UNIVERSIDAD DE CUENCA

Facultad de Ingeniería

Maestría en Gestión Estratégica de Tecnologías de la Información

Diseño de una arquitectura de cadena de bloques y uso de contratos inteligentes para mejorar los procesos en las notarías

Trabajo de titulación previo a la obtención del título de Magíster en Gestión Estratégica de Tecnologías de la Información

Autor:

Roberth Fernando Ulloa Banegas

CI: 0105183115

Correo electrónico: roberth.ulloa@gmail.com

Director:

Pablo Leonidas Gallegos Segovia

CI: 0102593589

Cuenca, Ecuador

04-febrero-2022

Resumen

Blockchain se ha convertido en un referente de la seguridad de la información, esto debido a las diversas características que ofrece esta tecnología, captando el interés en su uso por parte de varios investigadores, eliminando el límite de esta a su aplicación dentro de las criptomonedas y expandiendo su intervención en otras áreas como son el Internet de las Cosas, instituciones gubernamentales en países en donde se ha regulado su uso dentro de sus procesos, procesos industriales, etc.

La presente investigación propone el uso de la cadena de bloques como mecanismo sustitutivo del sistema notarial actual, para ello se aplica el uso de contratos inteligentes, en los que se detallan todos los términos o cláusulas de una transacción tradicional, pero con nuevas capacidades y mecanismos de seguridad propios de blockchain debido a sus algoritmos de cifrado nativos, sin la intervención de terceros, la arquitectura propuesta establece los procesos de consenso y distribución del libro mayor en cada uno de los nodos, distribuidos en las diferentes entidades de certificación u organizaciones, así como cada uno de los componentes que intervienen durante el proceso de generación de una nueva transacción que se iniciará con el acuerdo entre un vendedor y un comprador sobre un bien, ya sea un vehículo, una casa, un terreno, etc., buscando también eliminar la intervención de varias entidades estatales en los procesos notariales, además de cumplir con todas las cláusulas de los contratos generados.

Palabras claves: Cadena de Bloques. Contrato Inteligente. Notaría. Arquitectura. Simulación.

Abstract

Blockchain has become a reference point for information security, due to the different characteristics offered by this technology, creating interest in its use by several researchers, eliminating its limits to its application within cryptocurrencies and expanding its intervention in other areas such as the Internet of Things, government institutions in countries where its use has ben regulated within their processes, industrial processes, etc.

The present investigation proposes the use of the blockchain as a replacement mechanism for the current notarial system, the use of smart contracts is applied for this purpose, in which all the terms or clauses of a transaction are detailed, as in a traditional contract, but with new capabilities and security mechanisms specific to blockchain due to its native encryption algorithms, without the intervention of third parties, the proposed architecture establishes the processes of consensus and distribution of the general ledger in each of the nodes, distributed in the different certification entities or organizations, as well as each of the components that intervene during the process of generating a new transaction that will begin with the agreement between a seller an a buyer on a good, whether a vehicle, a house, a land, etc., also seeking to eliminate the intervention of a several state entities in the notarial processes, in addition to complying go fully all the clauses of the contracts generated.

Keywords: Blockchain. Smart Contract. Notary. Architecture. Simulation.

Tabla de contenido

Índice de Figuras

Cláusula de licencia y autorización para publicación en el Repositorio Institucional

Yo, Roberth Fernando Ulloa Banegas en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación "Diseño de una arquitectura de cadena de bloques y uso de contratos inteligentes para mejorar los procesos en las notarías", de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el repositorio institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 04 de febrero del 2022

Roberth Fernando Ulloa Banegas

C.I: 0105183115

Cláusula de Propiedad Intelectual

Yo, Roberth Fernando Ulloa Banegas, autor del trabajo de titulación "Diseño de una arquitectura de cadena de bloques y uso de contratos inteligentes para mejorar los procesos en las notarías", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

Cuenca, 04 de febrero del 2022

Roberth Fernando Ulloa Banegas

C.I: 0105183115

Agradecimientos

Agradezco primeramente a Dios por la salud y la guía para culminar una meta tan importante como la Maestría.

Al Ing. Pablo Gallegos Segovia PhD., por la amistad y por haber estado al pendiente en todo momento del presente proyecto, así como la atención brindada para culminar con el mismo.

A la Universidad de Cuenca por la oportunidad brindada para lograr acceder a la formación de posgrado y culminar esta meta para mi desarrollo profesional.

A mi esposa, mis padres y hermanos por su apoyo incondicional y por su impulso para superarme cada día.

Gracias.

Roberth Fernando Ulloa Banegas

Dedicatoria

Dedico este trabajo de titulación a Dios, por su guía espiritual en cada momento de mi vida, cuidándome y brindándome la fortaleza necesaria para continuar adelante.

A mis padres, quienes siempre han estado al pendiente de mí, por sus valores inculcados en mi persona, por sus enseñanzas y apoyo incondicional en cada etapa de mi vida.

A mis hermanos, con quienes hemos vivido varias experiencias las cuales nos han permitido compartir y apoyarnos mutuamente para lograr cumplir con cada una de nuestras metas tanto personales como familiares.

A mi esposa Gabriela, quien siempre ha estado a mi lado, apoyándome incondicionalmente, gracias por ser un pilar fundamental para cumplir con nuestras metas.

A todas las personas, quienes de manera directa e indirecta han ayudado para que pueda llegar a este punto cumbre en mi vida profesional.

Roberth Fernando Ulloa Banegas

Abreviaciones y Acrónimos

SRI: Servicio de Rentas Internas.

DINARDAP: Dirección Nacional de Registro de Datos Públicos.

ARCOTEL: Agencia de Regulación y Control de las Telecomunicaciones.

IoT: Internet de las Cosas.

ICAT: International Conference on Applied Technologies.

Capítulo 1 – Introducción

En el presente capítulo se detallan los siguientes puntos: antecedentes, la identificación del problema y la solución propuesta con los objetivos generales y específicos. Además, se detalla la metodología usada en el desarrollo del presente trabajo y el artículo para congreso que se ha generado en conjunto con el mismo.

Antecedentes

Según Función Judicial del Ecuador (2014), los notarios son los funcionarios investidos de fe pública para autorizar, a requerimiento de parte, los actos, contratos y documentos determinados en las leyes. Entre algunas de las funciones específicas están las siguientes:

- Autorizar los actos y contratos a que fueren llamados y redactar las correspondientes escrituras, salvo que tuvieren razón o excusa legítima para no hacerlo.
- Protocolizar instrumentos públicos o privados por orden judicial o a solicitud de parte interesada patrocinada por abogado, salvo prohibición legal.
- Autenticar las firmas puestas ante él en documentos que no sean escrituras públicas.

Durante el año 2020, se elabora la resolución 075-2020, mediante el cual se resuelve expedir el reglamento para la implementación progresiva de actos, contratos y diligencias notariales a través del uso de medios electrónicos y reducción de tarifas, en la cual se detalla la progresividad en la prestación del servicio notarial electrónico definiendo los siguientes actos a llevarse a cabo por dichos medios y la validez de estos (Función Judicial del Ecuador, 2020):

- Protocolización de instrumentos públicos o privados por orden judicial o a solicitud de parte interesada.
- Certificación electrónica de documentos desmaterializados.
- Certificación electrónica de documento electrónico original.
- Certificación de documento materializado desde página web o de cualquier soporte electrónico.
- Inscripción de contratos de arrendamiento con la petición firmada electrónicamente por el solicitante.
- Peticiones electrónicas para sentar razones y marginaciones.

Además, se detalla las disposiciones generales como los sistemas a los que los procesos notariales deberán tener acceso para realizar dichos trámites, sin embargo a pesar de las disposiciones y leyes redactadas para esta rama como son las notarías, los procesos siempre resultan demorados, necesitan varios documentos, y en ocasiones los contratos que dan fe los notarios resultan con errores que a su vez provoca ser rechazados en otras instituciones como por ejemplo el Registro de la Propiedad, SRI, etc., lo que conlleva a volver nuevamente a corregir los papeles en cuestión, esto abre un hueco en los procesos que podrían sellarse con el uso de otras tecnologías que

ofrezcan mayor seguridad y optimice las transacciones notariales de tal manera que su uso otorgue facilidades y confiabilidad a la población sobre este servicio que es necesario día a día.

Planteamiento del problema

Los gobiernos tienen la responsabilidad de administrar y mantener registros oficiales tanto de ciudadanos como de empresas. Las aplicaciones habilitadas para blockchain pueden cambiar la forma en que los gobiernos a nivel local o estatal operan al des intermediar las transacciones y el mantenimiento de registros (World Government Summit, 2017). El gobierno además tiene la responsabilidad de automatizar y digitalizar los registros públicos, en sistemas que requieren trazabilidad como transacciones financieras o mercantiles. Y la seguridad que ofrece la cadena de bloques para el manejo de registro público podría eventualmente obstruir la corrupción y hacer que los servicios gubernamentales sean más eficientes. Más aun cuando la veracidad de un documento depende de un individuo y como consecuencia puede ser "interpretada" a conveniencia de una de las partes (World Government Summit, 2017).

Los procesos notariales son obligatorios para poder dar fe por escrito sobre varios procesos, entre estos se encuentran los contratos de compra y venta de un bien como puede ser un vehículo, una casa o un terreno, proceso en el cual intervienen varios entes de gobierno como son DINARDAP, Consejo de la Judicatura, Servicio de Rentas Internas, Registro de la propiedad, entre otras. A pesar de que estos sistemas están interconectados de cierta manera, la información no está compartida entre sí de manera correcta e íntegra. Es por eso, que se vuelve necesario el desarrollar una nueva arquitectura para sustituir al proceso actual, garantizado con esto la reducción de tiempo en los procesos a realizar en las notarías, centralizar de cierta manera la información de la población (personas naturales y jurídicas), mantener la integridad de la información y con esto brindar a la sociedad la seguridad de que sus transacciones tienen un respaldo de sus datos que no podrán ser alterado por terceros.

Solución propuesta

Para llevar a cabo este proyecto, se tiene planificado realizar una investigación literaria sobre el estado actual de los procesos notariales, así como de las tecnologías relacionadas con blockchain y contratos inteligentes.

Posteriormente y partiendo de la investigación, se planteará una arquitectura que permita solventar los problemas que tienen las notarías en los procesos que manejan, buscando mantener siempre la integridad de la información de tal manera que los trámites puedan ser más fáciles y sencillos con el uso de las herramientas detalladas anteriormente.

Finalmente, con los resultados obtenidos se podrá evidenciar cómo funcionan actualmente dichos procesos en esta área gubernamental y también se agregará una alternativa al gobierno digital y a la transparencia de la información con el uso de la tecnología en la propuesta diseñada.

Objetivo general

Plantear una arquitectura basada en cadena de bloques, aplicando el uso de contratos inteligentes para desintermediación de la información modernizando los procesos de las notarías dando transparencia y seguridad a la información.

Objetivos específicos

- Desarrollar una arquitectura de cadena de bloques que permita mantener la integridad de la información en cada transacción notarial.
- Realizar un análisis de Blockchain en el área planteada.
- Plantear un prototipo de evaluación.
- Generar un protocolo de pruebas.
- Evaluar los resultados obtenidos.

Metodología de la investigación

En el presente trabajo se propone realizar una investigación a cerca de los procesos notariales, y una revisión sobre los conceptos relacionados con blockchain y contratos inteligentes con la finalidad de poder diseñar una arquitectura basada en la cadena de bloques que mejore los procesos que se llevan actualmente en las notarías, para el desarrollo de dicha arquitectura se plantea utilizar una metodología de investigación experimental.

De acuerdo con Llopis Castelló (2020), la metodología experimental en una investigación cubre varias etapas del método científico, para esto luego de recolectar la información necesaria se debe hacer una selección sobre que variables deben ser consideradas en el estudio y cómo se van a usar dichas variables en el estudio, en el llamado diseño experimental.

Una vez determinada la forma en que se va a llevar a cabo el experimento o prueba, en el caso de este proyecto, la simulación de la arquitectura y con toda la información obtenida se debe proceder a la generación de la propuesta y luego a configurar el software necesario para iniciar con la simulación y extracción de datos (Llopis Castelló, 2020).

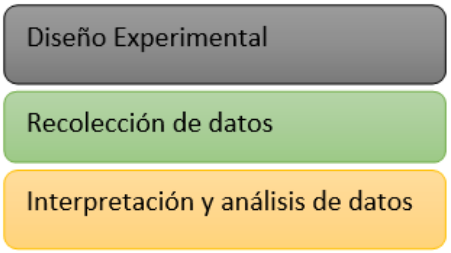

Figura 1 -Etapas del método científico Experimental (Llopis Castelló, 2020)

Estructura del trabajo

Este trabajo de titulación se encuentra estructurado de la siguiente manera:

- Capítulo 1 – Introducción: en esta sección se definen los antecedentes, el planteamiento del problema y la propuesta de la solución, además, se detallan los objetivos tanto general como los específicos, la metodología de investigación utilizada en el desarrollo del proyecto de tesis y el artículo científico elaborado en base al mismo.
- Capítulo 2 – Marco teórico: aquí se describen los conceptos necesarios para entender el presente trabajo, también se desarrolla el estado del arte a cerca de la aplicación de blockchain en diferentes proyectos los cuales se relacionan con este documento.
- Capítulo 3 – Arquitectura propuesta: en este capítulo se detalla todo el proceso desarrollado para plantear la arquitectura con cada uno de sus componentes y su funcionamiento. Además, se genera un protocolo de pruebas, así como también la evaluación de los resultados obtenidos en las mismas.
- Capítulo 4 – Conclusiones y trabajo futuro: En este capítulo se presentan las conclusiones obtenidas de la investigación y se proponen trabajos futuros para complementar la misma.

Aporte científico

A partir del presente proyecto de titulación, se desarrolló un artículo científico presentado en una conferencia, a continuación, se detalla el nombre de este y la conferencia en la cual fue expuesto:

“Design of a blockchain architecture and use of smart contracts to improve processes in notary offices”, presentado en ICAT 2021: International Conference on Applied Technologies (Ulloa Banegas & Gallegos Segovia, 2021).

Capítulo 2 – Marco teórico

En este capítulo se dan a conocer los conceptos relacionados a las diferentes tecnologías que son utilizados en el desarrollo de este trabajo de titulación. Dichos conceptos permitirán tener un mayor entendimiento a cerca de varios temas que se darán a conocer durante el desarrollo del mismo.

Conceptos

Blockchain

La tecnología blockchain se creó como respuesta a la crisis de confianza que azotó al mundo a raíz de los problemas financieros de 2008 que se ha atribuido a la quiebra de instituciones confiables como bancos y otras instituciones financieras.

Esta tecnología surge como una posible solución a la erosión de la credibilidad en las instituciones tradicionales eliminando la necesidad de confianza entre las partes, con blockchain los usuarios se someten a la autoridad de un sistema tecnológico que da la seguridad de ser inmutable independientemente del fin para el que se utilice una cadena de bloques pública (Mannan & Reijers, 2020).

Según Lakshimi Siva Sindhu & Sethumadhavan (2017), blockchain es un libro mayor distribuido, transparente e inmutable, de acuerdo con este autor, un protocolo llamado protocolo de consenso forma parte del núcleo de la cadena de bloques, es este núcleo es quien decide cómo funciona blockchain.

El libro mayor se mantiene actualizado por participantes llamados mineros, ejecutando un protocolo que mantiene la estructura de datos conocida como cadena de bloques. Una de las ventajas que tiene esta tecnología es el proporcionar un conjunto inicial de argumentos con el cual se pueden prevenir ataques o irregularidades de tal manera que el atacante no pueda reorganizar la cadena de bloques a su forma inicial (Garay, Kiayias, & Leonardos, 2015).

Componentes de blockchain

De acuerdo con Yahari Navarro (2019), la tecnología está basada en cuatro fundamentos: el registro de las transacciones (ledger), el consenso para verificar las transacciones, un contrato que determina las reglas de funcionamiento de las transacciones y finalmente la criptografía, que es el funcionamiento de todo, a continuación, se detallan los componentes que permiten a la cadena de bloques funcionar:

1. **Bloques:** La cadena de bloques es un registro de todas las transacciones que se empaquetan en bloques que los mineros luego se encargan de verificar, posteriormente

es agregado a la cadena una vez que se termine su validación y distribuido a todos los nodos que forman la red. Un bloque está conformado por (Yahari Navarro, 2019):

- Un código alfanumérico que lo enlaza con el bloque anterior.
- El paquete de transacciones.
- Otro código alfanumérico que enlazará con el siguiente bloque.

2. **Mineros:** Son ordenadores dedicados que aportan su poder computacional a la red para verificar las transacciones que se llevan a cabo. Son computadoras que se encargan de autorizar la adición de los bloques de transacción, para lograr todo esto deben cumplir los siguientes puntos (Yahari Navarro, 2019):
    - Las nuevas transacciones se transmiten a todos los nodos.
    - Cada nodo de la minería recoge nuevas transacciones en un bloque.
    - Cada nodo minero trabaja en la búsqueda de una prueba de trabajo para su bloque.
    - Cuando un nodo de la minería encuentra una prueba de trabajo, este transmite al bloque a todos los nodos.
    - Los demás nodos aceptan el bloque solo si todas las transacciones son válidas y no se hayan gastado.
    - Los nodos expresan su aceptación del bloque trabajando en la creación del próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash anterior.
3. **Nodos:** Son computadoras conectadas a la red utilizando un software que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques. Cada vez que un bloque se valida y se añade a la cadena, el cambio es comunicado a todos los nodos y este se añade a la copia que cada uno almacena (Yahari Navarro, 2019).

Tipos de blockchain

Según Preisegger, Muñoz, Pasini, & Pesado (2019), existen tres tipos de blockchain:

1. **Públicas:** No hay restricciones para la lectura de datos ni para la realización de operaciones por parte de los usuarios.
2. **Privadas:** La lectura de datos y las operaciones sobre la red están limitadas a participantes determinados, los participantes deben obtener permisos por parte de un administrador de la red para poder utilizarla.
3. **Federadas o híbridas:** Utiliza lo mejor de las soluciones de las blockchain públicas y privadas, existen determinadas organizaciones que se encargan de administrar la red y mantener las copias del registro sincronizadas, el acceso a la red se hace mediante una interfaz web que los administradores ponen a disposición del usuario brindando al mismo tiempo un acceso controlado y libertad.

Características de blockchain

Según Preisegger, Muñoz, Pasini, & Pesado (2019), en función de los tipos estructurales de blockchain se presentan las siguientes características:

- **Administración:** La estructura de blockchain va a determinar de forma directa su administración, la misma puede ser centralizada, semi-centralizada o descentralizada.
- **Persistencia:** Cada transacción que se extiende por la red blockchain debe ser validada por todos los nodos, para esto se agrupan en bloques con otras transacciones para que puedan ser confirmados y registrados en la cadena.
- **Identificación:** En base al tipo de estructura de blockchain la identificación puede variar, en las privadas o híbridas se requiere la identificación de los usuarios para obtener permisos mientras que en las públicas se permite la interacción a través de la utilización de claves generadas por lo que un usuario no se identifica con sus datos personales.
- **Auditabilidad:** Las transacciones de todos los tipos se validan y registran con una marca de tiempo, los usuarios según su nivel de permisos pueden verificar y rastrear fácilmente los registros anteriores accediendo a cualquiera de los nodos de la red.
- **Participación:** Esta característica determina el grado de intervención que se permite a cada usuario que actúa en la red.
- **Transparencia:** En función del nivel de participación y del modo de administración, se obtendrá un determinado grado en el nivel de transparencia de la blockchain. Esto determinará si cualquier persona puede velar por la integridad de la información contenida en la red o no.

Smart Contracts

La cuarta revolución industrial trajo el blockchain en la cual dentro de sus grandes utilidades y formas de aplicación que se le han dado a este sistema destacan los contratos inteligentes, los cuales consisten en un programa informático que ejecuta acuerdos establecidos entre dos o más partes contratantes, buscado que ciertas acciones sucedan o no como resultado del cumplimiento o incumplimiento de una serie de condiciones específicas y ya pactadas. Algo sobresaliente en todo esto es que no se necesita de un tercero que verifique si los hechos han sucedido o no, esto se vuelve totalmente revolucionario en el ámbito jurídico por lo que en un futuro se espera que no sea necesario ir ante un tercero cada vez que se quiera validar o dar fe de un contrato (Valencia Ramírez, 2019).

Según Figueroa Castillo et ál. (2021), blockchain en conjunto con los contratos inteligentes son tecnologías que pueden ayudar a combatir la corrupción considerado actualmente como un problema social, esto es posible debido a la seguridad y la base del sistema descentralizado convirtiéndose en el cimiento de los contratos inteligentes, estos dos conceptos son alternativas prometedoras con las cuales la sociedad puede erradicar la corrupción que es un grave problema que ha estado vinculado siempre a la política de los diferentes países.

Atributos de un Contrato Inteligente

De acuerdo con Ortega Pérez (2019), un contrato inteligente cuenta con tres atributos a destacar respecto de los negocios habituales:

1. **Son acuerdos autoejecutables:** Implica que, si las condiciones predefinidas en el programa se cumplen, la consecuencia contractual se ejecuta de manera autónoma.
2. **Son acuerdos digitales:** Este atributo permite que se halle en blockchain y que pueda ser interpretado tanto por humanos como por máquinas, dicha interpretación consiste en que las máquinas puedan leerlo y ejecutarlo.
3. **Son acuerdos descentralizados:** Evita al intermediario y proporciona veracidad y seguridad gracias a la tecnología de la cadena de bloques.

Notario

De acuerdo con Naranjo Acosta (2018), se lo cataloga como una persona versada en derecho y posesionario de fe pública emanada del gobierno a través del respectivo órgano legal. El Consejo de la Judicatura es el responsable de la selección y delegación de la fe pública a los notarios en el Ecuador.

Según Chico González (2018), el notario público realiza una función pública delegada por el estado que consiste en servir a la sociedad como un testigo imparcial en acuerdos que consten por escrito, tomando juramentos, certificando documentos e identificando a las partes dentro de un contrato. A todas estas actividades se les llama actos notariales.

Estado del arte

En la presente sección se detalla la información más relevante sobre la revisión de la literatura que trata sobre proyectos que se relacionan con el presente trabajo de titulación, y sobre los cuales se tratan los diferentes usos que se le puede dar a la tecnología blockchain en la actualidad.

Durante los últimos años, se han realizado varias investigaciones relacionadas a la aplicación de blockchain y contratos inteligentes, esto debido a que su uso no se limita solamente al ámbito de las criptomonedas, sino que puede ser utilizado en otras áreas que son cotidianas en el diario vivir de la sociedad.

De acuerdo a Schuschny (2017), Blockchain puede contribuir al desarrollo y certificación de los sistemas de generación distribuida entre otras posibles aplicaciones en el ámbito de la energía eléctrica, con la creación del Bitcoin, posterior a esto se pudo determinar que esta tecnología no solo se puede usar en el mundo de las criptomonedas sino que también es posible su integración en diversas aplicaciones y en incontables ámbitos de la actividad económica, basadas en la tecnología sobre la cual se asienta el Bitcoin. Un uso particular para esta tecnología es dentro de las operaciones de notarización y certificación que, hasta hoy, son realizadas por los escribanos o

notarios quienes actúan como agentes fedatarios. Diferentes tipos de transacciones y registros como matrimonios, escrituración de propiedades, custodio de activos financieros, certificados de nacimiento, registro y transferencia de activos, de propiedad intelectual o física como automóviles, patentes, testamentos, auditorías contables, podrían certificarse a través de sistemas basados en blockchain.

De la misma manera, según Moreno Ballesteros (2019), propone un proyecto de investigación y desarrollo de servicios estructurados para mejorar los procesos académicos y administrativos a nivel de gestión de datos en la educación superior implementando tecnologías descentralizadas de libro contable. Este proyecto tiene como objetivo acreditar los logros académicos de forma segura, descentralizar la gestión de recursos académicos y desarrollar un sistema de incentivos para la creación de conocimientos y redes expandidas de apoyo para las universidades, para lograr esto, se propone el uso del software de código abierto llamado Tendermint (Tendermint, 2021) que consta de dos piezas principales: un motor de consensos quienes decidirán si los bloques generados son válidos o no y una interfaz de aplicación genérica. También detalla la gobernanza que tendrá el sistema, en este caso una blockchain federada para que opere bajo el mando de varias instituciones académicas, se escoge este tipo de blockchain debido a que las arquitecturas federadas son más rápidas al momento de transaccionar además de ofrecer una mayor escalabilidad y proporcionar privacidad en las transacciones.

Otro tema muy investigado de acuerdo con Eterovic, Cipriano Marcelo, García, & Torres (2020), es la aplicación de blockchain en IoT (Internet de las Cosas), uno de los mayores retos al que se enfrenta la seguridad en IoT proviene de la propia arquitectura del sistema actual, debido a que este se basa en un modelo cliente-servidor a través de la nube, ante lo cual, sumando también el aumento del uso de estas tecnologías provoca que los dispositivos se vuelvan vulnerables ante posibles ataques maliciosos debido a las pocas capacidades o características que dichos dispositivos tienen a diferencia de equipos más robustos como celulares, computadores, tablets. Una solución para este efecto puede ser el uso de blockchain debido a la capacidad de gestionar, controlar y asegurar los equipos de IoT en conjunto con contratos inteligentes para potenciar su beneficio logrando de esta manera anular cualquier intento de ataque malicioso hacia una red con equipos IoT.

Otro estudio realizado por García Mateo (2018), indica que cada vez la sociedad reclama una mayor transparencia, participación y cooperación ciudadana entre las partes en materia de actividades públicas que competen a las administraciones en el sector público, por lo que blockchain entra en un debate social en distintos sectores e industrias por la amplitud de servicios, oportunidades y desafíos que pueden ofrecer. La complejidad de esta tecnología es un tema que muchos gobiernos están empezando a explotar para desarrollar diversas plataformas que favorezcan al sistema de sus estados buscando aumentar la confianza de la población en los diferentes entes estatales, este autor concluye que existen varias referencias actuales sobre blockchain, sin embargo, pocas de ellas se aplican en los procesos de las entidades públicas a pesar del interés que tienen los diferentes gobiernos en el uso de esta tecnología.

En el estudio de Ferrer-Sapena & Sánchez Pérez (2019), se busca revolucionar el contexto tecnológico de la documentación científica mediante el uso de blockchain, presentando un panorama actualizado de las iniciativas basadas en blockchain para la gestión de la documentación científica y tecnológica, destacando aquellos aspectos que hacen de esta tecnología una herramienta diferente y novedosa. En este artículo se concluye que la mayor parte de los proyectos que usan la tecnología de la cadena de bloques están relacionados con las áreas detalladas anteriormente. Sin embargo, se encuentran también iniciativas en otros sectores relacionados al ámbito tecnológico como la ingeniería química y la agricultura. También da a conocer que el mayor peligro para el uso de nuevas tecnologías como lo es blockchain es que las entidades económicas que actualmente controlan el mercado (las editoriales en el caso de la documentación científica), se apoderen de las iniciativas para provocar un monopolio en esta área.

Otros estudios se centran también a detallar de manera más profunda la aplicación de blockchain dentro del manejo de documentos no solo científicos como el estudio anterior, sino también en la gestión de documentos legales como es el caso de García Morales (2017), en el cual indica que blockchain en los diferentes campos de aplicación en los que se puede utilizar y la forma en que queden documentados los registros de las transacciones, tendrán importantes implicaciones en cómo se crean, almacenen y gestionen los documentos en el futuro. Blockchain tiene como uno de sus propósitos el producir y mantener registros y/o documentos que sean garantía de las transacciones, con el paso de los años se espera que aparezcan nuevos tipos de documentos electrónicos en los que se diluye aún más la ya débil frontera entre datos y documentos basados en los Smart Contracts.

Sin embargo, existen aún más campos sin explorar en los cuales se podría implementar la tecnología de blockchain con contratos inteligentes, para esto se debe diseñar una arquitectura que se adapte a los diferentes procesos de cada una de las áreas a estudiar, este es el caso de los procesos notariales en el Ecuador, en el cual se necesita una arquitectura que cumpla con todos los procesos en los cuales están inmersos varias entidades estatales y que hacen que la información pueda ser vulnerada y usada con fines ilegales.

Capítulo 3 – Diseño de Arquitectura

Actualmente las notarías públicas cuyo ente de regulación en el Ecuador es el Consejo de la Judicatura, han tratado de centralizar en parte los procesos que realizan, sin embargo, la información necesaria para realizar los trámites se encuentra esparcida entre varias entidades de gobierno, para lo cual se necesita de varios procesos de validación de información y registrar los cambios o transacciones en cada uno de los sistemas a los que se debe recurrir durante un proceso notarial.

Anteriormente luego de realizar por ejemplo un contrato de compraventa de un vehículo, se debía acudir posteriormente al SRI, proceso que en la actualidad ya no es necesario debido a la conectividad que existe con esta entidad, sin embargo, continúa siendo tedioso al ser un trámite demorado y que necesita de varia documentación y aún más al momento de realizar un contrato de compraventa de un bien inmueble, para el cual se debe acudir a otras entidades externas tanto antes como después del proceso notarial, todo esto provoca errores tanto en el registro de la información en el sistema, como también en el documento impreso que se entrega a los usuarios, los mismos que en algunas ocasiones deben ser corregidos nuevamente en la notaría en la cual se realizó el trámite.

Funcionamiento Actual de las Notarías

Para poder tener un mayor entendimiento a cerca de los procesos notariales, se realizó una investigación sobre cómo funciona o cómo se lleva a cabo los procesos notariales en dos casos específicos, estos son el proceso de compraventa de un vehículo y el proceso de compraventa de un terreno o casa.

Proceso de compraventa de un vehículo

Para realizar un contrato de compraventa de un vehículo en el Ecuador, en la notaría debe seguirse los pasos que se listarán a continuación, aquí se detallan cada una de las instituciones que intervienen en el proceso.

1. Ingreso al sistema del SRI en el cual se debe registrar los datos del vehículo y del vendedor, este paso permite al notario conocer si los datos registrados concuerdan con la información almacenada en la base de datos del Servicio de Rentas Internas.
2. Una vez que se valide que la información es correcta se realiza una consulta de información en el Consejo de la Judicatura y la DINARDAP (Dirección Nacional de Registro de Datos Públicos) registrando las calidades (Vendedor y Comprador).
3. Una vez registrada la información de las calidades, se imprime el documento con la información de estos (Vendedor y Comprador), el cual debe validarse si es correcto o no lo es.

4. Luego de impreso y validado el documento del Consejo de la Judicatura, se procede a la elaboración del contrato de compraventa con la información obtenida tanto del SRI como del Consejo de la Judicatura.
5. Al momento de redactar el contrato, también se debe registrar el valor de la transacción en la base de datos de avalúos del SRI y del Consejo de la Judicatura.
6. A continuación, se realiza una nueva verificación de datos en la base de datos del Registro Civil.
7. Se procede a la Certificación y firma del Notario en el documento.
8. Después se genera un ticket de pago para realizarlo en la caja, dicho ticket es generado en el Consejo de la Judicatura.
9. Con el ticket generado se procede a realizar el pago en la caja de la Notaría, si se procesa el pago correctamente se confirma la actualización de la información con los nombres del nuevo dueño del vehículo en el SRI y en el Consejo de la Judicatura. Sin embargo, puede darse el caso en el que exista algún problema por el cual no se pueda proceder con el pago, si esto ocurre debe revisarse nuevamente la información del vehículo en el SRI e identificar porque no se puede proceder con la venta, con la información detallada de la situación, los usuarios deben solucionar este problema para volver a generar el documento de compraventa.

Como se puede observar, el proceso es extenso y muchas de las veces se redunda con los pasos a seguir ya que se vuelve a validar algún tipo de información que ya fue verificado anteriormente, de la misma manera se necesita de demasiadas entidades públicas para poder completar el proceso, en este caso las que intervienen son el SRI, Consejo de la Judicatura, DINARDAP y Registro Civil lo que lo vuelve poco óptimo en el manejo de datos a este tipo de transacción notarial, en la Figura 2 se detalla los pasos listados anteriormente para una mejor comprensión.

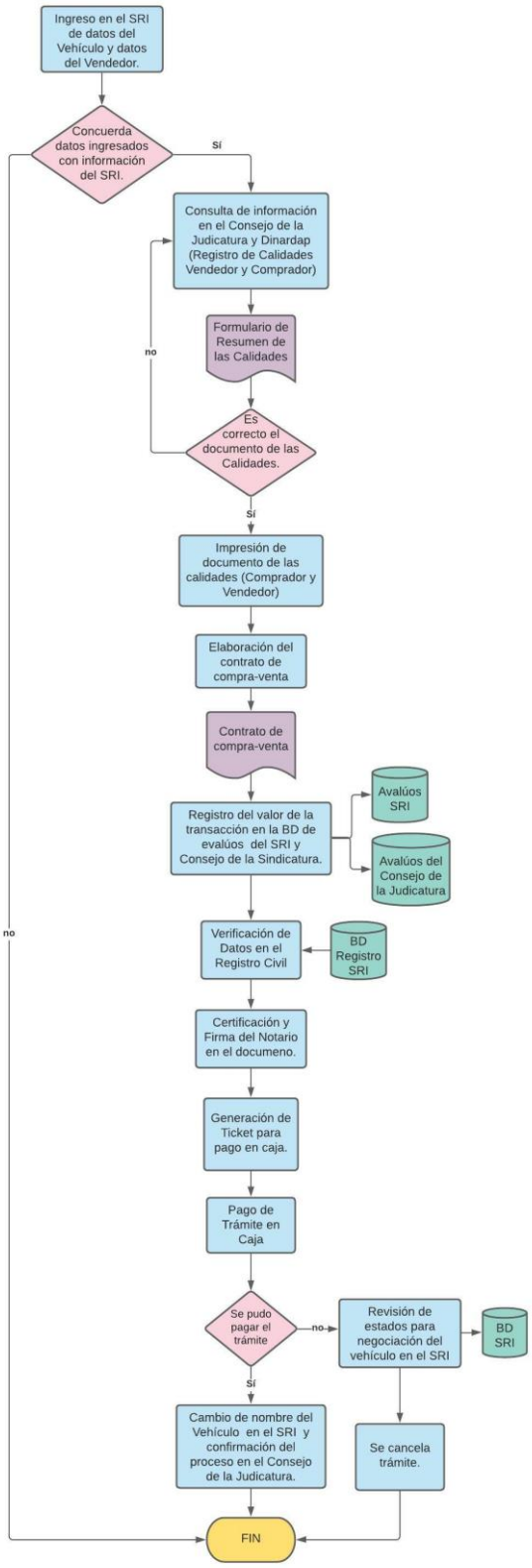

Figura 2 -Diagrama del proceso de compraventa de un vehículo

Proceso de compraventa de una casa o terreno

Para el proceso de compraventa de una casa o terreno, el proceso notarial es parecido en algunos pasos al de los vehículos, sin embargo, intervienen otras entidades, dicho proceso se detalla a continuación:

1. Pago de alcabalas y plusvalía en el Municipio.
2. Consulta de datos personales de las calidades (Vendedor y Comprador) en la Dirección Nacional de Registro de Datos Públicos (DINARDAP).
3. Ingreso de datos de las calidades y el valor de la propiedad en el Consejo de la Judicatura.
4. Luego del registro de esta información, se procede a imprimir el formulario de resumen de las calidades.
5. Si la información es correcta, se define si la propiedad es una casa o un terreno.
6. Posteriormente se debe identificar el valor más alto entre el valor ingresado y el registrado en la carta predial.
7. Tras definir los valores, se genera un Extracto Notarial y se procede a la elaboración de las escrituras.
8. Tras la firma de las escrituras se procede a ingresar el trámite en el Registro de la Propiedad.
9. Luego se debe verificar los datos en el sistema del Registro Civil.
10. Después se procede a la Certificación y firma del notario en el documento.
11. Finalmente se genera el ticket de pago para proceder con la cancelación de los valores en la caja.
12. Tras realizar el pago se da por terminado el trámite notarial, sin embargo, el comprador debe terminar el proceso acercándose personalmente al Registro de la Propiedad y posteriormente al municipio para cambiar de dueño la propiedad.

Este trámite también está compuesto de varios pasos y varias entidades, en este caso del Registro de la Propiedad y el municipio, lo que al igual que en el caso de los vehículos se vuelve susceptible a errores en la información, en la Figura 3 se detalla este proceso para un mejor entendimiento.

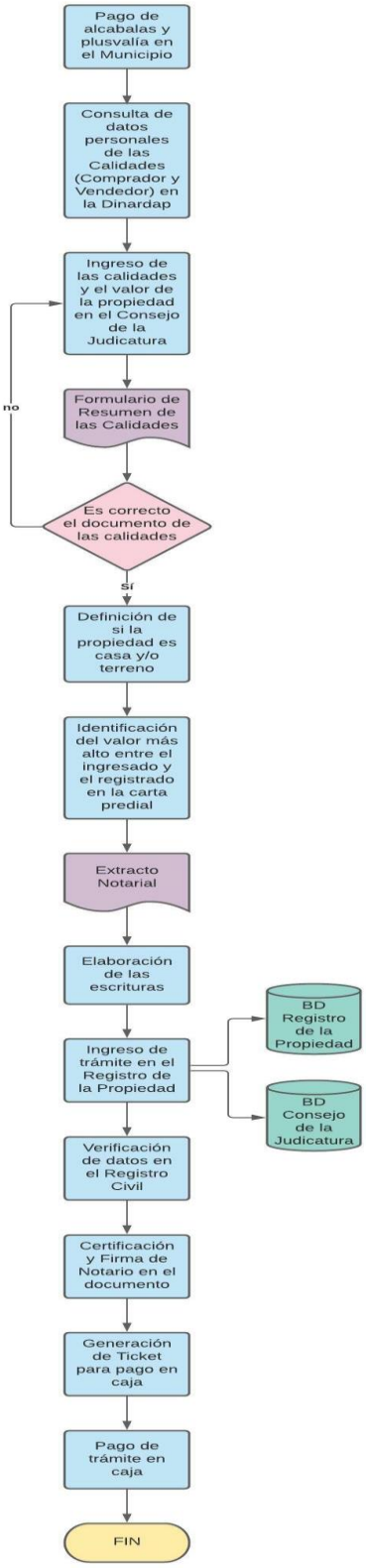

Figura 3 -Diagrama del proceso de compraventa de un terreno o casa

Desarrollo de la Arquitectura

Para desarrollar la arquitectura que cumpla con todos los requisitos necesarios para sustituir los procesos actuales, es necesario tratar de dividir en capas a la cadena de bloques, posteriormente se debe detallar los componentes que conformarán esta arquitectura y las entidades que regularán su funcionamiento.

Capas de Blockchain

Según Singhal, Dhameja, & Sekhar Panda (2018) y Vintimilla Tapia, y otros (2020), todavía no existen estándares en común que especifiquen claramente los componentes de la cadena de bloques en varias capas, sin embargo, se realiza una formulación de capas de blockchain para poder comprender mejor la tecnología y construir una analogía comparativa entre las variantes de blockchain y criptomonedas que existen actualmente, para esto se han identificado cinco capas que se detallan a continuación:

1. **Capa de Aplicación:** En esta capa se codifican las diferentes funcionalidades que pueden ser necesarias para los diferentes procesos, por lo general implica un conjunto de tecnología tradicional para el desarrollo de software como construcciones de programación al lado del cliente, es posible que estos desarrollos deban alojarse en algunos servidores web debido a que será la capa que interactúe directamente con los usuarios.
2. **Capa de Ejecución:** En esta capa se lleva a cabo la ejecución de las diferentes instrucciones ordenadas por la capa de aplicación en todos los nodos de una red blockchain, los cuales deberán ejecutar los diferentes scripts de forma independiente, es importante considerar que siempre serán los mismos datos de entrada para cada nodo al igual que la salida será la misma en cada uno de ellos.
3. **Capa Semántica:** Es una capa lógica debido a que existe un orden entre las transacciones y los bloques de la cadena, posee un conjunto de instrucciones que pasa por la capa de ejecución, pero las mismas se validan en la capa semántica, aquí también se definen las diferentes reglas del sistema, así como los modelos y las estructuras de datos.
4. **Capa de Propagación:** Esta es la capa de propagación entre las partes que permite a los nodos identificarse unos a otros y comunicarse entre sí, aquí los nuevos bloques generados por cada transacción son difundidos en toda la red para que pueda ser conocido por todos los nodos de esta para su posterior validación.
5. **Capa de Consenso:** El objetivo de esta capa es conseguir que todos los nodos de la red se pongan de acuerdo en un estado coherente del libro contable, la seguridad de blockchain se garantiza en esta capa ya que cada nodo indicará si el nuevo bloque generado es válido o no ante lo cual dependerá si dicho bloque es o no aceptado y por consiguiente agregado o no a la cadena de bloques.

Como se puede apreciar, cada una de las capas en las que divide el autor citado tiene una función específica dentro del proceso de validación del nuevo bloque, dicha composición de la cadena de bloques resulta interesante y válida para partir desde este punto con el desarrollo de la arquitectura que cubra todos los requerimientos que cumplen actualmente las notarías del país.

Capas de Blockchain en Procesos Notariales

Luego de analizar cada una de las capas de las que está compuesta blockchain, se define que, para la arquitectura de este proyecto, se utilicen cuatro de las cinco capas listadas anteriormente.

En la Figura 4 se identifican las capas a utilizar en la arquitectura para manejarlas en los diferentes procesos notariales.

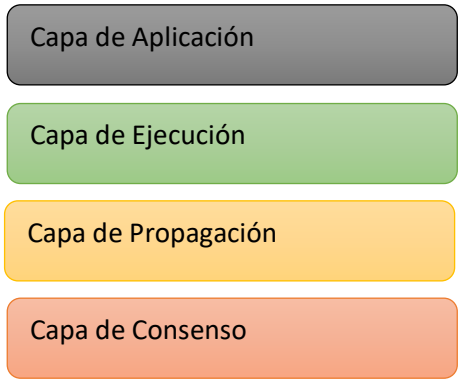

Figura 4 -Capas de Blockchain a utilizar en la arquitectura para procesos notariales

A continuación, se detalla la función que cumplirá cada una de las capas dentro de la arquitectura con el uso de los contratos inteligentes:

- **Capa de Aplicación:** En esta capa se encontrará la aplicación a la cual se deberán acceder tanto el comprador como vendedor para iniciar el proceso de la negociación, lo cual permitirá cerrar la venta del bien (Vehículo, Terreno o Casa), para esto, el vendedor deberá ingresar con sus datos personales al sistema en el cual se encuentra la información de la propiedad de la misma que es de conocimiento general para los diferentes nodos que acceden al libro mayor, esta capa se la podría comparar con las billeteras de criptomonedas que son usadas actualmente.
- **Capa de Ejecución:** Esta capa permitirá introducir en la arquitectura el uso de los contratos inteligentes, es en esta sección en la cual se generarán los contratos inteligentes con las diferentes cláusulas o instrucciones que posteriormente deberán ejecutarse para dar el cumplimiento a este tipo de documento, todo esto deberá realizarse antes de generar el nuevo bloque, dicha ejecución puede ser realizada por cualquiera de los nodos de la red de blockchain y de la misma manera cada uno de los nodos deberá tener conocimiento de

estas ejecuciones lo que quiere decir que cada paso o proceso que se dé, deberá ser presentado inmediatamente a los demás integrantes de la arquitectura.

- **Capa de Propagación:** En esta capa luego de haber terminado la ejecución del contrato inteligente elaborado en la capa anterior y de haber dado a conocer a todos los nodos la culminación de este proceso, uno de los nodos actuará de minero generando el nuevo bloque el cual estará compuesto por el nuevo hash, el hash anterior y registrando los datos actualizados de la propiedad del cual se trata la transacción, a continuación el bloque deberá ser enviado como copias hacia los demás nodos de la red.
- **Capa de Consenso:** Finalmente en esta capa, todos los nodos al recibir el nuevo bloque generado deberán validar el mismo, así como la cadena ya existente a cerca del bien y posteriormente llegar a un acuerdo para agregar o no dicho bloque al libro mayor, es importante recalcar que, para agregar este nuevo bloque, todos los nodos deben estar de acuerdo con la validación del bloque en cuestión.

Entidades Consideradas en el Proceso

Con la arquitectura a presentarse a continuación, se pretende limitar la intervención de varios organismos del estado de tal manera que solo necesiten de las Entidades de control principales para cada tipo de contrato de compraventa (SRI, Registro de la Propiedad) que son las encargadas de mantener la información actualizada en su base de datos y adicionalmente las Entidades de Certificación de Información existentes en el Ecuador, es importante recalcar que estas entidades certificadoras serán transparentes para los usuarios debido a que su función será la de actuar como los nodos de la red blockchain.

De acuerdo con Torres Torres & Ramírez Arenas (2017), las entidades de certificación llevan a cabo varias actividades, como son, emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas y emitir certificados sobre la verificación respecto a la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, todas estas actividades deben ser realizadas a cabalidad por dichas instituciones ya que de no hacerlo, se afectan los derechos de los suscriptores. Al ser responsables de varias actividades relacionadas con la parte informática y electrónica, se ha considerado importante que estas instituciones sean las que se encarguen de la validación de los bloques ya que adicionalmente cuentan con autorizaciones del estado para realizar sus operaciones en el país y están comprendidas no solo entidades del sector público sino también del sector privado, lo que brinda imparcialidad en el proceso.

A continuación, se indican las Entidades de Certificación que funcionan actualmente en el Ecuador según ARCOTEL Ecuador (2020):

- Banco Central del Ecuador.
- Registro Civil.
- Consejo de la Judicatura.

- ANFAC Autoridad de Certificación del Ecuador C.A.
- UANATACA Ecuador S.A.
- Security Data Seguridad en Datos y Firma Digital S.A.

Contrato Inteligente

En el contrato inteligente se deberá especificar cada una de las acciones a ejecutar para cargar la información necesaria para la transacción, esto dependerá del tipo de bien que se vaya a negociar, el precio de la transacción que se debe cancelar al Consejo de la Judicatura y la validación del valor a pagar por la compra del bien, dicha información se encontrará registrada en los bloques anteriores, así como en el nuevo a generarse en la transacción actual.

Existen varias herramientas o lenguajes de programación que hacen posible desarrollar la lógica necesaria de un contrato inteligente para su cumplimiento, a continuación, en la Figura 5 se muestra un ejemplo sencillo de un contrato inteligente, las funciones listadas en dicho ejemplo son solamente para tener un mayor contexto de cómo debería armarse este tipo de código.

```
1
2 public class SmartContract {
3
4   public String getVendedor () {
5         return vendedor();
6   }
7
8   public void setComprador(String datosComprador) {
9       String datosCompradorActual = datosComprador;
10  }
11
12  public String getNuevoDuenio () {
13      return nuevoDuenio();
14  }
15
16  public String getDatosPropiedad () {
17      return datosPropiedad();
18  }
19
20  public void setValorPropiedad(Integer valorPropiedad) {
21      Integer valorActualPropiedad = valorPropiedad;
22  }
23
24  public void setValorTransaccion (Integer valorTransaccion) {
25      Integer valorUltimaTransacion = valorTransaccion;
26  }
27
28 }
```

Figura 5 -Ejemplo de código de un contrato inteligente

El código que se desarrolla dentro de un contrato inteligente debe ejecutarse cada vez que se cumpla las condiciones de este, para que se genere el nuevo bloque y con esto dar por finalizada

la transacción, es necesario que todas las cláusulas se cumplan, caso contrario la compraventa del bien no se podrá llevar a cabo, en la figura 6 se muestra un ejemplo sencillo sobre cómo debe funcionar un contrato electrónico en la arquitectura a desarrollar en el presente trabajo.

Figura 6 -Funcionamiento de un Contrato Inteligente

Arquitectura

Para comenzar, es importante indicar que el tipo de blockchain para la arquitectura a desarrollar será de tipo privada, esto debido a que cualquier persona podrá acceder a la red siempre y cuando tenga alguna propiedad como casa, terreno y/o vehículo es decir que no todos los usuarios tendrán acceso a la misma hasta que sea dueño de algún bien, además, deberán tener autorización por parte de las entidades estatales que en este caso serán el Servicio de Rentas Internas y el Registro de la Propiedad para poder acceder a su información.

En la capa de aplicación como ya se detalló en las secciones anteriores, se permitirá a las calidades (Vendedor y Comprador) generar una nueva transacción por la compraventa de una propiedad, posteriormente en la capa de ejecución se procederá a elaborar y ejecutar el contrato inteligente con las diferentes cláusulas, las cuales deberán llevarse a cabo y cumplirse por completo para que se pueda generar el nuevo bloque con la información del nuevo dueño de la propiedad, finalmente, tras terminar la ejecución de todo el contrato, un nodo minero en la capa de propagación deberá generar el nuevo bloque con la siguiente información:

- Hash Anterior, para relacionar al nuevo bloque con el bloque actual.

- Hash Nuevo, generado y asignado al nuevo bloque de la transacción, si se genera un nuevo proceso de compraventa, este hash pasará a ser el hash anterior del último bloque existente.
- Contrato inteligente en el cual se encuentran las cláusulas ejecutadas en el proceso de compraventa, dicho contrato deberá haber cumplido todas las condiciones para que pueda generarse el siguiente bloque de la cadena.
- Información sobre el dueño actual y el dueño anterior, esto como resultado del contrato inteligente, esta información podría servir para dar una trazabilidad a las diferentes transacciones realizadas en base a los bienes existentes.

Una vez que se haya generado el nuevo bloque, este se deberá enviar a todos los nodos de la red, quienes en la capa de consenso verificarían que no exista anomalías en el nuevo bloque y agregarlo a la cadena para mantener actualizado el libro mayor con todas las transacciones el mismo al que tendrán acceso todas las Entidades de Certificación (Nodos de la red blockchain) luego de la distribución del bloque en toda la red.

Es importante considerar que, al ser una arquitectura nueva, el nodo génesis de la cadena de bloques de cada una de las propiedades será generado inicialmente por el Servicio de Rentas Internas (SRI) para el caso de los vehículos, mientras que el Registro de la Propiedad hará lo mismo en el caso de ser un terreno o casa. Esto se debe a que dichas entidades de gobierno son quienes deberán mantener actualizada la información de las diferentes propiedades una vez que el nuevo bloque sea agregado en la cadena por cada transacción de compraventa.

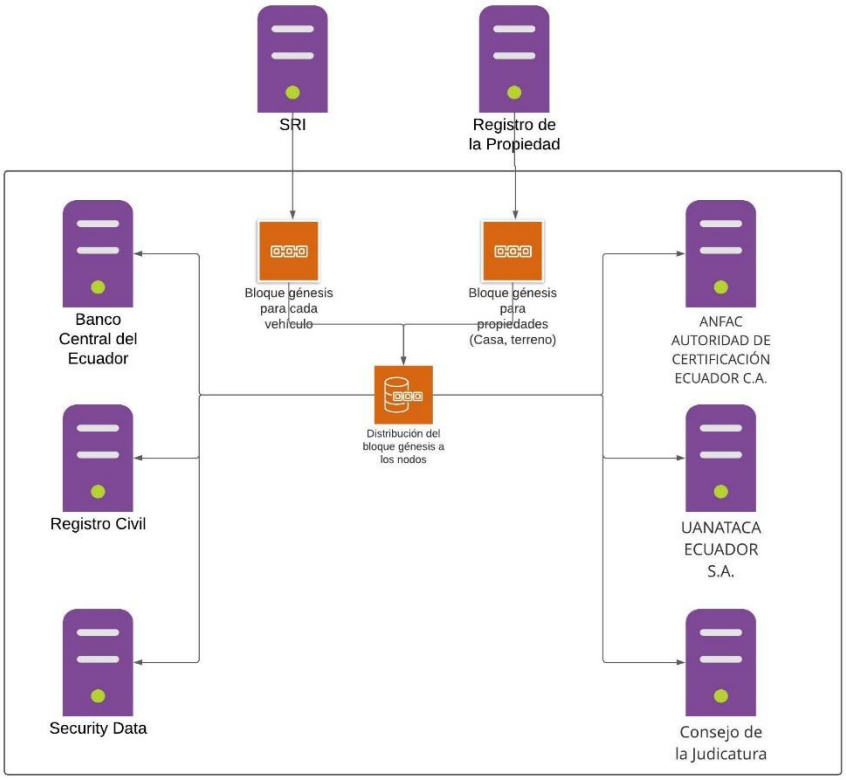

Figura 7 -Diagrama de generación del bloque génesis y su distribución a los nodos de la red

En la Figura 8, se puede observar de manera global el proceso de generación de una nueva transacción de compraventa, en el mismo se especifica cada uno de los componentes que intervienen en el proceso de la nueva transacción entre las partes logrando de esta manera completar una acción sin la intervención de terceras personas, así como eliminando la necesidad de utilizar o llamar a varias instituciones para el registro, validación y corrección de la información lo que a su vez ocasionaba demoras en el proceso.

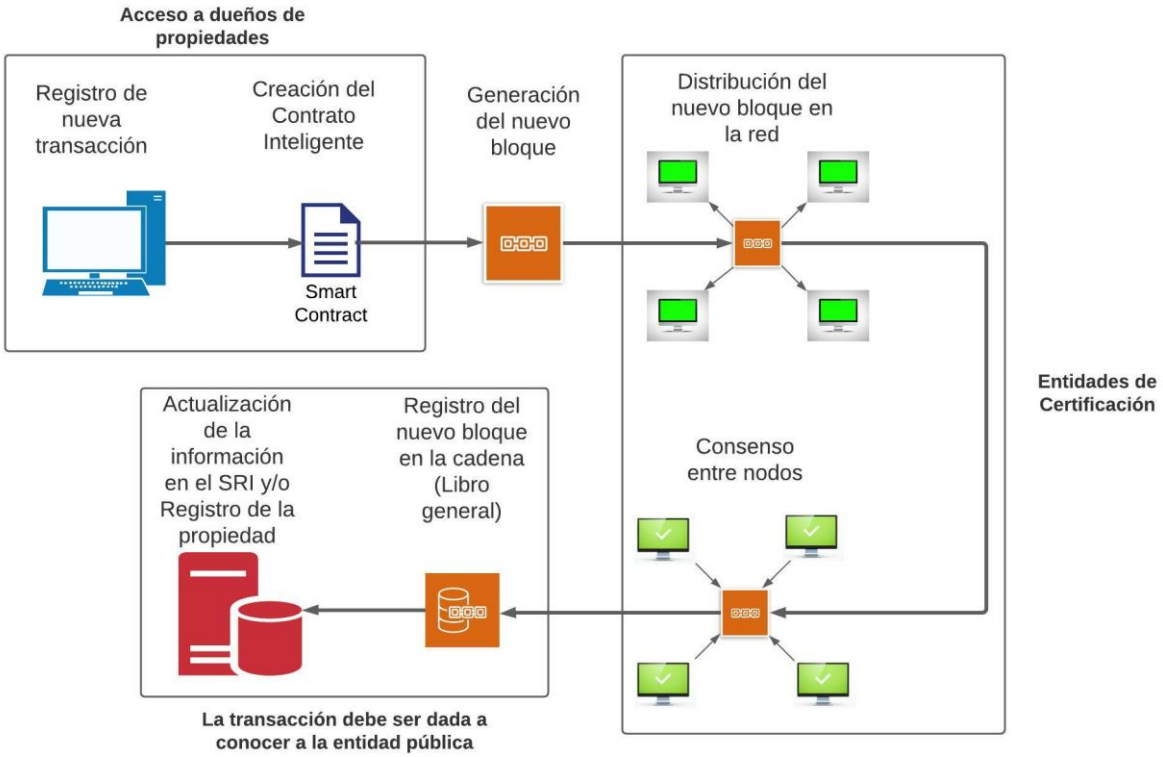

Figura 8 -Proceso global de la arquitectura para el registro de una nueva transacción de compraventa de un bien

Detalle de la Arquitectura Propuesta

Como se indicó en las secciones anteriores, la arquitectura de blockchain necesaria para cumplir con el trabajo de las notarías deberá estar compuesto por cuatro capas, las mismas que se detallan en la Figura 9, en la cual se puede observar lo siguiente:

- **Capa de Aplicación:** Se necesitan del comprador y el vendedor para iniciar la transacción, una vez definido a estos actores, se utilizará un software que estará implementado y funcionando en la web en el cual será necesario la autenticación para iniciar con el proceso de compraventa.
- **Capa de Ejecución:** Con los acuerdos generados entre las calidades, se generará el contrato inteligente y posteriormente se ejecutará el mismo para que se cumpla a cabalidad lo dispuesto en el mismo, finalmente se creará el nuevo bloque.
- **Capa de Propagación:** El bloque se distribuye a todos los nodos.
- **Capa de Consenso:** En esta capa a la cual pertenecen las entidades de certificación del Ecuador que actúan de nodos en la red, decidirán si el nuevo bloque es válido para ser agregado a la cadena y posteriormente actualizar el libro mayor.

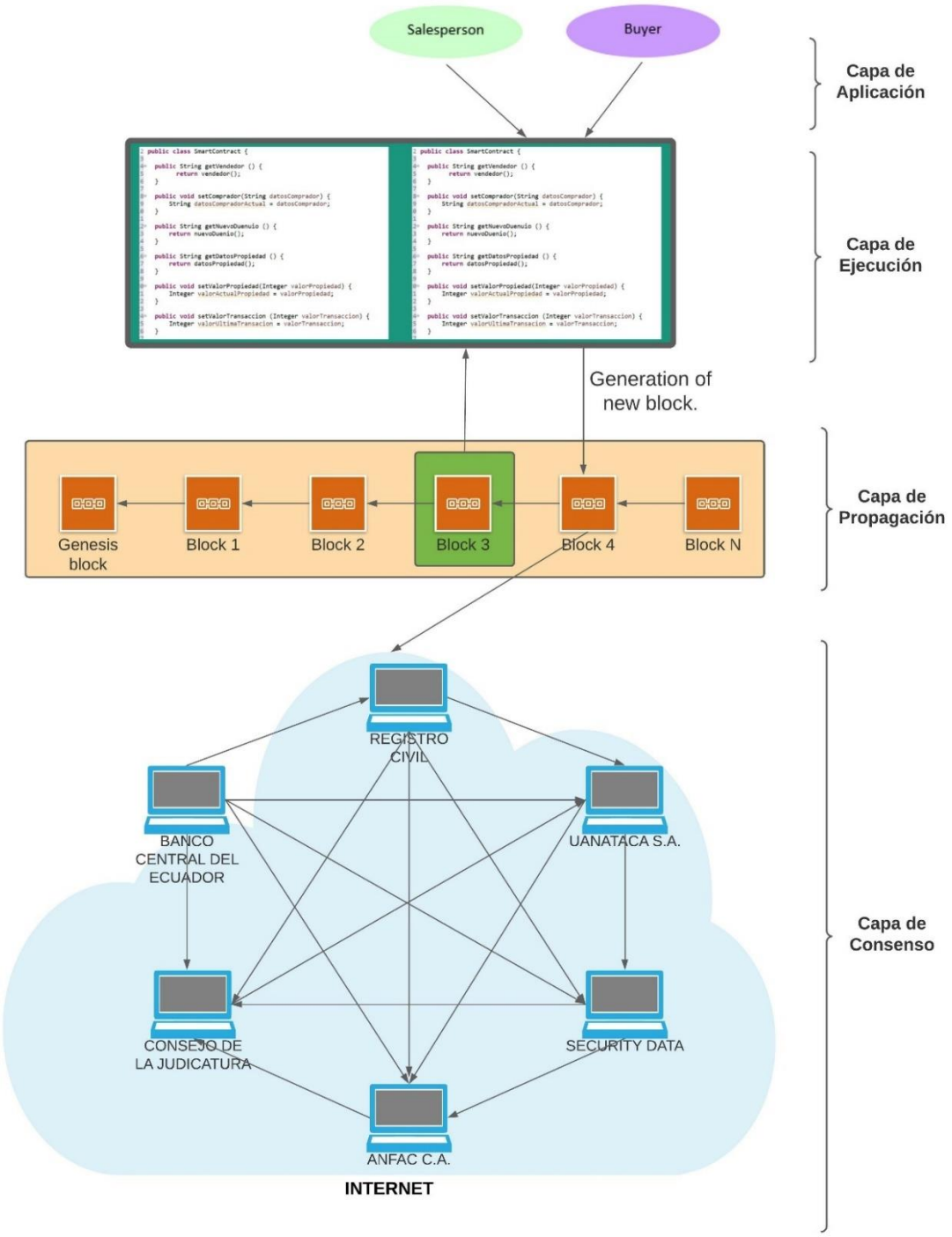

Figura 9 -Arquitectura propuesta de blockchain para las Notarías Detallado por Capas

Experimento de Simulación

Luego de detallar el diseño de la arquitectura planteada, se procede a evaluar la misma mediante la simulación de varias transacciones de compraventa sobre un mismo bien, es necesario indicar

que no existen métricas definidas para el uso de blockchain en los procesos notariales, ante esto, en la prueba se procedió a analizar el proceso de la generación de los bloques ejecutando y generando 100 transacciones con diferentes contratos inteligentes, es decir cambiando la información básica del contrato como son los nombres del comprador, vendedor y valor de la propiedad además de la manera en la que se agregan dichos bloques en la cadena.

Para llevar a cabo la simulación para poner a prueba la arquitectura diseñada, se necesita utilizar el siguiente software: Ganache versión 2.5.4, Truffle versión 5.3.14 y node js versión 16.4.2.

El proceso de instalación de cada una de las herramientas es el siguiente.

Node js

Esta herramienta está ideada como un entorno de ejecución de JavaScript orientado a eventos asíncronos, Node.js está diseñado para crear aplicaciones network de red escalables (Open JS Foundation, s.f.), en este caso esta herramienta fue utilizada para poder ejecutar los contratos inteligentes en la simulación realizada.

El proceso de instalación se lo realiza de la siguiente manera:

1. Se debe descargar el instalador de la página web: https://nodejs.org/es/download/
2. Al terminar la descarga se debe ejecutar el archivo de instalación en el cual al iniciar con el proceso aparecerá la pantalla de la Figura 10.

Figura 10 -Pantalla inicial de instalación de Node js

3. Posteriormente se debe aceptar los términos de la licencia, en la Figura 11 se puede observar una captura de pantalla de esto.

Figura 11 -Pantalla de términos de licencia para el uso de Node JS

4. A continuación, se debe seleccionar la ruta en donde se va a instalar la herramienta, en la Figura 12 se puede observar este paso.

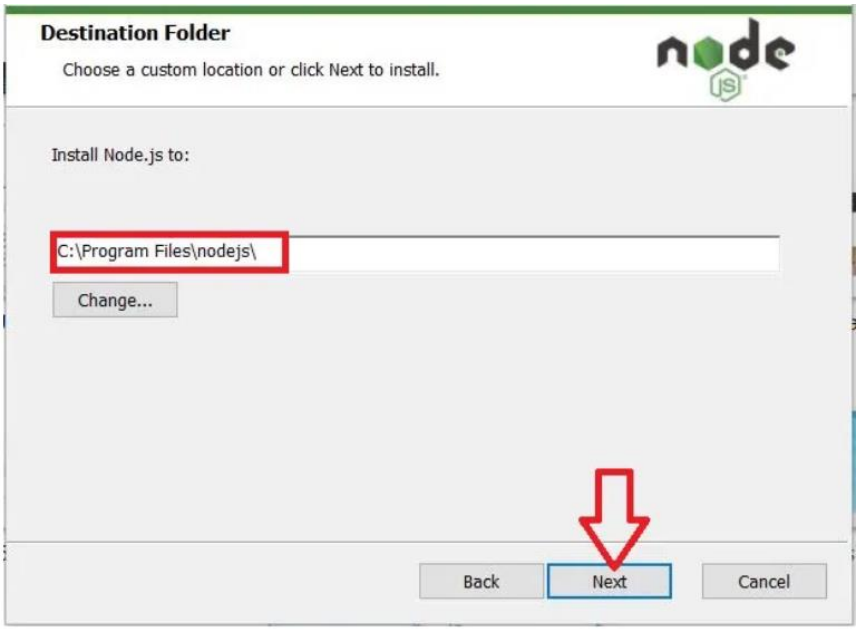

Figura 12 -Pantalla de selección de ruta para instalación

5. Finalmente aparecerá la última pantalla del proceso en la cual se debe hacer clic sobre el botón “Install”.

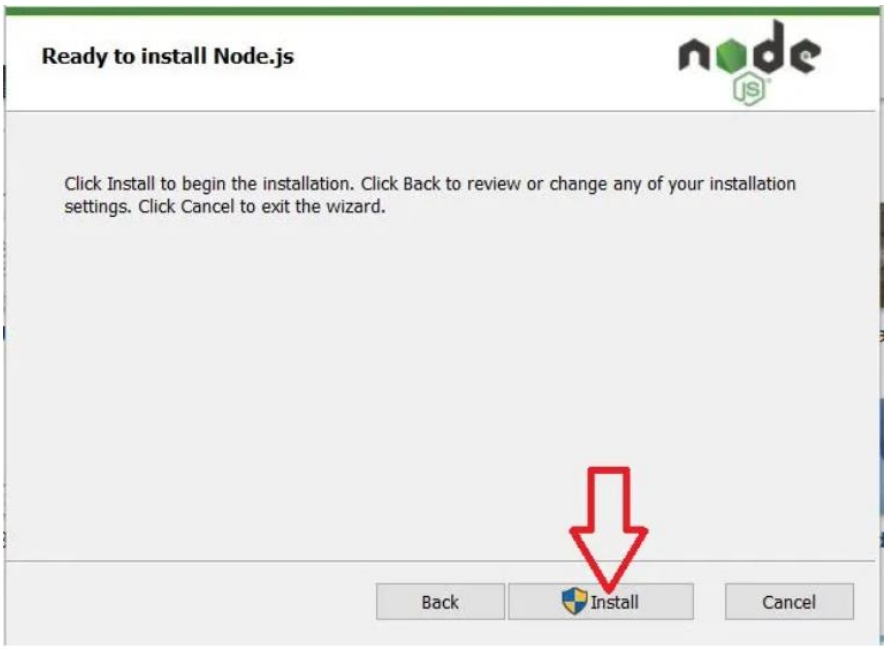

Figura 13 -Pantalla para iniciar la Instalación de Node js

6. Una vez finalizada la instalación, para verificar si el software se instaló correctamente se debe ejecutar el comando “node -v“ en el símbolo del sistema, el cual nos retornará una respuesta parecida a la Figura 14.

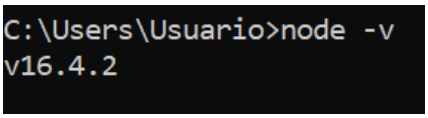

Figura 14 -Verificación de instalación de Node js

Ganache

Ganache es una cadena de bloques personal, esta herramienta es usada para el desarrollo rápido de aplicaciones distribuidas de Ethereum y Corda (Truffle Suite, 2021), dentro de la simulación, esta aplicación da a conocer la cadena de bloques que se formó tras ejecutar las diferentes de compraventa entre las calidades (Vendedor y Comprador).

Para instalar Ganache se deben seguir los siguientes pasos:

1. Descargar el instalador de la siguiente página: https://www.trufflesuite.com/ganache
2. A continuación, se debe ejecutar el archivo descargado el cual presentará una pantalla parecida a la siguiente, en este caso se debe seleccionar la opción “Iniciar Rápido”:

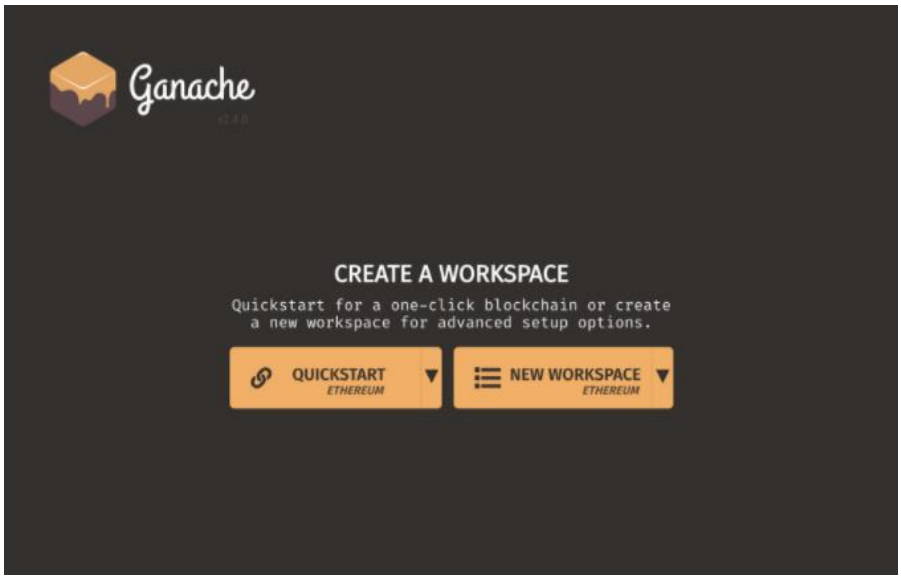

Figura 15 -Pantalla inicial de Ganache

3. Al hacer clic en la opción de Inicio Rápido, Ganache iniciará el entorno de blockchain generando 10 cuentas con 100 ETH para cada una, la pantalla será parecida a la Figura 16, con esto se tendrá iniciado el sistema.

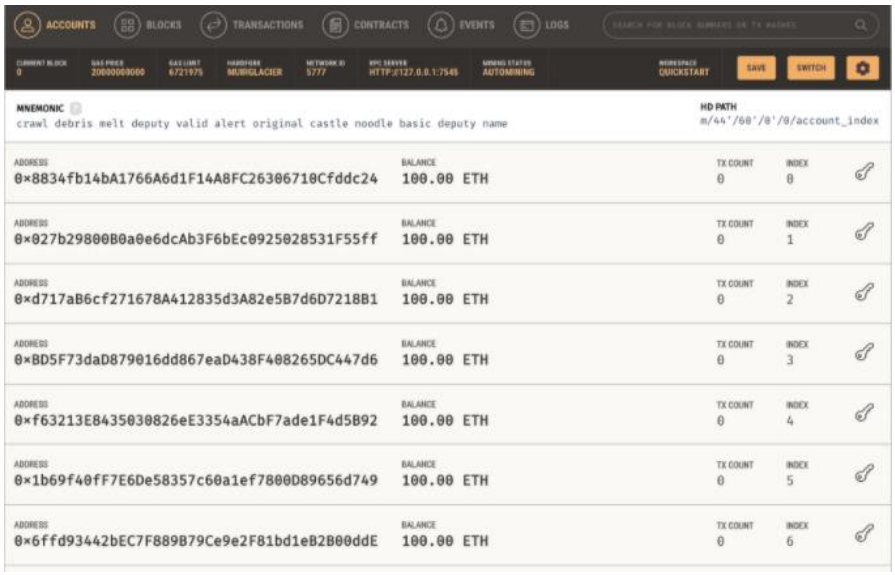

Figura 16 -Listado de cuentas generadas para el uso de blockchain

Truffle

Truffle es un entorno de desarrollo, un marco de prueba y una máquina virtual Ethereum, esta herramienta permite compilar, vincular y gestionar los diferentes contratos inteligentes, debido a

las ventajas que ofrece esta herramienta y a la compatibilidad con ganache (Truffle Suite, 2021), se usó este software para compilar los contratos inteligentes de la simulación.

En este caso para desplegar los contratos inteligentes se debe añadir la configuración de la Figura 17 en el archivo truffle-config.js.

```
1  module.exports = {
2      networks: {
3          development: {
4              host: 'localhost',
5              port: 7545,
6              network_id: '*',
7              gas: 5000000
8          }
9      }
10 }
```

Figura 17 -Configuración del archivo truffle-config.js

Una vez configurado el archivo, se debe ejecutar en la consola el comando truffle deploy para poder visualizar los contratos inteligentes, esta opción se parecerá a la Figura 18.

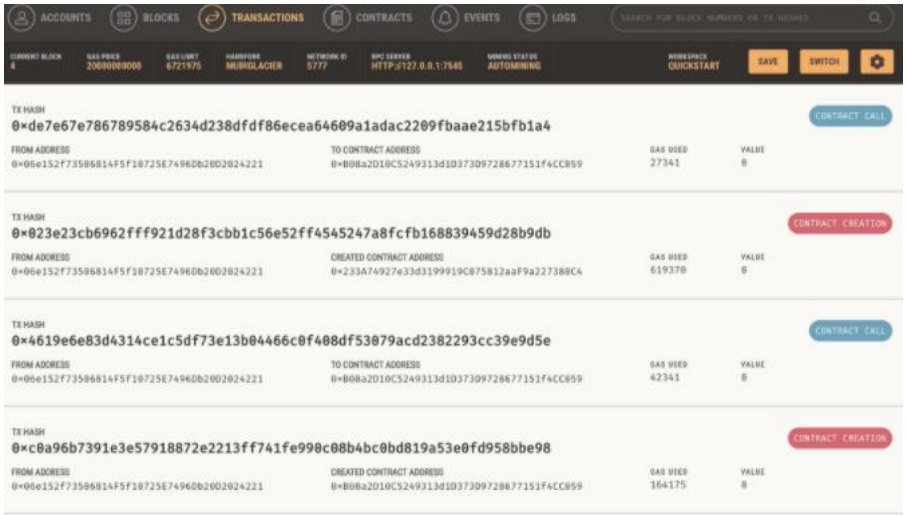

Figura 18 -Despliegue de contrato inteligente en Ganache

Detalle de Simulación

Para la presente simulación, se definió un conjunto de procesos a seguir para llegar a completar toda la transacción de manera correcta, en la Figura 19 se puede observar un diagrama con la sucesión de pasos especificando de manera detallada el proceso a presentar.

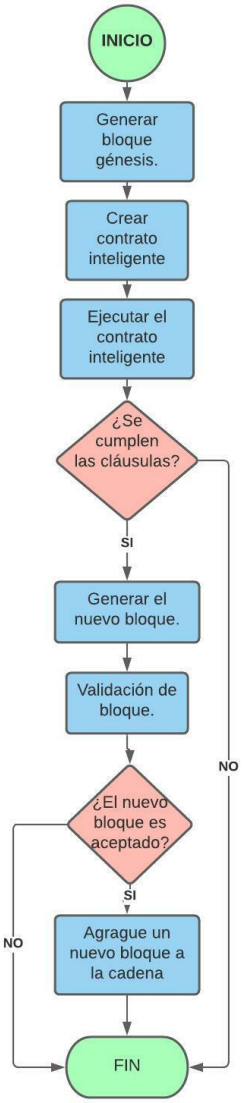

Figura 19 -Diagrama de proceso de generación de nuevos bloques a partir del bloque génesis

De acuerdo a la arquitectura definida, en el caso de la presente simulación llevada a cabo en un computador portátil con el software detallado anteriormente, se planteó como escenario el realizar varias transacciones sobre un terreno, el cual ya tiene definido su nodo génesis, el mismo que en primera instancia debe ser generado por el Registro de la Propiedad debido a que esta es la organización encargada de regular los bienes inmuebles en el país, al ser este el nodo génesis quiere decir que el mismo no fue generado por ninguna transacción, esto se puede apreciar en la Figura 20, en la que se detalla que no existen transacciones posteriores al bloque génesis o bloque 0 de acuerdo al software utilizado.

Figura 20 -Bloque génesis con la feca de generación, se especifica que no existen transacciones generadas

Una vez que se ha generado el bloque génesis de la cadena, se procedió a generar el contrato inteligente, el cual posteriormente fue compilado en el aplicativo de Truffle para que sea reconocido dentro del proceso, y luego ejecutarlo, al momento de iniciar con la ejecución del contrato, se inicia la generación del nuevo bloque para ser agregado a la cadena de bloques que se encuentra en Ganache y Truffle, con lo cual ambos software se sincronizan de tal manera que el nuevo bloque de la transacción actual no se genere sin antes haber terminado la ejecución de las cláusulas programadas en el contrato, en la Figura 21 se muestra el log de la ejecución del contrato de compraventa y los detalles de la generación del nuevo bloque como el número de bloque y el hash correspondiente a la transacción.

```
Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


2_initial_migration.js
======================

   Replacing 'ContratoCompraVenta'
   -------------------------------
   > transaction hash:    0x971729752875a7f4beb71eefebf69029ad85e459f120efc7d40f66b5fe46dff9
   > Blocks: 0            Seconds: 0
   > contract address:    0xe12D6857593884C2DFCC0C5b0a23AFeB20950aEa
   > block number:        30
   > block timestamp:     1625788633
   > account:             0xE392FC72088A2FC3267481F23bc34f9a5C7150FC
   > balance:             99.6794362
   > gas used:            531593 (0x81c89)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.01063186 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:          0.01063186 ETH
```

Figura 21 -Log de ejecución de un contrato inteligente y la posterior creación del nuevo bloque

Al finalizar la creación del nuevo bloque, en el mismo se registra la información de la transacción como por ejemplo el contrato inteligente, información de la fecha y hora de creación, el nuevo

hash y la información de donde fue creado el contrato y desde donde se envió a ejecutar el mismo, esto es importante debido a que permitirá mantener la confiabilidad en la arquitectura ya que como se indicó en secciones anteriores, los nodos mineros deberán ser únicamente las entidades de certificación que funcionan en el país lo que permitirá tener un mayor control incluso si se identificase alguna irregularidad en el proceso pudiendo también poner en una lista negra a los nodos que hayan tenido irregularidades al crear o aceptar un nuevo bloque en la red, de esta manera se generaron los cien bloques que fueron agregados a la cadena, a continuación en la Figura 22 se puede visualizar lo indicado.

BLOCK 100	MINED ON 2021-07-08 19:03:30
BLOCK 99	MINED ON 2021-07-08 19:03:22
BLOCK 98	MINED ON 2021-07-08 19:03:17
BLOCK 97	MINED ON 2021-07-08 19:03:12
BLOCK 96	MINED ON 2021-07-08 19:03:07
BLOCK 95	MINED ON 2021-07-08 19:02:56
BLOCK 94	MINED ON 2021-07-08 19:02:51
BLOCK 93	MINED ON 2021-07-08 19:02:46

Figura 22 -Cadena de Bloques generada con 100 transacciones

Discusión de Simulación

De acuerdo con Schuschny (2017), un uso particular para blockchain, es su aplicación dentro de las operaciones de notarización y certificación que, hasta hoy, son realizados por los escribanos o notarios quienes actúan como agentes fedatarios. Entre algunas de las transacciones como son el registro y transferencia de activos, de propiedad intelectual o física como automóviles, patentes, testamentos, auditorias contables, podrían certificarse a través de sistemas basados en blockchain.

Dicha afirmación del autor citado, se puede observar en la Figura 21, con el uso de la cadena de bloques en la cual , toda la información relacionada al contrato inteligente se almacenará en el mismo, manteniendo actualizados todos los datos del último dueño de la propiedad transaccionada, eliminando de esta manera procesos engorrosos y papeleos que muchas de las veces están sujetas a errores tipográficos, los mismos que al acudir a otras entidades públicas para

terminar todo el proceso de compra y venta son rechazados y enviados a corregir, proceso final que también será reemplazado con la arquitectura presentada.

Al tener todo el proceso centralizado y administrado o monitoreado por las entidades de certificación existentes en el país se reduce de un proceso que puede tardar horas o incluso días a cuestión de minutos, tiempo durante el cual se generará el nuevo bloque que pasará a formar parte de la cadena pudiendo acceder a todo el historial del bien dando la seguridad al usuario de que su solicitud o compra no tiene ningún problema para cerrar el trato lo que garantiza que el contrato inteligente se cumpla a cabalidad en todas sus cláusulas.

Capítulo 4 – Conclusiones y Trabajos Futuros

En el contexto planteado en nuestra investigación hemos constatado que existen barreras para la aplicación de blockchain como una tecnología disruptiva de la transformación digital entre los que describimos:

La brecha digital, dentro de la población ecuatoriana existe una franja amplia de personas que aún son analfabetos digitales y por falta de conocimientos informáticos y temor se constituyen en una de las barreras más fuertes para un cambio tecnológico.

Falta de políticas estatales y voluntad política, en nuestro país existen una gran resistencia a los cambios tecnológicos que habiliten la reducción de procesos burocráticos y el poder político y el tráfico de influencias y la corrupción que mina las posibilidades de una nueva tecnología que dinamiza los procesos y reduce los costos, más aún cuando la población se beneficiaría del uso de la cadena de bloques para aportar de una manera más eficiente en el pago de impuestos.

Por otra parte, la arquitectura de blockchain y el uso de contratos inteligentes tienen como objetivo dinamizar los procesos notariales actuales agregándoles nuevas características de seguridad, eficiencia, disponibilidad y confidencialidad, muy diferente a la forma tradicional en la que es llevado en la actualidad, mejora los procesos reduciendo el tiempo y los acciones secundarias como pagos entre las diferentes empresas involucradas, por lo tanto también mejora la recaudación de pagos de impuestos a las arcas estatales locales y gubernamentales.

Así mismo, nuestra arquitectura deja la alternativa de una estandarización de procesos y la ubicuidad de poder realizar un trámite sin la necesidad de la presencia física de los interesados, de tal manera que una persona puede llegar a un acuerdo mercantil y generar una mayor dinámica de mercado, el ingreso de la cadena de bloques a la cadena de valor mercantil crea nuevas oportunidades en los ecosistemas de las economías modernas.

Uno de los grandes retos que conlleva la implementación de esta arquitectura de blockchain en los procesos notariales y que se identificó durante la simulación, es el de simplificar el uso de entidades de gobierno en los cuales se encuentra distribuida la información de la población (SRI, Registro Civil, Consejo de la Judicatura, Registro de la Propiedad) de tal manera que no sea necesario el acceder a las mismas durante las transacciones y especialmente durante la generación de los contratos inteligentes en el cual se detalla todos los datos necesarios para cerrar un proceso de compraventa.

En una versión extendida del presente trabajo, se deben dar a conocer a manera más detallada las tecnologías a utilizar para la implementación de la arquitectura elaborada ya que en el presente documento se desarrolló un prototipo de ejemplo con software de simulación, así como también las políticas necesarias para lograr la operatividad plena de la presente propuesta.

Referencias

ARCOTEL Ecuador. (2020). *Agencia de Regulación y Control de las Telecomunicaciones*. Obtenido de Agencia de Regulación y Control de las Telecomunicaciones: https://www.arcotel.gob.ec/listado-de-las-entidades-de-certificacion-de-informacion-y-servicios-relacionados-acreditados-y-terceros-vinculados-debidamente-acreditadas/

Chico González, L. Á. (2018). *Notario Público y Notary Public.*

Eterovic, J., Cipriano Marcelo, García, E., & Torres, L. (2020). *Seguridad en Internet de las Cosas usando soluciones Blockchain.* Obtenido de SEDICI; Repositorio Institucional de la UNLP: http://sedici.unlp.edu.ar/handle/10915/104030

Ferrer-Sapena, A., & Sánchez Pérez, E. A. (2019). Aplicaciones de la tecnología blockchain en la documentación científica: situación actual y perspectivas. *El profesional de la información*, 11.

Figueroa Castillo, V. A., Villacreses Parrales, C. A., Chóez Calle, J. E., Barreto Pin, J. X., & Maldonado Zuñiga, K. (2021). El blockchain y los contratos inteligentes; una forma de reducir la corrupción. *Serie Científica de la Universidad de las Ciencias Informáticas*, 10.

Función Judicial del Ecuador. (20 de Mayo de 2014). *Función Judicial del Ecuador*. Obtenido de Función Judicial del Ecuador: http://www.funcionjudicial.gob.ec/

Función Judicial del Ecuador. (2020). Resolución 075-2020.

Garay, J. A., Kiayias, A., & Leonardos, N. (2015). The Bitcoin Backbone Protocol: Analysis and Applications. *Conference Paper*, 45.

García Mateo, P. (2018). *Blockchain aplicado al sector público.* Valencia: Escola Técnica Superior d'Enginyeria Informática.

García Morales, E. (2017). Good and bad points on the impact of the blockchain in document management. *Iwe Tel*, 7.

Lakshimi Siva, S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of Consensus Protocols on Blockchain Applications. *International Conference on Advanced Computing and Communication Systems*, 5.

Llopis Castelló, D. (2020). Metodología Experimental. *GIIC*, 15.

Mannan , M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology of Society*, 14.

Moreno Ballesteros, A. M. (2019). BLOCKU - una aproximación a la certificación, trazabilidad y transmisión de valor en la educación superior. *ACADEMIA Accelerating the world's research.*, 14.

Naranjo Acosta, W. H. (2018). *Análisis de la difusión social de las atribuciones y competencias de los notarios en la ciudad de Guayaquil.* Guayaquil.

Open JS Foundation. (s.f.). *NODE JS*. Recuperado el 8 de Julio de 2021, de https://nodejs.org/es/about/

Ortega Pérez, I. (2019). Smart contracts and Blockchain: legal qualification of Smart. *Smart contracts and Blockchain: legal qualification of Smart*, 48. Zaragoza.

Preisegger, J. S., Muñoz, R., Pasini, A., & Pesado, P. (2019). Blockchain y gobierno digital. *XXV Congreso Argentino de Ciencias de la Computación*, 11.

Schuschny, A. (2017). La Blockchain y sus posibles aplicaciones en el ámbito de la energía. *enerLAC*, 23.

Singhal, B., Dhameja, G., & Sekhar Panda, P. (2018). *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions.* Berlín: Apress.

Tendermint. (2021). *Tendermint*. Obtenido de https://tendermint.com/

Torres Torres, A. Y., & Ramírez Arenas, O. A. (2017). La responsabilidad civil de las entidades de certificación en Colombia. *Dialnet*, 29.

Truffle Suite. (2021). *Truffle Suite*. Recuperado el 8 de Julio de 2021, de https://www.trufflesuite.com/ganache

Ulloa Banegas, R., & Gallegos Segovia, P. (2021). Design of a blockchain architecture and use of smart. *ICAT 2021: International Conference on Applied Technologies*, (pág. 15). Santo Domingo, Ecuador.

Valencia Ramírez, J. P. (2019). Smart Contracts. *RITI Journal Vol. 7*, 10.

Vintimilla Tapia, P., Bravo Torres, J., López Nores, M., Gallegos Segovia, P., Ordóñez Morales, E., & Ramos Cabrera, M. (2020). VaNetChain: A framework for trustworthy exchanges of information in VANETs based on blockchain and a virtualization layer. 15.

World Government Summit. (2017). *Building the Hyperconnected Future on Blockchains.* World Government Summit.

Yahari Navarro, B. (2019). Blockchain y sus aplicaciones. 19.