

Modelo Blockchain para el aseguramiento de la Información en Certificados de Notas SSA-UMSA (Sistema de Seguimiento Académico - UMSA)

Cristhian Jesús Mejía Fernández
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
crismefe@gmail.com

Resumen—Desde sus inicios la palabra Blockchain está relacionada con Bitcoin. También heredó la especulación y la exageración. Se mencionó y se continúa mencionando que Blockchain es la tecnología disruptiva de esta década. La tecnología que cambiará los silos de información centralizados en la nube por bases de datos descentralizadas. La tecnología que quitará los intermediarios y proveerá confianza entre desconocidos en todo tipo de transacciones. Asegurar la información es crítico, ya que a partir de esta se da confianza a los datos que almacenan. La metodología aplicada a la investigación es exploratoria y la técnica de investigación es observacional. Es por ese motivo que el actual Sistema de Seguimiento Académico en la emisión de Certificados de Notas tiene un rol crucial en lo que se refiere a la Integridad de la Información, siendo que la información que va ser contenida en estos documentos no debe de ser alterada, debe ser verificable y se trazable. Se presentan de esta manera certificados estampados y registrados en una estructura de datos inalterable y verificable, lo cual representa una solución a la susceptibilidad de alteración o falsificación de certificados de notas.

Palabras Clave—bitcoin, blockchain, sistema de seguimiento académico SSA, DLT, BPM, hyperledger.

I. INTRODUCCIÓN

La información hoy en día es considerada como uno de los activos más importantes para cualquier entidad, institución, empresa o incluso una persona. Todo se debe a que la digitalización de la misma hace que el tratamiento de esta sea más eficiente además de brindar resultados al realizar consultas con la misma.

Ante esto, los Sistemas de Información fueron desarrollados con el fin de gestionar la información de manera eficaz, eficiente y oportuna. Pero debido al crecimiento significativo en esta última década (2009-2019), la información puede sufrir diferentes tipos de amenazas y riesgos que conllevarían a que los resultados no sean los adecuados y por ende puedan repercutir negativamente a la entidad.

Es por eso que la seguridad de la información promueve un conjunto de medidas preventivas y reactivas, para que las

organizaciones puedan proteger y mantener la confidencialidad, la disponibilidad y sobre todo la integridad de la misma.

Ante diferentes riesgos y amenazas que sufre la información incluso cuando está siendo administrada por algún intermediario que proteja la misma, el contratista desconoce las medidas de seguridad que están siendo tomadas para el resguardo de esta.

Siendo que la información es delicada y más aún cuando se trata de información financiera, esta debe de garantizar más que todo, su integridad, ya que, aunque se tengan medidas de confidencialidad o de disponibilidad, si esta es alterada pierde el sentido que se le dio.

Así mismo la información académica de estudiantes es crítica, dado que de ella depende el rendimiento académico, además a tomar decisiones con el uso de estadísticas académicas. Más aún si se certificaran estos datos en documentos que posteriormente serán utilizados de manera legal (en muchos de los casos) o como el interesado lo requiera.

Es por eso que hoy en día se crearon nuevas técnicas para asegurar la integridad de la información en diferentes Sistemas de Información. Una de ellas es el Blockchain que es utilizada en el intercambio de criptomonedas o criptodivisas (dinero digital) [1].

Blockchain, según la página Economía simple.net: “Las cadenas de bloques es una tecnología creada para dotar de propiedad digital a las personas en el mundo online sin necesidad de ningún intermediario, ni ninguna autoridad central que controle a los usuarios que participan en una transacción y las cosas que adquieren” [2].

Es en sí un marco de trabajo (Framework) o también en otros textos como una nueva estructura de datos, con el cual se puede asegurar la integridad de la información, de esta manera se garantiza que el procesamiento de esta información sea altamente confiable y que además se pueda realizar un seguimiento a todas las transacciones que fueron realizadas desde un inicio (Génesis).

Así mismo la seguridad de la información tiene tres características que se deben de contemplar, los cuales son:

Para referenciar este artículo (IEEE):

[N] C. Mejía, «Modelo Blockchain para el aseguramiento de la Información en Certificados de Notas SSA-UMSA (Sistema de Seguimiento Académico - UMSA)», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, n° 8, pp. 52-57, 2020.



¹ DLT: Traducción del inglés a Tecnologías de Registro Contable Distribuida

confidencialidad, disponibilidad e integridad. En el presente trabajo nos enfocaremos en la integridad de la información el cual es, “El objetivo de la integridad es que los datos queden almacenados tal y como espera el usuario: que no sean alterados sin su consentimiento” [3].

En el presente trabajo, de acuerdo al fundamento teórico que tiene Blockchain, se realizara un modelo con el cual se asegure la integridad de la información contenida en los certificados de notas que se emiten en el Sistema de Seguimiento Académico de la Universidad Mayor de San Andrés - UMSA.

En este sentido se planteó el problema que existe en la integridad de los Certificados de Notas que es el siguiente: ¿Cómo asegurar la integridad de la información, al momento de la emisión de certificados de notas mediante el Sistema de Seguimiento Académico de la UMSA (SSA-UMSA)?

Para poder solucionar este problema se plantea un modelo de aseguramiento de la integridad de la información utilizando Blockchain en la emisión de certificados de notas del SSA.

Al realizar el análisis pertinente del problema se pudo realizar su operacionalización identificando las siguientes:

TABLA I. OPERACIONALIZACIÓN DE VARIABLES

Variables Independientes	Variables Dependientes	Variables Intervinientes
Blockchain. Certificados de Notas.	Plantear un modelo de aseguramiento de la integridad de la información.	Sistema de Seguimiento Académico - UMSA

Justificación: Al asegurar la información, los actores registraran y verificaran información íntegra, de esta manera existirá confianza en el uso del SSA. Si se requiere asegurar la información utilizando otro tipo de tecnología o infraestructura el costo sería elevado por lo utilizando *blockchain* se reducen los recursos económicos. Blockchain es una tecnología que moderna y que está a la vanguardia de la integridad de la información, es una nueva herramienta que se puede utilizar en otros proyectos. El uso de métodos criptográficos y otros mecanismos para asegurar la información hace que se siga investigando en el desarrollo de nuevos algoritmos que sean más eficientes.

El desarrollo de la investigación se realizará en el Departamento de La Paz, donde se encuentran los servidores que están instalados el SSA-UMSA.

Se trabajará sobre los datos que se encuentran en el SSA-UMSA a partir de marzo de 2012, (ya que se empezó a utilizar el sistema mediante la Resolución de Honorable Consejo Universitario Nro. 87/2012) [4] hasta la presente gestión.

II. BLOCKCHAIN

A. Una breve definición

A nivel técnico, *blockchain* se puede definir cómo un registro contable (*ledger*) que registra transacciones agrupadas en bloques dentro de una red distribuida de nodos, donde cada nodo mantiene una copia del ledger. Los nodos ejecutan un protocolo de consenso que valida las transacciones,

agrupándolas en bloques, y construyendo una cadena de seguridad con hash.

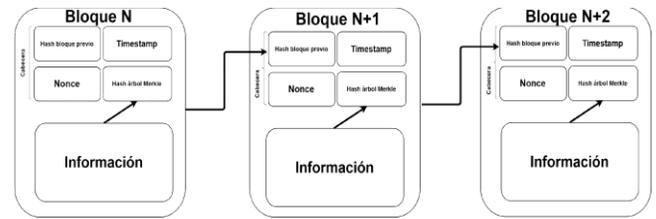


Fig. 1. Cadena de Bloques

B. Historia

Blockchain promete resolver fundamentalmente problemas de tiempo y confianza para acometer las ineficiencias y los costos en industrias tales como servicios financieros, cadenas de suministro, logísticas y sanitarias. Las características clave de blockchain incluyen la inmutabilidad y un libro de registro contable (*ledger*) distribuido donde las actualizaciones sobre las transacciones se realizan mediante un sistema de confianza basado en consenso, que puede facilitar una auténtica interacción entre múltiples partes, porque solo es posible su actualización mediante la suma de un bloque vinculado al bloque anterior.

Esta interacción digital no solo está limitada por una confianza sistémica, sino que además asegura que la procedencia transaccional del registro mantiene un historial inmutable de interacción entre las partes. Con el diseño del sistema blockchain, se intenta construir un sistema que lleva implícita la confianza, lo que conduce a reducir riesgos, y, con varias construcciones tecnológicas aplicadas, tales como criptografía, encriptación, *smarts contracts* y consenso, con lo que se consigue fundir una mayor seguridad en el sistema de transacciones.

Inicialmente la tecnología blockchain se gestó e implementó en 2008, por Satoshi Nakamoto², como una infraestructura destinada al Bitcoin que mejoraba la confianza digital mediante la descentralización, ya que, a partir de un núcleo se extraen bloques que, mediante la interconexión forman cadenas mayores cuya finalidad es transportar transacciones.

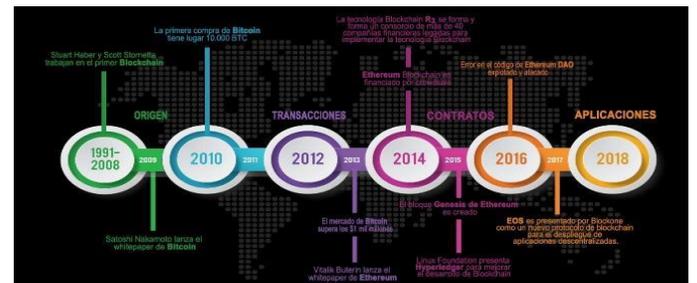


Fig. 2. Historia de la Tecnología Blockchain [5]

Posteriormente Vitalik Buterin, uno de los primeros desarrolladores de Bitcoin, comenzó a formar Ethereum, presentado en 2015 como blockchain pública para mejorar las funcionalidades del Bitcoin, pasando de ser solamente una criptomoneda a una nueva plataforma para el desarrollo de aplicaciones descentralizadas. Ethereum actualmente es de las

² Satoshi Nakamoto: Creador de la criptomoneda Bitcoin, sin embargo, se cree que solo es un seudónimo ya que hasta la fecha no se conoce a dicha persona.

tecnologías blockchain más importantes, al incorporar los conceptos de contrato inteligente y aplicaciones descentralizadas.

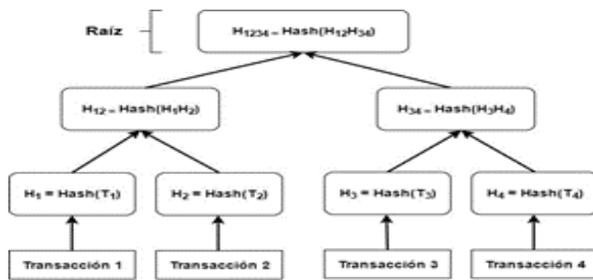


Fig. 3. Árbol Hash de Merkle

Existen dos tipos de blockchain, *permissionless* (públicas) y *permissioned* (privadas).

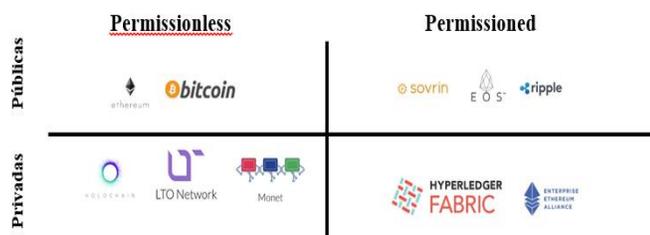


Fig. 4. Tipos de Blockchain

C. Permissionless Blockchain

Un *blockchain permissionless* o pública, es un tipo de blockchain completamente descentralizado que no requiere ningún tipo de autorización, solamente es preciso colaborar con la red para mantener el consenso. Todos los miembros tienen el derecho de realizar todas las acciones, incluyendo agregar y validar transacciones, contratos inteligentes, etc.

Las ventajas de este tipo de blockchain son:

- Ofrecen una plataforma descentralizada, lo que significa que la información no se almacena en un repositorio central y cualquier persona puede acceder a la información en cualquier momento y desde cualquier lugar.
- Proporciona firmas inmutables para todos los registros. Todo el intercambio de información y las transacciones se cifran criptográficamente, lo que hace que todo el sistema y los datos permanezcan seguros.
- Anonimato: Los mineros y participantes en la red permanecen en el anonimato.
- Transparencia: Todos los datos e información son visibles para todos.
- Transacciones rápidas y fáciles.

Las desventajas son:

- Anonimato: aunque es una buena señal de que la identidad de las partes comerciales permanezca en el anonimato, esto puede volverse un problema. En caso

de que haya un fraude o alguien quiera rastrear a las partes que están negociando, esto se vuelve difícil, debido a estas características, se puede utilizar blockchain para actividades ilícitas.

- Mecanismo de consenso: este tipo de blockchain, funciona según el principio de *Proof-of-Work*³ donde los participantes tienen que resolver el complejo rompecabezas matemático, lo que requiere el consumo de una gran cantidad de recursos, y por lo tanto, es muy costoso.
- Ofrece un tamaño de bloque limitado.
- No es necesario probar la identidad. Lo único necesario es comprometer la capacidad de procesamiento para convertirse en parte de la red. Cualquier minero que resuelva el rompecabezas puede convertirse en parte del sistema.

Estos inconvenientes del sistema *blockchain permissionless* hacen que muchas compañías cuestionen el sistema. Por lo que *Ethereum*, *blockchain* de este tipo, está cambiando su mecanismo de consenso *proof-of-work* a *proof-of-stake*⁴.

Dos de los ejemplos más representativos que utilizan este tipo de Blockchain son Bitcoin y Ethereum.

D. Permissioned Blockchain

En las *blockchain permissioned* o privadas a diferencia de las públicas vistas anteriormente, la participación en la red no es abierta. Se controla el acceso de los participantes a ciertas funciones de la red mediante roles, que se establecen de forma flexible y que se ajusta a las situaciones particulares.

El establecimiento de los roles es flexible y puede ajustarse a condiciones particulares, esto quiere decir, que la lectura y la escritura que se efectúa en la base de datos debe ser autorizada total o parcialmente para cada componente.

En este tipo de blockchain no existe la necesidad de utilizar una criptomoneda, ya que no es necesario crear ningún sistema de estímulo *como proof-of-work* o *proof-of-stake*.

Las ventajas de este tipo de blockchain, son:

- Ofrecen un rendimiento más eficiente en comparación con las redes públicas de blockchain. En una red de blockchain, todos los nodos de la red deben calcular y validar las transacciones en la red. Estos nodos a menudo realizan cálculos redundantes para validar transacciones en la red. Debido a que los *permissioned blockchain* solo requieren que sus nodos miembros validen las transacciones, ofrecen un mejor rendimiento en relación con la cantidad de cómputo utilizada para la validación.
- Tienen estructuras de gobierno claramente definidas en comparación con las redes públicas de blockchain. Los *blockchain* públicos funcionan como foros públicos donde cualquier persona que opere un nodo completo tendría algo que decir en el gobierno y las reglas de la red. Como consecuencia, las actualizaciones y los desarrollos en estas redes son increíblemente lentos, ya

³ Proff of Work: Prueba de Trabajo traducción al español. Es un método de consenso que se utiliza para la creación de nuevos bloques dentro de la red Bitcoin.

⁴ Proff of Stake: Prueba de Estaca traducido al español. Es un método más eficiente que la prueba de trabajo. Este también es un mecanismo de consenso utilizado por Ethereum.

que varios nodos independientes, actuando en su propio interés, deberían llegar a un consenso para activar una actualización de la red. Sin embargo, los nodos en permissioned blockchain son capaces de avanzar con las actualizaciones mucho más rápido. Si bien a veces puede haber debates sobre las actualizaciones de una red de permissioned blockchain, estos debates son más fáciles de resolver entre un consorcio de empresas en comparación con una arena pública de cientos de miles de personas y entidades.

Como principales desventajas:

- La seguridad depende completamente de la integridad de sus miembros. Si un grupo interno de miembros en un permissioned blockchain se confabula para cambiar los datos, puede arruinar la integridad de la red en su beneficio.
- En comparación con las bases de datos públicas, los permissioned blockchain son más propensas a la censura y la regulación. Debido a que estos blockchain son administrados por un consorcio de empresas, deben cumplir con las mismas regulaciones que sus miembros. De forma que, en teoría, un regulador podría imponer sus leyes censurando las transacciones que considere oportunas. Si bien la amenaza de la regulación puede no afectar las operaciones diarias de las empresas que ya cumplen con las leyes vigentes, evitaría que las empresas que necesitan las características no censurables de los blockchain públicos puedan operar en los permissioned blockchain.

E. Hyperledger

Hyperledger es una permissioned blockchain o blockchain privada, en el que varios equipos de desarrollo están colaborando para crear código abierto (*open source*), iniciado en 2015 por la Fundación Linux, que incluye líderes en finanzas, banca, IoT, cadena de suministro, fabricación y tecnología.

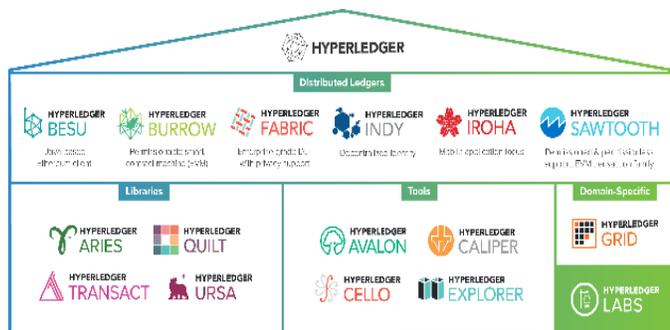


Fig. 5. Paraguas de DLT y herramientas de Hyperledger [6]

F. Hyperledger Fabric

Hyperledger Fabric es una tecnología ledger distribuida privada aplicable al negocio, privada es la palabra clave que diferencia a Hyperledger de otras tecnologías Blockchain más orientadas hacia el dominio público como Ethereum y Bitcoin. La aplicación comercial requeriría que el sistema de ledger distribuida tenga ciertas características que son muy diferentes

de las características deseadas en una tecnología de Ledger distribuida pública.

Hay cuatro características que hacen que Hyperledger Fabric sea adecuado para implementar negocios basados en aplicaciones DTL (distributed ledger technology). Hyperledger Fabric es una red permissioned, por lo que soporta transacciones confidenciales, no es precisa la utilización de criptomonedas y es programable.

Con estas características Hyperledger Fabric consigue establecer confianza, transparencia y responsabilidad entre los participantes en la red.

Hyperledger Fabric permite crear una red de permisos, proporciona herramientas para que los propietarios de la red puedan restringir quién puede acceder, y qué pueden hacer en la red. Requiere que los participantes en la red sean conocidos y que, para unirse a la red los participantes deban conseguir permisos de la autoridad reguladora.

Hyperledger es una red privada, esto quiere decir que es necesario asignar identidades a los participantes en el proyecto, las empresas negocian con entidades conocidas, proveedores de materias primas o compradores de bienes.

En algunas industrias, por ley, se supone que las empresas solo interactúan con entidades conocidas, por ejemplo, en la industria bancaria, los bancos deben conocer la identidad de cada cliente.

Luego están las agencias reguladoras que interactúan con las empresas. Una tecnología de contabilidad distribuida se basa en aplicaciones para negocios que requieren soporte para administrar identidades en las redes, la aplicación de negocio define los roles que se asigna a los participantes y el acceso se concede o no en base a estos roles. Un servicio abstracto denominado proveedor de servicios de miembros (*membership service provider*) se encarga de generar las credenciales para los distintos participantes.

La identidad de los miembros en la red de Hyperledger se gestiona mediante certificados X509⁵, cuando se crea una identidad se le expide un certificado, cada vez que este participante inicia una transacción se certifican las claves privadas en la firma, de forma que cualquier componente de la red puede validar la autenticidad de la transacción, utilizando la clave pública asociada. Los certificados siguen el proceso típico de emisión y la revocación por parte de las autoridades de certificación en la red.

G. Aspectos legales y normativos

De acuerdo al decreto supremo Nro. 1793 de 13 noviembre de 2013 en su artículo 3 respecto a Seguridad Informática, firmas y certificados digitales, tratamiento de datos personales y el artículo 4 de los principios documentos digitales, autenticidad, integridad, no repudio, transparencia, seguridad y confidencialidad, tiene como objeto “Reglamentar el acceso, uso y desarrollo de las Tecnologías de Información y Comunicación – TIC, en el marco del Título IV de la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación” y su ámbito de aplicación es “...se aplicará a personas naturales o jurídicas, públicas o privadas que realicen actividades o presten servicios

⁵ Certificados X509: Es un documento digital que ha sido codificado y/o firmado digitalmente de acuerdo a la RFC 5280.

relacionados con la certificación digital, gobierno electrónico, software libre, correo electrónico y el uso de documentos y firmas digitales en el Estado Plurinacional de Bolivia” [7]. En este sentido mediante este decreto reglamenta el uso de las certificaciones digitales y documentos electrónicos para cumplir con el objetivo y principios que fueron mencionados.

Que mediante Resolución del Honorable Consejo Universitario Nro. 87/2012, considera que “El Sistema de Seguimiento Académico integrado permitirá a la autoridades universitarias obtener en línea información del estudiante, ... estudiantes pueden obtener información académica donde se encuentre y exista internet a fin de revisar sus notas y datos personales”, “Que en la Universidad existen varios sistemas de seguimiento académico de estudiantes con el mismo objetivo; el Sistema de Seguimiento Académico propuesto, permitirá utilizar un sistema con tecnología de punta y está conformado por una aplicación web, con el uso de formularios normalizados, estadísticas confiables, para agilizar los trámites en la División de Gestiones y Admisiones y la División de Títulos y Diplomas” aprueba en su artículo segundo “Aprobar la obligatoriedad que tienen todas las Unidades Académicas (Facultades, Carrera e Institutos) de la Universidad Mayor de San Andrés, utilizar el Sistema de Seguimiento Académico” [4].

Que mediante Resolución de Honorable Consejo Universitario Nro. 576/2014, considera la aprobación de la Matricula Electrónica Universitaria y el Certificado Único de Calificaciones que “... está conformado en su primera parte, por los datos personales del estudiante, incluido la fotografía y el código DATAMATRIX; en la segunda parte se encuentran las materias aprobadas por el estudiante plasmado de forma cronológica” aprueba en el artículo primero “Aprobar la implementación de la Matricula Electrónica y el Certificado Único de Calificaciones de la Universidad Mayor de San Andrés, la misma que será aplicada en todas las Facultades que tomen la decisión de utilizarla” [8].

III. MÉTODOS

Para el enfoque de la presente investigación, donde se pretende modelar sobre una tecnología nueva y no utilizada aun en aplicación en el ámbito de la UMSA y sobre todo por el planteamiento del objetivo y definición del problema, el proyecto de investigación el diseño será experimental, el tipo será aplicada; utilizará la investigación exploratoria, la técnica de investigación será la observación.

El proceso de desarrollo se enfocará únicamente en el diseño del modelo y arquitectura de la Blockchain que se utilizará para resolver el problema de investigación.

Para ello el Sistema de Seguimiento Académico solo debe de utilizar una API (*Application Programming Interfaces*) para poder enviar información al Blockchain que será de tipo privativa ya que los nodos distribuidos estarán ubicados en los mismos servidores que tienen instalados los Sistemas de Seguimiento Académico de una Facultad, Carrera o Instituto. Si estos nodos no se encuentran certificados para poder acceder a la red serán rechazados. El modelo de muestra en la siguiente figura:

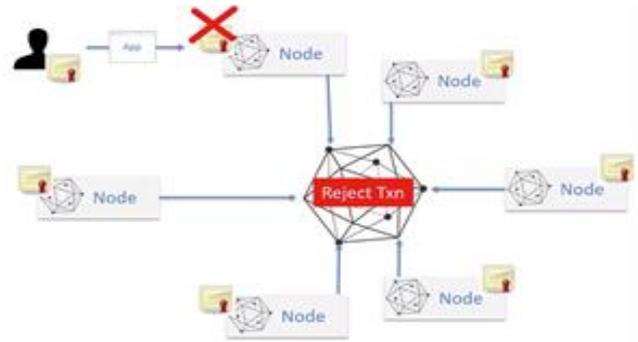


Fig. 6. Ejemplo de transacción rechazada porque un nodo tiene un certificado no válido [9]

Hay tres tipos distintos de nodos, como se ve en la figura 7, el primer tipo es el nodo *cliente*, que usan las aplicaciones para iniciar las transacciones. El segundo tipo es el nodo *Peer*, que mantienen el *ledger* sincronizado a través de la red y el tercer tipo, son los nodos *Orderers* que son los responsables de la distribución de transacciones.

Estos nodos deben de estar funcionando en cada uno de los servidores que contendrá el Blockchain, así como el Sistema de Seguimiento Académico.

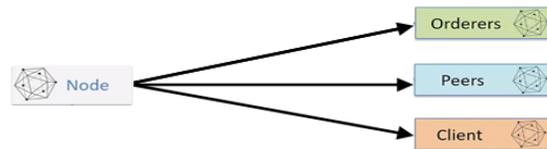


Fig. 7. Tipos de Nodos [9]

Así mismo se utilizar el modelo se adaptara a la arquitectura de negocio de procesos de gestión de BPM⁶, de esa manera se integrara el proceso de generación de Certificados de Notas con *Hyperledger Fabric*.

IV. RESULTADOS ESPERADOS

El modelo que se plantea está en función de cliente, que en este caso será el Sistema de Seguimiento Académico junto al proceso de generación de certificados de notas, los cuales son los que serán registrados en la Blockchain. Para ellos el flujo de trabajo está representado en el siguiente diagrama de secuencia de acuerdo a un BPM.

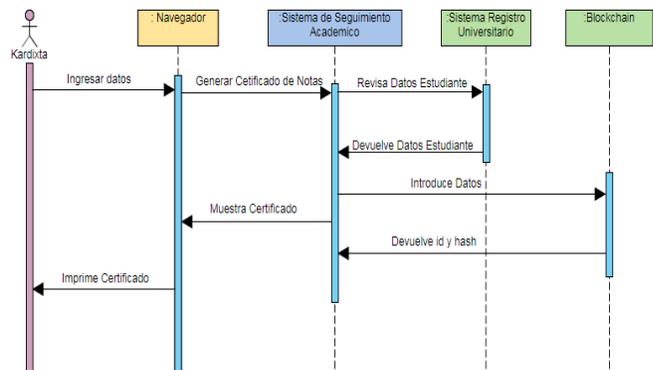


Fig. 8. Modelo de aplicación de Blockchain para el Sistema de Seguimiento Académico

⁶ BPM: Gerencia de Procesos de Negocios.

Hyperledger Fabric será la Blockchain que se encargará de realizar el registro de los metadatos del Certificado de Notas. Los componentes para dicho registro se muestran en la siguiente figura:

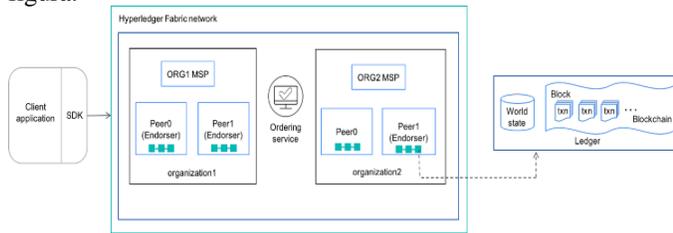


Fig. 9. Los componentes de una red de Hyperledger Fabric [9]

De esta manera cada vez que los clientes que utilicen el Sistema de Seguimiento Académico al momento de realizar el proceso de generación de Certificados de Notas irán registrando estos metadatos en la Blockchain.

V. DISCUSIÓN

De los resultados obtenidos se pudo verificar que el uso de una Blockchain no permisiva se ajusta a la arquitectura de una aplicación que ya se encuentra en desarrollo y producción como es el Sistema de Seguimiento Académico.

Así mismo los resultados obtenidos coinciden con los presentados por [10] que indica: *Hyperledger Fabric* es la infraestructura de desarrollo de aplicaciones para construir aplicaciones de blockchain basándose en Hyperledger. En otras palabras, *Hyperledger Fabric* ayuda a crear definiciones de red empresariales, que se implementan en Hyperledger, donde se ejecutan.

La belleza de *Hyperledger Fabric* reside en que proporciona una capa de abstracción de alto nivel que se puede utilizar para crear el modelo de red empresarial, escribir funciones de JavaScript para las transacciones, y exponer esas funciones como APIs para el desarrollo de aplicaciones cliente. Debido a que el nivel de programación necesario es mínimo, los propietarios empresariales que no son necesariamente desarrolladores de aplicaciones pueden crear modelos y escribir fácilmente funciones de transacciones para las redes de blockchain.

Como conclusión, la tecnología blockchain es especialmente adecuada para escenarios en los que se requiera almacenar de forma creciente datos ordenados en el tiempo, sin posibilidad de modificación ni revisión y cuya confianza pretenda ser distribuida en lugar de residir en una entidad certificadora.

Para saber si un proyecto es un caso de uso para blockchain, se aplica el siguiente enunciado y si es válido y tiene sentido para el proyecto, entonces es un caso de uso para blockchain: “un grupo de participantes, actuando como “peers” que tienen un flujo de trabajo que involucra a todos los participantes y no quieren depender de intermediarios. Pero necesitan visibilidad y transparencia a través de toda la solución” [1].

REFERENCIAS

- [1] F. Ontiveros, «Medium.com,» 10 10 2019. [En línea]. Available: <https://medium.com/@feronti/d%C3%B3nde-usar-blockchain-9fb0e23d0d53>. [Último acceso: 12 10 2019].
- [2] Economía simple .net, «¿Qué es Blockchain o Cadena de Bloques?,» 2016. [En línea]. Available: <https://www.economiasimple.net/que-es-blockchain-o-cadena-de-bloques.html>.
- [3] J. F. Roa Buendía, Seguridad informática, Aravaca, Madrid: McGraw-Hill, 2013.
- [4] Honorable Consejo Universitario - UMSA, «Gaceta Universitaria UMSA,» 23 marzo 2012. [En línea]. Available: <https://gaceta.umsa.bo/bitstream/umsa/201002/1/HCU-87-12.pdf>. [Último acceso: 12 10 2019].
- [5] N. Rodríguez, «101 Blockchains,» 3 diciembre 2018. [En línea]. Available: <https://101blockchains.com/es/historia-de-la-blockchain/>. [Último acceso: 12 10 2019].
- [6] Hyperledger, «Hyperledger,» [En línea]. Available: <https://www.hyperledger.org/>. [Último acceso: 12 10 2019].
- [7] Estado Plurinacional de Bolivia, «Bolivia Digital,» Julio 2017. [En línea]. Available: <https://agetec.gob.bo/2-plan-de-implementacion-de-gobierno-electronico.pdf>. [Último acceso: 12 10 2019].
- [8] H. C. U. -, UMSA, «Gaceta Universitaria UMSA,» 26 noviembre 2014. [En línea]. Available: <https://gaceta.umsa.bo/bitstream/umsa/357441/1/HCU-576-14.pdf>. [Último acceso: 12 10 2019].
- [9] H. Fabric, «Wiki Hyperledger Fabric» septiembre 2019. [En línea]. Available: <https://wiki.hyperledger.org/display/fabric/Hyperledger+Fabric>. [Último acceso: 12 10 2019].
- [10] Shikha Maheshwari, «IBM,» 14 diciembre 2018. [En línea]. Available: <https://www.ibm.com/developerworks/ssa/library/cl-blockchain-hyperledger-fabric-hyperledger-composer-compared/index.html>. [Último acceso: 12 10 2019].

Breve CV del autor

Cristhian Jesús Mejía Fernández es Licenciado en Informática por la Universidad Mayor de San Andrés (La Paz 2008); Certificado en Mikrotik: MTCNA, MTCRE, MTCWE y MTCTCE; Actualmente realiza la Maestría en Gerencia Estratégica en Tecnologías de Sistemas de Información GETSI en el Postgrado en Informática UMSA.

Ejerce profesionalmente como Encargado de Sistemas en la Facultad de Agronomía en la UMSA.

Obtuvo el 2do lugar Concurso ACM UMSA La Paz 2003. Es miembro del grupo Blockchain Latinoamérica.

Sus intereses investigativos incluyen Teleinformática, Desarrollo de software y Blockchain. Email: crismefe@gmail.com.