DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: SISTEMA PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN IDENTIDADES DIGITALES APLICANDO TECNOLOGÍA BLOCKCHAIN

AUTORES: TUNALA LLUMIUGSI, MARILYN ANABEL
MONCAYO FELICITA, RONNIE EDUARDO

DIRECTOR: ING. FUERTES DÍAZ, WALTER MARCELO PhD

SANGOLQUÍ

2018

CERTIFICADO DEL DIRECTOR

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"SISTEMA PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN IDENTIDADES DIGITALES APLICANDO TECNOLOGÍA BLOCKCHAIN"*** fue realizado por la señorita ***Tunala Llumiugsi, Marilyn Anabel*** *y el señor* ***Moncayo Felicita, Ronnie Eduardo*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustenten públicamente.

Sangolquí, 01 de agosto del 2018

Ing. Walter Marcelo Fuertes Díaz, PhD
C.C.: 1707017701

AUTORÍA DE RESPONSABILIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERIA DE SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Nosotros, **Marilyn Anabel Tunala Llumiugsi y Ronnie Eduardo Moncayo Felicita**, declaramos que el contenido, ideas y criterios del trabajo de titulación: **Sistema para mejorar la seguridad de la información en identidades digitales aplicando tecnología Blockchain** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 01 de Agosto del 2018

Marilyn Anabel Tunala Llumiugsi
1727331827

Ronnie Eduardo Moncayo Felicita
1721798518

AUTORIZACIÓN

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERIA DE SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, **Marilyn Anabel Tunala Llumiugsi y Ronnie Eduardo Moncayo Felicita**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **Sistema para mejorar la seguridad de la información en identidades digitales apiicando tecnoiogía Biockchain** en ei Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 01 de Agosto del 2018

Marilyn Anabel Tunala Llumiugsi
1727331827

Ronnie Eduardo Moncayo Felicita
1721798518

DEDICATORIA

A mis padreas Rocio y Carlos por su amor, dedicación y apoyo constante, que me han llevado a cumplir una meta más. Los quiero mucho.

A mis hermanos Erika y Jhon por inspirarme cada uno de una manera diferente, convirtiéndome en quien soy.

A mis abuelos en especial a mis seres queridos que están en cielo, espero que desde allá estén orgullosos de mí.

Marilyn Tunala

Quiero dedicar este documento que tiene envuelto miles de momentos duros, difíciles, largos, lindos, una mezcla de sentimientos a las personas que siempre estuvieron ahí, apoyándome en todo, las personas que siempre confiaron en mí, las persona que más amo en este planeta, esto te lo dedico a ti Juana Felicita, madre mía, Luis Moncayo el mejor padre, Angie, Anabel mis hermanas, este triunfo es suyo.

Ronnie Moncayo

AGRADECIMIENTO

Quiero agradecer a Dios por darme la vida, por guiarme, por esas maravillosas personas que ha puesto en mi camino, esas grandes oportunidades, y en realidad por dármelo todo. A mis padres gracias por su esfuerzo, que se refleja en un éxito más. A igual que toda mi familia y amigos que me ha apoyado y creído en mí. A la Universidad de las Fuerzas Armadas ESPE, por abrirme las puertas de tan prestigiosa institución. A mis maestros por convertirme en una profesional, en especial a mi director de tesis Ing. Walter Fuertes, por compartir sus conocimientos, su sabiduría y su afecto. Finalmente quiero agradecer a mi compañero Ronnie por esta desafiante tesis que nos propusimos en nuestro afán de buscar innovar y crear.

Marilyn Tunala

Quiero agradecer a todas las personas que fueron partes de este proceso que con este documento finaliza, a todas las personas que me ayudaron siempre en lo que podían y me demostraron su afecto e hicieron que esta etapa sea una de las mejores de mi vida, muchas gracias a todos mis amigos de la Universidad, del colegio, mi familia, recalcar el agradecimiento a esa personita que hizo de la Universidad, una estadía genial, Anabel. También a mis ingenieros que supieron brindarme su conocimiento y enseñanzas de vida, gracias a todos, gracias vida por darme esta oportunidad y gracias ESPE.

Ronnie Moncayo

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La era digital en el siglo XXI ha traído consigo cambios fundamentales sobre la gestión de la información especialmente sobre el manejo de identidades digitales. Donde los datos de los individuos se han convertido el activo más importante de las organizaciones convirtiéndose así en un objetivo atractivo para los delincuentes informáticos, además de que algunas organizaciones se han adueñado de la información de los usuarios, sin su consentimiento, y la han usado a su conveniencia. En consecuencia, este trabajo plantea una forma de mitigar estos problemas de seguridad, con la utilización de la tecnología Blockchain. Esta tecnología se ha popularizado con la aparición de criptomonedas como Bitcoin, tras su difusión se ha investigado para aprovechar sus bondades en diferentes áreas, entre las cuales está el manejo de la información. Blockchain es una red descentralizada que entre sus características ofrece un registro inmutable de todas sus transacciones, almacenadas en bloques que encriptan los datos, cuenta con contratos inteligentes que son programas que simulan a un contrato legal, además de un algoritmo de consenso que evita alterar los registros del Blockchain o algún tipo de fraude dentro de la red. Para este trabajo se ha realizado un análisis sobre identidades digitales, se ha investigado frameworks de Blockchain, se desarrolló un prototipo, se realizaron pruebas, evaluación y validación de resultados.

PALABRAS CLAVES:

- **BLOCKCHAIN**
- **IDENTIDAD DIGITAL**
- **CONTRATO INTELIGENTE**
- **ALGORITMO DE CONSENSO**
- **RED DESCENTRALIZADA**

ABSTRACT

The digital age in the 21st century has brought about fundamental changes in the management of information, especially on the management of digital identities. Where the data of the individuals have become the most important asset of the organizations thus becoming an attractive target for the computer delinquents, besides that some organizations have taken possession of the information of the users, without their consent, and have used it at your convenience. Consequently, this work proposes a way to mitigate these security problems, with the use of Blockchain technology. This technology has become popular with the appearance of cryptocurrencies such as Bitcoin, after its dissemination has been researched to take advantage of its benefits in different areas, among which is the handling of information. Blockchain is a decentralized network that, among its features, offers an immutable record of all its transactions, stored in blocks that encrypt data, has smart contracts that are programs that simulate a legal contract, as well as a consensus algorithm that avoids altering the Blockchain records or some type of fraud within the network. For this work an analysis of digital identities has been carried out, Blockchain frameworks have been researched, a prototype was developed, tests were carried out, evaluation and validation of results.

KEYWORDS:

- **BLOCKCHAIN**
- **DIGITAL IDENTITY**
- **INTELLIGENT CONTRACT**
- **CONSENSUS ALGORITHM**
- **DECENTRALIZED NETWORK**

CAPÍTULO I

INTRODUCCIÓN

1.1 Antecedentes

El mundo está experimentando un cambio fundamental al ser impulsado por los datos, desde la comunicación, las finanzas hasta el entretenimiento, han migrado en gran medida a Internet. Con el aumento de la información digital han surgido desafíos y oportunidades para entidades privadas y públicas. Uno de estos desafíos y oportunidades es la identidad digital (Bertino et al.,2009).

De acuerdo con Camp (2004), la identidad digital es equivalente a la identidad real de una persona jurídica o natural, que está vinculada a uno o más identificadores digitales, como una dirección de correo electrónico, URL o nombre de dominio. Se la utiliza para identificación en conexiones o transacciones desde PC, teléfonos inteligentes u otros dispositivos. Es común que las identidades sean controladas por organizaciones que interactúan con el titular de esta información.

El óptimo manejo de la identidad digital abre paso a una revolución en la forma en que los individuos interactúan con las instituciones públicas. Y el sector privado también se está involucrando rápidamente. Con una identidad digital las personas podrían acceder a servicios o productos sin tener que presentar físicamente documentos, como pasaportes, partidas de nacimiento, licencias de conducir u otros papeles. También podría resolver problemas para los consumidores en mercados más desarrollados, donde la identidad sea un problema (Mellmer et al., 2014).

De acuerdo con YOTI (2017), "La verificación de edad en línea evitará que los menores de edad abran cuentas de redes sociales inapropiadas y se asegurará de que los menores no puedan

acceder a contenido para adultos. Esto ayudaría a los minoristas en línea a confirmar que alguien es elegible para comprar productos con restricciones de edad, como DVD, juegos de computadora, alcohol, cigarrillos y armas ".

El ex presidente de Google, Eric Schmidt, prevé que la identidad se convertirá en el producto más valioso para los ciudadanos en el futuro, existiendo principalmente en línea.

La identidad digital ofrece varias oportunidades, pero también algunos desafíos como lo mencionan Daemen & Rubinstein (2006), entre los cuales están: la legitimidad de la identidad, el control sobre el uso de la información personal, la seguridad de las transacciones, la falta de confianza entre diferentes partes que no se conocen mutuamente.

Un modelo de confianza distribuida es una nueva forma de gestionar identidades. La tecnología Blockchain permitiría a los usuarios controlar su propia identidad y compartir entre entidades confiables con su consentimiento. Además, ninguna institución puede comprometer la identidad del consumidor (IBM, 2017).

Blockchain es la tecnología detrás de Bitcoin. De acuerdo a Zyskind y Nathan (2015), esta nueva tecnología pretende revolucionar la concepción del manejo de la información descentralizada, comprometiéndose a salvaguardar la seguridad de la misma. Esta tecnología funciona a partir de la criptografía y la compartición de datos peer to peer, que consiste en la comunicación entre dos usuarios sin necesidad de utilizar un servidor central.

1.2 Problemática

De acuerdo con Phillip J. Windley (2014), “La identidad en Internet está rota. Hay demasiadas fugas de privacidad. Demasiados negocios y casos que están siendo pobremente atendidos por las soluciones actuales”. La identidad digital es crítica para muchas transacciones

comerciales y sociales. Permite formas de interactuar con miles de millones de usuarios en el mundo digital. Sin embargo, los sistemas de identidad tradicionales son costosos, inconexos, falibles y obstaculizan la innovación y una mayor experiencia del cliente (IBM, 2017).

Incluso en las economías desarrolladas, las personas no tienen la privacidad, seguridad y control necesarios sobre su información digital. Una identidad digital efectiva, privada, segura y controlada por el individuo, permitirá a las personas acceder a los recursos a los que tienen derecho, tales como servicios gubernamentales, servicios financieros, educación, comercio electrónico y comunicaciones.

Según Omidyar Network (2017), la identidad digital solo puede conducir al empoderamiento si se pone al individuo en control de su identidad y se construye con estándares y medidas para proteger la información personal de los individuos. El autor considera que las identidades digitales deben estar disponibles para las personas, no ser discriminatorias, estar diseñadas para la inclusión, y el usuario debe tener el control sobre su privacidad.

Para que un sistema de identidad digital sea exitoso, se debe considerar tanto el diseño técnico como la gobernanza. De hecho, el diseño técnico puede ser más eficaz para proteger a las personas que el marco de privacidad legal de un país determinado, dada la dificultad de hacer valer los derechos. Existe un creciente esfuerzo sobre la privacidad, la protección de datos y principios de identidad (Omidyar Network, 2017).

1.3 Justificación

Es indudable los beneficios de las identidades digitales. El óptimo manejo de estas, contribuirá a sectores privados, públicos y a los usuarios. Optimizará procesos, ayudará a romper las barreras de tiempo y espacio. A lo largo de este documento se ha mencionado algunas de las

características de identidades digitales, y se ha recalcado que el principal desafío es la seguridad de la información ya que en concordancia con Sullivan y Burger (2017) la integridad, disponibilidad y confidencialidad, son imprescindibles para los usuarios debido a que, las personas no se sienten seguras al revelar tanta información personal.

De acuerdo con Lootsma (2017), entre las características de Blockchain se encuentra la encriptación de la información, la cual ayuda a mantener la integridad de los datos debido a que guarda las transacciones en bloques encriptados y cada bloque contiene el Hash del anterior. Se aplica el concepto de disponibilidad ya que utiliza una red descentralizada peer to peer. También trazabilidad al mantener un sistema de registros inmutables a través del tiempo, además utiliza una tecnología Ledger distribuida, que cuenta con varios nodos donde se encuentran una réplica exacta de la información, aplicando el concepto de redundancia. Según estas características la tecnología Blockchain es ideal para aplicarse en identidades digitales.

En el manejo de identidades digitales también es importante la confidencialidad de los datos, lo que no necesariamente cumple el Blockchain tradicional, utilizado por criptomonedas como Bitcoin, donde su uso y transacciones están abiertas al público. Sin embargo, para este proyecto se utiliza un Blockchain privado que comparte la información solo con las entidades que se les haya otorgado un permiso, cumpliendo así con la confidencialidad de la información. Para desarrollar este Blockchain privado se ha realizado una evaluación sobre Frameworks de código abierto con el fin de seleccionar el que mejor se adapte al manejo de identidades digitales.

A lo largo de este documento se han mencionado las características y bondades de Blockchain, promete ser el futuro en el manejo de la información para diferentes ámbitos, desde educativos, sociales, financieros, y está abierto para nuevas ideas. Debido a todo lo expuesto

anteriormente sobre esta tecnología un análisis de este tema es muy enriquecedor tanto para el desarrollo profesional de los autores como una contribución para la comunidad universitaria y científica. Dejar constancia de la experiencia y los resultados ayudará a futuros trabajos ya que existen aún muchas áreas sin explotar con esta tecnología. Cabe destacar que son muy pocas las implementaciones de Blockchain conocidas en campos diferentes a las monedas criptográficas.

1.4 Objetivos

1.4.1 Objetivo General

Analizar, diseñar e implementar un prototipo para mejorar la seguridad de la información en identidades digitales utilizando la tecnología Blockchain.

1.4.2 Objetivos Específicos

i. Realizar una revisión de literatura sobre identidades digitales.
ii. Evaluar los frameworks de Blockchain de código abierto para determinar el más adecuado en el manejo de identidades digitales y proponer una solución.
iii. Diseñar e implementar un prototipo de la solución propuesta.

1.5 Alcance

El alcance del presente proyecto abarca desde una revisión de literatura sobre identidades digitales, la etapa de investigación sobre la tecnología Blockchain, una solución propuesta para el manejo de identidades digitales en base a la seguridad de la información, pasando por la selección de frameworks y herramientas necesarias para desarrollar un prototipo, hasta el diseño e implementación del mismo, que desplegará un Blockchain donde se simulará el manejo de identidades digitales.

CAPÍTULO II

ANÁLISIS DE LA IDENTIDAD DIGITAL

En esta sección se analizan los fundamentos teóricos sobre la identidad y la aparición de un nuevo tipo denominada identidad digital, se detalla los requisitos para un óptimo manejo de ésta. Y finalmente los desafíos a los que se enfrenta en la era digital del siglo XXI.

2.1 La identidad digital

La identidad tiene varios aspectos. Desde el punto de vista filosófico como lo señala Gaitán (2010), busca responder la pregunta ¿Quién soy yo?, analiza cómo el individuo se muestra ante la sociedad, con la intención de modelar un comportamiento propio. Las descripciones tradicionales de los sociólogos (Comte, Durkheim, Weber, Marx) apoyan implícitamente la idea de que la identidad de un sujeto está determinada por el lugar que éste ocupa en la sociedad.

A lo largo de los años, la sociedad ha desarrollado mecanismos donde las entidades solicitan credenciales para la autenticación de las personas y así dar acceso a los recursos. Las diferencias en los enfoques se basan en los requisitos del sistema, las políticas administrativas, las tecnologías y los riesgos de seguridad. Sin embargo, la capacidad de uso de los mecanismos de identificación sigue siendo fundamental para todos estos factores. (Bramhall, 2007)

Con la promulgación de Internet en la sociedad actual, los individuos están más interconectados. Esto se puede apreciar en la Figura 1, donde se ve un notable incremento del acceso a Internet en los hogares ecuatorianos, de un 7% en el 2008 a un 30% en el 2015. De igual forma se puede observar en la Figura 2 la diminución del analfabetismo digital del 2008 en un 32.4% al 2016 en un 11.5%, en una población de entre 15 -49años.

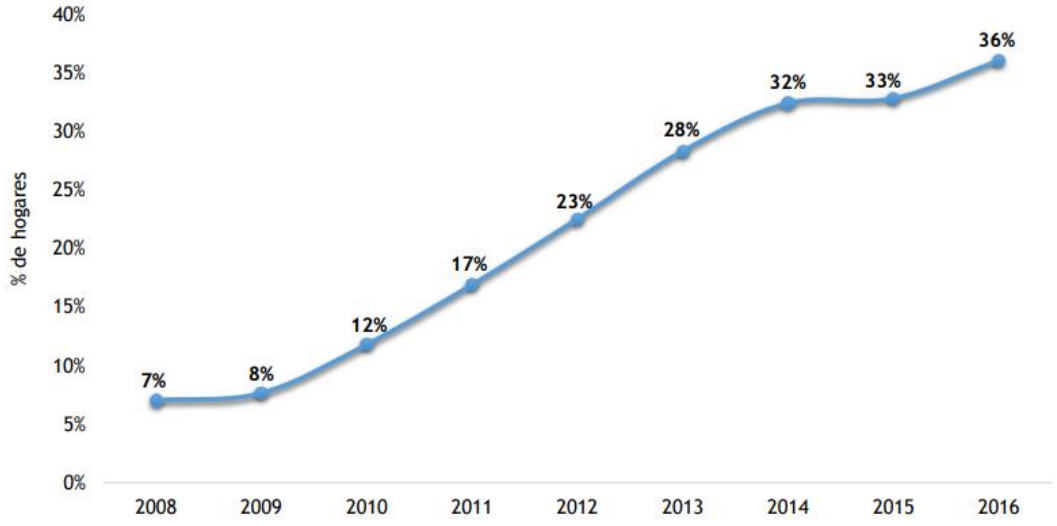

Figura 1. Acceso a Internet en Ecuador
Fuente: (Instituto Nacional de Estadísticas y Censos, 2017)

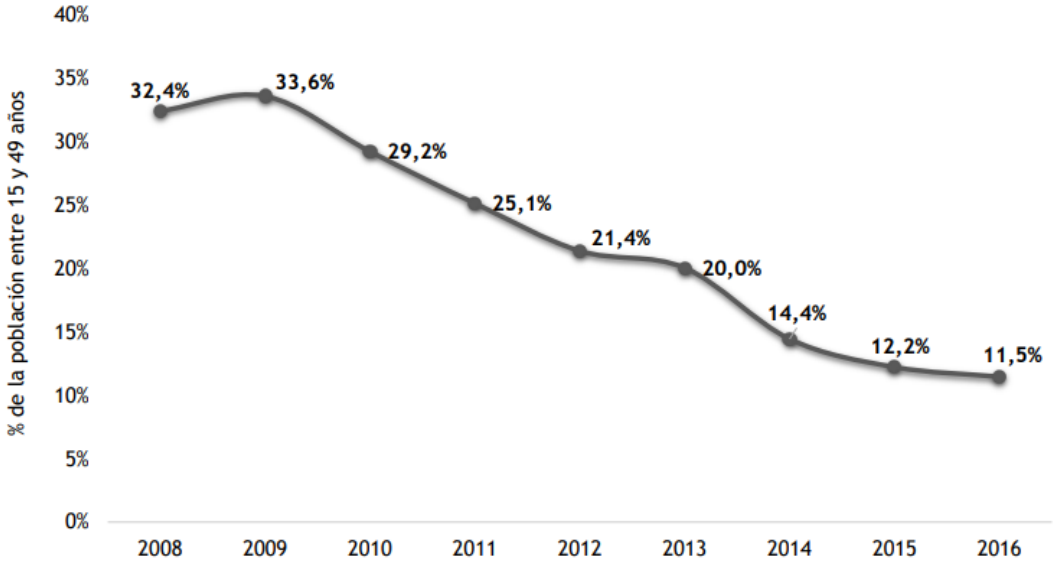

Figura 2. Analfabetismo Digital
Fuente: (Instituto Nacional de Estadísticas y Censos, 2017)

Debido a la digitalización que se está viviendo en la sociedad es forzoso la creación de una identidad digital (Halim, 2009). Como lo sostiene Ana Isabel Segovia, economista en el área de Regulación digital en BBVA Investigación, "El papel de la identidad digital en el futuro es clave ya que toda la actividad económica y social se trasladará al mundo digital. Además, la posibilidad

de que las empresas y los usuarios puedan realizar transacciones a través de Internet de forma segura y no fragmentada será clave para el desarrollo de la economía digital".

En la identidad digital los usuarios registran sus datos en varias plataformas Web, y deben crear y memorizar numerosas claves. Lo que conduce a que la gente no pueda actualizar todas sus credenciales e identidades digitales simultáneamente. Otro hecho a considerar es que los usuarios tienen poco o ningún control sobre la información que se almacena sobre ellos y cómo se utiliza. Además esa información está centralizada y administrada por las plataformas que registraron al usuario (Calderón, 2010).

Esta centralización quebranta la seguridad como lo demostró en los últimos meses el hacker que atacó a Equifax, los malos actores necesitan entrar en una sola base de datos para obtener toda la información de los usuarios. De hecho, desde 2013, más de 9 mil millones de registros de datos se perdieron o fueron robados. Lo sorprendente es que, de estos solo el 4% se encriptaron y, por lo tanto, se volvieron inútiles después de haber sido robados (Gemalto NV, 2018). En resumen, las prácticas de identidad de datos actuales son insostenibles.

2.2 Requisitos para un óptimo manejo de la identidad digital.

Para garantizar la facilidad de uso, seguridad y privacidad, las identidades digitales deben ser implementadas utilizando métodos técnicos avanzados. Por lo tanto, la tecnología debe ser aplicada en al menos tres de las siguientes áreas: la autenticación, protocolos de seguridad, almacenamiento y mejoras.

Aguilera (2011), plantea algunas las técnicas de autenticación que se extienden de un solo factor a múltiples factores. A continuación, se muestra una lista de métodos comunes utilizados en los sistemas de autenticación: (i) Contraseña o número de identificación personal (PIN), es un

método tradicional en el que se proporciona al usuario un nombre y una contraseña. Sin embargo, muchos han demostrado que esta técnica es a menudo fácil de adivinar o robar. Con el fin de hacer el proceso de autenticación más seguro, surge la Autenticación con contraseña de un solo uso (OTP), el usuario sólo introduce la contraseña una vez y debe solicitar otra desde el servidor en el siguiente intento de entrar o hacer una transacción. El PIN tiene, básicamente, el mismo mecanismo que una contraseña, pero se compone de un plazo numérico solamente, por lo general con cuatro a seis dígitos. Un mecanismo de autenticación basada en PIN se utiliza comúnmente para los servicios financieros tales como pagos de cajeros automáticos y tarjetas de crédito. (ii) Simbólico funciona según el principio de autenticación de dos factores. En lugar de utilizar un nombre de usuario y la contraseña, se añade un nivel a través de contador de tiempo limitado, típicamente una clave criptográfica o contraseña, que se utiliza para otras transacciones durante la sesión. (iii) La criptografía de clave pública utiliza mecanismos criptográficos que se acoplan un par de claves asimétricas: una clave pública y una clave privada. El cifrado de clave pública utiliza ese par de claves para el cifrado y el descifrado. La clave pública se hace pública y se distribuye ampliamente y libremente. La clave privada nunca se distribuye y debe mantenerse en secreto (CGI, 2004). (iv) La autenticación biométrica requiere un estilo diferente, es el proceso que asegura que las personas son quienes dicen ser. Este enfoque se basa en la singularidad biológica de una persona, utilizando, por ejemplo, huella digital física o el reconocimiento del iris. Una técnica de coincidencia de patrones es esencial, también requieren dispositivos de sensores para recoger la característica del usuario. (v) Tarjeta electrónica, la tecnología de tarjetas inteligentes por lo general se presenta en dos formas: una tarjeta de plástico o un dispositivo USB, cada uno con un chip informático incrustado. El uso de una tarjeta inteligente para almacenar la contraseña de archivos es su aplicación más simple.

En cuanto a los protocolos de seguridad Duncan (2001), sostiene que estos protocolos se valoran por sus fuertes atributos de identidad, la verificación y autenticación. Específicamente, están diseñados para transferir datos de autenticación entre dos entidades. Los protocolos de autenticación generalizados utilizados para hacer frente a los problemas de seguridad dentro de las redes abiertas son Secure Sockets Layer (SSL), Internet Protocol security (IPSec), Secure Shell (SSH), y Kerberos.

Según Tómas (2009), las nuevas tecnologías que contribuyen a la mejora de almacenamiento tienen una repercusión importante en la creación de sistemas de identidades digitales robustas. Hay dos nuevas tecnologías que pueden mejorar los métodos de almacenamiento de base de datos. El primero distribuye la tecnología del libro mayor, o Blockchain, esto permite que la información se almacene en una red peer-to-peer transferida en forma dispersa e inmutable. El segundo consiste en estándares de identidad federados, que crean la interoperabilidad entre las redes de gestión de identidad y aplicaciones externas, permitiendo a estos sistemas de identidad federados escalar para acomodar un gran número de proveedores de identidad y las partes de confianza.

2.3 Desafíos

La mayoría de las tecnologías de gestión de identidades difieren de un conjunto de problemas causados principalmente por el legado, la falta de seguridad y privacidad en las tecnologías actuales. Kikitamara (2017), describe los problemas más graves actuales que se resumen de la siguiente manera:

Identificadores globales son utilizados por varios sistemas para identificar a los usuarios, tales como números de seguridad social, URL o direcciones de correo electrónico. Los

identificadores globales permiten a los diferentes sitios correlacionar la información acerca de los usuarios, que por lo general consiente a los sitios para obtener más información que fue específicamente permitido por el usuario (Bramhall, 2007).

Las herramientas típicamente utilizadas por los usuarios para el acceso a Internet no prestan un entorno seguro. Los virus y otros programas maliciosos pueden infectar fácilmente y otorgar control sobre todas las actividades del usuario a terceros, uno de tantos ejemplos se puede observar en la Figura 3 que describe como se ha popularizado el ataque Ransomeware entre el 2015 y 2016. Muchos esquemas de firma digital del gobierno también pueden ser alterados usando software malicioso del lado del cliente (IBM, 2018).

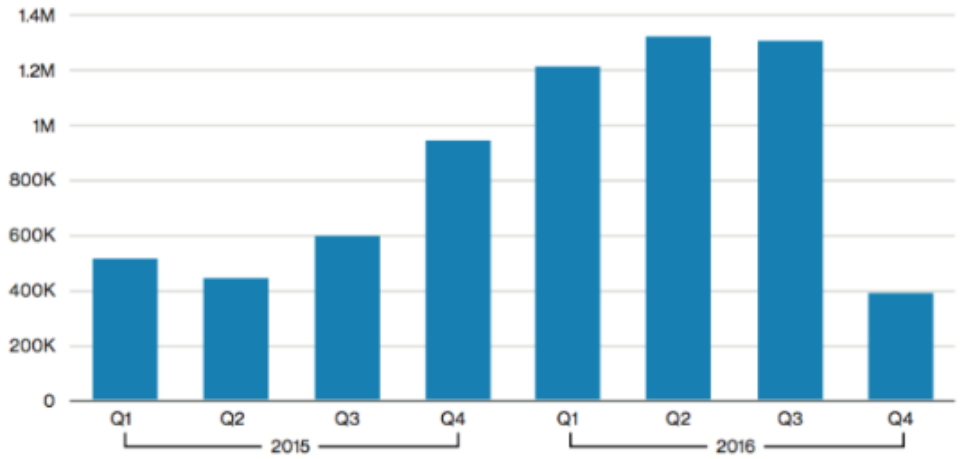

Figura 3. Afectación de Ransomware
Fuente: (Laboratorios de McAfee, 2017)

Finalmente, la centralización de la información personal puede ser muy conveniente desde una perspectiva de gestión de datos, pero dicho repositorio crea un objetivo muy atractivo para los atacantes. Ya que solo deben ingresar a una base datos para obtener toda la información. Además, las compañías centralizan la información de los usuarios, sacando beneficio de estos datos, incluso compartiéndolos con terceros sin el consentimiento del usuario (Zyskind, 2015).

CAPÍTULO III

INVESTIGACIÓN DE CAMPO

En este capítulo se explica algunos conceptos sobre la tecnología Blockchain, y se muestra una evaluación sobre sus frameworks de código abierto, con la finalidad de seleccionar el más óptimo para ser utilizado en el proceso de identidades digitales.

3.1 Tecnología Ledger Distribuido

"Ledger" traducido al español significa "libro mayor", es un tipo de estructura de datos que reside en múltiples dispositivos informáticos, generalmente distribuidos en ubicaciones o regiones. (The Linux Foundation and Hyperledger, 2017). La tecnología Ledger distribuida incluye tecnologías blockchain y contratos inteligentes. De acuerdo con Pinna y Ruttenberg (2016), antes de Bitcoin ya existían ledgers distribuidos, el blockchain de Bitcoin marca la convergencia de una serie de tecnologías, incluyendo sellado de tiempo de las transacciones, las redes peer-to-peer (P2P), criptografía y potencia de cálculo compartida, junto con un nuevo algoritmo de consenso.

La tecnología de contabilidad distribuida generalmente consta de tres componentes básicos: i) Un modelo de datos que captura el estado actual del libro mayor; ii) Lenguaje de transacciones que cambia el estado del libro mayor; iii) Protocolo utilizado para generar consenso entre los participantes acerca de qué transacciones serán aceptadas, y en qué orden. La Figura 4 pretende dar una vista simple de un Ledger distribuido, cada nodo contiene una copia exacta del Blockchain, que actualiza a todos simultáneamente.

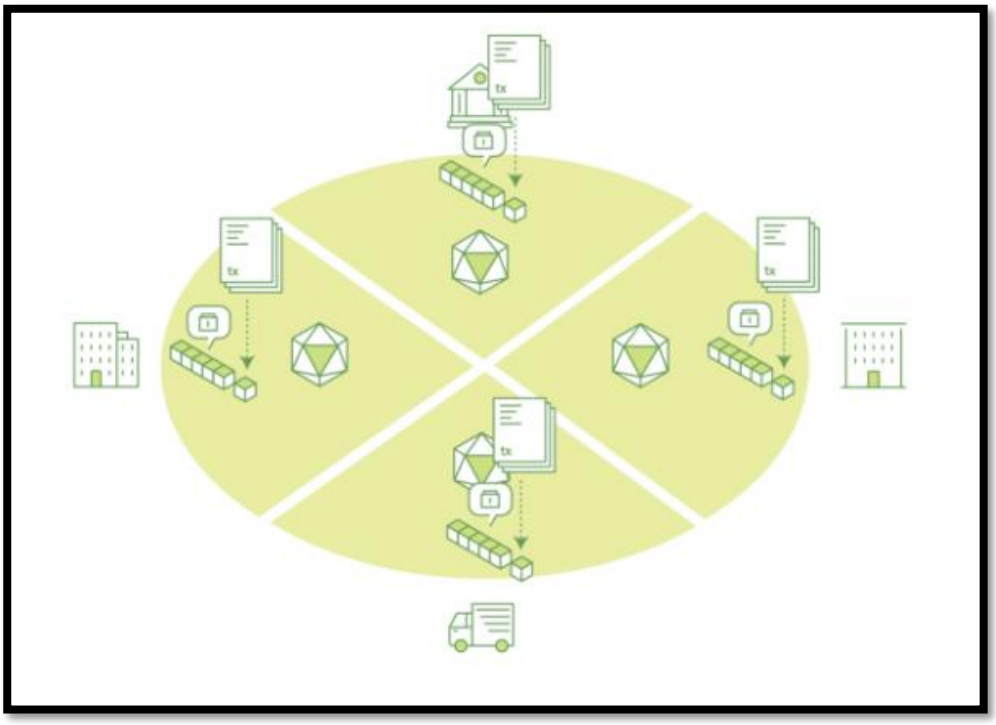

Figura 4. Ledger Distribuido
Fuente: (Hyperledger Fabric, 2017)

3.2 Tecnología Blockchain

De acuerdo con hyperledger.org, "Un Blockchain es un Ledger distribuido peer-to-peer forjado por consenso, combinado con un sistema para contratos inteligentes y otras tecnologías asistenciales". Los contratos inteligentes son simplemente programas informáticos que ejecutan acciones predefinidas cuando se cumplen ciertas condiciones dentro del sistema. El consenso se refiere a un sistema para asegurar que las partes acuerden un cierto estado del sistema como el estado verdadero.

Blockchain es una forma o subconjunto específico de tecnologías Ledger distribuidas, que construye una cadena cronológica de bloques, de ahí el nombre 'block-chain' o cadena de bloques. Un bloque se refiere a un conjunto de transacciones que se agrupan y se añaden a la cadena al mismo tiempo. Cada bloque almacena una cantidad determinada de transacciones. En la red de

Bitcoin, los mineros deben resolver un desafío criptográfico para proponer el siguiente bloque. Este proceso se conoce como "prueba de trabajo" y requiere una potencia de cálculo significativa (Gupta, 2017).

3.2.1 Inmutabilidad de los datos en Blockchain

La inmutabilidad de los datos que se encuentran en el Blockchain es quizás la razón más poderosa y convincente para implementar soluciones basadas en Blockchain para una variedad de procesos socioeconómicos que actualmente se registran en servidores centralizados. Esta característica de inmutabilidad o "inalterable en el tiempo" hace que la cadena de bloques sea útil para la contabilidad, las transacciones financieras, la administración de identidades, la propiedad, administración y transferencia de activos, solo por nombrar algunos ejemplos. Una vez que se escribe una transacción en la cadena de bloques, nadie puede cambiarla o, al menos, sería extremadamente difícil cambiarla (Weber et al., 2016).

De acuerdo con Antony Lewis, el Director de Investigación en R3, empresa de software dedicada el desarrollo de una plataforma de contabilidad distribuida, "Cuando la gente dice que las cadenas de bloques son inmutables, no significan que los datos no se puedan modificar, significan que es extremadamente difícil cambiar y si se lo intenta, es muy fácil detectar el intento ".

Es extremadamente difícil cambiar las transacciones en una cadena de bloques, porque cada bloque está vinculado al bloque anterior al incluir el Hash del bloque previo. Este Hash incluye el Hash de raíz de todas las transacciones en el bloque anterior. Si una sola transacción fuera a cambiar, no solo cambiaría el Hash raíz, sino también el Hash contenido en el bloque modificado. Además, cada bloque subsiguiente debería actualizarse para reflejar este cambio.

En la Figura 5, se muestran los bloques originales y las transacciones para el Bloque 11. Específicamente, la raíz para las transacciones en el Bloque 11 es Hash #ABCD, que es el hash combinado por las cuatro transacciones en este bloque. Si alguien intentaría cambiar la Transacción A por la Transacción A'. Esto, a su vez, modifica los hashes que se almacenan, y la raíz cambia a Hash # A'BCD. Además, el hash del Bloque Anterior almacenado en el Bloque 12 también necesita ser modificado para reflejar el cambio general en el hash para el Bloque 11. Por lo que mientras más transacciones se realicen será mucho más difícil cometer algún tipo de alteraciones.

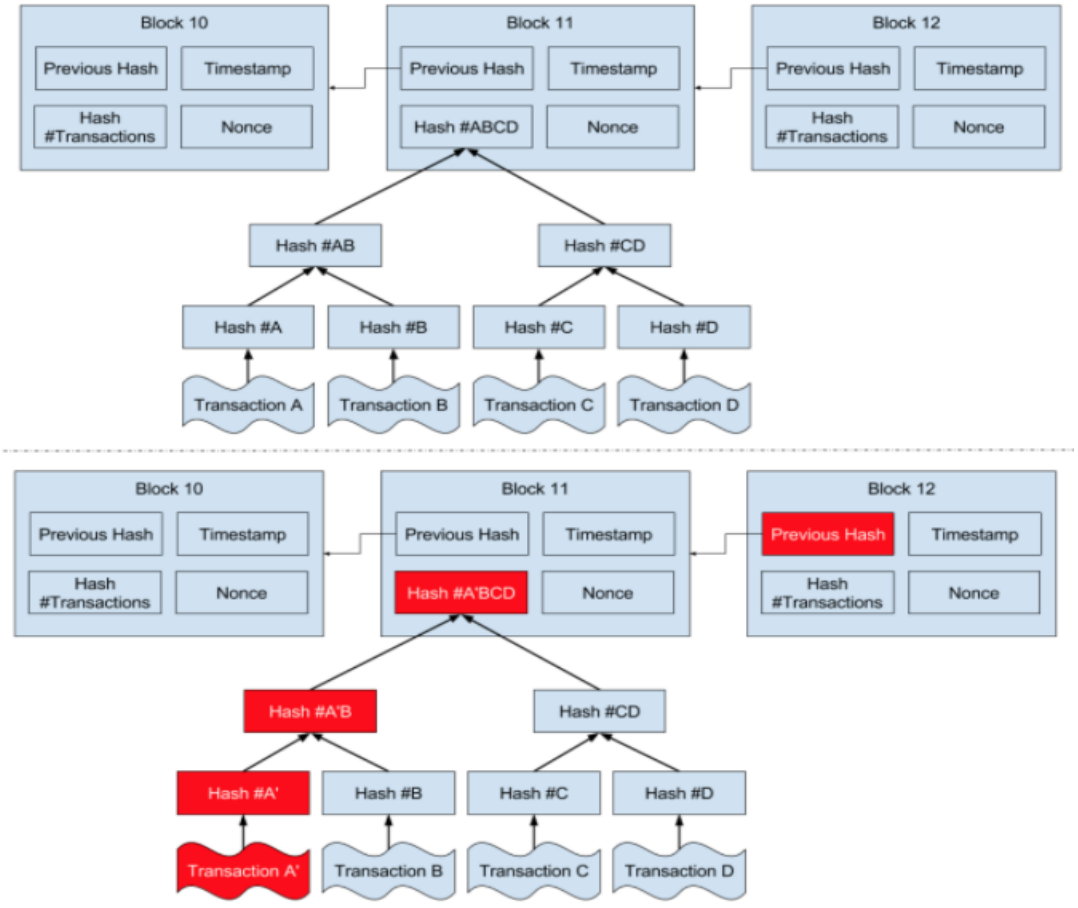

Figura 5. Inmutabilidad del Blockchain
Fuente: (The Linux Foundation and Hyperledger, 2017)

3.2.2 Tipos de Blockchain

Un Blockchain puede ser sin permiso, o estar autorizado. Un Blockchain sin permiso también se conoce como Blockchain público, porque cualquiera puede unirse a la red. Una cadena de bloques autorizada o cadena de bloques privada requiere una verificación previa de las partes miembro dentro de la red, y estas partes generalmente son conocidas entre sí (Weber et al., 2016).

Una cadena de bloques autorizada restringe a los actores que pueden contribuir al consenso del estado del sistema. En una cadena de bloques autorizada, solo un conjunto restringido de usuarios tiene los derechos para validar las transacciones en bloque.

La cadena de bloques sin permiso es todo lo contrario. Aquí cualquiera puede unirse a la red, participar en el proceso de verificación de bloque para crear consenso y también crear contratos inteligentes. Un buen ejemplo de Blockchain sin permisos son Bitcoin y Ethereum, donde cualquier usuario puede unirse a la red.

3.3 Algoritmos de consenso

El consenso se refiere al proceso de lograr un acuerdo entre los participantes de la red sobre el estado correcto de los datos en el sistema. El consenso lleva a que todos los nodos compartan exactamente los mismos datos. Por lo tanto, asegura que los datos en el libro mayor son los mismos para todos los nodos de la red y, a su vez, evita que los actores malintencionados manipulen los datos (edX, 2017). En 2015, Marc Andreessen, el decano de Silicon Valley, especificó al modelo de consenso distribuido de Blockchain como la invención más importante desde Internet (Crosby, 2016). Estos algoritmos de consenso varían con las diferentes implementaciones de Blockchain. A continuación, se explica una breve descripción de estos algoritmos.

3.3.1 Prueba de trabajo (PoW)

El algoritmo de consenso de prueba de trabajo implica resolver un desafío computacional con el fin de crear nuevos bloques en el Blockchain de Bitcoin. Coloquialmente, el proceso se conoce como 'minería', y los nodos de la red que se dedican a la minería se conocen como 'mineros'. La prueba de trabajo (PoW) es el resultado de un proceso de minería exitoso y, aunque la prueba es difícil de crear, es fácil de verificar. El incentivo para las transacciones mineras radica en los pagos económicos, donde los mineros que compiten son recompensados con 12.5 bitcoins y una pequeña tarifa de transacción (Aumasson, 2016).

Existen múltiples críticas para el algoritmo de consenso PoW, ya que requiere una gran cantidad de energía que se gastará, dado el algoritmo computacionalmente pesado. Además, PoW tiene una alta latencia de validación de transacciones, y la concentración de la potencia minera se encuentra en países donde la electricidad es barata. En términos de seguridad de la red, PoW es susceptible al “ataque de 51%”, que se refiere al ataque a una cadena de bloques por un grupo de mineros que controlan más del 50% de la potencia de computación de la red (edX, 2017).

3.3.2 Prueba de Estaca (PoS)

El algoritmo de prueba de estaca es una generalización del algoritmo de prueba de trabajo. En el trabajo de Vasin (2014), Blackcoin's proof-of-stake, explica que PoS tiene como objetivo reemplazar la forma de lograr el consenso en un sistema distribuido; en lugar de resolver la Prueba de trabajo, el nodo que genera un bloque debe proporcionar una prueba de que tiene acceso a una cierta cantidad de monedas antes de ser aceptado por la red. Al igual que en PoW, el proceso de generación de bloques se recompensará a través de tarifas de transacción En PoS, los nodos se

conocen como los "validadores" y, no se debe realizar una extracción, ya que todas las monedas existen desde el primer día.

En este algoritmo los nodos se seleccionan aleatoriamente para validar los bloques, y la probabilidad de esta selección aleatoria depende de la cantidad de participación que se tenga. La implementación específica de PoS puede variar, dependiendo del caso de uso, o como una cuestión de diseño de software. El algoritmo PoS ahorra costosos recursos computacionales que se gastan en la minería bajo un régimen de consenso PoW (Houy, 2014).

3.3.3 Prueba de tiempo transcurrido (PoET)

Propuesto por Intel, el algoritmo de consenso Prueba de tiempo transcurrido emula la Prueba de trabajo de estilo Bitcoin. En lugar de competir para resolver el desafío criptográfico y extraer el próximo bloque, como en el Blockchain de Bitcoin, el algoritmo de consenso PoET es un híbrido de una lotería aleatoria y de un orden de llegada. PoET aprovecha la informática para imponer tiempos de espera aleatorios en la construcción de bloque. El validador con el menor tiempo de espera para un bloque de transacción en particular es elegido líder. Este “líder” consigue crear el siguiente bloque de la cadena (Chen, 2017).

3.3.4 Tolerancia de falla bizantina redundante

Según Aublin, Mokhtar, y Quéma (2013), Byzantine Fault Tolerance o tolerancia a fallas bizantinas (BFT), es un protocolo de replicación que toleran fallas arbitrarias de una fracción de las réplicas. Los protocolos BFT no proporcionan un rendimiento aceptable cuando se producen fallas. Debido a que todos los protocolos BFT existentes que apuntan a alto rendimiento usan una réplica especial, llamada primaria, que indica a otras réplicas el orden en que las solicitudes deben

procesarse. Este primario puede ser malicioso y degradar el rendimiento del sistema sin ser detectado por réplicas correctas.

A fin de mejorar estos problemas los autores presentan Tolerancia de falla bizantina redundante, es un nuevo enfoque para el diseño de protocolos robustos de BFT. En RBFT, se ejecutan varias instancias de un protocolo BFT en paralelo. Cada instancia tiene una réplica principal. Las diversas réplicas primarias se ejecutan en diferentes máquinas. Mientras que todas las instancias de protocolo realizan solicitudes, solo una instancia (llamada instancia maestra) las ejecuta de manera efectiva.

Otras instancias (llamadas instancias de copia de seguridad) ordenan las solicitudes para comparar el rendimiento que alcanzan con el logrado por la instancia maestra. Si la instancia maestra es más lenta, el principal de la instancia maestra se considera en paralelo sin esperar la recepción de respuestas de solicitudes anteriores.

De hecho, en un sistema de circuito cerrado, la tasa de solicitudes entrantes estaría condicionada por la tasa de la instancia maestra. Dicho de otra manera, las instancias de respaldo nunca serían más rápidas que la instancia maestra. RBFT además implementa un mecanismo de equidad entre los clientes al monitorear la latencia de las solicitudes, lo que asegura que las solicitudes de los clientes se procesen de manera justa.

3.4 Comparación de los algoritmos de consenso

El consenso puede implementarse de diferentes maneras, como mediante el uso de algoritmos basados en la lotería, Prueba de tiempo transcurrido (PoET) y Prueba de trabajo (PoW) o mediante el uso de métodos basados en votación, incluida Tolerancia redundante a errores

bizantinos (RBFT). Cada uno de estos enfoques se dirige a diferentes requisitos de red y modelos de tolerancia a fallas (Chen, 2017).

Los algoritmos basados en lotería son ventajosos porque pueden escalar a una gran cantidad de nodos, ya que el ganador de la lotería propone un bloqueo y lo transmite al resto de la red para su validación. Por otro lado, estos algoritmos pueden conducir a bifurcaciones cuando dos "ganadores" proponen un bloqueo. Cada tenedor debe resolverse, lo que resulta en un tiempo más largo para la finalidad (Aublin, 2013).

Los algoritmos basados en votación son ventajosos ya que proporcionan una finalidad de baja latencia. Cuando la mayoría de los nodos valida una transacción o bloque, existe consenso y ocurre la finalidad. Debido a que los algoritmos basados en votación típicamente requieren que los nodos transfieran mensajes a cada uno de los otros nodos en la red, mientras más nodos existan en la red, mayor será el tiempo necesario para alcanzar el consenso. Esto resulta en una compensación entre escalabilidad y velocidad.

Hyperledger supone que las redes de cadenas de negocio funcionarán en un entorno de confianza parcial. Por lo que no incluye enfoques de consenso estándar de prueba de trabajo con los mineros anónimos. Debido a que estos enfoques imponen un costo demasiado grande en términos de recursos y tiempo para ser óptimos para las redes comerciales de cadenas de bloques (Hyperledger, 2017). La Figura 6 ofrece una vista rápida de las principales consideraciones, los pros y los contras de los diferentes enfoques comerciales de Blockchain para llegar al consenso.

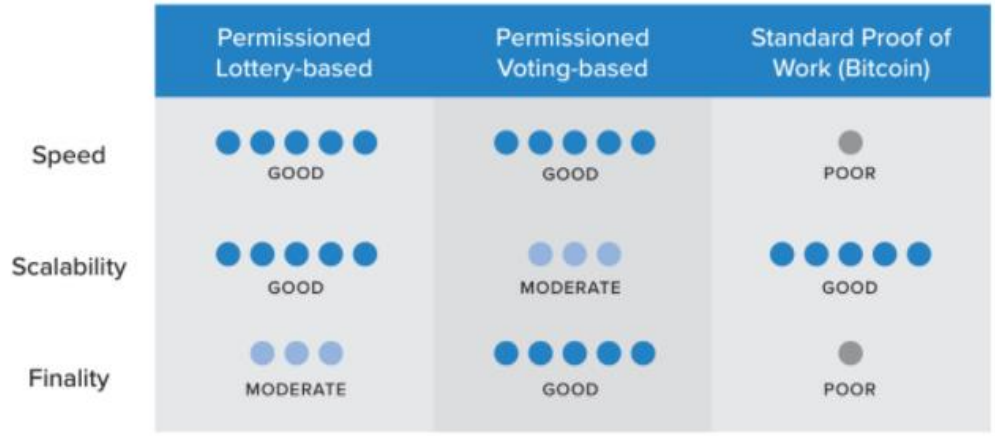

Figura 6. Comparación de enfoques de consenso permisibles y POW estándar
Fuente: (Hyperledger, 2017)

3.5 Contrato Inteligente

El código de contrato inteligente se refiere a software escrito en un lenguaje de programación. Actúa como un agente de software o delegado con la intención de que cumpla con ciertas obligaciones, ejerza los derechos y pueda tomar el control de los activos dentro de un libro mayor distribuido de manera automatizada. De forma que los contratos inteligentes permiten realizar transacciones de forma segura sin terceros de confianza. En el caso de incumplimientos, garantiza que las partes honestas obtengan una compensación acorde a lo estipulado (Kosba, 2016).

3.6 Blockchain de Bitcoin

Bitcoin es la mejor carta de presentación de Blockchain. Bitcoin es una moneda criptográfica o moneda digital creada en 2009 por una persona o grupo denominado Satoshi Nakamoto, que no requiere una institución intermediaria para realizar pagos, las transacciones las realiza a través de una red descentralizada con una infraestructura distribuida y de propiedad pública, que funciona como un sistema "sin permiso", consta de varios nodos donde cada nodo contiene una réplica exacta de la información de estas transacciones (Nakamoto, 2008).

La popularidad de Bitcoin también trajo controversias ya que ayuda a habilitar un mercado global multimillonario de transacciones anónimas sin un control gubernamental. Por lo tanto, tiene que lidiar con una serie de regulaciones y cuestiones que involucran a los gobiernos nacionales e instituciones financieras (Crosby, 2016).

En concordancia con el sitio Web Coin Market Capitalizations, a partir de octubre de 2017, la capitalización bursátil de Bitcoin fue de casi $ 100 mil millones. Según AngelList (2017), se han creado más de mil nuevas empresas para aprovechar las tecnologías relacionadas con Bitcoin y Blockchain desde el inicio del sistema de pago Bitcoin. Cientos de grandes empresas y docenas de gobiernos y universidades se han involucrado activamente en la investigación, prueba y creación de prototipos de protocolos, plataformas y aplicaciones de Blockchain. En particular, el sector de servicios financieros ha estado invirtiendo activamente en la exploración de aplicaciones más amplias de tecnologías de contabilidad distribuida, de las cuales Blockchain es un subconjunto, desde finales de 2015.

3.7 Usos de Blockchain en la industria y sociedad

La hipótesis principal es que Blockchain establece un sistema para crear un consenso distribuido del mundo en línea. Por lo que varios autores definen los posibles escenarios para aprovechar los beneficios de Blockchain, algunos de los cuales se describen a continuación.

El mercado de las criptomonedas se ha beneficiado de esta tecnología, con una computación auditable y de confianza, lo que es posible utilizando una red descentralizada de pares acompañada de un libro público, que realizar transacciones sin la necesidad de pasar por diferentes entidades (Zyskind, 2015).

En el trabajo titulado “Blockchain technology: Beyond Bitcoin” los autores mencionan algunas alternativas de Blockchains sugeridas para implementar aplicaciones como DNS, autoridad de certificación SSL, almacenamiento de archivos, proceso de conozca a su cliente (KYC) y votación electrónica.

Christidis y Devetsikiotis (2016) en su trabajo “Blockchains and smart contracts for the Internet of things” concluyen que la combinación Blockchain y el Internet de las cosas, es poderoso y puede causar transformaciones significativas en varias industrias, allanando el camino para nuevos modelos de negocio y aplicaciones novedosas y distribuidas.

Empresas como IBM, Samsung, Overstock, Amazon, Ebay, Verizon Wireless y muchas más, están explorando usos alternativos y novedosos de la cadena de bloques para sus propias aplicaciones. Nueve de los bancos más grandes del mundo, incluidos Barclays y Goldman Sachs5, se unieron recientemente con la firma de tecnología financiera R3 en septiembre de 2015 con el fin de crear un marco para el uso de la tecnología Blockchain en el mercado financiero (Crosby, 2016).

3.8 Limitaciones de Blockchain

Una de las limitaciones de Blockchain es la Complejidad, ya que aplica conceptos nuevos, o poco comunes. Los principales son contratos inteligentes, criptografía y algoritmos de consenso. En caso de que una cadena de bloques no tenga una red sólida con una red de nodos bien distribuida, tal vez no sea posible obtener el máximo beneficio de dicha tecnología. Ya que mientras más grande la red, el libro mayor distribuido tiene más registros lo que mejora la integridad de la información que alberga y la vuelve más segura (Angraal, Krumholz, & Schulz, 2017).

La falla, también conocida como "ataque del 51%", se refiere a una situación en la que un grupo de "mineros" de alguna manera toma el control de más de la mitad de la potencia de

computación de la red Blockchain. Es una ocurrencia teóricamente posible, ya que la red de Bitcoin es gratuita y abierta. En otras palabras, si un minero o un grupo de mineros logran de alguna manera adquirir suficiente poder de cómputo, lo cual es un esfuerzo muy costoso. No existe una autoridad centralizada para evitar que influyan en toda la red de Bitcoin (Aumasson, 2016).

3.9 Seguridad en Blockchain

El Internet de las cosas está empezando a aprovechar las características de seguridad que presta Blockchain. El trabajo “Blockchain for IoT security and privacy: The case study of a smart home” muestra un caso exitoso de seguridad en un hogar inteligente basado en Blockchain, mediante un análisis enfocado a confidencialidad, integridad y disponibilidad. También Aitzhan,y Svetinovic (2016) presentan un sistema de comercio de energía descentralizado, que utiliza la seguridad de Blockchain principalmente para las transacciones comerciales. A continuación, se describen algunas características sobresalientes en cuanto a la seguridad de Blockchain.

Una cadena de bloques de Blockchain está conectada a todos los bloques antes y después de él. Esto hace que sea difícil alterar un solo registro porque un pirata informático tendría que cambiar el bloque que contiene ese registro, así como los vinculados a él para evitar la detección.

Los registros en una cadena de bloques están asegurados a través de la criptografía. De acuerdo con IBM (2018) los participantes de la red tienen sus propias claves privadas que se asignan a las transacciones que realizan y actúan como una firma digital personal. Si se altera un registro, la firma se volverá inválida y la red sabrá de inmediato que algo ha sucedido.

Los Blockchain están descentralizados y distribuidos a través de redes peer-to-peer que se actualizan continuamente y se mantienen sincronizadas. Aumasson (2016) sostiene que, al no estar contenidos en una ubicación central, las cadenas de bloques no tienen un solo punto de falla y no

se pueden cambiar desde una sola computadora. Por lo que requeriría enormes cantidades de potencia informática para acceder a cada instancia, o al menos una mayoría de una determinada cadena de bloques y modificarlas todas al mismo tiempo.

De acuerdo con Karame (2016), se espera que la cadena de bloques estimule cambios considerables en cuanto a la seguridad de la información, en una gran cantidad de productos y tendrá un impacto positivo en la experiencia digital de muchas personas en todo el mundo.

3.10 Frameworks de Blockchain

A partir de la popularidad que adquiere la criptomoneda Bitcoin se descubre del potencial de la tecnología Blockchain. Por lo que aparecen varios proyectos enfocados al desarrollo de esta nueva tecnología.

3.10.1 Ethereum

En el 2014 empieza el desarrollo del proyecto Ethereum, el cual permite crear aplicaciones con un Blockchain personalizado. El principal objetivo de Ethereum es facilitar transacciones confiables entre personas y que de otro modo no tendrían los medios para confiar el uno en el otro. Para lo cual utiliza contratos inteligentes, donde se aplica los acuerdos establecidos de forma automática (Ethereum, 2017).

En Ethereum, todos los participantes deben llegar a un consenso sobre el orden de todas las transacciones. El orden de las transacciones es concluyente para la consistencia del libro mayor. Si no se puede establecer un orden de transacciones definitivo, podría producirse registros dobles o algún tipo de inconsistencia. El Blockchain de Ethereum es público por lo que podría involucrar a partes no confiables y anónimas. Entonces se debe emplear un mecanismo de consenso que proteja

el libro mayor contra los participantes fraudulentos para lo cual utiliza el algoritmo de prueba de trabajo (Wood, 2014).

Ethereum se desenvuelve bajo su propia criptomoneda denominada Ether. Según el portal CoinMarketCap, Ether es la segunda criptomoneda más popular hasta el momento, después de Bitcoin y osila entre los $459, esto ha variado en los últimos meses con altas y bajas. Se utiliza para pagar recompensas a los nodos que contribuyen a llegar a un consenso mediante bloques de minería, también para pagar las tarifas de transacción.

3.10.2 Multichain

En 2015 aparece el proyecto de código abierto Multichain, para construir y desplegar aplicaciones Blockchain. Promete un desarrollo amigable, un despliegue rápido y ayudar a mejorar la seguridad.

MultiChain es una plataforma de código abierto para Blockchains privados, que ofrece un extenso conjunto de características que incluyen amplia capacidad de configuración, implementación rápida, administración de permisos, activos nativos y flujos de datos. MultiChain proporciona la máxima compatibilidad con el ecosistema bitcoin, incluido el protocolo peer-to-peer, los formatos de transacción, bloque y APIs. MultiChain está licenciado bajo la licencia de código abierto GPLv3 (MultiChain , 2018).

3.10.3 Corda

Corda es una plataforma de contabilidad distribuida de código abierto, diseñado para empresas, que admite múltiples proveedores de consenso y se puede emplear diferentes algoritmos en la misma red.

Corda elimina costosas fricciones en las transacciones comerciales al permitir a las empresas realizar transacciones directamente. Al utilizar la tecnología de contrato inteligente y Blockchain, Corda permite desplegar redes empresariales existentes para reducir los costos de transacción y mantenimiento de registros y simplificar operaciones de negocios (Corda Enterprise., 2018).

El consenso en Corda realiza la transacción involucrando solo a las partes. La validez se garantiza ejecutando el código de contrato inteligente asociado con una transacción, verificando todas las firmas requeridas y asegurando que todas las transacciones a las que se hace referencia también sean válidas. La unicidad se refiere a los estados de entrada de una transacción. Específicamente, se debe garantizar que la transacción en cuestión sea el único consumidor de todos sus estados de entrada. El algoritmo BFT, se puede aplicar en Corda.

3.10.4 Hyperledger

Otro proyecto es Hyperledger, es un esfuerzo de código abierto en busca de avances para la tecnología Blockchain organizado por The Linux Foundation, es una colaboración global de más de cien miembros de diversas industrias y organizaciones, algunas de ellas son IBM, CISCO, HUAWEI, INTEL, entre otras (Linux Foundation, 2017). A continuación, se describen los frameworks que Hyperledger alberga.

Hyperledger Burrow

Hyperledger Burrow fue lanzado en diciembre de 2014. Actualmente se encuentra bajo incubación. Hyperledger Burrow es una máquina de contratos inteligentes que proporciona un cliente modular de Blockchain con un intérprete de contrato inteligente construido en parte para la

especificación de la máquina virtual Ethereum (EVM). Dentro del Proyecto Burrow, EVM es el intérprete de contratos inteligentes que se ejecutan en la red de Ethereum (Hyperledger , 2018).

Hyperledger Indy

Hyperledger Indy es un ledger distribuido especialmente diseñado para la identidad descentralizada. Contribuido por la Fundación Sovrin, Hyperledger Indy permite a las personas administrar y controlar sus identidades digitales. Actualmente se encuentra en estado de incubación (Hyperledger, 2018).

Uno de los principios clave de Hyperledger Indy es su enfoque a la privacidad por diseño. Dada la naturaleza inmutable del Ledger Distribuido, es aún más importante que las identidades digitales se manejen con sumo cuidado.

Hyperledger Iroha

Iroha es un es un marco de Blockchain hospedados por The Linux Foundation, que fue aportado originalmente por los desarrolladores japoneses Soramitsu, Hitachi, NTT Data y Colu (Hyperledger, 2017).

Iroha se muestra como una construcción simple; diseño moderno y orientado al dominio de C ++. Está enfocado al desarrollo de aplicaciones móviles y utiliza un nuevo algoritmo de consenso tolerante a errores bizantinos. Está diseñado para ser sencillo y fácil de incorporar en proyectos que requieren tecnología ledger distribuida. Actualmente este framework se encuentra en estado Activo.

Hyperledger Fabric

Hyperledger Fabric fue aportado inicialmente por Digital Asset e IBM, este framework proporciona una arquitectura modular, que permite que los componentes como el consenso y los

servicios de membresía sean plug-and-play. Es revolucionario al permitir que las entidades realicen transacciones confidenciales sin pasar información a través de una autoridad central. Esto se logra por medio de diferentes canales que se ejecutan dentro de la red, así como la división del trabajo que caracteriza a los diferentes nodos. A diferencia de un Blockcahin público como el de Bitcoin, Hyperledger Fabric admite implementaciones autorizadas. Aprovecha la tecnología de contenedores para alojar contratos inteligentes denominados "chaincode" que concentran la lógica del negocio. Este proyecto se encuentra en estado activo, y actualmente se encuentran contribuyendo 159 ingenieros y 28 organizaciones (Hyperledger, 2017).

De acuerdo con Brian Behlendorf, Director Ejecutivo de Hyperledger, lo más distintivo de Fabric hasta el momento es que utiliza canales privados para compartir datos solo con ciertas partes.

3.11 Evaluación entre los frameworks de Blockchain

A continuación, se realiza una comparativa entre los Frameworks presentados, con el objetivo de definir el más adecuado para utilizarse en identidades digitales. Para la comparación de Hyperledger se utilizó en Fabric.

De los proyectos que alberga Hyperledger el más adecuado para el tema de identidades digitales es Indy. Hyperledger Indy se focaliza exclusivamente en el manejo de identidades digitales y muestra un escenario idóneo del comportamiento de los participantes. Sin embargo, actualmente el proyecto se encuentra en estado de incubación, por lo que aún no se puede desarrollar un aplicativo estable con este framework. También se descarta a Burrow por su estado de incubación, además de que se comporta como un complemento de los contratos de Ethereum. Iroha se centra en Blockchain para aplicaciones móviles que por ahora no es de relevancia para el objetivo de esta tesis. Entonces el proyecto seleccionado para representar en esta comparativa es

Hyperledger Fabric. Su principal característica es la privacidad que mantiene a través de canales, el uso de certificados digitales, flexibilidad para implementar diferentes escenarios, contratos inteligentes y facilidad para modelar las reglas de negocio. Además, se tomó en cuenta su estado activo, que es el proyecto más estable de Hyperledger. Fabric tiene más de 100 ingenieros contribuyendo, cuenta con una amplia documentación, blogs y foros que ofrecidos por la comunidad que lo respalda, etc.

Se ha realizado una comparación entre los frameworks Hyperledger, Ethereum, Corda y Multichain, resumidos en la Tabla 1. Se ha tomado los aspectos más relevantes para la comparativa como: Descripción de la plataforma; nombre de la organización que alberga los proyectos; Moneda, se refiere a las criptomonedas que se han popularizado en los últimos meses; Recompensa Minera, el pago que se da por la prestación de recursos computacionales para procesar los algoritmos de consenso; Forma de almacenamiento de la información; Algoritmo de consenso (ver sección 3.3); Modo de operación, forma de acceder al Blockchain; Contratos Inteligentes (ver sección 3.5); Consenso, participación de los usuarios para llegar lograr un acuerdo y los Sistemas Operativos que soportan estos frameworks.

Tabla 1
Comparativa entre Frameworks de Blockchain

	Hyperledger	**Ethereum**	**Corda**	**Multichain**
Descripción de la plataforma	Blockchain de propósito general	Blockchain de propósito general	Blockchain de propósito financiero	Pagos Blockchain
Organización	Fundación Linux	Ethereum	R3	Multichain
Moneda	Ninguna	Ether	Ninguna	Permite crear activos (monedas)
Recompensa Minera	N / A	Sí	N / A	Si
Almacenamiento	Base de datos de valores clave	Datos de la cuenta	Base de datos de valores clave	Datos de la transacción
Algoritmo de consenso	RBFT (Dependiendo de los requisitos específicos de la aplicación se pueden utilizar varios algoritmos)	Minería basada en Prueba de Trabajo (PoW)	BFT	Mineria basada en Prueba de Trabajo (PoW)
Modo de operación	Bajo permisos (privado)	Público o privado	Bajo permisos (privado)	Público
Contratos Inteligentes	Varios lenguajes de programación como Java, GO.	Lenguaje de programación 'Solidity'	Lenguajes de programación como Kotlin y Java	Lenguajes de programación como Go y Java
Consenso	Llegan a consenso solo los involucrados (mejora la escalabilidad, rendimiento y privacidad).	Todos deben llegar a consenso, aunque no tengan participación (afecta el desempeño de la red)	Llegan a consenso solo los involucrados (mejora la escalabilidad, rendimiento y privacidad).	Todos deben llegar a consenso, aunque no tengan participación
Sistemas Operativos	Linux, MAC y Windows	Linux, MAC y Windows	MAC y Windows	Linux y Windows

Para el objetivo de identidades digitales se ha decidido descartar a Ethereum, debido a que las transacciones las realiza bajo su moneda Ether, el segundo inconveniente es que utiliza la minería basada en Prueba de Trabajo (PoW) para validar las transacciones y llegar a un consenso, lo que consume cuantiosos recursos en la capacidad del computador y energía.

También se descarta a Multichain ya que se maneja a base de activos, simulando una criptomoneda, lo que impide la flexibilidad que se requiere para el objetivo principal de este trabajo sobre identidades digitales, y al igual que Ethereum utiliza minería basada en Prueba de Trabajo (PoW) para llegar a un consenso en las transacciones.

Corda es una opción para soluciones de Blockchain empresariales, sin embargo, para no presta la flexibilidad para la construcción de un escenario que simule el manejo de las identidades digitales, ya que su enfoque es netamente empresarial.

Se ha decidido enfocarse en Hyperledger debido a las variaciones que utiliza para evitar la minería, la flexibilidad, la privacidad que ofrece los canales, la comunidad que lo respalda con grandes organizaciones y cientos de ingenieros que aportan a este proyecto.

CAPÍTULO IV

DISEÑO E IMPLEMENTACIÓN DEL PROTOTIPO PROPUESTO

Como guía para la planificación, desarrollo y evolución del proyecto se ha basado en la metodología ágil de desarrollo de software SCRUM, ya que según Trigas (2012), “Scrum aparece como una metodología destinada a los productos tecnológicos que se caracterizan por tener entornos de incertidumbre, auto-organización y control moderado. Se basa en la idea de crear ciclos breves de desarrollo llamados iteraciones o Sprints”.

En la Figura 7 se puede visualizar las actividades de la metodología Scrum, que constan de: (i) Selección de los requisitos; (ii) Planificación de la iteración; (iii) Ejecución de la iteración; (iv) Demostración de los requisitos completos; (v) Retrospectiva; (vi) Refinamiento de la lista de requisitos y cambios en el proyecto. La metodología establece para cada actividad el personal involucrado, el tiempo y la forma de ejecución (Proyectos agiles - Funcionamiento, 2017). A continuación, se muestra la implementación del prototipo.

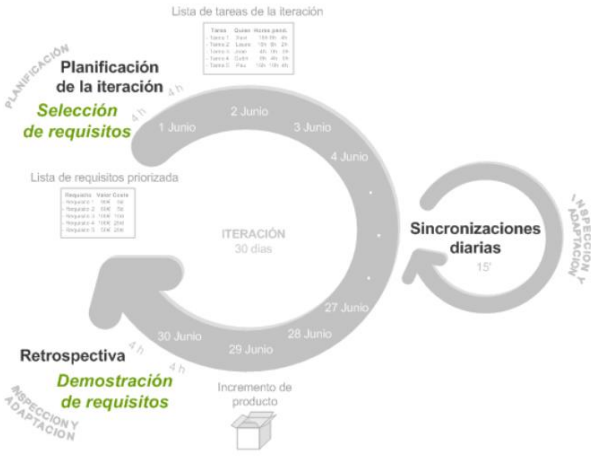

Figura 7. Metodología Scrum
Fuente: (Proyectos agiles -Funcionamiento, 2017)

4.1 Diseño propuesto para identidades digitales aplicando tecnología Blockchain

En esta sección se detalla la primera y segunda actividad de SCRUM. Para lo que se han definido las historias de usuario con base en la investigación sobre Identidad Digital del capítulo 2 y el framework Hyperledger Fabric seleccionado en el capítulo 3. Para la etapa de planificación se diseñó, los diagramas de casos de uso, secuencia, la estructura de base de datos y diagrama de arquitectura.

4.1.1 Selección de requisitos

Schwaber & Sutherland (2013) describen a una historia de usuario como una funcionalidad que debe incorporar un sistema, y cuya implementación aporta valor al cliente. A continuación, las historias de usuario en las tablas [2 - 6]; que se han identificado en base al estudio realizado en el capítulo 2 sobre Identidades Digitales, orientadas a la propuesta del manejo de Identidad Digital a través de la tecnología Blockchain.

Tabla 2
Historia de usuario UH001

Id	UH001
Nombre	Crear identidades digitales.
Descripción	Un administrador podrá registrar la información de los usuarios para crear la identidades.
Entradas	Cédula, Nombres, Apellidos, Dirección, Fecha de nacimiento, Lugar de nacimiento, Género, Nacionalidad y Estado civil.
Salidas	Mensaje de confirmación de identidad creada correctamente.
Proceso	1. Ingresar todos los valores. 2. Validar la información en el nodo.

Continua

	3. Registrar la identidad en el Blockchain.
Precondiciones	Ingresar al sistema con perfil Administrador.
Post condiciones	El administrador habrá creado la identidad digital. Identidad registrada en el Blockchain.
Prioridad	Alta
Rol que lo ejecuta	Administrador y Usuario

Tabla 3
Historia de usuario UH002

Id	UH002
Nombre	Consultar la información del usuario.
Descripción	El usuario podrá visualizar la información que almacena su identidad digital.
Entradas	Tarjeta de red empresarial
Salidas	Toda la información almacenada sobre el usuario.
Proceso	1. Identificarse. 2. Visualizar la información.
Precondiciones	La identidad digital del usuario debe estar creada.
Post condiciones	El usuario conocerá toda la información almacenada sobre él.
Prioridad	Alta
Rol que lo ejecuta	Usuario

Tabla 4
Historia de usuario UH003

Id	UH003
Nombre	Actualizar la información del usuario.
Descripción	Solo el administrador y el propietario de la identidad digital puede actualizar su información.
Entradas	Tarjeta de red empresarial
Salidas	Mensaje de confirmación de identidad actualizada correctamente
Proceso	1. Identificarse 2. Actualizar información en el Blockchain.
Precondiciones	La identidad digital del usuario debe estar creada.
Post condiciones	El usuario habrá actualizado la identidad digital. Actualización del Blockchain.
Prioridad	Media
Rol que lo ejecuta	Usuario

Tabla 5
Historia de usuario UH004

Id	UH004
Nombre	Permitir el acceso a la información del usuario.
Descripción	El usuario puede compartir su información con otra persona o con una empresa/entidad.
Entradas	Tarjeta de red empresarial
Salidas	Se agrega la persona o empresa a la lista de entidades con quien el usuario ha compartido la información.

Continua

Proceso	1. Identificarse 2. Dar permiso de acceso a su información
Precondiciones	La identidad digital del usuario debe estar creada.
Post condiciones	El usuario habrá compartido su información con otra persona o entidad. Actualización en el Blockchain.
Prioridad	Alta
Rol que lo ejecuta	Usuario

Tabla 6
Historia de usuario UH005

Id	UH005
Nombre	Revocar el acceso a la información del usuario.
Descripción	El usuario puede revocar el permiso para compartir su información con otra persona o con una empresa/entidad.
Entradas	Tarjeta de red empresarial
Salidas	Se elimina la persona o empresa, que se ha revocado el acceso, de la lista de entidades con quien el usuario comparte su información.
Proceso	1. Identificarse 2. Revocar el acceso a su información
Precondiciones	La entidad seleccionada debió haber tenido acceso a la información del usuario.
Post condiciones	El usuario habrá revocado el permiso para compartir su información con otra persona o entidad. Actualización en el Blockchain. Registro de evento

Continua

Prioridad	Alta
Rol que lo ejecuta	Usuario

Requerimientos de Seguridad

- El sistema mantendrá la confidencialidad de la información.
- El sistema manejará de manera íntegra la información almacenada.
- El sistema manejará la disponibilidad de información de acuerdo a los niveles de acceso que tenga el usuario.
- El sistema no expondrá al público la información de los participantes.

4.1.2 Diagramas de casos de uso

De acuerdo con (Pressman, 2010) un caso de uso describe el comportamiento sobre cómo interactúa el usuario final con el sistema en situaciones determinadas. A continuación, se identifican los casos de uso que se aplican para la propuesta del manejo de Identidad Digital.

Los casos de uso definidos para el Administrador de la red se los puede apreciar en la Figura 8. El administrador puede acceder al portal, crear las identidades digitales con los datos definidos en la historia de usuario UH001, visualizar y editar la información de los usuarios.

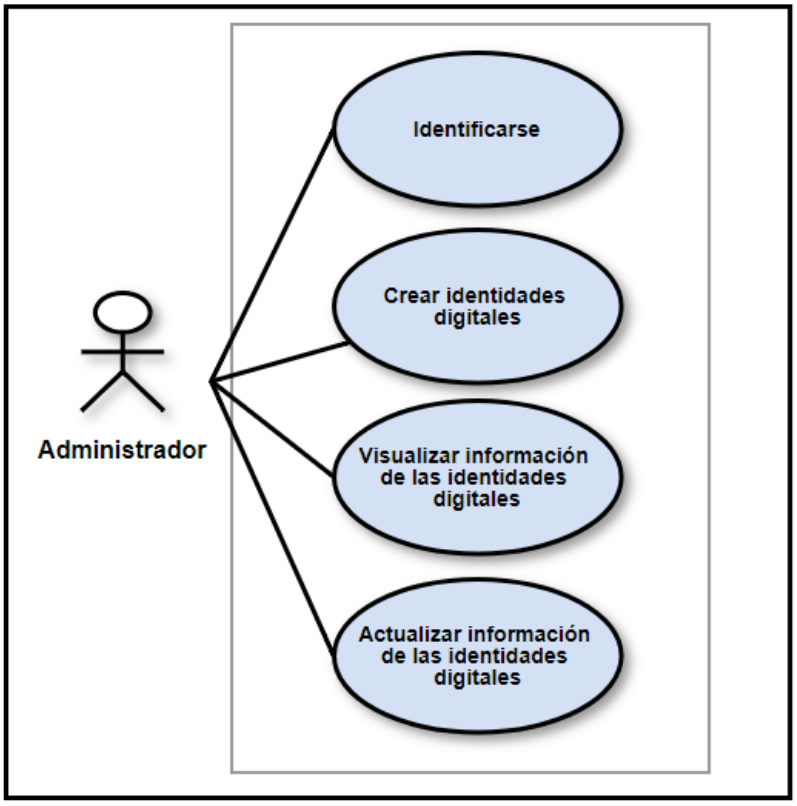

Figura 8. Casos de uso – Administrador

En la Figura 9 se muestran los casos de uso para una persona. La persona debe identificarse, puede visualizar y editar solo su información. Además, puede dar permiso para que una persona o empresa tenga acceso a la información de su identidad digital, de igual forma puede revocar estos permisos para dejar de compartir esta información.

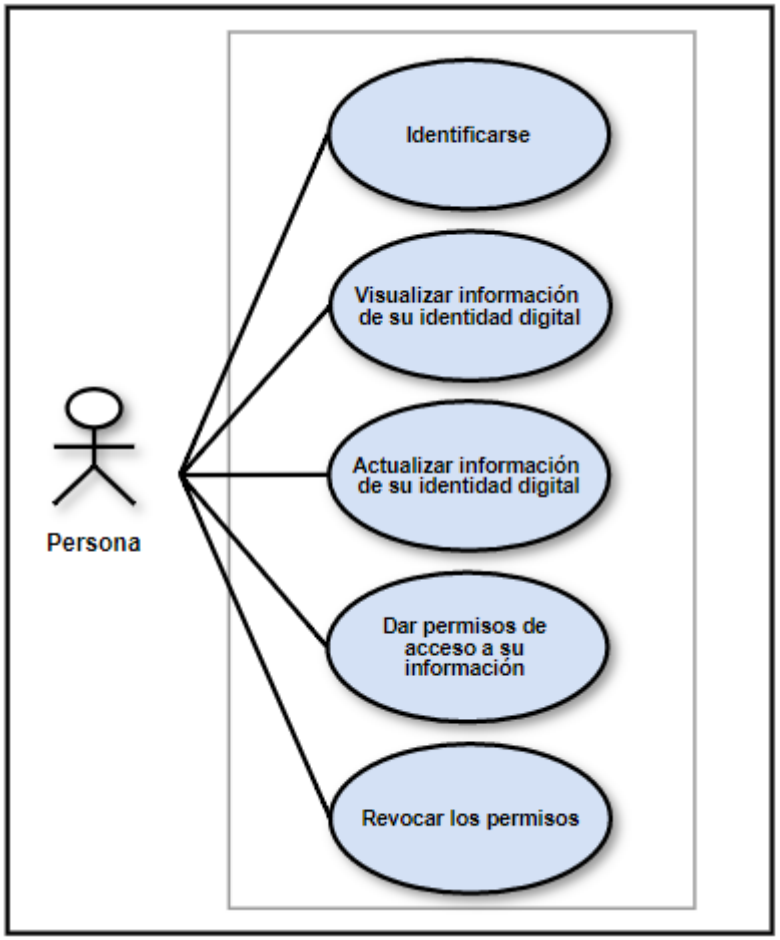

Figura 9. Casos de uso – Persona

En cuanto a la empresa, los casos de uso para este participante se muestran en la Figura 10. La empresa debe identificarse y puede ver únicamente la información de los clientes quienes dieron su autorizaron para compartir la información de su identidad digital con la empresa seleccionada.

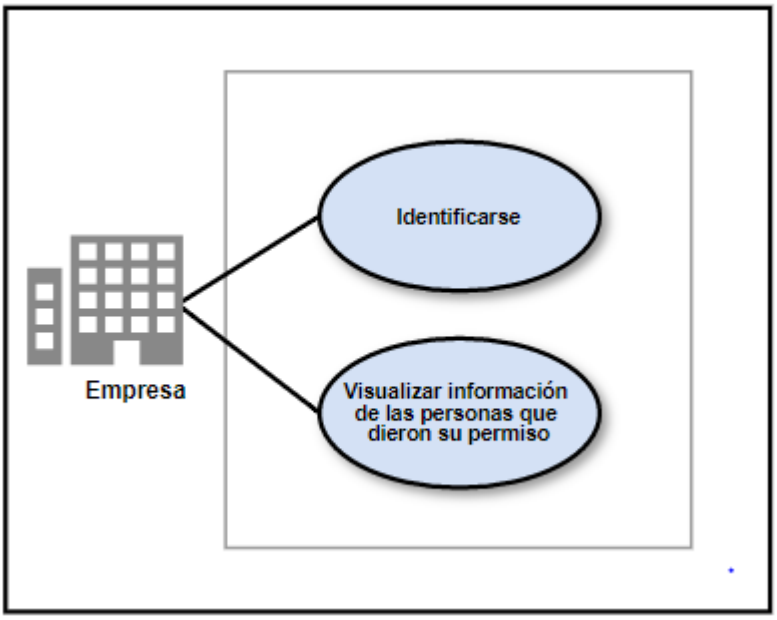

Figura 10. Casos de uso – Empresa

4.1.3 Diagrama de secuencia

Un diagrama de secuencia se utiliza para mostrar las interacciones entre los objetos en el orden secuencial en que ocurren durante un escenario concreto (Booch, 1999). En la Figura 11 se puede observar la secuencia para el registro de la identidad digital, donde el Administrador puede ingresar al portal y registrar su información para crear su identidad. Esta información pasará a un nodo que valida la integridad de estos datos. Una vez validada esta información se agrega al Blockchain, y esta cadena es replicada en todos los nodos miembro de la red.

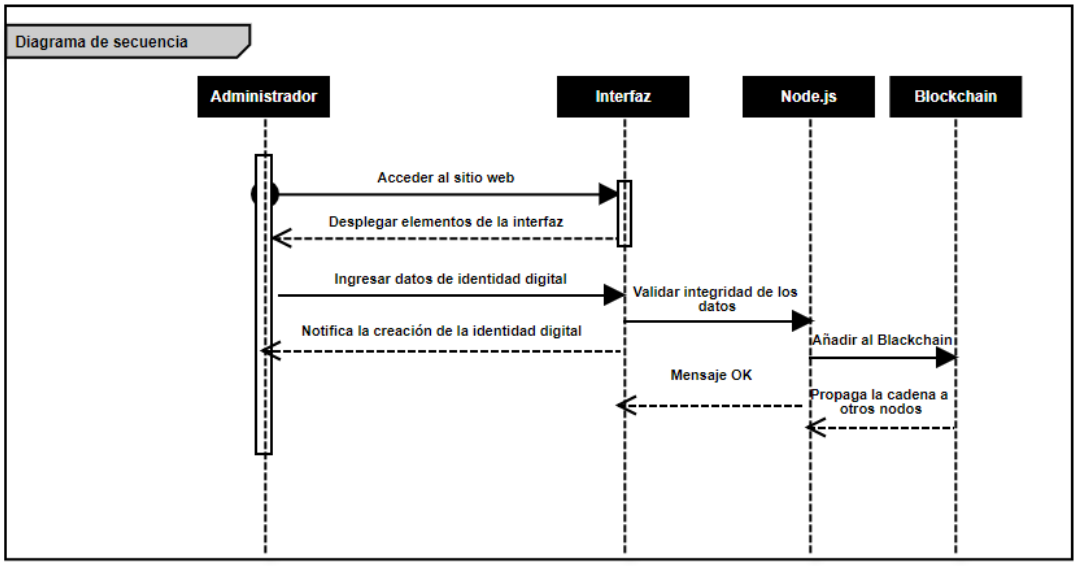

Figura 11. Escenario: Creación de identidad digital

Dentro de los principios de la identidad digital se establece que el propietario de esta identidad debe conocer los datos almacenado sobre sí mismo. En la Figura 12 se presenta el escenario de consulta del usuario hacia el Blockchain, a través de un API para consultas, que devuelve una trama de respuesta en formato JSON.

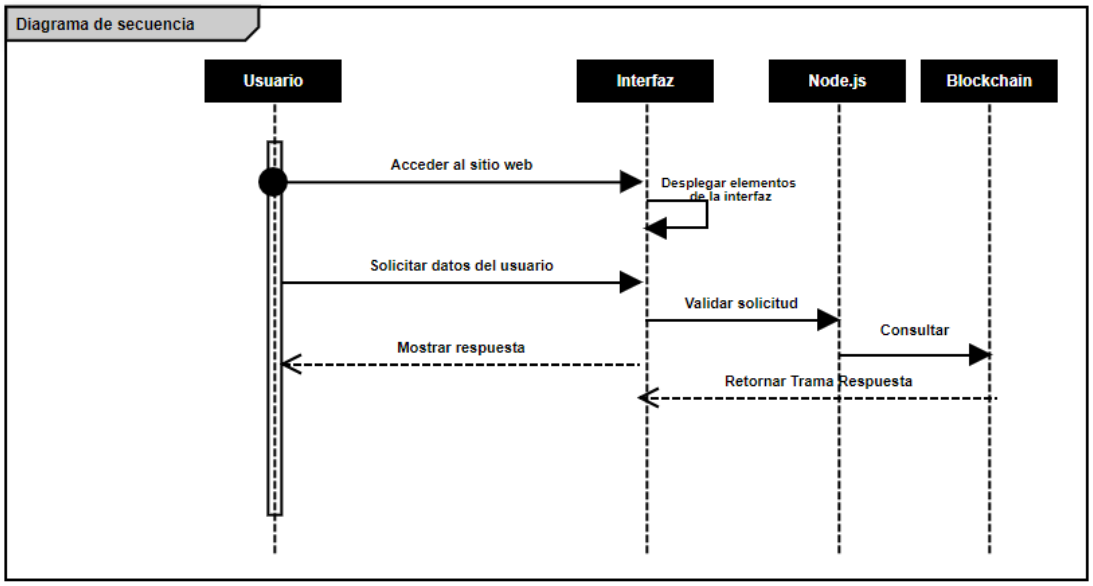

Figura 12. Escenario: Visualizar información de identidad digital

En la Figura 13 se ilustra el diagrama de secuencia que explica como el usuario actualiza la información, para esto realiza una solicitud de actualización. Desde el Blockchain se trae a la interfaz la información actual del usuario. El usuario modifica los datos, se valida los cambios en un nodo, se añade al Blockchain, se replica en todos los demás nodos de la red. Finalmente retorna el mensaje de respuesta a la Interfaz del usuario.

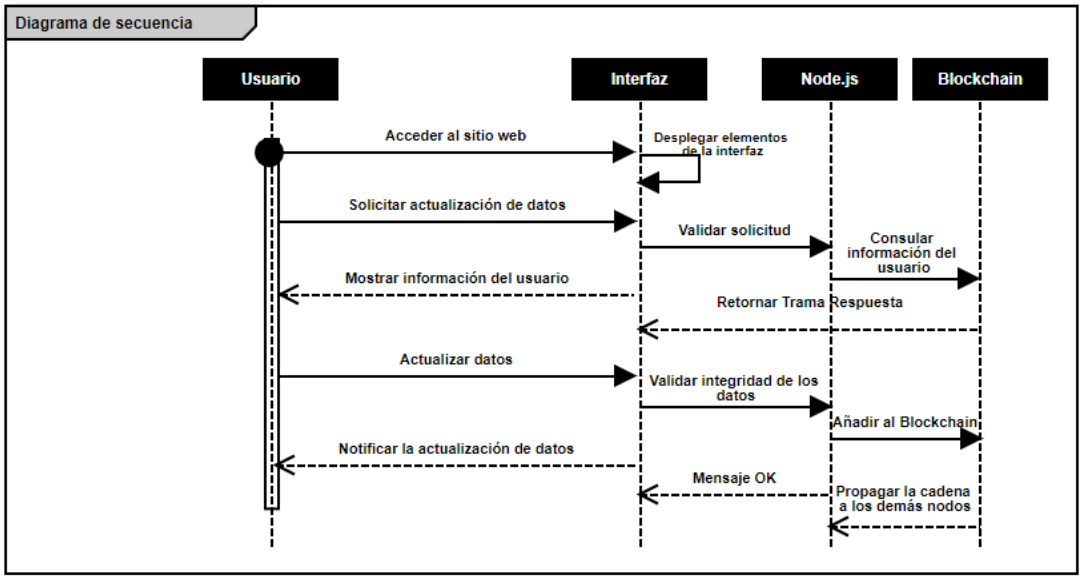

Figura 13. Escenario: Actualizar la información del usuario

4.1.4 Estructura de Base de Datos

Con el objetivo de tener escalabilidad, integridad y confiabilidad de los datos se ha seleccionado una base de datos No SQL, ya que aporta mayor flexibilidad, velocidad, y manejabilidad (Li, 2013), estas son características necesarias para la creación del Blockchain.

El motor de base de datos seleccionado es CouchDB. De acuerdo con los autores Anderson, et al (2010). CouchBD está orientada a documentos a No SQL, que se almacenan en formato JSON. Sus principales beneficios se enumeran a continuación.

- Ofrece un API para las consultas;

- Replicación incremental y flexible;
- Integridad y confiabilidad de los datos;
- Integración en varias plataformas, desde servidores hasta dispositivos móviles.

4.1.5 Diagrama de arquitectura

Según Pressman (2010), un diagrama de arquitectura ayuda a plantear una vista completa del sistema que se va a construir. Muestra la estructura y organización de los componentes de software. En este sentido, en la Figura 14 se muestra la arquitectura del sistema, que permite navegar, leer, editar y agregar información al Blockchain, mismo que se explica en el siguiente párrafo.

El usuario interactuará con la aplicación del cliente desde su navegador. Cuando este realiza alguna acción, la aplicación cliente llama a la API del servidor donde interactúa con la red del Blockchain. La solicitud accede al libro mayor para simular una transacción. Se construye la solicitud utilizando el SDK de Fabric y luego se envía a un nodo del Blockchain. En el nodo el contrato inteligente aplica la lógica del negocio definida para identidades digitales. Si no hay problemas, se firmará la transacción. Finalmente, el nodo validará el bloque, lo escribirá en su libro mayor, y respaldará la información en la base de datos clave – valor CouchDB. La transacción ahora es parte del Blockchain y cualquier lectura posterior reflejará este cambio.

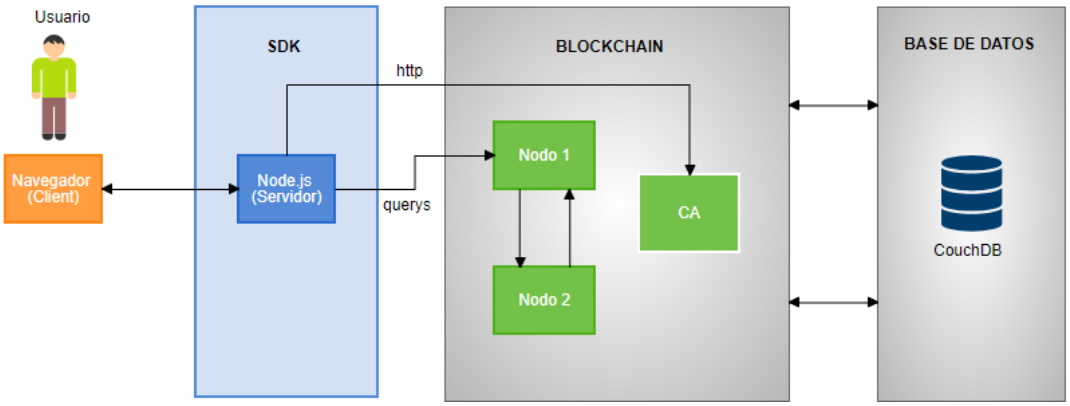

Figura 14. Diagrama de arquitectura

4.2 Desarrollo del Blockchain basado en Fabric

En esta sección se explica la tercera actividad de SCRUM, esta metodología de desarrollo ágil propone un desarrollo creciente en varias iteraciones. A continuación, se describe el desarrollo del Blockchain propuesto para el manejo de identidad digital. Para este desarrollo se ha utilizado Hyperledger Composer que según el sitio oficial de Hyperledger.org (2017) lo define como un conjunto de herramientas que facilita la construcción de aplicaciones Blockchain, para lo cual provee de contenedores Dockers. Hyperledger Composer está basado en Fabric, framework seleccionado en el capítulo 3.

El desarrollo del Blockchain que se describe a lo largo de este capítulo está basado principalmente en la documentación del sitio oficial de Hyperledger Composer (Hyperledger Composer, 2018). En la Figura 15 se puede apreciar una adaptación del modelo de Hyperledger Fabric y Composer para la construcción de un Blockchain sobre el manejo de identidades digitales. Donde un usuario necesita una tarjeta de red para acceder al Blockchain a través de un canal, que permite la interacción con los nodos. Cada nodo cuenta con un Ledger, una base de datos CouchDB, y un contrato inteligente, que se lo interpreta como un contrato inteligente. Composer maneja todos

estos elementos a través de lo que denomina Red Empresarial. Más adelante se explica estos conceptos.

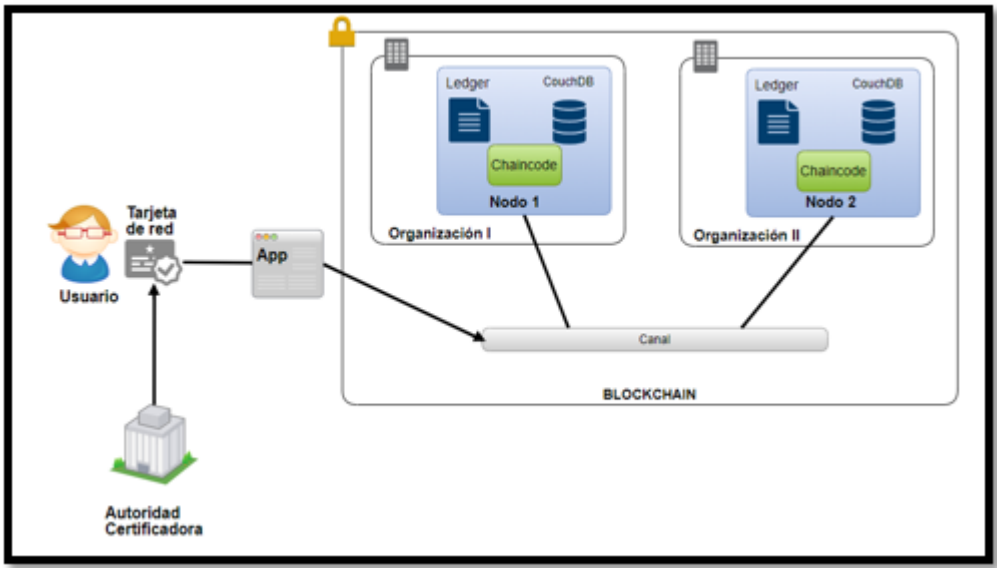

Figura 15. Modelo de identidad digital propuesto con Hyperledger Composer

4.2.1 Crear una estructura de red empresarial

Composer define a una red empresarial como un grupo de entidades que trabajan juntas para lograr determinados objetivos. La red empresarial está compuesta por activos, participantes, transacciones, reglas de control de acceso, eventos y consultas. Estos componentes se representan a través de un archivo de modelo que contiene las definiciones para los activos, participantes y transacciones en la red, un fichero de lógica de transacción, también contiene un documento de control de acceso con reglas básicas. Se utilizó la herramienta Yeoman para crear un directorio, que contiene todos los componentes necesarios para generar una red empresarial básica. La Figura 16 muestra la estructura y organización de los archivos que conforman esta red.

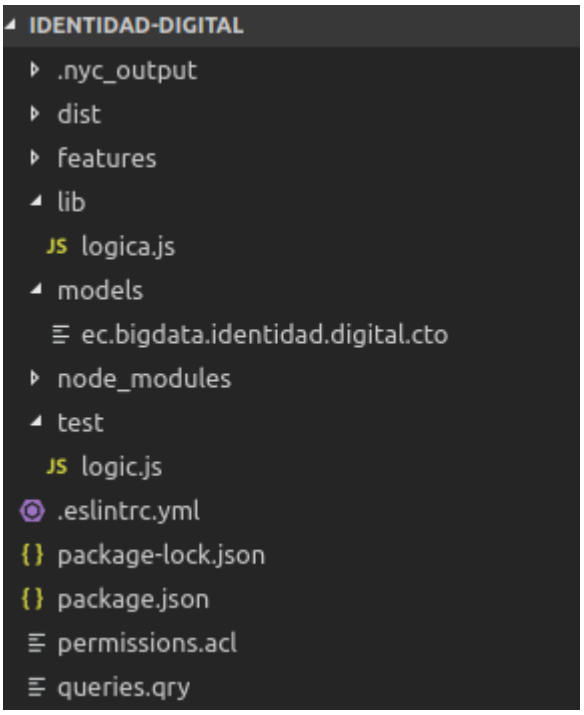

Figura 16. Archivos de la rede empresarial

Las tarjetas de red empresariales simplifican el proceso de conexión a una red empresarial, contiene una identidad para un único participante dentro de la red desplegada. Las tarjetas de red constan de un perfil de conexión, un certificado digital y metadatos. Un perfil de conexión es un documento JSON, que contiene la información necesaria para conectarse a la red. El certificado debe ser emitido por una Autoridad Certificadora. Los metadatos contienen opcionalmente el nombre de la red comercial a la que va conectarse.

Hyperledger Fabric (2017) define a un canal como una "subred" privada de comunicación entre dos o más miembros específicos de la red, con el propósito de realizar transacciones privadas y confidenciales. Un canal está definido por miembros, el libro mayor compartido, el o los nodos del servicio de ordenamiento. Cada transacción en la red se ejecuta en un canal, donde cada parte debe estar autenticada y autorizada para realizar transacciones en ese canal.

Los nodos son las entidades de comunicación de la cadena de bloques. La función de un nodo es respaldar la red manteniendo una copia de una cadena de bloques y, en algunos casos, procesando las transacciones. Los nodos son las partes individuales de la estructura de datos más grande que es una cadena de bloques.

4.2.2 Definir una red empresarial

Modelado de activos, participantes y transacciones

Este archivo está escrito usando el lenguaje de modelado Hyperledger Composer denominado CTO. El modelo contiene las definiciones de cada activo, transacción, participante y evento. Como se muestra en la Figura 17 consta con la información básica de 3 tipos de participantes: Administrador, Persona y Empresa. También contiene transacciones para permitir que una persona o empresa acceda a la información de un participante, así como también la opción de revocar este permiso. Los eventos definidos lanzan las transacciones antes mencionadas.

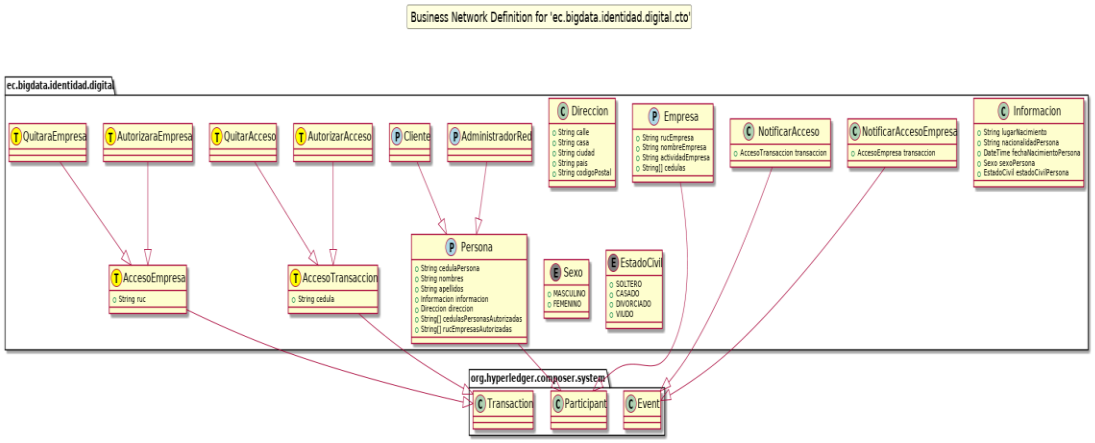

Figura 17. Definición de la red de negocios para identidades digitales

Para otorgar o revocar permisos en este modelo, se ha definido que cada persona cuenta con un arreglo cédulas y un arreglo con los números de ruc, para identificar a las personas y a las empresas

autorizadas que pueden leer su información. A continuación, la codificación del modelo propuesto para el manejo de identidades digitales en lenguaje CTO.

```
namespace ec.bigdata.identidad.digital

//Define el participante PERSONA
abstract participant Persona identified by cedulaPersona {
  o String cedulaPersona
  o String nombres
  o String apellidos
  o Informacion informacion optional
  o Direccion direccion optional
  o String[] cedulasPersonasAutorizadas optional
  o String[] rucEmpresasAutorizadas optional
}

//Define el participante Administrador
participant AdministradorRed extends Persona{
}

//Define el participante Empresa
participant Empresa identified by rucEmpresa
{
  o String rucEmpresa
  o String nombreEmpresa
  o String actividadEmpresa
  o String[] cedulas optional
}

//Define el objeto Direccion
concept Direccion
{
  o String calle
  o String casa
  o String ciudad
  o String pais
  o String codigoPostal
}

//Define información adicional del participante
concept Informacion
{
  o String lugarNacimiento
  o String nacionalidadPersona default = "ECUATORIANA"
  o DateTime fechaNacimientoPersona
  o Sexo sexoPersona
  o EstadoCivil estadoCivilPersona
}

//Define los tipos de sexo
enum Sexo
{
```

```
  o MASCULINO
  o FEMENINO
}

//Define los tipos de estado civil
enum EstadoCivil
{
  o SOLTERO
  o CASADO
  o DIVORCIADO
  o VIUDO
}

/*TRANSACCIONES*/

//Define una transacción de acceso abstracta para una persona
 abstract transaction AccesoTransaccion {
  o String cedula
}
//El participante autoriza compartir su información con otra persona
transaction AutorizarAcceso extends AccesoTransaccion {
}

//El participante revoca la autorización de compartir su infomación con la
persona
transaction QuitarAcceso extends AccesoTransaccion {
}

//Define una transacción de acceso abstracta para una empresa
abstract transaction AccesoEmpresa {
  o String ruc
}

//El participante autoriza compartir su información con una empresa
transaction AutorizaraEmpresa extends AccesoEmpresa {
}

//El participante revoca la autorización de compartir su infomación con una
empresa
transaction QuitaraEmpresa extends AccesoEmpresa {
}

/*EVENTOS*/
event NotificarAcceso {
  o AccesoTransaccion transaccion
}

 event NotificarAccesoEmpresa {
  o AccesoEmpresa transaccion
}
```

Lógica de transacción

El archivo de lógica define el comportamiento de las transacciones descritas en el modelo. Para identidades digitales el archivo está escrito en el lenguaje de programación JavaScript, describe el funcionamiento de las transacciones de autorización para leer la información de un participante y la revocación de la misma. Para otorgar el acceso a la información del participante primero se verifica que no posea estos permisos, se añade la cédula del participante al arreglo de cédulas, que es el identificador de la persona, se genera el evento y finalmente se almacena en el Blockchain. Para revocar una autorización se valida que el participante haya tenido esa autorización, se elimina el elemento del array que almacena las cédulas de los participantes que hayan dado autorización, se genera el evento, y finalmente se registra esta transacción en el Blockchain.

```
'use strict';
/**
 * Una persona otorga acceso a su información a otra persona.
 * @param {ec.bigdata.identidad.digital.AutorizarAcceso} autorizar
 * @transaction
 */
async function autorizarAcceso(autorizar) {
    const participante = getCurrentParticipant();
    console.log('Autorización: ' + participante.getIdentifier() +
                ' dando permisos para su información al usuario con cédula' +
autorizar.cedula );

    if(!participante) {
        throw new Error('No se encuentra el usuario con la cédula
ingresada.');
    }

    // Si el participante no está autorizado, se le autoriza
    let indice = -1;

    if(!participante.cedulasPersonasAutorizadas) {
        participante.cedulasPersonasAutorizadas = [];
    }
    else {
        indice =
participante.cedulasPersonasAutorizadas.indexOf(autorizar.cedula);
    }
```

```
    if(indice < 0) {
        participante.cedulasPersonasAutorizadas.push(autorizar.cedula);

        // Generar el evento
        const event = getFactory().newEvent('ec.bigdata.identidad.digital',
'NotificarAcceso');
        event.transaccion = autorizar;
        emit(event);

        // Almacena en el Blockchain
        const registroPersona = await
getParticipantRegistry('ec.bigdata.identidad.digital.Cliente');
        await registroPersona.update(participante);
    }
}

/**
 * Una persona revoca el acceso de su información a otra persona.
 * @param {ec.bigdata.identidad.digital.QuitarAcceso} quitar
 * @transaction
 */
async function quitarAcceso(quitar) {

    const participante = getCurrentParticipant();
    console.log('Quitar autorizacion: ' + participante.getIdentifier()
                + ' quitando el acceso a la informacion a la persona con
cedula: '
                + quitar.cedula );

    if(!participante) {
        throw new Error('No se encuentra el usuario con la cedula
ingresada.');
    }

    // Si la persona está autorizada se lo revoca.
    const indice = participante.cedulasPersonasAutorizadas ?
          participante.cedulasPersonasAutorizadas.indexOf(quitar.cedula) : -1;

    if(indice>-1) {

      //Elimina el elemento ubicado en el index:
      participante.cedulasPersonasAutorizadas.splice(indice, 1);

        // Genera un evento
        const event = getFactory().newEvent('ec.bigdata.identidad.digital',
'NotificarAcceso');
        event.transaccion = quitar;
        emit(event);

        // Almacena en el Blockchain
        const registroPersona = await
getParticipantRegistry('ec.bigdata.identidad.digital.Cliente');
        await registroPersona.update(participante);
```

```
    }
}

/**
 * Una persona otorga acceso a su información a otra persona.
 * @param {ec.bigdata.identidad.digital.AutorizaraEmpresa} autorizarE - the
authorize a ser procesada
 * @transaction
 */
async function autorizarAccesoEmpresa(autorizarE) {  //

    const participante = getCurrentParticipant();
    console.log('Autorizacion: la persona con ruc: ' +
participante.getIdentifier() +
                ' dando permisos para su informacion a la empresa con ruc:' +
autorizarE.ruc );

    if(!participante) {
        throw new Error('No se encuentra el usuario con la cedula
ingresada.');
    }

    // Si el miembro no está autorizado, se lo autoriza
    let indice = -1;

    if(!participante.rucEmpresasAutorizadas) {
        participante.rucEmpresasAutorizadas = [];
    }
    else {
        indice = participante.rucEmpresasAutorizadas.indexOf(autorizarE.ruc);
    }

    if(indice < 0) {
        participante.rucEmpresasAutorizadas.push(autorizarE.ruc);

        // Generar el evento
        const event = getFactory().newEvent('ec.bigdata.identidad.digital',
'NotificarAccesoEmpresa');
        event.transaccion = autorizarE;
        emit(event);

        // Guardar en el Blockchain
        const registroRuc = await
getParticipantRegistry('ec.bigdata.identidad.digital.Cliente');
        await registroRuc.update(participante);
    }
}

/**
 * Una persona quita el acceso a su información a otra persona.
 * @param {ec.bigdata.identidad.digital.QuitaraEmpresa} quitarE
 * @transaction
 */
async function quitarAccesoEmpresa(quitarE) {
```

```
    const participante = getCurrentParticipant();
    console.log('Quitar autorizacion: ' + participante.getIdentifier()
                + ' quitando el acceso a la informacion a la empresa con ruc:
'
                + quitarE.ruc );

    if(!participante) {
        throw new Error('No se encuentra el usuario con la cedula
ingresada.');
    }

    // Si la persona esta autorizada lo quitamos.
    const indice = participante.rucEmpresasAutorizadas ?
          participante.rucEmpresasAutorizadas.indexOf(quitarE.ruc) : -1;

    if(indice>-1) {
      //Se elimina el elemento ubicado en el index
        participante.rucEmpresasAutorizadas.splice(indice, 1);

        // Genera un evento
        const event = getFactory().newEvent('ec.bigdata.identidad.digital',
'NotificarAccesoEmpresa');
        event.transaccion = quitarE;
        emit(event);

        // Almacena en el Blockchain
        const registroEmpresa = await
getParticipantRegistry('ec.bigdata.identidad.digital.Cliente');
        await registroEmpresa.update(participante);
    }
}
```

Control de acceso

Las reglas de control de acceso permiten una revisión detallada sobre lo qué los participantes tienen acceso, a qué activos en la red y bajo qué condiciones. En el siguiente fragmento de código, se visualizan los controles de acceso propuestos para la gestión de identidades digitales. Cada regla consta de un nombre, una descripción operación, recurso y acción.

```
rule AutorizarAccesoEmpresaTransaccion {
    description: "Permitir que todos los participantes envíen transacciones de
autorización a empresas"
    participant: "ANY"
    operation: CREATE
    resource: "ec.bigdata.identidad.digital.AutorizaraEmpresa"
    action: ALLOW
}
```

```
rule QuitarAccesoEmpresaTransaccion {
    description: "Permitir que todos los participantes envíen transacciones
para revocar una autorización"
    participant: "ANY"
    operation: CREATE
    resource: "ec.bigdata.identidad.digital.QuitaraEmpresa"
    action: ALLOW
}

rule AccesoPropioEmpresa {
    description: "Permitir a todos los participantes acceso completo a su
propio registro"
    participant(p): "ec.bigdata.identidad.digital.Empresa"
    operation: ALL
    resource(r): "ec.bigdata.identidad.digital.Empresa"
    condition: (r.getIdentifier() === p.getIdentifier())
    action: ALLOW
}

rule AccesoAtorizadosEmpresa {
    description: "Permitir a los clientes acceder a los registros de otras
empresas si se les concede"
    participant(p): "ec.bigdata.identidad.digital.Empresa"
    operation: ALL
    resource(r): "ec.bigdata.identidad.digital.Cliente"
    condition: (r.rucEmpresasAutorizadas &&
r.rucEmpresasAutorizadas.indexOf(p.getIdentifier()) > -1)
    action: ALLOW
}

//Usuarios

rule AccesoAtorizadosEmpresaUsuario {
    description: "Permitir a los clientes acceder a los registros de otras
personas si se les concede"
    participant(p): "ec.bigdata.identidad.digital.Cliente"
    operation: ALL
    resource(r): "ec.bigdata.identidad.digital.Empresa"
    condition: (p.rucEmpresasAutorizadas &&
p.rucEmpresasAutorizadas.indexOf(r.getIdentifier()) > -1)
    action: ALLOW
}

rule AutorizarAccesoTransaccion {
    description: "Permitir que todos los participantes envíen transacciones de
autorizacion"
    participant: "ANY"
    operation: CREATE
    resource: "ec.bigdata.identidad.digital.AutorizarAcceso"
    action: ALLOW
}

rule QuitarAccesoTransaccion {
```

```
    description: "Permitir que todos los participantes envíen transacciones de
quitar autorizacion"
    participant: "ANY"
    operation: CREATE
    resource: "ec.bigdata.identidad.digital.QuitarAcceso"
    action: ALLOW
}
rule AccesoPropio {
    description: "Permitir a todos los participantes acceso completo a su
propio registro"
    participant(p): "ec.bigdata.identidad.digital.Cliente"
    operation: ALL
    resource(r): "ec.bigdata.identidad.digital.Cliente"
    condition: (r.getIdentifier() === p.getIdentifier())
    action: ALLOW
}

rule AccesoAtorizados {
    description: "Permitir a los clientes acceder a los registros de otras
personas si se les concede"
    participant(p): "ec.bigdata.identidad.digital.Cliente"
    operation: ALL
    resource(r): "ec.bigdata.identidad.digital.Cliente"
    condition: (r.cedulasPersonasAutorizadas &&
r.cedulasPersonasAutorizadas.indexOf(p.getIdentifier()) > -1)
    action: ALLOW
}

rule SystemACL {
    description:  "Permitir todo el acceso al sistema"
    participant: "org.hyperledger.composer.system.Participant"
    operation: ALL
    resource: "org.hyperledger.composer.system.**"
    action: ALLOW
}


rule NetworkAdminUser {
    description: "Grant business network administrators full access to user
resources"
    participant: "org.hyperledger.composer.system.NetworkAdmin"
    operation: ALL
    resource: "**"
    action: ALLOW
}

rule NetworkAdminSystem {
    description: "Grant business network administrators full access to system
resources"
    participant: "org.hyperledger.composer.system.NetworkAdmin"
    operation: ALL
    resource: "org.hyperledger.composer.system.**"
    action: ALLOW
}
```

4.2.3 Generar un archivo de red empresarial

Una vez se ha definido la red empresarial; los archivos de: modelo (.cto), lógica (.js) y control de acceso (.acl); pasan por un proceso de verificación y empaquetamiento, que de ser satisfactorios genera un fichero de extensión bna, similar al de la Figura 18, que se localiza en la raíz del directorio sobre el cual se está trabajando.

Figura 18. Archivo de red empresarial

4.2.4 Despliegue de la red

La implementación de la instancia de Hyperledger Fabric requiere la instalación del archivo de red empresarial (.bna), además necesita un administrador para el que nodo que se está levantando, denominado PeerAdmin. Después se crea un nuevo participante, identidad y tarjeta asociada para que sea el administrador de red. Finalmente, la tarjeta de red empresarial del administrador debe importarse para su uso, y se activa la red para verificar que está respondiendo.

Si el proceso descrito anteriormente es exitoso se presenta el mensaje en consola junto con las tarjetas de cada administrador como se muestra en la Figura 19. Para verificar que la red empresarial se ha implementado con éxito se puede realizar un ping a la red, como se puede observar en la Figura 20.

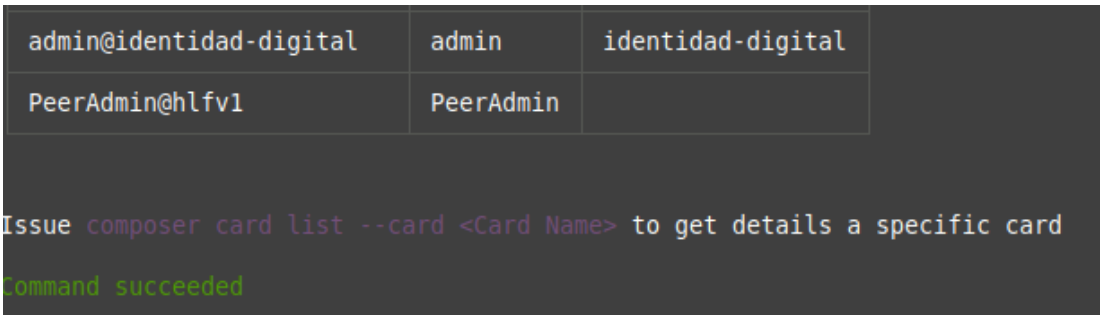

Figura 19. Tarjetas de red empresaial de los administradores.

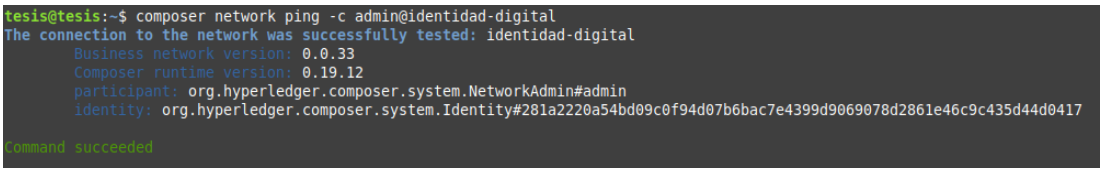

Figura 20. Ping a la red empresarial

4.2.5 Generación de un servicio REST

A través de Hyperledger Composer se creó un API REST basado en la red empresarial definida anteriormente, cuya lógica está basada en los requerimientos señalados para el manejo de identidades digitales. A continuación, se describen los principales métodos de esta API en las tablas [7- 10].

Tabla 7
Crear identidad digital para Persona

Campo	Descripción	Tipo		Ejemplo
cedulaPersona	Número de identificación de la persona.	String	Obligatorio	1725669832
nombres	Nombre o nombres de la persona, separados por un espacio.	String	Obligatorio	Ana María
apellidos	Apellidos de la persona, separados por un espacio.	String	Obligatorio	Vivar López
lugarNacimiento	Lugar de natal de la persona.	String	Obligatorio	Quito

Continua

fechaNacimiento	Fecha de nacimiento de la persona.	String	Obligatorio	1990-05-20
sexoPersona	Identifica el sexo de la persona.	String	Obligatorio	Femenino/ Masculino
estadoCivil	Estado civil de la persona.	String	Obligatorio	Casado
calles	Nombre de las calles donde reside la persona.	String	Obligatorio	Av. Amazonas
numCasa	Número de residencia de la persona.	String	Opcional	E-120
ciudad	Ciudad de residencia de la persona.	String	Obligatorio	Cuenca
pais	País de residencia de la persona.	String	Obligatorio	Ecuador
codigoPostal	Código postal de residencia de la persona.	String	Opcional	170524
cedulasPersonas Autorizadas	Cédulas de quienes pueden leer la información de la persona.	Array String	Opcional	1727331827, 1710424555, etc
RucEmpresas Autorizadas	Ruc de empresas que pueden leer la información de la persona	Array String	Opcional	1201656890001, 0236547892001

Ejemplo JSON


```
{
  "$class": "ec.bigdata.identidad.digital.Cliente",
  "cedulaPersona": "1725669832",
  "nombres": " Ana María",
  "apellidos": " Vivar López",
  "informacion": {
    "$class": "ec.bigdata.identidad.digital.Informacion",
    "lugarNacimiento": "Quito",
    "nacionalidadPersona": "ECUATORIANA",
    "fechaNacimientoPersona": "1990-07-22T03:41:59.971Z",
    "sexoPersona": "MASCULINO",
    "estadoCivilPersona": "SOLTERO",
    "id": "001"
  },
```

```
  "direccion": {
    "$class": "ec.bigdata.identidad.digital.Direccion",
    "calle": " Av. Amazonas",
    "casa": "E-120",
    "ciudad": "Cuenca",
    "pais": "Ecuador",
    "codigoPostal": "170524",
    "id": "string"
  },
  "cedulasPersonasAutorizadas": [],
  "rucEmpresasAutorizadas": []
}
```


Tabla 8

Crear identidad digital para Empresa

Campo	Descripción	Tipo		Ejemplo
rucEmpresa	Número de ruc que identifica a la empresa.	String	Obligatorio	1725669832001
nombreEmpresa	Nombre comercial de la empresa.	String	Obligatorio	EMPRESA ABC
actividadEmpresa	Principal actividad económica de la empresa.	String	Obligatorio	Agricultura
cedulas	Cédulas de personas que autorizaron compartir su información con la empresa.	Array String	Opcional	1727331827, 1710424555, etc

Ejemplo JSON


```
{
  "$class": "ec.bigdata.identidad.digital.Empresa",
  "rucEmpresa": "1725669832001",
  "nombreEmpresa": "Empresa ABC",
  "actividadEmpresa": "Agricultura",
  "cedulas": []
}
```

Tabla 9

Autorizar y revocar permiso a Persona

Campo	Descripción	Tipo		Ejemplo
cedula	Número de identificación de la persona con la que se comparte la información.	String	Obligatorio	1725669832
transactionId	Número identificador de la transacción.	String	Autogenerado/ Obligatorio	00001
timestamp	Fecha y hora de la transacción.	DataTime	Autogenerado/ Obligatorio	2018-07-22T03:41:59.971Z

Ejemplo JSON

```
{
  "$class": "ec.bigdata.identidad.digital.AutorizarAcceso",
  "cedula": "1725669832",
  "transactionId": "0001",
  "timestamp": "2018-07-22T03:41:59.890Z"
}
```

Tabla 10

Autorizar y renovar permiso a Empresa

Campo	Descripción	Tipo		Ejemplo
ruc	Número de identificación de la empresa con la que se comparte la información.	String	Obligatorio	1725669832001
transactionId	Número identificador de la transacción.	String	Autogenerado/ Obligatorio	00002
timestamp	Fecha y hora de la transacción.	DataTime	Autogenerado/ Obligatorio	2018-07-22T03:41:59.971Z

Ejemplo JSON

```
{
  "$class": "ec.bigdata.identidad.digital.AutorizarAcceso",
  "ruc": "1725669832",
  "transactionId": "0001",
  "timestamp": "2018-07-22T03:41:59.890Z"
}
```

4.2.6 Implementación del prototipo

Para la ejecución de la red empresarial se ha utilizado Playground, entorno que provee Hyperledger Composer para desplegar estas redes, crear tarjetas de conexión, participantes y demás acciones definidas en la lógica de negocios.

UH001 Crear identidades digitales

Solo el administrador puede crear identidades digitales, para ingresar a la aplicación utiliza su tarjeta de red como la que se muestra en la Figura 21, que incluye un certificado digital y un perfil de conexión como se explicó anteriormente. El administrador debe crear tarjetas de red empresarial para que otros usuarios puedan conectarse al Blockchain.

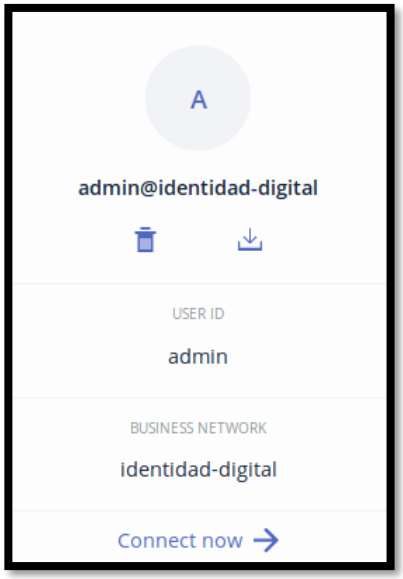

Figura 21. Tarjeta de red del Administrador

Al ingresar el Administrador al sistema puede ver los usuarios participantes que están registrados tanto personas como empresas, como se presenta en la Figura 22. Para la creación del participante se debe enviar los JSON descritos en la Tabla 7 Crear identidad digital para Persona o en la Tabla 8 Crear identidad digital para Empresa, según se requiera.

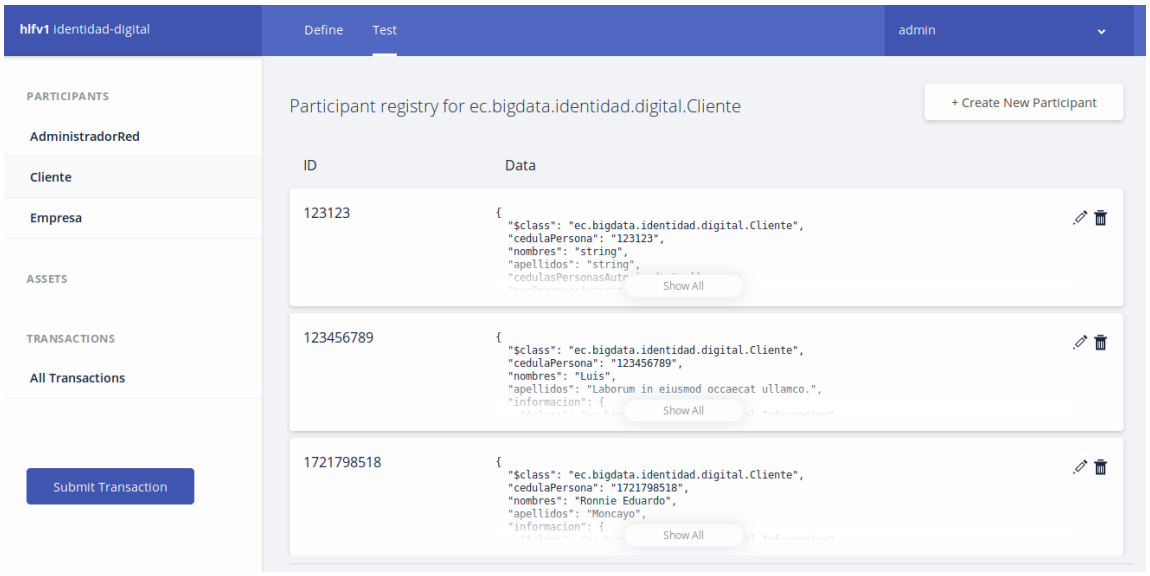

Figura 22. Participantes que puede ver el Administrador

En la ***Figura 23.*** Participante creado se muestra la creación de un participante, al crear al participante también se genera su certificado digital, con su clave pública y privada, que servirá para futuras transacciones.

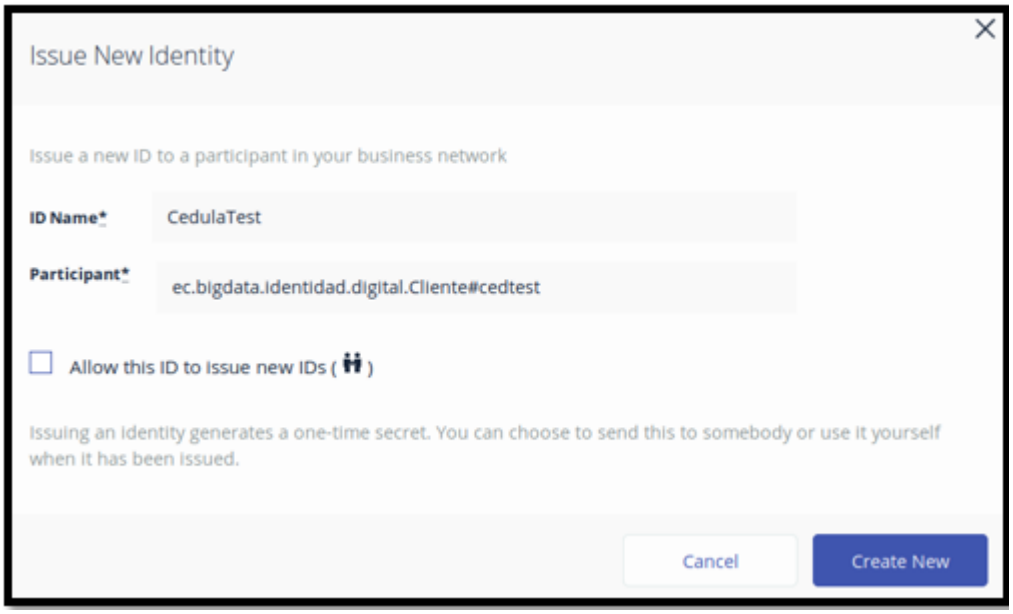

Figura 23. Participante creado

UH002 Consultar la información del usuario.

Después de autentificarse mediante la tarjeta de red empresarial el usuario de tipo Persona solo puede ver su información. A continuación, se presenta una captura de pantalla en la Figura 24 de como se muestra esta información para el usuario.

Figura 24. Información del usuario

UH003 Actualizar la información del usuario

Tanto el propietario como el administrador puede cambiar la información de una identidad digital. Los cambios de los valores se realizan en el JSON, al igual que en la demostración de la historia de usuario UH001.

UH004 Permitir el acceso a la información del usuario.

Para cumplir con este requerimiento el usuario debe seleccionar la Transacción para autorizar a una empresa a leer su información, para lo cual se añade el ruc de la empresa, como se muestra en la siguiente Figura 25.

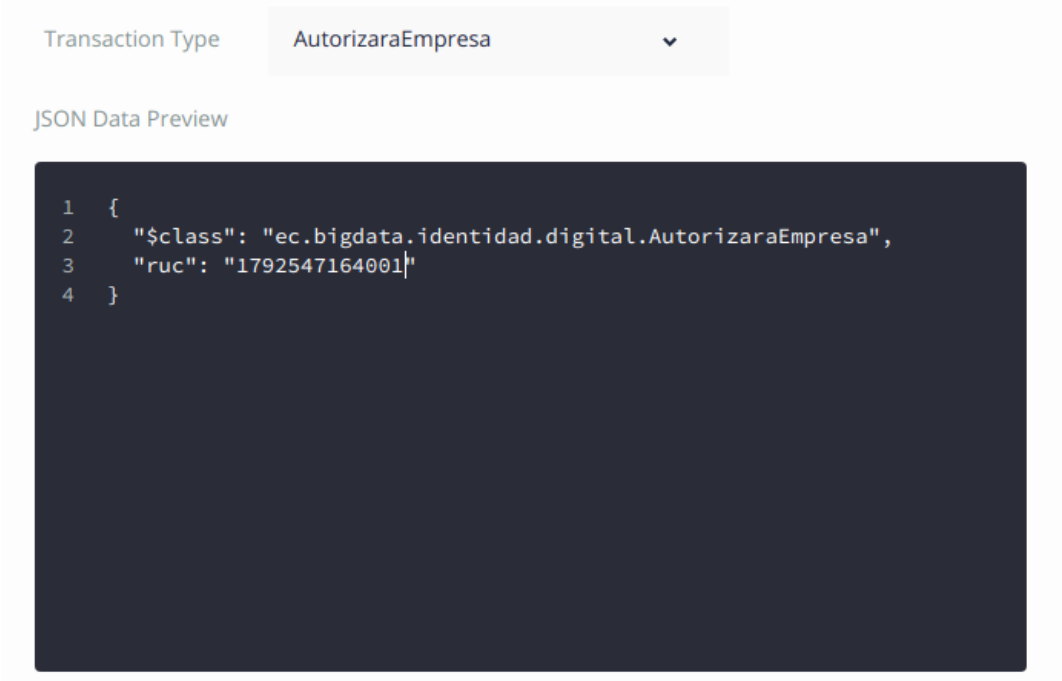

Figura 25. Conceder acceso a la información del usuario

Una vez el usuario haya dado los permisos para compartir su información con una determinada entidad, ahora esta entidad puede ver la información de el o los usuarios que lo han autorizado, como se puede apreciar en la ***Figura 26.*** Información de usuarios autorizados.

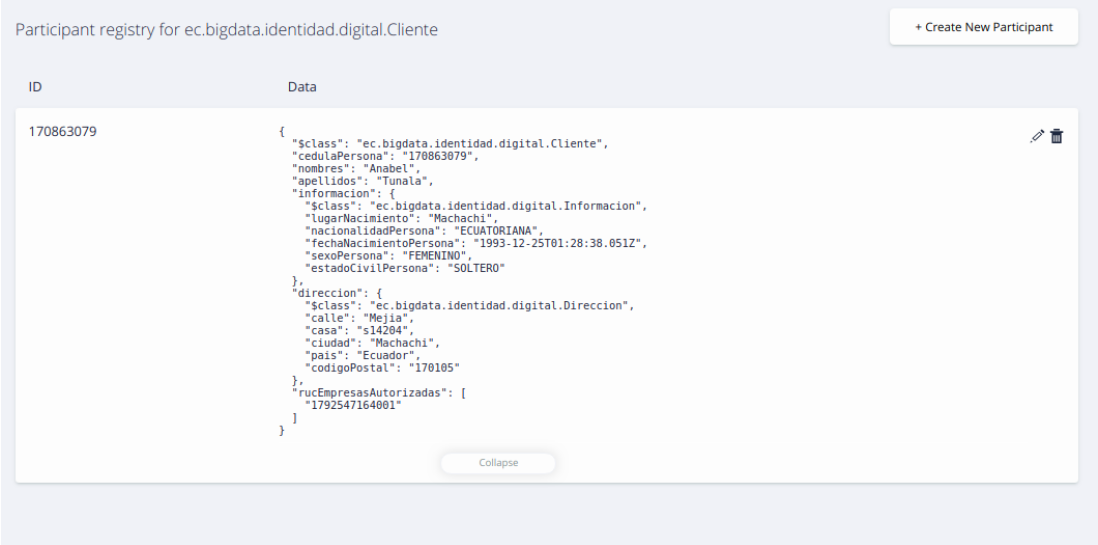

Figura 26. Información de usuarios autorizados

UH005 Revocar el acceso a la información del usuario.

Para que un usuario revoque un permiso, debe seleccionar el tipo de transacción Revocar, e ingresar en el ruc de la empresa que se desea revocar el permiso, como se muestra en la Figura 27.

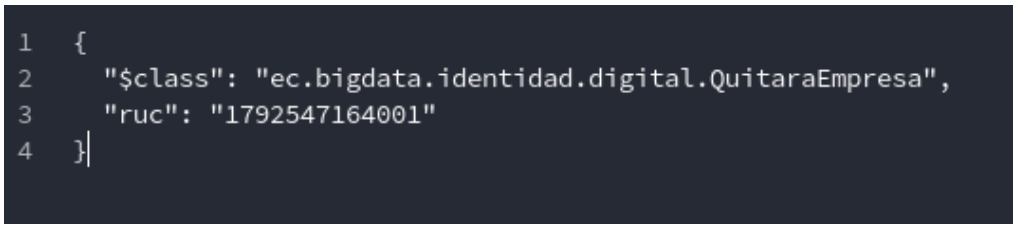

Figura 27. Revocar permisos de acceso a la información de una identidad digital

La empresa a quien se ha revocado el permiso, ya no puede ver la información del usuario, en el ejemplo mostrado se puede apreciar en la ***Figura 28.*** Vista de los usuarios que tiene acceso una entidad que a la empresa ahora no puede ver la información del usuario que revocó el permiso.

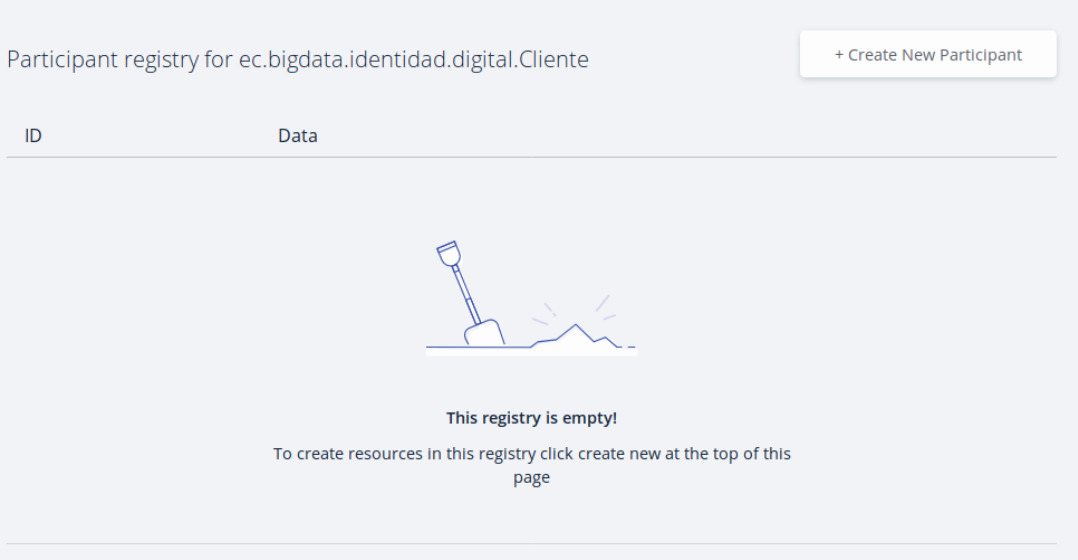

Figura 28. Vista de los usuarios que tiene acceso una entidad

CAPÍTULO V

PRUEBAS, EVALUACIÓN Y VALIDACIÓN DE RESULTADOS

Esta sección muestra las pruebas de caja blanca y caja negra. Proporciona también una evaluación de calidad basada en modularidad, acoplamiento y cohesión propuestos por Pressman (2010). Además, valida el rendimiento computacional del Blockchain propuesto para el manejo de identidades digitales. Finalmente, Presenta una discusión sobre la seguridad de la información basada en disponibilidad, integridad, confidencialidad, trazabilidad, autenticación y no repudio.

5.1 Pruebas

Se ha realizado pruebas de caja blanca y caja negra para demostrar el funcionamiento del sistema basado en Blockchain, que se describen a continuación.

5.1.1 Pruebas de caja blanca

Según Pressman (2010), las pruebas de caja blanca se basan en los detalles del procedimiento, las rutas lógicas a través del software y las colaboraciones entre componentes. De acuerdo con Barrientos (2014), dentro de la metodología ágil se encuentran las pruebas unitarias que se aplican a componentes individuales de un sistema de software. Se codifican pequeños programas que buscan acaparar todos o al menos la mayor parte de los posibles estados o configuraciones de una unidad de software, para simular el entorno del componente y encontrar posibles errores.

De forma que a fin de aportar mayor calidad al proyecto se han creado las pruebas unitarias utilizando Mocha y Chai, marcos de test para JavaScript que cuenta con características que se ejecutan en Node.js y en navegadores. La Tabla 11 resume estas pruebas, donde se busca especialmente verificar que los permisos se comportan de la forma esperada, el código se lo puede

ver en el Anexo 1 contenido en un archivo denominado “test”. En la Figura 29 se puede observar la consola al ejecutar el archivo test donde cada visto representa que los casos de la Tabla 11 fueron exitosos.

Tabla 11
Pruebas de caja blanca

Funcionalidades a probar	Creación de identidades digitales Verificar permisos de lectura Dar Acceso Revocar Acceso
Fecha de ejecución	25-07-2018
Objetivo	Verificar el correcto funcionamiento a nivel de código sobre la creación de usuarios y permisos de los participantes.
Pre-condiciones	Configuración de la red empresarial. Configuración de las tarjetas de red de los participantes.
Flujo de las pruebas	Crear identidad para Anabel (Persona). Crear identidad para Ronnie (Persona). Crear identidad para BigData (Empresa). Crear identidad para Emagic (Empresa). Verificar que cada usuario puede ver sólo su información. Anabel da permiso a Ronnie de ver su información. Ronnie puede leer la información de Anabel. Ronnie da permios a BigData de ver su información. BigData puede leer la información de Ronnie.

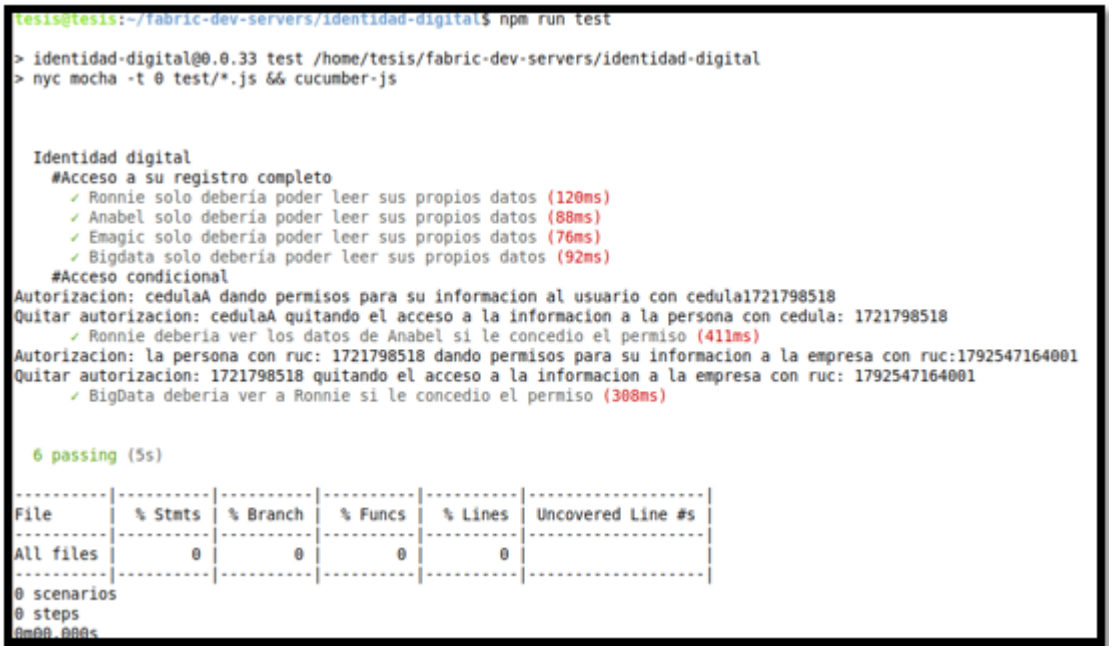

Figura 29. Consola al ejecutar las pruebas unitarias con Mocha y Chai

5.1.2 Pruebas de caja negra

De acuerdo con Pressman (2010), las pruebas de caja negra examinan los requerimientos de software sin preocuparse por la estructura interna del sistema. A continuación, se detallan estas pruebas basadas en los requisitos para identidades digitales planteados anteriormente. En las tablas [12 – 17] se muestra un registro de las pruebas de funcionalidad realizadas, donde el sistema se ha comportado como se esperaba.

Tabla 12
Prueba funcional "Crear identidad digital para una persona"

Funcionalidad a probar	Crear identidad digital
Responsable	Anabel Tunala
Fecha de ejecución	26-07-2018
Objetivo	Emitir identidad digital para una persona.

Continua

Criterio de éxito	Se crea la identidad digital de una persona, para que pueda ingresar al sistema.
Criterio de falla	No se puede emitir la identidad digital para el usuario.
Pre-condiciones	El usuario que crea las identidades digitales debe estar registrado como Administrador.
Perfil del usuario	Administrador
Flujo del caso de prueba	1. Dar clic en “Cliente”. 2. Dar clic en “Nuevo participante”. 3. Ingresar cédula de la persona. 4. Ingresa nombres de la persona. 5. Ingresar apellidos de la persona. 6. Ingresar lugar de nacimiento de la persona. 7. Ingresar nacionalidad de la persona. 8. Ingresar fecha de nacimiento de la persona. 9. Ingresar sexo de la persona. 10. Ingresar estado civil de la persona. 11. Ingresar dirección de la persona. 12. Dar clic en “Crear nuevo”.
Resultados obtenidos	La información de la persona se agrega a la lista de personas creadas por el administrador.
Post condiciones	El propietario de la identidad digital emitida puede ingresar al sistema.

Tabla 13
Prueba funcional "Crear identidad digital para una empresa"

Funcionalidad a probar	Crear identidad digital
Responsable	Ronnie Moncayo
Fecha de ejecución	26-07-2018
Objetivo	Emitir identidad digital para una empresa.
Criterio de éxito	Se crea la identidad digital de una empresa, para que pueda ingresar al sistema.
Criterio de falla	No se puede emitir la identidad digital para la empresa.
Pre-condiciones	El usuario que crea las identidades digitales debe estar registrado como Administrador.
Perfil del usuario	Administrador
Flujo del caso de prueba	1. Dar clic en "Empresa". 2. Dar clic en "Nuevo participante". 3. Ingresar ruc de la empresa. 4. Ingresa nombre comercial de la empresa. 5. Ingresar actividad económica de la empresa. 6. Dar clic en "Crear nuevo".
Resultados obtenidos	La información de la empresa se agrega a la lista de empresas creadas por el administrador.
Post condiciones	La empresa puede ingresar al sistema con la identidad digital creada.

Tabla 14
Prueba funcional "Actualizar la información"

Funcionalidad a probar	Actualizar la información
Responsable	Anabel Tunala
Fecha de ejecución	26-07-2018
Objetivo	Actualizar información de la identidad digital de una persona.
Criterio de éxito	Se actualiza correctamente la información de la identidad digital.
Criterio de falla	La información no fue actualizada correctamente.
Pre-condiciones	Los usuarios que pueden actualizar la información de las identidades digitales son el Administrador y el propietario de la identidad digital.
Perfil del usuario	Administrador
Flujo del caso de prueba	1. Dar clic en "Cliente". 2. Seleccionar el usuario a modificar. 3. Dar clic en el icono "Editar". 4. Modificar los datos requeridos. 5. Dar clic en "Actualizar".
Resultados obtenidos	La información de la identidad se actualiza en la lista de usuarios creados.
Post condiciones	La empresa puede ingresar al sistema con la identidad digital creada.

Tabla 15
Prueba funcional "Permitir el acceso"

Funcionalidad a probar	Permitir el acceso a la información del usuario
Responsable	Ronnie Moncayo
Fecha de ejecución	26-07-2018
Objetivo	La persona otorga un permiso a una empresa, para que ésta pueda leer su información.
Criterio de éxito	La empresa a la que se da el permiso puede leer la información de la persona.
Criterio de falla	No se puede otorgar este permiso.
Pre-condiciones	Únicamente el propietario de la identidad digital puede otorgar permisos.
Perfil del usuario	Persona
Flujo del caso de prueba	1. Dar clic en "Enviar transacción". 2. Seleccionar el tipo de transacción "Autorizar acceso". 3. Ingresar ruc de la empresa. 4. Dar clic en "Enviar".
Resultados obtenidos	Se muestra esta transacción en el histórico de actividades del usuario.
Post condiciones	La empresa ya puede leer la información de la persona.

Tabla 16
Prueba funcional "Consultar la información"

Funcionalidad a probar	Consultar la información
Responsable	Anabel Tunala
Fecha de ejecución	26-07-2018
Objetivo	Consultar la información de la identidad digital de una persona.
Criterio de éxito	Se muestra la información de la persona que otorgó permiso a la empresa.
Criterio de falla	No se muestra correctamente la información de la persona.
Pre-condiciones	Un participante de tipo Empresa, únicamente puede leer la información de las personas que dieron su autorización.
Perfil del usuario	Empresa
Flujo del caso de prueba	1. Dar clic en "Cliente". 2. Seleccionar un usuario de la lista.
Resultados obtenidos	Se muestra la información de la persona seleccionada.
Post condiciones	Ninguna.

Tabla 17
Prueba funcional "Revocar el acceso a la información"

Funcionalidad a probar	Revocar el acceso a la información
Responsable	Ronnie Moncayo
Fecha de ejecución	26-07-2018

Continua

Objetivo	La persona quita el permiso que otorgó a una empresa, para que pueda leer su información.
Criterio de éxito	La empresa ya no puede leer la información de esta persona.
Criterio de falla	La empresa aún puede leer la información de la persona.
Pre-condiciones	Únicamente el propietario de la identidad digital puede revocar permisos.
Perfil del usuario	Persona
Flujo del caso de prueba	1. Dar clic en “Enviar transacción”. 2. Seleccionar el tipo de transacción “Quitar acceso”. 3. Ingresar ruc de la empresa. 4. Dar clic en “Enviar”.
Resultados obtenidos	Se muestra esta transacción en el histórico de actividades del usuario.
Post condiciones	La empresa no puede leer la información de la persona.

5.2 Evaluación De Calidad

Para prolongar el valor del software durante un largo período de tiempo, se debe procurar que sea fácil de cambiar. Larry Constantine (1979) define las métricas de acoplamiento y cohesión como parte de un diseño estructurado, basado en las características de buenas prácticas de programación que ayuda a reducir los costos de mantenimiento y modificación.

5.2.1 Modularidad

Es necesario definir la modularidad del sistema para hablar de cohesión y acoplamiento. Pressman (2010) define a la modularidad como “la manifestación más común de la división de problemas. El software se divide en componentes con nombres distintos y abordables por separado, en ocasiones llamados módulos, que se integran para satisfacer los requerimientos del problema”.

En la Figura 30, se muestra los módulos identificados en el sistema propuesto, encontrando las características morfológicas descritos en la Tabla 18 Caracteterísticas morfológicas

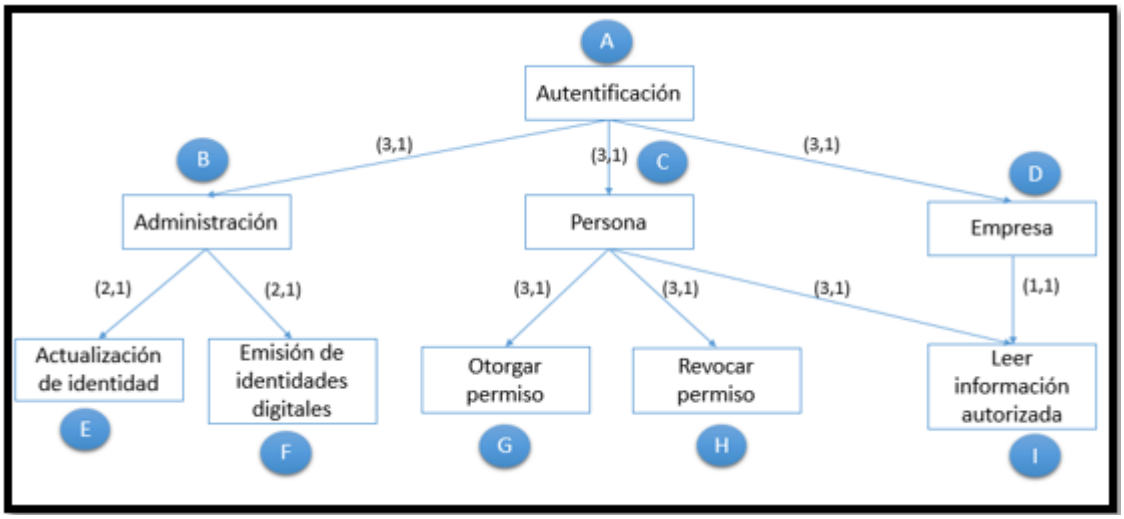

Figura 30. Modularidad del sistema de manejo de identidades digitales

Tabla 18
Caracteterísticas morfológicas

Característica	Valor
Tamaño	9
Arcos	8
Profundidad	3
Ratio	1.125

5.2.2 Acoplamiento

Según Pressman (2010), “El acoplamiento es la medición cualitativa del grado en el que las clases se conectan una con otra”. En el diseño de software uno de los principales objetivos es

mantener el acoplamiento lo más bajo posible. El número de acoplamiento varía de aproximadamente 67% como bajo acoplamiento, a 100% como altamente acoplado.

Ejiogo (1991), define la siguiente fórmula para medir el acoplamiento:

$$Acoplamiento = 1 - \frac{1}{d_i + 2 \times c_i + d_0 + 2 \times c_0 + g_d + 2 \times g_c + w + r}$$

Donde,

di: número de parámetros de entrada

ci: número de parámetros de control

do: número de parámetros de salida

co: número de parámetros de control de salida

gd: número de variables globales usadas como data

gc: número de variables globales usadas como control

w: número de módulos llamados

r: número de módulos llamantes bajo consideración

$$Acoplamiento\ A = 1 - \frac{1}{1 + 0 + 1 + 0 + 0 + 0 + 3} = 80\%$$

$$Acoplamiento\ B = 1 - \frac{1}{1 + 0 + 0 + 0 + 0 + 0 + 1 + 2} = 75\%$$

$$Acoplamiento\ C = 1 - \frac{1}{1 + 0 + 0 + 0 + 0 + 1 + 3} = 80\%$$

$$Acoplamiento\ D = 1 - \frac{1}{1+0+0+0+0+1+1} = 67\%$$

$$Acoplamiento\ E = 1 - \frac{1}{1+0+0+0+0+0+1} = 50\%$$

$$Acoplamiento\ F = 1 - \frac{1}{1+1+0+0+0+0+1} = 67\%$$

$$Acoplamiento\ G = 1 - \frac{1}{1+1+0+0+0+0+1} = 67\%$$

$$Acoplamiento\ H = 1 - \frac{1}{1+1+0+0+0+0+1} = 67\%$$

$$Acoplamiento\ I = 1 - \frac{1}{1+0+0+0+0+0+1} = 50\%$$

$$\overline{Acoplamiento} = 67\%$$

El acoplamiento promedio obtenido es de 67% lo que se considera como bajo acoplamiento.

5.2.3 Cohesión

De acuerdo con Pressman (2010) la cohesión es una medida del grado que implica que un módulo únicamente contiene atributos y métodos que se relacionan de cerca uno con el otro. En del diseño de software se busca obtener mayor cohesión. Ejiogo (1991), define la proporción de cohesión

como el número de módulos funcionales sobre el número total de módulos. Para el presente caso de estudio la cohesión es de 78%.

$$Porción\ de\ Cohesión = \frac{7}{9} = 78\%$$

5.3 Discusión sobre la seguridad del sistema

Los principales requerimientos de seguridad según la ISO 27000 son disponibilidad, integridad y confidencialidad. Además, se ha considerado la trazabilidad, autenticación y no repudio que maneja COBIT dentro de su marco seguridad de la información. A continuación, se describe como estas características están presentes en el Blockchain desarrollado.

5.3.1 Disponibilidad

Los contratos inteligentes ayudan a proteger al Blockchain de ataques que pueden afectar la disponibilidad del sistema, como los ataques de Denegación de Servicios, ya que define la lógica del sistema y trabaja en conjunto con un certificado digital que es necesario para que el usuario realice todas las transacciones, desde el ingreso al sistema, hasta cualquier tipo de actualizaciones. Es importante recalcar que estos certificados están respaldados por una autoridad certificadora (Hyperledger, 2017).

5.3.2 Confidencialidad

El diseño de una red Blockchain debe respaldar los requisitos de confidencialidad. La confidencialidad es una característica clave y muy sensible para los participantes en la red propuesta, en el manejo de identidades digitales. Hyperledger Fabric respalda la confidencialidad a través de algunas características. Fabric protege los datos en tránsito al habilitar el protocolo Transport Layer Security (TLS). También provee un Control de Acceso que se detalla en la sección

4.2.1 donde se ejemplificó para el modelo propuesto. Además de que cifra la información con el certificado del participante (IBM, 2018).

5.3.3 Integridad

De acuerdo con Kuchkovsky, Fernández, & Molero (2018), la integridad se ve influenciada por la cantidad de bloques de la red, debido a que cada bloque está vinculado al anterior mediante los hashes que se generan al cifrar cada transacción. Así que si se pretende alterar un registro debe modificarse todos los hashes anteriores y posteriores lo que resultaría ser demasiado complejo, esto se explicó en la sección 3.21. También los algoritmos de consenso están diseñados específicamente para detectar inconsistencias y rechazarlas de inmediato.

5.3.4 Trazabilidad

La Organización Internacional para la Estandarización ISO 9001:2008, define a la trazabilidad como la capacidad para seguir la historia, la aplicación o la localización de todo aquello que está bajo consideración y seguir su ruta a lo largo de toda la cadena de transformación y distribución. (ISO 9001, 2013)

En este documento se ha mencionado el Ledger o Libro Mayor de Blockchain, este Ledger contiene todas las transacciones realizadas por los usuarios sin ninguna excepción, mostrando un registro histórico inmutable que da trazabilidad al sistema de manejo de identidades digitales. En la Figura 31 se puede observar en el panel derecho las opciones que el administrador puede realizar, entre estas “Ver todas las transacciones” que muestra todos los registros con la fecha, hora, tipo y el participante que la ejecutó. En la **Tabla 19** *Información de trazabilidad de transacciones* se presentan los mensajes e información de

trazabilidad que se registra en el Blockchain propuesto, y que servirá de insumo para los controles de auditoría y seguimiento en los procedimientos críticas para el manejo de identidades digitales.

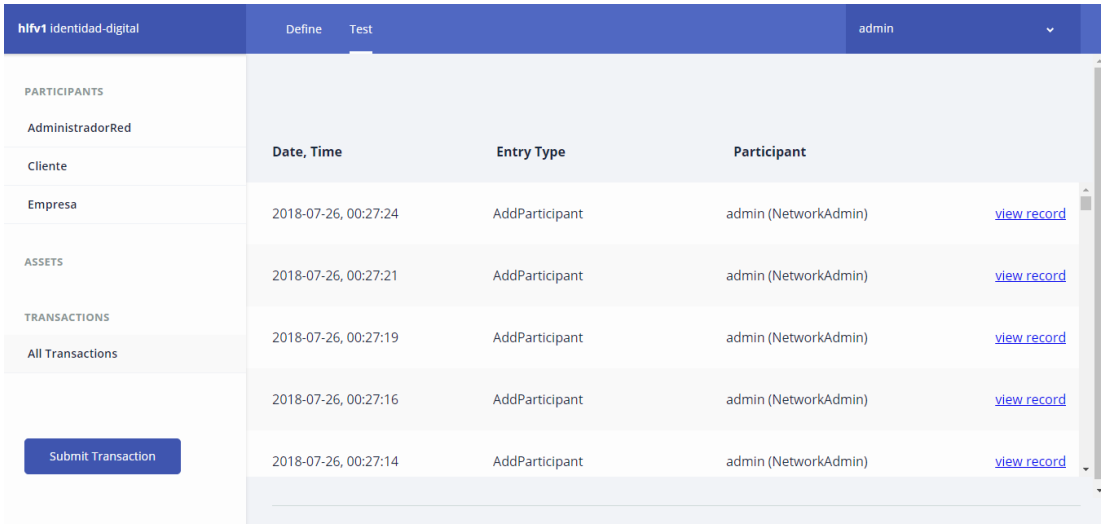

Figura 31. Histórico de transacciones desde la vista del Administrador

Tabla 19
Información de trazabilidad de transacciones

Tipo de transacción	**Código**	**Descripción**
Añadir participante	AddParticipant	Esta transacción únicamente la puede realizar el Administrador, para agregar a nuevos participantes.
Eliminar participante	RemoveParticipant	Esta transacción únicamente la puede realizar el Administrador, para borrar un participante.
Actualizar participante	UpdateParticipant	El administrador puede editar la información de los participantes, también el participante puede editar su propia información.
Visualizar participante	ViewParticipant	El administrador puede ver la información de todos los participantes, también el participante puede acceder su propia información.

Continua

Autorizar acceso	AutorizarAcceso	Sólo el participante puede dar acceso a otra persona o empresa para ver su información.
Quitar acceso	QuitarAcceso	Sólo el participante puede revocar el acceso a otra persona o empresa para ver su información.
Emitir identidad	IssueIdentity	Únicamente el administrador emite las identidades con las que el participante puede ingresar.
Activar la identidad actual	ActivateCurrentIdentity	Se activa la identidad cuando el participante ingresa al sistema.

5.3.5 Autenticación

La autenticación es el mecanismo que pretende comprobar si el usuario que pretende acceder al sistema es quien dice ser (Aitzhan, 2016). Para este Blockchain está identidad se la valida a través del certificado digital del participante que debe ser emitido por una autoridad certificadora lícita. Un participante necesita su tarjeta de red para acceder a la red Blockchain, la misma que requiere un certificado digital del participante como se describió en la sección 4.2.2.

5.3.6 No repudio

No repudio quiere decir que cuando se reciba un mensaje el remitente no pueda negar haberlo enviado ni el destinatario haberlo recibido (Kuchkovsky, Fernández, & Molero, 2018). En el Blockchain desarrollado esta situación se resuelve al contar con un registro histórico de todas las transacciones realizadas desde el despliegue de la red. Además de la utilización de certificados digitales, donde la información cifrada con la clave privada únicamente se la puede descifrar con la clave pública correspondiente.

5.4 Evaluación del desempeño

Con la finalidad de evaluar el desempeño del prototipo basado en Blockchain se ha realizado una comparativa entre la API generada en este proyecto y una API tradicional. La de Blockchain está desarrollada en lenguaje JavaScript con servidor NodeJS, y como base de datos CouchDB. La tradicional fue creada en lenguaje JAVA en su versión 9, con base de datos MariaDB versión 10.3 y servidor Tomcat 9.

En la API de Tomcat se ha procurado aplicar la misma lógica de negocios que la de Blockchain. En esta segunda API los permisos se han manejado a través de la base datos a fin de cumplir con los requerimientos funcionales establecidos. Desde el punto de vista del usuario las dos APIs interactúan de la misma forma. Sin embargo, su seguridad difiere.

Cada API fue probada en distintas máquinas con características iguales que se muestran en la Tabla 20. Las mediciones se realizaron en cuanto a tiempo de procesamiento, uso de CPU, uso de memoria RAM, estadísticas de E / S, número total de procesos creados por segundo y la cantidad de paquetes por segundo.

Tabla 20
Características de las máquinas

Descripción	Valor
RAM	4GB
CPU	2 vCPUs
ROM	80 GB SSD
TRANSFERENCIA	4TB

5.4.1 Tiempo

Se ha tomado los datos de las dos APIs al enviar 10, 100 y 500 registros a cada una. La Tabla 21 muestra como el prototipo basado en Blockchain tarda más en la inserción y consulta de los registros en comparación con el API de Tomcat. Además, que el porcentaje de diferencia entre ambas continúa creciendo en relación a la cantidad de registros insertados. En la Figura 32 se visualiza la diferencia que existe debido a que el Blockchain realiza procesos internos más complejos, como las configuraciones para las conexiones a la red, el cifrado y descifrado de la información.

Tabla 21
Comparativa entre tiempos de transacción

	TIEMPO (Segundos)		**Diferencia**	
	TOMCAT	BLOCKCHAIN	Segundos	Porcentaje
ESTADO NORMAL	-	-	-	-
INSERCIÓN 10 REGISTROS	5,13350	27,17860	22,04510	529,4%
INSERCIÓN 100 REGISTROS	17,27984	254,19246	236,91262	1471,0%
INSERCIÓN 500 REGISTROS	73,35630	1269,31636	1195,96006	1730,3%

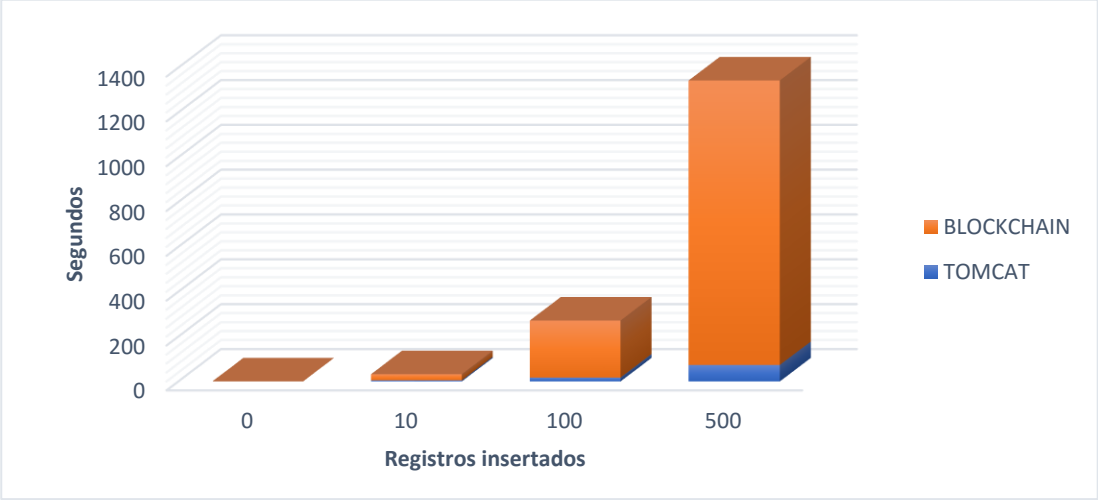

Figura 32. Comparativa de inserción de registros

5.4.2 CPU

La Figura 33 indica el consumo del uso del CPU, donde se observa que la API de Blockchain consume en promedio 29 % más que la API de Tomcat debido a la arquitectura propia de Blockchain, ya que no solo interactúa con una base de datos, también realiza pruebas de seguridad, autenticación y manejo de permisos por cada consumo de su servicio REST.

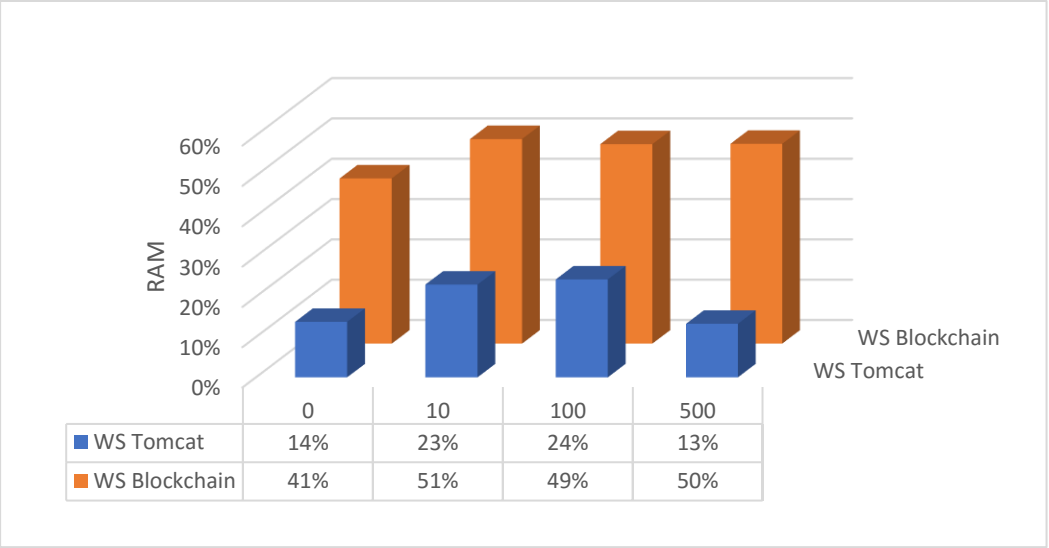

Figura 33. Consumo de CPU

5.4.3 RAM

Como se puede apreciar, en la Figura 34 el consumo de las dos APIs se mantiene casi constantes en la inserción de los registros. Sin embargo, el sistema basado en Blockchain continúa consumiendo más memoria RAM, aproximadamente 10% más, lo que se debe a que tiene más instancias y procesos corriendo que la API de Tomcat.

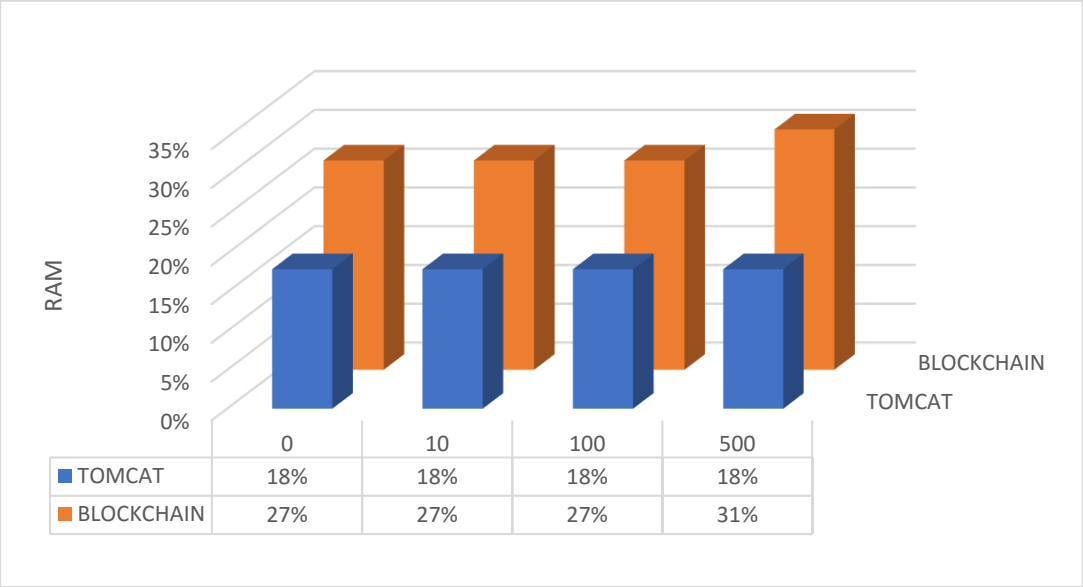

Figura 34. Consumo de memoria RAM

5.4.4 IOTRANSFER

Se puede observar en la Figura 35 que el sistema de Blockchain escribe más bloques por segundo en comparación con el API de Tomcat, de forma especial en la inserción de los últimos 500 registros con una diferencia 329%.

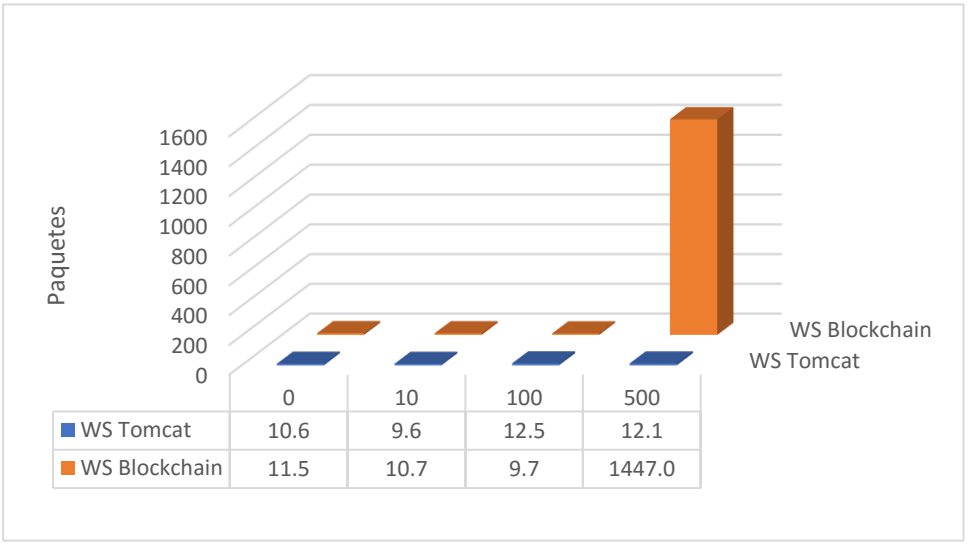

Figura 35. Paquetes escritos por segundo

5.4.5 Procesos

En Figura 36 se visualiza que en los primeros 100 registros las dos APIS se comportan similar. Sin embargo, al insertar los últimos 500 registros crece exponencialmente debido a que se van creando más bloques, y todos están encadenados lo que consume más recursos para el sistema.

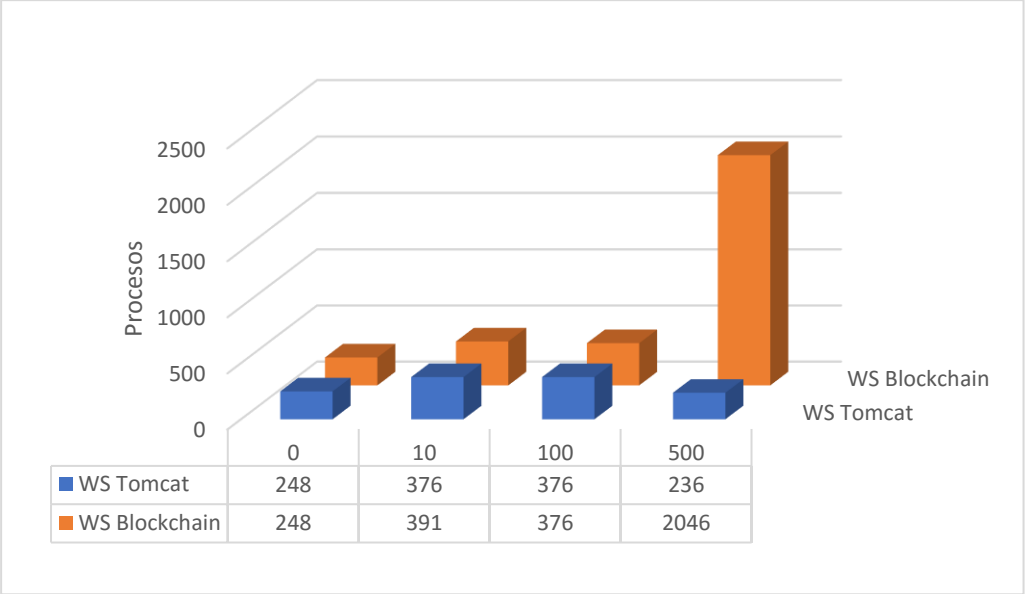

Figura 36. Procesos creados por segundo

5.4.6 Desempeño de la red

En las figuras 37 y 38 se muestra el tráfico de los servicios al insertar 500 registros. El tráfico que se envía por medio del Blockchain llega a los 2100 paquetes siendo mayor que el de Tomcat, el cual llega a un máximo de 32 paquetes. Estos datos fueron tomados durante 21 minutos que demoró el sistema de Blockchain en ingresar los 500 registros.

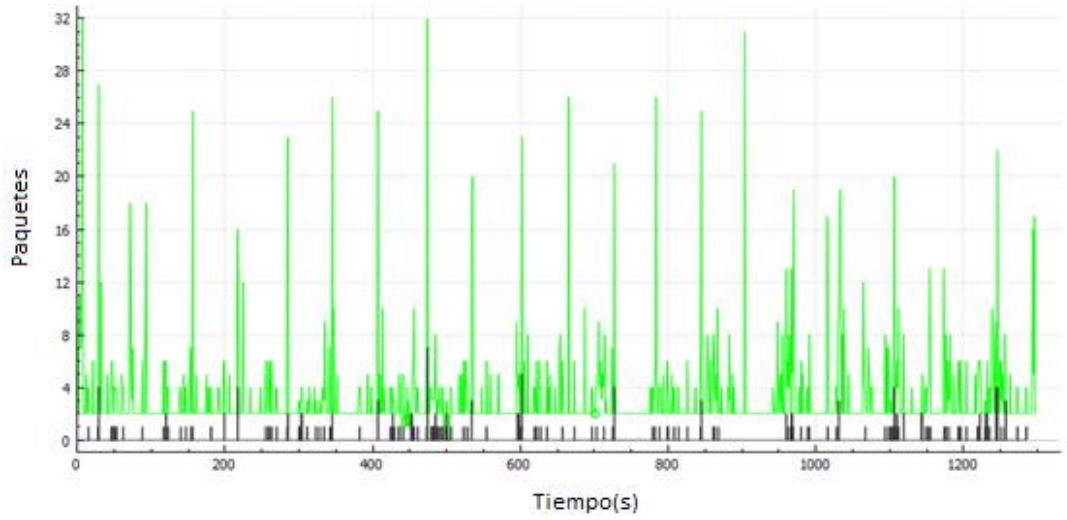

Figura 37. Tráfico para Tomcat

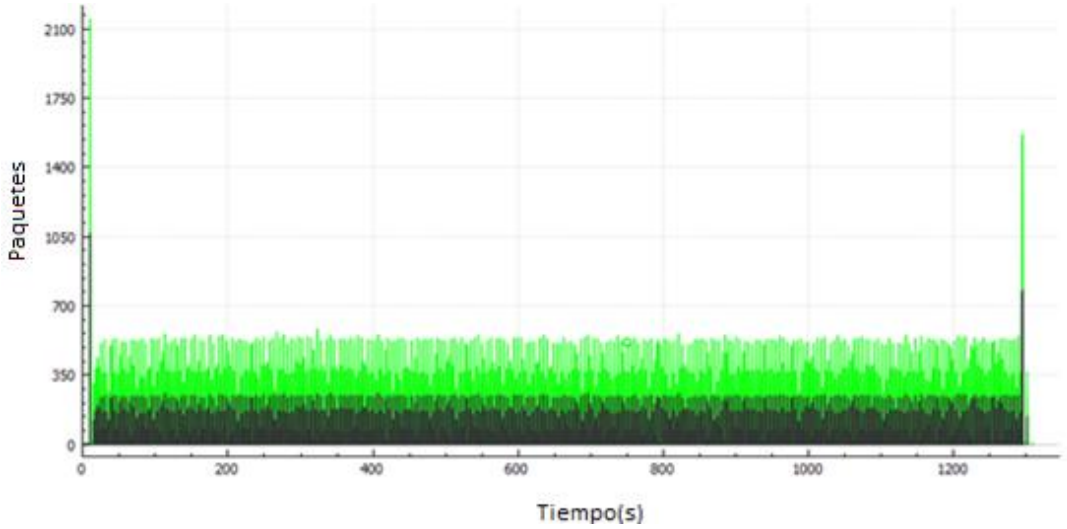

Figura 38. Tráfico para Blockchain

A través del análisis realizado se ha argumentado como el Blockchain desarrollado mejora la seguridad de la información. Sin embargo, esta seguridad significa un sacrificio en cuanto a los recursos computacionales que se observaron en las figuras [32-38], lo que es comprensible ante los procesos que el sistema de Blockchain ejecuta para mantener la confidencialidad e integridad de los datos.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

En el siglo XXI el derecho de identidad digital y la identificación debe ser garantizada por la legislación de cada país, de forma tal que es imprescindible un sistema para el manejo de identidades digitales que ofrezca la seguridad necesaria para que los usuarios puedan confiar su información personal y así evitar delitos como el robo de información o suplantación de identidades.

El presenta trabajo se originó en busca del desarrollo de un prototipo para el manejo de identidades digitales utilizando tecnología Blockchain. Para cumplir con este objetivo se ha buscado las herramientas más adecuadas que se adapten a la privacidad que exige la gestión de identidades digitales, seleccionando así el framework Hyperledger Fabric por la seguridad que ofrece en cuanto a disponibilidad, confidencialidad, integridad, trazabilidad, autenticación y no repudio. Este framework lo aloja la fundación Linux, con la contribución de ingenieros de IBM.

El prototipo desarrollado cumple con los requerimientos funcionales sobre identidades digitales, que se basa principalmente en que la persona es dueña de su información, conoce todos los datos que se almacenan, decide cuándo y con quien compartirla. Además, el prototipo maneja la seguridad a través de las características de Blockchain descritas en este documento, donde se destaca la criptografía, la descentralización, el Ledger que contiene el historial inmutable de transacciones, el manejo de permisos a través de llave pública y privada, entre otras.

Actualmente Blockchain carece de una metodología específica, por lo cual se decidió aplicar la metodología de desarrollo ágil SCRUM, que permitió realizar el proyecto en iteraciones.

Las primeras iteraciones fueron investigativas ya que el proceso de comprensión de esta tecnología es amplio y complejo, pues utiliza varios términos nuevos o poco conocidos. Por ejemplo, se encontró tesis de maestría solo dedicadas al estudio de algún tipo de algoritmo de consenso, otras exclusivas para identidades digitales, para contratos inteligentes, etc.

Como contribución de este estudio fue el acoplamiento de la tecnología Blockchain a las principales necesidades del manejo de identidad digital que se extendió a un prototipo funcional, ya que a la fecha de la escritura de este documento, únicamente se ha encontrado estudios teóricos sobre el manejo de identidades digitales con Blockchain, por lo que este proyecto presenta un aporte sustancial donde se verifica que es posible crear un Blockchain privado, a diferencia de las criptomonedas de acceso público, el modelo planteado en este proyecto maneja permisos de lectura específicos para cada participante.

La tecnología Blockchain aún se encuentra en sus primeros años y, por supuesto, existen grandes desafíos por delante para reemplazar por completo los antiguos sistemas de gestión de identidad con tecnología moderna. La programación robusta y criptográficamente segura del Blockchain presta confidencialidad de la información, pero se deben establecer aún la supervisión, regulaciones y estándares de consenso antes de que sea posible la adopción generalizada. Asimismo, sin la aceptación de los consumidores, ninguna solución basada en Blockchain para identidades digitales será útil.

6.2 Recomendaciones

Se recomienda a la legislación de cada país tomar conciencia de la importancia de la protección de datos, para que los derechos de las personas sean respetados en forma integral en Internet. También promover y fortalecer una Cultura de Identidad Digital segura.

Se debe considerar de los peligros que la tecnología Blockchain puede traer. Uno de los que más parece preocupar es justamente su carácter de registro inmutable, que puede ser claramente positivo para algunos campos, como negativo para otros.

Es importante continuar estudiando un método para la formalización de autenticación de los usuarios en sistemas digitales que incremente fiabilidad al proceso.

Se recomienda continuar investigando nuevos campos de aplicación de esta tecnología descentralizada que pretende mejorar la seguridad de la información y disminuir identidades intermedias.

REFERENCIAS BIBLIOGRÁFICAS

Aitzhan, N. Z. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*.

Anderson, J. C. (2010). *CouchDB: The Definitive Guide: Time to Relax.* San Francisco: O'Reilly Media, Inc.

Angraal, S., Krumholz, H., & Schulz, W. (2017). Blockchain technology: applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, 9.

Aublin, P. M. (2013). Rbft: Redundant byzantine fault tolerance. *IEEE 33rd International Conference*, pp. 297-306.

Aumasson, J. &. (2016). Blockchains in 2016: status quo and scaling challenges. *Kudelski Security*.

Barrientos, P. (2014). *Enfoque para pruebas de unidad basado en la generación aleatoria de objetos.* La Plata: Universidad Nacional de La Plata.

Bertino, E., Paci, F., Ferrini, R., & Shang, N. (2009). Privacy-preserving digital identity management for cloud computing. *IEEE Data Eng. Bull*, 21-27.

Booch, G. R. (1999). *El lenguaje unificado de modelado.* Madrid: Addison Wesley.

Bramhall, P. H. (2007). User-centric identity management: New trends in standardization and regulation. *IEEE Security & Privacy*, vol. 5, no 4.

Calderón, C. A. (2010). *La presentación del sí-mismo en los entornos virtuales.* Madrid: Universidad Complutense de Madrid.

Camp, J. (2004). Identidad digital. *IEEE Technology and society Magazine*, 34-41.

Castro, M. &. (2002). Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)*, 398-461.

Chen, L. X. (2017). On Security Analysis of Proof-of-Elapsed-Time (PoET). *In International Symposium on Stabilization, Safety, and Security of Distributed Systems. Springer, Cham*, 282-297.

Christidis, K. &. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access*, 2292-2303.

Corda Enterprise. (2018). *R3 Corda*. Obtenido de Corda: https://www.corda.net

Crosby, M. P. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 6-10.

Daemen, T., & Rubinstein, I. (2006). The identity metasystem: Towards a privacy-compliant solution to the challenges of digital identity. *MICROSOFT CORPORATION*.

Dorri, A. K. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE International Conference* , 618-623.

edX. (2017). *Blockchain for Business - An Introduction to Hyperledger Technologies*. Obtenido de edX: https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/course/

Halim, R. S. (2009). Digital Identity Management. *Linköpings university, Sweden*.

Houy, N. (2014). It Will Cost You Nothing to'Kill'a Proof-of-Stake Crypto-Currency. *University of Lyon*.

Hyperledger . (2018). *Hyperledger Burrow v0.16*. Obtenido de Hyperledger Burrow : https://github.com/hyperledger/burrow/

Hyperledger. (2017). *Hyperledger Sawtooth documentation.* Obtenido de Hyperledger Sawtooth: https://sawtooth.hyperledger.org/docs/

Hyperledger. (2017). Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus. *Hyperledger Architecture, Volume 1*.

Hyperledger. (2017). *Welcome to Hyperledger Fabric*. Obtenido de Hyperledger Fabric: http://hyperledger-fabric.readthedocs.io

Hyperledger. (2018). *Indy Node*. Obtenido de Hyperledger Indy: https://github.com/hyperledger/indy-node/

Hyperledger Composer. (30 de 06 de 2018). *Introduction Hyperledger Composer*. Obtenido de Docs Hyperledger Composer: https://hyperledger.github.io/composer/latest/introduction/introduction

IBM. (2018). *Blockchain security: What keeps your transaction data safe?* Obtenido de Blockchain Unleashed: IBM Blockchain Blog: https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/

ISO 2700. (22 de Febrero de 2018). *ISO 27000.es*. Obtenido de http://www.iso27000.es/iso27000.html

ISO 9001. (2013). *ISO 9001 calidad*. Obtenido de Sistemas de Gestión de Calidad según ISO 9000: http://iso9001calidad.com/definicion-de-terminos-586.html

Karame, G. (2016). On the security and scalability of bitcoin's blockchain. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1861-1862.

Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954.

Kosba, A. M. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *In Security and Privacy (SP), 2016 IEEE Symposium*, 839-858.

Kuchkovsky, C., Fernández, R., & Molero, I. (2018). *Blockchain: La revolución industrial de internet.* Bogotá: Planeta Colombiana S.A.

Li, Y. &. (2013). A performance comparison of SQL and NoSQL databases. In Communications, computers and signal processing (PACRIM). *IEEE pacific rim conference*, (pp. 15-19.

Linux Foundation. (Septiembre de 2017). *Hyperledger*. Obtenido de About Hyperledger: https://hyperledger.org/about

Lootsma, Y. (2017). Blockchain as the Newest Regtech Application—the Opportunity to Reduce the Burden of KYC for Financial Institutions. *Banking & Financial Services Policy Report*, 16-21.

Mellmer, J. A., Young, R. T., Perkins, A. D., Robertson, J. M., Sabin, J. N., McDonald, M. C., & Carter, S. R. (2014). *U.S. Patent No. 8,631,038.* Washington: Patent and Trademark Office.

MultiChain . (01 de Marzo de 2018). *MultiChain* . Obtenido de MultiChain : https://www.multichain.com/

Pressman, R. (2010). *Ingeniería del software un enfoque práctico.* México: The McGraw-Hill.

Proyectos agiles - Funcionamiento. (11 de Julio de 2017). Obtenido de https://proyectosagiles.org/como-funciona-scrum/

Proyectos agiles - Introducción. (14 de Julio de 2017). Obtenido de https://proyectosagiles.org/que-es-scrum/

Robert J, & Jenkins Jr. (1997). *Hash Functions for Hash Table Lookup.* Burtleburtle. Obtenido de Burtleburtle.

Schwaber, K., & Sutherland, J. (2013). *La Guía Definitiva de Scrum: Las Reglas del Juego.*

Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review*.

Trigas, M. (Julio de 2012). *Metodología Scrum*. Obtenido de SCRUM: https://www.scrumguides.org/docs/scrumguide/v1/scrum-guide-es.pdf

Vasin, P. (2014). *Blackcoin's proof-of-stake protocol v2.* Obtenido de https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 1-32.

YOTI. (2017). *Your Digital Identity*. Obtenido de Yoti: https://www.yoti.com/

Zyskind, G. &. (2015). Decentralizing privacy: Using blockchain to protect personal data. *Security and Privacy Workshops (SPW), IEEE* , 180-184.