© Academia Journals 2019

IMPLEMENTACIÓN DE UN ENTORNO DE VIRTUALIZACIÓN EN SERVIDORES, PARA UN INTERCAMBIO DE DOCUMENTOS DIGITALES SEGUROS UTILIZANDO BLOCKCHAIN

Ing. Jorge Alberto Pitacua Pérez[1], Dr. Heberto Ferreira Medina[2], Dr. Anastacio Antolino Hernández[3], M.C. Cristhian Torres Millarez[4] y M.C. Rogelio Ferreira Escutia[5]

***Resumen*—Debido a los cambios en innovación tecnológica durante los últimos años, las empresas y organizaciones han tenido que irse adaptando y evolucionar hacia nuevas formas de trabajar. La virtualización es una tecnología que está cobrando importancia, debido a las numerosas ventajas que puede proporcionar. Con ésta se ahorran recursos, tiempo y dinero, permitiendo aumentar la disponibilidad de los servicios. Con su uso se pueden tener varios en máquinas virtuales (MV), donde se puede alojar más de uno.**

La virtualización garantiza la integridad de la información para un intercambio seguro con el uso de Blockchain, a través de la herramienta Hyperledger Fabric (HLF); su función es la de gestionar aspectos de seguridad, implementar tecnologías de llave pública (PKI), protocolos o tecnologías que permitan tener una integridad. La digitalización de la información es la manera de tratar los problemas que los documentos en físico suelen traer. El objetivo de este proyecto es abarcar aspectos relacionados a la virtualización para un intercambio tipo Blockchain a través de HLF.

***Palabras clave*— Virtualización, Hyperledger Fabric, Blockchain, PKI.**

***Abstract* - In line with advances in technological innovation, in recent years, companies and organizations have had to adapt and evolve new ways of working. Virtualization is a technology that has been taking importance, because of the benefits it can provide. It saves resources, time and money, since it can increase the availability of network services, with this use you can have in virtual machines (VM), where it is possible to have more than one per VM.**

Virtualization guarantees the support of the information that allows its secure exchange using a Blockchain technology, through the tool Hyperledger Fabric (HLF); which function is to manage security aspects, implement Public Key Infrastructure technologies (PKI), protocols or technologies that allow to have integrity of the information. The digitalization of information is the way to deal with problems that physical documents usually lead. The objective of this project is to cover aspects related to virtualization for a Blockchain exchange through HLF.

***Keywords* - Virtualization, Hyperledger, Blockchain, PKI.**

Introducción

La innovación tecnológica y la revolución de la información en los últimos años traen nuevos retos a las empresas y organizaciones, las cuales deben adaptarse a las nuevas formas de trabajo, desde procesos automatizados, nuevas herramientas de software, migración de datos hacia la nube, etc. La industria se ha modernizado en todos estos aspectos. Como se puede observar, esta abarca distintos niveles de la organización y dentro de este cambio y avances tecnológicos, se encuentra la virtualización, que es una tecnología que está cobrando importancia, debido a las numerosas ventajas que puede proporcionar a las organizaciones. Con ésta se ahorran recursos, tiempo y dinero; se puede tener una mejor respuesta a fallas o incidencias en el uso de las TIC (Tecnologías de la Información y comunicaciones) y por lo tanto tener mejor respuesta de funcionamiento de los servicios que se ofrecen aumentando la disponibilidad. La manera tradicional de la arquitectura de un servidor consistía en un solo servidor físico en donde

[1] Ing. Alberto Pitacua Pérez es Ingeniero en Sistemas Computacionales, del Tecnológico Nacional de México / I.T. Morelia, Michoacán, México, jpitacuaperez@gmail.com
[2] Dr. Heberto Ferreira Medina, es académico del Instituto del Instituto de Investigaciones en Ecosistemas y Sustentabilidad de la UNAM campus Morelia, también es profesor del Tecnológico Nacional de México / I.T. Morelia, en el Departamento de Sistemas y Computación, hferreira@iies.unam.mx
[3] Dr. Anastacio Antolino Hernández, es profesor titular del Departamento de Sistemas y Computación, del Tecnológico Nacional de México / I.T. Morelia, Michoacán, México, antolino@itmorelia.edu.mx
[4] M.C. Cristhian Torres Millarez, es profesor titular del Departamento de Sistemas y Computación, del Tecnológico Nacional de México / I.T. Morelia, Michoacán, México, ctorres@itmorelia.edu.mx
[5] M.C. Rogelio Ferreira Escutia, es profesor titular del Departamento de Sistemas y Computación, del Tecnológico Nacional de México / I.T. Morelia, Michoacán, México, rogelio@itmorelia.edu.mx

© Academia Journals 2019

se alojaba un conjunto de servicios en específico; base de datos, correo, servidor de documentos, servidor de dominios (DNS), Active Directory Service (ADS), entre otros. Con el uso de la virtualización se pueden tener los servicios mencionados anteriormente en un solo servidor o varios, de manera que tenemos diferentes MV, donde se puede alojar más de un componente de software en específico.

Con la implementación de entornos de virtualización, una solución en específico es la de garantizar la integridad de los documentos que se generan y que se digitalizan en los departamentos administrativos, para su intercambio con cadenas de bloques (*Blockchain*) a través de la herramienta HLF (*Hyperledger Fabric*); su función es la de gestionar aspectos de seguridad, implementar tecnologías de infraestructura de llave pública (PKI), protocolos o tecnologías que permitan tener una integridad de la información en un Blockchain, convirtiendo la gestión de accesos a la información en un sistema confiable. La digitalización de documentos es la manera de tratar los problemas que los documentos en físico suelen traer, tales como: riesgo de pérdida parcial o total, amenaza de desastres naturales, deterioro del documento con el paso del tiempo, riesgos de acceso no autorizado de personas, entre otros. Toda la implementación requerida debe tener como base una infraestructura de virtualización para lograr ser lo más eficiente posible, debido a las ventajas inherentes. Por lo tanto, el objetivo de este proyecto es abarcar aspectos relacionados al entorno de virtualización que es el soporte para generación de Blockchain a través de HLF, para de esta forma ser una base de intercambio segura.

El uso de documentos digitales en muchos sectores de la industria se ha convertido en una necesidad para el intercambio de información, además que ayudan a la sustentabilidad y preservación de los recursos naturales. La implementación del entorno de virtualización ofrece los siguientes beneficios: entorno de soporte en donde se puedan utilizar contenedores de Blockchain, firmas digitales PKI y la gestión de documentos digitales. Es posible utilizar entonces tecnología Open Source para este propósito. En Morteo (2007) se establecen las ventajas de la virtualización como tecnología, que en la tabla 1 se pueden observar de manera sintetizada.

Tabla 1. Ventajas de utilizar la virtualización (Morteo, 2007).

Ventaja	Descripción
Reducción del TCO	El costo total de la inversión en hardware y software (TCO, *Total Cost of Ownership*) de una empresa se puede ver sustancialmente reducida, al consolidar la infraestructura de cómputo (servidores), ya que se reduce el consumo de energía eléctrica y la generación de calor, el espacio utilizado y los costos de mantenimiento. Se aprovechan las arquitecturas de 64 bits en microprocesadores, multiprocesadores y el uso de recursos compartidos (*POOL*)
Mejoramiento de la productividad del usuario	La creación de MV ha demostrado ser una excelente herramienta para la distribución y puesta en marcha (*deployment*) de ambientes de prueba y servidores de producción en diversas compañías. La migración de aplicaciones y el soporte se vuelve más accesible y manejable debido a la existencia de herramientas que facilitan la transferencia de archivos entre MV, incluso permite implementación de clústeres.
Seguridad mejorada y facilidad de recuperación de desastres	Permiten la creación de redes de datos virtuales las cuales bien pueden encontrarse aisladas del resto de los equipos de la organización o dentro del esquema de compartición de recursos. Asimismo, se restringen al entorno de la MV las contingencias de seguridad, alertas por virus/spyware y las fallas totales del sistema. La infraestructura de software del sistema de virtualización hace que el respaldo de las MV sea cada vez más simple.
Agilidad	La creación de una MV es un proceso muy rápido, se utilizan plantillas para este propósito. Por tanto, si necesitamos una nueva MV se crea en el momento (aprovisionamiento bajo demanda).
Flexibilidad	Es posible crear MV con las características de: CPU, memoria, disco y red que requieran, sin necesidad de "comprar" un equipo de hardware. También ejecutar diferentes MV con sistemas operativos (*SO*) distintos.

© Academia Journals 2019

En este contexto existen cuatro modelos de virtualización que son ampliamente utilizados por las empresas, unos tienen ventajas sobre otros, la inversión en infraestructura es la principal diferencia.

Tabla 2. Modelos de virtualización utilizados en las empresas.

Modelo	Descripción	Recurso abstraído	Submodelo
1) Virtualización de Plataforma	Consiste en la abstracción del hardware subyacente de una plataforma, de manera que múltiples instancias de SO, puedan ejecutarse de manera independiente. Los recursos se comparten.	Plataforma Hardware completo.	Sistemas operativos invitados, emulación, virtualización completa, paravirtualización, virtualización a nivel del SO, virtualización a nivel del kernel.
2) Virtualización de recursos	Consiste en abstraer los recursos del hardware; conexión a la red, almacenamiento principal y secundario, dispositivos de E/S, entre otros.	Memoria RAM, enlaces de red, red, disco de almacenamiento, E/S.	Encapsulación, memoria virtual, virtualización del almacenamiento, virtualización de red, unión de interfaces de red (*Ethernet Bonding*), virtualización de E/S, virtualización de memoria.
3) Virtualización de aplicaciones	Las aplicaciones son ejecutadas sobre SO de manera que, aunque creen que interactúan con él y con el hardware de la manera habitual, la plataforma es virtualizada.	SO, Software.	Virtualización de aplicaciones limitada, virtualización de aplicaciones completa.
4) Virtualización de escritorio	Es la manipulación de forma remota del escritorio de un usuario, que se encuentra separado de la máquina física, almacenado en un servidor remoto en lugar de en el disco duro del computador local.	Sistema completo	

Para este propósito es importante la comparativa de las principales plataformas de virtualización, utilizando los indicadores de FURPS y McCall (Pressman, 2015), esta permite determinar cuál será la posible tecnología para utilizar como soporte. Estos indicadores definen una métrica para medir la calidad del software. Los indicadores de funcionalidad (capacidades, seguridad), usabilidad o facilidad de uso (estética, consistencia), confiabilidad (precisión, predicción), prestación o desempeño (velocidad, eficiencia) y soporte o documentación (mantenimiento), se utilizan para hacer una comparativa de las características que se buscan en una tecnología de virtualización.

En la tabla 3 se muestran los indicadores y la percepción al utilizar las tecnologías (porcentaje que se logró). También se realiza la comparativa con las métricas de McCall que permiten medir la operación o fiabilidad, revisión o flexibilidad y transición o portabilidad, se comparan algunas características importantes en virtualización y los costos por licencias.

Como se observa vSphere, Vmware (2019), Hyper-V, Microsoft (2019) y Xensever, Citrix (2019) son las tres tecnologías mejor evaluadas. Xen Project (2019) es otra alternativa totalmente open source pero carece de documentación extensa. La plataforma de Xenserver fue la elegida para implementar el soporte para almacenar los documentos digitales y el Blockchain, utilizando un servidor de almacenamiento de iSCSI en un NAS (Network Attached Storage) conectado a los sistemas de virtualización. Su principal ventaja es el soporte que provee Citrix y su licencia open source permite utilizarlo en forma gratuita.

© Academia Journals 2019

Tabla 3. Comparativa de los principales sistemas de virtualización.

Tecnología de Virtualización							
Métricas	Indicador		VMware vSphere	Citrix XenServer	Open source Xen/KVM	Microsoft Hyper-V	IBM, Power VM (2019)
FURPS	Funcionalidad		90%	80%	70%	80%	80%
	Usabilidad/Facilidad de uso		90%	95%	80%	90%	75%
	Confiabilidad		90%	90%	80%	90%	80%
	Prestación/Desempeño		80%	90%	80%	90%	80%
	Soporte/documentación		90%	80%	80%	90%	80%
McCall	Operación	Fiabilidad	90%	80%	90%	90%	80%
	Revisión	Flexibilidad	90%	80%	90%	80%	70%
	Transición	Portabilidad	90%	70%	70%	80%	60%
	PROMEDIO		**88.7 %**	**83.1%**	**80.0%**	**86.2 %**	**75.6 %**
Características adicionales			vSphere	Xenserver	Xen/KVM	Hyper-V	Power VM
Tipo de Hypervisor			Baremetal	Baremetal	Bare/Soft	Baremetal	Baremetal
Soporte de drag & drop			Sí	Si	No	Sí	No
Integración con otros productos (Sinergia)			Sí	No	No	Sí	No
Live migration (MV que cambia de servidor en ejecución)			Sí	Sí	No	Sí	Sí
Costo de licencia por core o CPU			USD $1,300.00 Por core	USD $800.00 Por core	Open source	USD $3,700 Por core	USD $850 Por core
Tipo de licencia			1 a 3 años	1 año	GNU	Servidor	1 año
Capturas/Snapshoot			Sí	Sí	Sí	Sí	Sí
Permite Windows y Linux como SO invitado			Sí	Sí	Sí	Sí	No (Solo AIX, IBMi Y Linux)
Aplicación para administración centralizada de MVs			Sí	Sí	No	Sí	Sí

Blockchain evolución

De acuerdo con Preukschat, Alex (2018) el nacimiento de Bitcoin en el año 2009, puso en evidencia la existencia de una nueva tecnología denominada Blockchain, que posibilitaba pasar del actual Internet de la información al Internet del valor (Bitcoin). En menos de 10 años de existencia, esta nueva tecnología disruptiva está creando a su alrededor todo un nuevo ecosistema que va mucho más allá de Bitcoin y su uso original como mera criptomoneda. En torno a la tecnología del Blockchain se está construyendo un nuevo modelo económico que se conoce como "criptoeconomía" o "tokenomics", caracterizado por la descentralización y porque puede transformar radicalmente muchas de las estructuras económicas y sociales actuales. Se están acuñando términos como Criptomonedas, Tokens, ICO´s (*Initial Coin Offering*), Filecoin, entre otros.

En este contexto el Filecoin es una tecnología que se define como una red descentralizada que convierte el almacenamiento en la nube en un mercado algorítmico. Un mercado de intercambio P2P (entre pares) que acepta solicitudes y ofertas para liquidar transacciones de almacenamiento de datos descentralizados que construyen un Blockchain. Básicamente es un servicio de almacenamiento en la nube, descentralizado. La construcción de herramientas y software de soporte se describen en Rodríguez–Nelson (2018), en donde se realiza una comparativa de las principales plataformas de construcción de Blockchain. De esta comparativa sobresalen Etherium (2019), Hyperledger Fabric (2019) y Corda R3 (2019) como las más utilizadas en la industria. Esta comparativa describe la magnitud y la competencia de las tecnologías de registros distribuidos. Si bien las tres muestran los beneficios y las aplicaciones de las tecnologías de registros distribuidos, estas difieren mucho en lo que respecta a la visión, así como a un posible campo de aplicación. Hyperledger y Ethereum vienen con diferentes casos de uso concretos, mientras

© Academia Journals 2019

que Corda R3 deriva la mayoría de sus aplicaciones en la industria de servicios financieros. En la tabla 4 se muestra resultados de la comparativa.

Tabla 4. Comparativa entre los principales sistemas de Blockchain (Rodríguez, 2018).

Comparativa	**Ethereum**	**Hyperledger Fabric**	**R3 Corda**
Casos de uso	Popular entre las aplicaciones generalizadas y se utiliza principalmente para operaciones P2P y B2C	La plataforma preferida para las operaciones B2B, utilizada principalmente en empresas	Se ejecuta en una plataforma personalizada de registros distribuidos para las necesidades de la industria financiera
Gobernanza	Realizado por desarrolladores (DAO)	Fundación Linux a cargo	Empresa R3 a cargo
Modo de operación	Blockchain pública: No se necesita permiso para acceder al contenido de la red	Blockchain privado: la red está limitada a personas con permiso	Blockchain privado: se necesita permiso para acceder al contenido de la red
Consensos	Se basa en la proof-of-Stake para la toma de decisiones	No todos los nodos de una red deben participar en el proceso de consenso	Sólo las partes involucradas en la transacción participan en la toma de decisiones
Contratos inteligentes	Lenguaje de programación sólido	Lenguaje de programación Golang	Lenguaje de programación Kotlin
Moneda	Ether como criptomoneda nativa	No tiene criptomoneda nativa	No tiene criptomoneda nativa

Como se observa Hyperledger y Ethereum son los principales entornos utilizados, por lo que una comparativa más específica es necesario. Hyperledger brinda a las empresas y personas la flexibilidad de hacer que las transacciones sean visibles sólo para un subgrupo seleccionado mediante el uso de llaves de cifrado. Ethereum, por otro lado, es un proyecto de Blockchain transparente por lo cual cada transacción o detalles de un proyecto se mantienen en el dominio público para que todos en la red puedan verlos. Las transacciones realizadas en Ethereum son visibles o públicas. Es importante resaltar que quiénes participan como desarrolladores en proyectos de Blockchain, que los mecanismos de consenso utilizados y los lenguajes de programación, deben estar soportados por un SDK. En la tabla 5 se sintetiza está comparativa.

Tabla 5. Comparación entre Hyperledger y Ethereum (Rodríguez, 2018).

Características	**Hyperledger**	**Ethereum**
Usos	Preferida para operaciones B2B, utilizada principalmente en empresas.	Popular con aplicaciones generalizadas y se usa principalmente para negocios y operaciones de consumo.
Confidencialidad	Transacciones confidenciales altamente privadas.	Transparente.
Método de participación de otros	Al ser una red privada es necesario tener permiso para acceder al contenido de la red.	Puede ser tanto privado como público, por lo tanto es una red sin permisos.
Mecanismo de consenso	Depende de un algoritmo de consenso conectable por falta de la minería.	El algoritmo Proof of Stake ya que el consenso se logra mediante la minería.
Lenguaje de programación	Depende del lenguaje de programación Golang de Google.	Contratos inteligentes impulsados por el lenguaje de programación Solidity.
Criptomoneda	No tiene una criptomoneda nativa incorporada.	Criptomoneda nativa Ether.

Hyperledger Fabric.

© Academia Journals 2019

HLF es un concentrador de código abierto, que busca apoyar el desarrollo de Blockchain en la industria. Es un esfuerzo colectivo iniciado para acelerar el desarrollo de las tecnologías de Blockchain de la industria y se coloca como un software para B2B. Es un esfuerzo coordinado a nivel mundial, busca el ahorro de dinero, mejoras en el IoT, en la red de producción y la innovación. Linux Foundation (2019) aloja el centro de código abierto del Blockchain. El principal objetivo de HLF es avanzar en la colaboración entre industrias, en lo que respecta a la creación de Blockchains y distribuidores de registros, con la finalidad de mejorar su rendimiento y confiabilidad. La función es integrar protocolos y estándares abiertos independientes para módulos de uso específico. HLF 1.0 es un establecimiento para la creación de aplicaciones de registro diseminadas. Al igual que otras tecnologías, viene con un registro y utiliza contratos inteligentes que le permiten actuar como un sistema en el que las personas pueden administrar las transacciones.

Descripción del Método

Propuesta de implementación con Xenserver

XenServer de Citrix (2019) se ha posicionado en el mercado como una excelente alternativa de implementar un entorno de virtualización, debido a que es Open Source y el costo de licencia suele ser de los más bajos por núcleo, lo cual atrae a las PyMES. Algunas de las razones de su uso extensivo son:

- Cuenta con un buen soporte por parte del fabricante.
- Se pueden instalar las herramientas (*XenTools*) para mejorar la experiencia de gestión de MV, tales como: mayor integración entre el host, soporte para drag & drop, controlador de tarjeta de red optimizado, entre otras.
- Facilidad de migrar MVs.
- Soporta la mayoría de los SO para virtualizar.
- Fácil instalación y rápido aprovisionamiento de MV.

Cabe destacar que, a pesar de las ventajas anteriores, se encontraron algunas deficiencias con el uso de la tecnología. En la tabla 6 se puede apreciar un modelo FODA sobre XenServer.

Tabla 6. FODA para XenServer de Citrix.

Fortalezas	**Oportunidades**
Freemium. Soporta una gran cantidad de sistemas operativos. Creación fácil y rápida de MV. Permite recuperarse de fallas en las MVs a través de *snapshots* y alta disponibilidad.	Mayor soporte de sistemas *host* y *guest*. Soporte de *Easy Install* en sistemas operativos. Mejora del soporte.
Debilidades	**Amenazas**
Al ser *open source* no tiene el soporte como otras tecnologías. Depende de la máquina *host* con características de hardware de servidor.	Gran competencia en el mercado de virtualización. Poco interés por PyMES en temas de virtualización. No tiene difusión.

De acuerdo con los requerimientos de instalación de HLF en una MV para implementar un peer de Blockchain (nodo), se estableció una metodología de instalación para cada uno de los nodos que participarán en el prototipo de B2B para el intercambio de documentos digitales, cada nodo se define como una sucursal u oficina que utilizará los documentos digitales para consulta o modificación de éstos. Es importante señalar que este esquema de intercambio entre nodos es popular con aplicaciones generalizadas y se usa principalmente para negocios y operaciones de consumo. Los pasos se muestran en la tabla 7.

La cadena de suministro (SCM) es una técnica que resulta apropiada para este proyecto, ya que se desea intercambiar documentos digitales debidamente firmados entre nodos P2P y con esto se establece el modelo de negocios que se requiere.

© Academia Journals 2019

Tabla 7. Pasos para instalar el esquema de virtualización con alta disponibilidad en MV.

Proyecto / pasos	Descripción
Plan de proyecto	Elaborar un plan que ayude a tener un mejor proceso de implementación y control del mismo, el cual contenga etapas como: • Planeación: descripción, objetivos, requerimientos, dimensionamiento, costos, plan de trabajo. • Ejecución: Instalación y configuración de componentes necesarios como: hipervisor de virtualización, MVs, SO, etc. • Pruebas: Monitoreo de servidores, software faltante, rendimiento de los sistemas, etc. Y corrección de errores. • Liberación del proyecto.
Instalación y configuración del entorno de Virtualización de XenServer	Instalar el hipervisor XenServer en los servidores correspondientes. Además de configurar de manera correcta al instalar para así poder administrar dichos servidores desde la consola de XenCenter.
Instalación y configuración de un NAS	Se requiere el uso de un espacio de almacenamiento externo para hacer uso del Pool de servidores y de la Alta Disponibilidad.
Configuración de Pool de Servidores	A través de la consola de administración XenCenter, se configura el Pool de servidores para tratarlos en conjunto.
Creación y configuración de MV	De acuerdo a especificaciones del SO, se crean las MVs con las características requeridas.
Instalación del SO para cada MV	Instalación del SO elegido en cada MV.
Configuración de HA (Alta Disponibilidad)	Implementar característica de Alta Disponibilidad en el Pool de servidores
Pruebas de HA (Alta Disponibilidad)	Probar el correcto funcionamiento de la Alta Disponibilidad que provee XenServer.
Instalación de MV	Instalación del SO Linux para soporte a HLF en un Peer

Implementación de HLF para Blockchain

Muchas de las soluciones actuales de gestión de la cadena de suministro (SCM) todavía implican enormes cantidades de trabajo manual. Los procedimientos requeridos para mantener un registro adecuado a menudo dependen de la entrada manual, lo que los hace lentos y propensos a errores. Los términos adicionales, tales como los acuerdos de precios, las condiciones que deben cumplirse estrictamente, así como las sanciones por negligencia de este último, dependen en gran medida de la integridad y la exactitud de la información registrada. El desafío es mejorar la administración con la tecnología de Blockchain.

Desde que una implementación de Blockchain comenzó a servir como la tecnología subyacente para la criptomoneda, el concepto general de Tecnologías de Libro Mayor Distribuido (DLT) ha ganado mucha atención de la industria moderna. Los diversos enfoques y el desarrollo de la integración continua de características adicionales, como los "contratos inteligentes", han abierto nuevas posibilidades. Uno de los principales argumentos que justifican la importancia de estos sistemas es la creciente necesidad de la transparencia, escalabilidad y seguridad en el intercambio de documentos digitales. Su uso incluye la digitalización y la automatización de procesos complejos basados en la confianza, como los que existen en la gestión de la cadena de suministro, la gestión de la propiedad o la certificación de la procedencia (PKI).

El proyecto Hyperledger ofrece herramientas que ayudan a los desarrolladores a construir un modelo de escenario basado en una SCM. HLF ofrece un Composer (creación) y un Explorer (visor) para la creación de Blockchain desde un lenguaje de programación amigable. HLF fue originalmente ofertado con la tecnología Docker (virtualización de servicios), que hace compleja su utilización, sin embargo se ha reportado la implementación de HLF en una MV de Linux Ubuntu para un nodo, en el Blog Computer Science (2018) de la Universidad de Stuttgart Alemania se puede consultar este desarrollo.

© Academia Journals 2019

HLF es una arquitectura P2P que ofrece un "consenso" compartido, al mantener los llamados libros de contabilidad: representaciones de estado e historia, que se sincronizan continuamente entre los participantes (nodos confiables). El estado se almacena en una llave de valor-clave y es una instantánea de los participantes y sus datos, como el saldo de la cuenta. El historial de transacciones es la parte del libro mayor, donde se almacenan todas las transacciones. En cualquier momento, este historial se puede utilizar para reproducir y verificar el estado actual. En la figura 1 se muestra el modelo de P2P para establecer un consenso entre los participantes al intercambiar documentos digitales a manera de una SCM.

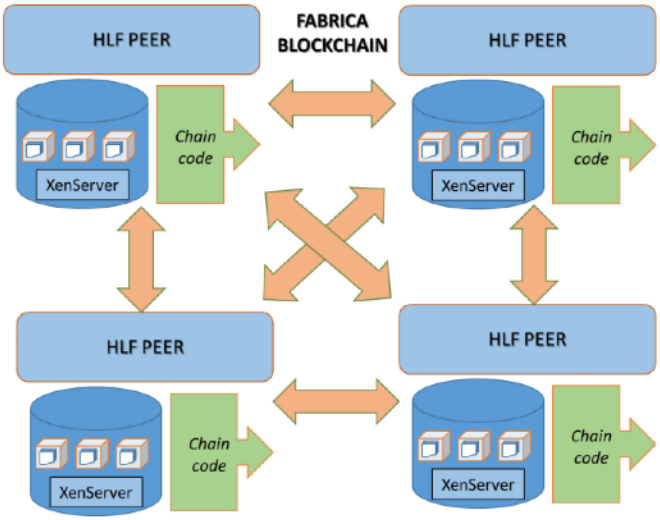


Figura 1. Intercambio de documentos entre Peers y establecimiento de un DLT para mantener la consistencia. (Blog Computer Science, 2018).

Ofrece un enfoque autorizado en donde los usuarios no son anónimos, deben estar autenticados y se les asigna una identidad única. Esto se logra mediante un proveedor de servicios de membresía (*MSP*), que proporciona una llave única de acceso, ésta puede ser adaptada al concepto de PKI. Cualquier proceso dentro de HLF, los miembros y las identidades se administran a través de transacciones en el libro mayor global. La autenticación es un objetivo necesario para la creación de canales confidenciales entre nodos.

En los DLT con un solo libro mayor global (BTC), cada transacción y estado es visible para cada miembro a través de un canal. Los miembros pueden unirse a canales, que son efectivamente subredes dentro de una red. Un canal mantiene su propio libro mayor y estado, que son invisibles fuera de éste. Se puede ofrecer a sus usuarios confidencialidad, un objetivo importante cuando las empresas competidoras coexisten en la misma red. Los nodos pares son las entidades versátiles puesto que pertenecen a miembros y pueden almacenar y ejecutar contratos inteligentes ("código de cadena") en su nombre, realizar operaciones de lectura/escritura en el libro mayor, y más.

Desde la perspectiva de un desarrollador, actúan como servidores y pueden interactuar con el uso de un SDK y herramientas compatibles con HLF Composer que facilita los siguientes aspectos: 1) modelado, codificación y prueba, 2) despliegue de redes empresariales creadas en HLF, 3) abstracción del MSP a través de tarjetas de identidad y 3) interfaz con los pares de la red a través de servicios REST para una WebApp. Finalmente, HLF Explorer ofrece la capacidad de visualizar los Blockchain construidos en la fábrica, permite seguir cada una de las transacciones que ocurrieron en el intercambio de documentos entre los nodos, ofrece también la posibilidad de conectarse a HLF utilizando servicios REST.

Comentarios Finales

La implementación de HLF para intercambio de documentos digitales conlleva varios retos desde la construcción de la arquitectura de nodos virtuales, la puesta en marcha de la fábrica de bloques, el intercambio de documentos digitales y finalmente el monitoreo y censado de las transacciones entre nodos pares. En la figura 2 se muestra el concepto de SCM que se desea construir para el intercambio de documentos digitales entre nodos confiables de la red.

© Academia Journals 2019

Resultados

Implementación del Modelo. Se basa en el modelo de negocio de SCM. Dado que ya existe conocimiento previo sobre su implementación en HFL. Durante la definición de modelo se definen algunos componentes:

- Participantes. Se determinaron los diferentes tipos de miembros de la red. Los roles son clave para el intercambio de documentos.
- Conceptos. Información contenida en los documentos.
- Categorización de elementos. Nombre y relación entre los elementos del modelo.
- Bienes. Valores y condiciones negociables como tipos de contrato, entre otros.
- Transacciones. Operaciones realizadas entre los participantes.
- Chaincode, lógica de transacción. Se utiliza para implementar toda la lógica de negocios que accede al libro mayor, ya sea por lectura o escritura, y normalmente se asocia con una transacción que se pasa como un argumento.
- Instalación y liberación del modelo.

En la figura 2 se muestra el modelo definido en HLF para el intercambio de documentos digitales entre los participantes del modelo. Es importante establecer criterios de asociación de los nodos y realizar un monitoreo continuo del comportamiento de los Blockchain.

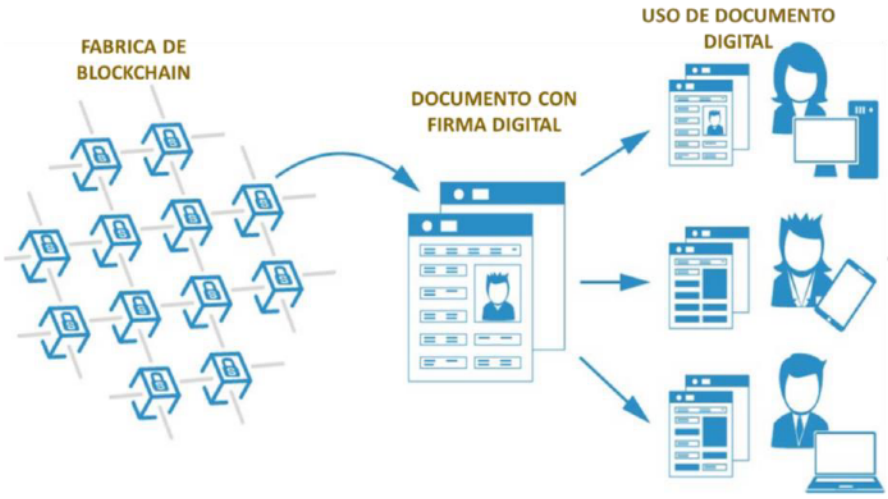


Figura 2. Documentos digitales y el uso de Blockchain como tecnología de transacciones.

En la figura 3 se muestra la propuesta completa de implementación del SCM, desde la generación de un documento digital PDF y su firma digital, después se envía a HLF Composer para la generación del Blockchain para su intercambio entre nodos. La implementación del Blockchain fue realizado con tres nodos, que en este caso fueron tres MVs sobre Xenserver/Docker (virtualización de aplicaciones). La arquitectura general de la solución es una propuesta de solución para una organización que requiere el intercambio de documentos digitales, en nuestro ejemplo se están manejando tres organizaciones educativas.

Cada organización cuenta con su aplicación cliente desarrollada en Java que es la encargada de brindar los archivos digitalizados en PDF, los metadatos y firmas digitales como entrada. Para que las organizaciones se puedan comunicar entre sí, se ocupa de al menos una entidad que gestione la comunicación con los demás nodos de la red Blockchain. Por lo tanto, el primer paso fue construir los nodos de la red Blockchain; para ello, fue necesario configurar el Composer con las especificaciones de la topología de la red. A través de esta herramienta podemos generar los certificados y claves para las organizaciones y los componentes dentro de ellas (usuarios y nodos). En este caso para las tres organizaciones se creó un solo nodo por organización y un solo cliente.

El segundo paso en la implementación, fue definir el nodo coordinador del Blockchain (se debe recordar que, aunque Blockchain es un mecanismo descentralizado, HLF entra en la categoría de blockchain privado con permisos,

© Academia Journals 2019

lo cual brinda aún más seguridad). Este nodo coordinador se define como el "orderer", que es el nodo principal encargado de la coordinación de los nodos.

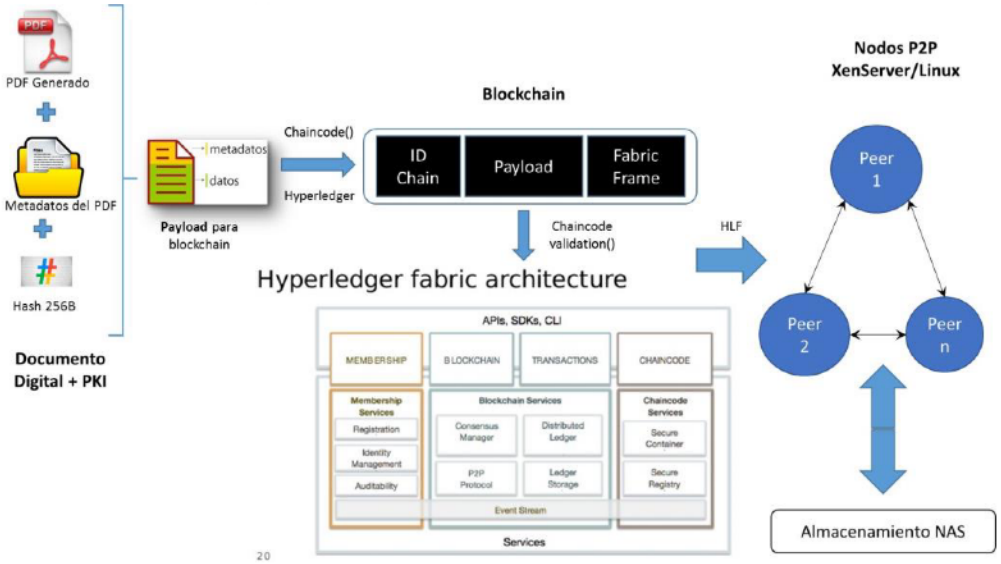


Figura 3. Modelo de blockchain con HLF para intercambio de expedientes digitales, P2P.

Conclusiones

A pesar de que XenServer es una plataforma open source (no llega a tener el mismo soporte como VMWare), por lo que es posible obtener ayuda de los usuarios activos en los foros de Citrix. Por lo tanto, si en una organización están dispuestos a sacrificar un poco del soporte "oficial", Citrix XenServer tiene un gran potencial como soporte. Además, que existiría un ahorro en cuanto a licenciamiento (dependiendo del requerimiento del proyecto). Es recomendable establecer un plan de implementación y debe seguir los pasos siguientes:

- Planeación del proyecto.
- Implementación del hipervisor (XenServer).
- Implementación del entorno de almacenamiento compartido (NAS).
- Creación de Pool de servidores con Alta Disponibilidad.
- Conocimiento de algunas tecnologías involucradas para Blockchain.
- Implementación de una distribución de Linux; Ubuntu Server.
- Configuración de HLF con su Composer.
- Seguimiento de las transacciones con HLF Explorer.

El uso de blockchain se combinó con la generación de documentos digitales y la distribución de los mismos. El proceso es sencillo, se genera el documento digital, se agregan metadatos de control, con parte de estos datos se genera un hash, que se firma con la llave privada del administrativo responsable de la gestión de documentos. Finalmente, este documento digital con la firma de la llave privada, se distribuye en el conjunto de nodos que forman la infraestructura del blockchain, guardando los datos de la distribución y la secuencia (o encadenamiento) de los mismos.

Las posibles mejoras en el futuro, para una implementación transparente, se podrían hacer de la siguiente manera:

- Pruebas de mayor impacto en un entorno real, donde se pueda lograr un mejor rendimiento, y de esta manera obtener una mejor retroalimentación y resolver errores de la mejor manera posible antes de implementar un proyecto en específico.
- Adaptar el entorno de virtualización a un diagrama de clúster que permita segmentar el direccionamiento; es decir, separar el tráfico de la red, por ejemplo, el tráfico de almacenamiento con el de los servidores a la red exterior, etc.
- Revisar los requisitos actualizados de los componentes a usar; XenServer, XenCenter, licenciamiento, distribución de Linux, Hyperledger Fabric, Docker, etc.

- Revisar aspectos de redundancia de los componentes del entorno de virtualización, por ejemplo, red y almacenamiento.

Agradecimientos

Al Tecnológico Nacional de México/I.T. Morelia por su apoyo al proyecto "Gestión de certificados de estudios con firma digital mediante PKI centralizado y utilizando blockchain" con clave no. 6758.18-P. Al Instituto de Investigaciones en Ecosistemas y Sustentabilidad de la UNAM, Campus Morelia, en especial a los maestros Atzimba López M. y Alberto Valencia G., por su apoyo técnico. A los estudiantes de residencias y servicio social por su ayuda en los análisis e instalación de las herramientas.

Referencias

Aguilar, Rosa (2011). Proceso Administrativo. Obtenido diciembre de 2018 de: http://www.ilustrados.com/tema/1871/Proceso-Administrativo.html

Blog Computer Science (2018). Supply Chain Management using Blockchain Technology – Hands-On Hyperledger. Obtenido marzo de 2019 de: https://blog.mi.hdm-stuttgart.de/index.php/2018/03/31/supply-chain-management-using-blockchain-technology-hands-on-hyperledger-part-1/

Corda R3 (2019). The Corda Platform, Blockchain for every business in every industry. Obtenido en marzo del 2019 de: https://www.r3.com/corda-platform/

Dolader Retamal, C., Bel Roig, J., & Muñoz Tapia, J. L. (2017). La Blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. Obtenido de Mincotur Web Site: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/DOLADER,%20BEL%20Y%20MU%C3%91OZ.pdf

Etherium Foundation (2019). About Etherium Foundation. Obtenido en marzo de 2019 de: https://ethereum.foundation/

Georges, Jonathan. (2017). La cadena de bloques (blockchain) Una tecnología disruptiva con el poder de revolucionar el sector financiero. Obtenido enero del 2019 de: https://www.equisoft.com/wp-content/uploads/2017/09/White-paper-Blockchain-ESP-1.pdf

Gestión Proyectos (2003). Metodología básica de gestión de proyectos. Obtenido en agosto de 2018 de: http://www.pcmanagement.es/editorial/Managem_powpoin/MetodologiadeGestiondeProyectos.pdf

Gómez de la Torre, M. C. (2015). Gestión de contenedores Docker-Kubernetes. Obtenido enero de 2018 de: http://informatica.gonzalonazareno.org/proyectos/2015-16/proyectoDK.pdf

Hyperledger Fabric (2019). Abot Hyperledger. Obtenido en marzo de 2019 de: https://www.hyperledger.org/about

Hyper-V server, Microsoft (2018). Microsoft Hyper-V Server 2016. Obtenido en agosto de 2018 de: https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/hyper-v-server-2016

IBM, powerVM (2019). ¿Qué puede hacer por su empresa? Obtenido en agosto de 2018 de: https://www.ibm.com/mx-es/marketplace/ibm-powervm

Isabel, M. (2008). Ventajas y desventajas de la virtualización. Obtenido en agosto de 2018 de: http://moodle2.unid.edu.mx/dts_cursos_mdl/lic/TIC/IT/AM/07/Ventajas.pdf

Linux Foundation (2019). Blockchain: Understanding Its Uses and Implications (LFS170). Obtenido en agosto de 2018 de: https://training.linuxfoundation.org/training/blockchain-understanding-its-uses-and-implications/

López, J., Maña, A., Montenegro, J. A., & Ortega, J. J. (2000). Aspectos de Implementación de una Infraestructura de Clave Pública Distribuida. Obtenido en enero de 2018 de: https://www.nics.uma.es/pub/papers/JavierLopez2000.pdf

Morteo, R. (2007). Ventajas y Consideraciones sobre la virtualización de infraestructura de Hardware. Obtenido enero de 2018 de: https://www.researchgate.net/profile/Rodrigo_Morteo/publication/277306305_Ventajas_y_Consideraciones_sobre_la_virtualizacion_de_infraestructura_de_Hardware/links/5566a00208aec22682ff1d50/Ventajas-y-Consideraciones-sobre-la-virtualizacion-de-infraestructura

Pressman, Roger (2015). Ingeniería del software. Un enfoque práctico. Séptima edición. Editorial McGraw-Hill. México. 2015

Preukschar Alex (2018). COMUNIDAD BLOCKCHAIN. El futuro de la criptoeconomía descentralizada y las ICO's. Ed. Iñigo Molero Manglano. Blockchain España. 2018.

Rodríguez, Nelson (2018). Hyperledger vs Corda R3 vs Ethereum: La guía definitiva. Obtenido en marzo de 2018 de: https://101blockchains.com/es/hyperledger-vs-corda-r3-vs-ethereum-la-guia/

RSA Data Security Company. (2001). UnderstandingPublic Key Infrastructure (PKI). Obtenido en julio de 2018 de: ftp://ftp.rsa.com/pub/pdfs/understanding_pki.pdf

Villar-Fernández, E. E. (2010). © Eugenio Villar y Julio Gómez http://www.adminso.esUniversidad de Almería Titulación de Ingeniero en Informática Virtualización de servidores de telefonía IP en GNU/Linux. Obtenido en agosto de 2018 de: http://www.adminso.es/images/d/dc/PFC_eugenio.pdf

vSphere,vmware (2019). vSphere: la plataforma eficaz y segura para su nube híbrida. Obtenido en enero de 2018 de: https://www.vmware.com/mx/products/vsphere.html

Xen, Project (2018). What is the Xen Project?. . Obtenido en setiembre de 2018 de: https://xenproject.org/about-us/

Xenserver, Citrix (2019). Optimized server virtualization for all your data center workloads. Obtenido en enero de 2019 de: https://www.citrix.com/products/citrix-hypervisor/

Apéndice

Hyperledger Fabric

HLF al igual que otras tecnologías de Blockchain, tiene un libro de contabilidad, utiliza contratos inteligentes y es un sistema mediante el cual los participantes administran sus transacciones. La diferencia radica en que HLF es privado y es a base de permisos. Los miembros de una red se inscriben a través de un proveedor confiable de servicios de membresía (MSP) en lugar de un sistema abierto sin permisos que permite que participen identidades desconocidas en la red. Los componentes de una red son: Ledgers (uno por canal), Smart Contracts (también conocido como chaincode), Nodos Peer, Ordering Services, Channels (canales), Fabric Certificate Authorities. De acuerdo a Suárez (2010), el flujo de transacciones y el cómo se llega al consenso para indicar que transacciones y en qué orden se graban en la Blockchain, es el siguiente:

- Propuesta de transacciones. Una transacción se inicia con una aplicación Cliente que envía una propuesta de transacción a una serie de nodos Endorsers.

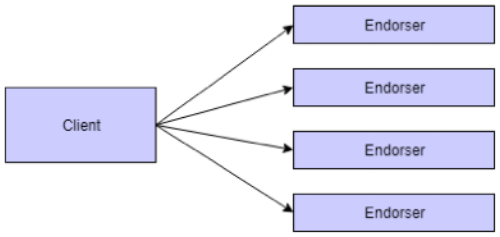


Figura 4. Propuesta de transacciones.

- Simulación y respaldo de transacciones. Cada uno de los Endorsers que ha recibido la propuesta de transacción simula la transacción con el estado actual del registro, pero sin hacer ningún cambio sobre éste, y genera un paquete denominado RW Set que contiene lista de Reads and Writes (lecturas y escrituras) generados por la transacción simulada. El RW Set es firmado por el Endorser y devuelto a la aplicación cliente.

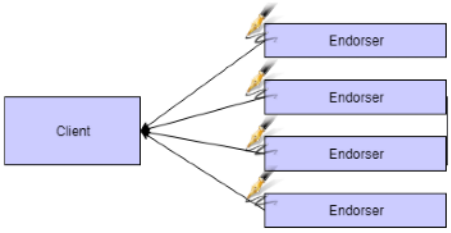
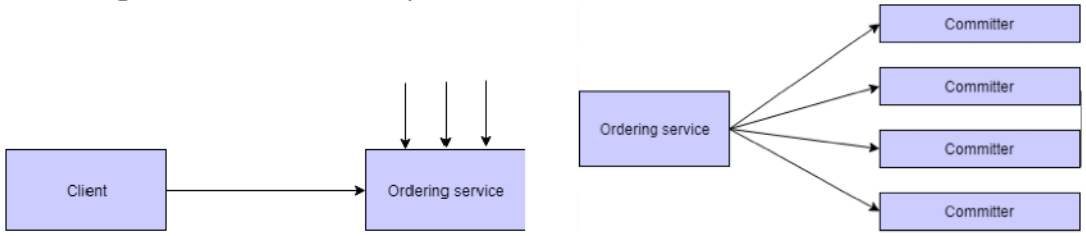


Figura 5. Simulación de transacciones.

- Ordenar transacciones. La aplicación cliente envía entonces la transacción firmada por el Endorser el RW Set al Ordering Service el cual es común para toda la red.



a) b)

© Academia Journals 2019

Figura 6. a) Envío de transacción y b) ordenamiento.

- Validación y almacenamiento. Los Committers comprueban entonces que los RW Sets recibidos aún son válidos generan la misma lista de R/W. Si una transacción resulta inválida durante este proceso, será incluida en el bloque, pero marcada como inválida y no modifica el estado del registro. Por último, los Committers informan a los Clientes si la transacción ha sido ejecutada con éxito o no.

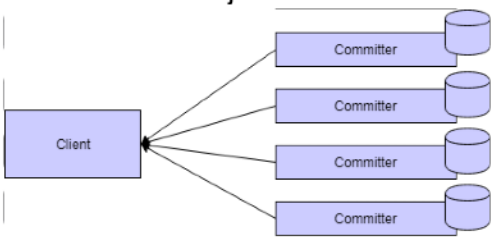


Figura 7. Validación de transacciones.

- Canales. Los canales es uno de los mecanismos de privacidad en Hyperledger Fabric y permite tener diferentes blockchains en la misma red de forma que sólo los participantes de un canal pueden conocer los detalles de las transacciones que ocurren en dicho canal. Por ejemplo, una red con tres participantes P1, P2 y P3. Dentro de dicha red podríamos tener cuatro canales: 1) Un canal formado por los tres participantes, 2) Un canal formado por P1 y P2, 3) Un canal formado por P2 y P3 y 4) Un canal formado por P1 y P3.

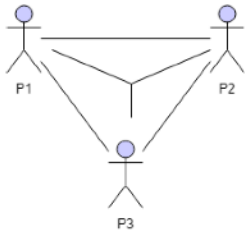


Figura 8. Canales.

- Bases de datos de estado. HLF guarda el estado actual en una base de datos que puede ser recreada en cualquier momento a partir de la cadena de transacciones almacenadas en la cadena de bloques. Es una forma eficiente de acceder al estado del registro (world state) a través de una tabla de clave-valor. Actualmente Hyperledger usa por defecto LevelDB como base de datos que puede ser reemplazado por CouchDB. Mientras LevelDB almacena una lista de clave-valor, CouchDB almacena objetos JSON y presenta una interfaz mucho más potente.

ISSN 1946-5351
Vol. 11, No. 2, 2019