Una Propuesta de utilización de Smart Contracts en el análisis de evidencia digital.

Sanchez, Ernesto
esanchez@ucasal.edu.ar
Facultad de Ingeniería, UCASAL
Arguimbau, Milagros
marguimbau@frch.utn.edu.ar
Facultad Regional Chubut, UTN
Parra, Herminia Beatriz
bgallo@ucasal.edu.ar
Facultad de Ingeniería, UCASAL

Abstract. *En los últimos años, el análisis forense digital ha cobrado relevancia importante, ya que los hechos que quedan registrados en dispositivos digitales se tornan esenciales para determinar y fundamentar la culpabilidad o inocencia del demandado ante un jurado. Por este motivo, la confiabilidad, autenticidad e integridad de las pruebas electrónicas son fundamentales para su admisibilidad en los tribunales. Es por esto que son muchas las organizaciones que trabajan constantemente en propuestas de marcos de trabajo que permitan estandarizar los procedimientos, principios de calidad y enfoques involucrados en el proceso de análisis antes mencionado. En una situación ideal, todos los laboratorios de forensia digital deberían adoptar el mismo protocolo de análisis siguiendo los estándares, pero en la práctica, la medida en que se puede lograr dicha armonización puede estar limitada por la experiencia personal, la disponibilidad de herramientas o equipos y otros factores. En base a esto, el presente trabajo tiene por objetivo proponer el uso de la tecnología de Blockchain, mediante el modelado de Smarts Contracts para el proceso de análisis de evidencia digital, que permitirá unificar y estandarizar procedimientos que aseguren la obtención de exámenes forenses de calidad.*

Palabras Clave: Forensia Digital, Blockchain, Smart Contracts, Análisis.

.

Introducción

El análisis forense digital ha cobrado relevancia importante en los últimos años como consecuencia de la incorporación y uso de dispositivos tecnológicos en procesos y actividades cotidianas de las personas, tanto en lo personal como en otros ámbitos. Es así como todo hecho cotidiano queda registrado por acción propia o por cámaras de seguridad. Estos registros se almacenan como datos digitales, textos, imágenes, o archivos multimedia.

En casos de un delito, donde tales dispositivos tecnológicos contengan registros vinculados al hecho, se tornan esenciales para determinar y fundamentar la culpabilidad o inocencia del demandado ante un jurado.

El proceso forense digital es una ciencia informática forense que implica el proceso de recolección, adquisición, análisis y presentación de la evidencia encontrada en dispositivos y medios electrónicos para su uso en un tribunal de justicia. Al tratarse de registros de datos almacenados de manera digital, éstos son susceptibles de ser eliminados o alterados de manera voluntaria o involuntaria. Por este motivo, la confiabilidad, autenticidad e integridad de las pruebas electrónicas son fundamentales para su admisibilidad en los tribunales [1].

La autenticidad de la evidencia electrónica se refiere principalmente a que “la información digital obtenida del

dispositivo, es en esencia, una representación fiel y precisa de los datos originales contenidos en el mismo", mientras que la integridad hace referencia a que tanto el dispositivo como los datos requeridos para ser presentados como pruebas son los mismos que se incautaron originalmente y posteriormente se tomaron en custodia", mientras que la confiabilidad se refiere a la medida en que un instrumento de investigación obtiene sistemáticamente los mismos resultados si se utiliza en la misma situación en repetidas ocasiones. [2]
Una alternativa que se presenta como un mecanismo para garantizar la confiabilidad, autenticidad e integridad en el proceso forense digital, es el uso de Blockchain, ya que por la metodología operativa abierta y distribuida similar a la de un libro de contabilidad foliado permite registrar transacciones entre dos partes de manera eficiente, verificable y permanente [3]. Al almacenar, compartir y sincronizar datos en una red de computadoras distribuidas por el mundo, la cadena de bloques puede resolver efectivamente el problema de la pérdida y falsificación de datos, reduciendo así los costos de información y confianza dado que proporciona un método más fiable para el tratamiento de las evidencias digitales [4].
Por ello, atendiendo a las ventajas de seguridad de Blockchain, el presente trabajo tiene por objetivo, presentar una propuesta de modelado de contrato inteligente para el proceso de análisis de evidencia digital, identificando los usuarios participantes, los atributos del contrato, el diagrama de transición de estado y modelo integrado del mismo.
Este artículo se organiza de la siguiente manera: la Sección 1 describe conceptos generales de la tecnología Blockchain, Smart Contracts y su aplicación a la forensia digital, la Sección 2 presenta una revisión de Guías y Buenas Prácticas en el Análisis de Evidencia Digital, la Sección 3 describe una propuesta técnico-informática que podría tomarse como base para aplicar las recomendaciones descritas en la sección anterior. Por último, la Sección 4 describe las conclusiones del trabajo.

I. La tecnología Blockchain

La tecnología Blockchain se puede describir brevemente como una lista de bloques vinculados mediante punteros hash para conformar una red descentralizada y distribuida de todas las transacciones de las que participan los integrantes en su red. Similar al registro contable en un libro mayor, cada integrante constituye un nodo de la red y mantiene una copia completa de ese libro. utiliza un sistema de verificación segura y confiable que no requiere de la participación de terceros
Cuenta con tres principios básicos técnicos: a) replicación del libro mayor entre todos los integrantes de la cadena y que mantiene el historial de todas las transacciones; b) uso de la criptografía tanto para garantizar la seguridad y privacidad de las transacciones como para confirmar la identidad de los participantes y, c) un algoritmo de consenso para definir las reglas que regulan la incorporación de nuevos bloques a la cadena o la modificación de los existentes [5].
En el ámbito de la forensia digital, esta tecnología ofrece beneficios sustanciales para todos los procedimientos de investigación forense, que incluyan la recopilación de datos, preservación, validación de evidencia, análisis de datos y la presentación del hallazgo. Específicamente, la cadena de bloques puede mejorar la transparencia y fiabilidad en cada una de las etapas anteriores. Por ejemplo, un perito podría identificar y seguir la trazabilidad de la evidencia con el objetivo de garantizar la veracidad y completitud de los resultados del análisis forense [6].

De acuerdo con Blockchain Federal Argentina, el proceso de análisis de evidencias digitales, involucra la ejecución de un conjunto de etapas, las cuales pueden considerarse como un flujo de tareas. Es así como, con el aporte de Blockchain, es posible crear "Smart Contracts", los cuales pueden ejecutarse como transacciones dentro de Blockchain. En un smart contract es posible programar un flujo de tareas preestablecido entre partes interesadas, apoyado en todas las garantías de confianza y transparencia que nos da una red de cadena de bloques, permitiendo seguir una trazabilidad del proceso de análisis de evidencias digitales. [7]

Algunos de los beneficios del uso de Smart Contracts en la forensia digital son:

- Confiabilidad: El elemento de evidencia se puede cifrar dentro de la Blockchain.
- Velocidad: Los contratos inteligentes pueden reducir significativamente los tiempos de examinación de las evidencias digitales.
- Ahorro: Permiten ahorrar costos por servicios de terceros como escribanos, notarios, testigos, etc.
- Precisión: Los contratos inteligentes se ejecutan bajo la supervisión de los nodos que forman parte de la red Blockchain, lo que garantiza su seguridad e inmutabilidad.

II. Guías y Buenas Prácticas en el Análisis de Evidencia Digital.

Con el propósito de identificar y comprender las acciones, herramientas de hardware, software y personal técnico intervinientes en el proceso de análisis de evidencias digitales, se realizó una revisión de publicaciones que a modo de conjunto de buenas prácticas proponen un marco de trabajo para los procedimientos, principios de calidad y enfoques involucrados en el proceso de análisis antes mencionado.

En [8], se identifican etapas múltiples que pueden operar en serie, en paralelo o en una combinación híbrida de acuerdo a los requisitos de análisis que se lleven a cabo, según se observa en la Figura 1.

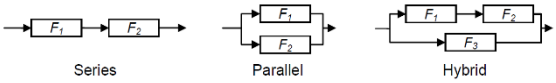

Figura 1: Mapeo de estados en el proceso de análisis de evidencia digital [8]

En [9] se detallan las siguientes recomendaciones:

- Se debe acordar y documentar una estrategia de examen entre el solicitante y el examinador.
- Si es posible, se debe evitar realizar un examen en los medios de prueba originales. Los exámenes deben realizarse en copias forenses o mediante archivos de imágenes forenses.
- Se deben utilizar controles y estándares apropiados durante el procedimiento de examen.
- El examen de los medios debe completarse de manera lógica y sistemática de acuerdo con los estándares de procedimientos del laboratorio que interviene en la etapa de análisis de la evidencia digital.

En [10] se menciona que la elección de la estrategia de trabajo más adecuada para determinados casos sólo puede hacerse en el momento del examen por parte del experto forense. Dadas las mismas circunstancias del caso, idealmente todos los laboratorios adoptarían el mismo protocolo de análisis, pero en la práctica, la medida en que se puede lograr dicha armonización puede estar limitada por la experiencia personal, la disponibilidad de herramientas o equipos y otros factores. Las diferencias en los sistemas legales también pueden afectar el protocolo de análisis. Por lo tanto, este protocolo puede actuar solo como una guía.

Sobre la base de esta última consideración, creemos que, si se aplicara la tecnología de Smart Contracts al proceso de análisis de evidencia digital, se podría contar con un protocolo estandarizado que garantice la calidad y veracidad de los resultados del proceso de análisis.

III. Modelado de Smart Contract

Como parte de las tareas iniciales a la propuesta de modelo de Smart Contract, se identifican las siguientes actividades en el proceso de análisis de evidencia digital:

- Recepción, desembalaje y documentación de inspección visual del dispositivo digital.
- Selección del hardware y software a utilizar para realizar la copia/imagen de la información contenida en el dispositivo digital. Documentación del procedimiento utilizado.
- Selección de la herramienta de software para la recuperación y adquisición de los datos almacenados en el dispositivo digital. Documentación del procedimiento utilizado.
- Elaboración de reporte de los datos obtenidos y recuperados del dispositivo digital.
- Devolución del dispositivo digital.

A continuación, se presenta el uso de Smart Contracts para el caso particular donde el activo físico a registrar en la cadena de bloques es el dispositivo digital, (PC, notebook, pendrive, Smartphone, tarjeta de memoria, etc.), sobre el cual se realizará el análisis forense.

Se identifican 4 (cuatro) participantes:

1. Personal Técnico que realiza la recepción y copia de datos del dispositivo digital.
2. Perito forense que realiza la recuperación y análisis de los datos de la copia obtenida.
3. Responsable del laboratorio forense que audita el reporte del análisis de la evidencia digital.
4. Autoridad o funcionario del Sistema Judicial.

Se establecen los siguientes atributos del contrato:

- Tipo de dispositivo digital
- Fecha y hora de recepción
- Responsable de copia de seguridad
- Perito que realiza el análisis y reporte
- Auditor que realiza revisión del reporte
- Fecha y hora de entrega
- Autoridad a quien se entrega informe

Según se define en el manual de referencia de Ethereum [11], en el contexto de una Cadena de Bloques, un “Estado” es una gran estructura de datos y una “Transacción” permite el cambio de un estado a otro. Estas transacciones se transmiten a toda la red. Cualquier nodo puede transmitir una solicitud para que se ejecute una transacción. A continuación, un validador autoriza y ejecuta la transacción propagando el cambio de estado resultante al resto de la red. Teniendo en cuenta este principio, en la Figura 2 se propone el Diagrama de Transición de Estado que describe el siguiente proceso:

- Recepcionado: La evidencia que se recibe para ser analizada, alcanza este estado luego de registrarse los datos que identifican el tipo de evidencia, acta de cadena de custodia, fecha y hora de recepción, datos personales de quien la entrega.
- Copiado: Sobre la evidencia recepcionada, en caso de que corresponda, se realiza una copia de seguridad, según los estándares descritos por Interpol [12], se registran fecha y hora de inicio y fin del copiado, datos del personal técnico que realiza la copia, herramienta de hardware y/o software utilizada, así como la técnica aplicada.

- Analizado: Sobre la copia realizada se procede al análisis forense de la misma, donde se debe registrar fecha y hora de inicio y fin de la tarea, datos del perito que realiza la misma, herramienta de hardware y/o software utilizado e informe de análisis realizado.
- Auditado: Según las recomendaciones descritas por el Working Group Forensic IT [10], el informe de análisis puede ser auditado por el especialista responsable del laboratorio, debiéndose registrar de fecha y hora de la actividad realizada, datos del responsable e informe de auditoría. Si la auditoría resultara satisfactoria, se pasa al estado final, caso contrario, se vuelve al estado anterior.
- Entregado: El informe final del análisis forense se entrega al funcionario de justicia que solicitó el mismo, se deja registro de fecha y hora de entrega, acta de recepción, e informe.

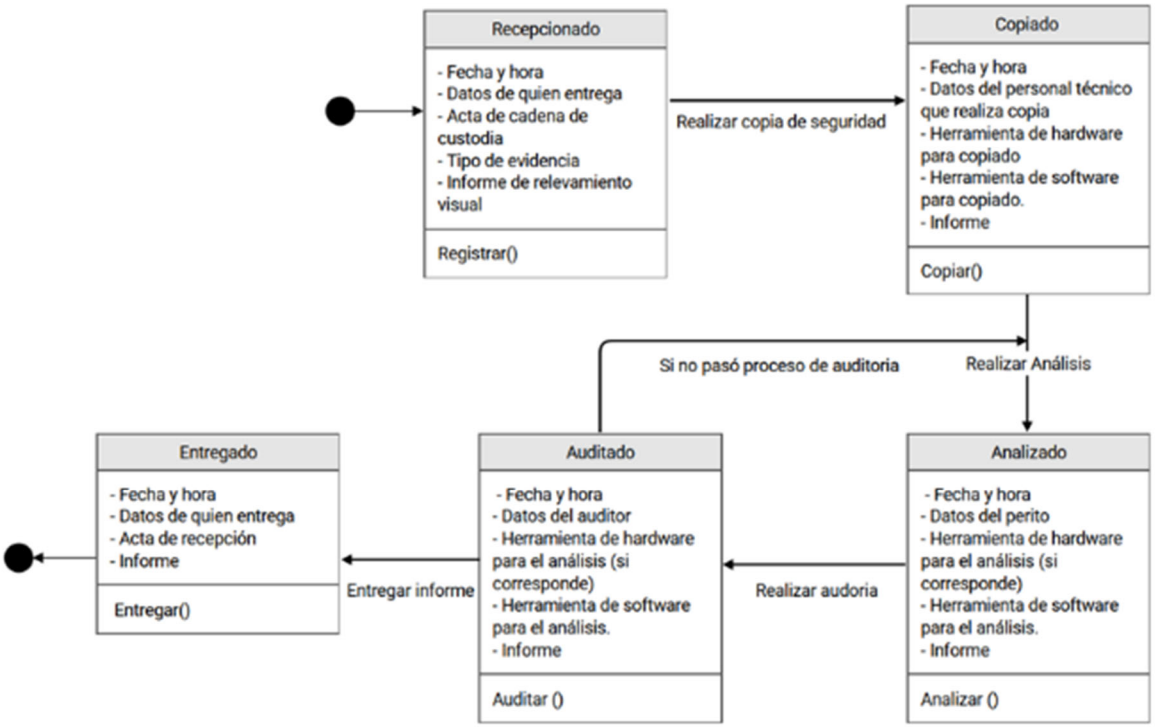

Figura 2: Diagrama de transición de estados en un Smart Contracts de Análisis de evidencia.

La actividad final de esta etapa de diseño se puede resumir en la Figura 3 que muestra la relación entre todos los elementos que definen el caso de uso de Smart Contracts aplicado al análisis de evidencia digital. Esta etapa inicial, es el punto de partida para la elección del lenguaje de programación para la implementación del contrato dentro de una Cadena de Bloques. Se puede observar la relación existente entre el activo, (evidencia), las acciones para modificar los estados del activo, (Recepcionado, Copiado, Analizado, Auditado, Entregado), las ejecuciones de transacciones que permiten los cambios de estados y los participantes, en este caso particular, el Laboratorio de Forensia Digital y el Sistema Judicial.

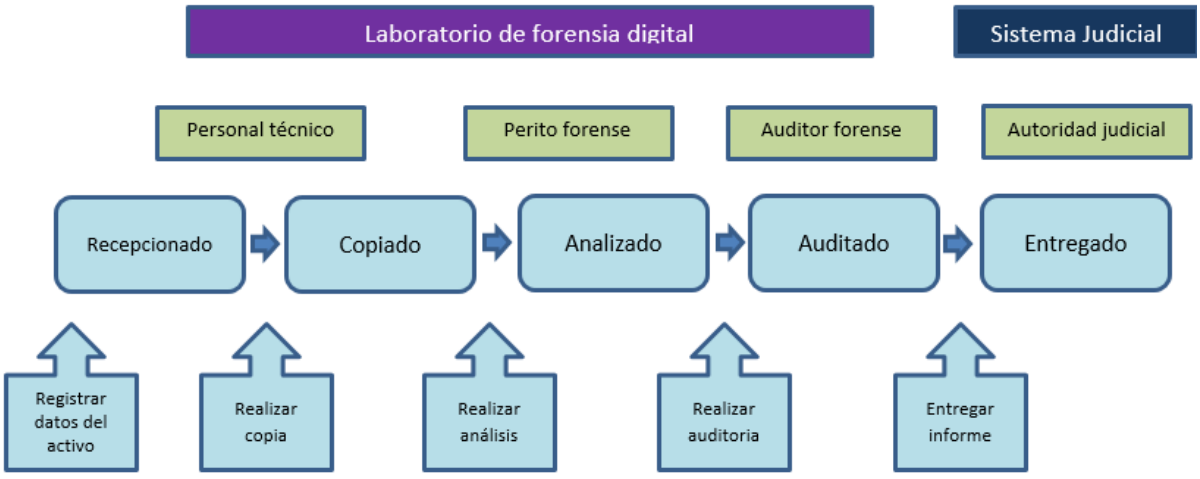

Figura 3: Modelo Integrado de Smart Contracts aplicado al análisis de evidencia digital.

Consideraciones sobre la tecnología Blockchain y lenguaje de programación para Smart Contracts

Por tratarse de un sistema que estará restringido a personas involucradas en casos judiciales, donde se debe identificar a los participantes, se propone una red Blockchain de tipo privada Ethereum dado que la misma es ampliamente utilizada, en conjunto con el lenguaje Solidity para la programación de los Smart Contracts. En cuanto a aspectos de seguridad, se sugiere la implementación de un Sistema híbrido basado en los mecanismos de consenso, "Prueba de Participación, (PoS)" y "Prueba de Trabajo, (PoW)" [14]. Por ultimo consideramos a futuro, analizar la viabilidad económica para la implementación de esta tecnología por lo que recomendamos seguir la propuesta de un marco de trabajo presentado en *"Blockchain feasibility assessment: A quantitative approach"* [15].

IV. Conclusiones

En la actualidad los sistemas judiciales no cuentan con técnicas, procedimientos, ni herramientas de hardware y software estandarizados, para el tratamiento y análisis de evidencias digitales. En algunos casos, ni siquiera se cuenta con profesionales informáticos certificados en forensia digital, por lo que deben recurrir a la asistencia de otras fuerzas externas al sistema Judicial como Policía Federal, PSA, Gendarmería, etc., Esto podría traer como consecuencia que se generar errores en los procesos e interpretaciones de los resultados obtenidos.

Sin duda alguna, contar con un contrato inteligente para el proceso de análisis de una evidencia digital, permitirá unificar y estandarizar procedimientos que aseguren la obtención de exámenes forenses de calidad. Se espera que la presente publicación siente las bases para futuros trabajos tendientes a la implementación de la tecnología de cadena de bloques en el proceso de análisis de evidencia digital.

Asimismo, consideramos que esta propuesta debe integrarse al proceso de análisis de evidencias digitales, por lo cual encontramos pertinente integrar la misma al trabajo realizado en Aplicación de Blockchain a la Cadena de Custodia de la Evidencia Judicial. [13]

Referencias Bibliográficas

[1] Computer Forensics: Digital Evidence. (2019). https://resources.infosecinstitute.com/topics/digital-forensics/computer-forensics-digital-evidence/

[2] "A Blockchain Enabled System for Security, Non-Repudiation and Integrity of Judiciary Proceedings", Velde, V., Parvez, F.A., Chaitanya. (2022). 1st International Conference on Electrical, Electronics, Information and Communication Technologies, ICEEICT 2022

[3] "Electronic evidence and its authenticity in forensic evidence". Moussa, A.F. (2022). Egyptian Journal of Forensic Sciences.

[4] "Electronic evidence in the blockchain era: New rules on authenticity and integrity". H. Wu, G. Zheng, (2020). Computer Law & Security Review, Vol 36

[5] "Bitcoin: A Peer-to-Peer Electronic Cash System". S. Nakamoto. (2008). https://www.debr.io/article/21260.pdf

[6] "Blockchain based Digital Forensics Investigation Framework in the Internet of Things and Social Systems". Shancang Li. (2019). Publisher IEEE Volume 6. https://ieeexplore.ieee.org/document/8777292

[7] "Smart Contracts". Blockchain Federal Argentina. (2023). https://bfa.ar/blockchain/smart-contracts

[8] "Best Practice Manual for the Forensic Examination of Digital Technology". (2015) ENFSI-BPM-FIT-01. www.enfsi.eu.

[9] "Best Practices for Computer Forensics". Scientific Working Group on Digital Evidence. (2015). https://www.oas.org/juridico/spanish/cyb_best_pract.pdf.

[10] "Guidelines for Best Practice in the Forensic Examination of Digital Technology". (2014). Working Group Forensic IT. https://cryptome.org/2014/03/forensic-digital-best-practice.pdf.

[11]Ethereum development documentation. (2023). https://ethereum.org/en/developers/docs/evm/.

[12] Guidelines for Digital Forensics First Responders. Interpol. (2021). https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf.

[13] Aplicación de Blockchain a la Cadena de Custodia de la Evidencia Judicial. B. P de Gallo. (2023). Proc. of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME).

[14] "A Hybrid POW-POS Implementation Against 51% Attack in Cryptocurrency System". K. Gupta, A. Rahman, S. Poudyal, M. Huda, M. Mahmud. (2019). https://www.ieeexplore.ieee.org/document/8968856

[15] Blockchain feasibility assessment: A quantitative approach. S. Spencer, S. L. Schutte, J. Vlok. (2023). https://www.frontiersin.org/articles/10.3389/fbloc.2023.1067039/full