Blockchain & IoT para un nuevo tipo de arquitectura segura y escalable

Carlos Andrés Sánchez Venegas – Jhordy Esteban Salinas Santiago

Estudiantes Maestría en Informática

Escuela Colombiana de ingeniería Julio Garavito

Director

Sergio Espinosa

Codirector

Claudia Patricia Santiago Cely

Bogotá, Colombia

carlos.sanchez-v@mail.escuelaing.edu.co

jhordy.salinas@mail.escuelaing.edu.co

Julio 2023

Tabla de contenido

Introducción **6**
Problemática 7
Motivación 8
Preguntas de investigación 8
Contribuciones 9
Objetivos **11**
Objetivo general 11
Objetivos específicos 11
Metodología **12**
Secuencia de actividades 12
Cronograma 14
Marco teórico **15**
Logística 15
Blockchain 16
Estructura 17
Implementaciones 18
Consenso 19
Contratos inteligentes 20
Ecosistema Blockchain - Ethereum 21
IoT 23
MicroPython 25
Cifrado 26
Estado del arte **28**
Estado del arte de la cadena de suministro 28
Arquitecturas para integración blockchain/IoT 31
Evolución de blockchain 33
Blockchain e *IoT* en la Industria 34
RSA 37
Desarrollo **40**

Arquitecturas 40
Montaje 46
Flujos principales 48
Pruebas 54
Entregables 61
Trabajo futuro 63
Conclusiones 65
Bibliografía 68

Resumen

El uso cada vez más frecuente de dispositivos IoT (Internet of things) y la inevitable dependencia humana de esta tecnología hacen que la falta de estándares claros para los protocolos de seguridad y comunicación sea un problema grave. Una sola vulnerabilidad en un componente de IoT podría tener un impacto negativo significativo. Por esta razón, se propone unir la tecnología IoT con la tecnología blockchain para crear infraestructuras IoT seguras, descentralizadas y confiables que garanticen la integridad de los datos almacenados en la red de blockchain. Además de la seguridad, esta unión también podría brindar la posibilidad de automatizar procesos que usen tecnología IoT a través de contratos inteligentes en una red blockchain, impulsando así el crecimiento de la industria 4.0, que incluye áreas como movilidad, logística, salud, etc. En este libro, se presenta la propuesta e implementación de una arquitectura que permita la interacción de dispositivos IoT de logística con la blockchain de Ethereum. Esta solución ofrece a las empresas una alternativa de código abierto para respaldar la interacción de sus sensores de logística. La implementación de esta arquitectura implica establecer una infraestructura segura y descentralizada, lo que brinda una mayor confianza en la integridad de los datos y mejora la eficiencia de los procesos logísticos.

Palabras clave – Internet de las cosas, blockchain, contratos inteligentes, Ethereum, aplicaciones descentralizadas, sistemas descentralizados, web3, MicroPython, Solidity, cadena de suministro, logística.

Abstract

The increasing use of IoT devices and the inevitable human dependency on this technology makes the lack of clear standards for security and communication protocols a serious problem. A single vulnerability in an IoT component could have a significant negative impact. For this reason, it is proposed to combine IoT technology with blockchain technology to create secure, decentralized, and reliable IoT infrastructures that guarantee the integrity of the data stored on the blockchain network. In addition to security, this union could also provide the possibility of automating IoT processes through smart contracts on a blockchain network, thus driving the growth of industry 4.0, which includes areas such as mobility, logistics, health, etc. In this article is presented and implementation of an architecture that allows the interaction of logistics IoT devices with the Ethereum blockchain. This solution will provide an open-source alternative for companies seeking to support the interaction of their logistics sensors. The implementation of this architecture will also involve having a secure and decentralized infrastructure, which in turn will provide greater confidence in the integrity of the data and greater efficiency in their logistics processes.

Keywords – IoT, Internet of Things, blockchain, smart contracts, Ethereum, Dapps, descentralized applications, descentralized systems, web3, MicroPython, Solidity, supply chain.

Capítulo 1

Introducción

Según estudios de Fortune Business Insights el valor del mercado para IoT fue de 384,70 mil millones de dólares en 2021, en 2022 aumento a 544 mil millones de dólares y se estima una tasa de crecimiento anual compuesta de 26,4%, lo que representa un valor de 2.465,26 mil millones de dólares en 2029 [1] [2], Además de ello, el mercado de *smart cities*, que está directamente relacionado con dispositivos IoT, tuvo un valor de 648,36 mil millones en 2020 y se estima una tasa de crecimiento anual compuesta de 25.2%, lo que representa un valor de 6.061 mil millones para el 2030, de manera proporcional el número de dispositivos se predice que pase 20 mil millones a 50 mil millones de dispositivos IoT en línea para el 2025 [3]. Por parte de blockchain se tiene un valor del mercado de 4.67 mil millones de dólares en 2021 y se estima una tasa de crecimiento anual compuesta de 56.3%, lo que representa un valor de 163.83 mil millones de dólares para el 2029 [4].

El enfoque global estará en entornos inteligentes como la seguridad pública basada en datos, el transporte inteligente, la energía resiliente y el desarrollo de infraestructura, se proyecta un mundo totalmente conectado. Estamos en un constante crecimiento de dispositivos IoT conectados a la red y esta es una tecnología que aún está en desarrollo, y no hay una definición clara de los protocolos, estándares o entornos que se deban emplear para el manejo de los datos de estos dispositivos. Al igual que IoT, Blockchain es una de las nuevas tecnologías que está en crecimiento, que desde su año de nacimiento (2008 dentro del proyecto Bitcoin) hasta hoy ha venido creciendo, y lo más importante ha venido demostrando gracias a *Ethereum*, que no solo es aprovechable en entornos financieros, si no que bajo el desarrollo de contratos inteligentes o *smart contracts*, los cuales son funciones que se ejecutan por medio de eventos dentro de la red, es posible construir lógica que soporte cualquier sector, para lograr así aprovechar ventajas como la transparencia, descentralización, inmutabilidad y confiabilidad. Lo más importante de lo anteriormente mencionado es que Blockchain y en especial *Ethereum* cada vez cuenta con una comunidad más grande que alienta y apalanca un mejor futuro para esta tecnología.

Problemática

Actualmente no existe un estándar claro en cuanto a los protocolos de seguridad y comunicación utilizados en los dispositivos IoT. Esta carencia plantea desafíos significativos, dado que la tecnología IoT se está volviendo cada vez más presente en nuestras vidas diarias, y nuestra dependencia de ella sigue en aumento. Por lo tanto, cualquier vulnerabilidad o falla en cualquiera de los componentes de esta tecnología puede tener un impacto negativo sustancial y perjudicial.

La ausencia de un estándar claro y ampliamente adoptado en cuanto a los protocolos de seguridad y comunicación en los dispositivos IoT genera una serie de problemas y riesgos que amenazan la integridad y confiabilidad de los sistemas de logística. Estos problemas incluyen:

(a) Vulnerabilidades de seguridad: La falta de un estándar de seguridad común facilita la aparición de vulnerabilidades en los dispositivos IoT. Esto puede conducir a brechas de seguridad o incluso que tomen el control de los dispositivos, comprometiendo así la integridad y confidencialidad de los datos y los sistemas logísticos.

(b) Interoperabilidad limitada: Sin un estándar de comunicación claro, los dispositivos IoT pueden tener dificultades para comunicarse entre sí de manera eficiente. Esto puede provocar problemas de compatibilidad y dificultades en la integración de diferentes sistemas y componentes, lo que a su vez afecta la eficiencia y la efectividad de los procesos logísticos.

(c) Falta de confianza: La falta de un estándar de seguridad y comunicación sólido genera incertidumbre y falta de confianza (la falta de confianza hace referencia a la incapacidad de verificabilidad) entre los actores involucrados en la cadena de suministro. Las empresas pueden dudar en adoptar plenamente la tecnología IoT debido a preocupaciones sobre la seguridad y la protección de sus datos.

(d) Complejidad en la gestión de riesgos: La ausencia de un estándar claro dificulta la gestión de riesgos en los sistemas de logística basados en IoT. Las empresas enfrentan desafíos

para identificar y evaluar adecuadamente las amenazas potenciales, lo que dificulta la implementación de medidas de seguridad efectivas y la mitigación de riesgos.

(e) Falta de escalabilidad: Sin un estándar común, es difícil lograr una escalabilidad adecuada en los sistemas de logística basados en IoT. La falta de interoperabilidad entre diferentes dispositivos y sistemas dificulta la expansión y adaptación de los sistemas logísticos para satisfacer las necesidades cambiantes y en constante evolución.

Motivación

La unificación de la tecnología IoT junto con la de *Blockchain* puede generar infraestructuras IoT confiables, descentralizadas y seguras que nos permitan tener confiabilidad en los datos que quedan guardados en la red *Blockchain*. De igual manera se plantea mostrar las virtudes que puede dar la unión de estas dos tecnologías a parte de los aspectos de seguridad como lo es la posibilidad de automatizar los procesos generados por IoT por medio de contratos inteligentes sobre una red *Blockchain* apoyando el crecimiento de la industria 4.0. El presente proyecto pretende unir estas dos tecnologías para poder aprovechar las ventajas con las que *Blockchain* puede complementar a IoT, tales como seguridad, inmutabilidad, confiabilidad y descentralización que son atributos exigentes y que actualmente no han sido totalmente resueltos sobre IoT, además de ello la posibilidad de usar *smart contracts* para poder automatizar procesos, reducir costos e incrementar de forma masiva el volumen de los procesos [5] y mejorar otros campos de la industria 4.0. Lo que se desea con este proyecto es comenzar con la estandarización del uso de estas dos tecnologías, estableciendo un grupo de herramientas (librerías, componentes y artefactos) para lograr implementar el uso de *Blockchain* para dispositivos IoT usados en el sector de la logística o cadena de suministro.

Preguntas de investigación

En este trabajo se busca resolver las siguientes preguntas de investigación:

Q1 ¿De qué manera el uso de tecnologías *Blockchain*, como *Ethereum*, puede mejorar la gestión de los datos en los dispositivos *IoT* y proporcionar beneficios en términos de transparencia, descentralización, inmutabilidad y confiabilidad?
Q2 ¿Cuál es el papel de la comunidad de *Blockchain*, especialmente en el caso de Ethereum, en el impulso y el desarrollo futuro de esta tecnología?, y ¿Cómo puede contribuir a un mejor aprovechamiento de sus ventajas y un mayor crecimiento en diferentes sectores?

Q3 ¿Cuáles son los principales desafíos relacionados con la falta de protocolos y estándares claros para el manejo de datos en los dispositivos *IoT?* y ¿Cómo afecta esto a su seguridad y eficiencia?

Q4 ¿Cómo puede la integración de tecnologías como IoT y blockchain mejorar la eficiencia, transparencia y seguridad en los procesos logísticos, desde la gestión de la cadena de suministro hasta el seguimiento de productos y la verificación de la autenticidad, en un entorno descentralizado y confiable?

Contribuciones

Científicos y tecnológicos

- Mejoramiento hacia una arquitectura reusable y aplicable para el sector de IoT.
- Registro y documentación de una librería para uso general.
- Impacto ideológico sobre la aplicabilidad que puede tener blockchain.

Impactos sobre la productividad y competitividad en el sector de desarrollo o áreas de desempeño relacionados

- Comunidad de IoT beneficiada con un nuevo estándar de comunicación entre dispositivos IoT para el sector de logística.
- Mayor competitividad por la seguridad sobre las comunicaciones.
- Mejor escalabilidad de dispositivos conectados entre ellos.

Impactos sobre el medio ambiente y la sociedad

- Uso de una blockchain con un mecanismo de consenso de bajo costo ambiental.
- Confiabilidad a las personas con dispositivos IoT con su privacidad.

Capítulo 2

Objetivos

Objetivo general

Crear un framework de comunicación entre dispositivos IoT usados en el sector de logística y la red blockchain *Ethereum*, incluyendo la implementación de la lógica de los contratos inteligentes, con el fin de mejorar la trazabilidad, seguridad y eficiencia en las operaciones logísticas aplicadas al seguimiento de un producto, desde su entrada a bodega hasta su entrega en el destino final.

Objetivos específicos

- Abstraer los procesos actuales involucrados en el sector de logística, identificando los puntos de optimización y mejora (seguridad, desempeño, trazabilidad, etc.) que pueden ser logrados por medio de la unión de IoT y blockchain.
- Investigar y analizar las tecnologías existentes de IoT y blockchain, junto con las arquitecturas que ya se han propuesto, para aprovechar al máximo las características que brindan cada una de ellas.
- Implementar una arquitectura que permita la interacción entre los dispositivos IoT y blockchain, que aproveche todas las ventajas que proporciona una red blockchain, usando como lenguaje de programación MicroPython para el desarrolló sobre los componentes IoT y Solidity para el desarrollo de los *smart contracts* en *Ethereum*.
- Aplicar la arquitectura desarrollada a un caso de uso real por medio de una PoC.
- Evaluar aspectos de escalabilidad, desempeño y seguridad de la arquitectura propuesta, para posteriormente presentar posibles trabajos futuros sobre la misma.

Capítulo 3

Metodología

La metodología adoptada para este proyecto de grado es una investigación experimental respaldada por el uso de la metodología ágil *Scrum* para el desarrollo de prototipos y pruebas de concepto. Se llevó a cabo una investigación exhaustiva en las áreas tecnológicas expuestas en el marco teórico, lo que proporcionó una base sólida para la ejecución ágil de un prototipo de software.

La ejecución del proyecto sigue un enfoque de desarrollo iterativo que comprende distintas etapas: formulación de la idea, diseño del prototipo, ejecución y reiteración. Se establecieron *sprints* de dos semanas, lo que permitió un ritmo constante y entregas incrementales en el desarrollo del prototipo.

El capítulo 6 del presente libro se dedica a profundizar en esta metodología ágil utilizada. Una de las principales ventajas de emplear esta metodología fue la capacidad de realizar iteraciones frecuentes y cortas. Estas iteraciones posibilitaron la revisión y replanteamiento de arquitecturas en respuesta a los nuevos desafíos que emergieron durante el proceso de desarrollo.

Secuencia de actividades

Para el desarrollo de los objetivos se llevará a cabo el siguiente proceso:

- Modelar los procesos actuales usados para el sector de logística y movilidad.
- Identificar los puntos de optimización o de aplicabilidad tanto para recopilación información con dispositivos IoT como para conectar lo recopilado con interacciones por medio de blockchain.
- Escoger los puntos de optimización que serán estandarizados, es decir, que quedaran disponibles para su uso dentro del framework que se construirá.

- Evaluar las distintas arquitecturas para la comunicación con la blockchain, lo importante es que todo lo recopilado interactúe con la blockchain, para la conexión deben realizarse pruebas de poner a correr un nodo directo el dispositivo, pero de no ser posible, se crea o usa (si existe) un bridge que permita dicha conexión.
- Construir una librería para el entorno de MicroPython que permita inicializar dispositivos o sensores que participen en dichos puntos dentro de los procesos, e interactuar con la blockchain.
- Construir los *smart contracts* necesarios para soportar la lógica de negocio escogida (ya sea persistir, loggear, conectar, emitir eventos, etc.) para dichos puntos dentro del proceso.
- Construir una interfaz gráfica para la interacción del usuario con sus dispositivos y las transacciones que ocurran sobre estos, que de una manera más visible logre gestionar y realizar consultas que requiera.
- Realizar el despliegue en una *testnet* de *Ethereum* (luego del *Merge* lo más probable es usa Goerli) y posteriormente la verificación de los contratos (con Etherscan) para que sea totalmente visible el code.
- Integrar el framework construido dentro de un caso de uso real particular ya existente, tal como el seguimiento a un producto desde su puesta en bodega hasta su destino final. Lo anterior para comenzar con la realización de pruebas de integridad, escalabilidad, desempeño y seguridad en un entorno real.
- Evaluar la arquitectura en el caso de uso particular escogido, sin olvidar que independientemente del sector, únicamente cambiando la lógica de negocio, la misma, debe ser aplicable para cualquier otro sector.
- Realizar una retrospectiva de los artefactos, librerías, y en generale elementos del estándar construido, para proponer trabajo futuro muy probablemente sobre estos, o sobre extensiones de estos para otros sectores de igual relevancia como por ejemplo el de la salud.

Adicional al paso a paso descrito anteriormente, habrá actividades como la construcción del artículo y la presentación del proyecto que serán desarrolladas de manera transversal durante el desarrollo del proyecto. En la construcción del cronograma se mencionan también las actividades a realizar y el tiempo que tomara el desarrollo de cada una.

Cronograma

Temas	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5			
Actividades	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Estado del arte y análisis de tecnologías																				
Investigación de protocolos actuales de comunicación entre dispositivos IoT																				
Investigación del aprovechamiento de blockchain sobre la industria 4.0																				
Propuesta de diseño de arquitectura a construir																				
Exploración y pruebas cortas de posibilidades de comunicación IoT-Blockchain																				
Propuesta inicial e iteraciones sobre el diseño de una arquitectura																				
Creación y montaje de las interfaces externas a IoT y Blockchain de la arquitectura																				
Implementación de librería de MicroPython																				
Configuración de la Wemos, instalación de dependencias																				
Construcción de módulos para lectura de periféricos conectados a la Wemos																				
Desarrollo de la posibilidad de conexión escogida, modularizar y generalizar																				
Inclusión de módulos anteriores al firmware de mycropython (nativo)																				
Pruebas de alcance desde dispositivo IoT a la blockchain de funcionalidades																				
Implementación de smart contracts																				
Desarrollo smart contracts para la exposición de servicios de comunicación con IoT																				
Desarrollo de la lógica de negocio para sector logística sobre los smart contracts																				
Despliegue y verificación de smart contracts sobre una testnet de Ethereum																				
Pruebas de funcionamiento de toda la arquitectura en conjunto																				
PoC																				
Desarrollo de la PoC para el caso de uso real escogido																				
Ajustes necesarios sobre los componentes de la arquitectura a razón de la PoC																				
Generación de libro (DOCUMENTACIÓN), articulo y presentación																				
Construcción y desarrollo del libro y articulo																				
Preparación de la presentación																				

Capítulo 4

Marco teórico

Logística

La logística desempeña un papel fundamental en la economía mundial, abarcando una amplia gama de operaciones que incluyen la adquisición, almacenamiento, gestión de inventarios y transporte [6]. Los distintos tipos de logística se dividen en logística externa, logística interna, logística de salida y logística de reintegro.

La logística externa se encarga de la recolección de materia prima y su posterior transformación en productos finales. Por otro lado, la logística interna se ocupa del envío, distribución y almacenamiento de los productos en almacenes antes de su entrega al consumidor final. La logística de salida se encarga de la distribución de productos terminados a los clientes finales. Por último, la logística de reintegro se encarga de gestionar el retorno de productos ya consumidos para su reincorporación como materia prima.

En la actualidad, el proceso logístico se ve impulsado por la tecnología, dando lugar a lo que se conoce como logística 4.0. El objetivo de esta nueva tendencia es construir redes logísticas que sean eficientes, efectivas y rápidas, apoyándose en la utilización de datos y tecnología. La implementación de tecnologías como la logística 4.0 permite a las empresas gestionar sus recursos de manera más eficiente, reducir costos y optimizar los procesos.

La logística 4.0 se basa en la integración de tecnologías avanzadas, como el Internet de las Cosas (IoT), la inteligencia artificial (IA), el aprendizaje automático (*machine learning*) y la analítica de datos. Estas herramientas permiten recopilar información en tiempo real, optimizar la planificación y la toma de decisiones, así como automatizar ciertas tareas logísticas. Gracias a la logística 4.0, las empresas pueden mejorar la visibilidad de su cadena de suministro, anticiparse a posibles problemas y responder de manera ágil a las demandas del mercado.

Blockchain

Blockchain nació en 2008 como una tecnología principalmente para un contexto económico (soportar una moneda digital por medio de Bitcoin), pero sus propiedades tecnológicas hacen que sea el interés de muchos otros sectores de tecnología como lo son el cuidado de la salud, manufactura, retail y servicios de gobierno por todas sus cualidades, principalmente que es una red distribuida, inmutable, auditable, integra, es descentralizada y provee confianza y transparencia por la forma en como fue diseñada [7].

El detalle de algunas de las ventajas de usar blockchain para almacenar datos en comparación con los sistemas tradicionales son [8]:

- Seguridad: Blockchain usa cartografía para garantizar la seguridad de los datos, ya trae consigo la manera de proteger los datos y además los bloques en sí mismos están enlazados de manera criptográfica, lo cual hace casi imposible la modificación de los datos.
- Inmutabilidad: Los datos son inmodificables sin el consenso de la mayoría de los nodos de la red esto garantiza que no puedan ser alterados, ni borrados.
- Transparencia: Una de sus cualidades más destacadas es cualquier persona puede ver los datos almacenados en la cadena, manteniendo un estado publico todo el tiempo (generando confianza en los *stakeholders*
- Eficiencia: Los medios de almacenamiento actuales a menudo requieren intervención de terceros para hacer auditoria de los datos (verificar y validar), en una blockchain la validación se lleva a cabo automáticamente gracias a su diseño de nodos, reduciendo tiempo y costo de validación o a menudo sincronización de datos

- Autenticidad: Blockchain autentica y valida todas las transacciones por medio de una firma digital, lo que garantiza que antes de ser persistidos los datos no hayan sido manipulados ni falsificados.
- Distribución: Esta cualidad de las redes blockchain permite que, aunque puedan ocurrir fallas en algunos nodos, los nodos restantes aún son capaces de validar y registrar transacciones, agregando así disponibilidad y en caso tal recuperación de datos.
- Costos: Como parte de una ventaja derivada de las anterior, al no necesitar validación ni intermediarios se ve una reducción en los costos, además que los costos de infraestructura se ven repartidos en los miembros de la red, lo cual si se plantea en un esquema de negocio puede ser provechoso para la entidad prestadora del servicio.

Estructura

Las redes blockchain son sistemas de registro compartido que almacenan de forma descentralizada cadenas de bloques o transacciones. Cada bloque agregado al libro de registro está compuesto por diversos elementos que garantizan su integridad y seguridad.

En primer lugar, cada bloque tiene un identificador único y un número aleatorio llamado "nonce". Además, incluye la información relativa a la transacción, como transferencias de dinero o ejecuciones de modificaciones en contratos inteligentes. También contiene el hash generado previamente del bloque anterior.

Sin embargo, lo que hace realmente especial a la tecnología blockchain es su método de enlace de bloques. Cada bloque posee un hash que se genera utilizando toda la información mencionada anteriormente, incluido el hash del bloque anterior. Este enlace crea una cadena inalterable de información, ya que cualquier modificación en un bloque anterior alteraría su hash y, por ende, los enlaces posteriores, garantizando así la integridad de los datos.

Este enfoque descentralizado y la estructura en cadena de bloques hacen de las redes blockchain una solución confiable y segura para diversos propósitos, como la verificación de transacciones, la trazabilidad de productos y la ejecución de contratos inteligentes. [9]

Implementaciones

Actualmente existen una gran cantidad de tecnologías que usan el patrón blockchain, cada uno con características especiales, entre las cuales se encuentran [10]:

Bitcoin:

Es la primera red blockchain basada en un consenso de prueba de trabajo o por sus siglas en inglés (PoW), el cual una forma de prevención de fraude ante un posible atacante que permite que la red de blockchain tenga una forma de validar las transacciones que se está agregando sobre las cadenas de bloques [11]. Bitcoin está escrito en el lenguaje C++ el cual nace con el objetivo de ser una plataforma de pagos descentralizada, es decir, que se puedan realizar transacciones de pago sin tener que pasar por un intermediario con el uso de una red peer-to-peer.

Ethereum:

Ethereum es una red blockchain que es ejecutada sobre EVM o *Ethereum virtual machines* que son *Turing-complete* permitiendo la creación de contratos inteligentes para la generación de aplicaciones descentralizadas [12]. *Ethereum* usa el conceso POS o proof - of-stake, el cual tiene algunas ventajas a diferencia de PoW como lo son, mejor consumo de energía y reducción de barreras de entrada dado que ahora los nodos no necesitan capacidad de cómputo adicional.

IOTA:

Es una red muy similar a la red de blockchain que propone una implementación llamada *tangle* [13], el cual consiste en un grafo acíclico dirigido (DAG) que permite verificar transacciones de manera masiva, mejorando la cantidad de transacciones procesadas por segundo en comparación con *Bitcoin* o *Ethereum*. *IOTA* es una red *feeless* es decir que las transacciones

ejecutadas sobre ella no tienen ningún costo, esto supone ventajas para la creación de aplicaciones IoT sobre esta red

Hyperledger-Fabric:

Es una red blockchain basada en Java y Golang, esta red tiene la gestión de permisos lo que permite proveer confidencialidad al encriptar las transacciones, esta red blockchain a diferencia de *Bitcoin* y *Ethereum* no es una red pública, sino está enfocada en ser una red empresarial, modular, en donde cada empresa u organización puede gestionarla y administrarla a su manera [14].
Estas redes son las más representativas actualmente para la implementación de una aplicación descentralizada de IoT, cada una de estas posee ventajas o características que las hace únicas, es por esto por lo que es valioso ser resaltadas en el documento para que puedan ser tomadas en consideración al momento de tratar de implementar algo con tecnología blockchain

Consenso

Existen diferentes algoritmos de consenso sobre las redes blockchain, cada uno tiene ciertas características, algunos de los más comunes y relevantes son [9].

- Prueba de trabajo (POW): Se basa en resolver un problema costoso de computación, es realizado para poder atacar algunos problemas como seguridad como lo puede ser el ataque de 50 por ciento más uno, dado que se da prioridad a los nodos mineros que tengan más recursos de CPU y GPU. Esto a su vez trae desventajas como lo son la cantidad de recursos eléctricos que se puede consumir.

- Prueba de participación (POS): Es el algoritmo actualmente usado por la red Ethereum, se basa de una lógica de lotería, y probabilidad en donde, el que tiene más tiquetes (definido por la cantidad e Ethereum que el nodo tenga) tiene mayor posibilidad de ganar.

- Prueba de participación delegada (DPOS): Es igual que el algoritmo mencionado previamente con la exclusión de que se puede tener observadores (testigos) y votar por ellos para que tomen a responsabilidad de validar las transacciones.

- Prueba de participación alquilada (LPOS): Es un algoritmo diseñado por Waves, encargado de poder alquilar los *tokens* que tienen los nodos para generar nuevas transacciones

- Prueba de tiempo transcurrido (POET): Este consenso normalmente es usado en redes que son privadas (aunque de igual manera se pueda usar en redes públicas) o requieran autenticación de los nodos, se basa en poner un tiempo aleatorio de espera en los nodos para poder validar los bloques de la red. Este algoritmo fue desarrollado por Hyperledger Sawtooth

- Tolerancia a práctica de fallos bizantinos (PBFT): Su nombre es dado por la historia de los generales bizantinos, el cual se basa en poder generar un consenso de manera correcta sin importar que algunos de los nodos sean maliciosos.

Contratos inteligentes

La automatización de procesos de logística es crucial en la industria para mejorar la eficiencia y reducir los costos. Una de las grandes ventajas de la tecnología blockchain son los contratos inteligentes, los cuales permiten tomar acciones automáticas ante eventos específicos. Para el manejo de logística, esto es especialmente útil, ya que permite monitorear estadísticas y tomar acciones en tiempo real gracias a su seguridad, trazabilidad y transparencia de la red blockchain al poder generar relaciones de confianza entre los pares de logística [15].

Un caso de uso interesante es el monitoreo de la cadena de frío de productos. La cadena de frío se refiere al proceso de mantener ciertas temperaturas para asegurar la calidad de los productos refrigerados o congelados. En la logística, es fundamental monitorear la cadena de frío para garantizar que los productos no se dañen y lleguen a su destino en óptimas condiciones [16]. Esto trae grandes beneficios para las empresas como lo es el monitoreo de los alimentos, reducción de

costos al prevenir que los alimentos, medicamentos u otros elementos se dañen por su mal manejo de cadena de frio.

Usando contratos inteligentes en la blockchain, se puede crear un sistema automatizado que monitoree constantemente la cadena de frío de los productos. Si la temperatura se desvía de los valores aceptables, se puede generar automáticamente un evento que notifique al personal de logística para que tomen medidas inmediatas para solucionar el problema. Esto incluye la identificación del producto afectado y la eliminación de cualquier producto que haya sido dañado.

Además, la tecnología blockchain justo con smart contracts permite a los actores involucrados en la logística de un producto, como los proveedores, los transportistas y los minoristas, tener acceso a información actualizada y confiable en tiempo real sobre el estado de los productos. Esto mejora la transparencia en la cadena de suministro, lo que a su vez mejora la calidad y la seguridad de los productos y reduce el riesgo de pérdidas financieras.

En resumen, la tecnología blockchain y los contratos inteligentes tienen un gran potencial para mejorar la automatización de procesos de logística. Al monitorear y tomar medidas automáticas ante eventos específicos, como la ruptura de la cadena de frío de un producto, podemos mejorar la eficiencia y la calidad de la logística de manera significativa.

Ecosistema Blockchain - Ethereum

En la EVM de *Ethereum*, existen ciertas reglas sobre lo que puede ser considerado como una cuenta o más precisamente una dirección para alcanzar un activo interno de la blockchain ya sea una dirección de cuenta con dueño o un *smart contract*.

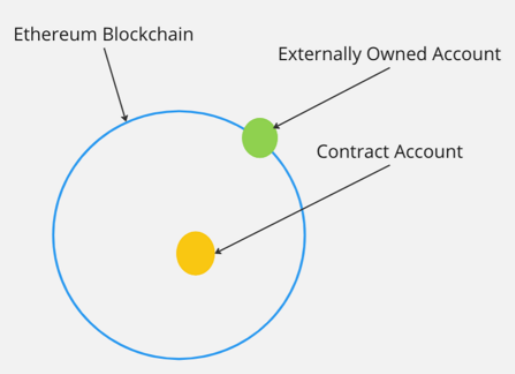


Ilustración 1. EOA y contract accounts

En el ecosistema blockchain existen dos categorías de cuentas: la primera se crea a través de una clave privada que se utiliza más a modo de wallet digital y se conoce como **cuenta de usuario**. La segunda categoría de cuentas son los contratos inteligentes, que también tienen una dirección única en la red *Ethereum* y se utilizan para ejecutar lógica programable en la cadena de bloques. Estas últimas son conocidas como **cuentas de contrato**.

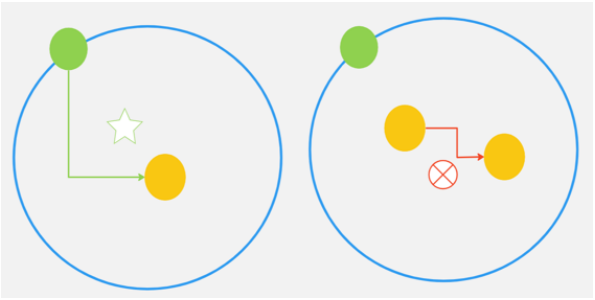


Ilustración 2 Creación o inicialización de cuentas de Ethereum

Es importante destacar que en el ecosistema blockchain, sólo una cuenta de usuario (EOA) puede iniciar una transacción. Por lo tanto, si un contrato inteligente necesita realizar una acción, debe ser llamado por una cuenta de usuario para ejecutar la función programable correspondiente. Es decir, el contrato inteligente no puede iniciar una transacción por sí solo. Sin embargo, una vez que el contrato ha sido inicializado por una cuenta de usuario, puede realizar acciones adicionales y ejecutar otras funciones programables e incluso otros contratos (que pudieron haber sido inicializados previamente por otras EOA) [17].

En otras palabras, en una arquitectura basada en *Ethereum* y orientada a gemelos digitales o *digital twin*, el control de los recursos se gestiona mediante direcciones válidas generadas a partir de la

creación de una cuenta (ya sea una cuenta de usuario o una cuenta de contrato) en la red *Ethereum*. Por lo tanto, es importante considerar esta característica al diseñar este tipo de arquitectura.

En adición a lo anterior, existen otras características de blockchain que permiten la interacción o detonación de acciones entre *smart contracts* e incluso con interfaces externas, y estos son los eventos (logs). Lo eventos en *Ethereum* funcionan como medio de comunicación tanto interna como externa, es decir pueden ser escuchados por otros *smart contracts* o por interfaces externas que por medio de la librería de web3 sean capaces de inicializar la instancia del *smart contract* para escuchar sus eventos, de esta manera el registro a un evento es posible con la dirección del contrato dentro de la blockchain y por supuesto con el nombre del evento. Lo anterior convertiría a los eventos como la segunda forma de interacción con la blockchain (primero son las funciones para hacer llamados e inicializar transacciones) y seguido a esto eso estarían los eventos para emitir normalmente los datos pertinentes cuando finaliza la transacción [18].

IoT

En la actualidad, la tecnología ha avanzado a pasos agigantados y ha permitido el desarrollo de nuevos dispositivos que se han vuelto cada vez más relevantes en nuestras vidas cotidianas. Entre ellos, destacan los dispositivos IoT, que se han convertido en una tendencia en aumento en el mercado tecnológico. Se espera que el número de dispositivos IoT conectados a la internet alcance los 27 mil millones de dispositivos en los próximos años. Sin embargo, con este crecimiento también surgen riesgos de seguridad y privacidad, lo que hace que sea de vital importancia tener en cuenta los aspectos de seguridad y el tratamiento de la información en estos dispositivos [19]. Con respecto a la arquitectura se tiene:

Capa de sensores

Los sensores, como componentes fundamentales de los sistemas IoT, desempeñan un papel crucial en la recopilación y el análisis de datos de diversas fuentes, como el clima, la temperatura, la humedad, entre otros. La función principal de estos dispositivos es obtener medidas del entorno y

transmitirlas a la siguiente capa de procesamiento. Dependiendo de su tipo, los sensores pueden ser capaces de recopilar información de diferentes fuentes, lo que permite la monitorización en tiempo real y la toma de decisiones basadas en datos precisos y fiables.

Capa de Gateway

Esta capa es la encargada de pedirle a la capa de sensores toda la información necesaria y posteriormente enviarla a una base de datos persistente en la nube. Son equipos de procesamiento que se encuentran del lado del dispositivo IoT, que tienen acceso a internet y que son capaces de procesar mensajes para comunicarlos hacia la nube

Capa de nube

Esta capa es la encargada de recibir toda la información procesada por los dispositivos IoT y persistirla, dentro de esta se pueden encontrar otras subcapas como lo es la capa *Fog computing* o *Edge computing* que son una subcapa muy cercana a los dispositivos IoT posicionalmente que le permite procesar de manera mucho más rápida información que no necesariamente debe ser enviada a la nube [20]

Capa de aplicación

Capa de aplicación o capa de presentación esta es la encargada de mostrarle la información necesaria recopilada previamente por los dispositivos IoT a los usuarios finales, para que estos puedan recibirla, leerla y poder tomar acciones con dicha información

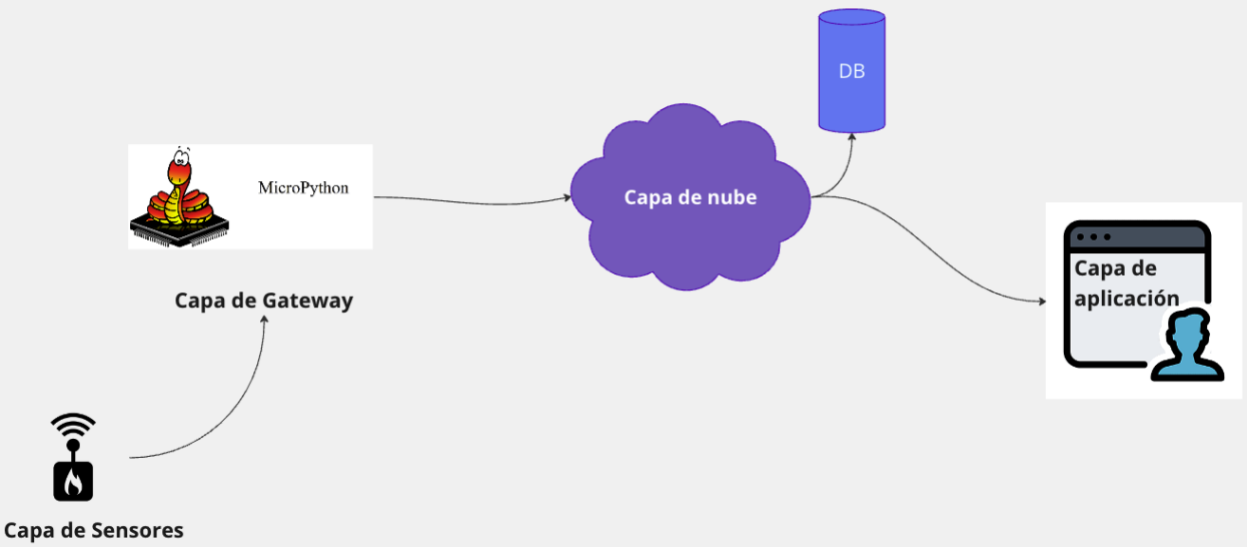


Ilustración 4 ***Diagrama de las diferentes capas de comunicación en arquitecturas IoT***

MicroPython

MicroPython es una implementación especializada de Python3 diseñada específicamente para microcontroladores. Su propósito principal es permitir la programación a un nivel más bajo utilizando un lenguaje sencillo como Python. Esta característica resulta especialmente útil para desarrolladores de sistemas embebidos que buscan una manera más accesible de interactuar con los microcontroladores.

Una de las ventajas significativas de MicroPython radica en su capacidad para acceder a los recursos de los microcontroladores a nivel de pines a través de bibliotecas dedicadas. Esto proporciona a los desarrolladores un control granular sobre los componentes físicos de sus dispositivos y les permite interactuar directamente con ellos. Además, MicroPython ofrece herramientas como ampy, que facilitan la comunicación y la transferencia de datos entre el microcontrolador y otros dispositivos.

Un aspecto destacado de MicroPython es su eficiente recolector de basura. Dado que los microcontroladores a menudo tienen limitaciones de recursos, como memoria y capacidad de procesamiento limitadas, la gestión adecuada de la memoria es crucial. El recolector de basura de

MicroPython se encarga de liberar automáticamente la memoria no utilizada, lo que contribuye a maximizar la eficiencia y el rendimiento de los microcontroladores en entornos con recursos limitados. [21]

Cifrado

Encriptación simétrica

Este método de encriptación es usado por medio de una llave privada, en donde dicha llave es conocida tanto por la entidad que escribe el mensaje como la entidad que recibe el mensaje, y por medio de esta llave y el mensaje encriptado, puede descifrar lo que el mensaje dice.
Existen muchos algoritmos de encriptación simétrica, los más conocidos de ellos son *Advance encription standards* (AES), *Data encription standards* (DES), y *blowfish* entre otros [22].

Encriptación asimétrica

Este método de encriptación a diferencia de la encriptación simétrica la cual solo requiere una llave privada conocida por las dos entidades, este posee dos llaves, una llave pública encargada de descifrar el mensaje y una llave privada que permite cifrar el mensaje, esto permite que la persona o entidad encargada de enviar el mensaje cifre por medio de la llave privada y la otra entidad que quiere leer el mensaje puede hacerlo con la llave pública, asegurándose autenticidad, confidencialidad y autorización de la información.

Existen diferentes algoritmos de encriptación asimétrica, algunos de los más conocidos son RSA y ECDSA entre otros. El mecanismo de encriptación RSA, desarrollado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman [23], es uno de los pilares fundamentales de la seguridad de la información en la era digital. RSA (acrónimo de las iniciales de sus creadores) se basa en el concepto de criptografía de clave pública, que permite a los usuarios cifrar y descifrar información utilizando dos claves distintas pero relacionadas: una clave pública, que se comparte libremente, y una clave privada, que se mantiene en secreto.

La fortaleza de RSA radica en la dificultad computacional de factorizar números primos extremadamente grandes, un problema conocido como factorización de enteros. La seguridad de RSA se basa en el hecho de que factorizar números de gran tamaño es un proceso exponencialmente costoso y computacionalmente complejo, incluso para los algoritmos más eficientes conocidos. Esto significa que, si se utiliza una clave lo suficientemente larga, el mecanismo RSA proporciona una protección sólida contra los intentos de descifrar la información cifrada sin poseer la clave privada correspondiente.

El uso generalizado de RSA se ha extendido a numerosas aplicaciones, como la seguridad de las comunicaciones en línea, el cifrado de datos almacenados, las transacciones financieras y la autenticación de identidad en sistemas informáticos. Dado su papel fundamental en la protección de la privacidad y la confidencialidad de la información sensible, la seguridad de RSA es de vital importancia en nuestra sociedad cada vez más interconectada y dependiente de las comunicaciones digitales [22].

Capítulo 5

Estado del arte

Estado del arte de la cadena de suministro

En el contexto actual de la globalización y los cambios en el mercado global, los procesos logísticos se enfrentan a desafíos sin precedentes. Cada componente necesario para la producción de productos se encuentra disperso en diferentes ubicaciones, bajo la administración de diversas empresas. La capacidad de unificar todos estos recursos de manera efectiva se vuelve crucial, lo que implica la adopción constante de nuevas tecnologías para alcanzar los objetivos de la cadena de suministro. Asimismo, la visibilidad de las empresas de logística interconectadas se vuelve esencial para operar de manera eficiente en esta red logística tan compleja [24].

En este sentido, el uso de redes blockchain en la cadena de suministro adquiere una relevancia significativa para aquellas empresas que buscan demostrar confianza, transparencia y mejorar la seguridad en sus procesos. Las redes blockchain, basadas en la descentralización, la inmutabilidad y la criptografía, ofrecen una solución prometedora para abordar los desafíos (como gestión del inventario, cumplimiento normativo, falta de transparencia) inherentes a la cadena de suministro.

Al utilizar la tecnología blockchain, las empresas pueden crear un sistema distribuido y seguro donde cada transacción y registro de productos se registra de forma permanente y transparente.

Esto permite rastrear el movimiento de los productos a lo largo de toda la cadena de suministro, desde la obtención de materias primas hasta la entrega final al cliente. Además, al estar basado en la criptografía, el blockchain proporciona una capa adicional de seguridad, asegurando la integridad de los datos y protegiéndolos contra alteraciones malintencionadas.

La adopción de blockchain en la cadena de suministro ofrece numerosos beneficios. En primer lugar, mejora la trazabilidad, lo que permite identificar y solucionar rápidamente cualquier problema o incidencia que pueda surgir en el proceso logístico. Esto tiene un impacto directo en la eficiencia operativa, reduciendo los tiempos de respuesta y minimizando los riesgos asociados a la falta de visibilidad en la cadena de suministro. Además, la transparencia proporcionada por la tecnología blockchain fomenta la confianza entre las partes involucradas en la cadena de suministro. Al tener acceso a un registro inmutable y verificable de todas las transacciones, se eliminan las dudas y se fortalecen las relaciones comerciales. Esto es especialmente relevante en un entorno global donde las empresas deben colaborar con socios y proveedores de confianza en diferentes ubicaciones geográficas. Otro aspecto importante es la mejora en la seguridad. Al utilizar la criptografía y la descentralización, el blockchain protege los datos y evita la manipulación o falsificación de la información. Esto es especialmente valioso en la cadena de suministro, donde la autenticidad y la integridad de los datos son fundamentales para garantizar la calidad y la procedencia de los productos. La implementación de blockchain en la cadena de suministro no está exenta de desafíos. Requiere una cuidadosa planificación y coordinación entre todas las partes involucradas, así como la integración con los sistemas existentes. Además, el escalado de la tecnología para manejar grandes volúmenes de transacciones y la interoperabilidad entre diferentes redes blockchain también son consideraciones importantes.

Cadena de suministro del sector de la salud

En el ámbito de la cadena de suministro del sector de la salud, nos enfrentamos actualmente a desafíos significativos que requieren abordarse de manera efectiva. Entre estos desafíos se encuentran la seguridad, la transparencia y la manipulación de productos médicos, así como la proliferación de medicamentos falsificados. Además, gran parte del proceso de validación y

transporte de medicamentos hasta llegar al usuario final todavía se lleva a cabo de forma manual, lo que consume una cantidad considerable de tiempo.

Sin embargo, se ha demostrado que la incorporación de dispositivos de Internet de las cosas (IoT) y redes blockchain en la cadena de suministro del sector de la salud puede ofrecer numerosas ventajas. Por ejemplo, en el artículo [25], Nada resalta que estas tecnologías pueden garantizar la autenticación de los productos, permitir la trazabilidad de estos, combatir eficazmente los medicamentos falsificados y proporcionar transparencia y seguridad en todo el proceso. Además, el uso de IoT y blockchain también permite obtener información en tiempo real, lo que facilita la toma de decisiones y la automatización de los procesos, incluyendo los cobros y pagos mediante contratos inteligentes.

La inclusión de dispositivos IoT en la cadena de suministro de productos médicos permite monitorear y rastrear el movimiento de los productos en cada etapa del proceso, desde la fabricación hasta la entrega final. Esto proporciona una visibilidad completa y precisa de la ubicación y el estado de los productos en tiempo real. Además, los dispositivos IoT pueden enviar datos sobre las condiciones de almacenamiento, como la temperatura y la humedad, lo que es crucial para garantizar la calidad y eficacia de los medicamentos.

Por otro lado, la implementación de redes blockchain en la cadena de suministro del sector de la salud brinda una mayor confianza y seguridad en las transacciones. La tecnología blockchain permite crear registros inmutables y transparentes de todas las transacciones y actividades relacionadas con los productos médicos. Esto garantiza la integridad de los datos y reduce el riesgo de fraude, falsificación o manipulación de productos. Además, la trazabilidad de la blockchain facilita la identificación y eliminación rápida de productos falsificados, lo que contribuye a proteger la salud y la seguridad de los pacientes.

La utilización de contratos inteligentes, una característica clave de las redes blockchain, también ofrece beneficios significativos en la cadena de suministro del sector de la salud. En el contexto de la cadena de suministro, los contratos inteligentes pueden automatizar los procesos de cobros y pagos, lo que agiliza las transacciones y reduce los errores y los costos administrativos. Además,

al basarse en una infraestructura segura y descentralizada, los contratos inteligentes brindan mayor confianza y transparencia en las transacciones comerciales entre los participantes de la cadena de suministro.

Arquitecturas para integración blockchain/IoT

La manera en que se pueden interactuar blockchain e IoT puede obedecer a alguna de las siguientes arquitecturas [26]:

Arquitectura #1: IoT-Blockchain

En este enfoque todas las interacciones pasan por blockchain, lo que permite un registro inmutable de interacciones. Este enfoque garantiza que todas las interacciones elegidas sean rastreables, ya que sus detalles se pueden consultar en la cadena de bloques y, además, aumenta la autonomía de los dispositivos IoT. Las aplicaciones de IoT que pretenden comercializar o alquilar, pueden aprovechar este enfoque para proporcionar sus servicios.

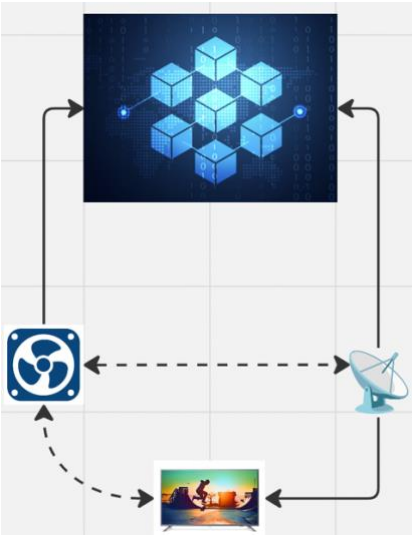


Ilustración 5 Interacción y datos de los dispositivos son persistidos en la blockchain.

Arquitectura #2: IoT-IoT

Los dispositivos IoT deben poder comunicarse entre sí, lo que generalmente implica mecanismos de descubrimiento y enrutamiento. Solo una parte de los datos de IoT se almacena en la cadena de bloques, mientras que las interacciones de la IoT tienen lugar sin usar la cadena de bloques.

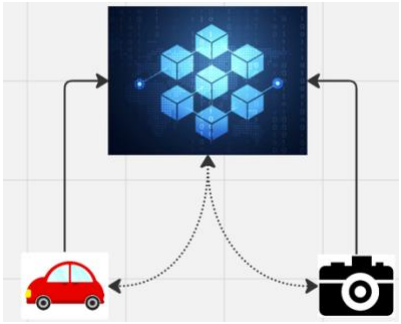


Ilustración 6 Interacción directa entre dispositivo IoT y datos persistidos en la blockchain.

Arquitectura #3: Acercamiento hibrido (Fog/Cloud)

Un diseño híbrido donde solo una parte de las interacciones y los datos tienen lugar en la cadena de bloques y el resto se comparte directamente entre los dispositivos IoT. En este enfoque podría entrar en juego la *Fog computing* (capa en la nube muy cerca físicamente de los dispositivos IoT) e incluso *Cloud computing*, para complementar limitaciones que pueda haber de la cadena de bloques y el IoT.

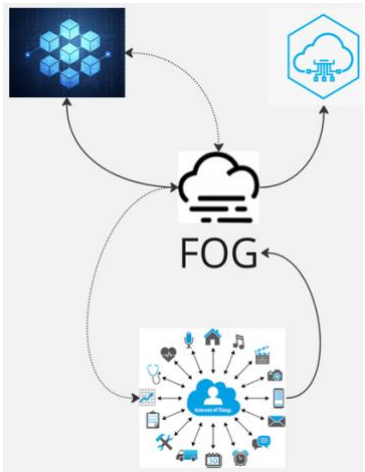


Ilustración 7 Interacciones y datos ocurren una parte en la cloud y otra sobre blockchain.

Para realizar la integración, es necesario decidir donde se llevarán a cabo esas interacciones, ya que todas son alternativas validas. Actualmente las soluciones asociadas expuestas, son propuestas

como un componente adicional a la arquitectura (es decir la arquitectura #1) y persisten la información allí para poder tener la confiabilidad que la blockchain provee sobre algunos datos, pero no existe un estándar de uso para una solución que haga una implementación de comunicación directa entre los dispositivos IoT y una red Blockchain, que provea directamente toda la información para una verdadera autenticidad y veracidad de la información generada por los sensores (arquitectura #2), administrando en todo momento tanto la información como las interacciones entre dispositivos.

Evolución de blockchain

En este momento todas las redes Blockchain está en constante cambio [27], debido a la propuesta de valor que exponen, por ello comienzan a ser más demandadas y a construir comunidades cada vez más grandes. Principalmente para la red de *Ethereum* (la más usada en el presente) hay un roadmap que abarca problemáticas muy grandes que se tienen actualmente [28], en donde se divide el trabajo en diferentes etapas llamadas:

- *The merge*: Ya sucedió y se realizó la principal transición al algoritmo de proof of stake, permitiendo a la red de *Ethereum* ser una red más viable de manera ecológica [29] bajando significativamente el uso de recursos de hardware para minar, además de la velocidad de minado.
- *The surge*: Hace una implementación inicial de sharding mejorando la velocidad y alcance de la red, con ejecución paralela de bloques y proyecciones de ejecución de entre 2000 y 1000 transacciones por segundo con bajo costo. También con consecuencia de un mercado de micro transacciones en la segunda capa.
- *The verge*: Permite que los nodos sobre la red no tengan que mantener toda la información de manera local sino solo algunos nodos "padres" serán los encargados de tener todas las transacciones sobre la red, como consecuencia habrá nodos ultraligeros (dando lugar con mayor fuerza a los dispositivos IoT para poder ser nodos fácilmente).
- *The purge*: Es una fase de la limpieza en donde se busca bajar la memoria y transacciones viejas sobre la red que no son necesarias, además se propone alcanzar *darksharding* y rollups para proyectar 100000 transacciones por segundo.

- *The splurge*: En esta fase se espera una nueva revolución con miles de millones de sensores en una red global de coordinación, dando paso a *Ethereum* como el "Ledger of things", una plataforma de coordinación global para IoT.

Todo esto que se está haciendo actualmente sobre las redes blockchain y principalmente sobre la red más usada de blockchain que es la red de *Ethereum*, permite algunas funcionalidades que antes no era tan viables por la cantidad de transacciones permitidas sobre la red blockchain, ahora se puedan ver como una posibilidad, como por ejemplo guardar masivamente transacciones sobre los dispositivos IoT a nivel global de manera eficiente. Esto es un proceso que aún no ha finalizado y cada vez se va optimizando de una manera más efectiva, gracias a la misma comunidad que construye (pues de esta manera es que se mueve una tecnología en furor).

Blockchain e *IoT* en la Industria

Muchos sistemas de IoT no pueden ser desplegados de manera productiva a menos que sean implementadas soluciones de seguridad congruentes [30], los problemas más grandes que tiene actualmente las diferentes arquitecturas de IoT es la seguridad en los aspectos de autorización, autenticación y control de acceso [31]. Es por esto por lo que es indispensable poder diseñar un sistema en el que todos los participantes puedan creer en los datos que hay en el sistema.
Se han propuesto algunos framework distribuidos para el manejo de los recursos como *Secure and Distributed Framework for Resource Management* (SDFRM por sus siglas en inglés) sobre la industria 4.0 en donde se garantiza una fuerte privacidad sobre los procedimientos asociados con el control de acceso soportado sobre Blockchain. De la misma forma, se han usado algunas implementaciones para:

- Contrarrestar la falsa activación del monitoreo de signos vitales de los pacientes epilépticos [32], en donde por medio de IoT se monitorea de manera continua la presión de la sangre, ritmo cardiaco, y el estado del dispositivo, si este se encuentra activo o inactivo. Todos estos datos por su máxima seguridad se guardan en una Blockchain privada por medio de una conexión *Wifi*.
- Permitir la persistencia de los datos generados por los sensores en el campo de agricultura mejorando la forma en la que los dispositivos IoT se comunican entre ellos [33]. Aplicar

Blockchain a la agricultura, permite tener mejor trazabilidad de los recursos físicos y digitales, además de una mejor trazabilidad de los recursos, esto en la cadena de suministro de productos alimenticios es crítico. De cada cadena de suministro alimenticio se podría rastrear todo lo que ha sucedido desde el inicio del producto hasta que es finalmente consumido, desde que prácticas de usaron de cultivo, que fertilizantes. Permitiendo a los consumidores finales, asegurarse de su autenticidad [34].

- Mejora en la implementación de nuevos mecanismos de movilidad como lo es el car-sharing (compartir un vehículo) y car-leasing (arrendar un vehículo) fomentando una economía colaborativa en donde se mejoran los aspectos de seguridad, evitando robos por medio de mecanismos de autenticación existentes den las redes Blockchain al igual que mejora la trazabilidad por medio de las redes Blockchain e IoT y en donde por medio de contratos inteligentes se automatiza todo el proceso de pago, usando pago digital [35].

Así mismo, se ha aumentado el crecimiento en los últimos años de manera exponencial de la unión de estas dos tecnologías [36] en donde primeramente se intenta enfocar en los aspectos de la seguridad, para asegurar la integridad de los datos manejados por los dispositivos IoT o proteger la confidencialidad de dichos datos. También se busca mejorar la eficiencia de los dispositivos IoT por medio de la interacción con la lógica potencialmente soportada por los *smart contracts,* reduciendo costos y mejorando la eficiencia energética.

Las redes blockchain junto con la tecnología IoT pueden ser un muy buen complemento para el manejo de la logística, transformando este sector de una manera más ágil, segura, confiable y transparente. El verdadero desafío es abordar el flujo continuo de productos en toda la cadena de abastecimiento, desde que se extrae la materia prima hasta que se entrega un producto finalizado y además lograr la visibilidad de los productos en cada etapa aún no se ha abordado [37]. La aplicación de Blockchain junto con IoT sobre la logística tiene algunas ventajas como:

- Evitar la falsificación de los productos en la cadena de suministro por medio de su trazabilidad dentro de la Blockchain y generando sistemas de autenticación en dos pasos que permitan ver la veracidad del producto.

- Mejora de visibilidad de los productos, actualizando continuamente su estado sobre la blockchain.
- Eliminar los procesos manuales de papeleo en el ciclo de vida de los productos por medio de la automatización lograda con los *smart contracts*.

Otro gran ejemplo donde existe una buena aplicabilidad de la fusión de estas dos tecnologías es en el sector transporte, uno de los grandes pilares en la construcción de *smart cities*. Un sistema de movilidad inteligente exige la creación de un sistema de tránsito interconectado para garantizar la flexibilidad y la eficiencia, por ello se plantean modelos y mecanismos que permitan la implementación de una solución con interacciones integradas con blockchain [27] .

La aplicabilidad de estas dos tecnologías es un hecho que seguirá expandiéndose, y como toda gran expansión, en este momento es importante comenzar con la creación de mecanismos, protocolos y estándares que puedan ser reutilizables y aprovechados bajo ciertos escenarios presentados con mayor frecuencia, donde se involucren sensores con comportamiento especifico, para poder atacar e iterar cada vez más sectores de la industria, que hagan uso de dispositivos IoT, dándoles el trato correcto a cada uno de los escenarios, permitiendo reducir la heterogeneidad existente en el campo.

Un Aspecto de seguridad importante para la comunicación de dispositivos IoT es poder verificar la autenticidad de un dispositivo, para esto, en la red blockchain se han hecho algunas pruebas de concepto, entre ellas está la definición de una identidad digital descentralizada (DiD) por medio de la creación de un gemelo digital. Con la ayuda de los contratos inteligentes sobre las redes de blockchain se pueden crear sistemas de gestión de accesos distribuidos seguros [38] [39] . En este artículo se propone un sistema descentralizado de identidad digital.

Con respecto a la búsqueda de la representación o el modelamiento de los dispositivos IoT sobre blockchain para manejar su lógica y los datos asociados en tiempo real, encaja perfecto un modelo digital twin, el cual es una versión digital de una operación física o sistema del mundo real que busca actualizarse constantemente con datos en tiempo real para que coincida con las propiedades

y los comportamientos reales del objeto físico o proceso que representa. La utilización de los *digital twin* en torno a la tecnología blockchain ha presentado los siguientes hallazgos [40]:

- La seguridad, registros descentralizados, la posibilidad de compartir información, una conexión extrema a extremo, una trazabilidad confiable y la capacidad de escalar son todos los aportes que brinda blockchain con gemelos digitales de manera predeterminada.
- Los múltiples gemelos digitales pueden colaborar eficientemente mediante una estructura jerárquica y detallada gracias al uso de blockchain, aprovechando la información colectiva para controlar y monitorear con precisión los datos relacionados con el ensamblaje del producto.
- Se recurre a un contrato inteligente adicional para automatizar determinadas operaciones con el fin de fortalecer la confiabilidad y eficacia en la transmisión de datos, brindar información fiable, facilitar el uso eficiente de los datos y monitorear las acciones relevantes para las partes involucradas en la creación de gemelos digitales.

A pesar de que existen propuestas de implementación de digital twin sobre blockchain, cabe aclarar que es necesario profundizar en la investigación de varios desafíos con el fin de identificar, evaluar y minimizar los riesgos potenciales impulsados por gemelos digitales basados en blockchain.

Para la programación sobre dispositivos IoT se ha desarrollado un lenguaje de programación en C llamado MicroPython el cual es una versión ligera de la versión Python. El lenguaje de programación ha venido en gran crecimiento y actualmente es de los lenguajes de programación más usados para los desarrolladores de software [41] por su fácil y rápida habilidad de aprendizaje, es un lenguaje en el cual se puede programar aplicaciones de componentes IoT de una forma rápida para las personas que apenas están iniciando en el mundo de la programación o también para personas ya con amplia experiencia en el desarrollo de software [42].

RSA

El algoritmo de encriptación asimétrica, ampliamente conocido como RSA, ha mantenido su relevancia y significado en el campo de la seguridad informática desde su propuesta en 1977. A lo

largo de décadas, RSA ha demostrado ser un mecanismo confiable y seguro para la encriptación de datos. Sin embargo, en la actualidad, en un entorno tecnológico en constante evolución, es imperativo que examinemos el estado de arte de RSA para comprender su vigencia y adaptabilidad frente a los avances tecnológicos más recientes. Este análisis nos permitirá valorar adecuadamente la capacidad de RSA para abordar los desafíos de seguridad y privacidad en el panorama digital actual. Al comprender el lugar de RSA como estado de arte, podremos apreciar su relevancia continua y su potencial para la protección de la información sensible en un mundo tecnológico en constante cambio.

En el campo de la seguridad de la información, el mecanismo de encriptación RSA ha demostrado ser una piedra angular durante décadas. Sin embargo, en los últimos años ha surgido una preocupación creciente: la amenaza potencial que representa la computación cuántica para la seguridad de RSA. A medida que la tecnología cuántica avanza, se plantea la posibilidad de que los avances en la computación cuántica puedan desencriptar rápidamente las claves utilizadas en el sistema RSA, comprometiendo así la seguridad de las comunicaciones y la protección de la información confidencial. Según una simulación y estudio hecho por científicos de Fujitsu usando el algoritmo de Shor (algoritmo de computación cuántica enfocado en descomposición de factores primos) [43], aun se proyecta para un tiempo lejano, debido a:

- Limitaciones de los algoritmos cuánticos actuales: Aunque el cómputo cuántico ha avanzado significativamente en los últimos años, los algoritmos cuánticos conocidos para la factorización de números enteros, como el algoritmo de Shor, aún no son lo suficientemente eficientes para romper la encriptación RSA utilizada en muchas aplicaciones de seguridad. Estos algoritmos cuánticos tienen requisitos de hardware y capacidad de procesamiento extremadamente altos, lo que limita su aplicabilidad práctica. Aunque se han logrado algunos avances en la factorización de números pequeños utilizando computadoras cuánticas, aún queda un largo camino por recorrer para desencriptar claves RSA de tamaño real.

- Longitud de las claves RSA: La seguridad del cifrado RSA radica en la dificultad de factorizar grandes números primos, utilizados para generar las claves públicas y privadas. La longitud de estas claves es crucial para resistir los ataques criptográficos. Actualmente, se

recomienda el uso de claves RSA de 2048 bits o más, ya que la factorización de números de este tamaño es extremadamente difícil incluso para los algoritmos de factorización cuántica más avanzados. La capacidad actual de los ordenadores cuánticos está muy lejos de ser capaz de desencriptar claves RSA de esta longitud de manera efectiva [43].

- Tecnología en desarrollo: La computación cuántica se encuentra en una etapa temprana de desarrollo y todavía enfrenta numerosos desafíos técnicos. Aunque se han logrado avances significativos en la creación de *qubits* más estables y en el control de errores cuánticos, todavía no se ha alcanzado un punto en el que sea posible construir una computadora cuántica lo suficientemente grande y estable como para romper el cifrado RSA de manera eficiente. Incluso si se lograra un avance significativo en la computación cuántica, la comunidad criptográfica tiene tiempo para desarrollar y adoptar algoritmos de cifrado más resistentes a los ataques cuánticos, conocidos como criptografía post-cuántica, antes de que el poder de cómputo cuántico suponga una amenaza real para RSA.

En esta era de avances tecnológicos rápidos, es crucial reconocer y abordar los desafíos emergentes de seguridad. A medida que la investigación en computación cuántica continúa, es imperativo que la comunidad criptográfica y los expertos en seguridad exploren y desarrollen soluciones alternativas resistentes a los ataques cuánticos, conocidas como criptografía post-cuántica. El objetivo es mantener la integridad y la confidencialidad de la información en un entorno en el que la computación cuántica pueda ser una realidad. En este sentido, la comprensión y la anticipación de las amenazas que la computación cuántica plantea a RSA es esencial para garantizar la seguridad a largo plazo de nuestros sistemas de información

Capítulo 6

Desarrollo

Arquitecturas

Primera versión

En la primera versión del proyecto de grado, se planteó la idea de conectar dispositivos IoT de manera generalizada directamente a una red blockchain, es decir, la arquitectura #1 mencionada previamente en la sección número 5, arquitecturas para integración blockchain/IoT. Sin embargo, se tuvo conocimiento previo de la limitación de recursos de cómputo, espacio de memoria y procesamiento, lo que llevó a descartar esta opción. Para conectarse a una red blockchain, es necesario poder actuar como un nodo en la red, y existen cuatro tipos de nodos: nodos completos, nodos mineros, nodos de validación y nodos ligeros.

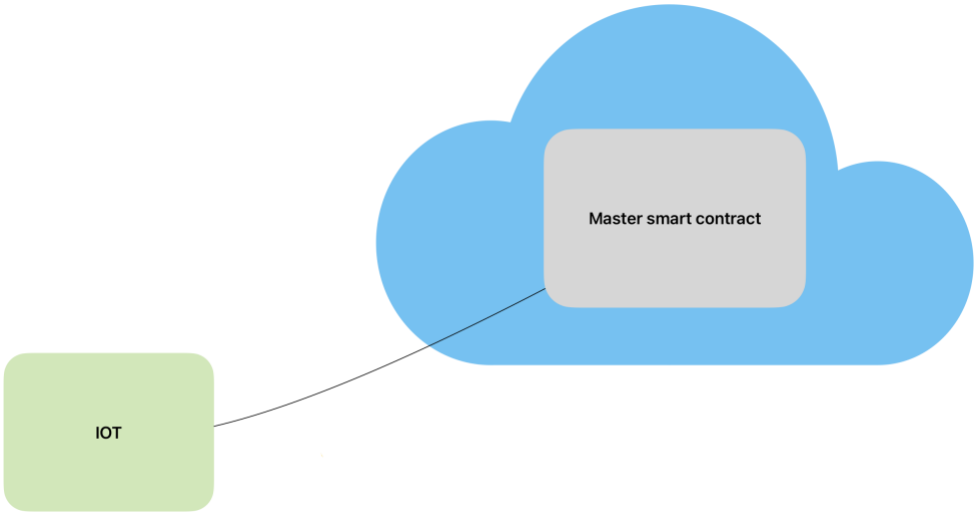


Ilustración 8 Primera versión arquitectura

Los nodos completos no son viables para dispositivos IoT, ya que estos tienen toda la información de la blockchain y sería imposible para un dispositivo IoT almacenar tal capacidad. Los nodos mineros se encargan de validar las nuevas transacciones que quedan persistidas en la blockchain y tampoco son adecuados para el caso de uso de este proyecto. Los nodos de validación, al igual que los nodos mineros, no son relevantes para este proyecto. Por último, los nodos ligeros no tienen la información completa de la blockchain y dependen de otros nodos para validar la información, lo que podría ser un buen caso de uso para conectar dispositivos IoT a la blockchain.

Sin embargo, desafortunadamente, tanto los dispositivos IoT como la red blockchain de *Ethereum* requieren más procesamiento del que estos dispositivos pueden proporcionar. Para ejecutar un nodo ligero en *Ethereum*, se requiere al menos 4GB de RAM y un procesador de dos núcleos, lo que supera las capacidades de muchos dispositivos IoT.

Es importante mencionar que existen otras redes blockchain que permiten trabajar con dispositivos IoT directamente, como IOTA. Sin embargo, para *Ethereum*, que es el caso de uso actual, la primera versión del proyecto que involucra la conexión directa de dispositivos IoT a la blockchain queda descartada debido a limitaciones de recursos.

Segunda versión

En vista de las limitaciones de recursos que se enfrentaron, la idea inicial de conectar directamente los dispositivos IoT a la blockchain resulta inviable. Por tanto, se propone una segunda solución que involucra un intermediario encargado de recibir y transmitir la información generada por los dispositivos IoT hacia la blockchain. Este intermediario será un proxy llamado Kangaroo que funcionará como un nodo ligero de la red. La conexión entre los dispositivos IoT y Kangaroo se realizará mediante un protocolo HTTP.

Kangaroo será responsable de recibir los mensajes de los diferentes dispositivos IoT y enviarlos a la blockchain. En la blockchain, un contrato maestro se encargará de recibir todas las transacciones provenientes de los dispositivos IoT y, posteriormente, enviarlas al contrato final para su persistencia.

No obstante, esta solución plantea ciertos problemas de seguridad. Por ejemplo, el proxy Kangaroo no podrá saber con certeza si el mensaje que recibe proviene realmente de un dispositivo IoT conectado a nuestro sistema o de algún intruso. Para prevenir esta situación, proponemos enviar un api-key junto con las transacciones, lo que permitiría aceptar únicamente peticiones que incluyan el api-key correcto. No obstante, cualquier persona que tenga acceso al api-key podría enviar transacciones sobre la red sin restricciones.

Además, durante el envío de la información a la blockchain, pueden presentarse problemas de seguridad, ya que Kangaroo u otro agente externo podrían modificar la información antes de que esta llegue a la blockchain.

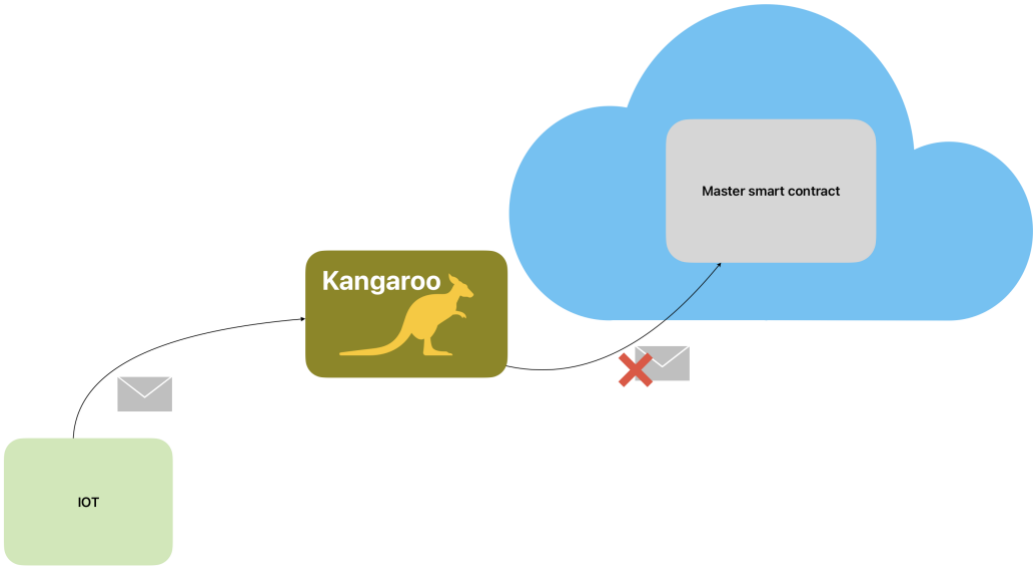


Ilustración 9 Segunda versión arquitectura

Tercera versión

La solución propuesta para manejar la seguridad tanto del cliente como del lado de la blockchain implica el uso de una tecnología llamada One Time Password (OTP). La OTP se basa en que tanto el dispositivo IoT como la red blockchain tienen almacenado un valor secreto que solo ellos conocen. Por medio de una secuencia o un timestamp y el valor secreto, estos pueden generar un nuevo código que se envía del lado del cliente al servidor para validar que la información sea enviada por el dispositivo IoT legítimo. Si el código OTP es correcto, la blockchain acepta la transacción y la almacena correctamente en la cadena de bloques. En caso contrario, la información es invalida y no se procesa.

Esta solución permite validar que el dispositivo IoT sea el único que envía información y si alguien en el medio escucha el token, únicamente podrá enviar mensajes por un corto periodo de tiempo si el OTP se basa en el tiempo o ninguna vez si el token se basa en una secuencia. Del lado de la blockchain, podemos validar y guardar transacciones realmente válidas.

Para implementar esta solución, se replantea la solución de blockchain en donde únicamente hay un contrato principal y se propone una solución con varios contratos. Esto hace referencia a un gemelo digital, en donde cada dispositivo IoT tiene asociado un contrato inteligente en la

blockchain encargado de mantener el secreto y validar las transacciones de su respectivo dispositivo IoT. Sin embargo, esta solución parece prometedora, pero tiene un problema muy grande, y es que la información persistida sobre la blockchain es pública, y aunque se genere como un valor privado, este puede ser leído al momento de generarse, haciendo que sea posible vulnerar fácilmente la seguridad del contrato.

Para resolver este problema, se puede considerar el uso de técnicas de cifrado y ofuscación de código para proteger la información almacenada en los contratos inteligentes. Además, se pueden implementar políticas de control de acceso para restringir el acceso a los contratos solo a los dispositivos IoT autorizados y validar que las transacciones sean enviadas ´únicamente por ellos. Estas medidas de seguridad adicionales pueden mejorar significativamente la seguridad del sistema y garantizar la integridad de la información almacenada en la blockchain.

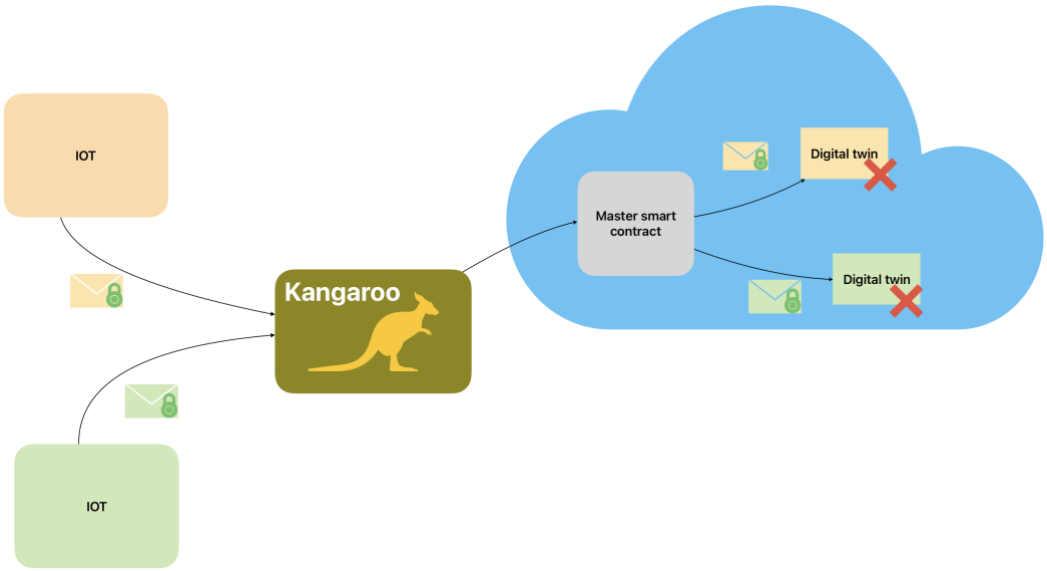


Ilustración 10 Tercera versión arquitectura

Cuarta versión

En el contexto de la tecnología blockchain, la seguridad y privacidad de la información son de gran importancia, ya que cualquier persona puede acceder a la red y consultar los datos almacenados. Por esta razón, se ha propuesto la solución de la encripción de clave pública para proteger la información de los secretos en la blockchain.

Esta solución implica que el dispositivo IoT firma los mensajes con su clave privada, lo que garantiza la autenticidad y la integridad de los datos enviados. Además, la red blockchain, a través del gemelo digital, valida la autenticidad de los mensajes utilizando la clave pública del dispositivo IoT.

Es importante mencionar que la generación de claves pública y privada se realiza en el momento de la creación del gemelo digital, lo que garantiza su seguridad y evita posibles vulnerabilidades. Anteriormente, se presentaba una limitante en la capacidad del dispositivo IoT para encriptar y enviar los mensajes debido a los escasos recursos que tiene, sin embargo, esta limitación ha sido superada en el proyecto.

La solución de encripción de clave pública es efectiva para solucionar el problema de la privacidad y la seguridad de la información en la blockchain. Además, esta solución evita que alguien dentro de la red conozca la clave privada y, por lo tanto, pueda validar los mensajes generados por el dispositivo IoT como auténticos. Incluso si un atacante logra obtener la clave pública, no puede generar un mensaje encriptado que pueda pasar la validación de seguridad de la red blockchain.

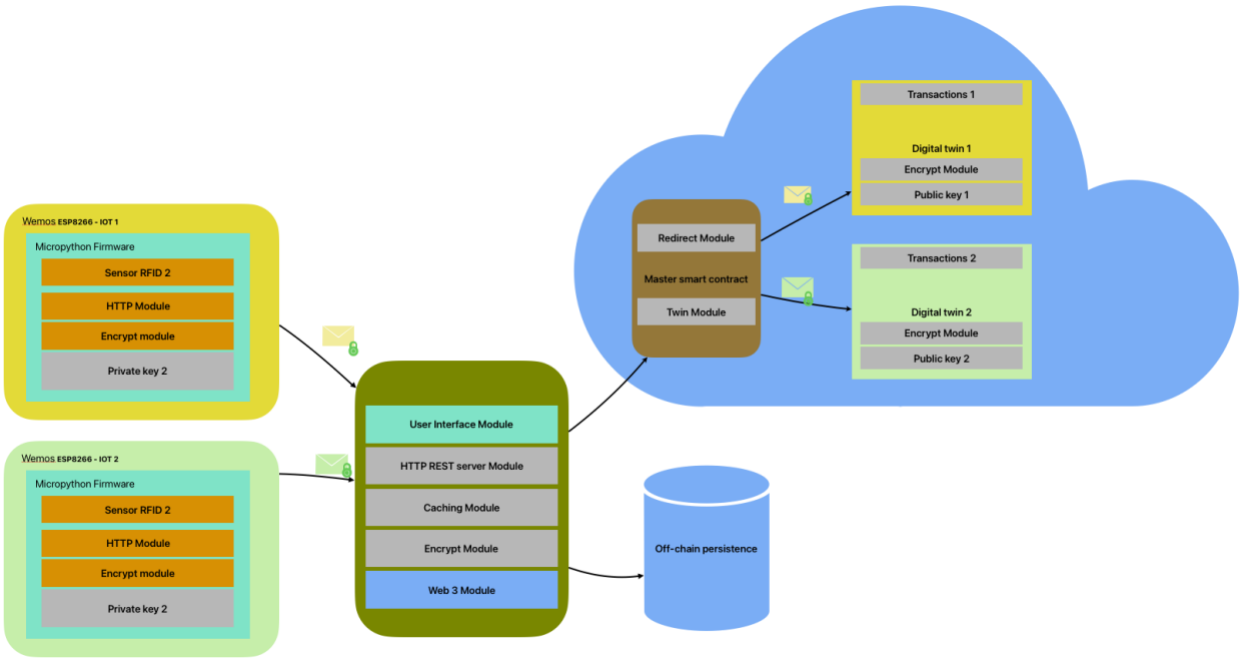


Ilustración 11 Cuarta versión arquitectura

Montaje

Dispositivo IoT

Cuando se trata de dispositivos IoT, es fundamental tener en cuenta los recursos de CPU y memoria disponibles para poder encriptar y firmar correctamente. En este caso, el proyecto se enfocó en un dispositivo Wemos Esp32. Para poder integrar los aspectos criptográficos y de comunicación necesarios con la blockchain, se utilizó un firmware personalizado basado en la implementación de MicroPython.

Para llevar a cabo este proyecto de investigación en el ámbito de la ingeniería de software, se ha utilizado un dispositivo IoT específico mencionado previamente. Este dispositivo ha sido equipado con un firmware modificado de *MicroPython* para permitir su interacción con una red blockchain. El Wemos ESP32 se caracteriza por su potente procesador Xtensa Dual-Core LX6 de 32 bits, que opera a frecuencias de 160 o 240 MHz. Cabe destacar que uno de los núcleos del procesador está especialmente diseñado para el procesamiento de protocolos inalámbricos como el WIFI, mientras que el otro núcleo se encarga de los demás procesos requeridos.

Además, el dispositivo cuenta con una memoria RAM de 520KB, que proporciona suficiente capacidad de almacenamiento para ejecutar las tareas necesarias. La unidad de procesamiento del Wemos ESP32 desempeña un papel crucial en el proyecto, ya que se encarga de cifrar todos los mensajes generados por el sistema y de enviarlos a la red blockchain correspondiente. Además, el dispositivo proporciona una serie de pines de conexión que permiten la configuración de otros elementos de IoT, como es el caso de un lector de etiquetas RFID, que desempeña un papel fundamental en este proyecto.

Este firmware incluye librerías personalizadas diseñadas específicamente para el manejo de la encriptación y la comunicación entre la red blockchain y Kangaroo, así como también la eliminación y limpieza de componentes no necesarios para hacer el firmware lo más ligero posible y evitar problemas de procesamiento y memoria durante la ejecución.

Es importante mencionar que, gracias a esta implementación personalizada, se puede asegurar que el dispositivo IoT pueda encriptar y firmar los datos de manera segura y eficiente, sin comprometer su rendimiento o capacidad de procesamiento. Además, esta solución permite que los dispositivos IoT puedan interactuar directamente con la blockchain y Kangaroo, lo que facilita el proceso de comunicación y verificación de datos de manera transparente y eficiente.

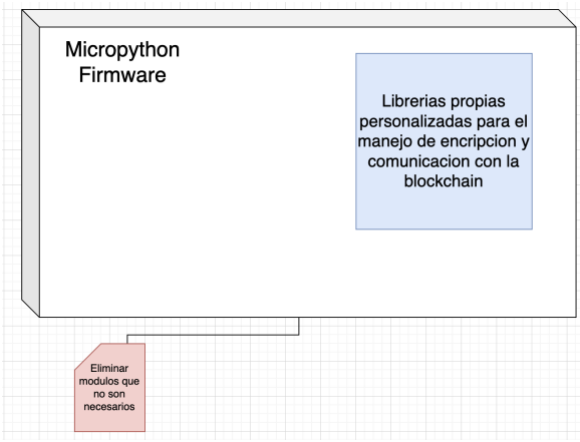


Ilustración 12 Firmware personalizado de MicroPython

Lector RFID

El lector de etiquetas RFID, también conocido como identificador de radiofrecuencia, es una tecnología ampliamente utilizada en el ámbito de la logística y el control de inventario. A diferencia de los códigos de barras convencionales, los cuales contienen información limitada, las etiquetas RFID ofrecen una mayor capacidad de almacenamiento y proporcionan medidas de seguridad adicionales para evitar la duplicación de registros. Estas etiquetas permiten almacenar una gran cantidad de información relacionada con los productos o elementos a los que están asociadas.

En el caso concreto de este proyecto, el lector de etiquetas RFID se conecta a la unidad de procesamiento del Wemos ESP32. El dispositivo IoT ejecuta un programa especialmente diseñado

que monitorea las entradas provenientes del lector RFID y captura la información contenida en las etiquetas. Una vez recopilada esta información, el Wemos ESP32 se encarga de transmitirla a la red blockchain correspondiente, donde se almacena de manera segura y se registra de forma inmutable.

Este enfoque permite que el sistema sea capaz de rastrear y auditar de manera eficiente el movimiento de los productos o elementos etiquetados a lo largo de la cadena de suministro.

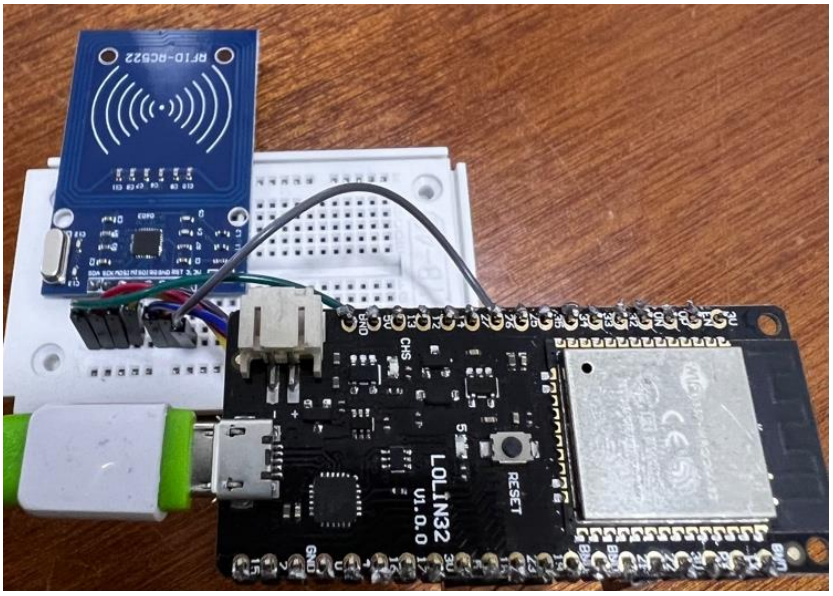


Ilustración 13 Dispositivo IoT

Flujos principales

Para garantizar la seguridad en la comunicación entre dispositivos IoT y la blockchain, es necesario implementar mecanismos que permitan validar la autenticidad de los dispositivos y la información que se va a almacenar en la cadena de bloques. Para lograr esto, se utilizan mecanismos criptográficos RSA, el cual como se mencionó previamente, utiliza una clave pública y una clave privada para firmar los datos y validar su autenticidad.

Aunque se ha utilizado RSA como ejemplo en este libro, es importante destacar que existen otros mecanismos criptográficos que pueden ser utilizados para garantizar la seguridad en la comunicación entre dispositivos IoT y la blockchain.

En los diagramas que se presentan a continuación, se describe el proceso de comunicación entre dispositivos IoT y la red de blockchain, detallando los tres flujos principales: la integración de un nuevo dispositivo IoT en la red de blockchain, el envío seguro de datos a la cadena de bloques y la visualización de los datos almacenados en la red de blockchain por parte de los usuarios.

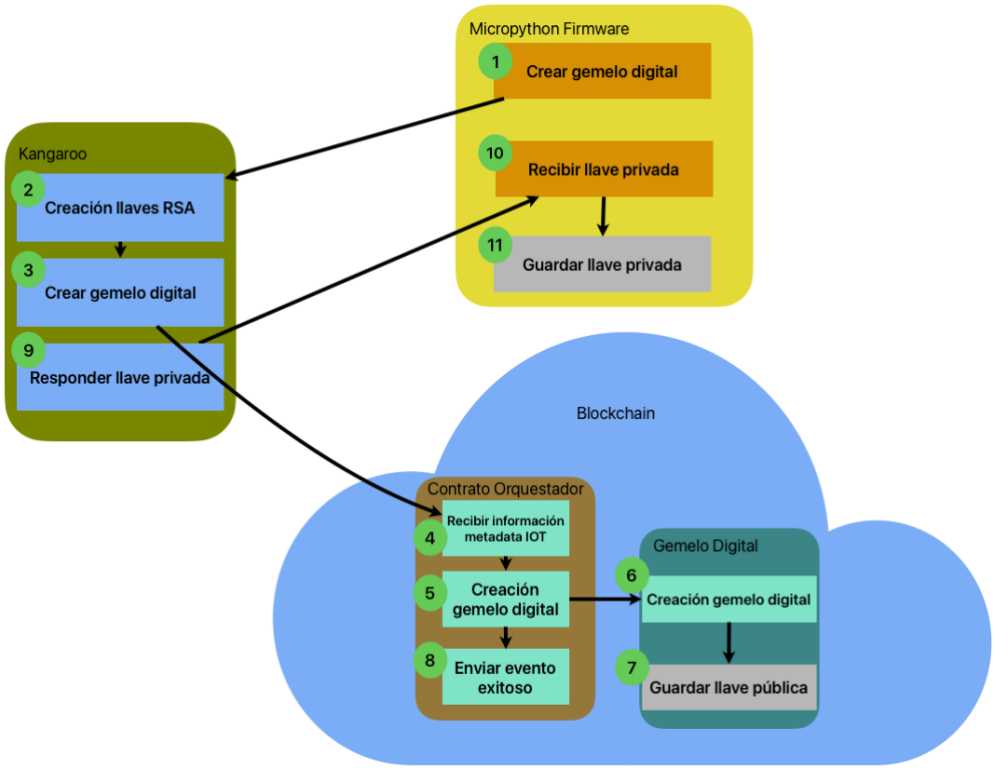


Ilustración 14 Flujo creación de dispositivo

El primer paso es el más importante, en donde se establece la comunicación de manera segura entre el dispositivo IoT y la red blockchain por medio de mecanismos de encriptación y la generación de contratos inteligentes sobre la red de *Ethereum.*

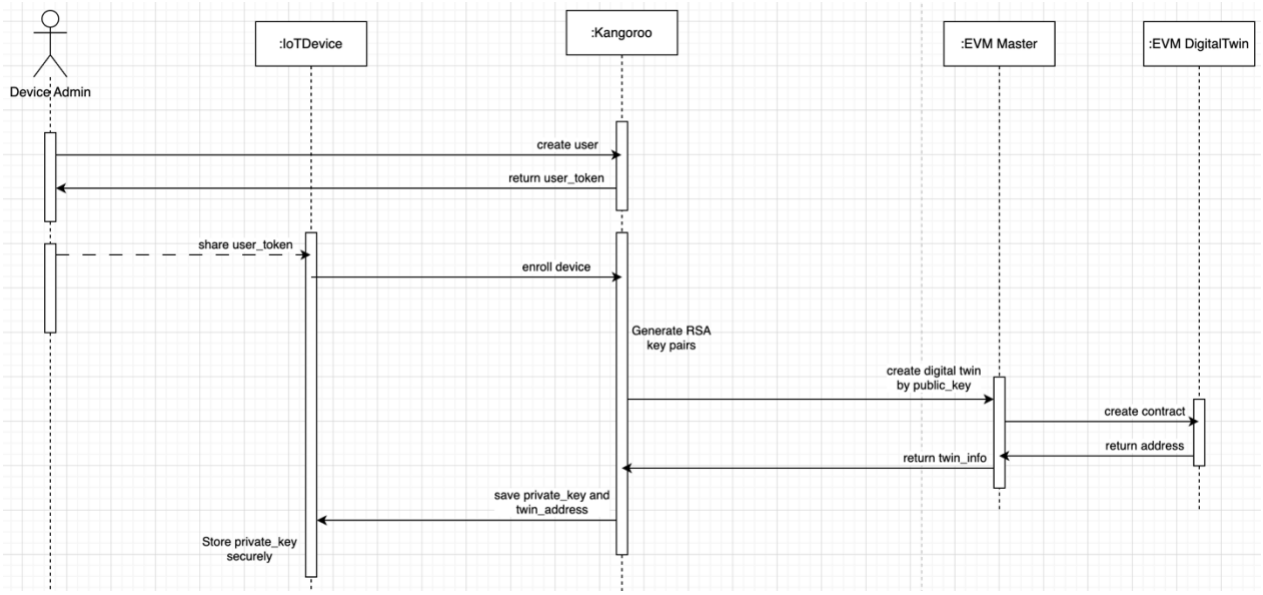


Ilustración 15 Diagrama secuencia creación de nuevo dispositivo

La Figura 15 ilustra el flujo de comunicación entre el dispositivo IoT y la blockchain para enviar transacciones con la información deseada. Para poder realizar esta comunicación de manera segura, es necesario asociar previamente el dispositivo a un usuario o empresa, lo cual se logra mediante una entidad intermediaria llamada Kangaroo. Esta entidad se encarga de mantener la información de los usuarios y los dispositivos que están asociados a ella.

Para comenzar el proceso, un usuario crea una cuenta en Kangaroo y genera un api-token que permite que el dispositivo IoT se conecte a la red de blockchain. En el caso de la logística, por ejemplo, los elementos que leen los códigos QR de los productos pueden utilizarse para leer la información asociada al usuario desde la aplicación móvil, y así conectarse a la red blockchain con el token previamente generado.

Una vez que el dispositivo IoT tiene la información necesaria para comunicarse con Kangaroo, envía la información asociada al dispositivo, como la dirección MAC. Kangaroo se encarga de generar las claves privadas y públicas necesarias para el dispositivo mediante el algoritmo RSA sha-256. Una vez que se generan las claves, Kangaroo envía una transacción a la red blockchain con la clave pública.

Dentro de la blockchain, existe un contrato maestro llamado EVM Master, que orquesta la comunicación entre Kangaroo y los gemelos digitales de los dispositivos IoT. Cuando el contrato maestro recibe la solicitud de Kangaroo, genera un nuevo contrato asociado a la clave pública del dispositivo IoT, llamado gemelo digital.

Kangaroo luego regresa la información de la clave privada al dispositivo IoT para que éste la persista de manera segura en una memoria persistente y pueda firmar las transacciones futuras con la clave privada previamente generada. Luego se genera un evento dentro de la red de blockchain, que Kangaroo escucha para asociar el id del nuevo gemelo digital con el dispositivo correspondiente. Esta información se almacena en Kangaroo, fuera de la red de blockchain.

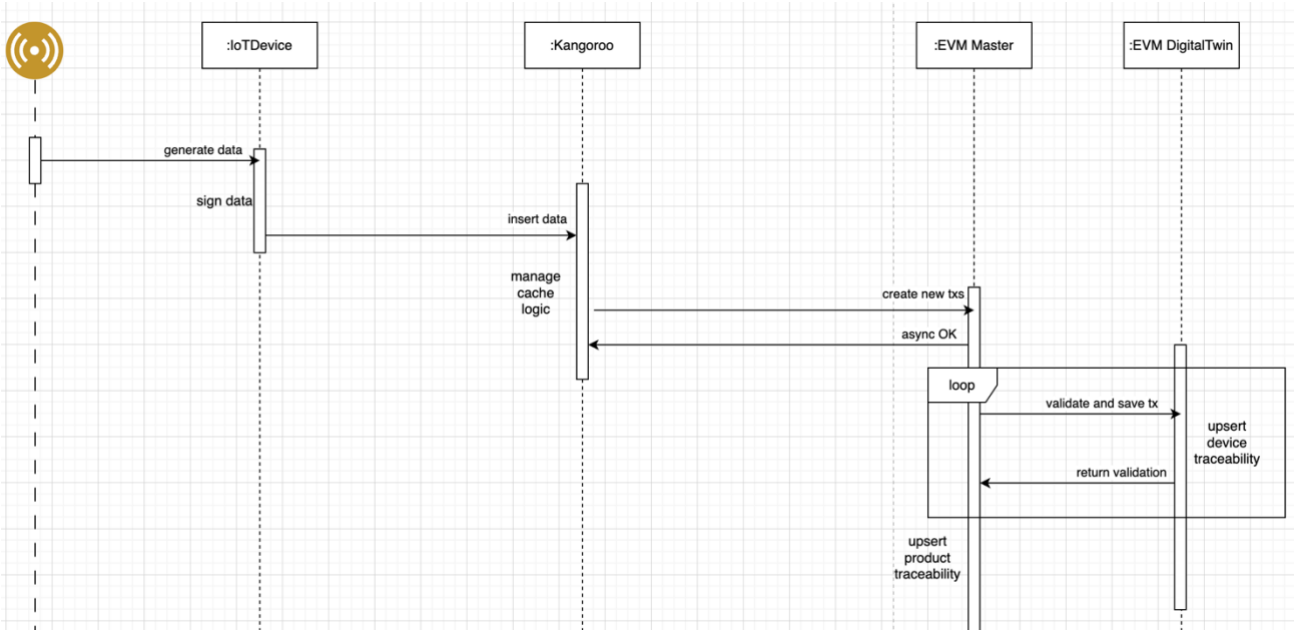


Ilustración 16 Diagrama secuencia envió de transacción

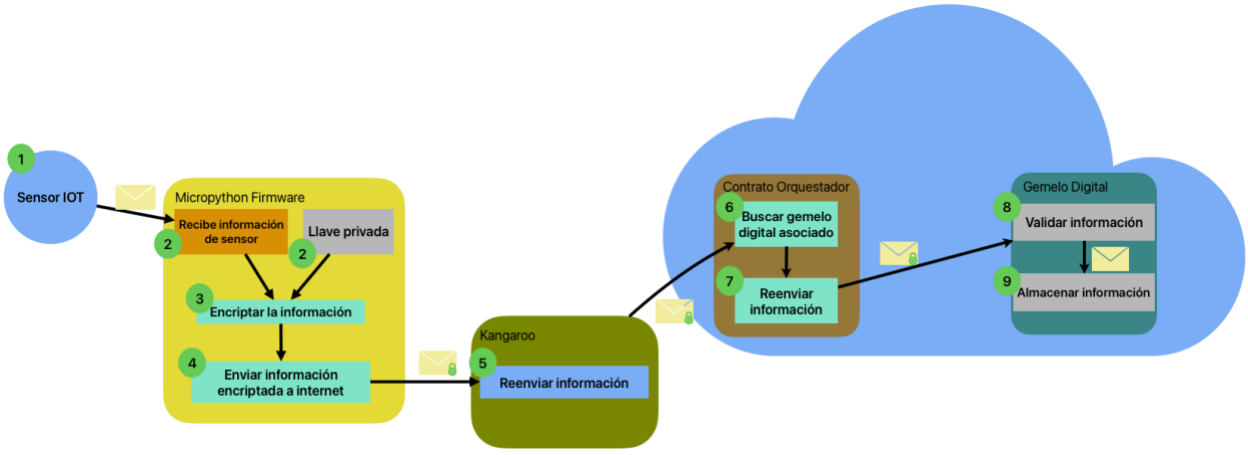
La comunicación de transacciones entre dispositivos IoT y la red blockchain es un paso fundamental para asegurar la integridad y autenticidad de los datos generados. Una vez que el dispositivo IoT ha completado el primer paso, que implica la asociación de un dispositivo a un usuario o empresa y la generación de una clave privada para el dispositivo, y que en la red blockchain existe un gemelo digital con la clave pública, el siguiente paso es la comunicación de las transacciones.

El dispositivo IoT recibirá información de los sensores correspondientes, como el sensor de temperatura o la lectura de un código QR, y firmará los eventos con su clave privada asociada. Posteriormente, enviará los eventos a un intermediario Kangaroo, que enviará la información de varios de los eventos generados a la blockchain. Kangaroo tendrá una capa de cache para ignorar eventos duplicados y enviará cada cierto tiempo al contrato maestro dentro de la blockchain la información necesaria.

El contrato maestro enviará la información al gemelo digital correspondiente, que se encargará de verificar la autenticidad de la información utilizando la clave pública asociada. El gemelo digital también se encargará de persistir la información y enviar los eventos necesarios para confirmar el procesamiento correcto de la transacción.

Es importante destacar que este proceso de comunicación de transacciones debe realizarse de manera segura y confiable para garantizar que la información persistida en la blockchain sea verídica y que el dispositivo IoT asociado sea una fuente confiable. Para esto, se utilizan mecanismos criptográficos como RSA sha-256, que se encargan de generar las claves tanto privadas como públicas y firmar los textos generados para validar su veracidad.

En resumen, la comunicación de transacciones entre dispositivos IoT y la red blockchain es un proceso crítico que asegura la integridad y autenticidad de los datos generados por los dispositivos IoT. Es fundamental contar con mecanismos de seguridad y criptográficos para garantizar la confiabilidad de la información persistida en la blockchain y que el dispositivo IoT asociado sea una fuente confiable.



lustración 17 Flujo envió de transacción

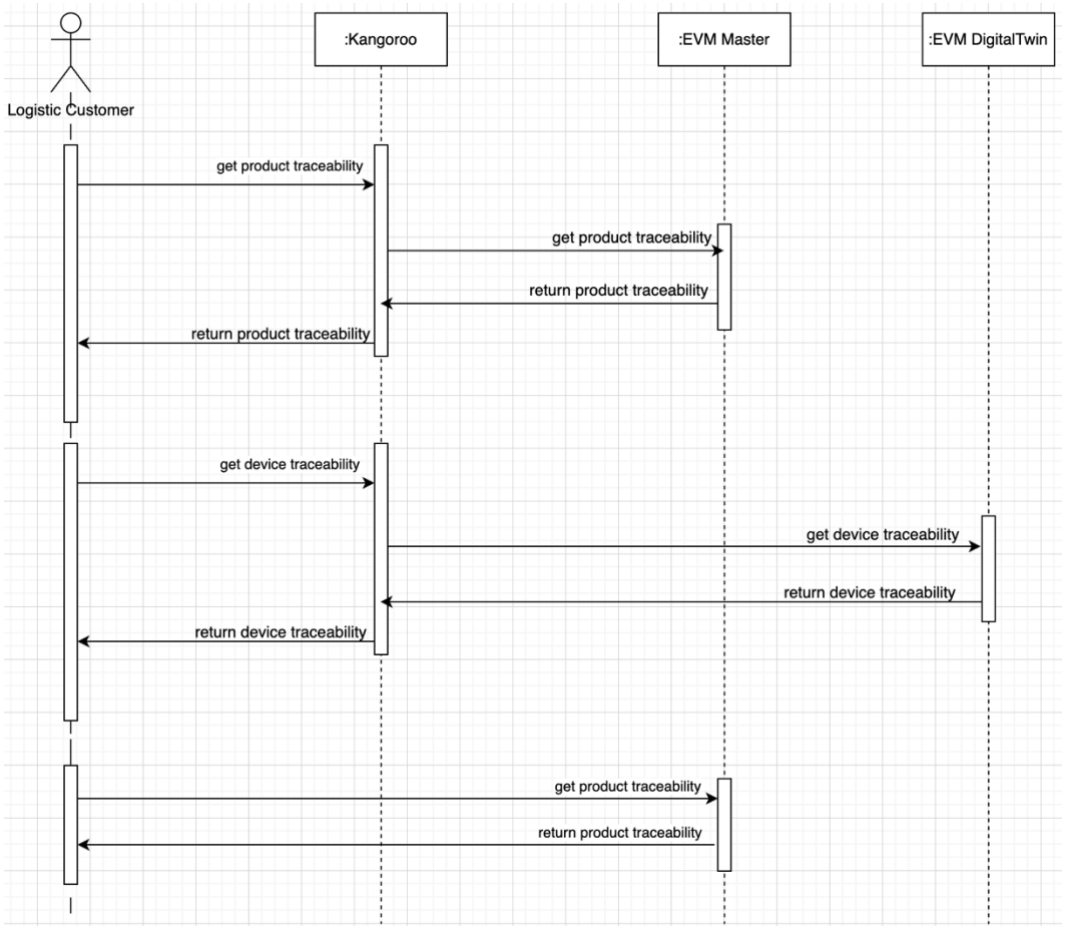


Ilustración 18 Flujo consulta de trazabilidad

Para garantizar la transparencia y la libre verificación de los datos, se ha diseñado un esquema que permite la lectura pública de la información almacenada en los contratos asociados a los sistemas de gemelos digitales. Esto significa que cualquier persona interesada puede acceder a los datos de los productos y ver la información almacenada en la blockchain.

En el sistema generado en el proyecto, tanto el cliente como cualquier otra persona pueden ver los datos directamente en la blockchain a través del contrato maestro o de cualquiera de los gemelos digitales que se encuentren en la red. Además, también pueden acceder a los datos a través de Kangaroo, nuestra entidad intermedia.

Una vez se accede a los datos, se puede ver todo lo que se ha registrado para un producto en particular. Podemos ver por cuáles gemelos digitales o dispositivos IoT ha pasado el producto y qué datos han registrado en cada caso. Además, también podemos ver el historial de cada

dispositivo o gemelo digital, incluyendo qué transacciones han generado y a qué productos se han asociado con qué valores.
Este esquema de lectura pública garantiza la transparencia y la confiabilidad de la información almacenada en la blockchain, lo que puede ser de gran utilidad para los clientes y otros actores interesados en el seguimiento de los productos a lo largo de la cadena de suministro.

Finalmente, para que no quede duda alguna con respecto a los flujos y a el *journey* del usuario, se desarrolla un diagrama de *Customer Journey Map* que da una explicación detallada de los flujos que se siguen.

https://miro.com/app/board/uXjVNG0wG08=/

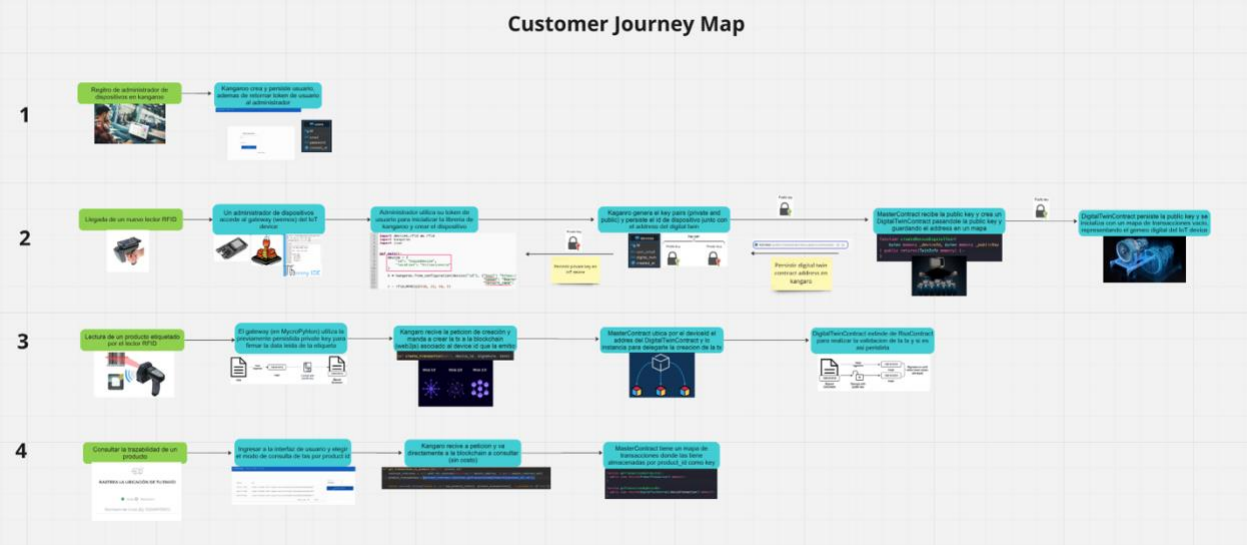


Ilustración 19 Customer Journey Map

Pruebas

El caso de prueba será un flujo completo, desde la creación del dispositivo, hasta el seguimiento de transacciones registradas por este sobre la *Blockchain*.

Se tendrán entonces 3 *Smart Contracts* construidos en *Solidity* y desplegados con ayuda de una herramienta llamada *truffle* sobre una blockchain local muy conocida llamada *ganache.* Posterior a tener los 3 contratos desplegados, se toma la información de *abi array* y el *address* (información necesaria para instanciar el contrato y poder llamar sus servicios) donde quedo desplegado el

MasterContract, el cual es el contrato encargado de recibir todas las “peticiones” emitidas por la interfaz intermedia que construimos sobre *Python* llamada *Kangaroo*. De esta manera una vez el dispositivo emita algún tipo de acción, ya sea registro de sí mismo o registro de una transacción el flujo completo a seguir será *MicroPython-Kangaroo-MasterContract*.

Teniendo los contratos ya finalizados, se les realizan también pruebas unitarias, que pretenden probar el correcto funcionamiento de un módulo o trozo de código en específico. Estos se realizan con ayuda de *JavaScript*, librerías de web3 e incluso de *truffle* que facilitan su emulación de una interacción en una red *Blockchain*.

lustración 20 Pruebas unitarias contratos con JS

Por estándar se construye de la misma manera que las migraciones, un archivo de pruebas por cada *Smart Contract* y en cada archivo se suelen realizar diferentes pruebas que usualmente son directamente proporcional a la cantidad de funciones que tenga el Smart Contract, o las variaciones que puede tomar la función. Luego de tener todo listo se ejecuta el comando de truffle para probar, en este caso sobre la red *ganache.*

Lustración 21 Ejecución comando truffle

Ya seguros, se despliegan los *Smart Contract* en la red local.

```
(base) jhordysalinas@192.168.1.10 /Users/jhordysalinas/Documents/iot-blockchain/blockchain [master]
% truffle migrate --network ganache

Compiling your contracts...
===========================
> Compiling ./contracts/DigitalTwinContract.sol
> Compiling ./contracts/MasterContract.sol
> Compiling ./contracts/RsaContract.sol
> Artifacts written to /Users/jhordysalinas/Documents/iot-blockchain/blockchain/build/contracts
> Compiled successfully using:
   - solc: 0.8.17+commit.8df45f5f.Emscripten.clang


Starting migrations...
======================
> Network name:    'ganache'
> Network id:      1690646740177
> Block gas limit: 30000000 (0x1c9c380)
```

Lustración 22 Despliegue contratos en red ganache

Lo siguiente es *setear* el *abi array* y el *address* del *MasterContract* en las variables de entorno de Kangaroo y también proceder a desplegar Kangaroo.

Para el ABI:

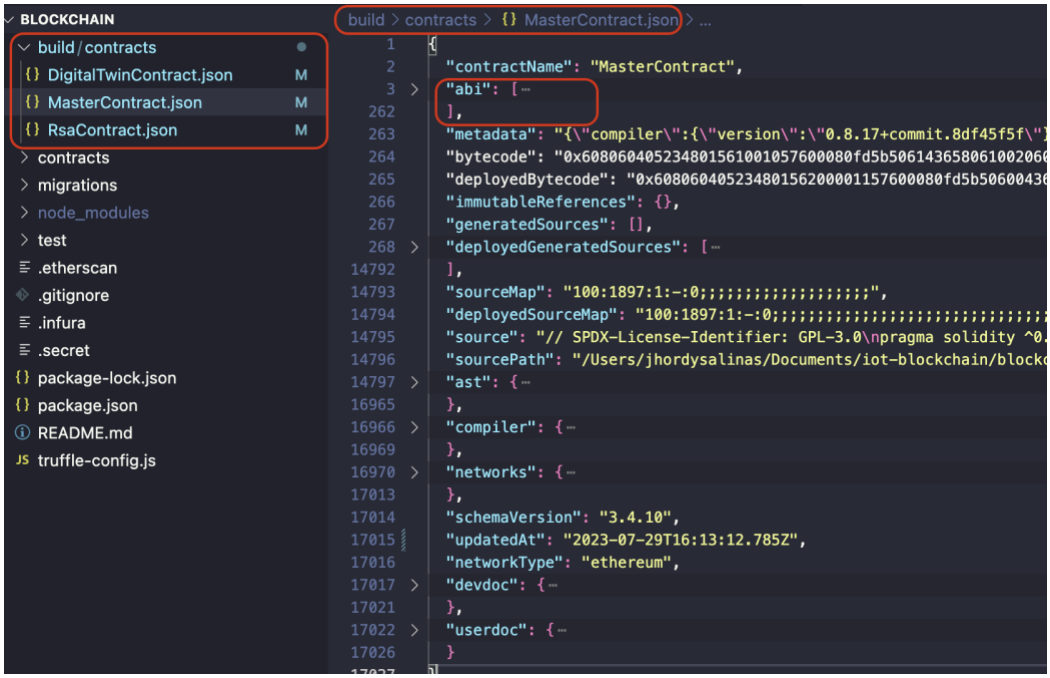


ILustración 23 ABI del contrato maestro

Para el address:

```
03-master-deployment.js
=======================
ganache [
  '0x234070bB2a50DD3E4B0DF63c8e03B16E735e8508',
  '0xF7C4921425AcD6ccccddd47027787Ff9014324A41',
  '0x19C2e1adE81b142C20aFd129EdF3AdaF0bf217ee',
  '0xfbc4fccaC81C642D33F4F7D1EE596112eD6BeaF8',
  '0x5598fE1418DB0dbE9170B1AecA2E688C43c4B7eC',
  '0x19B247B907217355b98F8c2c692780c0d51Bf0F3',
  '0x67c57fA000e4a1b24E59E3FAFD6EdDbEcaCF712A',
  '0x82a26E60408B88857185c5a1b40c00051Ab71b67',
  '0x055839695a08De6116D352D4071A458382ece057',
  '0x7650aB53446Aa2D42e17750a12126De45a8d4228'
]

   Deploying 'MasterContract'
   --------------------------
   > transaction hash:    0x93c37aeea61a0ec7c4d5cc389f70ba0677470267ee78225bca89904ffeed4660
   > Blocks: 0            Seconds: 0
   > contract address:    0x68446F7de3be120772f87463B1861B04a0A3d976
   > block number:        9
   > block timestamp:     1690647192
   > account:             0x234070bB2a50DD3E4B0DF63c8e03B16E735e8508
   > balance:             999.931554145162746249
   > gas used:            3763452 (0x396cfc)
   > gas price:           2.858103896 gwei
   > value sent:          0 ETH
   > total cost:          0.010756336823608992 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.010756336823608992 ETH
```

ILustración 24 Dirección asignada al contrato maestro

Para el address se modifica una variable de entorno llamada “MASTER_CONTACT_ADDRESS”

Y para el abi.json, hay que reemplazar el contenido del file en el archivo del *base path*

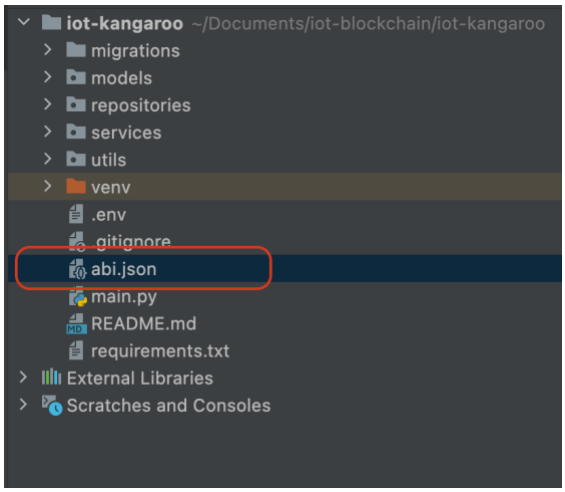


ILustración 25 Archivo abi.json

Una vez ya tengamos la lógica del servidor de la arquitectura se procede a levantar el módulo de *MicroPython* en que ya incluimos la librería de conexión con *Kangaroo* de forma nativa.

Se crea el dispositivo dentro del sistema (lo cual representa el despliegue de un contrato de tipo *DigitalTwinContract.* Además, al dispositivo se le puede embeber la información que se desee (json)

```
port devices.rfid as rfid
port kangaroo
port json


f main():
  device = {
      "id": "Esp32Device",
      "location": "Villavicencio"
  }
```

ILustración 26 Ejemplo información a enviar a blockchain

Posteriormente realizamos la lectura de una tarjeta RFID, el sensor una vez lea emitirá a Kangaroo y este a la red de blockchain .

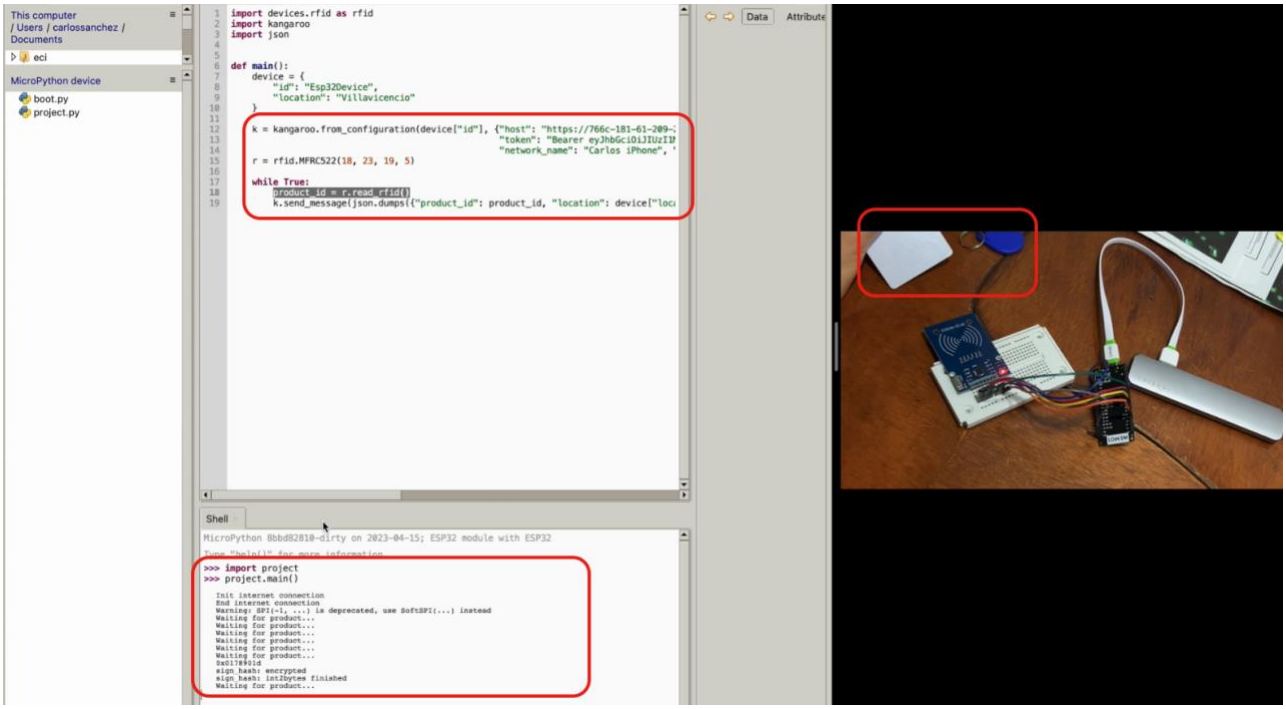


ILustración 27 Demostración de Wemos usando firmware de Micropython para conexión a blockchain

Finalmente revisamos la interfaz gráfica que es una aplicación web desarrollada en *React*, para poder listar transacciones y gestionar los dispositivos que tenga el usuario *logueado*.

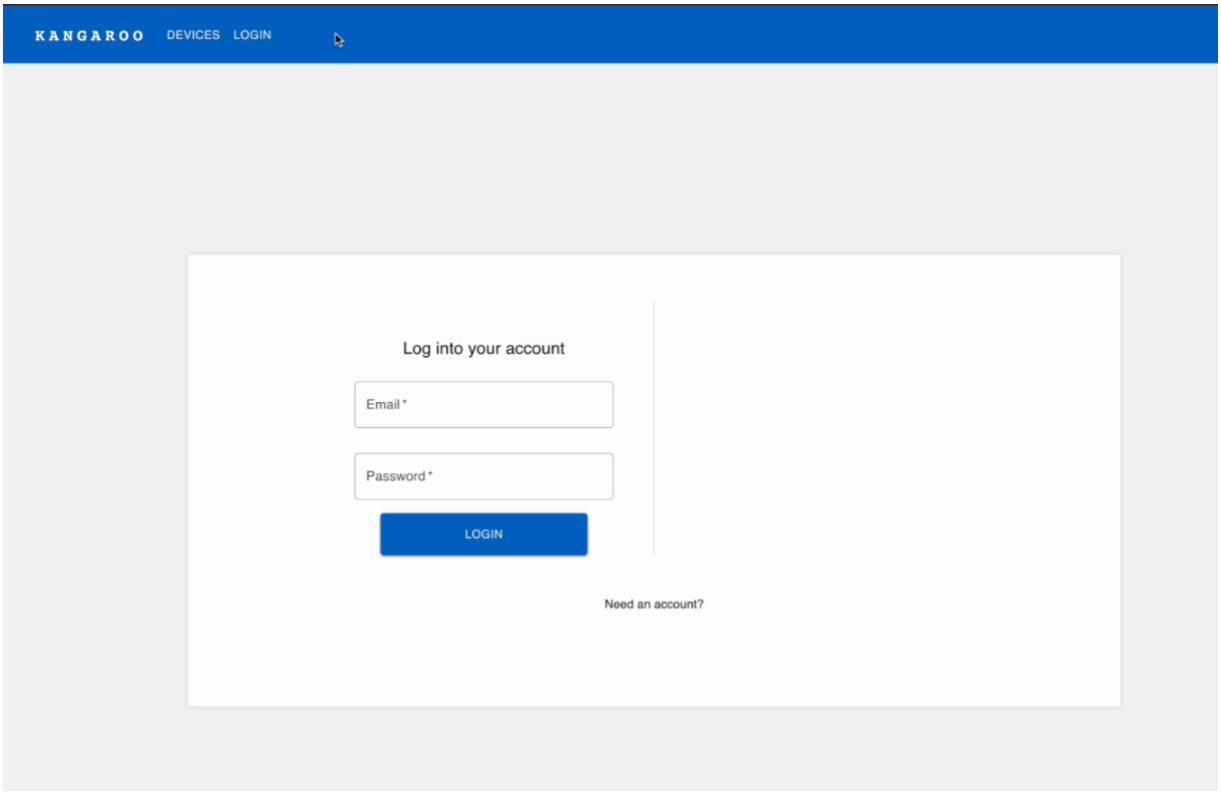


ILustración 28 Interfaz gráfica: Login

La primera vista que encontramos es la de dispositivos creados

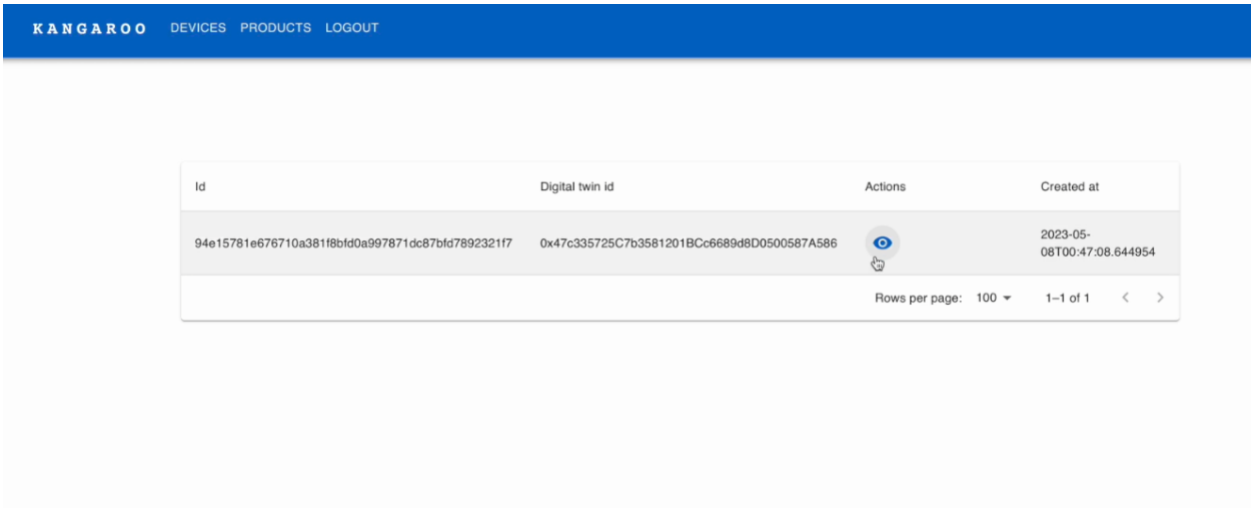


ILustración 29 Interfaz gráfica: Consulta dispositivos

Por cada dispositivo se puede consultar la trazabilidad que ha hecho es decir los productos que han pasado por allí, ejemplo acá han pasado 2 productos por este dispositivo de logística y la ubicación es en la ciudad de Villavicencio

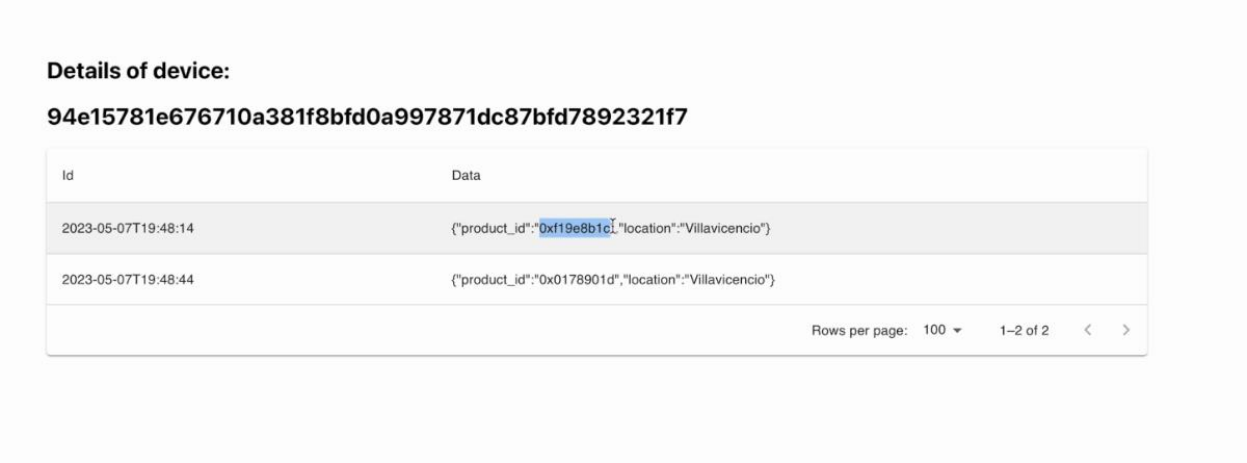


ILustración 30 Interfaz gráfica: Detalle de dispositivo

Luego copiamos el identificador del producto si deseamos ver todos los dispositivos por los que además este ha pasado, para ello está la pestaña de “products”, realizar consultas por ID, allí se detalla que paso por otros 3 *devices* en la misma ciudad, vale aclarar que si quisiéramos embeber el detalle del *device* se podría, acá únicamente se usó la ubicación para efectos de prueba.

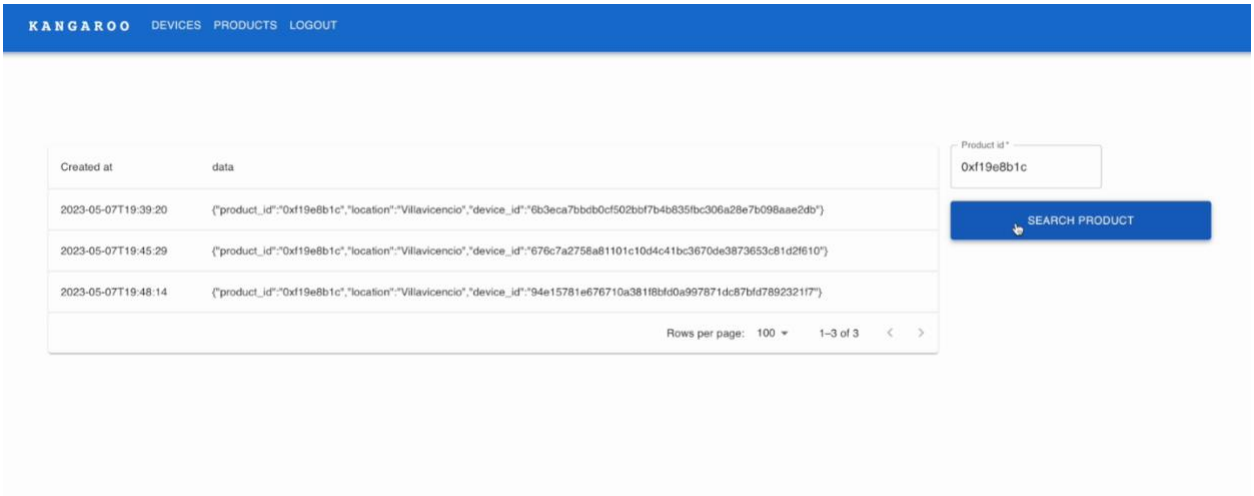


ILustración 31 Interfaz gráfica: Detalle de producto

Capítulo 7

Entregables

Producto	Descripción
La implementación de una librería en MicroPython para lograr la conexión con la blockchain de Ethereum.	Documentación y código fuente de un marco de trabajo que permita a dispositivos IoT lograr establecer una comunicación segura entre ésta y la blockchain de Ethereum.
Contratos desplegados sobre Ethereum que se encarguen de coordinar la lógica de los procesos de logística.	Documentación y código fuente de los archivos con los contratos desarrollados en Solidity y las direcciones (sobre alguna testnet de Ethereum) asignadas con que fueron desplegados y realizada la PoC.
Una interfaz que permita la conexión entre dispositivos IoT y la blockchain de Ethereum.	Documentación y código fuente de la API.
Una interfaz gráfica para la gestión de dispositivos y transacciones.	Una interfaz gráfica que permita tener control sobre los dispositivos registrados y sus transacciones correspondientes.

Una prueba de concepto que utilice los anteriores entregables.	Una prueba de concepto que demuestre la usabilidad y aplicabilidad de los 4 entregables anteriormente mencionados en la gestión de procesos de logística.
Un artículo en relación con la unión de estas dos tecnologías.	Un artículo que contiene el resultado del proyecto muestra los avances de la conexión entre IoT y blockchain junto con la nueva propuesta planteada y desarrollada en el proyecto.
Un libro de proyecto.	Un libro que contenga todo lo investigado y el paso a paso detallado (documentación) de las versiones por la cuales fue evolucionando el proyecto desde el inicio de éste.

Capítulo 8

Trabajo futuro

En la actualidad, uno de los desafíos más significativos en la red de *Ethereum* es la restricción en la cantidad de transacciones que puede procesar por segundo. Esta limitación se convierte en un problema considerable cuando se trata de dispositivos IoT, ya que generan grandes volúmenes de información. La solución actual propuesta ha sido implementar una capa intermedia en nuestro servidor Kangaroo, que retiene las transacciones durante un período de tiempo para luego generar una única transacción en la blockchain. Sin embargo, esta solución no debe considerarse definitiva si se desea lograr que la red de *Ethereum* sea escalable para aplicaciones descentralizadas de Internet (Daaps, por sus siglas en inglés).

En el ámbito de blockchain, se ha trazado un roadmap con los próximos pasos que la tecnología debe seguir para que la red pueda procesar miles de transacciones por segundo mediante la implementación del particionamiento dentro de la blockchain. Este enfoque permitiría que solo un conjunto selecto de nodos sea responsable de validar cierto grupo de transacciones, en lugar de requerir que todos los nodos validen todas las transacciones. Esta técnica de particionamiento es fundamental para mejorar la escalabilidad de la red y permitir que los dispositivos IoT puedan interactuar de manera eficiente con la blockchain.

Además de los desafíos relacionados con la escalabilidad de la red, otro aspecto importante a considerar en el futuro es la capacidad limitada de los procesadores actuales utilizados en dispositivos IoT. Al implementar los algoritmos de inscripción necesarios para el desarrollo de este proyecto, estos procesadores alcanzan sus límites en términos de recursos disponibles y, en algunas ocasiones, pueden experimentar problemas de memoria. Estas limitaciones pueden afectar

el proceso de encripción y envío de información desde el dispositivo IoT hacia la red blockchain, lo que puede resultar en problemas de rendimiento y eficiencia.

Asimismo, si un dispositivo IoT es accesible físicamente, su capacidad de procesamiento limitada puede representar un riesgo para la seguridad. Los archivos de configuración que contienen información privada no poseen una gran capacidad de encripción debido a las limitaciones de los procesadores. Esto hace que los archivos sean más susceptibles a vulnerabilidades y ataques por parte de terceros malintencionados. Para garantizar el intercambio de llaves privadas, en el momento de la creación del gemelo digital en la red blockchain, se pueden agregar mecanismos adicionales de seguridad para evitar la intercepción de los mensajes y generar problemas de autenticidad. Uno de estos mecanismos, el cual fue trabajado en una de las versiones por las que se pasó en el desarrollo (versión 2), puede ser un sistema de OTP que sea incremental, lo cual ayude a evitar posibles problemas de clonación de llaves privadas.

Capítulo 9

Conclusiones

- En el contexto actual, las redes *Blockchain* y los dispositivos IoT han experimentado un crecimiento significativo y su combinación ofrece un amplio abanico de ventajas tecnológicas en diversos sectores económicos. Este proyecto se enfoca en la aplicación de estas tecnologías en el sector de la logística, sin embargo, también es relevante explorar su potencial en otros sectores como en el sector de la salud. La adopción de redes blockchain en el sector de la salud puede tener un impacto transformador. Esta tecnología se caracteriza por su capacidad para crear registros inmutables y transparentes, lo que resulta especialmente relevante en un ámbito tan sensible como el de la salud. La integridad de los datos y la confianza en las transacciones se vuelven fundamentales en un entorno donde la seguridad y la privacidad son prioritarias.

- La incorporación de tecnologías *Blockchain*, como *Ethereum*, en la gestión de datos de dispositivos *IoT* ofrece ventajas cruciales para un mejor funcionamiento de estos sistemas. La descentralización elimina la dependencia de una autoridad central y aumenta la resistencia y seguridad del sistema. La transparencia y la inmutabilidad aseguran un seguimiento preciso de las operaciones y evitan la manipulación maliciosa o accidental de los datos. La confiabilidad, respaldada por algoritmos criptográficos y validación de la red, aumenta la precisión y la confianza en la información almacenada. En resumen, esta integración potencia la eficiencia y la seguridad, brindando nuevas oportunidades para aplicaciones y servicios seguros en el contexto del *IoT*.

- La aplicación precisa de conceptos de desarrollo de software, como las metodologías ágiles, en proyectos con niveles altos de investigación, proporciona la ventaja de una iteración ágil para abordar de manera efectiva los cambios necesarios durante el desarrollo. Aunque el enfoque principal se mantiene en el logro del objetivo previamente establecido, la adopción de metodologías ágiles permite resolver rápidamente los obstáculos encontrados durante la ejecución del proyecto. Esta flexibilidad en el proceso de desarrollo ha demostrado ser una

estrategia eficaz para alcanzar resultados sólidos y adaptarse con agilidad a las demandas cambiantes del entorno tecnológico y de negocio.

- La red *Ethereum* ocupa un lugar destacado entre las redes que conforman la denominada web 3.0, una evolución significativa de internet que promueve la descentralización, la interoperabilidad y la seguridad de los datos. *Ethereum* se ha posicionado como una plataforma líder para el desarrollo de aplicaciones descentralizadas (*Dapps*) y contratos inteligentes, gracias a su capacidad para ejecutar código de manera autónoma y transparente en una red distribuida de nodos. Sin embargo, a medida que la adopción de *Ethereum* y las aplicaciones descentralizadas continúa creciendo, también surgen desafíos y limitaciones técnicas. En particular, la escalabilidad se ha convertido en una preocupación importante para la red *Ethereum*. Para superar estos obstáculos y lograr su visión de convertirse en una red capaz de procesar miles de millones de datos y facilitar transacciones masivas de dispositivos IoT en la blockchain, *Ethereum* está trabajando en una serie de desarrollos y mejoras técnicas, que serán alcanzadas de la misma manera que lo logran diferentes tecnologías, que es con el respaldo de una comunidad abierta, interesada por mantener y evolucionar el producto, por eso mismo es importante desarrollar soluciones en torno a la tecnología, para que dicha comunidad evidencia que está teniendo mayor acogida y que cualquier mejora puede ser un cambio significativo en la aplicabilidad individual que se le dé en los proyectos que se implemente *Ethereum*.

- El manejo de datos en dispositivos IoT presenta desafíos significativos en términos de interoperabilidad, calidad, seguridad y eficiencia. La ausencia de una normativa común dificulta la integración y colaboración entre dispositivos y sistemas de distintos fabricantes, lo que puede resultar en una fragmentación de la red y datos inconsistentes. Además, esta falta de uniformidad crea vulnerabilidades de seguridad al dejar “lagunas” en las defensas y dificultar la implementación de prácticas de seguridad sólidas. Asimismo, la gestión de actualizaciones y parches se ve obstaculizada al no contar con lineamientos estandarizados. En términos de eficiencia, la falta de protocolos puede generar demoras y sobrecargas en la comunicación, afectando el rendimiento y escalabilidad del sistema. Para superar estos desafíos, es fundamental establecer normativas comunes, mejores prácticas y fomentar la colaboración entre industrias y organismos reguladores para priorizar la seguridad y eficacia de los dispositivos *IoT* en un futuro

conectado y seguro, por ello la integración con *Blockchain* es una propuesta de estandarización para el manejo seguro de datos.

- La restricción en la capacidad de procesamiento de transacciones en la red de *Ethereum* representa un desafío importante para la integración de dispositivos IoT. Para superar esta limitación, es crucial seguir el roadmap establecido por la tecnología blockchain, que incluye el particionamiento de la blockchain para permitir una mayor escalabilidad. Además, se deben tener en cuenta las limitaciones de los procesadores utilizados en los dispositivos IoT, así como los posibles riesgos de seguridad asociados con la capacidad limitada de encripción de la información privada en estos dispositivos. Estos desafíos deben abordarse de manera efectiva para garantizar el rendimiento, la eficiencia y la seguridad en la interacción entre dispositivos IoT y la red blockchain. Por otro lado, si se desea poner en marcha la arquitectura actual, se podría optar por la alternativa de desplegar una red privada (propia) donde no exista el concepto de gas o que no represente el mismo costo que en Ethereum, siendo asi podría implementarse y además el procesamiento de las transacciones al ser proporcional a la cantidad de transacciones, serian más rápidas y enfocadas en el ámbito que se desee implementar.

Capítulo 10

Bibliografía

[1] fortunebusinessinsights, «Internet of Things (IoT) Market Size, Share & COVID-19 impact analysis by component(platform, solution & services) by end-use industry and regional forecast 2022-2029,» *fortunebusinessinsights*, 2022.

[2] 3. b. b. 2. The global Internet of Things (IoT) market is projected to grow from $662.21 billion in 2023 to $3, «fortunebusinessinsights,» 1 4 2023. [En línea]. Available: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307. [Último acceso: 25 06 2023].

[3] K. Kumar, P. Borasi y V. Kumar, «smart cities market by component (hardware, sftware, and service) and funcional area (smart infraestructure, smart covernance and smart education, smart energy, smart mobility, smart, health care, smart buildings, and others): global opportunity analysis,» 2022.

[4] fortunebusinessinsights, «The global blockchain market is projected to grow from $7.18 billion in 2022 to $163.83 billion by 2029, at a CAGR of 56.3% in forecast period, 2022-2029... Read More at:- https://www.fortunebusinessinsights.com/industry-reports/blockchain-market-100072,» 2021.

[5] A. R. S. y. P. Muthuswamy, «Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics,» 2022.

[6] S. Ferraro, A. Cantini, L. Leoni y F. D. Carlo, «Sustainable Logistics 4.0: A Study on Selecting the Best Technology for Internal Material Handling,» 2023.

[7] V. Mannayee y T. Ramanathan, «An Efficient SDFRM Security System for Blockchain Based Internet of Things,» 2022.

[8] V. J. C. Choez, «Análisis comparativo de un sistema de auditoría tradicional y un sistema de auditoría Blockchain e IPFS,» *UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO*, pp. 11-14, 2020.

[9] MinTIC, «Guía de Referencia para la adopción e implementación de proyectos con tecnología blockchain para el Estado colombiano,» 2022.

[10] A. Jain, S. Arora1, Y. Shukla1, P. T. B. Patil y P. S. Sawant-Patil, «Proof of Stake with Casper the Friendly Finality Gadget Protocol for Fair Validation Consensus in Ethereum».

[11] A. Peslak y M. Conforti, «COMPUTER PROGRAMMING LANGUAGES IN 2020: WHAT WE USE, WHO USES THEM, AND HOW DO THEY IMPACT JOB SATISFACTION,» 2020.

[12] C. Bell, «MicroPython for the Internet of Things,» 2017.

[13] M. Şimşek, «A Study of Blockchain In IOT Architecture,» 2021.

[14] M. A. ,. T. C. ,. S. D. ,. A. D. ,. G. F. ,. F. R. ,. B. T. ,. L. V. ,. F. Z. Olivier Alphand†, «IoTChain: A Blockchain Security Architecture for the Internet of Things,» 2018.

[15] T. K. Agrawal, J. Angelis, W. A. Khilji, R. Kalaiarasan y M. Wiktorsson, «Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration,» 2022.

[16] J. Jo, S. Yi y E.-k. Lee, «Including the reefer chain into genuine beef cold chain architecture based on blockchain technology,» 2022.

[17] C. Smith, «Ethereum.org,» Ethereum, 09 02 2023. [En línea]. Available: https://ethereum.org/en/developers/docs/accounts/. [Último acceso: 04 05 2023].

[18] V. M. Palacios, «Explorando la Blockchain de Ethereum y el desarrollo de smart contracts,» *UPC Escuela de Ingeniería de Telecomunicación y Aeroespacial de Castelldefels*, pp. 27-29, 2018.

[19] M. R. Naresh Adhikari, «IoT and Blockchain Integration: Applications, Opportunities, and Challenges,» 2023.

[20] P. R. M. A. T. A. Abhishek Hazra, «Fog computing for next-generation Internet of Things: Fundamental, state-of-the-art and research challenges,» 2023.

[21] E. C. Ribeiro, «Micro-containerization in Microcontrollers for the IoT,» 2022.

[22] N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, S. M. N. Islam, J. He y M. Aslam, «An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method,» 2022.

[23] D. O. Georgeana GLOBA*, «PRIME NUMBERS: HISTORY, THEORIES AND APPLICATIONS,» 2022.

[24] S. TiwariPankaj, SharmaTsan-Ming y C. LimGomez-Mejia, «Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap,» 2023.

[25] S. K. Nanda, S. K. Panda y M. Dash, «Medical supply chain integrated with blockchain and IoT to track the logistics of medical products,» 2023.

[26] «cryptoapis.io,» 2022. [En línea]. Available: https://cryptoapis.io/blog/113-beyond-the-merge-the-surge-verge-purge-and-splurge-explained.

[27] A. I. A. A. ,. M. A. ,. T. A. E. E. H. A. S. A. G. a. F. K. K. Abdelzahir Abdelmaboud, «Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions,» 2022.

[28] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008.

[29] E. org, «ethereum.org,» ethereum.org, 11 12 2023. [En línea]. Available: https://ethereum.org/en/whitepaper/. [Último acceso: 2 12 2023].

[30] G. Karthikeyan y G. Kousalya, «GTCS-Vagus Nerve Stimulator Automation Using Private IoT-Blockchain Smartcontract,» 2022.

[31] S. Awan, S. Ahmed, F. Ullah, A. Nawaz, A. Khan, M. I. Uddin, A. Alharbi, W. Alosaimi y H. Alyami, «IoT with BlockChain: A Futuristic Approach in Agriculture and Food Supply Chain,» 2021.

[32] S. Auer, S. Nagler, S. Mazumdar, R. Rao y Mukkamala, «study, Towards blockchain-IoT based shared mobility: Car-sharing and leasing as a case,» 2022.

[33] A. Alkhateeb, C. Catal, G. Kar y A. Mishra, «Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review,» 2022.

[34] C. M. J. C. E. S. y. M. D. . Reyna, «On blockchain and its integration with IoT. Challenges and opportunities,» *Future Generation Computer Systems,* vol. 88, pp. 173-190, 2018.

[35] «Klapita, V. Implementation of Electronic Data Interchange as a Method of Communication between Customers and Transport Company,» 2021.

[36] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy y a. A. A. A. El-Latif, «Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities,» 2021.

[37] V. V. V. S. G. T. R. G. y. V. R. R. Chaganti, «Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture.,» 2022.

[38] S. Popov∗, «The Tangle,» 2018.

[39] S. Venkatraman, «Developing an IoT Identity Management System Using Blockchain,» 2022.

[40] A. Sasikumar, V. Subramaniyaswamy, K. Ketan, V. Indragandhi, R. Logesh, S. Ganeshsree y A. Ajith, «Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things,» *Future Generation Computer Systems,* vol. 141, pp. 16-27, 2023.

[41] H. Foundation, «An Overview of Hyperledger Foundation,» 2021.

[42] A. Tandon, A. Kumar y D. Boscovic, «Device identity management on Hyperledger Fabric,» 2022.

[43] F. Limited, «fujitsu,» 23 01 2023. [En línea]. Available: https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0123-01.html. [Último acceso: 10 05 2023].

[44] A. R. Santhi y P. Muthuswamy, «Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics,» 2022.

[45] AnaReyna, CristianMartín, JaimeChen, EnriqueSoler y ManuelDíaz, «On blockchain and its integration with IoT. Challenges and opportunities,» 2018.