ARQUITECTURA DE SEGURIDAD PARA EL PROCESO PENAL ORDINARIO

Andrés Camargo Delgado, Andrés Felipe López Suárez, Julián Camilo Sánchez Peña

Departamento de Ingeniería de Sistemas y Computación
Facultad de Ingeniería
Universidad de los Andes
Bogotá, Colombia
Noviembre, 2021
{a.camargo, a.lopez31, j.sanchezp}@uniandes.edu.co

Abstract - Este articulo presenta el proceso utilizado para Arquitectura de Seguridad del proceso penal ordinario en Colombia. Es una propuesta de solución a la problemática que actualmente tiene la Fiscalía General de la Nación, sobre quejas y reclamos que conducen a manifestaciones de inconformidad y que son evidenciados en los informes de PQRS. Para esta investigación se tomaron los informes correspondientes al periodo abril a junio de 2021. Con esta propuesta se busca ofrecer garantías de integridad, autenticidad y trazabilidad de un proceso penal y así minimizar las consecuencias adversas que tiene el llevar un proceso penal sin estas garantías.

Palabras Clave: Ethereum, blockchain, proceso penal, firma digital, evidencia digital, trazabilidad, integridad.

I. INTRODUCCIÓN

La Fiscalía General de la Nación es una entidad pública de la rama judicial, cuyo objetivo es administrar la justicia al hacer cumplir lo que establezca la ley en Colombiana. Sus delegados tienen competencia en todo el territorio nacional para garantizar a los ciudadanos la investigación, tanto en lo favorable como en lo desfavorable en un proceso penal, y así mismo, hacer respetar sus derechos fundamentales y las garantías procesales.

De acuerdo con los adelantos tecnológicos que contribuyen al logro de los objetivos misionales de la Fiscalía y la subdirección de Tecnologías de la Información, se ha convenido que los diversos sistemas tecnológicos son indispensables para la entidad, por lo cual, es necesario protegerlos contra diversos factores que puedan atentar contra el objetivo de garantizar acceso a la justicia de manera oportuna y eficaz. La Fiscalía cuenta con una gran cantidad de controles de seguridad, con el fin de proteger los sistemas críticos y procesos misionales que manejan información sensible que puede ser expuesta a la afectación de los principios de seguridad (confidencialidad, integridad y disponibilidad). Sin embargo, en la actualidad un proceso penal tiene la participación de un juez quien administra la justicia, y procesa las denuncias de acuerdo con las leyes y evidencias del caso, por lo que requiere verificar que las evidencias presentadas sean auténticas y así se pueda procesar de manera adecuada un proceso penal. Sin embargo, algunos procesos penales el juez no tiene la posibilidad de verificar la trazabilidad, autenticidad y no repudio de un proceso penal (información en cada etapa) y esto puede generar errores en un juicio.

II. PROBLEMA

Es conocido que la Fiscalía como cualquier entidad u organización busca mejorar en sus procesos internos, dado que esto es reflejado en sus informes de PQRS (Peticiones, quejas, reclamos y sugerencias). Las quejas y reclamos son las que conducen a manifestaciones de inconformidad, y son motivos de estudio del presente proyecto. [1]

En los informes de PQRS de la Fiscalía en el periodo correspondiente de abril-junio del 2021 se evidencia que las quejas y reclamos corresponden al 3%, es decir, a 1932 de las 64.374 PQRS. [1]. Este 3% representa consecuencias negativas de gran impacto para las personas involucradas y reducción de la confianza en la entidad.

Entre las principales consecuencias de no poder garantizar la trazabilidad y autenticidad podemos mencionar fallos de sentencias a personas inocentes que son enviados a un centro carcelario, personas que quedan en libertad a pesar de que son culpables y, demandas al estado colombiano por llevar los procesos penales de manera inadecuada, los cuales en muchas ocasiones tienen una demora en la resolución que conduce a vencimiento de términos. Todo esto genera una pérdida de confianza y reputación de la entidad por parte de la ciudadanía colombiana.

III. PROPUESTA DE SOLUCION

Este trabajo propone diseñar una arquitectura de seguridad que permita garantizar confianza, trazabilidad y no repudio

sobre los documentos asociados con un proceso penal ordinario.

Adicionalmente, es necesario plantear una integración entre los sistemas de información, usuarios y la solución propuesta que permita preservar los datos de una manera confiable, como se ilustra en la siguiente (Figura 1).

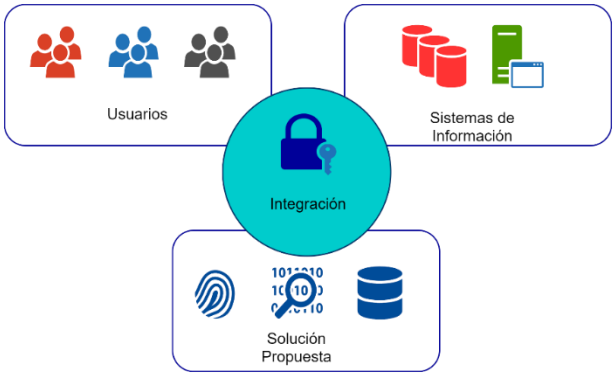

Fig. 1. Esquema de Solución

- Usuarios: Partes interesadas que interactúan en desarrollo de un proceso penal, por ejemplo: juez, fiscal, victima entre otros.
- Sistemas de información: Se refiere a los sistemas de información actuales de la entidad en los que se almacena las denuncias.
- Solución propuesta: Elementos que hacen parte del nuevo sistema que permita asegurar la información y generen confianza, trazabilidad y no repudio.
- Integración: Es el desarrollo de un sistema que permite el procesamiento de los datos de un proceso penal a través de una tecnología criptográfica y de la cual hacen parte los interesados.

A continuación, se presenta una propuesta de alto nivel (Figura 2) conformada por 3 capas:

- **Capa de cliente:** En esta capa se planta realizar lo que corresponde a la ingesta de datos, es decir, a la recepción y diligenciamiento de la denuncia en el sistema SPOA (Sistema penal oral acusatorio) de la Fiscalía. Así mismo, está capa corresponde a todos los registros digitales que son agregados dentro de un proceso penal que son recolectados como evidencia.

- **Capa de Frontend:** La capa de frontend corresponde a todas las interfaces gráficas de los sistemas de información actuales como SPOA y lago de datos con ECM (Enterprise Content Management). Esta capa es la que permite la interacción del usuario con un sistema de información, a través de un sistema gráfico que permita autenticación, y por ende un control de identidad para posteriormente presentar las interfaces gráficas de acuerdo con sus permisos y realizar la ingesta de datos.

- **Capa de Backend:** La capa de backend tiene integración con la capa de frontend por medio de una API, que permite la interacción de los sistemas actuales con el sistema de trazabilidad y no repudio. Esta capa de backend maneja y controla todos los datos por medio de códigos programables que no son vistos por los usuarios en su capa de cliente y de frontend. La capa de backend contiene la lógica del negocio.

A continuación, se presenta la propuesta de alto nivel que incluye las capas anteriormente descritas (Figura 2).

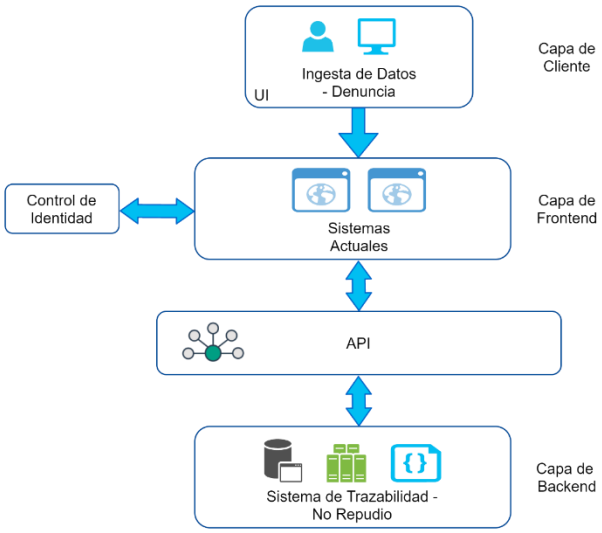

Fig. 2. Propuesta de Alto Nivel

IV. MARCO LEGAL

A. Descripción del Proceso Penal Ordinario

El proceso penal ordinario esta divido en principalmente en 3 etapas claramente definidas:

• **Indagación**: Esta fase inicia con la noticia criminal en la cual la policía judicial recolecta los elementos probatorios y evidencia física para determinar la existencia de un posible delito y así identificar a los posibles autores y ubicación. De acuerdo con lo anterior esta fase trata el conocimiento por parte de la Fiscalía de un acto que está tipificado como delito dentro del código penal colombiano.

• **Investigación**: Esta fase inicia la etapa investigativa con el fiscal y el cuerpo policial, elementos probatorios, información legal y evidencia con la finalidad de fortalecer el conocimiento de los hechos.

• **Juicio:** En esta fase se realiza el juzgamiento según la documentación, elementos materiales probatorios y se determina la responsabilidad del imputado. Esta se lleva a cabo ante el juez de conocimiento, quien debe escuchar a las partes y finalizar el proceso con una sentencia.

La siguiente figura presenta un esquema de las etapas mencionadas (Figura 3).

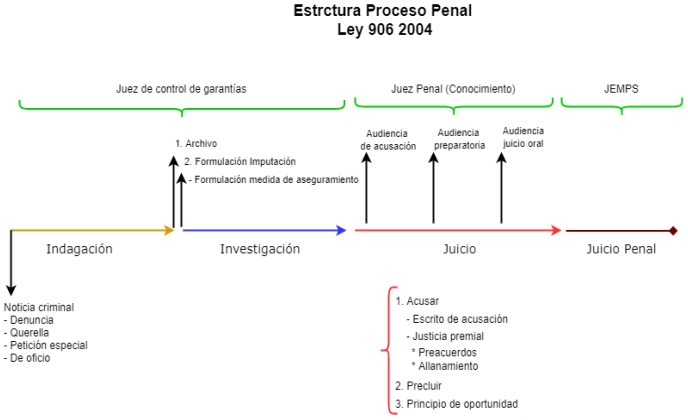

Fig. 3. Estructura del proceso penal elaborado por el profesor Ricardo Molina López

B. Participantes en el Proceso Penal Ordinario

En el marco del proceso penal ordinario intervienen una serie de participantes que interactúan o validan la evidencia digital o registro de un proceso penal ordinario, así como, participantes que no intervienen, pero hacen parte.

- Fiscal
- Juez de control de garantías
- Juez de conocimiento
- Víctima
- Imputado
- Defensa
- Investigador experto
- Asistente de fiscalía
- Policía Judicial

Teniendo en cuenta la lista de participantes en el proceso penal, se definieron los siguientes roles y permisos:

- Permiso de Lectura: Es la capacidad que tiene el usuario de poder leer o visualizar la información que se ha ido registrando durante un proceso penal.

- Permiso de Escritura: Es la capacidad que tiene el usuario de poder añadir nueva información en el proceso.

La siguiente tabla consolida los permisos asociados con cada rol de los interesados en un proceso penal (Tabla 1).

Participante	Permiso	
	Lectura	Escritura
Fiscal	Si	Si
Juez de control de garantías	Si	No
Juez de Conocimiento	Si	No
Victima	No	No
Imputado	No	No
Defensa	Si	No
Investigador experto	Si	Si
Asistente de fiscalía	Si	Si
Policía Judicial	Si	Si

Tabla 1. Permisos de los actores del proceso penal

V. TECNOLOGÍAS CRIPTOGRÁFICAS

Como parte de esta propuesta se realizó una comparación entre las tecnologías criptográficas actuales que podrían dar solución al problema planteado. Entre ellas tenemos:

A. Firma digital

La firma digital es un mecanismo de la criptografía que permite realizar la verificación de autenticidad e integridad de los datos, de tal manera que, permita al receptor de la información que se envía a través de un mensaje validar o corroborar la entidad o persona, es decir, el emisor original del mensaje. Esta tecnología permite ofrecer algunos de los principios de seguridad de la información como integridad y no repudio, puesto que, permite confirmar que el mensaje no ha sufrido alteraciones o modificaciones desde que el remitente envió el mensaje. [2]

A continuación, se puede evidenciar el funcionamiento de la firma digital, en el cual se observa el proceso de hash y cifrado de los datos (Figura 4).

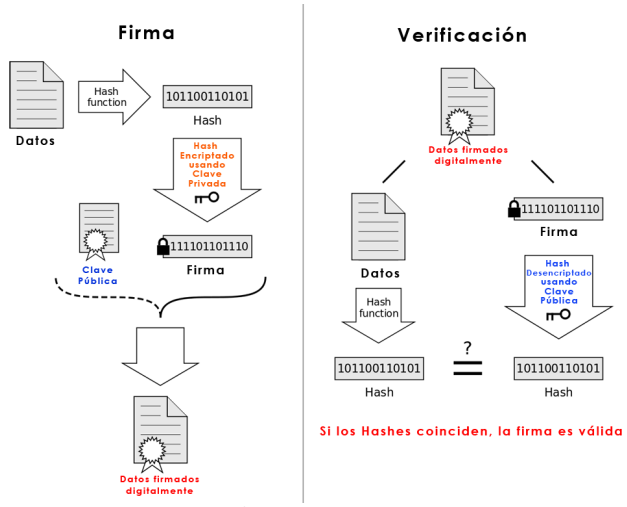

Fig. 4. Proceso firma digital. Tomado de: [3]

B. *Blockchain*

La tecnología blockchain también conocida como "cadena de bloques" contempla cualquier transferencia que registra datos en una red peer-to-peer o en una red descentralizada, en la cual cada participante de la red es considerado un nodo que, puede visualizar, verificar o rechazar los datos a través de protocolos de consenso definidos que permiten garantizar la integridad, autenticidad y veracidad de las transacciones realizadas. [4]

C. *Hashgraph*

Hashgraph es una tecnología relativamente nueva. La arquitectura de Hashgraph se basa en un DAG (*directed acyclic graphs*), que es un gráfo dirigido finito sin bucles entre dos elementos. Hashgraph ejecuta un protocolo de chismes *(gossip protocol)*, que es único entre protocolos DLT (*Distributed Ledger Technologies*). Su funcionamiento se basa en el uso de tokens y sus creadores indican que puede atender hasta diez mil transacciones por segundo, tiene un alto rendimiento en la prueba de trabajo PoW (proof of work) y tiene la posibilidad de eliminar archivos almacenados en la plataforma por las entidades autorizadas. En cuanto a seguridad los adversarios están limitados computacionalmente por el esquema de firma digital y funciones de hash utilizadas. [5]

D. *Tangle*

Tangle es una tecnología basada en el consenso DAG gráfico acíclico dirigido. De forma similar a blockchain, su función principal es crear una red de transacciones independientes y autogestionadas de manera descentralizada. Sus funciones principales son: organizar, registrar, almacenar y verificar la información en redes. A diferencia de blockchain que gestiona las transacciones de forma lineal Tangle utiliza cadenas entre lazadas que generan el grafo acíclico, las nuevas transacciones son aprobadas basado solo en las dos transacciones anteriores y todos los participantes pueden validar y emitir transacciones. En cuanto a seguridad su trazabilidad no es completa y aún es vulnerable a ataques externos según pruebas en la última versión. [6]

E. *Árboles de Merkle*

El árbol de Merkle es el producto de un algoritmo que toma como datos de entrada el conjunto de transacciones almacenadas en un bloque, con el fin de verificar que las mismas no hayan sido alteradas. El bloque no se procesa como un todo, sino que cada transacción es evaluada por separado, mientras el algoritmo las agrupa en segmentos vinculados, produciendo al final un hash del bloque completo. [7].

A continuación, se presenta la estructura que tiene los árboles de Merkle (Figura 5).

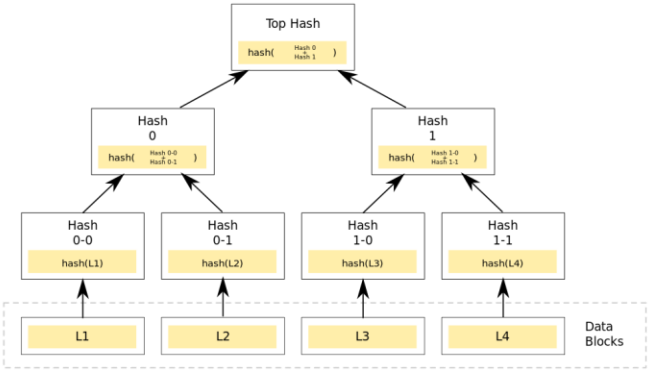

Fig. 5. Árbol de Merkle. Tomado de: [8]

VI. ELECCIÓN DE LA TECNOLOGÍA

A continuación, se describe la evaluación multicriterio realizada para seleccionar la tecnología criptográfica más apropiada para el caso de interés.

A. *Evaluación multicriterio*

Una evaluación multicriterio es frecuénteme usada para la selección de soluciones tecnológicas, y el método más usado es el analítico de jerarquía. [9]. A continuación, se presentan los pasos típicos:

1) Selección de alternativas tecnológicas
2) Selección de criterios de decisión
3) Creación de matriz de comparación de criterios con alternativas tecnológicas
4) Ubicación de los pesos en los criterios de decisión
5) Valoración de cada alterativa tecnológica de acuerdo con cada criterio
6) Elección de la mejor alternativa de acuerdo con la mejor calificación
7) Informe de resultados

Con base en la problemática abordada, en la cual se hace necesario la trazabilidad y confianza por parte de los interesados en un proceso penal se identifican los siguientes criterios de decisión:

- Trazabilidad
- No repudio
- Disponibilidad
- Integridad
- Escalabilidad
- Usabilidad

Los pesos de los criterios van acorde a las necesidades del problema, así como, a la importancia que consideran los interesados. Para el presente proyecto la ponderación de los criterios de selección se basó en una encuesta a funcionarios de la Fiscalía, y la realización del análisis de prioridades por

medio del siguiente proceso basados en la escala de Saaty que se usa para realizar la calificación o escala de juicio en cada una de la comparativa de los criterios. [10].

De acuerdo con los resultados de los encuestados, la integridad tiene la mayor importancia en los criterios, seguido de la trazabilidad, no repudio, y usabilidad, lo cual se muestra en la siguiente gráfica (Figura 7).

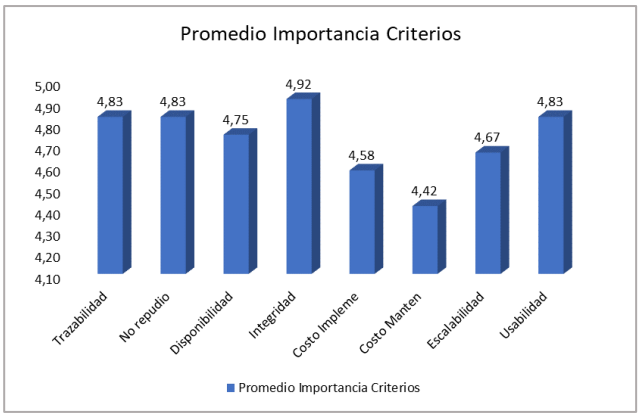

Fig. 7. Gráfica promedios evaluación importancia de criterios

Para identificar la importancia de un criterio con otro, se usó la escala de Saaty, la cual establece las escalas numéricas para representar esta importancia en la comparación y así tener una decisión de juicio. [11].

ESCALA DE SAATY		
Escala Numérica	**Escala Verbal**	**Explicación**
1	Igualmente importante	Dos elementos contribuyen en igual medida al objetivo
3	Moderadamente importante	Preferencia leve de un elemento sobre otro
5	Fuertemente importante	Preferencia fuerte de un elemrnto sobre otro
7	Importancia muy fuerte o demostrada	Mucho mas preferencia de un elemento sobre otro
9	Importancia extremadamente fuerte	Preferencia clara y absoluta de un elemento sobre el otro
2,4,6,8	Valores intermedios	Cuando se necesita un compromiso de ambos elementos, es un intermedio de los valores anteriores

Tabla 2. Matriz de Saaty

De esta manera se procede con la calificación y comparación de la importancia de un criterio frente a otro:

MATRIZ DE COMPARACIÓN DE CRITERIOS								
Criterios	**Trazabilidad**	**No repudio**	**Disponibilidad**	**Integridad**	**Costo Impleme**	**Costo Manten**	**Escalabilidad**	**Usabilidad**
Trazabilidad	1	1	3	1/3	5	9	5	1
No repudio	1	1	3	1/3	7	9	5	3
Disponibilidad	1/3	1/3	1	1/5	5	7	3	1/3
Integridad	3	3	5	1	7	9	5	3
Costo Impleme	1/5	1/7	1/5	1/7	1	5	1/3	1/5
Costo Manten	1/9	1/9	1/7	1/9	1/5	1	1/5	1/9
Escalabilidad	1/5	1/5	1/3	1/5	3	5	1	1/5
Usabilidad	1	1/3	3	1/3	5	9	5	1
TOTAL	**6,84**	**6,12**	**15,68**	**2,65**	**33,20**	**54,00**	**24,53**	**8,84**

Tabla 3. Matriz comparación de criterios

Una vez se realiza este procedimiento se procede a realizar la normalización:

Matriz Normalizada									
Criterios	Trazabilidad	No repudio	Disponibilidad	Integridad	Costo Impleme	Costo Manten	Escalabilidad	Usabilidad	Promedio
Trazabilidad	0,15	0,16	0,19	0,13	0,15	0,17	0,20	0,11	0,16
No repudio	0,15	0,16	0,19	0,13	0,21	0,17	0,20	0,34	0,19
Disponibilidad	0,05	0,05	0,06	0,08	0,15	0,13	0,12	0,04	0,09
Integridad	0,44	0,49	0,32	0,38	0,21	0,17	0,20	0,34	0,32
Costo Impleme	0,03	0,02	0,01	0,05	0,03	0,09	0,01	0,02	0,03
Costo Manten	0,02	0,02	0,01	0,04	0,01	0,02	0,01	0,01	0,02
Escalabilidad	0,03	0,03	0,02	0,08	0,09	0,09	0,04	0,02	0,05
Usabilidad	0,15	0,05	0,19	0,13	0,15	0,17	0,20	0,11	0,14

Tabla 4. Matriz normalizada

Con base en estos resultados se obtiene el promedio por cada criterio, dando como resultado el peso de cada uno:

Criterio	**Ponderación**
Trazabilidad	0,16
No repudio	0,19
Disponibilidad	0,09
Integridad	0,32
Costo de Implementación	0,03
Costo de Mantenimiento	0,02
Escalabilidad	0,05
Usabilidad	0,14

Tabla 5. Ponderación según criterios

Finalmente, la evaluación de la selección de la mejor alternativa se basa en los valores de los criterios de cada tecnología, de acuerdo con la investigación realizada de cada una de las herramientas. Ello permite obtener la siguiente matriz de resultados:

Tecnología/Criterio	Trazabilidad	No repudio	Disponibilidad	Integridad	Costo Impleme	Costo Manten	Escalabilidad	Usabilidad	Suma
Firma Digital	1	5	4	5	3	4	4	4	4,00
Blockchain	5	5	5	5	2	2	5	2	4,41
Hashgraph	3	5	5	3	3	2	5	2	3,50
Tangle	2	4	5	4	2	2	4	2	3,38
Árbol de Merkle	3	1	1	5	4	4	4	5	4,00
Cadena de Hashes	1	1	1	5	4	4	4	5	4,00

Tabla 6. Matriz de evaluación alternativa con criterios.

La sumatoria final de cada una de las alternativas determina cuál es la mejor alternativa según los criterios seleccionados.

Los valores asignados para cada uno de los criterios se basaron en las características que cada tecnología brinda, y se presenta una tabla con la descripción completa en el documento completo de este proyecto.

B. Resultado

A continuación, presentan los resultados de priorización de la evaluación multicriterio (Figura 8).

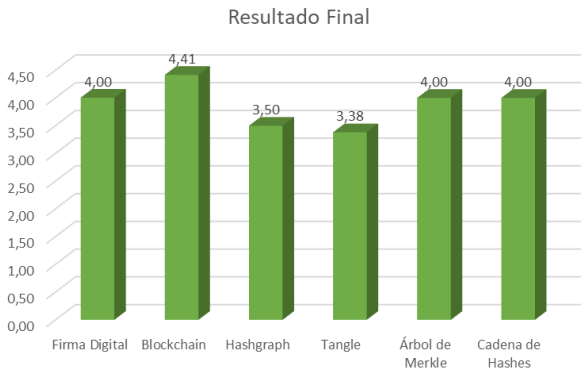

Fig. 8. Resultados evaluación multicriterio

Los resultados presentados en la gráfica anterior arrojan que la tecnología Blockchain tiene mayor valor con base en los diferentes criterios, y con base en el entendimiento del problema actual. Este resultado permite definir la tecnología que se va a usar para el desarrollo de la arquitectura de seguridad para soportar las tareas en el manejo de un proceso penal ordinario, y que permite mejorar la trazabilidad y confianza, garantizando el no repudio e integridad en los registros digitales.

VII. TECNOLOGÍA SELECCIONADA: BLOCKCHAIN

Blockchain es una estructura de datos de bloques que se encadenan para formar una colección de registros, llamado libro de cuentas, siendo la criptografía un ingrediente clave en el proceso. Una cadena de bloques no tiene un mecanismo de almacenamiento, sino un conjunto de protocolos que rigen la forma en que se almacena la información. Así, una cadena de bloques puede almacenarse en archivos planos o en una base de datos.

La tecnología blockchain y su arquitectura proporciona a los integrantes de la red de blockchain la capacidad o habilidad para actualizar un nodo de información que comparte el libro mayor, a través de un sistema de replicación P2P cada vez que una transacción o un evento ocurre. Es decir, cada vez que haya un nuevo bloque sobre los registros del proceso penal este será replicado a todos los nodos de la red. [12]. Cada nodo puede recibir o enviar nuevas transacciones, y estos son sincronizados en la red de blockchain.

A. Tipos de blockchain

La tecnología blockchain es categorizada en 4 grandes tipos de acuerdo con la disponibilidad y accesibilidad de los usuarios:

- Blockchain público
- Blockchain privado
- Blockchain hibrido
- Blockchain federada o consortium

La siguiente imagen (Figura 10) muestra una comparación de los diferentes tipos de blockchain.

Property	Public	Consortium	Private
Consensus Determination	All Miners	Selected Set of nodes	Limited to one organization
Read Permission	Public	Public/Restricted	Public/Restricted
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus Process	Permissionless	Permissioned	Permissioned

Fig. 10. Comparación tipos de blockchain. Tomado de: [13].

B. Capas de blockchain

La tecnología blockchain está formada por una estructura no jerárquica divida en las siguientes 6 capas (Figura 11): datos, red, consenso, contrato, servicio y aplicación. Cada una estas aportan al desarrollo y funcionamiento de blockchain.

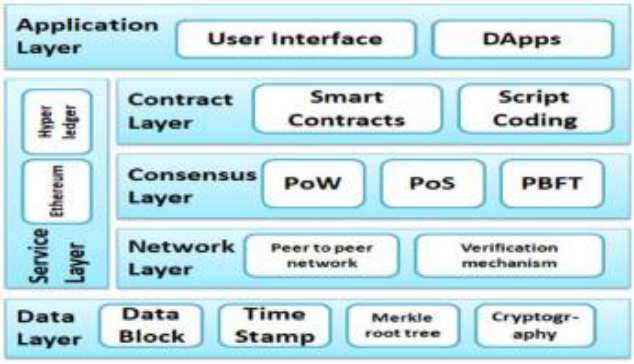

Fig. 11. Capas de Blockchain. Tomado de: [13].

Cada una de estas capas contiene diferentes componentes como se presentan a continuación:

Capa	Componentes
Datos	Bloque de datos, estructura de la cadena, sello de tiempo, arboles de Merkle, criptografía
Red	Redes P2P, mecanismo de verificación, protocolo de broadcast
Consenso	PoW, PoS, DPoS, PBFT
Contrato	SmartContract, codificación de scripts, mecanismos incentivos
Servicio	Ethereum, Hyperledger, IBM Azure BaaS, Bitcoin
Aplicación	Criptomonedas, salud, servicios nube, educación, entre otros

Tabla 7. Componentes Blockchain

C. Tecnología Blockchain seleccionada: Ethereum

Conforme a los requisitos de negocio para el desarrollo de este proyecto se seleccionó Ethereum como la tecnología más apropiada para la implementación. Ethereum ofrece las siguientes ventajas:

- **Lenguajes permitidos:** El más relevante para el desarrollo del proyecto es Solidity que es uno de los más usados y popular entre los desarrolladores. Como resultado impactaría positivamente en búsqueda de personal y en la integración de la plataforma.

- **Mecanismo de consenso:** Corresponde al algoritmo usado en una red blockchain, para regular la manera en la cual los nodos aceptan un nuevo bloque, es decir, los miembros de una blockchain aceptan que la información no ha sido manipulada.
- **Gobierno y modelo de negocio:** La gestión del blockchain a través de Ethereum puede ser híbrida por la necesidad de integración de las plataformas actuales.

La tecnología Ethereum es una plataforma de código abierto (*open source*) de blockchain que a su vez puede manejar permisos (*permissioned blockchain*), es decir, es una blockchain privada restringida solamente a los participantes autorizados a través de limitación en las operaciones o transacciones que estos pueden realizar.

La red de Ethereum puede estar constituida por cientos de nodos, donde cada computador es considerado un nodo, el cual puede ejecutar el software de la blockchain de Ethereum de tal manera que, a través de los Smart Contracts pueda realizar las transacciones y procesar los datos replicando a cada uno de los nodos de la red, garantizando disponibilidad en un ambiente distribuido.

La red de Ethereum posee dos tipos de nodos en la blockchain: nodos ligeros y nodos completos. Los nodos ligeros son nodos que no realizan el protocolo de consenso, es decir, no tienen la capacidad de realizar la verificación de las transacciones generadas de cada bloque. Por otra parte, los nodos completos verifican todos los bloques generados en la red de blockchain. La siguiente gráfica ilustra los componentes de la red blockchain (Figura 12).

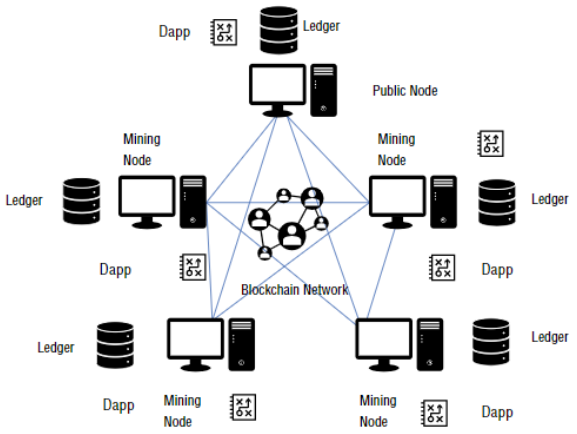

Fig. 12. Arquitectura distribuida blockchain Ethereum. Tomado de: [14].

VIII. DISEÑO DE ARQUITECTURA

El proceso penal ordinario este compuesto por una serie de registros digitales que en la fase de indagación e investigación se constituyen como evidencia para el proceso, sin embargo, estos registros digitales deben conservar su integridad y deben ser ubicados de tal manera que el ente que decide o toma una decisión sobre el caso, es decir, el juez pueda tener su trazabilidad para la verificación de estos. La siguiente figura presenta una arquitectura lógica del desarrollo del proceso penal ordinario con base en tecnología blockchain (Figura 13).

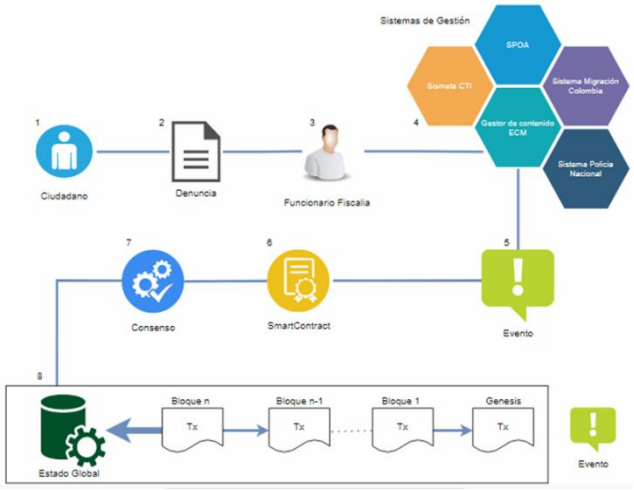

Fig.13. Proceso Penal Ordinario con Blockchain

Como paso inicial un ciudadano (1) que se ha visto afectado por otro, interpone una denuncia (2) en una entidad como la Fiscalía, la cual es recibida por un funcionario de la Fiscalía (3), el cual digitaliza los datos en un sistema de información (4) como SPOA. Estos a su vez, generan un evento (5), el cual invoca un contrato digital establecido (6) dentro de la blockchain, este contrato permite la generación de una nueva transacción la cual debe enviarse a los nodos de la red blockchain para realizar un consenso (7), que permita agregar o rechazar los nuevos datos de la denuncia a la cadena de datos de la red blockchain. (8).

A. Arquitectura blockchain para proceso penal ordinario

Para la ejecución del sistema de blockchain sobre el proceso penal se proponen nodos distribuidos, es decir, los registros se encontrarán en servidores de cada organización que haga parte de la red. Esta arquitectura distribuida brinda alta disponibilidad y protección de ciberataques, ramsonware, ataques DDoS (Distributed Denial of Service), entre otros. La descentralización del sistema de blockchain para el proceso penal ordinario propicia mayor disponibilidad puesto que todos los nodos tienen una réplica de los registros digitales.

Teniendo en cuenta que en el proceso penal pueden existir muchos registros digitales confidenciales que son considerados evidencias, como documentos o imágenes, estos deben ser almacenados fuera de la red blockchain en los sistemas de aplicaciones de la Fiscalía. Sin embargo, sí se realiza el registro del hash de los registros digitales en la blockchain, permite garantizar la integridad y la trazabilidad del documento.

La siguiente gráfica ilustra los componentes de la red Ethereum del proceso penal (Figura 14).

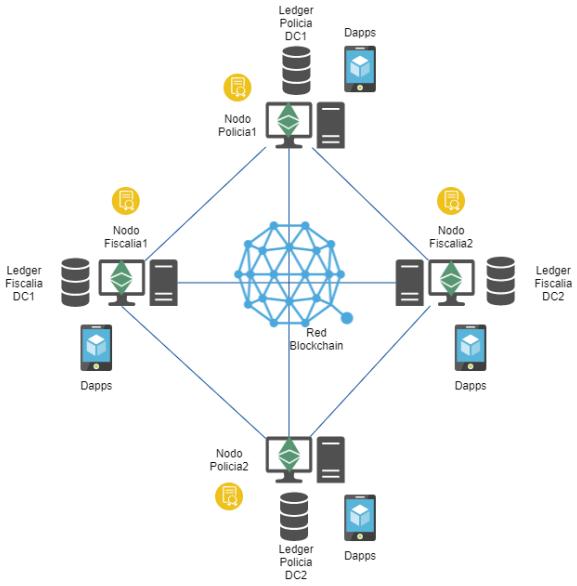

Fig. 14. Red Ethereum proceso penal

B. Tipos de datos

Los sistemas de información actuales manejan diferentes tipos de datos. Estos tipos de datos también harán parte del sistema de seguridad con blockchain y se presentan a continuación:

- Datos estructurados
- Datos semiestructurados
- Datos no estructurados

La siguiente gráfica ilustra el sistema blockchain del proceso penal (Figura 15).

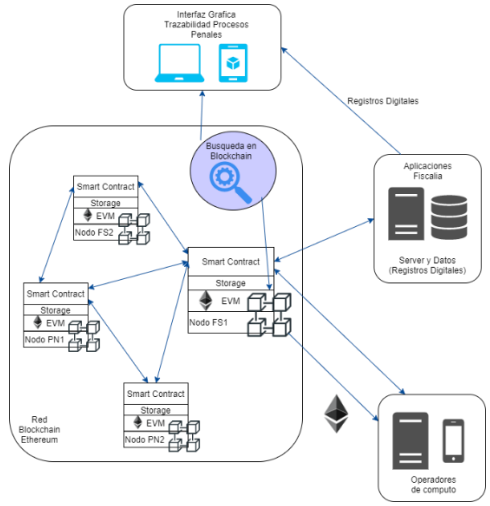

Fig. 15. Sistema Blockchain Ethereum del Proceso Penal

C. Estructura de la transacción

En el proceso penal colombiano actualmente se gestionan una serie de datos en el momento de la creación de una denuncia a través del sistema de información SPOA. La mayoría de los datos que se registran en la plataforma son considerados privados y restringidos, a excepción de algunos datos que son considerados públicos, como el lugar de los hechos.

Los siguientes, son algunos de los datos que se registran al momento de la creación de una denuncia y deben almacenarse en la transacción generada para la blockchain:

Dato	Descripción
ID del Caso	Identificación del Caso
NUNC	Número Único de Noticia Criminal
Fecha de la denuncia	Fecha de la denuncia
Etapa del caso	Etapa del caso (Etapa del proceso penal)
Departamento hechos	Departamento donde se producen los hechos
Municipio hechos	Municipio donde se producen los hechos
Lugar hechos	Lugar de los hechos
Fecha hechos inicial	Fecha de los hechos inicial
Fecha hechos final	Fecha de los hechos final
Seccional caso	Seccional donde se encuentra el caso
Despacho caso	Despacho en donde se encuentra el caso
Unidad caso	Unidad en la que se encuentra el caso

Tabla 8. Lista de metadatos para ingresar en blockchain

Para soportar la confidencialidad, la red blockchain debe integrar roles y permisos que permitan establecer control de acceso sobre los datos. La siguiente tabla presenta los roles y permisos de los participantes (Tabla 9).

Rol	Permisos
Personal Administrativo	El usuario creara la denuncia o noticia criminal y adjuntara la evidencia de los hechos
Fiscal	El usuario puede agregar evidencias adicionales en el caso
Juez de control de garantías	El usuario cambiará de estado de la evidencia como admitida o no.
Juez de Conocimiento	El usuario emitirá la sentencia qué genera un cambio de estado en el proceso penal

Victima	El usuario podrá consultar la información y estado del proceso penal
Imputado	El usuario podrá consultar la información y estado del proceso penal
Defensa	El usuario podrá consultar la información y estado del proceso penal
Investigador experto	El usuario puede agregar evidencias adicionales en el caso
Asistente de fiscalía	El usuario agregara información administrativa del caso como citaciones.
Policía Judicial	El usuario puede agregar información de los delitos en curso del proceso penal

Tabla 9. Listado permisos usuarios en sistema blockchain

La información confidencial que se almacena en la cadena de bloques tiene la siguiente estructura en la transacción que permite tanto adicionar campos como consultar los datos de una transacción.

La siguiente gráfica ilustra la estructura de una transacción (Figura 16).

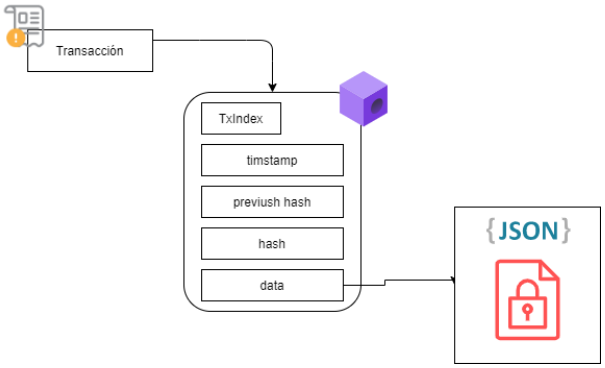

Figura 16. Estructura transacción blockchain

Cada transacción que se genera en el sistema lleva a cabo un proceso que inicia con la generación de una firma digital sobre el registro digital nuevo que se está agregando a la blockchain, el cual a su vez debe cumplir con un proceso de validación por cada uno de los nodos que conforman la red privada de blockchain de la Fiscalía.

Por medio del protocolo de consenso PoS (*Proof of State*), teniendo en cuenta, los factores de seguridad y costos de energía e infraestructura. Una vez se realiza la validación por parte de los nodos, la transacción es registrada en la cadena de bloques, y puede ser visualizada por los usuarios interesados permitiendo una trazabilidad sobre el proceso penal, como se evidencia en la siguiente imagen (Figura 17).

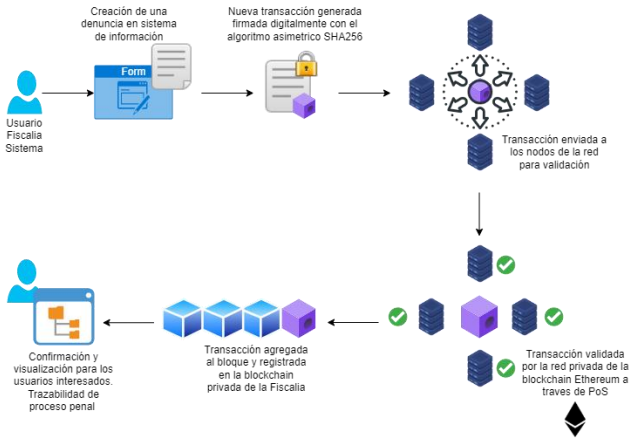

Figura 17. Flujo transacción blockchain

IX. REQUERIMIENTOS DEL PROYECTO

El estudio de viabilidad del proyecto trata de recopilar información adicional necesaria: aspectos legales, acuerdos de niveles de servicio, infraestructura y costos, con el fin de saber si es razonable la realización de este.

A. Viabilidad legal

Para el desarrollo del proyecto se validó la posibilidad de aceptación de blockchain como una nueva tecnología que contribuye a la preservación de la evidencia gestionada en medios tecnológicos. Su aporte en trazabilidad, inmutabilidad genera confianza para las partes interesadas del proceso penal ordinario, por lo cual, es posible incluirla. Los artículos 242, 242B y 239 de la Ley 906 aprueban el uso de tecnología que funciona como un agente encubierto de manera virtual con el objetivo de asegurar y controlar la evidencia.

B. Requerimientos tecnológicos

A continuación, se describen los requerimientos tecnológicos necesarios para el sistema de aseguramiento del proceso penal ordinario y la integración con el sistema actual SPOA.

1.) Requerimientos funcionales: Los requerimientos funcionales describen el comportamiento o resultado particular del sistema cuando un usuario realiza una tarea, por lo cual se definen en características del software comprendiendo las salidas según la entrada.

2.) Requerimientos no funcionales: Los requerimientos no funcionales comprenden una amplia variedad de comportamientos operativos del sistema y en cómo cumple sus funciones. Estos comportamientos se traducen en capacidades que garantizan cómo debe funcionar el sistema. [15].

En las siguientes tablas (Tabla 10 y 11) se muestran los principales requerimientos funcionales y no funcionales.

Requerimientos Funcionales
La red blockchain debe ser privada y permisionada
Los usuarios deben ser identificados e identificables
El sistema se debe integrar con el sistema de autenticación actual (Directorio activo)
Integración de los sistemas actuales y el sistema propuesto
El sistema debe generar eventos de lectura, escritura, descarga.
El sistema debe generar operaciones mediante contratos inteligentes
Los nodos se deben comunicar y sincronizan continuamente

Tabla 10. Requerimientos funcionales y no funcionales

Requerimientos No Funcionales
El mínimo de transacciones permitidas por segundo (TPS) debe ser 1-15 a 5-20
El sistema debe contar al menos cuatro nodos en la red.
El sistema debe permitir transacciones de consulta privadas y publicas
Mantener la latencia por debajo de 300 ms
El sistema de contar con una interfaz móvil y web de fácil uso para usuarios y desarrolladores
El sistema de contar con mecanismos que permitan la escalabilidad
El sistema debe contener al menos 4 instancias de CPU por nodo

Tabla 11. Requerimientos no funcionales

C. Acuerdos de niveles de servicio

Los niveles de servicio son los niveles mínimos requeridos para que la calidad del servicio sea aceptable, dependiendo del nivel que se haya definido para los diferentes elementos que componen la solución con el objetivo de satisfacer las necesidades de los interesados en un proceso penal.

1.) Tipo de aplicación: El tipo de aplicación para la solución propuesta se define como un servicio en línea de consulta e ingesta de datos, es decir, el sistema esta alineado a las necesidades del proceso penal en la búsqueda de registros de un caso, así como, el ingreso de nuevos elementos o registros digitales dentro de un proceso.

2.) Tiempo de respuesta de la aplicación: Con base en la disponibilidad continua del servicio, la operación y el funcionamiento del sistema exige un tiempo de respuesta requerido de 5 segundos. Estos requerimientos van alineados a métricas de conformidad de un usuario frente a la espera de una aplicación online.

3.) Número máximo de TPS (transacciones por segundo): El sistema de aplicación debe permitir entre 1 a 15 TPS. Tomando como base un total de 12.000 denuncias por mes las cuales se realizaron en el periodo de octubre 2021 según el reporte dado por la Fiscalía. [16]. estás denuncias corresponden a aproximadamente a 400 denuncias por día. Tomando el horario hábil de recepción de denuncias equivalente a 9 horas es equivalente a una denuncia equivalente a una TPS. Así mismo se tomó como referencia que la tecnología Ethereum puede procesar hasta 15 TPS según estudios realizados que determinan el número de transacciones por segundo. [17]. Sin embargo, puede haber un incremento del 30%, que corresponde a un valor de referencia interno para los sistemas de información, por lo cual, el sistema deberá permitir entre 5 a 20 TPS.

4.) Usuarios simultáneos y esperados: El sistema debe permitir 3000 usuarios conectados simultáneamente en la plataforma según referencia de funcionarios y se espera un crecimiento del 10% por año en base a los valores de referencia internos que tiene la Fiscalía, es decir, hasta 3300 usuarios concurrentes a partir del segundo año.

La siguiente tabla presenta el resumen de los acuerdos de niveles de servicio (Tabla 12).

Requerimiento	Indicador
Tiempo de respuesta	5 s
Usuarios simultáneos	3000
crecimiento de usuarios esperado	3300
Transacciones por segundo (TPS)	1-15
crecimiento en (TPS) esperado	5-20

Tabla 12. Resumen acuerdos niveles de servicio

5.) Fallas: Las fallas están determinadas dependiendo del tiempo que estas duren y se clasifican en fallas menores, fallas intermedias y fallas mayores, como se presenta en las siguientes tablas (Tabla 13, 14 y 15).

Máximo número de fallas menores por periodo de tiempo	Tiempo de recuperación	Disponibilidad
1 cada 8 menes	10 min	0,99997

Tabla 13. Tiempo fallas menores

RTO Fallas intermedias	RPO Fallas intermedias
10 min	2 min

Tabla 14. Tiempo fallas intermedias

RTO Fallas mayores	RPO Fallas mayores
8 horas	2 horas

Tabla 15. Tiempo fallas mayores

X. ANÁLISIS

Para este proyecto se realizó la evaluación multicriterio la cual determino que blockchain es una tecnología criptográfica apropiada para garantizar trazabilidad, transparencia, confiabilidad, integridad en la evidencia digital que es utilizada dentro de un proceso penal en Colombia. Blockchain representa un reto innovador mediante el uso de tecnologías criptográficas, sin embargo, también plantea varios retos en la implementación desde la descentralización de los datos y de las aplicaciones, el desarrollo o programación de la tecnología, así como, el consumo de energía que es utilizado por las transacciones realizadas en blockchain.

A. Caso de éxito

Una de las fuentes de inspiración y confianza son los casos de éxito que pueden tener terceros en el mismo tema a desarrollar. Para la rama judicial y el gobierno en general la adopción de nuevas tecnologías es una fuente de incertidumbre dado que la justicia debe ser precisa y transparente para los ciudadanos, es por esto por lo que identificamos el siguiente caso de éxito en la implementación de tecnologías blockchain.

- Un tribunal de Hangzhou y Guangzhou [18], China utilizo la tecnología blockchain por medio de contratos inteligentes. Su mayor logro ha sido la reducción del almacenamiento de documentos en costo que paso de USD 140 – 280 a una disminución de USD 1.4

B. Beneficios

La tecnología blockchain en la actualidad es una de las mejores en cuanto a disponibilidad por su funcionamiento descentralizado. El reto principal de las Dapp (*Decentralized applications*) pueda darse en la sincronización de los eventos, la descentralización del almacenamiento es un reto económico dado que cada nodo debe tener su propio almacenamiento con el fin de no depender de los demás, otro reto muy importante es el consumo de energía que genera cada transacción por lo que el valor económico puede incrementarse de manera exponencial de acuerdo con las transacciones por segundo que se ejecuten en los Smart Contracts.

1.) *Impacto ambiental:* Según la investigación realizada se identificó que las transacciones realizadas por medio de blockchain generan consumos altos de energía según el tipo de consenso programado para las transacciones, especialmente se ve un mayor consumo de energía si el algoritmo de consenso es PoW (*Proof of Work*). Sin embargo, con el desarrollo y avances de otros algoritmos de consenso como PoS (*Proof of State*) o PoA (*Proof of Autority*) se ha reducido el procesamiento de cómputo que se debe hacer por una transacción y por ende el consumo de energía. Para el proyecto la blockchain privada de Ethereum tiene un consumo de 63kWh por transacción por segundo teniendo en cuenta el informe presentado por la comisión europea. [19].

   La Fiscalía como ente y organización que se encarga de garantizar la justicia, la verdad y reparación de las víctimas en el estado colombiano, procesa una gran cantidad de denuncias que serían para términos del proyecto nuevos eventos, y por ende nuevas transacciones por segundo en la red privada de la tecnología criptográfica Ethereum. Las grandes cantidades de transacciones que podría generar la Fiscalía se verán reflejadas en un alto consumo de energía que son avaluadas en aproximadamente $ 1.496.880.000 un costo alto con un impacto ambiental alto.

   El alto consumo de energía reflejado por una alta tasa de transacciones ejecutadas en la red podría generar un alertamiento ambiental dadas las condiciones de la capacidad eléctrica en el país. Además del impacto por la generación de dióxido de carbono en la atmosfera que según la comisión europea la red de Ethereum a nivel mundial está generando 12.35 Mt CO2 casi igual a lo generado por el país de Panamá. [19].

   Según un análisis y estudio de Digiconomist [20] con el uso del algoritmo PoS se ha reducido gradualmente el consumo de energía en Ethereum, sin embargo, aun así, la red de Ethereum consume mucha más electricidad que un gran número de países. Ethereum está catalogado actualmente en el puesto 38 entre la lista de consumo de energía por países. [20].

2.) *Impacto financiero:* La implementación del uso de una tecnología criptográfica como blockchain conlleva un presupuesto anual para el soporte y mantenimiento de la plataforma, en el cual se incluye los costos tecnológicos, y costos operativos principalmente. Por otro lado, se debería generar un impacto financiero en beneficio de la fiscalía, puesto que, actualmente la fiscalía lleva varios procesos administrativos en su contra. Para el periodo 2021 en el Decreto 1805 del 31 de diciembre de 2020, el estado destino un presupuesto para la fiscalía en el rubro de sentencias y conciliaciones de alrededor de $40.107’100.000 pesos. [21].

   Los procesos administrativos que son llevados en contra de la fiscalía podrían reducirse mediante la implementación de blockchain en la entidad, ya que, la transparencia, confiabilidad, integridad y trazabilidad

ofrecidas por la tecnología mejoraría el desarrollo de los procesos penales llevados a cabo por la entidad.

3.) *Impacto reputacional:* En los últimos años la Fiscalía ha tenido un impacto negativo en su imagen reputacional, puesto que, muchos de los procesos llevados a cabo por la entidad han tenido alguna anomalía en el desarrollo normal lo cual ha sido como consecuencia de la corrupción política y social que ocurre en el estado colombiano. La tecnología blockchain por medio de sus características permite garantizar transparencia en el desarrollo de los procesos penales mejorando así la percepción que los ciudadanos pueden tener en la entidad.

4.) *Impacto legal:* La Fiscalía es el ente encargado de velar por la justicia, verdad y reparación de los ciudadanos que han sido víctimas de alguna conducta punible por parte de otro ciudadano. Para el mes de octubre de 2021 la organización recibió alrededor de 12000 noticias criminales. [16]. La implementación y desarrollo de una tecnología de seguridad brindará y servirá como una herramienta de apoyo a las decisiones tomadas por un juez brindando trazabilidad e inmutabilidad de los documentos digitales del proceso. Así mismo, el desarrollo del proyecto puede generar un impulso para confiar en la evidencia electrónica basada en blockchain y fomentar así la creación de nuevos artículos y decretos que determinen la aceptación y prevalencia de la evidencia digital en la tecnología blockchain.

La tecnología blockchain garantizaría la disponibilidad de los documentos, así como, el debido control y proceso de cambios sobre los mismos, puesto que, esta debe ser aprobada a través de los mecanismos de consenso garantizando así siempre un documento aceptado y verificado. Esto le brinda seguridad al proceso, y por ende a identificar los usuarios que estén relacionados con filtraciones de los documentos digitales de un proceso penal, por lo que se convierten en evidencias fundamentales para para disminuir la incidencia de estás actividades. Al disminuir o eliminar la filtración de los datos es posible garantizar integridad, lo cual brinda mayor seguridad en la administración de la justicia llevada a cabo por parte de la Fiscalía.

C. Cumplimiento de objetivos

La implementación de una tecnología criptográfica como blockchain en una red privada a través del uso de la tecnología Ethereum permitirá garantizar el cumplimiento de los objetivos principales propuestos durante el proyecto en materia de seguridad de la información, es decir, que se garantiza trazabilidad, confianza, no repudio e integridad de la siguiente manera:

- *Trazabilidad:* la tecnología blockchain garantizaría una trazabilidad completa sobre los procesos penales, puesto que, se puede tener un registro desde la creación de una denuncia hasta la finalización del proceso. Esta trazabilidad permite identificar los registros de consulta o escritura sobre un proceso penal. Esta trazabilidad se cumple con el uso de tecnología criptográfica hash.

- *Confianza:* la tecnología blockchain puede ofrecer confianza a los interesados dentro de un proceso penal tanto para ellos mismos como hacia la entidad, debido a que dos entidades diferentes tienen una copia exacta e independiente de los datos de un proceso.

- *No repudio:* blockchain permite a la organización identificar los actores que realizan consultas y agregación de registros digitales. En el caso de que haya una infiltración de un proceso penal, esta característica permite identificar quién realizó una consulta o agregación de registros a un proceso penal. Esto se da por medio de la autenticación en el sistema, la cual se podría reforzar con un segundo factor de autenticación.

- *Integridad:* La manipulación de los datos es una de las principales fallas en el proceso penal actual en Colombia, sin embargo, con la tecnología blockchain la adulteración de los registros digitales en un proceso penal puede controlarse dado que no se pueden realizar cambios o alteraciones sobre los registros digitales, puesto que, se necesita de una aprobación de todos los nodos involucrados en la red privada por medio del uso del algoritmo de consenso PoS.

XI. CONCLUCIONES

Blockchain como tecnología criptográfica aporta integridad, trazabilidad y no repudio en los documentos de los procesos penales en Colombia.

Blockchain es una tecnología nueva, sin embargo, de acuerdo con la evaluación de criterios puede ser considerada una tecnología apropiada para apoyar la toma de decisiones en un proceso penal que necesita de trazabilidad, inmutabilidad, integridad, no repudio, y así garantizar la confianza de todos los participantes involucrados en una investigación.

Teniendo en cuenta el impacto ambiental que tiene la tecnología blockchain sería recomendable pensar en más proyectos futuros que traten la generación de energía renovable en Colombia, de esta manera se podrá utilizar la tecnología blockchain de una forma responsable con el medio ambiente.

REFERENCIAS

[1] Fiscalía General de la Nación, «www.fiscalia.gov.co,» 24 08 2021. [En línea]. Available: https://www.fiscalia.gov.co/colombia/gestion/informe-de-peticiones-quejas-y-reclamos/#1519922458227-3e25c1e0-3302.

[2] W. Castillo, H. Correa y J. Muñoz, «Guía de implementación y uso de ceriticados y firmas digitales para las Mypymes que permitan garantizar integridad, autenticidad y no repudio en los documentos electrónicos,» Universidad Piloto de Colombia, Bogota, 2014.

[3] V. Iglesias, «Como funciona la firma digital,» 4 Agosto 2017. [En línea]. Available: https://www.victoriglesias.net/como-funciona-la-firma-digital/.

[4] J. Cano, «Blockchain: "Cadena de bloques". Reflexiones sobre seguridad y control,» Revista Sistemas ACIS, Bogotá, 2017.

[5] Nataša Živić, Member IEEE Esad Kadušić, Member IEEE y Kerim Kadušić, «Directed Acyclic Graph as Hashgraph: an Alternative DLT to Blockchains and Tangles,» IEEE, 2020.

[6] Leemon Baird, Atul Luykx, «The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers,» IEEE, 2020.

[7] J. P. Claros, «Aplicación de Blockchain para el uso de transportes,» Universidad de la Laguna, España, 2020.

[8] Criptodinero, «Árboles de Merkle y Blockchain,» Enero 2020. [En línea]. Available: https://criptodinero.es/bitcoin/arboles-de-merkle-bitcoin/.

[9] A. Grajales, E. Serrano y C. Hahn, «Los métodos y procesos multicriterio para la evaluación,» *Luna Azul*, 2013.

[10] A. Mendoza, C. Solano, D. Palencia y D. Garcia, «Aplicación del proceso de jerarquía analítica (AHP) para la toma de decisión con juicios de expertos,» *Revista Chilena de Ingeniería*, 2019.

[11] J. Moreno, «El proceso analítico jerárquico (AHP). Fundamentos, metodología y aplicaciones,» *Universidad de Chile*, 2002.

[12] K. Raj, Foundations of Blockchain : The Pathway to Cryptocurrencies and Decentralized Blockchain Applications., Birmingham: Packt Publishing, 2019.

[13] B. Murthy, L. Shri, S. Kadry y S. Lim, «Blockchain Based Cloud Computing: Architecture and Research Challenges,» *IEEE Access*, 2020.

[14] J. Holbrook, Architecting enterprise blockchain solutions, Canada: John Wiley & Sons, 2020.

[15] S. Espinosa, Guía de Referencia para la adopción e implementación de proyectos con tecnología blockchain para el Estado Colombiano, Bogotá: Ministerio de Tecnologías de la Información y las Comunicaciones, 2020.

[16] Fiscalía General de la Nación, Octubre 2021. [En línea]. Available: https://www.fiscalia.gov.co/colombia/noticia-criminal/.

[17] R. Pava, J. Pérez y L. Niño, «Perspectiva para el uso del modelo P6 de atención en salud bajo un escenari soportado en IT y blockchain,» *Tecnura*, 2020.

[18] Vivien Chan and Anna Mae Koo, «Blockchain Evidence in Internet Courts in China: The Fast Track for Evidence Collection for Online Disputes,» [En línea]. Available: https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb.

[19] European Commission, «Energy Efficiency of Blockchain Technologies,» EUBlockchain Observatory & Forum, 2021.

[20] Digiconomist, «Ethereum Energy Consumption Index,» 2021.

[21] Fiscalía General de la Nación, 2021. [En línea]. Available: https://www.fiscalia.gov.co/colombia/sentencias-y-conciliaciones-que-se-han-pagado-por-parte-de-la-fiscalia-general-de-la-nacion/.