José Pastor Galiana

j.pastor.galiana@gmail.com

ERC20, ERC721, ERC725 y ERC735

Sistema dual con un token identificativo para las asignaturas y un token que representa ECTS adquiridos, ambos ligados a un mecanismo de identidad digital.

TFE: Sistema titulaciones tokenizado

Experto Universitario en desarrollo de aplicaciones BlockChain

# Contenido

[1 Contenido 1](#_Toc32880619)

[2 Estado del arte de la digitalización de las titulaciones académicas 2](#_Toc32880620)

[3 Descripción funcional del proyecto 2](#_Toc32880621)

[4 Justificación del uso de blockchain 3](#_Toc32880622)

[5 Solución técnica 14](#_Toc32880623)

[6 Referencias 16](#_Toc32880624)

# Estado del arte de la digitalización de las titulaciones académicas

Se nos solicita que como primer paso, realicemos un análisis del estado del arte en cuanto a

la digitalización de títulos académicos y su integración entre las distintas universidades

# Descripción funcional del proyecto

El proyecto que se expone atendiende al caso número 2 presentado en el ambito del curso “Experto Universitario en desarrollo de aplicaciones BlockChain”.

El proyecto se desarrollará de acuerdo con tres roles, alumno, universidad y empresa, que añadirán al actual modelo de relaciones habitual, un conjunto de evidencias y afirmaciones registradas en la BlockChain.

…tokens de sus asignaturas, en caso de querer solicitar un traslado de expediente, solo habría que

presentar los tokens de las asignaturas finalizadas, y así todas las aplicaciones que se puedan generar.

Se nos indica que debemos tener en cuenta que se dispone de una identidad digital y que es esta la que

posee los tokens de las asignaturas.

Se nos solicita que como primer paso, realicemos un análisis del estado del arte en cuanto a la

digitalización de títulos académicos y su integración entre las distintas universidades.

Al realizar el modelo del título lo ideal sería un sistema dual con un token que identifique la asignatura y un

token para la cantidad de créditos que utiliza.

La aplicación debe tener tres roles distintos:

• Alumno

• Profesor

• Administración

La funcionalidad de cada uno debe ser detallada, así como las interacciones con los tokens que tendrá

cada uno.

Cualquier duda que pueda surgir en el desarrollo de este trabajo debe ser consultada con el cliente; en

nuestro caso, lo haremos con el director que tengamos asignado.

El presente manual se presenta como un *Step by step,* pues para alguna de las tareas pudiera ser necesario haber completado las anteriores. Es importante seguirlo en orden.

Este documento no es únicamente para leer, también se ofrece indicaciones de como ir completando las diferentes acciones de la aplicación. Busque el texto Probarlo en rojo que aparece a lo largo del documento para comprobar el correcto funcionamiento.

En los ejemplos y URLs que aparecen en el documento se ha supuesto que el despliegue de la aplicación se ha realizado de acuerdo con el manual de despliegue. En el caso de no haber seguido dicho manual, sustituya <http://localhost:8000> por lo correspondiente en su caso.

# Justificación del uso de blockchain

Las cadenas de bloques (blockchain) son un mecanismo de almacenamiento de datos que fue creado para dar soporte a las necesidades que se planteó Bitcoin en el 2009 [1]. Sin embargo, posteriormente se descubrió que éste mecanismo puede tener múltiples aplicaciones que van mucho más allá de las criptomonedas. A partir de este momento las cadenas de bloques cobraron importancia y muchas empresas comenzaron a explorar su uso. El problema es que el uso de una cadena de bloques no siempre es una buena decisión. Gartner sugiere que el 90% de los proyectos empresariales basados en blockchain, lanzados entre 2016 y la primera mitad de 2017, fracasarán en un lapso de 24 meses [2]. Por esta razón, antes de comenzar un proyecto basado en esta tecnología, es necesario tomarse el tiempo de analizar las necesidades del proyecto para determinar si estas pueden ser cubiertas por un sistema de bases de datos tradicional o bien es necesario recurrir a las cadenas de bloques.

En este artículo presentamos una serie de criterios que ayudan a determinar cuándo tiene sentido almacenar datos en un blockchain. Para entender la manera en que se utiliza esta lista de criterios, los aplicamos en un ejemplo sencillo.

Parte 1. Criterios de decisión

A continuación enumeramos un conjunto de criterios, obtenidos a partir de [3] y [4], que son útiles para identificar si un proyecto es candidato a ser desarrollado usando la tecnología de cadena de bloques. Al final de cada criterio se incluye una pregunta que deben ser respondida para guiar en el proceso de toma de decisión. Cabe señalar que si se responde de manera afirmativa a todas las preguntas, entonces es muy probable que el sistema que se desea desarrollar se vea beneficiado por el uso de una cadena de bloques.

Necesidad de una base de datos

El primer paso es tener claras las necesidades de persistencia de datos. Si bien en la actualidad la gran mayoría de proyectos de software requieren una base de datos, esto no significa que tenga que implementarse con una cadena de bloques. Las bases de datos tradicionales han hecho un buen trabajo almacenando datos desde hace décadas, y en los últimos años han evolucionado significativamente para incorporar nuevas capacidades (ej. NoSQL). Así que la pregunta que debemos hacernos en este punto es: ¿En verdad es insuficiente una base de datos tradicional (relacional o no relacional) para cubrir las necesidades del proyecto?

Existencia de múltiples escritores

En muchos sistemas los cambios son realizados de forma centralizada o mediante una entidad que recibe peticiones y verifica si es posible hacer cambios en los datos y, de ser así, los lleva a cabo. En ciertos escenarios, sin embargo, es deseable que existan diversas entidades, o escritores, que sean capaces de modificar los datos de forma independiente. Si el sistema que se busca desarrollar tiene esta necesidad, entonces tal vez tenga sentido usar una cadena de bloques. Por lo anterior, debemos responder a la siguiente pregunta ¿Se pueden identificar múltiples escritores en el sistema a desarrollar?

Confidencialidad

En una base de datos tradicional tenemos la libertad de elegir mediante diferentes métodos a los usuarios que tienen derecho a ingresar a la información contenida en ella, incluso es posible asignar niveles de usuario con la finalidad de regular el acceso a los datos manteniéndolos seguros y confidenciales. Por otro lado, la transparencia de datos es una característica de las cadenas de bloques. Recordemos que una cadena de bloques almacena la información de las diferentes transacciones que se han realizado desde que esta se creó y que, además, existen múltiples réplicas de la misma que son usadas para verificar la validez de una transacción. En otras palabras, los nodos que poseen una réplica tienen acceso a la información ahí almacenada. Por lo anterior, si existen restricciones de confidencialidad que impliquen que la información no pueda estar replicada en varios nodos, es probable que la cadena de bloques no sea la mejor opción. Es necesario entonces responder a la pregunta ¿Los datos pueden ser replicados en varios nodos sin violar las restricciones de confidencialidad?

Rendimiento

Una de las principales limitaciones del almacenamiento en cadenas de bloques es que no pueden almacenar mucha información dentro de un bloque y tampoco son capaces de tolerar una alta demanda de transacciones. En consecuencia, si el proyecto de software requiere de almacenar grandes cantidades de datos además de un alto rendimiento, será necesario buscar alternativas para satisfacer esos requerimientos. Por ejemplo, en el blockchain se podrían guardar únicamente apuntadores a archivos almacenados independientemente. De esta forma se evita guardar mucha información en la cadena y potenciar el rendimiento. Por lo anterior, debemos preguntarnos ¿El sistema a desarrollar maneja una cantidad limitada de información y no requiere alto rendimiento?

Desconfianza

Anteriormente se había mencionado que una cadena de bloques soporta la existencia de múltiples escritores que pueden modificar directamente los datos. Es posible que ante esta situación exista desconfianza entre los escritores; es decir, si un escritor puede modificar entradas que le pertenecen a otro escritor o bien las propias a su conveniencia, existe desconfianza entre ellos. Si en el sistema que queremos desarrollar existe desconfianza entre los múltiples escritores, entonces el uso de una cadena de bloques es recomendable. Por lo anterior, debemos responder a la siguiente pregunta ¿Existe desconfianza entre los múltiples escritores que participan dentro del sistema?

Desintermediación

El problema de una base de datos distribuida con múltiples escritores que desconfían entre sí no es un problema nuevo. De hecho, existe una solución a este problema y son los intermediarios de confianza, es decir colocar un ente que funcione como regulador y validador de las transacciones que se realizan entre usuarios. En este caso es necesario que todos los usuarios del sistema confíen en que el intermediario realiza sus tareas sin preferencia por ningún usuario.

En las cadenas de bloques los nodos que poseen una réplica validan la integridad de la información y rechazan transacciones malintencionadas. Esta característica permite eliminar a los intermediarios de confianza. Por ejemplo, en la red de Bitcoin las transferencias no requieren de una institución bancaria que valide cada una de ellas. Por esta razón, las cadenas de bloques son útiles en proyectos donde se desea eliminar a los intermediarios de confianza o cuando no existe un intermediario que cumpla con los requerimientos del proyecto. En consecuencia, es importante responder a la pregunta ¿Se desea eliminar intermediarios de confianza?

Validadores

Una cadena de bloques como su nombre lo indica, es literalmente una serie de bloques encadenados entre sí; cada bloque contiene un conjunto de transacciones que le indican a todos los nodos de la red cuales son las transacciones válidas que se han realizado hasta el momento así como el orden cronológico en el que se realizaron. No todos los nodos tienen la capacidad de agregar un bloque a la cadena y, en consecuencia, es necesario especificar qué nodos se encargarán de esta tarea. Estos nodos llevan por nombre validadores o mineros y pueden ser elegidos de diferentes formas dependiendo el tipo de cadena de bloques. Por ejemplo en una cadena de bloques privada, los validadores pueden ser un grupo básico de nodos que mantengan la cadena, en contraste con la red de Bitcoin, donde un validador puede ser cualquier nodo con la capacidad computacional para realizar los cálculos requeridos por la red. Debemos entonces responder ¿Es posible identificar quiénes tomarían el papel de validadores en su sistema?

Reglas de validación

Independientemente de quiénes sean los validadores o qué algoritmo utilicen para llegar al consenso, el propietario de una copia de la base de datos debe seguir las reglas establecidas para determinar si una transacción es válida o no. En consecuencia se debe responder a la pregunta ¿Se tienen claras las reglas a seguir para determinar la validez de una transacción?

Dependencia entre transacciones

Hasta el momento sabemos que las cadenas que bloques se asemejan a una base de datos distribuida. En esta base de datos se almacenan bloques que contienen un cierto número de transacciones, cada bloque nuevo que se crea se enlaza al anterior creando una cadena de bloques y permitiendo que las diferentes transacciones que se realizan tengan un orden cronológico entre ellas. Esta característica permite tomar una decisión cuando dos transacciones dependen una de otra, por ejemplo: Suponga que el individuo A desea transferir $50 al individuo B y luego el individuo B los transfiere al individuo C, la transferencia del individuo B al C depende de la transferencia que realizó el individuo A al B, ya que si no se realiza en el orden correcto la transferencia del individuo B al C sería rechazada por falta de fondos, podríamos decir entonces que esta serie de transacciones son dependientes. Las cadenas de bloques soportan dependencia entre transacciones. Debemos entonces preguntarnos ¿El sistema involucra transacciones que sean dependientes?

Inmutabilidad e historia

Una de las principales ventajas que nos proporciona una cadena de bloques es la inmutabilidad de los datos. Gracias a esta característica los nodos pueden confiar en que la información almacenada en ella es confiable y no ha sido modificada a conveniencia de algún nodo en particular. Anteriormente se comentó que existe desconfianza entre los diferentes nodos que conforman la red, pero esto no quiere decir que no exista un ente de confianza. La confianza se traslada a la cadena de bloques y es ella quien indica cuales son las transacciones válidas.

La inmutabilidad de la cadena permite generar la historia de los datos; es decir, debido a que los datos que pertenecen a la cadena de bloques no pueden cambiar, es fácil rastrear la evolución de un dato. De hecho, muchas de las aplicaciones que existen actualmente en el mercado explotan esta característica de las cadenas de bloques (por ejemplo rastrean origen de oro, diamantes, alimentos, etc.). Por lo anterior, podemos hacernos la pregunta siguiente ¿El sistema requiere que los datos sean inmutables?

Parte 2. Ejemplo

Con la intención de mostrar de manera práctica cómo utilizar el cuestionario descrito anteriormente, analizaremos si es pertinente utilizar las cadenas de bloques para implementar un sistema de manejo de inventario de bienes de inversión.

Consideremos una institución académica donde la adquisición de algún bien material (computadoras, escritorios, sillas, etc) involucra la realización de una petición por escrito al Departamento de Administración indicando información personal, 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 y una vez que el bien es recibido se notifica al solicitante para que pueda acudir a retirarlo. En cuanto el bien es retirado por la persona que lo solicitó queda bajo su resguardo y a partir de este momento esta persona 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 descompostura. Existe un caso especial en donde un trabajador 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. La institución desea implementar un sistema de manejo de inventario que se ejecute en distintos dispositivos y que gestione de manera eficiente y segura los procesos descritos anteriormente.

A continuación analizaremos cada uno de los puntos mencionados anteriormente en el contexto del problema planteado.

Pregunta

Respuesta

Justificación

a)

¿Una base de datos tradicional (relacional o no relacional) es insuficiente para cubrir las necesidades del proyecto?

SI

- Existe la necesidad de eliminar intermediarios

- Se desea que el sistema sea descentralizado para aumentar la disponibilidad

b)

¿Se pueden identificar múltiples escritores en el sistema a desarrollar?

SI

- Los escritores en el proyecto son el trabajador y proveeduría, ya que los demás serían innecesarios una vez implantada la solución

c)

¿Es posible que los datos se encuentren replicados en diversos nodos?

SI

- No se tienen limitaciones en cuanto al hecho de que la información sea confidencial y no pueda estar replicada en distintos nodos

d)

¿El sistema a desarrollar soporta un manejo de una cantidad limitada de información y no requiere alto rendimiento?

SI

- La cantidad de transacciones no es elevada y el manejo de inventario no requiere en este caso de grandes volúmenes de información

e)

¿Existe desconfianza entre los múltiples escritores que participan dentro del sistema?

SI

- Un trabajador podría, por ejemplo, modificar la base de datos para simular un traspaso sin que este se realice realmente

f)

¿Se desea eliminar intermediarios de confianza?

SI

- Los únicos participantes deberían ser los trabajadores y proveeduría, los demás intermediarios que participan actualmente en el proceso pueden ser eliminados.

g)

¿Es posible identificar quienes tomarían el papel de validadores en su sistema?

SI

- No sería una buena idea forzar a que cada usuario (nodo) que utilice el sistema tenga que ser un validador. La alternativa más viable sería designar a un grupo de nodos encargados de la escritura de la cadena de bloques.

h)

¿Se tienen claras las reglas a seguir para determinar la validez de una transacción?

SI

- Las reglas para que un usuario adquiera y se libere del resguardo de un bien están claras.

i)

¿El sistema involucra transacciones que sean dependientes?

SI

- Por ejemplo, no es posible realizar una transacción de traspaso entre trabajadores si previamente no existe una transacción que involucre la recepción del bien por parte del trabajador que traspasa el bien

j)

¿El sistema requiere que los datos sean inmutables?

SI

- Es necesario conocer las distintas transacciones que han ocurrido a lo largo de la vida útil de un bien

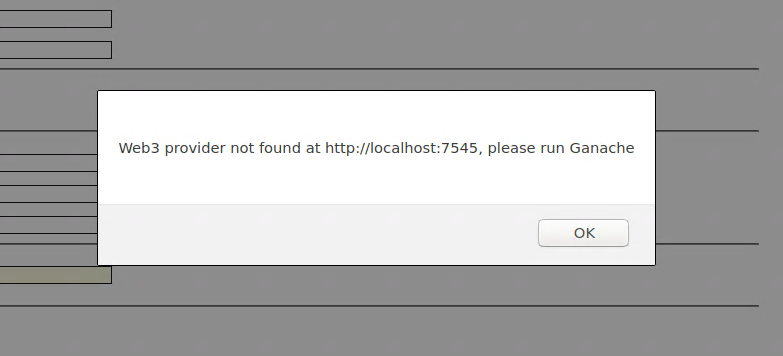
A partir de este análisis, es posible concluir que este sistema sí se vería beneficiado por el uso de una cadena de bloques.

Conclusiones

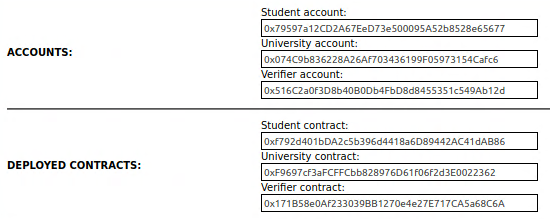
Las cadenas de bloques son una de las tecnologías que ha cobrado mayor popularidad en los últimos años, sin embargo muchos de los proyectos que utilizan cadenas de bloques son iniciados de manera apresurada y sin detenerse a pensar si es realmente necesario el hacer uso o no de dicha tecnología. Responder a la serie de preguntas que presentamos aquí es un ejercicio que conviene hacer antes de lanzarse en un proyecto que haga uso de una cadena de bloques con el fin de reducir las posibilidades de tomar una mala decisión.

El inicio de la aplicación consistirá unicamente en acceder a <http://localhost:8000/index.html>.

Tras acceder, la aplicación inicializa las cuentas y valores necesarios. La aplicación requiere que en el mismo servidor se encuentre disponible un web provider testnet que ofrezca al menos 3 cuentas en <http://localhost:7545>. En caso de que este no se encontrara arrancado tras el inicio, la aplicación nos mostrará una advertencia sugiriendo que iniciemos Ganache, de acuerdo con el manual de despliegue.



Si efectivamente el web provider se encontraba correctamente funcionando en dicho puerto, la aplicación iniciará las constantes de las cuentas a utilizar y desplegará los diferentes contratos necesarios para los 3 roles necesarios, estudiante, universidad y empresa.



Igualmente, si hemos utilizado Ganache, podremos comprobar que las 3 cuentas utilizadas coinciden con las 3 primeras ofrecidas por dicha aplicación:

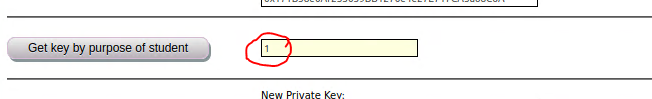


# Solución técnica

El objetivo de este paso es la obtención de la clave de gestión del alumno, no obstante, hemos generalizado el método para que sea válido para obtener cualquier tipo de clave.

Probarlo: Introducir el tipo de clave en la que estamos interesados y obtenerla.

1. Coloque el cursor en el campo en amarillo que aparece a la derecha del botón **Get key by purpose of student** e indiqué el tipo de clave en el que está interesado, por defecto el tipo 1, management.



1. Pulse el botón **Get key by purpose of student** y obtendrá la clave del tipo indicado. Si ha mantenido el 1 obtendrá la “management key” del alumno.

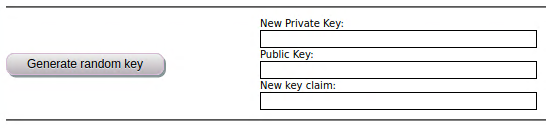


Generación de una nueva clave aleatoria

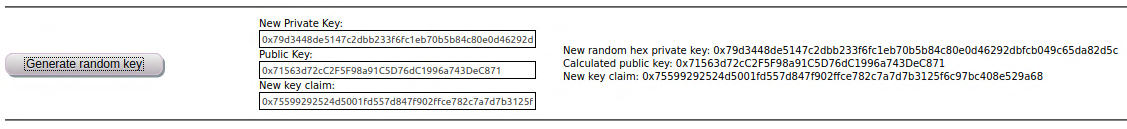
Con el objetivo de añadirla posteriormente como una clave de tipo claim, generaremos en este punto una nueva clave aleatoria.

Probarlo: Dirijase al apartado correspondiente y siga los siguientes pasos

1. Pulsé sobre el botón **Generate random key**.



1. La clave generada aleatoriamente aparecerá en los campos de texto correspondientes.

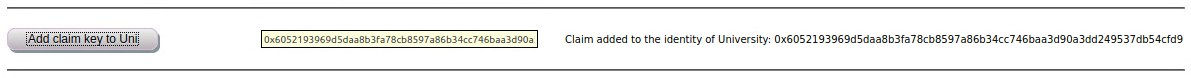


Añadir “claim key” a la universidad

Para facilitar la prueba, la aplicación copia directamente la nueva “**New key claim**” generada en el apartado anterior, al campo de entrada de este ejercicio, no obstante, usted puede modificarlo introduciendo manualmente una cuenta.



Probarlo: Pulse el botón **Add claim key to Uni** y se añadirá la clave indicada como nueva clave de tipo claim a la universidad.



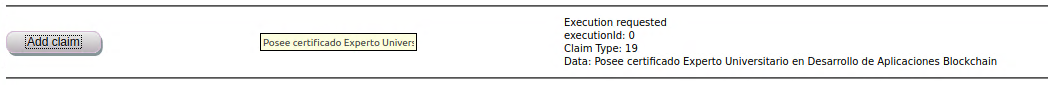
Añadir claim al estudiante

En este apartado, con la cuenta de la universidad, añadiremos un **claim de tipo 19**, con una alegación asociada, a la identidad del alumno.

Por defecto, el campo alegación ha sido inicializado por defecto con el texto “Posee certificado Experto Universitario en Desarrollo de Aplicaciones Blockchain”, no obstante, puede ser modificado libremente.



Probarlo: Pulse el botón **Add claim** y se añadirá el claim correspondiente a la cuenta del alumno.

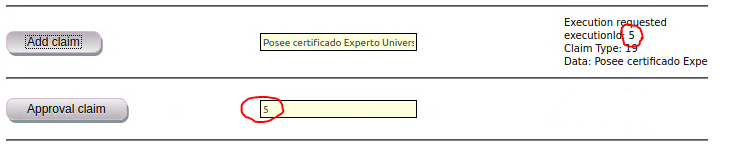


**Análisis:** Tras este paso el claim ha quedado añadido a la cuenta del alumno pero se encuentra pendiente de validación por su parte. Para referirnos posteriormente a esta petición, utilizaremos el *ExecutionID* que hemos obtenido.

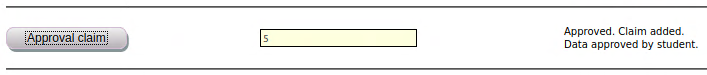
El estudiante aprueba el claim

En este ejercicio, con la cuenta del estudiante debe aprobarse el claim añadido en el ejercicio anterior.

Por defecto la aplicación informa el campo de entrada del *ExecutionId* con el último obtenido en el apartado anterior, aunque podríamos personalizarlo manualmente.



Probarlo: Pulse el botón **Approval claim** y se aceptará el claim por parte del alumno.



# Referencias

S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. https://bitcoin.org

P. Christy, “7 Strategies to Gain Value From a Doomed Blockchain Project”. Smarter with Gartner. http://swgu.ru/wp

S. K. Lo, X. Xu, Y. K. Chiam & Q. Lu, “Evaluating suitability of applying blockchain” International Conference on Engineering of Complex Computer Systems (ICECCS), pag. 158-161, IEEE, 2017.

G. Greenspan, “Avoiding the pointless blockchain project”. http://swgu.ru/wq