Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

BlockChain Como Solución para la administración de expedientes digitales

Vindas Córdoba Eduardo José

Agosto, 2019

Declaratoria de Derechos de autor

Dedicatoria

Dedico esta Investigación a mi familia, en particular a mis hermanos quienes ha sido inspiración y como modelos a seguir, tanto desde una perspectiva académica, profesional, así como ética y personal.

Agradecimientos

Agradezco en primer lugar a Christopher López quien “me enrolo” a iniciar el camino de la Ciberseguridad desde una perspectiva académica.

Agradezco a Mi profesor tutor Miguel Pérez por su apoyo al proyecto, y dedicación y paciencia para con mi dicción del texto presente en esta investigación.

Agradezco al profesor Rodrigo Calvo, quien me motivo en su curso de análisis de código malicioso para aprender más sobre Análisis estático de código e ingeniería inversa, y que gracias a esas habilidades eh logrado una oportunidad en esta área en el ámbito laboral.

Agradezco a todos los profesores y equipo de la Universidad Cenfotec en general por la ayuda, conocimientos y facilidades provistas durante la trayectoria de la carrera.

Tabla de contenidos.

Tablas.

Tabla de Figuras.

Resumen Ejecutivo

La investigación se enfoca en determinar si la tecnología *blockchain* es útil para indexar o gestionar expedientes digitales, esta tecnología que es considerada por algunos expertos como una solución definitiva al problema de trazabilidad, confianza y seguridad, y aunque mucho se expresa sobre esto, hay pocos escenarios conocidos, fuera del área financiera, que hayan sido implementados exitosamente, por tanto, se investigan sus usos, posibles aplicaciones y su idoneidad para su aplicación en este ámbito, aunado a realizar una búsqueda de soluciones existentes en el mercado.

Para encontrar respuestas a las preguntas planteadas, se investiga en un marco evaluativo y más precisamente una Investigación-Acción dividida en dos grandes partes: la recopilación de información de qué es y cómo funciona la tecnología de *blockchain* y cómo se puede aplicar, mediante la generación de una prueba de concepto para solucionar el problema propuesto. Esto generando una respuesta integral para el estudio del tema, y aplicación de una posible solución en un ambiente hipotético, el cual puede ser utilizado en futuras investigaciones para soluciones completas y aplicables al mercado.

Los resultados muestran que el uso de la tecnología de *blockchain* provee una solución factible al problema propuesto y que su puesta en marcha en organizaciones públicas y privadas es posible. Sin embargo, se demuestra a su vez que las cualificaciones de las personas para aplicar esta tecnología son muy elevadas, puesto que se deben tener conocimientos amplios en criptografía, seguridad informática, administración de TI, tecnologías de comunicación y redes, desarrollo de software, y amplia capacidad analítica. Aunado a la posible necesidad de múltiples equipos distribuidos cumpliendo con propósitos intrínsecos en la tecnología. Aunque esto no sea mandatorio.

La investigación insta en prepararse mediante la centralización del conocimiento holístico de los diferentes ámbitos relacionados con la tecnología. Además, brindar perspectivas a los interesados en la tecnología para sus negocios y cómo

se puede alcanzar el uso de esta tecnología y cuáles aplicaciones prácticas existen.

Palabras claves: blockchain, hash, expedientes digitales, trazabilidad.

Capítulo I: Introducción

1. Generalidades.

En los últimos años se ha presentado un auge en la automatización de tareas cotidianas y la presentación, captación y administración de la información. En la actualidad los sistemas utilizan, cambian, mueven y presentan información de forma casi inmediata, logrando así automatizar tareas que en el pasado eran manuales y requerían tiempo para ser realizadas, cumplen con los objetivos para administrar la información de una forma competente. Sin embargo, recientemente se presenta una creciente necesidad por asegurar que estos datos sean tratados para asegurar confianza mediante su confidencialidad, integridad y disponibilidad. Los tres conceptos anteriores son parte del triángulo “CIA” (por sus siglas en inglés *Confidentiality*, *Integrity* y *Availability*) (Chia, 2012); estos aspectos son parte importante para asegurar que la información presentada en los sistemas sea de utilidad. De esta forma, se presenta una creciente necesidad de asegurar los datos, ya sea por la sensibilidad, valor o criticidad de la información, en los sistemas, como se puede ejemplificar en tecnologías bancarias, de salud, legales y otras.

La información se asegura en varios puntos, desde su reposo (almacenada en los servidores), en transmisión (cuando se transportan o viajan de una computadora a otra), y en algunos casos incluso cuando es presentada; sin embargo, en muchos ámbitos no se asegura una parte importante y critica de la información, cuando esta es adquirida, mediante el no repudio. El no repudio (Rouse, 2008) se define cómo el factor o demostración (de autoría) por utilizar para asegurar que la información fue creada por quien dice ser su autor y lograr asegurarlo por algún método. Los sistemas informáticos poseen vulnerabilidades al no tener seguridad

de la autoría de la información que es ingresada y mantenida, dada la carencia de evidencia veraz, lo cual hace difícil la trazabilidad de algunas de sus funciones, y pone en tela de duda la viabilidad legal de los sistemas, principalmente en aplicaciones tales como expedientes médicos, protocolos de abogados, registros de bienes, entre otros. Este problema da origen a la pregunta que inicia la investigación:

¿Es posible implementar tecnología que logre reforzar los aspectos de no-repudio, integridad y trazabilidad, a los expedientes digitales?

2. Antecedentes del problema.

2.1. Métodos de desarrollo de aplicaciones

Los sistemas informáticos son robustos que se dividen en múltiples Módulos, desde su presentación visual, sus llamados a servicios, realización de computaciones (o cálculos) y transformaciones de información hasta el almacenamiento en bases de datos o archivos, u otros métodos, al utilizar una variedad de patrones de diseño, pero en la actualidad se utiliza de forma extensa el modelo llamado “modelo, vista, Controlador” o MVC. Como indica (Freeman, Robson, Sierra, & Bates, 2004) da una muestra de cómo las aplicaciones robustas y grandes generalizan el uso de este modelo dado a que es una muy aceptada forma de lograr una separación entre diferentes aspectos o componentes y además al permitir la intercomunicación y separación de estos, aunado se logra también generar formas más simples para la comunicación entre diferentes aplicaciones mediante el uso de “modelos” o “controles” que se exponen mediante servicios en la Web. En un ejemplo, un servicio puede exponer elementos para servir a aplicaciones web, móviles y de escritorio.

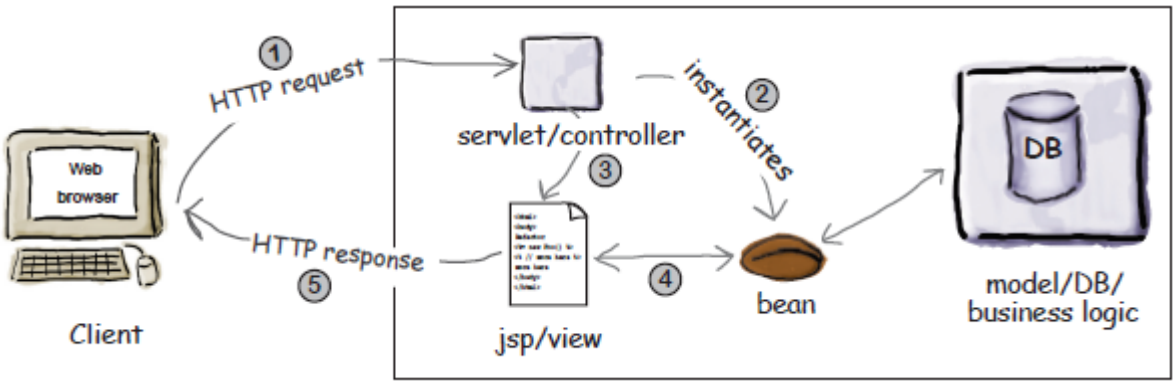


Figura No. 1 Modelo MVC

(Freeman, Robson, Sierra, & Bates, 2004)

Por tanto, gracias a la ventaja que posee para los involucrados y en muchos casos a los terceros, este patrón es uno de los más famosos si no el más famoso, cuando se habla de arquitectura de aplicaciones.

Otro método de exponer aplicaciones y procesos de negocios para lograr computación en la nube es utilizando lo que se conoce como “Web Services” (Deitel & Deitel, 2012). Los servicios web son definidos como una forma de reutilizar aplicaciones en la Internet, son componentes de software expuestos en la red(internet) los cuales se consumen mediante tecnologías como XML (Soap) o Json (Restful). Estas dos son maneras de darle formato a los datos transmitidos por la red y hacia los servidores que procesan las solicitudes. Mediante la compresión de MVC, se ejemplifica que los Servicios Web son una forma de exponer Controles a las aplicaciones (de Internet, de escritorio, entre otros)

Uno de los ejemplos más vehementes en el ámbito costarricense es el Sistema de Hacienda, el cual expone Servicios para la creación de Facturas digitales. El Ministerio de Hacienda de Costa Rica define estos documentos de la siguiente forma:

> *Los comprobantes electrónicos son archivos electrónicos generados y transmitidos en un formato universal para documentos y datos estructurados en Internet (XML), que cumplen con los*

requisitos legales y reglamentarios establecidos por la Dirección General de Tributación para las facturas, tiquetes, notas de crédito y notas de débito, garantizando la autenticidad de su origen y la integridad de su contenido.

La factura electrónica o tiquete electrónico que se emite y entrega al cliente a la hora de vender un bien o servicio, tienen la misma eficiencia jurídica y fuerza probatoria que lo tiene hoy un comprobante físico.

Recuerde que el comprobante electrónico que se emite debe ser "aceptado", "aceptado parcialmente" o "rechazado" por el receptor del comprobante electrónico cuando sea este un contribuyente, acto que se debe realizar en un plazo de 8 días hábiles para el respaldo de los gastos. Este trámite se realiza a través del mismo sistema adoptado para la emisión de comprobantes electrónicos.

Para poder anular o modificar los efectos contables de la factura electrónica o tiquete electrónico que se ha emitido, se incluye la nota de crédito electrónica y nota de débito electrónica, con la finalidad de que el documento origen y el número consecutivo prevalezcan, los cuales no podrán ser reutilizados nuevamente. - (Ministerio de Hacienda, 2018)

Esta herramienta es un ejemplo que aplica para demostrar un aspecto (control), además de definir algunos aspectos sobre seguridad POR tomar en consideración en los apartados siguientes.

En los sistemas tradicionales la información se almacena en diferentes medios como lo son en bases de datos, discos duros, almacenamiento en la nube (box, Dropbox, OneDrive, Amazon Drive, Google Drive, MediaFire), entre otros, estos sistemas pueden garantizar la integridad, disponibilidad, autoría (opcionalmente), sin embargo esto no es posible garantizar que un administrador, un tercero con

suficientes privilegios en los servidores(ya sea desarrolladores, Auditores, administradores, agentes, etc.) pueda alterar esta información en los sistemas, bases de datos o inclusive elimine altere los documentos. En estos casos en los sistemas tradicionales es posible dado a que no posee mecanismos que brinde integridad a los cambios, con algunas excepciones. (como es el caso de sistemas centralizados que cumplen con estándares de seguridad muy estricta como es el caso de certificaciones tales como PCI DSS, HIPPA, Entre otros estándares de seguridad.

En Costa Rica existe evidencia de casos donde se ha materializado esta vulnerabilidad en donde auditores, usuarios, administradores de como indica (Soto, 2019) es posible eliminar datos sin que se registre quién, y cómo se hizo, generando riesgos para las organizaciones, empresas, e inclusive el gobierno.

3. Definición y descripción del problema

3.1. Al asegurar las comunicaciones de las aplicaciones

Independientemente del método por utilizar para crear aplicaciones es indispensable el uso de tecnologías para asegurar que los datos se transmitan y posean medidas de seguridad. Existen diferentes formas de asegurar el acceso, autenticación y transferencia de datos, como es el uso de certificados digitales para proteger la transferencia de información mediante el uso de SSL/TLS, de la misma forma existen metodologías con utilización de varios métodos criptográficos para asegurar la autorización, autenticación y acceso a los datos. Evitando de esta forma que se den ataques para ver o alterar los datos en transmisión como muestra Mitani et al. (Mitani, Shinichi, Idero, & Corp, 2018), mediante el uso de la criptografía asimétrica se logra evitar vulnerabilidades y problemas con las transferencias de la información sin seguridad, mediante el uso de TLS y HTTPS para la comunicación, lo cual consiste en transmitir mediante un certificado con la llave pública y el uso de esta llave para lograr asegurar la transmisión de otra información de forma que solamente el emisor y el receptor puedan entender.

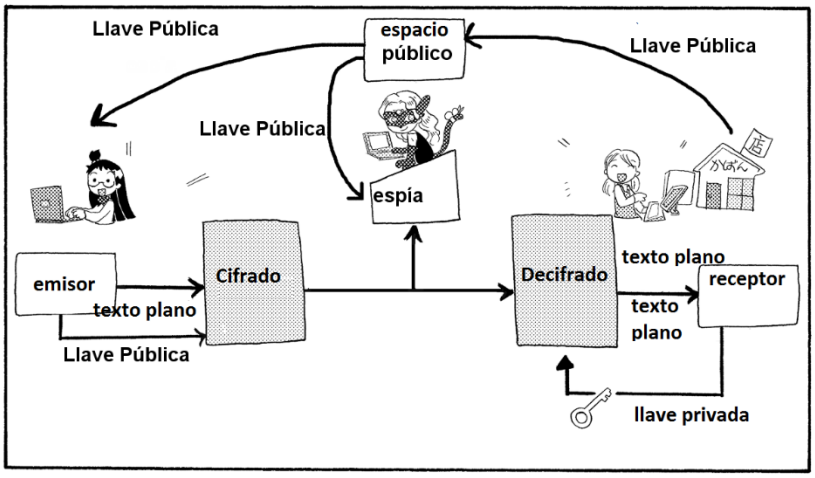


Figura No. 2 Cifrado Asimétrico

(Mitani, Shinichi, Idero, & Corp, 2018)

Cuando se ha controlado la privacidad de la comunicación entre el receptor y emisor y la protección de los datos en tránsito mediante medidas de seguridad, se eliminan posibles vulnerabilidades y posibles problemas que se pueden dar ante la publicación y trasmisión de los datos en texto plano por canales de comunicación abiertos, sin embargo, otro posible vector de ataque es el caso del hombre en el medio, que puede y debe ser manejado mediante el uso de certificados y herramientas que aseguren que el certificado sea de quien dice ser y crear una “cadena de confianza”, y en el caso de aplicaciones, es necesario tomar algunas medidas para evitar ataques que puedan generar posibles vulnerabilidades.

Un ataque de hombre en el medio es un tipo de ataque en donde, como el nombre lo dice, una persona en medio de la conversación intercepta la comunicación y se hace pasar tanto por el emisor como el receptor de las comunicaciones y donde el atacante puede cambiar el contenido de los mensajes, como muestra Mitani et al (Mitani, Shinichi, Idero, & Corp, 2018).

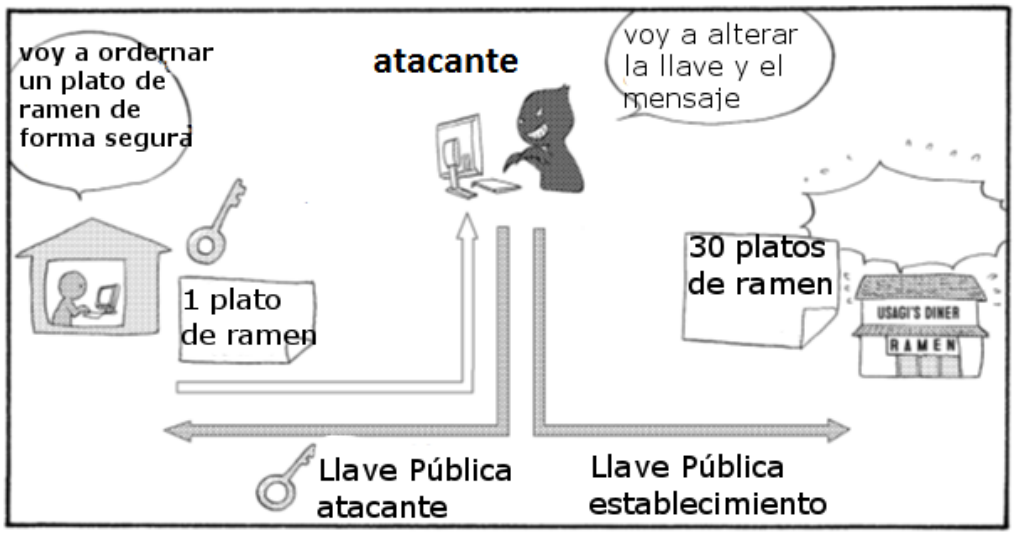


Figura No. 3 Ataque del hombre en el medio

(Mitani, Shinichi, Idero, & Corp, 2018)

En el ejemplo sobre el aplicativo del sistema del Ministerio de Hacienda se hace uso de varios métodos para asegurar que los documentos son enviados mediante medios seguros utilizando TLS, Open ID y además los documentos están firmados digitalmente (Ministerio de Hacienda, 2018), de esta forma minimizan posibles ataques de “hombre en el medio” en donde la factura podría ser alterada en tránsito mediante el uso de certificados no auténticos.

Mediante el uso de firmas en los documentos se asegura que exista integridad mediante la confirmación de la consistencia del mensaje (verificando la firma y el contenido del XML) y además logrando un no repudio para quien envió el documento, sin embargo, existen otros problemas que aún son posibles en este sistema y medidas a tomar tanto en este como en otros sistemas, los cuales se pueden mejorar mediante el uso de tecnologías en auge.

3.2. Vulnerabilidades latentes en los sistemas actuales.

Aun cuando se toman medidas aceptadas para asegurar la transmisión, recepción, autenticación y captación de la información, existen otras

vulnerabilidades que en muchos casos no son tomadas en cuenta, puesto desde una perspectiva del sistema, se asume que este está seguro (se asume que no existe una vulnerabilidad desde el interior o se han tomado las medidas necesarias para evitar la materialización de un riesgo debido a esta vulnerabilidad) o se asume una confianza absoluta en el administrador de las aplicaciones o se confía que la información suministrada por los usuarios es cien por ciento veraz y confiable, aun cuando existen más partes involucradas. Para lograr una comprensión a profundidad es necesario hacer énfasis en estos puntos.

3.2.1. El no repudio:

El no repudio es el atributo que se logra mediante medidas que aseguren que el receptor de la información tenga evidencia verificable por ambas partes que un evento, mensaje u otro es de autoría del emisor, y este a su vez sea identificable y no pueda negar dicha autoría. (esto es aplicable a ambos lados cuando se habla de una conversación y no un mensaje en particular):

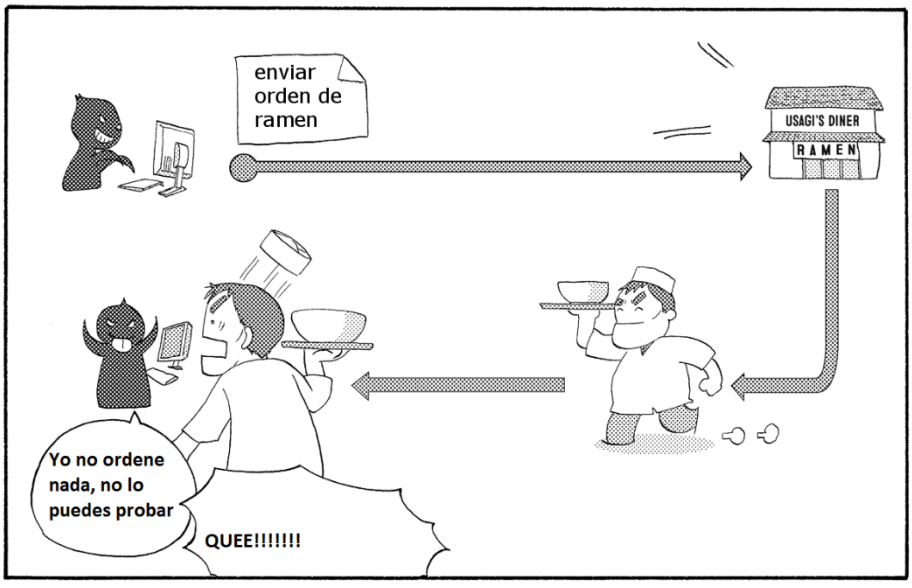


Figura No. 4 Repudio de una Solicitud

(Mitani, Shinichi, Idero, & Corp, 2018)

Al continuar con el ejemplo de Hacienda, en esta institución se logra el no repudio, por parte del contribuyente, mediante el uso de la firma digital en los documentos (Ministerio de Hacienda, 2018), mediante el uso de certificados que las organizaciones, puntos de venta e individuos deben de poseer, mediante el uso de este certificado se firma y se certifica la autoría y creación de una factura digital. Sin embargo, por parte del contribuyente no existe una medida que se pueda tomar para lograr la confirmación de la integridad y confidencialidad, puesto la respuesta indica una firma digital y respuesta desde el Ministerio de Hacienda, pero no indica donde se puede consultar la factura a posteriori, lo cual ante un incidente tal como un problema con la base de datos en el Ministerio, podría exponer a la pérdida de los documentos de un lapso de tiempo, en este caso no existe una forma de asegurar la integridad de las facturas y el contribuyente no puede verificar que su factura requiere ser enviada nuevamente. Al continuar con este ejemplo, en el caso de un sabotaje, o un borrado de facturas por impericia o de forma deliberada (ya sea mediante un acceso no autorizado exitoso o un ataque de un empleado interno) para impactar intereses individuales o de una organización, se perdería trazabilidad sobre dichas facturas puesto que el resto de la información continúa siendo íntegra.

Otro ejemplo, en donde el no repudio es necesario, es el caso de expedientes médicos. En Costa Rica gracias a la Ley 9162, se genera la necesidad de la implementación de tecnologías para pasar los expedientes físicos de salud a un medio digital. En el artículo quinto, esta ley dice que “La solución tecnológica deberá contener, al menos, las siguientes características claves (…) c) Seguridad: el expediente digital y las soluciones informáticas que interactúen con este deberán cumplir los criterios que para tal efecto se establezcan en los ámbitos tecnológico, científico, ético y administrativo, en aras de garantizar la integridad, confidencialidad y disponibilidad en el uso, manejo, archivo, conservación y propiedad de los datos contenidos en el expediente clínico.” (Ley N° 9162, 2013) y también menciona “k) Trazabilidad: el expediente digital deberá permitir llevar un registro y seguimiento de los movimientos de cada paciente, así como los suministros y recursos en los diferentes centros de salud, de tal manera que dicha

información se encuentre disponible para la toma de decisiones, bajo los principios de confidencialidad y privacidad que para tal efecto se establezcan.” (Ley N° 9162, 2013)

En la actualidad existe una implementación llamada “*Edus*” o “Expediente digital único de salud” pero no posee sistemas que garanticen la trazabilidad e integridad, puesto que no hay forma de garantizar que los elementos no han sido manipulados en la base de datos, se pueden firmar los datos y recetas médicas, pero no se firma las entradas a la base de datos, y es por tanto, y similar al ejemplo anterior, que es posible que los datos sean alterados o suprimidos en la base de datos.

Trazabilidad:

En la actualidad, una forma de garantizar una cadena de confianza es mediante la trazabilidad de los datos, desde el momento en que alguien los crea (y los registra), hasta el momento que se brinda un servicio, producto o información. Por tanto, se garantiza, poder determinar que no existen problemas con la información en los datos que son utilizados en las aplicaciones, sin embargo debido a que en la actualidad pocas aplicaciones utilizan metodologías que garanticen la trazabilidad, dependerá completamente de la confianza de los usuarios de las aplicaciones creer que la información presentada es veraz, y por parte de los administradores de la aplicación confiar que los usuarios registrados son y brindan la información que dicen brindar.

Finalmente, para lograr asegurar y evitar las vulnerabilidades anteriores es necesario el uso de nuevas tecnologías que se están desarrollando en el mercado y el uso de la tecnología de cadena de bloques resulta en una buena opción.

4. Justificación

Dada la necesidad de nuevas medidas de seguridad, tales como el no-repudio, que se deben brindar por ambas partes (los administradores o creadores de aplicaciones y los usuarios de las aplicaciones), la necesidad de lograr llevar un control y permitir la trazabilidad en los sistemas, en particular aquellos que hacen

uso de Expedientes digitales (como el caso de Expedientes médicos, legales (Judiciales, Notariales, etc.), documentos varios(facturas, u otros) y además de brindar transparencia en los procesos(tanto en la administración de la información como también en la consistencia de esta), razones por las cuales se van a exponer las ventajas y la necesidad del uso de la tecnología de cadena de bloques ("*Blockchain*") para garantizar la consistencia de los expedientes digitales y se va a llevar a cabo una prueba de concepto para ejemplificar su posible uso.

Al aplicar esta tecnología se logra bajar la cantidad de posibles vulnerabilidades en seguridad y problemas por la falta de confianza en la información, ya sea por parte del creador de esta o del administrador de los sistemas y su posible uso en causas judiciales donde se deben certificar los expedientes de forma íntegra y es indispensable cada pieza de información.

Aunado a esto se busca crear una implementación básica que demuestre las bondades de la tecnología y que a su vez sea lo suficientemente simple para su estudio académico con uso de conceptos por tanto se deberá considerar para la aplicación en un ambiente en producción que la puesta en marcha del producto, una prueba de concepto puede necesitar mayor análisis con profundidad de la solución subyacente a la presente investigación

5. Estado de la Cuestión

Se busca formular criterio, mediante la investigación, dónde se realiza un análisis de materiales, textos y documentos académicos publicados sobre la materia, para su análisis y extender conversación, discusión y ejecución mediante el uso de los conocimientos adquiridos.

5.1. Planificación de la Revisión.

En la revisión se mencionan los estudios relevantes que se han realizado y la bibliográfica consultada para llevar a cabo el desarrollo sobre el tema de la creación, modificación y aplicación de cadena de bloques, y se especifican en

esta sección los repositorios, libros, páginas y otros recursos consultados para la búsqueda de la información, así como los criterios de inclusión y exclusión utilizados en los estudios para obtener los estudios primarios.

5.1.1. Foco de la pregunta.

Esta revisión sistemática recopila los trabajos cuyo tema por tratar sea relacionado con la Cadena de bloques ("*blockchain*") o tecnologías relacionadas y su historia. Al igual que información sobre metodologías para lograr implementar esta tecnología

5.1.2. Pregunta de investigación.

¿Cómo implementar la seguridad de los expedientes digitales mediante el uso de cadenas de bloques?

5.1.3. Palabras Clave

Área	Palabra Clave	Conceptos relacionados
Software	*Blockchain*	Bitcoin Cryptocurrency
	Smart contract	
	Security	Cybersecurity File Signature
	Hashing	
	File	

	Cryptography	File Storage
	Development	

Tabla 1 Palabras claves

5.1.4. Lista de Fuentes

La lista de fuentes sobre la cual se llevará a cabo la Revisión Sistemática es la siguiente

- Google Scholar
    - IEEE Xplore
- Microsoft Academic
- Worldwide Science
- Libros sobre el tema en posesión del autor.

5.1.5. Definición del Criterio de Selección de Fuentes.

El autor de esta investigación ha seleccionado las fuentes antes mencionadas por la facilidad y acceso al conocimiento, de la mano a la abundancia de documentación con relación en el tema.

5.1.6. Lenguaje de estudio.

Las palabras claves utilizadas en la cadena de búsqueda están en idioma inglés, por ende, los resultados obtenidos a partir de la búsqueda son mayoritariamente en este lenguaje, no obstante, el informe de la revisión sistémica se realiza en el lenguaje español

5.1.7. Cadena de búsqueda.

Para las búsquedas contextuales se utilizó la siguiente cadena de texto:

> *"((blockchain or smart contract) AND (Security and computer systems)) AND NOT (Cryptocurrency or Money or Finance)*
>
> from 2008 – 2018".

Este texto define una búsqueda sobre “cadena de bloques” y “*Smart Contracts*” de forma que excluya todo aquel que sea sobre “dinero, inversiones o criptomonedas” puesto que la investigación es con relación en la tecnología y no la parte financiera o sobre las monedas relacionadas.

5.1.8. Selección de estudios.

Se accede con los repositorios para obtener una lista de estudios iniciales por medio de la cadena de búsqueda, de esta lista se analizan los estudios tomando en consideración los criterios de inclusión con el fin de obtener una lista depurada. Finalmente se aplican los criterios de exclusión para obtener una lista de estudios primarios.

5.1.9. Definición de criterios de inclusión y exclusión de estudios.

Los criterios de inclusión son. Análisis del título, Palabras Claves. Resumen o Abstracto son acordes con las palabras clave. Y el tema de elección para el estudio.

Los Criterios de exclusión. Se excluye toda obra que se enfoque a la parte de criptomoneda, dado a que el enfoque e interés es sobre el aspecto técnico y funcionalidad de “*Blockchain*” además de analizar el contenido de la publicación con el fin de determinar si la misma abarca de una manera parcial o total la respuesta a la pregunta formulada.

5.2. Ejecución de la Revisión.

Ver anexos: Ejecución de la Revisión.

6. Viabilidad

6.1. Punto de Vista técnico

El conocimiento y comprensión de la tecnología y técnicas para crear o aplicar la cadena de bloques es amplia, razón por la cual se realiza una investigación en el tema de la cadena de bloques y cómo adaptar esta tecnología a la necesidad del negocio y las áreas a las cuales se podría aplicar, y por tanto se hacen búsquedas de los estudios previos sobre esta tecnología, los cuales están disponibles en los repositorios de información, como el caso de "*Google Scholar*", pero también el uso de textos varios en el área de seguridad. Lo anterior hace que el estudio sea técnicamente viable pues se tiene acceso al conocimiento necesario para su diseño e implementación.

6.2. Punto de Vista Operativo

No se prevé una disrupción operativa durante el desarrollo de la prueba de concepto, sin embargo, puede existir una disrupción operativa ante la puesta en marcha de una solución integral que incluya esta tecnología en su sistema informático, dado a los cambios que se deben adoptar para su implementación a sistemas ya existentes y sus interfaces para aplicarlo a soluciones nuevas. No obstante, al existir las aplicaciones necesarias para la implementación de la solución se considera que operativamente este proyecto es viable.

6.3. Punto de Vista Económico

Esta investigación y creación de prueba de concepto no requiere inversión económica, el acceso a los repositorios es totalmente gratuito, por lo cual se considera económicamente viable.

7. Objetivos

7.1. Objetivo General

- Proponer una especificación de la tecnología de cadena de bloques, para la administración y seguimiento de los expedientes digitales.

7.2. Objetivos específicos

- Conocer la tecnología de la cadena de bloques, así como las diferentes implementaciones disponibles en el mercado.
- Analizar aquellas soluciones existentes y determinar si son aptas y adaptables para el uso en la solución al problema propuesto.
- Explicar las ventajas y bondades del uso de una solución basada en cadena de bloques y sus posibles aplicaciones.
- Justificar el uso de la tecnología de la solución basada en cadena de bloques en los ámbitos propuestos.
- Generar documentación para el aprendizaje del desarrollo de la tecnología de cadena de bloques para los desarrolladores cuyo conocimiento en seguridad es limitado.
- Desarrollar una prueba de concepto para exponer los beneficios y utilización de la tecnología de cadena de bloques en los expedientes digitales.

8. Alcances y limitaciones

8.1. Alcances

La investigación plasma documentación en donde se consolidan datos sobre la tecnología de cadena de bloques, algunas de las soluciones encontradas en el mercado y a su vez al generar un diseño de una propuesta y una prueba limitada del concepto, la cual servirá como muestra y documentación educativa para soluciones a futuro, para aplicar en desarrollos de software en donde se requiera

del no repudio, integridad de expedientes, completitud, trazabilidad y transparencia ante el almacenamiento de la información en sistemas informáticos pre existentes.

La creación de la prueba de concepto tiene el alcance limitado a los aspectos de la cadena de bloques (“*blockchain”)* y no se contempla como una solución integral para la admiración de expedientes o documentos digitales, por tanto, la creación de sistemas que almacenen los documentos (como son los archivos de imágenes, documentos de Word, PDF, etc.), no son tomados en consideración para la prueba de concepto.

Además, ante el uso de librerías, códigos fuentes de terceros o herramientas, cuales no se vean directamente relacionados con el tema de investigación, estos no serán, analizados con profundidad con la excepción de aquellas que sean críticas para la comprensión de las tecnologías relacionadas con la cadena de bloques.

La investigación a su vez analiza una solución en la cual sea adaptable para diferentes escenarios de aplicación, sin implicar o garantizar conocimientos de las soluciones existentes en los ámbitos para los cuales se propone, de forma que, sea una solución general la cual pueda ser fácil de adaptase y evolucionar a la necesidad de otras aplicaciones u organizaciones.

Para la prueba de concepto, se limitará al ciclo de vida de las transacciones y documentos asociados y por tanto elementos tales como la sincronización entre nodos, almacenamiento entre los nodos quedará fuera de los alcances de la investigación.

8.2. Limitaciones

La investigación está limitada a comprender la tecnología detrás de la cadena de bloques y no profundiza en aspectos relacionados con las Criptomonedas, exceptuando en los criterios donde estas sean ejemplos o necesarias para la exposición académica de la funcionalidad de la tecnología.

La prueba de concepto sobre la tecnología de cadena de bloques (“*blockchain”)* no garantiza que esta sea una solución completa o integral, dado a todas las posibles permutaciones de métodos utilizados en “*Blockchain*” aunado a su extensión y cambios constantes en la tecnología asociadas.

La prueba de concepto se limita a una prueba local con uso de múltiples hilos de ejecución para simular la existencia de múltiples servidores que autorizan las transacciones, aunado esta no presenta persistencia en la cadena de bloques. Y por tanto no ejecuta código para asegurar la persistencia de la cadena de bloques.

La aplicación de prueba hace uso de la firma digital pero no cuenta con confirmación de las transacciones con la firma digital, dado a que la finalidad de la investigación está enfocada en la materia de “*BlockChain*”, y agregar estas confirmaciones implica agregar una inversión en investigación y desarrollo de módulos para estos fines.

9. Marco de Referencia Organizacional y Socioeconómico

9.1. Historia

Blockchain (o traducido literalmente como cadena de bloques) es una tecnología la cual fue creada por Satoshi Nakamoto en un documento llamado “*Bitcoin: A Peer-to-Peer Electronic Cash System*”, Satoshi es un seudónimo que según indica Khatwani (Khatwani , 2018) su verdadera identidad real a la fecha es desconocida, pero existen varias teorías sobre su posible identidad. Como indica Khatwani (Khatwani , 2018) existen varios postulantes desde profesores, criptógrafos e inclusive colaboración de empresas que conforman el nombre “*Satoshi Nakamoto*”. Por tanto, no existe una certeza de quien es realmente el autor de la idea y la tecnología de cadena de bloques. En el documento, Satoshi describe un sistema para generar y lograr crear transacciones de forma segura mediante el uso de una cadena continua de transacciones en donde cada una es conservada de forma que las partes sin confiar en la otra pueden realizar transacciones entre ellos, este elemento plasmado en la implementación llamada

Bitcoin, este sistema revolucionario que se considera una amenaza para los grandes entes que manejan transacciones financieras, y es esta una de las razones por la que existe la creencia que el autor desea ser anónimo como indica Bearman (Bearman, 2017), además se cree que otra razón es el simple deseo de ser un desconocido, uno de los problemas que existe con el uso de *Bitcoin* es el posible doble gasto o por su nombre en inglés: "*Double Spend*" al cual se refiere en el capítulo II.

Años después se dieron copias de código con diferente nombre y algunos insignificantes cambios a Bitcoin, sin embargo y como apunta Gupta (Gupta, 2018) luego apareció un programador llamado *Vitalik Buterin* un desarrollador de 22 años que estaba involucrado en el desarrollo de Bitcoin, en el 2014, quien brinda un estudio sobre un sistema para la descentralización de la organizaciones luego conocida como Ethereum, este fue creado como un sistema para descentralizar la ejecución de aplicaciones(llamados Contratos Inteligentes) de forma distribuida, pero estas ejecuciones no son gratuitas y de forma similar a cómo se realiza en Bitcoin mediante el uso de "*Ether*" o "gas" se tiene una especie de moneda para pagar y gastar en la ejecución de los en este caso "contratos inteligentes" además cabe destacar que en el año 2016 se dio un evento en el cual se detectó y explotó el uso de un error donde un código recursivo (que se llama a si mismo) puede realizar transacciones para adquirir más "*Ether"*, esto causó una baja en la confianza en el sistema (aunque esto no vulneró a toda el sistema pero a la forma de recomenzar y realizar contratos).

Dado a que en Ethereum es un sistema de contratos, estos deben ser programados para ser procesados en la cadena de bloques y para ello requiere un lenguaje de programación que define las funciones y el código por ejecutar.

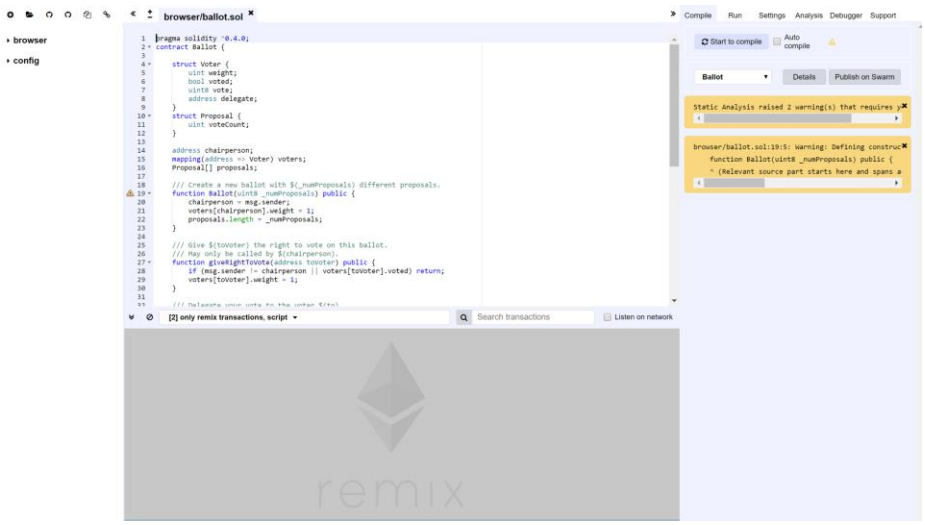


Figura No. 5 Ethereum Solidity

(Gupta, 2018)

Gupta (Gupta, 2018) indica que Hyperledger inicia en diciembre del 2015, formado por líderes en la industria de TI, como son IBM, Cisco, Accenture, SAP, NEC, CA, Intel, Red Hat, entre otros. Esta propuesta no fue diseñada con un propósito en específico, y por el contrario se diseñó con la finalidad de ser una tecnología base para crear cualquier tipo de cadena de bloques sin la necesidad de hacer una copia o adaptación de las tecnologías existentes, *Hyperledger* es administrado por la "*Linux Foundation*" otra ventaja de *Hyperledger*, es que no está relacionada a una Moneda, sino que el control se puede dar de forma granular puesto existe un nivel de control sobre la cadena.

9.2. Tipo de Negocio y Mercado Meta

La investigación está diseñada para la comunidad informática y el público que presente interés en brindar un nivel de seguridad y confianza sobre la información documental que está siendo almacenada en los sistemas, mediante el uso de la infraestructura de cadena de bloques.

El mercado meta se encuentra, pero no está limitado a las industrias tales como el sector Médico, Judicial, legislativos, hacendario, registral y cualquier otro sector que requiera la administración de documentos de forma segura, confiable,

generando no repudio gracias a las bondades de la tecnología de cadena de bloques, que permite el almacenamiento seguro de históricos de documentos o bitácoras de cambios de archivos.

9.3. Tecnología "*Blockchain"* en Costa Rica

El panorama en general sobre la tecnología *Blockchain* demuestra que es una tecnología en auge, pero cuya adopción es lenta, dado a que la tecnología no es de simple adopción y requiere capacitaciones en múltiples disciplinas, de las cuales se ha mencionado, Informática, Criptografía, Matemática, y Seguridad. Cada una de estas disciplinas son complejas y requieren mucho tiempo para la adquisición del conocimiento.

Pese a lo expuesto anteriormente, Costa Rica no escapa de la exposición de nuevas tecnologías, y el compromiso e inversión de varias instituciones, empresas e individuos es evidente en el ámbito de estas tecnologías, con diferentes grados de exposición. Entre las empresas e individuos que han realizado inversiones en esta tecnología se puede citar a:

- EOS Costa Rica: Gabriel "Gabo" Esquivel, Rodrigo Fernández
- WorldSibu: Walter Montes, Diego Barahona, y todos los colaboradores de WorldSibu
- Tecnológico de Costa Rica: posee un programa de "Especialización en *Blockchain*" el cual brinda una introducción muy superficial al tema de la tecnología de *blockchain* mayoritariamente enfocada desde la perspectiva del usuario final (quien tenga el interés de uso en su empresa y sus impactos en el ambiente de las industrias. (Tecnológico de Costa Rica, 2018)
- CryptoReds: Daniel Rojas, quien es consultor, educador en temas de *Blockchain* En Costa rica.
- Cenfotec. La Universidad Cenfotec. A pesar de no tener programas específicos de estas tecnologías, cuenta con un Programa General de Ciberseguridad en donde el tema es mencionado y las tecnologías

relevantes son área de estudio, aunado a que ha sido partícipe y anfitrión de eventos relacionados con la actividad de *Blockchain*.

Se han presentado actividades en Costa Rica relacionadas con *Blockchain,* sin embargo, es de destacar que muchas de estas actividades no cuentan con la exposición tan marcada de otras tecnologías como por ejemplo en el campo del "*Machine Learning*" (e inclusive extendiéndose a Inteligencia Artificial) esto debido a la perspectiva y educación del público y las organizaciones sobre la tecnología de *Blockchain* que para muchos está directamente conectada al aspecto de criptomonedas, lo cual no es cierto puesto que está tecnología puede ser aplicada en muchos más ámbitos fuera del sistema monetario, pero aun con estas limitantes, en Costa Rica se han brindado exposiciones, realizado actividades de aplicación y exposición de tecnologías al aplicar las bases de tecnologías de "*BlockChain"* para la trazabilidad de productos. Y por tanto se menciona dos actividades destacables en Costa Rica:

Hackathon de "*BlockChain"* (Cenfotec)

El sábado 27 y domingo 28 de octubre del 2018 se realizó una Hackathon, en la cual se expuso a grupos de desarrollo para la creación de una solución basada en Código de WorldSibu, este que a su vez realizaba una implementación de *Hyperledger* (una especificación de código abierto de *Blockchain*) para generar y asegurar la trazabilidad del café costarricense que se exporta al exterior. (Universidad Cenfotec, 2018)

Figura No. 6 Boucher de la Actividad Hackathon

En esta actividad se llevó a cabo la aplicación de grupos de desarrollo para la creación de aplicaciones que lograran brindar una solución a problemas de trazabilidad de productos como el café costarricense el cual es nuestro “grano de oro” y un producto el cual en Costa Rica y el mundo se considere el mejor (Instituto del Cafe de Costa Rica, 2019)

Sin embargo, esta actividad demostró una problemática latente en general para los desarrolladores. La cual es, la grave falta de conocimiento sobre los componentes de la tecnología con la cual trabajan. Desde la tecnología específica de *blockchain,* así como los aspectos de seguridad relacionados como lo son la criptografía (*hashing*, criptografía simétrica y criptografía asimétrica), seguridad informática, estampado del tiempo, protocolos de comunicación. A la hora de exponer las soluciones se denotaron algunas redundancias entre lo que se guardaba en las transacciones versus lo que la tecnología ya realiza “por defecto”. Estas observaciones son oportunidades de importancia por considerar puesto que para lograr un crecimiento en los profesionales actuales y futuros en las tecnologías en auge como es el caso de *blockchain* es indispensable que la tecnología se aplique con conocimiento indicado y sin redundar en la información utilizada

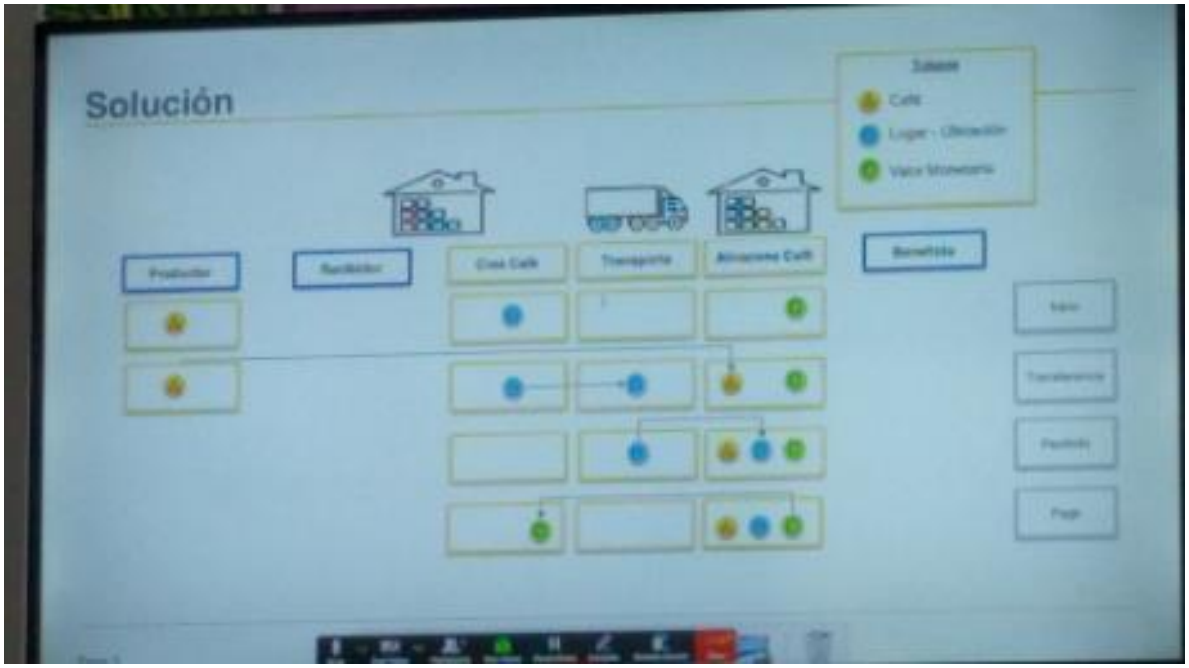


Figura No. 7 Exposición de solución en la conferencia

TicoBlockchain

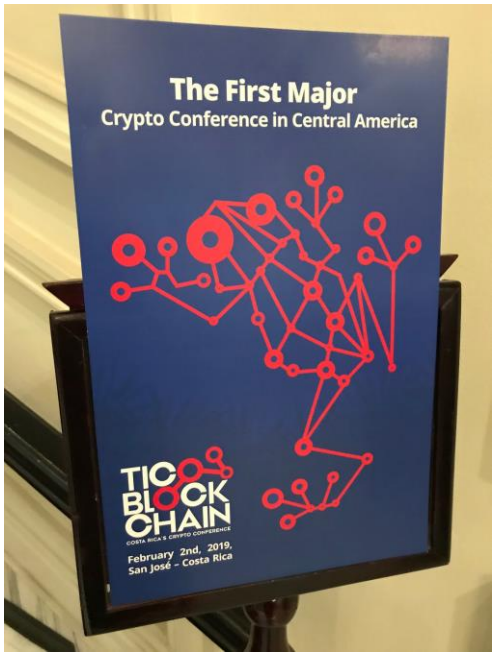


Figura No. 8 Poster de la actividad Tico Blockchain

(Esquivel, 2019)

El “TicoBlockchain” fue una conferencia con diferentes exposiciones brindada por expertos en los temas de *Blockchain* en Costa Rica, en el Club Unión el día dos

de febrero del dos mil diecinueve. En estas conferencias se realizaron exposiciones en diferentes niveles y ramas de conocimiento. Al exponer diferentes tecnologías, e inclusive introduciendo los conceptos de "*Blockchain"* a personas tanto técnicas como no técnicas. Además, permitió a profesionales del área de la informática realizar "*networking"* con posibles interesados en la tecnología expuesta en campos como: alimentos, medicina, legal, bancario, entre otros.

Además, exponer tecnologías alternas a los contratos inteligentes como fue el caso de la tecnología de "EOS", la cual es un protocolo de "*Blockchain*" similar a Ethereum, que posee exposición y negocios en Costa Rica.

Capítulo II: Marco Teórico

1. Conceptos base

La investigación se basa en la documentación y evaluación de los conceptos preexistentes sobre la tecnología de cadena de bloques y sus posibles usos prácticos para la administración de expedientes y sistemas aplicables en el mercado. Por tanto, se realiza un marco teórico de las definiciones encontradas en los documentos de referencia vistos en el estado de la cuestión.

La tecnología que se desea aplicar requiere la definición de algunos métodos criptográficos utilizados muy fuertemente utilizados en la tecnología de cadena de bloques, en particular las funciones de Hash. Como define Mitani et al (Mitani, Shinichi, Idero, & Corp, 2018) una función Hash es una "función de una sola dirección", el mensaje no puede ser derivado desde el valor de resultado, este funciona como una huella digital, la cual es única y exclusiva para el mensaje de entrada. Y por tanto se utiliza de forma fuerte en muchos medios como una forma de confirmar la consistencia, el contenido y la veracidad de un mensaje o documento.

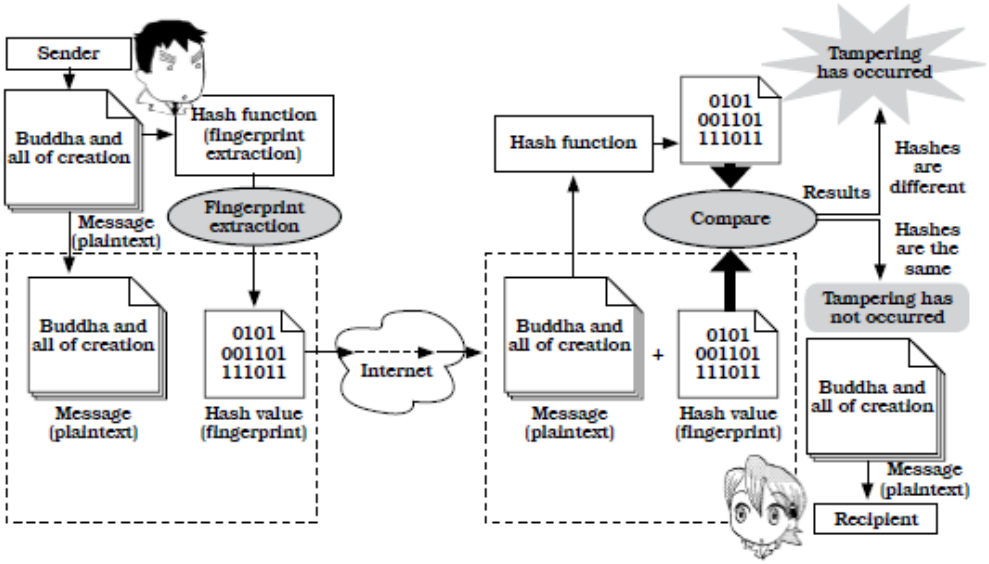
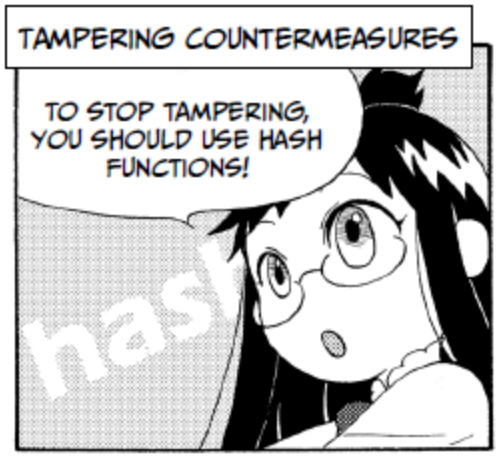


Figura No. 9 Firma digital de un Mensaje

(Mitani, Shinichi, Idero, & Corp, 2018)

Por tanto, con estas fórmulas matemáticas que son utilizadas para verificar los mensajes se podrá determinar qué usos tendrán en la tecnología y esto permite una característica crítica para la tecnología de cadena de bloques.



(contramedidas contra alteraciones. "para detener las alteraciones usted debería usar funciones Hash.", traducción libre)

Figura No. 10 Contramedidas para evitar alteración

(Mitani, Shinichi, Idero, & Corp, 2018)

Otro concepto necesario para comprender la tecnología de cadena de bloques es la criptografía asimétrica.

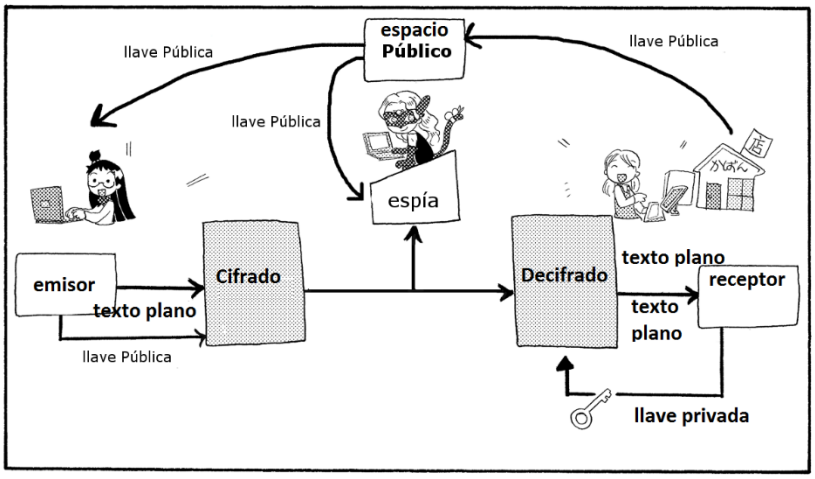


Figura No. 11 Cifrado Asimétrico, traducción libre

(Mitani, Shinichi, Idero, & Corp, 2018)

En el caso de cadena de bloques, la criptografía de llave asimétrica es utilizada como medio de mantener las “llaves de identificación” y de firma para el uso en las funciones de Hash, y por tanto la criptografía de llave simétrica usa dos llaves: una llave privada, la cual es un valor el cual se debe mantener privado, confidencial y la llave pública que es la parte que se brinda públicamente a todos en el sistema para que se pueda confirmar la identidad y confirmar las firmas.

Estas llaves son utilizadas para autenticación e identificación en los sistemas, así como firmar las transacciones donde la llave privada es utilizada para saber o permitir transacciones y la llave pública para firmar los “recibos” de las transacciones que son ingresadas en el sistema. Como se analizará a continuación es una de las piezas claves para los sistemas basados en cadena de bloques.

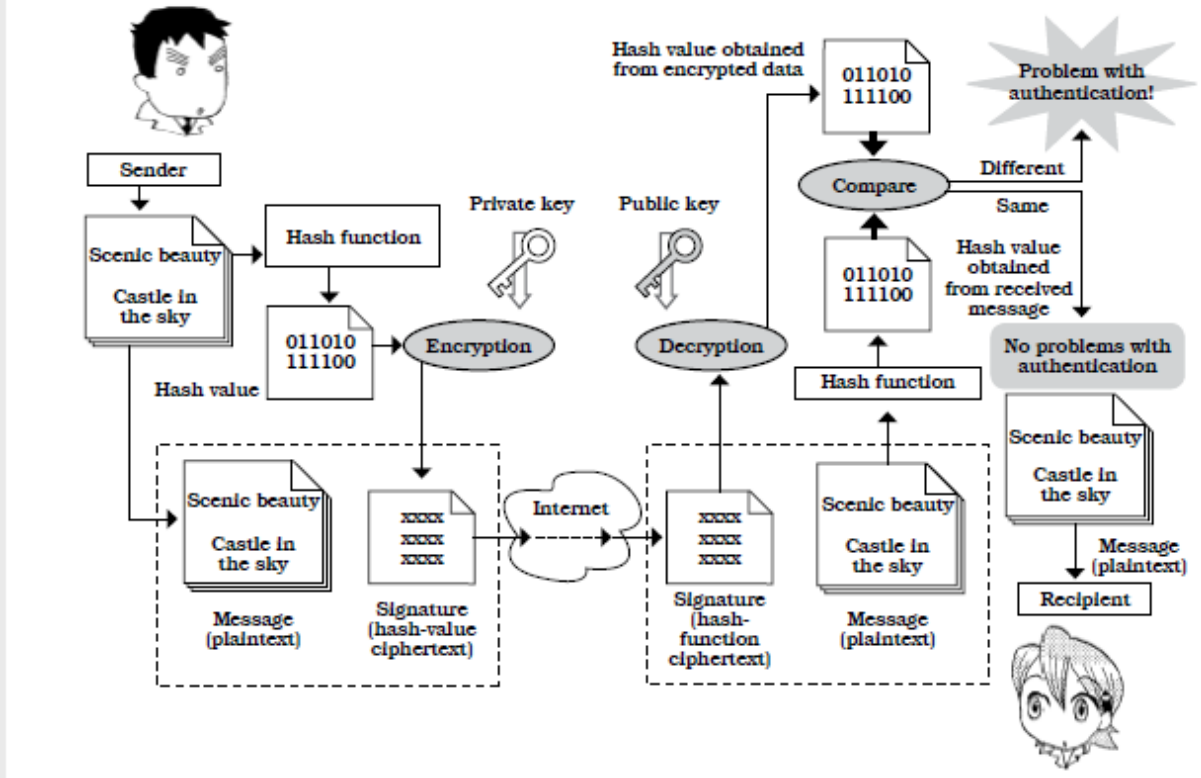


Figura No. 12 Autenticación Mediante Llave Asimétrica

(Mitani, Shinichi, Idero, & Corp, 2018)

2. Engranaje de la cadena de bloques

Como se menciona en apartados anteriores, la tecnología de cadena de bloques fue creada por Satoshi Nakamoto, la propuesta que crea Satoshi se basa en una cadena conceptual de bloques que están compuestos por transacciones.

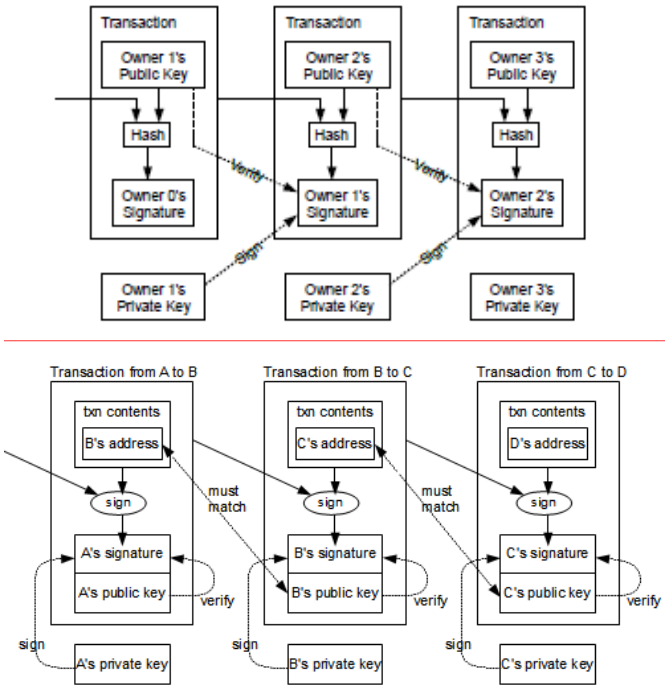


Figura No. 13 Estructura de transacciones

(Nakamoto, 2008) (Sherriff, 2014)

Como se muestra en la propuesta, se define que en una cadena existen varias transacciones.

Una transacción es una forma de describir cambios en la cadena de bloques, estas pueden representar cambios de valores (dinero, artículos, ventas, datos, etc.) o movimientos de otra índole (transferencia de datos o ingresos con base de datos) estas usualmente están compuestas, por “metadatos”, los cuales dan contexto lo que se hace o almacena en la cadena de bloques, es usual encontrar datos tales como: emisor, receptor y dato transaccionado. Se generaliza por tanto una transacción de la siguiente forma:

Campo	Descripción
Emisor	Quién o dónde solicita enviar o realizar la transacción
Receptor	Quién o dónde se recibe la transacción
Cambios	Los datos o cambios a la cadena en cuestión

Tabla 2 Abstracto de una transacción

Fuente: confección propia

En estas transacciones se calcula un valor numérico único o Hash, el cual "firma" la transacción mediante el uso de las llaves criptográficas y pueden ser confirmadas por la llave privada de los dueños, o las llaves públicas (para otras verificaciones) y es mediante estas firmas que se logra consistencia y autoría de las transacciones al igual que no repudio, el bloque en sí se crea mediante una lista de transacciones en un "bloque".

El "bloque" se puede expresar de una forma abstracta de la siguiente manera:

Campo	Descripción
Hash del bloque (ID)	Identificador, único del bloque
Cabeceras (metadatos)	Datos relevantes sobre el bloque
Datos	El contenido particular del bloque (usualmente un árbol de Merkle)
Hash Previo (id anterior)	Identificador, único del bloque anterior
Firma de tiempo	Firma de tiempo del block (tiempo de creación)
<otros datos>	Otros datos que puede encontrar (varía en cada implementación) Por ejemplo el "*Nonce*"

Tabla 3 Abstracto de un bloque

Fuente: confección propia

Dentro del bloque se firman las transacciones vía Hash, y un valor "aleatorio" llamado "*Nonce*" (o valor de uso único), el cual es utilizado en aquellas cadenas de bloques que basan su método de "consenso" en algo llamado "Prueba de Trabajo" (*Proof-of-Work*) (Nakamoto, 2008)

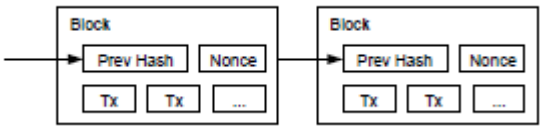


Figura No. 14 Estructura de bloque

(Nakamoto, 2008)

Este concepto se puede simplificar de otra manera, como una cadena donde cada nodo es continuado por otro, y estos se enlazan entre sí mediante un identificador que indica dónde se encuentra el anterior o siguiente, en el ámbito de desarrollo de Software y estructuras de datos sería similar a una lista enlazada. Con la diferencia de que la lista de la cadena de bloques es inmutable (no puede cambiar puesto que un cambio en esta dejaría la cadena en un estado inconsistente)

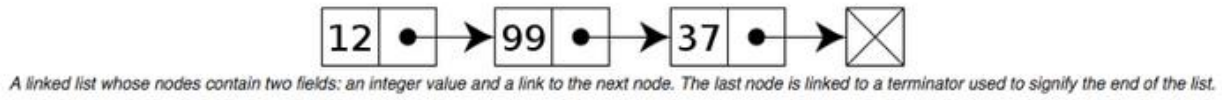


Figura No. 15 Descripción de una lista enlazada

(Marín, 2018)

3. Métodos de consenso.

Los métodos de consenso son procesos mediante los cuales la cadena de bloques verifica que su información sea consistente y que la nueva información cumpla con dicha consistencia, similar a un disparador (“*trigger”*) en base de datos, sin embargo a diferencia de las bases de datos estos procesos son obligatorios para determinar que los datos son consistentes a la cadena, además en algunas especificaciones de cadenas de bloques estos procesos expanden sus funciones, entre otras pueden hacer verificaciones de gastos o valores dentro de las transacciones (verificar que la persona realiza una transacción válida, posee suficiente del recurso (esto es variable y dependiente del tipo de cadena a utilizar), inclusive se puede definir funciones cargadas de forma dinámica por los programadores, de aspectos en la cadena de bloques.

En la publicación de Satoshi, se indica únicamente un método para la verificación y lograr la distribución del trabajo de la creación de bloques. Estos son creados mediante una actividad a la cual se le llama “minar”.

Por tanto, minar desde una perspectiva técnica, es el proceso de tomar transacciones que están en un apartado del sistema de cadena de bloques como

“no inscritas”, o dicho de otra forma que están en espera de formar parte de la cadena, se toman se verifica la consistencia matemática mediante las funciones hash, contra la cadena y las verificaciones de las firmas, “*Nonce*” y “hash previo”, con estos datos, se calcula un nuevo Hash el cual debe cumplir una regla matemática para el bloque por ingresar a la cadena y de ser así, se considera que se encontró el “hash dorado” el cual se agrega a la cadena. Los “mineros” son aquellos que se encargan de calcular los bloques, a su vez ante el descubrimiento de un bloque el “minero” (o grupo de) se ve recompensado. Sin embargo, este método no es el único, como indica Gupta (Gupta, 2018), quien brinda una perspectiva más amplia dado a la evolución de la tecnología, y existen otros métodos de consenso ya sea descentralizado o incluso centralizado (aunque un poco menos populares dado el propósito de la tecnología.)

4. Verificación de transacciones

Otro de los aspectos por destacar sobre la tecnología de cadena de bloques es como se verifican las transacciones sin la necesidad de verificar todo el histórico de las mismas (ver qué, cómo y cuánto se transaccionó) esto se logra mediante una metodología de búsqueda binaria en un árbol de “Merkle”.

Creado por Ralph C. Merkle y patentado (Estados Unidos Patent No. US4309569A, 1979) como indica Kozliner (Kozliner, 2017). La forma en que se aplica este método en bitcoin y en la publicación de Nakamoto (Nakamoto, 2008) es mediante el uso de los valores *Hash* de las transacciones. Por tanto, para ejemplificar se posee:

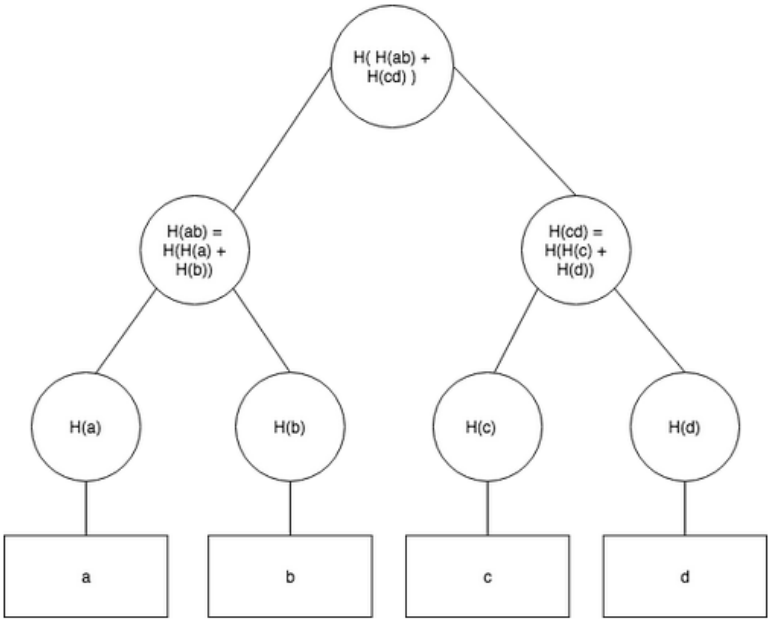


Figura No. 16 Árbol de Merkle

(Kozliner, 2017)

En donde ($h(x)$) es la función Hash y por tanto para verificar que la transacción sucedió se verifica la transacción contra el hash y también permite verificar la consistencia del bloque y que las transacciones son parte de este bloque.

Esto a su vez permite una mejora en los tiempos de cálculo y verificación de la constancia de datos dentro de la cadena, puesto que una verificación manual daría tiempos de computación inaceptables, Buchmann (Buchmann, 2007) además explica la raíz de estos árboles la cual está de la mano a propuestas creadas por Whitfield Diffie y Martin E. Hellman, Winternitz,

5. Red de nodos

Con lo anterior definido, concluye la documentación presentada por Nakamoto (Nakamoto, 2008) pero no es el final de los conceptos utilizados en las cadenas de bloques, por ejemplo, cada una de las implementaciones requiere algún tipo de almacenamiento ya sea permanente o temporal para guardar “la cadena”, las transacciones pendientes, y otros aspectos específicos de cada tipo de cadenas, dado a la variedad de estos métodos no se ingresará a ser definido en este capítulo.

Con relación a la red, dado que la tecnología de bloques no es una tecnología centralizada, pero en la publicación de Satoshi, no hay información específica sobre cómo mantener la red, Nakamoto (Nakamoto, 2008) menciona la existencia de una red y que las transacciones se deben transmitir a los “nodos” pero no menciona qué son y cómo funcionan. Algo que expande Gupta (Gupta, 2018) y muestra cómo los nodos son servidores que forman parte de la red que genera un consenso en cómo la cadena es “aceptada” (aparte del consenso de aceptar un bloque también debe existir el consenso de cuál bloque seguir)

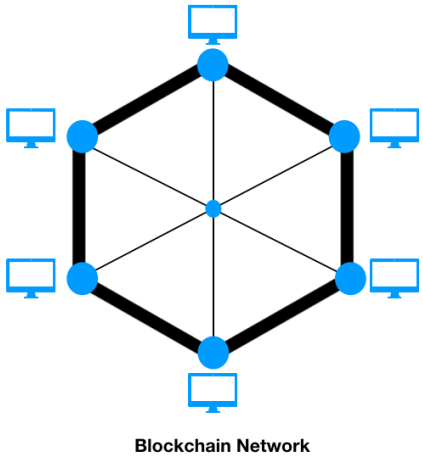


Figura No. 17 Red De Blockchain

(Gupta, 2018)

Existe una cantidad de consideración de medios de comunicación. En el caso de Bitcoin se utiliza la tecnología llamada “*Json-RPC*”, esta tecnología se divide en dos partes:

- *Json*. Son siglas que significa “*JavaScript Object Notation*”. La cual es una notación para la escritura de archivos y transmisión de datos por internet de forma liviana, si el propósito es lograr persistir datos y estructuras (inicialmente de *JavaScript*) en archivos o texto que fuera fácil de leer tanto para máquinas como humanos (Ecma, 2017), hay que considerar que a la fecha las metodologías (e inclusive aun en uso) persisten la información en formatos muy verbosos como es el *eXtensible Markup Language (XML)* en donde los datos son altamente repetitivos para enviar datos simples.

Considérese el siguiente ejemplo:

XML	Json

<?xml version="1.1"?>
<greeting>Hello, world! **<**/greeting>
	{
	" greeting ": " Hello, world!"
	}

Tabla 4 Comparación de XML vs Json

Fuente: confección propia

Por tanto, en el anterior ejemplo se demuestra no solo el requisito de más datos, además se demuestra la innecesaria redundancia de datos (el identificador se repite) para efectos de envió de información amplia, como podría ser enviar transacciones de muchas páginas y datos se necesitaría redundar muchos datos. Para su transmisión, si bien existen herramientas en los lectores como el uso de compresión previo y posterior a la transmisión de los datos en la práctica se ha demostrado no ser aplicado. Y por tanto *Json* ha es una herramienta muy importante en la evolución de internet. De igual manera para el uso de las cadenas de bloques es de interés puesto simplifica la cantidad y formato de los datos.

- "*remote procedure call*" (RPC): en Computación RPC es in método por el cual se crean métodos para llamar o ejecutar código en otro o el mismo equipo, estas llamadas pueden ser en el mismo proceso o en otro proceso, en una computadora externa, inclusive en la internet, en los lenguajes orientados a objetos este mismo procedimiento se puede llamar RMI por sus siglas, "*Remote Method Call*" (Satran, 2018)

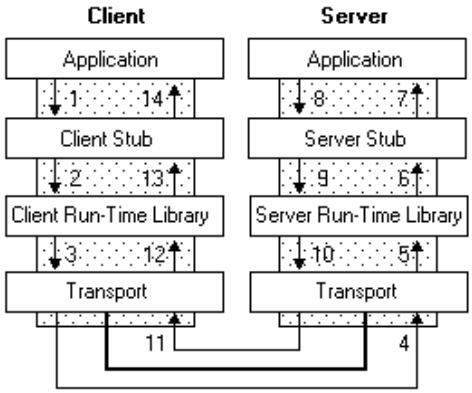


Figura No. 18 Diseño abstracto de una propuesta para la cadena de bloques

(Satran, 2018)

Aun con este concepto claro se debe aclarar, esta tecnología no es la única. Para la comunicación y sincronización de la cadena de nodos, Este es intercambiable. otros métodos se pueden aplicar, en el tanto cumplan con ciertas reglas, las cuales garantizan la comunicación, seguridad, y consistencia de la red de nodos:

- Todos los nodos deben tener la posibilidad de comunicarse entre sí y registrarse para recibir notificaciones, entre los distintos nodos
- Las comunicaciones deben ser entre las partes directamente (de un nodo a otro) o conocido también como "*Peer To Peer"*

Para cumplir con estas reglas múltiples cadenas de bloques implementan diferentes métodos de comunicación entre los cuales se mencionan los siguientes:

- Apache Kafka (hyperledger, 2017)
- Google gRPC (Zih-Ci, 2017)
- Redis (Meunier, 2016)
- Java JMS
    - IBM MQ (IBM, 2019)
    - Apache Camel (Bilgin, 2018)

6. Diversidad de la cadena de bloques

La tecnología de cadena de bloques, no se limita a los aspectos que se definieron en su publicación inicial, gracias a la naturaleza abierta y “código libre” lo que permite a cualquier persona con el conocimiento suficiente en programación y criptografía a realizar cambios, mejoras, e inclusive tomar la idea y alterarla a conveniencia para otro propósito, ya sea con fines comerciales, gubernamentales, u otros, y es gracias a esta facilidad que existen otras cadenas de bloques aparte de la cadena creada por Satoshi. Algunos son simplemente copias o puestas en marcha por otras personas, pero algunos son cambios drásticos, donde la cadena posee conceptos distintos en distintas secciones.

Por ejemplo, en el caso de Ethereum (Gupta, 2018) quien brinda una perspectiva de cómo funciona esta cadena, en contraste a Bitcoin, Ethereum no se enfoca en el libro contable, sino se enfoca más en “contratos inteligentes”(*Smart Contracts*), lo que permite crear programas que definen las reglas base que se utilizarán en la ejecución de un plan, o un programa, un tabla, juegos, entre otros. Por ejemplo, en Ethereum es posible crear código de programación que funcione de forma tal que pueda ejecutar juegos de azar, similar a una lotería, o juegos de cartas, y de esta manera lograr poner en marcha un “casino online” sobre la base de Ethereum y por ende la cadena de bloques. Un ejemplo de juegos basado en esta tecnología es “CryptoZombie” (Loom Network et all., 2018) una plataforma que enseña a codificar videojuegos en Ethereum.

Posterior a introducir el próximo ejemplo es necesario definir que es un DNS (en este trabajo se hace una definición de DNS de una forma limitada dado a que esta tecnología no es relevante para la investigación y no se hará uso extensivo de esta tecnología para propósitos prácticos de la investigación). En el libro “*DNS and Bind*” (Liu & Albitz, 2006) se define DNS como las siglas para “*Domain Name System*”, una base de datos distribuida, la cual guarda información de los nombres de las direcciones que son utilizadas en los navegadores, traducidas a números de direccionamiento IP relacionados a estos nombres.

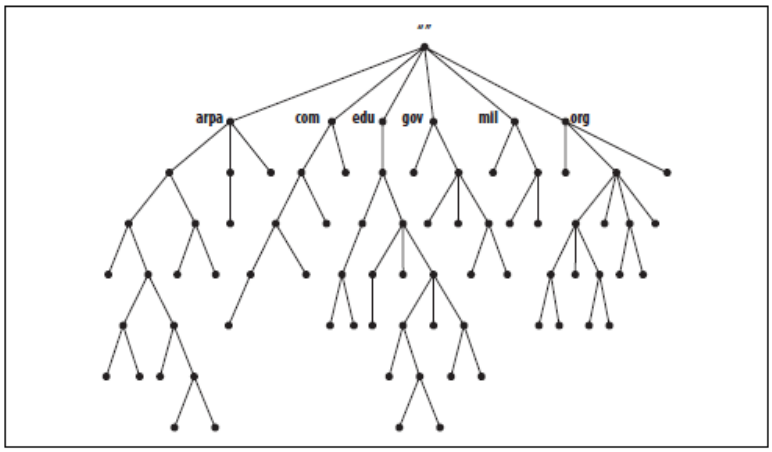


Figure 2-1. The structure of the DNS namespace

Figura No. 19 Estructura de DNS

(Liu & Albitz, 2006)

En este árbol se muestra un diagrama representativo de la organización de la base de datos. (Liu & Albitz, 2006)

```
movie.edu. IN SOA toystory.movie.edu. al.movie.edu. (
                        1       ; Serial
                        3h      ; Refresh after 3 hours
                        1h      ; Retry after 1 hour
                        1w      ; Expire after 1 week
                        1h )    ; Negative caching TTL of 1 hour

;
; Name servers
;
movie.edu.  IN NS  toystory.movie.edu.
movie.edu.  IN NS  wormhole.movie.edu.

;
; Addresses for the canonical names
;
localhost.movie.edu.      IN A     127.0.0.1
shrek.movie.edu.          IN A     192.249.249.2
toystory.movie.edu.       IN A     192.249.249.3
monsters-inc.movie.edu.   IN A     192.249.249.4
misery.movie.edu.         IN A     192.253.253.2
shining.movie.edu.        IN A     192.253.253.3
carrie.movie.edu.         IN A     192.253.253.4
wormhole.movie.edu.       IN A     192.249.249.1
wormhole.movie.edu.       IN A     192.253.253.1

;
; Aliases
;
toys.movie.edu.       IN CNAME toystory.movie.edu.
mi.movie.edu.         IN CNAME monsters-inc.movie.edu.
wh.movie.edu.         IN CNAME wormhole.movie.edu.

;
; Interface specific names
;
```

Figura No. 20 Un ejemplo de la base de datos en forma “texto plano”

(Liu & Albitz, 2006)

Otro ejemplo de otra metodología de manejar una cadena de bloques es el caso de remplazar los servidores de DNS. "*Blockstack"* es una solución propuesta por Ali et al (Ali, Shea, Nelson, & Freedman, 2017) donde proponen un sistema el cual funciona en Bitcoin, Ethereum, y otras cadenas de bloques, y propone algo que llaman BNS ("*Blockchain Name System*"). Lograr correr el sistema sobre varias cadenas de bloques se logra mediante el uso de capas que separan las diferencias en las cadenas, y además agrega funcionalidad necesaria para el BNS.

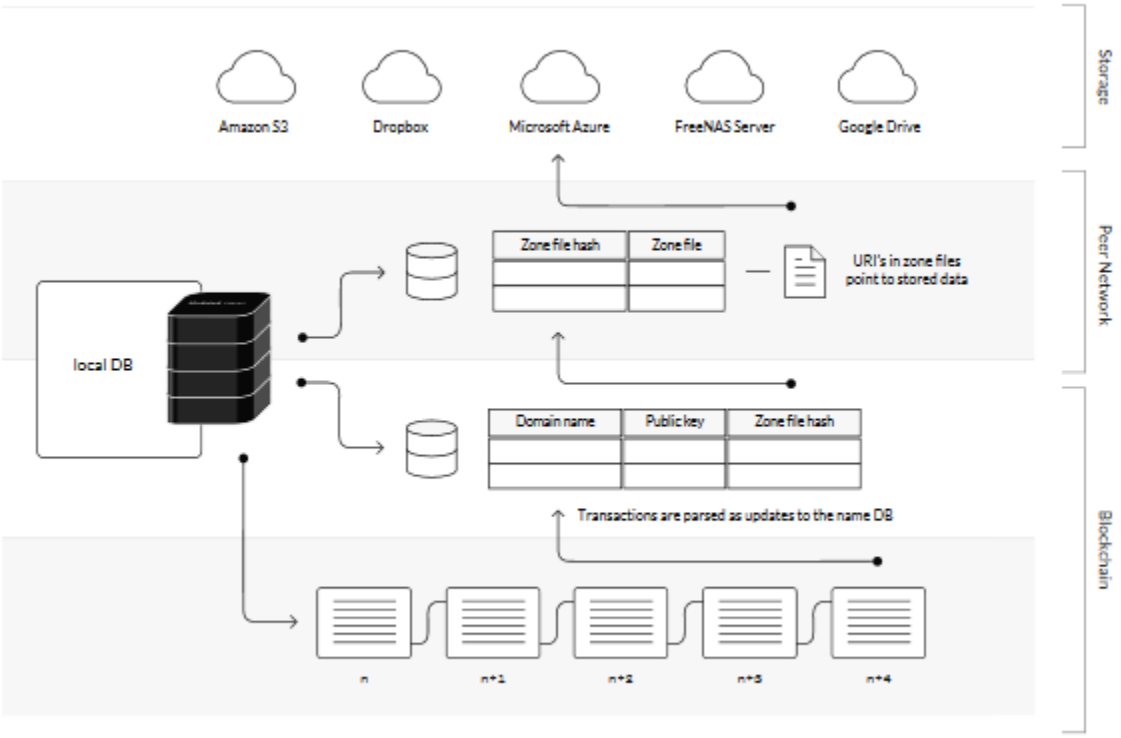


Figura No. 21 Estructura de "BlockStack Blockchain"

(Ali, Shea, Nelson, & Freedman, 2017)

En la figura anterior se muestra la forma en que se separa el sistema. Se separa en las siguientes capas:

1. Cadena de bloques. Donde la cadena funciona como medio de proveer consenso a los cambios o nuevos nombres que se añaden al sistema y como base para almacenar parte de los datos. Un dato interesante es que

el sistema que define “*Blockstack”* utiliza “cadenas virtuales” que funcionan sobre las cadenas, lo cual permite que sea agnóstico de la cadena sobre la cual trabaja. Lo cual es una funcionalidad que para el propósito de la investigación puede no ser útil, pero se considera una característica muy interesante y rescatable.

2. La red (Peer Network). Es una red de personas (similar a como funciona Torrents con los “Seeds Y leachers” o personas involucradas con la información) en este caso se utilizan los “p*eers”* similar a diccionarios para saber a dónde se encuentran los repositorios de datos (las nubes) ya sea Dropbox, Amazon, Azure, etc.
3. Almacenamiento. La capa más alta. Es la capa de almacenamiento la cual puede o no ser confiable. Dado que utiliza la cadena virtual para la verificación de la consistencia y si es veraz.

Esta última característica en la capa de almacenamiento es importante porque es algo útil para la implementación deseada en la investigación, sin embargo, esta cadena tiene una implementación más compleja de lo deseado para los fines prácticos a los cuales se desea aplicar a la investigación.

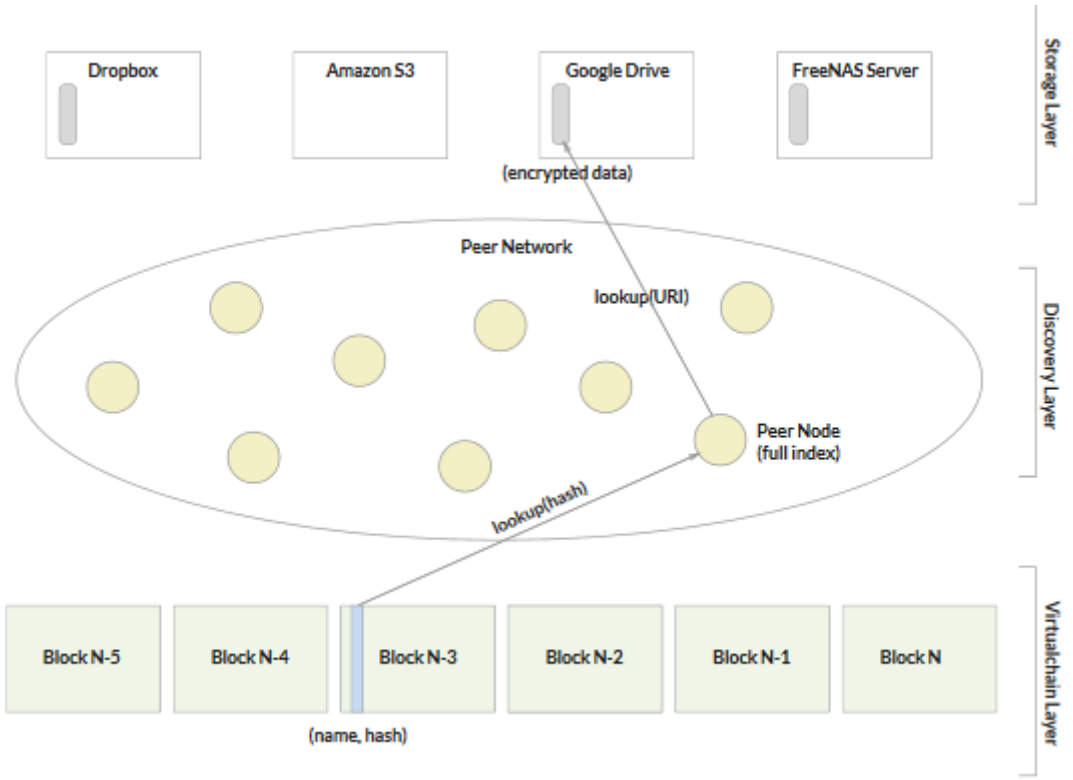


Figura No. 22 Diagrama de Funcionamiento para Buscar datos en "BlockStack"
(Ali, Shea, Nelson, & Freedman, 2017)

Como se muestra en el diagrama, (Ali, Shea, Nelson, & Freedman, 2017) "*Blockstack"* crea una forma de guardar datos descentralizada y siendo la cadena (cadena virtual) la cual indica donde se encuentra en la red de "Peers" el archivo y mediante el Peer obtener el archivo en cuestión que se encuentra cifrado.

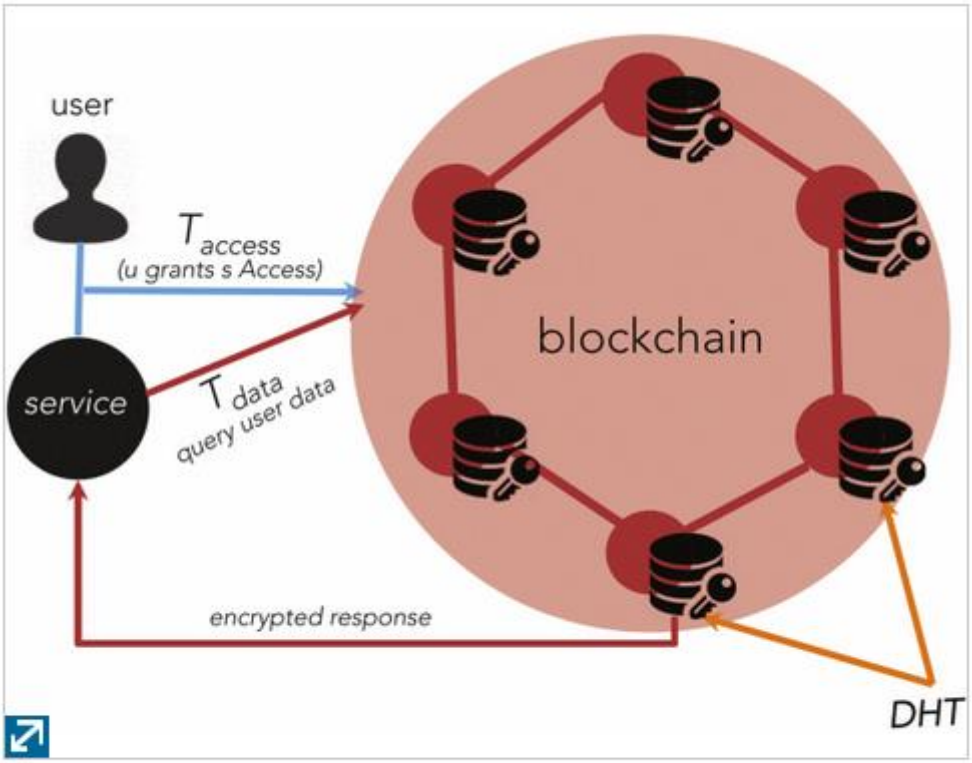


Fig. 1.
Overview of the decentralized platform.

Figura No. 23 Blockchain de datos privados

(Zyskind, Nathan, & Pentland, 2015)

Un problema presentado por Zyskind et al (Zyskind, Nathan, & Pentland, 2015) crea claridad en el problema de "partes" de la cadena de bloques no puede ser cerrado por partes y partes de estos no pueden ser privadas. Esto al menos utilizando la tecnología tradicional de la cadena de bloques. Puesto toda transacción es pública, y parte de sus datos deben ser públicos para lograr ser procesados por las metodologías de consenso, esta característica generar dificultad para utilizar una cadena pública para solucionar la pregunta propuesta en esta investigación, y siendo esto un aspecto crítico en la investigación que requiere ser verificado.

7. Métodos de consenso aplicados en el mercado

Las cadenas de bloques según define Nakamoto (Nakamoto, 2008) son un método de consenso mediante la "*Proof of Work*", este método lo que realiza es

trabajo computacional para lograr generar un bloque en la cadena, pero este método es “dinámico”, de otra forma se puede expresar que el método de prueba es intercambiable por otro método que defina una forma de generar de forma aceptable y segura el bloque. Inicialmente encontrar métodos que no fueran “*Proof of Work*” y lograr ser una plataforma descentralizada aun no era posible. Gupta (Gupta, 2018) lista algunos de los métodos que son aplicados, los cuales incluyen:

- “*Proof of Stake*” (PoS) traducible como Prueba de Inversión, similar a “*Proof of Work*” (PoW) o prueba de trabajo, es un método que provee consenso mediante el uso de un método que es descentralizado, pero a diferencia de PoW este método no requiere poder computacional sino una prueba de inversión sobre una transacción.

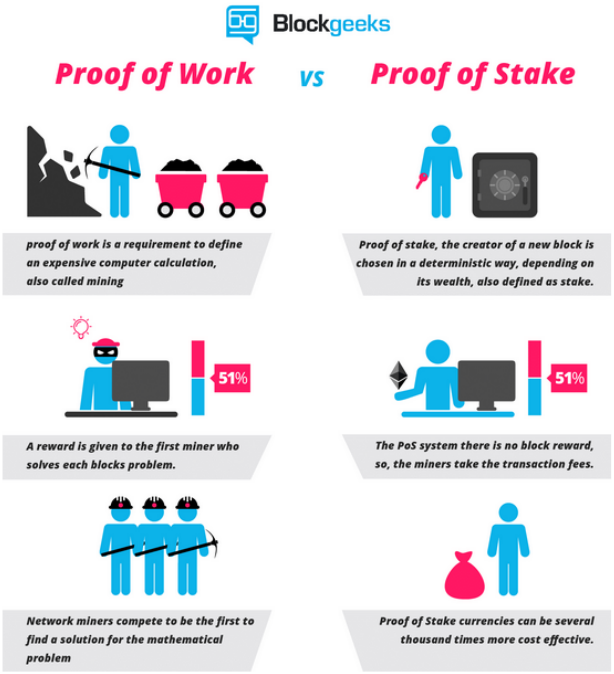


Figura No. 24 Comparativa entre Proof of Work y Proof of Stake

(Rosic, 2018)

- “*Byzantine Fault Tolerance*”. La tolerancia bizantina a fallas es un método el cual es utilizado para detectar inconsistencias y actuar ante la caída o inconsistencias en un nodo, este método es la base del *Proof of Authority*.

- "*Proof of Storage*". Prueba de almacenamiento es un método utilizado para evitar el uso del poder computacional, pero en su lugar solicitar almacenamiento y transmisión de datos para brindar un consenso. Esto se hace a su vez para utilizar el espacio para mantener los datos de la cadena y el "minero" es recompensado por permitir el uso del espacio.
- "*Proof of Authority*". Prueba de autoridad, es un método en donde se utiliza similar a "*Proof of Stake"*, pero en este método se autoriza a personas a ser aquellos que autoricen las transacciones o la creación de bloques, como indica (De Angelis, 2018), su velocidad de procesamiento de los bloques es mucho más alta, lo que permite la confirmación de las transacciones y verificación de estos en la cadena de forma más rápida, este sistema de consenso. Los Algoritmos basados en "*Proof of Authority*" dependen de que los nodos (o llamados en este caso "Autoridades") sean de confianza y honestos, o al menos un 51% ($\frac{n}{2} + 1$). Esto se considera de esta forma para asegurar que las transacciones aceptadas sean Verificables y autorizadas. Para lograr el consenso, esta metodología aplica una distribución de responsabilidades de la creación de bloques, entre los Nodos, estos proponen un nuevo bloque a los demás nodos, y los otros aceptan o rechazan (implementación Aura), ante la aceptación estos replican la aceptación a otros nodos. O simplemente lo acepta sin proceso de votación (Implementación Clique) u otros son simples como Paxos (PEASE, R, & LAMPORT, 1987) o Tolerancia Bizantina a errores ("*Byzantine Fault Tolerance*")

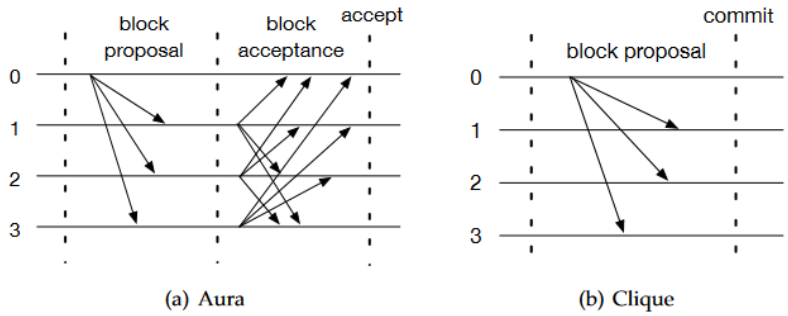


Figura No. 25 Implementaciones PoA

(De Angelis, 2018)

Estos no son todos los métodos existentes e inclusive es posible la creación de más metodologías para alcanzar el consenso en la red.

¿Qué tipos de *Blockchain* posee el mercado?, Y ¿cuál es el idóneo para la investigación?

Como indica De Angelis (De Angelis, 2018) existen varias clasificaciones de las cadenas de bloques. Y como se expone con anterioridad existen varios métodos de implementación, pero como se analiza en la siguiente tabla, las clasificaciones son relativas al nivel de privacidad o público meta.

tipo	Lectura	Escritura	confirmación
Público sin permisos	Abierto a todo público	Posible por cualquier persona	Cualquier persona puede colaborar
Consorcio o partes interesadas	Restringido a las autoridades que participan	Autoridades participantes	Todas las partes involucradas
Privado o con permisos especiales	Completa privacidad limitado a los nodos o autorizados	Operador de la red	Operador de la red

Tabla 5 Tipos de Sistema de Cadena de Bloques

(De Angelis, 2018) traducción libre

De esta forma se brinda los conocimientos necesarios para iniciar la creación de una cadena de bloques basando algunas ideas que se plasman en la bibliografía.

8. Ataques Y Vulnerabilidades

Double Spend, es un tipo de ataque en donde en las redes de *Blockchain* y como menciona (Hill, Chopra, & Valencourt, 2018) en donde indican que, al utilizar o realizar transacciones, estas realizan el uso de algún recurso, una vez que se

utiliza esté toma una cantidad determinada de tiempo en verse reflejada en la cadena y por tanto es posible utilizar un recurso más de una vez, a pesar de haber sido utilizado. Otra forma de realizar un doble gasto es mediante el control del 51% de la cadena.

Otro ataque posible indicado por (Hill, Chopra, & Valencourt, 2018) es el ataque del 51%, este consiste en que si una organización, persona, grupo de personas, etc. controlan el poder de la cadena de bloques a un mínimo del 51%, tiene el poder de influir las transacciones que son aceptadas en la cadena

Capítulo III: Marco Metodológico

La investigación se desarrolla en el marco flexible donde la prueba de concepto de este pueda ser utilizada en múltiples ámbitos. Se plantea como una solución a problemas existentes mediante la aplicación de tecnologías de seguridad informática, al utilizar tecnologías y estudios existentes y de vanguardia.

El estudio se lleva a cabo mediante la “Investigación-Acción”, metodología propuesta por Kurt Lewin, pero se utiliza mediante la definición que genera ELLIOTT, J: la investigación – acción se entiende como «el estudio de una

situación social para tratar de mejorar la calidad de la acción en la misma».” (Herreras, 2004), aunado a esto muestra la literatura (Rodriguez Gomez & Valldeoriola Roquet, Metodologia de la investigacion, 2009) que es un paradigma interpretativo cuyo principal objetivo es transformar la realidad, mediante la “Actividad Reflexiva” (investigación) y hacia “Actividad Transformadora” (educar, ejemplificar y crear una prueba de concepto con el material de investigación.)

Hay aspectos que caracterizan la investigación-acción los cuales son:

“*Los cinco grandes rasgos que nos permiten distinguir una investigación-acción de cualquier otra actividad investigadora o experiencia educativa son:*

1. *El objeto de la investigación-acción es la transformación de la práctica educativa o social, a la vez que se procura comprenderla mejor.*
2. *Hay una articulación permanente de la investigación, la acción y la formación a lo largo de todo el proceso.*
3. *Se da una manera particular de acercarse a la realidad: vincular conocimiento y transformación.*
4. *El protagonismo es de los educadores-investigadores.*
5. *Hay una interpelación del grupo*

” (Rodriguez Gomez & Valldeoriola Roquet, Metodologia de la investigacion, 2009)

Estos son rasgos que son considerados

al brindar a su vez una ventaja, al conocimiento generado, se propone una continuidad, mediante investigaciones posteriores a esta para lograr una mejora continua y soluciones especializadas para diferentes necesidades futuras. Este concepto se ejemplifica mejor con la siguiente figura:

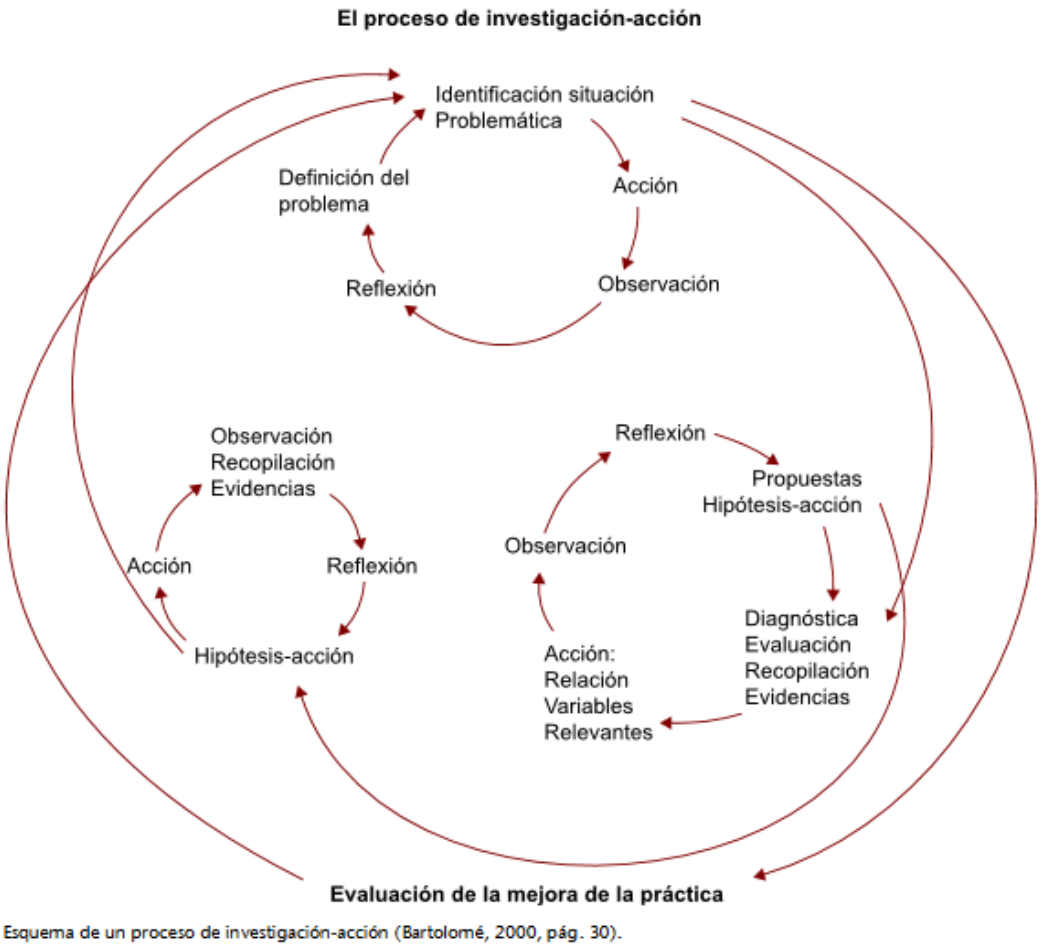


Figura No. 26 Esquema del proceso investigación-acción

(Rodriguez Gomez & Valldeoriola Roquet, Metodologia de la investigacion, 2009)

1. Tipo de Investigación

Según indica Serrano et al (Serrano Pastor, Ato García, & Amorós Poveda, 2008) la investigación evaluativa "*constituye una síntesis al mismo tiempo que una extensión de una amplia gama de métodos de investigación que aportan información sobre cuestiones planteadas en torno a los programas educativos, con el fin de facilitar la toma de decisiones sobre los mismos*".

Aunado como indica Hernández y Martínez (Hernandez Sanchez & Dolores Martínez, 2014) "*podría decirse que la investigación evaluativa pretende resolver problemas concretos a partir de la generación de vías alternativas de proceder*

sobre la realidad estudiada. La generación de sugerencias u opciones de cambio han de ir orientadas hacia la toma de decisiones, necesaria para incidir en el cambio o cambios concretos. Este tipo de investigación es fuertemente reconocida por su utilidad social y por su capacidad de cambio en beneficio de la mejora, siempre sobre la base de unos criterios básicos de credibilidad, isomorfismo y factibilidad."

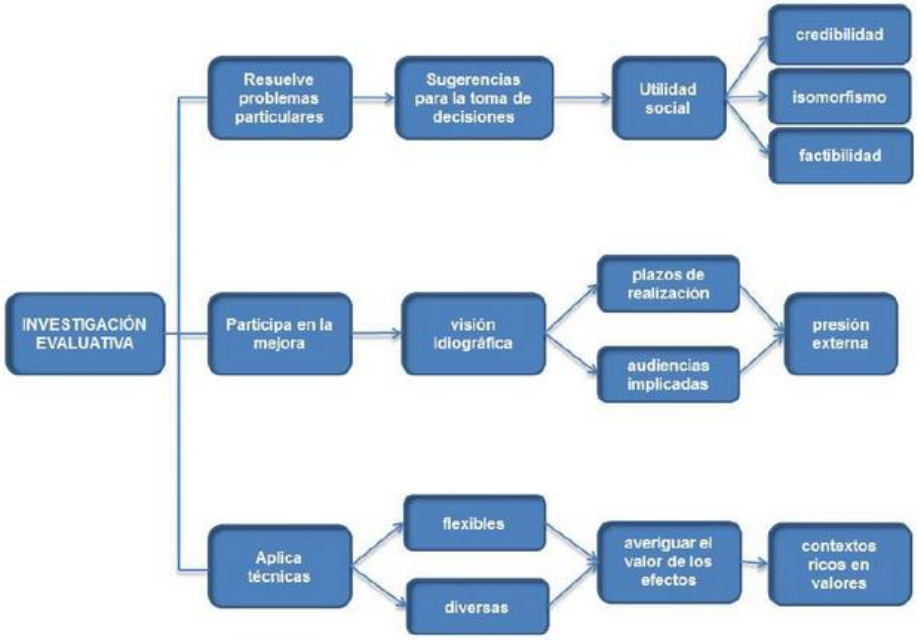


Figura No. 27 Desglose para la Investigación Evaluativa

(Hernandez Sanchez & Dolores Martínez, 2014)

Lo anterior expresado es aplicable a la investigación dado a que recopila en estudios existentes información de las diferentes metodologías y técnicas existentes para la creación de cadenas de bloques aunado a esto se busca realizar una Mejora y crear una prueba de concepto para generar una visión Idiográfica y lograr generar una demostración de las bondades de la tecnología aplicada al mercado.

2. Alcance Investigativo

El alcance de la presente investigación se limita a documentar, estudiar, interpretar y generar una prueba de concepto limitada la cual implementará las

ventajas de la tecnología estudiada. El estudio no aporta una solución completa sino una prueba de concepto limitada a demostrar las posibilidades de la aplicación para un nuevo método creación de sistemas para la admiración de expedientes, archivos, folios, bitácoras entre otros donde la tecnología pueda ser implementada.

3. Enfoque

Como indica Serrano et al (Serrano Pastor, Ato García, & Amorós Poveda, 2008) para la investigación evaluativa indica que ambos enfoques posibles son seleccionables, pero dependerá del tema y tipo de datos por utilizar, en este caso se selecciona el enfoque de carácter Cualitativo mediante el análisis de los estudios previos y la generación de prueba de concepto y recomendaciones sobre el uso de la tecnología.

4. Diseño

Siguiendo las recomendaciones de Serrano et al (Serrano Pastor, Ato García, & Amorós Poveda, 2008), el diseño para la investigación seria Cualitativo - Acción puesto se aborda una recopilación evaluativa de datos existentes y una acción de generar una prueba de concepto como indican Rodríguez y Valldeoriola (Rodriguez Gomez & Valldeoriola Roquet, Metodologia de la investigacion, 2009)

5. Población y Muestreo

La población meta se encuentra en varios ámbitos en sectores diversos, que van desde el área Médica, Legal, Hacendario, Gubernamental e incluso empresas privadas dada la versatilidad y posibles aplicaciones de la tecnología propuesta. Sin embargo, la investigación enfoca sus posibles aplicaciones a un escenario donde los sectores mencionados (médico y legal) se vean impactados.

Capítulo IV: Análisis del Diagnóstico

1. Análisis de tecnologías disponibles para la creación de la cadena

En los apartados anteriores se mencionaron algunas de las tecnologías que se encuentran en el mercado de *Blockchain*, por tanto, se realiza un análisis de las tecnologías y si estas son aptas para la solución que se propone para la administración de expedientes digitales y si estas a su vez cumplen con los objetivos propuestos.

- Ethereum. Esta red de bloques no es una buena opción puesto esta posee el problema que sus métodos para su uso requiere utilizar “dinero” ya sea virtual o real para la puesta en marcha desde la perspectiva de uso de “*Gas*”(o poder computacional) o el uso de “*Ether*” para transaccionar en la Cadena de bloques, además de esto si bien es posible el cambio a una metodología de *Proof of Authority*, la documentación para realizar este cambio es complejo de asimilar y posee ciertas limitaciones en la puesta en marcha.

  Otro inconveniente detectado es ante la creación de un contrato inteligente para la administración de este sistema se estaría generando una complejidad alta y un costo muy elevado, suponiendo que la solución escale o se utilice como una solución aplicada dado a que a mayor cantidad de expedientes en los contratos requeriría mayor demanda por parte de las máquinas virtuales dentro de un contrato inteligente
- *Bitcoin*. La cadena de bloques original, la cual es el génesis de la revolución de las cadenas de bloques, sin embargo, esta no cumple con las necesidades del proyecto, puesto bitcoin está diseñado específicamente para las transacciones de naturaleza de cambio de bienes (monedas o valor) y lo que se propone es la administración de expedientes digitales, por tanto, requiere valores más complejos e información más extensa que solo la transacción y movimientos de valor

- *BlockStack*. Esta solución es muy atractiva, y posee ventajas que serían de mucha utilidad para la solución por implementar, sin embargo, esta solución posee problemas de que es altamente compleja, posee muchos aspectos que requieren investigación que sobrepasa el alcance de esta investigación. Y además el uso de esta tecnología dificultaría mejoras futuras sobre esta propuesta, y posiblemente sería complicado de modificar para aplicarlo sobre otras tecnologías de cadenas de bloques.
- *Hyperledger (Fabric).* La tecnología creada por una gran variedad de organizaciones, pero cuyos mayores "inversionistas" de conocimiento son la fundación Linux, IBM, Cisco, Red Hat, JP Morgan, ANZ bank, entre otros es una opción interesante, todo lo que forma esta tecnología es de código abierto. *Hyperledger* es un término sombrilla para una cantidad variada de productos entre los que se encuentran "*Hyperledger Fabric, Indy, Iroha, Sawtooth, caliper*" entre otros. (Santos & Moura, 2019)

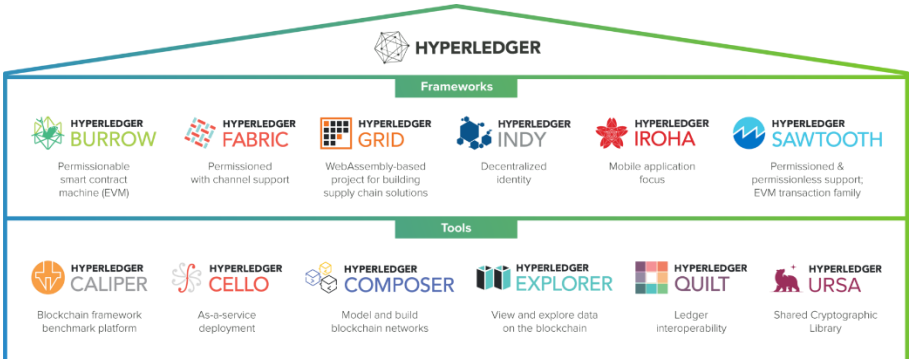


Figura No. 28 Tecnologías Hyperledger

(Santos & Moura, 2019)

Las tecnologías de *Hyperledger* se dividen en familias de "productos", algunos como se puede mencionar:

- *Sawtooth* es una colección de interfases y códigos escritos en diferentes lenguajes de programación diseñados para simplificar escribir aplicaciones que interactúen con los servicios de un B*lockchain*.

- *Ursa* es una colección de librerías y algoritmos criptográficos utilizados en la mayoría de los proyectos *Hyperledger* la razón de centralizar estas librerías es con el propósito de facilitar el proceso de actualización y reparar posibles problemas que se puedan dar con las librerías de seguridad.
- *Composer.* Es una herramienta que facilita y hace más simple la creación de contratos inteligentes en el *blockchain* sin embargo esta herramienta no es compatible con la última versión de *Fabric*

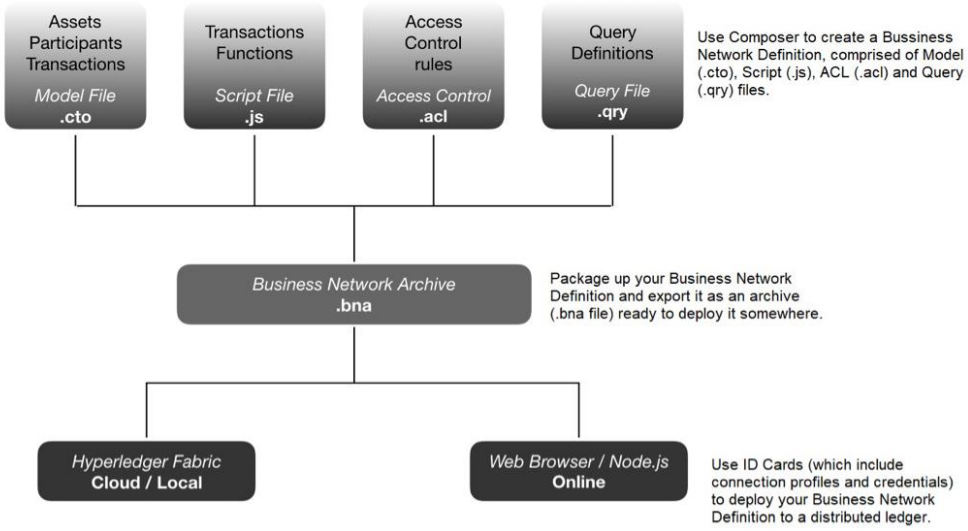


Figura No. 29 Representación de la arquitectura de la Herramienta Composer

(Santos & Moura, 2019)

- *Fabric*. Es la implementación de "*blockchain"* realizada por la organización de empresas que forma *Hyperledger.*

Hyperledger es una excelente opción para crear cadenas de bloques privadas en donde su método de consenso puede ser variable. Sin embargo adaptar una opción específica para lograr consenso es complicado puesto requiere crear los "módulos de consenso" desde cero o en su defecto utilizar "Apache Kafka", quien es un sistema el cual permite distribuir cargas (en este caso distribuir la carga de quien se encargará de procesar y anunciar la creación de un bloque en la cadena) , en la práctica

el uso de esta aplicación general un método de consenso basado en "votación" (Kumar, 2018).

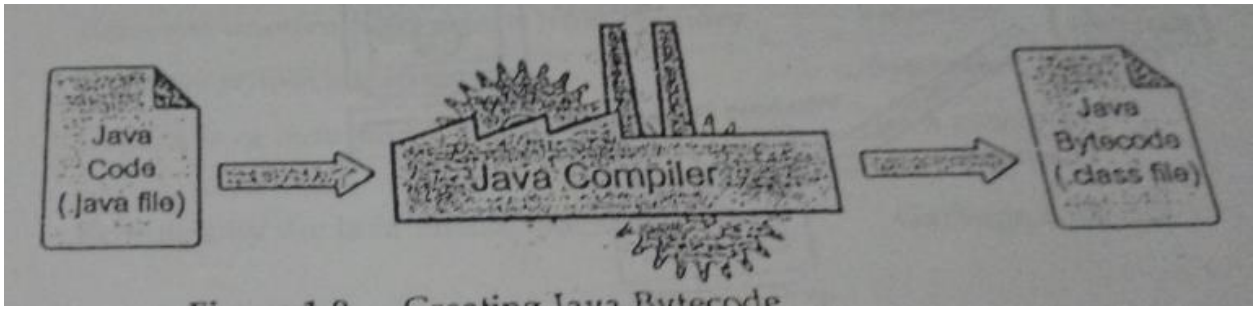
Un problema que se presenta con el uso de *Hyperledger* en la propuesta es la complejidad que posee para su implementación y comprensión académica, puesto no solo es necesario un entendimiento avanzado en la tecnología de "*blockchain",* además posee la limitante de a pesar de ser una tecnología con un tiempo en el mercado no es una tecnología madura, y cambia constantemente, aunado posee limitantes con respecto de las tecnologías que son compatibles para su uso dado a que se limita a tecnologías de lenguajes de programación como "*Go*" y "*JavaScript*" y otros lenguajes a pesar que poseen soporte, es limitado o posee limitantes que generan posibles vulnerabilidades ante su implementación y como se menciona (Papegaaij, 2018) en la conferencia J-Spring 2018. Hay aspectos que *Hyperledger* que aún no son maduros e intuitivos para realizar aplicaciones complejas.

- Implementación de un *Blockchain* de cero. Crear una implementación desde cero, es una opción posible para realizar una prueba de concepto, pero con el costo de realizar el estudio de los códigos que se deben de implementar además del estudio de las librerías de seguridad a utilizar y extender el estudio a los códigos utilizados, siendo esto bueno desde la perspectiva académica para explicar, documentar y exponer, pero en contraste se expone el costo de crear, entender y documentar esta información. Además de generar posibles vulnerabilidades dado la falta de pruebas y uso de la tecnología, vs el extenso uso de las tecnologías disponibles en el mercado.

Capítulo V: Propuesta De Solución

1. Tecnología por utilizar

Para la puesta en marcha de la prueba de concepto se ha tomado la decisión de hacerlo “desde cero” al utilizar el lenguaje de programación *Java*, el cual permite desarrollar una prueba de concepto de forma que muchos profesionales en informática puedan comprender el código (desarrolladores Java, C, C++, JavaScript), además brinda bondades del lenguaje que permite crear un prototipo maduro en poco tiempo dado ventajas tales como: uso agnóstico de la plataforma (puede ser ejecutado en cualquier sistema que permita el uso de la máquina virtual de Java tales como Windows, Linux, Mainframes, etc. Esto debido a que Java no compila o crea ejecutables para máquinas sino para la máquina virtual de Java la cual está disponible en muchas plataformas, como expresa (Sun Microsystems Inc., 2002)



Código java -> compilador Java -> “bytecode” Java (traducción libre)

Figura No. 30 Compilación de código Java *(Sun Microsystems Inc., 2002)*

Por tanto, con código que es generado para máquinas virtuales pueden luego ser ejecutado en cualquier máquina virtual en todas las diferentes plataformas soportadas.

Otra de las ventajas de utilizar este lenguaje, que ayuda a evitar varios problemas de seguridad por la mala administración de memoria o referencias (sin embargo, no los elimina completamente)

Otra de las razones para seleccionar la puesta en marcha de cero, se debe a la oportunidad de exposición académica del código para el aprendizaje de los lectores. Puesto durante la investigación se detecta una carencia de implementaciones que sean simples para aprender y comprender la tecnología a profundidad.

Una puesta en marcha al utilizar *Hyperledger* es posible, más causa un problema que para el analista y los académicos no brinda aprendizaje

2. Actores usuales de la cadena de bloques

En el *blockchain* existen una variedad de actores que son similares indistintamente de la implementación, algunos poseen nombres distintos sin embargo al final sus responsabilidades serán las mismas. Por tanto, se listan los actores más comunes o listados con sus nombres genéricos.

- Arquitecto del *blockchain*(A). El Arquitecto es aquella persona que se encargará de generar el diseño inicial de la cadena de bloques, de hacer el análisis de los requerimientos y hacer las consultas con los posibles clientes para realizar el levantamiento de los casos de uso.
- Desarrollador del *blockchain*(D). El Desarrollador es el encargado de crear las aplicaciones (o en su defecto los API) para que los clientes (u otros desarrolladores) puedan hacer uso del *blockchain.*
- Operador de la red (del *blockchain*) (O). Similar a infraestructuras de sistemas informáticos clásicos se debe tener un administrador, en este caso en contraste es un poco más crítico dado a la naturaleza descentralizada(posible) de los servicios, servidores de la infraestructura y además asegura el acceso protegido y seguro de las comunicaciones entre los equipos.

- Plataformas de sistemas informáticos (-). Realiza las computaciones necesarias en el sistema de cadena de bloques(*blockchain*).
- Fuentes de información (bases de datos) (-). No es secreto que los datos deben estar localizados en algún lugar, en el caso de *blockchain los datos* privados pueden estar guardados en bases de datos tradicionales, ya sea de forma centralizada o distribuida, controlados por una sola entidad o por varios. Por bases de datos Relacionales tradicionales (SQL) o no Relacionales (No-SQL)
- Servicios de membresía (ALC): servicios o tecnologías que controlan el acceso o permisos sobre la información encontrada en la cadena de bloques (*blockchain*)
- Usuarios (U). Los usuarios pueden tener diferentes roles y niveles de acceso, sin embargo, se generaliza que los Usuarios son aquellos que pueden ingresar nuevas transacciones a la cadena. Se exponen los siguientes ejemplos:
    - Cadena De bloques de expedientes médicos
        - medico
        - paciente
        - Secretario
        - Farmacéutico

        En estos casos cada uno de los listados anteriores son usuarios de la cadena de bloques.

- Reguladores/ Auditores(R). Son aquellos actores que no tienen acceso a la cadena más allá de la consulta de la cadena. Dependiendo de la implementación puede o no tener acceso a los datos descifrados. O simplemente acceso a las relaciones en las transacciones, por ejemplo:
    - Un auditor puede ver que un ciudadano tuvo una cita médica. Pero puede (o no) tener acceso a los detalles de (quién fue) cual fue el contenido y/o diagnóstico de la consulta, quién fue el médico que realizó el diagnóstico. Etc.

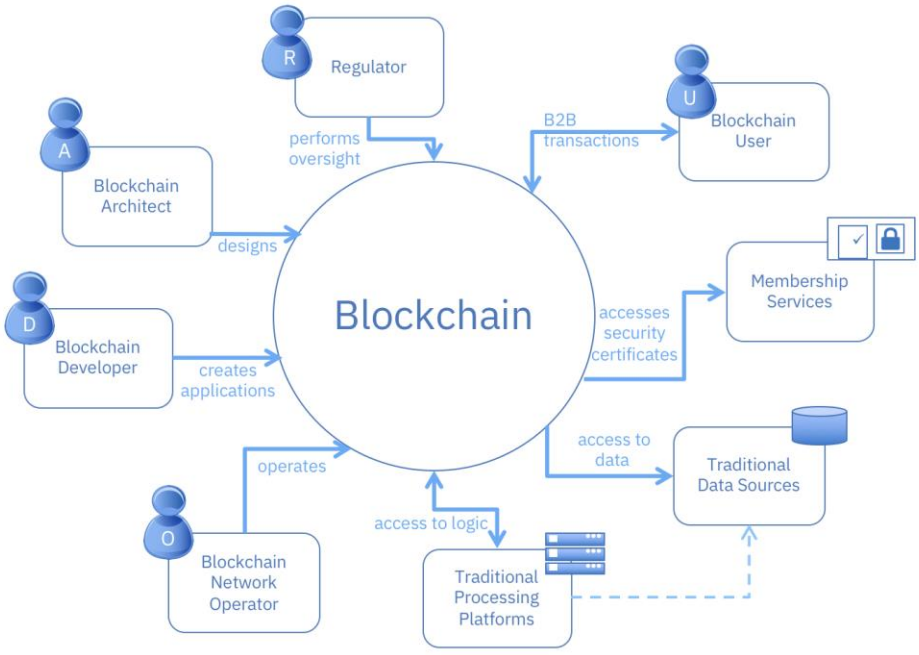


Figura No. 31 Actores que interactúan con Blockchain

(Gaur, et al., 2018)

2.1. Actores de la implementación de la cadena de bloques

En la prueba de concepto es una puesta en marcha minimalista, pero a su vez intenta ser lo más amplia o general para cubrir varios posibles escenarios donde se puede adaptar para su uso práctico como académico. Por tanto, se generan una lista de posibles usuarios “genéricos” los cuales para trabajos futuros deben ser detallados para saciar las necesidades de un cliente, organización o industria.

- Desarrollador del *Blockchain*
- Usuario del *Blockchain*
- Entes de aprobación de los bloques
- Médico/abogado u miembro de institución a la cual se pone en marcha el *Blockchain (*quien solicita la transacción para el Usuario*)*

Esto se debe a que estos actores no son críticos para la puesta en marcha y no son indispensables para el uso de *blockchain* si se recomienda se agreguen las interfaces relacionadas a estos usuarios a la puesta en marcha.

3. Tareas por realizar en la prueba de concepto:

La prueba de concepto debe realizar de forma satisfactoria tareas que permitan el uso de la tecnología de *blockchain* su uso para asegurar los datos que están tradicionalmente almacenados en bases de datos y en archivos.

Para lograr que esta condición se logre y mediante lo investigado en relación con la tecnología de cadenas de bloques, lo que se realiza es tomar los datos y agregarlos a una transacción en esta cadena.

4. Conceptos clave

- Los datos que se almacenarán en la cadena deberán ser Inmutables, esto significa que una vez que se almacenan a la estructura de la cadena no deben, ni pueden ser modificados.
- Toda transacción debe ser verificable mediante el uso de la tecnología de la cadena de bloques.
- Dado la naturaleza de la propuesta se busca el uso de un método de consenso que asegure el control sobre la cadena de bloques, además se busca una opción que pueda ofrecer confidencialidad de ser necesario. Y de acuerdo con (Gupta, 2018) una de las opciones es utilizando un método de consenso basado en Prueba de autoridad.
- Tiempo Epoch es una medida de tiempo relativa al 1 de enero de 1970. Y hasta la fecha. La cual es una medida utilizada para medir milisegundos.
- Firma de tiempo, la firma de tiempo es un método de confirmación por parte de una persona de confianza quien firma y garantiza que los datos provistos son íntegros y fueron firmados en un momento particular en el tiempo.

5. Cadena de bloques implementada en la prueba de concepto

En la implementación se crean las generalidades de la cadena de bloques, pero estos conceptos siguen siendo relativamente abstractos de forma que sea simple adaptar software existente y procesos actuales para que se puedan agregar o migrar a un "*blockchain"* que se base en la solución propuesta por la presente investigación, una bondad de la realización en este formato es lograr la adaptabilidad de la solución a múltiples ámbitos de aplicación como es el caso de administración de expedientes médicos, registros contables, registros de hacienda, registros sobre la propiedad. Más cabe destacar que en cada una de estas se deberá realizar una especificación sobre esta estructura abstracta para lograr mayor utilidad en cada uno de los escenarios.

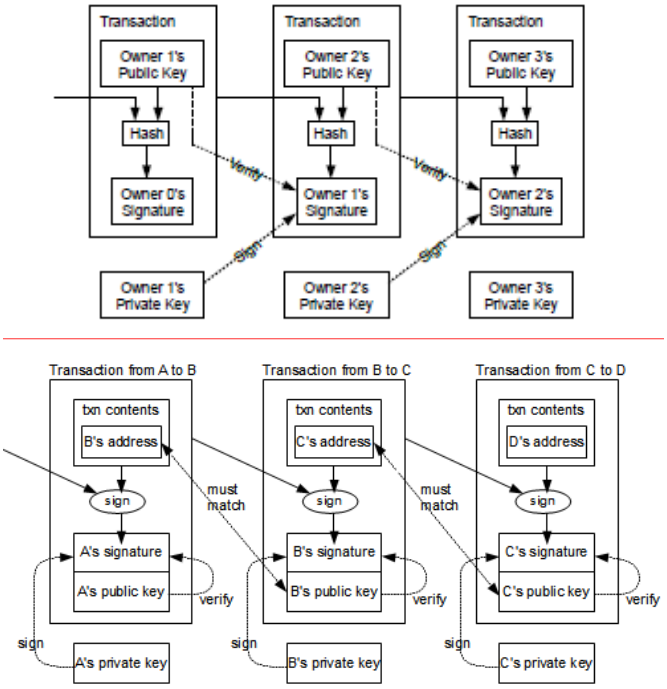


Figura No. 32 Estructura de transacciones (generalidad)

(Nakamoto, 2008) (Sherriff, 2014)

Por tanto, que debe ser el contenido de una Transacción en el bloque en una implementación abstracta.

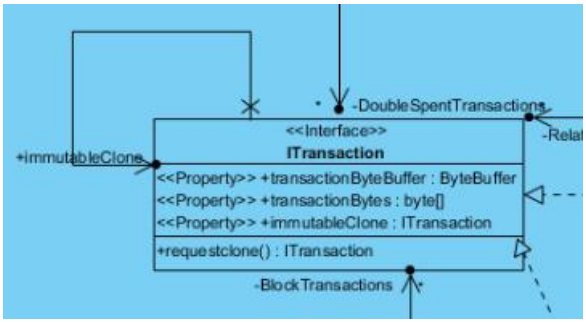


Figura No. 33 Diagrama de clase transacción de la puesta en marcha de Blockchain

Fuente: confección propia

En la representación anterior se muestra una interfaz la cual solo define 3 funciones

- Obtener bytes (aquellos que son o representan los datos que hacen única a la transacción) nótese que esta interfaz puede representar cualquier dato.
- Obtener los datos en una estructura inmutable (*byte buffer*)
- Clonar (donde se crea o solicita una copia (Inmutable) del objecto para uso y transporte en el sistema.

Para almacenar los datos en bloques la representación de los bloques es la siguiente:

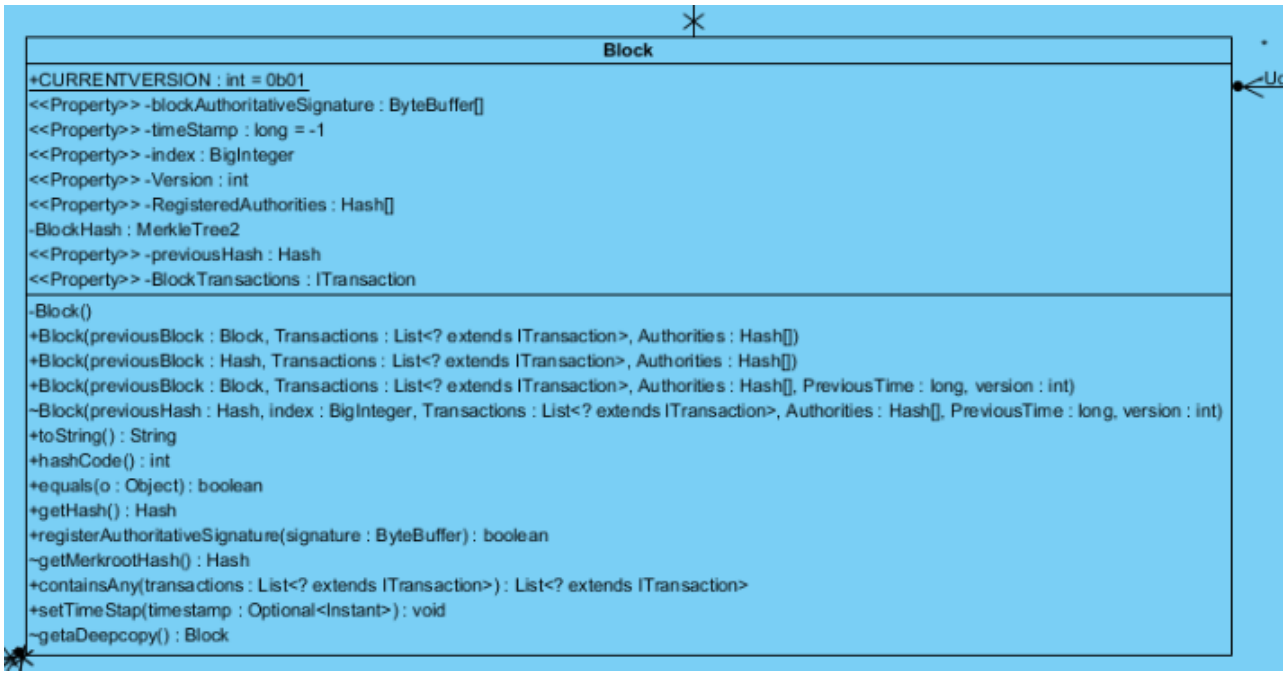


Figura No. 34 Diagrama de clase del bloque de Blockchain

Fuente: confección propia

Campo	Descripción
Hash del bloque (ID)	Identificador, único del bloque
Cabeceras (metadatos)	Índice de la cadena Autoridades firmantes registradas
Datos	El contenido particular del bloque árbol de Merkle
Hash Previo (id anterior)	Identificador, único del bloque anterior
Firma de tiempo	Timestamp [puede ser firma de tiempo o un Epoch]
<otros datos>	Firmas de los entes autorizadores.

Tabla 6 Representación del bloque en la propuesta

Fuente: confección propia

5.1. Árbol de Merkle

Durante la implementación de los árboles de *Merkle* se determina un problema entre la teoría y la práctica del uso de estos árboles, de acuerdo con Kozliner (Kozliner, 2017) estos árboles pueden ser implementados en formas que permitan árboles que no son "binarios", esto refiere a aquellos árboles en donde la cantidad de nodos no sean "*potencias de 2*" o expresado de forma matemática 2^X donde "*X"* indica la cantidad de niveles que el árbol posee, sin embargo esto aun no es claro, para aclarar esto de una forma más directa se puede expresar:

$$\mathrm{f(N)} = \log_2 N$$

Donde "*N"* es la cantidad de valores que el árbol debe almacenar y "*F(N)"* la potencia de 2 necesaria para almacenar esta cantidad de nodos.

El problema se suscita cuando "*F(N)"* no es un valor Entero y lo cual a su vez significa que la cantidad de nodos no son valores que ingresen perfectamente en un árbol binario

El problema suscitado en este caso es que el árbol no quedará en balance a menos que se agreguen elementos o eliminen elementos, pero para casos en donde la cantidad de nodos es alta

Por tanto, se expone este ejemplo:

100 nodos

$$\mathrm{f(100)} = \log_2 100$$

Es equivalente a 6.643856189774725

Por tanto, en 2^6= 64 y 2^7= 128

Por tanto, en un árbol perfecto de 6 niveles se pierden 32 posiciones y en un árbol perfecto de 7 niveles se desperdician 28 posiciones (las cuales por razones de seguridad se debe poblar, lo cual es posible, pero es información desperdiciada.)

¿Cómo resolverlo?

Existen dos formas de resolver el problema propuesto. Se puede tomar dos rumbos. De acuerdo con (Chapweske & Mohr, 2003) indican una forma de solucionar esto es mediante la “elevación” del nodo huérfano a un nivel siguiente de forma que este se utilice en el momento en que sea de conveniencia para el árbol ejemplo:

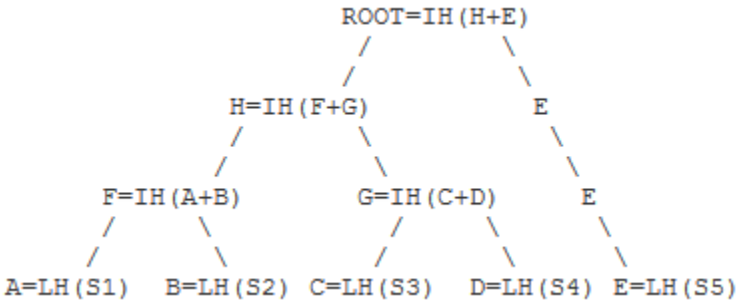


Figura No. 35 Árbol merkle con nodos no par

(Chapweske & Mohr, 2003)

Otro método el cual es utilizado por el *blockchain*: *bitcoin* es mediante el uso de duplicar el valor del nodo cuando en el nivel el valor no cumple con la regla de ser nodos pares.

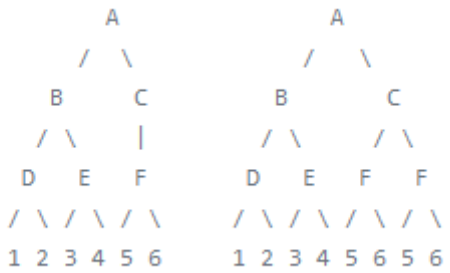


Figura No. 36 Árbol merkle con nodos no par aproximación de Bitcoin

(Bitcoin CodeBase, 2018)

En la puesta en marcha solucionado esto al limitar la cantidad de transacciones por cada bloque a un valor que sea potencia de 2. O dicho de otra forma que si raíz cuadrada sea un valor entero. Mayor o igual a dos. Esto para evitar posibles fraudes con transacciones que sean Muy similares o erróneamente duplicadas.

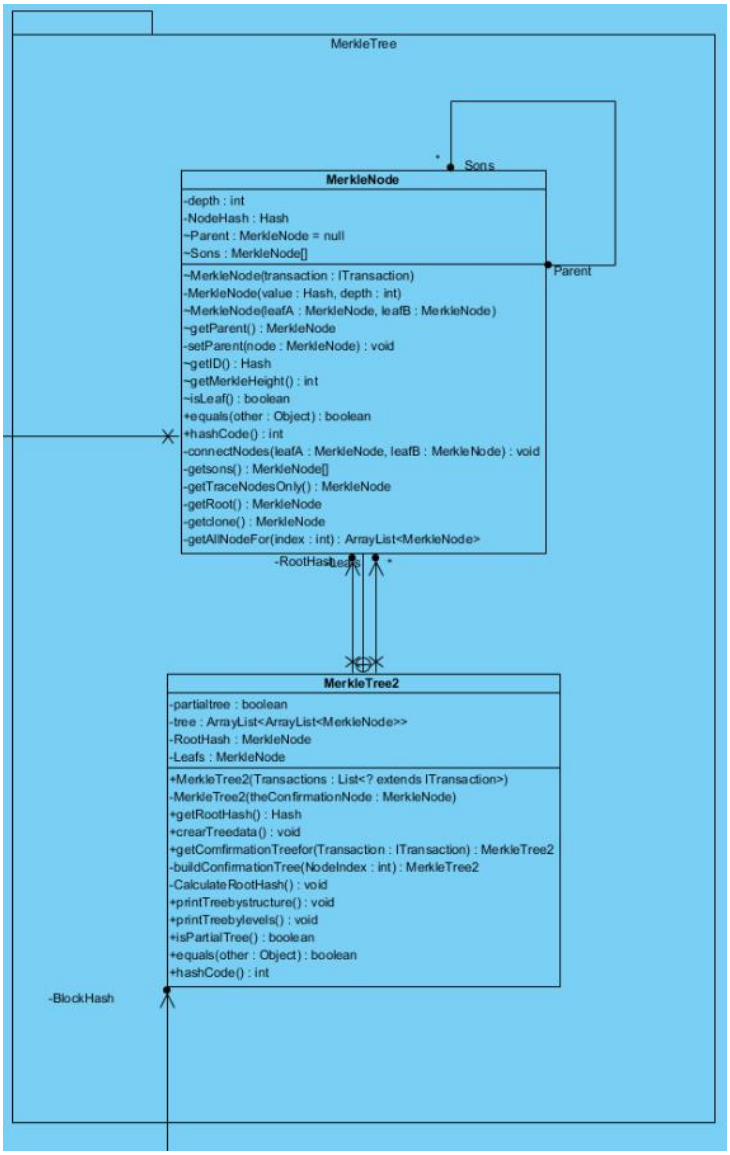


Figura No. 37 Diagrama de clases del árbol merkle y sus nodos

Fuente: confección propia

La cadena de bloques como tal es representada por una clase “blockchain” esta representará en tiempo de ejecución la estructura que mantiene y administra la cadena, en la prueba de concepto se mantiene limitada a tareas de agregar, verificar el concenso pero en una puesta en marcha para una solución integral esta deberá además tener las tareas asociadas a la persistencia y verificación de su consistencia en persistencia (guardado en disco, base de datos u otra tecnología) que sea congruente entre los nodos

5.2. Cadena de bloques

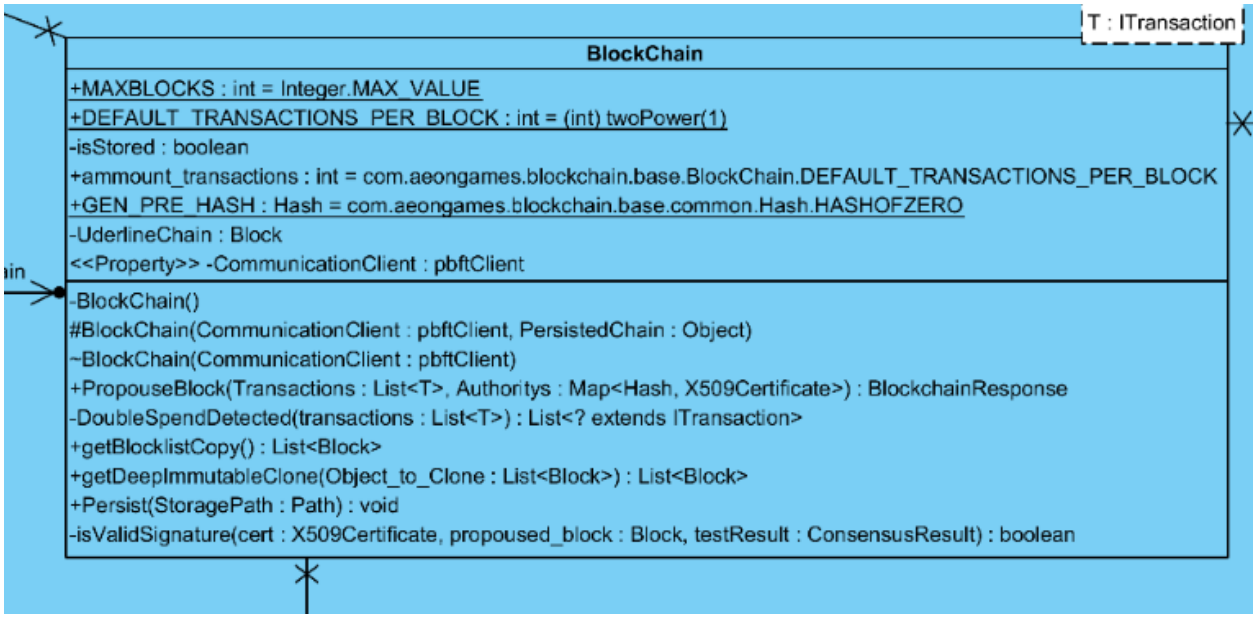


Figura No. 38 Diagrama de clases de la cadena de bloques

Fuente: confección propia

Dado las limitaciones intrínsecas en el lenguaje de programación la cadena de bloques está limitada a almacenar hasta el máximo permitido por los números enteros en Java que es equivalente a $MAX\_VALUE = 2^{31} - 1$

Cuando la cadena de bloques en la prueba de concepto llegue a este límite se puede encontrar un posible error, esta afirmación debe ser considerada por aquellos que deseen realizar mejoras sobre esta implementación. Para esta

prueba de concepto no se considera como una limitante, se sugiere una solución simple.

En tiempo de ejecución se deberá hacer una verificación de la cadena y mantener un valor indicando cuántos valores de la cadena están en memoria, y cuántos están persistentes en disco, bases de datos o inclusive otras estructuras de memoria. De esta forma la cadena de bloques puede poseer un “buffer” en memoria sobre el cual se trabaja, y otro bloque en el cual se encuentra en persistencia de esta forma se evita consumos excesivos de memoria por preservar la totalidad de la cadena.

A esto además hay que sumarle posibles medidas a tomar para asegurar que los datos sea provistos con la velocidad y tiempos de respuesta indicados. Esto sin embargo se encuentra fuera del alcance de la investigación

5.3. Piscina de transacciones

Durante la escritura de la solución se determinó que la mejor forma para llevar el control de las transacciones fue mediante la creación de una “*piscina de transacciones*” esta estructura almacenara las transacciones que aún no se almacenan en la cadena de bloques hasta que se dé una condición de procesar las transacciones que aún no han sido agregadas a la cadena de bloques.

Esta estructura está representada por la siguiente clase:

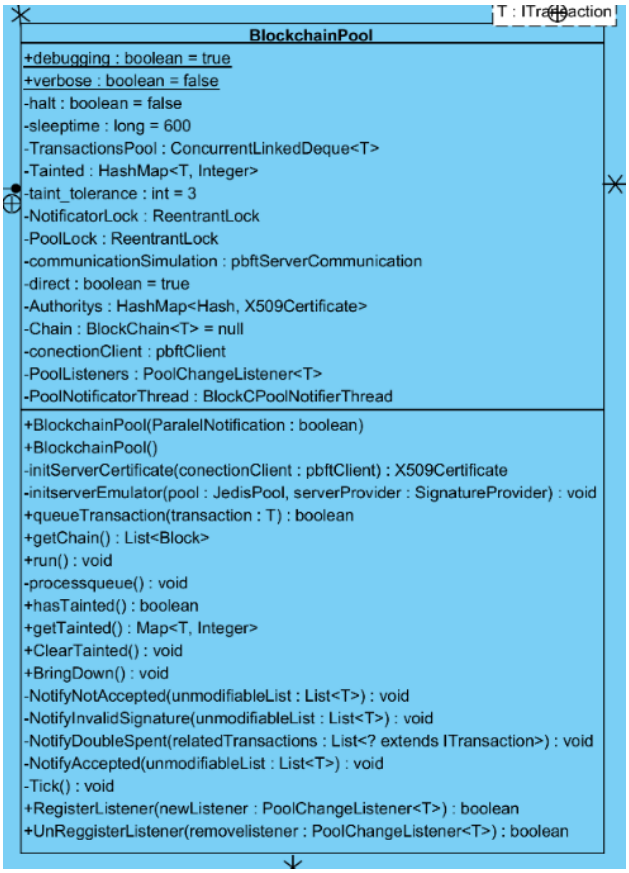


Figura No. 39 Diagrama de clases de la piscina de transacciones

Fuente: confección propia

Sin embargo, esta estructura, aunque encapsula el acceso no permite realizar las computaciones por otros, el crea su propio hilo de ejecución para llevar a cabo las transacciones de forma paralela y por tanto cuando este es llamado él posee su propio tiempo, aunado existe la opción de realizar o iniciar la ejecución de un hilo de ejecución adicional el que se encargue del procesamiento de las notificaciones de cambios en la cadena de bloques.

5.3.1. Consideraciones importantes en puesta en marcha

- en la puesta en marcha en un ambiente en producción o una aplicación real se debe considerar la necesidad de poseer un método en donde la piscina de transacciones sea distribuida o

pueda ser distribuida entre varios nodos de forma que se pueda verificar o hacer nuevos bloques sobre transacciones.

- Otra alternativa es que cada nodo sea responsable que asegurar que se dé una sincronización de las transacciones.

Ambas consideraciones u otras que se puedan dar quedan por fuera de los alcances de la puesta en marcha. En la prueba de concepto. Y por tanto no se contempla durante la creación de la prueba de concepto.

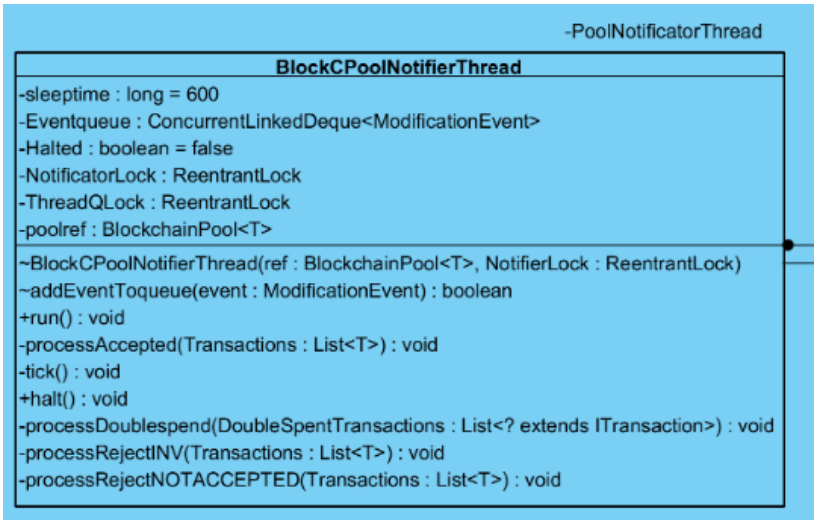


Figura No. 40 Diagrama de clases del hilo de notificación de transacciones

Fuente: confección propia

Para procesar las nuevas solicitudes en el "*blockchain*" se logra mediante la ejecución de una estructura cuyas responsabilidades son la de procesar las transacciones hacia la cadena, una vez que se detecten que hay suficientes transacciones para satisfacer la cantidad que se pueden ingresar por cada bloque.

En la prueba de concepto se ha tomado la decisión de permitir el ingreso de dos transacciones por cada bloque en el Árbol de "*Merkle"* y de esta forma lograr realizar una demostración de forma rápida y que sea congruente con las necesidades de seguridad para evitar la posible vulnerabilidad encontrada con anterioridad, pero si fuera necesario se puede utilizar otras cantidades de transacciones.

5.4. Expedientes

Sobre los expedientes como tal, se definen de una forma abstracta para lograr de esta manera se pueda adaptar la definición de “expediente” en la cadena de bloques de forma tener una versión más específica o abstracta, con mayor o menor cantidad de atributos en la puesta en marcha.

Por tanto, en los expedientes se definen las siguientes clases:

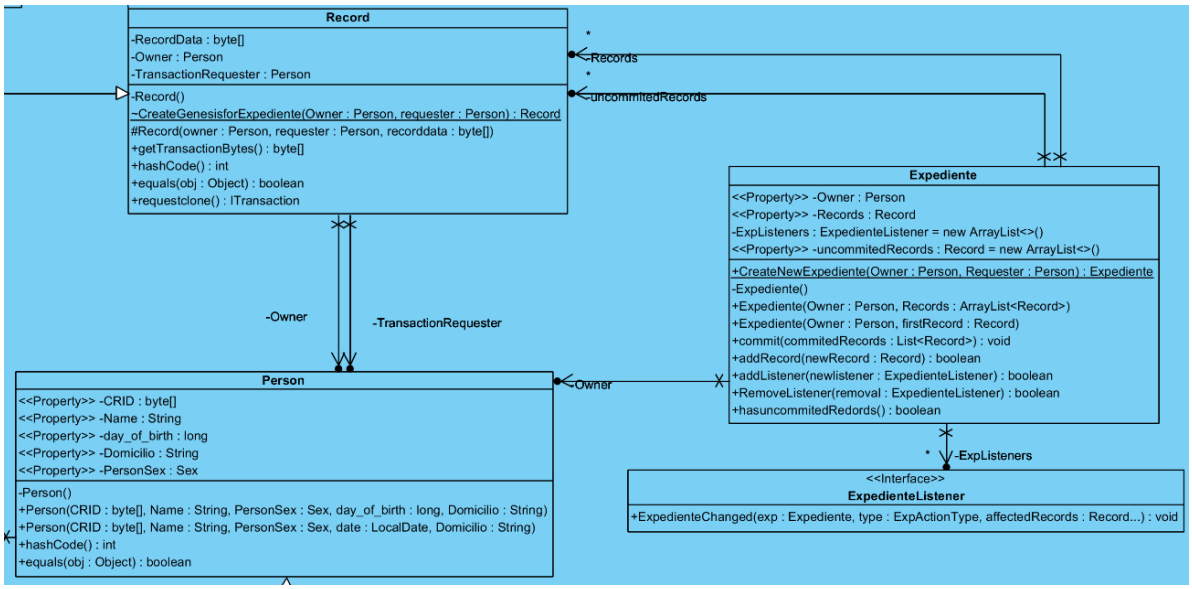


Figura No. 41 Clases Base de expediente(s)

Fuente: confección propia

Como se ilustra en la figura demuestra las clases principales de “objectos” que son almacenados y utilizados en la cadena de bloques. Estos elementos son:

- Expediente:

  el expediente cuenta con:

  - un dueño (la persona dueña o afectado directo del expediente)
  - Una cadena o lista de elementos relacionados al expediente, se realiza la analogía de que estos son páginas de un libro o un folder. Donde dicho folder es el expediente.
- “*record*” o registro. Para nuestros propósitos se puede definir cómo una “hoja” de expediente. Estos son para nuestros propósitos Transacciones, cada cambio a un expediente se registra como un “*record*” que se guarda

en una estructura “tradicional” (el expediente) pero a su vez se registra y se mantiene registrado su integridad y trazabilidad de cuándo, quién o quiénes crearon el registro. En la cadena de bloques mediante el uso del “*record*” como transacción.

  - Los datos del “*record*” (datos binarios expresados en bytes)
  - El dueño o persona afectada directamente por esta hoja en el expediente o transacción.
  - Solicitante. La persona asociada a la creación de la transacción por ejemplo El médico, abogado, dependiente, etc.

- Persona.

  la persona es una estructura auto explicativa. Es una representación de la información de un ciudadano. Y posee los atributos:

  - CRID, la cédula de identidad.
  - Nombre
  - Fecha de nacimiento
  - Domicilio
  - Sexo.

5.5. Metodología de consenso.

Uno de los grandes retos del desarrollo de la puesta en marcha fue realizar la implementación de un método de consenso. Puesto fuera de la prueba de trabajo (*Proof-of-Work*) la bibliografía es menor y más escasa que los documentos cuyo tema sean el método más utilizado (*Proof-of-Work*) sin embargo como demuestran (Rosic, 2018), (De Angelis, 2018), (PEASE, R, & LAMPORT, 1987), existen otros métodos. Después de analizar los diferentes modelos y revisar posibles implementaciones. Se toma la decisión de implementar “Tolerancia práctica a fallos bizantino” (“*Practical Byzantine Fault Tolerance*”), este método refinado por (Castro & Liskov, 1999) indica una solución al problema los generales bizantinos

5.5.1. El problema de los generales bizantinos

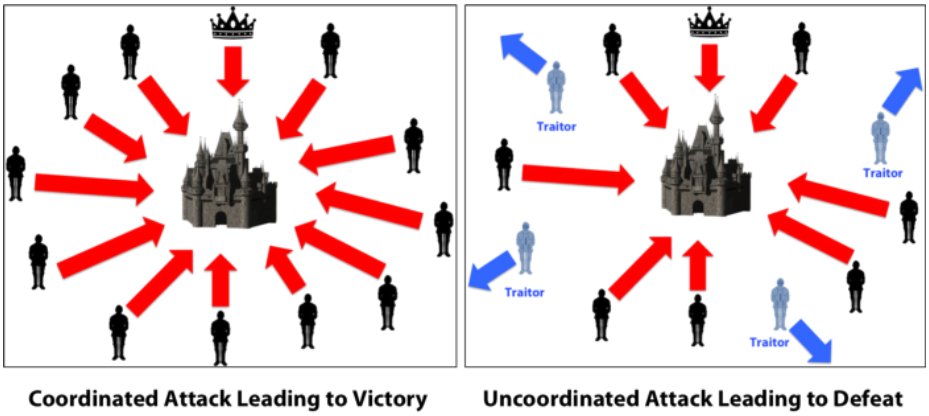


Figura No. 42 Problema de los generales bizantinos

Ataque coordinado lleva a la victoria // ataque desordenado lleva a la derrota (traducción libre)

(Ghosh, 2016)

Se plantea un problema en donde se tienen un ejército que rodea un castillo el ejército posee varios grupos esperando las órdenes de sus generales, los generales no pueden dar señales visuales o auditivas puesto esto generaría detección por parte del enemigo en el castillo. Por tanto, para poder llegar a consenso de atar o retirase se debe hacer mediante mensajes. Esto genera varias preocupaciones:

- Si se envía a un mensajero, pero este puede ser capturado y enviar un mensaje incorrecto
- Uno de los generales puede ser un traidor y enviar un mensaje incorrecto o enviar un mensaje y realizar una acción diferente.

5.5.2. Solución al problema de los generales

Mediante el uso de la solución presentada por (Castro & Liskov, 1999) indica una solución la cual funciona mediante la tolerancia a una cantidad determinada de fallos, en este caso la tolerancia a

fallos se determina mediante el cálculo de la totalidad de réplicas ($\mathcal{R}$) requeridas para tolerar un fallo en(f) nodos mediante el cálculo:

$$\mathcal{R} = 3f + 1$$

Figura No. 43 Ecuación de réplicas necesarias

(Castro & Liskov, 1999)

Por tanto, si se desea tolerar un máximo de 1 fallo se requiere un mínimo de 4 nodos. (1/4) si se desea realizar el cálculo inverso (saber cuál es la tolerancia con ($\mathcal{R}$) cantidad de servidores se realiza mediante la ecuación:

$$f = \frac{R - 1}{3}$$

Figura No. 44 Ecuación para el cálculo de toleración dado R nodos

(Castro & Liskov, 1999)

Esta solución se puede expresar de forma gráfica de la siguiente manera:

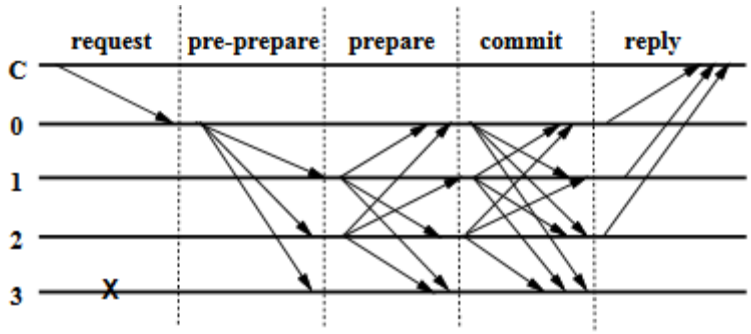


Figura No. 45 Caso normal de operación en PBFT

(Castro & Liskov, 1999)

Además, esta propuesta define estados en los cuales se ingresan a estados de comunicación los cuales son:

- Solicitud (“request”)
- Pre- Preparación (“pre-prepare”)
- Preparación (“prepare”)
- Perpetrar o persistir (“commit”)
- Respuesta (“reply”)

Estos 5 estados son los necesarios para el envío y recepción de la respuesta. Esta propuesta fue concebida como una solución a problemas de transmisión y replica de sistemas en red al utilizar el sistema NFS, pero en la actualidad se puede ver utilizado en equipos tales como en aviones Boeing como en los sistemas de cohetes reciclables (Space-X Dragon Flight Control System.) (Montresor, 2018)

Por tanto, para la solución de la puesta en marcha se aplica Tolerancia práctica a fallos bizantino. Para lograr realizar una implementación de manera exitosa se realizó una búsqueda de código ya disponible en el mercado que cumpliera con los requisitos para agilizar la realización del proyecto. Por tanto, en el proyecto se realizó adopta y se analizó a profundidad el código escrito por Johnny Cao. (Cao, 2019), la razón para optar por esta versión de una implementación de PBFT es

dado lo simple del código. Este código relativamente simple de comprender y utilizar.

Como beneficio adicional en el ejemplo que demuestra Johnny indica el cómo utilizar un API que permitirá y facilitará la comunicación entre nodos sin realizar esta tarea directamente mediante aplicación escrita desde cero.

En esta implementación se designan los pasos por seguir para implementar los pasos de la comunicación y aceptación de la solución al problema de los generales bizantinos.

Pero esta librería debe adaptarse ligeramente para la aplicación en la cadena de bloques que se implementa como prueba de concepto por tanto se genera el siguiente paquete y clases:

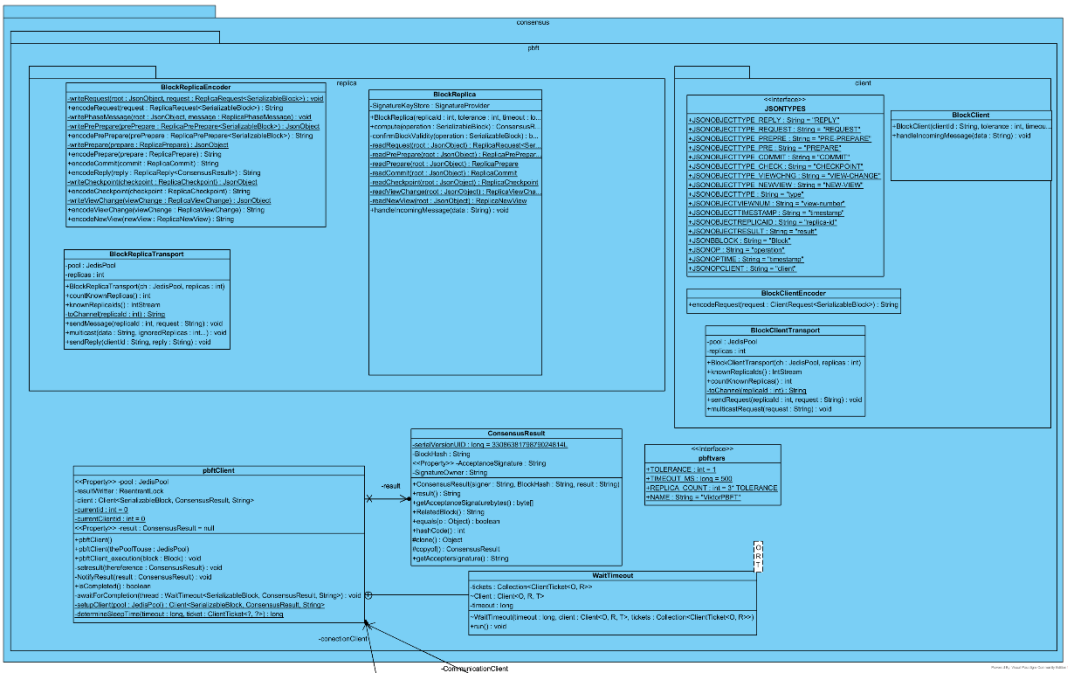


Figura No. 46 Paquete implementación PBFT (propias)

Fuente: confección propia

Estas clases son necesarias para lograr la comunicación entre nodos de “aprobación” para la prueba de autoridad. Sin embargo, la raíz y clases bases de la comunicación para la Tolerancia practica a fallos bizantino necesitan pocos cambios para ser adaptados al proyecto.

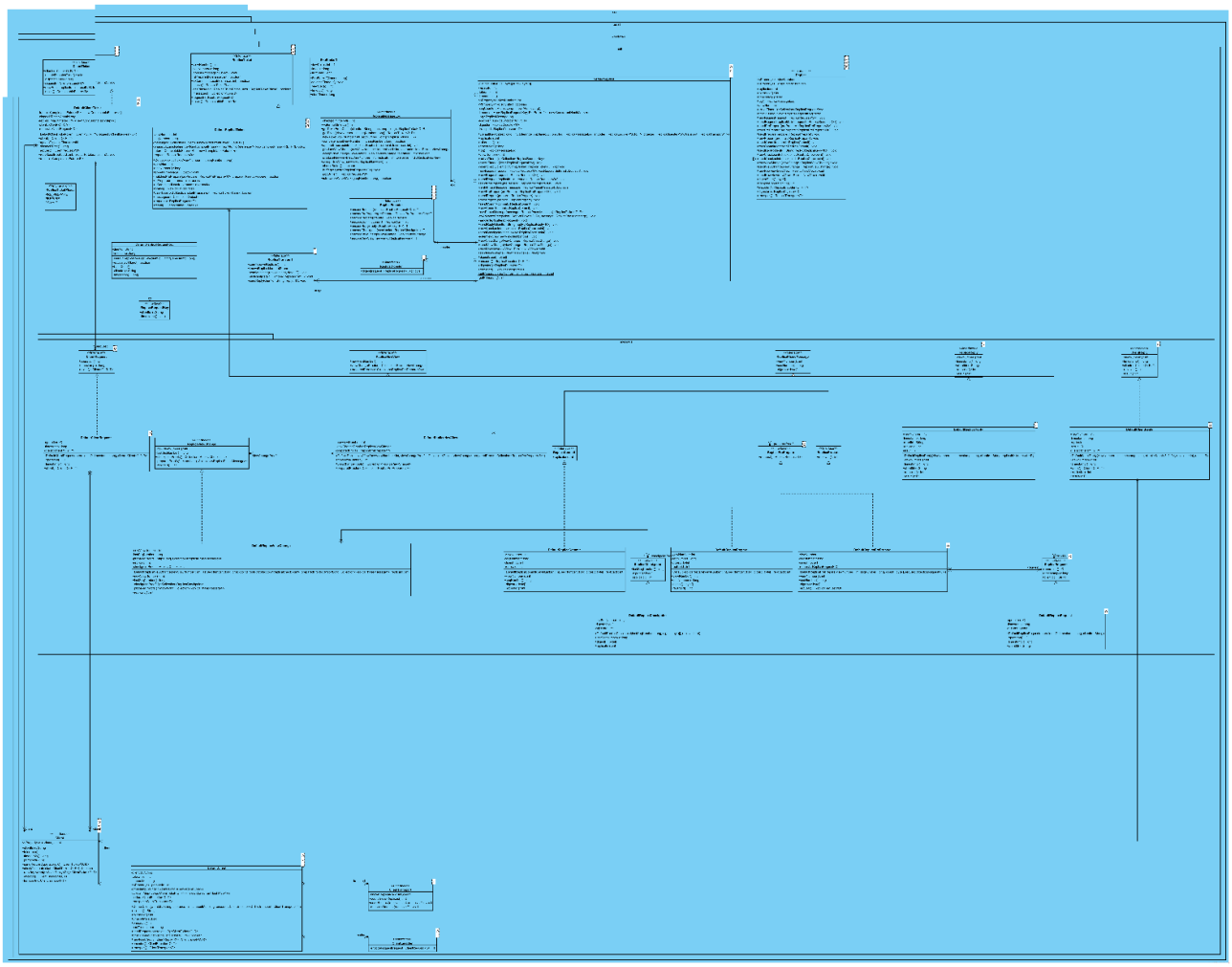


Figura No. 47 Librería de PBFT (externa)

(Cao, 2019)

Las clases definidas para el consenso además requieren el uso de un método de comunicación entre los nodos que puede o no estar en diferentes servidores. En la puesta en marcha de la prueba de concepto por tanto se opta por la selección del sistema de datos "*Redis*", Redis es una estructura de datos localizada en Memoria, que es utilizada como "*corredor de datos*" soporta estructuras como texto, sets, listas etc.

Figura No. 48 Logo de Redis

(redis, 2019)

La razón de selección se basa en dos factores, por un lado, es simple de utilizar, por otro esta solución ya es utilizada en el mercado para soluciones de cadena de bloques. Y finalmente dado a que se poseen librerías simples, fáciles de adaptar y utilizar en el lenguaje de programación de elección de la prueba de concepto. La librería especifica llamada "*jedis*" (Leibiusky, 2019)

Aunque ante la expansión de una puesta en marcha existe la posibilidad de migrar esta solución a otro sistema como puede ser el caso de *Apache Kafta.*

5.6. Herramientas Criptográficas: Certificados, *SmartCards* y firmas digitales

Para el desarrollo de la puesta en marcha de la cadena de bloques es necesario el uso de algoritmos criptográficos, desde los métodos para calcular los Hash, la comunicación entre los nodos, el uso de Smart Cards (firma digital), entre otros.

Temporalmente para la puesta en marcha de la prueba de concepto, las comunicaciones no implican que estén cifradas. Esto debido a que estas medidas no son necesarias temporalmente. Inclusive es mejor para el análisis y estudio de posibles problemas. Por tanto, queda fuera de los alcances del proyecto asegurar la comunicación entre los nodos. Sin embargo, esto es simple de realizar mediante la librería de Redis. Donde se puede configurar un certificado de SSL/TLS.

Para la generación de los valores Hash se utiliza el Algoritmo de Hashing SHA-256 este algoritmo de Hashing es el estándar para el uso de firmas y comunicaciones seguras en internet, aunque se está pasando de este método hacia SHA-3, SHA-256 es a la fecha suficientemente seguro y confiable para los propósitos de este proyecto.

La fórmula de SHA-256 en pseudo código puede ser expresada de la siguiente forma:

SHA-256(M):
(* Let M be the message to be hashed *)
for each 512-bit block B in M **do**
$W = f_{exp}(B)$;
(* Initialize the registers with the constants. *)
$a = H_0$; $b = H_1$; $c = H_2$; $d = H_3$; $e = H_4$; $f = H_5$; $g = H_6$; $h = H_7$;
for $i = 0$ **to** 63 **do**
(* Apply the 64 rounds of mixing. *)
$T_1 = h + \Sigma_1(e) + f_{if}(e, f, g) + K_i + W_i$;
$T_2 = \Sigma_0(a) + f_{maj}(a, b, c)$;
$h = g$; $g = f$; $f = e$; $e = d + T_1$; $d = c$; $c = b$; $b = a$; $a = T_1 + T_2$;
(* After all the rounds, save the values in preparation of the next data block. *)
$H_0 = a + H_0$; $H_1 = b + H_1$; $H_2 = c + H_2$; $H_3 = d + H_3$;
$H_4 = e + H_4$; $H_5 = e + H_5$; $H_6 = e + H_6$; $H_7 = e + H_7$;
(* After all 512-bit blocks have been processed, return the hash. *)
return concat(H_0, H_1, H_2, H_3, H_4, H_5, H_6, H_7);

Figura No. 49 Pseudo código para el cálculo de Hash

(Penard & van Werkhoven, 2014)

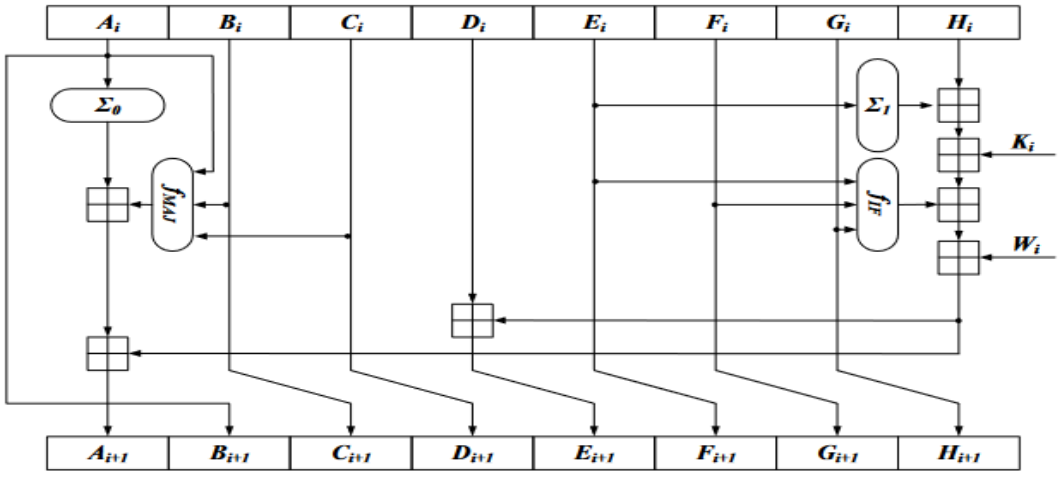


Figura No. 50 Diagrama del algoritmo SHA-256 Hash

(Penard & van Werkhoven, 2014)

Para los propósitos prácticos de la implementación no es necesario el conocimiento profundo o ampliación de la formula, dado a que Java posee una robusta librería de algoritmos criptográficos llamada "*Java Cryptography Architecture*" (Oracle, 2018) el cual permite además de utilizar algoritmos

criptográficos definidos en Java. Logrando mayor simplicidad de las actualizaciones en librerías criptográficas ya sea aquellas disponibles por defecto o librerías extra, como, por ejemplo: "*Bouncy Castle"* (the Legion of the Bouncy Castle, 2019)

Con respecto a certificados digitales. estos son utilizados para aplicar el sistema de consenso. Dado a que el sistema no hace minería de hash, puesto esta tarea no es necesaria para la creación de bloques, sino que es por medio de una autoridad, para demostrar autoría, además de la demostración, se realiza para asegurar la integridad de los datos que fueron firmados. Por tanto, la autoridad utiliza el certificado para brindar no repudio e integridad (cada bloque puede ser confirmado mediante el uso de la llave pública).

Además de utilizar los certificados para firmar los bloques propuestos, se puede utilizar los certificados en "*SmartCards"* "*Athena"*, las cuales son homologadas por el Banco Central de Costa Rica para el uso de la firma digital (Banco Central de Costa Rica, 2019) u otras las cuales se pueden almacenar Certificados Digitales.

En *Java* existe una particularidad con respecto a las "*SmartCards"*. Esto consiste en un proveedor de seguridad especial el cual carga los controladores de los lectores y tarjetas como tal y utilizan sus algoritmos internos para firmar los datos al utilizar las llaves contenidas en las tarjetas tales como la de la firma digital. El proveedor específico para el uso de la firma digital es *"SunPKCS11"* sin embargo la dificultad del uso de este método para la firma, autenticación y otros, es que no es simple configurar el controlador asociado con la firma digital.

Los certificados digitales y firmas son utilizados para firmar los datos, tanto desde la perspectiva de la autoridad sino además desde los actores para brindar una garantía de no repudio ante una posible auditoría o revisión de las transacciones.

6. Arquitectura tecnológica

6.1. Diseño de la red

En la implementación de la prueba de concepto no se contempla la realización de una red distribuida en múltiples servidores. Sin embargo, dado a los beneficios de la tecnología adaptar el sistema para que se distribuya entre múltiples servidores es relativamente simple y esperado en una red en producción y crecimiento.

Por otro lado, en la propuesta del diseño ante una solución realista de una red distribuida se puede realizar de múltiples maneras sin embargo se sugiere para la implantación del ambiente se formalice de una forma similar al siguiente diagrama:

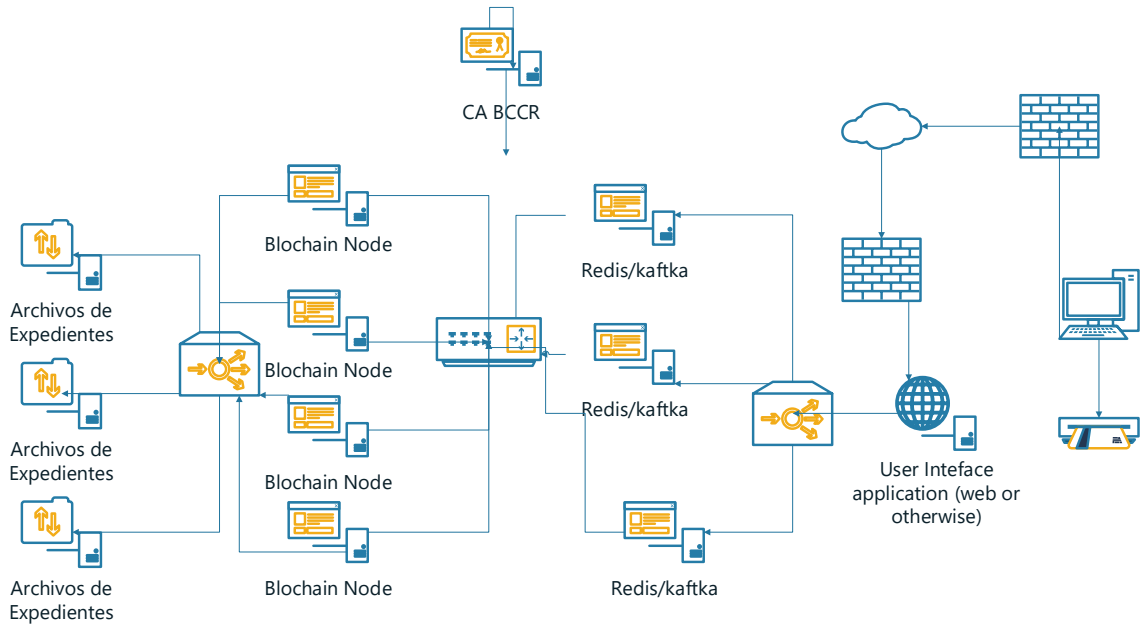


Figura No. 51 Diseño abstracto de una propuesta para la cadena de bloques

Fuente: confección propia

6.2. Diseño de los Servidores

Se destaca que las especificaciones del hardware pueden no ser las ideales para una implementación en producción. La prueba de concepto se ejecuta en un sistema virtualizado con las siguientes características “virtuales”:

Procesador(es): 3 núcleos de ejecución (basado en una computadora Real AMD FX – 8350 de 8 núcleos @ 4.01 GHz)
Memoria RAM Virtual: 8192 MB
Aceleración: Activa (AMD-V)
Aceleración video: No, el servidor no requiere o utiliza Interfaz de usuario
OS: Windows 7 64 bits
Dispositivo de red: Modo *Bridge*

Tabla 7 Características del servidor virtual

Dadas las características del ambiente de desarrollo, la solución es agnóstica del servidor de su puesta en marcha. Por lo que la especificación del sistema operativo no es de alta relevancia. Más es de destacar que durante el desarrollo de la solución se opta por realizar las pruebas y ejecuciones en un ambiente que ejecuta Windows 7 de 64 bits. Un ambiente por demás un tanto obsoleto.

Para la implementación tiene la capacidad de ejecutar en un ambiente de Servidores con el Sistema Operativo Linux, Unix, solaris

7. Especificaciones de la puesta en marcha.

La prueba de concepto posee ciertas particularidades que no se encuentran en soluciones como *Bitcoin* pues la puesta en marcha no posee un sistema de *“Proof-of-Work”* sino que utiliza un sistema de “Proof-of-Authority”. De esta forma no es necesario que los nodos de la Cadena de bloques realicen una tarea computacionalmente intensiva de “minar” hash, sino que los valores son computados en el momento en que son solicitados y se realiza una “firma” del bloque el cual es después asignado a la cadena. Esto puede ser reflejado en el diagrama de secuencia ver. Figura No. 52 .

En el diagrama de secuencia tenemos una demostración generalizada de cómo la prueba de concepto realizará la transmisión y puesta en marcha de la cadena de bloques, sin embargo, esto es desde una perspectiva técnica.

Para la puesta en marcha en el ejemplo de un expediente médico se tiene un diagrama que sería más extenso, por tanto, se obviará la parte de consenso y se mostrará desde una puesta en marcha que toma en consideración mostrar la perspectiva de una puesta en marcha integral que a su vez requiere una transición de un sistema tradicional. Ver Figura No. 53

Finalmente, una de las particularidades del sistema, es el uso de algoritmos de firma digital, para asegurar consistencia entre los métodos que se pueden con el uso de firma digital y el uso de certificados particulares para la firma de datos, se debe utilizar métodos soportados en ambos ambientes (tanto en las computadoras como en los *smartcard*) para tener congruencia en el cómo se firman los datos en la cadena. En este caso se tomó como base el uso del algoritmo "*SHA256withRSA*" el cual es utilizado en la firma digital y también se utiliza para las firmas de las autoridades.

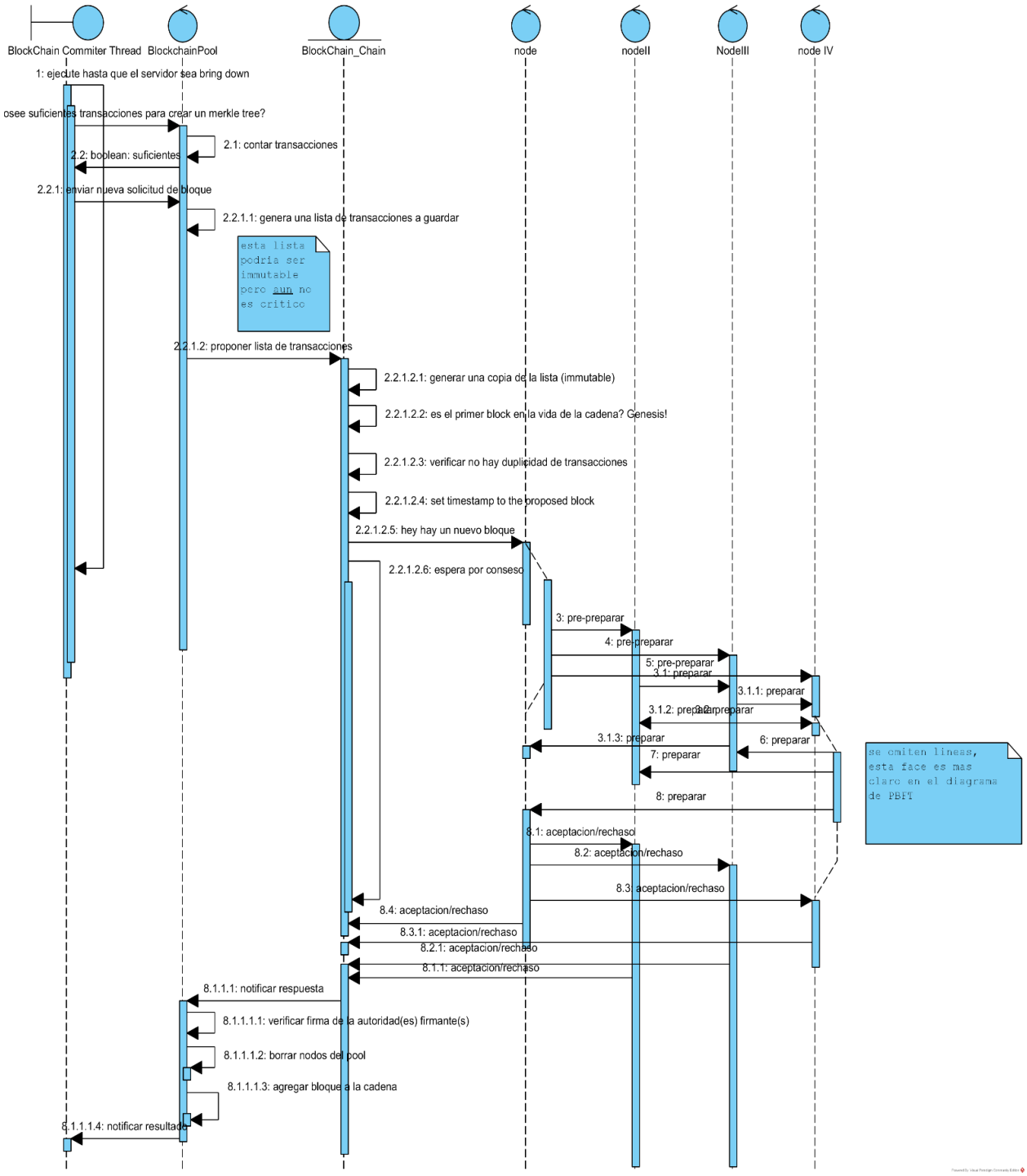


Figura No. 52 Diagrama de Secuencia generación de bloque

Fuente: confección propia

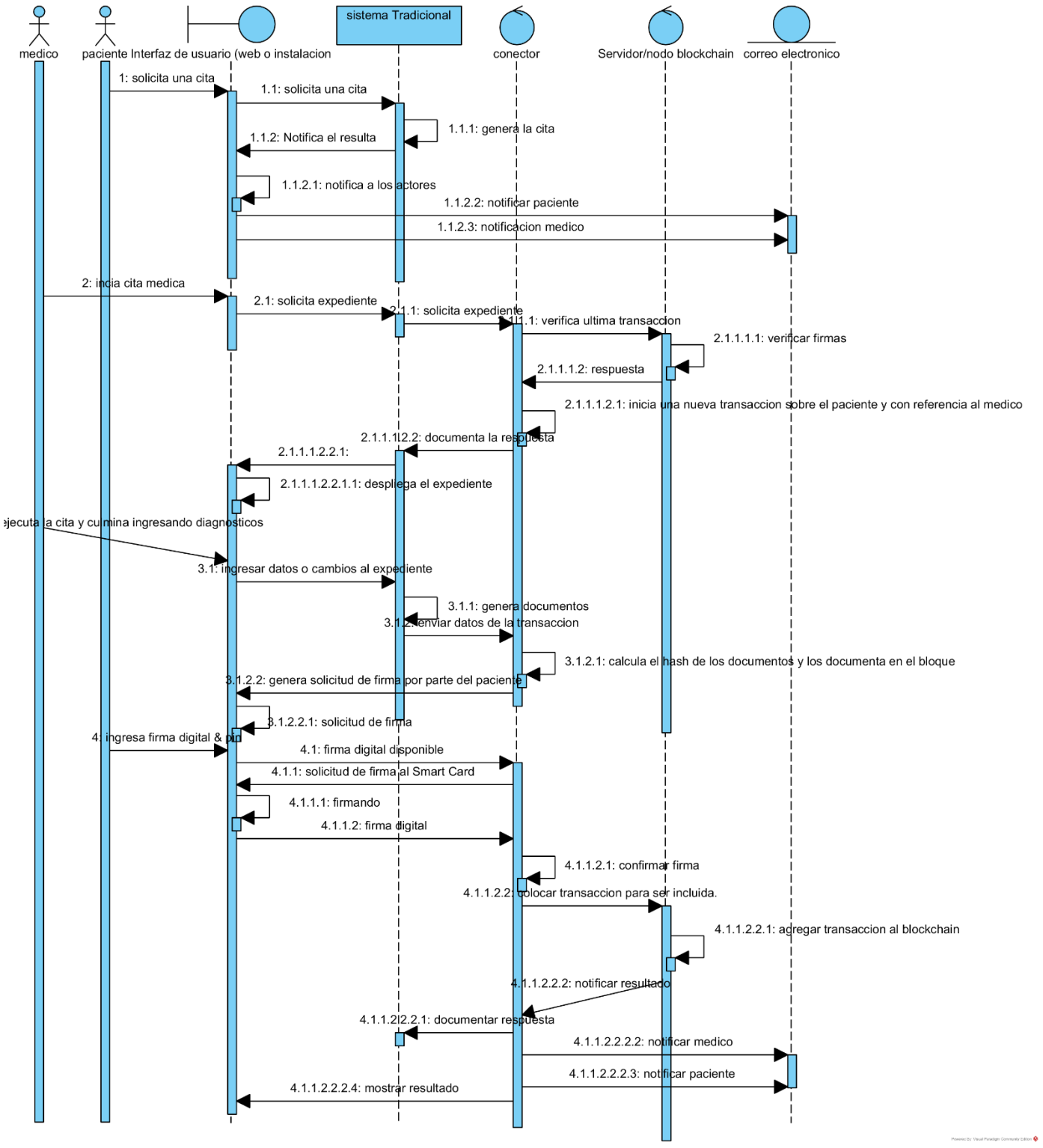


Figura No. 53 Diagrama de secuencia ingreso de archivos médicos

Fuente: confección propia

8. Demostración de la prueba de concepto

Una vez concluida la fase de prototipado y desarrollo, se logra los objetivos de la tecnología investigada, el cual se bautiza como "*Viktor BlockChain*".

El proyecto utiliza una estructura de archivos y carpetas que debe respetar dado al lenguaje de programación "*Java*" lo requiere para que el código ejecute de forma correcta. Esta estructura puede se visualiza en la Tabla 9: Estructura de carpetas del proyecto programado.

Inicialmente el código posee código para la realización de pruebas sobre ciertos elementos. También conocido como "pruebas unitarias". En un ambiente integrado de desarrollo se pueden ejecutar estas pruebas.

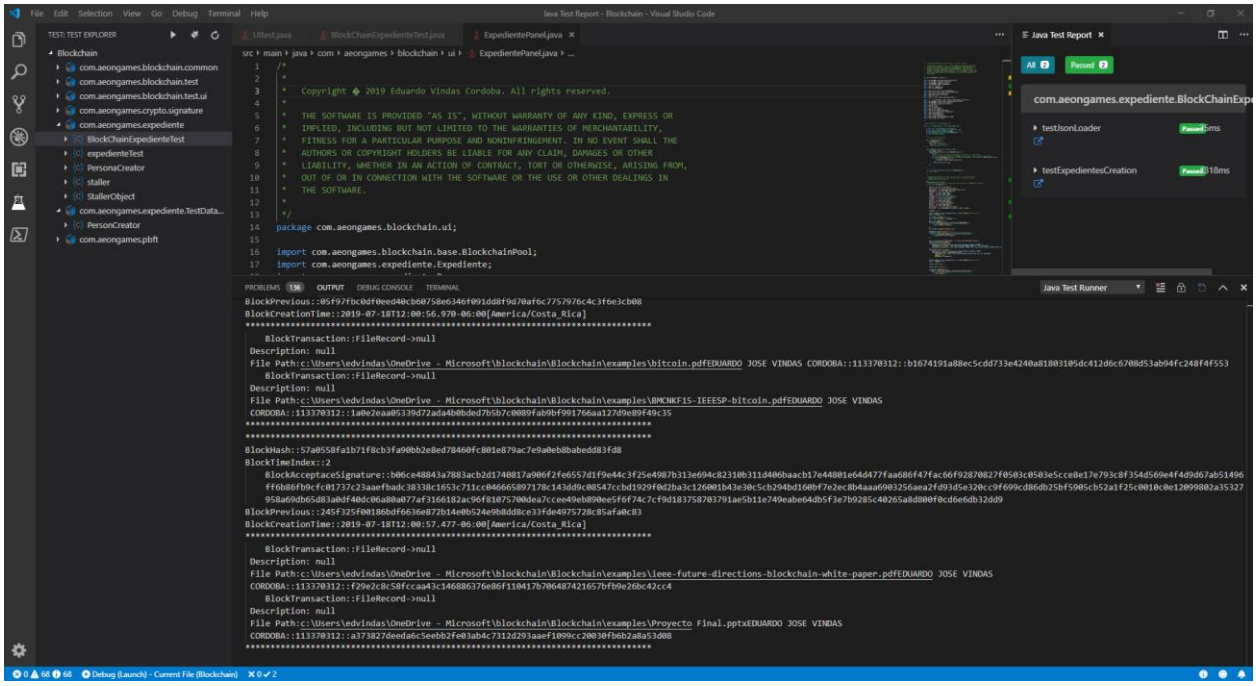


Figura No. 54 Captura de pantalla de prueba unitaria

Fuente: confección propia ejecutando *Microsoft VS Code*

En el proyecto se desarrollaron pruebas unitarias para realizar pruebas de integridad en los componentes:

- Metodología de consenso (Tolerancia practica a fallos bizantino)

- Creación y persistencia de información de personas
- Prueba de Expediente
- Prueba de la cadena de bloques con expedientes
- Prueba con datos aleatorios en la cadena de bloques
- Prueba de árboles de merkle
- Pruebas de “Hashing”
- Pruebas de uso de firma digital
- Pruebas de interfaz de usuario

Para de demostración de la cadena de bloques se desarrolló una aplicación la cual de la mano del código de la cadena se utiliza para la representación gráfica de los datos en la cadena.

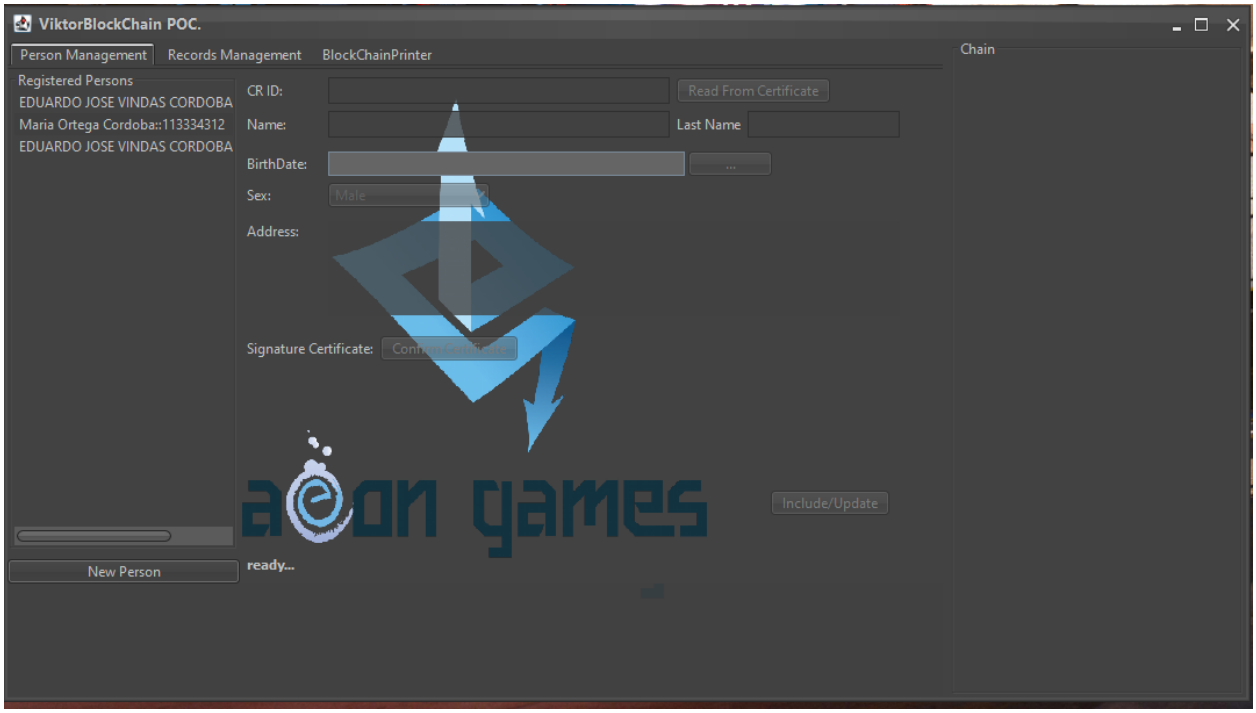


Figura No. 55 Captura de pantalla de la aplicación gráfica

Fuente: confección propia

Para la ejecución de la aplicación es necesario el uso de información de personas, y para evitar la duplicidad de acciones y lograr hacer demostraciones

de forma rápida se almacena una lista de datos de personas, en un archivo. Además, la aplicación cuenta con la opción y elementos para administrar los datos de personas.

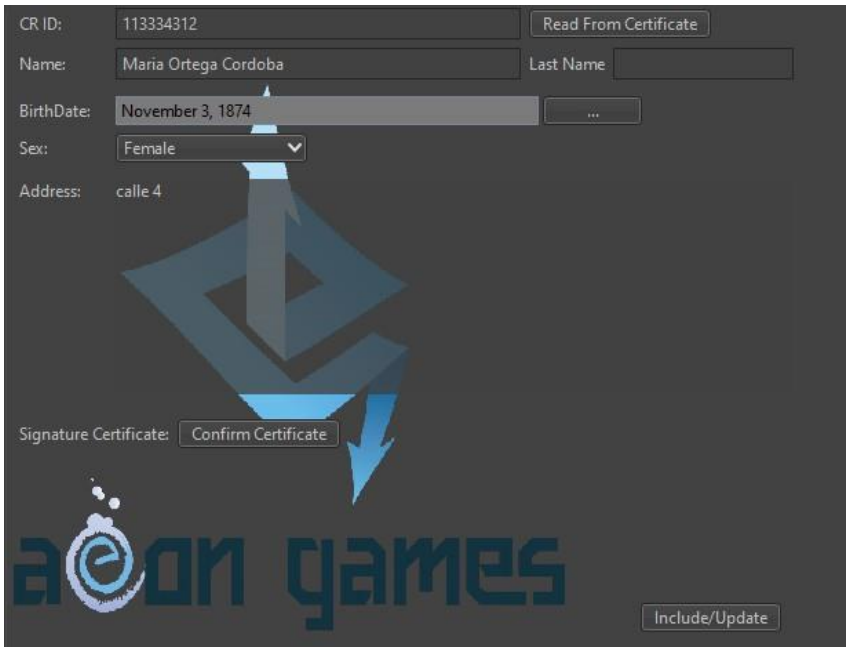


Figura No. 56 Captura de pantalla de administración de usuarios

Fuente: confección propia

La aplicación cuenta con la opción de soporte de la firma digital costarricense. Con la cual se puede utilizar para verificar la autoría y no repudio de las transacciones. Para ello contamos con la opción de leer los datos desde el certificado y también “verificar certificado” el cual permite confirmar que se pueda firmar datos con el certificado.

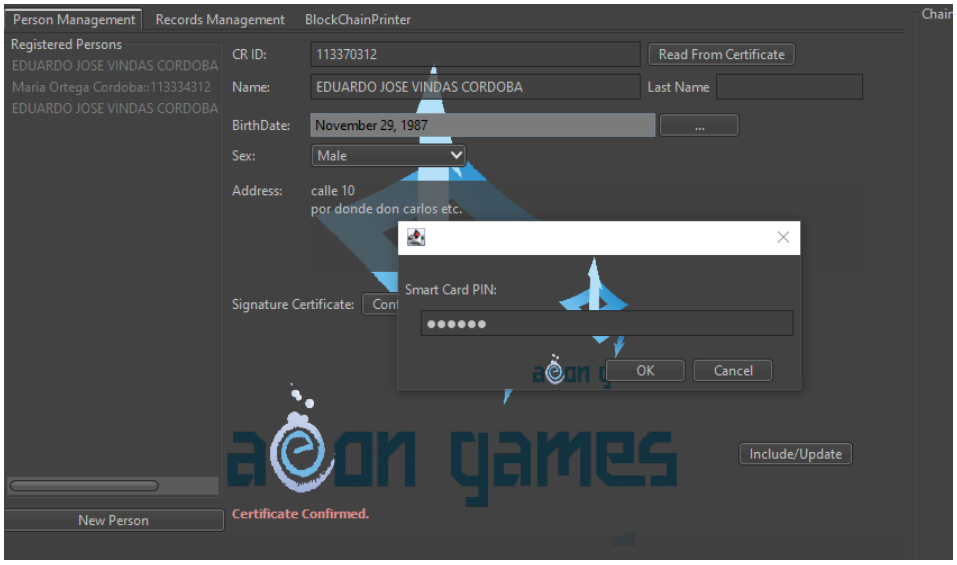


Figura No. 57 Captura de pantalla de confirmación de certificado

Fuente: confección propia

Para la administración y procesamiento de transacciones hacia los expedientes debe se seleccionar la pestaña de “Records Management”.

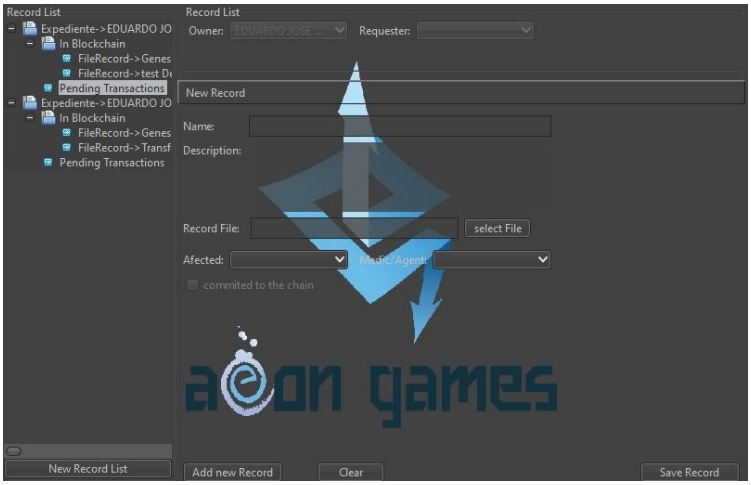


Figura No. 58 Captura de pantalla de administración de expedientes

Fuente: confección propia

En “Records Management” se puede realizar la inclusión, y visualización de transacciones a la cadena de bloques o ver el estado de las transacciones

actuales ya existentes. Para la inclusión de transacciones es posible utilizar la firma digital para firmar las transacciones, sin embargo, por limitaciones de la versión actual solo realiza la firma y no la confirmación en el bloque.

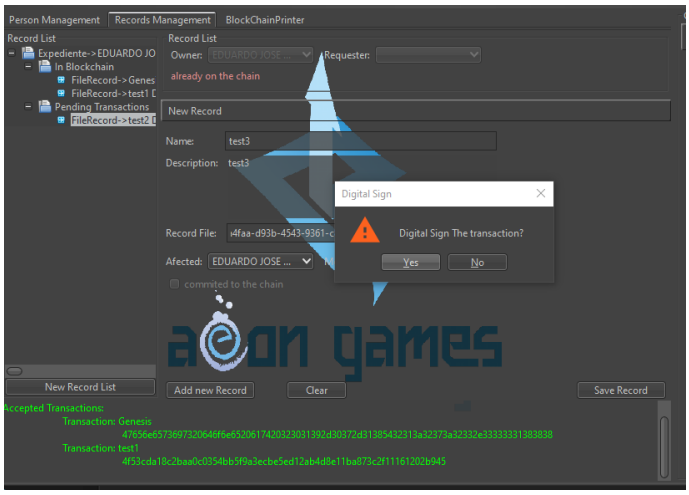
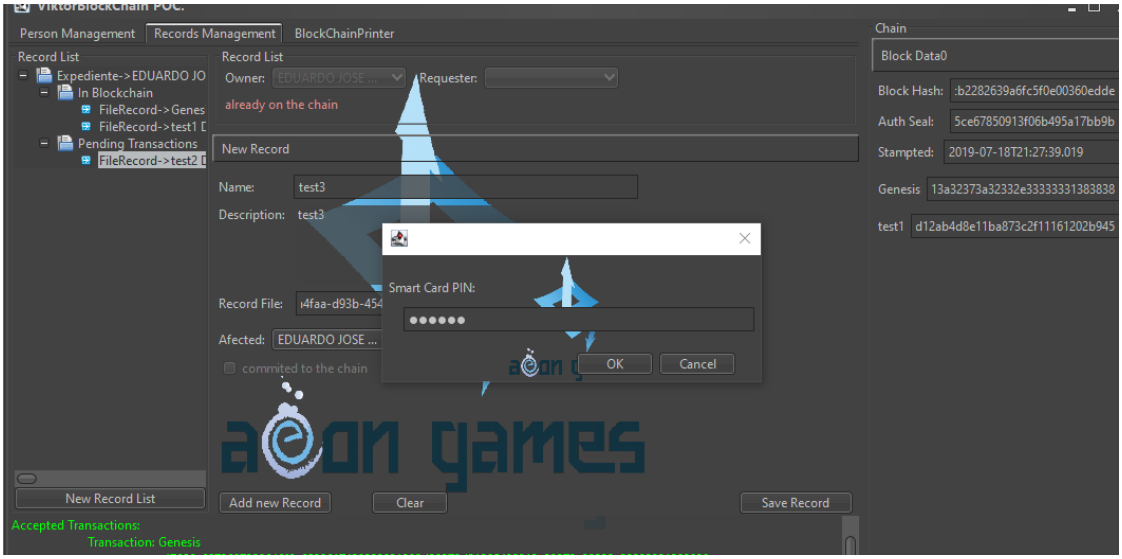


Figura No. 59 Captura de pantalla, confirmación de firma

Fuente: confección propia



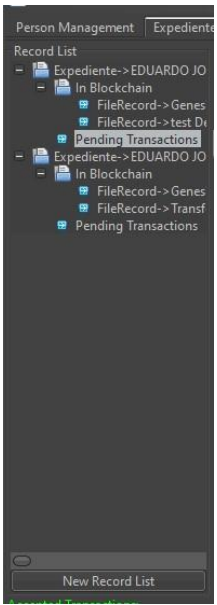


Figura No. 60 Captura de pantalla, firma de transacción

Fuente: confección propia

Los posibles estados son:

- La transacción se encuentra registrada en la cadena de bloques
- La transacción se encuentra pendiente.

Figura No. 61 Captura de pantalla, lista de Expedientes

Fuente: confección propia

La aplicación también posee dos apartados generales donde podemos visualizar la cadena de bloques(A) de forma gráfica (como un listado de paneles) y otra donde se muestra los resultados de las interacciones de la cadena de bloques(B).

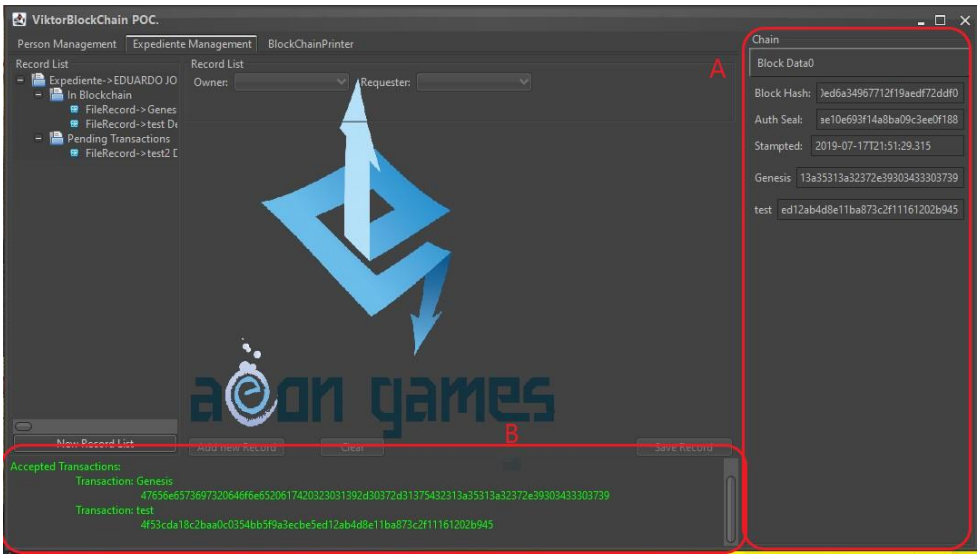


Figura No. 62 Captura de pantalla muestra de componentes

Fuente: confección propia

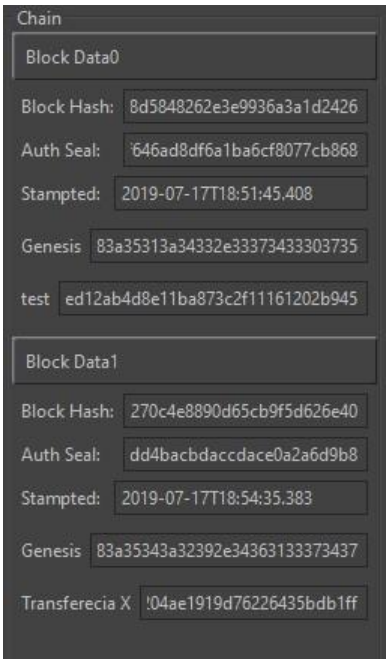


Figura No. 63 Captura de pantalla muestra la cadena (componente A)

Fuente: confección propia

Figura No. 64 Captura de pantalla muestra extendida de componente B

Fuente: confección propia

Finalmente, en la demostración se puede ver una pestaña la cual se utiliza para “imprimir” en pantalla, el contenido de la estructura de la cadena de bloques.

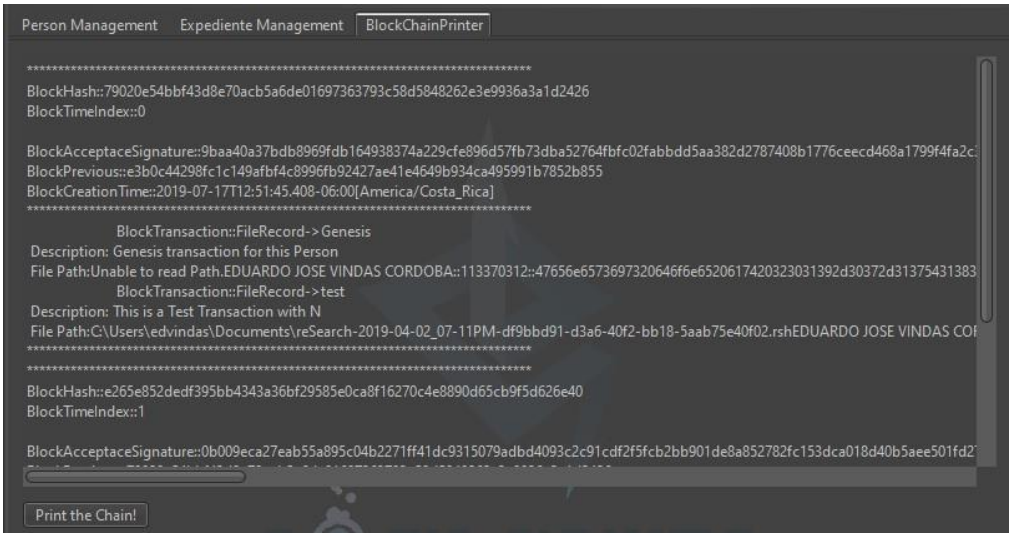


Figura No. 65 Captura de pantalla muestra de la impresora de la cadena de bloques

Fuente: confección propia

9. Control de acceso

La prueba de concepto no aplica control de acceso, puesto no es el foco de estudio, sin embargo, para una puesta en marcha realista y que cumpla con estándares de seguridad y confidencialidad es necesario aplicar control de acceso. Es por tanto vital definir una forma de control de acceso para los datos que se encuentran tanto en los expedientes como aquellos que están en persistencia en la cadena de bloques.

Para definir el control de acceso es necesario determinar una forma de acceso de los datos que brinde acceso únicamente a aquellos quienes poseen el nivel de permiso adecuado. Particularmente para el ambiente de expedientes médicos (Huynh, Frappier, Pooda, Mammar, & Laleau, 2016) plantean una solución mediante el uso de un sistema llamado *SGAC (Solution de gestion automatisée du consentement)* o *"Solución de gestión automatizada del consentimiento"* este sistema permite a la aplicación que tiene acceso a información sensible y privada (en particular del ámbito médico) a autorizar o denegar acceso a los datos ya sea a un grupo, a un médico en particular, a una especialización, esta particularidad

de la propuesta se considera como una excelente opción para una puesta en marcha en producción sobre sistemas de expedientes digitales. Dado a las bondades de este sistema de no solo dar acceso a los datos sino además poseer una opción de prohibir el acceso a los actores relacionados en el sistema. Por ejemplo.

“Un médico se enferma y necesita ser atendido por otro médico, dado a la naturaleza de su profesión este médico es atendido y conoce a los otros médicos y tiene conocimiento de otros médicos que si acceder su expediente pudieran no tener la mejor de las intenciones por tanto para evitar conflictos el médico solicita negar el acceso a su expediente médico a sus colegas excepto al médico que le atenderá de esta forma se logra un nivel de confidencialidad” ejemplo adaptado de (Huynh, Frappier, Pooda, Mammar, & Laleau, 2016).

¿Pero en este mismo ejemplo que pasa si se da una emergencia y un médico que previamente tiene negado el acceso necesita ver los detalles del expediente?

En estos casos específicos se da la acción de prioridades en las reglas de acceso:

Regla	Recurso	sujeto	prioridad	Modo	Condición
R1	Paciente	Emergencia	1	+	La vida del paciente está en peligro
R2	Paciente	Médico “<Bob>” tratante	2	+	El paciente atendiendo a su cita

R3	Paciente = “David”	Médicos	2	-	True
…	…	…	…	…	…
Rn	Vitales	Enfermería	3	+	True

Tabla 8 Representación del bloque en la propuesta

Fuente: adaptado de: (Huynh, Frappier, Pooda, Mammar, & Laleau, 2016)

Por tanto, como se ilustra en la tabla. Todos los médicos excepto por el médico tratante no pueden ver el expediente del médico. Con excepción del médico “Bob” y cuando se dé la condición descrita, en este caso ser atendido en la cita médica.

Y finalmente ante una emergencia, en ese caso como la regla posee la mayor prioridad, en este caso, el médico de emergencias podrá ver el expediente de paciente David.

Utilizando *SGAC* también es posible segregar el acceso dependiendo del área como se menciona en la tabla, pero para dejarlo con mayor claridad se ilustra de la siguiente forma:

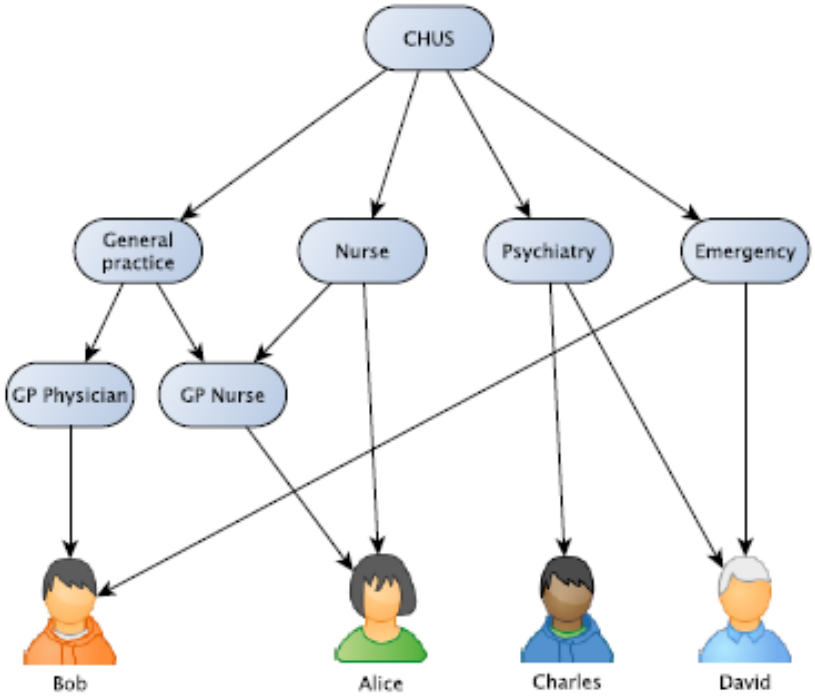


Figura No. 66 Gráfico de sujetos

(Huynh, Frappier, Pooda, Mammar, & Laleau, 2016)

Capítulo VI: Conclusiones y Recomendaciones

Conclusiones

Basado en el análisis y estudio de la tecnología de cadena de bloques, se llega a un entendimiento general sobre los componentes que forman esta tecnología, las tecnologías asociadas, así como las diferentes permutaciones existentes para resolver distintos problemas. Y se evalúa con profundidad los aspectos comunes utilizados en la mayoría de *Blockchain* en el mercado.

Se confirma que esta tecnología es idónea para el uso en la puesta en marcha de sistemas que requieran trazabilidad, completitud, integridad a los datos y además que brinde confianza a los usuarios con la estabilidad de los resultados expuestos

en estos sistemas, dado a que requiere su expreso permiso y no es posible cambiar los datos en la cadena sin dañar de forma permanente el sistema y romper la integridad de los datos. Por tanto, se concluye que, en el ámbito de expedientes digitales de índole, médica, legal, financiera la solución es viable y provechosa para estas industrias.

Se expusieron las soluciones en el mercado tal como *Hyperledger*, *Ethereum*, *bitcoin*, entre otras. Con la comprensión de las funcionalidades básicas y extenderlo a algunas particularidades de cada tecnología. Mediante el estudio de estas tecnologías comprendemos que de las estudiadas *Hyperledger* y *Ethereum* podrían ser utilizadas para los fines de creación y puesta en marcha de expedientes digitales.

Con el fin de ahondar en los objetivos académicos y comprensión de posibles problemas que se pueden presentar en las cadenas de bloques se tomó la opción de crear la cadena de bloques propia sin uso de una de las opciones del mercado. Esto permite profundizar la compresión de algunos temas presentes en la tecnología.

Se puede justificar el uso de la tecnología de *Blockchain* en ámbitos como el médico, legal, gubernamental, votación, entre otros mediante la comprensión de la tecnología y las bondades que brinda, más es de destacar que el uso de estas tecnologías no es simple, y además posee un impacto (mayormente en las necesidades de computación y tiempos de respuesta), el cual en la mayoría de las industrias es justificable.

Recomendaciones

La puesta en marcha es una prueba de concepto y como tal no se recomienda su uso en ambientes de producción sin previo estudio y adaptarlo a las necesidades específicas de la organización que aplicará su uso, pero en contraste se recomienda su uso y estudio con fines académicos y para ser utilizada en una solución más robusta e integral.

La prueba de concepto no cifra los datos que son trasmitidos por las redes, es por tanto recomendado que se adapte a una puesta en marcha con el uso de certificados, o en su defecto que las comunicaciones sean enviadas por “túneles” cifrados en una red privada.

Se recomienda el análisis e ingreso de otros actores como expone la Figura No. 31 Actores que interactúan con *Blockchain*

La implementación de la cadena de bloques actualmente no posee persistencia. Y está limitada a una cantidad de datos cuyo valor es a $MAX\_VALUE = 2^{31} - 1$ por tanto se recomienda ante una puesta en marcha donde se garantiza o exista la posibilidad de que las transacciones superen esta cantidad que estos sean persistentes en bases de datos (las cuales además deberán ser replicada por otros nodos)

Ante una puesta en marcha real, se realiza una recomendación de utilizar *Apache Kafta* a cambio de *Redis*, esto se debe a que *Kafta* posee opciones para balancear el trabajo entre los nodos, además de esto ayuda con el control de pilas de trabajo. Redis por otro lado es una excelente opción para mantener una piscina de datos. Y bajo las necesidades de la prueba de concepto es muy útil.

Para una puesta en marcha de *blockchain* se recomienda el estudio de la solución *Hyperledger*

Capítulo VII: Trabajos Futuros

En la presente investigación se realizó una prueba de concepto con la cual se puede demostrar las bondades de las tecnologías de bloque, es de esta manera que existe una gran cantidad de aspectos donde se puede ahondar a partir del estudio actual:

- Crear cadenas de bloques basadas en la solución propuesta en donde se profundice en aspectos que esta investigación no indagó. Como puede ser el caso de cifrado de las transmisiones hechas en la cadena de bloques.

- Implementar a profundad la verificación y uso de Certificados digitales (listas de revocación y firmas digitales) que si bien se utilizan en la presente solución no se ahonda en la verificación de la validez del certificado.
- Presentar la presente investigación a las autoridades y actores interesados en los ámbitos de las instituciones públicas y privadas para las cuales esta investigación pretende demostrar una solución. Como es el caso de las autoridades de la Caja Costarricense del Seguro Social, en donde se demostró interés durante la conversación que se dio en la exposición del Tico *Blockchain*.

Se sugiere invitar a personal del Poder Judicial, de Hacienda y otros en donde se puede adaptar la solución propuesta.

Aunado a las limitaciones de la prueba de concepto, trabajos futuros pueden ser desarrollados para aplicar la persistencia de la cadena de bloques en una base de datos a elección del investigador.

La prueba de concepto es un ejemplo que está en un estado muy temprano un trabajo futuro es el darle seguimiento a esta prueba de concepto y llevarla a un mayor nivel de madurez en donde pueda ser propuesto como una solución que requiere menores tiempos para adaptarse a los diferentes posibles ámbitos de implementación.

Otra posible línea de investigación es el uso de soluciones ya disponibles en el mercado a manera de realizar un contraste con la presente investigación en donde se aplica una implementación de autoría propia.

Capítulo VIII: Reflexiones Finales

El tema de la tecnología de *blockchain* es muy amplia, no se limita a algo simple como la cadena como tal, sino que además incluye temas como, criptografía, comunicación distribuida, consenso, inclusive en muchos aspectos puede estar

asociado a la industria específica en donde se ve aplicada la tecnología. Es por tanto que puede ser inicialmente engañoso todos los temas asociados, sin embargo, al tener una cantidad importante de temas asociados y varios de estos temas son complejos. Hacen altamente retador poseer o adquirir el conocimiento integral sobre esta tecnología.

Por tanto, se puede decir *blockchain* por si misma es un área multidisciplinario de estudio el cual no puede ser entendido en tiempos cortos. Requiere un grupo de profesionales con conocimientos especializados desde matemáticos (criptógrafos), ingenieros de software, ingenieros de seguridad.

En la actualidad *blockchain* se ha transformado en un "*buzzword"* al igual que en el pasado lo fuel "*la nube*" (en el ámbito de las tecnologías de información), "*CISCO*", "*contenedores*". El hecho que caiga en esta categoría no es indicativo que sea un peyorativo, pero si indica que está en la boca de muchos quienes a su vez y lamentablemente no comprenden las implicaciones de estas palabras y por dar un "*factor wow*" tratan de implementar estas palabras a sus empresas, negocios, organizaciones. Sin la comprensión holística necesaria para discernir si estas palabras van acordes con la misión y visión de sus organizaciones. Es por tanto parte de la motivación de la investigación realizar una compilación académica en donde se clarifiquen estos temas y dar claridad a la complejidad asociada y brindar definiciones de dónde y cómo es posible que la tecnología propuesta sea utilizada.

Para la prueba de concepto se determina que es una versión "*pre-alpha*" lo que significa que es una implementación muy temprana, y requiere mayor desarrollo. Por tanto, se invita a todo desarrollador interesado a extender sobre esta prueba de concepto.

Para una Puesta en producción se sugiere a los interesados a aplicar y utilizar implementaciones de *SGAC (Solution de gestion automatisée du consentement)* de forma que se pueda dar un control de acceso global que sea adaptable y utilizable en múltiples ámbitos tanto médico, legal, etc. Y no solo brinda acceso sino además de poder negarlo o prohibirlo a manera que sea posible evitar casos

de conflicto de intereses o espionaje como en casos que se pueden mencionar dados en Costa Rica como el de Espionaje de información sensible Fiscal de Keylor Navas (Fallas M(La Nacion), 2016)

Bibliografía

Khatwani , S. (10 de 11 de 2018). *https://coinsutra.com/satoshi-nakamoto-facts/*. Obtenido de coinsutra: https://coinsutra.com/satoshi-nakamoto-facts/

Ali, M., Shea, R., Nelson, J., & Freedman, M. J. (12 de Octubre de 2017). *Blockstack: A New Internet for Decentralized Applications*. Obtenido de Blockstack: A New Internet for Decentralized Applications: https://blockstack.org/whitepaper.pdf

Banco Central de Costa Rica. (Junio de 2019). Obtenido de Banco Central de Costa Rica: https://www.bccr.fi.cr/seccion-firma-digital/firma-digital/homologaci%C3%B3n-de-tarjetas-y-lectores

Bearman, S. (27 de Octubre de 2017). *cnbc.* Obtenido de cnbc: https://www.cnbc.com/2017/10/27/bitcoins-origin-story-remains-shrouded-in-mystery-heres-why-it-matters.html

Bilgin, I. (21 de July de 2018). *medium.com*. Obtenido de medium.com: https://medium.com/@bibryam/enterprise-integration-for-ethereum-fa67a1577d43

Bitcoin CodeBase. (2018). *codigo de arbol merkle*. Obtenido de codigo de arbol merkle: https://github.com/bitcoin/bitcoin/blob/master/src/consensus/merkle.cpp

Buchmann, J. (Abril de 2007). Merkle Tree Traversal Techniques. Darmstadt University of Technology.

Cao, J. (01 de 06 de 2019). *agenttroll.github.io*. Obtenido de agenttroll.github.io: https://github.com/AgentTroll

Castro, M., & Liskov, B. (04 de November de 1999). *http://pmg.csail.mit.edu/papers/osdi99.pdf*. Obtenido de MIT computer Science & artificial Intelligence Laboratory: http://pmg.csail.mit.edu/papers/osdi99.pdf;https://www.microsoft.com/en-us/research/wp-content/uploads/2017/01/p398-castro-bft-tocs.pdf

Chapweske, J., & Mohr, G. (04 de marzo de 2003). *Tree Hash EXchange format (THEX)*. Obtenido de Tree Hash EXchange format (THEX): http://web.archive.org/web/20080316033726/http://www.open-content.net/specs/draft-jchapweske-thex-02.html

Chia, T. (20 de August de 2012). *blogoverflow.com*. Obtenido de blogoverflow.com: https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

De Angelis, S. (18 de Mayo de 2018). *Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains*. Obtenido de University of Rome: https://arxiv.org/pdf/1805.03490.pdf

Deitel, P., & Deitel, H. (2012). Java How To Program 9 edicion. En P. Deitel, & H. Deitel, *Java How To Program 9 edicion* (pág. 1300). Pearson.

Ecma. (diciembre de 2017). *The JSON Data Interchange Syntax*. Obtenido de The JSON Data Interchange Syntax: http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-404.pdf

Esquivel, G. (02 de febrero de 2019). *https://twitter.com/gaboesquivel*. Obtenido de https://twitter.com/gaboesquivel: https://twitter.com/gaboesquivel/status/1091757045357916161

Fallas M(La Nacion), G. (06 de Abril de 2016). *Sala IV reprocha a OIJ y Fiscalía por caso de espionaje a datos de Keylor Navas*. Obtenido de Nacion.com: https://www.nacion.com/sucesos/judiciales/sala-iv-reprocha-a-oij-y-fiscalia-por-caso-de-espionaje-a-datos-de-keylor-navas/I3FT6Z3QDNHYTM663VJJBLKBAI/story/

Freeman, E., Robson, E., Sierra, K., & Bates, B. (2004). Head First Design Patterns. En E. Freeman, E. Robson, K. Sierra, & B. Bates, *Head First Design Patterns* (págs. 535-582). 'reilly.

Gaur, N., Desrosiers, L., Ramakrishna, V., Novotny, P., A. Baset, D., & O'Dowd, A. (2018). *Hands-On Blockchain with Hyperledger.* Birmingham: Packt Publishing Ltd.

Ghosh, D. (5 de abril de 2016). *medium*. Obtenido de How the Byzantine General Sacked the Castle: A Look Into Blockchain: https://medium.com/@DebrajG/how-the-byzantine-general-sacked-the-castle-a-look-into-blockchain-370fe637502c

Gupta, R. (2018). *Hands-On Cybersecurity with Blockchain.* Livery Place: Packt Publishing Ltd.

Hernandez Sanchez, A., & Dolores Martínez, M. (2014). La investigación evaluativa: enfoque estratégico para una educación a distancia en entornos virtuales de calidad. Aula de encuentro. En A. Hernandez Sanchez, & M. Dolores Martínez, *La investigación evaluativa: enfoque estratégico para una educación a distancia en entornos virtuales de calidad. Aula de encuentro* (págs. 106-129.). Obtenido de https://www.researchgate.net/publication/303017054_La_investigacion_evaluativa_enfoque_estrategico_para_una_educacion_a_distancia_en_entornos_virtuales_de_calidad

Herreras, E. B. (2004). LA DOCENCIA A TRAVÉS DE LA INVESTIGACIÓN–ACCIÓN. *Revista Iberoamericana de Educación, 35*(1), 1-9. Obtenido de https://rieoei.org/RIE/article/view/2871

Hill, B., Chopra, S., & Valencourt, P. (2018). *Blockchain Quick Reference.* Birmingham: Packt Publishing Ltd.

Huynh, N., Frappier, M., Pooda, H., Mammar, A., & Laleau, R. (25 de agosto de 2016). *2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS)*. Obtenido de SGAC: A patient-centered access control method: https://ieeexplore.ieee.org/document/7549286

hyperledger. (2017). *hyperledger readthedocs*. Obtenido de hyperledger readthedocs: https://hyperledger-fabric.readthedocs.io/en/v1.0.5/kafka.html

IBM. (21 de Junio de 2019). *IBM knowledgecenter*. Obtenido de IBM knowledgecenter: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_9.0.0/com.ibm.mq.con.doc/q130880_.html

Instituto del Cafe de Costa Rica. (29 de 04 de 2019). *Instituto del Cafe de Costa Rica*. Obtenido de Instituto del Cafe de Costa Rica: http://www.icafe.cr/nuestro-cafe/el-mejor-cafe-del-mundo/

Kozliner, E. (27 de Setiembre de 2017). *hackernoon*. Obtenido de hackernoon: https://hackernoon.com/merkle-tree-introduction-4c44250e2da7

Kumar, S. (21 de Mayo de 2018). *skcript*. Obtenido de skcript: https://www.skcript.com/svr/consensus-hyperledger-fabric/

Leibiusky, J. (2019). *Jedis is a blazingly small and sane Redis java client.* Obtenido de Jedis is a blazingly small and sane Redis java client.: https://github.com/xetorthio/jedis

Ley N° 9162. (23 de Setiembre de 2013). *Sistema Costarricense de Informacion Juridica Ley N° 9162*. Obtenido de Sistema Costarricense de Informacion Juridica:

http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=75700&nValor3=93998&strTipM=FN

Liu, C., & Albitz, P. (2006). DNS and BIND. En C. Liu, & P. Albitz, *DNS and BIND* (págs. 4-10). Sebastopol, CA 95472.: O'Reilly.

Loom Network et all. (2018). *cryptozombies*. Obtenido de cryptozombies: https://cryptozombies.io/#learn-more

Marín, J. (26 de Julio de 2018). *https://medium.com*. Obtenido de https://medium.com: https://medium.com/@juliomacr/blockchain-as-a-data-structure-3bd125d8ddda

Merkle, R. C. (1979). *Estados Unidos Patente nº US4309569A.* Obtenido de https://patents.google.com/patent/US4309569

Meunier, S. (29 de Diciembre de 2016). *medium.com*. Obtenido de medium.com: https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118

Ministerio de Hacienda. (11 de setiembre de 2018). *https://www.hacienda.go.cr/*. Obtenido de https://www.hacienda.go.cr/: https://www.hacienda.go.cr/contenido/14350-factura-electronica

Mitani, M., Shinichi, S., Idero, H., & Corp, V. (2018). The Manga Guide™ to Cryptography. En M. Mitani, S. Shinichi, H. Idero, & c. Verte, *The Manga Guide™ to Cryptography* (págs. 105-120). Tokyo: No Starch Press.

Montresor, A. (06 de diciembre de 2018). *Universidad de Trento*. Obtenido de Universidad de Trento: http://disi.unitn.it/~montreso/ds/handouts17/10-pbft.pdf

Nakamoto, S. (31 de Octubre de 2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Oracle. (2018). Obtenido de https://docs.oracle.com/en/java/javase/11/security: https://docs.oracle.com/en/java/javase/11/security/java-cryptography-

architecture-jca-reference-guide.html#GUID-2BCFDD85-D533-4E6C-8CE9-29990DEB0190

Papegaaij, E. (12 de Setiembre de 2018). *J-Spring 2018*. Obtenido de J-Spring 2018: https://www.youtube.com/watch?v=J9zlqv6w82w

PEASE, M., R, S., & LAMPORT, L. (1987). *Reaching Agreement in the Presence of Faults*. Obtenido de Reaching Agreement in the Presence of Faults: http://lamport.azurewebsites.net/pubs/reaching.pdf

Penard , W., & van Werkhoven, T. (2014). On the Secure Hash Algorithm family. En W. Penard, & T. van Werkhoven, *On the Secure Hash Algorithm family* (págs. 7-9). Obtenido de https://web.archive.org/web/20141014172403/http://www.staff.science.uu.nl/~werkh108/docs/study/Y5_07_08/infocry/project/Cryp08.pdf

redis. (2019). *https://redis.io/*. Obtenido de https://redis.io/: https://redis.io/

Rodriguez Gomez, D., & Valldeoriola Roquet, J. (2009). *Metodologia de la investigacion.* Catalunya: Universitat Iberta de Catalunya. Obtenido de zanadoria.com/syllabi/m1019/mat_cast-nodef/PID_00148556-1.pdf: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/77608/2/Metodolog%C3%ADa%20de%20la%20investigaci%C3%B3n_M%C3%B3dulo%201.pdf

Rodriguez Gomez, D., & Valldeoriola Roquet, J. (2009). *Metodologia de la investigacion.* Catalunya: Universitat Iberta de Catalunya. Obtenido de zanadoria.com/syllabi/m1019/mat_cast-nodef/PID_00148556-1.pdf.

Rosic, A. (noviembre de 2018). *blockgeeks*. Obtenido de blockgeeks: https://blockgeeks.com/guides/blockchain-consensus/

Rouse, M. (1 de setiembre de 2008). *techtarget*. Obtenido de techtarget: https://searchsecurity.techtarget.com/definition/nonrepudiation

Santos, M., & Moura, E. (2019). Hands-On IoT Solutions with Blockchain. En M. Santos, & E. Moura, *Hands-On IoT Solutions with Blockchain* (págs. 61-65). Birmingham: Packt Publishing Ltd.

Satran, M. (05 de Mayo de 2018). *How RPC Works*. Obtenido de Microsoft Dev Center: https://docs.microsoft.com/en-us/windows/win32/rpc/how-rpc-works

Serrano Pastor, F., Ato García, M., & Amorós Poveda, L. (2008). *METODOLOGÍA DE UNA INVESTIGACIÓN EVALUATIVA.* Obtenido de gte2.uib.es/edutec/sites/default/files/congresos/edutec05/edutecNo20.pdf.

Sherriff, K. (Feb de 2014). *righto.com*. Obtenido de righto.com: http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html

Soto, M. M. (23 de Abril de 2019). *BCR borró videos de cuando exfiscal Dall'Anese ingresó al banco para sacar documentos protegidos por secreto bancario*. Obtenido de CRhoy: https://www.crhoy.com/nacionales/bcr-borro-videos-de-cuando-exfiscal-dallanese-ingreso-al-banco-para-sacar-documentos-protegidos-por-secreto-bancario/

Sun Microsystems Inc. (2002). *Fundamentals of the Java Programming Language.* Broomfeld: Sun Microsystems Inc.

Tecnológico de Costa Rica. (01 de 11 de 2018). *Tec - Especialización en Blockchain*. Obtenido de Tec - Especialización en Blockchain: https://www.tec.ac.cr/documentos/normativa-requisitos-especializacion-blockchain

the Legion of the Bouncy Castle. (2019). *https://www.bouncycastle.org/*. Obtenido de https://www.bouncycastle.org/: https://www.bouncycastle.org/latest_releases.html

Tutorials Point (I) Pvt. Ltd. (2017). *https://www.tutorialspoint.com*. Obtenido de https://www.tutorialspoint.com: https://www.tutorialspoint.com/mvc_framework/

Universidad Cenfotec. (25 de 10 de 2018). *Hackathon de Blockchain*. Obtenido de Hackathon de Blockchain: http://www.ucenfotec.ac.cr/blog/hackathon-de-blockchain

Zih-Ci, L. (11 de Noviembre de 2017). *medium.com*. Obtenido de medium.com: https://medium.com/getamis/grpc-in-dapp-architecture-8c34125356c7

Zyskind, G., Nathan, O., & Pentland, A. '. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. En *IEEE Security and Privacy Workshops* (págs. 180-184). San Jose, CA, 2015, pp. 180-184.: IEEE Security and Privacy Workshops. Obtenido de Decentralizing Privacy: Using Blockchain to Protect Personal Data.

Anexos

1. Librerías de Terceros utilizadas

La implementación de "*Practical Byzantine Fault Tolerance*" (PBFT) utilizada en la prueba de concepto puede ser descargado desde: https://github.com/AgentTroll/pbft-java

La librería utilizada para conectar el Código Java con los servidores Redis se llama Jedis, esta librería puede ser obtenida y estudiada en: https://github.com/xetorthio/jedis

Redis es un estructura en memoria, esta puede ser instalada en los diferentes distribuciones de Linux, la versión específica de Windows puede ser adquirida en: https://redis.io/download o en https://github.com/microsoftarchive/redis/releases

Se utilizó la librería *Bouncy castle*, esta es una librería de diferentes algoritmos criptográficos, de los cuales se aplica "*SHA256withRSA*" y puede ser adquirida en el siguiente link: https://www.bouncycastle.org/latest_releases.html

La puesta en marcha utiliza una librería visual llamada "*Radiance*" las cuales fueron escritas por Kirill Grouchnikov y puede ser descargada desde: https://github.com/kirill-grouchnikov/radiance

2. Ejecución de la Revisión.

2.1. Ejecución en la Fuente Google Scholar

Información extraída de los estudios principales.

Identificación
Título: Decentralizing Privacy: Using Blockchain to Protect Personal Data
Publicación: 2015 IEEE Security and Privacy Workshops
Autores: Guy Zyskind, Oz Nathan, Alex 'Sandy' Pentland
Referencia:
Repositorio: IEEE (Mediante Búsqueda en Google Scholar) https://ieeexplore.ieee.org/abstract/document/7163223
Descripción
Área: Seguridad, Privacidad
Resumen En esta publicación se define el problema con relación a la privacidad y define métodos a proponer para dar seguridad a los datos de un “usuario” y mediante solicitar permisos se da acceso a los usuarios de las aplicaciones a la base de datos distribuida mediante la tecnología de cadena de bloques. La publicación entra en detalles técnicos y matemáticos como el uso de la tecnología de cadena de bloques puede ser adaptada para asegurar que los datos personales de los individuos sean mantenidos de forma que se asegure “quien es dueña” de la información, transparencia y facilitar la auditoria de los datos. y control sobre los datos.
Aspectos por destacar
Esta publicación es valiosa para la investigación dada a su relación al tipo de criterio a proteger, datos privados brindando seguridad, control y definir el autor. Aunado a ello esta publicación es valiosa para la integración de otros aspectos de seguridad a una implementación de cadena de bloques que mantenga datos de personas.

Identificación
Título: Bitcoin: A Peer-to-Peer Electronic Cash System
Publicación: https://bitcoin.org/bitcoin.pdf
Autores: Satoshi Nakamoto
Referencia:
Repositorio: Google Scholar
Descripción
Área: blockchain, Privacidad
Resumen En esta publicación es la publicación inicial que inicia las definiciones e inicia la aventura de la tecnología de *blockchain*, define la estructuras, define algunos posibles escenarios problemáticos y como atacarlos mediante la tecnología propuesta
Aspectos por destacar
Esta publicación es valiosa para la investigación dada a que es la base de la tecnología a utilizar para la investigación. Define los componentes críticos y las fórmulas o métodos a aplicar para crear una implementación de la cadena en un sistema de libros contables.

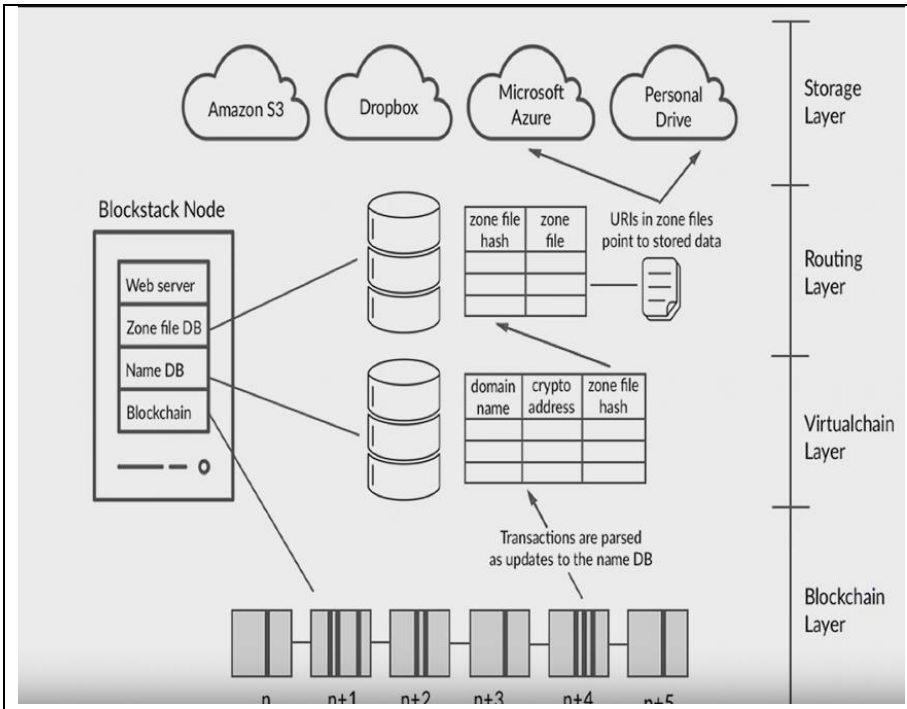
Identificación
Título: Architecture of the Hyperledger Blockchain Fabric
Publicación: IBM Research – Zurich
Autores: Christian Cachin
Referencia:
Repositorio: Google Scholar https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf
Descripción
Área: Blockchain, Technology
Resumen Se brinda una pequeña introducción a la tecnología de "*Hyperledger*", y explica como mediante el uso de la tecnología colaborativa fue posible crear un conjunto de cogidos los cuales son utilizables para la creación y aplicación de la tecnología de cadena de bloques para cualquier propósito. Además de esto también indica algunos de métodos que esta tecnología utiliza para brindar confianza a las posibles implementaciones de cadena de bloques.
Aspectos por destacar
Esta publicación, define y explica un poco sobre la tecnología existente para el uso y creación de cadena de bloques privados existente en el mercado que puede ser considerado para la aplicación en la investigación.

2.2. Microsoft academic

Información extraída de los estudios principales.

Identificación
Título: Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab
Publicación: *Financial Cryptography*, vol. 2015, 2016
Autores: Delmolino, Kevin, et al.
Referencia:
Repositorio: Microsoft Academic https://academic.microsoft.com/#/detail/2293230997
Descripción
Área: Security, Smart contracts
Resumen Esta publicación indica algunos argumentos sobre el uso de "*Smart Contracts*" en particular con el uso de Ethereum, esta publicación brinda algunos ejemplos y métodos utilizados para la creación y ejecución de laboratorios de prueba de concepto basado en la tecnología de cadena de bloques. Además, introduce a algunos conceptos que no están presentes en la literatura sobre algunas de las diferencias de bitcoin y la tecnología de Ethereum.
Aspectos por destacar
es de utilidad puesto indica algunos aspectos utilizado para la creación de contratos y posibles errores que se pueden encontrar en el uso de la herramienta, aunado brinda algunas ideas de cómo aplicar contratos y en que escenarios estos son útiles y en cuales es mejor hacer un estudio a profundidad para determinar la idoneidad del uso de la tecnología de contratos inteligentes en el negocio al cual se desea aplicar.

Identificación
Título: “Blockstack: A Global naming and storage system secured by blockchains”
Publicación: Usenix Annual Technical Conference, 2016, pp. 181–194**.**
Autores: Ali, Muneeb, et al.
Referencia:
Repositorio: Microsoft Academic https://academic.microsoft.com/#/detail/2410750382
Descripción
Área: blockchain, Computer science, Distributed computing Software, Real-time computing, Computer security
Resumen Esta publicación define una investigación llevada a cabo para la construcción de un sistema basado en cadena de bloques para remplazar el sistema actual de DNS y PKI. En los hallazgos de este estudio definen rasgos de cómo se podrían utilizar estas tecnologías como remplazo, pero al costo. El costo dependiente de algunos eventos en control y fuera del control de quien implementa el sistema. Además, las implementaciones son basadas en *Blockchain* existentes (Bitcoin) y se detecta limitaciones dado a la naturaleza del conceso de la cadena debe tomar. Además, otro límite es el tamaño del bloque. Con estas limitantes se describe como es que se logran realizar implementaciones sobre diferentes sistemas para lograr generar un PKI y un DNS (llamado BNS), el cómo está actualmente formado este sistema se muestra:



Aspectos por destacar

Esta publicación da una buena introducción a una opción de utilizar un sistema de cadena de bloques Existente para lograr crear un sistema sobre este, pero a su vez también describe las vulnerabilidades de realizar estas implementaciones de esta forma y los costos relacionados.

2.3. Worldwide Science

Información extraída de los estudios principales.

Identificación
Título: Blockchain and Trusted Computing: Problems, Pitfalls, and a Solution for Hyperledger Fabric
Publicación: arxiv
Autores: Marcus Brandenburger; Christian Cachin; Rüdiger Kapitza; Alessandro Sorniotti
Referencia:
Repositorio: Worldwide Science https://arxiv.org/pdf/1805.08541v1.pdf
Descripción
Área: blockchain, Computer science, Distributed computing Software, Real-time computing, Computer security
Resumen en esta publicación se enfoca en describir como el sistema basado en cadena de bloques es muy poderoso, y posee muchas aplicaciones, pero posee una limitante en lo que respecta a mantener la información de forma secreta. Con este respecto en esta publicación se hace la sugerencia de la utilización de metodologías las cuales puedan brindar la confidencialidad necesaria para las aplicaciones que son creadas en *Hyperledger*.
Aspectos por destacar
La tecnología básica de cadena de bloques por sí sola no se existe una forma de asegurar la información que es manipulada en las transacciones es pública para todos y puede determinar que pasa y que información se transmite en la red. Y esto es un detalle importante para una implementación donde existe la posible necesidad de confidencialidad.

2.3.1. Libros sobre el tema en posesión del autor.

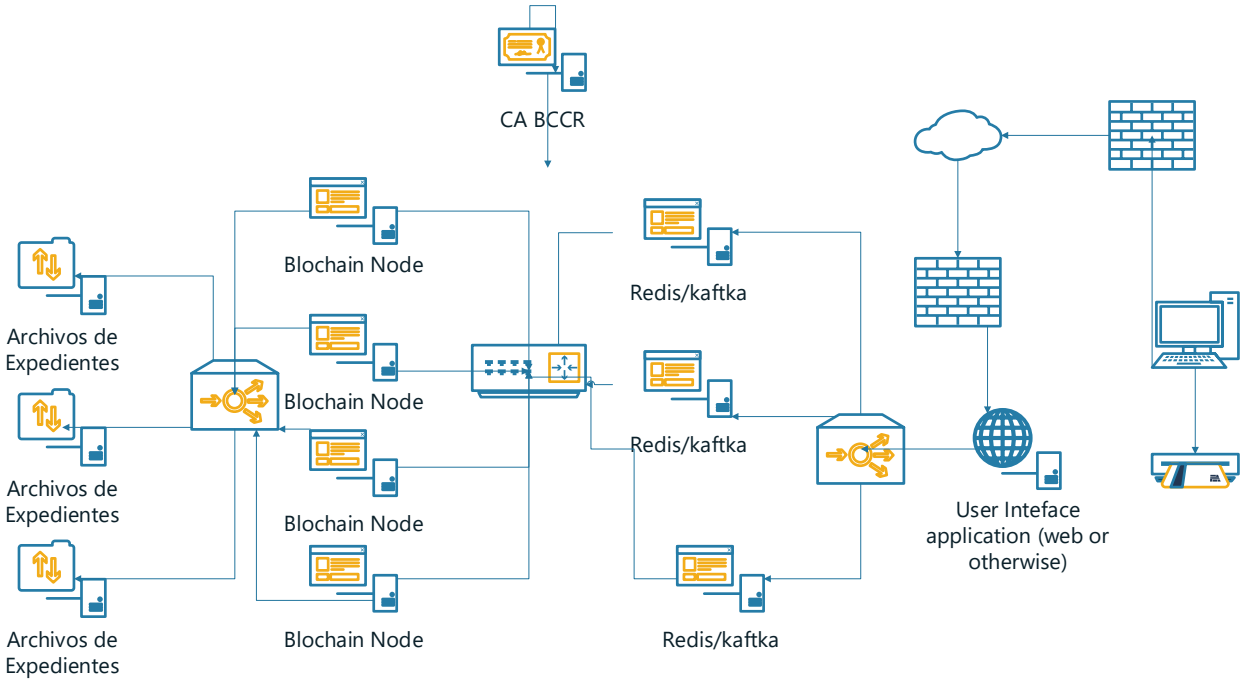
Información extraída de los estudios principales.

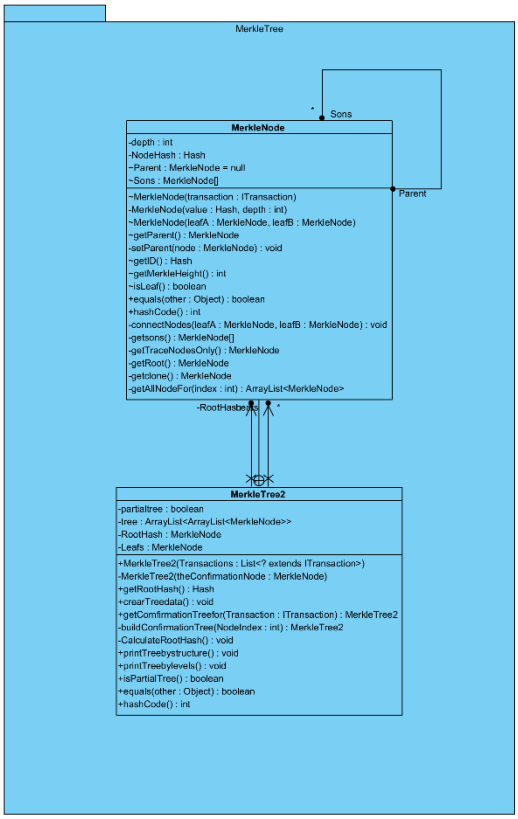
Identificación
Título: Hands-On Cybersecurity with Blockchain
Publicación: Packt book ISBN 978-1-78899-018-9
Autores: Rajneesh Gupta
Referencia:
Repositorio:
Descripción
Área: blockchain, security
Resumen El Libro se enfoca en el tema de cómo asegurar las aplicaciones mediante el uso de la tecnología de cadena de bloques, y en explicar las bondades del uso de estas tecnologías. Explicando algunas de las tecnologías disponibles en el mercado. Incluyendo Ethereum, Bitcoin, *Hyperledger*. Y detalles técnicos de cómo aplicar la tecnología
Aspectos por destacar
¿Qué es la tecnología y cómo funciona? Preguntas con respuestas planteadas por las lecturas sobre aspectos técnicos además, brinda información y justificaciones validad y convincentes para comprender cuándo y por qué se debe dar el uso de esta tecnología.

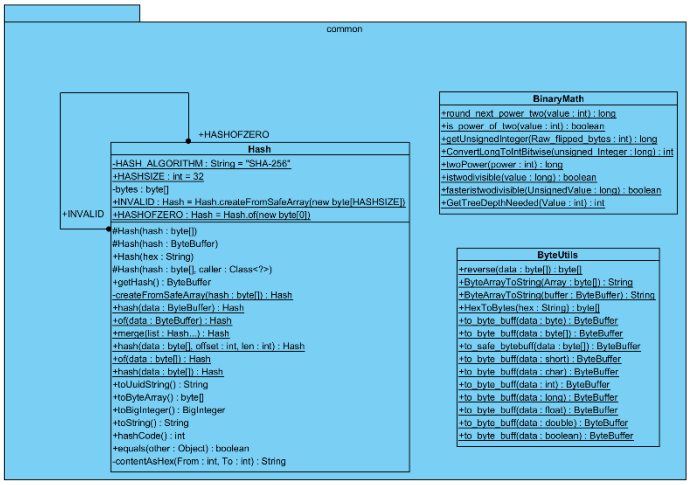
Identificación
Título: The Manga Guide™ to Cryptography
Publicación: no starch press ISBN 978-1-59327-742-0
Autores: Mitani, Masaaki; Shinichi, Sato; Idero, Hinoki; Corp, Verte
Referencia:
Repositorio:
Descripción
Área: cryptography, security, mathematics, functions, hash
Resumen El Libro brinda una introducción a los conceptos que se utilizan en los sistemas criptográficos y explica la matemática de una forma amigable y fácil de entender y explicar al público general.
Aspectos por destacar
Brinda una introducción a los conceptos criptográficos que son clave en la tecnología a exponer, el libro es un buen recurso para hacer referencia y exponer información para explicar las fórmulas y matemática de los algoritmos a utilizar

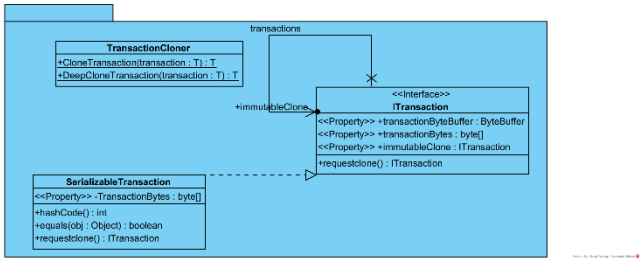
4. Diagramas:

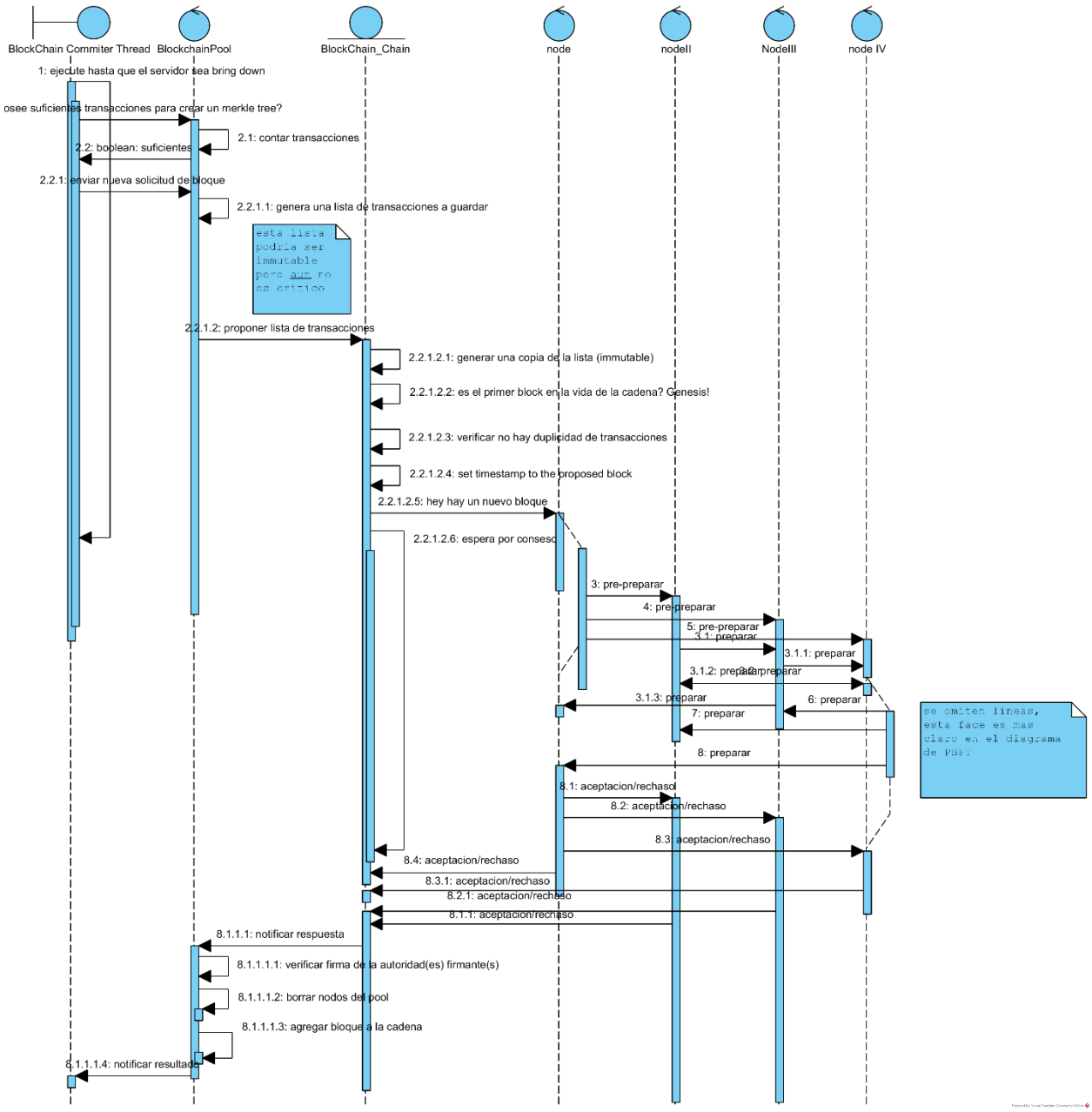
Los diagramas a continuación son de autoría propia:

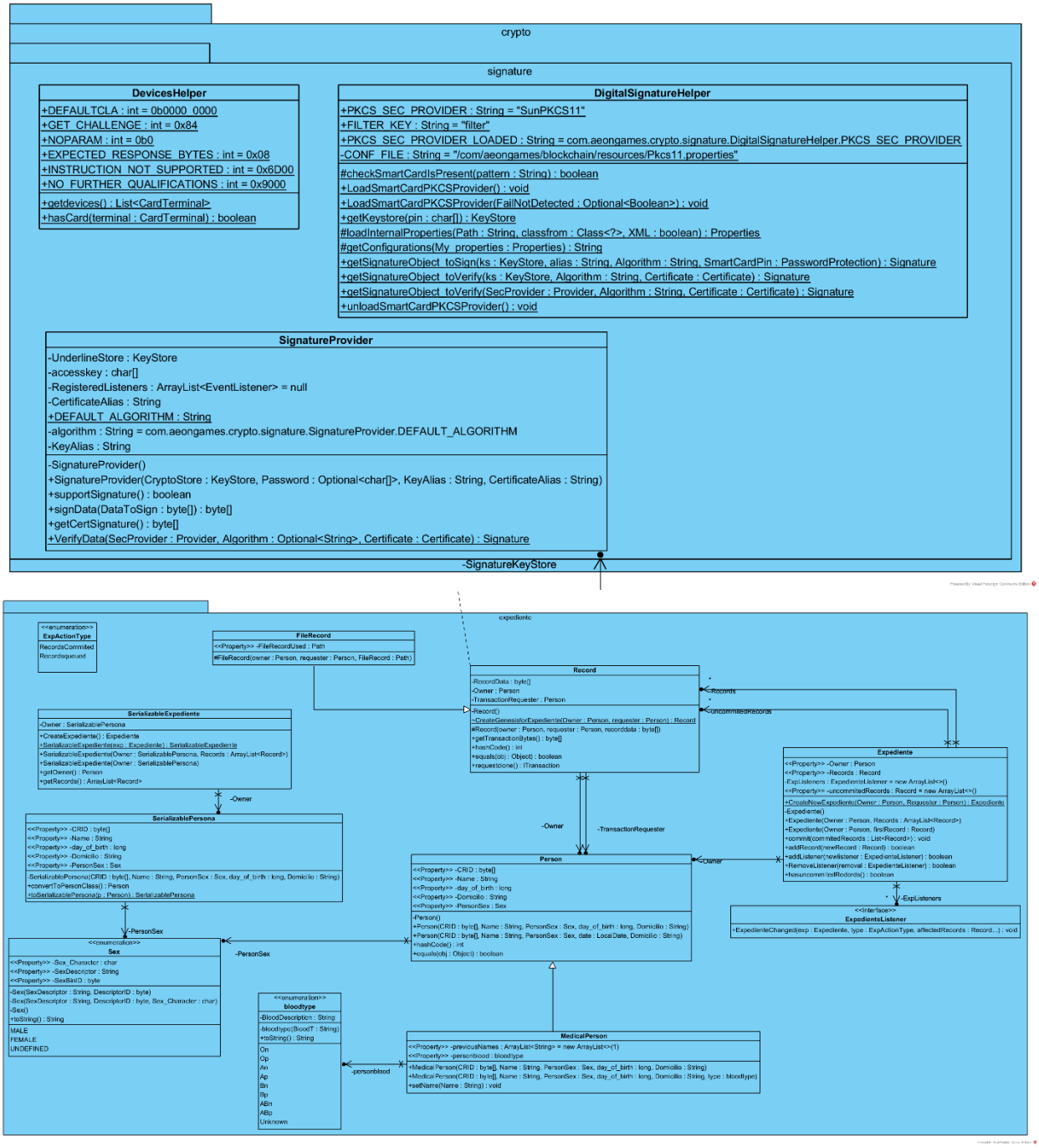


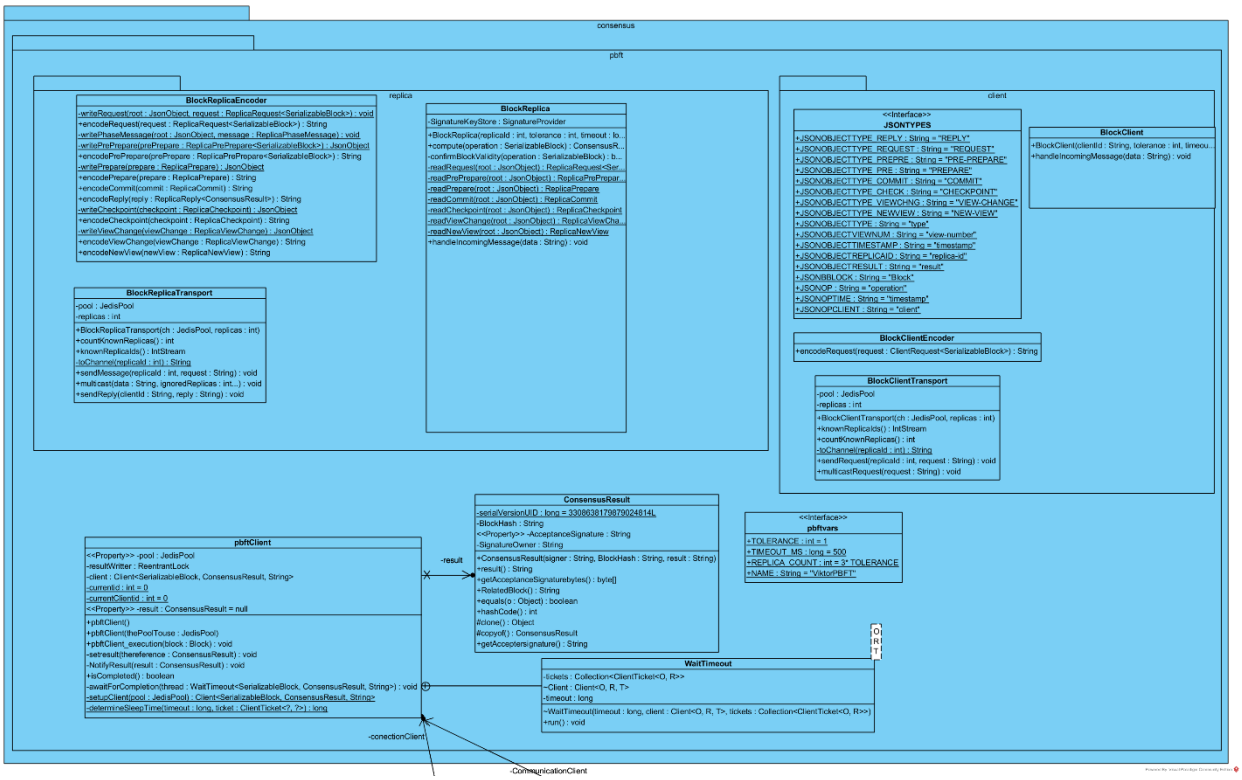

MerkleTree
Sons
MerkleNode
-depth : int
-NodeHash : Hash
-Parent : MerkleNode = null
~Sons : MerkleNode[]
~MerkleNode(transaction : ITransaction)
-MerkleNode(value : Hash, depth : int)
~MerkleNode(leafA : MerkleNode, leafB : MerkleNode)
~getParent() : MerkleNode
-setParent(node : MerkleNode) : void
~getID() : Hash
~getMerkleHeight() : int
~isLeaf() : boolean
+equals(other : Object) : boolean
+hashCode() : int
-connectNodes(leafA : MerkleNode, leafB : MerkleNode) : void
-getsons() : MerkleNode[]
-getTraceNodesOnly() : MerkleNode
-getRoot() : MerkleNode
-getclone() : MerkleNode
-getAllNodeFor(index : int) : ArrayList<MerkleNode>
Parent
-RootHasbeen
MerkleTree2
-partialtree : boolean
-tree : ArrayList<ArrayList<MerkleNode>>
-RootHash : MerkleNode
-Leafs : MerkleNode
+MerkleTree2(Transactions : List<? extends ITransaction>)
-MerkleTree2(theConfirmationNode : MerkleNode)
+getRootHash() : Hash
+crearTreedata() : void
+getComfirmationTreefor(Transaction : ITransaction) : MerkleTree2
-buildConfirmationTree(NodeIndex : int) : MerkleTree2
-CalculateRootHash() : void
+printTreebystructure() : void
+printTreebylevels() : void
+isPartialTree() : boolean
+equals(other : Object) : boolean
+hashCode() : int

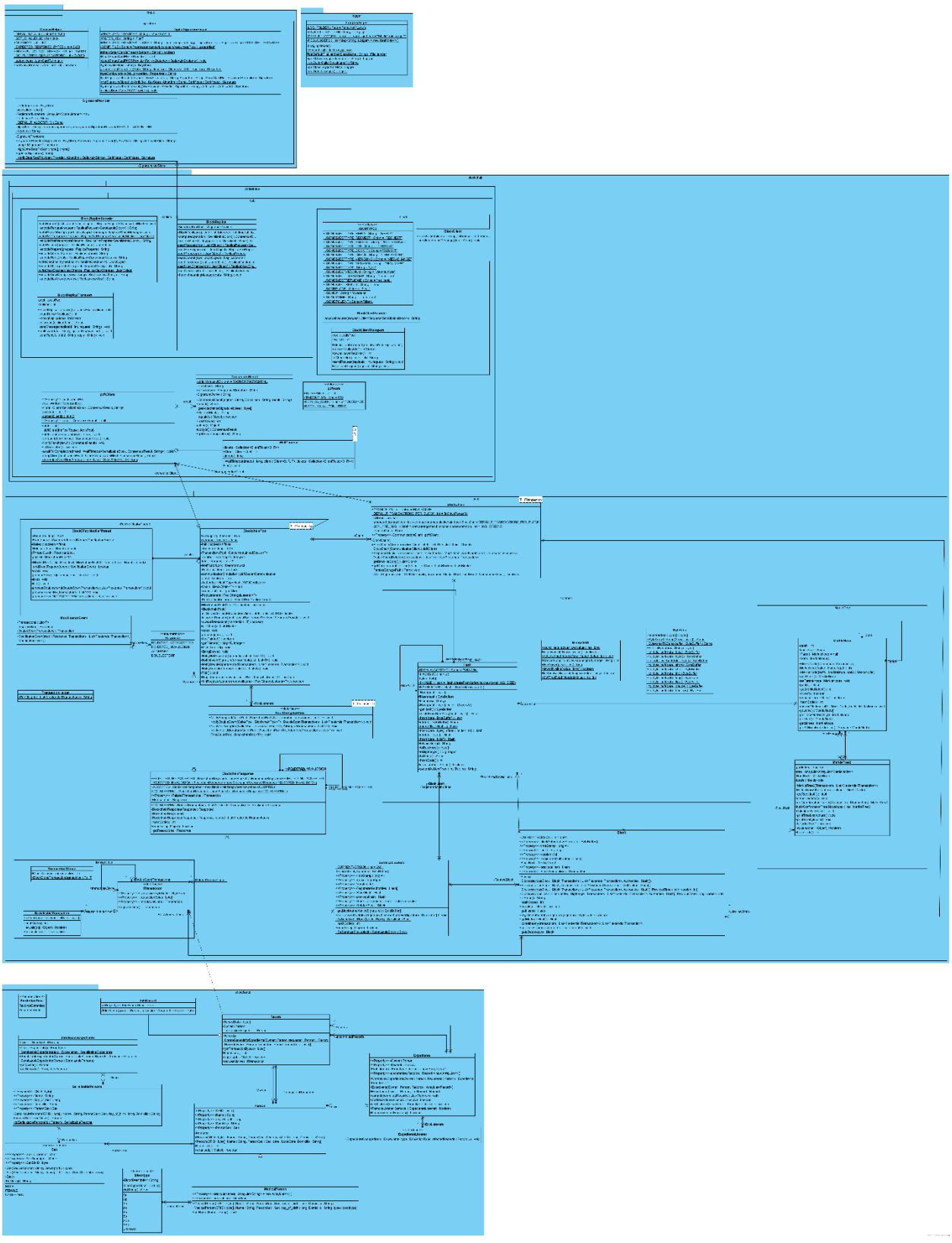

common
+HASHOFZERO
Hash
-HASH_ALGORITHM : String = "SHA-256"
+HASHSIZE : int = 32
-bytes : byte[]
+INVALID : Hash = Hash.createFromSafeArray(new byte[HASHSIZE])
+HASHOFZERO : Hash = Hash.of(new byte[0])
+INVALID
#Hash(hash : byte[])
#Hash(hash : ByteBuffer)
+Hash(hex : String)
#Hash(hash : byte[], caller : Class<?>)
+getHash() : ByteBuffer
-createFromSafeArray(hash : byte[]) : Hash
+hash(data : ByteBuffer) : Hash
+of(data : ByteBuffer) : Hash
+merge(list : Hash...) : Hash
+hash(data : byte[], offset : int, len : int) : Hash
+of(data : byte[]) : Hash
+hash(data : byte[]) : Hash
+toUuidString() : String
+toByteArray() : byte[]
+toBigInteger() : BigInteger
+toString() : String
+hashCode() : int
+equals(other : Object) : boolean
-contentAsHex(From : int, To : int) : String
BinaryMath
+round_next_power_two(value : int) : long
+is_power_of_two(value : int) : boolean
+getUnsignedInteger(Raw_flipped_bytes : int) : long
+ConvertLongToIntBitwise(unsigned_Integer : long) : int
+twoPower(power : int) : long
+istwodivisible(value : long) : boolean
+fasteristwodivisible(UnsignedValue : long) : boolean
+GetTreeDepthNeeded(Value : int) : int
ByteUtils
+reverse(data : byte[]) : byte[]
+ByteArrayToString(Array : byte[]) : String
+ByteArrayToString(buffer : ByteBuffer) : String
+HexToBytes(hex : String) : byte[]
+to_byte_buff(data : byte) : ByteBuffer
+to_byte_buff(data : byte[]) : ByteBuffer
+to_safe_bytebuff(data : byte[]) : ByteBuffer
+to_byte_buff(data : short) : ByteBuffer
+to_byte_buff(data : char) : ByteBuffer
+to_byte_buff(data : int) : ByteBuffer
+to_byte_buff(data : long) : ByteBuffer
+to_byte_buff(data : float) : ByteBuffer
+to_byte_buff(data : double) : ByteBuffer
+to_byte_buff(data : boolean) : ByteBuffer

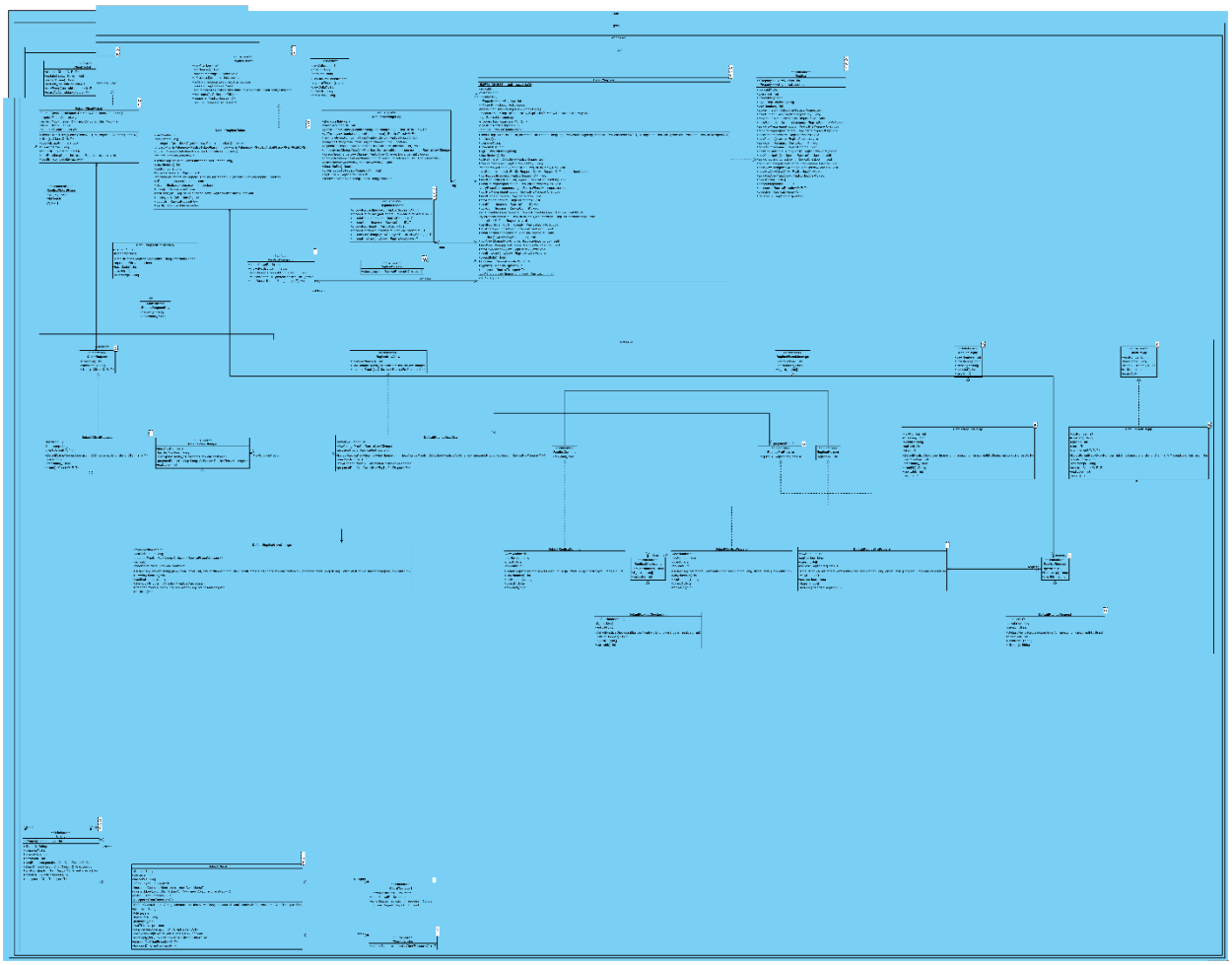

transactions
TransactionCloner
+CloneTransaction(transaction : T) : T
+DeepCloneTransaction(transaction : T) : T
+immutableClone
<<Interface>>
ITransaction
<<Property>> +transactionByteBuffer : ByteBuffer
<<Property>> +transactionBytes : byte[]
<<Property>> +immutableClone : ITransaction
+requestclone() : ITransaction
SerializableTransaction
<<Property>> -TransactionBytes : byte[]
+hashCode() : int
+equals(obj : Object) : boolean
+requestclone() : ITransaction

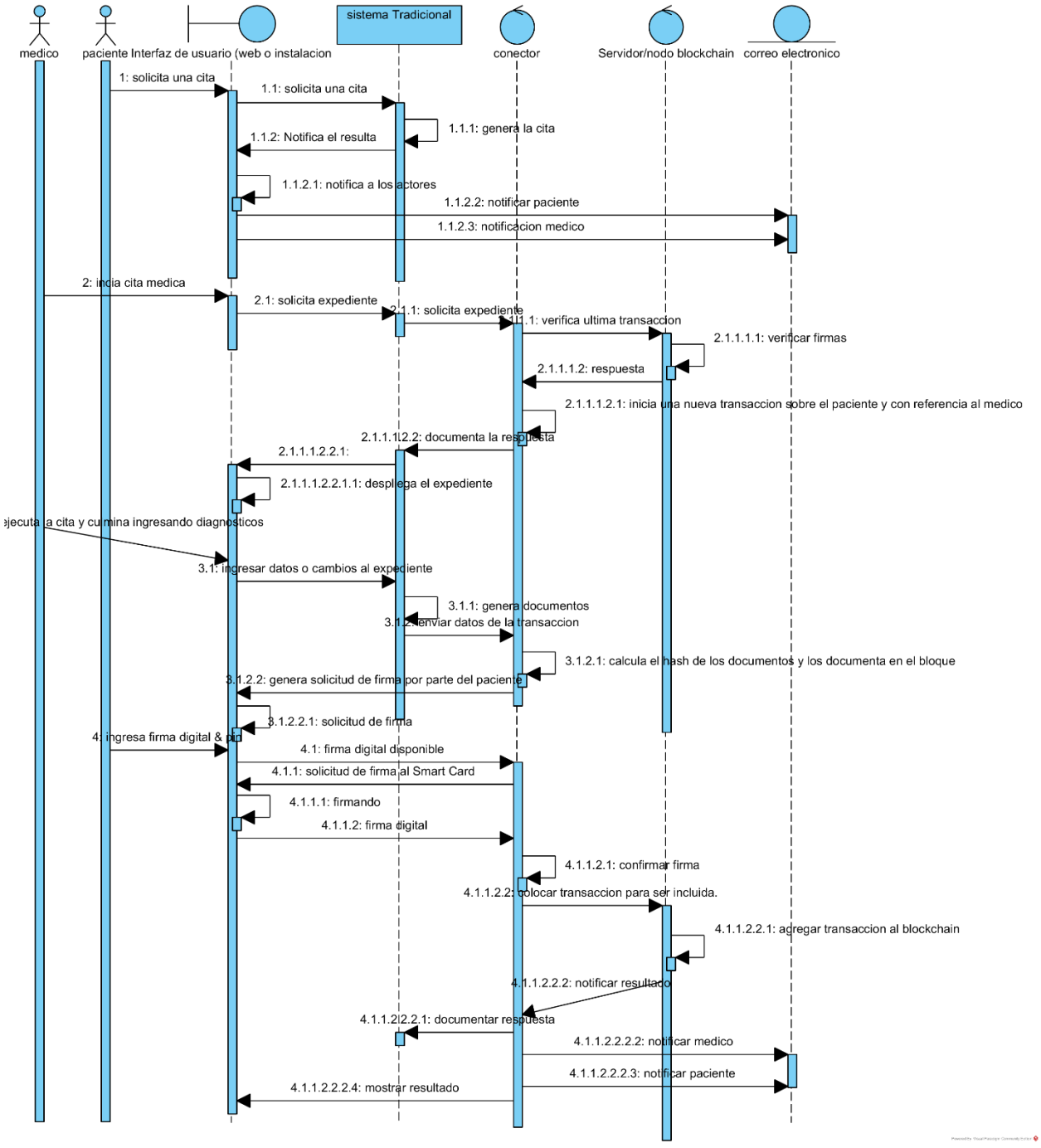

BlockChain Commiter Thread
BlockchainPool
BlockChain_Chain
node
nodeII
NodeIII
node IV
1: ejecute hasta que el servidor sea bring down
osee suficientes transacciones para crear un merkle tree?
2.1: contar transacciones
2.2: boolean: suficientes
2.2.1: enviar nueva solicitud de bloque
2.2.1.1: genera una lista de transacciones a guardar
esta lista podria ser immutable pero aun no es critico
2.2.1.2: proponer lista de transacciones
2.2.1.2.1: generar una copia de la lista (immutable)
2.2.1.2.2: es el primer block en la vida de la cadena? Genesis!
2.2.1.2.3: verificar no hay duplicidad de transacciones
2.2.1.2.4: set timestamp to the proposed block
2.2.1.2.5: hey hay un nuevo bloque
2.2.1.2.6: espera por consesc
3: pre-preparar
4: pre-preparar
5: pre-preparar
3.1: preparar
3.1.1: preparar
3.1.2: prepar
3.1.3: preparar
6: preparar
7: preparar
8: preparar
se omiten lineas, esta face es mas claro en el diagrama de PBFT
8.1: aceptacion/rechaso
8.2: aceptacion/rechaso
8.3: aceptacion/rechaso
8.4: aceptacion/rechaso
8.3.1: aceptacion/rechaso
8.2.1: aceptacion/rechaso
8.1.1: aceptacion/rechaso
8.1.1.1: notificar respuesta
8.1.1.1.1: verificar firma de la autoridad(es) firmante(s)
8.1.1.1.2: borrar nodos del pool
8.1.1.1.3: agregar bloque a la cadena
8.1.1.1.4: notificar resultado

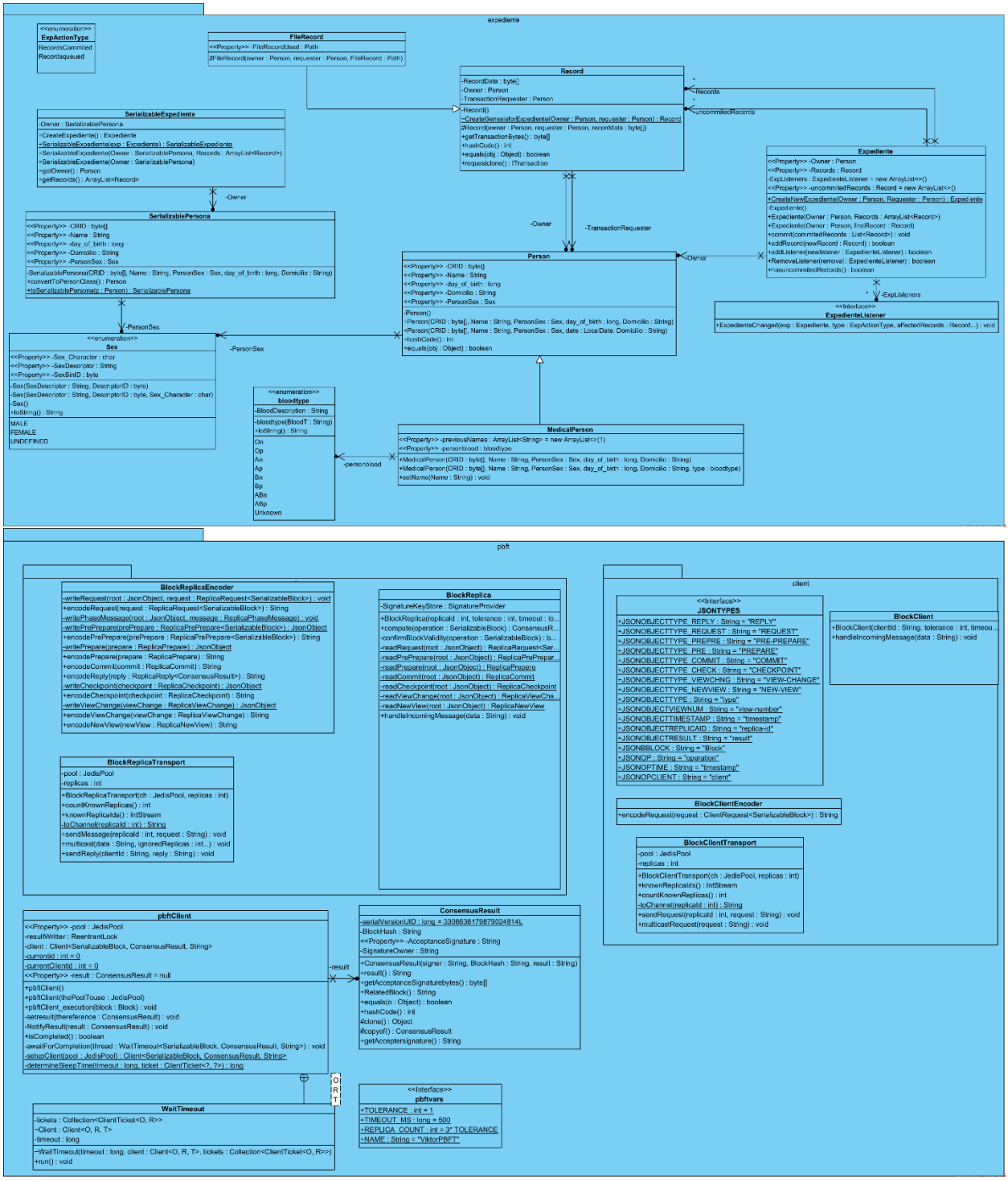

crypto
signature
DevicesHelper
+DEFAULTCLA : int = 0b0000_0000
+GET_CHALLENGE : int = 0x84
+NOPARAM : int = 0b0
+EXPECTED_RESPONSE_BYTES : int = 0x08
+INSTRUCTION_NOT_SUPPORTED : int = 0x6D00
+NO_FURTHER_QUALIFICATIONS : int = 0x9000
+getdevices() : List<CardTerminal>
+hasCard(terminal : CardTerminal) : boolean
DigitalSignatureHelper
+PKCS_SEC_PROVIDER : String = "SunPKCS11"
+FILTER_KEY : String = "filter"
+PKCS_SEC_PROVIDER_LOADED : String = com.aeongames.crypto.signature.DigitalSignatureHelper.PKCS_SEC_PROVIDER
-CONF_FILE : String = "/com/aeongames/blockchain/resources/Pkcs11.properties"
#checkSmartCardIsPresent(pattern : String) : boolean
+LoadSmartCardPKCSProvider() : void
+LoadSmartCardPKCSProvider(FailNotDetected : Optional<Boolean>) : void
+getKeystore(pin : char[]) : KeyStore
#loadInternalProperties(Path : String, classfrom : Class<?>, XML : boolean) : Properties
#getConfigurations(My_properties : Properties) : String
+getSignatureObject_toSign(ks : KeyStore, alias : String, Algorithm : String, SmartCardPin : PasswordProtection) : Signature
+getSignatureObject_toVerify(ks : KeyStore, Algorithm : String, Certificate : Certificate) : Signature
+getSignatureObject_toVerify(SecProvider : Provider, Algorithm : String, Certificate : Certificate) : Signature
+unloadSmartCardPKCSProvider() : void
SignatureProvider
-UnderlineStore : KeyStore
-accesskey : char[]
-RegisteredListeners : ArrayList<EventListener> = null
-CertificateAlias : String
+DEFAULT_ALGORITHM : String
-algorithm : String = com.aeongames.crypto.signature.SignatureProvider.DEFAULT_ALGORITHM
-KeyAlias : String
-SignatureProvider()
+SignatureProvider(CryptoStore : KeyStore, Password : Optional<char[]>, KeyAlias : String, CertificateAlias : String)
+supportSignature() : boolean
+signData(DataToSign : byte[]) : byte[]
+getCertSignature() : byte[]
+VerifyData(SecProvider : Provider, Algorithm : Optional<String>, Certificate : Certificate) : Signature
-SignatureKeyStore
expediente
<<enumeration>>
ExpActionType
RecordsCommited
RecordsRequeued
FileRecord
<<Property>> -FileRecordUsed : Path
#FileRecord(owner : Person, requester : Person, FileRecord : Path)
Record
-RecordData : byte[]
-Owner : Person
-TransactionRequester : Person
-Record()
+CreateGenesisforExpediente(Owner : Person, requester : Person) : Record
#Record(owner : Person, requester : Person, recorddata : byte[])
+getTransactionBytes() : byte[]
+hashCode() : int
+equals(obj) : Object) : boolean
+requestclone() : ITransaction
-Records
-uncommitedRecords
SerializableExpediente
-Owner : SerializablePersona
+CreateExpediente() : Expediente
+SerializableExpediente(exp : Expediente) : SerializableExpediente
+SerializableExpediente(Owner : SerializablePersona, Records : ArrayList<Record>)
+SerializableExpediente(Owner : SerializablePersona)
+getOwner() : Person
+getRecords() : ArrayList<Record>
-Owner
Expediente
<<Property>> -Owner : Person
<<Property>> -Records : Record
-ExpListeners : ExpedienteListener = new ArrayList<>()
<<Property>> -uncommitedRecords : Record = new ArrayList<>()
+CreateNewExpediente(Owner : Person, Requestor : Person) : Expediente
-Expediente()
+Expediente(Owner : Person, Records : ArrayList<Record>)
+Expediente(Owner : Person, firstRecord : Record)
+commit(commitedRecords : List<Record>) : void
+addRecord(newRecord : Record) : boolean
+addListener(newlistener : ExpedienteListener) : boolean
+RemoveListener(removal : ExpedienteListener) : boolean
+hasuncommitedRodords() : boolean
-ExpListeners
SerializablePersona
<<Property>> -CRID : byte[]
<<Property>> -Name : String
<<Property>> -day_of_birth : long
<<Property>> -Domicilio : String
<<Property>> -PersonSex : Sex
-SerializablePersona(CRID : byte[], Name : String, PersonSex : Sex, day_of_birth : long, Domicilio : String)
+convertToPersonClass() : Person
+toSerializablePersona(p : Person) : SerializablePersona
-Owner
-TransactionRequester
Person
<<Property>> -CRID : byte[]
<<Property>> -Name : String
<<Property>> -day_of_birth : long
<<Property>> -Domicilio : String
<<Property>> -PersonSex : Sex
-Person()
+Person(CRID : byte[], Name : String, PersonSex : Sex, day_of_birth : long, Domicilio : String)
+Person(CRID : byte[], Name : String, PersonSex : Sex, date : LocalDate, Domicilio : String)
+hashCode() : int
+equals(obj : Object) : boolean
-Owner
<<Interface>>
ExpedienteListener
+ExpedienteChanged(exp : Expediente, type : ExpActionType, affectedRecords : Record...) : void
-PersonSex
<<enumeration>>
Sex
<<Property>> -Sex_Character : char
<<Property>> -SexDescriptor : String
<<Property>> -SexBinID : byte
-Sex(SexDescriptor : String, DescriptorID : byte)
-Sex(SexDescriptor : String, DescriptorID : byte, Sex_Character : char)
-Sex()
+toString() : String
MALE
FEMALE
UNDEFINED
-PersonSex
<<enumeration>>
bloodtype
-BloodDescription : String
-bloodtype(BloodT : String)
+toString() : String
On
Op
An
Ap
Bn
Bp
ABn
ABp
Unknown
-personblood
MedicalPerson
<<Property>> -previousNames : ArrayList<String> = new ArrayList<>(1)
<<Property>> -personblood : bloodtype
+MedicalPerson(CRID : byte[], Name : String, PersonSex : Sex, day_of_birth : long, Domicilio : String)
+MedicalPerson(CRID : byte[], Name : String, PersonSex : Sex, day_of_birth : long, Domicilio : String, type : bloodtype)
+setName(Name : String) : void


consensus
pbft
replica
BlockReplicaEncoder
-writeRequest(root : JsonObject, request : ReplicaRequest<SerializableBlock>) : void
+encodeRequest(request : ReplicaRequest<SerializableBlock>) : String
-writePhaseMessage(root : JsonObject, message : ReplicaPhaseMessage) : void
-writePrePrepare(prePrepare : ReplicaPrePrepare<SerializableBlock>) : JsonObject
+encodePrePrepare(prePrepare : ReplicaPrePrepare<SerializableBlock>) : String
-writePrepare(prepare : ReplicaPrepare) : JsonObject
+encodePrepare(prepare : ReplicaPrepare) : String
+encodeCommit(commit : ReplicaCommit) : String
+encodeReply(reply : ReplicaReply<ConsensusResult>) : String
-writeCheckpoint(checkpoint : ReplicaCheckpoint) : JsonObject
+encodeCheckpoint(checkpoint : ReplicaCheckpoint) : String
-writeViewChange(viewChange : ReplicaViewChange) : JsonObject
+encodeViewChange(viewChange : ReplicaViewChange) : String
+encodeNewView(newView : ReplicaNewView) : String
BlockReplica
-SignatureKeyStore : SignatureProvider
+BlockReplica(replicaId : int, tolerance : int, timeout : lo...
+compute(operation : SerializableBlock) : ConsensusR...
-confirmBlockValidity(operation : SerializableBlock) : b...
-readRequest(root : JsonObject) : ReplicaRequest<Ser...
-readPrePrepare(root : JsonObject) : ReplicaPrePrepar...
-readPrepare(root : JsonObject) : ReplicaPrepare
-readCommit(root : JsonObject) : ReplicaCommit
-readCheckpoint(root : JsonObject) : ReplicaCheckpoint
-readViewChange(root : JsonObject) : ReplicaViewCha...
-readNewView(root : JsonObject) : ReplicaNewView
+handleIncomingMessage(data : String) : void
BlockReplicaTransport
-pool : JedisPool
-replicas : int
+BlockReplicaTransport(ch : JedisPool, replicas : int)
+countKnownReplicas() : int
+knownReplicaIds() : IntStream
-toChannel(replicaId : int) : String
+sendMessage(replicaId : int, request : String) : void
+multicast(data : String, ignoredReplicas : int...) : void
+sendReply(clientId : String, reply : String) : void
client
<<Interface>>
JSONTYPES
+JSONOBJECTTYPE_REPLY : String = "REPLY"
+JSONOBJECTTYPE_REQUEST : String = "REQUEST"
+JSONOBJECTTYPE_PREPRE : String = "PRE-PREPARE"
+JSONOBJECTTYPE_PRE : String = "PREPARE"
+JSONOBJECTTYPE_COMMIT : String = "COMMIT"
+JSONOBJECTTYPE_CHECK : String = "CHECKPOINT"
+JSONOBJECTTYPE_VIEWCHING : String = "VIEW-CHANGE"
+JSONOBJECTTYPE_NEWVIEW : String = "NEW-VIEW"
+JSONOBJECTTYPE : String = "type"
+JSONOBJECTVIEWNUM : String = "view-number"
+JSONOBJECTTIMESTAMP : String = "timestamp"
+JSONOBJECTREPLICAID : String = "replica-id"
+JSONOBJECTRESULT : String = "result"
+JSONBBLOCK : String = "Block"
+JSONOP : String = "operation"
+JSONOPTIME : String = "timestamp"
+JSONOPCLIENT : String = "client"
BlockClient
+BlockClient(clientId : String, tolerance : int, timeou...
+handleIncomingMessage(data : String) : void
BlockClientEncoder
+encodeRequest(request : ClientRequest<SerializableBlock>) : String
BlockClientTransport
-pool : JedisPool
-replicas : int
+BlockClientTransport(ch : JedisPool, replicas : int)
+knownReplicaIds() : IntStream
+countKnownReplicas() : int
-toChannel(replicaId : int) : String
+sendRequest(replicaId : int, request : String) : void
+multicastRequest(request : String) : void
ConsensusResult
-serialVersionUID : long = 3308638179879024814L
-BlockHash : String
<<Property>> -AcceptanceSignature : String
-SignatureOwner : String
+ConsensusResult(signer : String, BlockHash : String, result : String)
+result() : String
+getAcceptanceSignaturebytes() : byte[]
+RelatedBlock() : String
+equals(o : Object) : boolean
+hashCode() : int
#clone() : Object
#copyof() : ConsensusResult
+getAcceptersignature() : String
<<Interface>>
pbftvars
+TOLERANCE : int = 1
+TIMEOUT_MS : long = 500
+REPLICA_COUNT : int = 3* TOLERANCE
+NAME : String = "ViktorPBFT"
pbftClient
<<Property>> -pool : JedisPool
-resultWriter : ReentrantLock
-client : Client<SerializableBlock, ConsensusResult, String>
-currentId : int = 0
-currentClientId : int = 0
<<Property>> -result : ConsensusResult = null
+pbftClient()
+pbftClient(thePoolTouse : JedisPool)
+pbftClient_execution(block : Block) : void
-setresult(thereference : ConsensusResult) : void
-NotifyResult(result : ConsensusResult) : void
+isCompleted() : boolean
-awaitForCompletion(thread : WaitTimeout<SerializableBlock, ConsensusResult, String>) : void
-setupClient(pool : JedisPool) : Client<SerializableBlock, ConsensusResult, String>
-determineSleepTime(timeout : long, ticket : ClientTicket<?, ?>) : long
-result
WaitTimeout
-tickets : Collection<ClientTicket<O, R>>
-Client : Client<O, R, T>
-timeout : long
+WaitTimeout(timeout : long, client : Client<O, R, T>, tickets : Collection<ClientTicket<O, R>>)
+run() : void
-conectionClient
-ComunicationClient






medico
paciente
Interfaz de usuario (web o instalacion
sistema Tradicional
conector
Servidor/nodo blockchain
correo electronico
1: solicita una cita
1.1: solicita una cita
1.1.1: genera la cita
1.1.2: Notifica el resulta
1.1.2.1: notifica a los actores
1.1.2.2: notificar paciente
1.1.2.3: notificacion medico
2: incia cita medica
2.1: solicita expediente
2.1.1: solicita expediente
2.1.1.1: verifica ultima transaccion
2.1.1.1.1: verificar firmas
2.1.1.1.2: respuesta
2.1.1.1.2.1: inicia una nueva transaccion sobre el paciente y con referencia al medico
2.1.1.1.2.2: documenta la respuesta
2.1.1.2.2.1:
2.1.1.1.2.2.1.1: despliega el expediente
ejecuta la cita y culmina ingresando diagnosticos
3.1: ingresar datos o cambios al expediente
3.1.1: genera documentos
3.1.2: enviar datos de la transaccion
3.1.2.1: calcula el hash de los documentos y los documenta en el bloque
3.1.2.2: genera solicitud de firma por parte del paciente
3.1.2.2.1: solicitud de firma
4: ingresa firma digital & pin
4.1: firma digital disponible
4.1.1: solicitud de firma al Smart Card
4.1.1.1: firmando
4.1.1.2: firma digital
4.1.1.2.1: confirmar firma
4.1.1.2.2: colocar transaccion para ser incluida.
4.1.1.2.2.1: agregar transaccion al blockchain
4.1.1.2.2.2: notificar resultado
4.1.1.2.2.2.1: documentar respuesta
4.1.1.2.2.2.2: notificar medico
4.1.1.2.2.2.3: notificar paciente
4.1.1.2.2.2.4: mostrar resultado


expediente
ExpActionType
RecordsCommited
Recordsqueued
FileRecord
Record
SerializableExpediente
SerializablePersona
Expediente
Person
Sex
bloodtype
MedicalPerson
ExpedienteListener
pbft
BlockReplicaEncoder
BlockReplica
BlockReplicaTransport
client
JSONTYPES
BlockClient
BlockClientEncoder
BlockClientTransport
pbftClient
ConsensusResult
WaitTimeout
pbftvars

5. Licencia Creative Commons

Creative Commons Atribución/Reconocimiento-CompartirIgual 4.0 Licencia Pública Internacional — CC BY-SA 4.0

Al ejercer los Derechos Licenciados (definidos a continuación), Usted acepta y acuerda estar obligado por los términos y condiciones de esta Licencia Internacional Pública de Atribución/Reconocimiento-CompartirIgual 4.0 de Creative Commons ("Licencia Pública"). En la medida en que esta Licencia Pública pueda ser interpretada como un contrato, a Usted se le otorgan los Derechos Licenciados en consideración a su aceptación de estos términos y condiciones, y el Licenciante le concede a Usted tales derechos en consideración a los beneficios que el Licenciante recibe por poner a disposición el Material Licenciado bajo estos términos y condiciones.

Sección 1 – Definiciones.

a. **Material Adaptado** es aquel material protegido por Derechos de Autor y Derechos Similares que se deriva o se crea en base al Material Licenciado y en el cual el Material Licenciado se traduce, altera, arregla, transforma o modifica de manera tal que dicho resultado sea de aquellos que requieran autorización de acuerdo con los Derechos de Autor y Derechos Similares que ostenta el Licenciante. A los efectos de esta Licencia Pública, cuando el Material Licenciado se trate de una obra musical, una interpretación o una grabación sonora, la sincronización temporal de este material con una imagen en movimiento siempre producirá Material Adaptado.
b. **Licencia de adaptador** es aquella licencia que Usted aplica a Sus Derechos de Autor y Derechos Similares en Sus contribuciones consideradas como Material Adaptado de acuerdo con los términos y condiciones de esta Licencia Pública.
c. **Una Licencia Compatible con BY-SA** es aquella que aparece en la lista disponible en creativecommons.org/compatiblelicenses, aprobada por Creative Commons, como una licencia esencialmente equivalente a esta Licencia Pública.
d. **Derechos de Autor y Derechos Similares** son todos aquellos derechos estrechamente vinculados a los derechos de autor, incluidos, de manera enunciativa y no taxativa, los derechos sobre las interpretaciones, las emisiones, las grabaciones sonoras y los Derechos "Sui Generis" sobre Bases de Datos, sin importar cómo estos derechos se encuentren enunciados o categorizados. A los efectos de esta Licencia Pública, los derechos especificados en las secciones 2(b)(1)-(2) no se consideran Derechos de Autor y Derechos Similares.
e. **Medidas Tecnológicas Efectivas** son aquellas medidas que, en ausencia de la debida autorización, no pueden ser eludidas en virtud de las leyes que cumplen las obligaciones del artículo 11 del Tratado de la OMPI sobre Derecho de Autor adoptado el 20 de diciembre de 1996, y/o acuerdos internacionales similares.

f. **Excepciones y Limitaciones** son el uso justo (fair use), el trato justo (fair dealing) y/o cualquier otra excepción o limitación a los Derechos de Autor y Derechos Similares que se apliquen al uso el Material Licenciado.
g. **Elementos de la Licencia** son los atributos que figuran en el nombre de la Licencia Pública de Creative Commons. Los Elementos de la Licencia de esta Licencia Pública son Atribución/Reconocimiento y CompartirIgual.
h. **Material Licenciado** es obra artística o literaria, base de datos o cualquier otro material al cual el Licenciante aplicó esta Licencia Pública.
i. **Derechos Licenciados** son derechos otorgados a Usted bajo los términos y condiciones de esta Licencia Pública, los cuales se limitan a todos los Derechos de Autor y Derechos Similares que apliquen al uso del Material Licenciado y que el Licenciante tiene potestad legal para licenciar.
j. **Licenciante** es el individuo(s) o la entidad(es) que concede derechos bajo esta Licencia Pública.
k. **Compartir** significa proporcionar material al público por cualquier medio o procedimiento que requiera permiso conforme a los Derechos Licenciados, tales como la reproducción, exhibición pública, presentación pública, distribución, difusión, comunicación o importación, así como también su puesta a disposición, incluyendo formas en que el público pueda acceder al material desde un lugar y momento elegido individualmente por ellos.
l. **Derechos "Sui Generis" sobre Bases de Datos** son aquellos derechos diferentes a los derechos de autor, resultantes de la Directiva 96/9/EC del Parlamento Europeo y del Consejo, de 11 de marzo de 1996 sobre la protección jurídica de las bases de datos, en sus versiones modificadas y/o posteriores, así como otros derechos esencialmente equivalentes en cualquier otra parte del mundo.
m. **Usted** es el individuo o la entidad que ejerce los Derechos Licenciados en esta Licencia Pública. La palabra **Su** tiene un significado equivalente.

Sección 2 – Ámbito de Aplicación.

a. **Otorgamiento de la licencia**.
    1. Sujeto a los términos y condiciones de esta Licencia Pública, el Licenciante le otorga a Usted una licencia de carácter global, gratuita, no transferible a terceros, no exclusiva e irrevocable para ejercer los Derechos Licenciados sobre el Material Licenciado para:
        A. reproducir y Compartir el Material Licenciado, en su totalidad o en parte; y
        B. producir, reproducir y Compartir Material Adaptado.
    2. Excepciones y Limitaciones. Para evitar cualquier duda, donde se apliquen Excepciones y Limitaciones al uso del Material Licenciado, esta Licencia Pública no será aplicable, y Usted no tendrá necesidad de cumplir con sus términos y condiciones.
    3. Vigencia. La vigencia de esta Licencia Pública está especificada en la sección 6(a).

4. Medios y formatos; modificaciones técnicas permitidas. El Licenciante le autoriza a Usted a ejercer los Derechos Licenciados en todos los medios y formatos, actualmente conocidos o por crearse en el futuro, y a realizar las modificaciones técnicas necesarias para ello. El Licenciante renuncia y/o se compromete a no hacer valer cualquier derecho o potestad para prohibirle a Usted realizar las modificaciones técnicas necesarias para ejercer los Derechos Licenciados, incluyendo las modificaciones técnicas necesarias para eludir las Medidas Tecnológicas Efectivas. A los efectos de esta Licencia Pública, la mera realización de modificaciones autorizadas por esta sección 2(a)(4) nunca produce Material Adaptado.
5. Receptores posteriores.
    A. Oferta del Licenciante – Material Licenciado. Cada receptor de Material Licenciado recibe automáticamente una oferta del Licenciante para ejercer los Derechos Licenciados bajo los términos y condiciones de esta Licencia Pública.
    B. Oferta adicional por parte del Licenciante – Material Adaptado. Cada receptor del Material Adaptado por Usted recibe automáticamente una oferta del Licenciante para ejercer los Derechos Licenciados en el Material Adaptado bajo las condiciones de la Licencia del Adaptador que Usted aplique.
    C. Sin restricciones a receptores posteriores. Usted no puede ofrecer o imponer ningún término ni condición diferente o adicional, ni puede aplicar ninguna Medida Tecnológica Efectiva al Material Licenciado si haciéndolo restringe el ejercicio de los Derechos Licenciados a cualquier receptor del Material Licenciado.
6. Sin endoso. Nada de lo contenido en esta Licencia Pública constituye o puede interpretarse como un permiso para afirmar o implicar que Usted, o que Su uso del Material Licenciado, está conectado, patrocinado, respaldado o reconocido con estatus oficial por el Licenciante u otros designados para recibir la Atribución/Reconocimiento según lo dispuesto en la sección 3(a)(1)(A)(i).

b. **Otros derechos.**

1. Los derechos morales, tales como el derecho a la integridad, no están comprendidos bajo esta Licencia Pública ni tampoco los derechos de publicidad y privacidad ni otros derechos personales similares. Sin embargo, en la medida de lo posible, el Licenciante renuncia y/o se compromete a no hacer valer ninguno de estos derechos que ostenta como Licenciante, limitándose a lo necesario para que Usted pueda ejercer los Derechos Licenciados, pero no de otra manera.

2. Los derechos de patentes y marcas no son objeto de esta Licencia Pública.
3. En la medida de lo posible, el Licenciante renuncia al derecho de cobrarle regalías a Usted por el ejercicio de los Derechos Licenciados, ya sea directamente o a través de una entidad de gestión colectiva bajo cualquier esquema de licenciamiento voluntario, renunciable o no renunciable. En todos los demás casos, el Licenciante se reserva expresamente cualquier derecho de cobrar esas regalías.

Sección 3 – Condiciones de la Licencia.

Su ejercicio de los Derechos Licenciados está expresamente sujeto a las condiciones siguientes.

a. **Atribución/Reconocimiento**.
   1. Si Usted comparte el Material Licenciado (incluyendo en forma modificada), Usted debe:
      A. Conservar lo siguiente si es facilitado por el Licenciante con el Material Licenciado:
         i. identificación del creador o los creadores del Material Licenciado y de cualquier otra persona designada para recibir Atribución/Reconocimiento, de cualquier manera razonable solicitada por el Licenciante (incluyendo por seudónimo si este ha sido designado);
         ii. un aviso sobre derecho de autor;
         iii. un aviso que se refiera a esta Licencia Pública;
         iv. un aviso que se refiera a la limitación de garantías;
         v. un URI o un hipervínculo al Material Licenciado en la medida razonablemente posible;
      B. Indicar si Usted modificó el Material Licenciado y conservar una indicación de las modificaciones anteriores; e
      C. Indicar que el Material Licenciado está bajo esta Licencia Pública, e incluir el texto, el URI o el hipervínculo a esta Licencia Pública.
   2. Usted puede satisfacer las condiciones de la sección 3(a)(1) de cualquier forma razonable según el medio, las maneras y el contexto en los cuales Usted Comparta el Material Licenciado. Por ejemplo, puede ser razonable satisfacer las condiciones facilitando un URI o un hipervínculo a un recurso que incluya la información requerida.
   3. Bajo requerimiento del Licenciante, Usted debe eliminar cualquier información requerida por la sección 3(a)(1)(A) en la medida razonablemente posible.
b. **CompartirIgual**.

Además de las condiciones de la sección 3(a), si Usted Comparte Material Adaptado producido por Usted, también aplican las condiciones siguientes.

1. La Licencia del Adaptador que Usted aplique debe ser una licencia de Creative Commons con los mismos Elementos de la Licencia, ya sea de esta versión o una posterior, o una Licencia Compatible con la BY-SA.
2. Usted debe incluir el texto, el URI o el hipervínculo a la Licencia del Adaptador que aplique. Usted puede satisfacer esta condición de cualquier forma razonable según el medio, las maneras y el contexto en los cuales Usted Comparta el Material Adaptado.
3. Usted no puede ofrecer o imponer ningún término o condición adicional o diferente, o aplicar ninguna Medida Tecnológica Efectiva al Material Adaptado que restrinja el ejercicio de los derechos concedidos en virtud de la Licencia de Adaptador que Usted aplique.

Sección 4 – Derechos "Sui Generis" sobre Bases de Datos.

Cuando los Derechos Licenciados incluyan Derechos "Sui Generis" sobre Bases de Datos que apliquen a Su uso del Material Licenciado:

a. para evitar cualquier duda, la sección 2(a)(1) le concede a Usted el derecho a extraer, reutilizar, reproducir y Compartir todo o una parte sustancial de los contenidos de la base de datos;
b. si Usted incluye la totalidad o una parte sustancial del contenido de una base de datos en otra sobre la cual Usted ostenta Derecho "Sui Generis" sobre Bases de Datos, entonces ella (pero no sus contenidos individuales) se entenderá como Material Adaptado para efectos de la sección 3(b); y
c. Usted debe cumplir con las condiciones de la sección 3(a) si Usted Comparte la totalidad o una parte sustancial de los contenidos de la base de datos.

Para evitar dudas, esta sección 4 complementa y no sustituye Sus obligaciones bajo esta Licencia Pública cuando los Derechos Licenciados incluyen otros Derechos de Autor y Derechos Similares.

Sección 5 – Exención de Garantías y Limitación de Responsabilidad.

a. **Salvo que el Licenciante se haya comprometido mediante un acuerdo por separado, en la medida de lo posible el Licenciante ofrece el Material Licenciado tal como es y tal como está disponible y no se hace responsable ni ofrece garantías de ningún tipo respecto al Material Licenciado, ya sea de manera expresa, implícita, legal u otra. Esto incluye, de manera no taxativa, las garantías de título, comerciabilidad, idoneidad para un propósito en particular, no infracción, ausencia de vicios ocultos u otros defectos, la exactitud, la**

presencia o la ausencia de errores, sean o no conocidos o detectables. Cuando no se permita, totalmente o en parte, la declaración de ausencia de garantías, a Usted puede no aplicársele esta exclusión.

b. En la medida de lo posible, en ningún caso el Licenciante será responsable ante Usted por ninguna teoría legal (incluyendo, de manera no taxativa, la negligencia) o de otra manera por cualquier pérdida, coste, gasto o daño directo, especial, indirecto, incidental, consecuente, punitivo, ejemplar u otro que surja de esta Licencia Pública o del uso del Material Licenciado, incluso cuando el Licenciante haya sido advertido de la posibilidad de tales pérdidas, costes, gastos o daños. Cuando no se permita la limitación de responsabilidad, ya sea totalmente o en parte, a Usted puede no aplicársele esta limitación.

c. La renuncia de garantías y la limitación de responsabilidad descritas anteriormente deberán ser interpretadas, en la medida de lo posible, como lo más próximo a una exención y renuncia absoluta a todo tipo de responsabilidad.

Sección 6 – Vigencia y Terminación.

a. Esta Licencia Pública tiene una vigencia de aplicación igual al plazo de protección de los Derechos de Autor y Derechos Similares licenciados aquí. Sin embargo, si Usted incumple las condiciones de esta Licencia Pública, los derechos que se le conceden mediante esta Licencia Pública terminan automáticamente.
b. En aquellos casos en que Su derecho a utilizar el Material Licenciado se haya terminado conforme a la sección 6(a), este será restablecido:
    1. automáticamente a partir de la fecha en que la violación sea subsanada, siempre y cuando esta se subsane dentro de los 30 días siguientes a partir de Su descubrimiento de la violación; o
    2. tras el restablecimiento expreso por parte del Licenciante.

    Para evitar dudas, esta sección 6(b) no afecta ningún derecho que pueda tener el Licenciante a buscar resarcimiento por Sus violaciones de esta Licencia Pública.

c. Para evitar dudas, el Licenciante también puede ofrecer el Material Licenciado bajo términos o condiciones diferentes, o dejar de distribuir el Material Licenciado en cualquier momento; sin embargo, hacer esto no pondrá fin a esta Licencia Pública.
d. Las secciones 1, 5, 6, 7, y 8 permanecerán vigentes a la terminación de esta Licencia Pública.

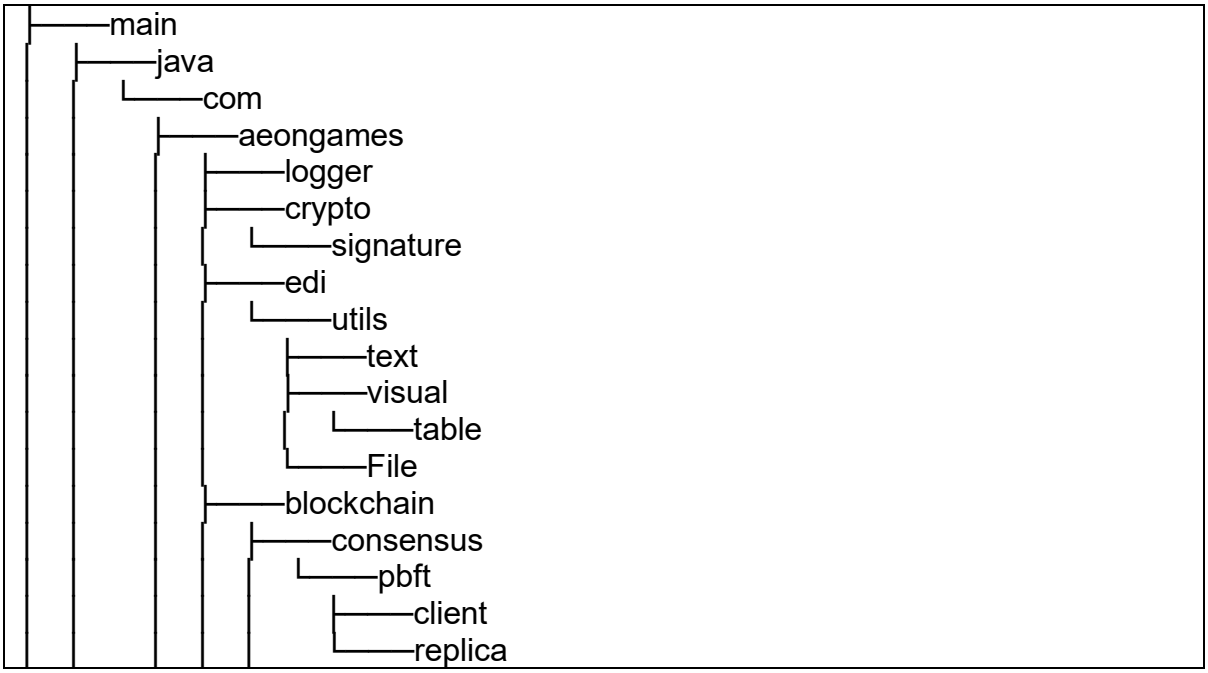
Sección 7 – Otros Términos y Condiciones.

a. El Licenciante no estará obligado por ningún término o condición adicional o diferente que Usted le comunique a menos que se acuerde expresamente.
b. Cualquier arreglo, convenio o acuerdo en relación con el Material Licenciado que no se indique en este documento se considera separado e independiente de los términos y condiciones de esta Licencia Pública.

Sección 8 – Interpretación.

a. Para evitar dudas, esta Licencia Pública no es ni deberá interpretarse como una reducción, limitación, restricción, o una imposición de condiciones al uso de Material Licenciado que legalmente pueda realizarse sin permiso del titular, más allá de lo contemplado en esta Licencia Pública.
b. En la medida de lo posible, si alguna disposición de esta Licencia Pública se considera inaplicable, esta será automáticamente modificada en la medida mínima necesaria para hacerla aplicable. Si la disposición no puede ser reformada, deberá ser eliminada de esta Licencia Pública sin afectar la exigibilidad de los términos y condiciones restantes.
c. No se podrá renunciar a ningún término o condición de esta Licencia Pública, ni se consentirá ningún incumplimiento, a menos que se acuerde expresamente con el Licenciante.
d. Nada en esta Licencia Pública constituye ni puede ser interpretado como una limitación o una renuncia a los privilegios e inmunidades que aplican al Licenciante o a Usted, incluyendo aquellos surgidos a partir de procesos legales de cualquier jurisdicción o autoridad.

6. Código Fuente



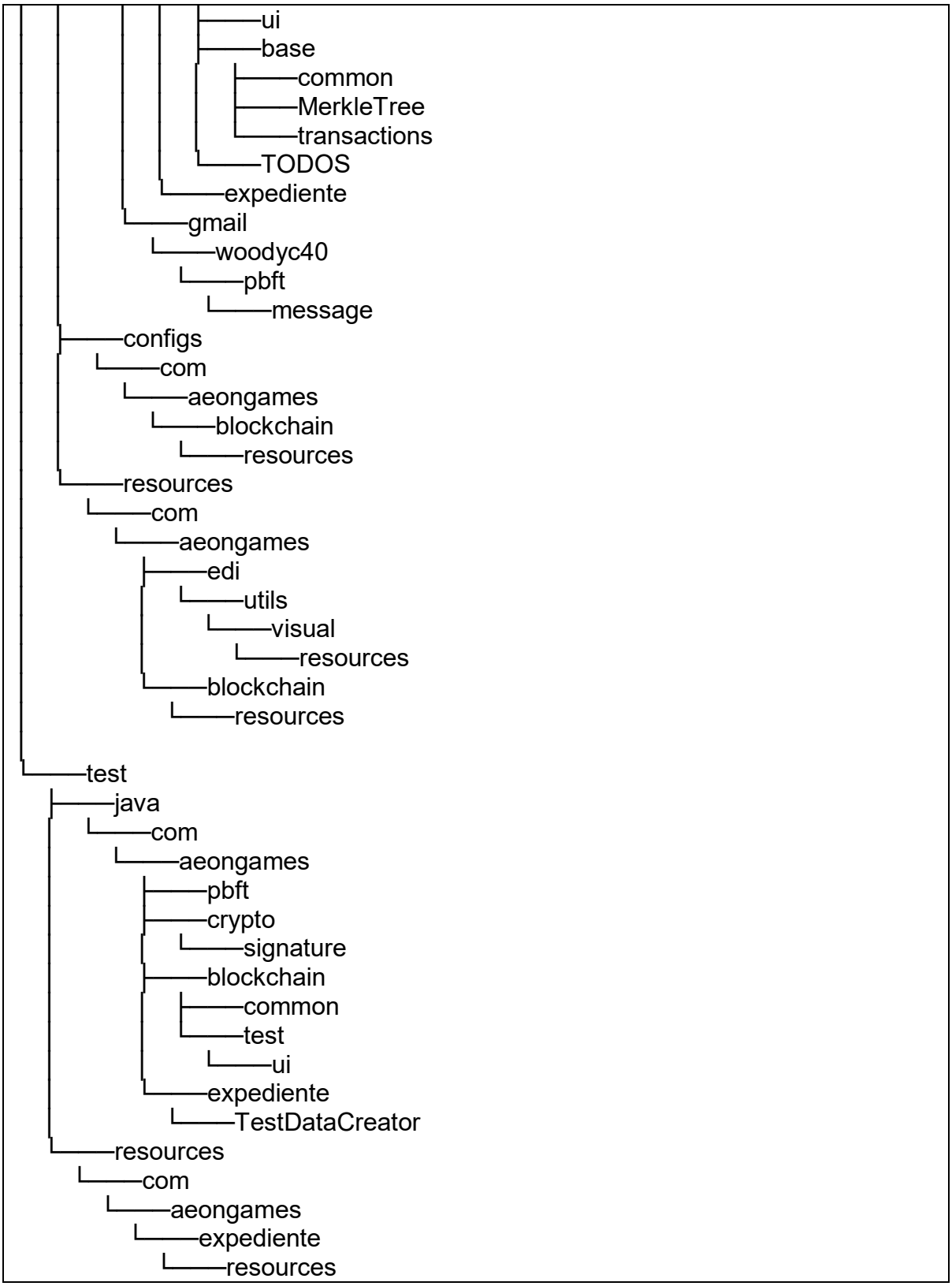


Tabla 9: Estructura de carpetas del proyecto programado.

El código fuente puede ser descargado desde GitHub:

https://github.com/ECartman/Viktor-Blockchain-POC