado cuando tratemos el documento electrónico, que en la medida de una relación género-especie, comparte varios de los mismos inconvenientes.

Respecto a la integridad de la prueba electrónica, es sabido que una de sus características que a su vez constituye una de sus principales problemáticas, es su carácter volátil. Ello implica que pueden ser fácilmente modificables. Este punto también se repite en el documento electrónico, tal como veremos más adelante.

1.4. Regulación legal

En el ordenamiento jurídico español, la Ley de Enjuiciamiento Civil[9] (en adelante LEC) no menciona específicamente a la prueba electrónica, por lo que no existe una definición legal, pero parece existir una regulación autónoma a través de los art. 299 y 382 a 384 LEC.

En el caso del primer desafío antes descrito, y siguiendo a Abel Lluch[10], la LEC intenta resolver la problemática de fuentes probatorias ilimitadas versus el carácter limitado de los medios de prueba clasificando los medios de prueba en “clásicos” (art. 299.1 LEC); “modernos” (art. 299.2 LEC); y “futuros” (art. 299.3 LEC). De esta manera, la última parte del referido artículo actúa como una cláusula abierta que puede servir para incorporar nuevas fuentes de prueba. No obstante, el autor aclara que, aunque el art. 299.3 LEC se refiera a medios de prueba en realidad la norma se está refiriendo a fuentes de prueba, al igual que el art. 299.2, ya que como se dijo anteriormente, lo que es ilimitado son las fuentes, frente a los medios que son limitados. Apoya este pensamiento la reciente

[7] Abel Lluch, «Prueba electrónica», 61.
[8] Abel Lluch, 78.
[9] Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (España: BOE, núm. 7, de 08/01/2000).
[10] Abel Lluch, «Prueba electrónica», 64.

Sentencia del Tribunal Supremo 706/2020[11], por cuanto reconoce que los medios de prueba son solo aquellos previstos por el art. 299.1 LEC, que tiene el carácter de *números clausus*.

Por otro lado, en cuanto a la regulación legal de la prueba electrónica, autores como Sanchís Crespo[12] sostienen que entre la prueba electrónica y el medio de prueba documental existe un paralelismo, ya que a pesar de que varía el soporte (tradicional o electrónico), no lo hace el hecho representado, que puede ser el mismo. Por ese motivo diferencia entre medios de prueba estrictamente documentales y los demás medios de prueba (no documentales).

Esta diferencia tiene implicaciones al momento de acudir a la normativa que va a regular la prueba. Así, sostiene la autora que, frente a los medios de prueba documentales, deberá seguirse principalmente a lo referido a la prueba documental, por cuanto dicha regulación es mucho más completa y precisa, a diferencia de las lagunas en la regulación de los medios de prueba de los arts. 382 a 384 LEC. Además, aclara que la distinción efectuada por la LEC entre medios audiovisuales e instrumentos de archivo no resulta pertinente, siendo innecesaria ya que ambos soportes pueden contener indistintamente diversas informaciones[13].

Así, en este último entendimiento, en el caso de la prueba electrónica, habrá dos regulaciones distintas en la LEC según si estamos ante prueba electrónica documental o no.

En el ordenamiento jurídico argentino, todo lo relativo al procedimiento se encuentra regulado en el derecho procesal, que articula el sistema probatorio, sin perjuicio de que el derecho de fondo o sustancial también pueda contener alguna regulación en tal sentido. Conforme el art. 75 inc. 12 de la Constitución Nacional, el dictado de los códigos de fondo (como lo es Código Civil) corresponde al Congreso de la Nación, mientras que *contrario sensu,* los códigos procesales son competencia de cada provincia, quienes conservan todo el poder no delegado al Gobierno federal (art. 121 de la Constitución Nacional).

[11] Sentencia del Tribunal Supremo (Sala de lo Social) 706/2020, de 23 de Julio de 2020, ponente Ilmo. Sr. D. Juan Molins García-Atance f.j. 3°-4°.
[12] Sanchís Crespo, «La prueba en soporte electrónico», 713.
[13] Sanchís Crespo, 726.

Ni en el Código Civil y Comercial de la Nación[14] (en adelante CCCN) ni en el Código Procesal Civil y Comercial de la Provincia de Córdoba[15] (en adelante CPCC) existe una definición legal de prueba electrónica o una regulación específica. Por ello debemos seguir los cauces establecidos según el tipo de prueba pertinente.

No obstante, a falta de regulación, esta tensión a la que hacíamos referencia entre fuentes de prueba ilimitados frente a medios de prueba limitados encontraríamos *a priori* solución en el art. 202 CPCC. Esta norma establece que frente a un medio de prueba idóneo y pertinente que no se hallare previsto por la normativa, el tribunal establecerá el mecanismo para su diligenciamiento, a cuyo fin usará el procedimiento establecido para otros medios de prueba análogos. De esta manera, aun frente a medios de prueba no considerados "clásicos", la legislación prevé una cláusula genérica para facilitar su incorporación.

Vemos así que el CPCC sigue una postura de neutralidad tecnológica, utilizando términos que pueden escindirse de los avances tecnológicos, lo que trae como beneficio que, frente al desarrollo de nuevas tecnologías, la normativa no quede desactualizada, permitiendo la incorporación de aquella prueba electrónica existente o a existir, utilizando analógicamente lo establecido para otros medios de prueba.

2. Documento electrónico

2.1. Planteamiento

Una vez tratada la prueba electrónica como género, debemos enfocarnos en el tratamiento de una de sus especies: el documento electrónico, que se erige como la principal modalidad de la prueba electrónica, quizás la más importante.

2.2. Concepto

Ingresando a la definición de documento electrónico, según Abel Lluch[16] este consiste en "todo objeto representativo de un hecho de interés para el proceso, fácilmente transportable, y que contenga una unidad de información, cualquiera que sea el soporte –

[14] Ley 26.994 del 01/10/2014 por el que se aprueba el Código Civil y Comercial de la Nación (Argentina: BORA, 08/10/2014).
[15] Ley 8.465 del 27/04/1995 por el que se aprueba el Código Procesal Civil y Comercial de la Provincia de Córdoba (Argentina: BOEC, 08/06/2014).
[16] Xavier Abel Lluch, «La impugnación de la prueba electrónica», *Justicia: revista de derecho procesal*, n.º 1 (2019): 223.

papel, audiovisual o informático– y la expresión –escrita, sonoro o visual– de dicha información".

A nivel positivo, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, en su anexo define al documento electrónico como la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado[17]. Más recientemente, el Reglamento (UE) 910/2014 sobre identificación electrónica y servicios de confianza para transacciones electrónicas[18] (en adelante Reglamento eIDAS), en su art. 3.35 define al documento electrónico como todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual.

Como vemos, el concepto de documento electrónico abarca un sinnúmero de supuestos, desde documentos de texto en diversos formatos hasta documentos de cálculo, imágenes, videos, etc.

El ordenamiento argentino, por su parte, utiliza una concepción amplia de documento. El legislador, reconociendo la pérdida de relevancia del soporte físico frente al soporte electrónico, mediante la sanción del nuevo CCCN reconoció expresamente a los documentos electrónicos como una especie más de documento. Así, el art. 286 CCCN establece que la expresión escrita puede tener lugar por instrumentos públicos o por instrumentos particulares, estos últimos firmados o no firmados (salvo que sea requerida determinada instrumentación), y finalmente aclara que estos pueden hacerse constar en cualquier soporte, "siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos".

La normativa hace una diferenciación entre documento electrónico y digital, por cuanto existe entre ellas una relación género-especie. Conforme la Ley de Firma Digital[19] (en adelante LFD) el documento digital es entendido como la representación digital de actos o hechos, sin importar el soporte utilizado tanto para su fijación, almacenamiento o

[17] Idéntica definición contenía la Ley 59/2003 de Firma Digital, hoy derogada.
[18] Reglamento (UE) n ° 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 (Unión Europea: Diario Oficial de la Unión Europea, núm. 257, 28/08/2014).
[19] Ley 25.506 del 14/11/2001 de Firma Digital, (Argentina: BORA, 11/12/2001).

archivo, y que satisface el requerimiento de escritura (art. 6 LFD). Así, mientras el concepto de documento electrónico es amplio y comprende numerosos conceptos asimilables, el documento digital que es una forma específica de este, concebido como una expresión de la voluntad, que tiene como fin establecer relaciones jurídicas, y con idéntica valor que el firmado ológrafamente[20].

Como podemos observar, en ambas legislaciones se reconoce un concepto amplio de documento electrónico. Por ello debemos entenderlo como un concepto que engloba no solo los instrumentos públicos y privados (en su carácter declarativo), sino también a otros objetos no escritos ni firmados, como puede ser una fotografía, un video, etc., (carácter representativo)[21]. Así, comprendiendo a los documentos electrónicos como un tipo de documento en el que varía el soporte, ellos podrán contener tanto una declaración como ser simplemente representativos de uno o varios hechos.

2.3. La problemática en la determinación de autoría e integridad

De la misma manera que resaltamos al momento de reseñar los desafíos de la prueba electrónica, dada la relación género especie que existe entre esta y el documento electrónico, muchos de sus inconvenientes se evidencian en los documentos electrónicos.

En relación con la fuerza probatoria de los documentos electrónicos debemos destacar tres aspectos esenciales: autoría, integridad y licitud. En estos ejes se asienta el denominado *test* de admisibilidad que hemos mencionado al tratar la prueba electrónica, necesario para que esta despliegue toda su eficacia probatoria, y al que hacen referencia numerosos autores tales como Abel Lluch[22] y Urbano Castrillo[23]. Ahora nos centraremos en los dos primeros, esto es, la autoría e integridad, descartando por el momento el tratamiento de la licitud, por cuanto la problemática de la obtención de la prueba con respeto a los derechos y libertades fundamentales excede de este trabajo.

Sobre el primer eje, cuando hablamos de autoría o autenticidad[24] nos referimos a la determinación del autor del documento electrónico, esto es, a quien este se le atribuye. Conforme explica Delgado Martín, la autenticidad es “la propiedad o característica

[20] Bielli y Ordoñez, *La prueba electrónica: teoría y práctica*, 57-58.
[21] Jorge L. Kielmanovich, *Teoría de la prueba y medios probatorios*, 4ª ed. (Santa Fe: Rubinzal Culzoni, 2010), 381-82.
[22] Abel Lluch, «Prueba electrónica», 78.
[23] Eduardo de Urbano Castrillo, *La valoración de la prueba electrónica* (Valencia: Tirant lo Blanch, 2009), 51.
[24] Usaremos estos términos de manera indistinta.

consistente en que se garantiza la autenticidad del origen de los datos, es decir, se garantiza la fuente de la que proceden los datos". Del mismo modo el anexo de la Ley 18/2011[25] la define como la "propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos".

El problema sobre este punto radica en que muchas veces no es posible determinar la autoría del documento electrónico. A diferencia del entorno físico, en donde podemos asegurarnos con mayor facilidad de la identidad de una persona (requiriéndole una identificación); y de la atribución de autoría mediante su firma manuscrita (mediante la propia presencia), en el entorno virtual nos enfrentamos con diversas barreras que dificultan la identificación de las partes intervinientes. Aquí adquiere relevancia la firma electrónica, que veremos más adelante, así como los sistemas que identifican y autentican los usuarios intervinientes, tema que trataremos en el apartado de identidad en la *blockchain*.

En definitiva, la falta de determinación de la autoría o la presencia de dudas sobre ella, afectan la eficacia probatoria de los documentos electrónicos. Así, el Tribunal Supremo[26] ha afirmado que la falta de autenticidad de un documento privado hará que este carezca de eficacia probatoria, mientras que, de probarse tal extremo, el documento será idóneo para probar por sí mismo. No obstante, no deben confundirse ambos conceptos por cuanto la autenticidad se refiere a la concordancia entre el autor aparente y el autor real, mientras que la eficacia probatoria refiere al valor atribuido al contenido de dicho documento. Así declaración de inautenticidad privará al documento de aptitud probatoria, mientras que frente a su impugnación o no reconocimiento tal aptitud deberá ser valorada en conjunto con el resto de las pruebas[27].

La integridad, por su parte, se refiere a que el documento no ha sufrido alteraciones desde el momento de su creación hasta su incorporación al proceso judicial, por lo que se mantiene exactamente igual al originalmente creado. El anexo de la Ley 18/2011 la define como la "propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada". En este punto la falta de

[25] Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (España: BOE, núm. 160, 06/07/2011).
[26] Sentencia del Tribunal Supremo (Sala de lo Civil) 558/2011, de 15 de julio de 2011, ponente Ilmo. Sr. Jesús Eugenio Corbal Fernández, f.j. 5°.
[27] Sentencia del Tribunal Supremo (Sala de lo Civil) 1109/2002, de 25 de noviembre de 2002, ponente Ilmo. Sr. Jesús Eugenio Corbal Fernández, f.j. 5°.

determinación de la integridad de un determinado documento afecta la eficacia probatoria al documento en cuestión.

La relativa facilidad con la que se manipulan los documentos electrónicos es de público conocimiento. Ya la misma jurisprudencia ha afirmado, al tratar controversias con relación a los sistemas de comunicación como WhatsApp o WeChat, que "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"[28], cuestión que es aplicable a la mayoría de los documentos electrónicos. En tal sentido, Abel Lluch[29] resalta la necesidad de contar con instrumentos mediante los cuales se pueda garantizar la integridad, confiabilidad y autenticidad del documento electrónico. El autor menciona medidas tales como la debida configuración e identificación del software empleado, la identificación de los usuarios y los mecanismos de control sobre la transmisión de información para que pueda ser determinado con mayor facilidad los cambios producidos dentro y fuera del sistema. En los apartados subsiguientes analizaremos si la *blockchain* puede satisfacer tal necesidad.

2.4. Regulación legal

En el ordenamiento jurídico español, la LEC parece regular de forma separada el documento y el documento electrónico. Se sostiene que en un principio el legislador procuró no forzar el concepto de documento tradicional por escrito, creando una nueva categoría especialmente dispuesta para los medios de prueba audiovisuales y para la prueba por instrumentos informáticos a través del art. 299.2 LEC, que pasan a constituirse como medios de prueba autónomos frente a los documentos públicos y privados[30].

Así pues, según la LEC podríamos considerar documento electrónico a las imágenes, palabras o sonidos grabados en formato digital y los datos, palabras, cifras y operaciones matemáticas archivadas en instrumentos técnicos, almacenados en formato digital o electrónico, siguiendo el tenor literal de su art. 299.2[31]. Por ello, los documentos electrónicos serían regulados como medio de prueba autónomo atendiendo al citado artículo, en concordancia con lo dispuesto en los arts. 382 a 384 LEC. Queda demostrada

[28] Sentencia del Tribunal Supremo (Sala de lo Penal) 754/2015, de 27 de noviembre de 2015, ponente Ilmo. Sr. Julián Artemio Sánchez Melgar, f.j. 3°.
[29] Abel Lluch, «Prueba electrónica», 40.
[30] Abel Lluch, 66.
[31] Delgado Martín, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 237.

entonces la intención del legislador español de mantener separados los documentos que considera tradicionales (en soporte papel) de aquellos en soporte electrónico, en los términos de los artículos citados.

Abel Lluch critica tal diferenciación y expone que lo ideal hubiera sido adoptar un concepto amplio de documento y que ingresaran al proceso siguiendo la aportación de los documentos y de los demás medios de prueba, según corresponda[32].

En la misma línea, y reiterando lo expresado al momento de hablar de prueba electrónica, Sanchís Crespo sostiene que en los medios de prueba documentales (en el que se encuentra el documento electrónico) deberá seguirse principalmente lo referido a la prueba documental, pues lo único que varía es el soporte (tradicional versus electrónico). Además de que su regulación es mucho más completa y precisa, a diferencia de las lagunas en la regulación de los medios de prueba de los arts. 382 a 384 LEC[33].

Por todo ello, y conforme lo que sostiene la autora puede considerarse incluido dentro de lo considerado un documento tanto a los electrónicos como a los en soporte papel referidos a un hecho controvertido[34].

Así, siguiendo este lineamiento, este tipo de documentos deberán aportarse, en caso de considerarse fundamentales, con la demanda o su contestación (art. 265.1.1 LEC), aplicándose estrictas reglas de preclusión (art. 269 LEC)[35].

Abona esta tesis el hecho que tal artificiosa distinción prevista por la LEC se ha ido diluyendo con el dictado de normas sucesivas, que han entremezclado las nociones que el legislador quiso separar. Tanto reformas a la misma LEC[36] como el dictado de otras normas[37] han contribuido a sostener una concepción amplia de la prueba documental.

A nivel jurisprudencial podemos destacar la reciente y ya citada Sentencia del Tribunal Supremo 706/2020, que entre varias cosas analiza en el marco de una controversia referida a la consideración del correo electrónico como prueba documental,

[32] Abel Lluch, «Prueba electrónica», 66.
[33] Sanchís Crespo, «La prueba en soporte electrónico», 726.
[34] Sanchís Crespo, 725.
[35] Abel Lluch, «Prueba electrónica», 32.
[36] En este sentido se resaltan los arts. 326.3, 327, 333 y 812.1.1 de la LEC.
[37] Podemos destacar el art. 24.2 de la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, que establece que el soporte electrónico de un contrato celebrado vía electrónica será admisible en juicio como prueba documental.

si la regulación establecida por los arts. 299.2 y 382 a 384 de la LEC implica un medio de prueba autónomo o si dichos artículos deben ponerse en relación con la prueba documental. En este caso el Tribunal Supremo concluye que los referidos artículos solo enumeran instrumentos y actividades orientados a resolver particularidades de estas fuentes de prueba, pero que los medios de prueba en sí son aquellos previstos por el art. 299.1 LEC, que tiene el carácter de *númerus clausus*. De esta manera no debe perderse de vista su naturaleza de prueba documental, aunque efectuando las adaptaciones necesarias conforme sus particularidades. Esta resolución viene a superar otros entendimientos por el que la prueba electrónica, ofrecida por ejemplo como capturas de pantalla, era entendida como un tipo de prueba ajeno a la documental, y regida por los arts. 382.1 y 382.3 de la LEC[38].

Por todo lo expuesto, coincidimos con esta última idea, por lo que para el desarrollo del presente trabajo consideraremos que el tratamiento de la documental electrónica (como fuente de prueba), debe seguir el cauce del medio probatorio documental.

Desde la óptica del ordenamiento argentino, en lo que a la regulación del documento atañe, también tenemos tanto normas emanadas del CCCN como por el CPCC de la Provincia de Córdoba. Ya referimos que la noción de documento electrónico se encuadra como una especie del género documento. De esta forma, el CCCN, en su Sección 3ª sobre forma y prueba del acto jurídico establece que la expresión escrita puede ser por instrumento público o particular, estos últimos firmados (en cuyo caso se denominan instrumentos privados) o no firmados, y que pueden "constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos".

A su vez, el art. 287 CCCN establece que los instrumentos particulares no firmados "comprende todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información".

Respecto a los primeros, considerados documentos digitales, al establecerse que estos satisfacen el requerimiento de la escritura, la ley expresamente lo concibe

[38] Sentencia de la Audiencia Provincial de Barcelona (Secc. 9) 224/2017, de 08 de marzo de 2017, ponente Ilmo. Sr. José Maria Torras Coll, f.j. 2°; entre otras resoluciones.

análogamente al documento en formato papel y, por consiguiente, se le aplica toda la regulación legal que aplicable a dicho formato[39].

La jurisprudencia no ha efectuado ningún reparo a la noción amplia de documento electrónico. Se reconoce que las nuevas tecnologías dan lugar a nuevas realidades documentales y se ha llegado a considerar incluso al recorrido virtual provisto por Google, denominado *Street View*, como documental, considerando que en estos casos estamos frente a un documento "grande", conformado por la unión de muchos otros documentos (cada una de las imágenes)[40].

Todo ello tiene incidencia en materia procesal, por cuanto el medio de prueba aplicable a los documentos electrónicos será el documental. Así, en el caso de Córdoba, ante pruebas admisibles que no tuvieren un cauce específico, y a tenor del art. 202 CPCC, un documento electrónico seguirá el medio de prueba documental.

2.4.1. Eficacia probatoria de los documentos electrónicos

Ya definido el documento electrónico y determinada la normativa que le resulta aplicable, ahora nos centráremos en aquellas normas que tienen incidencia específica en su eficacia probatoria.

En primer lugar, el Reglamento eIDAS establece que no deben denegarse efectos jurídicos ni la admisibilidad como prueba en procedimientos judiciales al documento electrónico por la sola circunstancia de ser electrónico (art. 46). En esta línea, el ordenamiento español establece que los documentos electrónicos (privados en nuestro caso) tendrán el valor y la eficacia jurídica correspondiente a su naturaleza, según la legislación que les sea aplicable (art. 3 de la Ley 6/2020[41], en adelante LSEC).

En concordancia con el Reglamento mencionado, en al ámbito civil la fuerza probatoria de los documentos privados se encuentra regulada en el art. 326 LEC (recientemente modificado con la sanción de la LSEC), que estará dada en primera medida por la actuación procesal de las partes. Por un lado, si los documentos no son impugnados harán plena prueba en el proceso y su eficacia será equivalente a un

[39] Bielli y Ordoñez, *La prueba electrónica: teoría y práctica*, 58.
[40] Sentencia de la Cámara de Apelaciones en lo Civil y Comercial de Morón (Sala II) 67/2019, de 23 de abril de 2019, en autos "Fleitas, Olga Esther c. Empresa del Oeste SA de Transporte y otros s/ daños y perj. autom. c/les. o muerte (exc. Estado)".
[41] Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (España: BOE, núm. 298, 12/11/2020).

documento público (art. 326.1 LEC)[42]. Y por el otro, ante la existencia de una impugnación de la autenticidad, integridad, fecha, hora u otras características del documento electrónico, el trámite a seguir dependerá de si el documento es acreditado con un servicio de confianza cualificado o no cualificado. En el primer caso existe una presunción de autenticidad e integridad del documento electrónico privado en el que intervino un servicio de confianza cualificado, por lo que en caso de ser impugnado será a cargo de quien impugna realizar las comprobaciones necesarias (art. 236.4 LEC). Y en el segundo, en caso de que haya intervenido en el documento electrónico un servicio electrónico de confianza no cualificado, su autenticidad e integridad deberá ser probada por los medios probatorios que se estimen útiles o pertinentes (art. 326.2 por remisión del art. 326.3 LEC).

En el caso del ordenamiento argentino, dada la específica equiparación del documento electrónico con los documentos en general, deberemos estar a las pautas generales sobre la prueba documental que establecen los códigos procesales, aunque con algunas particularidades.

Al igual que en el ordenamiento español, la eficacia probatoria dependerá en primer lugar de la actitud procesal de las partes. Para que despliegue todo su potencial deberá ser reconocido por la persona contra quien se presenten o que el tribunal los declare así (art. 248 CPCC). En cambio, frente a una impugnación, dependerá del tipo de documento ante el que nos encontremos y los medios de prueba propuestos.

En el caso de documentos con firma digital su validez goza de una presunción, conforme se verá a continuación. En cambio, los documentos con firma electrónica tendrán distinta consideración según la postura doctrinaria adoptada, motivo de un breve análisis en el epígrafe siguiente.

Finalmente, en caso del resto de los documentos electrónicos no firmados, el art. 319 CCCN dispone que su valor probatorio será apreciado por el juez teniendo en cuenta diversas pautas, entre las que destaca los usos y prácticas del tráfico, las relaciones

[42] Tal conclusión no podría ser derivada sobre un documento electrónico, si consideráramos que este se rige por las reglas de los arts. 382.3 y 384.3 LEC. Ello porque estos artículos remiten a las reglas de la sana crítica, aún frente a la falta de impugnación, lo que colocaría este tipo de prueba en inferioridad a la de tipo documental.

precedentes, la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen, entre otros.

2.5. La firma electrónica

2.5.1. Concepto y regulación

Antes de definir lo que se entiende como firma electrónica cabe efectuar unas aclaraciones. Tal como sostiene Abel Lluch, no debemos confundir firma electrónica con algún tipo de fuente o medio de prueba, sino que es un instrumento tecnológico que permite garantizar en los documentos electrónicos su autoría e integridad. De esta manera, al referirse a la eficacia probatoria de este tipo de documentos no hay que ceñirse a la firma electrónica en sí sino al documento que posee tal firma, que al fin y al cabo es el medio de prueba[43].

Ahora bien, volviendo a la conceptualización, la firma electrónica es "el conjunto de datos en forma electrónica, consignados junto a otros o asociados entre ellos, que pueden ser utilizados como medio de identificación del firmante"[44].

El uso de la firma electrónica, aunque con las diferencias que a continuación veremos, permite conocer quien firmó el documento, esto es su autoría, y también permite verificar que no se han efectuado alteraciones desde la fecha de su firma, esto es, su integridad.

En el ordenamiento jurídico español, en lo que atañe a la regulación de la firma electrónica, hasta hace un tiempo convivían el Reglamento eIDAS, y Ley de Firma Electrónica[45] (en adelante LFE). Debido a algunas incongruencias entre ambas regulaciones, esta última tenía partes derogadas dada la aplicación directa del reglamento. Sin embargo, recientemente mediante la sanción de la LSEC se derogó completamente la LFE con el objetivo de armonizar la legislación con el Reglamento eIDAS.

En primer lugar, este reglamento reconoce tres categorías de firma electrónica para las personas físicas:

1. Firma electrónica simple: son los datos en formato electrónico adjuntos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para

[43] Abel Lluch, «Prueba electrónica», 177.
[44] Abel Lluch, 26.
[45] Ley 59/2003, de 19 de diciembre, de firma electrónica, hoy derogada.

firmar (art. 3.10). Este tipo de firma es la más utilizada diariamente ya que por ejemplo supone la colocación de nombre y apellido en el final de un correo electrónico, un PIN introducido en el cajero bancario, etc.

2. Firma electrónica avanzada: es la firma electrónica que está vinculada de manera única al firmante, permitiendo su identificación y creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, que posee un alto nivel de confianza y está bajo su control exclusivo. Asimismo, al estar vinculada con los datos firmados permite detectar cualquier modificación ulterior (art 3.11 y remisión al art. 26).

3. Firma electrónica cualificada: es la firma electrónica avanzada creada mediante un dispositivo cualificado de creación de firmas electrónicas y basado en un certificado cualificado de firma electrónica (art. 3.12).

En segundo lugar, para el caso de las personas jurídicas, el Reglamento eIDAS establece el sello electrónico. De forma similar a la firma electrónica, se consignan tres categorías:

1. Sello electrónico: son los datos en formato electrónico adjuntos a otros datos en formato electrónico, o asociados de manera lógica con ellos, que garantizan el origen y la integridad de estos últimos (art. 3.25).

2. Sello electrónico avanzado: es el sello electrónico que está vinculado de manera única al creador del sello, permitiendo su identificación y creada utilizando datos de creación del sello electrónico que el creador del sello puede utilizar, que posee un alto nivel de confianza y está bajo su control exclusivo. Asimismo, al estar vinculada con los datos permite detectar cualquier modificación ulterior (art. 36).

3. Sello electrónico cualificado: es el sello electrónico avanzado creado mediante un dispositivo cualificado de creación de sellos electrónicos y basado en un certificado cualificado de sello electrónico (art. 3.27).

Siendo esto así, y centrándonos ahora en la legislación argentina, cabe aclarar que la terminología utilizada difiere en parte de la empleada en España. Para entender la diferencia, y siguiendo a Chomczyk[46], en el mundo del derecho se habla de firma

[46] Andrés Chomczyk, "Preguntas Frecuentes sobre Legislación Argentina de Firma Digital y Electrónica", *Signatura Blog*, 22 de mayo de 2020, https://blog.signatura.co/preguntas-frecuentes-sobre-legislación-argentina-de-firma-digital-y-electrónica-c6181ea3e865 (consultada el 05/05/2021).

electrónica mientras que en la informática lo es de firmas digitales, pero que a pesar de ello el legislador argentino confundió ambos conceptos (jurídico y técnico). En esta línea, se estableció la firma electrónica como el género y la digital como una especie.

Se entiende por firma digital "una cantidad determinada de algoritmos matemáticos (que se genera a través de un certificado digital emitido por una autoridad certificante licenciada por un órgano público) y que fue creada utilizando para ello (…) un método de cifrado denominado criptografía asimétrica"[47].

Son diversas las normas que regulan la firma digital en Argentina[48], que parten de la principal que es la LFD. Según el art. 2 de la referida normativa, la firma digital es el resultado de aplicar a un documento digital un determinado procedimiento matemático, a través de información que únicamente conoce el firmante y que se encuentra bajo su control absoluto. Esta firma debe poder ser verificada por terceros y permitir determinar la autoría e integridad del documento.

Por su lado, la firma electrónica se encuentra regulada en el art. 5 de la LFD, y es entendida como el conjunto de datos electrónicos que están integrados, ligados o asociados de una manera lógica a otros datos electrónicos, y que usa el signatario como medio de identificación, pero que no reúne todos los requisitos para ser considerado firma digital.

Respecto a la firma digital de las personas jurídicas, en principio solo puede realizarlo el representante que actúa en representación de ella. Así, el certificado de firma digital deberá tramitarlo una persona física en representación de la persona jurídica, y que podrá firmar en su representación. Sin embargo, esta opción en la práctica no es muy utilizada ya que en las numerosas reformas se derogaron los llamados sellos de competencia que permitían asociar un atributo de su titular (por ejemplo, su rol de representante), por lo que hoy en día la firma por parte del representante necesita ir acompañada "por fuera del sistema" de aquella documentación que justifica tal carácter[49].

[47] Gastón Enrique Bielli y Carlos Jonathan Ordoñez, *Contratos electrónicos: teoría general y cuestiones procesales*, vol. I (Buenos Aires: La Ley, 2020), 34.
[48] Ley de Firma Digital 25.506, Decreto N.º 182/19, Decreto N.º 892/17, entre otras. Portal Argentina, "Normativa de Firma Digital", https://www.argentina.gob.ar/firmadigital/normativa (consultada el 01/05/2021).
[49] Fernando Rey, «La firma digital en las empresas argentinas», en *Fintech: aspectos legales*, comp. Santiago J. Mora y Pablo A. Palazzi (Buenos Aires: Pablo Andrés Palazzi, 2019), 175-88.

En base a todo lo expuesto, con relación a la regulación argentina, podemos afirmar que los documentos electrónicos pueden ser de tres clases: los que tienen firma digital en los términos del art. 2 LFD; los que tienen firma electrónica en los términos del art. 5 LFD; y los que carecen de firma en los términos del art. 287 CCCN[50].

2.5.2. Eficacia probatoria de cada clase de firma

La eficacia probatoria del documento con firma electrónica también está regulada en el Reglamento eIDAS, complementado mediante la LSEC. Este establece, al igual que lo hace con el documento electrónico, que no deben negarse efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el solo hecho de serlo o porque no cumple los requisitos establecidos para la firma electrónica cualificada (art. 25.1). También asimila la firma electrónica cualificada a la firma manuscrita en cuanto a sus efectos jurídicos (art. 25.2). De esta manera si bien los tres tipos de firma tendrán valor probatorio, este será mayor en caso de la firma avanzada, dado los requerimientos que la ley impone y mucho mayor aún en la cualificada, que será la más confiable y que es equiparada a la firma manuscrita.

A diferencia con lo que establecía la derogada LFE, ahora el reglamento tan solo se limita a establecer que la firma electrónica cualificada equivale a la manuscrita. Surgen dudas entonces sobre si existe presunción de integridad y autenticidad en el caso de un documento con firma electrónica. Si bien las condiciones impuestas a la firma avanzada y cualificada tienden a garantizar la identidad e integridad del documento, no se establece ninguna presunción al respecto, sino tal solo en los casos que interviene un servicio de confianza cualificado.

De esta manera, la eficacia probatoria dependerá de la intervención de un servicio de confianza y la existencia de una eventual impugnación. En este último supuesto, se seguirá lo prescripto por el art. 326 LEC, que según el caso impondrá la carga de la prueba a una u otra parte. Así, si el documento fue firmado mediante un servicio de confianza cualificado, la carga de la prueba estará en cabeza de quien formuló la impugnación, mientras que, ante un documento en el que no intervino tal servicio, la carga de la prueba recaerá sobre quien presentó dicho documento.

[50] Eduardo Molina Quiroga, «La prueba en medios digitales», *Micro Juris*, (28 de octubre de 2013), 18. En el mismo sentido adhieren Bielli y Ordóñez.

En cuanto al sello electrónico, y al igual que con la firma electrónica, el Reglamento establece que no se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a un sello electrónico por el mero hecho de ser electrónico o por no cumplir los requisitos del sello electrónico cualificado (art. 35.1). Un aspecto interesante en la regulación es que se establece que el sello electrónico cualificado gozará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado (art. 35.2).

En Argentina, la normativa establece que la firma digital queda equiparada a la firma ológrafa[51]. La ley incluso establece una presunción de integridad a favor del titular del certificado digital (art. 7 LDF), y una presunción de autenticidad cuando el procedimiento de verificación aplicado a un documento de como resultado verdadero (art. 8 LFD), ambos salvo prueba en contrario. La consecuencia práctica de esta presunción es que invierte la carga de prueba, que pesará sobre quien alegare la falta de autenticidad o integridad del documento.

En el caso de la firma electrónica, la LFD no establece ningún efecto jurídico en particular. Si bien hasta hace un tiempo, el derogado decreto 2628/2002 consideraba que los documentos firmados electrónicamente satisfacían el requisito de la firma, su reemplazo por parte de la nueva reglamentación eliminó tal referencia. Asimismo, con la reforma al art. 288 CCCN, este considera cumplido el requisito de la firma cuando se utiliza firma digital "que asegure indubitablemente la autoría e integridad del instrumento", sin mencionar a la firma electrónica.

Todo ello supuso para muchos doctrinarios una modificación en cuanto al valor de la firma electrónica prevista en la LFD, ya que parecería ser que niega su validez[52]. Respecto a tal entendimiento no existen aún resoluciones judiciales de tribunales de máxima instancia, existiendo hasta el momento como referencia unos pocos fallos de primera instancia que no reconocen a la firma electrónica como firma. En tales

[51] El art. 3 LFD establece que "cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital"; en idéntico sentido el art. 288 CCCN establece que, en los documentos electrónicos, el requisito de la firma se cumple si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento.

[52] Para esta tesis, denominada restrictiva, el CCCN establece que el requisito de la firma en el caso de los documentos electrónicos, solo queda satisfecho si se usa una firma digital que asegure la autoría e integridad de dicho documento. Así, los documentos con "firma electrónica", al no ser esta estimada como una firma serían considerados instrumentos particulares no firmados en los términos del art. 287 CCCN. Horario R. Granero, «El expediente digital y la firma digital», en *Tratado de derecho procesal electrónico*, dir. Carlos Enrique Camps, 2ª ed. (Buenos Aires: Abeledo Perrot, 2019), 502-3.

resoluciones se afirma que un documento signado con firma electrónica solo será considerado como instrumento particular no firmado constituyendo un principio de prueba por escrito, al menos en el ámbito de un proceso preparativo de vía ejecutiva[53].

Sin embargo, sin entrar en tal discusión, entendemos que, a pesar de la falta de una referencia específica, del análisis armónico de la normativa vigente, surge que las reformas introducidas complementan y no derogan la LFD, por lo que la firma electrónica debe ser considerada una firma y, por ende, los documentos así firmados serán considerados instrumentos privados[54]. Asimismo, existen en el ordenamiento leyes en materias específicas que reafirman la validez de la firma electrónica, sobre todo en el ámbito financiero y de la Administración Pública[55].

Por ello, sostenemos aquella postura que afirma que los documentos signados con firma electrónica se consideran firmados, aunque puede admitirse que estos tienen una eficacia probatoria disminuida. En este caso adquirirá relevancia la actitud procesal de las partes: en caso de ser reconocido el documento adquirirá plena eficacia; aunque en caso de ser desconocido su autoría deberá ser probada por otros medios.

[53] Sentencia del Juzgado Nacional de 1° Instancia en lo Comercial Nro. 23, 135/2020, de 14 de febrero de 2020, en autos "Wenance SA c. Gamboa, Sonia Alejandra s/ ejecutivo".
[54] Para acceder a la totalidad de los argumentos que sostienen esta tesitura ver Bielli y Ordoñez, *La prueba electrónica: teoría y práctica*, 86-87.
[55] Por mencionar un ejemplo, de la lectura del Decreto 27/2018 del Poder Ejecutivo Nacional sobre Desburocratización y Simplificación pueden extraerse numeroso supuestos en los que se otorga eficacia como firma a la firma electrónica en el ámbito público y frente a algunos instrumentos financieros, siempre que permita asegurar la autoría e integridad.

III. LA *BLOCKCHAIN*

1. CONCEPTO

Una vez determinadas algunas bases teóricas respecto a ciertos puntos de la prueba y el documento electrónico, para poder abordar la problemática planteada, primero debemos comprender qué es la *blockchain* o cadena de bloques[56].

En cuanto a su concepto, Morales Barroso expresa que la *blockchain* es un registro descentralizado de información, creado con la finalidad de aumentar la confianza entre partes dentro de un negocio. Al respecto expresa que en ella:

> …se utilizan un conjunto de protocolos y técnicas criptográficas, gracias a los cuales los datos de la aplicación y los registros de operación se constituyen como una cadena de bloques de información unidos entre sí de forma descentralizada y pública, almacenándose en unos equipos interconectados a través de una red de ordenadores distribuidos, los nodos, para evitar cualquier punto central de fallo. Los nodos trabajan de forma colaborativa para almacenar, compartir y preservar el registro distribuido, utilizando un algoritmo de consenso para comprobar y garantizar la validez de cada bloque.[57]

Por su parte, en lo que a su definición respecta, Navarro sostiene que:

> Es una base de datos que no es controlada por una persona, sino por un conjunto de pares o nodos con un elemento central basado en la criptografía y con otro elemento esencial que no permite su cambio, es decir, que es inmutable. No existe una personalidad controlante de la red, por lo que el control de esta es conjunto y, por lo tanto, no puede ser coordinada la resolución o la modificación de esta.[58]

Finalmente, otro autor como Ibáñez Jiménez expresa que:

> … es una base de datos distribuida, esto es, descentralizada u operada desde diferentes puntos, servidores o nodos de una red, cuyos fundamentos técnicos se anclan en la llamada tecnología de registros distribuidos (Distributed-Ledger Technology, DLT) …[59]

---

[56] Usaremos ambas palabras indistintamente. Respecto al anglicismo *blockchain*, cabe aclarar que ambos géneros están justificados (la o el *blockchain*) por lo que también se los utilizará indiscriminadamente, https://www.rae.es/observatorio-de-palabras/blockchain (consultada el 24/04/2021).

[57] José Morales Barroso, «¿Qué es blockchain?», en *Criptoderecho. La regulación de Blockchain*, dir. Pablo García Mexía (Madrid: Wolters Kluwer, 2018), 42-43.

[58] Guillermo Navarro, «Blockchain y proceso electrónico», en *Tratado de Derecho Procesal Electrónico*, dir. Carlos Enrique Camps, 2ª ed. (Buenos Aires: Abeledo Perrot, 2019), 794.

[59] Javier Wenceslao Ibáñez Jiménez, «Blockchain y Legal Tech», en *Legal Tech.: la transformación digital de la abogacía*, dir. Moisés Barrio Andrés (Madrid: Wolters Kluwer, 2019), 91.

Se suele enmarcar esta tecnología como una especie dentro del género de los registros distribuidos o *distributed ledger technology* (DLT). La tecnología de DLT se refiere a una base de datos descentralizada, gestionadas por varios participantes y carente de una autoridad central. La *blockchain*, como una especie de esta, adiciona una serie de particularidades tales como el uso de criptografía y el almacenamiento "en bloques" que le da su nombre característico.

Aun así, algunos entienden que *blockchain* y DLT son conceptos idénticos. Sin embargo, en estos casos definen a las DLT como aquella que "permite a los usuarios grabar y almacenar permanente, simultánea y públicamente los datos introducidos en un programa que comparte un colectivo de personas en distintas máquinas telemáticas o servidores informáticos llamados nodos", y en donde "la inserción, introducción o carga de datos en dicho programa y en el propio sistema o red DLT se realiza empleando claves criptográficas[60]. Vemos así que en realidad se está describiendo a la cadena de bloques, y lo único que varía es la cuestión terminológica.

A pesar de las diferencias en cuanto al término empleado, dada la finalidad de la presente investigación, no consideramos útil ni esclarecedor seguir ahondando dicha cuestión, dejando simplemente expuesta la diferencia, y adoptando el criterio que entiende la cadena de bloques como una especie dentro de las DLT.

Volviendo a la cadena de bloques, tenemos que la *blockchain* actúa como una base de datos con especiales características, nacida con la finalidad de realizar transacciones entre terceros sin depender de un intermediario. Funciona de manera descentralizada mediante un protocolo para establecer consenso entre terceros desconocidos sobre la información a registrar. Toda la información se va almacenando en "bloques" concatenados entre sí, lo que le da su nombre característico, y lo que sumado a la utilización de funciones criptográficas garantiza la inmutabilidad de los registros y permite determinar con facilidad cualquier intento de manipulación. Así, si se intenta modificar información anterior, se produce una ruptura en la cadena, que es detectada por el resto de los participantes que poseen copias idénticas de toda la información.

Por todo lo anterior, podemos afirmar a nuestro criterio que la *blockchain* es una base de datos construida en torno a un conjunto de protocolos que definen la manera en

[60] Javier Wenceslao Ibáñez Jiménez, *Blockchain: Primeras cuestiones en el ordenamiento español* (Madrid: Dykinson, 2018), 15.

que sus participantes se comunican, y la forma en que la información es registrada. Es distribuida, ya que los datos son almacenados en cada una de las entidades que conforman la red, denominadas nodos, que poseen una réplica exacta de toda la información. Es descentralizada, ya que no existe una única autoridad central que regule el funcionamiento ni el modo de registrar la información, sino que ello se hace con base a un mecanismo de consenso. Es inmutable, ya que su funcionamiento basado en criptografía asegura que los datos en ella registrados no puedan ser modificados sin que se detecte tal alteración. Y es transparente, ya que facilita la trazabilidad de todas las operaciones efectuadas.

Conviene desde ya dejar sentado que en el presente trabajo también aludiremos a la *blockchain* como la "tecnología" o "red"[61] a los fines de evitar constantes reiteraciones del término.

Asimismo, debemos clarificar otro concepto al que haremos mucha referencia y que forma parte de la estructura de la *blockchain*: el *hash*, también llamado digesto criptográfico. Este es un algoritmo matemático que permite, a partir de cualquier conjunto de datos (como ser un documento electrónico), generar una serie de caracteres alfanuméricos de tamaño fijo. Es decir, no importa si estamos frente a un documento electrónico de gran tamaño o a uno con tan solo un párrafo, el código *hash* que obtendremos en cada caso tendrá un número fijo de caracteres. El código obtenido actúa como si fuera una huella digital de un documento electrónico, ya que frente a cada conjunto de datos distinto se generará un *hash* diferente. De esta manera, si se efectúa cualquier modificación por más mínima que sea al conjunto de datos original, el *hash* que se obtenga será totalmente diferente, lo que permitirá conocer fácilmente si el contenido ha sido alterado. Cabe destacar que el *hash* actúa unilateralmente, esto es que de un documento podemos obtenerlo, pero si queremos reconstruir el contenido de un documento electrónico a partir de un hash, ello no resulta posible, al menos en el estado actual de la tecnología. Finalmente, existen diversos algoritmos para obtener el *hash* a partir de un conjunto de datos, siendo uno de los más comunes el SHA256[62].

[61] Ya que es una tecnología que utiliza diversos procesos técnicos y también implica una red distribuida de nodos.

[62] Este es uno de los algoritmos más seguros, que trabaja con un conjunto de 256 bits que prácticamente mitiga el riesgo de colisión, esto es, la probabilidad de que de dos entradas distintas se obtenga el mismo *hash*. Los *hashes* se utilizan en numerosos ámbitos e incluso cualquier persona mediante un simple programa informático (por ejemplo 7-Zip) puede calcularlo sobre un documento que posea en su computadora.

2. ANTECEDENTES HISTÓRICOS

Esta tecnología se hizo sumamente conocida entre 2008 y 2009 con el nacimiento de la criptomoneda Bitcoin, cuyo desarrollo se estructura en base a la tecnología de cadena de bloques. Fue a partir de ese momento que el potencial de esta tecnología que subyacía al Bitcoin comenzó a ser explotado. No obstante, para descubrir a su génesis debemos remontarnos tiempo atrás.

Ya en 1991, los investigadores Stuart Haber y W. Scott Stornetta[63], haciendo eco de la relativa facilidad con la que los documentos electrónicos podían modificarse, idearon el concepto de marca de tiempo para establecer que no se efectuaron modificaciones desde que el documento se creó o se modificó por última vez, todo a través de un procedimiento computacional que evita también la falsificación de dicha marca. Este procedimiento implicaba la utilización de un sistema de confianza distribuida entre varios usuarios. Al año siguiente, en 1992, incorporaron a su idea la estructura denominada "árbol de merkle", que permitió alcanzar un sistema más eficiente.

Otro antecedente puede encontrarse en un artículo publicado en 1996, en el que el investigador Ross Anderson[64] propuso un sistema de almacenamiento de archivos a través de la cooperación de un gran número de sistemas unidos por un protocolo común, sin ninguna autoridad centralizada que pudiera ser coaccionada o corrompida. Así, a través de un sistema distribuido se proporcionaría resistencia contra errores y ataques, y ningún archivo podría ser borrado.

En 1997, Nick Szabo[65], consciente del problema de la confianza entre personas en una red y la delegación en terceros de confianza, ideó el reemplazo de estos intermediarios a través de un protocolo que pudiera cargar transacciones de manera segura e imparcial, que actuaría de manera automatizada sin el control específico de un tercero.

[63] Stuart Haber y W. Scott Stornetta, «How to time-stamp a digital document», *Journal of Cryptology* 3 (enero de 1991), *passim*, https://doi.org/10.1007/BF00196791.
[64] Ross J. Anderson, «The Eternity Service», *Cambridge University Computer Laboratory*, 1996, *passim*.
[65] Nick Szabo, "The God Protocols", *Satoshi Nakamoto Institute,* 1997, https://nakamotoinstitute.org/the-god-protocols/ (consultada el 15/05/2021).

Posteriormente, en 2002 David Mazières y Dennis Shasha[66] demostraron como implementar un sistema de archivos confiable en un servidor que no sea de confianza, con base en un protocolo en el que se utilizan firmas digitales y cifrado.

Finalmente, en el año 2008 una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto[67] publicó un protocolo para un sistema de dinero electrónico sin intermediarios. Este sistema supuso una solución al problema del doble gasto[68] a través de una red *peer to peer* (usuario a usuario) que va colocando sellos de tiempo en todas las transacciones mediante un *hash* inserto en una cadena continua, que forma un registro que no puede ser modificado. La seguridad del protocolo está basada en un mecanismo denominado *proof of work* (prueba de trabajo) que registra el historial de transacciones y hace impráctico y antieconómico un ataque informático.

Fue este último hito que dio origen a la criptomoneda denominada Bitcoin e hizo que la tecnología que garantizaba su buen funcionamiento, la *blockchain,* comenzara a hacerse conocida. A partir de ese momento, se la consideró como una nueva revolución tecnológica y su uso se extendió a los más variados casos, conforme veremos más adelante.

3. FUNCIONAMIENTO DE LA CADENA DE BLOQUES

Sin ánimos de efectuar una extensa explicación, que en rigor debería incluir numerosos aspectos técnicos, brindaremos una breve introducción al funcionamiento de la *blockchain*, cuyo entendimiento básico se muestra como necesario para entender los efectos de esta tecnología en el tráfico jurídico.

Esta tecnología implica un conjunto de protocolos y técnicas criptográficas por medio de los cuales todas aquellas transacciones se registran en cadenas de bloques unidas entre sí, almacenados de manera distribuida entre diversos ordenadores (denominados nodos). Estos nodos se encargan del almacenamiento, distribución y preservación de los

[66] David Mazières y Dennis Shasha, «Building secure file systems out of byzantine storage», en *Proceedings of the twenty-first annual symposium on Principles of distributed computing - PODC '02* (New York, 2002), 108-17, https://doi.org/10.1145/571825.571840.
[67] Satoshi Nakamoto, "Bitcoin: un sistema de efectivo electrónico usuario-a-usuario", trad. por Ángel León, 2008, https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf (consultada el 20/04/2021).
[68] El problema del doble gasto implica que un mismo activo digital pueda gastarse más de una vez. Así, un usuario −en fraude a la red− realiza transacciones en las que utiliza los mismos criptoactivos más de una vez.

registros, de manera colaborativa. Para incorporar un bloque a la cadena y garantizar su validez se utilizan mecanismos de consenso[69].

Una de las tecnologías subyacentes que hacen a la seguridad es el uso de la criptografía[70], principalmente de la asimétrica, que utiliza claves públicas y privadas. Este tipo de criptografía es el mismo que se utiliza para la firma digital (cualificada en España, o digital en Argentina). Sin entrar en detalles técnicos, podemos decir que la clave pública es la dirección que identifica a un usuario en la cadena de bloques. Está asociada criptográficamente a una clave privada, solo conocida por su propietario, que no se comparte y sirve para descifrar un mensaje enviado utilizando la clave pública. Para ejemplificar, podríamos decir que la clave pública opera como el usuario o email que identifica frente a terceros al emisor de la operación y permite leer la transacción, mientras que la clave privada sería la contraseña que posibilita efectuar dicha transacción. También existen sistemas *multisig*, en los que una clave pública está asociada a varias claves privadas que se requieren para efectuar una transacción.

En cuanto al almacenamiento de los documentos electrónicos, este puede ser dentro de la cadena (*on-chain*) o fuera de ella (*off-chain*). El primer caso implica que la cadena almacena directamente los archivos, sea de manera íntegra o en partes para mayor eficiencia y seguridad[71]. El almacenamiento fuera de la cadena −el caso más común, por cierto− supone que la *blockchain* solo almacena el *hash* de los datos vinculados y no los documentos en sí, que se encuentran almacenados en un soporte por fuera de la cadena. De esta manera los participantes de la red solo podrán ver el *hash,* pero no acceder al documento en sí.

Si bien cada implementación concreta de esta tecnología puede tener sus particularidades, en términos generales todo comienza con una transacción[72]. Esta puede ser desde enviar criptomonedas, registrar una operación en una red empresarial, hacer un sellado de tiempo a un documento, entre numerosos otros casos. En redes que manejen

[69] Morales Barroso, «¿Qué es blockchain?», 43.
[70] La criptografía es el desarrollo de un conjunto de técnicas que, aplicados a un mensaje o archivo, no permiten que sean leídos por aquellos usuarios que no están autorizados.
[71] Este sistema no es muy utilizado ya que replicar los documentos originales en todos los nodos (y no solo un resumen de ellos mediante el hash) lo torna costoso en términos de almacenamiento. Aun así, el servicio es prestado por diversas empresas como como Sia, Storj o Filecoin.
[72] Aquí el término transacción hace referencia a la realizacion de operaciones técnicas sobre la blockchain, lo que no implica en sí la realización de un negocio jurídico. Véase Ibáñez Jiménez, *Blockchain: Primeras cuestiones en el ordenamiento español*, 43.

criptomonedas[73], partiremos de una *wallet* o billetera electrónica[74], donde la transacción comenzará con un mensaje de datos que contendrá la cantidad a enviar y la dirección del destinatario. En caso de otros tipos de redes accederemos según la interfaz dispuesta en cada implementación.

La operación efectuada se envía al resto de los nodos (que son las entidades que conforman la red) para su verificación. Existen varios tipos de nodos: los nodos selladores (o también llamados nodos mineros), que son específicos y tienen como función incorporar los bloques a la cadena mediante un mecanismo de consenso; los nodos validadores, que verifican y validan todos los bloques de la red; los nodos de participación, que almacenan las copias de todas las transacciones de la red; los nodos transaccionales, que pueden enviar transacciones; entre otros, ya que al fin y al cabo el tipo de nodos depende del diseño específico de la red, por lo que pueden existir otras categorías y tener distintas funciones.

Volviendo al funcionamiento, una transacción enviada a la red finalizará con éxito cuando más de la mitad de los nodos la hayan validado, y será en este momento en el que se cree y agregue un bloque por un nodo sellador. Este bloque estará conformado por el *hash* del bloque anterior junto con todas las nuevas transacciones y una marca de tiempo, así como los demás elementos que puedan ser definidos según el protocolo de la red.

Así, las sucesivas operaciones de la red se aglomeran en bloques encadenados al bloque anterior, y así sucesivamente, lo que la dota del carácter de inmutabilidad. Ello hace que los datos anteriores no puedan modificarse, ya que si existe cualquier modificación por más mínima que sea, cambiará el *hash* de todo el bloque y ya no coincidirá con el bloque subsiguiente (recordemos que cada bloque se conforma también con el hash del bloque anterior) y tal anomalía será automáticamente detectada por el resto de los nodos y subsanada, de allí que se mencione la inmutabilidad como una de las características.

[73] Las criptomonedas pueden definirse como aquellos criptoactivos destinados a cumplir las funciones de la moneda, esto es, servir como medio de intercambio, depósito de valor y unidad de cuenta; y cuyo objeto es ser una alternativa a la moneda de curso legal, pero sin respaldo físico ni reconocimiento legal como dinero. Moisés Barrio Andrés, «Concepto y clases de criptoactivos», en *Criptoactivos. Retos y desafíos normativos*, dir. Moisés Barrio Andrés (Madrid: Wolters Kluwer, 2021), 53.

[74] La billetera electrónica es un programa de software o hardware que almacena las llaves públicas y privadas en un dispositivo determinado o en la nube, y que en la mayoría de los casos provee una interfaz gráfica para operar de manera intuitiva en la *blockchain*.

Como esta tecnología se creó para mediar transacciones entre terceros desconocidos, se establecen los llamados mecanismos de consenso, que regulan la manera a través de los cuales los nodos se ponen de acuerdo para agregar bloques en la cadena, destinados a garantizar la consistencia de la información y la seguridad, y que variarán según la red en que nos encontremos. En la *blockchain* de Bitcoin, por ejemplo, se utiliza la prueba de trabajo (*proof of work)* que implica que los nodos mineros deben resolver complejos problemas matemáticos, y así el primero que lo logre agregará el bloque a la cadena y obtendrá una recompensa a cambio. En Ethereum se utiliza la prueba de propiedad (*proof of stake)* que mediante criterios de cantidad de moneda reservada y tiempo de participación determina qué nodo sellará cada bloque. Otro mecanismo es el de prueba de autoridad, en el cual los bloques solo pueden ser agregados por aquellos nodos que se encuentren autorizados, que se van turnando y no se requiere la solución de problemas matemáticos ni operar con criptomonedas. Asimismo, existen otros numerosos mecanismos como la prueba de participación, de almacenamiento, de actividad, de capacidad, de tolerancia a las fallas bizantinas, etc.

Una vez sellado el bloque, todas las operaciones quedan registradas y dotadas del carácter de inmutabilidad. Dependiendo el tipo de red, en caso de que sea pública cualquier persona puede verificar libremente las transacciones realizadas y la información registrada en cada bloque.

Por último, estrechamente relacionado con esta tecnología y a su funcionamiento, se encuentran los denominados contratos inteligentes o *smart contracts.* Estos son entendidos como flujos de tareas programables ejecutados dentro de la *blockchain*. Estos programas se ejecutan en la red e interactúan con ella como una especie de usuario, ya que poseen su propio par de llaves pública-privada y registran las transacciones en la red como lo haría cualquier otro usuario.

4. CLASES DE *BLOCKCHAIN*

Si bien existen diversas clasificaciones de la *blockchain*, para este trabajo nos parece útil agruparlas en redes públicas y privadas, por un lado, y permisionadas y no permisionadas por el otro.

4.1. PÚBLICAS Y PRIVADAS

Lo que caracteriza a una *blockchain* pública es que todo su contenido es abierto, por lo que cualquier operación puede ser consultada por un tercero. Tanto su software como su desarrollo están abiertos a la comunidad. Cualquier persona puede comprobar la integridad y validez de los datos contenidos en la cadena, así como explorar las transacciones realizadas y el contenido de los bloques[75].

Por su parte, las *blockchain* privadas son de carácter cerrado, por lo que el detalle de las transacciones realizadas no será visible libremente. Para poder acceder se debe contar con la autorización de quienes administran la red.

4.2. PERMISIONADAS Y NO PERMISIONADAS

Según esta clasificación serán permisionadas cuando para efectuar determinadas operaciones en la red se necesita autorización de quien o quienes la administran. Algunas permiten el acceso solo a aquellos participantes que hayan validado efectivamente su identidad, mientras que otras pueden permitir a cualquiera entrar, pero solo podrán efectuar transacciones quienes hayan validado su identidad. Así por ejemplo puede existir una *blockchain* pública permisionada[76] en la que cualquiera puede ver la información y participar, pero solo algunos pueden ser nodos validadores. Respecto a las privadas, estas generalmente suelen ser permisionadas[77].

Por el contrario, en las no permisionadas cualquier integrante puede acceder, validar y procesar transacciones. Por ejemplo, en una *blockchain* pública no permisionada cualquiera pueda unirse y participar en ella, sea como nodo o simplemente como participante, tales como ocurre con la red de Bitcoin o Ethereum.

5. RELEVANCIA Y APLICACIÓN

La *blockchain* ha supuesto una disrupción en diversos ámbitos, ya que, al actuar como registro descentralizado, busca dotar de confianza las relaciones entre terceros desconocido en la ejecución de transacciones. Así, procura resolver los problemas derivados de la intermediación y la falta de confianza entre terceros. Su relevancia ya

[75] Dentro de esta categoría se encuentran: la red de Bitcoin puede ser explorada desde https://www.blockchain.com/es/explorer; la red de Ethereum desde https://etherscan.io/; la red de Blockchain Federal Argentina desde http://www.bfascan.com.ar/; entre otras.
[76] Ejemplos de estas redes pueden ser Alastria o Blockchain Federal Argentina.
[77] Un ejemplo de red privada permisionada sería el proyecto Hyperledger.

trasciende todos los sectores, y su adopción es cada vez mayor en empresas de diversa envergadura e incluso por parte de Administraciones Públicas. Asimismo, su importancia ha sido reconocida por diversos organismos, desde la OCDE[78] hasta la Comisión Europea[79].

Claro que esta tecnología no está exenta de algunas desventajas, por lo que la conveniencia de su adopción deberá ser analizada en el caso concreto, pero a pesar de ello no podemos negar la creciente relevancia que adquiere día a día. A continuación, veremos algunos casos de uso, tanto en el sector público como privado. Aún si se considera que estas referencias pueden resultar triviales para los juristas, consideramos que se torna relevante su mención a los fines de demostrar el variado y creciente campo de aplicación de esta tecnología de la que derivarán, en el corto y mediano plazo, diversas implicancias en el derecho, incluido el ámbito probatorio. Además, como ya se mencionó, en el ámbito civil la labor de recabar y generar prueba valorable racionalmente está a cargo de los abogados independientes, lo que hace necesario que poseer un conocimiento acabado del funcionamiento de esta tecnología y sus implicancias prácticas para desarrollar su actividad.

5.1. En el sector público

En los últimos tiempos, el sector público tanto de España como de Argentina ha encarado un proceso de transformación digital. En este proceso, la *blockchain* puede desempeñar un papel destacado, garantizando transparencia y generando confianza y seguridad en los administrados.

Con este fin, en Argentina se creó la Blockchain Federal Argentina (en adelante BFA) que funciona como una plataforma pública que integra servicios y aplicaciones sobre *blockchain*, con base al modelo de múltiples partes interesadas como modelo de gobernanza, que asegura la representación de todos los sectores en la toma de decisiones. En ella participan cinco sectores: la Administración Pública Nacional; los Gobiernos de las provincias y de la Ciudad Autónoma de Buenos Aires; el académico; el sector privado;

[78] Pueden consultarse diversos proyectos en marcha en: "Global Blockchain Policy Centre", Organización para la Cooperación y el Desarrollo Económicos (OCDE), https://www.oecd.org/finance/blockchain/ (consultada el 10/06/2021).
[79] A tal fin se ha creado el Observatorio y Foro Europeo de Blockchain, que es una iniciativa que busca acelerar la innovación de *blockchain* y el desarrollo de su ecosistema dentro de la Unión Europea. Más información en: "Observatorio y Foro Europeo de Blockchain", Comisión Europea, https://www.eublockchainforum.eu/about (consultada el 10/06/2021).

y la sociedad civil. BFA toma como base el software de código abierto sin utilizar ninguna criptomoneda. El mecanismo de consenso utilizado es la "prueba de autoridad", que implica que solo los nodos previamente autorizados pueden registrar información en la cadena, sin perjuicio de que la verificación de los datos es pública[80].

La BFA es utilizada por diferentes organismos estatales. Algunos ejemplos de uso están dados con el Boletín Oficial, que desde 2017 registra todas sus ediciones en la BFA para asegurar la inmutabilidad y facilitar la verificación de los datos. La Cámara de Diputados la utiliza para registrar los votos electrónicos; el Ministerio de Educación hace lo propio para registrar todo el proceso de certificación de diplomas y analíticos; entre muchos otros[81].

Otro caso interesante está dado para las licitaciones públicas. Es sabido que existe por parte de los ciudadanos gran incertidumbre acerca de la transparencia de los procesos de licitación, y no son pocas las acusaciones de fraudes que en su realización surgen. Así, su registro en la *blockchain* podría dotar de transparencia y trazabilidad todo el proceso, haciéndolo accesible tanto a ciudadanos como a los demás oferentes. Ello implica que ningún tercero o funcionario estatal podría manipular los datos con posterioridad, asegurando así la integridad de todo el proceso y facilitando una eventual determinación de responsabilidades[82].

En la provincia de Córdoba actualmente se está estudiando la posibilidad de implementar esta tecnología en el Registro de la Propiedad. Por su parte la Universidad Nacional de Córdoba también utiliza la cadena de bloques para registrar compras y contrataciones, así como diversos documentos académicos (actas de examen, de promoción, etc.). La Municipalidad de la ciudad de Córdoba también registra en la *blockchain* determinados datos con el fin de impedir que el mismo gobierno, sea actual o futuras gestiones, modifiquen o eliminen datos críticos que han sido publicados[83].

El sector público español tampoco ha sido ajeno a esta tecnología. Actualmente existen algunos proyectos para implementar la *blockchain* en el proceso judicial. En este

[80] "Qué es BFA", Blockchain Federal Argentina, https://bfa.ar/bfa/que-es-bfa (consultada el 16/06/2021)
[81] Otros casos de uso pueden consultarse en: "Aplicaciones", Blockchain Federal Argentina, https://bfa.ar/bfa/aplicaciones (consultada el 16/06/2021).
[82] Para una explicación detallada sobre el procedimiento en estos casos: "Casos de uso", Blockchain Federal Argentina, https://bfa.ar/blockchain/casos-de-uso/licitaciones (consultada el 16/06/2021).
[83] "Portal de Gobierno Abierto de la Municipalidad de Córdoba", Municipalidad de Córdoba, https://gobiernoabierto.cordoba.gob.ar/blockchain/ (consultada el 17/06/2021).

sentido, el Consejo General del Poder Judicial reconoce en su proyecto de Protocolo de Protección del Secreto Empresarial en los Juzgados Mercantiles de Barcelona, el uso de esta tecnología para preservar el secreto de documentos o información en el marco de un procedimiento regido por la LEC[84].

Otro ejemplo está dado por el Gobierno de Aragón, que con el fin de hacer más transparente y eficiente la contratación pública, utiliza la tecnología *blockchain* para dar entrada a los contratos públicos. Todo ello puede consultarse públicamente a través de la web, donde constan los datos ingresados en dos cadenas de bloques[85].

En definitiva, vemos que mediante el uso de esta tecnología el sector público pretende generar confianza y dotar de transparencia su actuación. Se asegura así que los datos no puedan ser manipulados y permite verificar su integridad por parte de cualquier interesado.

5.2. En el sector privado

La confianza constituye un pilar sobre el que debe desarrollarse la actividad comercial. En muchas ocasiones, dada la falta de confianza en la contraparte, la confianza se encuentra depositada en terceros (intermediarios), lo que no solo implica un mayor coste, sino que muchas veces no soluciona del todo el problema, ya que tampoco están exentos de manipulaciones, fraudes o hackeos.

El uso de la *blockchain* intenta solucionar esto, ya que la confianza no está depositada en un intermediario sino en la propia red, donde las partes −mediante un mecanismo de consenso− registran las operaciones. Así se garantiza que cada interviniente tiene una copia completa del registro y que estos no pueden ser modificados sin ser detectados.

Una de las principales ventajas de la implementación de la cadena de bloques en el mundo empresarial es la reducción de los costos, sobre todo por no tener que recurrir a intermediarios. El mecanismo de consenso implica una puesta en común y la delegación de confianza en el protocolo, que dota de transparencia todas las operaciones realizadas.

---

[84] "La CRAJ informa: Protocolo de protección del secreto empresarial. Juzgados Mercantiles de Barcelona", Ilustre Colegio de Abogacía de Barcelona, https://www.icab.es/es/actualidad/noticias/noticia/La-CRAJ-informa-Protocolo-de-proteccion-del-secreto-empresarial.-Juzgados-Mercantiles-de-Barcelona./ (consultada el 18/06/2021).

[85] "Visor Público de la Blockchain", Gobierno de Aragón, https://licitacion.aragon.es/ (consultada el 20/06/2021).

A través del modelo de confianza distribuida se evita la necesidad de un intermediario y todos los involucrados pasan a ser parte de la red *blockchain*, con los beneficios que ello implica en cuanto a la transparencia de las operaciones y la inmutabilidad de los registros.

Innumerables usos pueden darse a esta tecnología, que resulta útil para el resguardo de información sensible, propiedad intelectual, modelos de negocio descentralizados, proyectos de identidad auto soberana, entre otros. También son numerosos los casos de empresas que ofrecen servicios de confianza, que adicionan una capa extra de robustez mediante el uso de la *blockchain*[86].

Un proyecto colaborativo para destacar es el de *Hyperledger*, de código abierto y perteneciente a la Fundación Linux, que busca desarrollar soluciones de *blockchain* permisionadas a nivel empresarial[87].

En el caso específico de España, debemos mencionar a Alastria que es una asociación sin ánimo de lucro que ha establecido una red pública permisionada formada por empresas, asociaciones y entidades del sector público.

Finalmente, esta tecnología ha tenido un rol preponderante en el nacimiento de mecanismos alternativos de resolución de conflictos que algunos denominan "justicia descentralizada", a la que las partes se someten voluntariamente a los fines de dirimir un conflicto[88].

5.3. En el ámbito probatorio

Numerosos juristas han afirmado que el uso de esta tecnología aporta un valor agregado frente a un eventual proceso judicial, y que en principio podría utilizarse sin inconvenientes en estos casos.

En este sentido, autores como Navarro[89] han expresado que la cadena de bloques es un medio que permite asegurar la cadena de custodia de la prueba y que esta tecnología

[86] Por ejemplo, la empresa Safe Creative, dedicada al registro digital de derechos de autor, incorporó como capa adicional de seguridad un proceso de auditoría basado en *blockchain*. "Blockchain llega a Safe Creative", Safe Creative Blog, https://es.safecreative.net/2019/04/10/blockchain-llega-a-safe-creative/ (consultada el 06/06/2021).
[87] "An Introduction to Hyperledger", Hyperledger, https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf (consultada el 13/06/2021).
[88] Un proyecto en este sentido lo constituye Kleros, que utiliza la tecnología de cadena de bloques y el crowdsourcing para resolver disputas. "About Kleros", Kleros, https://kleros.io/about/ (consultada el 21/06/2021).
[89] Navarro, «Blockchain y proceso electrónico», 799.

puede actuar como generador de prueba y registrador en términos amplios, ya que otorga certificados de prueba y de creación. El referido autor expresa que, desde el punto de vista jurídico, la *blockchain* no se diferencia de otras pruebas electrónicas, por lo que su aportación al proceso no debería generar ninguna dificultad.

Mora[90] expresa que, dadas las características de la cadena de bloques, no debería existir ningún inconveniente en que todas aquellas anotaciones realizadas sean reconocidas como válidas, sobre todo atento la regulación vigente de documento electrónico y la LFD.

También se ha dicho que la *blockchain* "tiene naturaleza y finalidad eminentemente probatoria", por cuanto contribuye a dotar a los documentos electrónicos de validez acreditativa, y consiste en una prueba por interposición y por cotejo. Que, por un lado, el encadenamiento de los *hashes* mantiene inalterada la matriz de la prueba, protegiendo su contenido, y por el otro, el uso de criptografía como base de firmas digitales aporta la identidad[91].

En el mismo sentido, se ha afirmado que la *blockchain*, "por facilitar un registro como medio de prueba, representa un hecho que ocurrió en una determinada fecha y hora", y si bien no es responsable del contenido, sí lo es respecto a su validación y registro. Así, esta tecnología "es considerada una evidencia y prueba que materializa la inmutabilidad de los hechos a través de sus registros"[92].

En cuanto a la fuerza probatoria, se sostiene que los registros de la cadena de bloques no poseen el efecto legitimador y probatorio específico de los documentos que gozan de fe pública, pero sí del que corresponde a los documentos privados. En su mérito no existirá una presunción de que el contenido de la *blockchain* sea exacto, que será objeto de prueba[93].

[90] Santiago J. Mora, «La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso», *La Ley*, n.º 786 (2019): 6-7.
[91] José Maria Anguiano Jiménez y Ángel López Pérez, «Retos jurídicos ante la transformación digital», *Diario La Ley*, n.º 9011 (2017): 2-3.
[92] Diego Beltran Avila, «Derecho a la presunción de inocencia en el proceso penal: valor probatorio de la blockchain», *Revista de Direito Brasileira* 25, n.º 10 (2020): 316, http://dx.doi.org/10.26668/IndexLawJournals/2358-1352/2020.v25i10.6146.
[93] Miguel Ruiz-Gallardón García de la Rasilla, «Fe pública y tokenización de activos en blockchain», en *Criptoderecho. La regulación de blockchain*, dir. Pablo García Mexía (Madrid: Wolters Kluwer, 2018), 481-82.

Relativo a la integridad y no repudio de los documentos se ha manifestado que la cadena de bloques:

> …garantiza plenamente los elementos de integridad del documento firmado y el no repudio, puesto que la tecnología en sí ofrece una garantía de orden cronológico de los bloques que se van generando en la cadena, haciendo casi imposible de modificar la información contenida en el documento firmado, ya que la mínima mutación haría que cambiarán todos los "bloques" lo cual sería advertido pro todos los nodos de la red. Además, al no ser posible reescribir la información una vez integrada en la cadena, el rastreo de la información es sencillo y trasparente, lo que elimina toda posibilidad de negación por la parte firmante.[94]

Si bien podríamos continuar con afirmaciones de la doctrina, lo que nos atañe ahora y que será objeto de tratamiento en los apartados subsiguientes, será intentar desentrañar el porqué de afirmaciones en tal tenor. Para ello indagaremos con mayor detenimiento cómo el funcionamiento de esta tecnología puede incidir en dos de los aspectos más relevantes de la prueba digital y los documentos electrónicos: la autoría y la integridad.

6. Regulación legal

6.1. Normativa aplicable

Antes de adentrarnos a la regulación en los códigos de procedimiento, debemos dilucidar qué normas legales regulan expresamente la *blockchain*. El relevamiento solo tiene en cuenta normas que la reglamenten directamente, dejando de lado otra legislación dirigida exclusivamente a otros aspectos, como por ejemplo los criptoactivos.

De un relevamiento de la normativa argentina, solo nos encontramos con una norma que hace alusión a esta tecnología: el Decreto 182/2019[95], que enuncia como uno de los tipos de servicio de confianza prestado por un tercero de confianza a la operación de cadenas de bloques usados para la conservación de documentos electrónicos; la gestión de *smart contracts*; y otros servicios digitales. Así, la normativa refiere al uso de la *blockchain* específicamente utilizado por terceros de confianza, aunque tal instituto actualmente no es utilizado debido a la falta de reglamentación.

[94] Fernando Fernández-Miranda Vidal, Marta Llamazares Carreño, y Alba Carrasco Ventura, «Usos de la firma electrónica y sistemas de identificación electrónica en el entorno digital actual», en *Nuevas tecnologías 2021*, dir. Enrique Ortega Burgos (Valencia: Tirant lo Blanch, 2021), 311.
[95] Art. 36 del Decreto del Poder Ejecutivo Nacional 182/2019 del 11/03/2019 mediante el cual se reglamenta la Ley N° 25.506 de Firma Digital (Argentina: BORA, 12/03/2019).

En el ordenamiento jurídico español verificamos la existencia del Real Decreto-ley 14/2019[96] que expresamente vedó la posibilidad de utilizar −en las relaciones de los interesados con las Administraciones Públicas− sistemas de identificación y firma basados en tecnologías de registro distribuido hasta tanto no exista regulación específica en el marco del Derecho de la Unión Europea. En la exposición de motivos se hace la salvedad que tal prohibición no opera de manera generalizada, sino tan solo en el supuesto contemplado (relación Administración-administrados) y provisoriamente hasta tanto sea objeto de legislación europea.

Recientemente, dentro de los intentos de la Unión Europea para dar un marco jurídico que favorezca la innovación y con el fin de lograr un uso generalizado en los servicios financieros de las tecnologías de registro distribuidos, se efectuó una Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre un régimen piloto de las infraestructuras del mercado basadas en la tecnología de registro descentralizado[97], que implica una reforma al Reglamento eIDAS y hace expresa alusión a los registros distribuidos o DLT.

El proyecto de reforma al Reglamento eIDAS destaca la relevancia de la integridad de los datos en los sistemas descentralizados, en las soluciones de identidad auto soberana, para atribuir la propiedad frente a activos digitales, para el registro de los procesos comerciales, así como otros numerosos casos de uso. Señala que la tecnología de registros distribuidos proporciona una prueba de la integridad de los registros y permite la verificación de la secuencia de transacciones y registros, salvaguardando la integridad de los datos. Asimismo, reconoce que tal seguridad se logra por la combinación del sellado de tiempo junto con la concatenación de los datos, que actúa de manera similar a la firma electrónica con el beneficio adicional de poseer una gobernanza descentralizada. También expresa que esta tecnología permite a las empresas ahorrar costes ya que la coordinación se hace más eficiente, más seguro y facilita además la supervisión regulatoria.

[96] Art. 3 del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones (España: BOE, núm. 266, 05/11/2019).
[97] "Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento de un marco para una identidad digital europea", Comisión Europea, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:281:FIN (consultada el 25/06/2021).

De aprobarse esta propuesta, se incorporaría a las DLT como nuevos servicios electrónicos de confianza que asegurarían −previo cumplimiento de los requisitos establecidos− la autenticidad e integridad de los datos.

Cabe mencionar también que se hace alusión a la tecnología de registros distribuidos en el Anteproyecto de Ley del Mercado de Valores y de los Servicios de Inversión[98]; y que existen normas técnicas en cuanto a su funcionamiento, tal como el establecido por la Asociación Española de Normalización, que publicó un estándar sobre identidad digital descentralizada *blockchain*[99].

En definitiva, se observa que actualmente en ninguno de los dos países existe normativa que regule específicamente efectos jurídicos de la *blockchain*. Si bien a nivel europeo el proyecto de modificación al Reglamento eIDAS podría tener gran relevancia, por el momento deberemos hacer el análisis con base a la legislación actualmente vigente.

6.1.1. Normativa en la Unión Europea

A pesar de la falta de normativa específica antes vista, algunos países ya han incorporado regulación que atribuye determinados efectos jurídicos a la *blockchain*. Sin intención de realizar una reseña de todos los casos existentes, que excede el marco de este trabajo, consideramos interesante mencionar un caso existente en la Unión Europea.

Así, tenemos el caso de Italia, que mediante ley 12/2019 introdujo modificaciones al Decreto-ley 135 del de 14 diciembre de 2018[100], que realiza mención específica a esta tecnología. El art. 8 ter de la citada normativa expresa lo siguiente[101]:

> Artículo 8-ter
>
> (Tecnologías basadas en libros de contabilidad distribuidos y contrato inteligente).

[98] "Anteproyecto de Ley del Mercado de Valores y de los Servicios de Inversión y Reales Decretos de desarrollo", Portal del Ministerio de Asuntos Económicos y Transformación Digital, https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/ECO_Tes_20210430_AP_LMVySI_Texto_Ley_del_Mercado_de_Valores.aspx (consultada el 08/06/2021).

[99] "Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia", Asociación Española de Normalización, https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0064986 (consultada el 08/06/2021).

[100] Decreto-ley 135 del 14/12/2018 sobre Disposiciones urgentes sobre apoyo y simplificación para las empresas y la administración pública, (Italia: Gazzetta Ufficiale, 12/02/2019).

[101] Traducción propia.

> 1. Se definen como "tecnologías basadas en registros distribuidos" a la tecnologías y protocolos informáticos que utilizan un registro compartido, distribuido y replicable, accesible simultáneamente, arquitectónicamente descentralizado sobre una base criptográfica, que permita el registro, validación, actualización y archivo de datos de manera clara y protegidos por criptografía verificable por cada participante, no modificable y no editable.
>
> 2. Se define "*smart contract*" al programa para computadora que opera con tecnologías basadas en registros distribuidos y cuya ejecución vincula automáticamente dos o más partes, basadas en efectos predefinidos. Los contratos inteligentes cumplen con el requisito de forma escrita, previa identificación informática de las partes, a través de un proceso que reúna los requisitos establecidos por la Agencia para la Italia Digital con directrices a ser adoptadas dentro de los noventa días a partir de la fecha de entrada en vigor de la ley de este decreto.
>
> 3. El almacenamiento de un documento informático mediante el uso de tecnologías basadas en registros distribuidos producirá los efectos jurídicos del sellado electrónico de tiempo a que se refiere el artículo 41 del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014.
>
> 4. En un plazo de noventa días a partir de la fecha de entrada en vigor del presente decreto, la Agencia Italia Digital deberá identificar las normas técnicas que las tecnologías basadas en registros distribuidos deben poseer para producir los efectos según el apartado 3.

De esta manera Italia ha incorporado a su entramado normativo una definición específica tanto de las DLT como de los *smart contracts*. Se destaca sobre todo la asignación de efectos jurídicos a esta clase de registros, siempre que dicha tecnología sea desplegada conforme las normas técnicas estipuladas oportunamente. En este caso equipara el sello de tiempo utilizado en la cadena de bloques a un sello de tiempo simple. Resaltamos en este sentido el intento del legislador de dotar de mayor seguridad jurídica, atribuyendo de manera directa efectos jurídicos a un documento almacenado mediante esta tecnología.

6.2. La *blockchain* ¿medio o fuente de prueba?

Otra cuestión que es necesaria definir antes de ingresar a la normativa procesal, es acerca de si la cadena de bloques debe ser tratada como un medio de prueba o bien como fuente.

La *blockchain* puede servir de soporte a los documentos electrónicos, pero esta tecnología en sí −como registro distribuido− no puede ser considerada un documento,

aunque los datos enlazados a ella sí podrán tener consideración de documentos privados[102].

Para entender tal afirmación deben ser aclarados algunos aspectos. En primer lugar, siempre que se utilice la red, desde enviar un token, un criptoactivo o registrar un documento, se efectuará una operación que quedará asentada en un bloque determinado. Esta acción, denominada transacción, quedará incorporada a la red dentro de un bloque y podrá ser consultada en cualquier momento[103]. Si desglosamos ese bloque nos encontraremos con el *hash* del bloque anterior junto con el detalle de las transacciones contenidas y una marca o sello de tiempo, entre otras cosas.

A tenor de lo enunciado en el apartado II, consideramos que tanto el detalle de un bloque como una transacción en sí, debidamente incorporada a la cadena, pueden ser considerados como documentos electrónicos, ya que consisten en un conjunto de datos que representan un hecho de interés para el proceso. A partir de este punto, comenzaremos a referirnos a la transacción no como la operación efectuada por un usuario de manera primigenia que es sometida al proceso de validación y sellado, sino ya a la transacción que ha quedado debidamente validada y registrada en un bloque, y que plasma una operación que un determinado usuario ha realizado mediante la utilización de su par de llaves pública-privada.

En segundo lugar, hay que tener en cuenta que una transacción puede estar vinculada a un *smart contract* u a otro documento electrónico. En este último caso la vinculación estará dada por el *hash* del documento en cuestión, que aparecerá en los detalles de la transacción[104]. De esta manera la presentación del documento electrónico vinculado estará indefectiblemente a cargo de quien lo ofrezca, que tendrá a su cargo su almacenamiento y resguardo, diferenciándose de la transacción en sí como un nuevo documento.

[102] Javier Wenceslao Ibáñez Jiménez, «Cuestiones jurídicas en torno a la cadena de bloques ("blockchain") y a los contratos inteligentes ("smart contracts")», *Icade: Revista de la Facultad de Derecho*, n.º 101 (8 de febrero de 2018), 4, https://doi.org/10.14422/icade.i101.y2017.003.

[103] Para graficar el detalle de una transacción, se ha escogido una aleatoriamente de la red de Ethereum que puede consultarse en: https://etherscan.io/tx/0x1da3bd7c9607c6c13c8f5065be12d16e2cae0544f11f82b7bef18b14a44a0c97.

[104] Ello será así en las redes con almacenamiento *off-chain*, que como son la gran mayoría es a la que haremos referencia. Ante una red con almacenamiento *on-chain*, los diferentes nodos actuarán como soporte del documento electrónico en cuestión.

Efectuadas estas aclaraciones, la transacción, en su carácter de documento electrónico será el objeto de prueba, que contendrá información para probar de manera autónoma algún punto en particular o de manera complementaria cuando lo sea en relación con otro documento electrónico o *smart contract* a ella vinculada.

Como consideración aparte, se constata también que esta tecnología podría tener incluso otra perspectiva. Así como Abel Lluch[105] nos explicaba que no debemos confundir firma electrónica con una fuente o medio de prueba, sino que es considerada un instrumento tecnológico que permite garantizar en los documentos electrónicos su autoría e integridad, podríamos efectuar idéntica consideración con la *blockchain* como tecnología. Al fin y al cabo, estamos frente a un desarrollo tecnológico que impacta en determinados atributos de los documentos electrónicos. No obstante, por el momento no existe regulación legal específica que atribuya tales efectos *per se* a la cadena de bloques. Seguimos entonces la consideración de que, como regla, será una transacción en sí que operará como fuente de prueba.

También existen algunos autores que consideran a la *blockchain* como medio de prueba[106]. Recordemos que los medios de prueba son los elementos o instrumentos utilizados por las partes y el juez que suministran las razones o motivos que le llevan al juez la certeza sobre un hecho (siendo estos últimos fuente de prueba)[107]. Si bien el ordenamiento español prevé como medio de prueba los "instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso" (art. 299.2 LEC), en los que esta tecnología parecería encuadrar, en rigor la norma se está refiriendo a cualquier otra fuente de prueba, por cuanto no debemos identificar la fuente con el soporte que recoge su contenido[108].

Sumado a lo anterior, debemos tener en cuenta la reciente y ya referida Sentencia del Tribunal Supremo 706/2020, que reconoce el carácter *númerus clausus* del art. 299.1 LEC, motivo por el cual los medios de prueba serán solo aquellos previstos por dicho apartado. Por ende, la cadena de bloques no podrá ser considerada como medio de prueba

[105] Abel Lluch, «Prueba electrónica», 177.
[106] Letícia Melo, «Régimen jurídico de blockchain: una prueba atípica», *Revista de Bioética y Derecho*, n.º 46 (2019), *passim*, https://doi.org/10.1344/rbd2019.0.27071.
[107] Hernando Devis Echandia, *Teoría General de la Prueba Judicial*, vol. I (Buenos Aires: Zavalía, 1970), 33-34.
[108] Abel Lluch, «Prueba electrónica», 66.

desde la perspectiva del ordenamiento español, sino que tanto un bloque como una transacción tendrán la consideración de documento electrónico, que deberá ingresar al proceso por el medio de prueba documental.

Ahora situándonos desde la perspectiva del ordenamiento procesal cordobés, el art. 202 CPCC establece expresamente:

> Artículo 202. Otras pruebas admisibles. Cuando se ofreciere un medio de prueba idóneo y pertinente no prevista de modo expreso por la ley, el tribunal establecerá la forma de diligenciarlo, usando el procedimiento determinado para otras pruebas que fueren analógicamente aplicables.

La norma procesal consagra la libertad de medios de prueba, lo que permite no solo recurrir a los medios clásicos sino también a cualquier otro que pudiere llegar a existir, aunque para ello el tribunal deberá establecer el procedimiento adecuado utilizando algún mecanismo análogo a otro medio de prueba regulado.

Analizando la jurisprudencia existente sobre el tema, advertimos que el Tribunal Superior de Justicia de la Provincia de Córdoba se ha manifestado en idéntico sentido, reconociendo que:

> …los hechos conducentes y controvertidos que es menester acreditar a los fines del éxito de la pretensión no sólo pueden probarse a través de los medios de prueba previstos en el código: documental, informativa, confesional, testifical, pericial, reconocimiento judicial, sino también por cualquier medio de prueba que se disponga a pedido de parte o de oficio, que no afecte la moral, la libertad personal de los litigantes o de terceros o que no esté prohibida para el caso (conf. arts. 200, 202 y cc. del CPCC).[109]

Vemos así que, a diferencia de la referida Sentencia del Tribunal Supremo 706/2020, el máximo Tribunal de la provincia de Córdoba no considera que los medios de prueba sean limitados.

Por tales antecedentes podría llegar a indagarse la consideración de la cadena de bloques como un medio de prueba. No obstante, el mismo art. 202 CPCC ordena que, ante estos nuevos medios no previstos, deberá utilizarse el procedimiento lo previsto para un medio regulado que le sea análogo, que en nuestro caso y por los fundamentos ya

[109] Sentencia del Tribunal Superior de Justicia de Córdoba (Sala Civil y Comercial) 113/2005, de 26 de octubre de 2005 en autos "Torres Elba Inocencia Minetti de C/ E.P.E.C. – Ordinario – Recurso de Casación".

dados, será el documental. Con todo, no nos parece razonable entender la cadena de bloques como un medio de prueba distinto, cuando ya vimos que ella implica una tecnología que sirve de soporte a numerosas transacciones, que revisten el carácter de documentos electrónicos. Por ello, salvo particularidades del caso concreto, el instrumento adecuado para suministrar al proceso el motivo que sirve para dar certeza de un hecho, será el documental.

Descartada la consideración de la *blockchain* como medio de prueba, la fuente probatoria que representa la transacción debe ingresar al proceso a través de algunos de los medios previstos por cada legislación, que será −como regla general− el medio de prueba documental. Como el eje de la prueba será el documento o transacción en sí, entendidos estos como objetos representativos de un hecho de interés para el proceso −siendo secundario su soporte (pues este no constituye una nota esencial del documento)[110]−, deberá estarse a la regulación de la prueba documental para lo que es su aportación, impugnación, verificación y valoración se refiere.

[110] Abel Lluch, «Prueba electrónica», 54.

IV. LA AUTORÍA EN LA *BLOCKCHAIN*

1. PLANTEAMIENTO

Tal como hemos apuntado con anterioridad, uno de los presupuestos de la eficacia probatoria de un documento electrónico −junto con la integridad (tratada *infra*) y la licitud−, es su autenticidad, esto es, "la propiedad o característica consistente en que se garantiza la autenticidad del origen de los datos, es decir, se garantiza la fuente de la que proceden los datos"[111].

Mediante el uso de las llaves criptográficas en la *blockchain,* se asegura que las transacciones solo puedan ser realizadas por los poseedores del par de llaves pública-privada. Con este mecanismo queda garantizada la fuente de la que procede una determinada transacción, es decir, que quien la realiza es efectivamente quien "demuestra" ser a través de su clave pública.

Ahora bien, esta llave pública, también llamada dirección, que identifica a cada interviniente en la red, podría considerarse una identidad virtual o digital, entendida esta como "un conjunto finito de atributos que permite a una persona, animal, cosa o proceso ser identificado como único y probar su identidad frente a terceros electrónicamente"[112].

A partir de este punto nos surge un nuevo interrogante, ya que consideramos que para la atribución de efectos jurídicos y sobre todo frente a un proceso judicial se hace necesario contar con la identidad de los intervinientes. Nos referiremos a esta identidad como una identidad legal, que permita individualizar a una determinada persona natural o jurídica. Frente a una situación que involucre el uso de la cadena de bloques, resultará necesario entonces asociar la identidad virtual (en este caso exteriorizada mediante una clave pública o dirección) a la identidad legal, conforme se desarrollará en los puntos que siguen.

2. LA IDENTIDAD EN LA RED

En el comercio físico, la presencia de los intervinientes facilita la posibilidad de corroborar tanto la firma manuscrita como la identidad de los participantes mediante la

[111] Delgado Martín, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 80.
[112] Marcos Allende López, *Identidad digital auto-soberana: El futuro de la identidad digital: Auto-soberanía, billeteras digitales y blockchain* (Banco Interamericano de Desarrollo, 2020), 12, https://doi.org/10.18235/0002635.

exhibición de los documentos correspondientes. Por el contrario, en el mundo virtual existen diversas barreras que dificultan la identificación de las partes intervinientes. Si bien los ordenamientos prevén la existencia de sistemas de firmas electrónicas robustas que se equiparan a la firma manuscrita y garantizan la autoría (firma electrónica cualificada en España o firma digital en Argentina), su utilización es prácticamente ínfima en relación con la totalidad de operaciones que se realizan día a día en entornos virtuales.

Para la seguridad del tráfico jurídico virtual se hacen necesarios sistemas de identificación que posibiliten acreditar y autenticar de manera certera a los usuarios, asociándolos a una persona física o jurídica determinada.

Hasta ahora la mayoría de los sistemas de identidad desplegados en internet dependen de una entidad centralizada. Sin embargo, al no existir tal centralización en la cadena de bloques, nos preguntamos si es posible asociar una determinada transacción a un individuo en particular, a través de elementos que existan en la misma red o si es necesario recurrir a elementos que estén fuera de la cadena.

Cuando hablamos de identidad en la *blockchain* nos referimos a la identificación de quien efectuó la transacción. Como ya se dijo, en estas transacciones pueden intervenir otros documentos electrónicos (de manera autónoma mediante referencia a un *hash* o incluso por intervenir un *smart contract*), pero ahora el objeto de análisis radicará en la posibilidad de determinar la autoría de la transacción, aunque claro está, que tal determinación podrá tener injerencia sobre los demás documentos vinculados.

Dicho de otra manera, en la cadena de bloques −y lo que hace al objeto de este apartado− podemos corroborar en todo caso la autoría de quien efectuó la transacción. Si a esa transacción aparece ligado otro documento debemos estar a la identificación allí plasmada (como alguno de los tipos de firmas reconocidos por cada ordenamiento, por ejemplo), pero ante la ausencia de estos, la determinación de la autoría de la transacción en la que aparece vinculado también puede resultar un parámetro útil a probar.

2.1. Algunas pautas para determinar la identidad

Recordemos que en la *blockchain* se utiliza el sistema de clave pública y privada, y en las interacciones con la red solo podremos ver la clave pública o dirección de los participantes. A pesar de que la clave pública pueda ser considerada como un “usuario” que permite identificar a otro sujeto dentro de la red (como lo sería por ejemplo un correo

electrónico), ello no equivale a que pueda ser vinculado automáticamente con una identidad legal. En este punto el análisis dependerá del tipo de *blockchain* frente a la que estemos.

Aquí cobra relevancia el proceso de identificación y autenticación que implemente cada *blockchain* en particular. En el entorno virtual, se hace necesario adoptar un proceso que permita identificar a una persona física o jurídica y asociarla a un identificador, que en nuestro caso será la clave pública. Este proceso podrá tener distintos niveles de seguridad, conforme mayor sea el grado de confianza que se establezca entre tal asociación. Existen diversos mecanismos para efectuar la autenticación, esto es asociar la identidad al identificador, que van desde los más básicos (un usuario y contraseña) hasta otros más sofisticados, como por ejemplo mediante la utilización de datos biométricos, con el alto grado de seguridad que ello supone; o hasta mecanismos de acreditación de identidad provistos por el mismo Estado[113].

En las redes no permisionadas, su principal problema radica en el predominio de la anonimidad y privacidad de los intervinientes, ya que no existe una autoridad o mecanismo que previamente verifique la identidad de los participantes. En estos casos en principio no será fácil asociar una clave pública a la identidad legal de quien opera, ya que ella no vendrá vinculada de manera predeterminada, sino que será necesaria una mayor labor investigativa.

En las redes *blockchain* permisionadas, solo un grupo de participantes previamente habilitados puede sellar las transacciones y/o interactuar en la red. Según la red en particular, se realizará un proceso más o menos riguroso para asegurar la identidad de los participantes. Siempre que exista un sistema de gestión de identidad que efectúe una autenticación de los participantes se facilitará la asociación entre la clave pública y un individuo determinado, que será más o menos confiable según el mecanismo empleado. Aun así, en estos casos la identidad no estará determinada por la propia tecnología de cadena de bloques sino por procesos que son implementados junto con ella.

[113] Un ejemplo de ello es la plataforma que ofrece el Estado argentino llamada "Autenticar", que mediante la utilización de datos provistos por diversos organismos del Estado permite a las empresas que lo requieran validar la identidad de los ciudadanos de manera virtual y segura.

La cuestión se resolverá con relativa facilidad si estamos frente a redes utilizadas por parte de un servicio de confianza cualificado[114] o si se ha implementado el uso un sistema de identificación electrónica notificado conforme el Reglamento eIDAS, cuestión que excede al presente y que remite a las previsiones indicadas para esos casos por la normativa. La tarea también se facilitará cuando los participantes de la red, por requerimientos legales, apliquen reglas que impliquen verificar los datos del cliente (*know your customer*), por lo que poseerán los datos necesarios de identificación legal de los intervinientes. Este es el caso de entidades financieras o de los *exchanges*[115], que están sujetos a regulaciones que las obligan a requerir la identificación de sus clientes[116].

También existe la posibilidad de que tal determinación surja de la misma *blockchain* o de *smart contracts* asociados a ella. Como esta tecnología abre las puertas a numerosas posibilidades en lo relativo a la identidad, existen proyectos que buscan ahondar estos beneficios y crear una denominada identidad digital descentralizada o auto soberana. Sin en el objeto de profundizar esta cuestión que podría ser pasible de una investigación específica, diremos que la identidad auto soberana implica que un individuo posea y controle su identidad sin la intervención de autoridades centralizadas. Permite, entre varias cosas, una identidad digital fácil de emitir, administrar y verificar, todo mediante un identificador descentralizado que −según el caso− puede operar como una dirección en la *blockchain*[117]. De esta manera las transacciones realizadas por un identificador descentralizado específico podrán ser vinculadas a una identidad.

También existen proyectos de verificación de identidades que operan en la red pública de Ethereum, tales como *Proof of Humanity*, que asocian una determinada clave pública a una persona real, mediante el uso de redes de confianza, test de Turing inversos y resolución de disputas en línea para crear una lista de personas humanas verificadas. Se pretende solucionar la carencia de identidad que caracteriza a la internet de modo tal que

[114] Ello por el momento solo es aplicable al ordenamiento español, ya que en Argentina si bien se encuentran regulados, la ley aún no está reglamentada por lo que en la práctica no existe tal figura.
[115] Los *exchanges* son plataformas digitales que permiten intercambiar criptomonedas entre sí o por dinero de curso legal.
[116] Ya que en estos casos existe normativa propia que le es impuesta a los fines de una correcta determinación de la identidad de sus clientes. En Argentina por ejemplo podemos citar la Comunicación "A" 5717 y 5728 del BCRA, la ley 25.246 de Prevención de Lavado de Activos y Financiamiento del Terrorismo, Resolución N.º 30/2017 de la UIF, entre otras. Véase Andrés Chomczyk, «El desafío de las identidades digitales para la industria fintech», en *Fintech: aspectos legales*, comp. Pablo Andrés Palazzi y Santiago J. Mora (Buenos Aires: Pablo Andrés Palazzi, 2019), 231.
[117] Marcos Allende López, *Identidad digital auto-soberana, passim*.

todas aquellas transacciones llevadas a cabo por una clave pública que previamente se validó en *Proof of Humanity* sean fácilmente atribuibles a un individuo determinado[118].

Los casos antes mencionados, funcionan básicamente asociando una clave pública o dirección de la *blockchain* a diversos datos que engrosan la posibilidad de asociar la identidad digital a una legal, mediante el uso de *smart contracts* y diferentes grados de autenticación. No obstante, los proyectos mencionados se encuentran en desarrollo y son objeto de constante evolución. Además, los expresados son meramente ejemplificativos, ya que existe infinidad de estos, que deberán ser analizados en el caso concreto.

Si de las opciones vistas anteriormente aún no resulta posible una correcta identificación, se pueden utilizar técnicas que impliquen determinar indirectamente la autoría mediante patrones del uso de la red[119]. Otra opción será indagar las relaciones precedentes, pues puede ocurrir que las partes hayan efectuado transacciones anteriores en uso de dichas claves públicas, debidamente reconocidas en algún proceso o en algún intercambio de información (por email, WhatsApp, etc.).

En todos estos casos siempre hablamos desde la perspectiva de un proceso civil. En un proceso penal la cuestión puede ser diferente, ya que existe cada vez un mayor interés estatal por "des-anonimizar" transacciones ilícitas llevadas a cabo en la *blockchain*, mediante la utilización de software que analiza las redes existentes, al que recurren los Estados mediante convenios con las empresas prestatarias.

Por último, cabe aclarar que todo lo antes expuesto aplica siempre que al participante de la red le haya sido asignado su par de llaves público-privadas. Algunas implementaciones de la cadena de bloques, que ofrecen por ejemplo el servicio de sellado de tiempo, permiten que cualquier persona suba un documento y obtenga un comprobante que acredite la existencia e integridad del documento. Sin embargo, en realidad ese participante no está interactuando directamente desde la *blockchain*, sino que utiliza una interfaz provista por el servicio sin siquiera registrarse. En estos casos, el documento se

[118] No obstante, cada perfil de *Proof of Humanity* supone una identidad digital, que puede no ser exactamente igual a la identidad real, pero al tener asociado, entre varios datos, un video, puede facilitar tal asociación. Federico Ast, "Proof of Humanity: ¿Qué Es y Cómo Funciona?", *Blog Kleros*, 05 de mayo de 2021, https://blog.kleros.io/proof-of-humanity-que-es-y-como-funciona/ (consultada el 10/05/2021).

[119] Si se utiliza la clave pública a lo largo del tiempo, es posible detectar patrones, que podemos asociar a otra información (por ejemplo, la IP). No obstante, las direcciones IP del usuario no son almacenadas en la mayoría de las *blockchain* ni forman parte de la transacción, por lo que este tipo de información en sede civil será difícil de obtener. También existen mecanismos que crean una llave pública para cada transacción, de manera de dificultar el rastreo de patrones, por lo que no siempre será tarea sencilla.

envía a un nodo que es quien en definitiva genera la transacción mediante su par de llaves y da lugar al registro del documento en la cadena. Frente a estos casos la cadena de bloques no tendría incidencia alguna en la determinación de la identidad y habrá que estar a otros elementos que se encuentran fuera de la esfera de esta tecnología.

De lo visto, podemos afirmar que en la mayoría de los casos la *blockchain* por sí sola no nos dará una respuesta satisfactoria en cuanto a la determinación de esta identidad legal. Ello podremos determinarlo de diversas maneras: sea que su implementación conlleve algún sistema robusto de identificación y autenticación; mediante un análisis analítico de la cadena (patrones); mediante *smart contracts* asociados que provean soluciones de identificación; mediante recursos fuera de la cadena (reconocimiento de una determinada clave pública en otro proceso o documento), o por alguna de las otras formas antes vistas anteriormente así como por cualquier otra que pudiere llegar a existir en consecuencia de futuros avances tecnológicos. En todo caso muchas veces se exigirá recabar más información, la que tendrá carácter indiciario y llegado al caso, deberá ser objeto de prueba.

3. PRUEBA DE LA AUTORÍA EN EL PROCESO CIVIL

3.1. EQUIVALENCIA DE LA FIRMA UTILIZADA EN LA *BLOCKCHAIN*

Hasta ahora hemos visto que la cadena de bloques, por el uso de criptografía asimétrica, permite afirmar que cada transacción es realizada sin lugar a duda por la clave pública asociada a dicha transacción. Recordemos que para interactuar en la *blockchain* cada usuario es provisto de un par de llaves asociadas criptográficamente. Para poder operar debe ingresarse la llave privada correspondiente, que se encuentra en poder del usuario. La operación realizada y firmada con la respectiva clave privada, es identificada ante terceros con la clave pública. De esta manera, frente a cualquier transacción (identificada mediante su clave pública) podemos tener la certeza de que solo pudo ser realizada por el poseedor de la clave privada a ella asociada.

A pesar de esa certeza, lo problemático viene al momento de atribuir esa clave pública a una identidad legal, lo cual en un entorno virtual muchas veces no resulta fácil. Habiendo efectuado ya algunas pautas para posibilitar tal determinación, ahora veremos cómo es la actuación frente al proceso civil.

Entrando ahora al ámbito jurídico probatorio, partimos de que la *blockchain* utiliza un sistema de criptografía asimétrica asimilable a una firma electrónica simple. Esta consideración surge a partir de que el sistema utilizado de claves públicas y privadas implica el uso de datos electrónicos asociados de manera lógica utilizados por el firmante como medio de identificación. La firma utilizada en la cadena de bloques cumple las funciones que justamente debe desempeñar una firma: identifica al firmante (como mínimo a su identidad virtual); asegura el no repudio, esto significa que tal identidad virtual no puede desconocer frente a terceros haber realizado la transacción; y permite una asociación inequívoca del contenido a su emisor, todo en virtud del uso de criptografía asimétrica o de clave pública utilizada por la *blockchain*.

Por lo expresado hasta el momento, podemos subsumir la firma aplicada en la cadena de bloques a la firma electrónica simple definida por el art. 3.10 del Reglamento eIDAS y que torna aplicables los efectos del art. 25 de la norma referida. En Argentina por su parte podemos equipararla a la firma electrónica definida por el art. 5 de la LFD. En ambos ordenamientos podremos considerar entonces que la transacción constituye un documento electrónico con firma electrónica (simple en el caso de España) y que será admisible como prueba en juicio.

Algunos autores sostienen que la firma electrónica utilizada en la *blockchain* equivale a una firma electrónica avanzada, conforme el art. 26 del Reglamento eIDAS[120]. De la comparación entre la tecnología utilizada por la cadena de bloques y los requisitos establecidos por el referido artículo tenemos que parecen cumplirse *a priori* los siguientes requisitos: está vinculada al firmante de manera única (en referencia a la clave pública); ha sido creada utilizando datos de creación de la firma electrónica utilizados por el firmante que implican un alto nivel de confianza (en relación a la infraestructura de criptografía asimétrica) y se encuentran bajo su control exclusivo (en referencia a la llave privada); y está vinculada con los datos firmados de manera que cualquier modificación posterior puede ser detectada (dado por la característica de inmutabilidad de los registros).

Como consideración personal, creemos que no se cumple −en términos generales− el requisito de "permitir la identificación del firmante", ya que entendemos que la norma refiere a una identificación con garantía de certeza. La cadena de bloques permite asociar

[120] Eso sostienen autores como Ibáñez Jiménez, *Blockchain: Primeras cuestiones en el ordenamiento español*, 99-100.

de manera inequívoca una transacción al titular de la clave pública correspondiente, pero ello no equivale a una identificación del firmante en términos de identidad legal, aunque esto podría variar según la red en particular, y el uso que se haga de mecanismos de identificación y autenticación. Por ello, sostenemos que en principio esta tecnología asocia una firma a una identidad digital como mínimo, pero no a una identidad legal que entendemos requiere la norma. De igual manera habrá que analizar el caso concreto de cada implementación de la red, que puede contar con mecanismos robustos de identificación y autenticación que cumpla con la totalidad de los requisitos previstos por el art. 26 del Reglamento eIDAS.

En síntesis, en el ámbito español estaremos frente a un documento con firma electrónica simple como mínimo, aunque de la implementación particular la red pueda contar con mecanismos que permitan afirmar que estamos frente a una firma electrónica avanzada. En Argentina por su parte, en cualquier caso estaremos frente a una firma electrónica, aunque claro está que la robustez del sistema de identificación y autenticación utilizado será un elemento importante que acreditar en el proceso conforme veremos.

3.2. Actuación en el proceso civil

Efectuada la consideración de que el sistema de criptografía asimétrico utilizado por la cadena de bloques equivale a una firma electrónica prevista en los arts. 3.10 del Reglamento eIDAS y 5 de la LFD, procederemos a dilucidar su tratamiento en un juicio civil.

A falta de normativa específica sobre la cadena de bloques y en base a lo anteriormente expuesto, al presentar una transacción efectuada en la red, entendida esta como un documento electrónico, deberá seguirse el cauce establecido para la prueba documental.

En lo relativo a la aportación del documento electrónico, las particularidades estarán dadas por el caso concreto. Soluciones específicas de esta tecnología orientadas a proveer servicios de certificación de firma seguramente emitirán un comprobante respectivo que contendrá toda la información necesaria para ser presentada en juicio. En otros casos, si por ejemplo resulta necesario comprobar la autoría de una determinada transacción en una *blockchain* pública, podremos aportar los detalles de la transacción en sí, que pueden ser verificados libremente desde internet. En este último supuesto puede acompañarse captura de pantalla del detalle de la transacción junto a la dirección web

específica donde se obtuvo (si la red es verificable de manera pública), donde entre varias cosas figurará la clave pública interviniente.

La aportación del "pantallazo" es posible a tenor del art. 268.2 LEC que faculta a la presentación de copia simple del documento privado, que generará los mismos efectos que el original siempre que no sea controvertido. Aporta certeza la existencia de jurisprudencia que en casos similares se ha expresado en sentido de afirmar la validez de impresiones extraídas de una base de datos de una de las partes, reconociendo que la LEC debe ser interpretada teniendo en cuenta todos los avances tecnológicos[121].

Así, presentado el documento electrónico en juicio por una de las partes, a grandes rasgos pueden ocurrir dos cosas: que sea reconocido por la parte contra quien se presenta o que se impugne, en este caso, su autoría.

De no impugnarse el documento electrónico, estaremos frente a un supuesto de prueba tasada ya que hará plena prueba en el proceso (art. 326.1 LEC y art. 248 CPCC). Ante una eventual impugnación de la autenticidad del documento electrónico se deberá obrar de la siguiente manera según el ordenamiento jurídico aplicable:

En España, dependerá si se ha utilizado o no un servicio de confianza cualificado. Si se ha utilizado un servicio cualificado que utiliza la *blockchain* existirá una presunción a favor de la característica del documento que haya sido cuestionada. En cambio, frente a un servicio electrónico de confianza no cualificado se remite a lo indicado por el art. 326.2 LEC y al Reglamento eIDAS. De esta manera, ante a un documento electrónico en el que haya intervenido un servicio electrónico de confianza no cualificado o no haya intervenido directamente ninguno de estos servicios, la autenticidad en caso de ser impugnada deberá ser probada por cualquier medio de prueba que se considere pertinente, y a cargo de quien sostiene dicha característica.

Entonces, ante una eventual impugnación entrará en juego lo mencionado en el epígrafe anterior, de manera que deberá ofrecerse el medio de prueba que se considere pertinente según el caso concreto. Si la identidad puede probarse a través de elementos que estén asociados a la misma *blockchain*, los medios de prueba estarán enfocados sobre

[121] En tal sentido tenemos el Auto de la Audiencia Provincial de Barcelona (Sección 13) 6/2018, de 15 de enero de 2018, ponente Ilma. Maria del Pilar Ledesma Ibañez, f.j. 2°.

ella, de tal manera que esta será el objeto de prueba. Podrán ser utilizados todos los medios de prueba contemplados por el art. 299 LEC, con especial énfasis en el dictamen pericial.

Respecto a la práctica de los medios de prueba propuestos, habrá que tener en cuenta las características de la red. Si esta es pública, el acceso por las partes, el juez o los peritos será sencillo; en cambio si la red es privada, habrá que ver si permite la verificación pública de los datos. En redes completamente cerradas habrá que gestionar previamente con las entidades intervinientes el acceso para verificar la información, que en este caso no serán anónimas y será factible determinarlas. Si una de las partes del pleito es parte de la red, podrá ofrecer su nodo para la práctica de la prueba, ya que al fin y al cabo cada nodo posee una copia íntegra del contenido, aunque siempre deberá ser analizado en el contexto de la red.

Atento encontrarnos frente a una prueba electrónica, el medio de prueba más común a ser utilizado será el dictamen pericial. En este caso los puntos de pericia serán determinados en cada caso concreto, pero a modo orientador podemos deducir que el dictamen debe responder a lo siguiente: (1) que estamos ante una red considerada *blockchain*[122], cuyo diseño asegura la inmutabilidad de los datos; (2) que el documento cuya autenticidad se impugna se encuentra registrado en la cadena, en qué bloque y con qué fecha; (3) qué mecanismos de identificación y autenticación utiliza la red, así como su grado de robustez; y (4) finalmente, si es posible asociar la clave pública a una determinada persona, o en su defecto a un determinado ordenador (del que se realizó la transacción). En la mayoría de los casos la pericial informática será como una pericial complementaria; no obstante, también existe la posibilidad de ser solicitada de manera autónoma cuando por ejemplo sea necesario obtener un documento de la *blockchain* (en casos de almacenamiento *on-chain*) o si fuera necesario obtener los detalles de una transacción (aunque en la mayoría de los casos ello lo podría efectuar el mismo interesado si la red permite verificar los datos de manera pública).

No obstante, no solo es factible valernos del dictamen pericial, sino que podemos recurrir a cualquiera de los medios previstos por la legislación. Si bien suele afirmarse que cuando se impugna la autenticidad debe practicarse la prueba pericial para dilucidar tal extremo, la jurisprudencia ha afirmado que dicha pericia no será necesaria cuando de

[122] Para determinar si estamos ante un registro distribuido (DLT) o específicamente una *blockchain* pueden resultar útil determinar si cumplen con determinadas reglas del Organismo de Normalización en España (normas UNE) o normas ISO que determinan los requisitos para la estructura de estas redes.

otros elementos de la causa o por la práctica de otros medios de prueba no existieren dudas respecto a la autenticidad[123]. Si bien la jurisprudencia comúnmente refiere a impugnaciones que se dan en el marco de un sistema de comunicación, nada impide efectuar idéntica consideración en el caso, y más frente a los supuestos en los que se efectúe una impugnación genérica y estrictamente retórica, y se cuenten con otros elementos que permitan dar por probada la autenticidad del documento en cuestión.

De la práctica de los medios de prueba propuestos o de los demás elementos de la causa pueden ocurrir dos cosas: que se derive la autenticidad del documento en cuestión, o bien que ello no pudiere ser comprobado. Aún frente al caso en que la autenticidad no pudiere ser determinada, ya sea porque no se propusieron medios de prueba alternativos o porque de su práctica no se obtuvo el resultado esperado, ello no excluye la eficacia probatoria del documento, sino que el juzgador deberá valorar la prueba según las reglas de la sana crítica (art. 326.2 LEC). Recordemos que la sana crítica se refiere a "reglas no jurídicas derivadas de la lógica, la experiencia y la ciencia que sirven para fundar una valoración razonada de la prueba y permiten su control posterior por otro órgano de enjuiciamiento posterior"[124].

De esta manera, aunque una eventual pericial no arroje el resultado esperado, sobre todo frente a redes en las que predomina el anonimato y que no poseen un sistema adecuado de identificación y autenticación, el juez podrá valorar otros elementos presentados. Aquí cobra relevancia el rol de la parte que sostiene la característica impugnada, quien frente a este tipo de redes, debe aportar al juez otros elementos orientados a formar la convicción sobre la autoría del documento. Aquí aplican las recomendaciones efectuadas en el apartado pertinente, para asociar la clave pública a quien se le atribuye la autoría.

En este sentido entendemos que es de importancia un conocimiento, al menos básico, del juzgador sobre la *blockchain*, que le permita una adecuada valoración de toda la prueba propuesta. El juez tiene incluso la capacidad de apartarse fundadamente de algunos medios como el dictamen pericial, bajo ciertas condiciones, cuando pueda

[123] Sentencia del Tribunal Supremo (Sala de lo Penal) 375/2018, de 19 de julio de 2018, ponente Ilmo. Sr. Juan Ramon Berdugo Gómez de la Torre, f.j. 2°.
[124] Abel Lluch, «La impugnación de la prueba electrónica», 252.

demostrar que la opinión de un perito no posee una explicación técnica adecuada o posea algún elemento que le permita dudar de la credibilidad de tal dictamen[125].

Ahora situándonos en el ordenamiento procesal cordobés, la transacción como documento electrónico será considerado un instrumento particular[126] y seguirá el cauce de lo establecido para el medio de prueba documental.

En lo que hace a la aportación del documento, aplican las mismas consideraciones a las efectuadas al referirnos al ordenamiento español. La norma procesal también permite expresamente la incorporación de copias simples del documento (art. 87 CPCC) por lo que es factible acompañar capturas de pantalla de la transacción. Sobre la aportación de "pantallazos" la doctrina es pacífica en admitir tal posibilidad respecto a documentos electrónicos[127].

Una vez presentado el documento electrónico, su eficacia estará supeditada al reconocimiento por la persona contra quien es presentado o por una declaración en este sentido por parte del tribunal (art. 248 CPCC). Este reconocimiento puede ser expreso o tácito (art. 192, 197 y 243 CPCC; art. 314 CCCN). En definitiva, si el documento presentado es reconocido, no será necesaria la práctica de otros medios de prueba.

Frente al desconocimiento de la autenticidad, el CPCC solo establece en su art. 242 que "todo ofrecimiento de prueba documental lleva implícita la pericial caligráfica para el supuesto de negarse la autenticidad". Como la norma procesal no contempla el caso de documentos electrónicos, debemos recurrir a otras normas. Así, debemos contemplar conjuntamente el art. 5 LFD, que dispone que, al encontrarnos frente a una firma electrónica, ante a su desconocimiento corresponderá a quien la invoca acreditar su validez. Todo ello también debe ponerse en relación con el art. 314 CCCN que establece que la autenticidad de la firma puede probarse por cualquiera de los medios de prueba previstos por el ordenamiento.

[125] Carmen Ortiz Rodriguez, «¿Cuándo un juez deja de creer en un dictámen pericial?», en *La prueba en acción. Estrategias procesales en materia probatoria. Libro en homenaje al profesor Lluis Muñoz Sabaté*, dir. Joan Picó i Junoy (Barcelona: J.M. Bosch Editor, 2019), 237.
[126] La tesis contraria a la existencia de la firma electrónica, como se vio en el apartado correspondiente (punto II), consideraría a este documento como un instrumento particular no firmado, que podría ser considerado como un principio de prueba por escrito.
[127] Claudia E. Zalazar y Román A. Abellaneda, *Sistema probatorio en el proceso civil de Córdoba* (Córdoba: Alveroni Ediciones, 2021), 444.

Así, ante la impugnación del documento electrónico, deberán ser propuestos medios alternativos de prueba por parte de quien pretende probar este extremo, y en este sentido aplican idénticas consideraciones a las efectuadas respecto al ordenamiento español, en cuanto al acceso a la *blockchain* para la práctica de la prueba, la importancia del dictamen pericial y la proposición de determinados puntos de pericia.

Una vez diligenciada la prueba pertinente, ya en el ámbito de la valoración, el código de procedimiento cordobés determina que el juzgador deberá utilizar las reglas de la sana crítica, salvo que exista alguna disposición legal en contrario (art. 327 CPCC). Respecto al dictamen pericial, el mismo CPCC habilita al juzgador a apartarse del dictamen de los peritos (art. 252 CPCC). También se habilita al juez para tener en cuenta la conducta procesal observada por las partes (art. 316 CPCC). Fuera de la normativa procesal, el art. 319 CCCN establece algunas pautas de apreciación para tener en cuenta para determinar el valor probatorio de los instrumentos particulares.

A nivel de la Provincia de Córdoba es escasa la jurisprudencia que refiera a alguna cuestión vinculada a la prueba electrónica. No obstante, el único referente hasta el momento se encuentra en una sentencia de la Cámara de Apelaciones que admite la validez probatoria de correos electrónicos a tenor del principio de libertad de prueba, reconociendo que su validez se encuentra sujeta a que pueda comprobarse su autenticidad. La resolución considera que frente a un documento con firma electrónica la prueba deberá ser ponderada en función de las reglas de la sana crítica racional y según si ha sido o no reconocido por la parte en contra de quien se presenta, y en caso de haber sido impugnada, en correlación con el resto del material probatorio arrimado[128].

Aun así, frente a escasa jurisprudencia, resaltamos la importancia del ya mencionado art. 319 CCCN, que entre las pautas a tener en cuenta para valorar la prueba, se destacan dos que podrían tener especial incidencia en nuestro caso: las relaciones precedentes; y la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen.

En cuanto a las relaciones precedentes, si las partes ya han estado interactuando a través de ciertas claves públicas entre ellas, y se les han atribuido eficacia a tales actos, mal pueden alegar luego el desconocimiento de la transacción impugnando su autoría. De

[128] Sentencia de la Cámara de Apelaciones en lo Civil y Comercial de Córdoba 60/2014, de 22 de mayo de 2014, en autos "Pisanu Juan Mauro C. Carteluz Srl. Ordinario. Otros. EXP N° 1642556/36".

esta manera, el juzgador podrá considerar probada la autoría frente a la existencia de transacciones anteriores que las partes hubieren reconocido.

Asimismo, la robustez de la cadena y de todos los procedimientos técnicos que garantizan su funcionamiento, servirán como pauta de apreciación. A tal fin, y en lo que refiere a la identidad, si la implementación concreta de esta tecnología cuenta con procedimientos robustos de identificación y autenticación que garanticen que quien intervino en la transacción es quien dice ser, posibilitará la formación de convicción por parte del juzgador respecto a la autoría del documento impugnado.

4. CONSIDERACIONES FINALES RELATIVAS A LA AUTORÍA

La *blockchain* utiliza un sistema de criptografía asimétrica que hace que las firmas utilizadas en una transacción sean equivalentes a una firma electrónica simple. Esta firma, que ante terceros es representada mediante la clave pública, otorga la certeza de que la transacción en cuestión ha sido realizada por el poseedor del par de llaves pública-privada.

No obstante, si bien se asegura la autoría de la transacción por parte de una identidad virtual, en el marco de un proceso judicial es necesario su vinculación con una identidad legal. En este punto se encuentra el mayor inconveniente, ya que dependerá en concreto de cada implementación de la cadena de bloques y el uso que haga de mecanismos de identificación y autenticación. En algunos casos estos procesos podrán estar integrados dentro del software que compone la red, pero en otros puede ser necesaria una labor investigativa más ardua. A tal fin se intentó demostrar que existen varias alternativas para lograr tal atribución, sin perjuicio de que al ser una tecnología en constante desarrollo esto pueda variar con el tiempo.

Asimismo, el eventual reconocimiento de la autoría será relativo a una determinada transacción en la *blockchain*, que no necesariamente implica el reconocimiento de la autoría de otro documento electrónico vinculado, aunque podrá ser utilizado como un elemento probatorio más.

Entendiendo la transacción como un documento electrónico, si este es reconocido en juicio la cuestión no ofrecerá mayores dificultades, ya que hará plena prueba en juicio. Ahora bien, ante una eventual impugnación deberán ser desplegados otros medios de prueba previstos por el ordenamiento, valorados conforme las reglas de la sana crítica.

Sin ánimos de efectuar una proposición *lege ferenda*, las dificultades probatorias podrían reducirse si esta tecnología fuera reconocida como un instrumento tal como la firma electrónica, cuando exista un procedimiento robusto de validación de identidad, equiparando la firma efectuada en la *blockchain* como una firma electrónica cualificada (en España) o digital (en Argentina).

V. LA INTEGRIDAD EN LA *BLOCKCHAIN*

1. PLANTEAMIENTO

Continuando con el análisis propuesto, entramos en otro de los presupuestos que hacen a la eficacia probatoria de un documento electrónico −junto con la autoría (tratada *supra*) y la licitud−, esto es, su integridad. Recordemos que esta característica es entendida como "la propiedad o característica consistente en que los datos (activo de información) no han sido alterados de manera no autorizada"[129].

En la cadena de bloques, su robustez técnica tiene la capacidad de garantizar la inmutabilidad de los datos en ella contenidos conforme lo visto en el apartado respectivo. Es momento de indagar un poco más acerca de cómo se asegura tal característica, que se asienta no solo en su propia estructura a través de un conjunto de bloques asociados criptográficamente, sino mediante la utilización de sellos de tiempo.

2. SELLO DE TIEMPO E INTEGRIDAD

Los denominados sellos de tiempo implican una "prueba de existencia", es decir, permiten demostrar que cierto conjunto de datos existía en un tiempo determinado. La integridad de un documento implica que este no ha sido manipulado desde un determinado tiempo y en la determinación de ese momento entran en juego estos sellos.

La tecnología de cadena de bloques utiliza sellos de tiempo o *timestamp* para determinar la fecha y hora de creación de cada bloque, lo que garantiza el buen funcionamiento de la red. No obstante, obtenemos como beneficio adicional la posibilidad de conocer el momento temporal en que se ha realizado determinada transacción, con las implicancias que veremos.

Si bien cada implementación de la cadena de bloques en particular puede tener diferencias, en general se inserta un sello de tiempo al momento de incorporar un bloque en la cadena. La mayoría de las redes utiliza una marca de tiempo bajo el sistema de medición Unix[130] junto al estándar de Tiempo Coordinado Universal. Para tomar la hora,

[129] Delgado Martín, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, 81.
[130] Esto es, que utiliza mediciones expresada en valores de milisegundos contados desde la medianoche UTC del 1 de enero de 1970. Por ejemplo, la marca UNIX "1626272716" equivale a esa cantidad de segundas ocurridos desde la fecha antes mencionada, que convertida al sistema UTC equivale al 14/07/2021 a las 11:25:16 (UTC-03:00).

generalmente se utiliza el horario informado por los nodos, aunque para evitar manipulaciones la red toma como tiempo a la media de las horas informadas por todos los nodos. De esta manera, si alguno intentase manipular un sello de tiempo, se detectaría la inconsistencia y se evitaría un sellado fraudulento. Sin embargo, aun así, pueden existir pequeñas variaciones, por lo que se considera que la precisión de un sello de tiempo varía según cada red en particular, que puede ser de más o menos dos horas en redes como la de Bitcoin o de más o menos 900 segundos en redes como la de Ethereum.

Aún a falta de una precisión exacta, el sello de tiempo puede dar fe sin lugar a duda del día en que se realizó la transacción, y respecto al horario, con una variación que será menor o mayor según el diseño de la red.

Es importante resaltar que, como regla, la hora del *timestamp* estará dada por el sellado del bloque y no por el momento en que se realizó la transacción, ni mucho menos por el de la creación de un documento a ella vinculado. Entonces, un sello de tiempo no necesariamente puede coincidir con la fecha de creación de un documento vinculado o en la hora de realización de la operación, sino que quedará plasmada la del sellado del bloque.

Existen otras soluciones que incluyen un sellado de tiempo más exacto, ya que es enviado como metadato junto con la transacción. De esta manera tendremos un sellado de tiempo del momento en que se envió la transacción, y otro al momento de sellado del bloque, aunque claro dependerá de la configuración específica de la red.

También hay implementaciones que utilizan sistemas descentralizados de sellado de tiempo, como ser *OpenTimestamps*, que es un proyecto *open source* que define una serie de reglas a seguir para la creación de sellos de tiempo que luego puedan ser verificados de forma independiente. Este sistema utiliza servidores de calendario y hace que el sellado de tiempo solo tome entre uno y dos segundos[131].

De esta manera, el sellado de tiempo proporcionado por la *blockchain* resulta una solución robusta y fiable para garantizar la fecha de una determinada transacción. Aunque

[131] Peter Todd, "OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin", *Blog*, 15 de septiembre de 2016, https://petertodd.org/2016/opentimestamps-announcement#evidence-authenticity (consultada el 01/06/2021).

cada implementación puede tener diferencias en cuanto a la exactitud, siempre se estará dentro de un margen aceptable y se garantizará que el sello estampado es fiable.

Una vez efectuada la operación y estampado el sello de tiempo, la propia estructura de la cadena garantizará la consecuente integridad de la información. Recordemos que cada bloque de la cadena contiene no solo el conjunto de transacciones junto al sello de tiempo y otros metadatos, sino que se conforma con el *hash* del bloque anterior. Así, cada bloque nuevo se irá encadenando al anterior gracias al uso de técnicas criptográficas, de modo tal que, si eventualmente se quisiera realizar una modificación a un bloque específico, por más mínima que sea, el *hash* resultante cambiará indefectiblemente. Entonces, ese bloque adulterado implicará un *hash* diferente que ya no coincidirá con el que poseía el bloque subsiguiente, produciéndose una ruptura en la cadena fácil de detectar.

Ello podemos ejemplificarlo de a la siguiente manera: pensemos que el párrafo anterior está compuesto por una serie de oraciones (transacciones), las que en su individualidad poseen cada una un *hash* distinto. Sobre la totalidad de estos *hashes*, se aplicará nuevamente la función criptográfica por lo que obtendremos un nuevo *hash* que equivaldrá a la suma de todas las oraciones (párrafo completo)[132]. Ese número obtenido pasará a formar parte del párrafo subsiguiente (un nuevo bloque) y se complementará con el resto de las oraciones adicionadas, que poseen cada una también su respectivo *hash*. De todo este conjunto (*hash* del párrafo anterior, más *hash* de cada oración) obtendremos un nuevo hash que corresponderá a ese nuevo párrafo, y así ocurrirá sucesivamente en los nuevos párrafos creados.

Siguiendo el ejemplo anterior, si alguien intentara efectuar una modificación en una de las oraciones del primer párrafo, como borrar solo una letra, el *hash* resultante de esa oración se modificará, lo que producirá que el *hash* del párrafo también cambie por haber variado uno de sus datos de entrada (el valor de una oración). De esta manera el valor *hash* obtenido del primer párrafo ya no coincidirá con el valor criptográfico que poseía el segundo párrafo, y tal ruptura se replicará en todas las instancias subsiguientes por haber modificado tan solo una letra.

[132] Si bien su funcionamiento es algo más complejo que el ejemplo dado, esto se conoce como "árbol de merkle", que permite asociar numerosas transacciones en un único *hash*.

Por todo ello cualquier intento de modificación en la cadena de un nodo será fácilmente detectable y podrá ser subsanado, ya que habrá tantas copias íntegras de la cadena de bloques como nodos haya.

Por todo lo explicado, el sellado de tiempo sumado a la característica de inmutabilidad de los datos que ofrece esta tecnología nos permitirá probar que una determinada transacción fue efectuada en un momento determinado y que desde ese entonces tal registro no se ha modificado. Tal efecto recaerá no solo sobre la transacción en sí, sino que se trasladará sobre los documentos electrónicos asociados a dicha transacción mediante un *hash*. Ello porque ese *hash* también quedará vinculado a un momento de creación específico, y de la comparación con el *hash* actual del documento en cuestión, será fácilmente comprobable que no ha sufrido modificaciones si el resultado del algoritmo es idéntico. Por todo ello, la *blockchain* facilita la prueba de existencia y de inmutabilidad de las transacciones y documentos electrónicos a ella vinculadas.

Para continuar ejemplificando la cuestión sobre un documento específico, considérese el caso de BFA, que ofrece un sistema de sellado de tiempo abierto y gratuito, que opera en la tecnología *blockchain*, y funciona de la siguiente manera:

1. En el apartado de sellado de tiempo de la BFA (https://bfa.ar/sello2#/) se efectúa la carga del documento que se desea sellar;

2. A este documento se le aplica una función criptográfica (SHA256) y se obtiene su identificador único (*hash*);

3. Este *hash* se envía a un *smart contract* que lo almacena en al *blockchain* junto con determinados metadatos, incluido el sello de tiempo.

4. Finalmente cualquier persona puede verificar mediante el *hash* del archivo si se encuentra en la cadena de bloques y con qué fecha. En caso positivo devolverá la información con los datos del sello de tiempo, número de bloque, entre otros[133].

Por ejemplo, si a una versión preliminar de este trabajo (identificado con el *hash* *acf7aee6df20b441a1ce4eec0b391306130a4af5cc759960da4ecee1920700ae* utilizando el algoritmo SHA256 sobre el documento) quisiéramos hacerle un sello de tiempo,

[133] Para mayor claridad se puede observar el siguiente gráfico: "Sello de tiempo", Blockchain Federal Argentina, https://bfa.ar/sites/default/files/inline-images/Sello_1.png (consultada el 19/06/2021).

seguiríamos los pasos descritos para generar una transacción que quede sellada en un bloque de la cadena.

Si luego quisiéramos demostrar la existencia de tal versión con, debemos primero tener a mano el documento y aplicarle nuevamente el algoritmo SHA256 para obtener el *hash*. Con ese número podemos ingresar a la interfaz de verificación de la BFA adicionando a la dirección https://bfa.ar/sello2#/hash/ el hash de nuestro archivo, obteniendo así el siguiente enlace[134]: https://bfa.ar/sello2#/hash/acf7aee6df20b441a1ce4eec0b391306130a4af5cc759960da4ecee1920700ae. Ingresando a dicha dirección obtendremos un comprobante que nos indicará que el documento se encuentra sellado por un determinado nodo en determinado bloque y en la fecha y hora indicada.

Con ello comprobamos fácilmente dos cosas: que el *hash* del documento integra una transacción de la cadena de bloques; y el sello de tiempo asociado a dicha transacción. Así, se demuestra la existencia de ese documento y que este no se ha alterado desde entonces. Claro que esto representa una interfaz que simplifica la verificación, pero llegaríamos a idéntico resultado de un análisis minucioso de la red, como por ejemplo mediante una pericial, conforme veremos.

2.1. VALIDEZ LEGAL DEL SELLO DE TIEMPO

Dado que el sello de tiempo utilizado por esta tecnología implica la concatenación de datos electrónicos vinculados con un instante concreto de manera tal que se prueba la existencia en un momento determinado, podemos subsumir los sellos utilizados, a los previstos por el art. 3.33 del Reglamento eIDAS. Afirmamos entonces que la *blockchain* utiliza sellos de tiempo simples[135].

En consecuencia, estos sellos de tiempo podrán ser admitidos como prueba en un juicio a tenor del art. 41.1 del Reglamento eIDAS. En su mérito, a pesar de que dicho sello no gozará de la presunción de exactitud del sello de tiempo cualificado, no le serán denegados sus efectos jurídicos ni su admisibilidad como prueba en juicio

[134] Otra opción es utilizar directamente la interfaz provista por BFA, subir nuevamente el documento y presionar "verificar".
[135] Acompañan esta tesitura: Ibáñez Jiménez, *Blockchain: Primeras cuestiones en el ordenamiento español*, 42-43 y Javier González Granado, "Eficacia probatoria de la *blockchain*. Criptografía y artículo 1227 del Código Civil", *Taller de Derechos*, 25 de abril de 2016, https://tallerdederechos.com/eficacia-probatoria-de-la-blockchain-criptografia-y-articulo-1227-del-codigo-civil/ (consultada el 20/06/2021).

Cabe aclarar que el sello de tiempo estampado a las transacciones en principio no podrá ser considerado cualificado, salvo que la implementación particular cumpla con todos los requisitos del art. 42 del Reglamento eIDAS. Si bien por lo expuesto puede deducirse que la cadena de bloques puede vincular de manera confiable la fecha y hora con los datos, eliminando la posibilidad de realizar modificaciones sin ser ello advertido, y que muchas de ellas utilicen una fuente de información temporal relacionada con el sistema de Tiempo Universal Coordinado, no siempre intervendrá una firma o sello electrónico avanzado conforme requiere el punto 1.c del referido artículo.

Respecto al ordenamiento argentino, los sellos de tiempo forman parte de la infraestructura de firma digital conforme se desprende de la Resolución E399/2016 del Ministerio de Modernización[136] y del Decreto 182/2019. Si un sello de tiempo es otorgado por una Autoridad de Sello de Tiempo (AST) debidamente autorizada por la Secretaría de Innovación Pública (antes Ministerio de modernización), este gozará de plena validez probatoria sobre la fecha y hora respecto a un documento digital que estuviere firmado digitalmente, o de cualquier otra instancia de su ciclo de vida (art. 38 del citado decreto).

Sin embargo, al día de la fecha no existe una reglamentación que permita el efectivo funcionamiento de las AST como terceros de confianza, por lo que en Argentina no existe ningún sellado de tiempo que implique un efecto jurídico específico y no existe regulación que siquiera mencione una clase de sellos de tiempo “simples”, como lo hace el reglamento eIDAS. Por ello deberemos estar a lo normado por el CPCC para la generalidad de la prueba, aunque a nuestro entender ello no obsta a que continuemos llamando a este atributo como sello de tiempo, sobre todo por existir una sólida construcción doctrinaria a su alrededor.

Al considerar que sello de tiempo utilizado es simple, este aportará prueba de que los datos existían en un momento determinado, en el ámbito español. Desde la perspectiva argentina, nada obsta a llegar a igual consideración a tenor del principio de libertad probatoria, aunque con las consideraciones que efectuaremos oportunamente. A partir de allí, la integridad estará dada por la propia estructura de la cadena de bloques que asegura la inmutabilidad de su contenido.

[136] Resolución E399/2016 del 05/10/2016 del Ministerio de Modernización, (Argentina: BORA, 07/10/2016).

3. PRUEBA DE LA INTEGRIDAD EN EL PROCESO CIVIL

Por lo antes visto, la cadena de bloques ofrece una prueba de existencia y de inmutabilidad, al menos desde el punto de vista técnico. Cabe ahora analizar algunas cuestiones vinculadas en relación con un litigio en sede civil.

La transacción, entendida como documento electrónico, será tratada en el proceso conforme lo prescripto para la prueba documental. La presentación en juicio de dicho documento estará orientada a probar que la transacción se realizó en un momento determinado y que tanto ella como los metadatos asociados no han sido modificados desde entonces.

Si lo que se desea probar es la integridad de un documento vinculado a la transacción mediante un *hash,* deberán ser presentados ambos documentos. En este último caso la transacción en la *blockchain* será agregada con el fin de demostrar la existencia e integridad de otro documento, mediante la comparación de los *hashes*. Por dar un ejemplo, si quisiéramos probar la integridad de un documento vinculado a una determinada transacción −y retomando el ejemplo del epígrafe anterior respecto a BFA−, deberíamos aportar el documento original (junto a su *hash*, que es fácilmente comprobable), así como otro documento electrónico que sería la transacción, que contiene, entre varias cosas, detalles del *hash* del primer documento y el sello de tiempo.

Respecto a la aportación antes mencionada, puede incorporarse el comprobante de la transacción (cuando la red emite tal constancia) o bien captura de pantalla de la constancia emitida o del detalle de la transacción. En este último caso, de ser posible, será conveniente aportar la dirección web específica donde se obtuvo la constancia u obra la transacción y sus detalles, como se ejemplificó con BFA. Cabe recordar que la aportación de captura de pantalla será posible a tenor del art. 268.2 LEC que permite aportar copia simple del documento privado que tendrá idénticos efectos a la original siempre que no sea controvertida por las demás partes. Recordemos también que ello es apoyado por jurisprudencia, que frente a supuestos similares, ha afirmado la validez de las impresiones extraídas de una base de datos de una de las partes[137].

[137] En tal sentido tenemos el Auto de la Audiencia Provincial de Barcelona (Sección 13) 6/2018, de 15 de enero de 2018, ponente Ilma. Maria del Pilar Ledesma Ibañez, f.j. 2°.

Un beneficio que presenta la cadena de bloques respecto a la aportación del documento, lo constituye su carácter inmutable. Frente a otros tipos de prueba electrónica, como puede ser una página web, las capturas de pantalla pueden no constituir un medio eficaz debido a su posibilidad de modificación, lo que obliga a recurrir a mecanismos para anticipar dicha prueba (recurrir a un servicio de confianza, a un notario, entre otros) con sus consecuentes costos. Con la *blockchain* podemos aportar con tranquilidad la captura de pantalla de la transacción, ya que su contenido se mantendrá inalterable y seguirá disponible en el caso de que deba ser objeto de práctica de otros medios de prueba[138].

Así las cosas, una vez presentados los documentos electrónicos en juicio por una de las partes, estos podrán ser reconocidos por la parte contra quien se presenta o ser impugnados.

En el ordenamiento español, al igual que lo reseñado al momento de hablar de la autenticidad, la fuerza probatoria del documento electrónico estará a lo dispuesto por el art. 326 LEC. Así, si el documento no es impugnado, hará plena prueba en el proceso. Ante una eventual impugnación de su integridad o precisión de fecha y hora, si no ha intervenido un tercero de confianza o lo hizo un servicio electrónico de confianza no cualificado, los aspectos controvertidos deberán ser probados por cualquier medio de prueba que se considere pertinente. A tal fin pueden utilizarse cualquiera de los medios de prueba contemplados por el art. 299.1 LEC.

Sobre la práctica de los medios propuestos, reiteramos que todo dependerá de la red en particular. Así, frente a una red de acceso público, tanto las partes, el juez o los peritos podrán verificar la información de manera sencilla. Frente a redes privadas, habrá que gestionar el acceso, aunque si una de las partes integra la red podrá ofrecer su nodo para la práctica de la prueba, ya que recordemos que cada nodo posee una copia íntegra de toda la información, aunque ello deberá hacerse en el contexto de la red.

Asimismo, la cadena de bloques ofrece otra ventaja: el mismo diseño de la red ofrece una garantía de inmutabilidad fácilmente comprobable que despeja dudas que surgen cuando se efectúa una comprobación sobre un sistema bajo exclusivo control de

[138] Aun así, esta seguridad tendrá algunas excepciones, sobre todo en implementaciones que no se encuentren consolidadas, que posean muy pocos nodos o que no tengan el carácter descentralizado que caracteriza esta tecnología. Frente a ello puede ser conveniente tomar alguna medida para asegurar la prueba.

una de las partes. En estos casos, siempre existe un riesgo inherente de modificación o supresión del contenido por encontrarse el contenido bajo su potestad, que se disipan con los mecanismos de seguridad criptográfica de la cadena de bloques, siempre que el nodo se inspeccione en el contexto de la red y no aislado de esta.

De los medios propuestos ante una impugnación, el medio de prueba por excelencia será el dictamen pericial, ya que dadas las características reseñadas de esta tecnología será muy factible que su práctica arroje los resultados esperados en cuanto a la integridad y determinación de fecha y hora. De modo orientativo, podrán ofrecerse los siguientes puntos de pericia: (1) que estamos frente una red considerada *blockchain*[139], cuyo diseño asegura la inmutabilidad de los datos; (2) qué tipo de sello de tiempo utiliza la red y su grado de confiabilidad, esto implica conocer la fuente de fecha y hora utilizada, y el mecanismo mediante el cual se estampa el sello de tiempo; (3) si el documento electrónico en cuestión (sea la transacción o vinculado mediante el *hash*) integra un determinado bloque y su detalle; y (4) finalmente cuál es el horario estampado en el bloque (o en la transacción si fuere el caso) expresado según el sistema UTC.

Según la relativa facilidad de cada red para validar datos, también podría ser posible la realización de un reconocimiento judicial. Así como se admite que el juez pueda examinar por sí mismo una página web, no existe óbice para que también pueda corroborar la existencia de una determinada transacción o documento a ella vinculado en la *blockchain*, contrastando su hash, fecha, hora y demás datos, sobre todo en aquellas redes que ofrecen una interfaz simple e intuitiva para tal verificación como lo es BFA.

Una vez practicada la prueba, cada medio deberá ser valorado según lo prescrito. En el caso de la pericial, siendo el que se utilizará con mayor frecuencia, el dictamen será valorado conforme las reglas de la sana crítica (art. 348 LEC). De igual manera, consideramos que la robustez de la tecnología −conforme lo reseñado− otorga grandes chances de que la comprobación de la integridad del documento junto con la precisión de fecha y hora resulte claramente determinada, otorgando al juez la suficiente convicción en tal punto.

[139] Para determinar si estamos ante un registro distribuido (DLT) o específicamente una *blockchain* pueden resultar útil determinar si cumplen con determinadas reglas del Organismo de Normalización en España (normas UNE) o normas ISO que determinan los requisitos para la estructura de estas redes.

Posicionándonos ahora en el ordenamiento cordobés, la ley procesal no contiene ningún tipo de regulación que haga especial referencia a los documentos electrónicos y a sus particularidades en lo que a obtención, impugnación o valoración se refiere. Si bien respecto a la autenticidad, las leyes reguladoras de la firma digital o el nuevo CCCN hacen alguna mención, en lo relativo a las demás características del documento electrónico no existen pautas específicas.

Aun así, y a tenor de lo sostenido en los apartados respectivos, el documento en cuestión ingresará al proceso siguiendo el cauce establecido para el medio de prueba documental.

Presentado el documento electrónico, su eficacia dependerá de su reconocimiento por la persona contra quien es presentado o por una declaración en este sentido por parte del tribunal (art. 248 CPCC). Este reconocimiento puede ser expreso o tácito (art. 192, 197 y 243 CPCC; art. 314 CCCN). Si bien el art. 192 CPCC establece que frente su presentación, la contraparte deberá "reconocer o negar categóricamente la autenticidad de los documentos acompañados (…) bajo pena de tenerlos por reconocidos o recibidos, según el caso", entendemos que tal reconocimiento abarca también lo relativo a la integridad o precisión de fecha y hora.

Respecto a la aportación, se deberán seguir idénticas pautas a las antes brindadas para el caso del ordenamiento español. La incorporación de capturas de pantalla también se encuentra permitida por tratarse de una copia simple del documento (art. 87 CPCC), aspecto relativamente pacífico en la doctrina respecto al resto de los documentos electrónicos[140].

A diferencia de la LEC, en el CPCC no existe mención que aluda a una eventual impugnación de la integridad o precisión de fecha y hora de un documento electrónico. A pesar de ello, el momento para impugnar será el establecido para el medio de prueba documental, esto es, en la contestación de la demanda, de la reconvención, o cuando se diere traslado de nuevos documentos.

Impugnada la integridad o precisión de fecha y hora del documento electrónico, la cuestión deberá ser probada por cualquier otro medio de prueba, a cargo de quien aduce la característica impugnada. La doctrina sostiene que la prueba sobre estos aspectos del

[140] Zalazar y Abellaneda, *Sistema probatorio en el proceso civil de Córdoba*, 444.

documento electrónico solo procederá cuando sean desconocidos, en cuyo caso se ofrecerán todos los medios de prueba regulados por el ordenamiento y que se considere pertinentes[141].

No obstante, la falta de regulación procesal sobre estos aspectos y la ausencia de jurisprudencia específica hace que deban tomarse la mayor cantidad de recaudos posibles. Es consecuencia es recomendable que, junto con la presentación del documento, se ofrezcan de manera subsidiaria otros medios de prueba que puedan resultar pertinentes para, ante una eventual impugnación, dotar de certeza las características objetadas.

En definitiva, frente a la impugnación del documento electrónico, deberán ser propuestos los medios de prueba que se estimen útiles y pertinentes por quien pretende probar este extremo. En este punto se tornan aplicables las mismas consideraciones efectuadas respecto al ordenamiento español, en cuanto al acceso a la *blockchain* para la práctica de la prueba, la importancia del dictamen pericial, la proposición de determinados puntos de pericia y la posibilidad de realizar de un reconocimiento judicial.

Una vez diligenciados los medios de prueba propuestos, la prueba será valorada conforme las reglas de la sana crítica, salvo disposición legal en contrario (art. 327 CPCC). Se introducen como pautas a considerar la conducta procesal de las partes (art. 316 CPCC), la posibilidad de apartarse del dictamen de los peritos (art. 252 CPCC), así como las ya mencionadas pautas de apreciación del art. 319 CCCN. Dentro de las pautas para determinar el valor probatorio de los instrumentos particulares que ofrece este último artículo se encuentra la "confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen", que tendrá especial relevancia en nuestro caso.

En virtud de estas últimas consideraciones, el carácter inmutable, descentralizado y fácilmente trazable de la *blockchain* contribuye a erradicar cualquier sospecha sobre la existencia e integridad de la transacción o de los documentos electrónicos asociada a ella.

Una eventual impugnación deberá tratar de poner en duda la confiabilidad de los soportes utilizados, así como de aquellos procedimientos técnicos que se apliquen. No obstante, frente a un documento registrado en la cadena de bloques nos encontraremos en una posición mucho más favorable con motivo de la tecnología que la sustenta.

[141] Zalazar y Abellaneda, 444-45.

Un caso común en los tribunales y donde esta tecnología podría facilitar la prueba, es en aquellos supuestos en que la práctica de la prueba deba efectuarse sobre sistemas que están bajo control de una de las partes que alega la prueba. Frente a estos casos, la jurisprudencia siempre ha sido cauta al afirmar que la eficacia probatoria debe ser ponderada según los mecanismos de seguridad utilizados por dichos sistemas, que garantizasen la autoría e integridad de los documentos contenidos. Ello porque en estos casos, al ser el sistema de uso exclusivo de la parte, siempre está latente la posibilidad de que se haya alterado la versión original del contenido, por lo que resulta de suma importancia la posibilidad de detectar la trazabilidad para garantizar procedencia y autenticidad[142].

Sostenemos entonces que la cadena de bloques, por la robustez y fiabilidad que implica, cumple con creces el umbral de confiabilidad necesario por el juez para formar su convicción respecto a la integridad y precisión de fecha y hora del documento electrónico vinculado.

3.1. Existencia e integridad del documento como hecho notorio

Algunos autores como Quadri[143] sostienen que en determinados casos no haría falta recurrir a otros medios de prueba, ya que el documento electrónico inserto en la *blockchain* constituiría un hecho notorio, por lo que el juez podría tenerlo por cierto sin siquiera necesidad de prueba. Ello por existir una gran cantidad de equipos informáticos (nodos) que permiten comprobar que el documento presentado en juicio corresponde con el almacenado en los bloques de la red, y que a su vez se mantuvo inmutable desde su incorporación.

Sobre la aseveración anterior debemos realizar algunos reparos. En primer lugar, no todas las redes *blockchain* se encuentran compuestas por miles de nodos, sino que todo dependerá del caso particular. En segundo lugar, existen dudas de que aun así, lo referido pueda constituirse como un hecho notorio.

En principio, para que un hecho sea considerado notorio no es necesario que absolutamente todos lo conozcan, ni que sea de carácter permanente, sino que debe ser

[142] Sentencia de la Cámara Nacional de Apelaciones en lo Comercial de Capital Federal (Sala A), de 22 de octubre de 2019, en autos "Prenaval Seguridad SRL c/ Consorcio de Propietarios Santos Dumont 2719/21/23/55 s/ ordinario".
[143] Gabriel H. Quadri, «Prueba informática: medios en particular», en *Tratado de Derecho Procesal Electrónico*, dir. Carlos Enrique Camps, 2ª ed. (Buenos Aires: Abeledo Perrot, 2019), 402-7.

de conocimiento público por parte de personas de cultura media dentro del medio social donde ha ocurrido o existe ese hecho[144]. No obstante, de la misma manera en que se ha considerado que el contenido de una página web puede resultar notorio para quienes acceden a ella regularmente pero no así para la sociedad en general, o que en todo caso puede resultar notoria su existencia (como el caso de conocidos buscadores) pero no así su contenido[145], podemos derivar a la misma conclusión con la cadena de bloques: aunque pueda considerarse la existencia de la *blockchain* como un hecho notorio (o al menos así podrá serlo en unos años dado se creciente evolución), no puede considerarse de tal manera al contenido en ella inserto.

De las características explicadas, y dado el carácter novedoso de esta tecnología, sostenemos que los documentos o transacciones obrantes en la *blockchain* no adquieren el carácter de notorio conforme el 281.4 LEC ni según el ordenamiento argentino.

3.2. Atribución de fecha cierta

Con lo analizado hasta el momento surge un nuevo interrogante, acerca de si es posible equiparar el sellado de tiempo provisto por la cadena de bloques a la fecha cierta regulada por la normativa. Si bien este es un tema puntual que excede el marco de este trabajo, consideramos pertinente efectuar unas breves consideraciones dada la relación suscitada y dejar el interrogante sentado para un futuro trabajo.

La fecha cierta puede definirse como "aquella que otorga certeza de que el instrumento privado ya estaba firmado al momento de su producción, o no pudo ser firmado después de su acaecimiento"[146].

En el ordenamiento español la fecha cierta está contemplada en el art. 1227 del Código Civil. A grandes rasgos parecería que la norma es bastante restrictiva en lo que respecta a la acreditación de la fecha cierta, por cuanto esta solo procederá desde que el documento privado hubiera sido incorporado o inscripto en un registro público, desde la muerte de algún firmante o desde su entrega a un funcionario público con motivo de su oficio.

[144] Devis Echandia, *Teoría General de la Prueba Judicial*, I:113-14.
[145] Vicente Pérez Daudí, «Prueba electrónica y hecho notorio.», en *La prueba electrónica*, dir. Xavier Abel Lluch y Joan Picó i Junoy (Barcelona: J.M. Bosch Editor, 2011), 461.
[146] Julio César Rivera y Graciela Medina, *Código Civil y Comercial de la Nación Comentado*, vol. I (Buenos Aires: La Ley, 2014), 422.

Sobre este punto, Ibáñez Jiménez[147] sostiene que, frente a un documento privado, y siempre que la cadena de bloques no haya sido reconocida oficialmente como registro público oficial, su registro no produce los efectos de la constitución de fecha cierta oponible a terceros conforme establece el art. 1227 del Código Civil.

No obstante, muchas veces se ha puesto en duda el carácter *numerus clausus* del referido precepto. En este sentido, existe jurisprudencia que ha interpretado este artículo en relación con la libertad probatoria prevista en el art. 24.2 de la Constitución Española, considerando que la fecha cierta puede ser probada por otros medios, expresando en relación con el art. 1227 del Código Civil que "…tal precepto ha de interpretarse en sentido amplio, de modo que pueda estarse a la fecha del documento privado, siempre que la misma pueda acreditarse por otros medios de prueba admitidos en derecho[148]. También otras resoluciones han enunciado el carácter subsidiario de la norma en cuanto admiten que la veracidad de una fecha es admisible desde que pueda comprobarse en relación con otros actos que despejen cualquier duda de falsedad o simulación, y que han sostenido que "probada la autenticidad y certeza del documento, la fecha ha de tenerse por cierta para las partes y erga omnes"[149].

En el ordenamiento argentino la fecha cierta estará dada desde "el día en que acontece un hecho del que resulta como consecuencia ineludible que el documento ya estaba firmado o no pudo ser firmado después" (art. 317 CCCN). El mismo precepto establece que esta fecha podrá ser probada por cualquier medio, aunque deberá seguirse un estándar de apreciación riguroso por parte del juez sobre este punto.

Conforme la normativa reseñada, en principio el sello de tiempo no equivale necesariamente a fecha cierta. No obstante, la tecnología en la que se funda el *timestamp* basado en la *blockchain*, otorga robustez que puede servir como base a que a futuro pueda llegar a darse tal consideración en un caso concreto, aunque siempre bajo un estándar de

[147] Ibáñez Jiménez, *Blockchain: Primeras cuestiones en el ordenamiento español*, 41.
[148] Sentencia del Tribunal Superior de Justicia de Canarias (Sala de lo Contencioso) 420/2009, de 01 de septiembre de 2009, ponente Ilmo. Sr. Francisco Javier Varona Gómez-Acedo, f.j. 3°; que asimismo hace referencia a diversas resoluciones en idéntico sentido.
[149] Sentencia de Tribunal Supremo (Sala de lo Civil) 492/2006, de 23 de mayo de 2006, ponente Ilmo. Sr. Vicente Luis Montes Penades, f.j. 3°.

apreciación riguroso. Desde la perspectiva del ordenamiento español abona esta conclusión González Granado[150].

3.3. JURISPRUDENCIA EN EL DERECHO COMPARADO

Si bien ya hemos adelantado que no existe por el momento jurisprudencia específica de la temática analizada en España o Argentina, en la búsqueda hallamos algunos casos interesantes relacionados con la integridad (no así respecto a la autoría), en países distintos de los que son objeto de este trabajo. Si bien ello excede la presente investigación, consideramos útil e interesante hacer una breve reseña de alguna de estas resoluciones, sobre todo para aportar una mirada desde la jurisprudencia en el derecho comparado.

A nivel jurisprudencial ya son varios los casos que han otorgado a la cadena de bloques aptitud para probar la validez de los registros en ella incorporados.

En 2018, el Tribunal de Internet de Hangzhou de China, resolvió en el caso "Hangzhou Huatai Media Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co" atribuir eficacia probatoria a un conjunto de datos cuyo *hash* obraba en la cadena de bloques. El Tribunal afirmó que la tecnología *blockchain*, por el carácter distribuido de la información almacenada, los mecanismos utilizados para evitar manipulaciones y la posibilidad de verificar la trazabilidad, aporta ventajas en la fijación, preservación y extracción de evidencia electrónica. Ponderando esas características en el caso concreto, atribuyó plena eficacia probatoria a los datos ingresados en la cadena de bloques, en cuanto a su existencia en determinado momento e integridad[151].

---

[150] Para este autor, la cadena de bloques no atribuye de manera directa y automática la fecha cierta, sino que es necesario que concurran algunos requisitos: "1º) Ha de tratarse de un verdadero documento contractual, no de un simple proyecto, borrador, memorándum, declaración de intenciones o meras ofertas. 2º) Ha de estar firmado y en el ámbito digital es la firma electrónica cualificada (reconocida, en la terminología anterior) la que según el Reglamento 910/2014 tendrá un efecto jurídico equivalente al de una firma manuscrita. Cualquier otra marca, huella, o sello digital solo tendrán valor probatorio pleno si van acompañadas del oportuno dictamen pericial informático. 3º) Tratándose de contratos traslativos, ha acreditar no solo la existencia del contrato sino también la transmisión de la propiedad. En, efecto rige en nuestro Derecho la teoría del título y el modo; si no se acredita la entrega no puede iniciarse el plazo de prescripción del impuesto. La entrega puede ser material (algo que no se puede acreditar en el documento) o instrumental (la que realiza la escritura pública ex artículo 1462. 2 Código Civil). El documento privado nunca tiene ese efecto", Javier González Granado, "Eficacia probatoria de la blockchain. Criptografía y artículo 1227 del Código Civil", *Taller de Derechos*, 25 de abril de 2016, https://tallerdederechos.com/eficacia-probatoria-de-la-blockchain-criptografia-y-articulo-1227-del-codigo-civil/ (consultada el 20/06/2021).

[151] Sentencia de la Hangzhou Internet Court of the People's Republic of China, 27 June 2018, Hangzhou Huatai Media Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd. Case n° 055078 (2018) Zhe 0192 First Court No. 81.

Chomczyk[152] efectúa un análisis de este fallo y resume la consideración efectuada por el Tribunal sobre el mecanismo utilizado por la tecnología para preservar la integridad de la prueba, a saber: 1. la fecha cierta que se encuentra asociada al *hash* de un documento permite afirmar que este documento existía, como mínimo, desde la fecha registrada por el bloque que contiene dicha transacción; y 2. las tecnologías involucradas "no deberían descartarse o el estándar de determinación de las mismas no debería plantearse porque actualmente son medios técnicos novedosos y complejos, ni el estándar de determinación de los mismos debería reducirse porque es difícil alterar o eliminar la tecnología". En el caso, otro elemento que se tuvo en cuenta fue el hecho que intervino un tercero imparcial en la generación de la prueba digital e incorporación a la cadena de bloques.

El autor reseñado concluye que los jueces debieron resolver aplicando derecho común y no normativa específica para esta tecnología, lo que demuestra que de obtenerse un convencimiento de que la plataforma usada para la preservación es imparcial, no hay porqué denegar la admisibilidad de la prueba solo por la tecnología subyacente utilizada, esto es, la *blockchain*.

Otro pronunciamiento que puede traerse a colación es el dictado en 2019 por un Tribunal de San Pablo, Brasil[153], en donde se negó una medida cautelar de aseguramiento de la prueba, fundamentando −entre varias razones− que los datos ya se encontraban resguardados en una *blockchain*, que es hábil para comprobar la veracidad y existencia de los contenidos. Si bien el fallo es sumamente escueto, permite vislumbrar que poco a poco los jueces se inclinan más por asignar eficacia probatoria a aquellos documentos en los que se ha incluido la cadena de bloques como mecanismo de preservación.

5. Consideraciones finales relativas a la integridad

Mediante la utilización de un protocolo robusto que implica la utilización de criptografía y sellos de tiempo, la cadena de bloques asegura la integridad de los datos en ella contenidos. La conjunción de esta tecnología asegura una "prueba de existencia",

[152] Andrés Chomczyk, «Blockchain y evidencia digital: una aproximación desde el derecho argentino», en *Contract management*, comp. Ricardo Antonio Parada y José Daniel Errecaborde (Buenos Aires: Erreius, 2019), 22-23.
[153] Acórdão do Tribunal de Justiça de São Paulo (5ª Câmara de direito privado), Brasil, Agravo de Instrumento N° 2237253-77.2018.8.26.0000 de 19 de dezembro de 2018, relatora Fernanda Gomes Camacho.

esto es, que determinada transacción, o los datos a ella vinculados, existían en un tiempo determinado y que desde ese entonces no han sido modificados.

En la mayoría de los casos el sellado de tiempo se realiza al momento de sellar un nuevo bloque, por lo que la mayor o menor exactitud de la hora estará dada por la velocidad del protocolo específico en el minado de los bloques. Aun así, esta variación será como mucho de algunas horas, lo que no le resta utilidad como prueba, salvo en algún caso puntual en que sea necesaria una precisión de minutos para dirimir un conflicto. Asimismo, existen otras implementaciones adicionales que añaden el sello de tiempo como metadato al momento de enviar una operación, o que utilizan el servicio de servidores externos confiables de calendario que agregan aún más exactitud al sello de tiempo.

En la legislación española, podemos considerar que esta tecnología utiliza sellos de tiempo simples cuyos efectos jurídicos o admisibilidad como prueba en juicio no le podrán ser denegados (art. 41.1 Reglamento eIDAS). Aun así, frente a una eventual impugnación del documento en cuestión, la carga de la prueba estará en cabeza de quien asegure ese atributo, pudiendo utilizar todos los medios de prueba que considere pertinentes.

En el ordenamiento argentino, solo están previstos los sellos de tiempo suministrados por Autoridades de Sello de Tiempo debidamente autorizadas, aunque en la práctica al día de la fecha esta figura no se encuentra implementada. Tampoco existe una norma equivalente al art. 41.1 del Reglamento eIDAS que refiera a los efectos jurídicos de sellos de tiempo efectuados por fuera de los servicios de confianza. A pesar de ello consideramos que en virtud del principio de libertad probatoria estos extremos podrán ser invocados en juicio y de no ser desconocidos harán plena prueba. Frente a una impugnación, y a falta de regulación específica, quien alega la fecha y hora y la integridad del documento deberá probarlo por cualquiera de los medios de prueba previstos.

En cualquiera de los ordenamientos, y por la robustez de la tecnología subyacente en la cadena de bloques, consideramos que frente a una impugnación, un dictamen pericial podrá demostrar con relativa facilidad que una determinada transacción o documento a ella vinculado mediante *hash,* existían desde un tiempo determinado y que desde ese entonces no han sufrido modificaciones.

Aún frente a otros medios de prueba, dada la robustez de la tecnología interviniente, creemos que la *blockchain* aportará la convicción suficiente al juzgador para que, en uso de las reglas de la sana crítica, otorgue plena eficacia probatoria a un documento ingresado en la red, en lo que respecta a la determinación de su fecha y hora e integridad.

VI. CONCLUSIONES

Una vez desarrollado todo el trabajo de investigación pasamos a enumerar las siguientes conclusiones alcanzadas:

PRIMERA. Ni la LEC ni el CPCC otorgan una definición concreta de lo que se entiende por prueba electrónica, por lo que es necesario recurrir a la doctrina científica para determinar su concepto. Pese a ello, la LEC parece establecer una regulación autónoma a través de los art. 299 y 382 a 384; mientras que el CPCC no contiene ninguna regulación en este sentido. Aun así, ambos ordenamientos prevén la posibilidad de incorporar nuevas fuentes de prueba, entre las que pueden considerarse las electrónicas, haciendo eco de la garantía constitucional de libertad probatoria. Por todo ello, no existe óbice para que las nuevas fuentes de prueba producidas por el avance tecnológico, como podría ser la *blockchain*, puedan incorporarse al proceso en ambas regulaciones procesales.

SEGUNDA. Respecto al documento electrónico, en ambos ordenamientos es viable su admisibilidad como prueba en juicio, aunque existen algunas diferencias. En España, la LEC reguló de manera separada el documento (entendido como tradicional) y el documento electrónico, aunque tal separación ha quedado diluida a tenor de posteriores reformas a la norma procesal, por regulaciones extraprocesales y aún por reciente jurisprudencia del Tribunal Supremo, por lo que frente a un documento electrónico deberá seguirse en primera medida lo dispuesto para el medio de prueba documental. En Argentina, por su parte, se entiende al documento electrónico como una especie del documento, por lo que, a falta de previsión específica en el CPCC de Córdoba, la documental electrónica como fuente de prueba debe seguir el cauce del medio probatorio documental. Por último, en ambos ordenamientos la autenticidad e integridad de un documento electrónico constituyen presupuestos de su eficacia probatoria.

En referencia a la firma electrónica, como instrumento tecnológico que permite garantizar la autoría de un documento, en ambos países existe regulación al respecto, aunque con diferencias en su denominación y clasificación. Mientras que en España existe la firma electrónica simple, avanzada o cualificada; en Argentina se diferencia la firma electrónica de la digital, siendo la primera equivalente a una firma electrónica simple y la segunda a una cualificada.

TERCERA. Del relevamiento efectuado, no se encontró regulación normativa que incida sobre aspectos legales de la *blockchain* vinculados a la autoría e integridad. En lo que a la jurisprudencia se refiere, ni en España ni en Argentina existen pronunciamientos relevantes en la temática por parte de los tribunales relativos a esos aspectos.

CUARTA. La *blockchain* debe ser considerada como fuente y no como medio de prueba. Entendida en su conjunto no puede ser considerada como documento electrónico, sino que tendrán tal consideración los datos en ella contenidos. Así, sostenemos que el comprobante de una transacción realizada en la red debe tener la consideración de documento electrónico. Es por ello que su ingreso, tratamiento y demás cuestiones en el proceso seguirán lo prescrito para el medio de prueba documental.

QUINTA. En lo que respecta a la autoría, esta tecnología permite −mediante su robusto sistema de criptografía asimétrica− asegurar que cada transacción solo puede ser realizada por el poseedor del conjunto de llaves público-privada. Esto nos lleva a afirmar que cualquier transacción debidamente registrada en la red, fue ejecutada por el poseedor de dichas llaves, identificado mediante la llave pública interviniente. Así, la infraestructura de llave pública que utiliza esta tecnología nos permite llegar a la conclusión de que la firma utilizada para realizar la transacción en la cadena puede ser considerada una firma electrónica simple (en España) o una firma electrónica (en Argentina), ya que implica el uso de datos electrónicos asociados de manera lógica utilizados por el firmante como medio de identificación, conforme lo requiere la normativa.

Esta llave pública está vinculada a una identidad virtual, que en el marco de un proceso judicial debe necesariamente vincularse a una identidad legal. Es en este punto donde la *blockchain* generalmente no ofrece una solución satisfactoria por sí misma, sino que es necesario acudir a otros elementos. En concreto habrá que estarse a la implementación específica de esta tecnología, en cuanto puede prever mecanismos que permitan una identificación y autenticación fehaciente de sus intervinientes, que permitan asociar una clave pública a una identidad real. Si la red no cumple tal aspecto, lo que será común en las *blockchain* públicas, esta no será de utilidad para el fin propuesto, esto es, determinar la autoría de una determinada transacción por parte de un individuo específico. Se destaca entonces la importancia de la labor investigativa de los abogados en el marco

de un proceso civil, quienes frente a los desafíos propuestos deberán recabar toda la información necesaria para formar la convicción del juzgador en este punto.

Ante una eventual impugnación de la autoría, la carga de la prueba estará en cabeza de quien alega tal extremo. Si bien la tecnología utilizada asegura que la transacción fue realizada y firmada electrónicamente por el poseedor del par de llaves, que es identificado mediante su clave pública, deberá acreditarse la asociación de dicha clave a una identidad legal. A tal fin tendrá a su disposición todos los medios de prueba previstos por el ordenamiento que considere pertinentes, que serán valorados por el juez conforme las reglas de la sana crítica y demás pautas establecidas por la normativa aplicable.

SEXTA. Ahora bien, consideramos que el punto más fuerte de la *blockchain* es su utilidad para determinar la integridad de un documento electrónico. La solidez técnica de esta tecnología, que incluye desde el uso de criptografía hasta sellos de tiempo, permite acreditar que una determinada transacción (o un documento asociado a ella mediante un *hash*) existió en un momento determinado y que desde entonces no ha sufrido alteraciones. No obstante, a falta de regulación normativa o de jurisprudencia específica del tema, tal atributo no constituye una presunción ni genera efectos jurídicos por sí misma.

El sello de tiempo utilizado por esta tecnología puede considerarse “simple” en España a tenor del Reglamento eIDAS, por lo que no se le deben denegar efectos jurídicos y es viable su utilización como prueba en juicio. En contraposición, en Argentina no están previstos sellos de tiempo por fuera del otorgado como servicio de confianza debidamente autorizado, pero ello no obsta a que tal atributo sea alegado en juicio conforme el principio de libertad probatoria. Así las cosas, en ambas legislaciones, si la integridad o precisión de fecha de un documento no es impugnada, hará plena prueba en juicio. Frente a una impugnación, dicho extremo podrá ser probado utilizando cualquiera de los medios de prueba previstos y el juzgador resolverá aplicando las reglas de la sana crítica. Aun así, consideramos que mediante un dictamen pericial podrá obtenerse certeza acerca de la fecha y hora de creación (con diferente grado de exactitud según el caso) y el carácter inalterado del documento en cuestión.

Por todo lo visto, sostenemos que la *blockchain* garantiza la integridad de los datos en ella contenidos, desde la fecha de su incorporación y su consecuente estampado de sello de tiempo, hasta el momento de valoración de la prueba, e incluso más allá de eso.

SÉPTIMA. Finalmente, una vez dilucidadas las cuestiones objeto de la presente investigación, se evidencia que quedan algunos interrogantes abiertos. Por un lado, como consecuencia del efecto disruptivo que supuso la cadena de bloques, se originaron a partir de ella nuevos desarrollos innovadores, como los contratos inteligentes (*smart contracts)*, la llamada justicia descentralizada o proyectos de identidad auto soberana, los que pueden tener especial incidencia en el derecho y necesitan de un estudio separado y particularizado. Por otro lado, dado que la casuística es muy amplia, se abordó el objeto de investigación desde un enfoque generalizado, lo que puede derivar que, en un caso concreto, sea necesario poner lo analizado en relación con otra normativa. Así, frente a un pleito que involucre propiedad intelectual, contratación en línea, etc., también deberán tenerse en cuenta aquellas leyes especiales que rigen cada materia, para poder determinar la efectiva incidencia de la cadena de bloques.

A pesar de lo antes dicho, creemos que una vez comprendida la esencia de esta tecnología y su incidencia en dos aspectos tan relevantes que hacen a la eficacia probatoria de los documentos electrónicos, tal como la autoría e integridad, es posible continuar con el desarrollo de todas aquellas otras interrogantes que se nos plantean. Ello con el fin de determinar la cabal incidencia de la *blockchain* y sus derivaciones sobre todas las aristas procesales y probatorias que pueden darse en el marco de un proceso judicial.

VII. REFERENCIAS

1. BIBLIOGRAFÍA

Abel Lluch, Xavier. «La impugnación de la prueba electrónica». *Justicia: revista de derecho procesal*, n.º 1 (2019): 217-66.

———. «Prueba electrónica». En *La prueba electrónica*, dirigido por Xavier Abel Lluch y Joan Picó i Junoy, 21-230. Barcelona: J.M. Bosch Editor, 2011.

Allende López, Marcos. *Identidad digital auto-soberana: El futuro de la identidad digital: Auto-soberanía, billeteras digitales y blockchain*. Banco Interamericano de Desarrollo, 2020. https://doi.org/10.18235/0002635.

Anderson, Ross J. «The Eternity Service». En *Cambridge University Computer Laboratory*, 1996.

Anguiano Jiménez, José Maria, y Ángel López Pérez. «Retos jurídicos ante la transformación digital». *Diario La Ley*, n.º 9011 (2017).

Barrio Andrés, Moisés. «Concepto y clases de criptoactivos». En *Criptoactivos. Retos y desafíos normativos*, dirigido por Moisés Barrio Andrés, 37-62. Madrid: Wolters Kluwer, 2021.

Beltran Avila, Diego. «Derecho a la presunción de inocencia en el proceso penal: valor probatorio de la blockchain». *Revista de Direito Brasileira* 25, n.º 10 (2020): 307-20. http://dx.doi.org/10.26668/IndexLawJournals/2358-1352/2020.v25i10.6146.

Bielli, Gastón Enrique, y Carlos Jonathan Ordoñez. *Contratos electrónicos: teoría general y cuestiones procesales*. Vol. I. Buenos Aires: La Ley, 2020.

———. *La prueba electrónica: teoría y práctica*. Buenos Aires: La Ley, 2019.

Chomczyk, Andrés. «Blockchain y evidencia digital: una aproximación desde el derecho argentino». En *Contract management*, compilado por Ricardo Antonio Parada y José Daniel Errecaborde, 17-27. Buenos Aires: Erreius, 2019.

———. «El desafío de las identidades digitales para la industria fintech». En *Fintech: aspectos legales*, compilado por Pablo Andrés Palazzi y Santiago J. Mora, 225-41. Buenos Aires: Pablo Andrés Palazzi, 2019.

Delgado Martín, Joaquin. *Investigación tecnológica y prueba digital en todas las jurisdicciones*. 2ª ed. Madrid: Wolters Kluwer, 2018.

Devis Echandia, Hernando. *Teoría General de la Prueba Judicial*. Vol. I. Buenos Aires: Zavalía, 1970.

Fernández-Miranda Vidal, Fernando, Marta Llamazares Carreño, y Alba Carrasco Ventura. «Usos de la firma electrónica y sistemas de identificación electrónica en el entorno digital actual». En *Nuevas tecnologías 2021*, dirigido por Enrique Ortega Burgos, 294-312. Valencia: Tirant lo Blanch, 2021.

Granero, Horario R. «El expediente digital y la firma digital». En *Tratado de derecho procesal electrónico*, dirigido por Carlos Enrique Camps, 2ª ed., 485-566. Buenos Aires: Abeledo Perrot, 2019.

Haber, Stuart, y W. Scott Stornetta. «How to time-stamp a digital document». *Journal of Cryptology* 3 (enero de 1991): 99-111. https://doi.org/10.1007/BF00196791.

Ibáñez Jiménez, Javier Wenceslao. *Blockchain: Primeras cuestiones en el ordenamiento español*. Madrid: Dykinson, 2018.

———. «Blockchain y Legal Tech». En *Legal Tech: la transformación digital de la abogacía*, dirigido por Moisés Barrio Andrés, 89-108. Madrid: Wolters Kluwer, 2019.

———. «Cuestiones jurídicas en torno a la cadena de bloques (“blockchain”) y a los contratos inteligentes (“smart contracts”)». *Icade: Revista de la Facultad de Derecho*, n.º 101 (8 de febrero de 2018). https://doi.org/10.14422/icade.i101.y2017.003.

Kielmanovich, Jorge L. *Teoría de la prueba y medios probatorios*. 4ª ed. Santa Fe: Rubinzal Culzoni, 2010.

Mazières, David, y Dennis Shasha. «Building secure file systems out of byzantine storage». En *Proceedings of the twenty-first annual symposium on Principles of distributed computing - PODC ’02*, 108-17. New York, 2002. https://doi.org/10.1145/571825.571840.

Melo, Letícia. «Régimen jurídico de blockchain: una prueba atípica». *Revista de Bioética y Derecho*, n.º 46 (2019): 101-16. https://doi.org/10.1344/rbd2019.0.27071.

Molina Quiroga, Eduardo. «La prueba en medios digitales». *Micro Juris* (28 de octubre de 2013).

Mora, Santiago J. «La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso». *La Ley*, n.º 786 (2019).

Morales Barroso, José. «¿Qué es blockchain?» En *Criptoderecho. La regulación de Blockchain*, dirigido por Pablo García Mexía, 39-74. Madrid: Wolters Kluwer, 2018.

Navarro, Guillermo. «Blockchain y proceso electrónico». En *Tratado de Derecho Procesal Electrónico*, dirigido por Carlos Enrique Camps, 2ª ed., 793-817. Buenos Aires: Abeledo Perrot, 2019.

Ortiz Rodriguez, Carmen. «¿Cuándo un juez deja de creer en un dictámen pericial?» En *La prueba en acción. Estrategias procesales en materia probatoria. Libro en homenaje al profesor Lluis Muñoz Sabaté*, dirigido por Joan Picó i Junoy, 233-38. Barcelona: J.M. Bosch Editor, 2019.

Pérez Daudí, Vicente. «Prueba electrónica y hecho notorio.» En *La prueba electrónica*, dirigido por Xavier Abel Lluch y Joan Picó i Junoy, 455-61. Barcelona: J.M. Bosch Editor, 2011.

Picó i Junoy, Joan. *Las garantías constitucionales del proceso*. 2ª ed. Barcelona: J.M. Bosch Editor, 2012.

Pinto Palacios, Fernando, y Purificación Pujol Capilla. *La prueba en la era digital*. Madrid: Wolters Kluwer, 2017.

Quadri, Gabriel H. «Prueba informática: medios en particular». En *Tratado de Derecho Procesal Electrónico*, dirigido por Carlos Enrique Camps, 2ª ed., 275-592. Buenos Aires: Abeledo Perrot, 2019.

Rey, Fernando. «La firma digital en las empresas argentinas». En *Fintech: aspectos legales*, compilado por Santiago J. Mora y Pablo A. Palazzi, 175-88. Buenos Aires: Pablo Andrés Palazzi, 2019.

Rivera, Julio César, y Graciela Medina. *Código Civil y Comercial de la Nación Comentado*. Vol. I. Buenos Aires: La Ley, 2014.

Ruiz-Gallardón García de la Rasilla, Miguel. «Fe pública y tokenización de activos en

blockchain». En *Criptoderecho. La regulación de blockchain*, dirigido por Pablo García Mexía, 449-88. Madrid: Wolters Kluwer, 2018.

Sanchís Crespo, Carolina. «La prueba en soporte electrónico». En *Las tecnologías de la información y la comunicación en la administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio*, coordinado por Eduardo Gamero Casado y Julián Valero Torrijos, 707-34. Navarra: Aranzadi, 2012.

Urbano Castrillo, Eduardo de. *La valoración de la prueba electrónica*. Valencia: Tirant lo Blanch, 2009.

Zalazar, Claudia E., y Román A. Abellaneda. *Sistema probatorio en el proceso civil de Córdoba*. Córdoba: Alveroni Ediciones, 2021.

2. DOCTRINA JUDICIAL

Sentencia del Tribunal Supremo (Sala de lo Civil) 1109/2002, de 25 de noviembre de 2002, ponente Ilmo. Sr. Jesús Eugenio Corbal Fernández, f.j. 5° (ECLI:ES:TS:2002:7863).

Sentencia del Tribunal Superior de Justicia de Córdoba (Sala Civil y Comercial) 113/2005, de 26 de octubre de 2005 en autos "Torres Elba Inocencia Minetti de C/ E.P.E.C. – Ordinario – Recurso de Casación" (Actualidad Jurídica, n. 93, 2ª quincena enero 2006, p. 5989).

Sentencia de Tribunal Supremo (Sala de lo Civil) 492/2006, de 23 de mayo de 2006, ponente Ilmo. Sr. Vicente Luis Montes Penades, f.j. 3° (ECLI:ES:TS:2006:2962).

Sentencia del Tribunal Superior de Justicia de Canarias (Sala de lo Contencioso) 420/2009, de 01 de septiembre de 2009, ponente Ilmo. Sr. Francisco Javier Varona Gómez-Acedo, f.j. 3° (ECLI:ES:TSJICAN:2009:3161).

Sentencia del Tribunal Supremo (Sala de lo Civil) 558/2011, de 15 de julio de 2011, ponente Ilmo. Sr. Jesús Eugenio Corbal Fernández, f.j. 5° (ECLI:ES:TS:2011:5082).

Sentencia de la Cámara de Apelaciones en lo Civil y Comercial de Córdoba 60/2014, de 22 de mayo de 2014, en autos "Pisanu Juan Mauro C. Carteluz Srl. Ordinario. Otros. EXP N° 1642556/36" (TR LALEY AR/JUR/21863/2014).

Sentencia del Tribunal Supremo (Sala de lo Penal) 754/2015, de 27 de noviembre de 2015, ponente Ilmo. Sr. Julián Artemio Sánchez Melgar, f.j. 3° (ECLI:ES:TS:2015:5421).

Sentencia de la Audiencia Provincial de Barcelona (Secc. 9) 224/2017, de 08 de marzo de 2017, ponente Ilmo. Sr. José Maria Torras Coll, f.j. 2° (ECLI:ES:APB:2017:2135).

Auto de la Audiencia Provincial de Barcelona (Sección 13) 6/2018, de 15 de enero de 2018, ponente Ilma. Maria del Pilar Ledesma Ibañez, f.j. 2° (ECLI:ES:APB:2018:15A).

Sentencia de la Hangzhou Internet Court of the People's Republic of China, 27 June 2018, Hangzhou Huatai Media Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd. Case n° 055078 (2018) Zhe 0192 First Court No. 81.

Sentencia del Tribunal Supremo (Sala de lo Penal) 375/2018, de 19 de julio de 2018, ponente Ilmo. Sr. Juan Ramon Berdugo Gómez de la Torre, f.j. 2° (ECLI:ES:TS:2018:2949).

Acórdão do Tribunal de Justiça de São Paulo (5ª Câmara de direito privado), Agravo de Instrumento N° 2237253-77.2018.8.26.0000, de 19 de dezembro de 2018, relatora Fernanda Gomes Camacho (Registro: 2018.0001015661).

Sentencia de la Cámara de Apelaciones en lo Civil y Comercial de Morón (Sala II) 67/2019, de 23 de abril de 2019, en autos "Fleitas, Olga Esther c. Empresa del Oeste SA de Transporte y otros s/ daños y perj. autom. c/les. o muerte (exc. Estado)" (TR LALEY AR/JUR/8560/2019).

Sentencia de la Cámara Nacional de Apelaciones en lo Comercial de Capital Federal (Sala A), de 22 de octubre de 2019, en autos "Prenaval Seguridad SRL c/ Consorcio de Propietarios Santos Dumont 2719/21/23/55 s/ ordinario" (SAIJ: FA19130702).

Sentencia del Juzgado Nacional de 1° Instancia en lo Comercial Nro. 23, 135/2020, de 14 de febrero de 2020, en autos "Wenance SA c. Gamboa, Sonia Alejandra s/ ejecutivo" (TR LALEY AR/JUR/135/2020).

Sentencia del Tribunal Supremo (Sala de lo Social) 706/2020, de 23 de Julio de 2020, ponente Ilmo. Sr. D. Juan Molins García-Atance f.j. 3°-4° (ECLI:ES:TS:2020:2925).

3. NORMATIVA

Ley 8.465 del 27/04/1995 por el que se aprueba el Código Procesal Civil y Comercial de la Provincia de Córdoba. Argentina: BOEC, 08/06/2014. http://www.saij.gob.ar/8465-local-cordoba-codigo-procesal-civil-comercial-provincia-cordoba-lpo0008465-1995-04-27/123456789-0abc-defg-564-8000ovorpyel (consultada el 31/08/2021).

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. España: BOE, núm. 7, de 08/01/2000. https://www.boe.es/eli/es/l/2000/01/07/1/con (consultada el 31/08/2021).

Ley 25.506 del 14/11/2001 de Firma Digital. Argentina: BORA, 11/12/2001. http://www.saij.gob.ar/25506-nacional-ley-firma-digital-lns0004621-2001-11-14/123456789-0abc-defg-g12-64000scanyel (consultada el 31/08/2021).

Ley 59/2003, de 19 de diciembre, de firma electrónica, hoy derogada.

Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. España: BOE, núm. 160, 06/07/2011. https://www.boe.es/eli/es/l/2011/07/05/18/con (consultada el 31/08/2021).

Reglamento (UE) n ° 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. Unión Europea: Diario Oficial de la Unión Europea, núm. 257, 28/08/2014. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32014R0910 (consultada el 31/08/2021).

Ley 26.994 del 01/10/2014 por el que se aprueba el Código Civil y Comercial de la Nación. Argentina: BORA, 08/10/2014. http://www.saij.gob.ar/26994-nacional-codigo-civil-comercial-nacion-lns0005965-2014-10-01/123456789-0abc-defg-g56-95000scanyel (consultada el 31/08/2021).

Resolución E399/2016 del 05/10/2016 del Ministerio de Modernización. Argentina: BORA, 07/10/2016. http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/266312/texact.htm (consultada el 31/08/2021).

Decreto-ley 135 del 14/12/2018 sobre Disposiciones urgentes sobre apoyo y simplificación para las empresas y la administración pública. Italia: Gazzetta Ufficiale, 12/02/2019. https://www.gazzettaufficiale.it/eli/id/2019/02/12/19A00934/sg (consultada el 31/08/2021).

Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. España: BOE, núm. 266, 05/11/2019. https://www.boe.es/eli/es/rdl/2019/10/31/14/con (consultada el 31/08/2021).

Decreto del Poder Ejecutivo Nacional 182/2019 del 11/03/2019 mediante el cual se reglamenta la Ley N° 25.506 de Firma Digital. Argentina: BORA, 12/03/2019. http://servicios.infoleg.gob.ar/infolegInternet/anexos/320000-324999/320735/norma.htm (consultada el 31/08/2021).

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. España: BOE, núm. 298, 12/11/2020. https://www.boe.es/eli/es/l/2020/11/11/6/con (consultada el 31/08/2021).

4. WEBGRAFÍA

Asociación Española de Normalización. "Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia". https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0064986 (consultada el 08/06/2021).

Ast, Federico. 2021. "Proof of Humanity: ¿Qué Es y Cómo Funciona?", *Blog Kleros* (05 de mayo https://blog.kleros.io/proof-of-humanity-que-es-y-como-funciona/ (consultada el 10/05/2021).

Blockchain Federal Argentina. "Portal BFA". https://bfa.ar/ (consultada el 17/06/2021).

Chomczyk, Andres. 2020. "Preguntas Frecuentes sobre Legislación Argentina de Firma Digital y Electrónica". *Signatura Blog* (22 de mayo). https://blog.signatura.co/preguntas-frecuentes-sobre-legislación-argentina-de-firma-digital-y-electrónica-c6181ea3e865 (consultada el 05/05/2021).

Comisión Europea. "Observatorio y Foro Europeo de Blockchain". https://www.eublockchainforum.eu/about (consultada el 10/06/2021).

Comisión Europea. "Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento de un marco para una identidad digital europea". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:281:FIN (consultada el 25/06/2021).

Ilustre Colegio de Abogacía de Barcelona. "La CRAJ informa: Protocolo de protección del secreto empresarial. Juzgados Mercantiles de Barcelona". https://www.icab.es/es/actualidad/noticias/noticia/La-CRAJ-informa-Protocolo-de-proteccion-del-secreto-empresarial.-Juzgados-Mercantiles-de-Barcelona./ (consultada el 18/06/2021).

Gobierno de Aragón. "Visor Público de la Blockchain". https://licitacion.aragon.es/ (consultada el 20/06/2021).

González Granado, Javier. 2016. "Eficacia probatoria de la blockchain. Criptografía y artículo 1227 del Código Civil". *Taller de Derechos* (25 de abril). https://tallerdederechos.com/eficacia-probatoria-de-la-blockchain-criptografia-y-articulo-1227-del-codigo-civil/ (consultada el 20/06/2021).

Hyperledger. "An Introduction to Hyperledger". https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf (consultada el 13/06/2021).

Kleros. "About Kleros". https://kleros.io/about/ (consultada el 21/06/2021).

Municipalidad de Córdoba. "Portal de Gobierno Abierto de la Municipalidad de Córdoba". https://gobiernoabierto.cordoba.gob.ar/blockchain/ (consultada el 17/06/2021).

Organización para la Cooperación y el Desarrollo Económicos (OCDE). "Global Blockchain Policy Centre". https://www.oecd.org/finance/blockchain/ (consultada el 10/06/2021).

Portal Argentina. "Normativa de Firma Digital". https://www.argentina.gob.ar/firmadigital/normativa (consultada el 01/05/2021).

Portal del Ministerio de Asuntos Económicos y Transformación Digital. "Anteproyecto de Ley del Mercado de Valores y de los Servicios de Inversión y Reales Decretos de desarrollo". https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/ECO_Tes_20210430_AP_LMVySI_Texto_Ley_del_Mercado_de_Valores.aspx (consultada el 08/06/2021).

Safe Creative Blog. "Blockchain llega a Safe Creative". https://es.safecreative.net/2019/04/10/blockchain-llega-a-safe-creative/ (consultada el 06/06/2021).

Satoshi, Nakamoto. 2008. Bitcoin: un sistema de efectivo electrónico usuario-a-usuario. Traducido por Ángel León. https://bitcoin.org/files/bitcoin-paper/bitcoin_es_latam.pdf (consultada el 20/04/2021).

Szabo, Nick. 1997. The God Protocols. *Satoshi Nakamoto Institute.* https://nakamotoinstitute.org/the-god-protocols/ (consultada el 15/05/2021).

Todd, Peter. 2016. "OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin". *Blog* (15 de septiembre). https://petertodd.org/2016/opentimestamps-announcement#evidence-authenticity (consultada el 01/06/2021).