AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Modelo de arquitectura de software basada en la Nube para el registro seguro de evidencias digitales con Tecnología Blockchain

Cloud-based Software Architecture Model for the safe Digital Evidence records with Blockchain Technology

Presentación: 26 y 27 de octubre de 2022

Enzo Notario
Facultad de Ingeniería, Universidad Católica de Salta - Argentina
ernotario@ucasal.edu.ar

Jhon Grover Dorado
Facultad de Ingeniería, Universidad Católica de Salta - Argentina
jdorado@ucasal.edu.ar

Carlos Párraga
Facultad de Ingeniería, Universidad Católica de Salta - Argentina
licparraga1914@gmail.com

Oscar Carlos Medina
Facultad Regional Córdoba, Universidad Tecnológica Nacional – Argentina
omedina@frc.utn.edu.ar

Herminia Beatriz Parra de Gallo
Facultad de Ingeniería, Universidad Católica de Salta – Argentina
bgallo@ucasal.edu.ar

Resumen

En el ámbito de la Justicia, tiene un valor primordial el carácter de admisibilidad de la evidencia, entendiendo por tal a las condiciones de integridad, confidencialidad y confiabilidad que debe tener un elemento de prueba en un juicio. Estos criterios se respetan en un procedimiento procesal denominado Cadena de Custodia que actualmente cuenta con elementos registrales en papel, para el monitoreo constante de la evidencia como un conjunto de eventos que establecen la trazabilidad de ésta en todo momento, pues identifica donde y quien tiene bajo su responsabilidad dicho elemento de prueba. Para estudiar esta problemática, se conforma un equipo de trabajo entre la Facultad de Ingeniería de la UCASAL que a través del Grupo de Forensia Digital, pone a disposición la base de conocimiento experto en el tratamiento de la evidencia digital y el modelo de negocio de la Cadena de Custodia; y el CIDS, Centro de Investigación, Desarrollo y Transferencia de Sistemas de Información de la U.T.N. – Facultad Regional Córdoba, cuyo laboratorio de Blockchain aporta la experiencia, trayectos formativos y de investigación especializados en las tecnologías de redes Blockchain y contratos inteligentes.

Palabras clave: Blockchain, Cadena de Custodia, Forensia Digital, Computación en la nube, Contratos inteligentes

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Abstract

In the field of Justice, the admissibility of evidence is of paramount value, understanding as such the conditions of integrity, confidentiality and reliability that an element of evidence must have in a trial. These criteria are respected in a procedural procedure called Chain of Custody, which currently has registry elements on paper, for the constant monitoring of the evidence as a set of events that establish the traceability of this at all times, as it identifies where and who is responsible for this element of evidence. To study this problem, a working team is formed between the Faculty of Engineering of UCASAL, which through the Digital Forensics Group, makes available the expert knowledge base in the treatment of digital evidence and the business model of the Chain of Custody; and the CIDS, Centre for Research, Development and Transfer of Information Systems of the U.T.N. – Córdoba Regional Faculty, whose Blockchain laboratory provides the experience, training and research specialized in Blockchain network technologies and smart contracts.

Keywords: Blockchain, Chain of Custody, Digital Forensics, Cloud computing, Smart contracts

Introducción

Para una aproximación resumida de la problemática que aborda este proyecto, se puede considerar la definición de Cadena de Custodia del Ministerio Público Fiscal de nuestro país (Ministerio Público Fiscal, 2015), que señala: "*La cadena de custodia es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal. Debe garantizar que el elemento de prueba o evidencia que se presenta en juicio, con el objeto de probar una determinada afirmación, sea el que ha sido reclutado y que no haya sufrido adulteraciones o modificaciones de parte de quienes lo introducen o terceras personas*."

Al decir de (Chaia, 2013): "*Se debe tener especial cuidado en evitar cuestionamientos respecto del levantamiento y la custodia de los elementos o rastros que se presentan en el plenario, aventando cualquier sospecha sobre su procedencia y dejando en claro que se corresponden con los efectivamente secuestrados en la escena del crimen. Para llevar adelante esa actividad es preciso acreditar tanto el método utilizado, cuanto el personal que lo practicó. En definitiva, si las pruebas no se bastan a sí mismas –si es preciso identificar los objetos o huellas del delito, el sitio en que fueron encontrados, o la persona que tuvo a su cargo esa tarea-, resulta central prestarle atención al levantamiento y la conservación de ese material. Porque si el método es incorrecto, el almacenamiento inadecuado o la persona incapaz de cumplir su cometido, el trabajo será inútil y la evidencia inservible*.

Por otra parte, y en lo que respecta al manejo y preservación de evidencias digitales, la Resolución 528/21 (Ministerio de Seguridad de la Nación, 2021) aprueba el Protocolo de Actuación para la Investigación Científica en el Lugar del Hecho, el cual señala las responsabilidades del especialista en informática forense que actúa en un probable escenario delictivo, indicando particularmente los criterios de seguridad que deben mantenerse durante la recolección de la evidencia digital: *"10.66. El especialista en informática forense procurará que en el acta prevista en el artículo 7.13 y/o en el informe de su especialidad conste una fijación narrativa, precisa y detallada que suministre una noción clara del lugar donde fueron hallados los medios tecnológicos informáticos, de toda incidencia que hubiere acontecido durante el procedimiento policial, de los Potenciales Elementos de Prueba (PEP) de su interés detectados en el lugar del hecho y el estado en que éstos fueron hallados (encendido/apagado), incluyendo las características identificativas de cada dispositivo (por ejemplo, daños, marca, modelo, número de serie y cualquier marca de identificación). Cuando sea necesario y las circunstancias del hecho lo ameriten, el especialista en informática forense procurará que la fijación*

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

narrativa se complemente con fotografías, filmaciones y planos del lugar y del sitio de ubicación de cada efecto. Todo ello a fin de asegurar que el procedimiento pueda ser reconstruido, en caso de ser solicitado por la autoridad judicial."

De lo anterior queda clara la necesidad de contar con procedimientos de gestión documental seguros y confiables para el registro de la evidencia digital, y la importancia de reflejar los datos con el detalle necesario y suficiente para establecer la trazabilidad de la evidencia digital.

Objetivos del Proyecto

Será necesario orientar el estudio y la investigación a la utilización de las tecnologías de seguridad informática y análisis forense en el contexto de la tecnología Blockchain y la trazabilidad del proceso de Cadena de Custodia.

Por una parte, se deberá circunscribir el contexto de aplicación y experimentación del tema en estudio, según criterios de alcance, profundidad, oportunidad y acceso a problemáticas reales de la Cadena de Custodia.

Se propone contextualizar el trabajo orientándolo al estudio de metodologías, técnicas y herramientas propias de la tecnología Blockchain, y su aplicación en el caso de aplicación propuesto.

Otro aspecto que debe abordarse es el ámbito jurídico-legal de la Cadena de Custodia, i.e., abordar la investigación desde las normativas nacionales e internacionales existente para este tipo de casos.

Teniendo en cuenta lo antes mencionado, se propone como objetivos específicos de este proyecto de investigación los siguientes:

- Objetivo Específico 1: Formular un proyecto tecnológico que integre los recursos que cada parte aporta desde el rol que le compete, para el desarrollo de una arquitectura basada en los fundamentos metodológicos, técnicos y científicos requeridos por la Forensia Digital, con la adición de la trazabilidad inmutable de Blockchain.
- Objetivo Específico 2: Desarrollar un modelo de la arquitectura de software de tipo Blockchain en la nube que incorpore los resultados y conclusiones de OE1 considerando las estrategias necesarias para desarrollo a futuro de una aplicación informática específica para la gestión documental de la Cadena de Custodia.
- Objetivo Específico 3: Estudiar y analizar la normativa legal nacional e internacional aplicable a este tipo de entornos de registración documental en el ámbito de la justicia.

Marco Teórico

Desde el punto de vista del Derecho Procesal, vale considerar lo dicho por (Sandoval, 2020). cuando menciona que: *"... el proceso judicial constituye la principal garantía, ya que sirve como espacio adecuado para un debate amplio y contradictorio, que permita conocer o, por lo menos, acercarnos a la realidad litigiosa donde las partes de cada extremo del conflicto accedan... y, por tanto, en cualquier actuación debe «asegurarse la construcción del «debido proceso» o «proceso justo» que la humanidad exige para el juzgamiento de cualquier cuestión problemática, en consideración a lo subjetivos que con el proceso se persiguen".* El concepto de "debido proceso" incluye a las pruebas que cada parte puede presentar, y se garantiza la veracidad de estas a partir de su resguardo mediante la cadena de custodia respectiva, remarcando el rol que ésta cumple en el cumplimiento de las garantías procesales.

Respecto de Blockchain son válidos los aportes del trabajo de (Torres Zúñiga,2021) quien destaca – desde el enfoque de las ciencias jurídicas – la importancia de aplicar esta tecnología como sistema de registro y control de los indicios, hallazgos y evidencias relacionados con la investigación de un supuesto delito, así como la necesidad de dar a conocer las posibilidades de estas tecnologías a los profesionales de las Ciencias del Derecho.

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Estos conceptos iniciales señalan el marco jurídico que se debe considerar en este proyecto, para dar respuesta a la demanda de un proceso judicial más eficiente basado en propuestas de incorporación de tecnologías emergentes a dichos procesos. En particular, cuando se consideran los delitos mediados por las tecnologías, existe una abundante cantidad de elementos de prueba, que deben resguardarse de manera adecuada, principalmente para cuidar la admisibilidad de la evidencia según criterios de integridad, autenticidad, y confidencialidad.

En este contexto, y dadas las características de confiabilidad de la tecnología Blockchain, resulta una herramienta ventajosa y adecuada para aplicar en la Cadena de Custodia y resguardar la trazabilidad de la probable evidencia digital.

Por otra parte, la sistematización de los registros de la Cadena de Custodia trae aparejados beneficios adicionales, como la elaboración de estadísticas, informes de cruces de datos, etc., y todas las variantes que pueden devenir de contar con los registros en una estructura de base de datos organizada. La aplicación del análisis estadístico a los registros de la Cadena de Custodia permitirá contar con información que fundamente las políticas procesales y de seguridad que involucran al proceso penal, entregando a los actores de nivel superior información derivada de casos concretos, para que puedan tomar mejores decisiones sobre la organización y administración de justicia.

A pesar de sus evidentes beneficios mencionados, este tipo de herramientas y tecnologías digitales se encuentran ausentes a la fecha en el sistema judicial argentino, dando lugar a una vulnerabilidad estructural que podría ser subsanada con la solución que se propone en este proyecto.

Desde los espacios científicos especializados en la Forensia Digital, se considera a la evidencia digital como un objeto de estudio para el cual se investigan nuevos métodos, técnicas y herramientas forenses. En particular se pueden mencionar dos componentes de interés para el presente proyecto:

- La aplicación de tecnologías de tipo Blockchain son consideradas las más adecuadas en la actualidad para garantizar trazabilidad e inmutabilidad por las características intrínsecas de su base de datos (Querro, 2020).
- La definición de procesos y procedimientos ajustados a normas y protocolos internacionales para el tratamiento de la evidencia digital.

Si se considera el foco de trabajo en los procesos y procedimientos judiciales en sí mismos, es dable considerar las normas y protocolos internacionales para el tratamiento de la evidencia digital y la Cadena de Custodia. Al respecto existen investigaciones que abordan los vínculos entre la tecnología Blockchain y las normas ISO 9001.2015 (Gisbert Soler & Pérez Molina, A. I., 2019). y la ISO 27001:2017 (Tanadi et al., 2021).

Por otra parte, la norma ISO 22095:2020 (ISO, 2020), define un marco para la cadena de custodia proporcionando:

- un enfoque genérico consistente para el diseño, implementación y gestión de cadenas de custodia;
- terminología armonizada;
- requisitos generales para diferentes modelos de cadena de custodia;
- orientación general sobre la aplicación de los modelos de Cadena de Custodia definidos, incluida la orientación inicial sobre las circunstancias en las que cada modelo podría ser apropiado.

De aplicación en diversos ámbitos, la norma puede ser utilizada por diferentes organizaciones que operen en cualquier paso de una cadena de suministro, así como por organizaciones de establecimiento de estándares como punto de referencia para estándares específicos de la Cadena de Custodia.

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Entonces, se ha identificado plenamente la demanda de un registro confiable para la Cadena de Custodia, dicho por los propios actores del proceso judicial, que reconocen a la tecnología Blockchain como la herramienta fundamental para las necesidades de trazabilidad de la evidencia, y reconociendo su impacto en la eficacia procesal de la justicia a partir de las condiciones de integridad, confidencialidad e inalterabilidad que esta tecnología conlleva. Se identificaron, en un análisis preliminar, publicaciones relacionadas con la aplicación de tecnologías Blockchain al caso de uso Cadena de Custodia de evidencias de un proceso judicial (Al-Khateeb et al., 2019), (Lone & Mir, 2018) (Bonomi et al., 2018). Se prevé, además, la elaboración de una revisión sistemática de la literatura científica para determinar el estado actual de conocimiento de este tema.

Metodología y Plan de Trabajo

Como actividad indispensable para el inicio de la investigación se deberá realizar una revisión bibliográfica para profundizar el conocimiento en el área de investigación en la que se desarrollará el proyecto, así como las tecnologías y las diferentes propuestas existentes. Se recurrirá a técnicas comparativas para establecer las características comunes y diferenciales de las metodologías de análisis forense y de las herramientas forenses disponibles para trabajar con la tecnología Blockchain, con énfasis en los espacios de estudio dedicados a la cadena de custodia.

Desde el punto de vista ingenieril, las propuestas de gestión de proyectos según lineamientos del PMI (Project Management Institute), o métodos ágiles como “scrum”, servirán de utilidad para este trabajo.

El plan de trabajo incluye el desarrollo de sucesivas actividades que, con el grado de paralelismo y secuencialidad suficiente, permitan lograr los resultados esperados. Las actividades paulas son las siguientes: a) Estudio del Estado del Arte sobre Cadena de Custodia; b) Estudios del Estado del Arte sobre tecnologías Blockchain aplicadas al ámbito de la Justicia; c) Estudio de la normativa legal nacional e internacional aplicable a este tipo de tecnologías; d) Análisis de requerimientos sobre la trazabilidad de la Cadena de Custodia; e) Diseño y desarrollo de un modelo de la arquitectura de software de tipo Blockchain en la nube, para el desarrollo a futuro de una aplicación informática específica para la gestión documental de la Cadena de Custodia; f) Desarrollo de publicaciones de avance sobre la investigación realizada.

Conclusiones

Respecto de la tecnología Blockchain, la solución que se plantea es factible de ser implementada como una aplicación descentralizada de contratos inteligentes. La utilización de la Cadena de Custodia para el resguardo de las garantías de admisibilidad de la evidencia debe mantenerse durante todo el proceso penal, y es factible reemplazar el formato papel del registro actual con una aplicación informática sostenida en estructura de alta seguridad como las tecnologías de registro distribuido, manteniendo y fortaleciendo los criterios de trazabilidad, preservación y confidencialidad que debe respetarse durante el tratamiento de cualquier tipo de evidencia judicial.

A la fecha el proyecto se encuentra recién iniciado, y es de esperar que, con el modelo de arquitectura de software construido, sea posible el desarrollo e implementación de una aplicación informática destinada al registro de la Cadena de Custodia de la evidencia digital, como continuación de la línea de investigación.

Referencias

Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In *Blockchain and Clinical Trial* (pp. 149-168). Springer, Cham. http://blog.hakzone.info/wp-content/uploads/2020/05/Blockchain-for-Modern-Digital-Forensics-The-Chain-of-Custody-as-a-Distributed-Ledger.pdf [Consultado el 23/04/2022].

AJEA- Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1145.2022

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-coc: A blockchain-based chain of custody for evidences management in digital forensics. *arXiv preprint arXiv:1807.10359*. https://arxiv.org/abs/1807.10359 [Consultado el 23/04/2022].

Chaia, R. A. (2013). *La prueba en el proceso penal*. Hammurabi.

Gisbert Soler, V., & Pérez Molina, A. I. (2019). Blockchain vs ISO 9001: 2015. *3C Tecnología*, *8*(2), 37-48. https://riunet.upv.es/bitstream/handle/10251/157520/Gisbert?sequence=1 [Consultado el 09/09/2022].

ISO 22095:2020(en. Chain of custody — General terminology and models https://www.iso.org/obp/ui/es/#iso:std:iso:22095:ed-1:v1:en [Consultado el 09/09/2022]

Lone, A. H., & Mir, R. N. (2018). Forensic-chain: Ethereum blockchain based digital forensics chain of custody. *Sci. Pract. Cyber Secur. J*, *1*, 21-27. https://www.researchgate.net/publication/321746762_Forensic-chain_Ethereum_blockchain_based_digital_forensics_chain_of_custody [Consultado el 23/04/2022]

Ministerio de Seguridad de la Nación (2021). PROTOCOLO DE ACTUACIÓN PARA LA INVESTIGACIÓN CIENTÍFICA EN EL LUGAR DEL HECHO. http://servicios.infoleg.gob.ar/infolegInternet/anexos/355000-359999/357248/norma.htm [Consultado el 22/04/2022]

Ministerio Público Fiscal de la Nación (2015). MANUAL DE PROCEDIMIENTOS DEL SISTEMA DE CADENA DE CUSTODIA. https://www.mpf.gob.ar/capacitacion/files/2015/07/Cadena-de-Custodia.pdf [Consultado el 22/04/2022]

Querro, S.E. (2020). Smart Contracts. Qué son, para qué sirven: IJ Editores.

Sandoval, Z. M. P. (2020). Garantías procesales en la justicia digital. *La Revista Temas Procesales Vol. 33*

Tanadi, Y., Soeprajitno, R. R. W. N., Firmansah, G. L., & El Karima, T. (2021). ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology. *Riset Akuntansi dan Keuangan Indonesia*, *6*(2), 198-204. https://journals.ums.ac.id/index.php/reaksi/article/download/15146/7012 [Consultado el 09/09/2022]

Torres Zúñiga, V (2021). Aplicaciones de la Tecnología Blockchain en el Área Forense. https://www.researchgate.net/profile/V-Torres-Zuniga/publication/350850167_Aplicaciones_de_la_Tecnologia_Blockchain_en_el_Area_Forense/links/6075fd4e299bf1f56d560351/Aplicaciones-de-la-Tecnologia-Blockchain-en-el-Area-Forense.pdf [Consultado el 22/04/2022]