

Universidad de Oriente

Sede “Julio Antonio Mella”

Facultad de Ingeniería en Telecomunicaciones Informática y Biomédica

Ingeniería Informática

3er Año

**Informe de la Práctica Laboral**

Autor: Daniela de la Concepción González Domínguez

Tutor: MSc. Dionis López Ramos

Tema: La tecnología Blockchain y los contratos inteligentes en el lenguaje Solidity

Proyecto de Investigación: Soluciones Informáticas para la gestión de los procesos universitarios a partir de plataformas de gobierno electrónico.

Comercio electrónico con tecnologías emergentes CELTEM.

2022

“Año 64 de la Revolución”

**Resumen**

El presente trabajo tiene como objetivos principales la aprehensión de la tecnología Blockchain, que surgen para **garantizar la seguridad y la transparencia de las transacciones mediante conexiones directas y descentralizadas** y los Contratos Inteligentes (Smart Contract) como forma de hacer cumplir estas transacciones sin necesidad de intermediarios. El aprendizaje de la Programación de Contratos inteligentes en el lenguaje Solidity y el diseño de un Contrato Inteligente con elementos de sostenibilidad.

1. **Introducción**

El proyecto de investigación para lograr el uso de las tecnologías de Información y Comunicación (gobierno electrónico), perteneciente a la Facultad de Ingeniería en Telecomunicaciones Informática y Biomédica de la Universidad de Oriente, se ha basado en analizar la tecnología blockchain y la creación de contratos inteligentes. En el mismo daremos respuesta a como se hace la contratación de una entidad estatal a una particular.

Con el presente estudio se pretende ofrecer varias contribuciones en este campo de investigación. En primer lugar, se recogen los principales conceptos teóricos sobre esta tecnología, innovadora y reciente y los contractos inteligentes como forma segura de contratación. En segundo lugar, se analizará el aprendizaje de la programación de los contratos inteligentes en el lenguaje Solidity. Y en tercer lugar, diseñar la solución de las mismas con elementos de sostenibilidad.

**Blockchain surge en 2008, dentro del proyecto Bitcoin por Satoshi Nakamoto.** El origen del dinero digital fue posible gracias a la elaboración de un sistema de seguridad prácticamente impenetrable. Este sistema, se desarrolló **combinando la tecnología de redes existente Persona a Persona (P2P; siglas en inglés) con técnicas criptográficas avanzadas**. De ahí el término criptomoneda. **El objetivo del proyecto Bitcoin** era **garantizar la seguridad, la transparencia y la privacidad entre los usuarios**, a través de servidores de almacenamiento y gestión de datos particulares de clientes. Las **redes Blockchain, se han desarrollado y empiezan a funcionar para el usuario medio**. [1]

Los Smart Contracts surgieron en 1993 cuando el [criptógrafo](https://masterethereum.com/criptografia-seguridad-documentos-red) estadounidense Nick Szabo comenzó a utilizar este término. Szabo propuso el cambio de los contratos tradicionales a este sistema, pero no tuvo éxito debido a las limitaciones tecnológicas de ese momento. Sin embargo, en 2009 se creó el Bitcoin, lo cual cambió la situación. Los contratos inteligentes necesitaban un sistema de pagos que los pudiese poner en práctica, y ahí estaba el Bitcoin. A pesar de que el Bitcoin solo estaba pensado para ser una herramienta financiera, su tecnología era útil. En 2014, gracias también a la creación del Ethereum, los smart contracts cobraron vida. [2]

**2. Como gestionar o validar un contrato inteligente entre dos pares que al cumplirse X condiciones se haga una transferencia financiera de A a B.**

Los contratos inteligentes pueden definirse como acuerdos que tienen como objetivo principal programar y automatizar contratos “tradicionales” entre personas, después que las partes hayan acordado sus términos. Abren un mundo nuevo de posibilidades, como que las “cosas” interactúen entre sí y con personas en base a contratos que regulan las relaciones. Los Smart Contracts permiten, por ejemplo, automatizar repartos de fondos cuando se cumplen las condiciones, sin que tenga que intervenir ningún intermediario para validar las cláusulas del contrato, ni para ejecutarlas.[3]

Lo mejor para entender el concepto de un contrato inteligente es hacer una analogía con una máquina expendedora: cuando se introducen en la máquina monedas por el importe de un determinado producto, la máquina ejecuta internamente un código que acaba finalmente con la provisión, o no, de la bebida.

La máquina tiene programado que sólo puede lanzar el evento de suministrar la bebida si se ha introducido el precio del producto. Además, tiene programado que, en caso de haber introducido más dinero del que cuesta el producto, la máquina devuelva el cambio y que en caso de no haber un producto seleccionado aparezca en la pantalla “Producto Agotado”. No hay intervención humana, no hay precio negociable: si se cumplen las condiciones el producto se dispensará, si no se cumplen, no se obtendrá.

Esta programación interna de la máquina es lo que sería el Smart Contract, y las partes implicadas son la propia máquina y el usuario/cliente. Las reglas del contrato inteligente podrían ser las reglas que hemos mencionado anteriormente, y que se ejecutarán por sí solas si se cumplen las acciones correspondientes.

En el lenguaje informático esto funciona como una sentencia condicional llamada ‘if – then’, que significa “si… entonces…” y viene a simbolizar que “si se cumple la condición X… entonces que se ejecute Y…” [4]

Lo primero que ha de indicarse con respecto a las problemáticas asociadas a la ejecución automática de los contratos es que si el cumplimiento del contrato depende de un código de computador, debe garantizarse que dicho código no contenga errores.

En segundo lugar, es necesario que el código refleje de manera adecuada la voluntad de las partes. En efecto, quien codifique las condiciones contractuales y las traduzca de un lenguaje natural a un lenguaje de código puede generar resultados que se alejen de la verdadera intención de las partes contratantes.

En tercer lugar, un contrato inmutable requiere que todos los posibles eventos que puedan afectar su desarrollo sean previstos e incorporados en él, pues una vez introducido en la *blockchain,* no será posible que el ser humano intervenga o modifique su contenido.

En cuarto lugar, la inflexibilidad de los contratos inteligentes desconoce la realidad de las relaciones comerciales, en donde muchas veces el cumplimiento de las obligaciones de una de las partes se analiza bajo criterios de razonabilidad o buena fe.

El hecho de que los contratos inteligentes se encuentren inmersos en una *blockchain* no implica que se encuentren aislados del ordenamiento jurídico. En efecto, si la *blockchain* dejara de funcionar, los contratos seguirían existiendo, simplemente su ejecución debería llevarse a cabo en otro escenario. [6]

Originalmente existen seis fases en la creación de un contrato inteligente:

* Las partes manifiestan su voluntad para alcanzar un acuerdo.
* Los contratantes especifican las condiciones del contrato.
* Un programador escribe el código informático que permitirá la ejecución automática cuando sucedan los hechos previstos.
* Cada una de las cláusulas se cifra mediante sistemas de autenticación y verificación, en una cadena de bloques.
* Las cláusulas registradas en el bloque se verifican por el sistema de consenso, con lo que se ejecuta en forma automática la prestación.
* Ejecutada la prestación, todos los nodos del sistema la reconocen como tal, haciéndola inalterable en la cadena de bloques.[5]

**3. El Merge 2.0 de Ethereum: Ventajas y Desventajas**

La segunda criptomoneda más popular del mundo, ether, está a punto de cambiar a un nuevo modelo operativo más ecológico. Actualmente, para su "minería" consume la misma cantidad de energía que un país de tamaño medio. Ahora, lo que se conoce como "la fusión" hará que sus emisiones de carbono se reduzcan un 99,9%. Si bien las criptomonedas han sido una revolución en el mundo de la economía, su contribución al cambio climático es desafortunada debido a la cantidad de electricidad que usan las computadoras que gestionan su compraventa.

El plan para cambiar al nuevo modelo, cuenta Vitalik Buterin, cofundador de Ethereum (la plataforma digital cuya moneda es el ether), estaba en el horizonte desde que la criptomoneda se lanzó en 2014, pero se ha pospuesto por la complejidad técnica que supone.

Lo que cambiará a partir de ahora es que la cadena de bloques del sistema PoW se fusionará (lo que han llamado *The Merge* o "la fusión"), con una copia de carbón llamada *Beacon Chain* (cadena de baliza). Detrás de este nombre aparece un nuevo sistema de codificación de las criptomonedas del sistema Ethereum: el "proof of stake" (prueba de participación) o sistema PoS.

El sistema PoS reduce enormemente la cantidad de computadoras necesarias para mantener la cadena de bloques. Los criptomineros son reemplazados por una cantidad menor de "validadores" de la transacción. Además de reducir la carga energética de Ethereum, el sistema PoS reduce la cantidad de monedas entregadas como recompensa (que es la forma en que se generan las monedas digitales) y los organizadores dicen que disminuirá la cantidad total de divisas existentes.

Otro de los cambios es que con este sistema se pueden usar computadoras portátiles y de escritorio, en lugar de las potentes GPU (unidades de procesamiento de datos) que hasta ahora se usaban. [7]

**4. Análisis de estado del arte de las plataformas existentes para la creación automática en contratos inteligentes.**

Ethereum es una de las plataformas de computación distribuida más populares que hay en la actualidad. **Sirve para ejecutar contratos inteligentes peer to peer (P2P)** en Ethereum Virtual Machine (EVM), que es una máquina virtual descentralizada. Los **contratos inteligentes con Ethereum** están fundamentados en la teoría del Bitcoin, ya que, como esta tecnología, posee mineros e incluso cuenta con un Blockchain propio y la criptomoneda Ether. Sin embargo, Ethereum a diferencia del Bitcoin ha creado un intérprete del lenguaje de programación que es mucho más extenso. Por lo tanto, a este sistema para **crear contratos inteligentes** se le puede añadir una lógica mucho más compleja dentro del Blockchain, lo que ha permitido que estos softwares tengan mucho más posibilidades y funcionalidades que los de Bitcoin.

**Rootstock e**s una plataforma open source o de código abierto que tuvo como propósito aprovechar la seguridad de la red de Bitcoin para elaborar contratos inteligentes. Utiliza Solidity como principal lenguaje y la Prueba de Trabajo (PoW) de Bitcoin por medio de la minería fusionada. **Se conoce como el Ethereum de Bitcoin** y tiene el propósito de aprovechar la seguridad y la red que ofrece Bitcoin. RootStock permitirá que los mineros puedan participar de un modo activo debido a que tiene como principal objetivo añadir al ecosistema de Bitcoin valor y funcionalidad a través de smart contracts seguros en la red. Este sistema de gestión se vale de la moneda y la liquidez que tiene el Bitcoin con lo mejor de Ethereum, que es su ecosistema para programar contratos inteligentes. Se puede emplear para hacer pagos instantáneos con unas cadenas laterales (sidechain).

**Counterparty e**s una **plataforma de contratos inteligentes**de libre acceso con la que se pueden crear aplicaciones peer-to-peer, utiliza el lenguaje de programación de los **contratos inteligentes Solidity**para crear diferentes clases de instrumentos financieros y acuerdos digitales. Este se trata de un sistema con el que las acciones del mundo real se pueden transformar en código, y funcionar automáticamente sin presentar fallos ni tener la necesidad de intermediarios. La **moneda de contratos inteligentes**de Counterparty es el XCP, con la que se programan y realizan operaciones con activos digitales.

**EOS e**s una plataforma muy segura con la que se pueden desplegar servicios y aplicaciones distribuidas (DApps). Para crear los smart contracts no usa una máquina virtual sino una API de programación basado en C/C++, que contribuye a que estos programas sean veloces y bastante flexibles, de modo tal que posee una documentación amplia para programar contratos inteligentes.

Codius en el caso de esta plataforma, cabe mencionar que trabaja diferente a la tecnología de los **contratos inteligentes de Ethereum** o Bitcoin, debido a que estos se ejecutan en hosts independientes sin que exista una cadena de bloques que sea subyacente, tal como en el alojamiento tradicional. De esta forma, estos pueden interactuar con cualquier API o servicio, escalar de modo infinito y leer o escribir en cualquier clase de blockchain. Por esta razón, es una clase de contratos inteligentes que supera la interoperabilidad que es su desafío esencial.

Dtecdeal valiéndose de la tecnología Blockchain, así como el respaldo de abogados especializados y profesionales especialistas en Blockchain, esta plataforma ofrece soluciones contractuales mediante smart contracts sencillo y seguros. Estos crean contratos inteligentes para toda clase negocios, ayudando a **optimizar diferentes clases de actividades y darles a diversos procesos un valor agregado**, ya que con estos se podrá transformar de una forma notable el enfoque digital de las compañías que decidan implementarlos.

**Lisk e**ste es un sistema de gestión en el que se emplea el **lenguaje de programación JavaScript**para elaborar y ejecutar de un modo descentralizado contratos inteligentes que sean muy rápidos y seguros. Esta plataforma va a requerir de la moneda LSK para que funcionen los smart contracts y aunque actualmente se halla en una fase muy inicial, ya cuenta con diferentes conceptos DAPP como una red social para artistas o el “proof of existance” conocido como Discovr.

**Ivy Playground** es una herramienta con la que se pueden redactar, diseñar y poner a prueba los contratos inteligentes, que se van a poder albergar en la Blockchain de la empresa Chain. Utiliza el lenguaje de programación Ivy, que se ha diseñado para **elaborar contratos que tengan niveles de complejidad y seguridad bastante altos.** Pueden registrarse tanto en la test net que ofrece la herramienta, así como en un blockchain de Chain, ya que de este modo se podrá validar la efectividad que tiene antes de poder ejecutarlo abiertamente. A través de estos contratos inteligentes, se manejan los activos criptográficos que se hayan depositado. Cada contrato se encarga de controlar, bloquear o liberar un valor en específico, es decir, cierto número de unidades en un activo y atribuir los términos que se deban cumplir antes de que haya que desbloquear ese valor. [8]

# **5. Contrato inteligente ERC-20 en Avalanche con Infura**

Aunque Ethereum se ha establecido firmemente como la plataforma blockchain líder capaz de ejecutar contratos inteligentes, no está exenta de defectos. Ha resuelto algunos de sus problemas, como el enorme consumo de energía al cambiar a un protocolo de consenso de prueba de participación. Sin embargo, siguen existiendo problemas de escalado. Ethereum tiene un rendimiento de transacción bajo (aproximadamente 15 transacciones por segundo), una finalidad de transacción lenta (alrededor de 1 minuto) y, en ocasiones, tarifas de gas altas cuando la red está bajo presión.

Avalanche es una plataforma de cadena de bloques independiente diseñada para superar algunas de las barreras a la escalabilidad mencionadas anteriormente.  Avalanche es la plataforma de contratos inteligentes más rápida en la industria de la cadena de bloques, medida por el tiempo hasta la finalización. A diferencia de Ethereum o Bitcoin, Avalanche consta de varias cadenas, cada una de las cuales realiza una tarea específica. Las tres cadenas más importantes de la red Avalanche son la cadena C, la cadena X y la cadena P.

Mediante el uso de subredes y nuevos protocolos de consenso, Avalanche puede brindar los siguientes beneficios:

* **Transacciones teóricamente infinitas por segundo**: Dado que no existe un límite superior en la cantidad de subredes que se pueden crear y que las subredes funcionan de manera bastante independiente, Avalanche puede ofrecer tasas de transacciones por segundo extraordinariamente altas.
* **Baja firmeza de transacción**: Avalanche tiene el tiempo de finalización más bajo de la industria, con confirmación de transacción en menos de dos segundos.
* **Energía Eficiente**: Avalanche utiliza prueba de participación para asegurar su red, lo que la hace extremadamente eficiente en energía. También permite que participen validadores sin acceso a GPU de gama alta.
* **Extremadamente descentralizado**: Más de miles de validadores aseguran Avalanche. Y a diferencia de Ethereum o Bitcoin, una pequeña cantidad de grupos no controla la gran mayoría de la red.

**6. Tezos**

Tezos es una plataforma de blockchain descentralizada y multifuncional para alojar contratos inteligentes, aplicaciones y crear tokens. Su criptomoneda es el Tez, o Tezzie (XTZ). Esta moneda no está sujeta a la minería, por lo que los usuarios que tienen una cierta cantidad de Tezzie son recompensados con tokens cuando participan en el consenso de Prueba de Participación (PoS). Los productores de bloques se llaman “panaderos”, y el proceso de cocción se denomina validación de bloques. Los mineros realizan la misma función que los mineros: protegen y gestionan la red, verifican y validan las transacciones y distribuyen las recompensas de los bloques. Pero en lugar de un costoso equipo de minería, todo funciona utilizando el consenso Prueba de Participación (PoS).

El objetivo de Tezos es ampliar la funcionalidad de bitcoin mediante contratos inteligentes. El equipo de Tezos se centra específicamente en crear una blockchain que facilite la adaptación y el cambio a través del consenso de la comunidad con una mínima interrupción de la red. Tezos funciona con un algoritmo Prueba de Participación (PoS). Técnicamente, la red utiliza una de las variantes de PoS, llamada prueba de participación delegada (DPoS).

La arquitectura de Tezos permite a los usuarios actualizar la red sin realizar bifurcaciones duras. El sistema se divide en tres módulos: el módulo de consenso, el módulo de transacciones y el módulo de red.

La blockchain de Tezos se autorregula, lo que garantiza un alto nivel de seguridad. Tampoco hay bifurcaciones duras en el sistema de Tezos.  En el lado negativo, el ancho de banda de la red es bajo en la plataforma Tezos. Entre otras desventajas, también podemos mencionar que la posibilidad de inflación es bastante alta porque la emisión de tokens es ilimitada. Según el libro blanco de XTZ, su sistema de gobernanza puede dar voz a cada usuario de Tezos, pero la centralización de la riqueza y la apatía de los usuarios pueden hacer que el sistema sea ineficiente del mismo modo que Bitcoin, Ethereum y EOS. Además, ningún sistema de gestión puede satisfacer las necesidades de todos los usuarios. En este caso, la única decisión es la que se toma, y existe una gran posibilidad de que se produzcan bifurcaciones debido a usuarios descontentos. Sin embargo, debido a su enfoque único del proceso de actualización y recogida de votos, la plataforma puede ser más flexible que algunos competidores. Esto es potencialmente una gran ventaja a largo plazo. Tezos ha recorrido un largo camino antes de su lanzamiento y nos da la esperanza de que XTZ sea útil tanto para el gobierno como para los usuarios comunes. [10]

**7. Criptomonedas más utilizadas en Cuba**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Cambio | | | |
| Criptomoneda | Dólares | Libra Esterlina | Euro | Peso Cubano |
| BTC | 20791.10 | 17881.28 | 20619.48 | 498545.43 |
| Ether | 1563.81 | 1344.70 | 1551.17 | 37417.77 |
| LTC | 20751.60 | 17840.46 | 20569.56 | 1342.53 |
| KBC | 0.000217 | 0.000187 | 0.000215 | 0.00530 |
| USTD | 0.997228 | 1.0579 | 1.003 | - |

**8. Diseño de una plataforma**

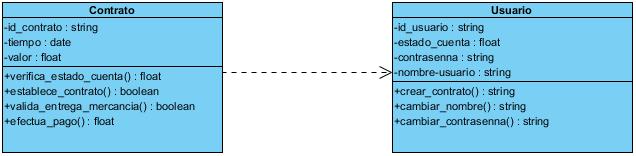
Se conformaría una blockchain con acceso a los estados de cuenta de la entidad donde sería la encargada de confirmar que se cuente con la suma necesaria para realizar el acuerdo y tomaría acciones en el caso de ser negativo el resultado de la verificación de estado.

El valor de la propuesta seleccionada para el diseño de la plataforma radica en que brinda la mejor solución a la problemática seleccionada como caso de estudio para esta investigación.

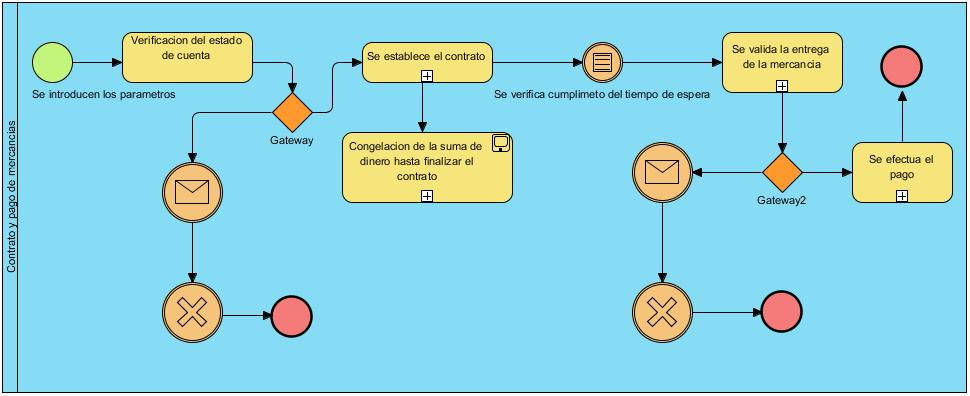
Al establecer el contrato se debe contar con 3 integrantes, garantizando de esta forma de que no queden parejas de opiniones en lo que respecta a la validación del correcto cumplimiento del contrato. Se establecerán 3 reglas, la fecha en la que se ejecutara el contrato, el monto por el cual se realizar y los integrantes que formaran parte del contrato; y al cumplimiento del 75% de las mismas (fecha y mención de las partes) se ejecutara el contrato.

El contrato no quedara establecido en la plataforma hasta que esta realice la verificación de los estados de cuento de la parte contratante de las mercancías, y se demuestre que cuente con la cantidad de dinero necesaria para el mismo y se congele dicha suma, garantizándose de esta forma que al culminar el contrato no se tengan respuestas negativas para efectuar el pago acordado por las partes.

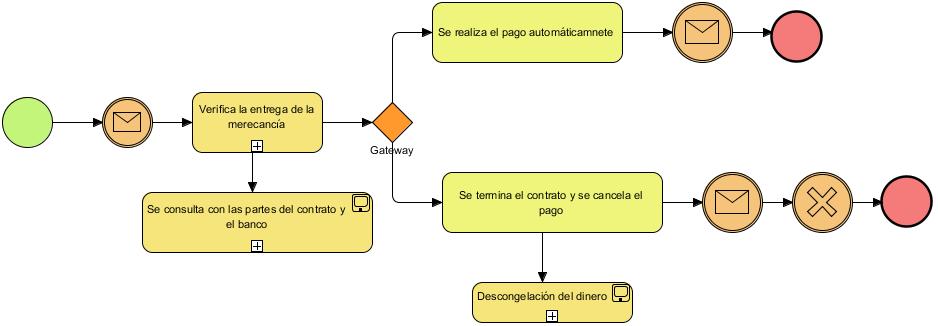
**8.1 Diagrama de clases**

****

**8.2 Diagrama de flujo**



**8.3 Diseño del protocolo o algoritmo de consenso para reconocer el cumplimiento de las condiciones.**

****

**8.4 Pseudocódigo**

Inicio:

Introducir las reglas:

* Fecha de culminación
* Monto del contrato
* Partes del contrato

;

Validación:

Si saldo de la cuenta >= monto del contrato:

Se establece el contrato

;

Si no:

Se notifica a las partes y se cancela el contrato

;

;

Se establece el contrato:

Se congela la suma correspondiente

;

Verificación de La fecha:

Si fecha del sistema == fecha de culminación:

Se notifica a las partes para verificar:

Si el número de aprobados > partes del contrato/2:

Se hace le pago y se notifica a las partes

;

Si no:

Se cancela el contrato y descongela el dinero

;

;

Si no:

En 24 horas se vuelve a verificar

;

;

Fin

**Conclusiones**

Se realizó una investigación de las plataformas de criptomonedas que viabilizaran la construcción de contratos inteligentes con ellas y a través del análisis de sus pros y contras se determinó cual era la más viable, a criterio de la autora de esta investigación, para el diseño y construcción de un contrato inteligente que sea viable para su implementación en nuestro país. También se realizó la propuesta de las herramientas a emplear para el desarrollo de la investigación y creación del contrato inteligente una vez escogida una de las 3 propuestas realizadas.

**Referencias Bibliográficas**

1. Martin, Pedro. 2021. Blockchain ¿Por qué y cómo surge? [https://visualeo.com/blockchian-por-que-y-como-surge/#](https://visualeo.com/blockchian-por-que-y-como-surge/)citado[02-05- 2022]
2. Universidad de Alcalá. Junio 2017. Historia de los Smart Contract. Citado[02-05-2022]
3. [Navarro](https://blog.addalia.com/author/wladimiro-navarro), Wladimiro. Jan 10, 2018. [*Smart Contracts o* Contratos Inteligentes ¿Qué son y para qué sirven?](https://blog.addalia.com/smart-contracts-nuevo-paradigma) <https://blog.addalia.com/smart-contracts-nuevo-paradigma/> [citado 30-9-2022]
4. Blockchain 2.0. 2022: *Los Smart Contracts* <https://enzyme.biz/blog/blockchain-2.0-los-smart-contracts> [citado 30-9-2022]
5. Nava González, Wendolyne y Morales Rocha, Víctor Manuel. Jun. 2021 Cumplimiento y ejecución de los acuerdos de transacción derivados de la mediación internacional a través de los contratos inteligentes. [https://www.scielo.cl/scielo.php?pid=S071925842021000100179&script=sci arttext](https://www.scielo.cl/scielo.php?pid=S071925842021000100179&script=sci%20arttext) citado [1-10-2022]
6. Padilla Sánchez, Jorge Alberto**.** Marzo 2020. Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos[\*](https://www.redalyc.org/journal/4175/417564980007/html/#fn76). <https://www.redalyc.org/journal/4175/417564980007/html/> citado [1-10-2022]
7. BC News Mundo. Septiembre 2022. Qué es "la fusión" de Ethereum y por qué aseguran que es "la mayor revolución en el mundo de las criptomonedas" desde el bitcoin. <https://www.bbc.com/mundo/noticias-62902390> citado [5-10-2022]
8. 2022. Sistema de gestión de *Smart Contract.* <https://contratosinteligentes.net/> citado [5-10-2022]
9. Vester, Juan. 2022. Cómo implementar un contrato inteligente ERC-20 en Avalanche con Infura. <http://dzone.com/articles/how-to-deploy-an-er-20-smart-contract-on-analanch> citado [17-10-2022]
10. Bit4you. 2022. <https://www.bit4you.io/> citado [23-10-2022]