IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS ENFOCADAS EN EL USO DE BLOCKCHAIN PARA PROTEGER DATOS

AUTOR

FRANCISCO JAVIER BRAVO ACEVEDO

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

FACULTAD DE INGENIERÍA

TECNOLOGÍA EN DESARROLLO DE SOFTWARE

MEDELLÍN

2022

IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS ENFOCADAS EN EL USO DE BLOCKCHAIN PARA PROTEGER DATOS

AUTOR

FRANCISCO JAVIER BRAVO ACEVEDO

Trabajo de grado para optar al título de

TECNÓLO EN DESARROLLO DE SOFTWARE

Asesor Técnico

MSc. OSCAR JULIÁN GALEANO ECHEVERRI

Asesor Metodológico

MSc. OSCAR IGNACIO BOTERO HENAO

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

FACULTAD DE INGENIERÍA

TECNOLOGÍA EN DESARROLLO DE SOFTWARE

MEDELLÍN

2022

Contenido

Lista de figuras

Pág.

Resumen

IMPLEMENTACIÓN DE NUEVAS TECNOLOGÍAS ENFOCADAS EN EL USO DE BLOCKCHAIN PARA PROTEGER DATOS

FRANCISCO JAVIER BRAVO ACEVEDO

Básicamente gran parte de mi motivación para realizar esta investigación se debe a mi gran interés por las nuevas tecnologías y más con tecnologías que ayudan a que la información sea más segura como lo es la blockchain ya que tiene mucho potencial y que poco a poco se ha ido posicionando en el ámbito empresarial.

Adicional esta investigación se hizo con el fin de ayudar a muchas mas personas a tener un concepto claro sobre blockchain resolver dudas acerca de lo que se puede lograr con esta tecnología y demostrar que se puede guardar información de una manera más descentralizada. El método que se usó para esta investigación fue un método de simulación donde por medio de un smart contract (contrato inteligente) y una blockchain privada a nivel local se logrará registrar datos utilizando una billetera como conexión a la red blockchain de prueba y estos datos se almacenaban en bloques con un identificador único (hash).

Lo que se encontró con esta investigación fue lo esperado y lo que se había planteado directamente con el método de simulación el cual cuando se ejecuta el smart contract los registros fueron tomados de inmediato y sin tener que depender de un servidor central estos datos quedaron almacenados de una manera muy descentralizada lo cual se demuestra que no solo la blockchain se usa para guardar transacciones con criptomonedas, sino que por medio de estos contratos se puede lograr guardar documentos información personal, imágenes (NFT) etc.…

Palabras Clave: Blockchain, Smart contract, Hash, NFT, Criptomoneda

Abstract

IMPLEMENTATION OF NEW TECHNOLOGIES FOCUSED ON THE USE OF BLOCKCHAIN TO PROTECT DATA

FRANCISCO JAVIER BRAVO ACEVEDO

Basically, a large part of my motivation to carry out this research is due to my great interest in new technologies and more with technologies that help make information more secure, such as the blockchain, since it has a lot of potential and that little by little it has has been positioning itself in the business world.

Additionally, this research was done in order to help many more people to have a clear concept about blockchain, resolve doubts about what can be achieved with this technology and demonstrate that information can be stored in a more decentralized way. The method used for this research was a simulation method where, through a smart contract (intelligent contract) and a private blockchain at the local level, data was recorded using a wallet as a connection to the test blockchain network and this data was stored in locks with a unique identifier (hash).

What was found with this investigation was what was expected and what had been raised directly with the simulation method which, when the smart contract was executed, the records were taken immediately and without having to depend on a central server, these data were stored automatically. a very decentralized way which shows that not only the blockchain is used to save transactions with cryptocurrencies but that through these contracts it is possible to save documents, personal information, images (NFT) etc...

Keywords: Blockchain, Smart contract, Hash, NFT, Cryptocurrency

Keywords: SCORM,

Glosario

Aplicación descentralizada: software o programa informático que funciona dentro de una cadena de bloques pública y cuyas interacciones se realizan mediante la transferencia de criptomonedas o tokens que se registran sin una entidad central de control.

Blockchain: se trata de una enorme base de datos que recoge y almacena la información de manera compartida y descentralizada.

Bitcoin: es una criptomoneda o moneda virtual, concretamente la primera que fue desarrollada.

Bloque: un bloque es un concepto pensado para optimizar el proceso de validación de las transacciones que se realizan.

Billetera de criptomonedas: en realidad es una interfaz de usuario que te permite acceder a la información de tus criptomonedas que están en la blockchain subyacente, recibir fondos de otros usuarios y enviar fondos a otras personas escribiendo las transacciones en la blockchain.

Criptomoneda: también llamada moneda virtual, es un tipo de moneda digital que solo existe electrónicamente.

Corda: es un software de registro distribuido que procesa y registra datos para promover un entorno de red descentralizado.

Contratos inteligentes: se trata de un algoritmo electrónico que se configura sobre una cadena de bloques para cumplir con un acuerdo previamente establecido entre dos o más partes. Una vez que las condiciones se cumplen, se ejecuta una tarea digital o transacción automática.

Descentralización: es el proceso de dispersar funciones, poderes, personas o cosas fuera de una ubicación o autoridad central.

DoS (ataque): por sus siglas en inglés «**D**istributed **D**enial **o**f **S**ervice», en español «ataque de denegación de servicio distribuido». Se refiere a una ampliación del ataque DoS, en la cual se satura un servidor realizando muchas peticiones desde distintos puntos de la red, comprometiendo la estabilidad y disponibilidad del servicio.

Ethereum: red con blockchain y con criptomoneda propia que permite la creación y ejecución de contratos inteligentes y aplicaciones descentralizadas. Fue creada en 2015 por Vitalik Buterin.

Ethereum Virtual Machine (EVM): es una máquina virtual donde se pueden ejecutar de manera segura los contratos inteligentes y protocolos de Ethereum.

Gas: específicamente dentro de la cadena de Ethereum, el gas es la unidad que mide el trabajo de cómputo necesario para llevar a cabo transacciones y contratos inteligentes. El gas no es un criptoactivo, sino una abstracción: ese trabajo se paga a los mineros en ETH.
Hash: es un algoritmo que cuenta con ciertas propiedades útiles para el cifrado de datos, esto es, proteger contenidos mediante el uso de claves.
Hyperledger (Project): es un proyecto colaborativo administrado por la Fundación Linux, cuya meta es la creación y desarrollo de cadenas de bloques diseñadas especialmente para cubrir necesidades empresariales.
Nodo: en redes de computadoras, se refiere a un ordenador o servidor conectado a la red, que es capaz de transmitir información a otros. Una blockchain descentralizada está compuesta por múltiples nodos.
NFT: es un certificado digital de autenticidad que mediante la tecnología blockchain, la misma que se emplea en las criptomonedas (los tokens), se asocia a un único archivo digital. recibir fondos de otros usuarios y enviar fondos a otras personas escribiendo las transacciones en la blockchain.
Prueba de Participación (PoS): protocolo de consenso distribuido en el que las transacciones son procesadas probando la posesión de las propias criptomonedas.
Prueba de Trabajo (PoW): protocolo de consenso distribuido consistente en la resolución de problemas matemáticos, en específico, una secuencia hash que tiene una variable que lo dificulta.

Solidity: es un lenguaje de programación basado en JavaScript, Python y C++, especialmente diseñado para crear contratos inteligentes. Es el más popular en su área y fue creado en 2014 para Ethereum en específico.

Token: En el mundo de las criptomonedas, es una moneda digital construida con criptografía que depende de la blockchain de otra moneda para existir, así que se rige por sus reglas.

Introducción

La presente investigación parte del conocimiento de una tecnología disruptiva que viene cambiando el mundo como lo es la blockchain donde por medio de la descentralización se puede lograr que un sistema de seguridad sea cada vez más confiable y no tan vulnerable a los ataques informáticos ya que como su nombre lo indica es una cadena de bloques y si un bloque es alterado con información diferente a la original la cadena se rompe pues cada bloque está conformado por un hash nuevo y hash anterior del bloque lo que lo hace casi imposible de alterar.

Por eso en este énfasis investigativo se encuentran varios temas como los son los tipos de blockchain que existen, smart contracts, dapps (aplicaciones descentralizadas) y adicional se dará a conocer una simulación en tiempo real de cómo funciona una blockchain privada utilizando un smart contract para registrar, actualizar y eliminar datos.

1. Planteamiento del problema

1.1 Descripción

En el mundo digital se sabe que hay muchas falencias en la seguridad y protección de datos e información a los cuales se ven expuestos millones de personas y empresas. En este orden de ideas se dará a conocer cuáles son los beneficios de utilizar nuevas tecnologías como lo sería la blockchain para la seguridad de la información y protección de futuros ataques cibernéticos.

A lo largo del tiempo son muchas las empresas que han sufrido ataques de hackers explotando vulnerabilidades y robando datos de usuarios, generalmente arremeten contra empresas grandes de talla mundial tales como: Sony, Samsung, Mercado Libre, eBay, etc.

Estas amenazas afectan económicamente e incluso pueden llevar a la quiebra a empresas que sean poco estables en el mercado y sigue pasando el tiempo y cada vez son más numerosos lo hackeos, es una problemática que quizás nunca acabara, pero si se puede llegar a minimizar.

Una de las noticias más recientes fue el ataque cibernético que sufrió la empresa mercado libre donde fueron expuestos datos sensibles de los usuarios, obligándolos a cambiar sus credenciales de seguridad por temor a un nuevo hackeo y exposición de sus datos personales.

En este caso me enfocare en la sistema de seguridad del centro de distribución de una empresa de productos de higiene ,este centro de distribución lleva más de 10 años ofreciendo una muy buena calidad en servicios de transporte de mercancía para los clientes y destaca por su rapidez a la hora de entregar los productos pero aunque su sistema nunca ha sido vulnerado no está excluido de que algo pueda pasarle además que todavía la información de los clientes se maneja de manera muy básica en archivos de Excel por lo que cualquier persona con conocimientos mínimos de informática puede acceder a estos datos y robar información.

Por consiguiente, se busca dar una solución y así evitar que en un futuro estos datos sean vulnerados y afecten la imagen de la empresa (la nación, 2022).

1.2 Formulación

¿Cómo una blockchain privada puede ser la solución a los problemas de ciberseguridad?

2. Justificación

En una cultura como la nuestra donde las empresas no tienen un amplio conocimiento sobre el uso de una blockchain privada y sus beneficios al implementar está a su sistema de seguridad, es necesario un soporte que sirva de base para entender la problemática.

Debido a esto me surge la necesidad de realizar una amplia investigación e implementación referente a las blockchain privadas, teniendo como referente los millones de ataques que sufren a diario cada una de las empresas colombianas, contando con una guía útil que ayudara a muchas personas que están interesados en el tema y lo quieran aplicar a sus negocios.

A causa de que la tecnología está en una constante evolución se pretende dar una solución y aclarar dudas a esta empresa de productos de aseo y a todos aquellos que deseen conocer sobre esta estrategia acerca de la seguridad de la información con la ayuda de blockchain privadas.

3. Objetivos

3.1 Objetivo general

Desarrollar una investigación e implementación acerca de las blockchain privadas para minimizar los ataques cibernéticos a empresas.

3.2 Objetivos específicos

- Indicar cuántas empresas utilizan blockchain privadas en sus sistemas de seguridad.
- Analizar con qué frecuencia son los ataques cibernéticos para su debida implementación.
- Determinar qué tan efectiva es esta tecnología en el uso empresarial.
- Calificar el impacto que generaría esta tecnología en la industria colombiana.

4. Marco teórico

La tecnología está en una constante evolución, el uso de la blockchain también conocida como “cadena de bloques” permite que él envió de datos digitales estén codificados de una forma totalmente segura. En la actualidad, muchas empresas han innovado con esta técnica y será fundamental en el futuro de las redes digitales.

Las blockchain públicas y blockchain privadas son constantemente confundidas, ya que son muy similares. Por ejemplo, ambas son redes que comparten un registro inmutable de transacciones. La diferencia real, a nivel técnico, es quién tiene acceso a ellas.

La blockchain privada solo los que tienen permiso pueden acceder a ella. El acceso a una cadena de bloques privada necesita de una invitación, que a su vez debe ser validada por la red o a través de parámetros de seguridad que son establecidos. Esta iniciativa es adoptada por las empresas para hacer uso de los beneficios de la tecnología blockchain, pero siempre manteniendo el control sobre la red y los datos que se ingresan a esta. El ejemplo de blockchain privada más conocido son Corda o Hyperledger Fabric, resaltando que esta cadena de bloques es liviana y tiene una mayor velocidad.

La blockchain privadas, estas se usan generalmente para el uso empresarial. La razón es el control, es decir, están controladas por un grupo de usuarios que pueden autorizar o rechazar permisos, alterar reglas, revertir transacciones y modificar saldos (esan business, 2019).

Entre sus ventajas más destacadas será: su rendimiento es mayor por ser una blockchain privada ya que al limitar el ingreso de las personas que van a participar en la red, el envío de datos se efectúa más rápido.

Este tipo de blockchain es más confiable ya que identifica a cada usuario que ingresa en la red, además el uso de esta no requiere ningún tipo de incentivo económico ya que el usuario de esta no debe pagar ninguna comisión por usar la red.

Una de sus desventajas sería la descentralización, esto quiere decir que red va a estar alojada en un servidor centralizado y es dirigida por una sola entidad. Otra de sus desventajas es que no es inmutable ya que se puede modificar la información o alterar solo si los nodos o usuarios participantes de esta red están de acuerdo, lo que quiere decir que debe de haber un consenso para modificar esta cadena de bloques (BSM BLOCKCHAIN SCHOOL MANAGEMENT, 2021).

El rápido progreso de las blockchain autorizadas y el interés de las grandes empresas se están apresurando en el camino para el desarrollo de más cadenas de bloques privadas, teniendo el poder de revolucionar muchos aspectos de la vida cotidiana.

4.1 Blockchain privado para el almacenamiento empresarial

La inmutabilidad y la trazabilidad de los datos son algunas de las ventajas que aporta la tecnología blockchain, gracias a la existencia de un libro mayor distribuido, del que hay una copia en cada nodo que forma parte de la cadena de bloques. Así, cualquiera de sus integrantes, ya sean los originarios o los nuevos usuarios, cuenta con una copia de ese libro, que sirve para verificar la veracidad de cualquier transacción de información. Esto garantiza la inmutabilidad de los datos y un control exhaustivo de cualquier cambio que se haya realizado en ellos, pero tiene una contrapartida importante, que es el bajo rendimiento en todos los procesos (almacenamientoit, 2020).

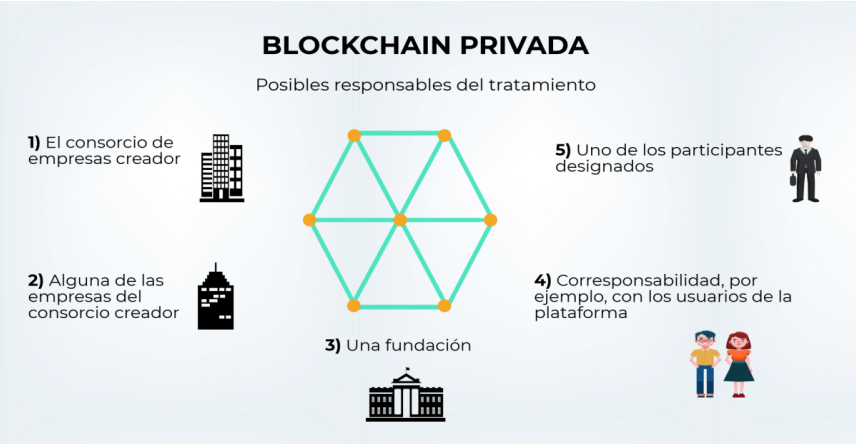


Figura 1. Blockchain privada.
Fuente: https://adefinitivas.com/arbol-del-derecho/nuevas-tecnologias/quien-es-el-responsable-del-tratamiento-en-blockch/

Esta imagen representa el cambio de la internet de pasar a de una web 1.0 a una web 3.0

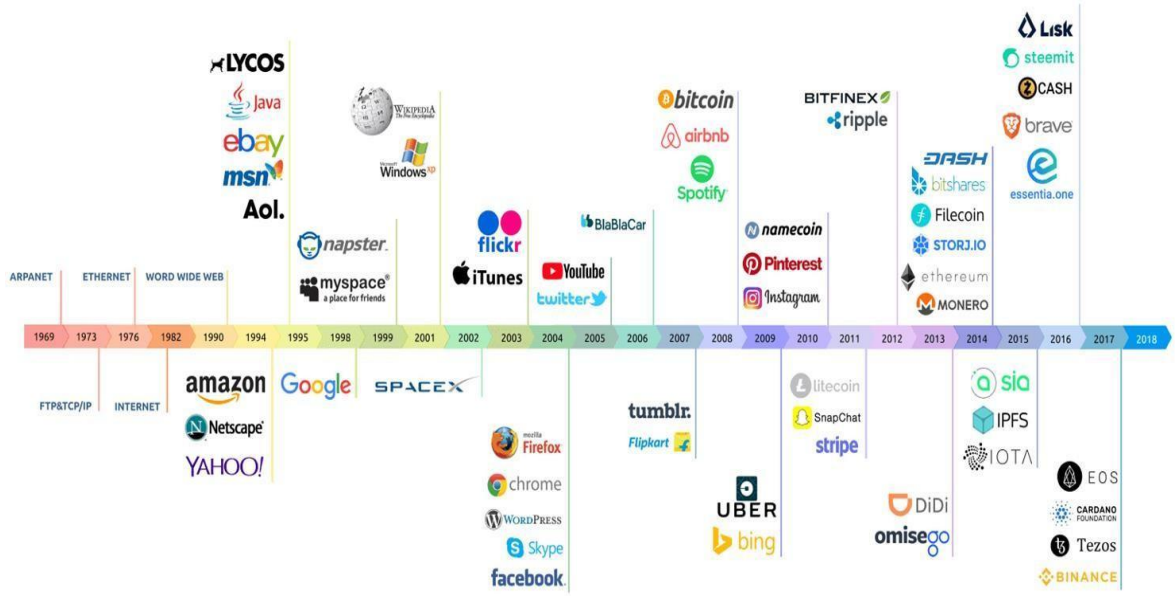


Figura 2. Cambio de web 1.0 a web 3.0
Fuente: https://acrobat.adobe.com/id/urn:aaid:sc:VA6C2:74c2fc8c-585f-4742-9beb-2251ab5bc33f

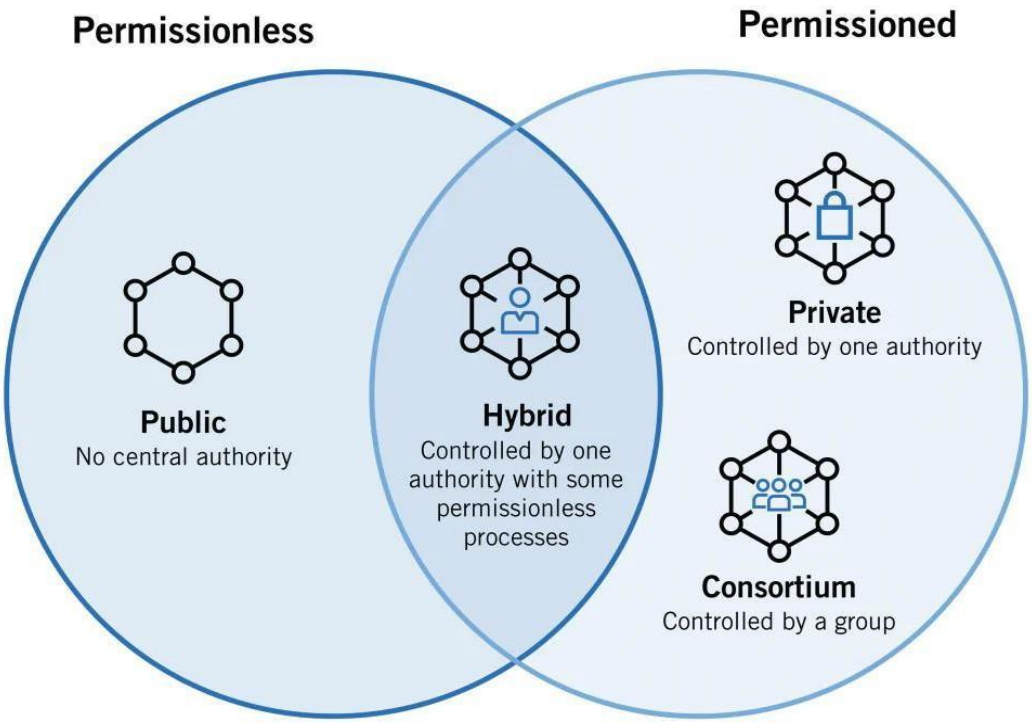


Figura 3. Tipos de permisos
Fuente: https://adefinitivas.com/arbol-del-derecho/nuevas-tecnologias/quien-es-el-responsable-del-tratamiento-en-blockch/

4.2 La descentralización

La descentralización hacer referencia a la gobernanza multipartes, donde no hay una entidad central o grupo cerrado de entidades que la controlen sino todos los participantes son tenidos en cuenta a la hora de tomar decisiones. La gobernanza multipartes trata de reunir a las partes interesadas para que participen en el diálogo, la adopción de decisiones y la aplicación de respuestas a problemas percibidos conjuntamente.

La gobernanza hace referencia a cómo las interacciones entre los distintos actores políticos (aquellos encargados de aplicar una política) y sus intereses impactan la calidad de vida del sistema que administran y de los individuos que hacen parte.

Con la aparición de la blockchain, se habla de gobernanza descentralizada, porque se elimina al órgano central que toma las decisiones de forma arbitraria y sin contar con todos los involucrados. En la gobernanza descentralizada nadie tiene el control total sobre el proyecto. Para hacer un cambio, la comunidad debe llegar a un consenso (internetsociety, 2018).

4.3 Investigaciones internacionales sobre blockchain

Casos de uso empresas internacionales con tecnología blockchain:

Objetivo: Indicar las empresas internacionales que adoptaron tecnología blockchain Para la mejora de sus procesos.

- **Honeywell**

Honeywell se ha convertido en uno de los mejores y primeros adoptantes en las ideas de proyectos de blockchain y otras empresas tecnológicas populares. Una popular empresa industrial de Nueva York. Ha transferido con éxito más de 3 millones de documentos relacionados con la aviación en una red de libro mayor de blockchain.

Honeywell ha aprovechado las características de Hyperledger Fabric para migrar los documentos de calidad de la aviación con éxito. Sin embargo, esto solo puede demostrar que todos sus clientes tienen acceso a los documentos de calidad de la aviación.

Además, gestiona la plataforma GoDirect Trade, un mercado de blockchain. El programa GoDirect Trade cuenta con más de $4B de inventario de componentes de aviación antiguos y ha atraído a más de 10.000 usuarios.

- **Boeing**

Boeing es otra empresa popular que entra en tiempo real entre las principales ideas de proyectos de blockchain en 2021. La rama empresarial HorizonX de Boeing ha invertido muchos esfuerzos para desarrollar SkyGrid. Boeing es popularmente conocido como un sistema de control de tráfico aéreo impulsado por blockchain para el seguimiento y la comunicación con los drones.

Lo más esencial de todo es que SkyGrid ha conseguido la aprobación de la FAA para proporcionar autorización de baja altitud a los pilotos de drones. Además, SkyGrid está disponible como aplicación de software gratuita en el iPad.

Se puede utilizar para desarrollar un registro permanente de datos para ayudar con el paquete de entrega y las inspecciones industriales. Sin embargo, al aprovechar la potencia de una plataforma basada en blockchain como GoDirect e Hyperledger, SkyGrid tiene el potencial de impulsar taxis voladores autónomos en el futuro.

- **Visa**

La abundancia de ideas de proyectos de blockchain también se conjuga con la imagen de Visa. Sus mayores puntos fuertes son su enorme red de puntos de acceso a Visa, que incluye más de 70 millones de establecimientos comerciales, y también, los bancos centrales se están centrando gradualmente en la creación de monedas digitales.

Por ello, Visa ha estado realizando una serie de intentos de investigación y desarrollo importantes para garantizar la seguridad y el flujo de dinero digital fuera de sus márgenes. Visa B2B Connect es una de las iniciativas comerciales esenciales de Visa.

Utiliza la ventaja de la tecnología blockchain de la cadena de suministro para ofrecer una mejor solución de pago transfronterizo. El hecho es que la tecnología blockchain de Visa puede proporcionar seguridad de datos rentable, contratos inteligentes, transparencia y un método rápido para procesar todos los pagos globales.

Sin embargo, Visa ya ha presentado más de 150 aplicaciones de patentes basadas en blockchain para diferentes usos; la biometría para validar la identificación de las personas y aumentar la seguridad de las transacciones son dos ejemplos reales de los últimos desarrollos de Visa blockchain.

Recientemente, Visa ha anunciado una asociación con la criptomoneda US Dollar como establo diseñado para aumentar la velocidad de las transacciones entre empresas (B2B).

- **Walmart**

El impacto de Walmart en la Iniciativa de Trazabilidad de los Alimentos no debe pasarse por alto al hablar de las principales ideas de proyectos de blockchain en 2021. Para detectar la contaminación y otros riesgos para la seguridad alimentaria, Walmart utiliza una Iniciativa de Trazabilidad Alimentaria basada en blockchain, que puede rastrear más de 500 productos diferentes, como carne, verduras de hoja verde frescas, mariscos y café.

El gigante minorista ayudó a la FDA en 6 investigaciones diferentes sobre seguridad alimentaria en el año anterior. Sin embargo, las aplicaciones de blockchain del comercio minorista ofrecieron amplia información sobre la fuente inicial de contaminación en menos de una hora.

Además, Walmart tiene previsto llevar a cabo un programa piloto con el Servicio de Aduanas y Protección de Fronteras de EE.UU. para hacer un seguimiento de las mercancías importadas.

- **Microsoft**

La empresa de software más popular del mundo también cuenta con una de las principales ideas de proyectos de blockchain en 2021. La empresa Microsoft se asoció con EY para desarrollar populares aplicaciones de blockchain basadas en las cadenas de bloques Ethereum y Quorum.

El negocio tiene una de las mejores aplicaciones de blockchain. La gestión de royalties y los derechos de contenido son algunas de las principales características de la aplicación blockchain. Productores de juegos como Xbox y Ubisoft fueron de los primeros en adoptar la nueva infraestructura de blockchain de Microsoft.

Sin embargo, el nuevo mecanismo de blockchain de la empresa para realizar pagos automáticos de derechos es superior al proceso tradicional.

- **MetLife**

Vitana resulta ser una de las ideas del proyecto blockchain en el que está trabajando la compañía MetLife. El laboratorio de desarrollo tecnológico LumenLab de la compañía MetLife, con sede en Singapur, ha elaborado recientemente un libro blanco basado en el proyecto Vitana, que es una idea paramétrica relacionada con los seguros. Sin embargo, Vitana se centra en el blockchain de los seguros para incorporar la tecnología a otras partes del sector. Esta iniciativa está trabajando ahora en la diabetes mellitus gestacional que afecta a las mujeres embarazadas.

Así, la compañía MetLife aprovecha el proyecto para ofrecer planes adaptados a las mujeres embarazadas para ayudarlas en el aspecto de combatir esta dolencia si se produce.

- **IBM Corporation**

IBM fue una de las primeras grandes corporaciones en dedicar recursos relevantes a proyectos de blockchain a gran escala en la industria. Sin embargo, utilizando la tecnología blockchain para reunir titulares en diversos círculos, IBM ha lanzado la Pase Digital de Salud aplicación.

Esta aplicación de Pass fue diseñada para ayudar a las empresas a confirmar los resultados de las pruebas de COVID-19 de las personas. Clientes como los operadores de estadios podrían utilizar la aplicación en función de su plataforma. Por ejemplo, los operadores de estadios pueden elegir si un individuo fue vacunado o no.

- **Shell**

Actualmente, Shell está trabajando en un proyecto de blockchain que construye un sistema descentralizado basado en el pasaporte digital como el comercio electrónico, uno de sus muchos proyectos futuros de blockchain.

Sin embargo, en esta idea de proyecto, la organización autentificará todos los aspectos, equipos y productos en la creación de seguridad y privacidad donde cada dato es procesado de forma segura y bien asegurada y trabajando en línea con una empresa para redefinir cómo funcionan sus cadenas de suministro.

- **Daimler**

Siendo una de las multinacionales de automoción más populares que fabrican coches de lujo en la industria del automóvil, como Mercedes-Benz, Daimler está colaborando ahora con Circulor. Están trabajando en una iniciativa de blockchain que hará un seguimiento de las emisiones de CO2 en su proceso de la cadena de suministro de Cobalt.

Su principal objetivo es la transparencia y las posibles soluciones de blockchain para mitigar la transmisión de CO2. Además, Daimler y Circulor quieren rastrear cualquier material secundario que pueda venir con su minería de Cobalto.

- **HSBC**

HSBC es, sin duda, una de las mejores empresas en el ámbito financiero con una visión de las iniciativas de proyectos de blockchain futuristas. El banco con sede en el Reino Unido aprovecha blockchain para mejorar la eficiencia de sus flujos de divisas en todas sus sucursales mundiales.

Las investigaciones muestran que el libro mayor de blockchain del HSBC ha ayudado a liquidar más de 1,8 millones de operaciones con un valor nominal de unos $1,8 billones. Digital Vault es uno de los proyectos más notables de HSBC, y es una plataforma tecnológica basada en blockchain que se centra más en la digitalización de todos los registros de transacciones de las colocaciones privadas.

Su departamento de Servicios de Valores está detrás de la plataforma. HSBC quiere asegurarse de que sus capitalistas de riesgo puedan acceder a sus activos digitales privados y los datos como los bienes inmuebles, la seguridad, la deuda o el capital. Es totalmente seguro y todo está en formato digital (startechup, 2021).

4.4 Investigaciones nacionales sobre blockchain

Casos de uso empresas nacionales con tecnología blockchain:

Objetivo: Indicar las empresas nacionales que adoptaron tecnología blockchain
Para la mejora de sus procesos.

- **Blockchain en la salud**

La Clínica Las Américas de Medellín anunció una solución blockchain para el sector salud y el cuidado de pacientes en el país. Gracias a IBM Blockchain, la clínica puede hacer seguimiento, control y abastecimiento de dispositivos médicos como catéteres, marcapasos, entre otros.

Gracias al blockchain se logró reducir a 24 horas las entregas de insumos, a un 90% el tiempo de facturación y en un 60% los errores en las órdenes de compra, impactando positivamente el suministro de insumos médicos que salvan vidas en momentos de urgencia.

Cornerstone y Roadlaunch, las empresas que implementan este modelo en la clínica aseguraron que este consiste en una red transparente de información inmutable y precisa en tiempo real, esta permite que, cuando a un paciente se le implanta un dispositivo médico este pueda ser reemplazado en el stock de la clínica en el menor tiempo posible.

Asimismo, gracias al blockchain, empresas de cannabis medicinal en Colombia pueden hacer seguimiento al crecimiento de la planta, sus características, el fruto que dará y las condiciones en las que se produce. La información puede ser vista en tiempo real por todos posibles compradores en todo el mundo.

- **Blockchain en la educación**

En la educación el blockchain planea aplicarse en el país mediante aplicaciones sencillas: Las instituciones educativas pueden hacer trazabilidad de materias, con esto, el estudiante obtendrá su diploma con base en los créditos alcanzados a través de los diferentes semestres de la carrera. “Esto ayuda a evitar el tráfico de diplomas”, según Ana María Moreno, coordinadora de la Red de Universidades para el Fomento de la Investigación en Tecnologías de la Información y la Comunicación.

- **Otras aplicaciones del blockchain en Colombia**

La Terminal de Contenedores de Buenaventura se convirtió en el primer puerto del país en usar el blockchain para realizar un seguimiento detallado a la mercancía que se mueve. La terminal opera gracias a la plataforma Trade Lens, la cual procesa 10 millones de eventos en cadena de bloques a la semana a nivel mundial; en Buenaventura se va generando una cadena de suministro que se alimenta con los datos de carga y descarga de los contenedores.

Este sistema es una oportunidad tanto para los comerciales como las autoridades ya que los productos que pasan por esta terminal pueden transportarse con transparencia y con más velocidad en el acceso a la información.

Otro caso es el Qubit Labs, una empresa creada en Cali y cuyo desarrollo permite adquirir boletas para eventos culturales, musicales y deportivos a través de un código QR en el celular. Este servicio blockchain reemplaza a las manillas o boletas físicas que, tradicionalmente, se usan para asistir a este tipo de eventos (sabermassermas, 2021).

4.5 Smart contracts

Objetivo

Definir que es un contrato inteligente y a su vez la usabilidad dentro de una cadena de bloques(blockchain).

Básicamente un contrato inteligente es un código informático que se caracteriza por ser capaz de ejecutar y cumplir por sí mismo cualquier tarea de manera automática y si necesidad de intermediarios ni validadores. Un contrato inteligente tiene validez sin depender de autoridades. Esto se debe a su naturaleza: es un código visible por todos y que no se puede cambiar al existir sobre la tecnología blockchain**.** Esto le confiere un carácter descentralizado, inmutable y transparente.

- **Los primeros contratos inteligentes**

La primera vez que se tiene constancia de forma pública sobre los Smart contracts es a través de Nick Szabo, jurista y criptógrafo Nick Szabo que mencionó públicamente el término en un documento en 1995. Dos años después, en 1997, desarrolló un documento mucho más detallado explicando los Smart Contracts.

Lamentablemente, pese a definir la teoría, era imposible hacerla realidad con la infraestructura tecnológica existente. Para que los contratos inteligentes se puedan ejecutar, es necesario que existan las transacciones programables y un sistema financiero que las reconozca, digitalmente nativo.

Precisamente, lo que Szabo definía como inexistente en 1995, en 2009 (casi 15 años después) se haría realidad con la aparición de Bitcoin y su tecnología, la cadena de bloques (*blockchain*) (academybit2me, 2020).

Básicamente hoy en día son mucho los usos que se le pueden dar a los contratos inteligentes; desde almacenamiento de registros, actividades comerciales, cadenas de suministro etc.

Figura 4. Contratos inteligentes
Fuente:
https://www.iberdrola.com/documents/20125/1264653/Infografia_Contratos_Inteligentes.pdf/cc43c9ff-3071-5fba-d39e-8307f0f165a4?t=1639391580149

- **¿Que blockchain adoptan esta tecnología de Smart contract?**

Para entender a fondo que blockchain adoptan esta tecnología primero debemos conocer que existen tres tipos de generaciones de blockchain:

- **Blockchain de primera generación**

La primera generación aparece en 2009 con el lanzamiento de Bitcoin creado por Satoshi Nakamoto, un individuo (o grupo de personas) cuya identidad real es desconocida. Esta generación establece por primera vez en la historia una forma de dinero digital descentralizado, sin necesidad de terceros de confianza, esta generación cuya blockchain no permite incorporación de contratos inteligentes no la excluye de ser pionera en muchos aspectos sobre seguridad en transacciones.

- **Blockchain de segunda generación**

La segunda generación surge con Ethereum, fundada por un grupo de desarrolladores entre los que se encuentra Vitalik Buterin, un joven programador. Ethereum surgió como una tecnología más experimental ya que en Bitcoin es difícil realizar cambios disruptivos. La idea de Ethereum fue crear una especie de ordenador mundial que pudiera ejecutar contratos complejos, los conocidos Smart contract (contratos inteligentes) la blockchain de Ethereum fue la primera en incorporar contratos inteligentes funcionando contratos y blockchain a lo que hoy se conoce como Dapps o aplicaciones descentralizadas que es la fusión entre un Smart contract con una interfaz donde el usuario puede interactuar fácilmente con estas tecnologías.

- **Blockchain de tercera generación**

Con el tiempo surge una tercera generación de blockchain que buscan solventar problemas de Ethereum. Estas blockchain están caracterizadas por el uso de un nuevo sistema de consenso llamado Proof of Stake, o prueba de participación. Ejemplos de esta generación son Polkadot, Solana, Cardano e incluso el propio Ethereum 2.0. En general, al igual que Ethereum, su visión

es crear los fundamentos de la web 3.0 con aplicaciones descentralizadas y contratos inteligentes (blogbitnovo, 2021).

- **Lenguajes de programación para la creación de contratos inteligentes**

Los smart contracts pueden ser escritos en distintos lenguajes de programación, siempre y cuando existan el compilador y librerías capaces de traducir y servir de interfaz con las distintas capacidades smart contracts de la blockchain que usemos.

- **Solidity**

Solidity es un lenguaje de alto nivel de tipado estático con el que se pueden programar smart contracts para la red de Ethereum. Su sintaxis es muy similar a la de lenguajes muy conocidos como C++ o Javascript. Solidity fue creado con el propósito de permitir la escritura de smart contracts de forma sencilla para la red Ethereum. Se trata de un lenguaje diseñado para sacar el máximo provecho a la Ethereum Virtual Machine, permitiendo la creación y desarrollo de smart contracts que puedan ser ejecutados de forma óptima en la EVM.

Para ello el programador puede desarrollar sus aplicaciones en un lenguaje sencillo de utilizar, leer y mantener para que, al terminar, el motor de Solidity convierta ese código sencillo en el código máquina que la EVM entenderá, un código máquina prácticamente imposible de entender por una persona.

Solidity es ampliamente usado en Ethereum y en cualquier otra blockchain construida con compatibilidad EVM, por ejemplo, BNB Chain, Polygon, Avalanche, Polkadot/Kusama (parachains como Moonbeam y Moonriver tienen soporte a Solidity), entre otras redes.

- **Vyper**

Vyper es un lenguaje de programación basado en Python dirigido a crear Smart contracts para la máquina virtual de Ethereum (EVM). Al estar basado en Python, este lenguaje disfruta

de una enorme facilidad para desarrollar Apps para quienes están acostumbrados a este lenguaje, y al mismo tiempo, se alimenta de las potentes herramientas de depuración que están creadas para el mismo.

- **Rust**

Rust es un lenguaje de programación compilado, de propósito general y multiparadigma que empezó su desarrollo como parte del proyecto Mozilla y que actualmente forma parte de la Rust Foundation. El lenguaje está centrado en ofrecer un alto nivel de seguridad, hasta el punto en que actualmente es considerado como uno de los lenguajes de programación más seguros para la generación de aplicaciones (academybit2me, 2022).

4.6 Dapps

Las DApps o aplicaciones descentralizadas son una categoría especial de aplicaciones que funcionan en base a una red descentralizada de computadores u ordenadores. Los datos generados por esta aplicación están alojados en una red de ordenadores que permite que esta información se mantenga segura y accesible.

Esta red descentralizada es una DLT generalmente basada en tecnología blockchain.

Para poner un ejemplo más fácil, podríamos imaginar a una DApp como una aplicación conocida como Facebook, Tinder o Robinhood pero que en vez de ejecutarse sobre un servidor central (suelen ser varios) se ejecuta en una red formada por miles de nodos u ordenadores.

- **Cómo funcionan las DApps**

Las aplicaciones tienen su código de backend (contratos inteligentes) ejecutándose en una red descentralizada y no en un servidor centralizado. Utilizan la cadena de bloques de Ethereum para el almacenamiento de datos y contratos inteligentes para su lógica de aplicaciones.

Un contrato inteligente es como un conjunto de reglas que viven en cadena para que todos vean y ejecuten exactamente de acuerdo con esas reglas. Imagina una máquina expendedora: si le suministra suficientes fondos y hace la selección correcta, obtendrá el artículo que desee. Y al igual que las máquinas expendedoras, los contratos inteligentes pueden mantener fondos de la misma manera que su cuenta de Ethereum. Esto permite que el código medie en acuerdos y transacciones.

Una vez que las dapps están desplegadas en la red Ethereum, no puede cambiarlas. Las dapps pueden descentralizarse porque están controladas por la lógica escrita en el contrato, no por un individuo o por una empresa (ethereum, 2022).

5. Metodología

5.1 Tipo de proyecto

Esta Investigación será de tipo descriptiva ya que se indagará de manera más completa sobre la seguridad que manejan las empresas en cuanto a información que se guarda en está aplicando el uso en la tecnología blockchain.

5.2 Método

Una de la hipótesis que se planeta en esta investigación es que se puede hacer para mejorar la seguridad de datos, ¿bastaría con una blockchain privada? o si por lo contrario se puede emplear una solución como guardar nuestra información en monederos virtuales, como por ejemplo las que se usan para guardar NFT o criptomonedas, si bien no se pueden demostrar, se pueden someter a pruebas y mecanismos de validación.

Entonces se resume que dado a que esta investigación tiene un problema cuya solución son las blockchain privadas se llega a la conclusión de utilizar un método de simulación basado en un contrato inteligente que sirva para registrar datos donde se pueda mirar a detalle como una blockchain funciona y así lograr que esta investigación donde el problema que se plantea tenga alguna validez.

5.3 Instrumentos de recolección de información

Esta investigación se centra en una población especifica la cual será las empresas colombianas, según estadísticas en mayo del 2021, en el país ya existían 469.099 empresas activas las cuales han sido vulneradas por lo menos 89.000 de ellas por esta razón las empresas han tomado mayor conciencia de estos riesgos. Los presupuestos de tecnología eran muy bajos hace unos años. Hoy vemos destinaciones de doble dígito (la república, 2021), (portafolio, 2021).

5.3.1 Fuentes primarias. Información obtenida de un grupo de personas especializadas en contenidos en específico y documentos oficiales de instituciones públicas.

5.3.2 Fuentes secundarias. Información obtenida de investigaciones de sitios web.

- Blog

Como usar blockchain en la empresa

https://blog.enzymeadvisinggroup.com/como-usar-blockchain-en-la-empresa

- Libro

La revolución blockchain

Autores Alex Tapscott, Don Tapscott

https://www.marcialpons.es/media/pdf/9788423426553.pdf

- Documentales

Blockchain City

https://www.youtube.com/watch?v=KiBke759DQs&t=1564s

- Videos

Conferencia blockchain

https://www.youtube.com/watch?v=yFmzolUP9iQ

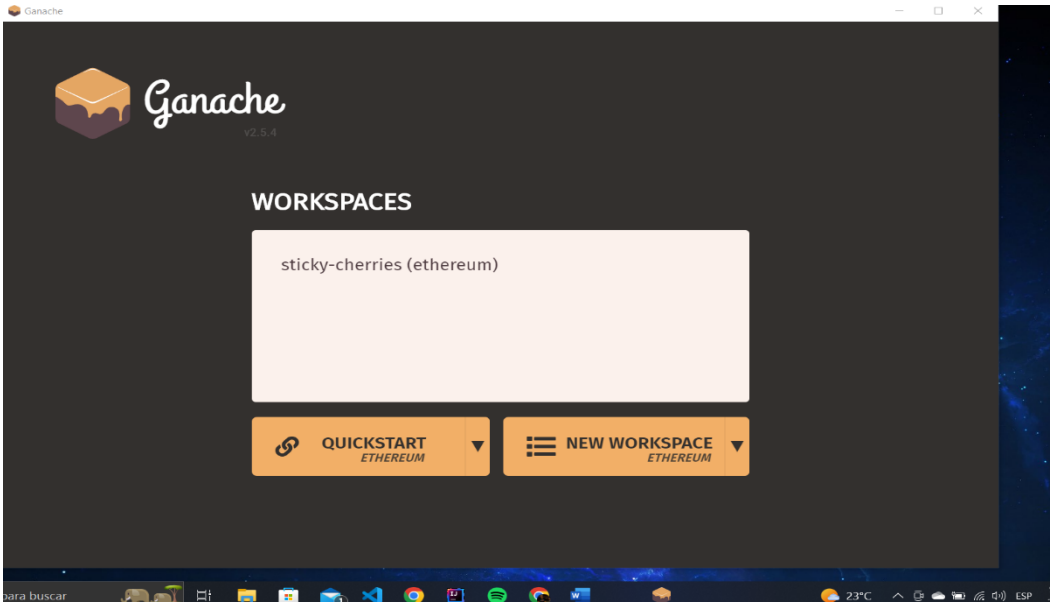
6. Resultados del proyecto

Comprender de una manera muy detallada como un smart contract se conecta a una blockchain y a su vez cómo puede el usuario interactuar con él para entender su correcto funcionamiento para almacenar datos los cuales quedan guardados en bloques con un identificador único y difícil de alterar.

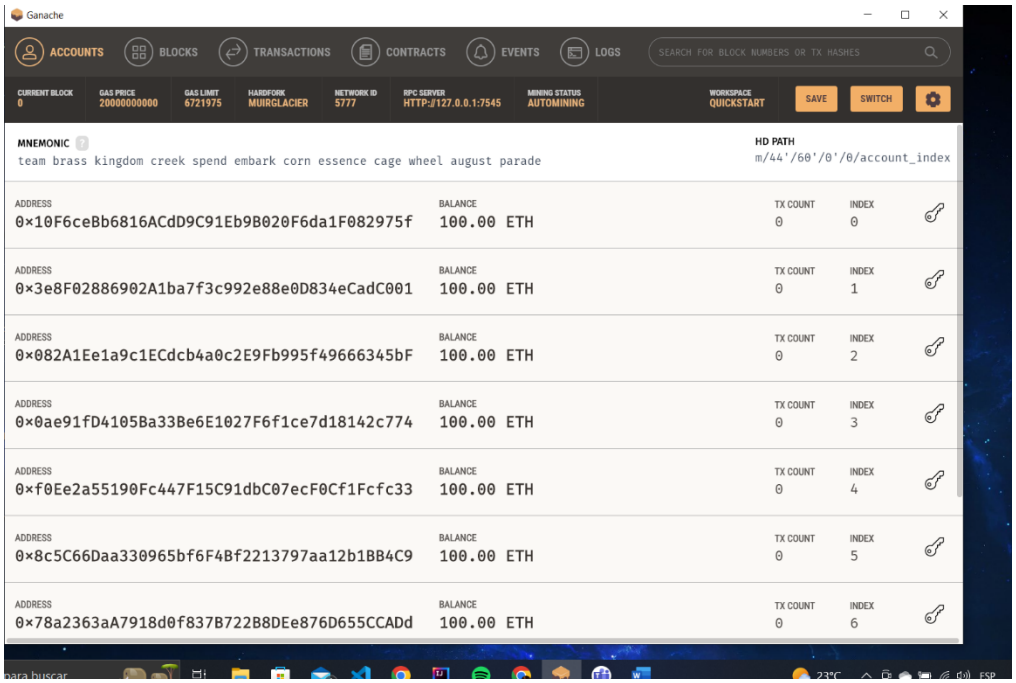
Se logró ejecutar un contrato inteligente dentro de una blockchain privada usando como software de simulación Ganache ya que simula una blockchain que trabaja con la máquina virtual de Ethereum logrando que este contrato se ejecute dentro de la red descentralizada.

Se evidencia de igual forma en las capturas de pantalla presentadas a continuación:

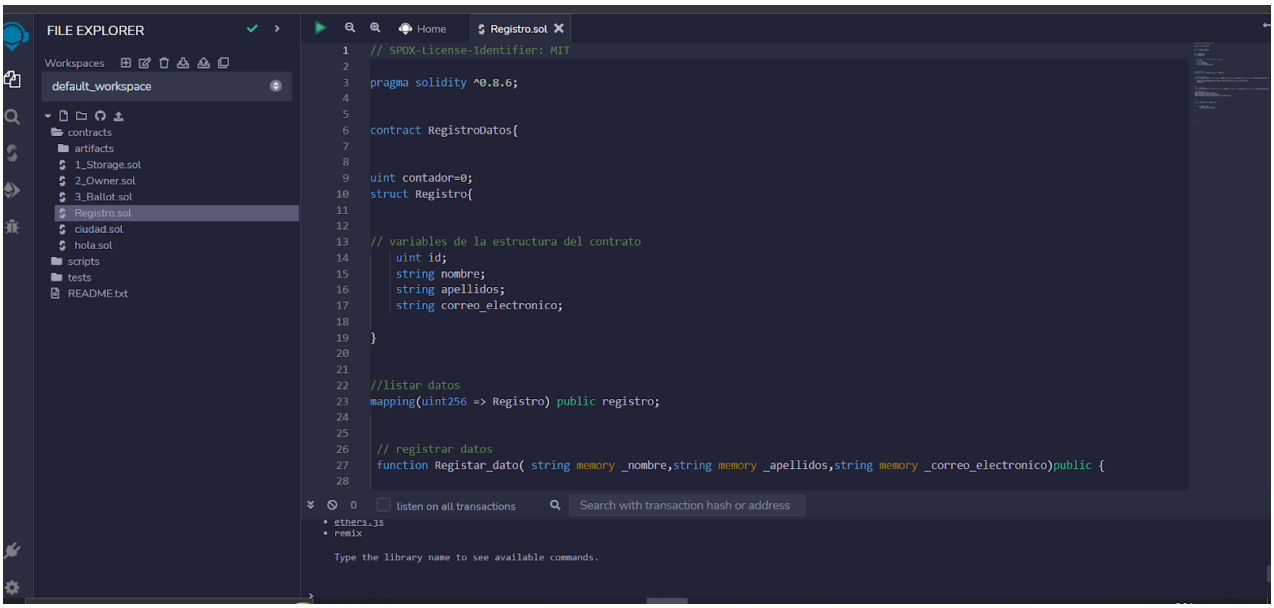
1. Ganache es un software que nos proporciona un ambiente simulado de una blockchain donde se pueden hacer pruebas localmente en la red de Ethereum entonces para iniciarlo se ejecuta primero este programa en nuestra computadora.



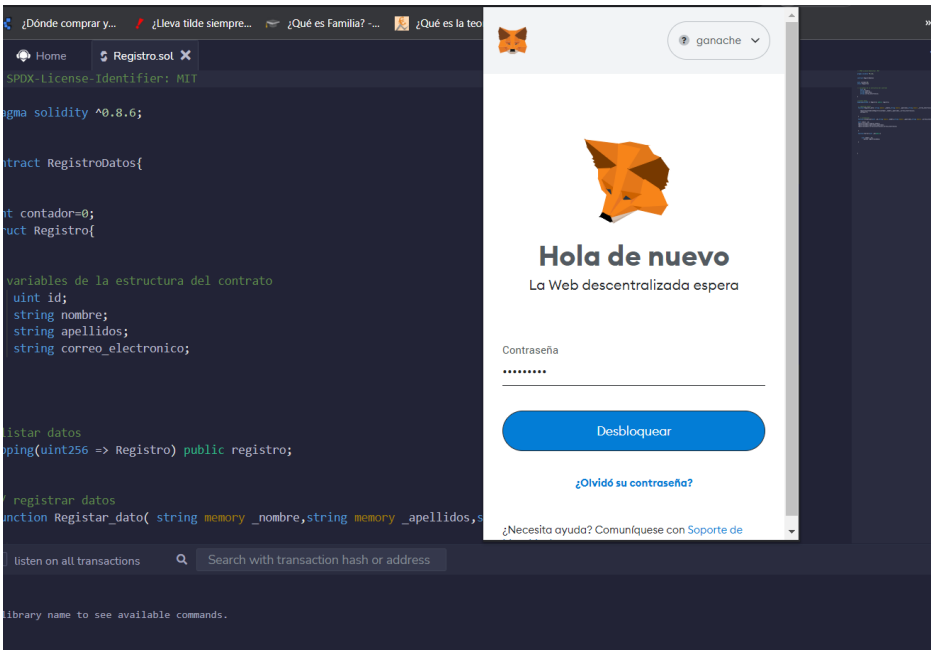
2. Luego de iniciar el software nos vamos a encontrar con una serie de direcciones donde cada una posee 100 ETH de prueba para que se puedan hacer las pruebas de simulación se puede escoger cualquier dirección.



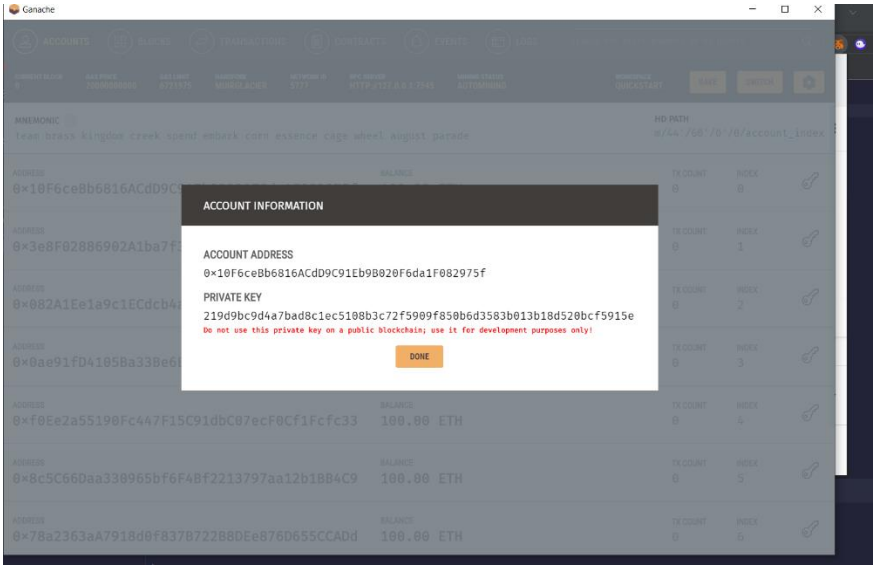
3. Este entorno de desarrollo se llama remix es un IDE para crear contratos inteligentes en un lenguaje llamado Solidity acá en esta imagen se puede observar el contrato que sirve para registrar actualizar y eliminar datos.



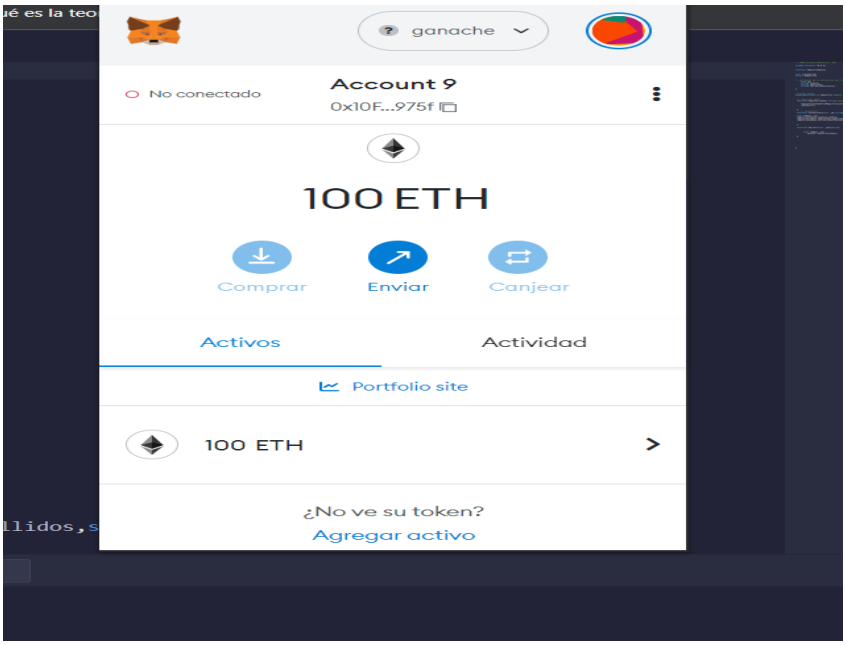
4. Para que se pueda interactuar con este contrato se debe tener previamente una billetera instalada ya sea en un navegador o propiamente instalada en nuestro computador acá como se puede observar en la imagen se ve una billetera que se llama metamask en el cual nos pide una contraseña para iniciar y poder conectarnos a nuestro smart contract.



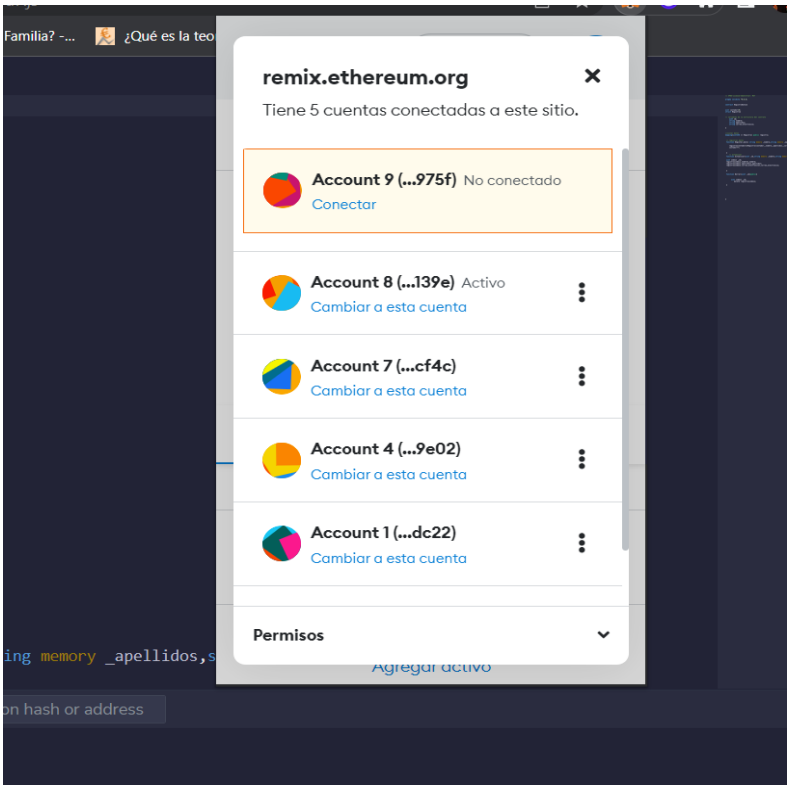
5. Cuando se escoge una dirección en el software de ganache y le damos en ver llave privada nos abre esta ventana donde se debe de copiar la dirección de prívate key y así pegarla en nuestra billetera de metamask y así tener los 100 ETH en nuestra wallet.



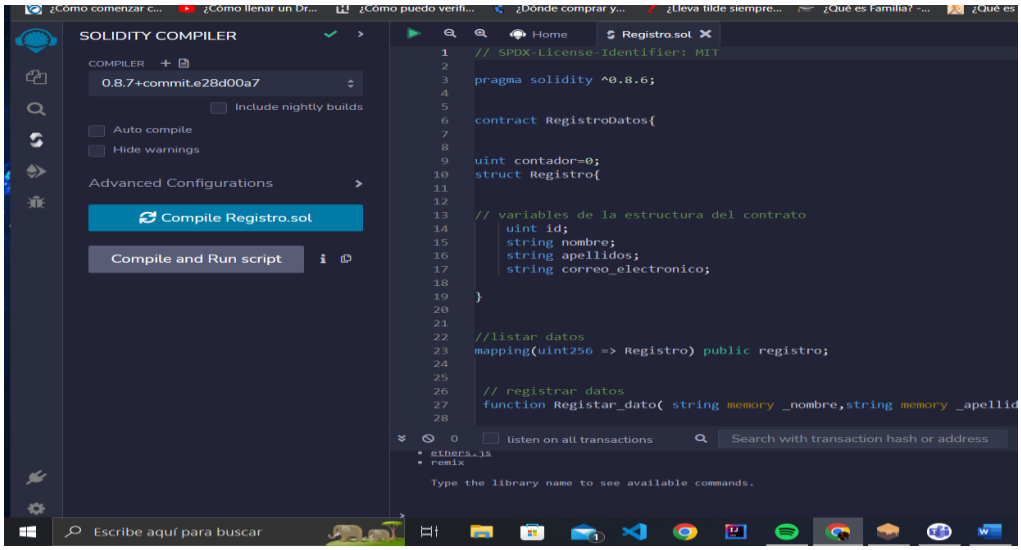
6. Como se explicaba en el punto anterior después de haber importado la llave privada en nuestra billetera se puede ver claramente la dirección y los 100 ETH de prueba.



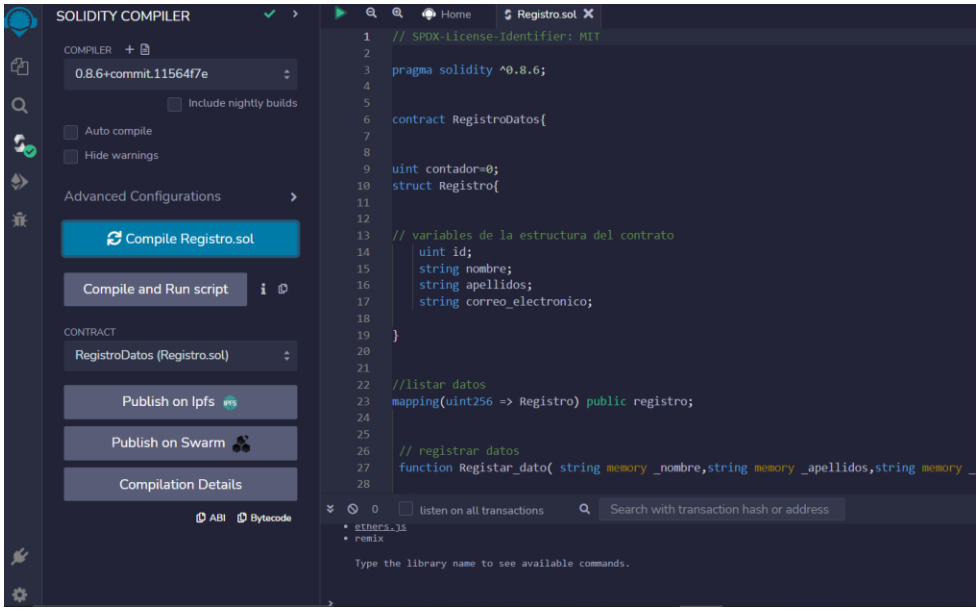
7. Luego se debe conectar esta billetera con remix para poder ejecutar el contrato solo se debe seleccionar la dirección que corresponde a nuestra billetera y le damos conectar



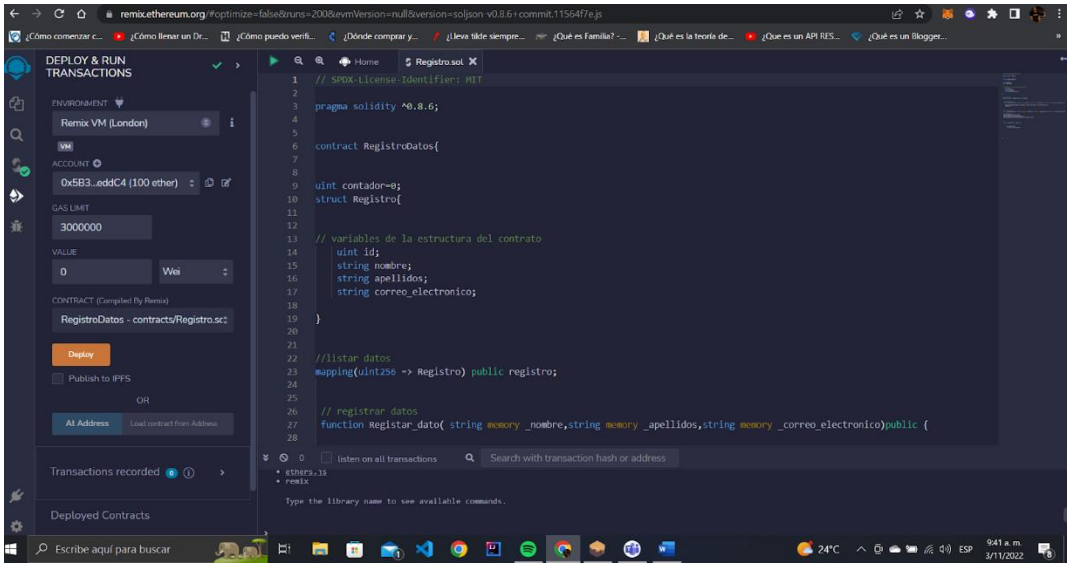
8. Después de tener conectada nuestra billetera con nuestro contrato procedemos a compilar el código del contrato para luego desplegarlo en la blockchain de prueba (Ganache).



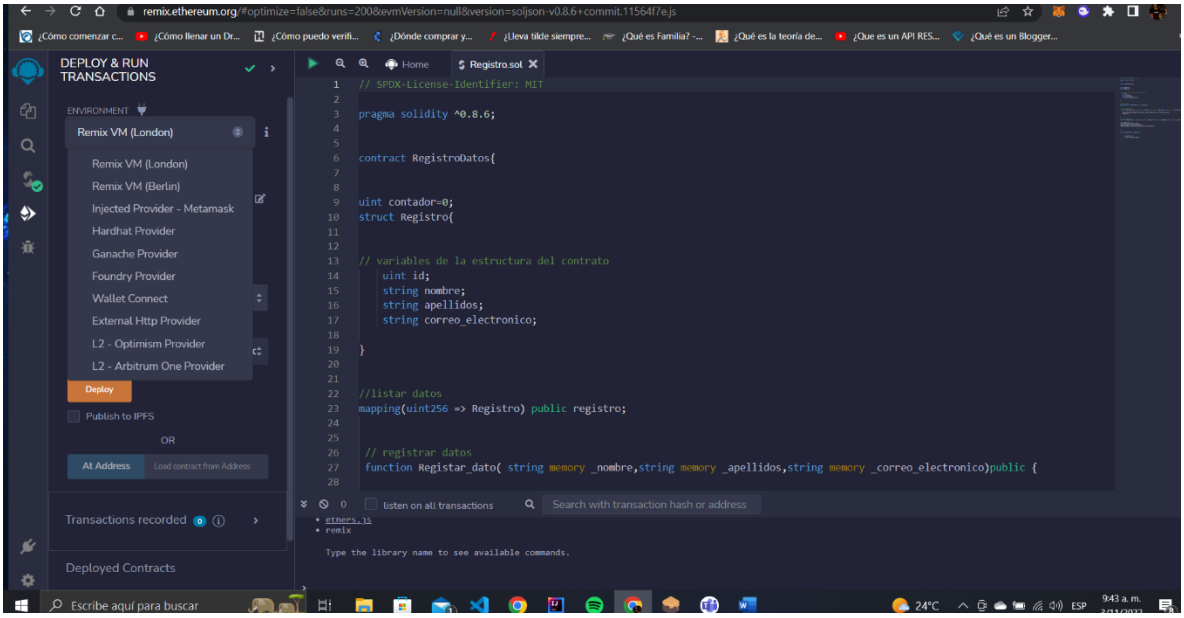
9. Acá tenemos ya el contrato compilado como se puede ver al costado izquierdo la confirmación en verde de que todo salió correcto adicional este código al compilar crear un archivo. json llamado ABI el cual sirve para conectarse con una interfaz ya sea en JavaScript o Python



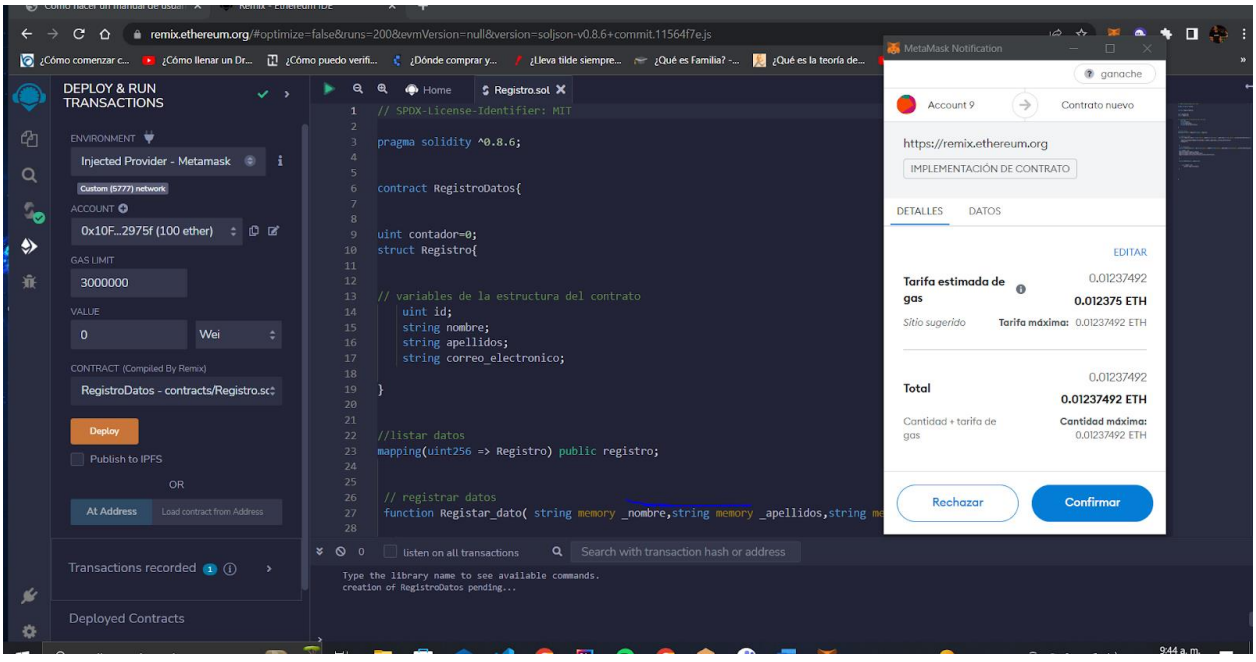
10. En esta captura se puede observar en la parte donde dice ACCOUNT la dirección de nuestra billetera con los 100 ETH de prueba ya solo queda darle en el botón Deploy para que se desplegué en la blockchain de prueba.



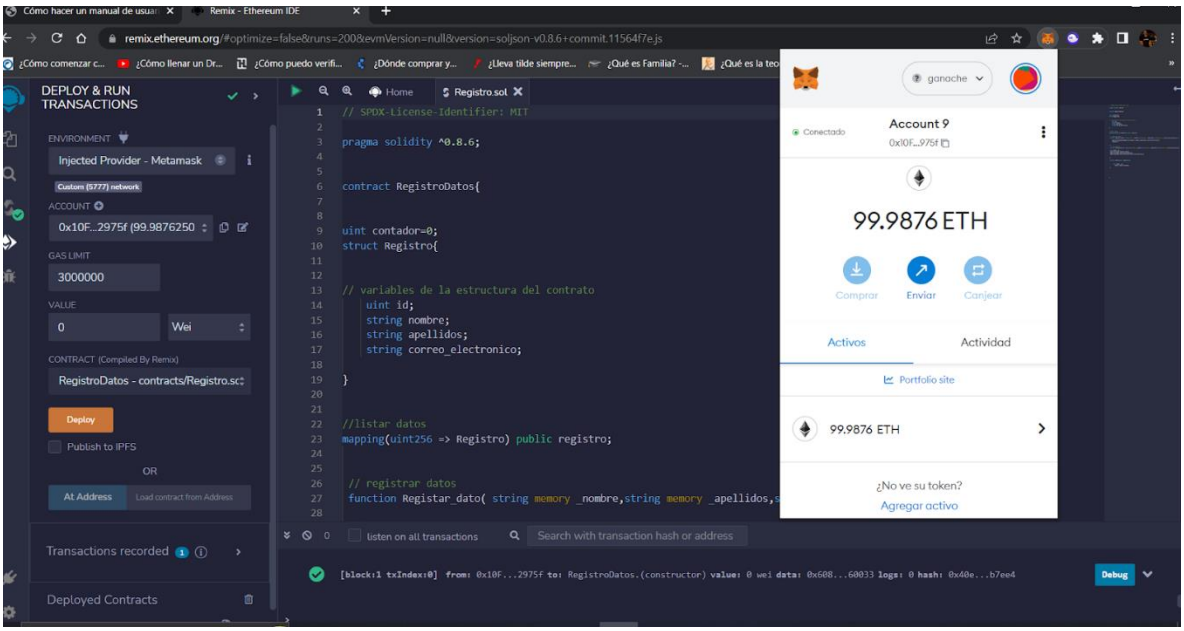
11. En la sección que dice Environment se selecciona injected provider metamask para que se pueda conectar a nuestra billetera y ejecutar el contrato.



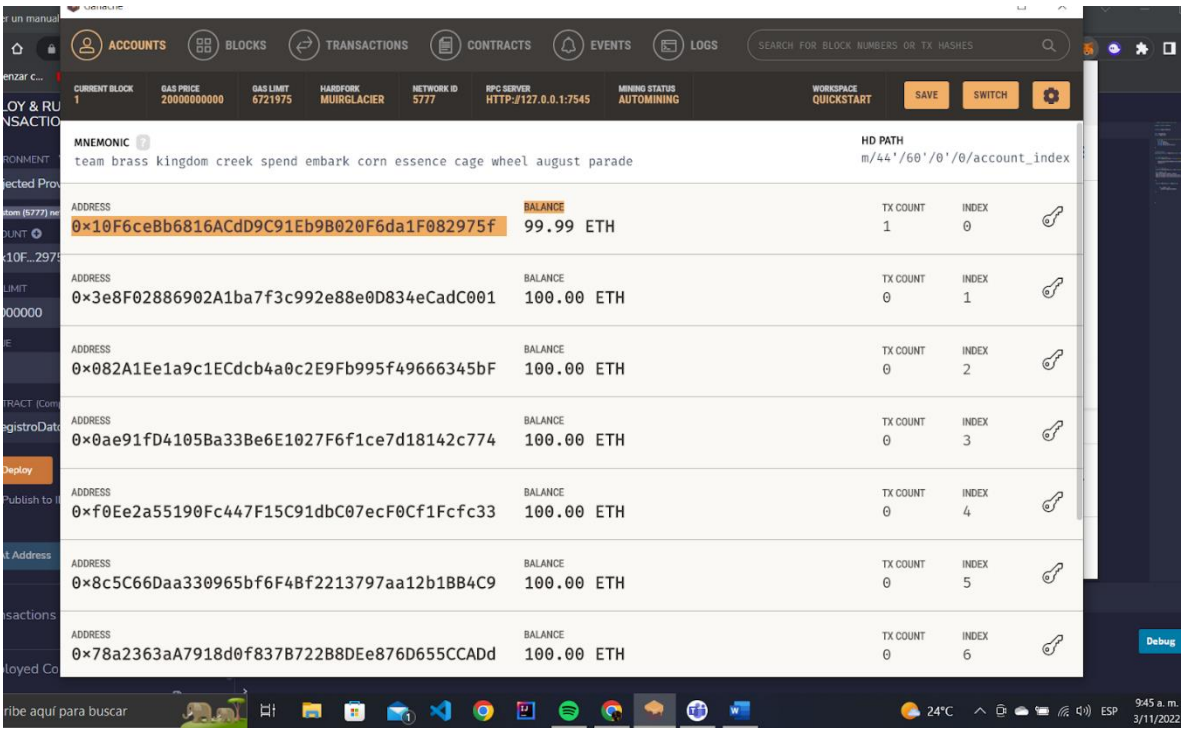
12. En este paso se puede observar cuando le damos en desplegar (Deploy) una confirmación de gas o feed en nuestra billetera para que el contrato se ejecute correctamente, para esto era el saldo que teníamos de los 100 ETH.



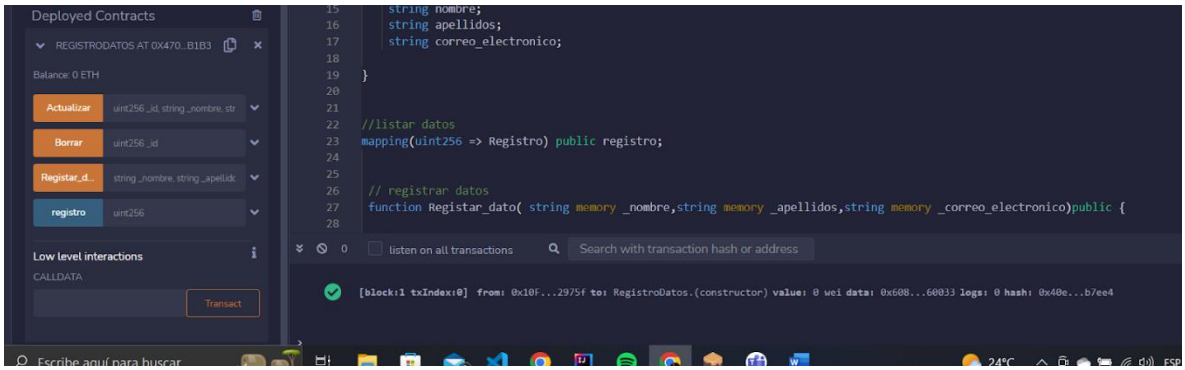
13. Como se puede observar después de pagar una pequeña comisión el contrato se ha creado correctamente y esta desplegado en la blockchain de prueba de Ethereum.



14. Como se puede observar en la dirección subrayada se ve que el balance disminuyo lo que quiere decir que el contrato se ejecutó de manera satisfactoria en la red de pruebas.



15. El contrato está listo para interactuar con él en la parte izquierda se puede observar las funciones de registrar actualizar y eliminar datos donde si el usuario desea registrar un dato debe habilitar los campos y cada vez que se haga una transacción se descontara un feed o comisión de nuestro saldo de prueba y toda esta.



La información quedara almacenada en un bloque en nuestra blockchain de prueba.

Lo que se encontró con esta investigación fue lo esperado y lo que se había planteado directamente con el método de simulación el cual cuando se ejecutó el smart contract los registros fueron tomados de inmediato y sin tener que depender de un servidor central estos datos quedaron almacenados de una manera muy descentralizada lo cual se demuestra que no solo la blockchain se usa para guardar transacciones con criptomonedas sino que por medio de estos contratos se puede lograr guardar documentos información personal, imágenes (NFT) etc.…

7. Conclusiones

Entendí que con esta investigación se puede dar un resultado positivo ya que se pudo evidenciar que actualmente a nivel nacional e internacional la tecnología blockchain cada vez se está posicionando en la industria y quitando así ese paradigma de que blockchain es solo bitcoin o cualquier otra criptomoneda y al contrario blockchain es mucho más que eso hoy en día son muchas las aplicaciones que se están creando bajo esta tecnología.

En esta investigación como se pudo observar se realizó una simulación para ver que todo lo que se habla en seguridad en donde cada dato quedo guardado en un bloque y garantizando una mejor seguridad de información.

Está claro que es una opción legal ante el problema del cual se menciona en el objetivo general y como tal se deseaba solucionar, esto puede transformarse en un hecho que rompería muchos mitos acerca de cómo se guarda la información y se puede emplear para futuras generaciones estudiantes docentes aprovechando muy bien esta tecnología.

8. Recomendaciones

Como futuros proyectos se puede tomar como base esta investigación y donde a futuro este contrato se pude llevar a una interfaz gráfica donde se pueda conectar el backend del contrato con el frontend de alguna tecnología web y guardar información en una wallet. Para esto es necesario que más personas se adentren a este mundo de la blockchain donde se puede tener básicamente un internet descentralizado no necesariamente tiene que ser a nivel universitario, sino que muchas más empresas se vinculen con esta tecnología disruptiva.

Entender esta tecnología no es fácil por esto se requiere de mucho estudio y parte de esta investigación tiene información muy buena para servir de buen acompañamiento para futuros proyectos blockchain.

9. Referencias bibliográficas

academybit2me. (15 de 12 de 2020). Obtenido de academy.bit2me: https://academy.bit2me.com/que-son-los-smart-contracts/

academybit2me. (22 de 08 de 2022). Obtenido de academybit2me: https://academy.bit2me.com/top-5-de-lenguajes-de-programacion-de-smart-contracts/

almacenamientoit. (06 de 05 de 2020). Obtenido de almacenamientoit: https://almacenamientoit.ituser.es/noticias-y-actualidad/2020/05/blockchain-privado-para-el-almacenamiento-empresarial

blogbitnovo. (03 de 10 de 2021). Obtenido de blogbitnovo: https://blog.bitnovo.com/que-es-una-blockchain-de-primera-generacion/#:~:text=En%20general%20se%20identifican%203,cuya%20identidad%20real%20es%20desconocida.

BSM BLOCKCHAIN SCHOOL MANAGEMENT. (5 de 10 de 2021). Obtenido de BSM BLOCKCHAIN SCHOOL MANAGEMENT: https://www.bsmexecutive.com/diferencias-entre-blockchain-publica-privada-e-hibrida/

esan business. (05 de 12 de 2019). Obtenido de esan business: https://www.esan.edu.pe/conexion-esan/blockchain-publica-vs-privada-cual-es-la-diferencia-1

ethereum. (8 de 10 de 2022). Obtenido de ethereum: https://ethereum.org/es/dapps/#what-are-dapps

internetsociety. (28 de 4 de 2018). Obtenido de internetsociety: https://www.internetsociety.org/es/resources/doc/2016/gobernanza-de-internet-por-que-funciona-el-enfoque-de-multiples-partes-interesadas/

la nacion. (08 de 03 de 2022). Obtenido de la nacion: https://www.lanacion.com.ar/tecnologia/mercado-libre-confirma-la-filtracion-de-datos-de-300000-usuarios-nid07032022/

larepublica. (7 de 09 de 2021). Obtenido de larepublica: https://www.larepublica.co/empresas/ataques-ciberneticos-ocurren-mas-frecuentemente-a-pequenas-y-medianas-empresas-3228459

portafolio. (10 de 08 de 2021). Obtenido de portafolio: https://www.portafolio.co/negocios/empresas/empresas-en-colombia-cuantas-han-cerrado-y-cuantas-hay-activas-a-mayo-del-2021-554985

sabermassermas. (30 de 11 de 2021). Obtenido de sabermassermas: https://www.sabermassermas.com/empresas-en-colombia-que-han-acogido-la-tecnologia-blockchain/

startechup. (10 de 09 de 2021). Obtenido de startechup: https://www.startechup.com/es/blog/blockchain-projects-you-need-to-know/