Almacenamiento de evidencias digitales soportado con blockchain privada.

Oscar Mauricio Cubillos Jiménez, Hernán Alberto Laborde, Laura Sofia Arias.

Resumen

La Fiscalía General de la Nación (FGN) es el principal órgano rector de la investigación y acusación penal en la República de Colombia. Sus actos investigativos abarcan desde delitos comunes, sindicatos criminales ramificados, insurgencia militar armada, y hasta delicados asuntos de seguridad nacional (CONSTITUCION POLITICA DE COLOMBIA 1991). Las evidencias digitales, recolectadas en diferentes tipos de dispositivos electrónicos, constituyen uno de los elementos fundamentales para esclarecer los hechos en esa amplia variedad y complejidad de casos. En la actualidad la FGN graba estas evidencias en medios ópticos y esto se guardan en depósitos o bodegas físicas. La naturaleza física de estos respaldos tiene ciertas características que exponen las evidencias durante el proceso judicial y durante el paso del tiempo. Los intereses criminales capaces de corromper funcionarios, el desarrollo de ciberataques cada vez más sofisticados capaces de alterar sistemas de información, los extravíos, así como también del deterioro de los materiales de fabricación de los medios ópticos son algunas de las amenazas a las que están expuestas las evidencias digitales.
En el presente trabajo presentamos una arquitectura tecnológica que tiene como objetivo conformar un Almacén de Evidencias Digitales que garantice la confidencialidad, integridad y autenticidad de la evidencia digital y la trazabilidad de la cadena de custodia.
La innovación propuesta en el presente trabajo consiste en el almacenamiento de los archivos de las evidencias en equipos de almacenamiento inmutable con redundancia en múltiples equipos junto con la incorporación de una red blockchain privada la cual contendrá un registro cronológico también inmutable de todas las actuaciones realizadas sobre las evidencias.

Palabras clave

Almacenamiento de evidencia digital, elemento material probatorio, imagen forense, blockchain privada, criptografía, Hyperledger Fabric.

I. INTRODUCCION

Para la Fiscalía General de la Nación y el derecho penal en general, la prueba es la piedra angular de cualquier investigación, y más si se trata de demostrar la culpabilidad de la(s) persona(s) que cometieron un delito. Esta entidad maneja grandes cantidades de evidencia como computadores, drones, discos duros, celulares, entre otros.

El deterioro, pérdida, acceso abusivo o alteración del Elemento Material Probatorio (EMP) y/o Evidencia Física (EF) puede ocasionar la pérdida de casos y por ende la Fiscalía debe indemnizar al acusado; generándole grandes pérdidas monetarias y reputacionales al Estado.

Las Organizaciones del Poder Judicial deben garantizar el debido proceso en los actos de investigación orientados a la obtención de evidencias. Por lo tanto, es crucial garantizar la integridad, confidencialidad y no repudio de la información recolectada.

Teniendo esto en cuenta, el siguiente proyecto tiene como objetivo diseñar un Almacén de Evidencia Digital para la Fiscalía General de la Nación, para almacenar las imágenes forenses obtenidas al realizar extracciones en los operativos, dando cumplimiento a los requisitos de seguridad que asegurarán la NO pérdida o desestimación de evidencia digital.

II. ARQUITECTURA PROPUESTA

A. Manejo de evidencia digital

La recolección de evidencia digital a partir de discos duros se hace mediante una estación de trabajo forense llamada Tableau TX1, la cual sirve para obtener las imágenes forenses de este tipo de dispositivos, tal como se muestra a continuación:

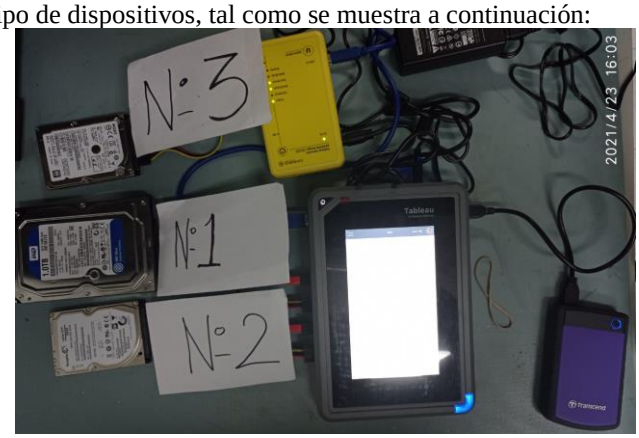

Ilustración 1. Adquisición de evidencia con Tableau TX1. Fuente: Elaboración propia

Para celulares se utiliza un kit de accesorios para conectar el celular con la estación de trabajo.

Ilustración 2. Conexión del celular a la estación de trabajo mediante dispositivo UFED 4PC. Fuente: recuperado de https://teeltech.com/mobile-device-forensic-tools/cellebrite/ufed-4pc/

Como se puede ver en la imagen anterior, se tiene un accesorio de la marca Cellebrite, el cual contiene el software Cellebrite UFED 4PC. Este hace el reconocimiento del dispositivo y muestra un resultado como el que se ve a continuación:

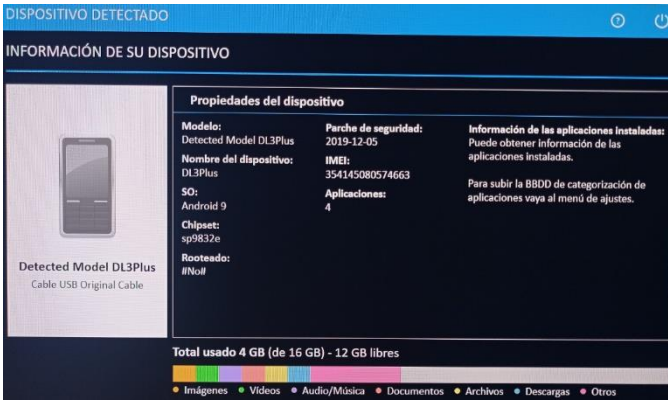

Ilustración 3. Vista de las propiedades del celular. Fuente: Elaboración propia

Luego de la adquisición de la imagen forense, el software genera un resultado parecido a la siguiente imagen:

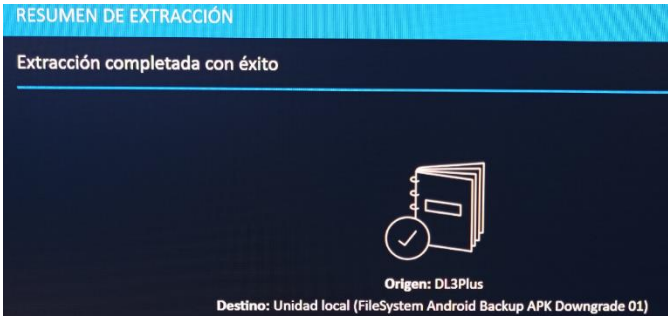

Ilustración 4. Vista de finalización de la extracción. Fuente: Elaboración propia

B. Almacén de evidencia digital

Luego del levantamiento de la evidencia forense, surge la necesidad de almacenarla asegurando la integridad y registrando la trazabilidad de la cadena de custodia. El sistema que proponemos se basa en dos pilares:

El almacenamiento en un sistema de archivos (File System) y en una Blockchain Privada complementaria donde quedarán registradas todas las interacciones realizadas con la evidencia a lo largo de su ciclo de vida.

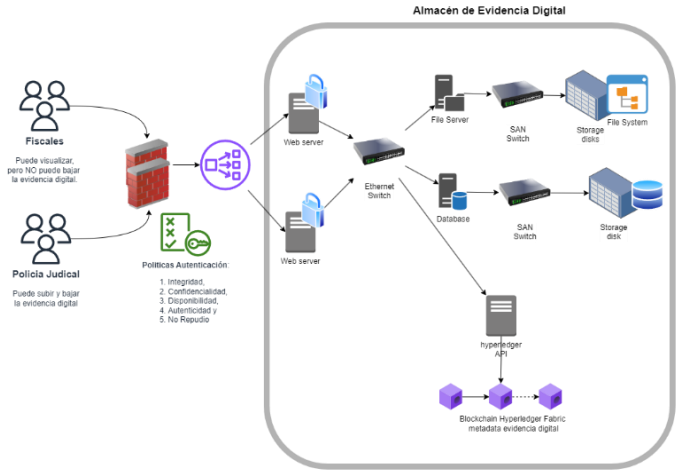

Ilustración 5. Arquitectura de alto nivel propuesta. Fuente: Elaboración propia

La interacción con el almacén digital estará acotada a solo dos tipos de usuarios del poder judicial: Los Fiscales y los Agentes de la Policía Judicial. Cada uno de estos grupos tendrá roles y políticas de acceso diferenciados, que establecerán el marco de operación sobre las evidencias.
Como podemos ver en el diagrama anterior los usuarios tendrán acceso a una aplicación web.
El proceso se iniciará cuando un Agente de Policía Judicial (APJ), después de autenticarse, sube la evidencia a través de la aplicación web.

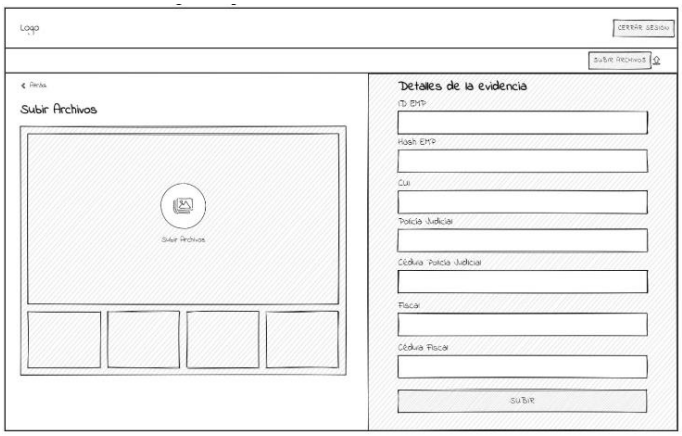

Ilustración 6. Prototipo de vista para cargar evidencia. Fuente: Elaboración propia

En el formulario de subida el APJ deberá indicar el CUI (código único de investigación), su número de cédula de ciudadanía, y el número de cédula de ciudadanía del fiscal asignado al caso. El identificador de EMP (ID_EMP) será un código

autogenerado por el sistema, y los nombres, tanto del APJ como del Fiscal, no se cargarán manualmente, sino que serán cargados a partir de una subconsulta al sistema del SPOA.

Luego de cargados estos datos el APJ podrá actualizar solo el número de cédula del Fiscal y también podrá transferir la custodia de la evidencia a otro APJ.

Los Fiscales por su lado solo podrán visualizar la evidencia y la cadena de custodia, pero no podrán hacer cargas de evidencias, cambios en el expediente ni transferencias de custodia de ningún tipo.

C. Almacenamiento Inmutable

Definición

El almacenamiento masivo es una solución que consiste en albergar grandes cantidades de datos de manera persistente en un entorno IT (Rouse, 2013); es decir, en un ecosistema digital que utiliza tácticas digitales que interactúan entre sí a fin de conseguir un objetivo en un contexto determinado (La importancia del ecosistema digital, 2023).

Esquema de la solución de almacenamiento masivo

Ese contexto consiste en una red de varios dispositivos de almacenamiento interconectados para compartir recursos a varios servidores denominado Red de Area de Almacenamiento o SAN, por sus siglas en inglés (Bigelow, 2023). Teniendo en cuenta que esta solución encaja perfectamente para el cumplimiento del objetivo del presente proyecto, pues cumple con todos los requerimientos de redundancia y ASL Tier 2:

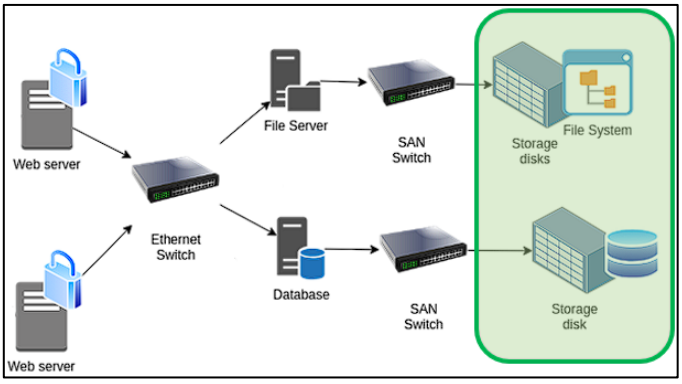

Imagen 05: Topología de red para el almacenamiento masivo

Para determinar el tamaño del almacenamiento inicial para la solución propuesta, tomamos como referencia los siguientes datos:

- Cantidad de evidencias registradas en el sistema de información SPOA en 19 años: 4’285,564.
- Cantidad de evidencias por año promedio: 225,556.
- Participación de las evidencias digitales en la cantidad de sus similares en SPOA por año: 55%, 124,055.

Considerando que el tamaño promedio de un archivo de evidencia digital es de 48 GB, podemos realizar una proyección anual de la cantidad de espacio requerido: 5,815.12 TB (5.68 PB).

Así las cosas, al buscar dentro de los no pocos dispositivos que existen en el mercado, se toma como referencia, sin prejuicio de descartar otras marcas y modelos, el Dell PowerProtect DP5900, el cual tiene las siguientes características en cuanto a niveles de seguridad y almacenamiento:

- Niveles de seguridad ofrecidos:

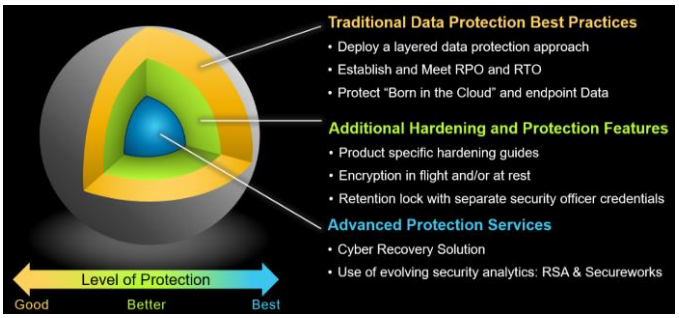

Imagen 06: Niveles de seguridad ofrecidos por la solución de almacenamiento (Recuperado de: https://education.dell.com/content/dam/dell-emc/documents/en-us/2020KS_Steen_Immutable_Data_Protection_for_Any_Application.pdf, página 4).

- Almacenamiento:

	DP4400	DP5900
BACKUP INGEST	Up to 9 TB/hr	Up to 33 TB/hr
LOGICAL CAPACITY[3]	80 TB to 4.8 PB[1] 240 TB to 14.4 PB[2]	960 TB to 18.7 PB[1] 2.8 to 56.1 PB[2]
USABLE CAPACITY	8 to 96 TBu[1, 4] Up to 288 TBu[2]	96 to 288 TBu[1] Up to 864 TBu[2]

Imagen 07: Características del dispositivo Dell PowerProtect DP5900 (Recuperado de: https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/powerprotect-dp-series-appliances-ds.pdf).

Es decir, que, haciendo una relación de máxima capacidad entre la cantidad de evidencia digital almacenada, se tiene que esta es una solución que podría soportar hasta 9 años. Además, también cumple con el requerimiento de inmutabilidad con un máximo de retención por 1827 días, los cuales se pueden prorrogar, garantizando así la integridad y disponibilidad de la información (Van Der Steen, 2020).

D. Selección del tipo de Blockhain.

A la hora de seleccionar una blockchain la primera gran división que encontramos es entre públicas y privadas (Arslanian, 2022).

- *Blockchains Publicas*: Entre ellas encontramos los desarrollos de Blockchain orientados a criptomonedas donde Bitcoin y Ethereum son sus más destacados representantes. Estas redes se caracterizan por no requerir una autorización previa para poder transaccionar y validar transacciones en la blockchain, cualquier nodo puede sumarse sin restricciones y en algunos casos el anonimato de los participantes es permitido. La garantía de la honestidad de los participantes se busca a través de un mecanismo de consenso llamado "Proof of Work" (Prueba de trabajo en Castellano) o Proof of Stake (PoS) (Prueba de Participación en Castellano) que impondría una barrera de costo computacional alto que mantendría alejados a actores maliciosos (Singhal, Dhameja, & Panda, 2018).
- *Blockchains Privadas*: En contraste, las blockchains privadas, requieren una autorización previa y un control estricto de la identidad de los participantes. En este contexto, un mecanismo de consenso como "Proof of Work" con su recompensa por el minado, representaría un costo computacional alto y por lo tanto una ineficiencia innecesaria en la transaccionalidad, por tal motivo en las redes privadas encontramos mecanismos de consenso como RAFT (The Secret Lives of Data, n.d.) o PBFT (Hyperledger, RAFT and BFT, 2023). En Hyperledger podemos podemos utilizar PBFT (Practical Byzantine Fault Tollerance) en el cual todos los nodos tienen una copia interna del estado de la blockchain y están actualizados sobre los resultados computacionales de los otros nodos de la red, con base en esto establecen una decisión final sobre la inclusión de una transacción en la blockchain la cual es también transmitida a todos los nodos. Es importante destacar una propiedad de PBFT, y es que siendo n el total de nodos de la blockchain soportará que hasta un $(n-1)/3$ de los nodos fallen o tuvieran comportamiento malicioso para revertir el consenso (Castro & Liskov, 1999) . Entre las opciones de redes privadas más destacadas, al momento de escribir este trabajo, encontramos a: Hyperledger Fabric (Hyperledger Fabric, n.d.), Corda (Corda, n.d.) y Private Ethereum (Private Ethereum, n.d.) .

E. Hyperledger Fabric

Examinando las características de cada tipo de red optamos, para nuestro presente caso de negocio, por una blockchain privada y en particular por Hyperledger Fabric.

Nuestros criterios de selección de Hyperledger Fabric fueron los siguientes:

1) Es un proyecto open source de The Linux Foundation: Esto nos da una relativa confianza en la continuidad del proyecto, ya que hay una comunidad que enriquece la tecnología dándole mantenimiento al proyecto y adicionalmente cuenta con el respaldo de una organización.

2) La abundancia y calidad de la Documentación: Este punto fue crucial para facilitar el aprendizaje de la tecnología y testear su funcionamiento en con pruebas locales.

3) Hyperledger Fabric ofrece hasta el momento la posibilidad de escribir los "Smart Contracts" en los lenguajes de programación de propósitos generales: Go, JavaScript, o Typescript. En contraste con Ethereum que requiere el aprendizaje de un lenguaje de programación específico como Solidity.

4) De las tres opciones de lenguaje de programación, elegimos Go para escribir los Smart Contracts, debido a que es un lenguaje estrictamente tipado, con una muy buena legibilidad y ampliamente difundido.

III. Roles y Control de acceso

Para Hyperledger una organización es un grupo de miembros con una administración lógica común (Hyperledger, Documentation, 2023), si bien Hyperledger está diseñado para operar con más de una organización, en nuestro caso de la FGN tendremos una sola. Ahora bien cada organización puede subdividirse en múltiples Unidades de Organización (OU), que en nuestro caso serán Fiscalía y Policía Judicial. Y por último cada Unidad de Organización esta compuestas por los diferentes usuarios que serán cada Fiscal y cada Agente de Policía Judicial. Podemos ver en la Ilustración 7 una representación de la estructura con un:

- Una Organización (la FGN)
- Dos Unidades de Organización (OU) (una para la fiscalía y otra para Policía Judicial)
- Dos Tipos de Roles (Fiscales y Policías)

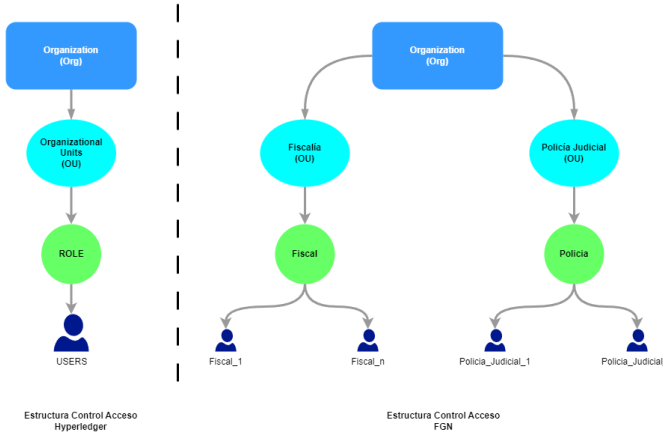

Ilustración 7. Comparativo de control de acceso de hyperledger vs. propuesto por nosotros. Fuente: Elaboración propia

Durante los Actos de Investigación de un caso criminal, la interacción con las evidencias (nuestros activos en la blockchain) será a partir de dos roles concretos: Los Fiscales y los Agentes de Policía Judicial.

Los Agentes de la Policía Judicial son los responsables de recolectar y custodiar la evidencia digital ajustándose al debido proceso. Este rol tendrá los siguientes alcances y limitaciones:

El Agente de Policía Judicial podrá:

- subir evidencias digitales.
- leer evidencias digitales.

El Agente de Policía Judicial no podrá:

- Modificar la evidencia una vez subida,
- Autorizar traslados o procedimientos,
- Anular una evidencia o borrarla.

Debemos pensar a los fiscales como el "gerente" de la investigación, este rol tendrá los siguientes alcances y limitaciones:

El Fiscal no podrá:

- Subir evidencias digitales de ningún tipo.
- Tampoco podrá borrarlas.

El fiscal podrá:

- Ver la evidencia,
- Autorizar o Rechazar la transferencia de la responsabilidad en la cadena de custodia
- Declarar una evidencia nula.

Para implementar la innovación técnica de Blockchain debemos considerar un nuevo rol para la Administración de la blockchain, el cual tendrá la responsabilidad de mantener y actualizar el Chaincode o Smart Contract, como veremos más adelante esto requiere habilidades técnicas y conocimientos de programación que no son propias de los Fiscales, ni de los Agentes de Policía, además la separación de este rol es necesaria para robustecer la seguridad del sistema.

La siguiente tabla describe los permisos que deben tener ambos roles sobre los activos de la blockchain.

Acción sobre el activo	Policía Judicial	Fiscal	SPOA Sync	Admin
Crear	✅	❌	❌	❌
Leer	✅	✅	✅	❌
Modificar	❌	❌	🚦	❌
Borrar	❌	❌	❌	❌
Anular	❌	✅	❌	❌
Transferir Responsabilidad de custodia	❌	✅	❌	❌
Actualizar Chaincode (Smart Contract)	❌	❌	❌	✅

Ilustración 8. Permisos de cada rol. Fuente: Elaboración propia

🚦: Solo para modificar los datos básicos de los Agentes de Policía Judicial y Fiscales (nombre y número de cédula) y estos son automáticamente heredados de la tabla de usuarios del sistema de información SPOA (Sistema Penal Oral Acusatorio).

Hyperledger denomina Membership Service Provider (MSP) a la estructura interna de control de acceso, esta estructura está basada en certificados digitales emitidos por una Autoridad de Certificación (CA). Es muy importante destacar que en Hyperledger absolutamente todas las transacciones son validadas por la blockchain, de acuerdo con las políticas asociadas a los roles, pero esta validación se hace basada fundamentalmente en los certificados digitales que deben acompañar a cada una. Estos certificados pueden emitirse para ser válidos a nivel de OU y se asocian a los roles e incluso a nivel de usuario.

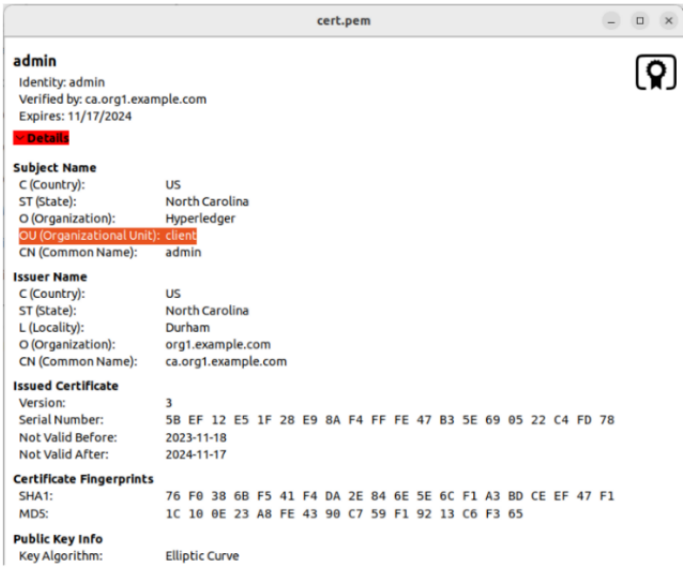

Ilustración 9. Certificado digital del rol Admin de la red. Fuente: Elaboración propia

En la imagen anterior se ve destacado en Naranja cómo se puede detallar la OU en el certificado digital.

Una vez definidos los roles, Hyperledger nos permite establecer políticas diferenciadas que se asocian a esos roles. La documentación de Hyperledger nos define muy bien qué son estas políticas en su documentación: "En su nivel más básico, una política es un conjunto de reglas que definen la estructura de cómo se toman las decisiones y se logran resultados específicos. Con ese fin, las políticas suelen describir un quién y un qué, como el acceso o los derechos que un individuo tiene sobre un activo."

"…representan cómo los miembros llegan a un acuerdo para aceptar o rechazar cambios en la red, un canal o un contrato inteligente." (Hyperledger Fabric)

Es importante explicar la sintaxis utilizada por Hyperledger para definir una política. Esta sintaxis esta basada en tres tipos de operadores: AND, OR y NOutOf.

- **AND**: Requiere que se tenga la validación (endorsment) de todos los elementos dentro del "and". Por ejemplo la siguiente definición: AND('Org1.Ou1.member', 'Org1.Ou1.member') indica que, para considerarse satisfecha, la política requiere la aprobación (endorsement) de dos miembros de Unidad Organizacional 1.
- **OR**: Requiere que se tenga la validación (endorsment) al menos uno de los elementos dentro del "or". Por ejemplo la siguiente definición: OR('Org1.Ou1.member', 'Org1.Ou1.member') indica que, para considerarse satisfecha, la política requiere la aprobación (endorsement) de al menos uno de los miembros de Unidad Organizacional 1.
- **NOutOf**: donde se puede establecer proporciones, por ejemplo: Podríamos indicar que se necesita la aprobación de 2 miembros de la Ou1 y 2 miembros de la Ou2 para considerar la política satisfecha.

En nuestro caso, para poder Transferir la custodia de la evidencia a otro policía judicial por ejemplo, se necesitaría la aprobación (endorsement) del Fiscal y la aprobación del Policía Judicial que la recibe (en este último la aprobación funcionaría como una marca de confirmación de recepción de la responsabilidad de la tenencia de la evidencia).

IV. Observaciones sobre el prototipo

Hyperledger Fabric ofrece en su instalación la posibilidad de desplegar una blockchain de pruebas, siendo posible reconfigurarla para adaptar el ensayo a nuestro caso de negocio. El laboratorio desplegado está basado en contenedores de Docker, que permiten desplegar los nodos de una pequeña red blockchain Hyperledger y una API para realizar operaciones CRUD.

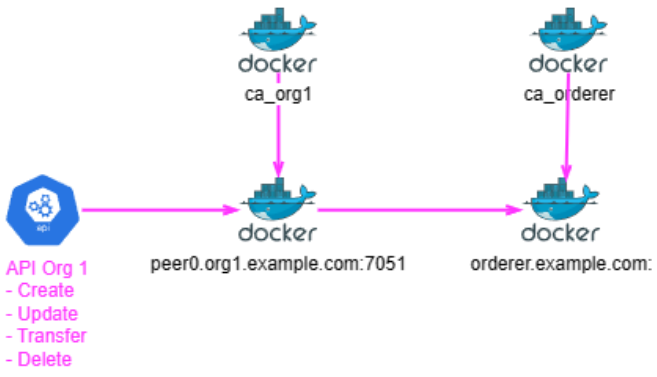

Ilustración 10. Nodos de la red. Fuente: Elaboración propia

Básicamente encontraremos tres tipos de contenedores desplegados: Peers, Orderer y CA.

- **CAs**: Estos componentes son la Autoridad de Certificación en la Hyperledger Fabric (Certificate Authority) y es el encargado de establecer los certificados digitales que tendrán asociados cada uno de los otros componentes (peers y ordereres) y también de los que estén asociados a roles y usuarios.
- **Peers**: Son entidades de red donde se almacena el Chaincode (Smart Code en la terminología de Hyperledger), también se mantiene el Ledger de la blockchain
- **Orderers**: Es un servicio que ordena las transacciones por orden de llegada en un bloque y luego lo trasmite a todos los peers de la red para su validación y commit a la blockchain.

El único activo con el que se realizarán transacciones en la blockchain será el registro de la evidencia, el cual contendrá los siguientes campos:

Nombre del campo	Descripción
ID	Este campo es un identificador único usado solo dentro de la blockchain, pero que puede ser generado fuera de esta de manera arbitraria.
CUI	Código Único de Investigación.
EMP_ID	Id del elemento material probatorio.
Hash_EMP	Hash del EMP generado por la Policía Judicial.
Owner	Nombre completo del Agente de Policía Judicial
NumeroCedulaOwner	Número de cédula del Agente de Policía Judicial.
NombreFiscal	Nombre completo del Fiscal
NumeroCedulaFiscal	Número de cédula del Fiscal
PathArchivoEvidencia	Path del archivo de evidencia digital en el cluster de storage inmutable.

Tabla 1: Diccionario de campos de un activo

Siendo definida la estructura de este en el chaincode (Smart Contract) de la siguiente manera (recordemos que seleccionamos Go como lenguaje de programación):

```
20  type Asset struct {
21      ID                  string `json:"ID"`
22      EMP_ID              string `json:"EMP_ID"`
23      CUI                 string `json:"CUI"`
24      Hash_EMP            string `json:"Hash_EMP"`
25      Owner               string `json:"Owner"`
26      NumeroCedulaOwner   string `json:"NumeroCedulaOwner"`
27      NombreFiscal        string `json:"NombreFiscal"`
28      NumeroCedulaFiscal  string `json:"NumeroCedulaFiscal"`
29      PathArchivoEvidencia string  `json:"PathArchivoEvidencia"`
30  }
```

Ilustración 11. Definición del activo. Fuente: Elaboración propia

En el Chaincode es donde también se definen las acciones que pueden realizarse sobre los activos. Por ejemplo, para crear y para leer un activo tenemos las funciones CreateAsset y ReadAsset que podemos ver en la siguiente figura.

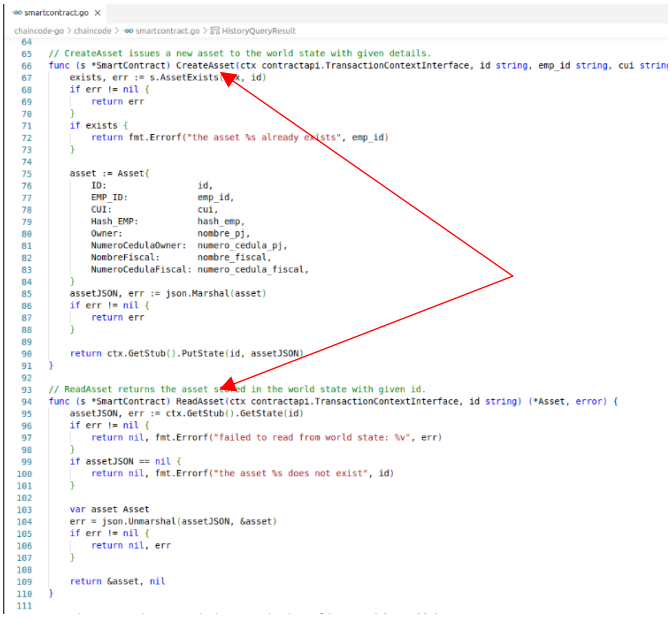

Ilustración 12. Funciones para crear y leer activos. Fuente: Elaboración propia

Estas funciones pueden ser accedidas mediante una API REST. A modo ilustrativo, presentaremos a continuación un ciclo de creación y transferencia de un activo y la posterior consulta de la historia donde podremos ver el registro cronológico de todas las transacciones realizadas. Para ello nos valemos de la herramienta Postman (Postman, n.d.), para la interacción con la API.

Creación de activo con la API: Como podemos apreciar en la imagen realizamos un POST al url de nuestro localhost, pasando como argumentos todos los campos que componen el activo.

Una vez creado el nuevo activo en la red, nos devuelve un ID de Transacción generado desde la blockchain.

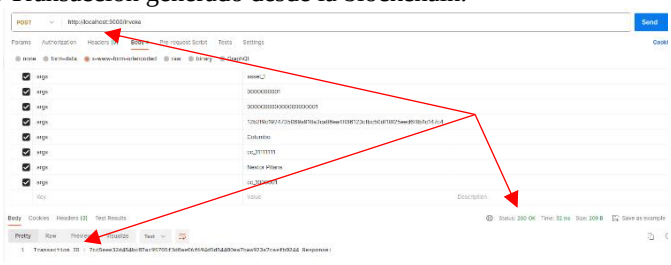

Ilustración 13. Creación de un activo mediante la API. Fuente: Elaboración propia

Transferencia de Activo: Imaginemos ahora que deseamos a transferir la tenencia del activo a otro policía judicial. Esta vez utilizaremos un verbo PUT y pasaremos como argumentos el ID del activo, la cédula de ciudadanía y el nombre del agente de policía judicial que recibirá el activo. Si la transacción se logra hacer exitosamente, la API nos devuelve el Status 200 OK y el ID de la transacción.

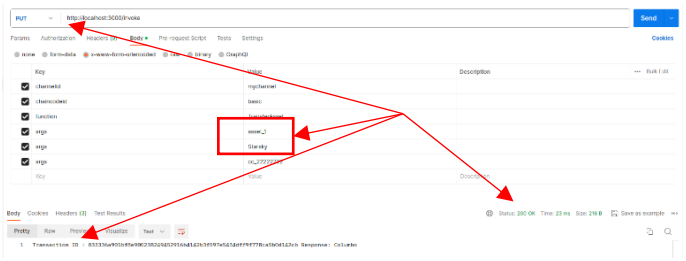

Ilustración 14. Transferencia del activo mediante API. Fuente: Elaboración propia

Consulta de historia del activo: Por último, para poder obtener todo el historial de transacciones que realizamos sobre el activo, invocamos la función GetAssetHistory através de la API pasándole como argumento el ID del activo. La API nos devolverá una lista de elementos en formato json. Dado que la API devuelve el json en formato compacto, tendremos que acomodar el formato para poder visualizar los resultados.

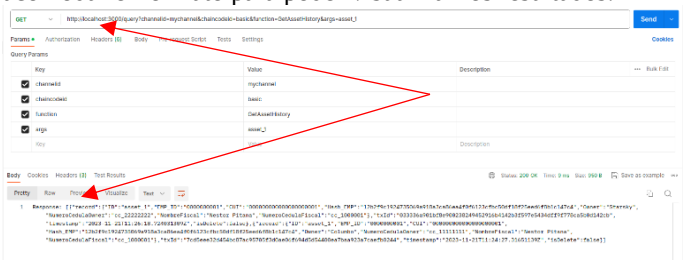

Ilustración 15. Consulta de la historia de un activo mediante API. Fuente: Elaboración propia

La siguiente es una presentación de la respuesta en un formato más amigable para el ojo humano:


```
[
    {
        "record":
        {
            "ID": "asset_1",
            "EMP_ID": "0000000001",
            "CUI": "00000000000000000001",
            "Hash_EMP": "12b2f9c1924735069a918a3ca86ea4f0f6123cfbc50df18f25eed6f8b1c147c4",
            "Owner": "Starsky",
            "NumeroCedulaOwner": "cc_22222222",
            "NombreFiscal": "Nestor Pitana",
            "NumeroCedulaFiscal": "cc_1000001"
        },
        "txId": "033336a901bf8e900238249452916b4142b3f597e5434dff9f778ca5b0d142cb",
        "timestamp": "2023-11-21T11:26:18.7240313097",
        "isDelete": false
    },
    {
        "record":
        {
            "ID": "asset_1",
            "EMP_ID": "0000000001",
            "CUI": "00000000000000000001",
            "Hash_EMP": "12b2f9c1924735069a918a3ca86ea4f0f6123cfbc50df18f25eed6f8b1c147c4",
            "Owner": "Columbo",
            "NumeroCedulaOwner": "cc_11111111",
            "NombreFiscal": "Nestor Pitana",
            "NumeroCedulaFiscal": "cc_1000001"
        },
        "txId": "7cd5eee32d454bc87ac95705f3d0ae06f694d5d54400ea7baa923a7caefb0244",
        "timestamp": "2023-11-21T11:24:27.316511392",
        "isDelete": false
    }
]
```


Ilustración 16. Histórico del activo en formato amigable para el usuario. Fuente: Elaboración propia

El orden en que se presentan las transacciones va desde lo más nuevo arriba hasta lo anterior abajo. Aquí podemos notar que Hyperledger guarda registro completo en la blockchain de cada transacción realizada agregando un campo timestamp donde está el registro en UTC de cuando se realizó cada transacción.

Otro campo interesante de destacar en la respuesta de la API es el campo isDelete. Este campo nos indica si un activo fue "borrado" lo que indica que el activo ya no está más disponible

para transaccionarse, sin embargo, la trazabilidad de la historia del activo es inmutable.

V. Vínculo entre almacenamiento inmutable y blochchain privada

La aplicación WEB ejecutará un proceso compuesto por dos acciones secuenciales:

1) *Copiará el archivo en el filesystem de storage inmutable.*
2) *Cargará todos los datos relacionados con el caso de investigación en la blockchain.*

Al cargar el archivo en el storage inmutable, el path donde es copiado está estructurado partiendo de una unidad mayor de agrupamiento como es el CUI (Código Único de Investigación) el cual contiene un directorio para cada evidencia. Este path es incorporado en la blockchain para que cuando el usuario deseara recuperar la evidencia, la aplicación web contará con un apuntador exacto a la ruta dentro del filesystem donde encontrar el archivo.

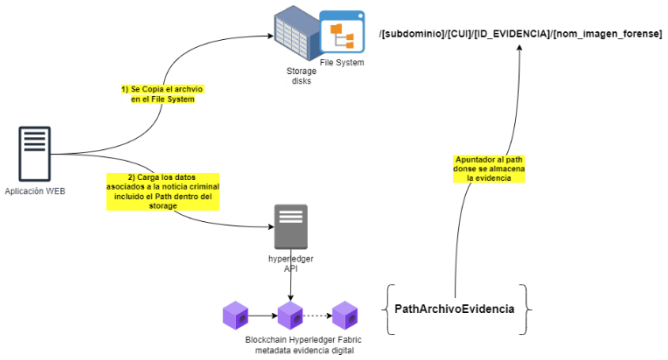

Ilustración 17- Path del Archivo de evidencia como apuntador al archivo en la Blockchain – Elaboración propia.

En la definición de nuestro activo en el chaincode de Hyperledger, tenemos un campo "PathArchivoEvidencia" (ver *Tabla 1* e *Ilustración 11*), es en este campo donde guardaremos el path del archivo de la evidencia.

IX. CONCLUSIÓN

La imagen forense como tal es un archivo de datos, ahora bien, ese archivo solo tiene valor cuando está perfectamente relacionado con otra metadata que conforma el expediente judicial, como son la nota criminal o el código único de investigación (CUI), el agente de policía judicial responsable y el despacho de fiscalía correspondiente. De hecho, es importante hacer notar que un archivo disociado de una relación con esa metada carece de valor y no puede usarse en un proceso judicial.

Al inicio de nuestra exploración de alternativas de arquitectura para construir el almacén de evidencia digital, uno de nuestros primeros impulsos fue montar el archivo de la evidencia forense dentro de la misma blockchain. Sin embargo, descubrimos que esto no es posible en la práctica debido a la gran cantidad de congestión de tráfico que se produciría, ya que cada nodo esta permanente interactuando con otros nodos para lograr el consenso, lo que hace que los datos (junto con sus certificados digitales) viajen múltiples veces a través de la red por cada intento de transacción hasta que esta es validada, queda en firme y se realiza el commit a la blockchain.

Sin embargo, existen para este fin dispositivos de almacenamiento inmutable que nos sirvieron de apoyo en el almacenamiento de los archivos de las evidencias. Encontramos que es determinante contar con un apuntador que permita vincular el archivo que se desea resguardar con la metadata asociada (hash incluido) para poder garantizarle al usuario que recuperará el archivo correspondiente.

Otro preconcepto importante con el que iniciamos este trabajo es que pensábamos a los activos de la blockchain como inmutables, sin embargo, como ya vimos, esta "inmutabilidad" dependerá de las funciones que se definan en el chaincode (Smart Code). Si en el chaincode definimos funciones que permitan actualizar campos e incluso "borrarlo" como ya vimos cuando explicamos el campo is_Delete, vemos que no podemos hablar de una inmutabilidad de los activos. Los activos no son inmutables, las que son inmutables son cada una de las transacciones que se realizaron con el activo las que constituyen un registro indeleble. Cada interacción, desde la creación, la actualización, la transferencia o el borrado de un activo queda registrado en la blockchain en la medida en que el smartcontract lo permita.

En ese sentido si, el requerimiento de un caso de negocio fuera la absoluta imposibilidad de eliminar un activo, en ese caso la recomendación es que en primer lugar no exista una función que permita borrar activos en el chaincode ya que esto implica un nivel más profundo de restricción que una restricción en la capa de asignación de roles.

Es importante señalar que el chaincode puede ser modificado por aquellos roles que tengan permitido hacerlo, y una vez establecido el consenso entre los nodos el nuevo chaincode será válido, agregando, modificando o eliminado funciones al chaincode anterior, permitiendo la evolución de la lógica del negocio.

VI. Referencias

(s.f.). Obtenido de Hyperledger Fabric: https://www.hyperledger.org/projects/fabric

(s.f.). Obtenido de Private Ethereum: https://ethereum.org/en/enterprise/private-ethereum/

(s.f.). Obtenido de Postman: https://www.postman.com/

Arslanian, H. (2022). Differences Between Private and Public Blockchains. En H. Arslanian, *The Book of Crypto, The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets* (pág. 123). Springer Nature Switzerland AG.

Bigelow, S. J. (2023). *What is a SAN? Ultimate storage area network guide*. Obtenido de https://www.techtarget.com/searchstorage/definition/storage-area-network-SAN

Castro, M., & Liskov, B. (Feb de 1999). Practical Byzantine Fault Tolerance. *Laboratory for Computer Science,*

Massachusetts Institute of Technology. Obtenido de https://pmg.csail.mit.edu/papers/osdi99.pdf

CONSTITUCION POLITICA DE COLOMBIA 1991. (s.f.). *Artículo 250, Cap 6* .

Corda. (s.f.). Obtenido de Corda: https://r3.com/products/corda/

Gómez, L. (May de 2023). Fiscalía desarticuló banda que se dedicaba a desocupar cuentas bancarias en Bogotá y Barranquilla. *Fiscalía desarticuló banda que se dedicaba a desocupar cuentas bancarias en Bogotá y Barranquilla*. Obtenido de https://www.infobae.com/colombia/2023/05/21/fiscalia-desarticulo-banda-que-se-dedicaba-a-desocupar-cuentas-bancarias-en-bogota-y-barranquilla/

Hellwig, D., Karlic, G., & Huchzermeier, A. (2020). Practical Byzantine Fault Tolerance (PBFT). En D. Hellwig, G. Karlic, & A. Huchzermeier, *Build Your Own Blockchain. A Practical Guide to Distributed Ledger Technology* (pág. 67). Springer Nature Switzerland AG.

https://www.hyperledger.org/projects/fabric. (s.f.). Obtenido de Hyperledger Fabric: https://www.hyperledger.org/projects/fabric

Hyperledger Fabric. (s.f.). *Policies*. Obtenido de https://hyperledger-fabric.readthedocs.io/: https://hyperledger-fabric.readthedocs.io/en/latest/policies/policies.html#chaincode-endorsement-policies

Hyperledger, D. (2023). *How Fabric networks are structured*. Obtenido de How Fabric networks are structured: https://hyperledger-fabric.readthedocs.io/en/latest/network/network.html

Hyperledger, D. (2023). *The Ordering Service*. Recuperado el 2023, de https://hyperledger-fabric.readthedocs.io/en/latest/orderer/ordering_service.html?highlight=PBFT

Hyperledger, Documentation. (2023). *How Fabric networks are structured*. Obtenido de How Fabric networks are structured: https://hyperledger-fabric.readthedocs.io/en/latest/network/network.html

Hyperledger, Documentation. (2023). *Membership Service Provider (MSP)*. Obtenido de https://hyperledger-fabric.readthedocs.io/en/latest/membership/membership.html

La importancia del ecosistema digital. (28 de Febrero de 2023). Obtenido de Universidad Europea: https://universidadeuropea.com/blog/ecosistema-digital/

López, O. M. (12 de Sep de 2023). Se ‘extraviaron’ pruebas de las investigaciones contra ‘narcofiscales’ amigos de la vicefiscal Martha Mancera. *Se ‘extraviaron’ pruebas de las investigaciones contra ‘narcofiscales’ amigos de la vicefiscal Martha Mancera*. Obtenido de https://www.infobae.com/colombia/2023/09/12/se-extraviaron-pruebas-de-las-investigaciones-contra-narcofiscales-amigos-de-la-vicefiscal-martha-mancera/

Palermo, A., Gentile, A., & Pellegrino, G. (2021). *Documentary heritage: fungal deterioration in Compact Discs*. (Springer, Ed.) Obtenido de Documentary heritage: fungal deterioration in Compact Discs.: https://doi.org/10.1186/s40494-021-00609-x

Rouse, M. (25 de Junio de 2013). *Mass Storage Device*. Obtenido de Techopedia: https://www.techopedia.com/definition/11901/mass-storage-device-msd

Singhal, B., Dhameja, G., & Panda, P. S. (2018). Proof of Work. En B. Singhal, G. Dhameja, & P. S. Panda, *Beginning Blockchain* (págs. 131-133). Apress.

The Secret Lives of Data. (s.f.). Obtenido de Raft, Understandable Distributed Consensus: https://thesecretlivesofdata.com/raft/

Van Der Steen, M. (2020). *Dell Technologies*. Obtenido de IMMUTABLE DATA PROTECTION FOR ANY APPLICATION: https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/powerprotect-dp-series-appliances-ds.pdf

What is IPFS. (s.f.). Obtenido de What is IPFS: https://docs.ipfs.tech/concepts/what-is-ipfs/