Universidad Nacional Autónoma de México

Facultad de Ingeniería

Ingeniería en Computación

Cómputo Móvil

Equipo:06

Tarea 2: Blockchain aplicado a contratos inteligentes.

Profesor: Ing Marduk Pérez de Lara Domínguez

Fecha de entrega: 09/09/2022

Semestre 2023-1

Integrantes:

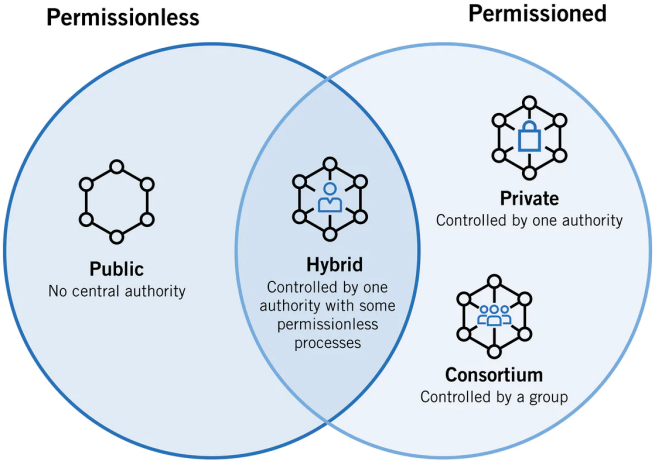
- Anizar Morales Víctor
- Avendaño Cabanillas Gustavo Eduardo
- Pérez Duarte Ana Patricia
- Villafañe Pérez Pamela Irais
- Torrecilla Jiménez Aarón Israel

ÍNDICE

Introducción

El blockchain es mayormente conocida por su aplicación en las criptomonedas, donde Bitcoin, es la más famosa de ellas. Sin embargo, el blockchain tiene un impacto en la industria más allá de las criptomonedas. En este documento conocerás en qué consiste la tecnología del Blockchain o traducido al español como cadena de bloques, para así conocer de qué trata esta tecnología de la que todo el mundo habla, con un enfoque en contratos inteligentes (smart contracts), la relación que tiene con el Cómputo Móvil y considerando cuáles son algunas de las aplicaciones que tiene esta tecnología y qué es lo que convierte en un factor de cambio. Además, aprenderás cómo a través de programas informáticos conocidos como “contratos inteligentes”, es posible crear aplicaciones no solo para el sector financiero, sino además, en ámbitos como la salud, los videojuegos, la cadena de suministro, e incluso en el arte.

Entonces, el BlockChain (concepto considerado como nuevo e innovador de los últimos años) es una tecnología que registra y comparte datos a través de una red, de manera muy similar a lo que hace el internet, con cuatro características: **inmutable**, es decir, una vez que una pieza dentro de la información es añadida, ya no puede ser modificada, **anónima**, se refiere a que protege tu identidad, **segura** ya que todos los registros están cifrados y por último estamos hablando de que es **distribuida**: se expande alrededor de todo el mundo y cada usuario tiene una copia de los datos.

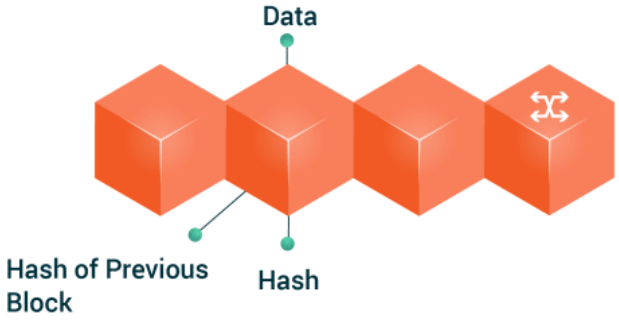


Hurtado, J. (2022, 4 marzo). *Funcionamiento de Blockchain*. IEBS. https://www.iebschool.com/blog/blockchain-cadena-bloques-revoluciona-sector-financiero-finanzas/

Existen varias formas de construir una red de blockchain: **privadas, públicas y autorizadas o construidas por un consorcio.**

- **Públicas**: es aquella en la que cualquiera puede unirse y participar, como por ejemplo bitcoin. Tiene la desventaja de requerir una gran potencia computacional, existe poca privacidad y la seguridad es débil.
- **Privadas:** esta es similar a una red pública, ya que es descentralizada entre pares ("peer-to-peer"), pero la diferencia es que una sola organización administra la red y controla quién tiene permiso de participar. Puede ejecutarse detrás de un firewall corporativo e incluso se puede alojar de forma local.
- **Autorizadas:** Las empresas que establecen una red privada de blockchain generalmente lo harán en una red de blockchain autorizada. Es importante señalar que las redes públicas de blockchain también pueden ser autorizadas. Esto impone restricciones en cuanto a quién puede participar en la red y en qué transacciones. Los participantes necesitarán una invitación o permiso para unirse.
- **Blockchain de consorcio:** Varias organizaciones pueden compartir las responsabilidades de mantener un blockchain. Estas organizaciones preseleccionadas determinan quién puede enviar transacciones o acceder a los datos. Un blockchain de consorcio es ideal para los negocios cuando todos los participantes deben estar autorizados y tienen una responsabilidad compartida respecto del blockchain.

La forma en que trabaja es que cada vez que algún miembro de la red realiza una transacción digital, dicha transacción genera unos datos asociados que quedarán almacenados en uno de los bloques. Cuando ese bloque está completo de información, el bloque se acopla a la cadena de bloques ya existente o blockchain.



Hurtado, J. (2022, 4 marzo). *Funcionamiento de Blockchain*. IEBS. https://www.iebschool.com/blog/blockchain-cadena-bloques-revoluciona-sector-financiero-finanzas/

La información que se almacena en dicha red dependerá del propósito para el que haya sido creada. Puede tratarse de una red que almacene datos de pago (moneda criptográfica o criptomonedas), información médica, datos logísticos o de trazabilidad de alimentos e inclusive recuento de datos electorales.

Pero bien, ¿cómo funciona esta tecnología?

La cadena de bloques es un registro de todas las transacciones, almacenadas y compartidas de forma pública. Los llamados mineros se encargan de verificar esas transacciones. Tras ello, se incluyen en la cadena y se distribuyen a los nodos que forman la red.

Veamos en qué consiste cada uno de estos elementos:

1. Bloques: Un bloque está constituido por un conjunto de transacciones. Cada uno forma parte de la cadena de bloques. La compañía Bit2me, especializada en el Bitcoin y su tecnología, define cada una de las partes que conforman un bloque:

    - Un código alfanumérico que enlaza con el bloque anterior.
    - El “paquete” de transacciones que incluye (cuyo número viene determinado por diferentes factores).
    - Otro código alfanumérico que enlaza con el siguiente bloque.

El siguiente bloque en progreso lo que intenta es averiguar con cálculos el código alfanumérico que permitía al anterior bloque enlazarse a éste.

2. Mineros: Los mineros son ordenadores/chips que se encargan de verificar todas las transacciones. Cuando alguien completa un bloque o realiza una transacción, recibe una recompensa en forma de Bitcoins.
3. Un nodo es un ordenador/chip que está conectado a la red Bitcoin. Se dedica a almacenar y distribuir una copia actualizada de la cadena de bloques. Por lo tanto, cada bloque nuevo que se confirma se añade a la cadena de bloques y a la copia que cada nodo almacena.

¿Qué son los Smart Contracts? Un contrato inteligente es una pequeña aplicación que se puede ejecutar por sí misma y obligar a cumplir ciertas reglas. Su objetivo principal es la optimización y eliminación de intermediarios, estas aplicaciones autónomas almacenan dentro de una red blockchain, los smart contracts permiten realizar transacciones que sean seguras, rastreables e irreversibles sin necesidad de intermediarios, esto ofrece una mayor seguridad a los contratos tradicionales y además reduce sus costos.

Eliminan el factor humano a la hora de tomar decisiones, y esto los convierte en un complemento o reemplazo de los contratos originales tal como los hemos conocido.

Estos contratos inteligentes también permiten almacenar, enviar y recibir fondos así como contactar con otros contratos. Utilizan una forma estructura muy sencilla “IF…THEN”, donde al ocurrir un evento predefinido el contrato ejecutará cierta acción.

Desarrollo

- Contexto histórico

El concepto de smart contract surgió entre 1994 y 1997, definido y propuesto por el informático norteamericano Nick Szabo, el cual definió como “un protocolo informático capaz de ejecutar cláusulas de un contrato”. (ESIC, 2018). Desde este momento en adelante fue un concepto e idea revolucionaria ya que permitía que desde la concepción de este tipo de contratos se visualiza que las relaciones entre comerciantes y entidades financieras fuera mucho más personal, sin demasiada burocracia ni mucho menos papeleo engorroso.

Nick Szabo propuso un modelo de contrato inteligente apoyado en un modelo de máquina expendedora el cual se resume en que “mediante la inserción del importe correspondiente en la ranura indicada y la introducción del código que identifica el producto que el consumidor desea adquirir, el comprador está proyectando su consentimiento para la adquisición del producto (formalización del contrato) y la máquina automáticamente ejecutará el contrato mediante la entrega y puesta a disposición del bien objeto del contrato de compraventa”. (Soler, Ana. 2019).

- Contexto actual

Tras la creación de las criptomonedas, en específico en el año 2009 junto con la criptomoneda bitcoin, los contratos inteligentes fueron tomando una gran relevancia en el mundo del blockchain y en general de todo el sistema de criptomonedas, ya que las criptomonedas recurrieron a la idea de los contratos inteligentes y los contratos inteligentes necesitaban a una moneda de la cual pudieran apoyarse para formalizar el contrato.

El número de contratos que se firman crece exponencialmente a diario, multiplicando los problemas y contratiempos que tradicionalmente llevan asociados los acuerdos tradicionales. (Soler, Ana. 2019). Es un hecho que el uso de los contratos inteligentes a la contratación masiva, por ejemplo, en la contratación de cuentas digitales de bancos podría ayudar a reducir dichas complicaciones contractuales a las que nos enfrentamos día a día, simplificando procesos y automatizando muchos aspectos bancarios.

Los usos más comunes que se vienen estudiando e intentando implementar integran desde acciones simples como votar una publicación en un sitio web, hasta acciones que conllevan procesos más rigurosos como garantías de préstamos y contratos de futuros, así como contratos sofisticados, por ejemplo, la fijación de prioridades de pago en notas estructuradas.

Por un lado, los contratos inteligentes pueden ser creados, además de por personas físicas y jurídicas, por máquinas o incluso otros programas que funcionan de forma autónoma. En tal sentido, tiene validez sin depender de autoridades. Esto se corresponde a su naturaleza: es un código visible e inmodificable debido a la tecnología blockchain. Esto le atribuye a las principales características de esta misma, que son: descentralizadas, imperturbables y transparentes.

Asimismo, son programas en la nube que actúan de igual manera y permiten acopiar información que no puede ser alterada. Son los programas más confiables y resguardados que un humano ha podido desarrollar, y sólo fallan cuando están mal programados.

- Relevancia en el sector de la Ingeniería en Computación

Entonces, de acuerdo a la definición proporcionada anteriormente, en este formato, los contratos se pueden convertir en código de computadora, almacenarse, replicarse en el sistema y ser monitoreados por la red de la computadora que ejecuta la cadena de bloques en la que se emiten los contratos. Los contratos inteligentes actuales, necesitan de modelos de desarrollo que permitan “automatizar las relaciones entre las diferentes partes que participan en las transacciones”, entonces, para lograr esto se tiene una nueva frontera, la cual se enfoca en aumentar la capacidad de conocer los significados para disminuir más el riesgo de error e “interpretación”.

Es así, que aportar conocimientos de semántica enfocado a los contratos inteligentes, permite tener una mayor precisión en el comportamiento de los mismos, además de tener una mayor precisión en la interpretación de los significados y acciones que los contratos inteligentes están llamados a gestionar. Es así que pasamos al concepto de “contrato automático” que consta de un automatismo inteligente, es decir, que está diseñado para aprender y modificar su comportamiento en función de las nociones adquiridas (inteligencia artificial).

A continuación, se describirán algunas plataformas que son más utilizadas para el desarrollo y ejecución de contratos inteligentes en blockchain:

- **Ethereum:** los contratos inteligentes se escriben en un lenguaje de programación llamado Solidity y son ejecutados por la máquina virtual de Ethereum. Es el más popular en la actualidad.
- **Hyperledger:** sistema *open source* desarrollado por Linux Foundation y que no es una criptomoneda, sino una plataforma flexible sobre la que pueden desarrollarse contratos inteligentes.
- **Counterparty:** esta plataforma incorpora datos a las transacciones de Bitcoin, es decir, utiliza el *blockchain* de esta criptomoneda y permite desarrollar contratos sobre ella.
- **Polkadot:** se trata de un *blockchain* alternativo y es famoso por su capacidad para albergar *parachains,* cadenas dentro de cadenas, que permiten realizar más transacciones de lo habitual. (Smart contracts: contratos inteligentes para formalizar acuerdos en la era digital, 2021).

Pérez, I. (2020, 30 abril). 4 plataformas de contratos inteligentes que todo desarrollador de blockchains debe conocer. https://www.criptonoticias.com/analisis-investigacion/contratos-inteligentes-desarrollador-blockchain-rsk-ethereum-cardano-eosio/

Podemos ver la historia y evolución de los contratos inteligentes junto con la tecnología de blockchain. En 2017 EOS.IO surgió como una plataforma de contrato inteligente y al mismo tiempo como un sistema operativo (SO) descentralizado, cuyo objetivo es el de fomentar el uso de aplicaciones descentralizadas, y una de esas aplicaciones sería la implementación de cadenas laterales.

Una cadena lateral es una cadena de bloques interoperable que se produce a partir del código de la cadena principal, pero que permite operaciones únicas e independientes. Esto no solo permite que las redes de la competencia compartan información para beneficio mutuo, sino que también permite que proyectos individuales establezcan múltiples blockchains con diferentes fortalezas y debilidades, y que utilicen cada una de ellas en el lugar donde pueden tener el mayor efecto. Este tipo de implementación con codificación de contrato inteligente podría ser interesante en un futuro próximo (NextCity Labs, 2021).

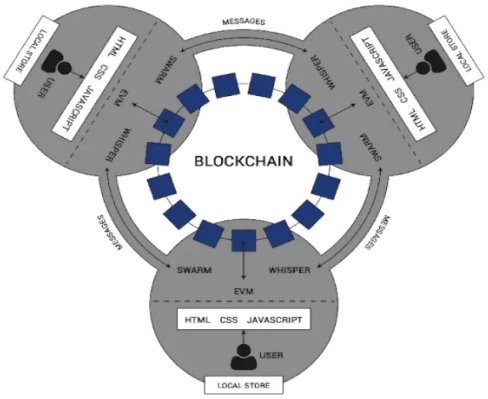
En conclusión, el futuro de los contratos inteligentes de la mano con la tecnología blockchain tienen una gran relevancia en el ámbito de la computación, debido a que hay distintas áreas relacionadas, como los programadores, desarrolladores de aplicación, y las áreas de inteligencia artificial y seguridad informática. Teniendo presente que la evolución de estos contratos se fusionaran en un híbrido de papel y con contenido digital, en donde dichos contratos se verificarán mediante blockchain y de igual manera en forma física.

- Relación con el Cómputo Móvil

La implementación de la tecnología BlockChain en las aplicaciones móviles ha traído un crecimiento cómo no se había visto antes, no solo hablando en temas de

desarrollo sino también hablando del tema económico y se han creado muchas nuevas oportunidades para las empresas y los desarrolladores independientes. Dentro de estas nuevas oportunidades podemos mencionar el desarrollo de aplicaciones descentralizadas, pero ¿De qué nos sirve el desarrollo de dichas aplicaciones? Pues bien estas aplicaciones nos pueden ayudar " eliminando el rol de entidades certificadoras terceras a la hora de realizar transacciones y automatizando acciones con el objetivo de reducir tiempos y costes."(Blanco Peris, Pablo ,2019).

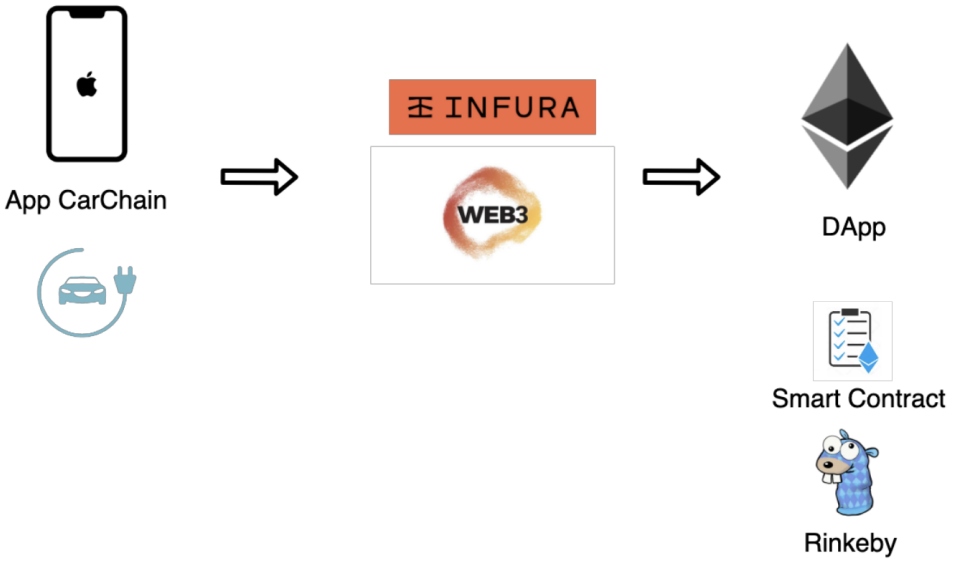
Algunos beneficios que podemos encontrar al utilizar smart Contracts en nuestras aplicaciones móviles son: Seguridad, descentralización, se basan en software libre.
La verdadera diferencia de estas aplicaciones se ve en el backend y màs específicamente en la forma en la que almacena la información, ya que en la mayoría de las aplicaciones convencionales los datos se guardan en un servidor central y al usar la tecnologìa del BlockChain te aseguras que esta información se guarde en la red de ordenadores. Cómo podemos ver en la siguiente imagen, los mensajes se encuentran en la BlockChain generando cierta seguridad de que esta información no será manipulada o accedida por terceros y llegará segura a su destino.



Saéz H.(2022, 25 Febrero). Qué son las DApps o Aplicaciones Descentralizadas y varios ejemplos. https://www.iebschool.com/blog/dapps-o-aplicaciones-descentralizadas-que-son-y-como-funcionan-finanzas/#:~:text=Para%20poner%20un%20ejemplo%20m%C3%A1s,miles%20de%20nodos%20o%20ordenadores

Para una mejor comprensión de cómo se aplican los contratos inteligentes en una aplicación móvil tomamos como ejemplo el trabajo desarrollado por Blanco Peris, Pablo (2019) *Interacción de un Smart contract con una app móvil.* En dónde muestra la arquitectura completa de una aplicación móvil. Cómo dijimos antes lo que

diferencia una app móvil que implementa contratos inteligentes es el backend. En la siguiente imagen podemos ver a la izquierda el frontend de la aplicación que se desarrolla de igual manera que en cualquier otra aplicación. En el centro podemos ver Infura y Web 3 que nos sirven para realizar la conexión entre el backend y el frontend. Del lado derecho podemos ver el backend de la aplicación, en este caso DApp es el acrónimo de Decentralized application y nuestro Smart contract se despliega sobre la red de blockchain de Rinkeby.



Blanco Peris, Pablo (2019) Interacción de un Smart contract con una app móvil. Recuperado 7 de septiembre de 2022, de https://eprints.ucm.es/id/eprint/57087/1/PabloBlancoPeris.pdf

- Apps existentes o que podrían existir en el mercado para este tema

La tecnología blockchain no se limita a un solo rubro, esta va desde sectores financieros, de salud, entretenimiento, hasta temas políticos.
En el área de la salud: el department the health y human service USA (departamento de salud y servicios humanitarios de Estados Unidos), desarrolló un sistema para reducir y dar transparencia a su proceso de adquisiciones,por ejemplo; en la compra de medicamentos, hacer alguna licitación, alguna obra del hospital, etc. Esto antes era un proceso lento que podría llevar días, además de poco confiable lo cual produjo una reducción de 200 a 90 días incrementando la transparencia.

Tiwari, Aisshwarya . (2019, 19 enero). BlockChain y el departamento de salud y servicios humanitarios de Estados Unidos . Cripto News. https://crypto.news/usa-blockchain-technology-revitalize-health-departments-contract-acquisition-function/

El Registro Público de la Propiedad de la República de Georgia en Europa, los cuales implementaron un certificado digital basado en esta tecnología del Blockchain con la cual los ciudadanos pueden verificar que son dueños de una propiedad, este proceso redujo los días a minutos.

En el ámbito financiero La aplicación que hizo el Banco Español BBVA, buscando reducir el tiempo y la complejidad de realizar transferencias internacionales. Este proceso se llevó a cabo por un programa piloto de proceso de compraventa de atún mexicano que se compraba en España, y se exportaba de México a España, en donde la verificación del pago que podía llegar a tardar varios días se redujo a tan solo unos segundos.

- Prospectiva (futuro de la tecnología)

Con toda esta nueva tecnología, la web 3.0, podemos tener soluciones que con la actual web (mejor conocida como web 2.0) no tenemos; la web 3.0 nos ofrece un control verdadero sobre nuestra información así como “privilegios monetarios”, esto, como ya se mencionó anteriormente, gracias a las bondades del Blockchain y las criptomonedas.

La tecnología blockchain puede ayudar a los usuarios a interactuar con diferentes servicios online bajo el gobierno de las conexiones punto a punto. Es importante mencionar que este tipo de conexión es una red descentralizada de computadoras; en vez de una red de servidores o equipos centralizados ubicados en una ubicación

en específico. Lo anterior tiene una gran ventaja, ya que elimina la necesidad de intermediarios.

Finalmente, podemos mencionar algunos grandes avances que se han logrado, así como nuevos desarrollos que están por venir:

1. Los sistemas de almacenamiento que antes estaban en Google Cloud, AWS, Microsoft azure; han ido migrando a sistemas de tipo IPFS, por sus siglas en inglés. IPFS es el Sistema de archivos Interplanetario, éste es un protocolo y una red diseñados para crear un método p2p para almacenar información en un sistema de archivos distribuidos.
2. Nuevos navegadores web como Brave presentan una alternativa descentralizada contra el popular navegador web de la web 2.0, Google Chrome.
3. La web 3.0 remarca los cambios en las finanzas con preferencias hacia las “cripto billeteras“, en vez de bancos convencionales.

Conclusiones

De forma simplificada podemos decir que el blockchain es como un gran libro de contabilidad inmodificable y compartido que van escribiendo una gran cantidad de ordenadores de forma simultánea. El carácter programable y abierto de esta tecnología permite innovar el sector financiero y los procesos administrativos para que sean más eficientes y transparentes, además que la burocracia disminuye.

En la actualidad hay transacciones comerciales tan complejas que se requieren de protocolos complejos para que se puedan materializar mediante los contratos inteligentes. Aún en la actualidad necesitamos de una ejecución manual, ya que aún es ineficiente o poco confiable la ejecución automática, debido a las dificultades de traducción, contexto y semántica del lenguaje natural al lenguaje de código.

Es así, que los contratos inteligentes introducen nuevos riesgos como error de programación y discrepancias entre la implementación del contrato y la intención de las partes, por lo que la mejor manera de crear un ambiente de regulación, consisten en regular a los intermediarios que participan en los sistemas involucrados con los contratos inteligentes.

Referencias

1. NextCity Labs. (2021, 22 julio). *¿Por qué importan los contratos inteligentes?* Recuperado 6 de septiembre de 2022, de https://nextcitylabs.com/global/en/por-que-importan-los-contratos-inteligentes/
2. Beillini, M. (2021, 16 noviembre). *Contratos Inteligentes: qué son, cómo funcionan y sus áreas de aplicación*. Innovación Digital 360. Recuperado 7 de septiembre de 2022, de https://www.innovaciondigital360.com/blockchain/contratos-inteligentes-que-son-como-funcionan-y-sus-areas-de-aplicacion/
3. *Smart contracts: contratos inteligentes para formalizar acuerdos en la era digital*. (2021, 22 abril). Iberdrola. Recuperado 7 de septiembre de 2022, de https://www.iberdrola.com/innovacion/smart-contracts#:%7E:text=Los%20contratos%20inteligentes%20se%20ejecutan,que%20automatiza%20pagos%20y%20contrapartidas
4. Molano, N. A. (2022, 27 abril). Claves para entender la tecnología 'blockchain'. BBVA NOTICIAS. Recuperado 7 de septiembre de 2022, dehttps://www.bbva.com/es/claves-para-entender-la-tecnologia-blockchain/
5. *¿Qué es la tecnología de blockchain? - IBM Blockchain | IBM*. (s. f.). Recuperado 7 de septiembre de 2022, de https://www.ibm.com/mx-es/topics/what-is-blockchain
6. Blanco Peris, Pablo (2019) Interacción de un Smart contract con una app móvil. Recuperado 7 de septiembre de 2022, de https://eprints.ucm.es/id/eprint/57087/1/PabloBlancoPeris.pdf
7. ESIC. Contratos Inteligentes: qué son, orígenes y principales aplicaciones. Recuperado el día 8 de septiembre de 2022 de: https://www.esic.edu/rethink/tecnologia/contratos-inteligentes-que-son-origenes-y-principales-aplicaciones
8. Soler Presas, Ana. LOS CONTRATOS INTELIGENTES: CONCEPTO, TRANSCENDENCIA JURÍDICA Y ALTERNATIVAS LEGALES TRADICIONALES DEL ORDENAMIENTO JURÍDICO ESPAÑOL. Recuperado el día 8 de septiembre de 2022 de: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/29418/TFG-Navarro%20Urosa%2C%20Marta%20Marila.pdf
9. Universidad de Alcalá. Historia de los Smart Contracts. Recuperado el día 8 de septiembre de 2022 de: https://masterethereum.com/historia-smart-contracts/#:~:text=%C2%BFCu%C3%A1ndo%20surgieron%20los%20Smart%20Contracts,limitaciones%20tecnol%C3%B3gicas%20de%20ese%20momento.