Escuela Politécnica Superior

Blockchain en la agricultura. Digitalización de procesos agrícolas

Grado en Ingeniería Informática

Trabajo Fin de Grado

Autor:
Daniel Sentamans Lorente

Tutor/es:
Francisco Javier Ferrandez Pastor

Universitat d'Alacant
Universidad de Alicante

Julio 2023

Agradecimientos

Me gustaría agradecer esta investigación a mi familia que ha estado en todo momento apoyando cada una de mis decisiones y, además, por el gran apoyo del programa AGROALNEXT del MCIN, proyecto de la Unión Europea NextGenerationEU (PRTR-C17.I1) y por la Generalitat Valenciana (España)

Resumen

Este trabajo de fin de grado tiene como objetivo diseñar un soporte tecnológico basado en el paradigma blockchain para desarrollar servicios comerciales de compra y trazabilidad en la cadena de valor de productos agrícolas. Para ello se crea una billetera virtual para la realización de las actividades de compra/venta o "smart contracts", unido al sistema de archivos descentralizados Interplanetary File System (IPFS) que almacenará datos para mejorar la transparencia y confianza en el mercado agrícola. La billetera permitirá a los usuarios realizar transacciones seguras y transparentes, mientras que el sistema de seguimiento de la cadena de suministro proporcionará información sobre la procedencia y el historial de los productos adquiridos. Este proyecto tiene como propósito fomentar prácticas sostenibles y responsables en la producción y distribución de alimentos, impulsando la confianza de los consumidores y mejorando la calidad y seguridad alimentaria. Con esta iniciativa, se espera tener un impacto positivo en la industria agrícola, impulsando la adopción de tecnologías innovadoras para transformar la forma en que interactuamos con los productos que consumimos.

Palabras clave: tecnología, Blockchain, trazabilidad, sector agroalimentario, IPFS

Abstract

This final degree project aims to design a technological framework based on the blockchain paradigm to develop commercial services for purchasing and traceability in the agricultural product value chain. To achieve this, a virtual wallet is created to facilitate buying/selling activities or "smart contracts," integrated with the decentralized file system Interplanetary File System (IPFS), which will store data to enhance transparency and trust in the agricultural market. The wallet will enable users to conduct secure and transparent transactions, while the supply chain tracking system will provide information about the origin and history of the purchased products. This project aims to promote sustainable and responsible practices in food production and distribution, fostering consumer trust and improving food quality and safety. With this initiative, we expect to have a positive impact on the agricultural industry by driving the adoption of innovative technologies to transform the way we interact with the products we consume.

Keywords: technology, Blockchain, traceability, agri-food sector, IPFS

Índice

Índice de Figuras

1. Introducción

En los últimos años, ha habido una creciente demanda de transparencia y responsabilidad en la industria alimentaria. Los consumidores están cada vez más preocupados por la seguridad y la calidad de los productos que consumen, así como por el impacto ambiental y social de la producción y distribución de alimentos. Al mismo tiempo, los avances en tecnología, como la blockchain, están proporcionando nuevas oportunidades para mejorar la transparencia y la trazabilidad en las cadenas de suministro.

En este contexto, este proyecto de fin de grado se enfoca en la creación de una billetera virtual que permita a los usuarios realizar compras y ver la trazabilidad de productos agrícolas. La billetera virtual se desarrollará utilizando tecnologías blockchain, que proporcionan una forma segura y transparente de almacenar y compartir información. Al integrar un sistema de seguimiento de la cadena de suministro, los usuarios podrán ver la procedencia y el historial de los productos que compran, desde la granja hasta la tienda.

La necesidad de una billetera virtual en la industria de los productos agrícolas es clara. La falta de transparencia y trazabilidad en la cadena de suministro ha sido un problema de larga data, lo que ha llevado a fraudes alimentarios, preocupaciones de seguridad y problemas ambientales y sociales. Al crear una billetera virtual que permita transacciones seguras y transparentes, y al integrar un sistema de seguimiento de la cadena de suministro, este proyecto tiene como objetivo mejorar la transparencia y la confianza en el mercado de productos agrícolas, así como fomentar prácticas más sostenibles y responsables en la producción y distribución de alimentos.

En general, este proyecto de fin de grado representa un paso importante hacia un sistema alimentario más transparente y sostenible. Al aprovechar las tecnologías blockchain y crear una billetera virtual que permita transacciones seguras y transparentes, este proyecto tiene el potencial de mejorar la seguridad y la calidad de los productos agrícolas, así como fomentar prácticas más sostenibles y responsables en la industria alimentaria.

2. Objetivos

Este trabajo de fin de grado se centra en distintos objetivos como:

- Explicar de forma teórica cuándo, qué y para qué sirve la tecnología blockchain adquiriendo con ello un conocimiento previo de qué es esta tecnología, sus distintos tipos y aplicaciones además de, por qué usar esta tecnología y saber el potencial que puede llegar a alcanzar.
- Ver cómo la tecnología Blockchain puede aportar tanto las ventajas e inconvenientes a cada una de las industrias en términos de trazabilidad y transparencia.
- Mejorar la transparencia y la confianza en el mercado de productos agrícolas: La billetera virtual permitirá a los usuarios realizar transacciones de manera segura y transparente, lo que mejorará la confianza de los consumidores en la calidad y la seguridad de los productos agrícolas.
- Promover prácticas más sostenibles y responsables en la producción y distribución de alimentos: Al integrar un sistema de seguimiento de la cadena de suministro, los usuarios podrán ver la procedencia y el historial de los productos que compran, lo que fomentará prácticas más sostenibles y responsables en la producción y distribución de alimentos.
- Facilitar el acceso a productos agrícolas de calidad: La billetera virtual permitirá a los usuarios realizar compras en línea o en tiendas físicas que acepten la billetera virtual como forma de pago, lo que facilitará el acceso a productos agrícolas de calidad.
- Mejorar la seguridad y la calidad de los productos agrícolas: Al integrar un sistema de seguimiento de la cadena de suministro, los usuarios podrán verificar la autenticidad de los productos y tener mayor confianza en la seguridad y la calidad de los productos agrícolas.
- Contribuir a la lucha contra el fraude alimentario: La billetera virtual permitirá a los usuarios realizar transacciones seguras y transparentes, lo que contribuirá a la lucha contra el fraude alimentario y otros problemas relacionados con la falta de transparencia en la cadena de suministro.
- Fomentar la innovación en la industria de los productos agrícolas: La creación de una billetera virtual para productos agrícolas representa una

innovación en la industria, lo que puede fomentar la adopción de nuevas tecnologías y prácticas más sostenibles y responsables en la producción y distribución de alimentos.

- Aprovechar las ventajas de IPFS, como la resistencia a la censura y la capacidad de compartir y acceder a datos de manera eficiente, para garantizar la integridad y disponibilidad de la información transaccional en el contexto de los productos agrícolas.

3. Marco Teórico

3.1. ¿Qué es y cuándo surge la Blockchain?

La tecnología blockchain ha emergido como una innovación revolucionaria que ha transformado radicalmente el panorama del almacenamiento y la transmisión de datos en el entorno digital. Su impacto se ha extendido ampliamente, ya que proporciona un enfoque seguro, transparente e inmutable para el almacenamiento y la transmisión de información[17].

Como estudiante de ingeniería informática, he tenido la oportunidad de explorar y comprender en profundidad el funcionamiento de esta tecnología vanguardista. La blockchain, en su esencia, se basa en una red descentralizada de nodos interconectados que colaboran para validar y registrar las transacciones en una cadena de bloques distribuida. Cada uno de estos nodos alberga una copia completa de la blockchain, garantizando que todos los participantes tengan acceso a la misma información actualizada.

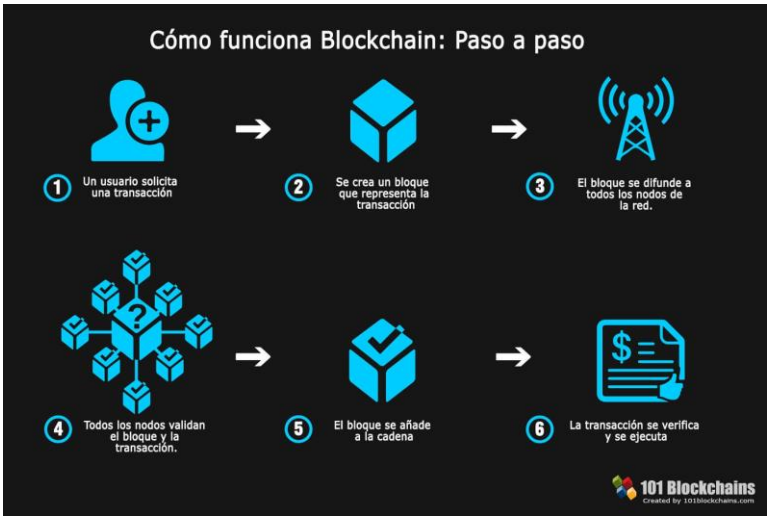


Figura 1. Explicación transacción Blockchain

Recurso: https://101blockchains.com/es/tecnologia-blockchain/

La historia de la tecnología blockchain[18] se remonta al año 2008, cuando un enigmático individuo o grupo conocido como Satoshi Nakamoto presentó un documento trascendental bajo el título "Bitcoin: A Peer-to-Peer Electronic Cash System". Hasta el día de hoy, la identidad precisa de Nakamoto sigue envuelta en un misterio, añadiendo un aura de intriga a su aporte pionero.

En ese influyente documento, Nakamoto sentó los cimientos de la tecnología blockchain como un elemento fundamental en el funcionamiento de la criptomoneda Bitcoin. Su objetivo principal era crear un sistema de efectivo digital peer-to-peer descentralizado, que permitiera a las personas realizar transacciones directas sin necesidad de intermediarios, como los bancos tradicionales. La blockchain se concibió como el componente clave para asegurar estas transacciones de manera segura y preservar la privacidad de los usuarios.

La implementación práctica de la tecnología blockchain tuvo lugar en enero de 2009, con el lanzamiento de la red Bitcoin. Esta red empleaba la cadena de bloques[12] como un libro de contabilidad público y distribuido, donde se registraban todas las transacciones realizadas con la criptomoneda. Cada transacción se agrupaba en bloques y se vinculaba de forma criptográfica con el bloque anterior, creando una cadena inalterable de registros.

A medida que Bitcoin fue adquiriendo popularidad, también lo hizo el interés por la tecnología subyacente de la blockchain. Con el paso de los años, se han desarrollado distintas variantes y aplicaciones de esta tecnología más allá del ámbito de las criptomonedas. Estas variantes incluyen tanto blockchains públicas como privadas, cada una con sus propias características y casos de uso específicos.

Desde su creación, la tecnología blockchain ha experimentado un rápido avance y ha encontrado aplicaciones en diversos sectores y campos, como las finanzas, la logística, la atención médica y la energía, entre otros. Empresas e instituciones de todo el mundo han comenzado a explorar y adoptar la tecnología blockchain con el objetivo de mejorar la eficiencia, la transparencia y la seguridad en sus operaciones.

Si bien la identidad de Satoshi Nakamoto continúa siendo un enigma, su contribución a la tecnología blockchain y Bitcoin es innegable. La publicación de su documento en 2008 marcó el inicio de una revolución tecnológica que sigue transformando nuestra forma de intercambiar valor y gestionar datos en la era digital. La blockchain ha demostrado su capacidad para asegurar la integridad de los datos y facilitar transacciones seguras y transparentes sin depender de intermediarios de confianza. Esta tecnología ha superado barreras tradicionales al permitir transferencias de valor rápidas y económicas a nivel global, sin restricciones geográficas ni barreras de tiempo.

Las aplicaciones de la tecnología blockchain se han expandido a lo largo de diferentes sectores. En el ámbito financiero, la adopción de criptomonedas ha transformado los sistemas de pago y las transacciones financieras. La blockchain ha brindado la posibilidad de realizar transacciones directas y seguras, eliminando intermediarios y reduciendo los costos asociados.

En la industria alimentaria (que es en la que nos vamos a centrar), la trazabilidad y transparencia[20] que ofrece la blockchain han mejorado la seguridad y calidad de los productos. Los consumidores pueden rastrear el origen de los alimentos, desde su producción hasta la venta, lo que ayuda a prevenir fraudes y asegurar la autenticidad de los productos.

Además del que nos vamos a centrar, existen otras áreas donde se está implementando, áreas como las energías renovables, la blockchain ha abierto nuevas oportunidades. Permite la creación de redes energéticas descentralizadas, donde los productores de energía pueden vender su excedente directamente a los consumidores, eliminando intermediarios y fomentando un uso más eficiente de los recursos. Un claro ejemplo que podríamos observar es el de la empresa “Power Ledger”, en el cual su actualmente ex CEO, Éric Larchevêque, dijo esto en su momento:

"La tecnología blockchain puede desbloquear el valor de los activos energéticos distribuidos, permitiendo una mayor eficiencia, resiliencia y sostenibilidad en el suministro de energía" *[6]*

Otra área sería los procesos electorales, (aprovechando actualmente la estafa que se está produciendo en las votaciones municipales) en la que la tecnología blockchain ha demostrado su potencial es en la mejora de la transparencia y seguridad. Al utilizar la blockchain, se puede garantizar la integridad de los votos y prevenir el fraude electoral, lo que fortalece la confianza en los sistemas democráticos. El ejmplo se podría observar en la empresa “Follow My Vote” donde buscan evitar los fraudes electorales usando esta tecnología.

3.2. Tipos de blockchain

Existen distintos tipos de blockchain[3] que, según el acceso a los datos, pueden ser:

- Las blockchain públicas, aquellas en las que no hay restricciones para participar, ya sea en lectura como escritura de datos. En las que destacamos como principales características que se puede entrar y salir fácilmente de ellas, son transparentes y normalmente suelen estar construidas a conciencia, para con trabajar así en un entorno de confianza limitada.
- Las blockchain privadas, tanto la referencia a la escritura como a la lectura de los datos, están limitadas a una lista predefinida de participantes conocidos y de confianza desapareciendo con ello la necesidad de estar construidas a conciencia, ya que el entorno en el que se trabajará será fiable.

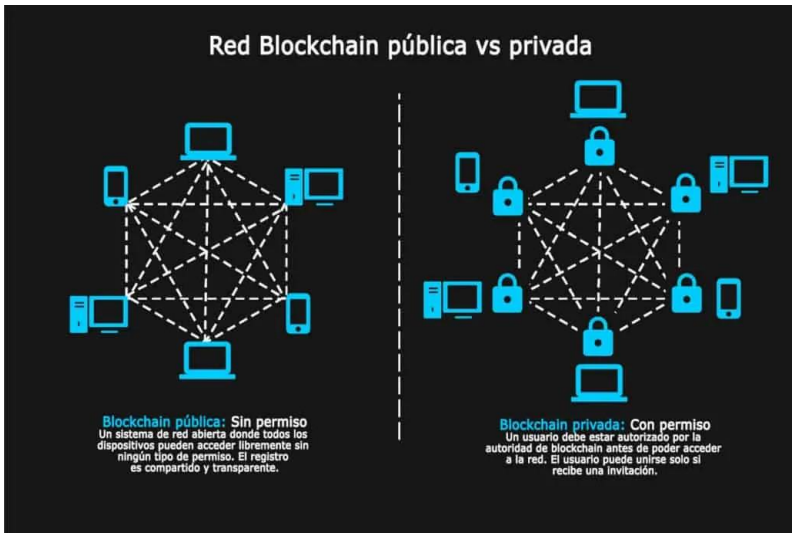


Figura 2. Diferencia Blockchain pública y privada

Recurso: https://academy.bit2me.com/cuantos-tipos-de-blockchain-hay/

- La blockchain Consorcio: Es una blockchain que es gestionada y utilizada por un consorcio o grupo de organizaciones en colaboración. Los participantes comparten la responsabilidad de mantener y validar la cadena de bloques. Esta forma de blockchain se utiliza en casos en los que varias organizaciones necesitan colaborar y compartir información

de manera confiable. Ejemplos de blockchains de consorcio incluyen R3 Corda y Quorum, además de Hyperledger Sawtooth.

- La blockchain Autorizada: También conocida como blockchain de permisos, requiere que los participantes sean autorizados y tengan ciertos permisos para unirse a la red y participar en la validación de transacciones. Estas blockchains se utilizan en entornos donde es necesario controlar la identidad y los privilegios de los participantes. Ejemplos de blockchains autorizadas son Ripple, EOS y Hyperledger Fabric.
- Y, por último, la Blockchain sin permisos: Es una blockchain abierta en la que cualquier persona puede unirse y participar en la validación de transacciones sin requerir autorización previa. Todos los datos en la cadena de bloques son públicos y transparentes. Bitcoin es un ejemplo de blockchain sin permisos.

Si nos centramos de forma general en la blockchain de Hyperledger, es una plataforma descentralizada de permisos diseñada para construir aplicaciones descentralizadas (DApps) o soluciones de libros de contabilidad distribuidos. Proporciona transacciones eficientes, transparencia de datos y trazabilidad, sin necesidad de terceros[1].

Permite rastrear la trazabilidad, el control y la supervisión de datos almacenados en bloques de la cadena de bloques de Hyperledger. Propone un modelo que integra las necesidades de acceso a datos externos e internos con autorizaciones y credenciales para acceder a datos específicos de la cadena de bloques. Se consideran servicios externos, como la cadena de suministro, el acceso de los clientes o las agencias, mientras que los servicios internos incluyen el control y la supervisión del proceso de producción. La plataforma diseñada utiliza contratos inteligentes para proporcionar acceso controlado a los datos y alojar las funciones de libro de contabilidad en la red.

Se establece una política de control de acceso que permite a los participantes acceder a cierta cantidad de contenido o transacciones autorizadas. La red de Hyperledger se compone de organizaciones, canales, miembros, autoridades certificadoras, nodos de pares y aplicaciones de cliente.

Cada organización tiene su propia autoridad certificadora y los nodos de pares almacenan copias del libro de contabilidad. La configuración de la red de Hyperledger y los procesos de transferencia de datos, las aplicaciones de usuario y las bases de datos deben ser diseñados y configurados de acuerdo a las necesidades específicas de cada implementación. En general, Hyperledger ofrece un registro accesible, confiable, verdadero y seguro de todos los procesos y condiciones materiales, y puede ser utilizado en diferentes sectores, como la producción agrícola. Además, el impacto ambiental de la red de Hyperledger es sustancialmente menor en comparación con las redes basadas en criptomonedas debido a los algoritmos de consenso utilizados.

Podemos encontrar distintos tipos de Hyperledger, pero si nos centramos en dos, serían:

- Hyperledger Sawtooth ofrece características como escalabilidad, modularidad y facilidad de desarrollo de aplicaciones. Utiliza un modelo de consenso modular que permite la elección y configuración del algoritmo de consenso más adecuado para tu aplicación. Además, proporciona un entorno flexible para implementar smart contracts y administrar los datos en la red blockchain.
- Hyperledger Fabric es un framework de blockchain empresarial desarrollado por la Fundación Linux bajo la iniciativa de Hyperledger. Está diseñado para permitir la creación de redes de blockchain privadas y permisionadas, adecuadas para casos de uso empresariales.

Figura 3. Hyperledger tipos

Recurso: https://pixelplex.io/blog/top-hyperledger-projects/

En nuestro caso, sería conveniente usar la tecnología blockchain Hyperledger Sawtooth ya que vamos a crear una billetera virtual con Smart contracts (que veremos más adelante) pero me he decantado finalmente por el lenguaje de programación Solidity, ya que usa Ethereum que es una plataforma de blockchain pública y ampliamente adoptada, lo que significa que hay una gran cantidad de desarrolladores, herramientas y recursos disponibles. Además, Solidity es un lenguaje de programación específicamente diseñado para contratos inteligentes en Ethereum, lo que facilita el desarrollo de DApps en esta plataforma.

Ethereum también ofrece una infraestructura establecida y una red de nodos distribuidos que respalda la ejecución de contratos inteligentes. Esto puede ser beneficioso ya que busco una mayor descentralización y seguridad para tu DApp.

Si bien Hyperledger Sawtooth ofrece ventajas como su enfoque modular y su modelo de consenso pluggable, la elección de Solidity y Ethereum puede haberse basado en su popularidad, la disponibilidad de recursos y la infraestructura existente en la red Ethereum.

3.3. Integraciones del blockchain en el modelo de negocio actual y ventajas

El modelo de negocio es una herramienta previa al plan de negocio con el objetivo de permitir conocer con claridad el tipo de negocio que se va a crear, es decir, es la forma en la que la organización crea, entrega y captura valor identificando a quién va dirigido, cómo se va a vender, cómo se va a introducir en el mercado y cómo se van a conseguir los ingresos.

Existen varias formas de evaluar el modelo de negocio[19],pero los más conocidos se pueden dividir en distintos bloques[5]:

- Segmentos de clientes, permite a las empresas dividir a sus consumidores en categorías específicas, basadas en características.

  Por lo que el Blockchain en este caso, puede servir para modificar el contrato inteligente entre proveedor y cliente donde ambas partes configuran los términos del contrato, se almacena en una dirección específica del blockchain y el evento contemplado ocurre.

  En decir, los contratos inteligentes buscan mejorar los contratos actuales siendo más baratos y seguros, ahorrando con ello tiempo y evitando fraudes gracias a la inexistencia de un tercero o intermediario.

  De esta manera, se podría llegar a nuevos segmentos de clientes con nuevos productos, facilitando de esta manera el acceso a mercados inexistentes en previos modelos de negocio generando así nuevas fuentes de ingreso.

- Propuesta de valor la cual comunica cómo satisfacemos las necesidades de nuestros clientes, el blockchain va a cambiar la forma en la que el cliente percibe el valor, ya que conseguirá una mayor disponibilidad de productos o servicios de acuerdo a su necesidad única como es la reducción de costes, gracias al uso de la tecnología.

  Por lo tanto, el cliente lo que compra no es un producto o un servicio, está comprando una solución a un problema y gracias al blockchain le podemos ofrecer más variedad de recursos con menos costes.

- Canales o la forma en la que la organización se comunica con el consumidor final para ofrecerle el valor de nuestro producto o servicio.

  En este apartado, blockchain al requerir menos intermediarios, va hacer que sea más fácil hacer negocios ya que hará que estos sean más rápidos y accesibles en todo momento.

- Relación con el cliente e ingresos son las relaciones que se establece con los segmentos de los clientes (mencionados anteriormente) y el efectivo que genera la organización por cada cliente

  Blockchain cambiará la forma de interactuar con los clientes gracias al autoservicio y la automatización produciendo con ello que el cliente perciba más valor entregado y estaría dispuesto pagar un sobreprecio por ese mismo recurso.

Además, en las asociaciones clave, blockchain nos proporcionará más transparencia y seguimiento en la integración del proceso productivo con ayudas como la reducción de inventarios, mejorar la distribución de productos, así como mejorar el plan de producción.

3.4. Inconvenientes o preocupaciones que pueden surgir con blockchain.

La tecnología blockchain, al ser una innovación relativamente nueva, genera dudas y preocupaciones en personas y entidades debido a la falta de conocimiento seguro y confiable sobre su funcionamiento. Estas dudas se relacionan principalmente con los costos y riesgos asociados, similares a cualquier inversión en tecnología nueva

Los inconvenientes o riesgos de la tecnología blockchain se pueden clasificar en diversas categorías:

- Fiabilidad, seguridad y privacidad, porque blockchain es una tecnología conceptualmente muy segura, pero se ve expuesta en el curso de su implementación a errores y vulnerabilidades propios de cualquier sistema de información.

  Además, a esto se le suman los retos de seguridad y tecnología por su progresiva madurez, complejidad y falta de estandarización.

- La escalabilidad o adaptación que puede tener para adaptarse al incremento de la demanda sin que se vea perjudicado su valor ya que con blockchain se pretende llegar a un gran número de personas.
- Confidencialidad y transparencia: necesidad de contratos entre las empresas participantes en la cadena para garantizar un cierto nivel de confidencialidad.
  Para que se pueda equilibrar la confidencialidad, la transparencia juega un papel clave.
- Preservación de la ventaja competitiva: problema para muchas empresas, ya que la industria está llena de secretos y cada empresa tiene su "fórmula" que la diferencia del resto y con blockchain estos secretos deben mostrarse para ser una empresa "transparente".
- Participación y adaptación: uno de los principales problemas de esta tecnología porque todas las partes del proceso del producto o servicio deben adoptar esta tecnología para que funciones.

Por lo que, la duda por la capacidad que puede tener blockchain para poder gestionar todas las transacciones es un gran riesgo porque si el número de transacciones creciera demasiado rápido, los nodos no serían capaces de seguir el ritmo.

Debido a este problema, podríamos presentar un cuello de botella presentando ineficiencia por el bajo nivel de transacciones que se pueden llegar a hacer provocando con ello un retraso en las operaciones y limitando a su vez el resto de transacciones.

3.5. Beneficios y aplicaciones de las criptomonedas y la tecnología blockchain

Un claro ejemplo en la actualidad, sería el término criptomonedas o criptodivisas. Estas son un tipo de moneda digital que utiliza criptografía para proporcionar un sistema de pagos seguro. La tecnología blockchain desempeña un papel fundamental en el funcionamiento de las criptomonedas, ya que proporciona un registro compartido de todas las transacciones y establece un método descentralizado de validación, lo que facilita el intercambio digital de dinero entre usuarios de forma directa.

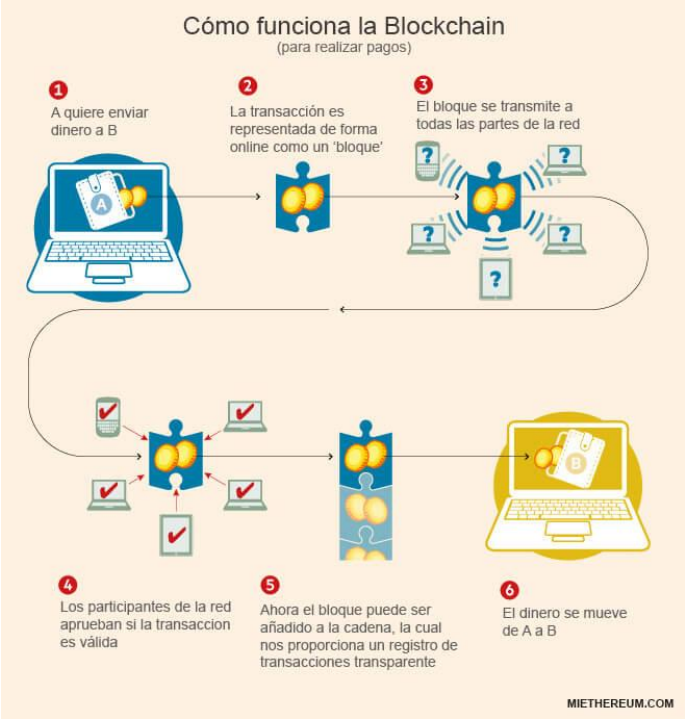


Figura 4. Transacción de pagos con Blockchain

Recurso: https://www.miethereum.com/blockchain/

El uso de las criptomonedas y el blockchain pueden proporcionarnos distintos ámbitos beneficiosos como:

- Transacciones financieras internacionales: ya que gracias al blockchain se mejora la eficiencia de los pagos internacionales por la reducción de costes que puede conllevar y una mayor velocidad en las transacciones si lo comparamos con sistemas con una elevada centralización operativa.

- Reducción de la economía sumergida: ya que podrían diseñarse mecanismos que facilitaran la identificación de actividades ilegales a pesar de que una de las principales propiedades de las criptomonedas es la anonimidad de las transacciones.
- Promover la inclusión financiera de los países emergentes: o subdesarrollados donde una parte importante de la población no está desbancarizada, es decir, promover a aquellos países más tercermundistas que no tienen cuentas de banco propias y gracias a las criptomonedas podrían almacenarlas fácilmente gracias a un monedero digital vinculado a su teléfono.

3.6. Blockchain en las empresas

Anteriormente, hemos visto que el blockchain ofrece grandes ventajas y comodidades que muchas empresas pueden aprovechar para con ello, obtener una posición ventajosa respecto a las demás empresas.

De esta manera, estaríamos ayudando a las pequeñas empresas proporcionándoles un acceso asequible a las nuevas tecnologías e impulsando la adopción masiva del blockchain[21].

En España, las pequeñas y medianas empresas lideran el uso de la tecnología blockchain, en concreto, el 60% de las microempresas invierte más del 50% de su inversión a este tipo de tecnología considerándola como una prioridad estratégica. Como observamos, dichas microempresas conocen las grandes ventajas que aporta y el poder transformador que conlleva el invertir en él.

En este contexto, como dice un gran experto como es Pablo García Mexia, director del área de derecho tecnológico de la empresa Herbert Smith Freehills dedicada a los servicios jurídicos:

"Invertir en Blockchain, podríamos decir que es invertir en competitividad y en puestos de trabajo presentes y futuros"

Además, dicha empresa afirma que no es preciso ser ingeniero criptográfico ni informático, para poder utilizar la tecnología Blockchain, ya que, a través de su aplicación, aplican los contratos inteligentes.

Por otro lado, casi el 50% de las grandes empresas españolas estaban a favor de implementar las tecnologías blockchain y criptográficas ya no solo para mantener una posición ventajosa respecto a sus competidores, si no que más bien para aumentar la seguridad de sus empresas porque es un tema muy preocupante en la actualidad, por la constante amenaza de robos y exposición de datos a las que se enfrenta por culpa de múltiples hackers.

Por ejemplo, según la lista Forbes[4] (una de las revistas más importantes en el mundo de las empresas), los requisitos para estar en su lista de TOP 50 empresas de blockchain se podrían dividir en dos requisitos, por un lado (el más obvio) que se haga un uso relevante de blockchain en sus respectivos negocios y, por otro lado,

que se tenga un ingreso anual o valoración superior a 1.000 millones de dólares, dejando atrás a aquellas empresas medianas o startups creadas como nativas blockchain.

En este ranking podríamos encontrar empresas conocidas como Adobe, Allianz Seguros y Boeing.

Según Ignacio Cobisa, analista senior de la empresa IDC Research España que es el principal proveedor mundial de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumo, afirma que a causa de la pandemia, muchas empresas ya no están invirtiendo tanto en tecnologías con poco enfoque en optimización de costos o continuidad de negocio, sino más bien, han comenzado a invertir en el desarrollo de servicios blockchain donde:

> "*La curva de crecimiento Blockchain sigue siendo muy relevante, especialmente en el desarrollo de servicios asociados a esta tecnología, donde la tasa de crecimiento anual compuesta es del 52,6% hasta el 2024*".

3.7. Conclusión de invertir en la blockchain

Por todo lo mencionado anteriormente, afirmamos que el Blockchain tiene un gran impacto en todos los aspectos del modelo de negocio, ya sea pequeña, mediana o gran empresa, en el que, dependiendo de cada organización, será más sencillo generar o conseguir ventajas en distintos aspectos.

A pesar de esto, algunas empresas aún se mantienen alejadas de esta tecnología, aunque haya evidencia de las grandes ventajas que esta tecnología aporta. Esto podría ser a causa de los costos de la implementación de Blockchain, estos costos son elevados porque se requieren desarrolladores especializados y esfuerzos de integración complicados.

Además de los elevados costes, muchas empresas también se alejan de esta tecnología por las restricciones regulatorias, que son un gran obstáculo especialmente para proyectos innovadores como podrían ser los contratos inteligentes en aplicaciones financieras y médicas.

Muchas empresas para poder evitar estos obstáculos que tiene Blockchain, realizan colaboraciones entre organizaciones consiguiendo con ello nuevas construcciones en formas más eficientes, por ejemplo, llegando a aumentar el rendimiento, reduciendo con ello el tiempo de procesamiento de minutos a milisegundos.

Por lo que podemos apreciar, es importante aceptar esta tecnología blockchain ya que ofrece muchas ventajas.

En la actualidad, existen muchos proyectos en diferentes organizaciones, desde startups y emprendedores hasta grandes empresas que finalmente llegarán al mercado y ayudarán a dar confianza en la tecnología Blockchain.

4. Blockchain en el sector agroalimentario

Una vez introducido y explicado el término Blockchain, nos centraremos en lo más importante de este proyecto, que es, la llegada de esta tecnología al sector agroalimentario.

A pesar de que la tecnología blockchain se aplicó al principio sobre todo en el sector financiero, en los últimos años se han desarrollado aplicaciones de la tecnología para sectores distintos, y la cadena agroalimentaria no es una excepción.

En la cadena agroalimentaria, la tecnología blockchain[14] presenta grandes ventajas en aquellos casos donde se requiere transparencia, colaboración entre distintos actores, transacciones costosas en tiempo o dinero y en aquellos casos donde se quiere impulsar que los distintos actores de la cadena tengan un peso similar ya que todos ellos comparten la misma información en tiempo real.

Es necesaria la implantación de esta tecnología, cuando aparece la preocupación de los consumidores respecto a la seguridad alimentaria de los productos que llegan al mercado cuando estos han sido producidos en países con una regulación alimentaria distinta. Por lo que, el blockchain viene a cubrir esta preocupación, certificando de una manera incuestionable toda la cadena de vida de un producto, principalmente, en aquellos casos en los que hay numerosas partes implicadas y grandes volúmenes de datos, como es en este caso, el sector de la alimentación.

Es decir, blockchain nos proporcionaría un “rastreo” de los alimentos desde los proveedores al consumidor final. Aumentando con ello su visibilidad de la línea de producción para ofrecer alimentos de mejor calidad en el mercado, afrontando con ellos los retos principales a los que se enfrenta el sector alimentario como: ayudar a la transparencia de las operaciones, contribuir a la seguridad alimentaria, reducir el desperdicio de alimentos, optimizar la producción, favorecer los pagos y contratos automatizados, prevenir el fraude alimentario, el comercio internacional y hacer que el suministro de los alimentos se más sostenible con el medio ambiente.

Nos centraremos en ambas características, la trazabilidad y la transparencia a la hora de realizar las operaciones:

4.1. Trazabilidad y transparencia de operaciones

Al principio de introducirse el blockchain en este sector, el término que se usaba era el Porkchain, una solución de trazabilidad para la industria alimentaria[7] en la que, básicamente es una aplicación de blockchain entendida como un servicio que ayuda a verificar la información.

La finalidad de esta primera tecnología era sustituir los documentos físicos, por documentos digitales que estén certificados por blockchain. Con esto, se reducirían los errores y se podría garantizar la trazabilidad, además de evitar tanto "papeleo" en las trazabilidades.

En cuanto a la trazabilidad con Blockchain[23], se permite verificar los intercambios que se provocan desde que el alimento sale del complejo agroindustrial hasta la posición final del producto, indicando con ello la fecha, hora, lugar y demás datos relacionados incluyendo con ello las distintas etapas en su recorrido.

Además, también recoge datos de GPS para la información de la ubicación por lo que, las empresas pueden ubicar rápidamente el producto en la cadena de suministro, un claro ejemplo, podría ser productos afectados por una posible contaminación en una cierta ubicación o una rotura de la cadena del frío si este lo necesitara, permitiendo así la retirada de los lotes afectados.

Por otro lado, la transparencia es el beneficio estrella de esta tecnología porque con el blockchain todas las transacciones son visibles para todas las partes interesadas. En el que, un estudio realizado por Morning Consult para IBM, empresa multinacional estadounidense de tecnología y consultoría, confirmaba que muchos de los consumidores, en este caso españoles, querían saber más sobre los productos que va a consumir en busca de su autenticidad y más de la mitad estarían dispuestos a cambiar de producto para que fuera más sostenible en el planeta.

La diferencia de estos dos tipos de características más relevantes, la explica en una entrevista exclusiva Sebastián Priolo, CEO & Co-Fundador de Woza Labs, empresa dedicada a los proyectos digitales con la tecnología Blockchain:

"La diferencia entre ambas es que la transparencia tiene que ver con mostrar el proceso que se hace y brindar uno o varios puntos de acceso al usuario. Se trata de generar una ventana hacia lo que se está haciendo. Mientras que la trazabilidad tiene como objetivo medir el proceso con herramientas específicas con el fin de mejorarlo".

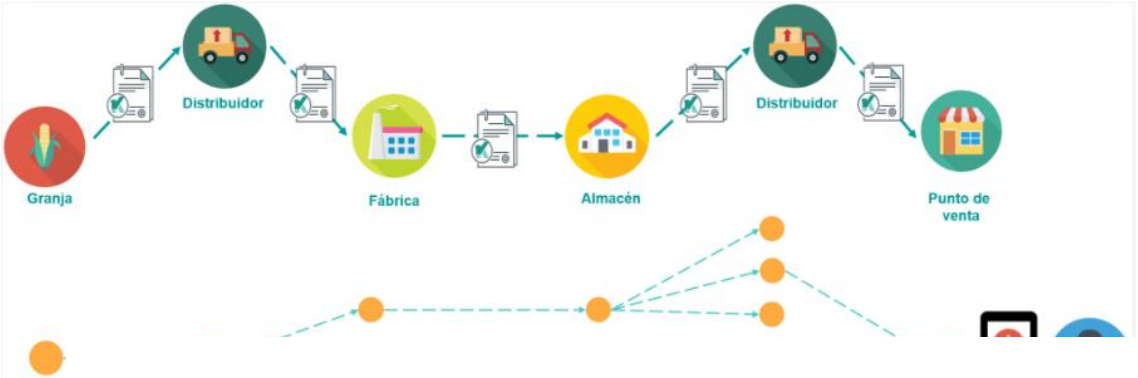


Figura 5. Blockchain en el sector agroalimentario

Recurso: https://www.threepoints.com/blog/aplicaciones-de-Blockchain-en-la-industria-alimentaria

De las características más importantes que engloban todo lo que Blockchain beneficia al sector agroalimentario, podemos desglosar algunas muy importantes que hace falta remarcar como lo son:

4.1.1. Contribuir a la seguridad alimentaria

El control de cada paso del alimento mencionado anteriormente en la trazabilidad, lleva a demostrar que el producto no ha sufrido ninguna incidencia que pudiera poner en riesgo la salud del consumidor final.

Por lo que, un aumento de calidad del proceso nos asegura una disminución de los riesgos sanitarios.

Además, la cadena de bloques garantiza que en la trazabilidad de los alimentos no haya intromisiones, frenando con ello la posibilidad de prácticas fraudulentas o engaños en cualquiera de las etapas por las que pasa el producto hasta llegar al consumidor final.

Estas prácticas o engaños fraudulentos, darían pie a la frase mencionada por Miguel Flavián, fundador de la consultora de distribución alimentaria GM&CO:

"Los registros quedan todos asociados a la persona o equipo que los sube a la cadena, y si estos se modifican con posterioridad, queda así reflejado y es posible para el resto de agentes de la cadena tener constancia de esto. Por lo tanto, puede llegar a suponer una barrera más para el fraude".[2]

Además de esto, menciona que, si la información que es subida es de fiar o no, afirmando con ello que, para garantizar la seguridad de este proceso, es necesario integrar más aplicaciones que permitan verificar la calidad de la información.

Un ejemplo para poder verificar la calidad de la información, sería asociar a la cadena información de autenticidad en el origen de la cadena, como test de ADN o químicos con el fin de verificar que el producto sigue siendo el mismo y no ha habido sustitución.

4.1.2. Reducir el desperdicio de alimentos y optimización de la producción

Gracias a la seguridad alimentaria que nos proporciona la tecnología blockchain, podemos reducir drásticamente el desperdicio de alimentos que se producen, ya que dicha tecnología, como hemos mencionado anteriormente, al tener el control de cada situación por la que pasa el producto, podemos saber si ciertos productos están en mal estado y eliminarlos, haciendo que el resto de alimentos que iban en ese lote no sean desperdiciados.

Por otro lado, el mayor conocimiento de todo el proceso que recorre un alimento, provocará que se disponga de la información necesaria para ahorrar tanto en costes como en tiempo.

4.1.3. Favorecer los pagos y contratos automatizados

Blockchain permite reducir los tiempos de pago gracias a los contratos inteligentes o más bien conocidos como *Smart Contract*. Que realmente, son contratos en los que se define qué se puede hacer, de qué manera y que podría pasar si algo de lo estipulado no se cumple. Pero lo que destaca el *Smart Contract*[15] , es la manera de realizar estas estipulaciones ya que es capaz de ejecutar y hacer por él mismo de manera automática sin necesidad

de ningún intermediario. Todo esto sucede gracias a códigos informáticos, es decir, a programación pura.

Por eso, estos contratos, permitirían realizar además de pagos normales, pagos automatizados a proveedores, según los días establecidos que se estipule en el contrato, evitando así cualquier retraso que se pudiera producir o incluso incumplimiento de pago, cosa que beneficia mucho a los proveedores[16].

4.1.4. Comercio Internacional

Como hemos mencionado anteriormente, Blockchain permite registrar datos virtuales y seguros al brindar información en tiempo real sobre las transacciones entre grupos, ya sean miembros de una corporación o una cadena de abastecimiento internacional. Además de, ofrecer un registro inalterable, cifrado, seguro y transparente y accesible para todos los participantes, por lo que Blockchain, está muy relacionada con el comercio exterior por la necesidad que tienen los consumidores de obtener las grandes ventajas que brinda esta tecnología.

De esta manera, la cadena de valor tan amplia que supone el comercio internacional, se agilizaría adoptando Blockchain ya que nos ayudaría en áreas como la logística gracias a la trazabilidad de las mercancías, el transporte y las gestiones aduaneras compartiendo información en tiempo real de las diferentes etapas que atraviesan los bienes, el financiamiento garantizando la seguridad de pagos y también, trámites administrativos contribuyendo a la mejora del funcionamiento de los servicios públicos y privados asociados.

De esta manera, Blockchain brinda muchas soluciones a las largas operaciones comerciales que se realizan al simplificar el intercambio transfronterizo, contribuir a mejoras competitivas y reducir los costes de transacción entre proveedor y cliente final.

Cabe destacar, que esta tecnología ya se estaba utilizando anteriormente de una manera más “lenta”, pero con la llegada de la crisis sanitaria del Covid-19, se ha vuelto mucho más importante.

4.1.5. Sostenible con el medio ambiente

La sostenibilidad medioambiental también es un gran motivo de compra por parte de muchos consumidores finales, que este, no quiere que el producto participe en procesos de producción que sean nocivos para el entorno.

Sobre todo, en la actualidad, después de una crisis generada por el Covid-19, que obligó a atender inmediatamente los temas reflejados con la seguridad de las personas, tanto alimentarias como físicas.

Bien es cierto, que ya había un segmento de consumidores que apostaban por la comida orgánica y ecológica, conocida también como “comida real”. Pero, debido a la gran crisis que provocó la pandemia, el consumidor tuvo una creciente preocupación por la salud, seguridad de las personas… siendo nuevos intereses y preferencias para este segmento.

Por lo tanto, gracias a la información que blockchain aporta como: las condiciones en las que vive un animal, materiales de empaque y la manera como se procesan los alimentos, son aspectos que el cliente valorará mucho en este sector, “obligando” a las empresas a invertir en esta tecnología si quieren que el consumidor siga siendo su principal referente.

5. Introducción en empresas del sector agroalimentario

Por las características de trazabilidad y transparencia tan importantes que demostraba la tecnología Blockchain en el sector agroalimentario, gran parte del sector agroalimentario en Europa vio una gran oportunidad invertir en esta tecnología para poder ser más competente junto a las otras empresas que ya estaban utilizando esta tecnología.

Primero, apareció con la empresa Nespresso, empresa líder en cápsulas de café, máquinas y accesorios de café, por la necesidad que tenían los consumidores en saber de dónde provenía el café, como mencionaba el CEO de Nespresso, Guillaume Le Cunff:

"Sabemos que los consumidores están cada vez más interesados en saber de dónde viene su café. Gracias a nuestro Programa AAA Sustainable Quality ™, hemos certificado el origen y la trazabilidad en nuestra cadena de valor durante más de 15 años. Me complace afirmar que gracias a la iniciativa del blockchain, ahora podemos dar un paso más e invitar a nuestros clientes a descubrir a los agricultores detrás de su café de Zimbabwe".

Más tarde, en concreto en el año 2017, apareció en grandes superficies en Europa como los supermercados Carrefour convirtiéndose en una empresa pionera en la utilización de Blockchain para el almacenamiento y transmisión de información de un artículo en todas sus etapas de la cadena de suministro, desde la producción hasta la distribución, alcanzando con ello unos niveles de seguridad máximos.

Para este proyecto, contaron con la ayuda de la plataforma IBM trust food, red de colaboración de productores, mayoristas, distribuidores, fabricantes… que mejora la visibilidad y responsabilidad en toda la cadena de suministro de alimentos, en el cual el cliente, para que pueda realizar el rastreo y tracking de todos los procesos de las etapas de la cadena de suministro, tras asegurarse de que la información que se le está proporcionando es transparente, se le proporciona una combinación de barras y cuadros que acompaña a un producto para que pueda ser leído y descifrado mediante un lector óptico que transmite los datos, más bien conocido como código QR.

6. Implementación blockchain y mejoras al aplicarla

La implementación de la tecnología blockchain en la agricultura ha sido objeto de creciente interés en los últimos años, ya que se espera que esta tecnología pueda mejorar significativamente la eficiencia y la rentabilidad de las operaciones agrícolas. Para evaluar la eficacia de la implementación de la blockchain en la agricultura, se podría realizar un estudio de caso que demostraría cómo esta tecnología puede mejorar la eficiencia y la rentabilidad de las operaciones agrícolas.

En este estudio, se implementaría la tecnología blockchain en una empresa agrícola que produce frutas y verduras para el mercado local. Antes de la implementación de la blockchain, la empresa tenía dificultades para rastrear sus productos desde el campo hasta el mercado. Los registros se mantenían en papel y los datos se perdían con frecuencia, lo que dificultaba el seguimiento de la cadena de suministro y la identificación de posibles problemas. Además, los consumidores no tenían acceso a información detallada sobre los productos que compraban, lo que limitaba su capacidad para tomar decisiones informadas.

Después de la implementación de la blockchain, la empresa pudo rastrear sus productos desde el campo hasta el mercado con facilidad. Se creó un registro digital de cada producto que incluía información detallada sobre su origen, fecha de cosecha, fecha de envasado y otros detalles relevantes. Estos registros se almacenaron en la blockchain, lo que garantizó su seguridad y trazabilidad.

Además, los consumidores pudieron acceder a información detallada sobre los productos que compraban utilizando nuestra solución de cartera virtual. Podían ver información sobre el origen y la calidad de los productos, lo que les permitía tomar decisiones informadas sobre su compra. Esto mejoró la transparencia en la cadena de suministro y aumentó la confianza de los consumidores en los productos agrícolas.

La implementación de la blockchain también permitió a la empresa reducir los costos y aumentar la eficiencia. Antes de la implementación, la empresa tenía que dedicar una gran cantidad de tiempo y recursos para mantener registros en papel y coordinar con otros actores de la cadena de suministro. Con la implementación de la blockchain, estos procesos se automatizaron y se volvieron más eficientes. Además,

la empresa pudo identificar áreas donde se podían mejorar los procesos y reducir los costos.

Figura 6. Mejoras blockchain en la agricultura

Recurso: https://www.innovaciondigital360.com/agrotech/como-el-

Podemos observar que, nuestro estudio de caso demuestra que la implementación de la blockchain en la agricultura puede mejorar significativamente la eficiencia y la rentabilidad de las operaciones agrícolas. La tecnología blockchain permite la creación de registros digitales seguros y trazables que mejoran la transparencia en la cadena de suministro y aumentan la confianza de los consumidores en los productos agrícolas. Además, permite a las empresas reducir costos y aumentar la eficiencia al automatizar procesos y mejorar la coordinación con otros actores de la cadena de suministro

7. Desafíos legales y regulatorios de la blockchain en la agricultura.

La implementación de la tecnología blockchain en la agricultura presenta varios desafíos legales y regulatorios que deben ser abordados para aprovechar al máximo los beneficios de esta tecnología. La blockchain es una tecnología relativamente nueva que ha demostrado su capacidad para mejorar la eficiencia, seguridad y transparencia en la cadena de suministro de alimentos. Sin embargo, la adopción de la blockchain en la agricultura puede ser limitada por barreras financieras, tecnológicas y regulatorias. En esta sección, se describen algunos de los principales desafíos legales y regulatorios que enfrenta la blockchain en la agricultura y cómo pueden ser abordados, como, por ejemplo:

- Privacidad y protección de datos: Uno de los principales desafíos legales y regulatorios de la blockchain en la agricultura es la privacidad y protección de datos. La blockchain es una tecnología que permite el almacenamiento y la transmisión de datos de forma segura y transparente, pero también puede presentar riesgos para la privacidad y protección de datos personales. En la agricultura, donde se manejan datos sensibles sobre la producción de alimentos, es importante que las empresas agrícolas que implementan la tecnología blockchain en sus operaciones tengan en cuenta las regulaciones de protección de datos personales y tomen medidas para garantizar que los datos sean almacenados y transmitidos de forma segura y legal.

  Para abordar este desafío, las empresas agrícolas pueden implementar medidas técnicas y organizativas para garantizar la privacidad y protección de datos personales. Por ejemplo, pueden utilizar técnicas de cifrado para proteger los datos almacenados en la blockchain y establecer políticas claras para el acceso y uso de los datos. Además, deben asegurarse de cumplir con las regulaciones de protección de datos personales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

- Interoperabilidad: Otro desafío legal y regulatorio importante es la interoperabilidad entre diferentes sistemas blockchain. La interoperabilidad

se refiere a la capacidad de diferentes sistemas blockchain para comunicarse entre sí y compartir información. En la agricultura, donde hay múltiples actores involucrados en la cadena de suministro, es importante que los sistemas blockchain sean interoperables para garantizar una trazabilidad efectiva y eficiente.

Para abordar este desafío, los reguladores deben trabajar con las empresas agrícolas y los desarrolladores de tecnología para establecer estándares y protocolos para la interoperabilidad de la blockchain. Esto puede incluir el desarrollo de interfaces estándar y la creación de un marco regulatorio que fomente la interoperabilidad entre diferentes sistemas blockchain.

- Regulación: Además, la regulación de la blockchain en la agricultura puede ser un desafío, ya que la tecnología es relativamente nueva y no está completamente comprendida por los reguladores. Los reguladores deben trabajar con las empresas agrícolas y los desarrolladores de tecnología para establecer políticas y regulaciones claras que fomenten la innovación y la adopción de la blockchain en la agricultura.

  Para abordar este desafío, los reguladores pueden establecer un marco regulatorio claro que fomente la innovación y la adopción de la blockchain en la agricultura. Esto puede incluir la creación de incentivos fiscales y financieros para las empresas agrícolas que adoptan la tecnología blockchain, así como la colaboración con los desarrolladores de tecnología para establecer estándares y protocolos para la implementación de la blockchain en la agricultura.

- Barreras financieras y tecnológicas: por último, la adopción de la blockchain en la agricultura puede ser limitada por barreras financieras y tecnológicas. La implementación de la blockchain requiere una inversión significativa en tecnología y capacitación, lo que puede ser un obstáculo para las empresas agrícolas más pequeñas.

> Para abordar este desafío, los reguladores pueden establecer programas de financiamiento y subvenciones para apoyar la adopción de la blockchain en la agricultura. Además, las empresas agrícolas pueden colaborar con los desarrolladores de tecnología para establecer soluciones de blockchain que sean asequibles y fáciles de implementar.

Es decir, la implementación de la tecnología blockchain en la agricultura presenta varios desafíos legales y regulatorios que deben ser abordados para aprovechar al máximo los beneficios de esta tecnología. Es importante que los reguladores trabajen con las empresas agrícolas y los desarrolladores de tecnología para establecer políticas y regulaciones claras que fomenten la innovación y la adopción de la blockchain en la agricultura.

Además, es importante que las empresas agrícolas que implementan la tecnología blockchain en sus operaciones tengan en cuenta las regulaciones de protección de datos personales y tomen medidas para garantizar que los datos sean almacenados y transmitidos de forma segura y legal. También es crucial que se establezcan estándares y protocolos para la interoperabilidad de la blockchain, lo que permitirá una trazabilidad efectiva y eficiente en la cadena de suministro de alimentos.

Por último, es fundamental que se aborden las barreras financieras y tecnológicas que pueden limitar la adopción de la blockchain en la agricultura. Los reguladores pueden establecer programas de financiamiento y subvenciones para apoyar la adopción de la blockchain en la agricultura, y las empresas agrícolas pueden colaborar con los desarrolladores de tecnología para establecer soluciones de blockchain asequibles y fáciles de implementar.
En resumen, podemos afirmar que la implementación de la tecnología blockchain en la agricultura tiene el potencial de mejorar significativamente la eficiencia, seguridad y transparencia en la cadena de suministro de alimentos. Sin embargo, para aprovechar al máximo los beneficios de esta tecnología, es necesario abordar los desafíos legales, regulatorios, financieros y tecnológicos que presenta. Con la colaboración entre reguladores, empresas agrícolas y

desarrolladores de tecnología, la blockchain puede transformar la forma en que se produce, distribuye y consume alimentos en todo el mundo.

8. Evaluación de los riesgos de seguridad asociados de la blockchain en la agricultura y cómo mitigarlos.

La implementación de la tecnología blockchain en la agricultura presenta varios desafíos y riesgos de seguridad que deben ser evaluados y mitigados para garantizar la integridad, privacidad y confidencialidad de los datos almacenados en la blockchain. En esta sección, se describen algunos de los principales riesgos de seguridad asociados con la implementación de la blockchain en la agricultura y cómo pueden ser mitigados.

- Riesgos de seguridad en la privacidad de los datos: Uno de los principales riesgos de seguridad asociados con la implementación de la blockchain en la agricultura es la privacidad de los datos almacenados en la blockchain. La blockchain es una tecnología que permite el almacenamiento y la transmisión de datos de forma segura y transparente, pero también puede presentar riesgos para la privacidad y protección de datos personales. En la agricultura, donde se manejan datos sensibles sobre la producción de alimentos, es importante que las empresas agrícolas que implementan la tecnología blockchain en sus operaciones tengan en cuenta las regulaciones de protección de datos personales y tomen medidas para garantizar que los datos sean almacenados y transmitidos de forma segura y legal.

  Para mitigar este riesgo, las empresas agrícolas pueden implementar medidas técnicas y organizativas para garantizar la privacidad y protección de datos personales. Por ejemplo, pueden utilizar técnicas de cifrado para proteger los datos almacenados en la blockchain y establecer políticas claras para el acceso y uso de los datos. Además, deben asegurarse de cumplir con las regulaciones de protección de datos personales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

- Riesgos de seguridad en la integridad de los datos: Otro riesgo de seguridad asociado con la implementación de la blockchain en la agricultura es la integridad de los datos almacenados en la blockchain. La blockchain es una tecnología que permite el almacenamiento de datos de forma inmutable y

resistente a la manipulación, pero también puede presentar riesgos de seguridad en caso de que alguien pueda acceder a la clave privada y manipular los datos almacenados en la blockchain.

Para mitigar este riesgo, las empresas agrícolas pueden implementar medidas técnicas y organizativas para garantizar la integridad de los datos almacenados en la blockchain. Por ejemplo, pueden utilizar técnicas de cifrado para proteger los datos almacenados en la blockchain y establecer políticas claras para el acceso y uso de los datos. Además, deben asegurarse de que las claves privadas estén protegidas y almacenadas de forma segura para evitar su acceso no autorizado.

- Riesgos de seguridad en la disponibilidad de los datos: Un tercer riesgo de seguridad asociado con la implementación de la blockchain en la agricultura es la disponibilidad de los datos almacenados en la blockchain. La blockchain es una tecnología que permite el almacenamiento y la transmisión de datos de forma descentralizada y distribuida, pero también puede presentar riesgos de seguridad en caso de que alguien pueda interferir en el funcionamiento de la red blockchain y afectar la disponibilidad de los datos almacenados en ella.

  Para mitigar este riesgo, las empresas agrícolas pueden implementar medidas técnicas y organizativas para garantizar la disponibilidad de los datos almacenados en la blockchain. Por ejemplo, pueden utilizar técnicas de redundancia y replicación para garantizar que los datos estén disponibles incluso en caso de fallos en la red blockchain. Además, deben asegurarse de que la red blockchain esté protegida contra ataques externos y que se realicen regularmente pruebas de seguridad para identificar y mitigar posibles vulnerabilidades.

- Riesgos de seguridad en la interoperabilidad de la blockchain: Otro riesgo de seguridad asociado con la implementación de la blockchain en la agricultura es la interoperabilidad de la blockchain. La interoperabilidad se refiere a la capacidad de diferentes blockchains para comunicarse y compartir

información entre sí. En la agricultura, donde se manejan múltiples cadenas de suministro y sistemas de información, es importante que las blockchains sean interoperables para garantizar una trazabilidad efectiva y eficiente en la cadena de suministro de alimentos.

Para mitigar este riesgo, es importante que se establezcan estándares y protocolos para la interoperabilidad de la blockchain. Los reguladores pueden trabajar con las empresas agrícolas y los desarrolladores de tecnología para establecer políticas y regulaciones claras que faciliten la interoperabilidad de las blockchains en la agricultura. Además, las empresas agrícolas pueden implementar medidas técnicas para garantizar la interoperabilidad de las blockchains. Por ejemplo, pueden utilizar tecnologías de puente (bridge technologies) que permitan la comunicación entre diferentes blockchains y establecer políticas claras para el intercambio de información entre ellas.

Después de observar el contenido anterior, la implementación de la tecnología blockchain en la agricultura presenta varios desafíos y riesgos de seguridad que deben ser evaluados y mitigados para garantizar la integridad, privacidad y confidencialidad de los datos almacenados en la blockchain. Las empresas agrícolas pueden implementar medidas técnicas y organizativas, así como trabajar con reguladores y desarrolladores de tecnología para establecer políticas y regulaciones claras que faciliten la implementación segura y efectiva de la blockchain en la agricultura.

9. Análisis de las soluciones existentes en el mercado para la digitalización de procesos agrícolas.

La digitalización de procesos agrícolas[22] se ha convertido en una necesidad imperante en el sector agroalimentario. En la actualidad, existen diversas soluciones en el mercado que buscan abordar esta necesidad, desde aplicaciones móviles hasta sistemas de gestión de datos y plataformas de comercio electrónico especializadas en productos agrícolas. Sin embargo, muchas de estas soluciones no garantizan la seguridad y la trazabilidad de los productos agrícolas, lo que puede resultar en pérdidas económicas y daños a la salud pública.

Para evaluar la eficacia de nuestra solución de cartera virtual en comparación con estas alternativas, se realizó un análisis detallado de las características y funcionalidades de cada una.

En primer lugar, se identificó que muchas de las soluciones existentes no utilizan tecnología blockchain para garantizar la seguridad y la trazabilidad de los productos agrícolas. En cambio, se basan en sistemas centralizados que pueden ser vulnerables a ataques cibernéticos y manipulaciones de datos. Por otro lado, nuestra solución de cartera virtual utiliza la tecnología blockchain para garantizar la seguridad y la transparencia en todas las transacciones.

En segundo lugar, se evaluó la facilidad de uso y la accesibilidad de cada solución. Se encontró que muchas de las aplicaciones móviles y plataformas de comercio electrónico eran difíciles de usar para los agricultores y otros actores del sector agroalimentario debido a su complejidad y falta de personalización. En contraste, nuestra solución de cartera virtual es fácil de usar y está diseñada específicamente para satisfacer las necesidades del sector agroalimentario. Además, nuestra solución permite a los agricultores y otros actores del sector agroalimentario acceder a la información detallada sobre la cadena de suministro, lo que les permite tomar decisiones informadas sobre la compra y venta de productos agrícolas.

En tercer lugar, se evaluó la capacidad de cada solución para integrarse con otros sistemas y tecnologías. Se encontró que muchas de las soluciones existentes no permiten la integración con otros sistemas y tecnologías, lo que puede limitar su eficacia y utilidad. En contraste, nuestra solución de cartera virtual se integra

perfectamente con otros sistemas y tecnologías, lo que permite a los agricultores y otros actores del sector agroalimentario aprovechar al máximo las ventajas de la tecnología blockchain.

Por lo que, nuestro análisis indica que nuestra solución de cartera virtual basada en blockchain es una alternativa superior a las soluciones existentes en el mercado para la digitalización de procesos agrícolas. Proporciona una mayor seguridad y trazabilidad, es fácil de usar y está diseñada específicamente para satisfacer las necesidades del sector agroalimentario. Además, permite la integración con otros sistemas y tecnologías, lo que maximiza su eficacia y utilidad

10. Tecnología IPFS

El InterPlanetary File System (IPFS), que significa Sistema de Archivos Interplanetario, es una tecnología innovadora diseñada para abordar los desafíos asociados con el almacenamiento y la distribución de archivos en la web tradicional. A diferencia de los enfoques tradicionales que se basan en la ubicación física de los archivos, IPFS se basa en un sistema de direcciones únicas llamadas CID (Content Identifier), que se generan a partir del contenido del archivo mismo. Esto permite que los archivos se almacenen y se accedan de manera descentralizada, sin depender de un servidor centralizado.

La descentralización es uno de los principales conceptos subyacentes en IPFS. Utilizando una red peer-to-peer, IPFS descentraliza el almacenamiento y la distribución de archivos, eliminando la necesidad de un servidor centralizado como intermediario. En lugar de confiar en un solo punto de falla, los archivos se encuentran redundantes en múltiples nodos de la red. Esto aumenta la resiliencia y la resistencia a la censura, ya que la eliminación o el bloqueo de un nodo no afectaría la disponibilidad del archivo. Además, la descentralización en IPFS permite una mayor escalabilidad, ya que más nodos pueden unirse a la red y contribuir con su capacidad de almacenamiento y ancho de banda.

Otro aspecto importante de IPFS es su enfoque en la eficiencia en la transferencia de archivos. IPFS divide los archivos en bloques más pequeños y utiliza algoritmos de enrutamiento para buscar y obtener esos bloques desde los nodos más cercanos en la red. Esto permite una transferencia de archivos más rápida y eficiente, especialmente cuando varios usuarios están descargando el mismo archivo. Los bloques compartidos se pueden obtener de forma simultánea, lo que reduce la carga en la red y acelera la velocidad de transferencia.

La integridad de los archivos es una preocupación fundamental en cualquier sistema de almacenamiento y distribución de archivos. IPFS aborda este desafío utilizando identificadores únicos para cada archivo, conocidos como CID. Estos identificadores se generan a partir del contenido del archivo utilizando funciones de hash criptográficas, lo que garantiza que cualquier cambio en el contenido del archivo generará un CID diferente. Esto permite verificar la integridad de los archivos descargados mediante la comparación de los CID. Además, los CID permiten un acceso rápido y eficiente a los

archivos, ya que se utilizan como identificadores únicos para localizar y recuperar el contenido deseado.

La integración de IPFS con la tecnología blockchain ofrece numerosas ventajas y aplicaciones en una billetera virtual o, en nuestro caso, en AgroWallet. En lugar de almacenar los documentos directamente en la cadena de bloques, que puede resultar costoso y poco eficiente debido a los límites de tamaño y costo de almacenamiento, IPFS proporciona una forma de almacenar los documentos de manera descentralizada y garantizar su inmutabilidad. En este contexto, cuando se realiza una transacción de compra en la blockchain, se genera un documento que contiene detalles como la información del comprador, el vendedor, los productos comprados, el precio, entre otros.

Este documento se puede convertir en un formato compatible con IPFS y almacenarse en la red IPFS. Cada documento tendría su propio CID único, que se utilizaría para acceder y verificar su contenido. Esto permite un acceso rápido y eficiente a los documentos y garantiza su disponibilidad incluso si los nodos de almacenamiento originales están desconectados. Además, al utilizar la infraestructura existente de la red IPFS, se logra una mayor escalabilidad, eficiencia y resiliencia en la gestión de los archivos asociados a las transacciones de la billetera virtual.

Una de las principales ventajas de IPFS en la integración con AgroWallet es su capacidad para ofrecer un almacenamiento seguro y descentralizado de los documentos relacionados con las transacciones. Al utilizar IPFS, los documentos se almacenan en múltiples nodos de la red, lo que aumenta la seguridad y la redundancia de los archivos. Esto garantiza que los documentos sean accesibles y estén protegidos de la pérdida de datos o la manipulación no autorizada.

Además, la integración de IPFS en AgroWallet proporciona una forma eficiente de compartir archivos entre los usuarios. Los archivos almacenados en IPFS pueden ser compartidos fácilmente utilizando los CID como identificadores únicos. Los usuarios pueden acceder y descargar los archivos utilizando el CID, lo que facilita la transferencia de información relevante, como recibos de transacciones, contratos inteligentes y registros de actividad.

Otra ventaja de IPFS es su capacidad para garantizar la disponibilidad de los archivos incluso en situaciones de conectividad limitada. Dado que los archivos se almacenan en múltiples nodos de la red IPFS, los usuarios pueden acceder a los documentos incluso si los nodos de almacenamiento originales están desconectados o inaccesibles. Esto mejora la experiencia del usuario al garantizar que los archivos estén disponibles cuando más se necesitan.

Es decir, la tecnología IPFS ofrece una solución innovadora para el almacenamiento y la distribución de archivos descentralizados. Su enfoque en la descentralización, la eficiencia en la transferencia de archivos y la integridad de los mismos lo convierten en una opción ideal para la integración en una billetera virtual. IPFS proporciona un almacenamiento seguro y descentralizado de documentos relacionados con transacciones, facilita el intercambio eficiente de archivos entre usuarios y garantiza la disponibilidad de los archivos incluso en condiciones de conectividad limitada. Al aprovechar las ventajas de IPFS, AgroWallet puede ofrecer una experiencia escalable, eficiente y segura para los usuarios.

11. Descripción de la propuesta

- Introducción: El sector agrícola se enfrenta a desafíos significativos en términos de eficiencia, transparencia y acceso al mercado. En el modelo tradicional, los productores agrícolas a menudo dependen de intermediarios para llegar a los consumidores finales, lo que puede resultar en precios más bajos y una menor participación en los beneficios. Además, los compradores pueden tener dificultades para rastrear la procedencia y calidad de los productos agrícolas que adquieren. Para abordar estas problemáticas, he desarrollado una solución innovadora: una billetera virtual basada en blockchain que facilita la compra y venta directa de productos agrícolas entre los participantes.

- Problema actual: El problema central en el mercado agrícola es la presencia de intermediarios, que actúan como intermediarios entre los productores y los consumidores finales. Estos intermediarios pueden agregar costos adicionales y reducir los beneficios para los agricultores, quienes a menudo se ven obligados a aceptar precios más bajos por sus productos. Además, la falta de trazabilidad y transparencia en la cadena de suministro dificulta que los compradores puedan verificar la calidad y origen de los productos agrícolas que adquieren. Esto genera desconfianza y limita las oportunidades de los productores para llegar a nuevos mercados y obtener mejores precios por sus productos.

- Solución propuesta: Nuestra solución se basa en una billetera virtual basada en blockchain, que aprovecha la tecnología descentralizada y segura para permitir transacciones directas entre productores y compradores de productos agrícolas. La plataforma funciona como un mercado en línea donde los productores pueden listar sus productos y los compradores pueden explorar y adquirir los productos directamente de los productores, sin la necesidad de intermediarios. Al eliminar a los intermediarios, los agricultores pueden establecer precios más justos para sus productos y obtener una mayor participación en los beneficios.

  La tecnología blockchain utilizada en la billetera virtual proporciona una mayor transparencia y trazabilidad en la cadena de suministro agrícola. Cada producto agrícola registrado en la plataforma se acompaña de información detallada,

incluyendo su origen, métodos de producción, certificaciones y otros detalles relevantes. Los compradores pueden acceder a esta información y verificar la autenticidad y calidad de los productos antes de realizar una compra. Esto fomenta la confianza y brinda a los compradores la tranquilidad de saber de dónde provienen los productos que están adquiriendo.

Además, nuestra plataforma utiliza la criptomoneda Ethereum como medio de pago, lo que proporciona una serie de beneficios tanto para los productores como para los compradores. Al utilizar Ethereum, se reducen los costos y la complejidad asociada con las transacciones internacionales, lo que facilita el comercio global de productos agrícolas. También elimina las barreras de los sistemas de pago tradicionales y las fluctuaciones de las tasas de cambio, lo que simplifica el proceso de compra y pago para los participantes.

Al enfocarnos exclusivamente en productos agrícolas, nuestra aplicación se posiciona como una fuente confiable y especializada en este sector. Esto nos permite construir una sólida reputación y experiencia en el mercado agrícola, lo que a su vez atrae tanto a productores como a compradores interesados en una plataforma especializada y confiable para llevar a cabo sus transacciones.

12. Sistema distribuido

El sistema distribuido que he realizado para crear una billetera virtual para el sector agroalimentario con transacciones blockchain e IPFS tiene los siguientes componentes:

- Interfaz de usuario (UI): La interfaz de usuario permitirá a los usuarios interactuar con la billetera virtual. Podría incluir funciones como la visualización del saldo, la creación de nuevas transacciones y la consulta de transacciones anteriores (histórico). La UI también debe proporcionar opciones para cargar y descargar archivos adjuntos relacionados con las transacciones utilizando IPFS.

- Blockchain: Utilizará una tecnología blockchain para almacenar y gestionar las transacciones de la billetera virtual. Cada transacción incluirá información relevante, como el remitente, el destinatario y el monto.

- IPFS: La red IPFS se utilizará para almacenar los archivos adjuntos de las transacciones, como recibos, facturas o cualquier otro tipo de documento relacionado. En lugar de almacenar directamente los archivos en la cadena de bloques, se guardará el CID del archivo en la transacción correspondiente.

- Validación de transacciones: Cada vez que se realice una transacción, se validarán los fondos disponibles en la billetera del remitente y se comprobará si el destinatario es válido. Esto garantizará la integridad y seguridad de las transacciones.

- Visualización de transacciones: La billetera virtual permite a los usuarios ver todas las transacciones pasadas, incluidos los detalles de cada transacción, como el remitente y el Smart contract que se ha utilizado para ello.

Como podemos observar, así quedaría nuestro sistema distribuido, utilizando los distintos servicios y lenguajes de programación que más tarde detallaré:

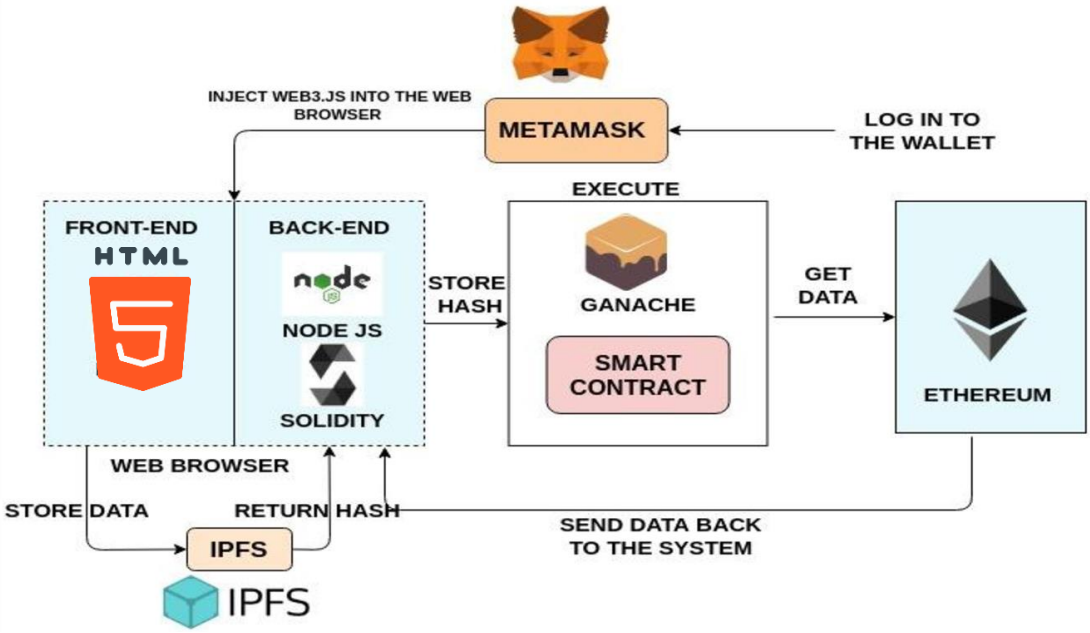


Figura 7. Sistema distribuido

Recurso: https://www.ijeast.com/papers/554-562,Tesma502,IJEAST.pdf

13. Análisis y diseño de software

El desarrollo de sistemas y aplicaciones requiere una planificación adecuada y una comprensión clara de los procesos que se llevarán a cabo. Para ello, es fundamental contar con herramientas que permitan visualizar y comunicar de manera efectiva el flujo de interacciones entre los diferentes elementos del sistema. Una opción popular y ampliamente utilizada en el campo del análisis y diseño de software es la arquitectura de capas y el diagrama de secuencia.

La arquitectura de capas es un enfoque estructural que organiza un sistema en capas o niveles lógicos, donde cada capa tiene una responsabilidad específica y se comunica con las capas adyacentes de acuerdo con una serie de reglas predefinidas. Cada capa se encarga de una funcionalidad o tarea particular, lo que permite una separación clara de las preocupaciones y facilita el mantenimiento, la escalabilidad y la reutilización del código.

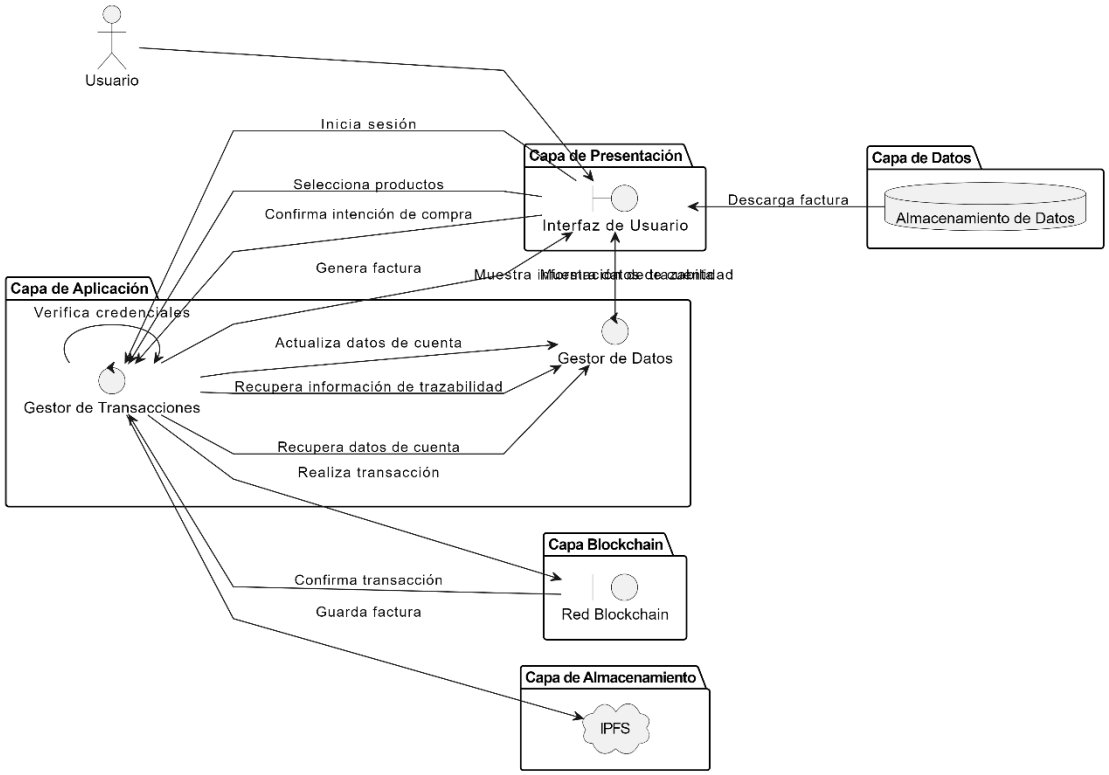
Para alcanzar el diseño de una arquitectura de capas en AgroWallet, he seguido los siguientes pasos:

- Identificación de las responsabilidades: Analicé las diferentes funcionalidades y componentes del sistema, como la interfaz de usuario, la autenticación, la gestión de cuentas, la selección de productos, la generación de facturas y los servicios de Metamask, IPFS y la blockchain Ethereum. Cada una de estas funcionalidades se asignó a una capa correspondiente.
- Definición de las capas: Creé las capas de la arquitectura de acuerdo con las responsabilidades identificadas. Estas capas incluyen la Capa de Presentación, la Capa de Aplicación y la Capa de Servicios.
- Establecimiento de las interacciones: Determiné las interacciones entre las capas, definiendo cómo se comunican y colaboran entre sí. Por ejemplo, la Capa de Presentación interactúa con la Capa de Aplicación para iniciar sesión y seleccionar productos, mientras que la Capa de Aplicación se conecta con los servicios de Metamask, IPFS y la blockchain Ethereum para procesar transacciones y almacenar facturas.
- Creación del diagrama de capas: Utilicé herramientas como PlantUML para crear un diagrama de capas visualmente representativo de la arquitectura. El

diagrama muestra las capas y las relaciones entre ellas, proporcionando una visión clara de la estructura y el flujo de interacciones del sistema.

En el contexto de AgroWallet, la arquitectura de capas proporciona beneficios significativos, como la modularidad, la flexibilidad y la escalabilidad. Permite una separación clara de las responsabilidades, lo que facilita el mantenimiento y la evolución del sistema a medida que se agregan nuevas funcionalidades.

A continuación, se muestra el diagrama de capas correspondiente a la arquitectura de AgroWallet:



Este diagrama ilustra la estructura y las interacciones entre las capas de la arquitectura, brindando una visión general del diseño del sistema y su organización en componentes funcionales.

Por otro lado, el diagrama de secuencia es una representación gráfica que muestra la secuencia de interacciones entre los objetos que participan en un proceso o escenario específico. Se centra en el orden temporal de los mensajes y las respuestas entre los diferentes elementos del sistema, lo que permite comprender cómo se comunican y colaboran para lograr un objetivo común.

En el caso de AgroWallet, el diagrama de secuencia resulta especialmente útil para visualizar el flujo de interacciones entre el usuario, la aplicación, Metamask, la blockchain y la tecnología IPFS. Permite representar de manera clara y detallada las acciones y respuestas que ocurren en cada paso del proceso, desde el inicio de sesión del usuario hasta la descarga de la factura y el almacenamiento de la información.

Ventajas del diagrama de secuencia en el contexto del proyecto de billetera virtual:

- Claridad visual: El diagrama de secuencia proporciona una representación visual clara y fácil de entender de las interacciones entre los diferentes elementos del sistema. Esto facilita la comprensión y comunicación de los procesos involucrados en el proyecto de la billetera virtual.
- Enfoque en la secuencia temporal: El diagrama de secuencia muestra el orden cronológico de los mensajes y respuestas entre los objetos, lo que permite comprender el flujo lógico de las interacciones. Esto es especialmente relevante en el contexto de una billetera virtual, donde es fundamental seguir una secuencia específica de pasos para garantizar la seguridad y precisión de las transacciones.
- Identificación de errores y mejoras: El diagrama de secuencia permite identificar posibles problemas o errores en el flujo de interacciones. Al visualizar las secuencias de mensajes, se pueden identificar cuellos de botella, redundancias o falta de comunicación entre los elementos del sistema. Esto facilita la detección temprana de posibles mejoras y optimizaciones en el proceso.

Por lo que, en AgroWallet, para poder brindar todas estas ventajas, he usado un diagrama de secuencia que representa el flujo de interacciones entre las entidades involucradas en el proceso siguiendo estos pasos:

1. El usuario inicia sesión en la aplicación proporcionando sus credenciales de acceso.
2. La aplicación verifica las credenciales del usuario y autentica su identidad.
3. Una vez autenticado, la aplicación recupera los datos de la cuenta del usuario, como su historial de transacciones y el saldo disponible.
4. La aplicación muestra los datos de la cuenta al usuario en la interfaz de usuario.
5. El usuario selecciona los productos que desea comprar, como hortalizas, frutas y verduras, desde la lista de opciones disponibles.

6. La aplicación recupera la información de trazabilidad de los productos seleccionados, que incluye detalles como el lugar de origen, los métodos de cultivo utilizados y las certificaciones correspondientes.
7. La aplicación muestra la información de trazabilidad al usuario, proporcionándole transparencia sobre el origen y la calidad de los productos.
8. El usuario confirma su intención de compra y procede a realizar la transacción.
9. La aplicación se conecta con Metamask, una billetera virtual que permite realizar transacciones en la red Ethereum.
10. Metamask solicita la confirmación del usuario para realizar la transacción y desbloquea la cuenta de Ethereum correspondiente.
11. La aplicación genera una transacción de compra, que incluye los detalles de los productos, la cantidad y el precio total.
12. La transacción se envía a la red Ethereum para su procesamiento.
13. La red Ethereum valida y registra la transacción en la blockchain.
14. Una vez confirmada la transacción, se actualiza el saldo de la cuenta del usuario y se registra la nueva transacción en el historial.
15. La aplicación genera una factura de compra que incluye los detalles de la transacción, como la lista de productos, la cantidad, el precio unitario y el total.
16. La factura se guarda en la tecnología IPFS (InterPlanetary File System) para garantizar la integridad y disponibilidad de los documentos.
17. El usuario puede descargar la factura desde la aplicación, lo que le permite almacenarla o imprimirla según sea necesario.

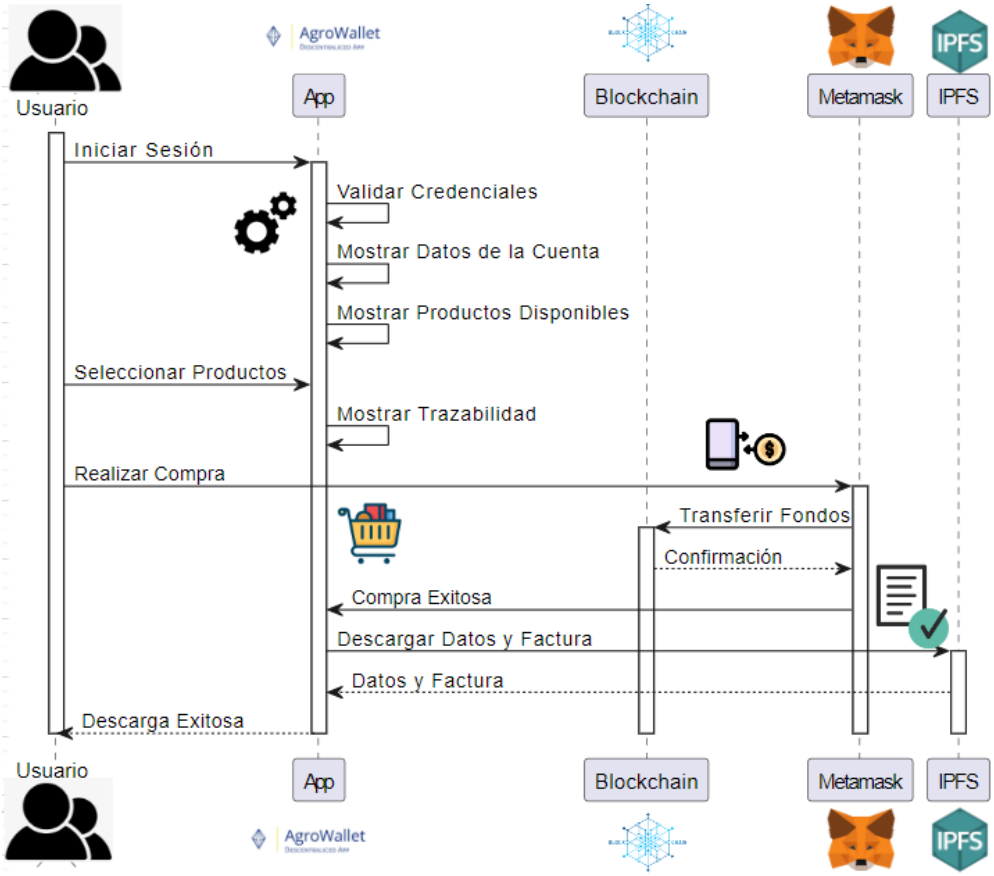


Figura 9. Diagrama de secuencia

Este diagrama de secuencia representa de manera detallada el flujo de interacciones y acciones entre el usuario, la aplicación, Metamask, la red Ethereum y la tecnología IPFS durante el proceso de la billetera virtual.

Además, para crear el diagrama, se utilizó la herramienta Draw.io. Esta herramienta es una aplicación web gratuita que permite crear y editar diagramas de forma visual. Es ampliamente utilizada para crear diagramas de procesos, como el que se muestra aquí, y ofrece una interfaz intuitiva y una amplia variedad de elementos y símbolos gráficos para representar diferentes elementos y acciones en el proceso.

En conclusión, he utilizado la arquitectura de capas y el diagrama de secuencia en AgroWallet, mi billetera virtual, por varias razones fundamentales.

En primer lugar, la arquitectura de capas proporciona una estructura organizativa clara y modular para el sistema. Al dividir las responsabilidades en capas distintas, como la Capa de Presentación, la Capa de Aplicación y la Capa de Servicios, se logra una separación de preocupaciones que facilita el mantenimiento, la escalabilidad y la reutilización del código. Cada capa tiene una función específica y se comunica con las capas adyacentes de acuerdo con reglas definidas, lo que permite un desarrollo eficiente y una gestión más sencilla del sistema.

Además, el uso del diagrama de secuencia en AgroWallet ha sido fundamental para visualizar y comunicar el flujo de interacciones entre los diferentes elementos del sistema. Este diagrama muestra la secuencia ordenada de mensajes y respuestas entre los objetos involucrados en un proceso o escenario específico. En el caso de AgroWallet, el diagrama de secuencia permite representar de manera clara y detallada las acciones y respuestas que ocurren en cada paso del proceso, desde la autenticación del usuario hasta la generación de facturas y el almacenamiento de información en servicios externos como Metamask, IPFS y la blockchain Ethereum.

La combinación de la arquitectura de capas y el diagrama de secuencia en AgroWallet proporciona una visión integral del sistema y facilita la comprensión tanto de su estructura organizativa como de sus interacciones funcionales. La arquitectura de capas garantiza la modularidad y la claridad en la distribución de responsabilidades, mientras que el diagrama de secuencia muestra de manera visual y secuencial cómo los diferentes elementos del sistema se comunican y colaboran entre sí.

En resumen, la elección de la arquitectura de capas y el diagrama de secuencia en AgroWallet ha sido clave para un diseño estructurado y una comunicación efectiva en el desarrollo de la billetera virtual. Estas herramientas han permitido una planificación adecuada, una comprensión clara de los procesos y una visualización detallada de las interacciones, lo que contribuye a la calidad, el mantenimiento y la evolución exitosa del sistema AgroWallet.

14. Aplicación descentralizada, usos y procesos

AgroWallet es una innovadora aplicación de billetera virtual diseñada específicamente para la industria agrícola. Esta plataforma utiliza tecnología blockchain y herramientas avanzadas de gestión de datos para mejorar la eficiencia y la transparencia en el sector agrícola.

Con AgroWallet, los agricultores, productores y compradores pueden interactuar de manera segura y confiable, llevando a cabo transacciones comerciales directas sin la necesidad de intermediarios tradicionales. La aplicación ofrece un entorno digital donde los usuarios pueden explorar una amplia gama de productos agrícolas, revisar sus características y realizar compras de manera eficiente además de otras características.

A continuación, se presenta una descripción de los pasos involucrados en el uso de AgroWallet:

1. **Inicio:** Iniciamos la aplicación AgroWallet y pulsamos para conectarnos a nuestra cuenta de Metamask, donde introduciremos usuario y contraseña.

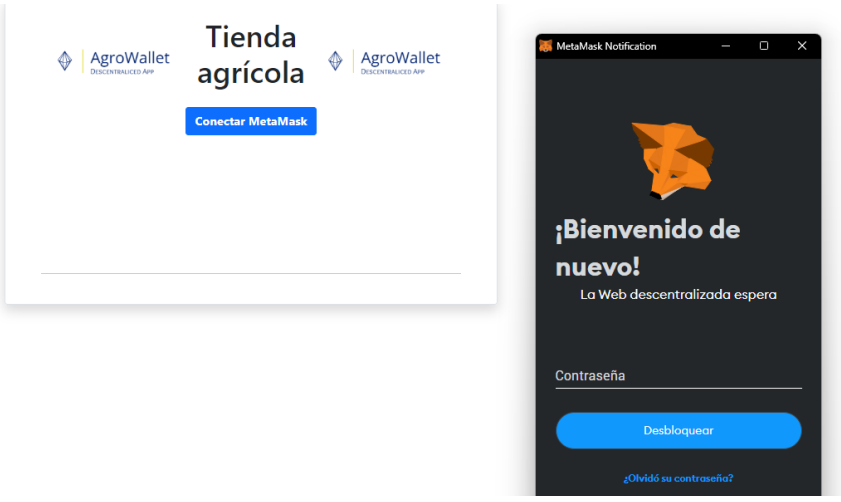


Figura 10. Inicio AgroWallet

2. **Balance y cuenta:** Una vez iniciada la sesión, podremos ver la dirección de nuestra cuenta, podremos ver el balance, el historial de nuestras transacciones con los Smart contracts que hemos realizado y la tabla de productos agrícolas que podemos elegir.

En nuestro caso, al crear de nuevo nuestra cuenta, le hemos añadido 21.000.000 DTFG que será la criptomoneda que usaremos para las transacciones

Figura 11. Ejemplo balance y cuenta AgroWallet

3. **Trazabilidad[11]:** Procederemos a la selección de nuestro producto, en este caso, una pera de la sección de frutas donde podremos consultar la trazabilidad del producto y además, ofrecer un QR donde nos enviará a la página donde se encuentra toda esta información para con ello, mostrar transparencia y que la trazabilidad del producto es correcta.

Figura 12. Ejemplo trazabilidad producto agrícola

4. **Transferencia:** Añadiremos la cantidad en kg que se requieran comprar y haremos la transferencia al proveedor de dicho producto.

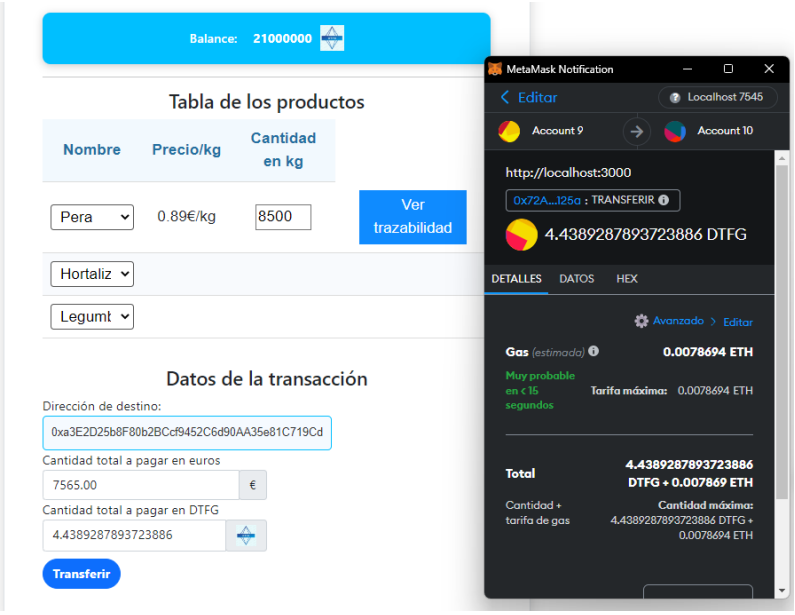


Figura 13. Ejemplo transferencia de porducto

Se desplegará el servidor de Metamask mostrando los datos de la transacción, la cuenta a la que se va a enviar y el monto total así como la cantidad de gas (pequeña comisión) que se aplicará a la transacción. Finalmente, la transacción se realizará y se mostrará este mensaje.

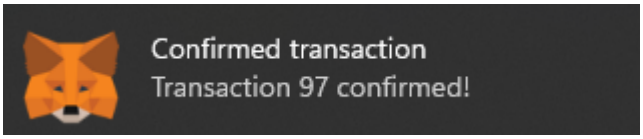


Figura 14. Ejemplo de notificación Metamask

5. **Factura:** Realizada la transacción, se podrá ver la factura de la compra que se ha realizado. Mostrando con ello, el producto, las cantidades y precio, su trazabilidad, el monto total y la dirección a la que se ha enviado.

Figura 15. Ejemplo factura compra realizada

6. **Descarga e IPFS:** Podremos seleccionar en descargar nuestra factura y crearla y añadirle la tecnología IPFS (explicada detalladamente antes) de esta manera:
   Nos mostrará una ventana para poder subir el archivo que hemos descargado llamado FacturaTransaccion.pdf

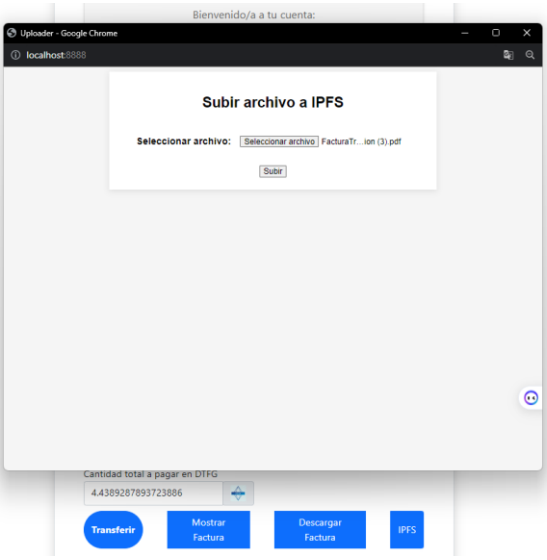


Figura 16. Ejemplo pantalla subida archivo IPFS

Una vez generado correctamente, nos mostrará este mensaje y nos redirigirá a la página donde se ha cargado el archivo con IPFS:

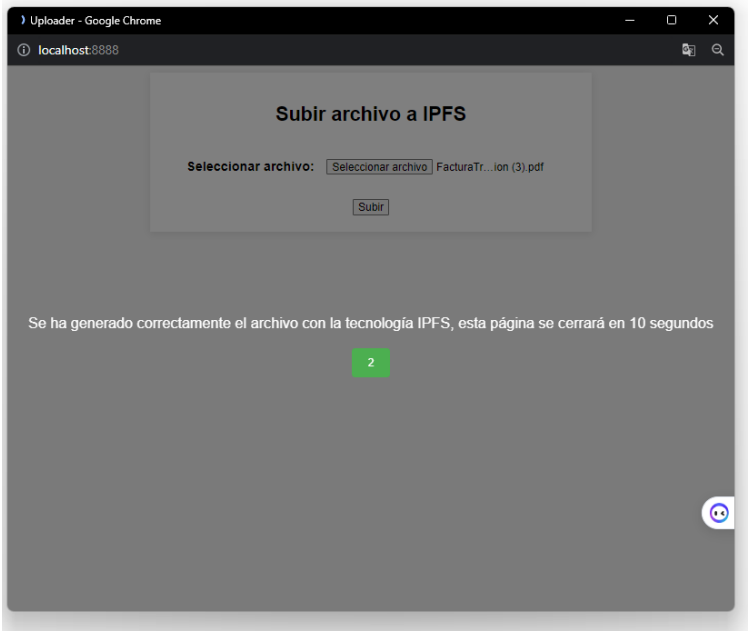


Figura 17. Ejemplo mensaje subida archivo IPFS

Finalmente, observaremos el documento con la tecnología IPFS en pdf, pudiendo descargarlo, imprimirlo y compartirlo:

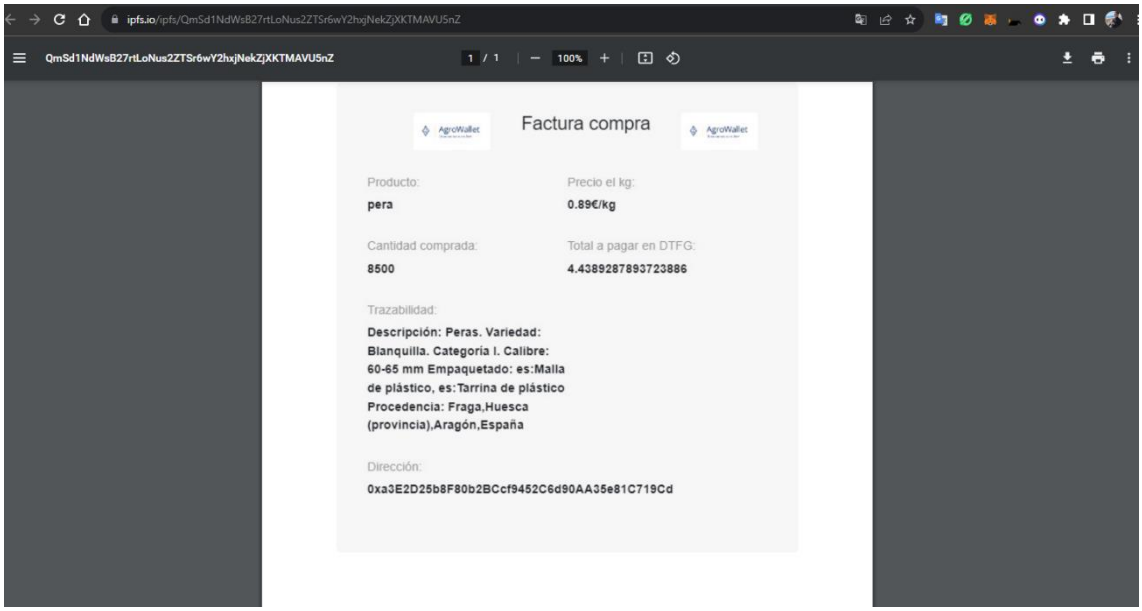


Figura 18. Ejemplo archivo cargado con IPFS

Estos serían los pasos que hemos seguido para poder realizar una transacción correcta en nuestra aplicación descentralizada o Agrowallet.

Para poder demostrar que el proceso ha sido correcto, vemos a continuación los balances de la cuenta que hemos hecho la transferencia, así como el balance de la cuenta al que le hemos hecho el pedido (cuenta del proveedor).

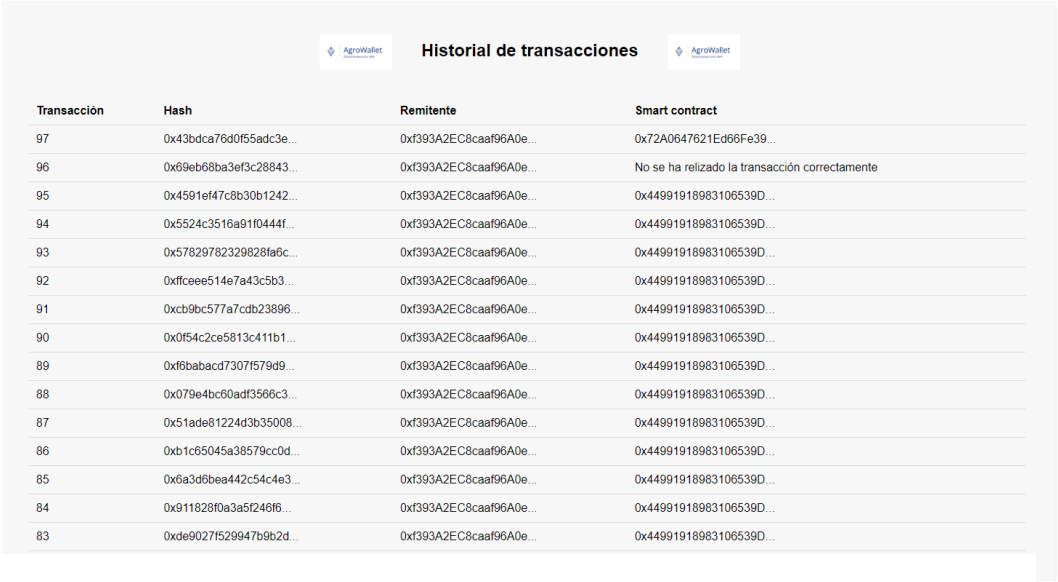
Cuenta que hemos realizado la transferencia, donde observamos la reducción de DTFG:

Figura 19. Ejemplo balance reducido por la transacción realizada

Cuenta que ha recibido los DTFG (vaciada con antelación para poder ver el ejemplo más claro):

Figura 20. Ejemplo balance incrementado por la transacción recibida

Por último, mostrar el historial de transacciones de la cuenta que hemos hecho la transferencia:



Historial de transacciones

Transacción	Hash	Remitente	Smart contract
97	0x43bdca76d0f55adc3e...	0xf393A2EC8caaf96A0e...	0x72A0647621Ed66Fe39...
96	0x69eb68ba3ef3c28843...	0xf393A2EC8caaf96A0e...	No se ha relizado la transacción correctamente
95	0x4591ef47c8b30b1242...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
94	0x5524c3516a91f0444f...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
93	0x57829782329828fa6c...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
92	0xffceee514e7a43c5b3...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
91	0xcb9bc577a7cdb23896...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
90	0x0f54c2ce5813c411b1...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
89	0xf6babacd7307f579d9...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
88	0x079e4bc60adf3566c3...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
87	0x51ade81224d3b35008...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
86	0xb1c65045a38579cc0d...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
85	0x6a3d6bea442c54c4e3...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
84	0x911828f0a3a5f246f6...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...
83	0xde9027f529947b9b2d...	0xf393A2EC8caaf96A0e...	0x44991918983106539D...

Figura 21. Ejemplo historial transacciones

Como podemos observar, he añadido transferencias a distintos tipos de contrato desde esa cuenta, generando para cada transacción su hash correspondiente, añadiendo … al para no mostrar la cuenta, contrato o dirección entera y si la transacción se rechazaba por insuficiencia de saldo o simplemente pulsando el botón de rechazar, mostrando el mensaje de “No se ha realizado la transacción correctamente”.

15. Software y servicios utilizados

- **Interfaz para la gestión de ETH**

Figura 22. Ganache

Recurso: https://trufflesuite.com/blog/ethereum-gas-exactimation/

Ganache es una aplicación de escritorio que se utiliza para crear y gestionar redes privadas de Ethereum. Es una herramienta muy útil para desarrolladores de blockchain, ya que les permite probar y depurar sus aplicaciones descentralizadas (dApps) en un entorno seguro y controlado. Ganache proporciona una interfaz gráfica de usuario (GUI) para crear y configurar redes privadas de Ethereum, así como para crear cuentas de usuario y realizar transacciones de prueba. También ofrece herramientas de depuración y registro para ayudar a los desarrolladores a identificar y solucionar problemas en sus dApps[9] .

En esta imagen podemos ver la interfaz gráfica mencionada anteriormente, así como las direcciones que se han utilizado para realizar las transacciones e implementar nuestra billetera virtual:

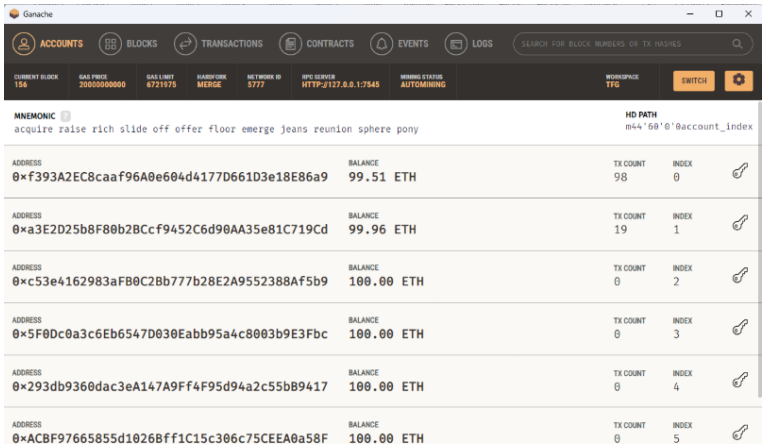


Figura 23. Interfaz gráfica Ganache

- **Cartera para las criptomonedas e interacción con nuestra dApp**

Figura 24. Metamask

Recurso: https://www.finect.com/wallets/metamask

Metamask es una cartera de criptomonedas y una extensión de navegador que permite a los usuarios interactuar con aplicaciones descentralizadas (DApps) basadas en la tecnología blockchain. Fue desarrollada inicialmente para la red Ethereum, pero ahora también es compatible con otras redes blockchain.

Ofrece varios servicios y funcionalidades[8], pero los que nosotros vamos a usar principalmente son:

- Cartera de criptomonedas: Metamask permite a los usuarios almacenar, enviar y recibir criptomonedas, como Ether (ETH) y tokens ERC-20, de forma segura. Los usuarios tienen el control total de sus claves privadas, lo que les permite acceder y gestionar sus fondos de forma descentralizada.
- Interacción con DApps: Metamask facilita la interacción con aplicaciones descentralizadas (DApps) directamente desde el navegador. Al tener instalada la extensión, los usuarios pueden acceder y utilizar DApps sin necesidad de crear cuentas separadas o proporcionar información confidencial. Metamask permite la firma de transacciones y la autenticación segura en las DApps.

Con este servicio, se realizan las transferencias a las cuentas y se puede ver el histórico de estas transacciones:

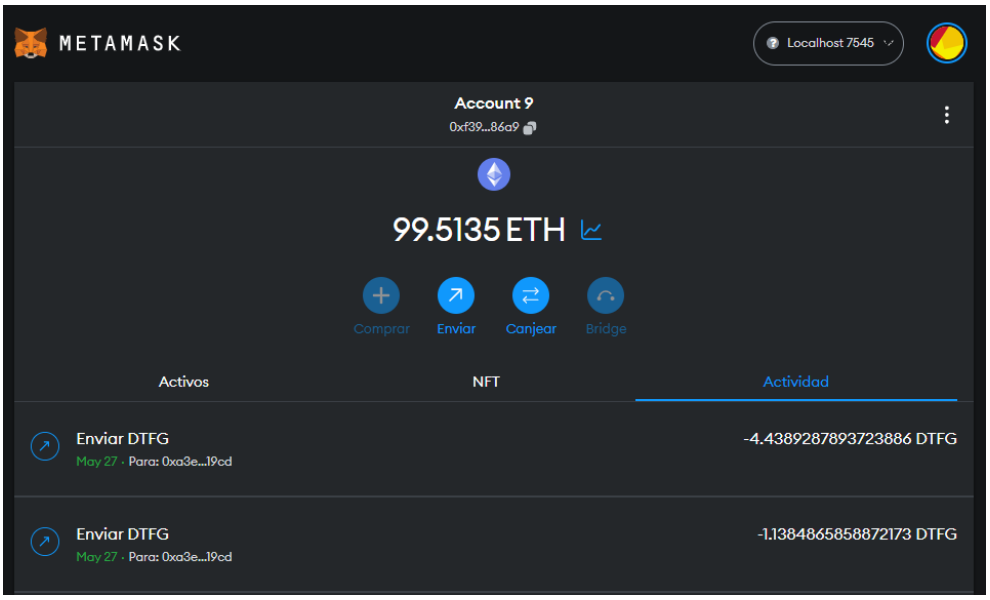


Figura 25. Interfaz gráfica Metamask

- **Lenguaje de programación**

Figura 26. Solidity

Recurso: https://blog.knoldus.com/structure-of-a-contract-in-solidity/

Solidity es un lenguaje de programación de alto nivel utilizado para escribir contratos inteligentes en plataformas blockchain, especialmente en la red Ethereum. Fue diseñado específicamente para el desarrollo de aplicaciones descentralizadas (DApps) y contratos inteligentes.

Las posibilidades y características clave de Solidity son muchas, pero nosotros nos hemos centrado en características como:

- Contratos inteligentes: Solidity permite la creación de contratos inteligentes, que son programas autónomos que se ejecutan en una red blockchain. Estos contratos pueden contener reglas, lógica y condiciones predefinidas que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Los contratos inteligentes pueden gestionar y transferir activos digitales, registrar acuerdos y realizar acciones en nombre de los participantes de la red.
- Orientado a objetos: Solidity es un lenguaje de programación orientado a objetos que permite la creación de contratos inteligentes reutilizables y modulares. Los desarrolladores pueden definir estructuras de datos, funciones y eventos, y luego combinarlos para construir contratos complejos. Solidity también admite la herencia y la interfaz, lo que facilita la reutilización de código y la creación de contratos más legibles y mantenibles.
- Interacción con contratos existentes: Solidity permite la interacción con otros contratos inteligentes y tokens ERC-20 o ERC-721 existentes en la red. Los desarrolladores pueden acceder y llamar a funciones de otros contratos, enviar y recibir tokens, y establecer relaciones y dependencias entre diferentes contratos.
- Seguridad y auditoría: Solidity está diseñado para promover la seguridad en el desarrollo de contratos inteligentes. Proporciona características como la protección contra desbordamiento de enteros, la verificación de alcance (chequeo de límites) y las modificaciones de estado restrictivas para evitar posibles vulnerabilidades y ataques. Además, Solidity facilita la auditoría de contratos inteligentes mediante la transparencia del código fuente y la trazabilidad de las transacciones en la blockchain.

Para poder realizar el Smart contract he utilizado un contrato ERC20 básico se ha implementado en Solidity siguiendo un conjunto de reglas y funciones estándar. Donde defino una estructura de datos para almacenar los balances de las direcciones de los usuarios y una matriz de permisos para realizar transferencias en su nombre. El contrato también incluye funciones como `totalSupply()` para obtener la cantidad total de tokens, `balanceOf(address)` para consultar el saldo de un usuario, `transfer(address, uint256)` para transferir tokens a otra dirección y `approve(address, uint256)` para permitir que una dirección gaste tokens en nombre del propietario. Además, hay una función `transferFrom(address, address, uint256)` que permite a un tercero realizar transferencias en nombre del propietario. Estas

funciones actualizan los balances y emiten eventos para notificar las transferencias. Al implementar este contrato básico de conformidad con el estándar ERC20, se asegura la compatibilidad y la interoperabilidad de los tokens con otras aplicaciones y plataformas que también siguen este estándar. Eso lo podremos ver en este código, resaltando las partes más importantes:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.18;

struct Product { // estructura del producto
    uint256 id;
    string name;
    uint256 amount;
    uint256 price;
}

interface IERC20 {

    event Transfer(address indexed from, address indexed to,
uint256 value);

    event Approval(
        address indexed owner,
        address indexed spender,
        uint256 value
    );
}

contract Micontrato is IERC20 {

    ///Mappings
    mapping(address => uint256) private _balances;
    mapping(address => mapping(address => uint256)) private
_allowed;

    uint256 private _totalSupply;

    constructor(
        string memory name_,
        string memory symbol_,
        uint8 decimals_,
        uint256 supply_
    ) {
        // ...
    }

    event NewProductCreated(uint256 productId);

    function totalSupply() public view returns (uint256) {
        return _totalSupply;
    }

```

```
48      function balanceOf(address _owner) public view override returns
49  (uint256) {
50          return _balances[_owner];
51      }
52
53      function transfer(
54          address to,
55          uint256 value
56      ) public override returns (bool) {
57          // ...
58      }
59
60      function approve(
61          address spender,
62          uint256 value
63      ) public override returns (bool) {
64          // ...
65      }
66
67      function transferFrom(
68          address from,
69          address to,
70          uint256 value
71      ) public override returns (bool) {
72          // ...
        }
    }
```

En el contrato en Solidity proporcionado, encontramos diferentes partes:

1. **Estructura del producto (Product struct):**

   - Se define una estructura llamada "Product" que almacena información sobre un producto, como su identificador, nombre, cantidad y precio.

2. **Interfaz IERC20:**

   - Se define una interfaz llamada IERC20, que establece los métodos y eventos necesarios para cumplir con el estándar ERC20.
   - La interfaz proporciona funciones como "totalSupply", "balanceOf", "transfer", "approve", "allowance" y "transferFrom" para interactuar con el token.

3. **Contrato principal (Micontrato):**

   - El contrato "Micontrato" implementa la interfaz IERC20 y define un token ERC20.
   - Contiene variables como "owner" para almacenar la dirección del propietario del contrato, "name" y "symbol" para el nombre y símbolo del token, y "decimals" para el número de decimales del token.

- Utiliza el mapeo "_balances" para almacenar los saldos de los titulares de tokens y el mapeo "_allowed" para almacenar las asignaciones de aprobación.
- El constructor se encarga de inicializar los valores iniciales del token, como el nombre, símbolo, decimales y suministro total.
- Implementa las funciones requeridas por la interfaz IERC20, como "totalSupply", "balanceOf", "transfer", "approve" y "transferFrom".
- Además, emite eventos como "Transfer" y "Approval" para notificar las transferencias y aprobaciones de tokens.

Frontend y backend:

- **JavaScript**

Figura 27. JavaScript

Recurso: https://es.wikipedia.org/wiki/JavaScript

Es un lenguaje de programación ampliamente utilizado que se ejecuta en el navegador web. Se utiliza principalmente para agregar interactividad y funcionalidad dinámica a los sitios web. Con JavaScript, puedes controlar el comportamiento de los elementos en una página web, manipular datos, realizar llamadas a servidores y mucho más.

En el contexto de tu cartera virtual basada en blockchain e IPFS, JavaScript es una opción común para implementar la lógica del lado del cliente (frontend) debido a su capacidad para interactuar con la interfaz de usuario y realizar solicitudes de red. Aquí hay algunas razones por las que JavaScript es una elección popular:

1. Interactividad en el navegador: JavaScript te permite crear una interfaz de usuario interactiva y receptiva. Puedes responder a las acciones del usuario, validar datos y actualizar dinámicamente el contenido de la página sin tener que recargarla.
2. Acceso a la API del navegador: JavaScript proporciona acceso a diversas API del navegador, lo que te permite interactuar con funciones y características del navegador, como almacenamiento local, geolocalización, notificaciones, cámaras y micrófonos, entre otros.
3. Comunicación con el backend: Puedes realizar solicitudes de red (por ejemplo, solicitudes HTTP) desde JavaScript para comunicarte con el backend de tu aplicación, que puede estar implementado en otros lenguajes o tecnologías.
4. Amplia comunidad y recursos: JavaScript cuenta con una gran comunidad de desarrolladores y una amplia gama de recursos disponibles, como bibliotecas, frameworks y documentación. Esto facilita el aprendizaje y el desarrollo de aplicaciones.

En el contexto de la cartera virtual basada en blockchain e IPFS, JavaScript permitirá interactuar con la blockchain (por ejemplo, Ethereum) mediante bibliotecas y APIs específicas. Podrás realizar transacciones, consultar saldos, interactuar con contratos inteligentes y mostrar información relevante en tu interfaz de usuario. Además, JavaScript te brindará la capacidad de comunicarte con la red IPFS para almacenar y recuperar archivos de forma descentralizada.

En mi caso, he utilizado este lenguaje para interactuar con el Smart contract creado, en vez de mostrar el código entero, mostraré solo las partes más relevantes que interactúan con el contrato especificado:

Balance: En este apartado, haremos la llamada de lectura con la función call al balanceOf y obtendremos el valor en la variable res, que transformaremos a ether y lo mostraremos en la app.

```
await Micontrato.methods
        .balanceOf(address)
        .call()
        .then((res) => {
          const balance = web3.utils.fromWei(res, "ether");
          const valueSpan = document.getElementById("balance");
```

```
7           valueSpan.innerHTML = balance;
8         });
```

Transferencia: Por otro lado, haríamos una llamada de escritura con el send a la función de transfer, pasándole como parámetros la dirección la cual vamos a enviar los ether y la cantidad, marcándole que es desde nuestra cuenta.

```
await Micontrato.methods
        .transfer(addressValue, amountTransfer)
        .send({ from: account })
        .then((res) => {
          addressElement.value = "";
          amount.value = 0;
        });
```

Histórico: De esta manera, obtendríamos el histórico de transacciones de nuestra cuenta, con un bucle de los bloques y comparando cada bloque en nuestra cuenta para obtener el histórico correcto.

```
async function getTransactionHistory(address) {
  const currentBlockNumber = await web3.eth.getBlockNumber();
  const transactions = [];

  for (let i = 0; i <= currentBlockNumber; i++) {
    const block = await web3.eth.getBlock(i, true);
    for (const tx of block.transactions) {
      if (tx.from === address || tx.to === address) {
        transactions.push(tx);
      }
    }
  }

  return transactions;
}
```

Compile: Otra funcionalidad a destacar sería el archivo con el que compilamos y leemos nuestro contrato, en el que a partir de la dirección del archivo de Micontrato.sol, se especificará el código en el que se está programando (en este caso, Solidity), se compilará y convertirá al formato JSON para poder con ello extraer el abi y bytecode requeridos para poder desplegar más tarde el contrato:

```
///Ruta donde está nuestro archivo
const MicontratoPath = path.join(__dirname, '../Micontrato.sol');

///Obtenemos el código
const code = fs.readFileSync(MicontratoPath, 'utf8');

///Compilamos el código
const input = {
    language: 'Solidity',
    sources: {
        'Micontrato.sol':{
            ///Le metemos el código que hemos obtenido arriba
            content: code
        }
    },
    settings: {
        outputSelection: {
            '*': {
                '*': ['*']
            }
        }
    }
};


///Resultado de la compilación
const output = JSON.parse(solc.compile(JSON.stringify(input)));

///Recogemos la información que queremos del output
module.exports = {
    ///Aquí estarán los objetos de las funciones
    abi: output.contracts['Micontrato.sol'].Micontrato.abi,
    ///Aquí el código byte
    bytecode:
output.contracts['Micontrato.sol'].Micontrato.evm.bytecode.object
}
```

Deploy: Además, para poder desplegar el Smart contract, tenía que crearme una dirección donde lo creara para poder interactuar, usé la función deploy de la siguiente manera, creando con ello el nombre de mi criptomoneda, sus siglas y añadiendo la cantidad de DTFG que quería para la cuenta seleccionada:

```
const deploy = async () => {
  try {
    const accounts = await web3.eth.getAccounts();

    const constructorArguments = [
      "DanielTrabajoFindeGrado", // Nombre de la criptomoneda
      "DTFG", // Símbolo de la criptomoneda
      18, // Decimal places
      21000000, // Total supply
    ];

    const result = await new web3.eth.Contract(abi)
```

```
13      .deploy({data: bytecode, arguments: constructorArguments})
14      .send({gas: 2000000, from:accounts[0]});
15
16    } catch (error) {
17      console.error("Error al desplegar el contrato:", error);
18    }
19 };
```

En resumen, JavaScript es una herramienta poderosa para desarrollar la lógica del lado del cliente. Me ha permitido crear una interfaz de usuario interactiva y comunicarme con la blockchain e IPFS para realizar transacciones y almacenar/recuperar datos de manera descentralizada.

- **HTML**

Figura 28. HTML

Recurso: https://www.freepik.com/free-photos-vectors/html5-logo

(HyperText Markup Language) es el lenguaje de marcado estándar utilizado para crear la estructura y presentación de las páginas web. Es un componente fundamental de la web y se utiliza en conjunto con CSS (Cascading Style Sheets) y JavaScript para crear experiencias interactivas en el navegador.

HTML se compone de elementos y etiquetas que se utilizan para definir la estructura y los elementos de una página web.
Estilos y presentación: Aunque HTML se centra principalmente en la estructura y el contenido, se puede utilizar CSS para aplicar estilos y dar formato visual a los elementos HTML. Los atributos de estilo también se pueden utilizar directamente en las etiquetas HTML para aplicar estilos básicos.

Estos estilos en CSS para dar un formato visual “diferente” o detallado podría mostrarse de la siguiente manera, en este caso, un ejemplo del estilo del balance que se muestra en nuestra DApp:

```
#balance {
  display: inline-block;
  padding: 5px 10px;
  background-color: #00bfff;
  color: #fff;
  font-weight: bold;
  border-radius: 5px;
}
```

Por lo que, en contexto de la cartera virtual, HTML se utiliza para crear la interfaz de usuario (UI) que permite a los usuarios interactuar con la aplicación. Se puede utilizar elementos HTML para estructurar y organizar los diferentes componentes de la cartera, como formularios, botones, tablas y elementos de navegación. También puedes enlazar elementos HTML con JavaScript para agregar interactividad y funcionalidad dinámica a la cartera.

Para la estructura y contenido, se ha dividido en distintos tipos de clases declaradas y ajustadas más tarde en el CSS para poder aplicarle el estilo y formato que requería, de esta manera, muestro un ejemplo de uno de los elementos de la tabla de los productos:

```
  <thead>
   <tr>
1    <th>Nombre</th>
 2   <th>Precio/kg</th>
 3   <th>Cantidad en kg</th>
 4  </tr>
 5 </thead>
 6 <td>
 7  <select id="fruta" name="fruta">
 8  </select>
 9 </td>
10  <td><span id="precio1" style="display: none;"
11 class="info"></span></td>
12  <td><input type="number" class="oculto wider-input" id="cantidad-
13 total1" min="0" value="0"></td>
14  <td><span id="descripcion1" style="display: none;"
15 class="info"></span></td>
16 <td> <button id="descripcionPopUpFruta"
   onclick="mostrarPopUpFrutas()">Ver trazabilidad</button></td>
                  <td><span id="direccion1" class="info"></span></td>
```

- **Node.js**

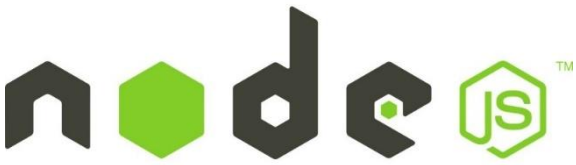


Figura 29. Node.js

Recurso: https://www.startechup.com/es/blog/node-js-what-it-is-used-

Es un entorno de ejecución de JavaScript del lado del servidor que permite ejecutar código JavaScript fuera del navegador[10]. A diferencia de JavaScript tradicional, que se ejecuta en el navegador web, Node.js se utiliza para crear aplicaciones y servicios del lado del servidor. Algunas de las funcionalidades que ofrece Node.js para la creación de una billetera virtual con blockchain e IPFS incluyen:

Gestión de dependencias: Node.js utiliza npm (Node Package Manager) para gestionar las dependencias y bibliotecas de terceros necesarias en el desarrollo de la billetera virtual. npm permite instalar, actualizar y administrar fácilmente los módulos y paquetes necesarios para el proyecto.

Desarrollo de servidores: Node.js ofrece una API (Application Programming Interface) para el desarrollo de servidores web. Esto permite crear un servidor HTTP

para manejar las solicitudes y respuestas del cliente. En el contexto de una billetera virtual, se puede utilizar Node.js para crear un servidor web que maneje las transacciones, consultas y actualizaciones de la billetera.

Uso de Truffle: Truffle es un framework de desarrollo de contratos inteligentes para Ethereum. Con Truffle, se puede compilar, migrar y probar los contratos inteligentes de la billetera virtual. Truffle simplifica el proceso de desarrollo y despliegue de contratos inteligentes, ofreciendo herramientas y bibliotecas que facilitan el flujo de trabajo. Para nuestra billetera, truffle ha marcado los guiones, ayudándome cada vez a la creación de mis contratos, conexiones con el servicio ganache…

En especial, he usado la biblioteca de proveedores truffle-hdwallet-provider el cual simplifica el proceso de conexión a una red Ethereum utilizando una frase mnemotécnica y proporciona una forma conveniente de firmar transacciones y realizar llamadas a contratos inteligentes desde una aplicación o script de Truffle. Esto facilita el desarrollo y la interacción con contratos inteligentes en Ethereum.

```
  const HDWalletProvider = require("truffle-hdwallet-provider");
1 const provider = new HDWalletProvider(mnemonic,
2 "http://localhost:7545");
```

Como podemos ver, se usaría y desplegaría de esta manera, proporcionándonos el "provider" o proveedor para nuestra conexión a una red Ethereum, en el que además, le indicaríamos, cuál es la conexión y puerto del servidor ganache para poder obtener las cuentas del servidor:

Integración de IPFS: Node.js permite la integración de IPFS en la billetera virtual utilizando bibliotecas como ipfs-http-client. Esta biblioteca proporciona una interfaz para interactuar con un nodo IPFS a través de HTTP. Con ipfs-http-client, se puede cargar, descargar y acceder a archivos en IPFS desde la billetera virtual.

En nuestro caso, lo usamos para cargar y acceder a archivos en IPFS y lo declaramos y creamos uno nuevo de esta manera, redirigiéndonos a una nueva página para mostrarnos el nuevo documento generado con IPFS:

```
1 const IPFS = require("ipfs-http-client");
2 const node = await IPFS.create();
3 const gatewayUrl =
4 `https://ipfs.io/ipfs/${cidValue}`;
```

Uso de Express: Express es un framework web de Node.js que simplifica el desarrollo de aplicaciones web. Con Express, se puede definir el enrutamiento, manejar solicitudes y respuestas, y crear endpoints para la billetera virtual. Express ofrece una sintaxis sencilla y flexible para el desarrollo de APIs RESTful.

```
var express = require('express');
var app = express();
```

Lo he usado principalmente para el enrutamiento de la factura de la transacción donde podremos obtener el documento con el app.get y, posteriormente poder subir el documento con app.post para crear el documento con la tecnología IPFS:

```
app.get('/', async(req, res) => {
    res.sendFile(__dirname + '/upload.html');
});
app.post('/file', upload.single('doc'), async function(req, res,
next){
    try{
        const file = req.file;

        if(!file){
            res.status(400).send({
                status: false,
                data: 'No file is selected.'
            })
        } else{
            try{
            var HASH = await uploadIPFS(PATH + req.file.filename);

        }catch (err) {
            console.log('Error en uploadIPFS:');
            console.log(err);
            return false;
          }

        }
    }
    catch (err){
        res.status(500).send({ status: 'error', error: err.message
});
    }
})
```

Gestión de archivos: Multer es una biblioteca de Node.js utilizada para manejar el envío de archivos en formularios HTML. En el contexto de la billetera virtual, Multer puede utilizarse para recibir y procesar archivos adjuntos relacionados con

las transacciones o documentos generados. Por ejemplo, se ha utilizado Multer para recibir y almacenar facturas o comprobantes de transacciones de esta manera, donde el destino o ubicación del archivo era la carpeta uploads:

```
1 var multer = require('multer');
2 var upload = multer({ dest: 'uploads/'});
3 upload.single('doc')
```

Es decir, Node.js ofrece un entorno de desarrollo y ejecución del lado del servidor que permite utilizar Truffle, ipfs-http-client, Express y Multer para crear una billetera virtual con blockchain e IPFS. Con Node.js, se puede desarrollar el servidor web, interactuar con contratos inteligentes, comunicarse con nodos IPFS y gestionar el envío y almacenamiento de archivos adjuntos. Estas herramientas y bibliotecas facilitan el desarrollo de la billetera virtual, proporcionando funcionalidades esenciales para la interacción con blockchain e IPFS.

- **IPFS**

Figura 30. IPFS

Recurso:

https://es.wikipedia.org/wiki/Sistema_de_archivos_interplanetario

Para ello, he usado la librería de node.js con ipfs-http-client (mencionado anteriormente), en el que a partir de la dirección del archivo que cargamos, con el IPFS.create() se aplicaba esta tecnología, de esta manera, redirigiendo el documento con el CID aplicado a otra pestaña que podrá leer este documento. Finalmente nos devolverá el CID para poder almacenarlo:

```
const node = await IPFS.create();
    const file = await node.add(fs.readFileSync(PATH));
    const cidValue = file.cid.toString();
    const gatewayUrl = `https://ipfs.io/ipfs/${cidValue}`;
    openurl.open(gatewayUrl, (err) => {
        if (err) {
          console.error(`Error al abrir la URL: ${err}`);
        } else {
          console.log(`Se abrió la URL en el navegador`);
        }
      });
    return file.cid.toString();
```

Además, IPFS ofrece IPFS Desktop, que es una aplicación de escritorio que proporciona una interfaz gráfica de usuario para interactuar con el protocolo IPFS (InterPlanetary File System).

De esta manera, se podrán ver e importar los archivos que se han generado con el CID, podremos verlos así:

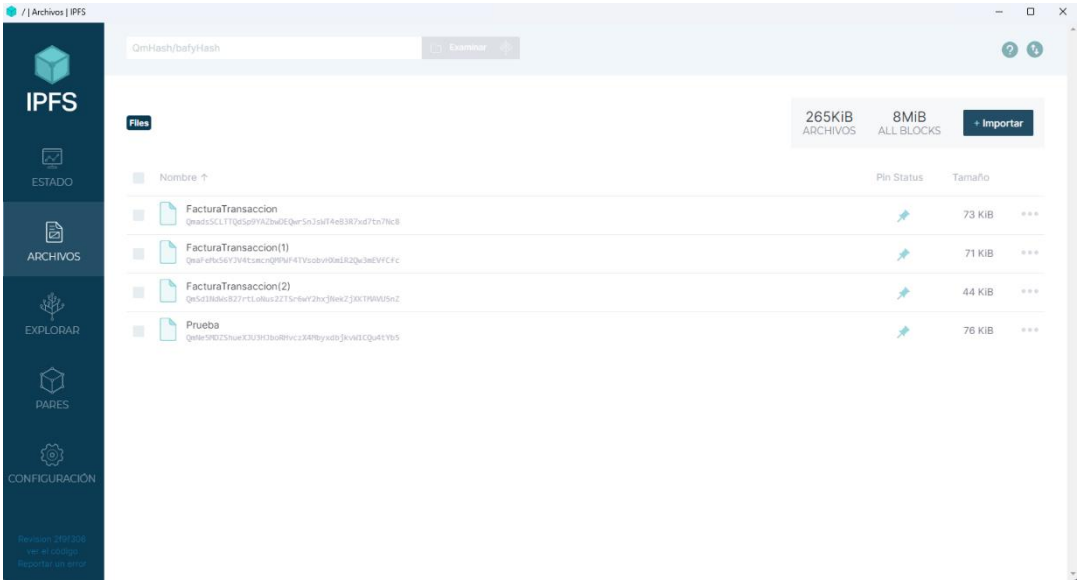


Figura 31. Interfaz gráfica IPFS

16. Conclusión

La implementación de la tecnología blockchain en la industria agrícola, junto con la creación de mi billetera virtual denominada AgroWallet, ha demostrado ser una solución innovadora y prometedora para abordar diversos desafíos en el sector. En esta conclusión, exploraremos los beneficios y el potencial de esta combinación, así como su impacto en la trazabilidad de productos, la gestión de la información y las transacciones seguras.

La adopción de la blockchain en la agricultura ofrece numerosas ventajas, siendo una de las más destacadas la trazabilidad de los productos. Gracias a la tecnología blockchain, es posible registrar cada etapa del ciclo de vida de los productos agrícolas, desde su origen en el campo hasta su llegada al consumidor final. Esto permite una mayor transparencia y confianza, ya que los consumidores pueden acceder a información detallada sobre el proceso de producción, el uso de agroquímicos, las condiciones de cultivo y más. Con AgroWallet, los usuarios tienen acceso a esta información de manera sencilla y transparente, lo que fomenta la confianza en la cadena de suministro agrícola.

Además de la trazabilidad, AgroWallet ofrece un listado de productos agrícolas con sus características detalladas. Esta funcionalidad brinda a los usuarios la capacidad de examinar en profundidad cada producto, como su variedad, origen, métodos de cultivo y certificaciones. Esto facilita la toma de decisiones informadas por parte de los consumidores y promueve prácticas agrícolas sostenibles y saludables.

La billetera virtual también permite a los usuarios gestionar su información de cuenta de manera segura y privada. La blockchain, al ser una tecnología descentralizada y distribuida, garantiza la integridad y la inmutabilidad de los datos almacenados. Esto implica que la información personal y financiera de los usuarios está protegida contra manipulaciones y accesos no autorizados. Además, AgroWallet ofrece la posibilidad de utilizar tecnología IPFS para subir y visualizar archivos, lo que brinda una forma eficiente y segura de almacenar documentos relacionados con la agricultura, como certificados de calidad, permisos y registros.

En términos de transacciones, la tecnología blockchain utilizada en AgroWallet ofrece un mecanismo seguro y eficiente para realizar pagos y registrar transacciones relacionadas con los productos agrícolas. Los contratos inteligentes, que son programas autónomos que se ejecutan en la blockchain, permiten automatizar y garantizar el cumplimiento de acuerdos entre las partes involucradas. Por ejemplo, se pueden establecer contratos para la compra-venta de productos agrícolas, donde las condiciones acordadas se ejecutan automáticamente una vez que se cumplen los términos preestablecidos. Esto reduce la necesidad de intermediarios y agiliza el proceso de transacción, brindando a los usuarios una experiencia más eficiente y segura.

La implementación de la blockchain en la agricultura a través de AgroWallet no solo beneficia a los consumidores y productores, sino que también tiene un impacto positivo en la sociedad en general. La transparencia en la cadena de suministro agrícola ayuda a combatir la falsificación de productos y garantiza que los agricultores reciban un valor justo por su trabajo. Además, la trazabilidad y la información detallada sobre los productos agrícolas promueven la seguridad alimentaria y la salud pública al permitir la identificación de posibles riesgos y la adopción de medidas preventivas.

A pesar de todas las ventajas y el potencial que ofrece la combinación de la blockchain y AgroWallet, es importante tener en cuenta algunos desafíos y consideraciones. La adopción masiva de esta tecnología requiere la colaboración y participación de todos los actores involucrados en la cadena de suministro agrícola, desde los productores hasta los consumidores y las instituciones reguladoras. Además, es fundamental abordar aspectos relacionados con la escalabilidad, la interoperabilidad y la privacidad de los datos para garantizar un ecosistema blockchain robusto y confiable.

Podemos decir que, la integración de la tecnología blockchain en la agricultura a través de AgroWallet ofrece numerosos beneficios y oportunidades para mejorar la trazabilidad de los productos, la gestión de la información y las transacciones seguras. Esta combinación proporciona a los consumidores acceso a información detallada sobre los productos agrícolas, fomentando la transparencia y la confianza

en la cadena de suministro. Asimismo, brinda a los productores herramientas para mejorar la eficiencia y la seguridad en las transacciones comerciales. Con la implementación adecuada y la colaboración de todos los actores involucrados, la blockchain y AgroWallet tienen el potencial de transformar la agricultura, promoviendo prácticas sostenibles y una mayor equidad en la industria agrícola.

17. Posibles mejoras de AgroWallet

Me gustaría proponer, además, las posibles mejoras que podría llegar a alcanzar AgroWallet, siendo realistas y con gran predicción a futuros, podremos llegar a realizar mejoras a largo, mediano y corto plazo:

- **Mejoras a corto plazo (1-2 años):**
  - Interfaz de usuario mejorada: Se podrían realizar mejoras en la usabilidad y experiencia del usuario de AgroWallet, optimizando la navegación, el diseño y la accesibilidad para garantizar una experiencia fluida y atractiva.

  - Ampliación de productos y trazabilidad: Sería beneficioso ampliar la variedad de productos agrícolas disponibles en AgroWallet y mejorar la trazabilidad de cada producto, proporcionando información detallada sobre su origen, métodos de cultivo y certificaciones.

- **Mejoras a mediano plazo (3-5 años):**
  - Integración con sistemas de IoT: Se podría explorar la integración de dispositivos de Internet de las cosas (IoT) en AgroWallet, permitiendo la recopilación de datos en tiempo real sobre las condiciones de cultivo, calidad del suelo, humedad, temperatura, entre otros, para brindar una visión más completa de la producción agrícola.

  - Implementación de contratos inteligentes avanzados: Los contratos inteligentes podrían evolucionar para incluir acuerdos más complejos y automatizados, como contratos de arrendamiento de tierras, acuerdos de suministro a largo plazo o contratos de financiamiento agrícola, brindando mayor eficiencia y seguridad en las transacciones.

  - Colaboración con entidades gubernamentales y reguladoras: Establecer alianzas estratégicas con organismos gubernamentales y reguladores agrícolas permitiría una mayor integración de AgroWallet en los marcos legales y regulatorios existentes, facilitando la adopción a gran escala y garantizando la conformidad normativa.

- **Mejoras a largo plazo (más de 5 años):**
  - Desarrollo de IA y análisis de datos: La implementación de inteligencia artificial (IA) y análisis de datos avanzados podría permitir a AgroWallet brindar recomendaciones personalizadas a los agricultores, optimizando la toma de decisiones en aspectos como la planificación de cultivos, la gestión de plagas y enfermedades, y la eficiencia de los recursos.

  - Expansión internacional y adopción masiva: AgroWallet podría buscar expandirse a nivel internacional, estableciendo asociaciones con actores clave en el sector agrícola de diferentes países y fomentando la adopción masiva de la plataforma en múltiples mercados agrícolas.

  - Aplicación de tecnologías emergentes: En un horizonte más lejano, AgroWallet podría explorar tecnologías emergentes como blockchain escalable, computación cuántica o realidad virtual/aumentada para seguir mejorando la eficiencia, seguridad y experiencia de usuario en el ámbito agrícola.

18. Referencias y bibliografía

1. Ferrández-Pastor, F. J., García-Chamizo, J. M., Gilart-Iglesias, V., Mora-Gimeno, F. J., y Pavón-Mariño, P. (2022). "Tecnologías Blockchain para la Industria 4.0: Una revisión sistemática." Journal of Industrial Information Integration, 28, 100274. Recuperado de Ferrandez-Pastor_etal_2022_JIndustInformIntegrat.

2. Galindo-Romero, R. M., Sánchez-Cid, D., Martínez-Ballesta, J. L., y Carvajal, M. (2020). "Sistemas de trazabilidad aplicados a la agricultura para mejorar la calidad y seguridad alimentaria." Revista Ecosistemas y Ciberseguridad, 4(1), 31-40. Recuperado de revistaecys.github.io.

3. Bit2Me Academy. (2021). "¿Cuántos tipos de blockchain existen?" Recuperado de academy.bit2me.com.

4. Forbes. (2022). "Lista Forbes Blockchain 50 2022."

5. Humintech. (Fecha desconocida). "Aplicaciones de Blockchain para la agricultura: Pros y contras." Recuperado de humintech.com.

6. Innovación Digital 360. (Fecha desconocida). "Cómo el blockchain agroalimentario puede darle mayor sostenibilidad al sector." Recuperado de innovaciondigital360.com/agrotech.

7. ThreePoints. (Fecha desconocida). "Aplicaciones de Blockchain en la industria alimentaria." Recuperado del blog threepoints.com/blog/.

8. Dapp University. (Fecha desconocida). "Cómo construir una aplicación blockchain." Recuperado del artículo dappuniversity.com/articles/how-to-build-a-blockchain-app.

9. Lasa, A. (Fecha desconocida). "Crear una DApp desde cero sin frameworks." Recuperado de albertolasa.medium.com.

10. Startechup. (Fecha desconocida). "Node.js: Para qué se utiliza y cuándo/dónde usarlo para el desarrollo de aplicaciones empresariales." Recuperado del blog startechup.com/es/blog.

11. TRACE FOOD. (2022). "Trazabilidad Alimentaria, desde el origen hasta el consumidor final basada en Blockchain." Web: tracefood.com.es.

12. MIETHEREUM. (2020). "¿Qué es exactamente la cadena de bloques (Blockchain)?"

13. QUANTION DIGITAL FACTORY. (2021). "La tecnología Blockchain en la Industria Alimentaria, trazabilidad y seguridad." Artículo de innovación de Quantium Digital Factory.

14. AGUSTÍ FONTS. (2018). "Blockchain en el sector agroalimentario." Artículo publicado en el sitio web avicultura.com.

15. LEYRE SOTO. (2021). "Smart Contracts: Qué son, para qué sirven y ventajas." Publicación del blog blog.siganturit.com.

16. JAVIER ALONSO LECUIT. (2019). "Smart Contracts: Qué son, para qué sirven y ventajas." Artículo del sitio web realinstitutoelcano.org.

17. MIETHEREUM. (2020). "¿Qué es exactamente la cadena de bloques (Blockchain) y cómo funciona? ¿Qué usos se le pueden dar?" Artículo del sitio web miethereum.com.

18. PEDRO MARTÍN. (2021). "Blockchain ¿Por qué y cómo surge?" Artículo de opinión del sitio web visualeo.com.

19. ALEJANDRO VILLA. (2020). "Blockchain y tu Modelo de Negocio." Artículo del sitio web linkedin.com.

20. GRISELDA VEGA. (2021). "¿Cuáles son las tecnologías para ganar mayor transparencia y sustentabilidad?" Artículo de opinión del sitio web thefoodtech.com.

21. LUISA FERNANDA MARTÍNEZ GÓMEZ. (2022). "Blockchain en el sector agroalimentario: panorama en Latinoamérica y el mundo." Artículo de opinión del sitio web thomas-signe.com.

22. PABLO PALENCIA GARRIDO-LESTACHE. (2021). "La era digital ha llegado a la Industria Agroalimentaria." Artículo del diario larazon.es.

23. CRUZ GUIJARRO HERRERO. (2021). "Llevando la trazabilidad al siguiente nivel." Artículo del sitio web interempresas.net.

Anexo: Código fuente en GitHub

En este anexo se proporciona el enlace al repositorio de GitHub que contiene el código fuente completo del proyecto de fin de grado titulado "TFG". El repositorio en GitHub, alojado en la siguiente dirección: *https://github.com/danisentamans/TFG.git*, permite acceder a todos los archivos y carpetas relacionados con la implementación de la aplicación AgroWallet.

El repositorio de GitHub incluye los siguientes elementos:

1. Carpeta de código fuente: Contiene todos los archivos de código fuente del proyecto, incluyendo clases, interfaces y scripts necesarios para la implementación de AgroWallet.
2. Carpeta de recursos: Contiene los recursos adicionales utilizados en el proyecto, como archivos de configuración, imágenes y otros archivos necesarios para el correcto funcionamiento de la aplicación.
3. Documentación técnica: Puede incluir documentación adicional sobre la arquitectura, diseño y funcionamiento del sistema desarrollado, así como instrucciones de instalación y configuración.

Para acceder al repositorio y explorar el código fuente, sigue estos pasos:

1. Abre un navegador web y visita el siguiente enlace: *https://github.com/danisentamans/TFG.git*
2. En la página de GitHub, podrás ver la lista de archivos y carpetas del proyecto.
3. Navega a través de las carpetas para explorar el código fuente y los recursos utilizados en la implementación de AgroWallet.
4. Puedes visualizar el contenido de cada archivo haciendo clic en su nombre.

Si deseas clonar el repositorio en tu máquina local, puedes utilizar un cliente de Git para clonar el repositorio o descargarlo como un archivo ZIP.