Aplicaciones de la Tecnología Blockchain en el Área Forense

Torres Zúñiga, Vicente
Universidad Nacional Autónoma de México, Facultad de Medicina,
Licenciatura en Ciencia Forense.

Resumen
La tecnología emergente llamada blockchain promete ser parte de procesos de certificación de documentos, transacciones y comunicaciones digitales. Por lo que, se ha utilizado con éxito como parte de esquemas de monedas digitales. En este texto presentamos sus posibilidades para aplicarse en situaciones diversas de interés forense. De modo sucinto describimos su funcionamiento y presentamos varios ejemplos de cómo puede ser de ayuda a los peritos en informática para preservar el indicio digital, además de mencionar posibles vías para que forme parte como cadena de custodia digital. Consideramos que es importante que el perfil profesional de los abogados conozca los alcances y aplicaciones que puede tener esta herramienta novedosa.

Palabras clave: cadena de custodia, legal blockchain, evidencia digital, blockchain forense.

Introducción

Un considerable grupo de expertos internacionales prevén, que en los próximos cinco años, la tecnología emergente llamada *blockchain* cambiará radicalmente el quehacer de los abogados de diferentes especialidades y a un nivel global [1-3]. Seguramente uno de los primeros ámbitos en mostrar los efectos será el mercantil; pero también toda aquella área donde se incluyen documentos digitales con posible valor probatorio [4]. Tal puede ser el caso de la cadena de custodia, que por ser un protocolo que vincula tiempo, personas, objetos y acciones, se vería beneficiada por una simplificación administrativa e incluso con una preservación de los indicios digitales. Por tanto, con el fin de aprovechar al máximo esta tecnología, los abogados relacionados con asuntos penales, especialmente en sistemas de justicia adversarial, deben conocer los fundamentos y alcances de esta novedosa herramienta informática. En los siguientes párrafos, describiremos las características, beneficios y retos para implementar cadenas de custodia digitales en nuestros contextos de impartición de justicia.

Sucinta revisión de la cadena de custodia

La cadena de custodia es un sistema de registro y control, que se aplica a los indicios relacionados con la investigación de un supuesto ilícito [5]. Inicia con el descubrimiento o aportación de una huella, vestigio, instrumento o producto de un presunto delito; finaliza cuando la autoridad determina que ha concluido su proceder con tal objeto. Su finalidad es evitar alteraciones, sustituciones, contaminaciones o bien la destrucción de los indicios. En caso de perder la secuencia lógica en el registro, se malogra la eficacia probatoria del objeto de estudio forense. Así, conforme avanzan las etapas de un proceso judicial, gana relevancia la información de los indicios y la cadena de custodia que la respalda; de tal modo el indicio se puede constituir en evidencia y posteriormente en prueba ante el tribunal. Tradicionalmente se utilizan formatos en papel para realizar la cadena de custodia; tal esquema puede ser

adecuado para vincular un indicio específico y material, como lo es un arma de fuego; dado que al día de hoy, es inexistente la tecnología capaz de duplicar a nivel microscópico un material macroscópico. Sin embargo, los indicios digitales cuentan con la particularidad de estar constituidos por información pura, la cual sí se puede duplicar a la perfección. Por lo que este tipo de objetos requieren una tecnología de registro y control más acorde a su naturaleza.

Las particularidades del indicio digital

Hoy en día, vivimos en una sociedad con cambios tecnológicos radicales cambios tecnológicos, especialmente en el área de las telecomunicaciones. Cotidianamente, en nuestras gestiones, comunicaciones y transacciones utilizamos cada vez más los dispositivos electrónicos, para desplegar información por vías multimedia; por ende, dentro de estos aparatos y con los que interaccionan, se guardan datos digitales diversos, muchos de ellos pueden ser relevantes para una pesquisa forense [6]. Si bien, tanto el dispositivo como sus datos pueden ser estudiados desde una perspectiva de la criminalística de campo, los indicios informáticos presentan características únicas, que obligan al perito a seguir medidas cautelares adicionales [7]. Por ejemplo, a diferencia del indicio material, los datos digitales son duplicables, modificables y eliminables en su totalidad. Por tanto, se debe asegurar que el indicio sea resguardado de modo que se evite toda interacción (entrada o salida) de señales electromagnéticas o información. Además, en el análisis posterior, se deben garantizar las condiciones de aislamiento y control en el estudio del indicio. Más aún, las herramientas para manipular el dato digital son cada vez más accesibles y cómodas para los usuarios; de modo que las precauciones deben ser mucho mayores. Asumir, por defecto, un rechazo a todas las evidencias digitales, por el hecho de ser más susceptibles al cambio, es un grave error. En una comunidad tan conservadora como la formada en el Derecho Penal, la adquisición de nuevas tecnologías suele ser más lenta que en otros ámbitos. Por ejemplo, hasta hace poco, las autoridades de la Ciudad de México fomentaban que los peritos utilizaran fotografía analógica en lugar de la digital; aunque, desde hace años su uso cuenta con amplio respaldo de diferentes autoridades judiciales y expertos del área [8]. Por ello, es comprensible que durante un proceso se cuestione principalmente la fuente y mismisidad del indicio informático, o sea se pone entre dicho a la cadena de custodia. Un atenuante a este problema es que el perito informático trabaje en conjunción con un notario público, siendo una figura que puede dar fe legal de lo que presencia, aunque carezca del conocimiento técnico de su significado. Así, en el esquema actual del debido proceso, las fotografías digitales o las comunicaciones electrónicas (por redes sociales, correos electrónicos o mensajes de voz) deben ir acompañadas por su soporte físico original (que es el indicio obtenido por el criminalista de campo: un teléfono celular, una computadora, una memoria portátil, un disco compacto, u otro tipo de tecnología), el dato relevante debe estar impreso –acompañando el dictamen pericial–, junto con el documento testimonial del notario público, y claro, la cadena de custodia [9]. Tal vez, la tecnología *blockchain* cuenta con el

potencial para cambiar toda esta tendencia, brindando alta seguridad y simplificando el trabajo burocrático.

La esencia de la tecnología *blockchain*

El protocolo informático *blockchain* se desarrolló alrededor de 1991, su intención era vincular una huella inalterable a los registros digitales para prevenir la manipulación en fechas [10, 11]. En cierto modo, este sistema funciona como un notario automático, quien da fe de la legalidad y autenticidad de la información que tiene ante sí. En el año 2009, Satoshi Nakamoto la implementó para el desarrollo del *bitcoin*, un tipo de moneda digital, hoy muy popular en el sector financiero, que es otra comunidad que se esfuerza por alcanzar altos estándares de seguridad [12]. Los empresarios que han adoptado el *blockchain*, lo defienden como un sistema de almacenamiento de información seguro, anónimo, descentralizado y libre de falsificaciones [13].

En términos técnicos, el *blockchain* consiste en un registro de cambios concatenados –como lo es una bitácora de uso de equipo o bien la misma cadena de custodia–. Su funcionamiento es simple, cada bloque contiene tres elementos fundamentales: **A)** Una etiqueta de identificación asociada al estado actual del archivo digital, **B)** Una etiqueta del estado anterior que presentaba el archivo digital y **C)** El respaldo de más del 51% de computadoras conectadas al *blockchain*. A continuación, abundaremos en qué consisten estos elementos:

Etiqueta de identificación digital.

Se utiliza una fórmula matemática –basada en la Teoría de Congruencia de Números Primos– aplicada a un archivo digital; la respuesta será el *hash*, que consiste en una cadena de unos pocos caracteres hexadecimales (*i.e.* números y letras) [14]. Existen diferentes algoritmos para obtener el hash; por ejemplo, el SHA-256, desarrollado por la Agencia de Seguridad Nacional de los EE.UU, es popular internacionalmente y se ha utilizado para autentificar evidencias ante la corte [15]. Si este se aplica a un texto extenso, como puede ser la constitución de un país, producirá una cadena de 64 caracteres, esa será su huella electrónica. Si por algún motivo a ese archivo se le añade o suprime un carácter (*e.g.* una coma) y se vuelve a calcular el *hash*: la respuesta será diferente. Sin necesidad de revisar a detalle todo el archivo puedo enterarme que presenta algún cambio, aunque sea mínimo. Lo mismo sucederá si se trata de otro tipo de archivo multimedia. La relación del archivo de interés y el identificador alfanumérico son parte de lo que en *blockchain* se llama bloque.

Etiquetas de seguimiento por bloques.

Digamos que de modo válido y legal, deseo añadir información a un archivo, como sucede en los formatos de cadena de custodia o bitácoras cuando se estampa la hora, se redacta un breve informe y se firma. Entonces, se crea un nuevo bloque, que entre otros objetos contiene: **1)** el archivo de interés, **2)** el *hash* del nuevo estado y **3)** el *hash* del estado anterior de ese archivo. De modo que siempre conoceré el estado anterior del archivo. El *blockchain* además de contar con medidas para respaldar la mismisidad del indicio, también le realiza seguimiento a los estados e informes previos, por lo que

también se preserva la trazabilidad dentro de la cadena de custodia [16].

Permítame usar una metáfora, los bloques son como cajas, adentro están los indicios e informes periciales, cada uno de ellos cuenta con su identificador *hash*. Con el fin de continuar con la investigación, el perito necesita trabajar con los objetos dentro de esa caja. Así que se crea una caja nueva que la vincula hacia la caja previa. Es decir, cada caja cuenta con un identificador y un sistema para rastrear la caja anterior, hasta conocer la caja primigenia. La relación entre los identificadores alfanuméricos forma una cadena entre los bloques, de donde proviene el nombre: *blockchain*. En la Fig. 1, se muestra un ejemplo didáctico: consiste en una cadena de tres elementos; el bloque se vincula hacia el dos, y este hacia el uno. El primer bloque es especial, es el bloque primigenio y siempre tendrá hash previo igual a 0. Si deseamos alterar el segundo bloque, se necesita cambiar su *hash*, pero a la vez ocasionará inválido al bloque tres y todos los siguientes bloques, porque ya no almacenan un *hash* válido al previo bloque. Será evidente la alteración porque al romper un eslabón, rompe toda la cadena.

En otras palabras, si alguien altera un bloque, entonces cambiará su identificador y romperá la cadena. Por tanto, necesitará recalcular los demás hashes de la cadena para ocultar la trasgresión. Con un alto poder de cómputo es posible realizar un ataque exitoso al *blockchain*. Por ello se adoptan más medidas para evitar alguna alteración: la prueba de trabajo y la democratización entre computadoras.

Prueba de trabajo y democracia en computadoras

La velocidad de las computadoras es muy alta, pueden calcular millones de hashes por segundo; entonces es simple alterar un bloque y recalcular todos los siguientes hashes de la cadena. Para reducir la probabilidad de adulteración, el *blockchain* cuenta con un mecanismo para garantizar la creación adecuada de bloques, llamada *prueba de trabajo*. Para el caso del *bitcoin*, se requieren 10 minutos para ejecutar el algoritmo de la prueba de trabajo y permitir agregar un nuevo bloque a la cadena. Este protocolo dificulta la falsificación de bloques, porque si se altera uno, se debe recalcular la prueba de trabajo para los bloques subsecuentes y en cada uno, esperar 10 minutos. De modo que una cadena larga es más segura que una corta.

Pero el *blockchain* incorpora una medida de seguridad adicional, la cual le brinda descentralización. En lugar de utilizar una central para administrar la cadena, el *blockchain* utiliza una red de ordenadores pares (*peer-to-peer* en inglés). Que consiste en conectar varias computadoras de modo que funcionen algunos de sus aspectos sin la necesidad de clientes o servidores fijos; haciendo que en su lugar, una serie de nodos se comporten como iguales entre sí. Así cuando en la red se conecta una computadora nueva, obtiene una copia completa de la cadena de bloques. Y al crear un nuevo bloque, se comparte con toda la red, y cada nodo verifica que el bloque sea intachable. Por consenso se asegura la integridad de la información,

pues los bloques rechazados se descartan de la cadena y los aceptados se agregan a la cadena de cada nodo.

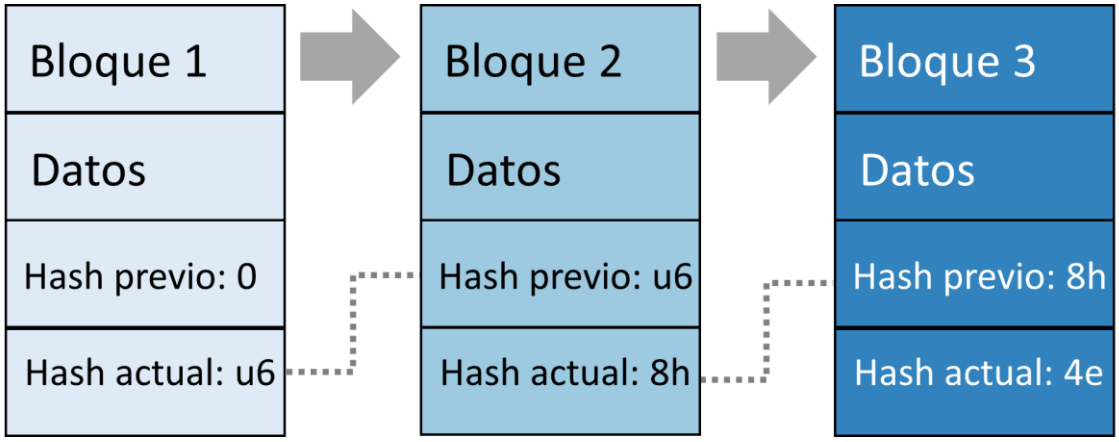

Figura 1. Esquema de tres bloques que forman un *blockchain*. Cada bloque cuenta con sus datos, un identificador alfanumérico y un identificador que señala al estado del bloque anterior.

Resumiendo, para alterar una cadena de bloques se necesita tres condiciones: **1)** manipular todos los bloques posteriores del bloque alterado para calcular los correspondientes hashes, **2)** recalcular la prueba de trabajo para cada bloque, esperando alrededor de 10 minutos por bloque. En cadenas cortas es factible ocultar el cambio, en blockchain largos la probabilidad de éxito es pequeña, y finalmente, **3)** controlar más del 50% de los nodos de la red de pares; para una red pequeña, hablamos de más de 1,000 equipos. Solo así, el bloque alterado se aceptará.

Por último, es oportuno señalar que se puede adoptar más medidas de seguridad, como la encriptación de la información (por lo general por medio de clave pública y clave privada), por lo que solo quien la cree en el bloque puede acceder a él.

Aplicaciones generales del blockchain

Además de su utilidad en el funcionamiento de cripto-divisas, en la literatura se proponen varias aplicaciones a esta tecnología emergente [17]. Por ejemplo, ser complemento en los expedientes médicos [11], auxiliares en servicios notariales, verificadores en la recolección de impuestos [12], así como gestionadores de contratos inteligentes o condicionados (*smart contracts*, como son llamados en inglés) [18]. Todos estos son casos de interés para los abogados, pero en el contexto forense también se puede aplicar.

El ministerio de seguridad pública de la república popular de China solicitó (a finales del 2018) patentar un sistema consistente de discos virtuales, registros de monitoreo API (siglas de *Application Programming Interfaces*, que significa interfaces de programación de aplicaciones) y cortafuegos, con el fin de resguardar y preservar evidencia de interés forense [19]. Parece que su intención es realizar una integración más rápida de los expedientes de investigación, mantener a disposición los indicios digitales y conservar la cadena de custodia. Previniendo la pérdida,

falsificación o ilegibilidad de la información, violaciones de privacidad, además de la duplicidad de datos. Es claro, que por ser una patente, muchos detalles son omitidos, pero también en la literatura académica existen ejemplos interesantes del uso de *blockchain* en el ámbito forense. Un caso relevante es en hechos de tránsito [20, 21], supongamos que todos los autos cuentan con tecnología para comunicarse entre sí. Se transmitirán pocos datos: un identificador de la unidad, el estado general del vehículo y velocidad. En caso de suceder una colisión, los indicios digitales se almacenarán en los automóviles involucrados, pero los carros que se encontraban en las inmediaciones antes y después del percance formarán un *blockchain* (que inició mucho antes de que aconteciera la colisión). Es decir, los vehículos cercanos se convertirán en testigos electrónicos que apoyaran la investigación forense, pues contarán con una bitácora digital basada en la tecnología de cadena de bloques. La Fig. 2 muestra un esquema de cómo podría funcionar esta tecnología aplicada en algunos automotores.

Como último ejemplo, mencionamos el potencial de incorporar la información de nuestros teléfonos celulares a un *blockchain* forense. Son muchos los casos donde las telecomunicaciones entre usuarios o bien videograbaciones realizadas por testigos se convierten en objetos de estudio de los peritos, eso es una tendencia creciente. Si una persona utiliza su *smartphone* para filmar un hecho, podría utilizar un servicio *blockchain* como primera etapa para asegurar que esas imágenes pueden ser utilizadas en la corte. Aquí el paradigma criminalístico informático cambia, pues es el testigo el que resguarda el dato. Su equivalente analógico, son los testamentos: pues son las personas las que acuden al notario público para que de fe sobre la información que quieren preservar. Por las razones expuestas, y muchas otras, es que se afirma que esta tecnología cambiará la forma en que hacemos muchos procesos legales.

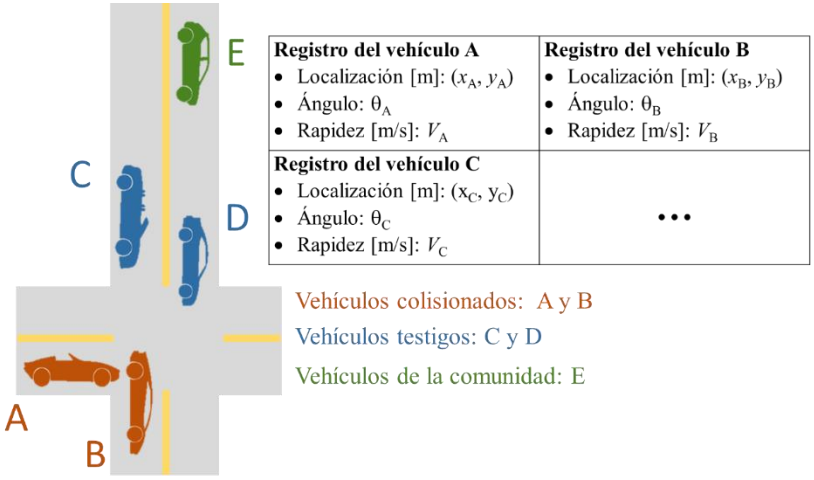

Figura 2. Esquema de cómo se puede aplicar la tecnología *blockchain* con el fin de fijar datos relevantes en una pericial de hechos de tránsito.

Retos principales

Si bien existen tecnologías antagonistas que pretenden vulnerar al *blockchain*, al día de hoy, se desconoce alguna que sea efectiva [22-23]. El estado actual del indicio digital y su cadena de custodia es más frágil sin tecnología de cadena de bloques. Con todo, es de esperar que mejoren estos algoritmos, pues se encuentran muchos beneficios involucrado. Por otro lado, es importante que la comunidad relacionada con el Derecho Penal (abogados, fiscales, jueces, peritos, entre otros) conozca esta tecnología, pues su irrupción dentro de la corte es inminente. Así, la divulgación y enseñanza básica del *blockchain* es importante y cuenta con varios frentes de acción. Por ejemplo, en general, los abogados deben conocer su funcionamiento y alcances en diferentes aplicaciones, con una profundización técnica menor al perfil de un ingeniero. Por tanto, estos temas –del llamado legal-tech– deben incorporarse en los planes de estudio y capacitación de los abogados, solo de ese modo nuestros sistemas de justicia estarán listos para esta clase de tecnologías emergentes.

Conclusiones

El *blockchain* es un protocolo electrónico de alta seguridad que permite la trazabilidad, mismisidad, preservación y reserva confidencial de indicios digitales, además de bitácoras electrónicas que pueden ser parte de la cadena de custodia. Esta tecnología se emplea ya en el área financiera con una tendencia creciente, por lo que es probable que otros sectores la adopten. En el campo forense puede ser una herramienta útil, siempre y cuando los profesionales técnicos y del derecho trabajen en conjunto para dejar en claro los alcances y beneficios de este herramienta.

Agradecimientos

El autor desea agradecer los comentarios técnicos del M.C. José Guadalupe Bañuelos Muñetón, el apoyo de la Dra. Zoraida García Castillo, Coordinadora de la Licenciatura en Ciencia Forense, así como el apoyo económico del proyecto UNAM-PAPIME-PE107216.

Datos de Contacto:

Vicente Torres Zúñiga. Universidad Nacional Autónoma de México, Facultad de Medicina, Licenciatura en Ciencia Forense, Circuito de la Investigación Científica s/n, Del. Coyoacán, C.P. 04510, México, Cd. Mx.

Email: vicentz@gmail.com

Referencias

1. M Fenwick, WA Kaal, EPM Vermeulen, *Legal education in the blockchain revolution*, J. Ent. & Tech. L., 2017.
2. M Fenwick, WA Kaal, EPM Vermeulen, *Legal Education in a Digital Age: Why 'Coding for Lawyers' Matters*, 2018.
3. MM Bues, E Matthaei, *LegalTech on the Rise: Technology Changes Legal Work Behaviours, But Does Not Replace Its Profession*, Liquid Legal, 2017.
4. K Takahashi, *Blockchain technology and electronic bills of lading*, JIML, 22, 2016
5. Código Nacional de Procedimientos Penales, 5/03/2014,
6. DR Méndez, "La revolución en los hábitos de uso y consumo de vídeo en teléfonos inteligentes entre usuarios millenials, la encrucijada revelada", Revista latina de comunicación social, 2017.
7. J Sammons, *The basics of digital forensics: the primer for getting started in digital forensics*, Elsevier, 2012.

8. V Torres-Zúñiga, Cap. “Las preguntas importantes ante la alteración de fotografías”, 187-208, en “Ciencia forense en el contexto del nuevo sistema de justicia penal”, editor. Z. García Castillo, Tribunal Superior de la Ciudad de México, 2016.
9. H Vite Perez, “Informatica forense, protocolo de actuación”, Flores, 2016.
10. H Halpin, M Piekarska, Introduction to Security and Privacy on the Blockchain, IEEE, 2017.
11. MB Hoy, *An Introduction to the Blockchain and Its Implications for Libraries and Medicine*, Medical Reference Services Quarterly, 36:3, 2017.
12. P Treleaven, RG Brown, D Yang, *Blockchain technology in finance*, Computer, 2017.
13. D Patel, J Bothra, V Patel, *Blockchain exhumed*, IEEE, 2017.
14. CHJ Wu, JD Irwin, *Introduction to computer networks and cybersecurity*, Taylor & Francis 2016.
15. AE Okeyinka, O Alao, B Gbadamosi, *Application of SHA-256 in Formulation of Digital Signatures of RSA and Elgamal Cryptosystems*, Operations Research and Information Engineering, 1(2): 61-66, 2018.
16. J Cosic, M Baca, P Grd, *The Necessity of Developing a Standard for Exchanging a Chain of Custody of Digital Evidence Data*, IJCSIS, 15(11), 2017.
17. M Crosby, P Pattanayak, S Verma, *Blockchain technology: Beyond bitcoin*, Applied Innovation Review, *2*, 2016.
18. K Christidis, M Devetsikiotis, *Blockchains and contracts for the internet of things*, IEEE, 2016.
19. *Wolfie Zhao, China’s Security Ministry Touts Blockchain for Evidence Storage, 9/04/2018, acceso: 10/01/2019.*
20. C Oham, SS Kanhere, R Jurdak, S Jha, *A Blockchain Based Liability Attribution Framework for Autonomous Vehicles, arXiv preprint arXiv:1802.05050, 2018*
21. F Gao, L Zhu, M Shen, K Sharif, Z Wan, K Ren, *A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks*, IEEE Network, 2018.
22. *M* Orcutt 19/02/2019, *Once hailed as unhackable, blockchains are now getting hacked*, acceso*:* 22/02/2019
23. C Sullivan, E Burger, *E-residency and blockchain*, Computer Law & Security Review, 2017.