

# **Solución IoT para robot de exploración ambiental de datos críticos con almacenamiento en blockchain**

**Esp. Ing. Gonzalo Carreño**

**Carrera de Maestría en Internet de las Cosas**

**Director:** Esp. Ing. Sergio Alberino (UTN-FRBA)

**Jurados:**

Jurado 1 (pertenencia)

Jurado 2 (pertenencia)

Jurado 3 (pertenencia)

*Ciudad de Buenos Aires, abril de 2025*



## *Resumen*

En este trabajo se presenta la implementación de un proyecto personal que consiste en el desarrollo de una solución de Internet de las Cosas aplicada a un robot de exploración ambiental. La implementación asegura la inmutabilidad y transparencia de los datos obtenidos por el robot.

Para su implementación se utilizaron conceptos y herramientas tales como el desarrollo de sistemas embebidos, mensajería asincrónica, almacenamiento y procesamiento distribuido en la nube, entre otros.



# Índice general

<b>Resumen</b>	<b>I</b>
<b>1. Introducción general</b>	<b>1</b>
1.1. Estado del arte	1
1.1.1. Introducción a las soluciones IoT	1
1.1.2. Soluciones IoT que utilizan robots exploradores	2
1.1.3. Soluciones IoT que utilizan blockchain	3
1.2. Motivación del trabajo	4
1.3. Alcance y objetivos	4
1.4. Requerimientos del producto	5
<b>2. Introducción específica</b>	<b>9</b>
2.1. Tecnologías de hardware y firmware utilizadas	9
2.1.1. Robot de exploración ambiental	9
2.1.2. Microcontrolador ESP32	9
2.1.3. Marco de trabajo ESP-IDF	10
2.1.4. FreeRTOS	10
2.2. Tecnologías de Amazon Web Services utilizadas	10
2.2.1. Amazon Web Services	10
2.2.2. AWS IoT Core	10
2.2.3. AWS App Runner	10
2.2.4. AWS Glue	10
2.2.5. AWS S3	11
2.2.6. AWS Athena	11
2.2.7. AWS SNS	11
2.2.8. AWS SQS	11
2.2.9. AWS Secrets Manager	11
2.2.10. AWS Lambda	12
2.2.11. AWS DynamoDB	12
2.2.12. AWS IAM	12
2.2.13. AWS CloudWatch	12
2.3. Tecnologías Azure utilizadas	13
2.3.1. Azure	13
2.3.2. Microsoft Fabric	13
2.4. Tecnologías blockchain utilizadas	13
2.4.1. Ecosistema Ethereum	13
2.4.2. Biblioteca Web3.js	15
2.4.3. Ganache	15
2.4.4. Truffle	15
2.4.5. Alchemy	15
2.4.6. Etherscan	15
2.4.7. Metamask	16

2.5.	Tecnologías de propósito general utilizadas	16
2.5.1.	Node.js	16
2.5.2.	MQTT	16
2.5.3.	Swagger	16
2.6.	Lenguajes de programación utilizados	16
2.6.1.	Lenguaje de programación Python	16
2.6.2.	Lenguaje de programación Javascript	16
2.6.3.	Lenguaje de programación C	17
2.6.4.	Solidity	17
2.7.	Tecnologías de desarrollo utilizadas	17
2.7.1.	Plataforma Docker	17
2.7.2.	Plataforma de CI/CD	17
2.7.3.	Visual Studio Code	18
2.7.4.	Sistema operativo Ubuntu	18
<b>3.</b>	<b>Diseño e implementación</b>	<b>19</b>
3.1.	Arquitectura de software del sistema	19
3.2.	Hardware e infraestructura del sistema	20
3.3.	Integración de los módulos y subsistemas	20
3.3.1.	Capa de percepción	20
3.3.2.	Capa de red	21
3.3.3.	Capas de procesamiento y almacenamiento - dApp (AWS) y Smart Contracts	21
3.3.4.	Capas de distribución de eventos	23
3.3.5.	Capas de procesamiento y almacenamiento de datos	24
3.4.	Plataforma de desarrollo y despliegue	28
3.5.	Tabla de todos los objetos cloud creados	28
<b>4.</b>	<b>Ensayos y resultados</b>	<b>29</b>
4.1.	Verificaciones funcionales del hardware	29
4.1.1.	Verificación del proceso de ingesta en tiempo real MQTT	29
4.1.2.	Verificación del proceso de distribución de eventos en AWS	30
4.1.3.	Verificación de fondos necesarios para realizar despliegues en redes Holesky y Sepolia	30
4.1.4.	Verificación del proceso de despliegue de los Smart Contracts	33
4.1.5.	Verificación del proceso de despliegue de la dApp	34
4.1.6.	Verificación del proceso de invocación de la dApp	35
4.1.7.	Verificación del proceso de invocación de los Smart Contracts	35
4.1.8.	Validación de los datos almacenados en Ethereum	35
4.1.9.	Verificación del proceso de almacenamiento de readings, transacciones y contracts en AWS S3	35
4.1.10.	Verificación del proceso de ingesta y transformación de datos batch en Fabric	37
4.1.11.	Validación del modelo de datos en el Semantic Model	38
4.1.12.	Validación del reporte final generado en PowerBI	38
4.2.	Pruebas funcionales del hardware	38
<b>5.</b>	<b>Conclusiones</b>	<b>39</b>
5.1.	Conclusiones generales	39
5.2.	Próximos pasos	39

**Bibliografia****41**





# Índice de figuras

2.1. Robot de exploración ambiental. . . . .	9
3.1. Arquitectura de la solución. . . . .	19
3.2. Configuración de redes de despliegue en Truffle. . . . .	22
3.3. Creación de base datos, tabla y esquema AWS Glue. . . . .	25
3.4. Azure Data Factory pipeline. . . . .	26
3.5. Dataflows pipeline. . . . .	27
3.6. Modelo semántico de PowerBI. . . . .	27
4.1. Prueba de recepción de mensajes MQTT. . . . .	29
4.2. Configuración de redirección de mensajes MQTT. . . . .	30
4.3. Obtención de créditos mediante Google Web3. . . . .	30
4.4. Saldo en Metamask. . . . .	31
4.5. Transacciones de generación de fondos de prueba. . . . .	31
4.6. Transacciones de despliegue en Sepolia. . . . .	32
4.7. Detalles del contrato desplegado en Sepolia. . . . .	33
4.8. Salida por pantalla durante el proceso de despliegue de los componentes blockchain. . . . .	33
4.9. Endpoints expuestos por la dApp. . . . .	34
4.10. Frontend the Alchemy. . . . .	35
4.11. Almacenamiento de mensajes JSON en AWS S3. . . . .	35
4.12. Consulta de datos SQL desde AWS Athena. . . . .	36
4.13. Correcta ejecución del pipeline punta-a-punta con Azure Data Factory y Dataflows. . . . .	37
4.14. Dashboard PowerBI. . . . .	38



# Índice de tablas

3.1. <a href="#">caption corto</a> . . . . .	20
3.2. <a href="#">caption corto</a> . . . . .	28



# Capítulo 1

## Introducción general

Este capítulo presenta la motivación, alcance, objetivos y requerimientos del producto en el marco del estado del arte y su importancia en la industria.

### 1.1. Estado del arte

#### 1.1.1. Introducción a las soluciones IoT

Las soluciones IoT (*Internet of Things* o Internet de las Cosas) se basan en la conexión de dispositivos físicos con aplicaciones informáticas para recopilar, transmitir y analizar datos en *streaming* y de forma *batch*. Esto mejora la automatización, observabilidad y toma de decisiones en diversos casos de uso.

Su arquitectura estándar en general incluye dispositivos y sensores para capturar datos, conectividad de red (Wi-Fi [1], 5G [2], LoRaWAN [3]) para su transmisión, una plataforma *backend* en la nube formada por sistemas distribuidos para el almacenamiento, procesamiento y análisis de datos, y una interfaz de usuario para la visualización de resultados. En ocasiones también puede incluir sistemas de publicación y distribución de eventos en *streaming*. En general, las soluciones IoT generalmente están organizadas en las siguientes capas:

- Capa de percepción (*Sensing Layer*): esta capa, la más cercana al entorno físico, captura datos del ambiente (temperatura, humedad, etc.) mediante dispositivos IoT y sensores. Generalmente, se usan sistemas embebidos con sensores y actuadores para interactuar con el entorno.
- Capa de red (*Network Layer*): se encarga de la transmisión de datos desde los dispositivos hasta los sistemas de procesamiento. Aquí es donde ocurre la conectividad mediante diversos protocolos de comunicación usando tecnologías inalámbricas (tales como Wi-Fi, Bluetooth [4], Zigbee [5], LoRaWAN, NB-IoT [6], etc.) y protocolos de red (por ejemplo, MQTT, CoAP, HTTP, etc.)
- Capa de procesamiento de borde (*Edge Computing Layer*): procesa datos cerca de donde se generan para reducir la latencia y el tráfico hacia la nube. Se toman decisiones inmediatas y solo los datos relevantes se envían a niveles superiores.
- Capa de almacenamiento y procesamiento *cloud* (*Data Storage/Cloud Layer*): almacena y procesa grandes volúmenes de datos recopilados en la nube, lo que permite realizar análisis más profundos, modelado de datos y aprendizaje automático. Se utilizan herramientas *cloud* (como AWS IoT Core [7], Azure Iot Hub [8], etc.) y Big Data.

- Capa de aplicación (*Application Layer*): es la interfaz que permite a los usuarios interactuar con el sistema IoT. Aquí se presentan los datos de manera visual o se automatizan acciones basadas en la información recibida. Se utilizan tecnologías web y mobile, orientadas a eventos *streaming* o dashboards para visualizar reportes *batch*.
- Capa de seguridad (*Security Layer*): esta capa es transversal a las capas anteriores y tiene como función asegurar la protección de datos, dispositivos y redes en todas las capas del sistema IoT. Es fundamental para evitar vulnerabilidades y ataques. Utiliza algoritmos de encriptación (como por ejemplo TLS/SSL y AES), protocolos de seguridad (como OAuth, OpenID Connect, etc).

### 1.1.2. Soluciones IoT que utilizan robots exploradores

Existen casos de uso de IoT en los cuales se utilizan robots exploradores como dispositivos físicos para la recopilación de datos en la capa de percepción. Los robots exploradores son dispositivos robotizados capaces de moverse de forma autónoma y/o controlados a distancia que utilizan sensores avanzados, inteligencia artificial y comunicación en tiempo real para navegar y monitorear condiciones ambientales en entornos peligrosos, como minas, plataformas petrolíferas, espacios confinados o áreas afectadas por desastres, entre otros. En agricultura, pueden inspeccionar cultivos; en medio ambiente, pueden monitorear la calidad del aire, del agua; en el espacio y océanos, son capaces de explorar lugares inaccesibles para el ser humano.

Tanto en el ámbito académico como en la industria, existen diversos trabajos, proyectos e implementaciones comerciales de soluciones IoT que utilizan robots para mejorar la seguridad, la eficiencia y la toma de decisiones basada en datos. Por ejemplo:

- En Lotus Mountain, Jilin, China, se implementó un sistema de seguridad para estaciones de esquí que utiliza perros robóticos equipados con sensores y tecnología de imágenes 3D. Estos robots patrullan las pistas para identificar peligros como desprendimientos y bloqueos, mejorando así la seguridad de los esquiadores [9].
- El implementado por el Ayuntamiento de Bilbao [10] para la inspección y mantenimiento de redes de saneamiento, que por medio de drones y robots, busca mejorar la eficiencia operativa y la seguridad de los trabajadores al reducir la necesidad de intervenciones humanas en entornos subterráneos y potencialmente peligrosos.
- El proyecto Tecnobosque [11] en Cuenca, España, que utiliza drones equipados con sensores e inteligencia artificial para crear cortafuegos preventivos y reducir significativamente las hectáreas de bosques en casos de incendios.
- Spot [12], desarrollado por Boston Dynamics, un robot explorador cuadrupedo de propósito general capaz de explorar, almacenar y enviar información en tiempo real.

- BIKE [13], desarrollado por Waygate Technologies, un robot con ruedas magnéticas, muy utilizado en la industria de petróleo y gas entre otras, capaz de desplazarse por el interior de tuberías para poder realizar inspecciones y comunicar hallazgos.
- El prototipo robótico de exploración minera publicado en varios artículos [14], [15], e impulsado por el Instituto de Automática de la Facultad de Ingeniería de la Universidad Nacional de San Juan en el marco de un convenio con la Comisión Nacional de Energía Atómica y el Gobierno argentino [16].
- El robot de exploración terrestre denominado Geobot [17] desarrollado por los ingenieros Nelson Dario García Hurtado y Melvin Andrés González Pino, de la universidad de Pamplona, capaz de realizar reconocimiento de zonas y manipulación de muestras de manera autónoma o asistida.
- El robot minero MIN-SIS 1.0 SDG-STR [18] desarrollado por los ingenieros Hernán L. Helguero Velásquez y Rubén Medinaceli Tórrez de la Universidad Técnica de Oruro, capaz de detectar gases, almacenar datos locales y enviar video e imágenes al puesto de mando.

### 1.1.3. Soluciones IoT que utilizan blockchain

Para la exploración y monitoreo de áreas ambientalmente sensibles (reservas naturales, sitios de desastre ecológico), la recopilación de datos críticos (contaminación, temperatura, etc.) requiere el almacenamiento en un sistema que garantice la integridad y transparencia, como una cadena de bloques.

Una arquitectura blockchain [19] se basa en el agrupamiento de transacciones que luego de ser procesadas, son almacenadas en bloques encadenados de forma distribuida e inmutable, entre los nodos de una red. Esta estructura de datos se conoce como una cadena de bloques y sus datos almacenados forma un *distributed ledger* (o asiento contable distribuido). De esta manera, como los datos forman registros que no se pueden modificar una vez creados, se puede asegurar la inmutabilidad, y como el almacenamiento y procesamiento de la red se encuentran distribuidos, se puede garantizar su transparencia.

La mayoría de las redes blockchain constan de ciertas tecnologías para la implementación de código ejecutable en la misma red, que aunque su nombre puede cambiar dependiendo de la red, usualmente se los conoce como *smart contracts* [20]. La ejecución de estos componentes es realizada por los nodos de la red en el proceso que se conoce como minería o validación. La forma de interactuar con los *smart contracts* se realiza a través de otro componente conocido como dApps (*de-centralized applications*) [21] que por medio del uso de ciertas tecnologías invocan a estos componentes para almacenar y obtener datos en y desde el *distributed ledger*.

El uso de blockchain en arquitecturas IoT ofrece ventajas como descentralización, cifrado, seguridad y consenso, lo que aumenta la trazabilidad, la transparencia y la automatización mediante *smart contracts*.

Existen en la industria varias implementaciones de casos de uso IoT en los que se ha utilizado blockchain como por ejemplo:

- La solución basada en blockchain implementada por Walmart [22] para mejorar la trazabilidad de productos alimenticios en su cadena de suministro.

Al integrar dispositivos IoT, la empresa puede monitorear en tiempo real variables como temperatura y humedad durante el transporte y almacenamiento de productos perecederos. Estos datos se registran en una blockchain para garantizar la inmutabilidad y transparencia de la información.

- La solución implementada por ScanTrust [23] que utiliza códigos QR seguros para conectar productos físicos con el entorno digital. Al integrar IoT y blockchain, permite a las empresas y consumidores autenticar productos y rastrear su origen y cadena de suministro en tiempo real. Los códigos QR, impresos en los envases, se escanean con dispositivos móviles para proporcionar información detallada y asegurar la autenticidad del producto.
- La solución implementada por la empresa Saltoki en colaboración con EcoMT [24], que permite monitorizar y gestionar el consumo energético, para certificar la producción renovable y los ahorros obtenidos mediante tecnología blockchain.

## 1.2. Motivación del trabajo

La motivación del presente trabajo fue primeramente volcar y unificar en un emprendimiento personal los conceptos aprendidos en la Maestría en Internet de las Cosas.

Se diseñó una arquitectura robusta y flexible, con el fin de ser implementada en la industria, donde la integración de sistemas embebidos con blockchain es crucial para el almacenamiento transparente e inalterable de datos sensibles.

Asimismo, se procuró crear un producto que pudiera fomentar el conocimiento público y el estado del arte de proyectos de código abierto relacionados con soluciones IoT integradas a blockchain en Argentina.

## 1.3. Alcance y objetivos

El objetivo del trabajo es la integración del dispositivo robótico de exploración ambiental [25] desarrollado en el marco de la Carrera de Especialización en Sistemas Embebidos, con un sistema *backend* desplegado en la nube pública [26], y una red blockchain [19] a fin de poder asegurar la inmutabilidad y transparencia de las lecturas ambientales.

A continuación, se detallan las funcionalidades incluidas en el alcance del trabajo:

- La publicación del endpoint MQTT [27] para la recepción de los datos enviados por el robot.
- La adaptación del sistema embebido del robot de exploración ambiental para la conexión segura con el *backend* vía MQTT.
- La arquitectura e implementación de los sistemas *backend* y el modelo de datos necesario para el almacenamiento de las mediciones enviadas por el robot.
- La arquitectura, implementación y despliegue de la dApp [21] y *smart contracts* [20] necesarios para el almacenamiento de las mediciones en una red blockchain.



- La definición de métricas agregadas de valor y posterior arquitectura e implementación de los sistemas analíticos para procesar de forma *batch* y/o *real-time* utilizando herramientas de procesamiento paralelo basadas en Big Data.
- La implementación de la interfaz gráfica para poder visualizar los datos enviados y analíticas calculadas.

## 1.4. Requerimientos del producto

A continuación, se listan los requerimientos del producto:

### 1. Requerimientos funcionales

- a) El robot de exploración ambiental debe poder enviar a la plataforma datos de mediciones de parámetros ambientales, incluyendo los datos de fecha, hora, localización geográfica (que puede ser implementada como un valor *mock*) y la categorización si es o no un valor crítico.
- b) El robot de exploración ambiental debe incorporar una lógica para categorizar los valores medidos de cada parámetro ambiental como valores críticos si:
  - 1) Representan un máximo o mínimo global sensado hasta el momento.
  - 2) Representan un máximo o mínimo local durante el último día.
- c) La solución a desarrollar debe poder recibir y almacenar las mediciones de parámetros ambientales enviadas por el robot.
- d) Los datos considerados críticos deben ser almacenados en un sistema inmutable.
- e) La solución a desarrollar debe poder procesar las mediciones de parámetros ambientales enviadas por el robot para generar métricas de valor para el usuario de negocio.
- f) La solución a desarrollar debe brindar dos *frontend* con interfaz web:
  - 1) El *frontend* para el usuario de negocio.
  - 2) El *frontend* para el usuario administrador.
- g) El *frontend* para el usuario de negocio debe proveer métricas para visualizar:
  - 1) Las lecturas históricas almacenadas.
  - 2) Agregaciones (máximo, mínimo, promedio, etc.) de cada parámetro ambiental agrupado por frecuencias (ventanas de tiempo) y coordenadas geográficas.
  - 3) Las referencias a los datos persistidos en blockchain.
- h) El *frontend* para el usuario de administración debe permitir:
  - 1) Acceder a los diferentes recursos utilizados por la herramienta (topics MQTT, *smart contracts*, *buckets*, etc.).

2) Resetear valores y estado.

## 2. Requerimientos no funcionales

- a) La solución a desarrollar debe contar con al menos un *backend* de procesamiento y acceso a datos operacionales para la lógica de negocio.
- b) La solución a desarrollar debe contar con al menos un *backend* de acceso, procesamiento, almacenamiento de datos analíticos para la generación de métricas.
- c) El envío de los valores ambientales censados al *backend* debe ser mediante MQTT.
- d) Las lecturas ambientales categorizadas como críticas deben ser almacenadas en blockchain para garantizar fiabilidad e inmutabilidad.
- e) La gestión de datos almacenados en blockchain debe ser implementada mediante *smart contracts* desplegados en la red.
- f) La interacción con los *smart contracts* debe realizarse desde una dApp.
- g) Los sistemas de transferencia y almacenamiento de datos utilizados deben contar con seguridad, permitiendo encriptación, autenticación y autorización.

## 3. Requerimientos de documentación

- a) Video demostrativo.
- b) Documentación de arquitectura técnica del diseño del sistema.
- c) Manual de usuario.
- d) Memoria final.

## 4. Requerimientos de testing

- a) Se deben incluir tests de unitarios de componentes.
- b) Se deben incluir tests funcionales (*smoke test*) del producto general.

## 5. Requerimientos opcionales

- a) De infraestructura y despliegue:
  - 1) Se permite realizar el despliegue de la dApp en un IPFS (preferentemente) o en la nube.
  - 2) Se permite la incorporación de nuevo hardware al robot para la captura de datos adicionales.
  - 3) Se permite agregar automatización para la creación de la infraestructura como código.
- b) De datos:
  - 1) Se permite almacenar cualquier otro dato adicional sensado o derivado.
  - 2) Se permite agregar cualquier implementación de gobierno de datos.

- 3) Se permite almacenar cualquier otra métrica o gráfico de explotación de datos adicional.



## Capítulo 2

# Introducción específica

En este capítulo se presenta una breve introducción técnica a las herramientas de hardware y software utilizadas en el trabajo.

### 2.1. Tecnologías de hardware y firmware utilizadas

#### 2.1.1. Robot de exploración ambiental

Como dispositivo físico en la capa de percepción, se utilizó el robot de exploración ambiental desarrollado en el marco de la Carrera de Especialización en Sistemas Embebidos [25]. En la figura 2.1 se puede apreciar una foto del robot.

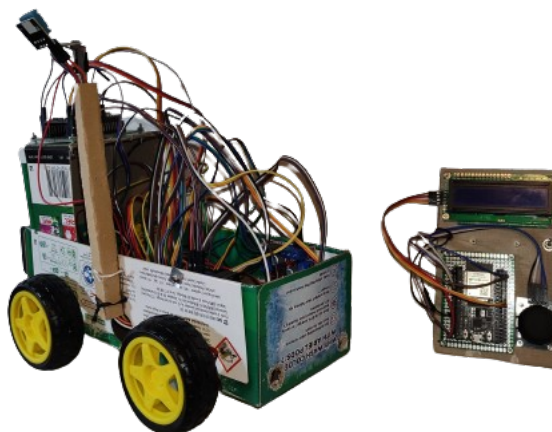


FIGURA 2.1. Robot de exploración ambiental.

El robot de exploración ambiental es un sistema embebido desarrollado con el marco de desarrollo ESP-IDF [28] de Espressif Systems que utiliza un microcontrolador ESP32 [29] y FreeRTOS [30] como sistema operativo. Está diseñado para explorar terrenos mediante control de joystick y para obtener parámetros ambientales como luminosidad, presión atmosférica, temperatura y humedad.

#### 2.1.2. Microcontrolador ESP32

ESP32 [29] es una serie de microcontroladores embebidos en un chip con Wi-Fi y Bluetooth integrados, de bajo costo y consumo, desarrollado por *Espressif Systems*. Emplea dos núcleos Xtensa® 32-bit LX6 CPU, incluye interruptores de antena, amplificador de potencia, amplificador de recepción de bajo ruido, un co-procesador ULP (*Ultra Low Power*), módulos de administración de energía y diversos periféricos.

### 2.1.3. Marco de trabajo ESP-IDF

El marco de trabajo ESP-IDF[28] de Espressif Systems proporciona un conjunto de recursos para facilitar el desarrollo de *firmware* para ESP32. Utiliza FreeRTOS como sistema operativo base y brinda varias utilidades de desarrollo y bibliotecas de código para poder acceder y controlar los diferentes recursos del microcontrolador.

### 2.1.4. FreeRTOS

FreeRTOS (*Free Real-Time Operating System*) [30] es un sistema operativo en tiempo real de código abierto, ligero y diseñado para microcontroladores y sistemas embebidos. Permite ejecutar múltiples tareas concurrentemente mediante planificación por prioridades, ofreciendo servicios como manejo de tareas, colas, temporizadores, semáforos y sincronización. Es ampliamente usado en aplicaciones IoT y sistemas críticos donde se requiere una respuesta rápida y predecible, y se puede portar fácilmente a una gran variedad de arquitecturas de hardware como ARM Cortex-M, RISC-V, entre otras.

## 2.2. Tecnologías de Amazon Web Services utilizadas

### 2.2.1. Amazon Web Services

AWS (*Amazon Web Services*) [31] es una de las principales plataformas de servicios en la nube pública proporcionada por Amazon, que ofrece una amplia gama de productos y herramientas para computación, almacenamiento, bases de datos, redes, inteligencia artificial, seguridad y herramientas de desarrollo.

### 2.2.2. AWS IoT Core

AWS IoT Core [7] es un servicio totalmente administrado de AWS que permite conectar dispositivos IoT a la nube de manera segura y confiable. Proporciona una infraestructura escalable para recopilar, procesar y analizar datos de dispositivos en tiempo real, así como para interactuar con otros servicios de AWS a los que se redirigen los mensajes recibidos mediante la configuración de reglas. Tiene soporte para varios protocolos de comunicaciones, entre los que se destacan principalmente MQTT, HTTP/S, WebSockets y LoRaWAN.

### 2.2.3. AWS App Runner

AWS App Runner [32] es un servicio completamente administrado de AWS que permite implementar y ejecutar aplicaciones web y servicios de forma rápida, sin tener que gestionar instancias de infraestructura. Está diseñado para simplificar el proceso de implementación y escalado automático de aplicaciones y permite aplicaciones directamente desde el código fuente o desde contenedores Docker [33].

### 2.2.4. AWS Glue

AWS Glue [34] es un servicio totalmente administrado de AWS diseñado para facilitar la extracción, transformación y carga de datos (ETL) en la nube. Permite a los usuarios descubrir, preparar y combinar datos de múltiples fuentes para su

análisis y almacenamiento en data lakes, data warehouses o bases de datos. Este servicio es útil para proyectos de Big Data y análisis de datos, ya que ofrece un catálogo de datos, asistencia para la generación de código ETL y ejecución de trabajos de procesamiento paralelo.

### 2.2.5. AWS S3

AWS S3 (*Simple Storage Service*) [35] es un servicio de almacenamiento de objetos totalmente administrado por AWS. Permite almacenar y recuperar cualquier cantidad de datos de forma segura, escalable y económica desde cualquier lugar. Es ideal para datos no estructurados de gran volumen, sitios web estáticos, archivos multimedia y copias de seguridad, entre otros.

### 2.2.6. AWS Athena

AWS Athena [36] es un servicio de análisis de datos sin servidor de AWS que permite consultar directamente datos almacenados en Amazon S3 y esquemas definidos en Glue, utilizando SQL estándar. No requiere configuración ni administración de servidores, y es ideal para analizar grandes volúmenes de datos de forma rápida y económica.

### 2.2.7. AWS SNS

Amazon SNS (*Amazon Simple Notification Service*) [37] es un servicio de mensajería totalmente gestionado que permite el envío de notificaciones desde aplicaciones a otros sistemas distribuidos, servicios en la nube o usuarios finales. Funciona bajo un modelo de publicación-suscripción (pub/sub), donde los productores de mensajes (publicadores) envían mensajes a un *topic*, y los consumidores (suscriptores) los reciben. Amazon SNS es ideal para aplicaciones que requieren alta disponibilidad, baja latencia y escalabilidad para distribuir eventos o alertas en tiempo real.

### 2.2.8. AWS SQS

Amazon SQS (*Amazon Simple Queue Service*) [38] es un servicio de colas de mensajes completamente gestionado que permite desacoplar y escalar componentes de aplicaciones distribuidas, eliminando la necesidad de administrar infraestructura de mensajería. SQS actúa como intermediario entre productores y consumidores de mensajes, almacenando mensajes de forma temporal hasta que los sistemas receptores estén listos para procesarlos. Amazon SQS es ideal para construir sistemas resilientes, desacoplados y altamente escalables, como pipelines de procesamiento de datos, flujos de trabajo asincrónicos o integración entre microservicios.

### 2.2.9. AWS Secrets Manager

AWS Secrets Manager [39] es un servicio gestionado que permite almacenar, gestionar, rotar y recuperar credenciales, claves API, contraseñas y otros secretos de forma segura. Brinda una API que permite a las aplicaciones recuperar secretos de forma programática, eliminando la necesidad de codificar credenciales directamente en el código fuente o archivos de configuración. Es compatible con varios servicios de AWS para la rotación automática de credenciales, y se integra muy

facilmente con todos los servicios de AWS, mejorando la seguridad, el cumplimiento y la gestión centralizada de secretos.

#### 2.2.10. AWS Lambda

AWS Lambda [40] es un servicio de computación serverless ideal para crear aplicaciones escalables, desacopladas, reactivas y de baja latencia, que permite ejecutar código en respuesta a eventos sin necesidad de aprovisionar ni administrar servidores. Permite cargar funciones escritas en lenguajes como Python, Node.js, Java, entre otros, y Lambda se encarga automáticamente de ejecutar el código cuando se produce un evento, escalarlo según la demanda y gestionar la infraestructura subyacente. Lambda se integra de forma nativa con otros servicios de AWS como S3, DynamoDB, API Gateway, SNS y SQS, lo que permite construir arquitecturas basadas en eventos de manera sencilla y eficiente.

#### 2.2.11. AWS DynamoDB

Amazon DynamoDB [41] es un servicio de base de datos NoSQL totalmente gestionado que ofrece almacenamiento de datos clave-valor y de documentos con alta disponibilidad, rendimiento escalable y baja latencia. Está diseñado para manejar cargas de trabajo intensivas y aplicaciones que requieren respuestas en tiempo real, ideal para casos de uso IoT por ese motivo. DynamoDB permite escalar automáticamente la capacidad de lectura y escritura, y ofrece opciones avanzadas como almacenamiento en caché, backup y restauración bajo demanda, replicación global y soporte para transacciones ACID.

#### 2.2.12. AWS IAM

AWS IAM (*AWS Identity and Access Management*) [42] es un servicio que permite gestionar de forma segura el acceso a los recursos de AWS mediante la creación y control de usuarios, grupos, roles y políticas de permisos. Con IAM se pueden definir quién puede acceder a qué recursos, en qué condiciones y con qué nivel de privilegio, aplicando el principio de mínimo privilegio. IAM permite la autenticación de identidades y la autorización de acciones tanto para usuarios internos como para aplicaciones y servicios de AWS. Además, admite políticas detalladas en formato JSON, control de acceso basado en atributos (ABAC) [43], autenticación multifactor (MFA) [44] y federación de identidades con directorios corporativos o proveedores externos.

#### 2.2.13. AWS CloudWatch

Amazon CloudWatch [45] es un servicio de monitoreo y observabilidad totalmente gestionado que permite recopilar, visualizar y analizar métricas, logs y eventos de recursos y aplicaciones en AWS. Facilita la supervisión del rendimiento, la detección de anomalías y la generación de alertas en tiempo real a partir de datos generados por servicios como EC2, Lambda, DynamoDB, RDS, entre otros, así como por aplicaciones personalizadas mediante agentes o APIs.



## 2.3. Tecnologías Azure utilizadas

### 2.3.1. Azure

Azure [46] es la plataforma de computación en la nube pública de Microsoft que ofrece una amplia gama de servicios para el desarrollo, implementación y gestión de aplicaciones y soluciones a través de una red global de centros de datos. Permite a las organizaciones ejecutar cargas de trabajo en modelos IaaS, PaaS y SaaS, con soporte para máquinas virtuales, bases de datos, inteligencia artificial, almacenamiento, redes, análisis de datos, IoT y seguridad, entre otros aspectos.

### 2.3.2. Microsoft Fabric

Microsoft Fabric [47] es una plataforma unificada de analítica de datos en la nube de Azure que integra múltiples herramientas en un entorno gestionado. Está diseñada simplificar la integración, transformación, análisis y visualización de datos. Entre sus componentes principales se encuentran:

- Lakehouse [48]: combina las capacidades de un data lake y un data warehouse, permitiendo almacenar y procesar grandes volúmenes de datos estructurados y no estructurados, compatible con Spark, notebooks y consultas SQL.
- Warehouse [49]: un entorno de base de datos relacional orientado a análisis empresariales y modelado dimensional, que permite ejecutar consultas SQL sobre los datos almacenados en OneLake.
- Data Factory [50]: herramienta de orquestación de flujos de datos que permite construir ETL/ELT mediante pipelines y actividades de copiado.
- Dataflows Gen2 [51]: herramienta de transformaciones de datos complejas que brinda una interfaz visual sin necesidad de escribir código y utiliza el motor Spark de forma subyacente.
- Power BI [52]: la herramienta de BI (Business Intelligence o inteligencia de negocios) en la nube de Azure, integrada de forma nativa en Fabric, permite crear visualizaciones, dashboards e informes interactivos directamente sobre datos almacenados en Lakehouse o Warehouse, mediante la abstracción de un Semantic Model que define métricas, jerarquías y relaciones, sin necesidad de mover ni duplicar los datos.
- OneLake [53]: actúa como repositorio de datos único para todos los servicios de Fabric, asegurando gobierno y seguridad de datos.

## 2.4. Tecnologías blockchain utilizadas

### 2.4.1. Ecosistema Ethereum

Ethereum [54] es una red blockchain pública diseñada para el procesamiento de transacciones de forma descentralizada con almacenamiento distribuido, inmutable y de acceso libre (*permissionless*) que se diferencia de otras redes blockchain, como Bitcoin, porque no es solo un *distributed ledger*, sino también una plataforma programable que permite desarrollar, desplegar y ejecutar aplicaciones. Se encuentra formada por distintos tipos de nodos EVM (*Ethereum Virtual Machine*)

[55] que tienen como función procesar transacciones y almacenarlas en una estructura de datos basada en una cadena de bloques. Tiene como *token* el Ether, cuyo símbolo es ETH y tiene varios usos, pudiendo ser utilizado como criptomoneda de cambio, entre los usuarios finales de la red, pero también para pagar el *gas fee*, o costo de ejecución de transacciones. Existen varios despliegues de Ethereum disponibles para distintos propósitos. La Mainnet [56] es su red principal para usos productivos. Además existen múltiples *testnets*, o redes de prueba, como Sepolia [57] y Holesky [58] entre otras, disponibles para ser usadas durante el desarrollo y evaluación de soluciones sin necesidad de pagar con fondos reales.

Las aplicaciones desarrolladas en blockchain son los *smart contracts*. Estos componentes permiten ejecutar código directamente en la red para automatizar, verificar y hacer cumplir acuerdos. Pueden ser invocados desde afuera de la blockchain o disparados cuando se producen ciertos eventos. Una vez desplegados en la blockchain, no se pueden modificar, y todas las transacciones quedan registradas públicamente. Se desarrollan en alguno de los lenguajes de programación y SDK soportados, como por ejemplo Solidity y Truffle. Una vez desarrollados, tras el proceso de compilación se obtiene un ABI [59] que especifica el contrato en formato JSON. Posteriormente, se despliega el código binario (no el ABI) en una nueva transacción blockchain.

Para la invocación a los *smart contracts* se utilizan las dApps como componente de abstracción. Estas son aplicaciones que se ejecutan fuera de la blockchain, como por ejemplo un *backend* en Node.js o un *frontend* Javascript, e interactúan con la blockchain a través de ciertas bibliotecas, como por ejemplo, Web3.js [60]. Para poder acceder a la red, y posteriormente invocar el *smart contract*, la dApp necesita utilizar un endpoint RPC publicado por cualquier nodo de la red y disponer de la especificación ABI del *smart contract* obtenido durante su compilación (y no se disponible en la red).

Cada vez que un *smart contract* es invocado, se genera una nueva transacción en la red que debe ser validada y agrupada en un bloque. El proceso de validación de transacciones y generación de bloques, a partir de la versión 2.0 de Ethereum, utiliza el protocolo PoS (*Proof-of-Stake*) [61] y propone un nuevo bloque aproximadamente cada doce segundos. El primer paso, es la recolección de transacciones enviadas por los usuarios a la red, luego un validador es seleccionado de forma aleatoria para proponer el siguiente bloque, y selecciona aquellas transacciones con tarifas de *gas* mas altas para maximizar su recompensa. Como resultado, el validador seleccionado confecciona un nuevo bloque que incluye las transacciones válidas, el estado actualizado del sistema, el *hash* del bloque anterior y los datos adicionales como la firma del bloque. Finalmente, un comité de validadores seleccionado de forma aleatoria revisa el bloque propuesto y verifica que las transacciones sean válidas, el bloque no esté duplicado o malicioso y sea coherente con el estado de la blockchain. Si más del 66,6 % de los validadores en el comité lo consideran válido, el bloque es agregado a la cadena de bloques de forma permanente.

El proceso de compensación y penalización de PoS retribuye a los validadores por diferentes acciones, con el fin de mantener la integridad y consenso de la red, aplica una técnica llamada *slashing* para la penalización por acciones malisiosas o incorrectas. El validador que propone el bloque recibe recompensas por bloque y tarifas de *gas*. Los validadores que votan correctamente para validar bloques también reciben recompensas proporcionales a su participación. Si el validador

no presenta comportamiento malicioso o inactividad, no es penalizado. Sin embargo, los validadores pueden perder parte o todo su capital en *stack* si proponen múltiples bloques en un mismo slot, votan de manera inconsistente, o están inactivos durante largos períodos de tiempo.

#### 2.4.2. Biblioteca Web3.js

Web3.js [60] es una biblioteca de JavaScript que permite interactuar con la blockchain de Ethereum y otros protocolos compatibles con EVM. Proporciona una forma sencilla de conectarse a nodos de Ethereum, realizar transacciones y leer datos de contratos inteligentes, directamente desde aplicaciones web o Node.js.

#### 2.4.3. Ganache

Ganache [62] es una herramienta de desarrollo de Ethereum que permite crear una blockchain local para probar, desarrollar y depurar contratos inteligentes y dApps de forma rápida y segura. Es parte del conjunto de herramientas de Truffle Suite y es ampliamente utilizada por desarrolladores para simular una red Ethereum sin necesidad de usar una red pública como Mainnet o Testnets (Goerli, Sepolia).

#### 2.4.4. Truffle

Truffle [63] es un framework de desarrollo para Ethereum y otras blockchains compatibles con EVM. Es parte de Truffle Suite y proporciona herramientas para compilar, desplegar y probar contratos inteligentes, además de facilitar la gestión de proyectos basados en Web3. Truffle automatiza gran parte del proceso de desarrollo de dApps, reduciendo errores y mejorando la eficiencia.

#### 2.4.5. Alchemy

Alchemy [64] es una plataforma de desarrollo blockchain que proporciona herramientas e infraestructura para crear y gestionar dApps en Ethereum y otras redes compatibles con EVM. Ofrece nodos como servicio y herramientas para facilitar la interacción con la blockchain sin necesidad de que los desarrolladores configuren y mantengan sus propios nodos. En el trabajo actual, se utilizó Alchemy como punto de integración entre la dApp y los Smart Contracts.

#### 2.4.6. Etherscan

Etherscan [65] es un explorador de bloques y plataforma de análisis para la red Ethereum. Permite a los usuarios buscar, verificar y rastrear transacciones, contratos inteligentes, direcciones de billeteras y otros datos en tiempo real. Es una herramienta fundamental para los desarrolladores y usuarios de Web3, ya que ofrece transparencia y acceso abierto a la información almacenada en la blockchain de Ethereum, tanto la Mainnet como las redes de prueba (Sepolia, Holesky, etc).

### 2.4.7. Metamask

MetaMask [66] es una billetera digital y extensión de navegador (también disponible como aplicación móvil) que permite a los usuarios interactuar con blockchains basadas en Ethereum y otros ecosistemas compatibles con Ethereum, como Binance Smart Chain (BSC) y Polygon. Es una herramienta fundamental para interactuar con aplicaciones descentralizadas (dApps), contratos inteligentes y realizar transacciones de criptomonedas directamente desde el navegador. En el presente trabajo se utilizó para almacenar los fondos en ETH obtenidos a través de *faucets* necesarios para pagar el gas de las transacciones.

## 2.5. Tecnologías de propósito general utilizadas

### 2.5.1. Node.js

Node.js [67] es un entorno de ejecución de código abierto basado en el motor V8 de Chrome, utilizado principalmente como servidor web. Emplea un modelo *single-thread* de *event loop* con I/O no bloqueante para gestionar múltiples solicitudes y paralelismo de tareas mediante callbacks asíncronos.

### 2.5.2. MQTT

MQTT (*Message Queuing Telemetry Transport*) [27] es un protocolo de comunicación asíncrono, ligero y orientado a mensajes, diseñado para dispositivos con recursos limitados y redes de baja ancho de banda. Ampliamente utilizado en IoT, permite la transmisión de datos en tiempo real entre dispositivos, sensores y aplicaciones mediante un modelo publish/subscribe y topics, donde los clientes se conectan a un broker para publicar o recibir notificaciones.

### 2.5.3. Swagger

Swagger [68] es un conjunto de herramientas para diseñar, documentar y consumir APIs RESTful. Utiliza el formato OpenAPI Specification (OAS) para describir de forma estandarizada la estructura de una API, permitiendo la generación automática de documentación interactiva, clientes SDK y pruebas.

## 2.6. Lenguajes de programación utilizados

### 2.6.1. Lenguaje de programación Python

Python es un lenguaje de programación de alto nivel, interpretado y de propósito general, conocido por su sintaxis clara y legible que favorece el desarrollo rápido y eficiente. Es ampliamente utilizado en áreas como desarrollo web, automatización, análisis de datos, inteligencia artificial y ciencia de datos, gracias a su gran ecosistema de bibliotecas, amplia documentación y comunidad activa. Fue utilizado en el trabajo en las funciones AWS Lambda.

### 2.6.2. Lenguaje de programación Javascript

JavaScript es un lenguaje de programación interpretado, de alto nivel y orientado a objetos, diseñado originalmente para el desarrollo web del lado del cliente. Se

utiliza tanto en el frontend como en el backend gracias a entornos como Node.js. Fue utilizado en el trabajo para el desarrollo de la dApp como backend Node.js.

### 2.6.3. Lenguaje de programación C

C es un lenguaje de programación de propósito general, compilado y de bajo nivel, conocido por su eficiencia, velocidad y control directo sobre el hardware. Es ampliamente utilizado en sistemas operativos, software embebido y desarrollo de sistemas donde el rendimiento y el acceso a memoria son críticos. Fue utilizado en el trabajo para el desarrollo del firmware del sistema embebido.

### 2.6.4. Solidity

Solidity [69] es un lenguaje de programación de alto nivel, orientado a contratos inteligentes, específicamente diseñado para funcionar en la EVM (*Ethereum Virtual Machine*). Fue creado en 2014 por Gavin Wood, Christian Reitwiessner y otros desarrolladores de Ethereum. Su sintaxis es similar a JavaScript, Python y C++, lo que facilita el aprendizaje para desarrolladores familiarizados con esos lenguajes. Fue utilizado en el trabajo para el desarrollo de los *smart contracts*.

## 2.7. Tecnologías de desarrollo utilizadas

### 2.7.1. Plataforma Docker

Docker [33] es un proyecto de código abierto que automatiza el despliegue de aplicaciones en contenedores, utilizando características de aislamiento del kernel Linux (cgroups y namespaces) para ejecutar contenedores ligeros y aislados, evitando la sobrecarga de máquinas virtuales.

### 2.7.2. Plataforma de CI/CD

Durante el proceso de desarrollo del producto se utilizó CI/CD (*continuous integration / continuous delivery*) mediante la integración de las siguientes herramientas:

- Github [70]: servicio de repositorio y control de versiones de código fuente.
- AWS CodePipeline [71]: servicio de compilación, empaquetado y ejecución *builds*.
- AWS Elastic Container Registry [72]: servicio de repositorio y control de versiones de imágenes Docker.

El objetivo de esta configuración de servicios es permitir que por cada cambio en el código fuente versionado en el controlador de versiones Github, se dispare un proceso de compilación y ejecución de tests unitarios notificando en tiempo real si dicho cambio agrega o no una falla al actual estado del desarrollo. En caso de pasar satisfactoriamente la compilación y ejecución de los tests entonces se genera una nueva imagen Docker con la última versión del código compilado y se versiona en AWS Elastic Container Registry.

### **2.7.3. Visual Studio Code**

Visual Studio Code [73] es un editor de código fuente desarrollado por Microsoft para Windows, Linux, macOS y Web. Incluye soporte para la depuración, control integrado de Git, resaltado de sintaxis, finalización inteligente de código, fragmentos y refactorización de código.

### **2.7.4. Sistema operativo Ubuntu**

Ubuntu [74] es una distribución Linux basada en Debian GNU/Linux y patrocinado por Canonical, que incluye principalmente software libre y de código abierto. Puede utilizarse en ordenadores y servidores, está orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario.

## Capítulo 3

# Diseño e implementación

En este capítulo se presentan los detalles técnicos de diseño e implementación de la solución IoT que se tuvieron en cuenta durante el desarrollo del trabajo.

### 3.1. Arquitectura de software del sistema

El sistema cuenta con una arquitectura multi-cloud en la que se integra como hardware el robot de exploración ambiental [25] desarrollado en el marco de la Carrera de Especialización en Sistemas Embebidos, con un sistema *back-end* desplegado en la nube de Amazon Web Services [31], Smart Contracts desplegados en la red Blockchain Ethereum [54], y un plataforma analítica de datos desplegada en la nube de Azure [46] utilizando la herramienta Microsoft Fabric [47].

En la siguiente figura 3.1 podemos apreciar la arquitectura de la solución.

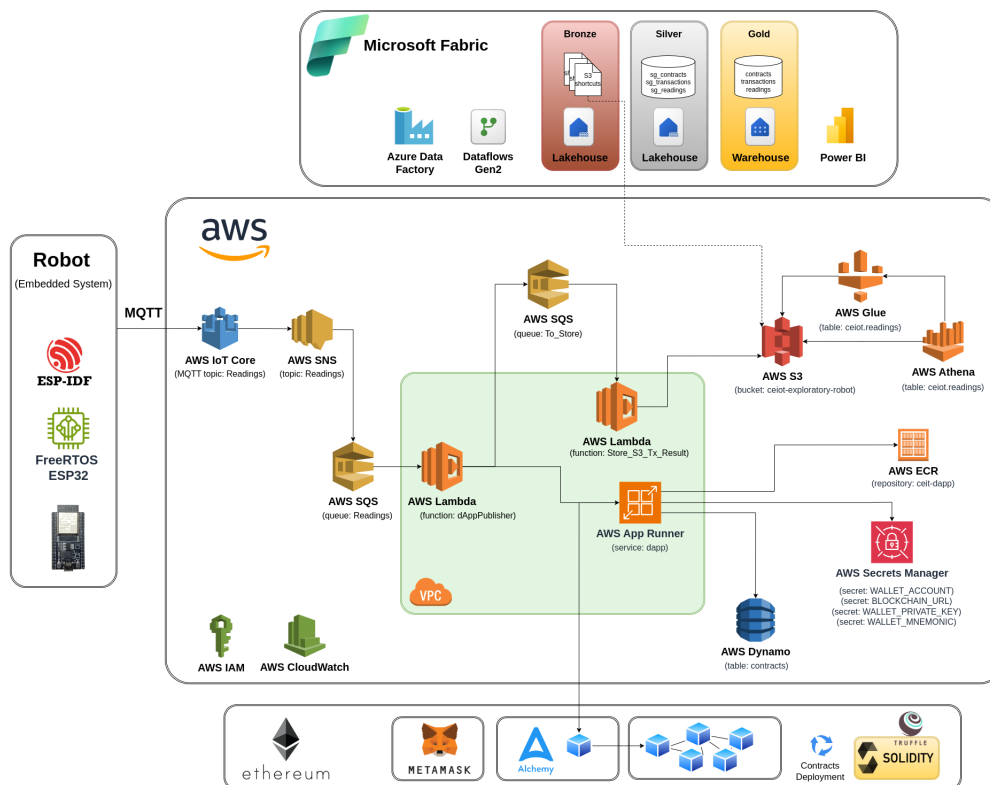


FIGURA 3.1. Arquitectura de la solución.

## 3.2. Hardware e infraestructura del sistema

<A desarrollar>

## 3.3. Integración de los módulos y subsistemas

### 3.3.1. Capa de percepción

El desarrollo e integración de los componentes de esta capa consistió en la adaptación del firmware desplegado en el robot explorador para extender sus funcionalidades y enviar las lecturas de parámetros ambientales al *topic* MQTT. Dentro de las funcionalidades que se le agregaron al robot explorador se encontraron:

- Capturar fecha y hora local del sistema.
- Generación de coordenadas geograficas (con datos *mock*).
- Conexión segura con tópico MQTT y envío de los datos generados.

La configuración de la fecha y hora se realizó por medio del uso del servicio SNTP [75] que permite la sincronización del hardware de una red con la fecha y hora provista por servicios externos en estandar en una zona horaria. Esta configuración se realizó incluyendo el encabezado **esp\_sntp.h** en el código del robot. Una vez realizado esto fue posible obtener la fecha y hora local invocando a la función *localtime*.

La generación de las coordenadas geograficas con datos *mock* se realizo mediante la generación de las ecuaciones 3.1 y 3.2 a continuación.

$$MockLat = \left( \frac{rand()}{RAND\_MAX} \right) (LAT\_MAX - LAT\_MIN) + LAT\_MIN \quad (3.1)$$

$$MockLong = \left( \frac{rand()}{RAND\_MAX} \right) (LONG\_MAX - LONG\_MIN) + LONG\_MIN \quad (3.2)$$

Finalmente, los datos capturados fueron enviados en formato JSON al tópico MQTT con la estructura de la tabla:

TABLA 3.1. Tabla de objetos AWS

Nombre del campo	Tipo del campo	Descripción
deviceId	string	Id del dispositivo
type	string	Tipo de lectura
value	string	Valor de la lectura
geoLat	string	Latitud geográfica
geoLong	string	Longitud geográfica
date	string	Fecha
time	string	Hora

A continuación podemos apreciar un valor de ejemplo del objeto JSON enviado por el robot:



```
{
    "deviceId": "12ad-dao23-ux23",
    "type": "Temperature",
    "value": "0.00",
    "geoLat": "-26.056772",
    "geoLong": "-64.014824",
    "date": "2025-04-1",
    "time": "11:23:59"
}
```

### 3.3.2. Capa de red

El desarrollo de los componentes de esta capa consistió en la publicación de un *topic* MQTT desde el servicio AWS IoT Core y la configuración de la lógica de redirección y almacenamiento de los mensajes recibidos en AWS S3.

Para la conexión segura con el tópico MQTT se configuró el servicio AWS IoT Core, donde se creó una nueva instancia de un dispositivo remoto con el nombre ESP32. Una vez creado este dispositivo se descargaron e instalaron en el código del robot los certificados listados a continuación:

- AmazonRootCA1.pem, renombrado a brokerCA.crt: Es la autoridad certificadora que AWS usa para firmar certificados de sus servidores. El dispositivo lo necesita para verificar la identidad del servidor AWS IoT al conectarse.
- dev-certificate.pem.crt, renombrado a client.crt: Contiene la clave pública correspondiente a la clave privada (.key) y está firmado por AWS (o por una CA en la que AWS confía) para verificar la identidad del dispositivo.
- dev-private.pem.key, renombrado a client.key: Usada por el dispositivo para firmar su identidad durante la conexión TLS. Nunca se comparte ni se sube a AWS. Tu dispositivo la usa para autenticar su certificado (.crt).

Una vez realizada la configuración del servicio AWS IoT core e integrado el robot con el tópico, se probó la recepción de lecturas con el cliente de prueba provisto por AWS suscrito al tópico *readings* como puede apreciarse en la figura 4.1.

Para el almacenamiento en AWS S3 de los mensajes recibidos, se configuró una *routing rule* o regla de redirección en AWS IoT Core, indicando mediante una consulta con sintaxis SQL, que todos los mensajes recibidos en el tópico *readings* deben almacenarse en el bucket S3 ceiot-exploratory-robot. En la figura 4.2 puede apreciarse esta configuración.

Como resultado de la configuración realizada, los mensajes recibidos en MQTT fueron redirigidos y almacenados en AWS S3 como puede apreciarse en la figura 4.11.

### 3.3.3. Capas de procesamiento y almacenamiento - dApp (AWS) y Smart Contracts

Uno de los primeros pasos para poder comenzar a desarrollar los componentes blockchain fue la obtención de tokens para poder realizar despliegues y ejecutar la aplicación en las redes de prueba de Ethereum sin utilizar fondos reales. Para poder realizar esto, primero fue necesario crear un *wallet* o billetera digital,

para lo que se utilizó el servicio Metamask. Luego, para la obtención de créditos se utilizaron los *faucets* de Google [76]. Como se puede apreciar en las figura 4.3 y tras seleccionar la dirección del *wallet* y 4.4, tras realizar las transacciones en el *faucet* se reciben los fondos en la billetera digital.

Posteriormente como podemos apreciar en la figura, en el servicio Etherscan las transacciones realizadas para generar fondos en la dirección de la billetera quedan publicadas en la red.

Una vez obtenidos los fondos de prueba en la billetera se procedió con el desarrollo de los componentes blockchain. Para el desarrollo de los *smart contracts* se utilizó Solidity como lenguaje de programación y Truffle como herramienta de gestión de configuración, compilación, empaquetado y despliegue. Truffle utiliza una configuración basada en archivos Javascript para la descripción de las tareas, y para realizar el despliegue a diferentes redes, como por ejemplo de forma local a Ganache o de forma remota a redes como Sepolia, Holesky y Mainnet. En la los archivos de configuración de Truffle se agregaron entradas para poder desplegar a Ganache y a Sepolia como se puede apreciar en la figura 3.2.

```
networks: {  
  development: {  
    host: "ganache", // Dirección de Ganache en el host local  
    port: 7545,      // Puerto donde Ganache está corriendo  
    network_id: "*", // Conecta a cualquier red  
  },  
  
  sepolia: {  
    provider: () => new HDWalletProvider(  
      MNEMONIC, // Frase secreta de MetaMask  
      `${BLOCKCHAIN_URL}` // URL RPC de la Red a la cual se despliega  
    ),  
    gas: 3000000, // Límite de gas  
    gasPrice: 5000000000, // 5 Gwei  
    network_id: 11155111, // ID de la red Sepolia  
    skipDryRun: true, // Evita correr una simulación en dry-run antes del despliegue  
  
    // confirmations: 2, // N° de confirmaciones antes de considerar la transacción válida  
    // timeoutBlocks: 200, // N° de bloques de espera antes de fallar  
  
    pollingInterval: 1800000,  
    disableConfirmationListener: true,  
  },  
}
```

FIGURA 3.2. Configuración de redes de despliegue en Truffle.

Como se puede apreciar en la figura 4.8, durante el proceso de despliegue se presenta cierta información por pantalla:

- La red a la cual se esta realizando el despliegue.
- Los *smart contracts* incluidos en el despliegue y la dirección que toman una vez desplegados.
- El *hash* o identificador de la transacción.
- El número de bloque en el que se encuentra la transacción de despliegue.
- La dirección de la billetera digital y el balance disponible previo a la transacción.
- La cantidad de gas utilizado en el despliegue, el costo unitario y el costo total de la transacción.

Luego de haber realizado el despliegue de los *smart contracts* a la red Sepolia, se puede evidenciar desde Etherscan las transacciones reportadas en la salida por

pantalla (figura 4.6) y comparar los valores. Como se puede apreciar en la figura 4.7, al ingresar a los detalles de la transacción podemos obtener mas información del contrato.

Desde el punto de vista del *backend* blockchain, se desarrolló la dApp utilizando Node.js y la biblioteca Javascript Web3.js para la comunicación con los *smart contracts*. Para la dApp, se desarrollaron varios *endpoints* y se expusieron mediante el estandar Open API [68] utilizando la biblioteca Swagger, que como se puede apreciar en la figura 4.9, genera una interfaz gráfica documenta y brinda un cliente de prueba para poder invocar los *endpoints* expuestos.

Para que la dApp pueda interactuar con la red debe poder conectarse a un endpoint RPC publicado desde cualquier nodo de la misma. Por este motivo se utilizó el servicio Alchemy que brinda publica endpoints para distintas redes, incluyendo Ethereum. Primero se creó un perfil en este servicio de manera gratuita y se creó un nuevo proyecto con el nombre `iot_robots_storage`. Una vez hecho esto se pudo acceder a los diferentes endpoints disponibles de Ethereum para las tres redes principales (Mainnet, Holesky y Sepolia) como se puede apreciar en la figura 4.10. Posteriormente, se configuró en la inicialización de la biblioteca Web3.js en la dApp, el endpoint provisto por Alchemy y el `app_key` del proyecto `iot_robots_storage`.

La dApp fue desplegada utilizando el servicio AWS App Runner por medio de la creación y publicación en AWS ECR de una imagen Docker con el código de la misma. Se configuró el despliegue de la dApp para que se encuentre en una VPC (red privada) con reglas que impiden el tráfico HTTP de ingreso desde la red pública, pero permiten el tráfico saliente, de esta manera la dApp puede acceder al servicio Alchemy e invocar los *Smart Contracts*.

Además de la URL y el key del proyecto en Alchemy, la dApp necesita ciertos datos sensibles para poder acceder a Ethereum, firmar transacciones, y realizar escrituras (ya que dichas operaciones requieren el pago de un fee). Estos datos al ser considerados sensibles, fueron almacenados en el servicio AWS Secret Manager, y accedidos a través del uso de su integración en los diferentes componentes. En la siguiente lista se pueden apreciar el propósito de los mismos:

- **Wallet Account:** identificador unívoco de una cuenta en la red de blockchain.
- **Wallet Mnemonic:** conjunto de entre 12 y 24 palabras que forman la semilla criptográfica para acceder (o recuperar la cuenta) y generar claves privadas, entre otras cosas.
- **Wallet Private Key:** Es generado mediante el Mnemonic, y es necesario para firmar transacciones de escritura.

### 3.3.4. Capas de distribución de eventos

Una vez configurados servicios AWS IoT Core y AWS AppRunner se procedió al despliegue de los componentes que permiten la distribución asíncrona de eventos desde el flujo de ingesta en tiempo real MQTT al posterior almacenamiento en blockchain de las lecturas y en S3 de los resultados de dichas transacciones. Para esto se configuraron los servicios AWS SNS y SQS para brindar, por medio de SNS, una interfaz pub/sub que permita la distribución en paralelo de los eventos

recibidos a los topicos suscriptos, y por medio de SQS, un encolamiento de eventos para cada suscriptor de forma que se pueda paralelizar el procesamiento de los eventos.

Dentro de la misma VPC donde se encuentra la dApp (en AWS App Runner) se desplegaron dos funciones AWS Lambda para la integración entre el flujo de lecturas ambientales, la dApp y el almacenamiento S3:

- **Send Reading to Blockchain (Python):** Implementa la lógica para recibir eventos provenientes de SQS, y construir el request que la dApp espera para poder invocar al Smart Contract pasando los datos como parámetros. Al invocar a la dApp espera la confirmación de la transacción en blockchain y cuando recibe la respuesta la envía a la cola ToStore para ser escrita en S3.
- **Write Readings and Transactions (Python):** Recibe de la cola ToStore la lectura y transacción confirmada, y posteriormente almacena ambos objetos en S3.

Desde el punto de vista de infraestructura, como AWS Lambda hace uso de los servicios SQS y S3, que se encuentran expuestos a la red pública, se configuraron AWS Endpoints para integrar la VPC con S3 y SQS de manera interna (sin pasar por la red pública).

### 3.3.5. Capas de procesamiento y almacenamiento de datos

Una vez realizadas las configuraciones de ingesta de datos en *streaming* se realizaron las configuraciones para poder accederlos, administrarlos y procesarlos de forma batch. Para ello se crearon una base de datos y una tabla en AWS Glue para representar el esquema de datos almacenados en AWS S3 en formato JSON, como se puede apreciar en la figura 3.3.

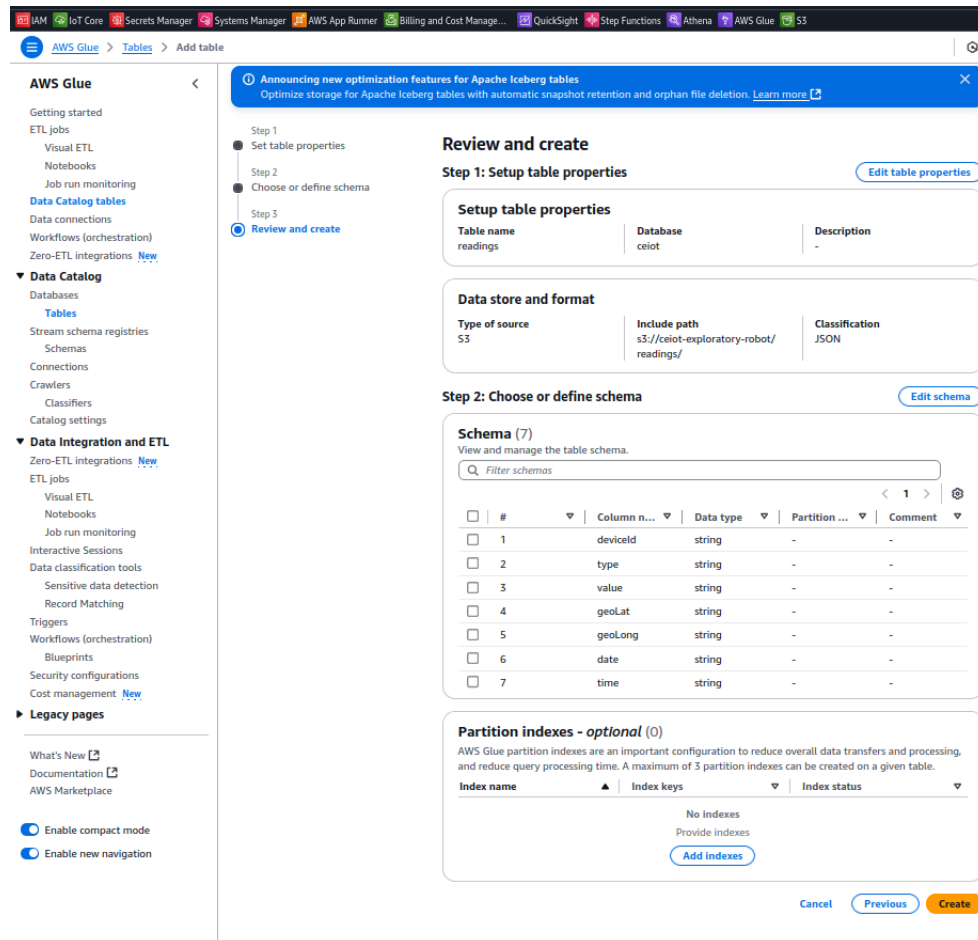


FIGURA 3.3. Creación de base datos, tabla y esquema AWS Glue.

Con el esquema de datos definido en el catálogo de AWS Glue, fue posible realizar consultas SQL sobre los datos almacenados en AWS S3 desde AWS Athena, como se puede apreciar en la figura

Para la capa de ingeniería de datos, procesamiento de analíticas y creación de reportes y dashboards, se decidió utilizar la suite de componentes provista por Microsoft Fabric en la nube de Azure. El diseño de la solución de datos implementada se basó en la arquitectura Medallion donde se implementaron las tres capas estándares (Bronze, Silver y Gold), y se almacenaron los datos en el Data Lake OneLake en formato Delta. La separación en capas se realizó de la siguiente manera:

- Capa Bronze: se integró el Fabric Lakehouse con el almacenamiento S3 mediante la configuración de *shortcuts*. Los datos se encontraron almacenados en crudo y con formato JSON.
- Capa Silver: se almacenaron y accedieron en el Fabric Lakehouse las tres diferentes entidades (contracts, transactions y readings) en formato de tablas Delta (con archivos Parquet), utilizando el lenguaje SQL a través del SQL Endpoint provisto por Lakehouse. En esta capa los datos se encuentran en estado *staging* en el cual sufren transformaciones y enriquecimiento para mejorar su calidad.
- Capa Gold: se almacenaron y accedieron en el Fabric Warehouse las tres diferentes entidades (contracts, transactions y readings) como tablas de un

modelo relacional SQL. En esta capa los datos se encuentran en su calidad final listos para poder ser entregados y consumidos desde herramientas de visualización y reportes.

El proceso de transformación de datos utilizado se basó principalmente en el uso de las herramientas Azure Data Factory y Dataflows Gen2. Con Azure Data Factory se diseñó la orquestación del procesamiento de datos y se utilizaron actividades de copiado y transformación de datos. En la siguiente figura 3.4 puede apreciarse el *data pipeline* en Azure Data Factory:

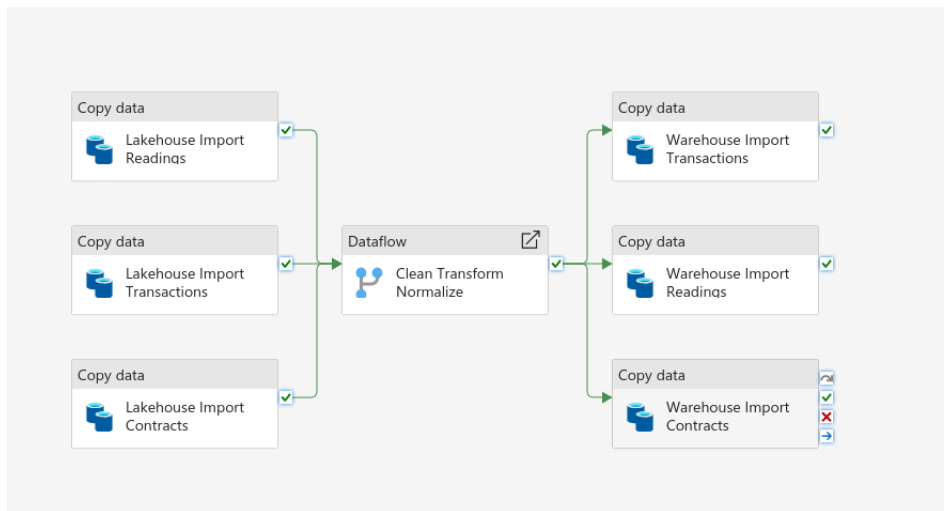


FIGURA 3.4. Azure Data Factory pipeline.

El flujo está estructurado de la siguiente manera:

- Las tres primeras actividades de movimiento de datos tienen como propósito la copia de datos desde AWS S3 a Fabric OneLake, transformando el formato de JSON crudo sin compresión a archivos Parquet con compresión Snappy (un 30 por ciento del tamaño original), con la generación y validación del esquema de datos al ser importado como tabla Delta dentro del LakeHouse. Esta actividad se realiza para las tres entidades (contracts, transactions, y readings).
- La siguiente actividad es la transformación y curado de los datos usando Dataflows Gen2. Los detalles de la misma se explican más abajo.
- Finalmente, las últimas tres actividades son el movimiento de los datos curados en el Lakehouse a la capa Gold en el Warehouse, donde ya se encuentran listos para ser utilizados en el Semantic Model de PowerBI.

Para la transformación y limpieza de datos se instanció el componente Dataflows Gen2 desde Azure Data Factory. Posteriormente desde la interfaz de la herramienta Dataflows se configuraron las diferentes actividades de transformación y curado de datos para cada una de las entidades procesadas. En la siguiente figura 3.5 podemos apreciar la orquestación de estas transformaciones desde Dataflows:

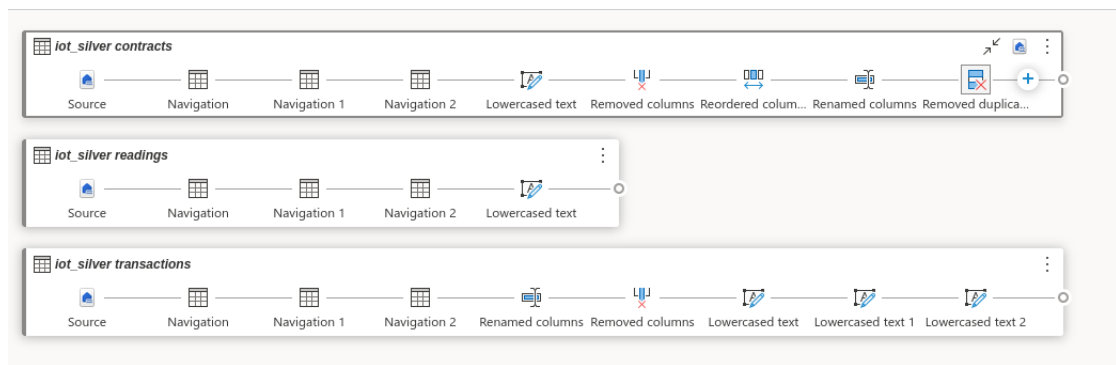


FIGURA 3.5. Dataflows pipeline.

Como podemos apreciar se aplican diferentes transformaciones dependiendo de la entidad. Las transformaciones realizadas fueron la transformación de los datos a lowercase para algunas columnas con el fin de poder ser cruzadas adecuadamente con las otras entidades, la eliminación de ciertas columnas innecesarias que solo consumen espacio y no resultan de interés para los reportes finales, el reordenamiento de las columnas para la presentación final, y el renombrado de algunas columnas para estandarizar el acceso.

Una vez en el data Warehouse en su capa Gold se creó un Semantic Model de Power BI para poder representar los datos en los reportes. Luego se establecieron las relaciones entre las tres entidades y se crearon ciertas métricas adicionales para poder facilitar el cálculo dinámico de valores en los dashboards. En la siguiente figura 3.6 podemos apreciar una imagen del mismo:

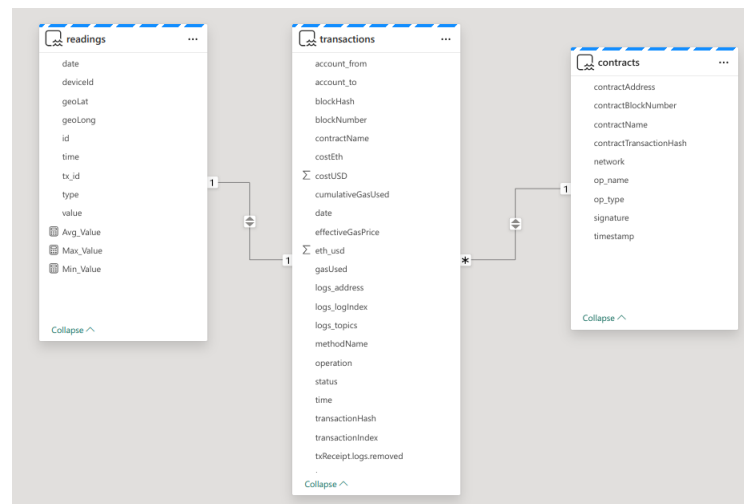


FIGURA 3.6. Modelo semántico de PowerBI.

Las métricas creadas fueron:

- Readings - Avg Value (valor promedio)
- Readings - Max Value (valor máximo)
- Readings - Min Value (valor mínimo)

Finalmente desde PowerBI se construyeron los reportes compuestos por tablas dinámicas y graficos. Como los datos fueron relacionados en el Semantic Model, al seleccionar valores en el reporte se realiza dinámicamente un filtrado lo cual

permite el análisis de la información para la toma de decisiones. En la siguientes figuras 4.14 podemos apreciar algunas capturas de algunos de los dashboards generados:

### 3.4. Plataforma de desarrollo y despliegue

### 3.5. Tabla de todos los objetos cloud creados

TABLA 3.2. Tabla de objetos AWS

Servicio	Propósito	Nombre de objeto
AWS IoT Core	<i>Thing</i>	ESP32
AWS IoT Core	<i>MQTT topic</i>	readings
AWS IoT Core	<i>Routing Rule</i>	StoreToS3
AWS S3	Bucket	ceiot-exploratory-robot
AWS Glue	Base de datos	ceit
AWS Glue	Tabla	<i>Readings</i>



## Capítulo 4

# Ensayos y resultados

Todos los capítulos deben comenzar con un breve párrafo introductorio que indique cuál es el contenido que se encontrará al leerlo. La redacción sobre el contenido de la memoria debe hacerse en presente y todo lo referido al proyecto en pasado, siempre de modo impersonal.

### 4.1. Verificaciones funcionales del hardware

#### 4.1.1. Verificación del proceso de ingesta en tiempo real MQTT

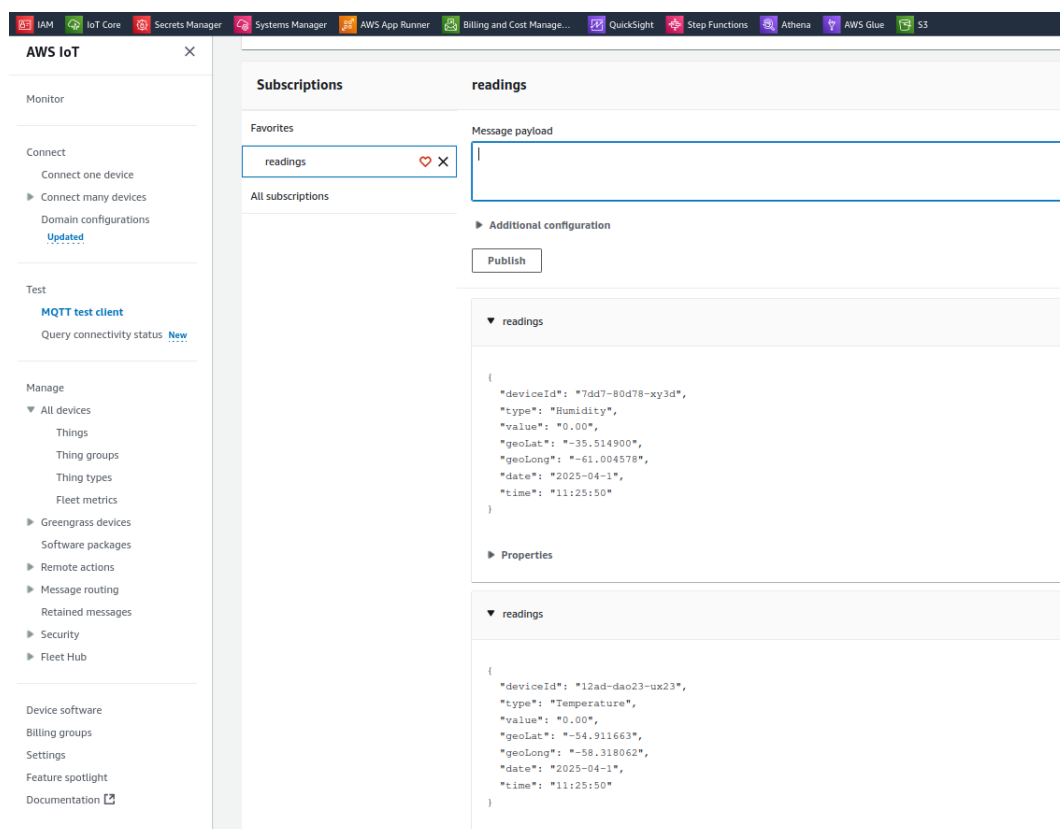


FIGURA 4.1. Prueba de recepción de mensajes MQTT.

### 4.1.2. Verificación del proceso de distribución de eventos en AWS

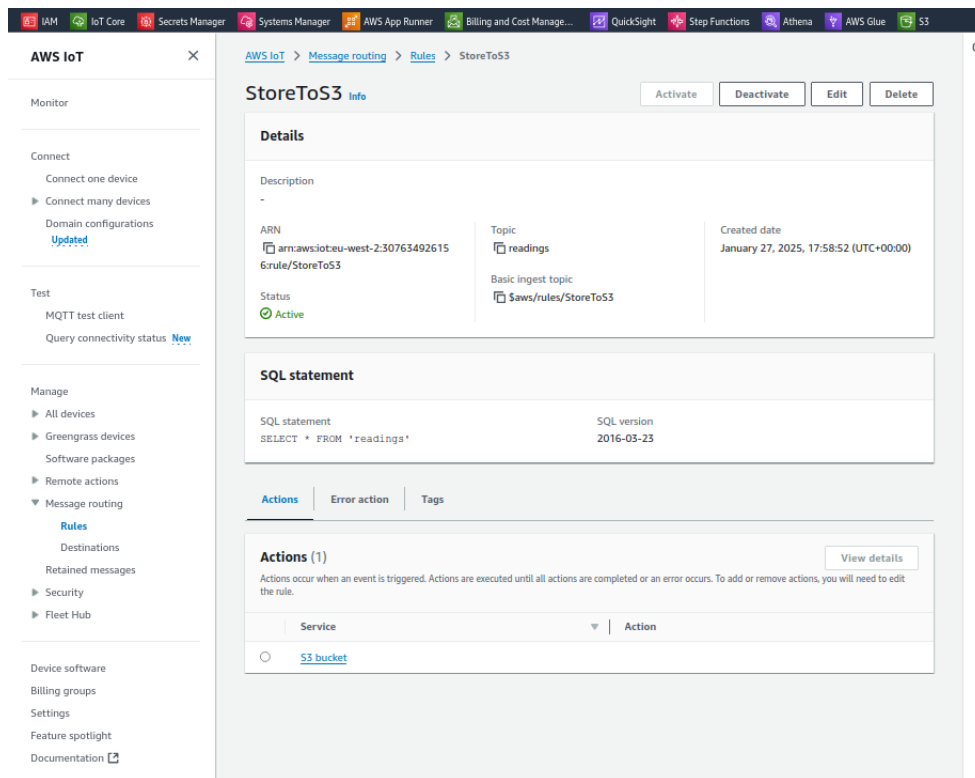


FIGURA 4.2. Configuración de redirección de mensajes MQTT.

### 4.1.3. Verificación de fondos necesarios para realizar despliegues en redes Holesky y Sepolia

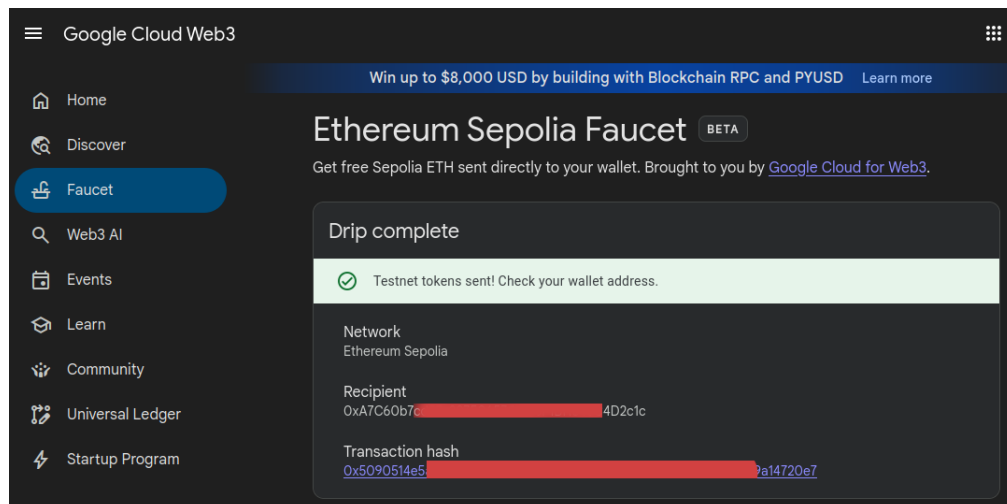


FIGURA 4.3. Obtención de créditos mediante Google Web3.

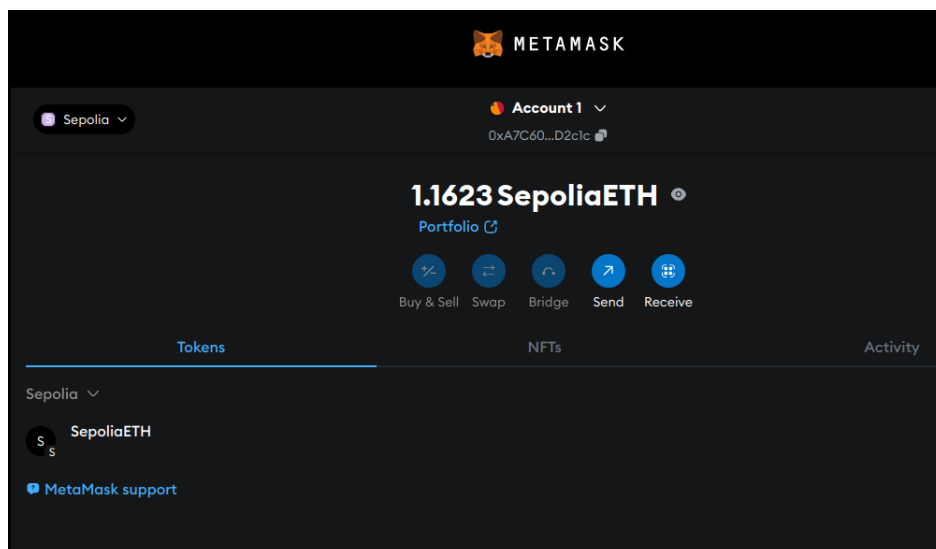


FIGURA 4.4. Saldo en Metamask.

Etherscan

Search by Address / Txn Hash / Block / Token

Home Blockchain Tokens NFTs More

Transactions

For 0xA7C60b7c...48C4D2c1c

A total of 27 transactions found

Download Page Data First Page 1 of 1 Last

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0x5090514e5a...	Transfer	8133551	5 mins ago	0xAFEDA61d...b37Bb5E4a	0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00000002
0xa3f98afe66...	Transfer	8111372	3 days ago	0x52f1984C...2E7aCEdD	0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00000002
0x5cc12c442d...	Transfer	8038092	14 days ago	0x52f1984C...2E7aCEdD	0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00000002
0x29be715ca1...	Transfer	7995217	20 days ago	0xC0f3838B...aA36Ab588	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00000007
0x3d1a82a920f...	Transfer	7964066	24 days ago	0x993a0f36...63293adD9	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00000011
0xc8e20e15db...	Transfer	7935605	28 days ago	0xAFEDA61d...b37Bb5E4a	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00002413
0x7d7b70ae03...	Transfer	7922748	30 days ago	0x6FB29CE...3D36bC033	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00000008
0x0883bd4e57...	Transfer	7880940	36 days ago	0x6FB29CE...3D36bC033	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00153677
0x8f864fb2f68...	Transfer	7866011	38 days ago	0x9a0C272b...EcB561d55	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00487357
0xd6cfd63b84...	Transfer	7852978	40 days ago	0x993a0f36...63293adD9	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00000005
0x0fec12e92d9...	Transfer	7838873	42 days ago	0x993a0f36...63293adD9	0xA7C60b7c...48C4D2c1c	0.03 ETH	0.00000079
0x952b824890...	Transfer	7831282	43 days ago	0x52f1984C...2E7aCEdD	0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00077191
0xb1dc431d34...	Transfer	7810363	46 days ago	0x15095Ec8...158ACe7aD	0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00007301
0x05ef85faf4...	Transfer	7792317	49 days ago	0xe560A09...1Ad101e47	0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00000655
0xe3e133543c...	Transfer	7784330	50 days ago	0x6FB29CE...3D36bC033	0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00030265

FIGURA 4.5. Transacciones de generación de fondos de prueba.

Sepolia Testnet

Search by Address / Txn Hash / Block / Token

Etherscan

Home Blockchain Tokens NFTs More

Address 0xA7C60b7...4D2c1c

Overview

ETH BALANCE

1.152988951990234204 ETH

More Info

TRANSACTIONS SENT

Latest: 23 hrs ago First: 61 days ago

FUNDED BY

0xAfEDA61d...b37Bb5E4a at txn 0x5086ac3565...

Multichain Info

N/A

Transactions Token Transfers (ERC-20)

Latest 25 from a total of 47 transactions

Download Page Data

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0xbcf4ae23825...	0x50806040	8133742	23 hrs ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00052838
0x22ab2c5826...	0x50806040	8133741	23 hrs ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00463312
0x7079452757...	0x50806040	8133740	23 hrs ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00145501
0x6976c05b07...	0x50806040	8133739	23 hrs ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00182386
0xb107df1d35a...	0x50806040	8133738	23 hrs ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00081972
0x5090514e5a...	Transfer	8133551	23 hrs ago	0xAfEDA61d...b37Bb5E4a	IN 0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00000002
0xa3f98aefe66...	Transfer	8111372	4 days ago	0x52f1984C...2E7aCEeD	IN 0xA7C60b7c...48C4D2c1c	0.05 ETH	0.00000002
0xf64909978b6...	0x50806040	8111364	4 days ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00062838
0x2872c024bc...	0x50806040	8111363	4 days ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00463312
0x53cf34ba1c6...	0x50806040	8111362	4 days ago	0xA7C60b7c...48C4D2c1c	OUT Contract Creation	0 ETH	0.00145501

FIGURA 4.6. Transacciones de despliegue en Sepolia.

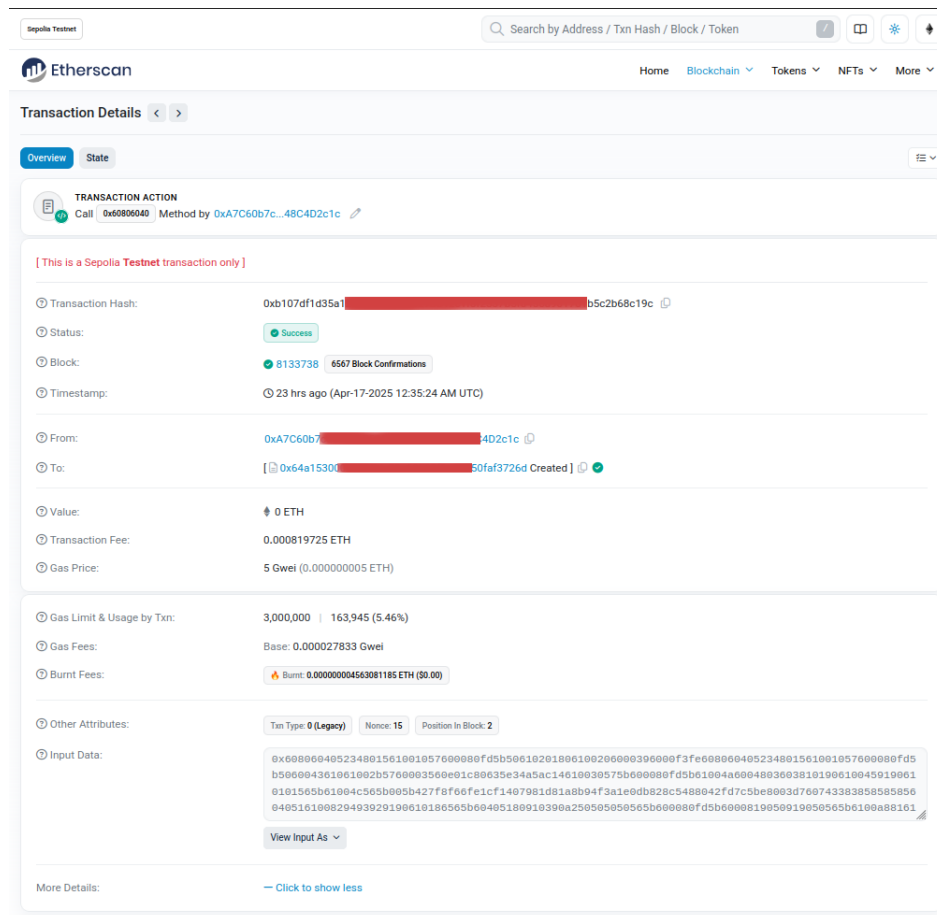


FIGURA 4.7. Detalles del contrato desplegado en Sepolia.

#### 4.1.4. Verificación del proceso de despliegue de los Smart Contracts

```
oc-ethereum-smart-contracts-deployer
oc-ethereum-smart-contracts-deployer
=====
> Compiling ./contracts/EnvironmentalDataStoredSingle.sol
> Artifacts written to /app/build/contracts
> Compiled successfully using:
   - solc: 0.8.17+commit.8df45f5f.Emscripten.clang

Starting migrations...
=====
> Network name: 'sepolia'
> Network id: 11155111
> Block gas limit: 35999965 (0x22550dd)

2 deploy_storage.js
=====
Contrato: EnvironmentalData
Contrato: EnvironmentalDataStoredMulti
Contrato: EnvironmentalDataStoredSingle
Contrato: Registry
Contrato: Storage

Replacing 'EnvironmentalData'
-----
> transaction hash: 0xb107dfd1d35a1 [REDACTED] b5c2b68c19c
> Blocks: 0 Seconds: 4
> contract address: 0x64A15300E [REDACTED] 0FaF3726D
> block number: 8133738
> block timestamp: 1744850124
> account: 0xA7C60b7 [REDACTED] 4D2c1c
> balance: 1.161529341990234204
> gas used: 163945 (0x28069)
> gas price: 5 gwei
> value sent: 0 ETH
> total cost: 0.000819725 ETH

Contrato EnvironmentalData desplegado con éxito

Enable Watch

oc-ethereum-smart-contracts-deployer
oc-ethereum-dapp
oc-ethereum-dapp
oc-ethereum-dapp
oc-ethereum-dapp
Registro de Storage en la Registry
Adding EnvironmentalData: 0x64A15300E [REDACTED] aF3726D to the Registry
Current Registry: [
  [ 'EnvironmentalData', '0x64A15300E [REDACTED] aF3726D' ]
```

FIGURA 4.8. Salida por pantalla durante el proceso de despliegue de los componentes blockchain.

#### 4.1.5. Verificación del proceso de despliegue de la dApp

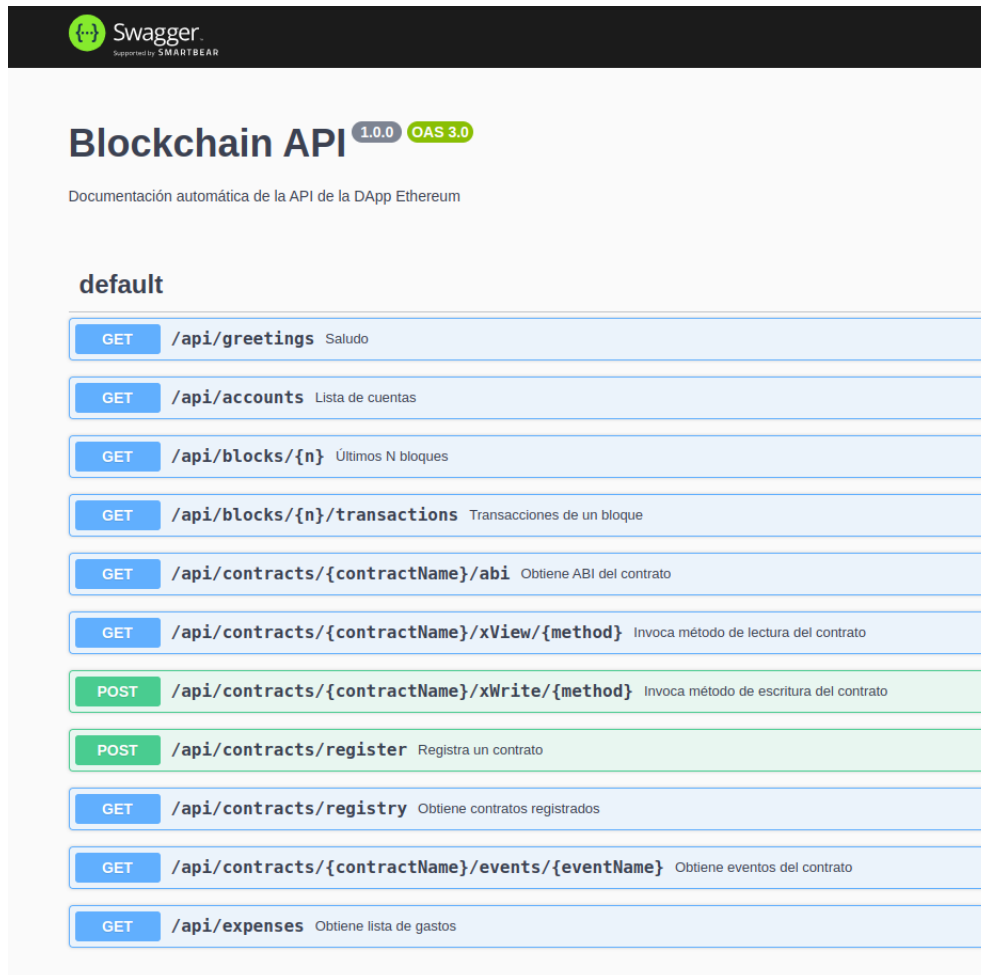


FIGURA 4.9. Endpoints expuestos por la dApp.

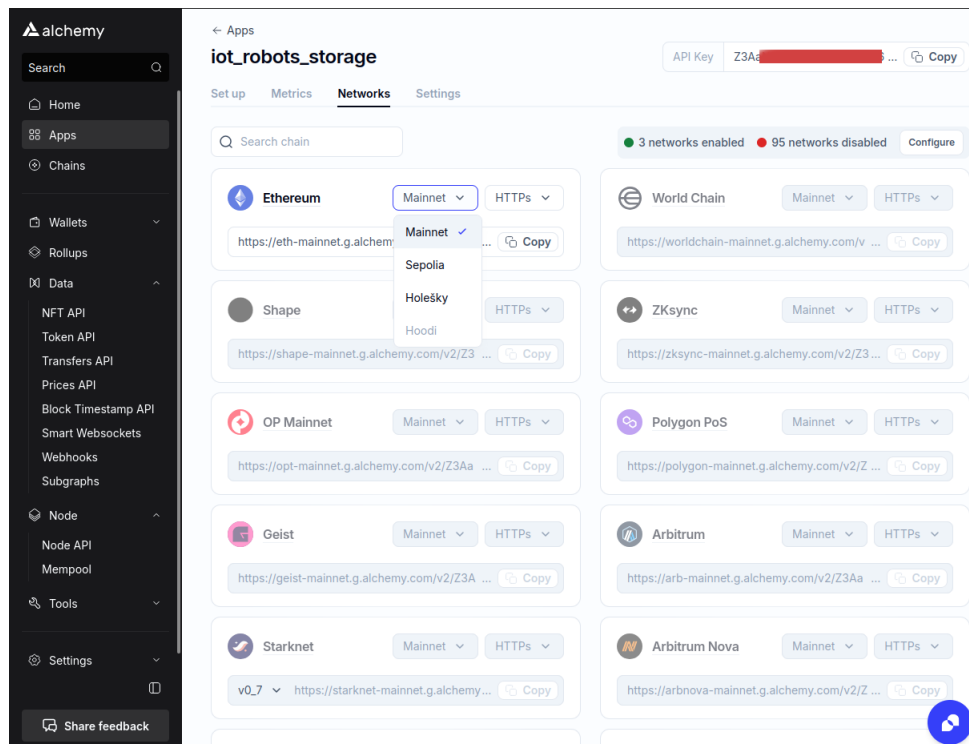


FIGURA 4.10. Frontend the Alchemy.

#### 4.1.6. Verificación del proceso de invocación de la dApp

#### 4.1.7. Verificación del proceso de invocación de los Smart Contracts

#### 4.1.8. Validación de los datos almacenados en Ethereum

#### 4.1.9. Verificación del proceso de almacenamiento de readings, transacciones y contracts en AWS S3

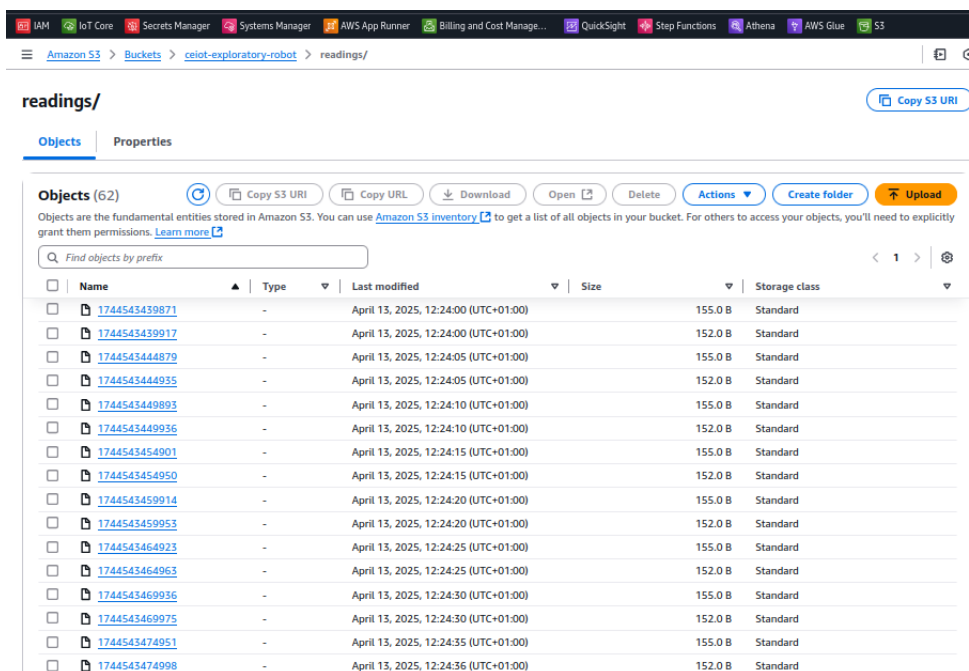


FIGURA 4.11. Almacenamiento de mensajes JSON en AWS S3.

The screenshot displays the Amazon Athena Query Editor interface. On the left, the 'Data' sidebar shows the 'Data source' as 'AwsDataCatalog', 'Catalog' as 'None', and 'Database' as 'celiot'. Under 'Tables and views', the 'readings' table is listed with columns: deviceid (string), type (string), value (string), geolat (string), geolong (string), date (string), and time (string). The main query editor shows a SQL query: `SELECT * FROM "celiot"."readings" limit 10;`. Below the query, the 'Query results' tab is active, showing a 'Completed' status with 'Time in queue: 53 ms', 'Run time: 433 ms', and 'Data scanned: 2.39 KB'. The results are displayed in a table with 10 rows.

#	deviceid	type	value	geolat	geolong	date	time
1	7dd7-80d78-xy3d	Humidity	0.00	-45.717163	-61.777348	2025-04-1	11:31:15
2	7dd7-80d78-xy3d	Humidity	0.00	-36.352222	-65.046944	2025-04-1	11:36:26
3	12ad-dao23-ux23	Temperature	0.00	-35.784000	-71.102203	2025-04-1	11:35:56
4	7dd7-80d78-xy3d	Humidity	0.00	-41.742722	-69.702713	2025-04-1	11:34:06
5	7dd7-80d78-xy3d	Humidity	0.00	-23.279711	-55.434586	2025-04-1	11:32:00
6	7dd7-80d78-xy3d	Humidity	0.00	-23.434233	-60.921886	2025-04-1	11:31:40
7	12ad-dao23-ux23	Temperature	0.00	-42.208134	-53.416115	2025-04-1	11:34:41
8	12ad-dao23-ux23	Temperature	0.00	-49.427284	-67.410004	2025-04-1	11:31:55
9	12ad-dao23-ux23	Temperature	0.00	-26.143887	-55.305141	2025-04-1	11:33:30
10	7dd7-80d78-xy3d	Humidity	0.00	-28.351419	-69.764854	2025-04-1	11:31:25

FIGURA 4.12. Consulta de datos SQL desde AWS Athena.



#### 4.1.10. Verificación del proceso de ingesta y transformación de datos batch en Fabric

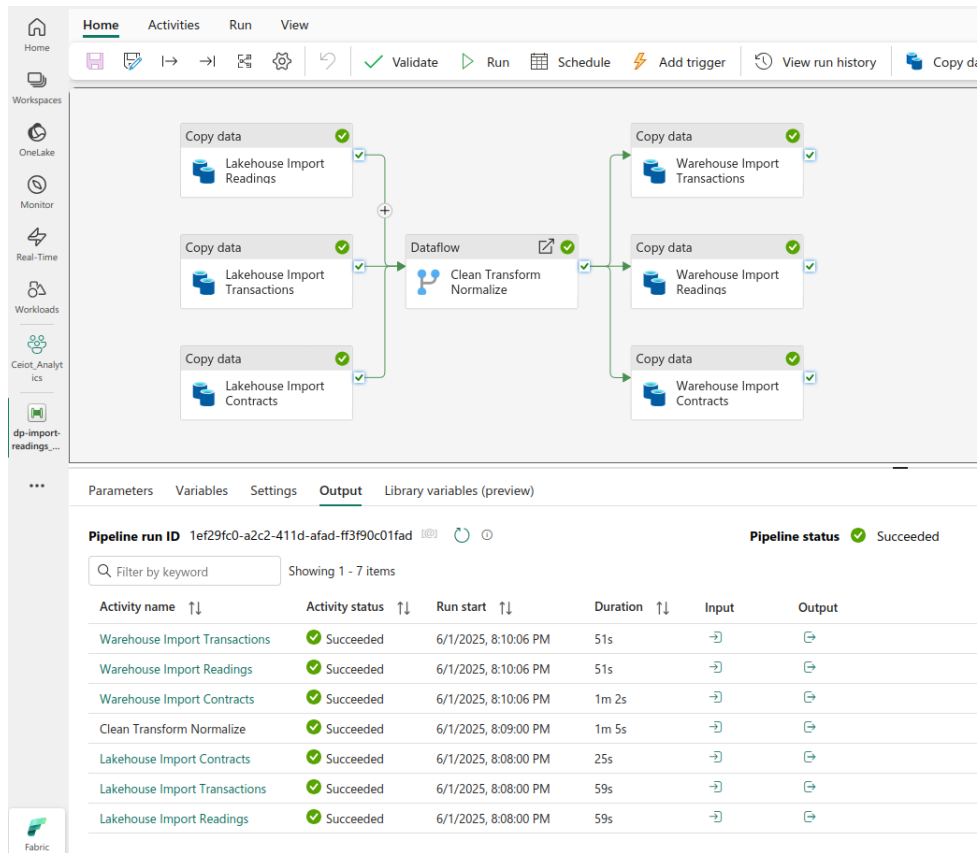


FIGURA 4.13. Correcta ejecución del pipeline punta-a-punta con Azure Data Factory y Dataflows.

#### 4.1.11. Validación del modelo de datos en el Semantic Model

#### 4.1.12. Validación del reporte final generado en PowerBI

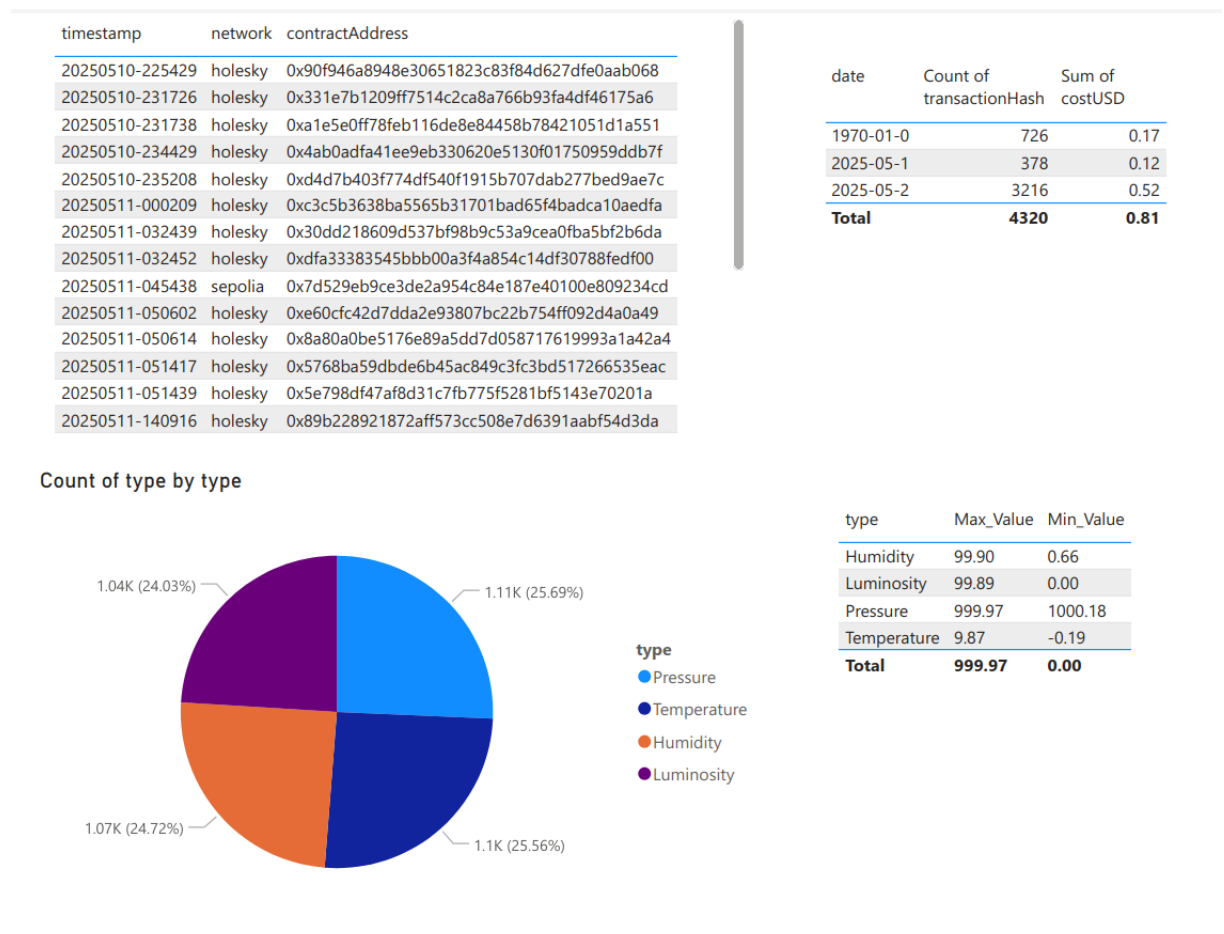


FIGURA 4.14. Dashboard PowerBI.

## 4.2. Pruebas funcionales del hardware

## Capítulo 5

# Conclusiones

Todos los capítulos deben comenzar con un breve párrafo introductorio que indique cuál es el contenido que se encontrará al leerlo. La redacción sobre el contenido de la memoria debe hacerse en presente y todo lo referido al proyecto en pasado, siempre de modo impersonal.

### 5.1. Conclusiones generales

La idea de esta sección es resaltar cuáles son los principales aportes del trabajo realizado y cómo se podría continuar. Debe ser especialmente breve y concisa. Es buena idea usar un listado para enumerar los logros obtenidos.

En esta sección no se deben incluir ni tablas ni gráficos.

Algunas preguntas que pueden servir para completar este capítulo:

- ¿Cuál es el grado de cumplimiento de los requerimientos?
- ¿Cuán fielmente se pudo seguir la planificación original (cronograma incluido)?
- ¿Se manifestó algunos de los riesgos identificados en la planificación? ¿Fue efectivo el plan de mitigación? ¿Se debió aplicar alguna otra acción no contemplada previamente?
- Si se debieron hacer modificaciones a lo planificado ¿Cuáles fueron las causas y los efectos?
- ¿Qué técnicas resultaron útiles para el desarrollo del proyecto y cuáles no tanto?

### 5.2. Próximos pasos

Acá se indica cómo se podría continuar el trabajo más adelante.



# Bibliografía

- [1] Wikipedia. *Wi-Fi*. URL: <https://es.wikipedia.org/wiki/Wifi>.
- [2] Wikipedia. *5G*. URL: <https://es.wikipedia.org/wiki/5G>.
- [3] Wikipedia. *LoraWAN*. URL: <https://es.wikipedia.org/wiki/LoRaWAN>.
- [4] Wikipedia. *Bluetooth*. URL: <https://en.wikipedia.org/wiki/Bluetooth>.
- [5] Wikipedia. *Zigbee*. URL: <https://en.wikipedia.org/wiki/Zigbee>.
- [6] Wikipedia. *Narrowband IoT*. URL: [https://en.wikipedia.org/wiki/Narrowband\\_IoT](https://en.wikipedia.org/wiki/Narrowband_IoT).
- [7] Amazon Web Service. *AWS Athena*. URL: <https://aws.amazon.com/iot-core/>.
- [8] Azure. *Azure IoT Hub*. URL: <https://azure.microsoft.com/en-gb/products/iot-hub>.
- [9] As.com | Marc Fontrodona. *Una estación de esquí china despliega una patrulla de perros robot*. URL: [https://as.com/deportes\\_accion/snow/una-estacion-de-esqui-china-despliega-una-patrulla-de-perros-robot-n](https://as.com/deportes_accion/snow/una-estacion-de-esqui-china-despliega-una-patrulla-de-perros-robot-n).
- [10] Cadenaser.com | Radio Bilbao. *Bilbao inspecciona sus redes de saneamiento con drones y robots para mejorar la eficiencia y la seguridad*. URL: <https://cadenaser.com/euskadi/2024/12/18/bilbao-inspecciona-sus-redes-de-saneamiento-con-drones-y-robots-para-mejorar-la-eficiencia-y-la-seguridad-radio-bilbao/>.
- [11] Los40.com | Dani Cabezas. *Así se gestiona un “tecnobosque”*. URL: <https://los40.com/2024/12/10/asi-se-gestiona-un-tecnobosque/>.
- [12] Boston Dynamics. *Spot*. URL: <https://www.bostondynamics.com/products/spot>.
- [13] Waygate Technologies. *BIKE - An advanced crawler robot for remote visual inspection*. URL: <https://www.bakerhughes.com/waygate-technologies/robotic-inspection/bike>.
- [14] Latam Mining. *Robots y minería: Gobierno argentino quiere implementarlos*. URL: <https://www.latam-mining.com/robots-y-mineria-gobierno-argentino-quiere-implementarlos/>.
- [15] Diario de Cuyo. *Gobierno pone la mira en el desarrollo de robots para la actividad minera*. URL: <https://www.diariodecuyo.com.ar/politica/Gobierno-pone-la-mira-en-el-desarrollo-de-robots-para-la-actividad-minera-20200202-0052.html>.
- [16] Universidad Nacional de San Juan. *Robots en la minería*. URL: [http://www.unsj.edu.ar/home/noticias\\_detalle/4810/1](http://www.unsj.edu.ar/home/noticias_detalle/4810/1).
- [17] Ing. Nelson Dario García Hurtado e Ing. Melvin Andrés González Pino. *Robot de exploración terrestre Geobot*. URL: [https://www.unipamplona.edu.co/unipamplona/portallG/home\\_40/recursos/01\\_general/revista\\_1/09102011/v01\\_09.pdf](https://www.unipamplona.edu.co/unipamplona/portallG/home_40/recursos/01_general/revista_1/09102011/v01_09.pdf).
- [18] Ing. Hernán L. Helguero Velásquez1 e Ing. Rubén Medinaceli Tórrez. *Robot Minero: Sistema Detector de Gases utilizando Sensores en Tiempo Real MIN – SIS 1.0 SDG-STR*. URL: [http://www.scielo.org.bo/scielo.php?script=sci\\_arttext&pid=S2519-53522020000100003](http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2519-53522020000100003).

- [19] Wikipedia. *Blockchain*. URL: <https://en.wikipedia.org/wiki/Blockchain>.
- [20] Wikipedia. *Smart Contracts*. URL: [https://en.wikipedia.org/wiki/Smart\\_contract](https://en.wikipedia.org/wiki/Smart_contract).
- [21] Wikipedia. *DApp - Decentralized Application*. URL: [https://en.wikipedia.org/wiki/Decentralized\\_application](https://en.wikipedia.org/wiki/Decentralized_application).
- [22] Walmart | Global Tech. *Blockchain in the food supply chain - What does the future look like?* URL: [https://tech.walmart.com/content/walmart-global-tech/en\\_us/blog/post/blockchain-in-the-food-supply-chain.html?utm\\_source=chatgpt.com](https://tech.walmart.com/content/walmart-global-tech/en_us/blog/post/blockchain-in-the-food-supply-chain.html?utm_source=chatgpt.com).
- [23] ledgerinsights | Nicky Morris. *ScanTrust's anti-counterfeit solution isn't just about blockchain*. URL: <https://www.ledgerinsights.com/scantrust-anti-counterfeit-blockchain/>.
- [24] Paula Eiroa Interempresas | Julio Lema. *Mejorar la eficiencia energética con IoT y blockchain*. URL: <https://www.interempresas.net/Energia/Articulos/446423-Mejorar-la-eficiencia-energetica-con-IoT-y-blockchain.html>.
- [25] Esp. Ing. Gonzalo Carreño. *LSE-FIUBA - Trabajo Final CESE- Robot de exploración ambiental*. URL: <https://lse-posgrados-files.fi.uba.ar/tesis/LSE-FIUBA-Trabajo-Final-CESE-Gonzalo-Carreno-2024.pdf>.
- [26] Amazon Web Services. *¿Qué es una nube pública?* URL: <https://aws.amazon.com/es/what-is/public-cloud/>.
- [27] OASIS. *MQTT Protocol Specification*. URL: <https://mqtt.org/mqtt-specification/>.
- [28] Espressif. *ESP-IDF Programming Guide | Get Started*. URL: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/get-started/>.
- [29] Espressif. *ESP32*. URL: <https://www.espressif.com/en/products/socs/esp32>.
- [30] FreeRTOS. *FreeRTOS | Real-time operating system for microcontrollers and small microprocessors*. URL: <https://www.freertos.org/>.
- [31] Amazon Web Service. *Amazon Web Service*. URL: <https://aws.amazon.com/>.
- [32] Amazon Web Service. *AWS Athena*. URL: <https://aws.amazon.com/apprunner/>.
- [33] Docker. *Docker*. URL: <https://docker.com/>.
- [34] Amazon Web Service. *AWS Glue*. URL: <https://aws.amazon.com/glue/>.
- [35] Amazon Web Service. *AWS Athena*. URL: <https://aws.amazon.com/s3/>.
- [36] Amazon Web Service. *AWS Athena*. URL: <https://aws.amazon.com/athena/>.
- [37] Amazon Web Service. *AWS SNS*. URL: <https://aws.amazon.com/sns/>.
- [38] Amazon Web Service. *AWS SQS*. URL: <https://aws.amazon.com/sqs/>.
- [39] Amazon Web Service. *AWS Secrets Manager*. URL: <https://aws.amazon.com/secrets-manager/>.
- [40] Amazon Web Service. *AWS Lambda*. URL: <https://aws.amazon.com/lambda/>.
- [41] Amazon Web Service. *AWS Dynamo*. URL: <https://aws.amazon.com/dynamodb/>.
- [42] Amazon Web Service. *AWS IAM*. URL: <https://aws.amazon.com/iam/>.
- [43] Wikipedia. *ABAC*. URL: [https://en.wikipedia.org/wiki/Attribute-based\\_access\\_control](https://en.wikipedia.org/wiki/Attribute-based_access_control).
- [44] Wikipedia. *MFA*. URL: [https://en.wikipedia.org/wiki/Multi-factor\\_authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication).
- [45] Amazon Web Service. *AWS CloudWatch*. URL: <https://aws.amazon.com/cloudwatch/>.

- [46] Microsoft. *Microsoft Azure*. URL: <https://azure.microsoft.com/>.
- [47] Microsoft. *Microsoft Fabric | Fundamentals*. URL: <https://learn.microsoft.com/en-us/fabric/>.
- [48] Microsoft. *Fabric | Data Lakehouse*. URL: <https://learn.microsoft.com/en-us/fabric/data-engineering/lakehouse-overview>.
- [49] Microsoft. *Fabric | Data Warehouse*. URL: <https://learn.microsoft.com/en-us/fabric/data-warehouse/data-warehousing>.
- [50] Microsoft. *Fabric | Azure Data Factory*. URL: <https://learn.microsoft.com/en-us/fabric/data-factory/data-factory-overview>.
- [51] Microsoft. *Fabric | Dataflows (Gen2)*. URL: <https://learn.microsoft.com/en-us/fabric/data-factory/dataflows-gen2-overview>.
- [52] Microsoft. *Fabric | Power BI*. URL: <https://learn.microsoft.com/en-us/power-bi/fundamentals/fabric-power-bi>.
- [53] Microsoft. *Fabric | OneLake*. URL: <https://learn.microsoft.com/en-us/fabric/onelake/onelake-overview>.
- [54] Ethereum.org. *Welcome to Ethereum*. URL: <https://ethereum.org/>.
- [55] Ethereum.org. *Ethereum Virtual Machine (EVM)*. URL: <https://ethereum.org/en/developers/docs/evm/>.
- [56] Truffle Suite. *Truffle | What is Truffle?* URL: <https://etherscan.io/>.
- [57] Truffle Suite. *Truffle | What is Truffle?* URL: <https://sepolia.etherscan.io/>.
- [58] Truffle Suite. *Truffle | What is Truffle?* URL: <https://holesky.etherscan.io/>.
- [59] Soliditylang.org. *Contract ABI Specification*. URL: <https://docs.soliditylang.org/en/latest/abi-spec.html>.
- [60] Web3.js. *Web3.js - Ethereum JavaScript API*. URL: <https://web3js.readthedocs.io/en/v1.10.0/>.
- [61] Wikipedia. *Proof of Stake*. URL: [https://en.wikipedia.org/wiki/Proof\\_of\\_stake](https://en.wikipedia.org/wiki/Proof_of_stake).
- [62] Truffle Suite. *Ganache | One click blockchain*. URL: <https://archive.trufflesuite.com/ganache/>.
- [63] Truffle Suite. *Truffle | What is Truffle?* URL: <https://archive.trufflesuite.com/docs/truffle/>.
- [64] Alchemy. *Alchemy | The most reliable way to build web3 apps*. URL: <https://www.alchemy.com/>.
- [65] Etherscan. *Etherscan*. URL: <https://etherscan.io/>.
- [66] Metamask. *Metamask | Your home in Web3*. URL: <https://metamask.io/>.
- [67] Node.js. *Node.js*. URL: <https://nodejs.org/en>.
- [68] swagger.io. *Open API Specification*. URL: <https://swagger.io/specification/>.
- [69] soliditylang.org. *Solidity programming language*. URL: <https://soliditylang.org/>.
- [70] Github. *Github*. URL: <https://github.com/>.
- [71] Amazon Web Services. *AWS CodePipeline*. URL: <https://aws.amazon.com/codepipeline/>.
- [72] Amazon Web Services. *AWS Elastic Container Registry*. URL: <https://aws.amazon.com/ecr/>.
- [73] Visualstudio. *Visualstudio Code*. URL: <https://code.visualstudio.com/>.
- [74] Ubuntu. *Ubuntu*. URL: <https://ubuntu.com/>.
- [75] IBM Documentation. *Simple Network Time Protocol*. URL: <https://www.ibm.com/docs/en/i/7.4.0?topic=services-simple-network-time-protocol>.
- [76] Google. *Google Cloud Web3*. URL: <https://cloud.google.com/application/web3/faucet>.