ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica
ISSN: 2007-5448
recibe@cucei.udg.mx
Universidad de Guadalajara
México

Solis Osorio, Carlos O.; Pérez Cortés, Elizabeth; Cervantes Maceda, Humberto
Hacia una metodologia para el diseño de contratos inteligentes
ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, vol. 8, núm. 1, 2019, Mayo-Octubre, pp. 1-15
Universidad de Guadalajara
Guadalajara, México

COMPUTACIÓN E INFORMÁTICA
Recibido *19/05/2019* ***ReCIBE, Año 8 No. 1, Octubre 2019***
Aceptado *20/07/2019*

HACIA UNA METODOLOGÍA PARA EL DISEÑO DE CONTRATOS INTELIGENTES

TOWARDS A METHODOLOGY FOR THE DESIGN OF SMART CONTRACTS

Carlos O. Solis-Osorio[1]
carlosomarso.003@gmail.com

Elizabeth Pérez-Cortés[1]
pece@xanum.uam.mx

Humberto Cervantes-Maceda [1]
hcm@xanum.uam.mx

[1]Universidad Autónoma Metropolitana campus Iztapalapa
Av. San Rafael Atlixco 186, Iztapalapa, CDMX., México

RESUMEN

Los contratos inteligentes representan un aspecto importante de las cadenas de bloques. Su objetivo es complementar a los contratos tradicionales que implican modificaciones sobre los datos almacenados en la cadena. En este artículo se define una metodología para el diseño de contratos inteligentes y se ilustra su uso con un caso de estudio.

PALABRAS CLAVE

Cadena de bloques, Contratos inteligentes, Diseño, Metodología.

ABSTRACT

Smart contracts represent an important aspect of blockchains. Their main objective is to complement the traditional contracts that involve modifications to the data stored in the chain. In this article we present a methodology for the design of smart contracts and we also illustrate its application with a case study.

KEYWORDS

Blockchain, Smart Contracts, Design, Methodology.

1. INTRODUCCIÓN

Las cadenas de bloques *blockchains* se presentaron en el 2009 como la tecnología que da soporte a *Bitcoin* (S. Nakamoto, 2009), sin embargo, posteriormente se descubrió que esta tecnología puede ser de gran utilidad en múltiples aplicaciones que van mucho más allá de las criptomonedas. Los tipos de aplicaciones que pueden beneficiarse al utilizar una cadena de bloques como almacenamiento se han diversificado considerablemente. Desde su lanzamiento en 2009 el número de proyectos relacionados con cadenas de bloques en la plataforma de GitHub creció en promedio 8600 proyectos por año y hasta 2017 existían aproximadamente 36000 proyectos en la plataforma (Jesus Leal Trujillo, Steve Fromhart y Val Srinivas, 2017).

Blockchain es una tecnología que permite realizar aplicaciones que involucran a varias partes (generalmente distintas organizaciones) que tienen la necesidad de compartir datos y realizar transacciones sin necesidad de la existencia de intermediarios y teniendo diversas garantías sobre los datos, tales como la inmutabilidad y el no repudio.

Un contrato inteligente (Nick Szabo, 1966) es un programa informático que permite plasmar aspectos contractuales relativos a las transacciones entre las partes mediante código. Si bien no todas las plataformas tecnológicas de cadenas de bloques soportan contratos inteligentes, existen algunas que ya cuentan con dicha característica tales como: Hyperledger Fabric, IBM Blockchain y Ethereum. Sobre estas plataformas, los contratos inteligentes están almacenados dentro de la cadena de bloques y no son controlados por ninguna de las partes implicadas. Una vez firmados y almacenados en la cadena de bloques, ya no pueden ser modificados de manera sencilla.

El código del contrato inteligente se ejecuta cuando alguna de las partes desea interactuar con la cadena y cumple con una serie de condiciones.

Una parte importante en el diseño de un sistema basado en cadenas de bloques es la identificación y diseño de los contratos inteligentes, ya que además de gestionar cierta parte de la lógica de negocio, serán cruciales en la toma de decisiones para la arquitectura general del sistema. De acuerdo a la investigación que realizamos, en la literatura especializada no se ha definido ninguna metodología que guíe el diseño de contratos inteligentes. En este documento se presenta una propuesta de metodología para el diseño de contratos inteligentes y su aplicación en un caso de estudio.

El resto de este documento está organizado de la siguiente forma: en la sección 2 se presentan los conceptos básicos que se necesitan para comprender este artículo, en la sección 3 se presenta nuestra propuesta de metodología, en la sección 4 se describe el caso de estudio, en la sección 5 se aplica la metodología propuesta al caso de estudio y finalmente, en la sección 6 se listan los resultados y se enuncian las conclusiones.

2. MARCO TEÓRICO

Las cadenas de bloques son un mecanismo de almacenamiento de datos distribuido que gestiona transacciones. Las transacciones representan modificaciones a los datos guardados en la cadena y son almacenadas en bloques. Cada bloque contiene un conjunto de transacciones y una firma que lo identifica como único, dicha firma es generada mediante una función hash aplicada a los datos que contiene el bloque y a la firma del bloque anterior. En consecuencia si la información de un bloque es modificada también sería afectada su firma y todos los bloques posteriores serán invalidados. Este mecanismo garantiza que la información contenida en la cadena no pueda ser modificada (Decker C. y Wattenhofer R, 2013). Además, cada que se desea agregar un bloque nuevo, se convoca a un proceso de consenso para verificar que el bloque que se desea añadir sea válido (Zheng Z., Xie S., Dai H., Chen X., y Wang H., 2017). Esta característica de las cadenas de bloques hace que las organizaciones involucradas en el proyecto intervengan en la validación de los bloques que se están añadiendo a la cadena y por lo tanto, una vez que se verifica un bloque, significa que la información que ahí se almacena es reconocida como correcta por todos los que la han validado y ninguno podrá negarla en el futuro, esta característica de la información se conoce como no repudio.

Como cualquier otra tecnología las cadenas de bloques presentan bondades y limitantes haciendo que su uso sea conveniente sólo en ciertos escenarios. A continuación, mencionamos algunas ventajas y desventajas de las cadenas de bloques (Gatteschi V., Lamberti F., Demartini C., Pranteda C., y Santamaría V., 2018).

Ventajas:

1. Almacenamiento de datos distribuido. Reduce la pérdida de datos en caso de eventos inesperados, ya que los datos se encuentran replicados en diferentes nodos que generalmente son parte de las organizaciones involucradas.

2. Descentralización. No requiere de intermediarios de confianza, permitiendo que las transacciones se realicen directamente entre dos o más organizaciones involucradas.

3. Transparencia. Los datos almacenados en la cadena son visibles para cualquier parte. Todas las organizaciones que tienen acceso a la cadena de bloques pueden leer el estado de una transacción o incluso la historia de los datos.

4. Inmutabilidad. La información almacenada en la cadena de bloques es inmutable, los datos no pueden modificarse ni eliminarse.

5. Automatización. Las cadenas de bloques con soporte para contratos inteligentes, permiten a través de estos, la automatización de actividades, garantizando la correcta ejecución de sus cláusulas sin beneficiar indebidamente a ninguna de las partes involucradas.

Desventajas:

1. Alto consumo energético. Las cadenas de bloques se caracterizan por un alto consumo energético ya que para el proceso de consenso usualmente se hace uso de la prueba de trabajo \textit{(proof of work)}, dicha prueba requiere de hardware costoso que consume una cantidad considerable de energía. Para solucionar este problema actualmente existen alternativas a la prueba de trabajo (Zheng Z., Xie S., Dai H., Chen X., y Wang H., 2017).

2. Almacenamiento. La replicación de los datos requiere mayor espacio de almacenamiento, los nodos encargados de validar las transacciones deben alojar una copia de la cadena de bloques. Por ejemplo, hasta enero del 2019 la cadena de bloques de *Bitcoin* tenía un peso aproximado de 244 GB (Cryptocurrency statistics, 2019) y aumentará conforme se añadan bloques nuevos.

3. Rendimiento. Las cadenas de bloques no toleran una tasa alta de transacciones. En la red de *Bitcoin* la adición de un bloque nuevo en la red tarda de 10 a 60 minutos (Cryptocurrency statistics, 2019).

4. Confidencialidad. La transparencia de los datos podría ser perjudicial si la información almacenada requiere de privacidad, aunque se puede optar por la utilización de algún algoritmo de cifrado que ayude a mantener la privacidad de los datos.

Si bien existen desventajas de usar cadenas de bloques, estas no siempre se presentan. Por ejemplo, la confidencialidad no siempre es necesaria y por lo tanto sólo representaría una desventaja cuando esta sea requerida. Decidir si un proyecto de software se verá beneficiado con la inclusión de una cadena de bloques es una tarea importante. Una lista de criterios para tomar dicha decisión se presenta en (Carlos Solis-Osorio, Elizabeth Pérez-Cortés y Humberto Cervantes-Maceda, 2018).

Con respecto al uso de contratos inteligentes en un proyecto de software, si se le compara con el uso de contratos tradicionales, trae consigo los siguientes beneficios:

1. Un contrato inteligente no está sujeto a interpretaciones pues está escrito en un lenguaje de programación. En contraste, un contrato tradicional está escrito en lenguaje natural.

2. Un contrato inteligente no requiere de un intermediario que le añada validez, reduciendo los costos y el tiempo que toma la ejecución del mismo.

3. Debido a que el contrato es alojado en la cadena de bloques no puede modificarse, haciéndolo más seguro en comparación con un contrato tradicional.

Para ilustrar mejor el concepto consideremos un ejemplo que involucra a tres organizaciones distintas: un proveedor de vegetales orgánicos y dos restauranteros. Dicho proveedor se encarga de abastecer de vegetales a cada uno de los restaurantes.
Cada restaurante tiene su propio sistema que se encarga de gestionar el almacén, sin embargo, se desea incluir un sistema de cadena de bloques que garantice la rastreabilidad de los vegetales suministrados, esto sin eliminar los sistemas con los que ya cuenta cada organización. Este es uno de los casos típicos que ameritan el uso de cadenas de bloques pues se desea registrar cada transacción de la que han sido objeto los vegetales, desde su origen hasta la entrega en el restaurante para su consumo. Este tipo de escenarios ya han sido resueltos mediante el soporte de las cadenas de bloques, como el rastreo de origen de oro (Royal Mint, 2019).

Dos de las reglas de negocio asociadas al sistema descrito en el ejemplo anterior se muestran a continuación:

1. Cuando un restaurante adquiere vegetales del proveedor, estos deben haber sido cosechados en los 10 días previos a la adquisición.

2. El sistema de almacén de los restauranteros es capaz de notificar al encargado cuando existan menos de 20 piezas de cualquier vegetal.

Dichas reglas de negocio pueden pertenecer a uno o más procesos de negocio. Recordemos que un proceso de negocio es un conjunto de actividades y tareas que una vez completadas, ofrecen un servicio o producto al cliente.

Los contratos inteligentes ayudan a modelar algunas de las reglas de negocio involucradas en nuestro sistema, principalmente aquellas que hacen uso de los datos que serán almacenados en la cadena. Además al modelar las reglas de negocio mediante contratos inteligentes aprovechamos las bondades que estos ofrecen para implementarlas de manera clara y concisa, proporcionando confianza a los diferentes involucrados, ya que dichas reglas no son ambiguas y garantizan la correcta ejecución de la lógica de negocio.

En el caso de nuestro ejemplo, un contrato inteligente es capaz de implementar todas las reglas de negocio mencionadas anteriormente, sin embargo, esto no siempre es la mejor opción. Si analizamos la segunda regla de negocio, los datos asociados a la existencia de vegetales no se encuentran almacenados en la cadena de bloques, estos son gestionados por el sistema que ya existía en los restaurantes y es de interés únicamente para un involucrado del sistema de tal forma que dicha regla de negocio será gestionada por el sistema ya existente. Por otro lado, la primera regla de negocio es pertinente dentro del contrato ya que debe ser validada en el momento en que se realizan transacciones entre el proveedor y el restaurante.

Las cadenas de bloques y los contratos inteligentes tienen muchas configuraciones distintas y, dependiendo el contexto, se debe seleccionar la más adecuada.

En particular, toda la lógica de negocio relacionada con los datos almacenados en la cadena deberá ser implementada mediante contratos inteligentes. Definir qué datos deben ser almacenados en la cadena, y en consecuencia qué parte de la lógica de negocio debe ser implementada en contratos inteligentes, es uno de los principales retos en el desarrollo de sistemas basados en cadenas de bloques.

Hasta donde sabemos, actualmente no se cuenta con una metodología que sirva de guía en el diseño de los contratos inteligentes. En este documento se presenta una propuesta de metodología para el diseño de contratos inteligentes y su aplicación en un caso de estudio.

3. METODOLOGÍA PARA DISEÑAR CONTRATOS INTELIGENTES

A continuación, presentaremos nuestra propuesta de metodología para el diseño de contratos inteligentes, tomando como base la identificación de las organizaciones y los procesos de negocio.

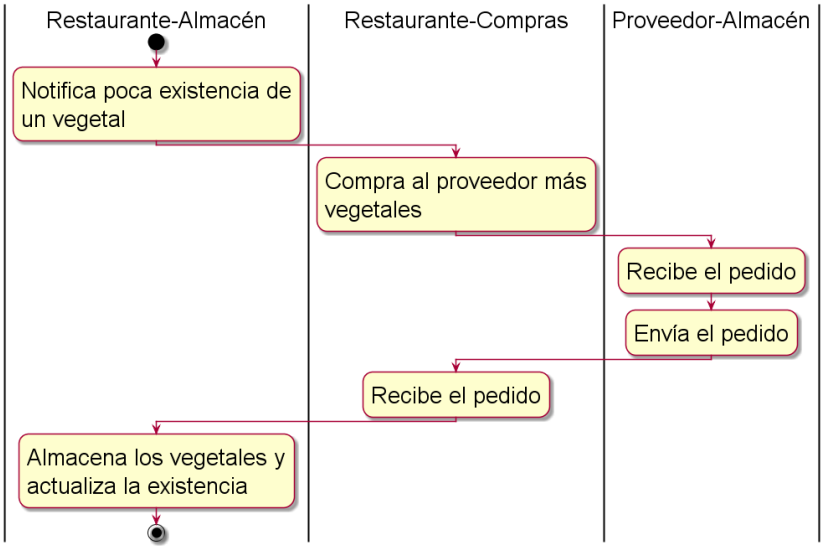
3.1 Identificación de las organizaciones involucradas y sus procesos de negocio

El primer paso es determinar cuáles son las organizaciones involucradas en el proyecto, para esto se puede consultar si existe una matriz de roles y responsabilidades y buscar en ella las diferentes organizaciones involucradas en el proyecto, de lo contrario, se puede analizar el caso de estudio en busca de las organizaciones involucradas.

Una vez identificadas las organizaciones es necesario definir los procesos de negocio del sistema, esto con la finalidad de tener claras las actividades que se realizarán dentro del sistema. Para identificar los diferentes procesos de negocio, se puede consultar si ya existe documentación de los procesos que se desean automatizar en las organizaciones involucradas, de lo contrario, se pueden realizar entrevistas con los involucrados en el proyecto con la finalidad de identificar los procesos de negocio. En el contexto del ejemplo mencionado anteriormente, la compra de vegetales sería un proceso de negocio.

Una vez que se tienen identificados los procesos de negocio, se tienen que documentar, por ejemplo mediante un diagrama de actividades (Figura 1). Los actores involucrados en el diagrama se muestran con la estructura Organización-Actor, indicando el actor y la organización a la que pertenece.

Fig. 1: Proceso de compra de vegetales



3.2 Identificar las entidades y los atributos requeridos para soportar los procesos de negocio

Una vez que se identificaron los diferentes procesos de negocio, es necesario determinar las entidades que forman parte del dominio del problema en cada uno de los procesos. Esto permitirá determinar posteriormente los atributos que darán soporte a la lógica de negocio del sistema.

Para determinar las diferentes entidades, es necesario utilizar el diagrama de actividades realizado en el paso previo e identificar los sustantivos que estén relacionados con las actividades del diagrama, por ejemplo, de la actividad *notifica poca existencia de un vegetal* obtenemos la entidad *VEGETALES*, posteriormente es necesario identificar los atributos asociados a cada entidad, por ejemplo, los atributos de un *vegetal* son: *nombre, precio, origen, recolector*, etc. Al final obtendremos una lista de entidades con sus respectivos atributos. Todas las entidades y atributos identificados formarán parte del conjunto de datos que dará soporte al proceso de negocio que se esté analizando.

3.3 Identificar las entidades y los atributos requeridos para soportar los procesos de negocio

Si bien se puede almacenar toda la información relacionada con el sistema dentro de una cadena de bloques, esto no siempre es adecuado, debido a que la capacidad de almacenamiento dentro de un bloque es relativamente baja. Es conveniente mantener en la cadena de bloques solo la información que requiera de las características que esta ofrece.

Para ayudar a decidir qué datos almacenar en la cadena, es necesario plantearse las siguientes preguntas para cada uno de los atributos pertenecientes a las entidades obtenidas anteriormente: ¿el atributo es de interés para más de una organización involucrada en el sistema?, de ser así, ¿el atributo requiere de la propiedad de no repudio?, ¿es de interés para las organizaciones involucradas obtener información acerca de las transacciones que han modificado el atributo? Si se responde que sí a las preguntas anteriores es muy probable que el dato que está siendo evaluado deba ser almacenado en la cadena de bloques. Todos los atributos para los cuales se obtenga una respuesta negativa podrán ser gestionados por una base de datos tradicional.

3.4 Identificar las diferentes operaciones que harán uso de la información almacenada en la cadena de bloques

Una vez que se identificaron los diferentes atributos que serán almacenados en la cadena de bloques, es necesario definir las diferentes operaciones o acciones que se requieren realizar sobre los atributos para cumplir con el objetivo del proceso de negocio. Para realizar dicha tarea es necesario retomar el diagrama de actividades descrito anteriormente y para cada una de las actividades contenidas en el diagrama, plantearse la siguiente pregunta: ¿esta actividad modifica los atributos almacenados en la cadena? Si se responde positivamente a dicha pregunta entonces la actividad deberá ser implementada mediante un contrato inteligente. Por ejemplo, en el diagrama de actividades de la figura 1, una de las actividades que modifica el estado de los atributos en la cadena es la compra de vegetales. Este procedimiento debe repetirse para cada una de las actividades de todos los procesos de negocio identificados previamente.

3.5 Identificar los contratos inteligentes

Las operaciones identificadas en la sección anterior deben ser agrupadas de acuerdo a la entidad de negocio de la que hacen uso y cada conjunto de operaciones resultante junto con su entidad de negocio serán modeladas por un contrato inteligente. Por ejemplo, si retomamos el contexto de los restauranteros, la operación compra de vegetales hace uso de la entidad *VEGETALES*, por lo tanto dicha operación formará parte del contrato inteligente *ManejoVegetales*. Para el nombrado de los contratos inteligentes se antepone la palabra *Manejo* al nombre de la entidad para indicar que ese contrato gestiona los atributos relacionados con dicha entidad.

4. CASO DE ESTUDIO

Con la intención de mostrar de manera práctica cómo utilizar la metodología descrita anteriormente, esta se aplicará a un sistema de manejo de inventario de bienes de inversión. Para determinar si el proyecto se vería beneficiado con el uso de una cadena de bloques, el caso de estudio fue sometido al análisis propuesto en (Carlos O. Solis-Osorio, Elizabeth Pérez-Cortés y Humberto Cervantes-Maceda., 2018), obteniendo un resultado aprobatorio.

Consideremos una institución académica donde la adquisición de algún bien de inversión (computadoras, escritorios, sillas, etc.) involucra la realización de una petición por escrito al Departamento de Administración, indicando información personal del solicitante, el bien solicitado y el costo del mismo; posteriormente la solicitud es enviada al Departamento de Patrimonio en donde se revisa y se autoriza la solicitud para después ser enviada a la Coordinación de Servicios Administrativos en donde es revisada nuevamente y enviada al Departamento de Proveeduría, es aquí donde se realiza la compra del bien. Una vez que el bien es recibido se notifica a la aseguradora; en cuanto el bien se encuentra asegurado se notifica al solicitante para que acuda a retirarlo. Una vez que el bien es retirado por la persona que lo solicitó, queda bajo su resguardo y a partir de este momento es responsable del bien material así como de su buen uso. Un proceso similar se lleva a cabo para dar de baja un bien por pérdida o robo, descompostura u obsolescencia. En el caso particular de la pérdida o robo de un bien, adicionalmente se inicia un proceso legal para hacer válido el seguro del bien.

Existe un caso especial en donde un empleado tiene el resguardo de cierto material y decide transferirlo a otro empleado. Este proceso se considera un traspaso de bienes y es realizado de forma similar al proceso de alta.

Adicionalmente se desea proporcionar a la Secretaría de Hacienda un medio confiable para que ellos puedan realizar auditorías sobre los recursos otorgados a la institución.

5. APLICACIÓN DE LA METODOLOGÍA PROPUESTA

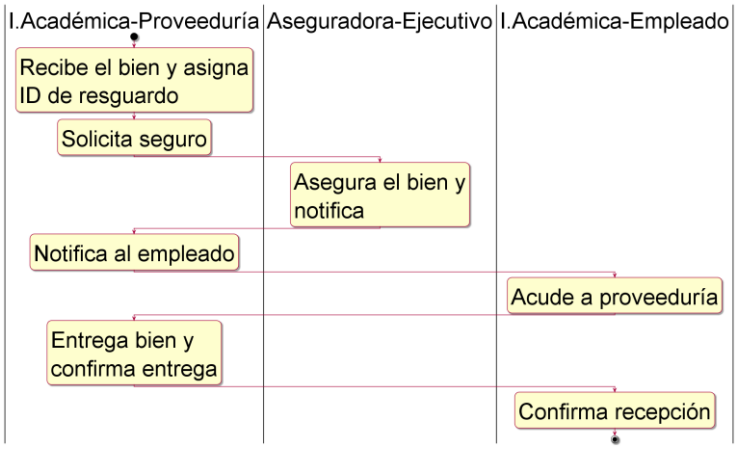
A. Identificación de las organizaciones involucradas y sus procesos de negocio.

Analizando el caso de estudio se puede identificar las organizaciones involucradas en el proyecto: la institución académica, la Secretaría de Hacienda y la aseguradora. Para la identificación de los procesos de negocio se llevaron a cabo entrevistas con el personal involucrado en el proyecto, a continuación se listan los procesos identificados:

- Alta, baja y traspaso de un bien.
- Aseguramiento de un bien.
- Auditoría de recursos.

Para ejemplificar el uso de la metodología se hará uso del proceso de negocio alta de un bien (Figura 2).

Fig. 2: Proceso de alta de un bien



B. Identificar las entidades y los atributos requeridos para soportar los procesos de negocio.

Analizaremos el proceso de negocio de *alta de un bien*. En este caso los atributos identificados pertenecen a tres entidades:

- Datos asociados a un *bien*: *identificador, tipo, costo, fecha de adquisición, responsable, lugar y descripción.*
- Datos asociados a un *seguro*: *prima, porcentaje de cobertura, vigencia y monto asegurado.*
- Datos asociados a un *trabajador*: identificador, correo electrónico y nombre.

C. Determinar qué información debe ser almacenada en la cadena de bloques.

Para decidir qué atributos almacenar en la cadena, es necesario plantear para cada uno de los atributos identificados, las preguntas definidas en el paso tres de la metodología, si se responde positivamente a las preguntas, entonces el atributo analizado deberá ser alojado en la cadena de bloques. Por ejemplo, para el atributo *costo* de la entidad *bien* aplicamos las preguntas:

- ¿El atributo es de interés para más de un involucrado en el sistema? podemos responder que sí a esta pregunta ya que el *costo* es un dato que es de interés para la institución educativa. De igual forma la aseguradora requiere de este dato para realizar los cálculos requeridos en el seguro como el *monto* asegurado, la *prima*, el *porcentaje de cobertura*, etc. Además, el dato también es de interés para la Secretaría de Hacienda, ya que realizarán auditorías acerca de los recursos invertidos en bienes de inventario.

- ¿El atributo requiere de la propiedad de no repudio? sí, ya que deseamos que todos los interesados en este dato lo reconozcan como válido.

- ¿Es de interés para los involucrados obtener información acerca de las transacciones que han modificado el atributo? sí, ya que el costo de un bien no cambia con el tiempo e identificar dicho cambio podría implicar un comportamiento malicioso.

Una vez que aplicamos dichas preguntas a todos los atributos identificados, obtenemos las entidades que serán alojadas en la cadena de bloques:

- Bien: *identificador, costo, fecha de adquisición y el responsable.*
- Seguro: *prima, porcentaje de cobertura, identificador del bien asegurado, vigencia y el monto asegurado.*
- Empleado: *identificador, nombre y jefatura.*

D. Identificar las diferentes operaciones que harán uso de la información almacenada en la cadena de bloques.

Para identificar las operaciones nos basamos en las actividades presentadas en el proceso de negocio de la figura 2 y para cada una de las actividades nos planteamos la siguiente pregunta: ¿esta actividad modifica los atributos almacenados en la cadena?

Las actividades del proceso de negocio alta de un bien que modifican los atributos almacenados en la cadena son las siguientes: *asignación de una etiqueta de resguardo, registro de un bien, aseguramiento de un bien y recepción de un bien solicitado por un empleado*.

E. Identificar los contratos inteligentes.

De acuerdo con la lista de actividades obtenida en el punto anterior, identificamos cuáles de esas actividades hacen uso de la misma entidad de datos. Por ejemplo, la actividad *aseguramiento de un bien* modifica la entidad de datos *SEGURO*, además en la vida cotidiana este tipo de procesos se realizan mediante contratos tradicionales, por lo tanto, es conveniente crear un contrato inteligente que se encargue de la gestión de los seguros. En cambio, las operaciones: *asignación de una etiqueta de resguardo, registro de un bien y recepción de un bien solicitado por un empleado*, modifican de la entidad *BIEN*, por lo tanto deberán ser gestionadas por otro contrato inteligente, en este caso el contrato *ManejoBienes*.

Una vez realizado el análisis anterior para todas las actividades identificadas, obtendremos una versión preliminar de los contratos inteligentes, en la figura 3 mostramos los contratos identificados. Es importante mencionar que dentro de cada contrato inteligente se encuentra una estructura de datos que coincide con las entidades identificadas en el paso tres de la metodología, dicha entidad define el modelo de datos que utilizará cada contrato inteligente. De igual forma las operaciones identificadas en el inciso *D* de la metodología se traducen en los diferentes métodos que es capaz de ejecutar el contrato, por ejemplo en el contrato *ManejoBienes* el método *insertarBien*, proviene de las operaciones: *asignación de una etiqueta de resguardo* y *registro de un bien.*

Para documentar el contrato inteligente se utilizó un diagrama de clases perteneciente a UML, añadiendo un ícono en la esquina superior izquierda como se sugiere en (Rocha H., y Ducasse S., 2018). Dicho ícono nos indica que se refiere a un contrato inteligente.

Fig. 3: Contratos inteligentes: *ManejoBienes*, *ManejoAuditorías*, *ManejoSeguros* y *ManejoEmpleados*.

6. CONCLUSIÓN

El diseño de un sistema basado en cadenas de bloques es una actividad importante que se divide en diferentes fases, una de las fases más importantes es el diseño de los contratos inteligentes. En este artículo presentamos una propuesta de metodología para el diseño de contratos inteligentes tomando como base la identificación de las organizaciones participantes y los procesos de negocio. La ejecución de la metodología propuesta cumplió con su objetivo y el diseño de los contratos obtenido será la base para la implementación de la lógica de negocio en contratos inteligentes. Además, dichos contratos inteligentes serán de suma importancia al momento de tomar decisiones sobre la arquitectura del sistema, ya que considerando los datos se definirá si se requiere usar un sistema adicional de almacenamiento de datos o no.

Como se mencionó anteriormente, al revisar la literatura científica no encontramos ninguna metodología para guiar el diseño de los contratos inteligentes. Lo más cercano es el proceso de diseño para aplicaciones basadas en cadenas de bloques que se presenta en (Xu X., Weber I., y Staples M., 2019). Dicho proceso coincide con nuestra propuesta en la necesidad de separar la lógica de negocio que será gestionada por la cadena de bloques y la que será gestionada por otras tecnologías, sin embargo, esa propuesta no aborda propiamente el diseño de los contratos inteligentes.

Por otro lado, es relevante la correcta documentación de cualquier sistema de software, ya que es una forma de modelar y transmitir los detalles del sistema. A lo largo del artículo utilizamos diagramas de clases pertenecientes a UML para poder modelar los contratos inteligentes, e hicimos uso de un ícono de una cadena para diferenciarlos, sin embargo, estos diagramas no fueron creados para modelar este tipo de artefactos. Además, por limitaciones de tiempo no se realizó una evaluación completa de la metodología. En consecuencia, como trabajo futuro, se estudiará la creación de patrones de diseño enfocados totalmente a las cadenas de bloques, se discutirá si es necesaria la creación de un lenguaje de modelado para sistemas orientados a cadenas de bloques y se aplicará a la metodología un protocolo de pruebas empírico mediante el uso de casos.

REFERENCIAS

S. Nakamoto. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/

Jesus Leal Trujillo, Steve Fromhart y Val Srinivas. (2017). Evolution of blockchain technology: Insights from the GitHub platform. https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html

N. Szabo. (1966). Smart Contracts: Building Blocks for Digital Markets. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Decker C., y Wattenhofer R. (2013). Information propagation in the bitcoin network. In IEEE P2P 2013 Proceedings. IEEE.

Zheng Z., Xie S., Dai H., Chen X., y Wang H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.

Gatteschi V., Lamberti F., Demartini C., Pranteda C., y Santamaría V. (2018). To blockchain or not to blockchain: That is the question. IT Professional, 20(2), 62-74.

Cryptocurrency statistics. (2019). https://bitinfocharts.com/

Carlos O. Solis-Osorio, Elizabeth Pérez-Cortés y Humberto Cervantes-Maceda. (2018). ¿Usar o no Blockchain para mi Sistema?. Software Guru, 57, pp. 32-34.

Royal Mint, How Blockchain is disrupting the finance industry, royal Mint News and Insights. (2019). http://rmg.royalmint.com/

Rocha H., y Ducasse S. (2018). Preliminary steps towards modeling blockchain oriented software. In 2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) (pp. 52-57). IEEE.

Xu X., Weber I., y Staples M. (2019). Architecture for blockchain applications (pp. 1-307). Berlin, Germany: Springer.

NOTAS BIOGRÁFICAS

Carlos Omar Solis Osorio es licenciado en Computación de la UAM-Iztapalapa y actualmente, estudiante de Maestría en Ciencias y Tecnologías de la Información, centrando su investigación en las cadenas de bloques y los retos que estas implican en la ingeniería de software.

Elizabeth Pérez Cortés es profesora-investigadora en la UAM-Iztapalapa. Realiza docencia e investigación en Sistemas Distribuidos, en particular en bases de datos distribuidas, sistemas par a par, datos abiertos enlazados y esquemas de incentivos.

Humberto Cervantes Maceda es profesor-investigador en la UAM-Iztapalapa. Además de realizar docencia e investigación dentro de la academia en temas relacionados con arquitectura de software, realiza consultoría y tiene experiencia en la implantación de métodos de arquitectura dentro de la industria.