UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA
COMPUTO MOVIL

Blockchain aplicado a contratos inteligentes

González Nova Rafael Antonio
Hernández Ku Rogelio
Lara Mandujano Diego Abraham
Olguin Castillo Luis Angel
Tellez Gallardo Carolina

Grupo: 3
Profesor: Marduk Perez de Lara Dominguez
Semestre 2023-2
Fecha de entrega: Viernes 31 de Marzo del 2023

ÍNDICE

INTRODUCCIÓN

Una de las tecnologías más innovadoras que se ha desarrollado en los últimos años ha sido el blockchain, no solo por la versatilidad que tiene, también por la seguridad y confianza que ofrece a todas las empresas que la utilizan. Además su adaptabilidad hace que sea una de las tecnologías que más se están utilizando en múltiples industrias y esté conquistando más horizontes.

El término blockchain se puede traducir de manera literal por "cadena de bloques". En esta cadena (chain), cada bloque (block) está lleno de datos, es decir, la información se registra y se agrupa en bloques, y cada bloque funciona como un eslabón.

Blockchain se puede definir como un libro mayor compartido e inmutable que facilita el proceso de registro de transacciones y de seguimiento de activos en una red de negocios, en el cual los activos puede ser tangibles como por ejemplo: una casa, un auto, dinero en efectivo, terrenos o intangibles (propiedad intelectual, patentes, derechos de autor, marcas). Prácticamente cualquier cosa de valor puede ser rastreada y comercializada en una red de blockchain, reduciendo el riesgo y los costos para todos los involucrados.

Por otro lado, los contratos inteligentes o smart contracts son programas informáticos diseñados para ejecutarse automáticamente a medida que las personas o empresas involucradas en un acuerdo van cumpliendo con las cláusulas del mismo.

CONTEXTO HISTÓRICO

La idea detrás de la tecnología blockchain se describió en 1991, cuando los científicos de investigación Stuart Haber y W. Scott Stornetta introdujeron una solución computacionalmente práctica para los documentos digitales con sello de tiempo para que no pudieran ser modificados o manipulados.
El sistema usó una cadena de bloques con seguridad criptográfica para almacenar los documentos con sello de tiempo y en 1992 se incorporaron al diseño los árboles Merkle, lo que lo hizo más eficiente al permitir que varios documentos se reunieron en un solo bloque. Sin embargo, esta tecnología no se utilizó y la patente caducó en 2004, cuatro años antes del inicio de Bitcoin.
En 2004, el informático y activista criptográfico Hal Finney (Harold Thomas Finney II) introdujo un sistema llamado RPoW, Reusable Proof Of Work (Prueba de Trabajo reutilizable). El sistema funcionó al recibir un token de prueba de trabajo no intercambiable o no fungible basado en Hashcash y, a cambio, creó un token firmado por RSA que luego podría transferirse de una persona a otra.
RPoW resolvió el problema del doble gasto manteniendo la propiedad de los tokens registrados en un servidor confiable que fue diseñado para permitir a los usuarios de todo el mundo verificar su exactitud e integridad en tiempo real.
RPoW se puede considerar como un prototipo temprano y un paso inicial importante en la historia de las criptomonedas.
A finales de 2008, una persona o un grupo con el seudónimo Satoshi Nakamoto publicó en una lista de correo de criptografía un libro blanco que introdujo un sistema de efectivo electrónico descentralizado entre pares (llamado Bitcoin).
Basado en el algoritmo de Prueba de Trabajo de Hashcash, pero en lugar de utilizar una función de computación confiable de hardware como el RPoW, la doble protección contra gastos en Bitcoin fue proporcionada por un protocolo descentralizado de igual a igual para el seguimiento y la verificación de las transacciones. En resumen, los mineros individuales "minan" bitcoin para obtener una recompensa utilizando el mecanismo de prueba de trabajo y luego lo verifican los nodos descentralizados en la red.
El 3 de enero de 2009, Bitcoin nació cuando el primer bloque de bitcoin fue minado por Satoshi Nakamoto, que tuvo una recompensa de 50 bitcoins. El primer receptor de Bitcoin fue Hal Finney, recibió 10 bitcoins de Satoshi Nakamoto en la primera transacción de bitcoin del mundo el 12 de enero de 2009.

En 2013, Vitalik Buterin, programador y cofundador de la revista Bitcoin, declaró que Bitcoin necesitaba un lenguaje de scripting para crear aplicaciones descentralizadas. Al no lograr un acuerdo en la comunidad, Vitalik comenzó el desarrollo de una nueva plataforma de computación distribuida basada en blockchain, Ethereum, que presentaba una funcionalidad de scripting, llamada contratos inteligentes.
Los contratos inteligentes son programas o scripts que se implementan y ejecutan en la cadena de bloques Ethereum; se pueden usar, por ejemplo, para realizar una transacción si se cumplen ciertas condiciones. Los contratos inteligentes se escriben en lenguajes de programación específicos y se compilan en un código de bytes, que una máquina virtual completa de Turing descentralizada, llamada la máquina virtual Ethereum (EVM) puede leer y ejecutar.
Los desarrolladores también pueden crear y publicar aplicaciones que se ejecutan dentro de la cadena de bloques Ethereum. Estas aplicaciones generalmente se denominan DApps (aplicaciones descentralizadas) y ya existen cientos de DApps que se ejecutan en la cadena de bloques Ethereum, incluidas las plataformas de redes sociales, aplicaciones de juegos de azar e intercambios financieros.
La criptomoneda de Ethereum se llama Ether, se puede transferir entre cuentas y se usa para pagar las comisiones de la potencia de cálculo utilizada al ejecutar contratos inteligentes.

CONTEXTO ACTUAL.

Las blockchains todavía siguen siendo principalmente como base de las criptomonedas y tokens, pero la arquitectura sirve para aplicaciones en una diversidad de industrias.
Muchas de las más prometedoras aplicaciones de esta novedosa arquitectura de base de datos dependen de la tecnología de contratos inteligentes de la blockchain. Es la posibilidad de manipular la información de la blockchain con código ejecutable que está almacenado en bloques, lo que hace que la blockchain sea un sitio tan flexible para aplicaciones en una amplia gama de situaciones.
Las criptomonedas modernas dependen del anonimato, transparencia, inmutabilidad y seguridad de los ledgers (libros) abiertos basados en blockchain que funcionen como valiosos activos digitales. El principal caso de uso para las blockchains es el soporte de criptomonedas y tokens.

La arquitectura de base de datos de la blockchain es ideal para almacenar historiales médicos. Los usuarios reciben almacenamiento permanente de historiales médicos donde haya una conexión a internet. Pueden compartir el acceso con médicos y compañías de seguro con una simple transacción en línea, y los médicos que tengan los permisos correspondientes podrán incluir nueva información al historial.

Las aplicaciones basadas en blockchain pueden eliminar el riesgo de fraude al mismo tiempo que agilizan el reembolso por perdidas en la industria de los seguros. Registros inmutables de valor de propiedad, reclamos y reembolsos traería una muy necesaria visibilidad a la industria de seguros. Y los contratos inteligentes podrían reducir mucho del papeleo que se requiere para los pagos de seguros.

Fabricantes, vendedores y consumidores tienen interés en rastrear las cadenas de suministro desde sus fuentes originales hasta la cesta del consumidor. Ya sea que se verifique que los alimentos no contengan contaminantes inorgánicos o asegurar que las tasas de importación son pagadas en las aduanas, la blockchain pueden jugar un rol clave en el rastreo de productos a lo largo de su viaje desde la creación hasta el uso.

Una base de datos de blockchain es perfecta para almacenar registros de títulos, certificados de finalización, licencias y otras cualificaciones vocacionales. Esto es esencial para instituciones médicas y prácticas legales, donde contratar personas sin las credenciales correctas puede llevar al desastre

En el mundo de los videojuegos y las apuestas la tecnología blockchain puede proporcionar un registro que establece la aleatoriedad de los juegos de dados, de poker y de eventos de juegos. La blockchain puede registrar las fortalezas del jugador en juegos de rol y las ganancias en juegos de azar.

La distribución digital de música, películas y otras obras de arte es muy conveniente para los usuarios, pero tanto artistas como productoras se quejan la piratería desenfrenada. La distribución basada en blockchain podría hacer que cada copia de un archivo multimedia digital fuera único y proporcionara un conveniente mecanismo donde los espectadores hicieran micropagos directamente a los creadores o las productoras.

Bitcoin fue lanzado en el 2009, y tomo unos años para que emergiera la primera aplicación de blockchain no relacionada con una criptomoneda. Esta tecnología todavía está en pañales, pero, casos de uso ya muestran que puede ser implementada de forma rentable en una variedad de segmentos de mercado e industrias. Cuando se trata de casos de uso de blockchain, el cielo es el límite.

RELEVANCIA EN EL SECTOR DE LA INGENIERÍA EN COMPUTACIÓN

Blockchain es la tecnología más confiable en los últimos tiempos que atiende a nuestra responsabilidad de cumplir con las obligaciones de cumplimiento de TI. La tecnología Blockchain no solo protege los datos y las transacciones, sino que también simplifica los procesos involucrados en el desarrollo de productos de software.

Blockchain llegó para quedarse, y estamos viendo que cada vez más desarrolladores lo utilizan para crear sus aplicaciones. Ya no se trata solo de criptomonedas: se trata de descentralizar las cosas. Durante este tiempo hemos visto un aumento en la cantidad de Dapps o aplicaciones descentralizadas que se están desarrollando. Estas aplicaciones están construidas con tecnología blockchain, lo que les permite ser utilizadas por múltiples usuarios sin necesidad de un servidor central.

La maduración tecnológica y el conocimiento en profundidad de sus principios, permitió que Blockchain sea extrapolada a casos de uso que excedan el sector financiero para el cual fue originalmente ideada. La incorporación de programas ejecutados en ella, llamados Smart Contracts o Contratos Inteligentes, potenciaron su alcance haciendo posible redefinir múltiples procesos, convirtiendo a esta tecnología en la candidata por excelencia para aquellos sistemas que precisan de confianza, seguridad, transparencia, eficiencia y reducción de costos operativos.

De esta manera gracias a la tecnología blockchain y las aplicaciones descentralizadas, pueden generar un cambio de paradigma en el sector del desarrollo de software. Si creamos un ecosistema basado en blockchain, se maximizará el valor del proceso de extremo a extremo. Como los componentes clave de blockchain se pueden combinar con el desarrollo de software, existe un gran potencial para que la tecnología pueda transformar la industria.

Sin embargo, el punto crítico en este contexto, es la ausencia de buenas prácticas de la ingeniería en software que utilizan los desarrolladores durante la construcción de las aplicaciones, lo cual se traduce directamente en productos resultantes de baja calidad, fruto de procesos impredecibles, mal controlados y reactivos.

RELACIÓN CON EL CÓMPUTO MÓVIL

El cómputo móvil y los contratos inteligentes están estrechamente relacionados, ya que el cómputo móvil proporciona una plataforma para ejecutar contratos inteligentes de forma descentralizada y en tiempo real.

El cómputo móvil permite que estos contratos inteligentes se ejecuten en dispositivos móviles, lo que significa que los usuarios pueden acceder y gestionar sus contratos desde cualquier lugar y en cualquier momento. Además, el cómputo móvil también permite la integración de múltiples tecnologías y servicios en los contratos inteligentes, lo que puede mejorar su funcionalidad y aumentar su valor.

El cómputo móvil proporciona la plataforma y la infraestructura necesarias para ejecutar contratos inteligentes de forma segura y eficiente en dispositivos móviles, lo que puede mejorar la accesibilidad, la eficiencia y la seguridad de los acuerdos comerciales y financieros.

El cómputo móvil permite la ejecución de una amplia variedad de servicios de contratos inteligentes, que pueden incluir:

- Pagos móviles: Los contratos inteligentes pueden utilizarse para automatizar los pagos móviles, lo que significa que los usuarios pueden realizar transacciones financieras desde sus dispositivos móviles sin necesidad de intermediarios.
- Identidad digital: Los contratos inteligentes pueden utilizarse para gestionar y verificar la identidad digital de los usuarios, lo que puede mejorar la seguridad y la privacidad de las transacciones.
- Gestión de activos: Los contratos inteligentes pueden utilizarse para gestionar y rastrear activos digitales, como criptomonedas, tokens y otros activos digitales, lo que puede mejorar la eficiencia y la transparencia de las transacciones.
- Contratos de seguros: Los contratos inteligentes pueden utilizarse para automatizar los procesos de reclamación y pago de seguros, lo que puede mejorar la eficiencia y la transparencia de la industria del seguro.

- Gobernanza empresarial: Los contratos inteligentes pueden utilizarse para automatizar los procesos de toma de decisiones en una organización, lo que puede mejorar la eficiencia y la transparencia de la gobernanza empresarial.

El cómputo móvil también puede ser utilizado para crear aplicaciones descentralizadas (dApps) que ejecutan contratos inteligentes. Estas aplicaciones pueden ser utilizadas para realizar transacciones financieras, gestionar identidades digitales, o ejecutar procesos de votación, entre otras cosas.

Las aplicaciones descentralizadas, también conocidas como dApps, son programas informáticos que se ejecutan en una red descentralizada, como una cadena de bloques. A diferencia de las aplicaciones tradicionales que se ejecutan en servidores centralizados, las dApps utilizan la tecnología de la cadena de bloques para ejecutar procesos de forma distribuida y segura, sin la necesidad de intermediarios.

Las dApps utilizan contratos inteligentes, además, las dApps no dependen de un servidor centralizado, lo que significa que no pueden ser controladas por una sola entidad o empresa.

APPS PARA CONTRATOS INTELIGENTES

Ethereum: Es una plataforma blockchain descentralizada que permite la creación y ejecución de contratos inteligentes. Esta utiliza su propio lenguaje de programación llamado Solidity para desarrollar contratos inteligentes.

Trust Wallet: Es una billetera de criptomonedas que permite a los usuarios almacenar, enviar y recibir criptomonedas, incluyendo tokens ERC-20 en la blockchain de Ethereum; a su vez, ofrece una funcionalidad de navegador dApp integrado que permite a los usuarios interactuar con contratos inteligentes directamente desde la aplicación.

Coinbase Wallet: Es una billetera de criptomonedas que también permite a los usuarios almacenar, enviar y recibir criptomonedas y tokens ERC-20 en la blockchain de Ethereum. Coinbase Wallet también ofrece una funcionalidad de navegador dApp integrado que permite a los usuarios interactuar con contratos inteligentes.

MetaMask: Es una extensión de navegador web que permite a los usuarios interactuar con la blockchain de Ethereum y sus contratos inteligentes. También tiene una aplicación móvil que funciona como una billetera de criptomonedas y un navegador dApp.

MyEtherWallet: Es una billetera de criptomonedas que permite manipular y gestionar criptomonedas, al igual que tokens ERC-20. También tiene una funcionalidad de navegador dApp integrado que permite a los usuarios interactuar con contratos inteligentes directamente desde la aplicación.

PROSPECTIVA

Los contratos inteligentes y la tecnología blockchain han sido una de las innovaciones más revolucionarias en el ámbito tecnológico de los últimos años. A medida que la tecnología avanza y la adopción de blockchain se generaliza, su aplicación en aplicaciones móviles se vuelve cada vez más relevante y prometedora.

En la actualidad, existen múltiples proyectos que se enfocan en la implementación de contratos inteligentes y blockchain en aplicaciones móviles. Estas aplicaciones pueden proporcionar numerosas ventajas en términos de seguridad, transparencia y automatización, así como nuevas oportunidades para el desarrollo de modelos de negocio innovadores.

Una de las aplicaciones más prometedoras de los contratos inteligentes y la tecnología blockchain en las aplicaciones móviles es en la gestión de identidad digital. Actualmente, la gestión de identidades digitales es un proceso complejo y costoso, que a menudo requiere una gran cantidad de recursos y tiempo. Con la implementación de contratos inteligentes y blockchain, es posible crear una identidad digital descentralizada, que proporciona un alto nivel de seguridad y privacidad para los usuarios, a la vez que reduce los costos y la complejidad de la gestión de identidades digitales.

Otra aplicación importante de los contratos inteligentes y blockchain en las aplicaciones móviles es en la gestión de pagos y transacciones. Las aplicaciones móviles pueden utilizar contratos inteligentes para automatizar y gestionar pagos en tiempo real, lo que permite a los usuarios realizar transacciones seguras y rápidas. Además, la implementación de blockchain en la gestión de pagos puede proporcionar una mayor transparencia y trazabilidad en las transacciones, lo que ayuda a reducir los fraudes y aumenta la confianza en el sistema.

Otro ámbito en el que los contratos inteligentes y blockchain pueden tener un gran impacto en las aplicaciones móviles es en la economía colaborativa. La economía colaborativa se basa en la idea de compartir y colaborar en lugar de competir, y los contratos inteligentes y blockchain pueden proporcionar una plataforma segura y transparente para facilitar estas transacciones. Las aplicaciones móviles pueden utilizar contratos inteligentes para gestionar acuerdos entre diferentes partes, estableciendo reglas claras y transparentes para la colaboración.

Además de estas aplicaciones, existen muchas otras posibilidades para la implementación de contratos inteligentes y blockchain en aplicaciones móviles. Por ejemplo, la gestión de activos digitales, la creación de marketplaces descentralizados, la automatización de procesos empresariales y la gestión de derechos de autor son solo algunas de las áreas en las que la tecnología blockchain puede proporcionar soluciones innovadoras.

CONCLUSIONES

Las actividades relacionadas con la implementación del blockchain dirigido a las criptodivisas han sido una manantial de dinero que han significado un cambio de paradigma multinivel para todo el mundo, en lo que a formas de pago y hacer negocios se refiere. Esto debido a que es un sistema descentralizado que no depende de un gobierno o institución, y que como se expuso anteriormente, este se implementa como un sistema distribuido que cualquier persona con una computadora lo suficientemente potente puede llegar a implementar para así pasar a formar parte de los miles de usuarios que respaldan y dan cabida a la existencia de este sistema. No es de extrañar que tendrá grandes impactos en un futuro que ya nos ha alcanzado, pues por ejemplo, algunos países se han visto beneficiados de este tipo de nuevos sistemas económicos. Tal es el caso de Rusia, que a principios del año (2022), fue castigado por un sector de la comunidad internacional con sanciones económicas, de las cuales destaca que ha sido excluido del Sistema Swift, esto a razón de la invasión militar sobre su país vecino Ucrania. El Sistema Swift es el encargado de permitir negociar en los mercados internacionales en dólares. Beneficiosamente, Rusia ha logrado paliar en parte esta carencia haciendo uso de criptodivisas que están descentralizadas.

Por otro lado, se hace notar como la habilidad de la programación o bien la habilidad de saberse comunicar con IA’s será pilar fundamental para las generaciones futuras, pues este tipo de inteligencia artificial blanda, comienza a permear en rubros como la toma de decisiones legales, implementando en su forma de contratos

inteligentes. Se advierte así pues, que ingenieros en software que conozcan sobre estos temas así como de derecho, o bien, logren trabajar a la par de expertos en el tema legal, se harán de un nicho de mercado el cual se le puede asegurar con casi total seguridad, tendrá una cantidad de trabajo impresionante.

No obstante, los sistemas relacionados con el blockchain tienen un gran talón de Aquiles, pues su explotación y uso le representan a la humanidad una carga ingente de recursos energéticos. Gran premio se llevará a la persona que logre encontrar una forma alternativa de realizar los cálculos necesarios para hacer posible esta técnica. De otra manera, sistemas como el blockchain deberían considerarse inviables por ser una bofetada ecológica en un mundo que cada día se puede dar menos el lujo de ser contaminado.

Referencias

- Coinbase. (2018). Coinbase Wallet: Cryptocurrency Wallet & DApp Browser. [Aplicación móvil]. Recuperado de https://www.coinbase.com/mobile
- Defiapps. (2021). ¿Qué son las DApps? 11 principales en 2023 – Defiapps. https://defiapps.es/dapps/
- Evaluando Software. (2021). Blockchain: Cómo hacer contratos inteligentes o smart contracts. Evaluando Software. https://www.evaluandosoftware.com/blockchain-contratos-inteligentes-smart-contracts/
- Ethereum. (26 de septiembre de 2022). Decentralized Applications (dApps). https://ethereum.org/en/developers/docs/dapps/
- MetaMask. (2016). MetaMask. [Aplicación móvil]. Recuperado de https://metamask.io/
- MyEtherWallet. (2015). MyEtherWallet. [Aplicación móvil]. Recuperado de https://www.myetherwallet.com/
- Viktor Radchenko. (2017). Trust Wallet. [Aplicación móvil]. Recuperado de https://trustwallet.com/
- Zamora Fernando (2019). Hacia una ingeniería de software orientada al blockchain. Universidad siglo XXI. https://repositorio.uesiglo21.edu.ar/handle/ues21/17873
- International Business Machines Corporation. ¿Qué es el blockchain?. Recuperado de https://www.ibm.com/mx-es/topics/what-is-blockchain