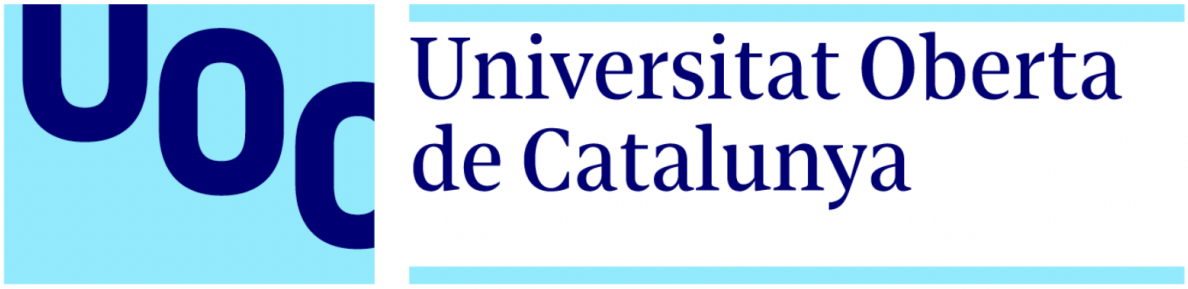


Máster en Ingeniería de Telecomunicación

Área de Sistemas de Comunicación

Curso académico 2023-2024

Trabajo Fin de Máster

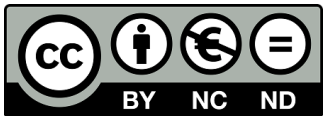
“Aplicación de tecnología blockchain para la gestión descentralizada de los servicios en un despliegue de coalición federada ”

Jorge Álvaro González

Tutor

Víctor Monzón Baeza

FECHA: Junio de 2024



FICHA DEL TRABAJO FINAL

Título del trabajo	Aplicación de tecnología blockchain para la gestión descentralizada de los servicios en un despliegue de coalición federada.
Nombre Autor/a	Jorge Álvaro González
Nombre Tutor/a TFM	Víctor Monzón Baeza
Nombre del/de la PRA	Carlos Monzo Sánchez
Fecha de entrega	10/06/2024
Titulación o Programa	Máster en Ingeniería de Telecomunicación
Área del trabajo final	Sistemas de Comunicación
Idioma del trabajo	Castellano
Palabras Clave	Blockchain, Federated Networking, interoperabilidad, seguridad, distribuido, redes, gobierno, SDN

Resumen

A lo largo de este trabajo se estudia las posibilidades que ofrece la tecnología blockchain para la gestión descentralizada de los servicios en un despliegue internacional y federado de una coalición cívico-militar de características similares a la OTAN. En este sentido, el análisis se puede encuadrar dentro de la corriente definida por los estudios de redes de misión federadas (FMN) de la OTAN, que buscan estandarizar los despliegues de coaliciones internacionales primando su interoperabilidad y eficacia desde los momentos iniciales de una misión con fuerzas pertenecientes a distintas entidades cooperativas.

Por ello, en el presente documento se analiza la información pública disponible para explorar el estado del arte de las espirales FMN en la actualidad y evaluar si sirve como marco en el que encuadrar el presente trabajo, para a continuación definir un caso de uso en el que analizar las funciones que podría incluir la aplicación Blockchain para la gestión descentralizada de los servicios, con el objetivo de asegurar la integridad, confidencialidad y disponibilidad para la federación.

En base a estos análisis, se desarrollará una aplicación basada en Blockchain cuya viabilidad se estudiará siguiendo el caso de uso definido, para validar la seguridad en la gestión de los despliegues naciones, así como garantizar la federación de los recursos y organizaciones.

Abstract

This paper studies the possibilities offered by the blockchain technology for the decentralized service management in an international and federated deployment of a civil-military coalition with with characteristics similar to those of the well known NATO. In this sense, the analysis can be framed within the current defined by NATO's Federated Mission Network (FMN) studies, which aim to standardize international coalition deployments by prioritizing their interoperability and efficiency from the initial moments of a mission with forces belonging to different coalition entities.

Therefore, this paper analyzes the public information to explore the current state of the art of FMN spirals and evaluates whether it serves as a framework in which to frame the present work, to then define a use case in which to identify the functions that could include the Blockchain application for the decentralized service management, with the aim of ensuring the integrity, confidentiality and availability for the federation.

Based on these analyses, a Blockchain-based application will be developed, whose feasibility will be studied following the defined use case, to validate the security in the management of nation deployments, as well as to guarantee the federation of resources and organizations.

DEDICATORIA

A mi familia; en especial a mi hermano Daniel, espejo en el que me miro y referente de la persona que quiero ser.

Porque nuestras decisiones y los pasos que hemos dado son los que nos han traído hasta aquí, y sólo nuestros próximos pasos definirán el camino que queda por andar y la persona que llegaremos a ser. Por no tener miedo a cambiar el rumbo del camino.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ACRÓNIMOS:

- **ACO:** Allied Command Operations
- **AMN:** Afghan Mission Networking
- **C2:** Command & Control
- **DAO:** Decentralized autonomous organization
- **DDoS:** Distributed denial of service
- **DoS:** Denial of service
- **FEDNET:** Federated network
- **FMN:** Federated mission networking
- **FOC:** Fully operative capabilities
- **GPO:** Group Policy Object
- **IaaS:** Infrastructure as a service
- **ICD:** Interface Control Document
- **IDE:** Entorno de Desarrollo Integrado
- **IOC:** Initial operative capabilities
- **JFC:** Joint Force Commands
- **MC:** Military Comitee
- **MFA:** Multi-Factor Authentication
- **NAD:** NATO Architecture Framework
- **NFV:** Network function virtualization
- **OTAN:** Organización del tratado del Atlántico Norte
- **Paas:** Platform as a service
- **POS:** Proof-of-stake
- **POW:** Proof-of-work
- **SaaS:** Software as a service

- **SDN:** Software defined network
- **SHAPE:** Supreme Headquarters Allied Powers Europe
- **SIEM:** Security information and event management
- **TACCIS:** Tactical Communication and Information Systems
- **TCN:** Troop contibuting nation
- **TSS:** Two Time Stamping Scheme
- **TSS:** Two time-stamping schemes
- **UAS:** Unmanned automated systems
- **VM:** Virtual Machine

1. INTRODUCCIÓN

1.1. Contexto y justificación

Los continuos avances tecnológicos y la aparición de tecnologías disruptivas como la amenaza que supone la computación cuántica para los modelos criptográficos más extendidos (tanto simétricos como asimétricos) [1], hacen que mantener la seguridad suponga un reto constante. Muchos trabajos han surgido para estudiar la aplicación de tecnologías emergentes en las comunicaciones tácticas con el objetivo de mejorar y ofrecer mayor seguridad, por ejemplo es el caso de 5G [2], nuevas formas de onda [3],[4], digital twin [5], [6] entre otras . La necesidad de asegurar los entornos de la información cobra especial relevancia por dos circunstancias principales:

- Por un lado, la sociedad ha sufrido un proceso de simbiosis con la tecnología, y cada vez más aspectos de la vida cotidiana dependen de tecnologías que almacenan, gestionan y controlan información sensible de gran cantidad de personas [7],[8].
- Por otro lado, la información manejada por la administración pública, y en especial en entornos militares, goza de especial sensibilidad y necesidad de protección, pues su vulneración podría afectar a la seguridad de gran parte de la población o comprometer el éxito de operaciones militares. El reto es aún mayor cuando el intercambio de información se convierte en una necesidad, como es el caso de organizaciones supranacionales como la Unión Europea[9] o despliegues de coaliciones cívico-militares como los de la OTAN[10].

En este contexto, surgió la iniciativa *'Federated Mission Networking'* (FMN) de la OTAN [11], que busca aumentar la interoperabilidad y la eficacia en los despliegues de coaliciones federadas, siendo uno de los pilares fundamentales la seguridad en estos escenarios. Por todo ello, el presente trabajo explora escenarios de coaliciones de naturaleza similar, para proponer una aplicación descentralizada de gestión de redes federadas que asegure la confidencialidad, la integridad y la disponibilidad de todas las operaciones realizadas para controlar las mismas, sirviendo como una propuesta de marco de referencia para futuros desarrollos centrados en la interoperabilidad.

1.2. Objetivos

En esta sección se especifican los objetivos principales que se esperan conseguir con el presente proyecto:

1. En primer lugar, resulta necesario alcanzar un nivel de conocimiento teórico suficiente para el desarrollo del aplicativo del proyecto. Este marco teórico deberá abarcar:

- Por un lado la tecnología Blockchain, incluyendo su funcionamiento, utilidad en distintos casos reales, y fundamentos de seguridad. A continuación, se estudiarán también sus aplicaciones en el sector Defensa.
- Por otro lado, es necesario un contexto teórico relativo a los despliegues de coaliciones federadas, su infraestructura y particularidades. Además, como el proyecto se centra en la gestión tecnológica de estos despliegues, este marco teórico deberá incluir dentro de su alcance los fundamentos de los despliegues de redes definidas por software(SDN) de estas coaliciones.

2. A continuación, se planteará un caso de uso de un despliegue federado de una coalición cívico-militar, que incluirá distintas necesidades(e.g. niveles de confidencialidad, políticas de gestión) y particularidades. Utilizando este caso de uso, se identificarán las utilidades de una aplicación descentralizada para la gestión de estos despliegues.

3. Antes de desarrollar las aplicaciones identificadas, se deberá disponer de un entorno de pruebas y desarrollo apropiado, por lo que el tercer objetivo será la preparación del mismo.

4. Disponiendo de la definición de las funciones y del entorno de desarrollo, se iniciará el desarrollo. Este objetivo incluirá las definiciones teóricas pertinentes, como la definición de modelos de datos, ICDs, etc.

5. Cuando la aplicación cumpla con los objetivos técnicos esperados, se evaluará su utilidad en el caso de uso y se comparará con el escenario en el que no se dispusiese de la aplicación desarrollada.

6. Por último, se plantean propuestas para la continuación del desarrollo de la aplicación propuesta.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Los recientes acontecimientos en diferentes conflictos armados a lo largo del mundo [12][13] han demostrado cómo las operaciones en el quinto dominio, conocido como el dominio del ciberespacio, de la información, de ciberseguridad o de inteligencia, no se restringen sólo a activos y organizaciones militares. Individuos, colectivos, organizaciones e infraestructura se han visto involucrados como parte activa en los conflictos, como objetivo o como atacantes. No es una circunstancia que resulte sorprendente, ya que es algo que múltiples teóricos y académicos han resaltado en los últimos años, como es el caso del General Dávila en su publicación 'El nuevo Arte de la Guerra'[14], en la que explica que gran cantidad de activos usados por civiles forman parte de un estado continuo de guerra de la información.

Como consecuencia lógica, las actuaciones en el ciberespacio tienen gran relevancia en la ciudadanía, y los desarrollos(como el propuesto en este trabajo) tienen implicaciones directas en la información de las personas, que se ven involucradas como parte activa o pasiva.

Por ello, las tecnologías como Blockchain, que no sólo aseguran la seguridad en las transacciones, sino que aportan una capa extra de privacidad, anonimización y descentralización [15]. Las aportaciones de esta tecnología fomentan la participación de una mayor cantidad de perfiles diversos, a los que ofrece una capa de uniformidad anónima que evita el tratamiento dispar de la información y los privilegios de los perfiles. Esto se uno a la creación de infraestructuras más potentes y seguras, garantizando un nivel de criticidad mayor [16]. En cierta manera, la mejora de las ciudades, las infraestructuras y los sistemas de comunicación contribuyen al desarrollo sostenible y por ende, el cumplimento de los objetivos de desarrollo sostenible [17].

En conclusión, la aplicación de la tecnología Blockchain para la gestión de la infraestructura y la capa de gestión de redes aporta múltiples beneficios en la corriente de los objetivos de desarrollo sostenible (también conocidos como Agenda 2030) planteados por las Naciones Unidas [18]. En particular, la mayoría de los beneficios pueden encuadrarse en el noveno punto, de industria, innovación e infraestructura, aunque también tiene implicaciones en el décimo (reducción de la desigualdad) y el quinto (igualdad de género) al eliminar la disparidades y ofrecer un acceso común (aunque restringido siguiendo unas apropiadas políticas de seguridad) a la gestión descentralizada de la infraestructura en despliegues de coaliciones cívico-militares y al aumentar la seguridad en las redes y de la información tratada y compartida dentro de las mismas.

1.4. Enfoque y método seguido

El presente trabajo se ha desarrollado siguiendo una metodología teórico-práctica con 5 etapas fundamentales:

- La primera etapa se centrará en analizar un análisis puramente teórico de la tecnología blockchain y de los despliegues de redes federadas. Esta etapa también abarca la evaluación de posibles tecnologías en las que fundamentar el desarrollo de la aplicación propuesta.

- En la segunda etapa se define un escenario de un despliegue de coalición cívico-militar, que servirá como caso de uso para evaluar la utilidad de la descentralización de la capa de control de las redes federadas y proponer funciones a desarrollar para la aplicación.

- La tercera fase incluye la preparación del entorno de pruebas y el desarrollo de las funciones identificadas. Esta fase se iniciará con las funciones definidas en la etapa anterior y finalizará cuando se haya completado el despliegue y las pruebas de funcionamiento técnicas.

- Durante la cuarta etapa se llevará a cabo una evaluación de las funcionalidades de la aplicación descentralizada respecto al caso de uso previamente definido. Esta fase también incluirá la comparativa del rendimiento respecto al caso de uso.

- La quinta y última etapa evalúa los resultados y propone futuros desarrollos que continuarían el trabajo realizado en el presente proyecto.

1.5. Planificación

El presente proyecto se ha desarrollado siguiendo una metodología basada en un total de cuatro entregas intermedias y una entrega final. Estas entregas se desarrollarán de manera secuencial, sin perjuicio de que ciertas actividades avancen de manera simultánea con el fin de optimizar el progreso del proyecto. El siguiente diagrama de Gantt incluído en la figura 1.1 muestra la planificación detallada de las actividades que componen el proyecto, así como la secuencia temporal en la que se desarrollarán.

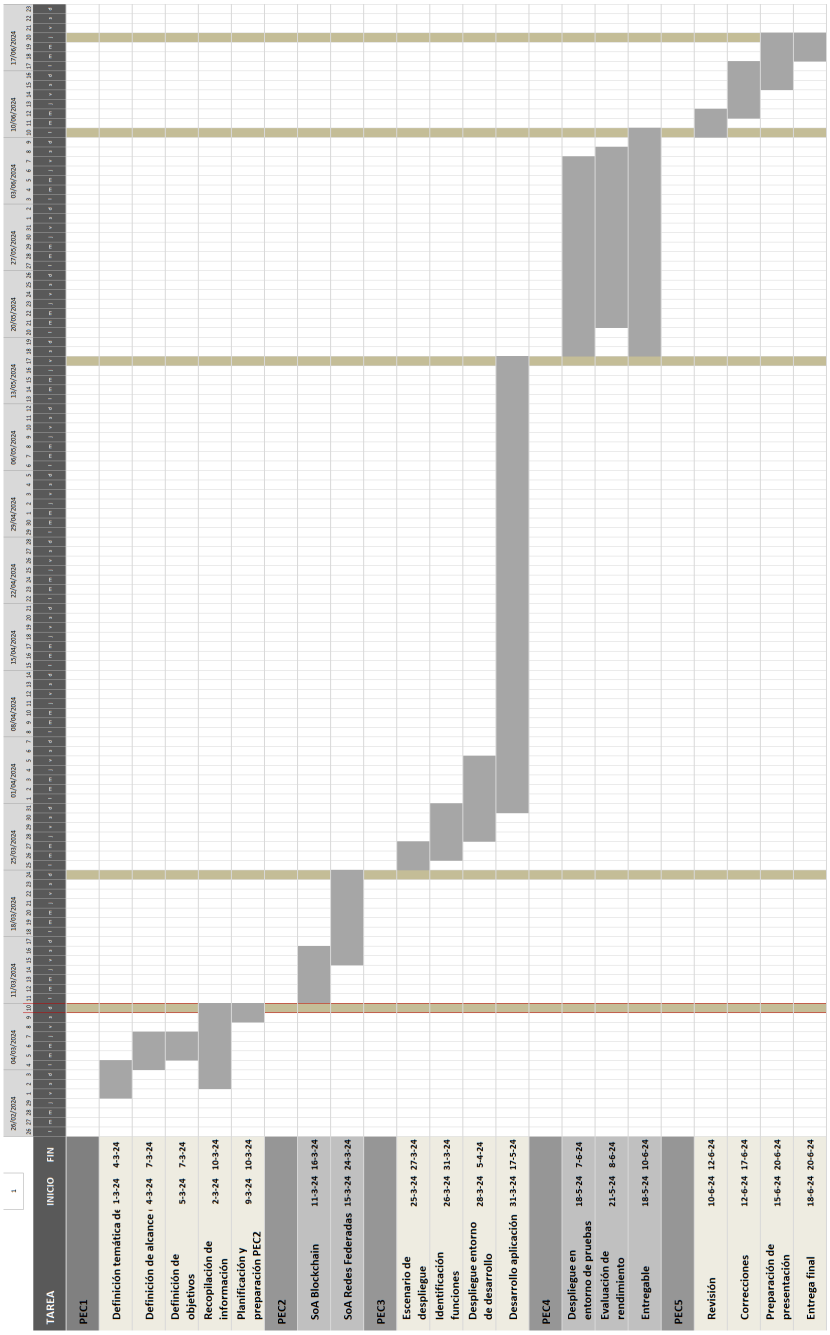


Fig. 1.1. Planificación del TFM.

1.6. Breve sumario de los productos obtenidos

Durante el desarrollo del presente proyecto se ha desarrollado de forma exitosa una aplicación descentralizada para la gestión de las directivas y políticas de seguridad que se aplicarán a los activos utilizados en los despliegues de coaliciones federadas.

Se optó por desarrollar la prueba de concepto en base a la aplicación de la gestión de directivas y políticas debido a que es tanto una funcionalidad necesaria para la correcta gestión de los despliegues federados como una aplicación que se beneficia de las ventajas proporcionadas por la tecnología Blockchain en cuanto a descentralización y seguridad.

En este desarrollo, de utilizan dos tipos de perfiles según los roles que desempeñen en el sistema: uno básico con permisos limitados y otro de administrador privilegiado con más funcionalidades. Gracias a Blockchain, todas las acciones ejecutadas por los usuarios quedarán registradas de forma inmutable en el sistema.

Esta prueba de concepto sirve para confirmar la utilidad de las aplicaciones descentralizadas para la gestión de una infraestructura que abarque diferentes organizaciones, como es el caso de una coalición federada como la analizada en el presente trabajo.

1.7. Breve descripción de otros capítulos de la memoria

Estado del arte: En este capítulo se analiza la situación actual con respecto a las tecnologías blockchain y los despliegues de coaliciones federadas, así como las líneas de desarrollo más novedosas en ambos casos.

Caso de uso: Antes de comenzar con la definición y el desarrollo de la prueba de concepto, en este capítulo se explora un caso de uso definido para analizar la utilidad de la tecnología Blockchain durante los despliegues y las misiones.

Funciones de gestión de servicios: Tras la definición y evaluación del caso de uso, en este capítulo se exploran diferentes funciones identificadas relacionadas con la gestión de los servicios ofertados en el despliegue de la coalición.

Diseño de arquitectura: En este capítulo, antes de iniciar el desarrollo, se analiza la arquitectura a nivel de capacidad operativa y de servicios de la aplicación descentralizada a desarrollar.

Desarrollo de dApp: Este capítulo engloba todo el desarrollo de la aplicación descentralizada propuesta. Por un lado, se definen los pasos seguidos para establecer un entorno de desarrollo apropiado; por otro lado, se desarrolla la aplicación una vez alcanzado un entorno de desarrollo estable.

La aplicación descentralizada propuesta se centra en la gestión de las políticas y directivas aplicables a los distintos activos federados dentro de la coalición.

Análisis de resultados y desafíos: En este capítulo se evalúan las funciones definidas en la aplicación descentralizada propuesta y su comportamiento ante diferentes usos por distintos usuarios definidos para las pruebas.

Conclusiones y líneas futuras: Tras la evaluación de los resultados y la prueba de concepto, en este capítulo se elaboran unas conclusiones finales del desempeño de las funciones.

Además, se establecen posibles líneas para futuros desarrollos basados en la aplicación descentralizada propuesta y otras funciones no desarrolladas necesarias para habilitar la capacidad operativa completa.

2. ESTADO DEL ARTE

En esta sección del proyecto se realiza una revisión de la literatura existente sobre el contexto tecnológico y de despliegues de dominios federados; en particular, se explorarán la tecnología Blockchain y los despliegues federados de coaliciones de naturaleza heterogénea (e.g. cívico-militares, público-privadas, multinacionales) con el objetivo de ofrecer una visión completa de los aspectos más esenciales, avances, tendencias y oportunidades de desarrollo de cada ámbito. Además, también se estudiarán distintos proyectos e iniciativas que exploran las aplicaciones de blockchain en el sector Defensa y en la gestión descentralizada de recursos.

2.1. Tecnología Blockchain

La tecnología blockchain ofrece un sistema de registro de transacciones en una red distribuida. Una de las características más relevantes es la inalterabilidad de los registros de transacciones, que a su vez se ejecutan mediante los denominados contratos inteligentes, automáticamente bajo ciertas condiciones definidas(aunque no obligatoriamente ni en todas las redes, como se verá a continuación).

2.1.1. Fundamentos del Blockchain

Como norma general, la tecnología Blockchain se basa en criptografía pública[1] y dos funciones criptográficas básicas:

- **Funciones de hashing**[19]: una función *hash* es una función matemática que recibe como argumento una cadena de longitud arbitraria y devuelve como resultado una cadena de longitud conocida, con la particularidad de no existir una operación matemática que revierta el proceso. Tienen tres características principales:
  - Resistencia de preimagen o no inversión: se refiere a que no exista una operación matemática que revierta la función *hash*.

$$H(n) \rightarrow v$$

$$H(n) \nleftarrow v$$

  - Resistencia a la colisión: hace referencia a la baja probabilidad de que dos argumentos produzcan el mismo resultado.

$$H(n) \neq H(m)$$

[1] La criptografía pública es aquella que utiliza una clave pública y otra privada para su funcionamiento.

- Resistencia débil a la colisión: derivado de los dos primeros, hace referencia a la baja probabilidad de que dos argumentos produzcan el mismo resultado, conociendo previamente el resultado y el argumento de una de las ejecuciones.

$$H(n) = H(m)$$
$$\Updownarrow$$
$$n = m$$

- **Funciones de firma digital**: la firma digital es una función de la criptografía asimétrica. En ella, el usuario hace uso de su clave privada y del *hash* de la información que desea transmitir, combinándolos y enviándolos junto a la información. El receptor, por su parte, puede:

  1. Verificar la identidad del emisor, gracias a la clave pública del mismo.
  2. Verificar la integridad de la información, ya que puede generar el *hash* de la información recibida y compararlo con el hash firmado.

  La figura 2.1 ilustra el proceso de firma digital y la verificación del receptor:

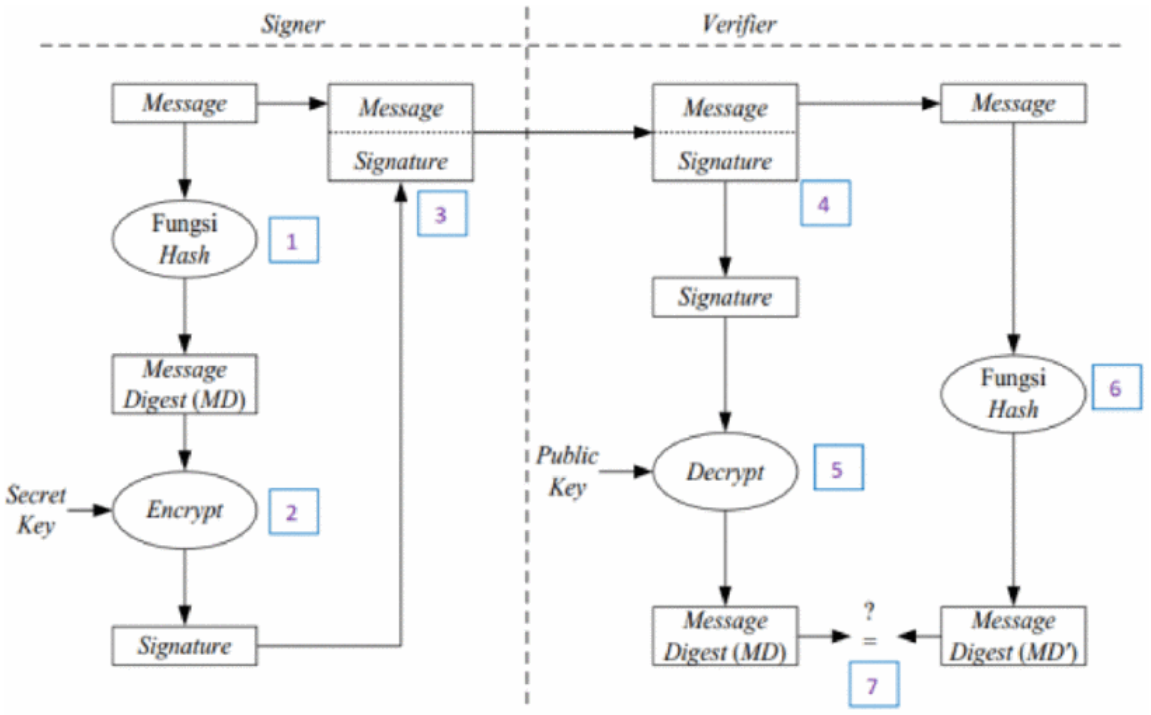


Fig. 2.1. Proceso de firma digital y verificación[20].

2.1.2. Los orígenes de Blockchain: *´Time-stamp'* digital

En 1991, los criptógrafos Stuart Haber y Scott Stornetta definieron la piedra sobre la que se cimentó la tecnología Blockchain. En su publicación *'How to Time-Stamp a Digital Document´*[21], propusieron una solución teórica que permitía añadir marcas temporales a documentos basada en las operaciones de *'hash'* y firma digital, y diseñaron el primer sistema de bloques que aseguraba la integridad de las acciones.

En el sistema propuesto, denominado esquema de doble marca temporal(*'Two Time-Stamping Schemes'*, TSS), se ataja la posibilidad de que para un algoritmo A que recibe como argumentos un documento y una marca temporal (x y τ), pueda recibir posteriormente una marca temporal τ ilegítima. Para ello, haciendo uso de la función *hash* y la firma digital, el sistema se fundamenta en:

- **Enlazamiento**: cuando un cliente realiza una solicitud, el esquema realiza dos pasos:

  1. TSS firma un certificado C_n (que incluye información del identificador ID_n, la marca de tiempo t_n, el orden de la secuencia n, el *hash* de la información o documento y_n, e información de la ejecución previa L_{n-1}):

     $$s = \sigma(C_n)$$

     $$C_n = (n, t_n, ID_n, y_n; L_{n-1})$$

  2. Cuando la petición del cliente se procesa, TSS informa al cliente sobre el identificador a usar en la próxima petición, ID_{n+1}.

     Posteriormente, gracias a las propiedades de la firma digital σ, el cliente puede verificar la información. Esta característica supone el inicio del concepto de cadena de bloques, Blockchain.

- **Confianza distribuida**: TSS también hace uso de un sistema de retos para verificar la información. Asumiendo que se dispone de una función de firma segura, es necesario también disponer de un generador de secuencias aleatorias. Este generador(G), que en la práctica basta con que sea pseudoaleatorio, recibirá como una entrada conocida(que será el *hash* y_n) y devuelve una salida de longitud conocida. Esta salida se dividirá en fragmentos, y cada fragmento se equiparará a los identificadores de k usuarios.

  $$G(y_n) = (ID_1, ID_2, ..., ID_k)$$

  A este conjunto de usuarios se les solicita un reto al que deben responder con una lista de firmas que incluyan el ID_n respectivo, el *hash* y_n y la marca temporal t_n. Posteriormente, el cliente puede verificar la información recibida gracias a las propiedades de la firma digital.

  Con este proceso, la mayoría de los usuarios consultados deberían actuar de forma coordinada e ilegítima para vulnerar el sistema. Por un lado, la mayoría de los usuarios

consultados en una petición deberían ser ilegítimos para deslegitimar una ejecución(A esto se le conoce como ataque de consenso[22]), aunque para vulnerar todo el sistema, sería necesario que los usuarios ilegítimos fuesen ϵ^{-k}, donde ϵ es el subconjunto de usuarios ilegítimos, y se estima que debería superar el 90 % de los usuarios.

2.1.3. Satoshi Nakamoto, Blockchain y el Bitcoin

El problema del esquema propuesto por Haber y Stornetta es que, como indicaron en su artículo, no dejaba de ser una solución teórica que aún debía ser validada de forma práctica.

Basándose en los mismos principios y operaciones criptográficas que el esquema TSS, Satoshi Nakamoto(pseudónimo que firma el *'whitepaper'*) propuso en el año 2008 un sistema de efectivo digital[23] que validase las transacciones sin necesidad de una entidad centralizada que las avalase. La figura 2.2 muestra la relación entre los bloques de la cadena propuestas por Nakamoto.

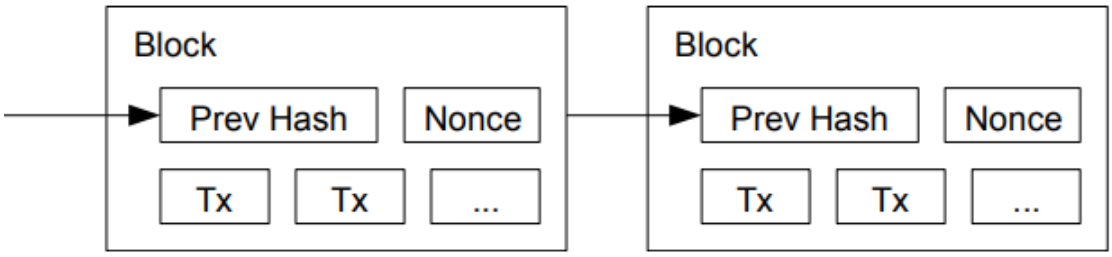


Fig. 2.2. Relación entre bloques de Bitcoin[23].

Este sistema define una prueba de trabajo (*'Proof-of-work'*, POW) necesaria para iniciar una nueva cadena de bloques en el sistema. Esta POW consiste en encontrar valores cuyo *hash* contenga cierta cantidad de bits con valor a cero en su comienzo; específicamente, el argumento usado debe ser una combinación de la marca temporal del sistema y un nonce añadido para cumplir la condición buscada. De esta manera, al priorizar el esfuerzo computacional como medio de prueba, se asume que la cadena más larga (asociada a un mayor coste computacional) es la más confiable, y un atacante que quisiera modificar bloques intermedios debería rehacer toda la POW. La figura anterior muestra cómo se enlazan entre sí los bloques para crear las cadenas.

La identificación de una nueva POW se considera una *'moneda'* del sistema bitcoin, y las cadenas añadidas a este bloque serán las transacciones. El proceso de uso de la red Bitcoin-Blockchain es:

1. Se anuncia la transacción a todos los nodos de la red.
2. Los nodos añaden la transacción en el bloque.
3. Los nodos buscan una POW para su bloque.

4. Cuando encuentran el POW, lo anuncian al resto de nodos.
5. Los nodos validan el bloque si todas las transacciones son válidas.
6. Los nodos aceptan los bloques al usarlo(mediante el correspondiente *hash*) para calcular el siguiente bloque de la cadena.

2.1.4. Ethereum

Tras el éxito recolectado por el sistema Bitcoin de Nakamoto, que fundamentó las bases de los sistemas de Blockchain descentralizados, diferentes iniciativas continuaron investigando el potencial de la tecnología Blockchain.

Una de las propuestas más relevantes es **Ethereum**, definida por Vitalik Buterin en 2014[24], que no es sólo una alternativa más, sino que nuevamente añade una nueva utilidad al Blockchain: la ejecución de contratos inteligentes.

Ethereum y los contratos inteligentes(conocidos comúnmente como *'Smart Contracts'*) surgen con la iniciativa de aunar las transacciones en Blockchain con la ejecución de *scripts* para definir así aplicaciones arbitrarias que fuesen escalables, estandarizadas, interoperables y completas. Además, los contratos inteligentes permiten definir organizaciones autónomas descentralizadas(*'Decentralized Autonomous Organization'*, DAO), al permitir controlar y condicionar su ejecución a un cierto subconjunto de los usuarios del sistema u organización.

Muchos otros sistemas han partido del concepto de los contratos inteligentes, dotando a la tecnología Blockchain de una gran cantidad de alternativas para desarrollar y definir DAOs, como Avalanche[25] o PolkaDot[26].

2.1.4.1. Ethereum Merge

El POW no es el único método de validación existente disponible en la tecnología Blockchain, existen muchos otros, como por ejemplo el *'Proof of Authority'*(Cada validador debe confirmar su identidad de manera confiable), *'Proof of Elapsed Time'*(Cada validador debe actuar esperando una cantidad determinada de tiempo), *'Proof of Capacity'*(en función del espacio de almacenamiento disponible en el equipo del validador) o *'Federated Byzantine Agreement'*(cada nodo confía en un grupo de nodos) entre otros[27].

Entre las alternativas, destaca la denominada *'Proof of Stake'*(POS), en el que un nodo que desea actuar como validador debe depositar cierta cantidad de un activo, normalmente de la criptomoneda asociada con el sistema, como garantías. Si se detecta que el validador ha actuado de forma ilícita, perderá el depósito. Este método de consenso es más centralizado que otras alternativas, aunque aporta un gran ahorro energético en los sistemas[28]. POS, en general, goza de gran popularidad entre los sistemas Blockchain más modernos.

En consecuencia, Ethereum decidió migrar a un sistema basado en POS en el año 2022 en lo que se conoce como *'Ethereum Merge'*, debido en parte al coste computacional que acarreaba el crecimiento del sistema en los últimos años con su POW. Aligerar los costes energéticos y computacionales ha propiciado a su vez que muchos desarrolladores hayan optado por sistemas como Ethereum o Avalanche, debido a las facilidades para realizar pruebas y desarrollos.

2.2. Federación de recursos

La federación de recursos es un concepto que se basa en la cooperación de los recursos que se encuentran localizados en diferentes infraestructuras con el fin de conformar un sistema con mayores capacidades, similar a un sistema distribuído, pero con la particularidad de ofrecer una capa de uniformidad y estandarización con un *framework* de control[29].

Los beneficios de la federación de recursos se han explorado en múltiples campos:

- ***Cloud* federadas**[30]: distintas infraestructuras compartiendo datos para aumentar las capacidades de cómputo de la nube. Incluye clasificaciones como las nubes híbridas o las nubes comunitarias entre otras, y se puede utilizar para múltiples niveles de servicio, incluyendo servicios de infraestructura (IaaS), plataforma (PaaS), software (SaaS) entre otros.
- **Algoritmos de aprendizaje federados[31]**: uno de los pilares fundamentales de los algoritmos de aprendizaje máquina es la cantidad de datos necesarios para alimentar los modelos de análisis, pero los datos en muchas ocasiones se encuentran dispersos en diferentes dominios y organizaciones en los que aplican distintas políticas y restricciones de acceso. Ante esta casuística, surge la alternativa del **aprendizaje federado**, una alternativa en la que múltiples dispositivos aportan sus recursos y resultados sin necesidad de compartir los datos originales(respetando así las distintas normativas).
- **Federación de seguridad**: distintos aspectos involucrados en la seguridad de la información se benefician de la gestión federada. De esta manera, escenarios que involucran a distintas organizaciones pueden gestionar sus políticas de seguridad y acceso[32] o las identidades de sus usuarios[33] asegurando el cumplimiento por igual en todos los recursos abarcados.

2.2.1. Federación de redes (FEDNETS)

La federación de redes(FEDNETS)[34] también ha sido un concepto explorado en los últimos años. Las FEDNETS se definen como despliegues *ad-hoc* temporales compuestos por un conjunto determinado de redes independientes. La temporalidad de esta infraestructura es un aspecto fundamental de las FEDNETS, ya que si el despliegue se prolongase de

forma indefinida en el tiempo, sería consecuente pensar que las redes acabarían conformando un único dominio, en el que por optimización se acabaría unificando su gestión. Otro aspecto destacable de la federación de redes es la existencia de un objetivo común que incita a la cooperación de los distintos dominios implicados en el despliegue de las redes; esta necesidad de cooperación incita a definir un conjunto de reglas que servirán como un marco de gobernanza, colaboración y funcionamiento para los dominios. En determinadas circunstancias, este marco de colaboración también podrá limitar al mismo tiempo las acciones o actividades permitidas para los organismos cooperantes.

2.2.2. *Afghan Mission Networking* (AMN)

Tras los atentados del 11 de septiembre del 2001, se iniciaron operaciones contra-terroristas de respuesta en Oriente Medio[35]. Estas operaciones dieron lugar al conflicto conocido como Guerra de Afganistán, que se prolongó durante 20 años y que involucró a fuerzas de en torno a 40 países a lo largo de sus distintas fases; la coalición de la OTAN involucró a 38 países, aunque la mayoría de las tropas pertenecían a Estados Unidos.

Tras aproximadamente 9 años de conflicto, en los que las distintas naciones cooperantes(*'Troop Contributing Nations'*, TCN) se vieron obligadas a colaborar en un escenario tecnológico adverso y heterogéneo, el Comité Militar(MC) aprobó la solicitud del Cuartel General del Mando Aliado de Operaciones(SHAPE) para establecer un dominio único de la información en el que las fuerzas aliadas pudieran colaborar eficazmente. Este dominio único debía conformarse a través de una federación de los dominios de las diferentes TCNs[36].

A este dominio único de federación de redes se le denominó *'Afghan Mission Network'*(AMN), y en julio del año 2010 ya podía ofrecer unas capacidades operativas básicas(IOC), aunque hasta 2012 no se consideró que ofreciera capacidades operativas plenas(FOC).

Por su naturaleza, se concibió al AMN a su vez como un sistema de mando y control(C2) extendido para la gestión y el intercambio de información, y como un marco que definiría futuras líneas de investigación. Los objetivos principales, tanto del AMN como de los futuros sistemas, debían centrarse en:

- Intercambio de información: las TCNs deben ser capaces de intercambiar información crítica para la misión. El proceso estandarizado para intercambiar información debe involucrar tanto a organizaciones militares como no militares.
- Gestión y gobernanza de la información: es necesario un marco común de políticas de seguridad, protocolos, tecnologías y estándares para establecer un marco interoperabilidad común para las comunicaciones entre los distintos *stakeholders*.

2.2.3. *Federated Mission Networking* (FMN)

Durante el desarrollo de la AMN, se decidió que debía continuarse el desarrollo para definir un marco de interoperabilidad, estandarización y optimización para los despliegues de coaliciones. De esta forma, se sentaron las bases del *'Future Mission Networking'*, que posteriormente fue sustituido por el *'Federated Mission Networking'*, compartiendo ambos conceptos las siglas FMN, que han sido utilizadas para referirse al concepto que engloban ambas definiciones[37].

Formalmente, se definió el objetivo de FMN como la mejora de la operatividad y la preparación en la actualidad y el futuro, bajo un término que se denominó "interoperabilidad desde el día 0" para las fuerzas de despliegue de las TCNs(*'Day Zero Interoperable Forces'*)[38], con dos componentes principales:

- **Operativa conjunta para aprovechar la ventaja estratégica**: este componente hace referencia a la capacidad de las TCN de cumplir con los requisitos de despliegue de las misiones de la OTAN de forma efectiva mediante actividades de validación y verificación.
- **Adaptación conjunta y contínua**: el segundo componente hace referencia a la necesidad de responder de forma conjunta a los desafíos tecnológicos a los que se enfrenta contínuamente la coalición, con la finalidad de mantenerse en la vanguardia de las tecnologías disruptivas para los despliegues de misión.

El objetivo principal de FMN, por lo tanto, es apoyar al C2 y a la toma de decisiones en futuras misiones de coalición a través de un intercambio efectivo de información adaptado a las necesidades y restricciones de las distintas entidades implicadas. En la figura 2.3 se pueden observar los requisitos necesarios para implementar FMN en unas fuerzas operativas.

Fig. 2.3. Requerimientos operativos para las fuerzas FMN[38].

El desarrollo y la implementación de la capacidad FMN busca definir un conjunto de

procesos, organizaciones, entrenamientos, tecnologías y estándares de forma coordinada para los organismos de la OTAN, las naciones de la OTAN y naciones aliadas no pertenecientes a la OTAN. Las tropas con capacidad FMN deben disponer del conjunto de subcapacidades definidas para la espiral determinada, según corresponda, seis meses antes del despliegue requerido, de la forma que resume la ilustración previa.

2.2.3.1. Espirales FMN

Las denominadas *espirales* FMN son etapas de desarrollo que estructuran la evolución de FMN. Las espirales se organizan de forma sucesiva, aunque las fases de definición de cada espiral se solapan con las fases finales de la espiral previa. En la imagen 2.4, se muestra el ejemplo de las espirales 5 y 6[37], con sus respectivos objetivos de desarrollo para cada año.

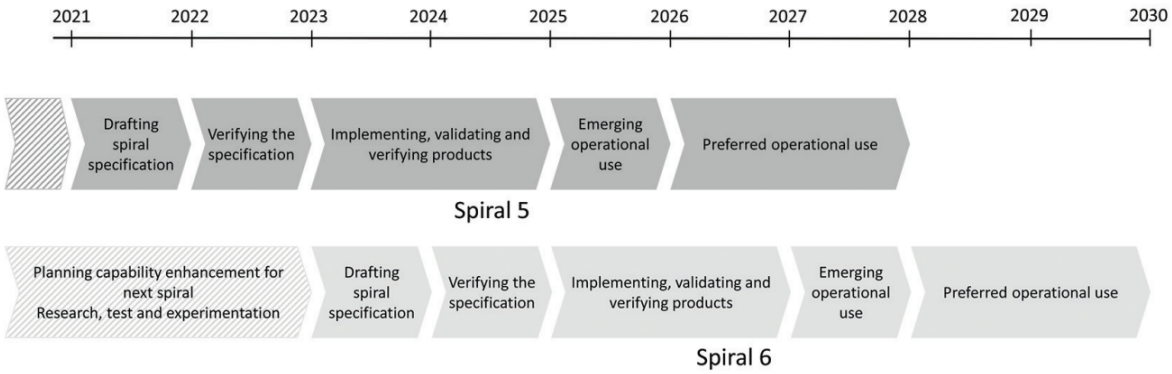


Fig. 2.4. Secuencia de etapas de las espirales 5 y 6 de FMN[37].

Además, cada espiral se enfoca en la definición, verificación, implementación y validación operativa de una capacidad específica; por ejemplo, la quinta espiral, que finaliza en el año 2028, se centra en el desarrollo de las comunicaciones tácticas para el intercambio de información durante las misiones(TACCIS, por sus siglas en inglés *Tactical Communication and Information Systems'*).

2.3. Blockchain para la gestión de infraestructura digital en despliegues de coaliciones cívico-militares

Las posibilidades que ofreció la aparición de los contratos inteligentes de Ethereum propiciaron que múltiples industrias se interesasen por las aplicaciones Blockchain. Ejemplos destacables pueden ser la industria sanitaria, con aplicaciones para gestionar el acceso acceso al historial clínico de los pacientes[39], en sistemas para mejorar la seguridad de entidades financieras[40] o la monitorización de nodos en sistemas industriales[41].

Múltiples iniciativas también estudian las aplicaciones de Blockchain en el sector Defensa, tanto a nivel nacional, con iniciativas tecnológicas para transformar los sistemas de mando y control[42] como a nivel supranacional[27]. Cabe destacar que las naciones que formen parte de coaliciones como la OTAN, deben encuadrar sus iniciativas y esfuerzos dentro de los esfuerzos de la organización; en el caso de la OTAN, siguiendo la cooperación establecida en el artículo 3 del Tratado del Atlántico Norte para los estados miembros[43]. Por esa razón, distintas iniciativas y proyectos para implementar la tecnología blockchain en el entorno de la OTAN involucran a distintas naciones, tales como:

- Un sistema de C2 aéreo que se beneficia de las aplicaciones blockchain para mejorar la seguridad en operaciones aéreas de emergencia[44].
- Una aplicación para asegurar el correcto etiquetado de los metadatos compartidos por sistemas IoT en los despliegues militares basado eb blockchain[45].

Una de las corrientes principales de los estudios es la utilidad de Blockchain para asegurar la gestión de los despliegues, la logística y la intendencia de la coalición[46]; la descentralización y la trazabilidad que ofrece un sistema privado de blockchain cobran especial relevancia en entornos militares.

En lo que respecta a la intendencia de los despliegues, entre las utilidades de los contratos inteligentes de Blockchain, se puede encontrar[47][48]:

- La validación de autorizaciones.
- La gestión de las órdenes de la misión, asegurando su integridad y confidencialidad.
- Control de drones(UAS, *'Unmanned Automated Systems'*).
- Gestión de la cadena de suministros entre distintas naciones y organizaciones.
- Gestión perimetral, tanto en seguridad física(e.g. asegurando la validez de los permisos o de los sistemas de vigilancia) como en seguridad lógica(e.g. definición de redes, aplicación de políticas, federación de recursos).

La aparición del paradigma de las redes definidas por software(*Software Defined Network*, SDN) ha beneficiado ampliamente los escenarios de despliegues de red que requieren dinamismo para aplicar políticas y configuraciones en infraestructura que abarque diferentes dominios(e.g dominios nacionales, geográficos o jurisdiccionales) [49].

Las SDN guardan una estrecha relación con la virtualización de funciones de red(*Network Function Virtualization*, NFV), en la que basan su funcionamiento. La NFV permite virtualizar y agilizar el despliegue y la configuración de funciones de red que previamente requerían *hardware* específico, tales como el *enroutado* de las comunicaciones, los *firewall* o el balanceo de carga en la red [50].

A pesar de los múltiples beneficios que conlleva la aparición de SDN/NFV para los despliegues de coalición, también conlleva riesgos y retos para la seguridad, tanto en la capa de aplicación, como en los planos de datos y control de SDN. Dado que el presente trabajo se centra en la infraestructura de los despliegues, a continuación se ahondará en los retos que supone SDN/NFV para el plano de control de la infraestructura de coalición. La siguiente figura 2.5 muestra las relaciones entre las diferentes capas de SDN, así como los vectores que pueden afectar a cada una de ellas. **Retos de seguridad en la capa de control SDN:** Los

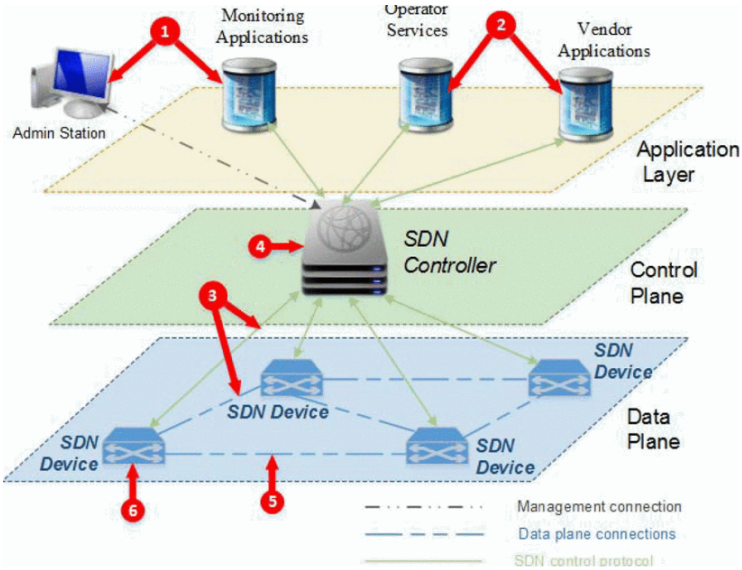


Fig. 2.5. Capas SDN[49].

fallos de seguridad en el plano de control suponen una gran amenaza para la estrategia, la planificación y la gobernanza de la red. En la figura anterior se pueden observar dos vectores de ataque para el plano de control, el 3 y el 4, que pueden llevar a:

- Ataques de denegación de servicio, tanto clásicos(DoS) como distribuidos(DDoS) [51][52]. En general, este tipo de ataques se centrarían en atacar la comunicación entre el plano de datos y el de control, insertando tráfico, modificando tráfico legítimo, añadiendo usuarios ficticios o modificando el estado de dispositivos conectados.

- Ataques al controlador SDN: este riesgo es propio y exclusivo de las SDN, ya que los usuarios y entidades asociadas pueden desplegar aplicaciones en el controlador de la red. Si no se establece ningún control, o el control es negligente, se podrían desplegar aplicaciones malintencionadas que podrían reconfigurar la totalidad de la red, ya que los controladores de la capa de control sólo transforman la configuración de la infraestructura[53].

La integración de Blockchain para securizar el control de las SDN y de los despliegues de dominios de una coalición puede ser beneficiosa para ambos casos, aunque especialmente en la gestión de la capa de control; emplear una tecnología Blockchain para gestionar todo

el tráfico de la red sería inabarcable debido a su escalabilidad, siendo más apropiado el despliegue de elementos de análisis de tráfico como SIEMs.

3. CASO DE USO

En este capítulo se define el caso de uso que sirve para contextualizar la utilidad del proyecto en el despliegue de una coalición federada. Al englobarse el proyecto en un esfuerzo común compartido con Ana María Saiz García y su trabajo 'Gestión descentralizada de la red en un despliegue de coalición federada mediante blockchain'[54], este caso de uso se ha definido de forma conjunta, y por lo tanto el presente capítulo se comparte en ambos proyectos.

3.1. Antecedentes del caso de uso

Para explorar la viabilidad del presente trabajo, a continuación se define un caso de uso en torno al cual trabajar para desarrollar una solución. Como ya se ha visto en apartados anteriores, el origen de las propuestas para la estandarización de las comunicaciones en despliegues cívico-militares se remonta al conflicto de Afganistán y el AMN, por ello, el caso de uso:

- Se basará en el escenario de despliegues de la coalición federada reales, pues están ampliamente documentados[55] y demuestran tanto su complejidad como su problemática. Esta decisión se fundamenta en disponer de un escenario verosímil en el que evaluar el desarrollo, aunque sólo servirá de inspiración conceptual y se propondrá un caso de uso propio en distinta localización.
- Para reducir la complejidad del caso de uso, se establecerá una localización en la que se despliegan 4 contingentes(3 de ellos aliados y uno adversario) y se especificarán los detalles para el presente proyecto.

3.2. Caso de uso

La región en la que se desarrolla el presente caso de uso abarca 3 despliegues de naciones aliadas, dentro de los cuales se incluye infraestructura perteneciente a diferentes organizaciones que deberán federarse bajo el marco de una coalición. Por simplicidad, a continuación se usará nomenclatura propia de las Fuerzas Armadas españolas, a pesar de que cada nación usará nomenclatura propia para diferenciar sus 3 ejércitos.

- Infraestructura del Ejército de Tierra.
- Infraestructura de la Armada.
- Infraestructura del Ejército del Aire.

- Infraestructura propia del Mando Conjunto, es decir, infraestructura nacional propia compartida por los diferentes ejércitos dentro de una nación con una función principal de C2 operacional y planificación, que deberá transponerse a operaciones en los distintos dominios y sus C2 correspondientes.

El siguiente diagrama, mostrado en la figura 3.1, esquematiza la jerarquía de C2 en el sistema de forma genérica. Como se puede observar

1. **Nivel de Coalición**: representado en la parte superior de la figura. Se compone del organismo supranacional de máxima autoridad en la federación. Los despliegues nacionales dependen de las decisiones tomadas por la coalición, que distribuirá órdenes de alto nivel a las distintas naciones federadas.
2. **Nivel Nacional**: situado en la franja central de la figura. En el Nivel Nacional se encontrarán los mandos nacionales, que reciben órdenes de alto nivel de la coalición y las trasponen para su ejecución.
3. **Nivel Operativo**: cada despliegue nacional de la federación contará con sus propias tropas que ejecutarán las órdenes definidas por su respectivo mando nacional. Se corresponde con la parte inferior de la figura.

Esta jerarquía se mantendrá a nivel operativo y de infraestructura.

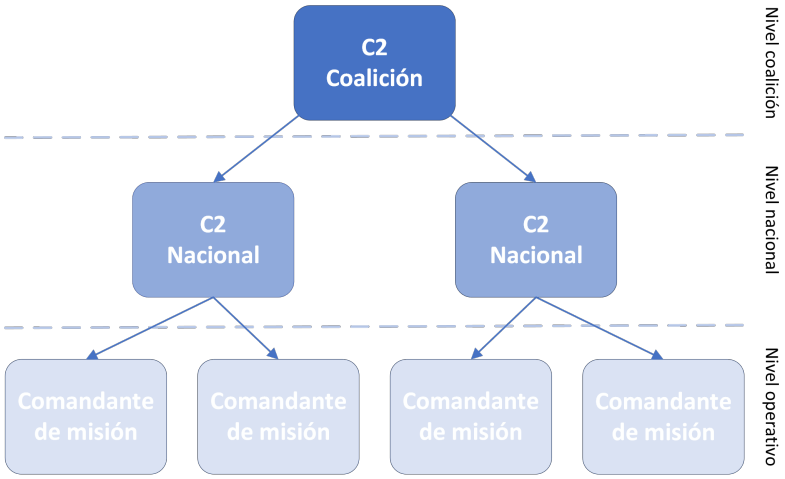


Fig. 3.1. Jerarquía de despliegue.

Particularizando la estructura para nuestro escenario, contemplaremos tres contingentes aliados que se desplegarán sobre el terreno, pertenecientes a España, Italia y Portugal. A la infraestructura nacional hay que sumarle una infraestructura supranacional de C2 propio de la coalición, que servirá como nexo de gobernanza del despliegue de la coalición. Específicamente, este organismo podría estar adscrito a la estructura de mando de operaciones aliadas de la OTAN('Allied Command Operations', ACO), en uno de los 3 niveles definidos; por

simplificar, se asemejará al segundo nivel de mando operacional('Joint Force Commands', JFC), aunque esta equiparación no es completamente precisa[56]. Se considera que esta capa consta únicamente de una infraestructura que comunicará con la infraestructura C2 de cada nación y la conformarán organismos con representación de todos los miembros de la coalición.

Adaptando la estructura del diagrama 3.1 a nuestro escenario, se obtiene el diagrama de la figura 3.2, en el que podemos observar:

- Un JFC de la OTAN a nivel de mando de la coalición.
- Estructuras de mando nacional de los tres países(i.e. España, Italia y Portugal).
- Tropas pertenecientes a los distintos contingentes. En este nivel se encuentran también la infraestructura IT federada y los activos propios de cada cuerpo de fuerzas armadas.

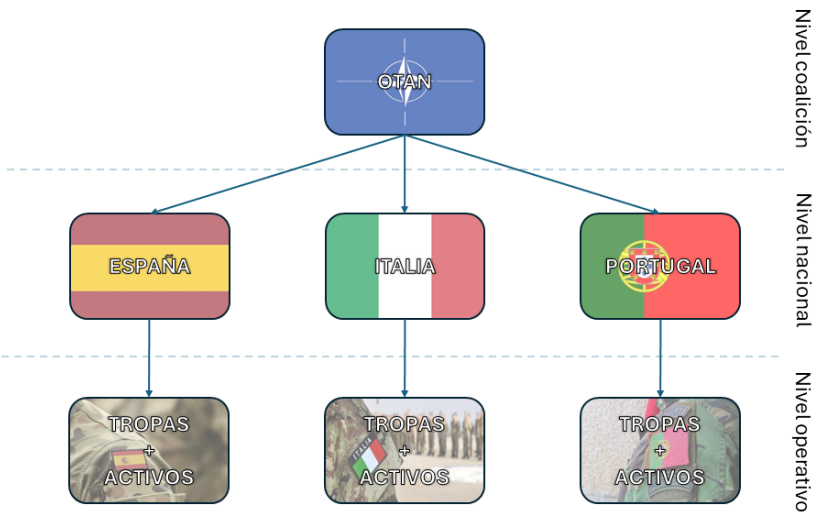


Fig. 3.2. Jerarquía particularizada.

Por otro lado, también se considerará infraestructura propia de organizaciones civiles que cooperarán con la coalición; esta capa incluye servicios de consultoría especializada, de infraestructura tecnológica y colaboradores que simplemente utilizarán sus propios dispositivos conectados a la red de la coalición(e.g. guías, traductores). Aquí se encuentra también cierta infraestructura civil no federada catalogada como neutral, es decir, infraestructura de comunicaciones que coexistirá con la infraestructura de la coalición, y cuyos usuarios son catalogados como agentes neutrales.

Por último, también se considerará una organización adversaria. Dentro de esta organización se dispone de cierta infraestructura propia y un indeterminado número de usuarios con

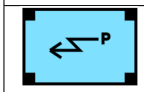
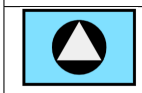
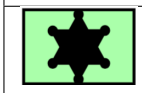
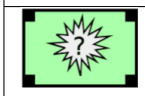
Símbolo	Descripción
	Puesto de mando - *Allied Command Operations*
	Puesto de mando Multinacional (coalición)
	Infraestructura terrestre de telecomunicaciones
	Patrulla
	Operación de emergencia
	Dron de comunicaciones
	Instalaciones sanitarias
	Instalaciones de fuerzas del orden
	Accidente con material explosivo peligroso
	Jamming adversario

TABLA 3.1. Iconografía APP-6 empleada.

distintos niveles de conocimiento tecnológico; de esta forma, siguiendo el principio de la *'Niebla de Guerra'*[57](concepto que hace referencia a la incertidubre en los escenarios de conflicto, debido a la falta de información, su imprecisión o la saturación de información), se considerará que disponen de amplios conocimientos e infraestructura especializada. Cabe destacar que los usuarios adversarios también pueden estar localizados en la infraestructura caracterizada como neutral, razón por la cual la información enrutada por esta infraestructura deberá tratarse adecuadamente sin una confianza directa.

A continuación se describe el escenario creado para este proyecto. La información mostrada en la figura 3.3 se ha representado según el estándar APP-6[58] que define la iconografía a emplear para representar la información en el entorno de la OTAN; los elementos incluidos en la figura se describen en la tabla 3.1.

Considerando lo anteriormente citado y un escenario con una gran urbe situada en el centro, tal y como se muestra en la figura 3.3, el despliegue se caracteriza por:

- La zona noroeste está identificada con los colores de la bandera de España (identificador número 1 en la 3.3), donde se localizan la infraestructura de comunicaciones, el centro de mando español y el centro de mando de la coalición.
- La zona sureste está identificada con los colores de la bandera de Italia (identificador número 2 en la 3.3), donde se localizan la infraestructura de comunicaciones y el centro de mando italianos.
- La zona este está identificada con los colores de la bandera de Portugal (identificador número 3 en la 3.3), donde se localizarán la infraestructura de comunicaciones y el centro de mando portugueses en una fase posterior.
- La gran urbe situada en el centro, denominada Al-Saíz (identificador número 4 en la 3.3), alberga la zona neutral. Aquí se encuentra la infraestructura de comunicaciones neutral (color verde), equipos sanitarios (color rosa) y tropas de patrullas aliadas (elementos 11 y 12).
- El resto de zonas, situadas principalmente al suroeste y el oeste, se consideran zonas adversarias y, por lo tanto, de baja confiabilidad para las comunicaciones, identificadas con color rojo (elemento 2).

El despliegue operativo se caracteriza por:

- España despliega su contingente en la zona noroeste.
- Las tropas italianas se localizan al sureste.
- El contingente portugués se localizará al este, pero se desplegará en una fase posterior.

Partiendo de este escenario, se plantea la siguiente situación para nuestro caso de uso:

1. La presencia de la coalición en la zona de conflicto se ha prolongado durante los últimos meses; los despliegues de España e Italia tienen una infraestructura consolidada, lo cual brinda canales de comunicación confiables para las tropas y el intercambio de información. Esta infraestructura la conforman los elementos 5 y 6 de la ilustración.
2. Dado que se espera que el despliegue, cuyo objetivo es asegurar la paz y la estabilidad en la zona, se prolongue durante los próximos 5 años, se ha decidido trasladar la localización temporal del centro de C2 de la coalición y establecerlo en el acuartelamiento del contingente español, identificado con el elemento 4 de la ilustración. Compartirán localización, pero supondrá una infraestructura independiente. La función principal de este centro será la coordinación de los esfuerzos de todos los despliegues, la definición de las órdenes estratégicas de alto nivel, la aplicación de unas políticas de seguridad consecuentes y la gobernanza general del sistema.

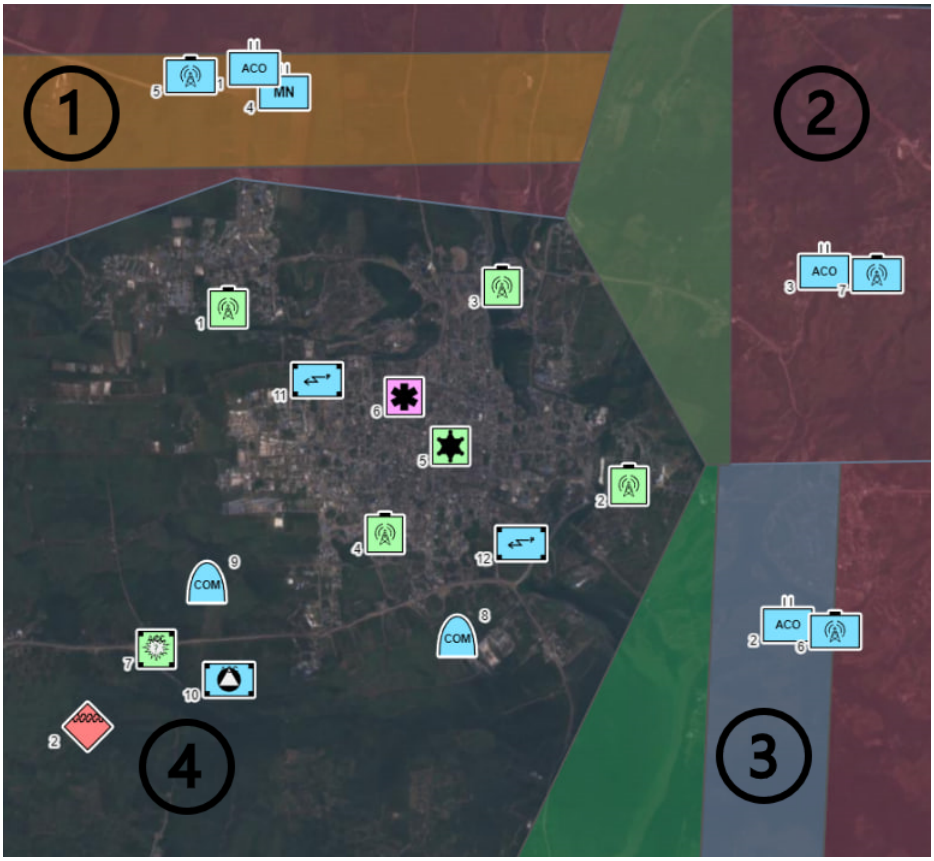


Fig. 3.3. Mapa del despliegue hipotético.

3. Con el fin de aumentar la seguridad en la zona, se ha decidido que durante los próximos meses, Portugal se unirá al despliegue, encargándose de la vigilancia de la zona este. Este añadido acarreará el despliegue de su correspondiente infraestructura de comunicaciones(elemento 7 de la ilustración), que deberá ajustarse a las políticas de seguridad establecidas desde el C2 de la coalición. En general, cada despliegue nacional debe encargarse de gestionar sus activos, trasponer los objetivos en misiones y órdenes aplicables y gobernar su infraestructura.

4. Entre las operaciones rutinarias de las tropas desplegadas se encuentra el realizar patrullas en el territorio neutral de Al-Saiz. Durante estas patrullas(elementos 11 y 12), los equipos harán uso de la infraestructura de comunicaciones de la ciudad para agilizar las comunicaciones entre las tropas cercanas, y además aprovechar para compartir información con los servicios de la zona, tales como fuerzas de seguridad o equipos sanitarios. La información que se comparta por estos canales deberá ser tratada de manera oportuna para asegurar su confidencialidad e integridad.

5. Eventualmente y debido a causas de fuerza mayor, puede requerirse que las tropas accedan a zonas consideradas conflictivas. En este caso, las tropas no harán uso de la infraestructura de comunicaciones de la zona y se optará por comunicaciones satelitales o el empleo de drones como repetidores para establecer las comunicaciones.

- Partiendo de esta hipótesis, se plantea la circunstancia en la que ha ocurrido un accidente con vertido de combustible(elemento 7 en la ilustración) en las proximidades de una gasolinera en la zona de baja confiabilidad(elemento 2 en la ilustración). Se decide que las tropas presentes en las proximidades, correspondientes a los contingentes español y portugués, acudan a prestar su auxilio y colaborar con los equipos de emergencias civiles presentes en la zona(elemento 10 en la ilustración). A las tropas les acompañarán unos drones para enrutar las comunicaciones(elementos 8 y 9, con el identificativo 'COM').
- Mientras las tropas prestan su auxilio, comienza a observarse comportamiento errático de uno de los drones, que entra en modo a prueba de fallos y acaba adentrándose en la zona adversaria, donde aterriza. Tras unas averiguaciones iniciales, se identifica el comportamiento del dron como una brecha de seguridad que deberá esclarecerse en posteriores investigaciones para evitar que vuelva a ocurrir. Ante esta situación, que parece indicar que la brecha de seguridad ha sido explotada por actuaciones adversarias, el equipo de comunicaciones decide optar por usar este hecho en beneficio propio.
  a) Los permisos de acceso disponibles para el dron deberán modificarse, eliminando los permisos legítimos y añadiendo otros nuevos. Estos nuevos permisos autorizarán el acceso a un "mockup" de la infraestructura e información, que actuará como "honeynet" para monitorizar e investigar las conexiones adversarias. En el capítulo 4 del presente documento se exploran con más detalle las funciones citadas.
  b) Paralelamente, deberá desplegarse un escenario que albergue la nueva infraestructura de comunicaciones.

En los siguientes diagramas, que parten de la jerarquía mostrada anteriormente, se esquematizan las comunicaciones principales que tendrían lugar entre los componentes principales del despliegue, tanto a nivel de infraestructura federada como a nivel operativo.

Por ejemplo, la figura 3.4 muestra unas posibles interacciones que tendrían lugar bajo el contexto del control y la gobernanza de la infraestructura federada. En general, las organizaciones deben aplicar las políticas y requisitos indicados por el organismo jerárquicamente superior, hasta transponerse con configuraciones de los dispositivos implicados en el despliegue; o lo que es lo mismo, el mando de la coalición definirá unas directivas que los mandos nacionales deberán adaptar en forma de políticas aplicabes a los activos conectados en sus respectivos dominios. Así mismo, se deben gestionar las claves propias del sistema, su publicación y validez, de forma transversal ya que al ser un dominio federado las distintas organizaciones deberán poder acceder a las mismas. En el diagrama, se ejemplifica con la adhesión de Portugal en el despliegue, cumpliendo así con el escenario planteado.

La figura 3.5, sin embargo, muestra un conjunto de interacciones necesarias para compartir información de forma segura dentro del entorno federado. El mando de la coalición

define y difunde órdenes de alto nivel, que comunica a los mandos nacionales situados en el estrato inmediatamente inferior. Posteriormente, los mandos nacionales defines y distribuyen órdenes de bajo nivel a sus tropas para cumplir con la misión y los objetivos planteados. De forma similar, pero con sentido opuesto, se generan reportes que van desde las tropas hasta los distintos niveles de mando, agregándose y analizándose oportunamente en cada estrato, tanto de forma manual por parte de las tropas como por una monitorización de los activos. Por último, en la parte inferior puede verse un nivel transversal, que permite compartir información y establecer comunicaciones entre las tropas desplegadas, independientemente de la organización a la que pertenezcan, una vez hayan sido autorizadas en el sistema. Toda la información que se comparta debe asegurar la confidencialidad y la autenticidad de la información, por lo que los usuarios deben estar correctamente identificados y autorizados en el sistema.

Las siguientes secciones del proyecto se centrarán en la gestión de los servicios planteados, como la propuesta de federación de activos en base a la aplicación de unas directivas de configuración planteada en la figura 3.4.

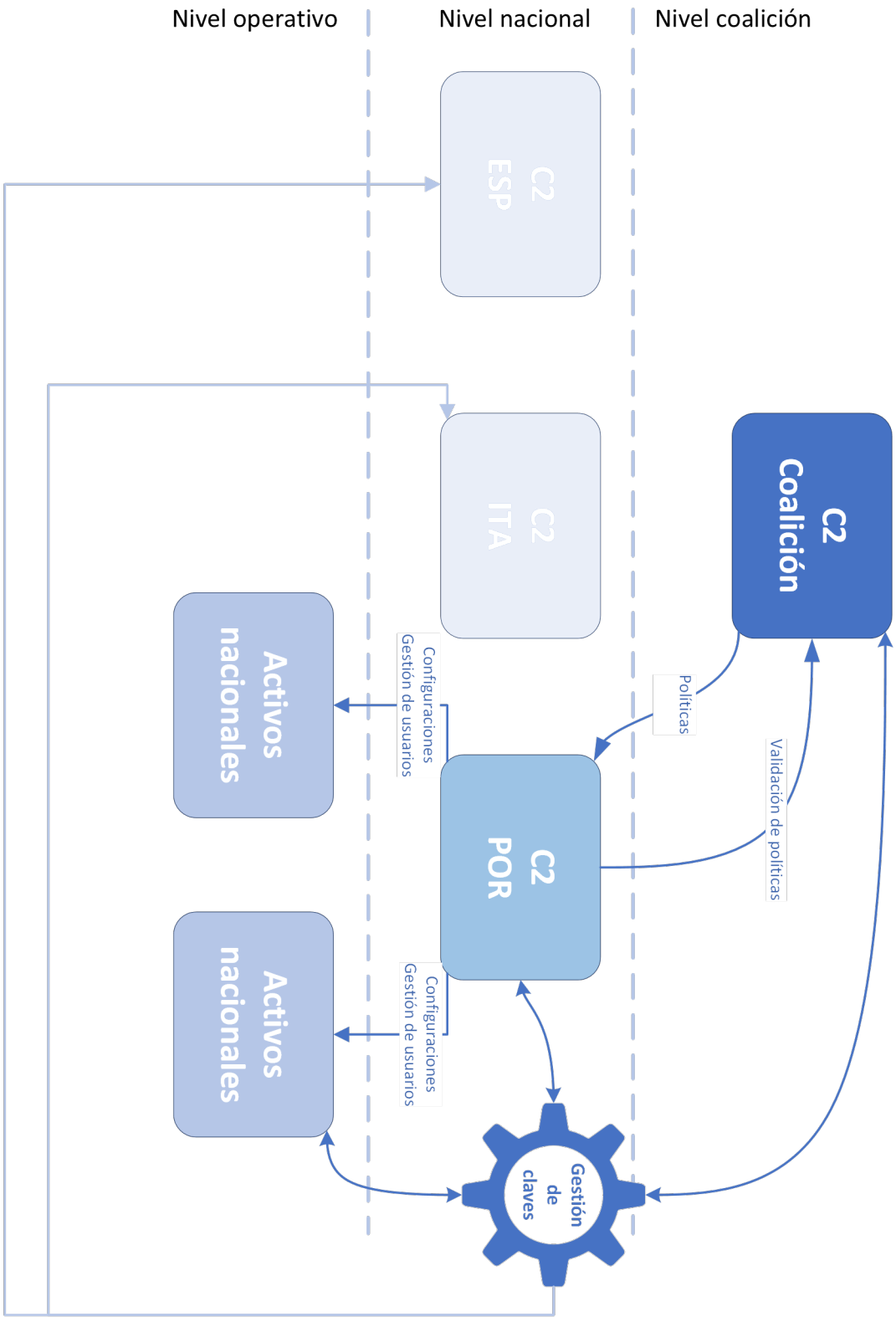


Fig. 3.4. Ejemplo de adhesión de fuerzas portuguesas.

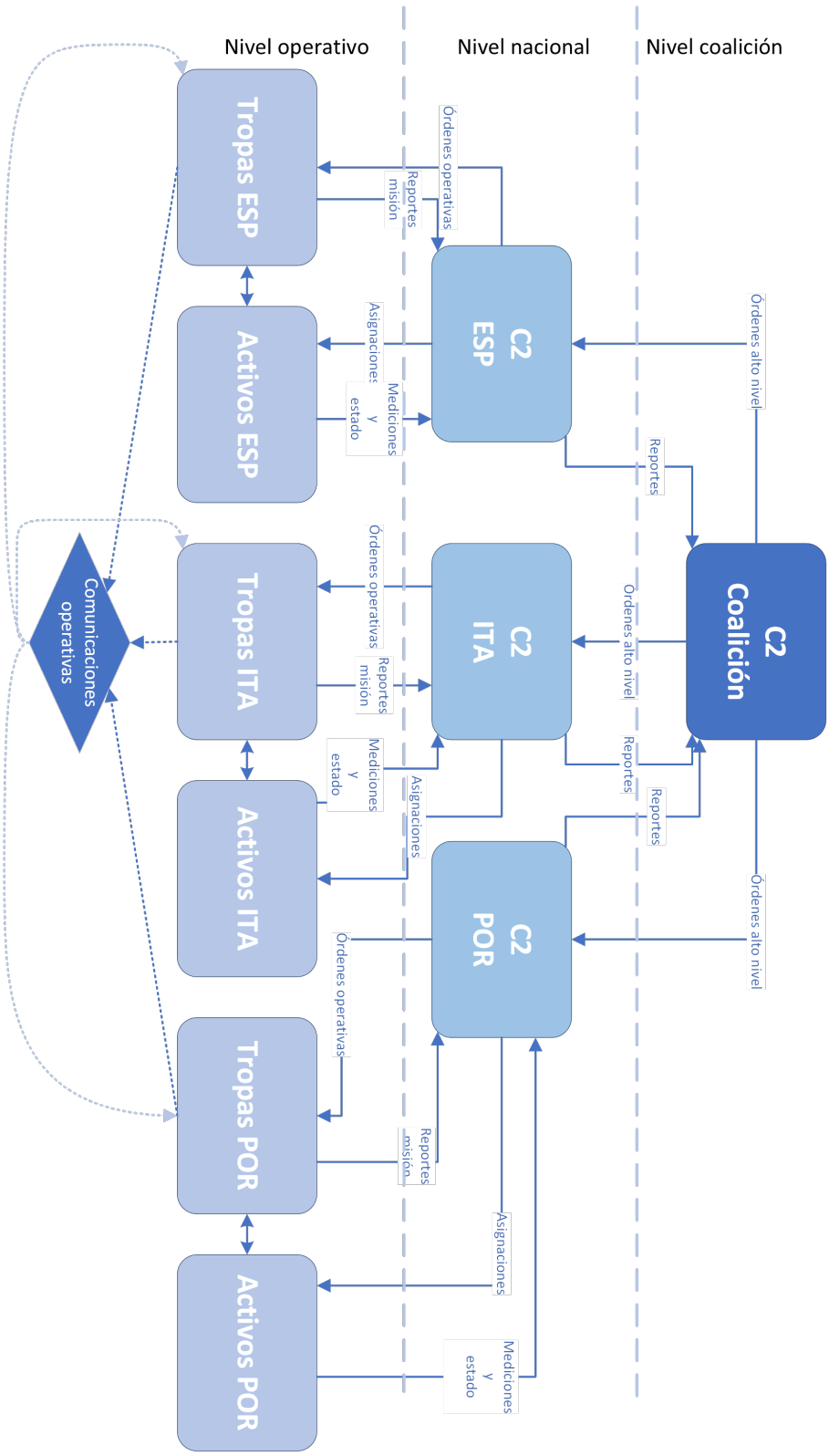


Fig. 3.5. Interacciones del despliegue.

4. FUNCIONES GESTIÓN DE SERVICIO

En la situación mencionada, donde múltiples naciones están presentes en una región conflictiva, Blockchain podría desempeñar diversas funciones en el ámbito del control y los datos, con el propósito de potenciar la seguridad, confiabilidad e integridad de la información [59]. Se examinan diversas funciones para evaluar su adecuación para su incorporación en una subred Blockchain, incluida la definición de órdenes estratégicas, la configuración de Honeynet, la aplicabilidad de políticas, el envío de información táctica de misión y la detección de intentos de acceso no autorizados. Se destaca la importancia de la aplicabilidad de políticas como servicio fundamental para proteger los activos y datos críticos en un entorno de conflicto militar. Los hallazgos de este estudio tienen implicaciones significativas para mejorar la eficiencia operativa y la seguridad en entornos militares desafiantes.

4.1. Definición de órdenes estratégicas

Los contratos inteligentes podrían utilizarse para definir y difundir órdenes estratégicas a nivel operativo para las naciones desplegadas. Estos contratos podrían establecer reglas y condiciones claras para la ejecución de las órdenes, garantizando la transparencia y la inmutabilidad de las mismas. Esta función implica definir y difundir órdenes estratégicas a nivel operativo para las naciones desplegadas en la zona de conflicto. Como requisitos se pueden definir:

- Un sistema de comunicación confiable entre los centros de mando y las unidades desplegadas
- Protocolos de seguridad para garantizar la autenticidad de las órdenes.

Evaluación: Evaluar la complejidad y la criticidad de esta función. ¿Es esencial para el éxito de la operación? ¿Hay sistemas existentes que puedan cumplir esta función de manera eficiente?

1. Complejidad y Criticidad: es esencial para el Éxito de la Operación. La definición y la difusión de órdenes estratégicas son críticas para el éxito de cualquier operación militar. Proporcionan orientación y dirección de las unidades desplegadas. Por lo tanto, esta función es esencial para el logro de los objetivos operativos. La complejidad de esta función radica en la necesidad de establecer las reglas y condiciones de forma clara para la ejecución de las órdenes, asi como, la garantía de la trasparencia y la inmutabilidad de las mismas. La implementación de contratos inteligentes podría simplificar el proceso al automatizar la ejecución de órdenes y garantizar su cumplimiento.

2. En cuanto a los requisitos técnicos, debe tratarse de un sistema de comunicación confiable y debe tener protocolos de seguridad.

   a) Sistema de comunicación Confiable: la red Blockchain (Avalanche, en nuestro caso) proporciona la capacidad de implementar sistemas de comunicación confiables mediante el uso de nodos independientes, bien gestionados y orquestados. Sin embargo, se requerirá una infraestructura de red estable y segura para garantizar la entrega oportuna y segura de las órdenes a las unidades desplegadas.

   b) Protocolos de Seguridad: Blockchain ofrece características de seguridad incorporadas, pero se requerirá un diseño adecuado y la implementación de medidas adicionales para garantizar la autenticidad y la integridad de las órdenes transmitidas a través de la red al implementar y ejecutar contratos inteligentes en Ethereum.

4.2. Configuración de Honeynet

Una de las múltiples virtudes de las redes SDN(introducidas en el apartado 2.3.1), es la agilidad para definir y configurar redes. Esto, unido al concepto de *honeynet*[60], que se basa en crear redes completas a modo de cebo para los atacantes, permite definir entornos adaptados que no puedan ser identificados como redes no legítimas. Por ello, Blockchain podría utilizarse para configurar una red de *honeynet* descentralizada que actúe como una trampa para los adversarios, además de monitorear la información de los sistemas(e.g. logs, conexiones de los firewalls de nueva generación) para investigar y analizar las conexiones adversarias. Los registros de estas conexiones podrían almacenarse de forma segura en la cadena de bloques para su posterior análisis, asegurando así la integridad de la información disponible.

Como requisitos, se puede definir:

- Implementación de nodos de monitoreo y nodos de registro en la cadena de bloques, gracias a una clasificación del tráfico monitorizado para registrar la información legítima y restringir el tráfico ilegítimo, como se ilustra en la figura 4.1
- Protocolos de seguridad para garantizar la integridad de los registros

Evaluación: Evaluar la necesidad de una honeynet en el contexto del despliegue militar. ¿Es crucial para la seguridad de la red? La evaluación de la viabilidad de implementar la Configuración de Honeynet en Blockchain implica considerar varios aspectos:

1. Necesidad y crucialidad: La configuración de una honeynet puede ser crucial para la seguridad de la red en el contexto del despliegue militar, ya que proporciona una capa adicional de defensa contra posibles amenazas cibernéticas y ayuda a monitorear e

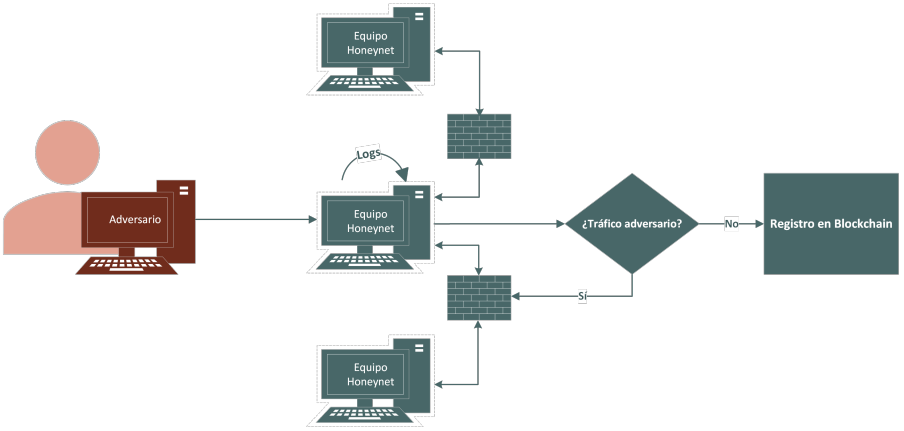


Fig. 4.1. Registros Honeynet.

investigar conexiones adversarias. Esta función puede ser esencial para detectar y mitigar ataques cibernéticos, protegiendo así la infraestructura de comunicaciones críticas utilizada por las fuerzas desplegadas.

2. Requisitos técnicos: Blockchain proporciona la capacidad de implementar nodos de monitoreo y registro en la cadena de bloques mediante contenedores bien gestionados y orquestados. Se requerirá un diseño cuidadoso de la arquitectura de la red para garantizar la distribución efectiva de los nodos y la recopilación segura de los registros de conexión.

4.3. Aplicabilidad de políticas

Al incluir una nueva infraestructura de red, el uso de Blockchain podría facilitar la aplicación de distintas políticas en los dispositivos. Esta función implica definir y aplicar políticas de seguridad en los dispositivos y sistemas desplegados en la zona de conflicto. Se pueden considerar los siguientes requisitos:

- Herramientas para definir y administrar políticas de seguridad
- Capacidades de auditoría y cumplimiento para garantizar que se cumplen las políticas.

Evaluación: Evaluar la importancia de las políticas de seguridad en el entorno de operaciones militares. ¿Son necesarias para proteger los activos y datos críticos? La evaluación de implementar esta función en Ethereum requiere considerar los siguientes aspectos:

1. Protección de Activos y Datos Críticos: Las políticas de seguridad son fundamentales en el entorno de operaciones militares para proteger los activos y datos críticos contra posibles amenazas y vulnerabilidades. Estas políticas ayudan a establecer reglas y procedimientos para el uso seguro y adecuado de la infraestructura de red, garantizando la confidencialidad, integridad y disponibilidad de la información.

2. Herramientas de Gestión de Políticas de Seguridad: Blockchain ofrece la flexibilidad para implementar herramientas de gestión de políticas de seguridad en forma de contenedores, lo que facilita la definición y administración de políticas en los dispositivos y sistemas desplegados en la zona de conflicto. Estas herramientas pueden incluir sistemas de gestión de configuraciones, sistemas de detección y prevención de intrusiones, y herramientas de monitoreo y auditoría.

3. Capacidades de Auditoría y Cumplimiento: Blockchain también proporciona capacidades integradas de auditoría y cumplimiento que pueden ayudar a garantizar el cumplimiento de las políticas de seguridad establecidas. Estas capacidades permiten realizar un seguimiento de los cambios en la configuración de los dispositivos, así como de los eventos de seguridad y las actividades del usuario, para garantizar que se cumplan las políticas definidas.

4.4. Envío de información táctica de misión

Los contratos inteligentes podrían utilizarse para distribuir órdenes y compartir información táctica de misión entre los centros de mando nacionales y las tropas desplegadas. Estos contratos podrían garantizar la confidencialidad de la información y su acceso autorizado por parte de las partes involucradas. Esta función implicaría distribuir órdenes e información táctica de misión entre los centros de mando y las tropas desplegadas. Como requisitos se pueden diferenciar:

- Sistema de comunicación confiable y seguro
- Protocolos para poder garantizar la confidencialidad de la información táctica

Evaluación: Evaluar la importancia de compartir información táctica en tiempo real para el éxito de las operaciones militares. La evaluación de la viabilidad de implementar el Envío de Información Táctica de Misión requiere considerar los siguientes aspectos:

1. Éxito de las Operaciones Militares: El envío de información táctica en tiempo real entre los centros de mando y las tropas desplegadas es crucial para el éxito de las operaciones militares. Proporciona a las unidades en el terreno la información necesaria para tomar decisiones informadas y responder de manera efectiva a las amenazas y situaciones cambiantes.

2. Sistema de Comunicación Confiable y Seguro: Blockchain ofrece la capacidad de implementar sistemas de comunicación confiables y seguros, como servicios de mensajería y canales de comunicación encriptados, que pueden utilizarse para distribuir órdenes e información táctica de misión de manera segura y eficiente.

3. Protocolos de Confidencialidad: Es necesario establecer protocolos de confidencialidad y autenticación para garantizar que la información táctica se comparta únicamente entre las partes autorizadas. Blockchain proporciona herramientas y características que pueden ayudar a garantizar la seguridad y privacidad de la información durante su transmisión.

4.5. Detección de intentos de acceso no autorizados

Blockchain podría utilizarse para detectar y registrar intentos de acceso a la red por parte de usuarios desconocidos y no autorizados. Mediante el uso de contratos inteligentes y registros en la cadena de bloques, se podría mantener un historial de intentos de acceso no autorizados, lo que permitiría identificar posibles amenazas y tomar medidas para proteger la red y sus datos. Esta función implica detectar y registrar intentos de acceso no autorizado en la red desplegada. Se pueden identificar los siguientes requisitos:

- Herramientas de monitoreo de red y detección de intrusiones
- Capacidad de registrar y analizar eventos de seguridad

Evaluación: Evaluar la importancia de la detección de intentos de acceso no autorizados para prevenir ataques cibernéticos en la zona de conflicto. La evaluación de la viabilidad de implementar la Detección de Intentos de Acceso No Autorizados en Blockchain implica considerar los siguientes aspectos:

1. Prevención de Ataques Cibernéticos: La detección y registro de intentos de acceso no autorizados son fundamentales para prevenir ataques cibernéticos en la zona de conflicto. Identificar posibles amenazas y tomar medidas proactivas para proteger la red y sus datos es crucial para mantener la seguridad operativa.
2. Herramientas de Monitoreo de Red y Detección de Intrusiones: Ethereum ofrece la capacidad de implementar herramientas de monitoreo de red y sistemas de detección de intrusiones para identificar actividades sospechosas en la red desplegada en la zona de conflicto.
3. Registro y Análisis de Eventos de Seguridad: Es necesario contar con capacidades para registrar y analizar eventos de seguridad, lo que puede lograrse mediante el uso de herramientas de registro de eventos y análisis de registros disponibles en Docker y otras plataformas.

Tras evaluar todas las gestiones de servicio descritas, se va a implementar en una subred privada la Aplicabilidad de políticas. Este servicio es importante para proteger los activos y datos críticos. La aplicabilidad de políticas requiere herramientas para definir y administrar

políticas de seguridad. Esta operación es importante ya que las políticas de seguridad son cruciales para proteger los activos y datos críticos. Ethereum ofrece herramientas y características que pueden facilitar la implementación de políticas de seguridad en dispositivos y sistemas desplegados en zona de conflicto.

5. DISEÑO DE ARQUITECTURA

En este trabajo, se estudia un ecosistema federado con múltiples organizaciones, sistemas y servicios que se coordinan y comunican entre sí. En consecuencia, resulta oportuno analizar y diseñar los sistemas de una forma estandarizada, beneficiando así su interoperabilidad; en este caso, al tratarse de un ecosistema de coalición cívico-militar, el estándar a utilizar ha sido el ***'NATO Architecture Framework Version 4' (NAFv4)***[61], que es un estándar desarrollado por la OTAN, pero cuyo uso no es exclusivo ni restringido, y las organizaciones que así lo deseen, pueden utilizarlo para definir sus arquitectura. El NAFv4 propone 5 niveles de diseño, que van desde conceptos generales y diseño de alto nivel, hasta el diseño detallado de bajo nivel:

1. Nivel de concepto o capacidad, de más alto nivel.
2. Nivel de especificación de servicios.
3. Nivel de especificación lógica.
4. Nivel de recursos físicos.
5. Nivel de metadatos de la arquitectura, ofreciendo detalle de todos los componentes del sistema a más bajo nivel.

Dentro de estos 5 niveles, se encuadran 46 vistas que se pueden utilizar para definir el producto, pero no es necesario emplear necesariamente las 46 posibles vistas; la organización que decida emplear este *framework* puede decidir qué vistas desarrollar, según cuáles se ajusten a sus necesidades. En este caso, se ha optado por desarrollar únicamente 4 de estas vistas, pues exploran los elementos más característicos del sistema a definir:

1. C1 - Taxonomía de la capacidades, pues define la capacidad general que habilita el servicio para los despliegues de la federación.
2. S1 - Taxonomía de servicios, pues define qué servicios involucrará el desarrollo del sistema.
3. S6 - Interacciones entre servicios, centrándose en el servicio a definir, define las interacciones que involucran al mismo.
4. P7 - Modelo físico de datos, para definir a alto nivel la información que se gestionará a través de las distintas interfaces del servicio.

La figura 5.1 muestra todas las vistas, resaltando las seleccionadas para este caso:

A continuación, se detallan los objetivos y resultados de cada vista.

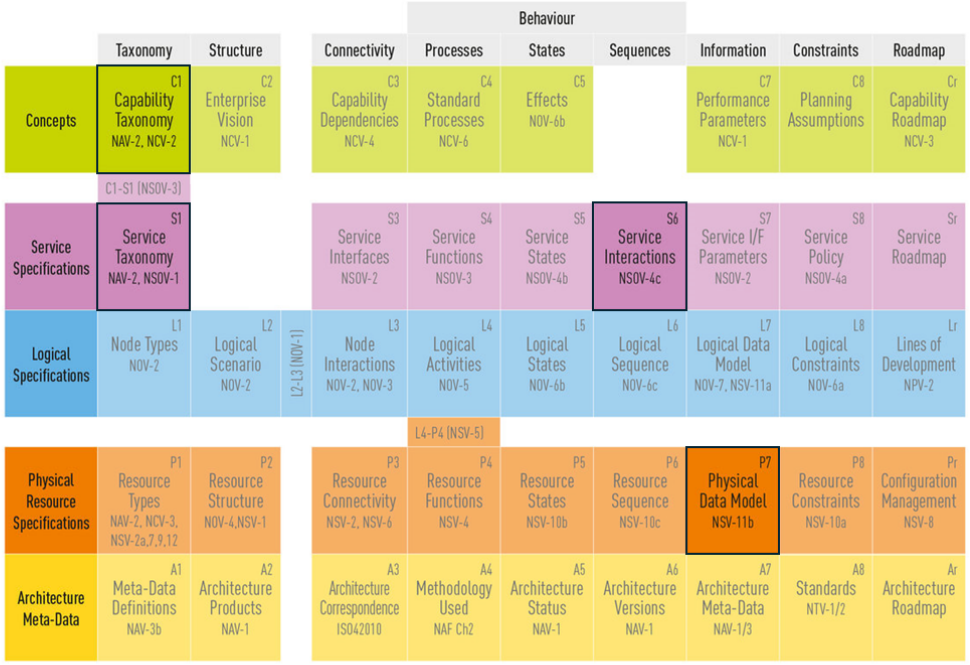


Fig. 5.1. Vistas NAF.

5.1. Taxonomía de capacidades

La vista C1 se encarga de identificar y organizar capacidades; en este caso, sólo se ha usado para identificar y organizar capacidades internas del sistema estudiado, es decir, las capacidades relativas a la implantación de un sistema basado en Blockchain. En la figura 5.2, las capacidades se diferencian en 3 niveles según su usuario objetivo, es decir, si se usará a nivel de federación, a nivel nacional o a nivel operativo en las misiones; además, la capacidad de análisis de resultados se encuentra transversalmente en los niveles nacionales y de coalición, ya que podría aplicarse en ambos escenarios. Las 3 capacidades destacadas en rojo, relativas a la gestión y el C2 de los despliegues, encuadran el foco que seguirán las siguientes vistas y el desarrollo del presente trabajo.

5.2. Taxonomía de servicios

De forma similar a la vista C1, la vista S1 trata de identificar y organizar los servicios, que en nuestro caso se equiparan a las funciones identificadas en el caso de uso. La organización presentada en la figura 5.3 clasifica los servicios en gestión de infraestructura y servicios habilitados por la propia infraestructura. El servicio destacado, de aplicabilidad de las políticas, será el considerado en las próximas fases del estudio.

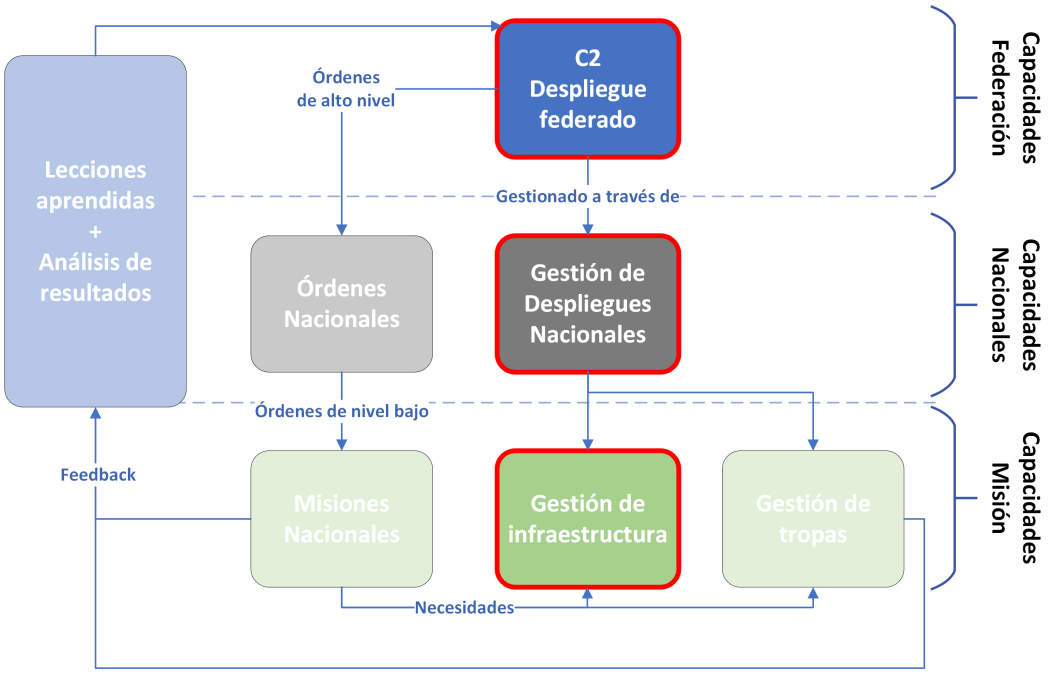


Fig. 5.2. Vista C1 NAF.

5.3. Interacciones entre servicios

La vista S6 de la figura 5.4, centrada en el servicio de aplicabilidad de políticas, identifica las interacciones, comunicaciones y dependencias entre servicios. El sentido de las interacciones indica qué servicio es el consumidor en cada caso, y la secuencia vertical indica el orden lógico que podría darse en la interacción entre servicios, aunque no es único ni excluyente.

5.4. Modelo físico de datos

Esta última vista P7, incluída en la figura 5.5, trata de identificar los tipos de datos que se usan en un servicio determinado. Como se hizo en la anterior vista, el centro de la vista P7 será el servicio de aplicabilidad de políticas, y se identificará el conjunto mínimo de datos necesario para ofrecer funcionalidades básicas del servicio. Además, se identifica la fuente de estos datos, en caso de proceder de otro servicio o interacción.

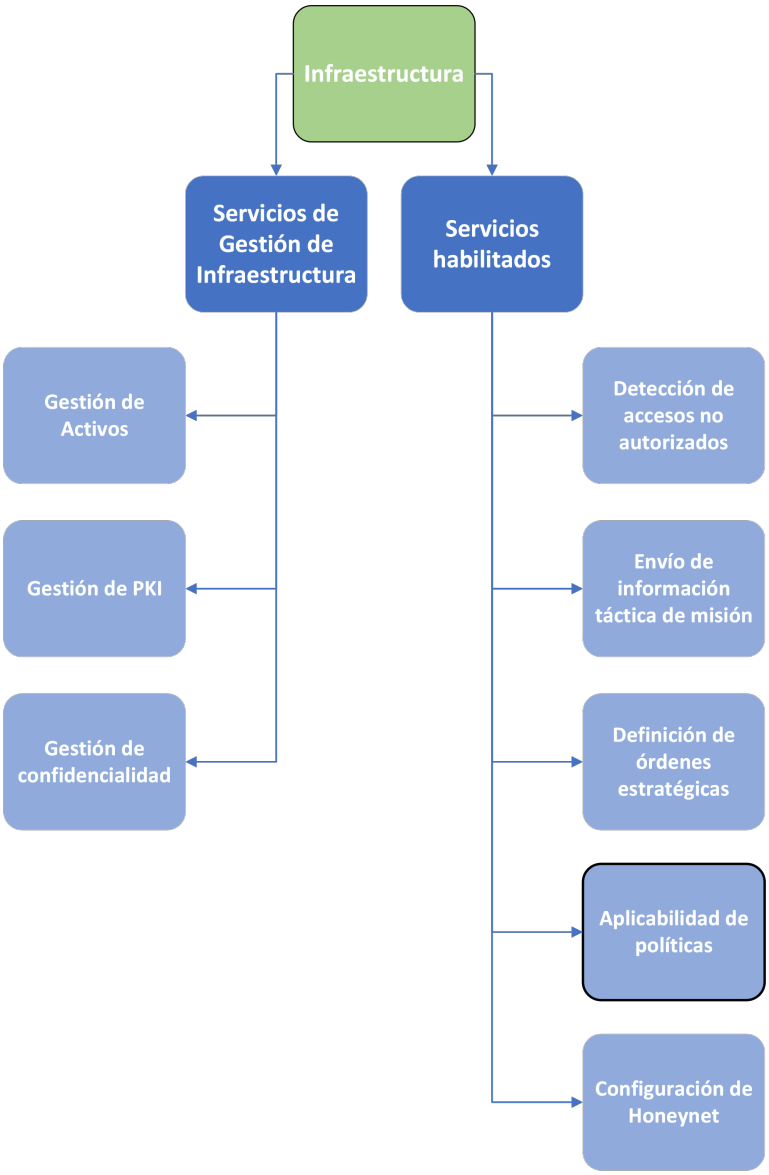


Fig. 5.3. Vista S1 NAF.

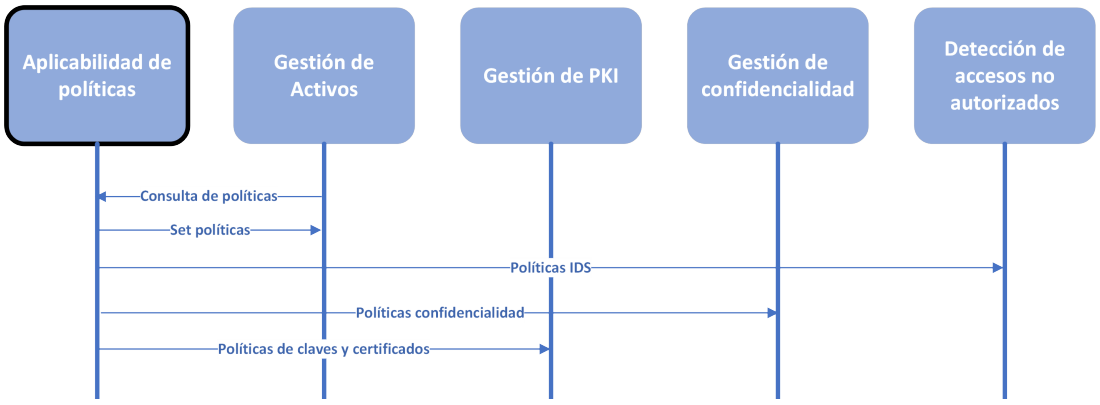


Fig. 5.4. Vista S6 NAF.

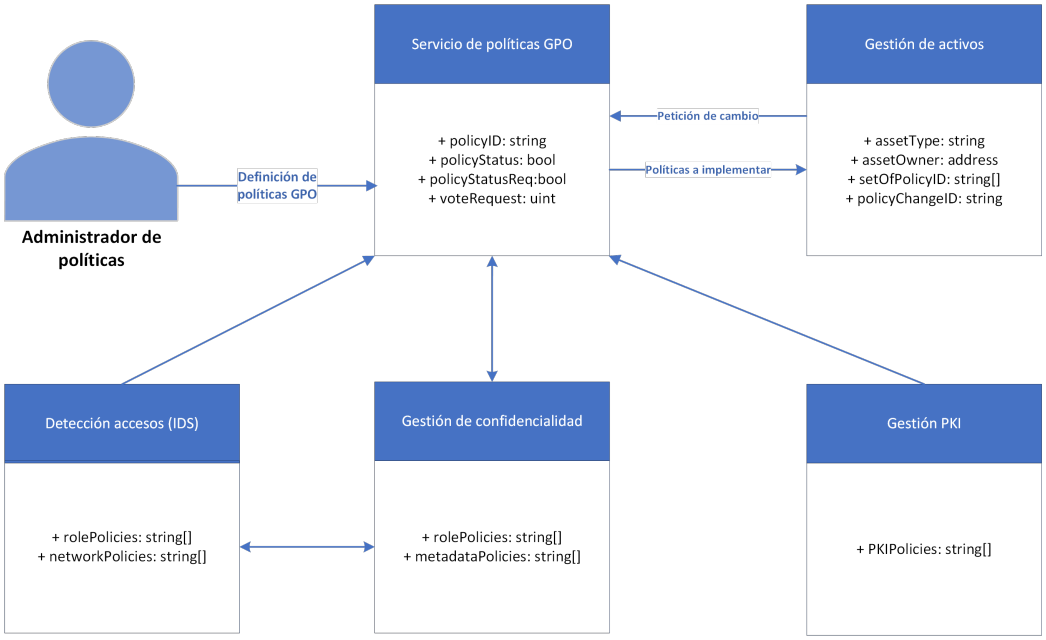


Fig. 5.5. Vista P7 NAF.

6. DESARROLLO DE DAPP

Como se ha visto hasta ahora, Blockchain no es un sistema único, y existen diversas alternativas disponibles. Para el caso de estudio, lo apropiado sería una blockchain privada; por ello, el primer paso es explorar los despliegues de blockchain privados.

Para ello, se ha usado **Avalanche-CLI**, una suite de Avalanche(Blockchain derivada de Ethereum) que permite hacer despliegues de subredes de prueba. En caso de configurar los despliegues y mantener el acceso a la red pública restringido, estas subredes se considerarán privadas.

6.1. Avalanche-CLI

La configuración y despliegue de la subred se realiza de forma sencilla y guiada, una vez se ha instalado Avalanche-CLI en el equipo, que en este caso fue una máquina virtual Ubuntu, ya que sólo está disponible actualmente para dispositivos Linux y Mac OS. En las ilustraciones 6.1 y 6.2 puede verse cómo se configura y despliega la subred 'TFMSubnet'.

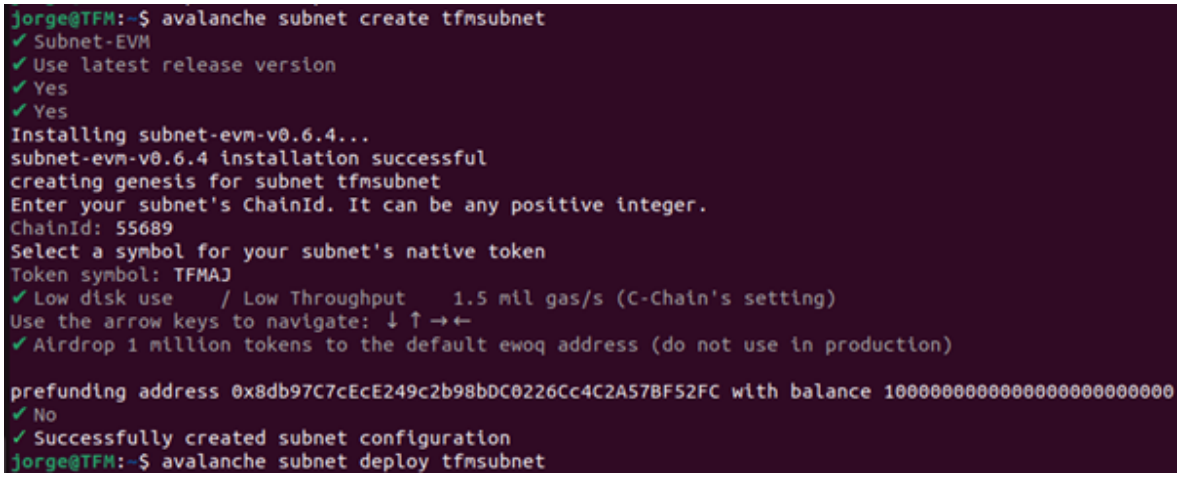


Fig. 6.1. Configuración de subred.

A continuación, con el fin de poder realizar pruebas de despliegue de contratos en nuestra subred privada, se utilizará el wallet **Metamask**, dado que tiene facilidades para integrarse con subredes privadas. Para configurar una cuenta, sólo es necesario crear un wallet y configurarlo con los datos obtenidos en el despliegue para poder conectarlo con nuestra subred, disponiendo así de los 10.000.000 tokens TFMAJ que hemos configurado para los nuevos nodos. Esta configuración, así como los fondos disponibles, pueden apreciarse en las figuras 6.3 y 6.4.

A continuación, es necesario seleccionar un IDE para realizar pruebas sobre nuestra su-

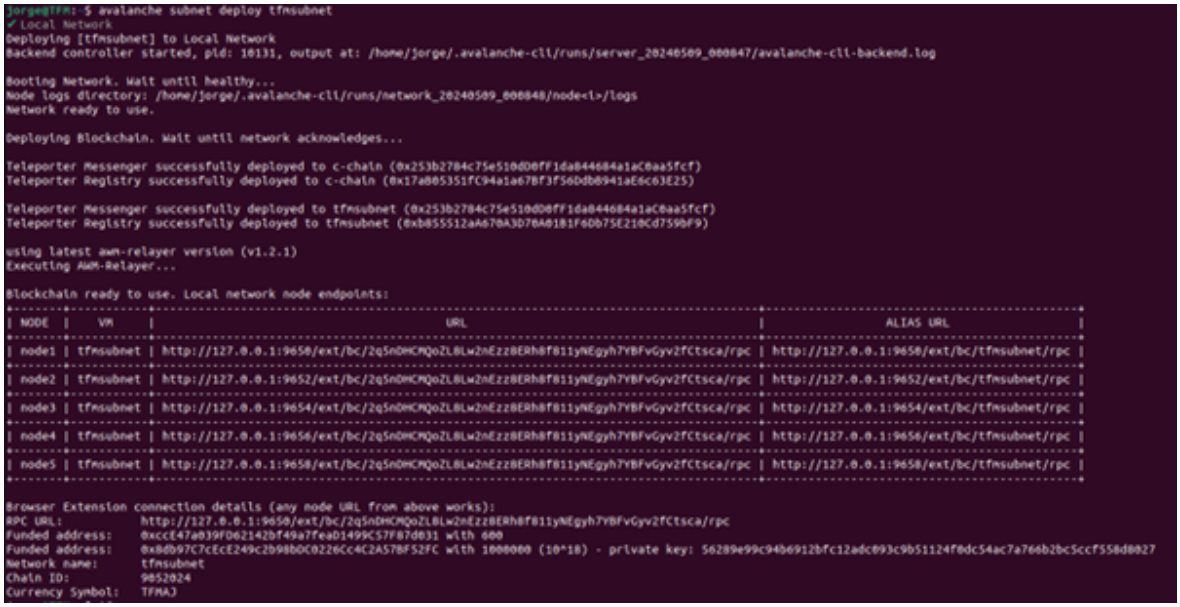


Fig. 6.2. Despliegue de subred.

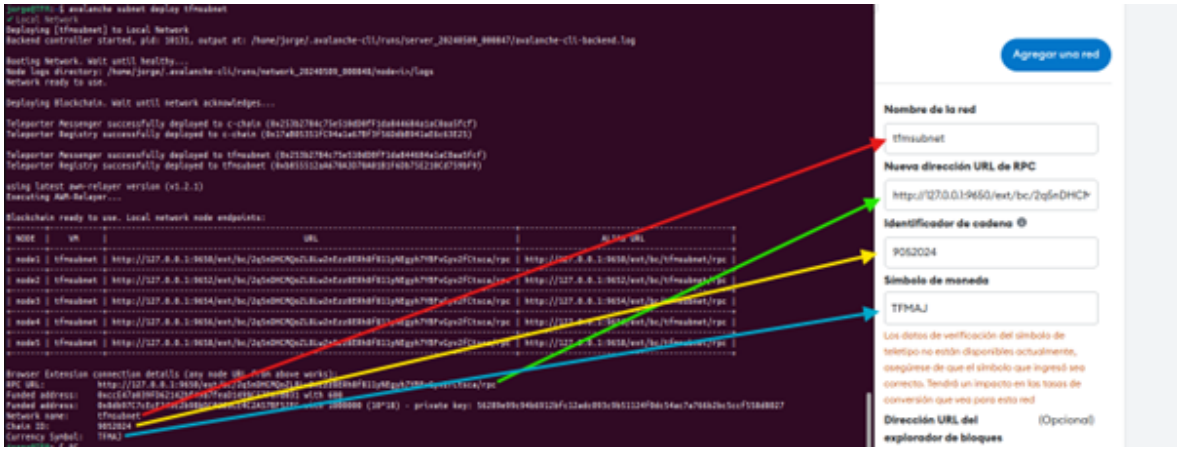


Fig. 6.3. Configuración del wallet.

bred. A pesar de que la opción de **Hardhat** es muy popular y extendida, es una opción que descartamos debido a los problemas que presenta la versión actual para integrarse con subredes privadas y la falta de soporte técnico; finalmente, la opción seleccionada fue **Remix**, que principalmente emplea el lenguaje Solidity(muy similar a JavaScript) para elaborar sus contratos, aunque diferentes plug-ins permiten desarrollar en distintos lenguajes, como variaciones de Python.

Gracias a la integración con Metamask, podemos conectar el IDE Remix con nuestra subred fácilmente, como muestra la figura 6.5.

Finalmente, para probar el correcto funcionamiento de la subred, se realiza un despliegue de un contrato de prueba ofrecido por Remix, un contrato de NFT. Para ello, sólo hay que realizar dos pasos:

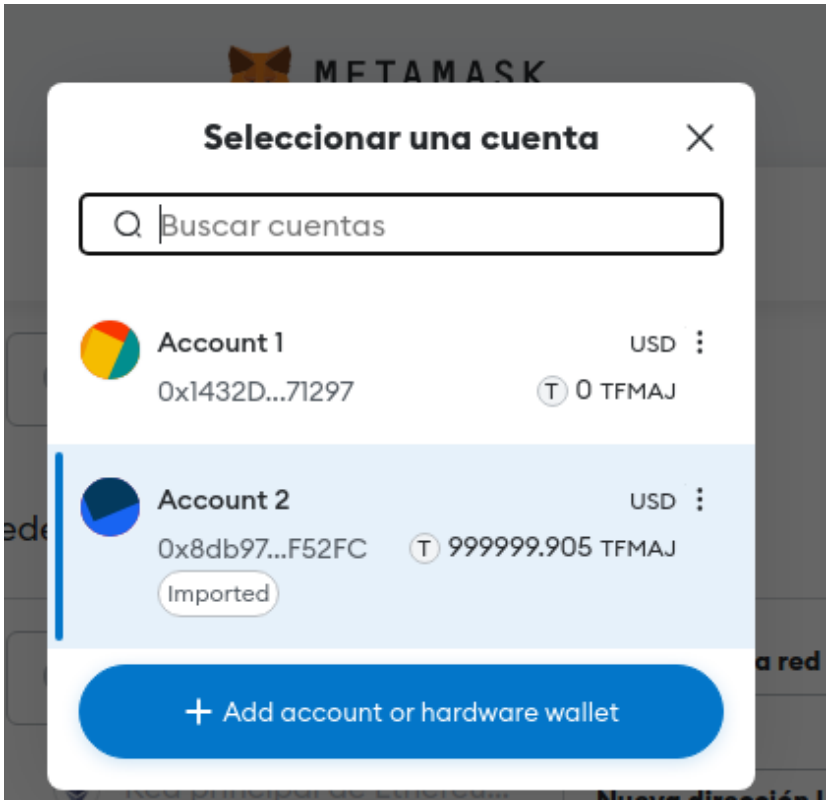


Fig. 6.4. Fondos disponibles.

1. Realizar una compilación del código para comprobar la correcta sintaxis del mismo. Este paso se puede comprobar en la figura 6.6.

2. Desplegar el contrato en la subred, confirmando el despliegue a través del wallet Metamask. Este paso se puede comprobar en la figura 6.7, con el detalle de confirmación en el wallet en la figura 6.8.

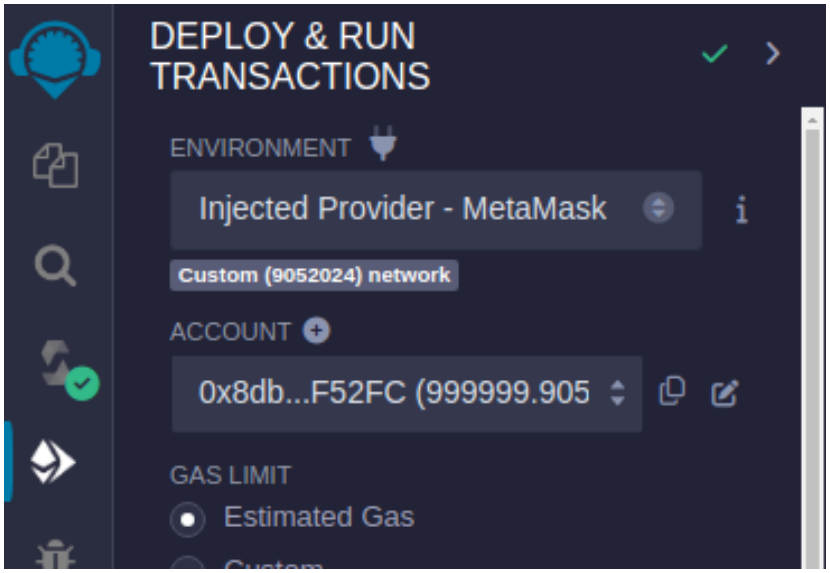


Fig. 6.5. Configuración Remix-Sunred.

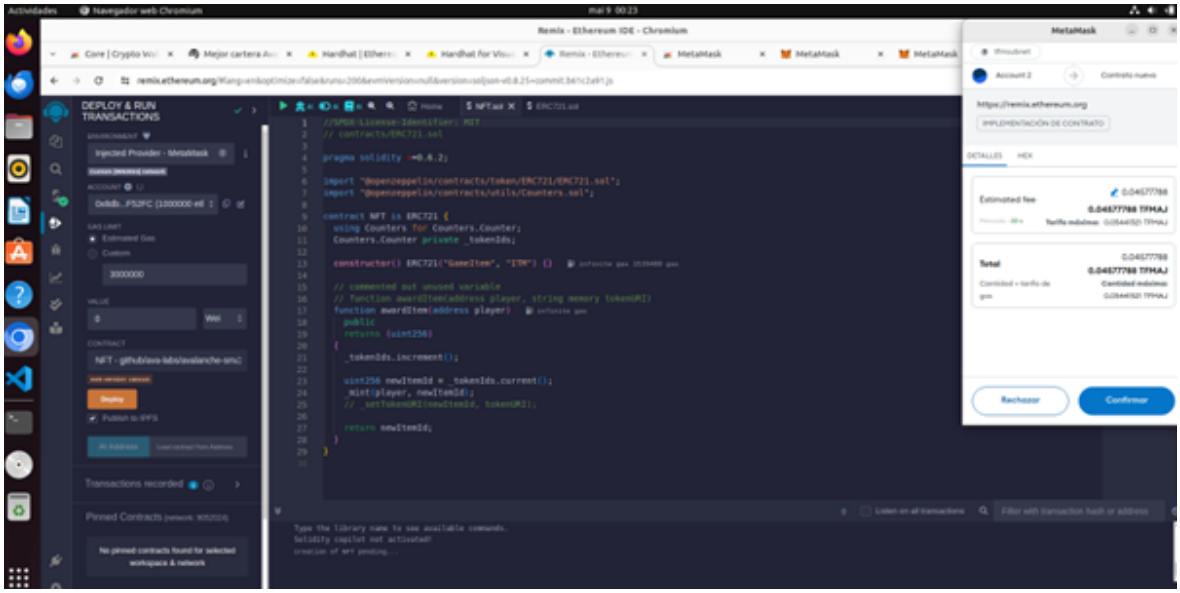


Fig. 6.6. Compilación del código.

Fig. 6.7. Comprobación de despliegue.

Fig. 6.8. Detalle de confirmación del despliegue.

6.2. Remix IDE y Remix VM

Como alternativa a continuar el desarrollo en una blockchain privada, se optó por utilizar los entornos de desarrollo ofrecidos por Remix. Conocido como **JavaScript VM**, Remix ofrece unos *sandbox* accesibles directamente desde el IDE para realizar desarrollos. En este caso, se han usado 5 indistintamente, ya que ofrecen idénticas características:

- **Remix VM (Cancun)**: *sandbox* referido al fork de Ethereum de Cancún.
- **Remix VM (Shanghai)**: *sandbox* referido al fork de Ethereum de Shanghai.
- **Remix VM (Paris)**: *sandbox* referido al main fork de Ethereum.
- **Remix VM (London)**: *sandbox* referido al fork de Ethereum de Londres.
- **Remix VM (Berlin)**: *sandbox* referido al fork de Ethereum de Berlín.

El código desarrollado, que implementa funciones simples para la gestión descentralizada de las políticas aplicables en un dominio, se desglosará a continuación. En nuestro caso, un dominio abarca todos los activos federados bajo una autoridad, que puede ser a nivel nacional o de coalición.

Tras indicar qué versión de compilador se usará, acorde con la versión que se encuentre desplegada en la blockchain a usar(0.8.7, la última disponible), se declara el contrato GPOPolicy y las estructuras de datos a usar:

- Una estructura de política arbitraria, **struct policy**, que consta de variables indicando su estado, el estado al que se solicitan cambios, un recuento de cuántos usuarios han solicitado el cambio y un identificador de política. Para simplificar el desarrollo, se han tomado sólo dos estados posibles para las políticas: activo o inactivo; estos estados resultan limitados para algunas políticas, y futuros desarrollos de este contrato deberían abarcar más posibiles estados.
- Dos mapeos, que son estructuras similares a los clásicos diccionarios de otros lenguajes, usados para enlazar una clave y un valor. El mapeo **isAuthorized** se emplea para comprobar la autorización de una dirección determinada; el mapeo **policies** se emplea para crear una estructura que almacene todas las políticas definidas.
- Una dirección **owner** que almacenará la dirección del nodo que despliegue el contrato.
- Un modificador, **onlyOwner**, que sirve para restringir el uso de determinadas funciones al resto de usuarios, y que sólo pueda ejecutarlas el nodo que desplegó el contrato.
- Un constructor, que haciendo uso de **owner** y **isAuthorized** comprueba que el usuario que despliega el contrato está autorizado.

```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.7;
contract GPOPolicy {
    mapping (address => bool) public isAuthorized;

    struct policy {
        bool status;
        bool reqStatus;
        string policyID;
        uint vote;
    }
    address public owner;
    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }
    mapping (string => policy) public policies;
    constructor () {
        owner = msg.sender;
        isAuthorized[owner] = true;
    }
    [. . .]
}
```

A continuación, se describen las funciones implementadas:

- Función **addPolicy**, usada para añadir una política a la lista desplegada en Blockchain, asegurando su integridad. Inicialmente, se creará inactiva, sin petición de cambio y con un ID determinado. Sólo podrá ser ejecutada por un administrador de políticas, en este caso, por el nodo desplegador del contrato

  El uso esperado de esta función es mediante un frontEnd o un script automatizado para crear una lista de políticas similar a la de cualquier solución LDAP.

```

    function addPolicy(string memory policyID) public onlyOwner{
        policy memory newPolicy = policy(false, false, policyID, 0);
        policies[policyID] = newPolicy;
    }
```

- Función **setPolicy**: esta función define el estado de una política definida. Al igual que la función anterior, su uso esperado es a través de un fronEnd o un script que automatice los estados iniciales de todas las políticas definidas.

  Cuando se modifica el estado de una política, se reinicia su posible petición de cambios.

```
1
2       function setPolicy(string memory policyUID, bool status) public
            onlyOwner {
3           policies[policyUID].status = status;
4           policies[policyUID].reqStatus = status;
5           policies[policyUID].vote = 0;
6       }
```

- Función **getPolicy**: esta función devuelve los detalles sobre el estado de una política determinada.

```
1
2       function getPolicy(string memory policyUID) public view returns
            (bool) {
3           return policies[policyUID].status;
4       }
```

- Función **requestPolicyChange**: cuando un usuario autorizado en el sistema quiera solicitar un cambio en las políticas, puede realizarlo utilizando esta función. Como se explicó anteriormente, se han simplificado los posibles estados de las políticas a un booleano que indica si se aplican o no.

```
1
2       function requestPolicyChange(string memory policyId, bool
            statusRequest) public {
3           require(keccak256(abi.encodePacked(policies[policyId].
                policyID)) == keccak256(abi.encodePacked(policyId))); //
                Verify policy exists
4           if(policies[policyId].reqStatus!=statusRequest){
5               policies[policyId].vote++; // Increase vote count
6               policies[policyId].reqStatus=statusRequest;
7           }
8           else{}
9
10      }
```

- Función **checkPolicyVote**: un administrador, o un proceso automático que así se desea, podrá comprobar las peticiones de cambio de una política para evaluar su posible modificación.

```
1
2       function checkPolicyVote(string memory policyId) public view
            returns (uint){
3           require(keccak256(abi.encodePacked(policies[policyId].
                policyID)) == keccak256(abi.encodePacked(policyId))); //
                Verify policy exists
```

```
        return policies[policyId].vote;
    }
```

- Función **applyPolicyChange**: Tras evaluar las solicitudes de cambio de una política, un administrador podrá aplicar los cambios solicitados

```

    function applyPolicyChange(string memory policyId, bool status)
        public onlyOwner {
        policies[policyId].status = status;
        policies[policyId].reqStatus = status;
        policies[policyId].vote=0;
    }
```

6.3. Avalanche C-Chain

Finalmente, tras definir un código funcional, se procede a desplegar en una blockchain pública que ofrezca un entorno de pruebas apropiado. La elección final fue la C-Chain de la blockchain Fuji, que es una red de pruebas de Avalanche.

Esta red de pruebas es una répica de la red principal de Avalanche, y ofrece todas sus funcionalidades. Es un entorno ideal para que los desarrolladores prueben y refinen sus desarrollos antes de desplegarlos en la red final.

Para realizar despliegues en C-Chain, sólo es necesario:

- Un wallet, en nuestro caso el wallet elejido fue **Core**, dado que tiene integración con los principales sistemas. En la figura 6.9 se muestra el wallet con una cuenta conectada a la red de pruebas C-Chain.
- Dado que el despliegue se realizará en una blockchain real, aunque sea de pruebas, es necesario disponer de tokens AVAX. Fuji tiene un grifo de tokens habilitado para solicitar tokens, y sólo es necesario cumplir ciertos requisitos que verifiquen la voluntad del usuario para desarrollar. En la figura 6.10 se pueden observar los requisitos y la validación de los mismos, mientras que en la figura 6.11 puede verse cómo se dispone de fondos en el monedero y en la figura 6.12 se pueden verificar las transacciones de tokens hacia el monedero creado para las pruebas.

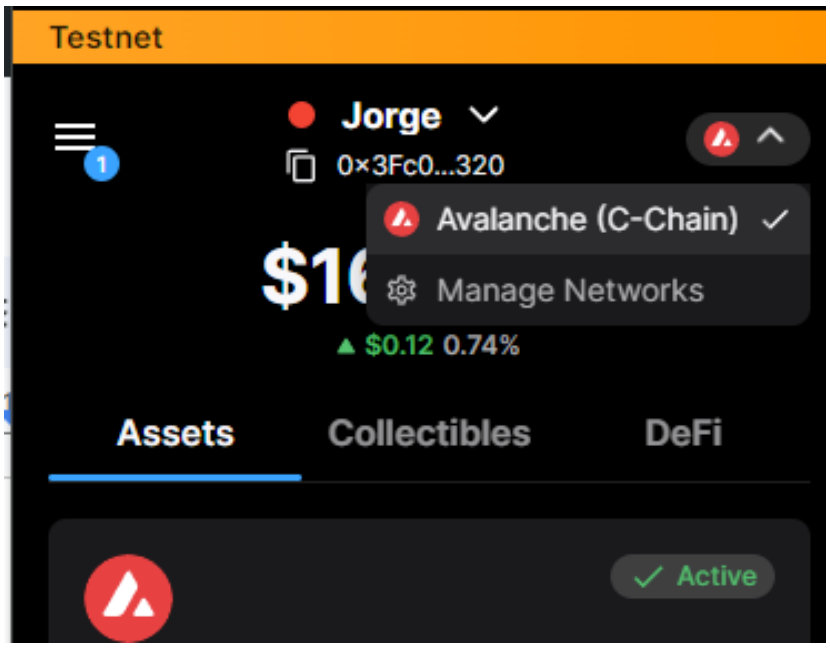


Fig. 6.9. Wallet Core.

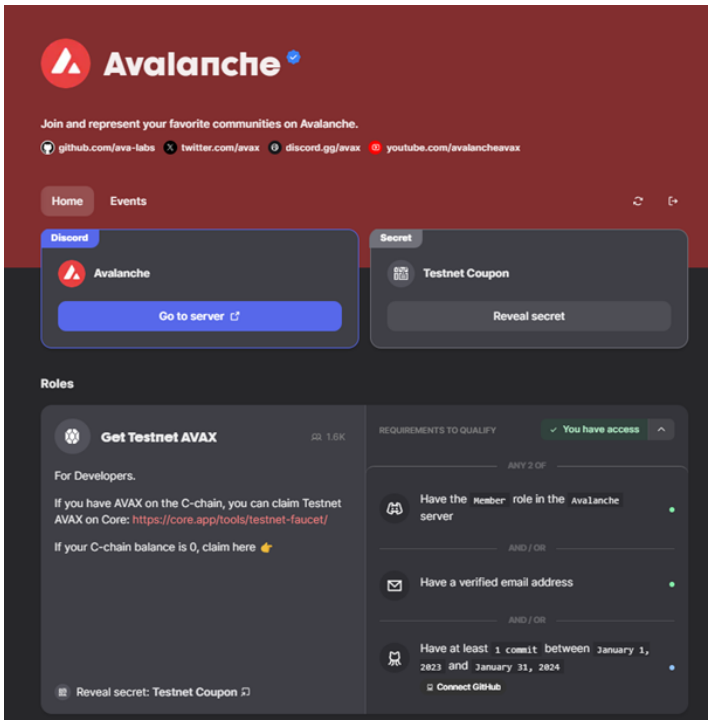


Fig. 6.10. Verificaciones Fuji.

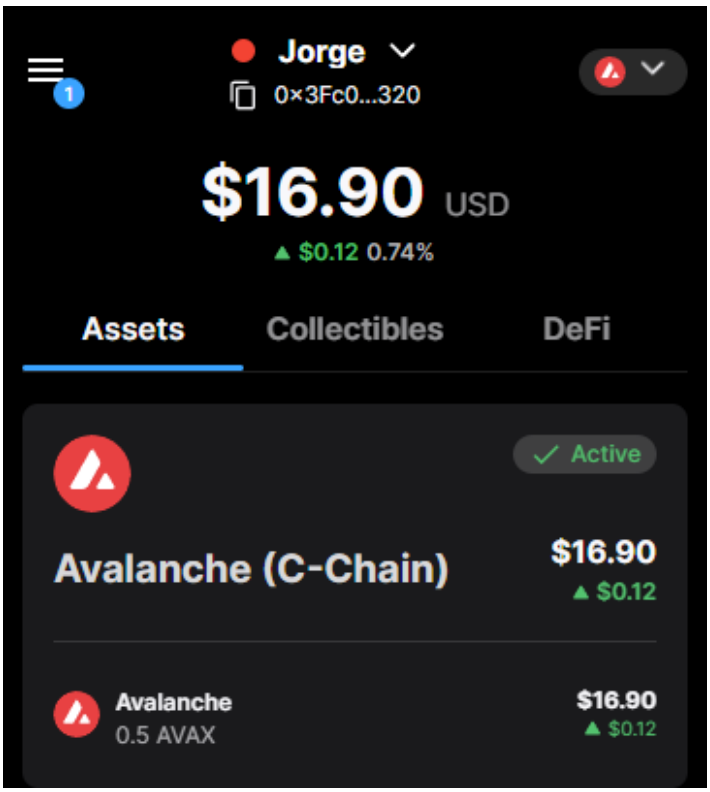


Fig. 6.11. Fondos en el monedero.

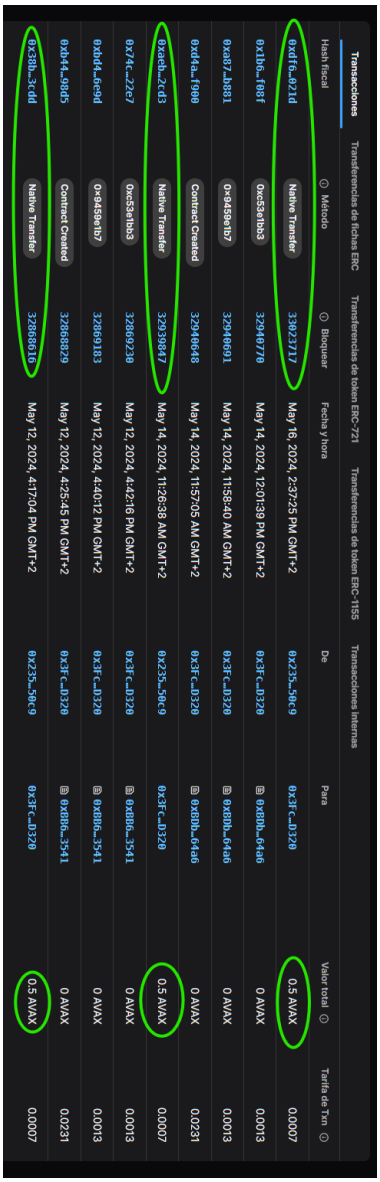


Fig. 6.12. Transacciones.

- Por último, para poder desplegar nuestro contrato en la red, es necesario conectar el IDE Remix con nuestra cuenta en Fuji C-Chain. Este proceso es sencillo, y sólo requiere integrar el Wallet en el entorno de Remix, como muestra la figura 6.13.

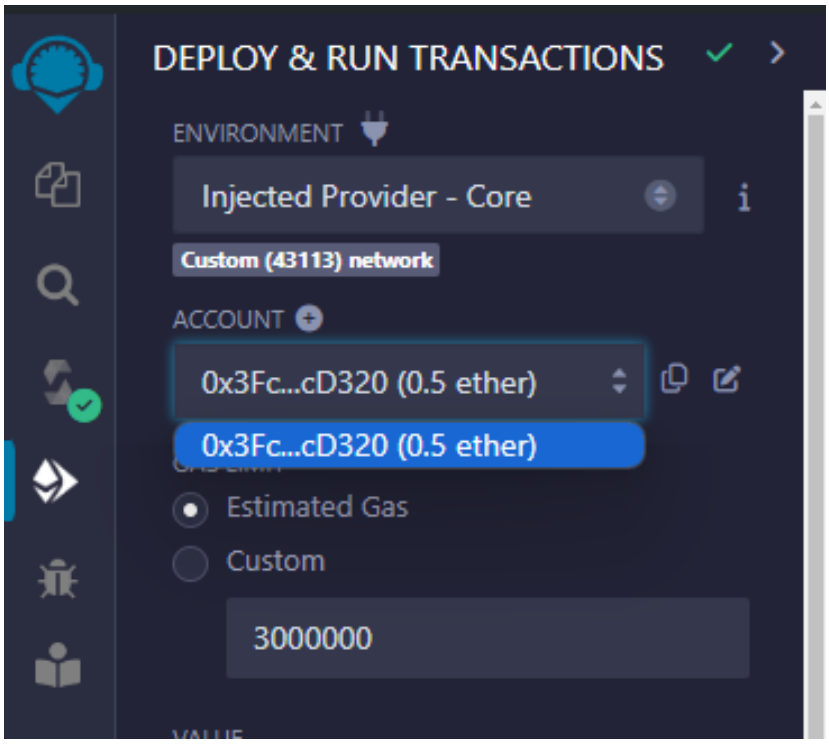


Fig. 6.13. Wallet Core.

Tras configurar todos los elementos, es posible realizar la compilación, el despliegue y la ejecución del contrato desarrollado. La figura 6.14 muestra cómo se compila el contrato con las marcas verdes, mientras que la marca roja muestra la correcta compilación del mismo. Finalmente, se puede proceder a su despliegue en la C-Chain, con la salvedad de que ahora es necesario confirmar los despliegues y las transacciones, como se puede apreciar en la figura 6.15.

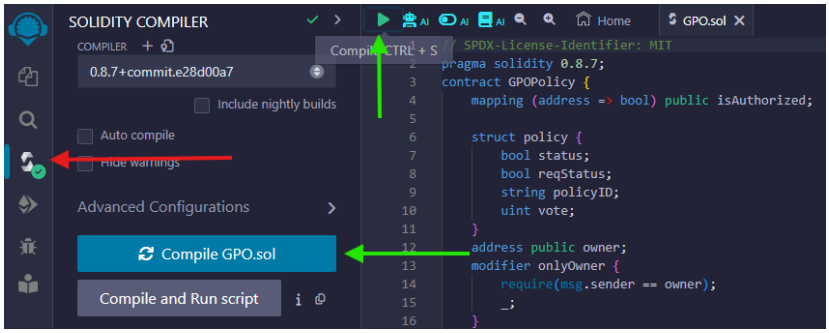


Fig. 6.14. Compilación en Remix IDE.

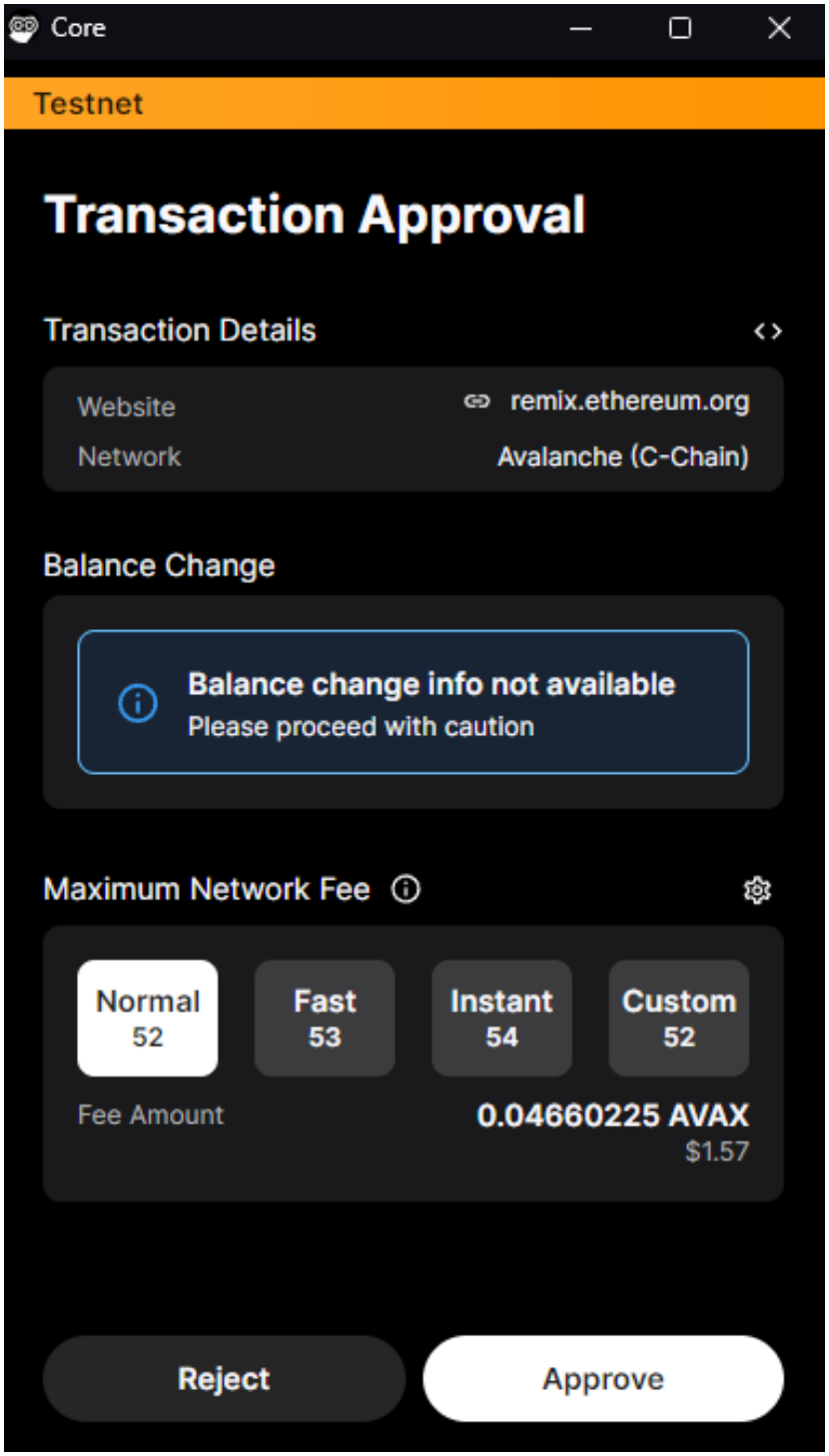


Fig. 6.15. Confirmación de transacción de despliegue de contrato.

En este punto es útil explicar el concepto de **tasa de gas** que se muestra en el IDE Remix, como se puede apreciar en el detalle de la figura 6.16. El concepto abstracto hace referencia a la cantidad de trabajo requerida para ejecutar una transacción en la red blockchain de Ethereum. Resulta más comprensible ver la *tasa de gas* como el coste energético asociado a la transacción, que se traduce en una determinada unidad monetaria.

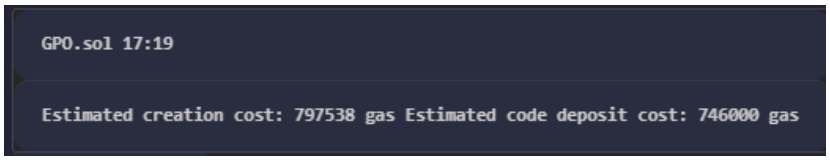


Fig. 6.16. Detalle de la tasa de gas estimada en Remix.

7. ANÁLISIS DE RESULTADOS Y DESAFÍOS

Tras el proceso de diseño y despliegue comentado en el capítulo 6, en este capítulo se presentará y evaluará el contrato diseñado para el servicio de políticas dentro de un dominio de la organización.

Atendiendo al diagrama mostrado en la figura 3.4, las políticas se definirán a nivel de federación, y acabarán por transponerse en configuraciones aplicadas a los distintos activos nacionales. La figura 7.1 particulariza las definiciones de la figura 3.4, mostrando las funcionalidades e interacciones propias del servicio de GPO definido.

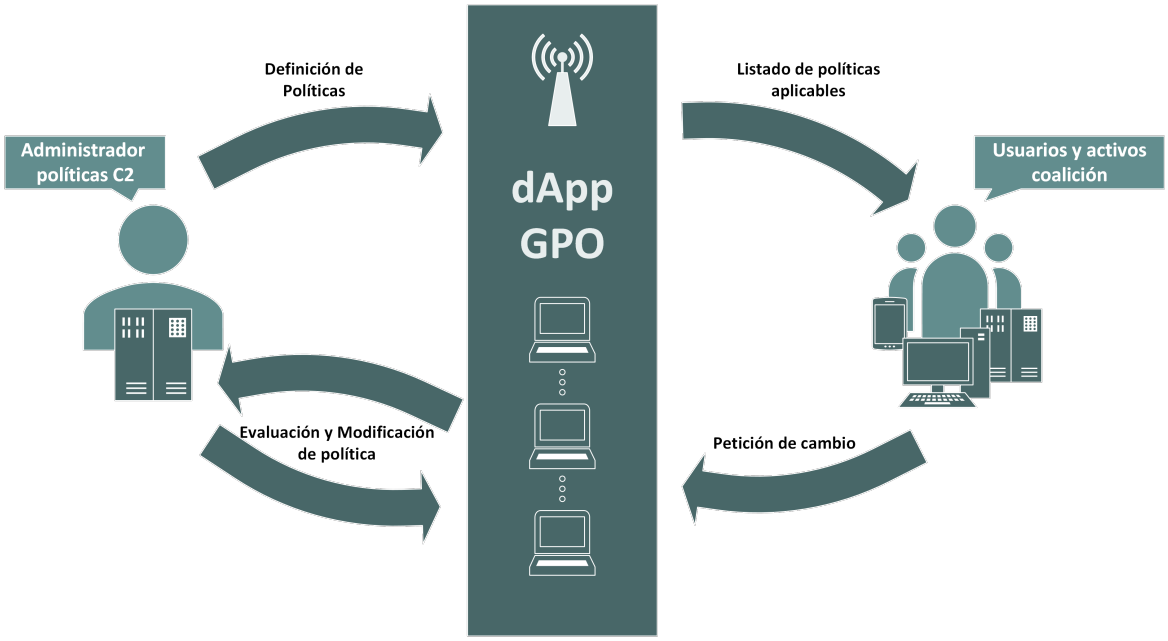


Fig. 7.1. Diagrama de servicio GPO.

En la figura puede observarse que se contemplan dos tipos de perfiles:

- Un perfil privilegiado, denominado **administrador de políticas C2**. Este perfil se encarga de definir las políticas y sus estados, y también evaluará y aplicará las peticiones de cambios sobre las mismas.
- Un perfil de usuario, que equivale al personal de la coalición. Estos usuarios harán uso de los activos en los que se aplicarán las políticas y configuraciones definidas.

  Si, en su uso habitual, detectaren deficiencias o mejoras en la configuración de las políticas, podrán solicitar un cambio en las mismas.

7.1. Despliegue y preparación para el análisis

El producto diseñado se basa en las funcionalidades básicas descritas en la sección 6.2, sobre las que se derivan ciertas funcionalidades avanzadas. A continuación, se muestran los resultados del despliegue(la figura 7.2 muestra la transacción en la red pública, mientras que la figura 7.3 muestra los detalles de la propia publicación del contrato) y las pruebas del producto desplegado sobre Fuji C-Chain.

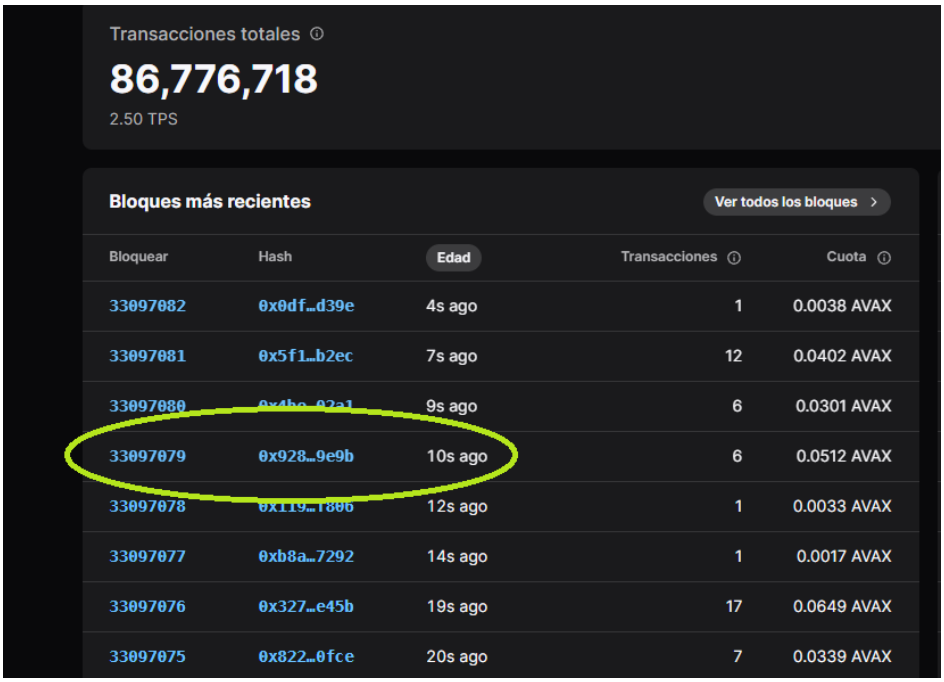


Fig. 7.2. Transacción en los registros públicos.

En ambas figuras, 7.2 y 7.3, puede observarse el mismo identificador de bloque, que sirve para comprobar que ambas capturas hacen referencia a la misma transacción, el ID 33097079. Además, en la figura 7.3, puede consultarse gran variedad de información de la transacción, como cuántos bloques la han validado hasta el momento (sexto campo), el tipo de transacción, su coste, etc.

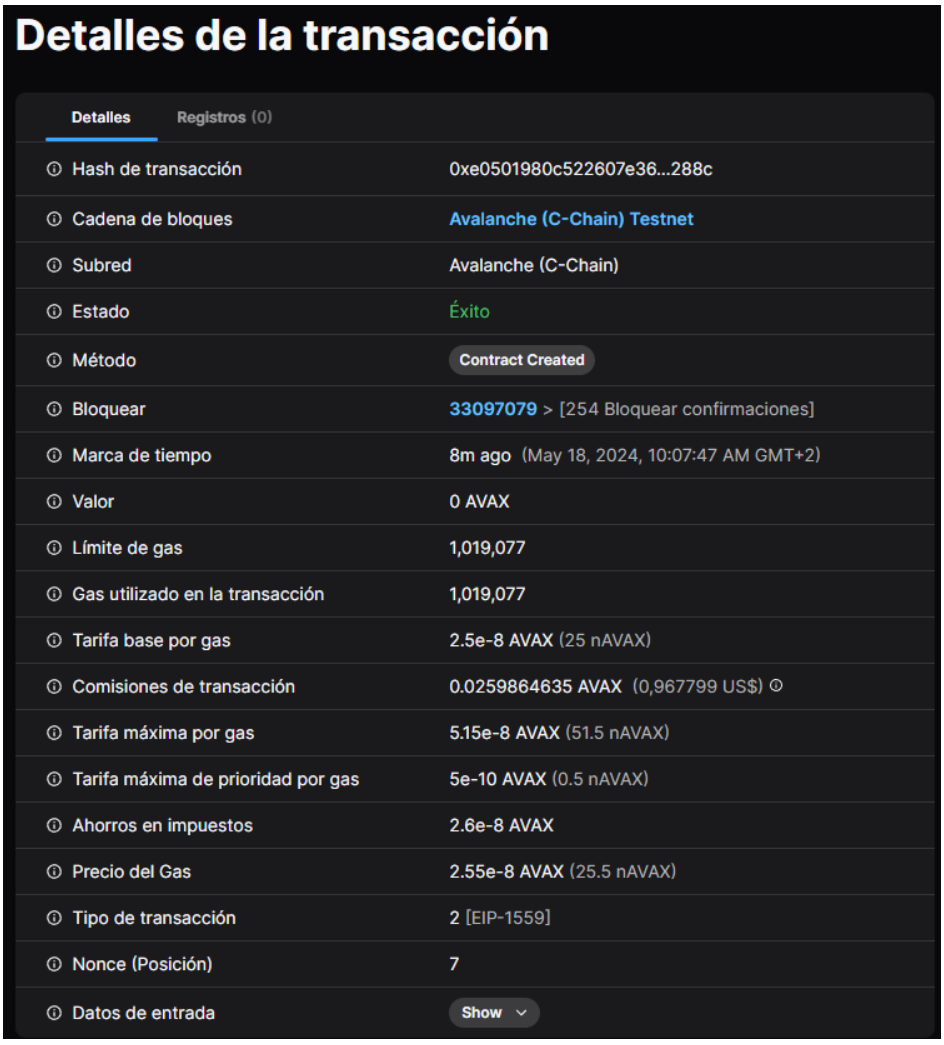


Fig. 7.3. Detalles de la publicación del contrato.

Tras el despliegue en C-Chain, se muestran dos tipos de funciones, como se puede apreciar en la figura 7.4.

- El primer grupo, resaltado con el color naranja, son aquellas funciones que guardarán y modificarán datos(de forma legítima) en la blockchain.
- El segundo grupo, identificado con el color azul, son funciones que sólo consultan los datos almacenados y validados en la blockchain.

Fig. 7.4. Funciones cargadas.

La figura 7.5 muestra el diseño de las pruebas realizadas sobre el contrato desplegado. El proceso es el siguiente:

1. La cuenta que desplegó el contrato, considerada el administrador, creará un set inicial de políticas, añadirá una más y las configurará todas.
2. Un usuario no autorizado tratará de desplegar y configurar políticas, y se le denegará el permiso para hacerlo.
3. Un usuario consultará el estado de las políticas que deberá aplicar en su dispositivo.
4. Un usuario solicitará cambiar la configuración de una política determinada.

5. Un administrador consultará las solicitudes de cambio, aplicará alguna y verificará el correcto cambio.

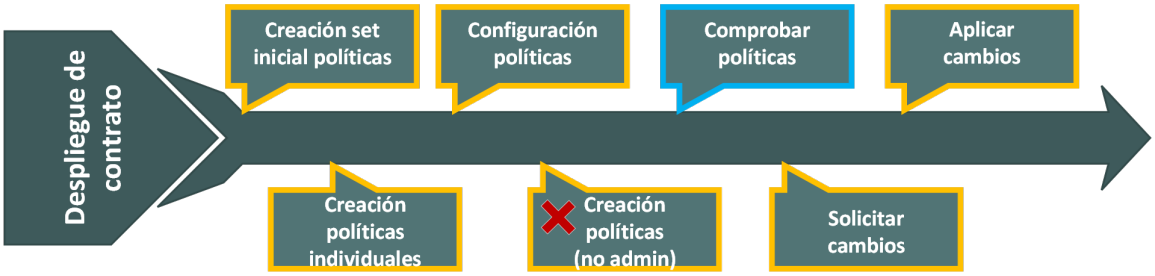


Fig. 7.5. Pruebas del sistema.

7.2. Ejecución de pruebas

A continuación se expondrán las pruebas realizadas, así como sus resultados. El diagrama con la lógica general del producto se muestra en la figura 7.6, mostrando las comprobaciones principales que realiza el sistema, su comportamiento y respuestas, en un lenguaje de alto nivel.

Las pruebas se han agrupado en 3 categorías:

- **Creación y configuración de políticas**: un administrador creará un conjunto de políticas y las configurará. También intentará realizar las mismas acciones un usuario no administrador.
- **Comprobación de políticas**: Un usuario comprobará el estado de las políticas que deberá aplicar.
- **Solicitud y aplicación de cambios**: tras comprobar los estados de las políticas, se solicitará la modificación de alguna de ellas.

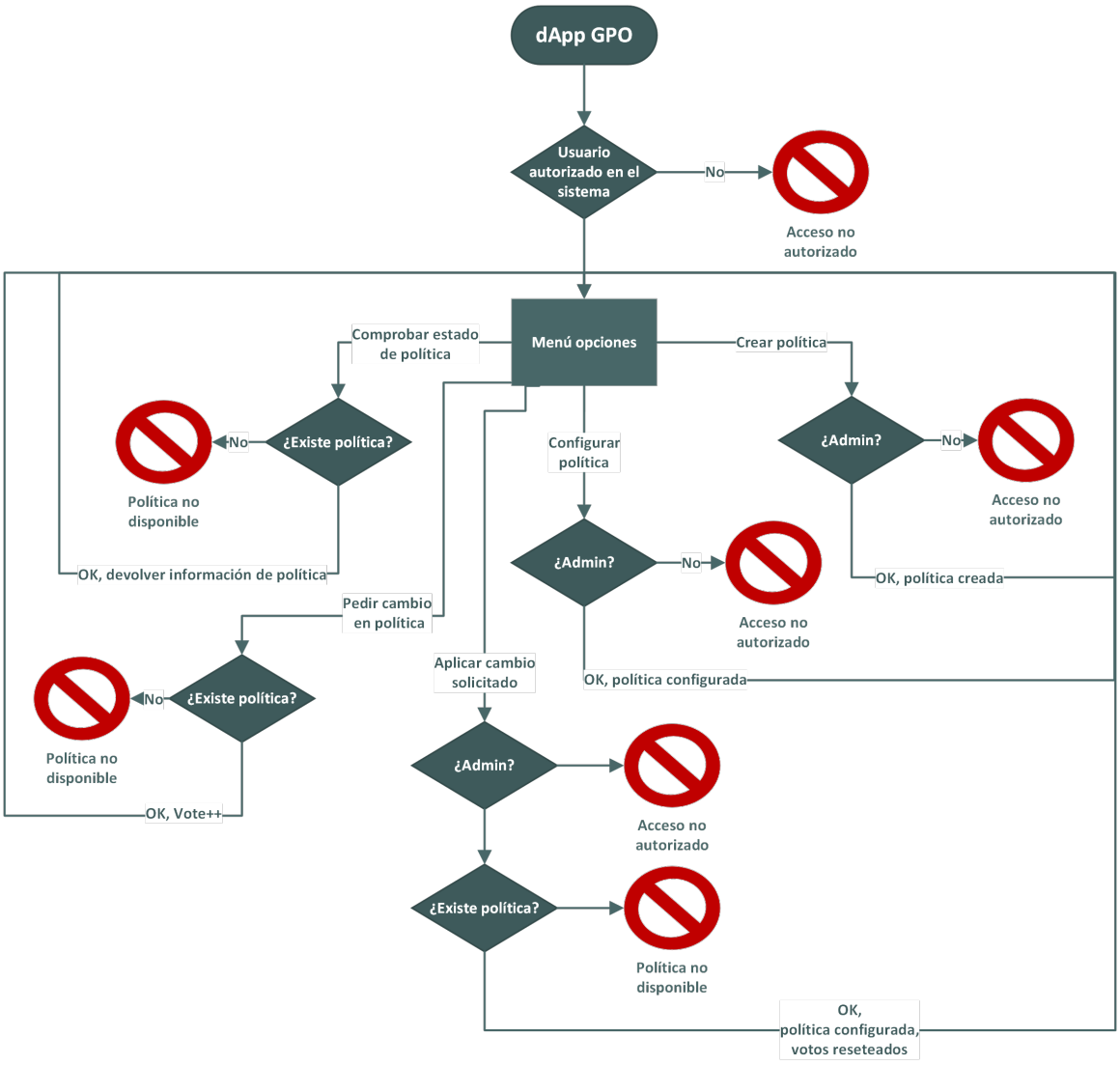


Fig. 7.6. Lógica del sistema.

7.2.1. Creación y configuración de políticas

Para la definición de políticas, se establecen 8 directivas de ejemplo:

- `gpo_forceMFA`: enabled.
- `gpo_allowMinusMayusPass`: enabled.
- `gpo_allowSpecialCharactersPass`: enabled.
- `gpo_enabledUSB`: disabled.
- `gpo_enabledCMD`: disabled.
- `gpo_allowCD`: disabled.
- `gpo_allowNetConf`: disabled.
- `gpo_enableDMZ`: enabled.

En la figura 7.7 se verifica que las transacciones se han ejecutado correctamente en la Blockchain. En este punto, si accedemos a una de las transacciones desde el explorador público,

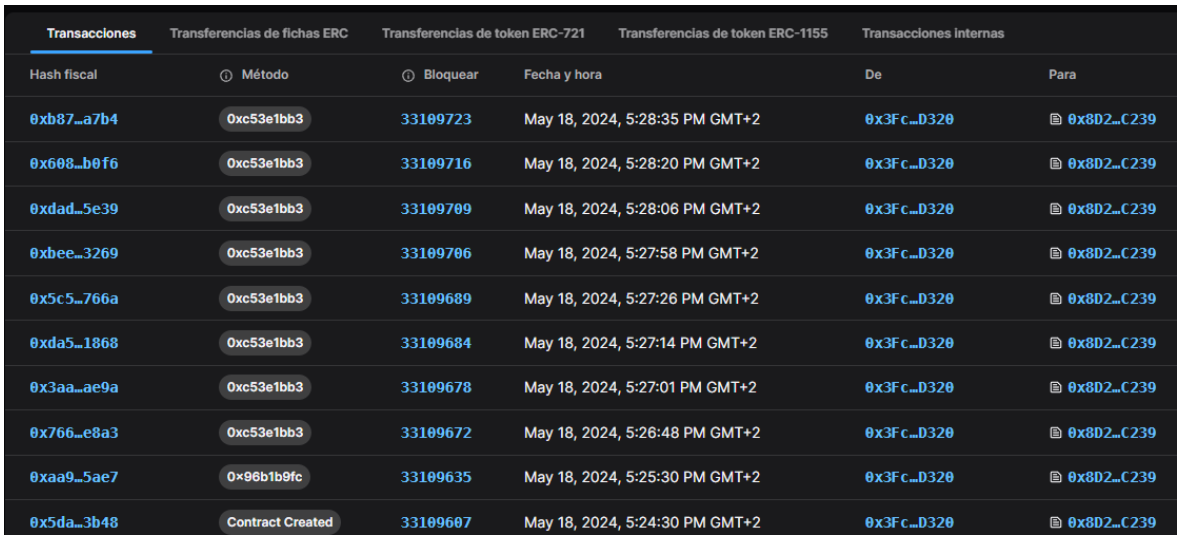


Fig. 7.7. Creación de políticas.

podemos comprobar que todos los detalles se encuentran cifrados. En la figura 7.8 puede comprobarse cómo se encuentran cifrados el ejecutor del contrato, la información del contrato y del método ejecutado, todas ellas resaltadas en azul; en la figura 7.9 puede verse cómo los datos de entrada de la función también se transmiten cifrados.

Dado que esta es una característica del sistema que se repetirá en todas las transacciones, en las próximas pruebas no se incluirá esta comprobación para no extender esta sección del documento.

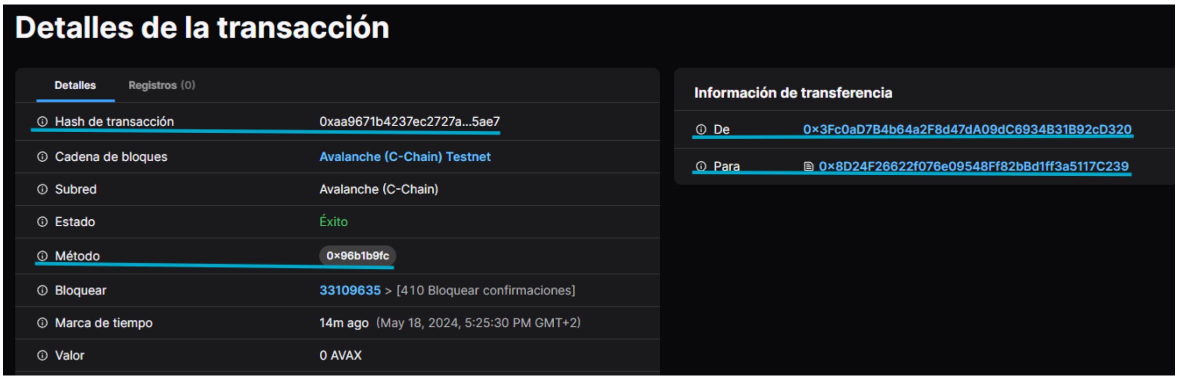


Fig. 7.8. Datos de la transacción cifrados.

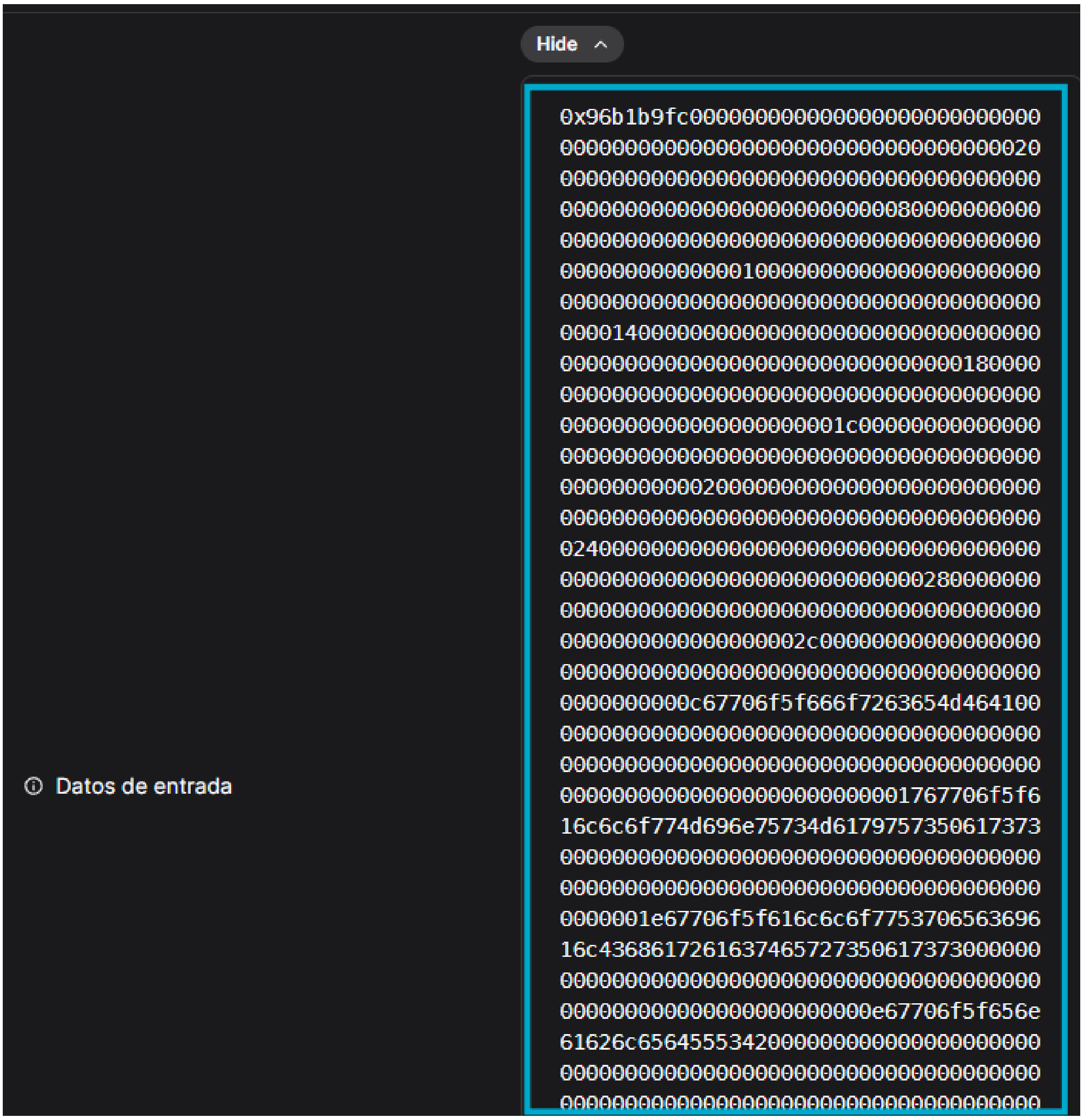


Fig. 7.9. Datos de entrada cifrados.

Si, en cambio, otro usuario que no sea administrador realiza una solicitud para crear una política, ésta no se creará, y la transacción no se completará. Para esta prueba, se crea otra cuenta con fondos disponibles, como muestra la figura 7.10.

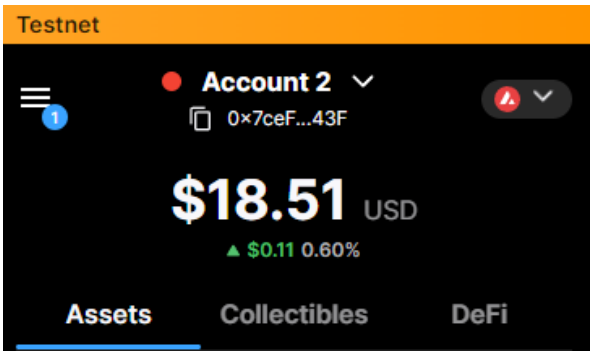


Fig. 7.10. Nuevo usuario no administrador.

Con esta cuenta, se intenta crear una nueva política, y, como muestran las figuras 7.11 y 7.12 (en ejecución y en el explorador público del blockchain, respectivamente), la transacción falla y no se completa.

Fig. 7.11. Fallo en Remix.

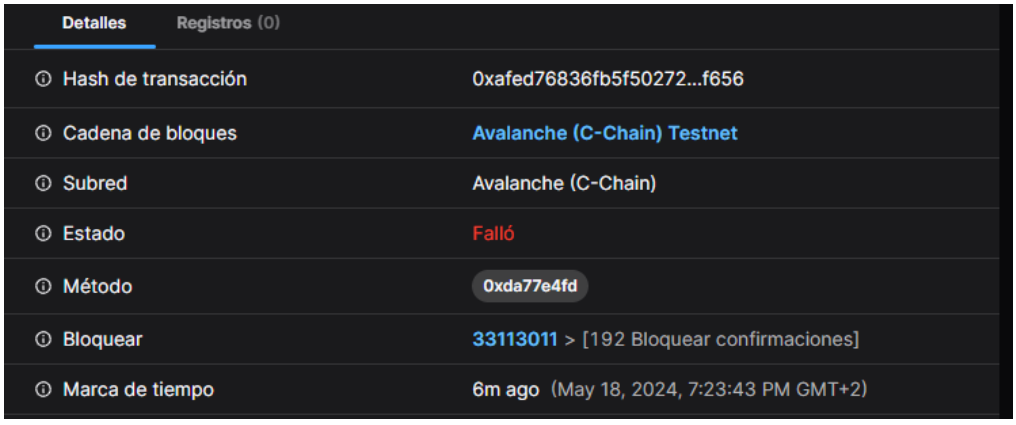


Fig. 7.12. Fallo en el explorador.

7.2.2. Comprobación de políticas

En este punto, asumimos el papel de un usuario que debe aplicar las políticas configuradas. Para ello, deberemos comprobar el estado de configuración (activas o inactivas) en el que se encuentran las políticas. En este caso, solicitaremos el estado de las políticas relacionadas con la configuración de contraseñas, es decir:

- `gpo_forceMFA`: enabled.
- `gpo_allowMinusMayusPass`: enabled.
- `gpo_allowSpecialCharactersPass`: enabled.

Dado que al consultar los valores no se modifica ningún valor de los datos de la blockchain, estas consultas no dejarán registros en el explorador público de la red Fuji C-Chain. Simplemente, al ser un usuario legítimo, podremos acceder a los datos descifrados, comprobando así que las 3 políticas están habilitadas, como se aprecia en las figuras 7.13, 7.14 y 7.15.

Fig. 7.13. Configuración MFA.

Fig. 7.14. Configuración mayúsculas y minúsculas.

Fig. 7.15. Configuración carácteres especiales.

7.2.3. Solicitud y aplicación de cambios

Ahora supongamos que cierto conjunto de los dispositivos del usuario, que podemos denominar como **subdominio A**, no permite la configuración de factores de autenticación extra añadidos a la autenticación por contraseña. Por ello, el usuario solicitará un cambio en la configuración de esta política.

El usuario realiza la solicitud, como se muestra en la figura 7.16, y se puede comprobar cómo se incrementan los votos que solicitan el cambio y la propuesta de configuración, como se puede observar en la figura 7.17.

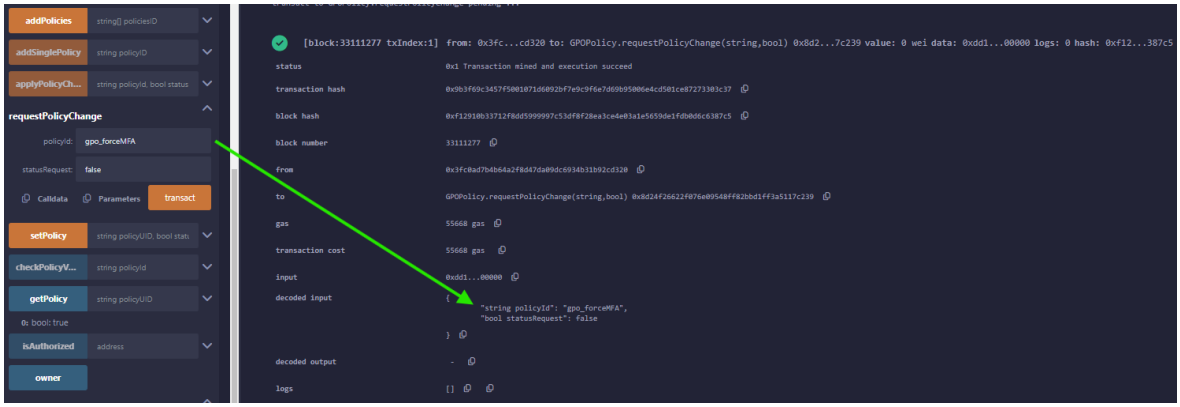


Fig. 7.16. Solicitud de cambio.

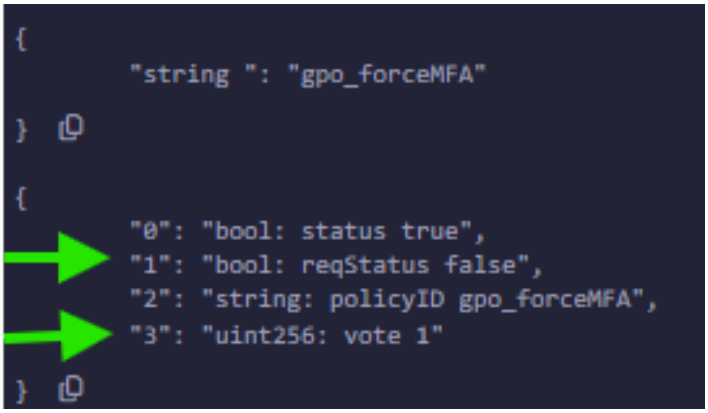


Fig. 7.17. Verificación de solicitud.

Dado que esta solicitud se ejecuta sobre una política(bloque) ya creado, puede comprobarse en el explorador de la blockchain cómo ahora hay dos transacciones sobre este bloque(Figura 7.18): una correspondiente a su creación y otra correspondiente a su modificación al solicitar el cambio de configuración.

Llegados a este punto, el administrador podrá consultar las solicitudes de cambio y decidir si aplicarlas o no. En cualquier caso, se reseteará el contador de votos, y sólo variará si se cambia o no la configuración. En la figura 7.19 se muestra cómo el administrador aplica el cambio solicitado, mientras que la figura 7.20 muestra los nuevos datos del bloque.

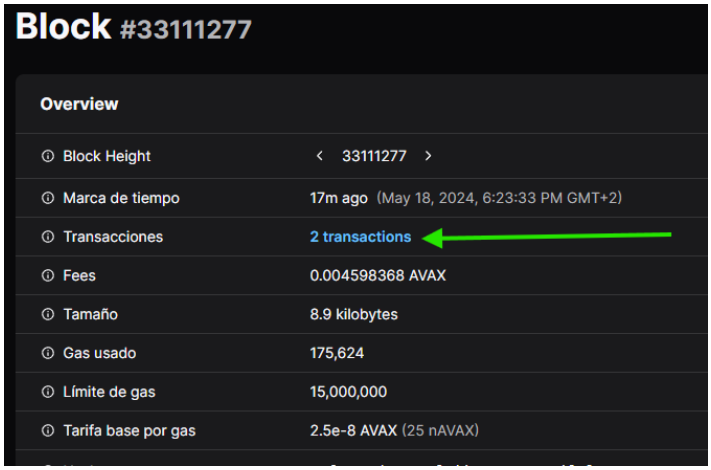


Fig. 7.18. Transacciones en el bloque MFA.

Fig. 7.19. Aplicación del cambio.

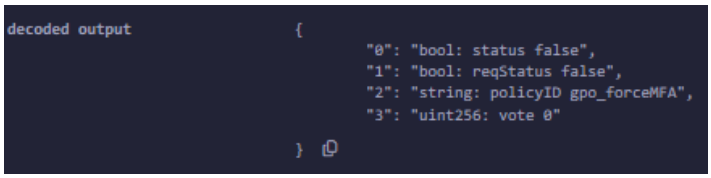


Fig. 7.20. Verificación de cambio de configuración.

7.3. Desafíos enfrentados durante el proyecto

El desarrollo del presente proyecto se ha visto obstaculizado en distintas fases. A continuación, se comentan los desafíos más relevantes que se han identificado durante el procedimiento:

7.3.1. Avalanche-CLI

El primer planteamiento para el desarrollo fue utilizar una subred de pruebas que se asemejase conceptualmente a una blockchain privada, que es el entorno deseable para esta propuesta.

Avalanche-CLI ofrece una alternativa para realizar despliegues locales de pruebas, pero se encontraron los siguientes inconvenientes:

- Los despliegues no disponen de una interfaz con la que explorar el estado de los nodos y las transacciones realizadas.
- La herramienta sólo funciona en distribuciones Linux y MacOS, aunque presenta problemas en algunas distribuciones Linux como Lubuntu, y en equipos que no dispongan de amplios recursos el rendimiento no es el deseable a pesar de requerir bajos recursos para ejecutar la herramienta.
- Los despliegues realizados con esta herramienta no resultan estables; los cambios de estado(e.g. reinicios, apagados) en la máquina host acaban acarreando una pérdida de la configuración desplegada, forzando a una reconfiguración contínua del escenario a pesar de mantener activo el servicio.

Es altamente probable que estos desafíos estén propiciados por el hecho de que la herramienta se encuentre en fases de desarrollo y se haya utilizado una versión beta; de cualquier manera, su uso se descartó para continuar con el proyecto y su aportación se limitó a una prueba de concepto de despliegues de contratos inteligentes en redes privadas.

7.3.2. Conexión a redes locales

Para poder realizar correctamente un despliegue de prueba en una red local, es necesario configurar un monedero y un entorno de desarrollo.

En cuanto a los monederos, existe una gran diversidad, pero la opción utilizada en el proyecto(**Core Wallet**) no ofrecía un entorno de conexión estable, resultando en fallos de conexión y desconfiguraciones. Por eso, temporalmente, se utilizó **MetaMask** como wallet para la integración con el entorno local.

En cuanto al entorno de desarrollo, la primera alternativa era emplear **HardHat**, ya que es un entorno muy popular entre los desarrolladores, pero esta herramienta también presentaba problemas de integración con el entorno local, posiblemente debido al entorno local y no a la herramienta de desarrollo. Tras consultar con la comunidad de Discord de HardHat y no recibir respuesta tras un plazo razonable, se decidió migrar al entorno de **Remix** empleado en este proyecto.

7.3.3. Explorador de redes públicas

Una de las ventajas del IDE Remix es poder desplegar contratos en sus *sandbox*, donde puede verificarse que un contrato se ha desarrollado correctamente en cuanto a sintaxis y compilación, así como realizar algunas pruebas básicas de funcionamiento.

Pero dado que los *sandbox* son entornos de pruebas aislados, y en cada reinicio o reconexión, la blockchain borra su estado y se inicia con un nuevo estado vacío, su naturaleza volátil hace que no sea posible explorar la blockchain para analizar los despliegues y las transacciones, por lo que este entorno sólo se ha usado para agilizar el desarrollo del contrato desplegado.

8. CONCLUSIONES Y LÍNEAS FUTURAS

En este apartado se evaluarán los resultados obtenidos durante las pruebas realizadas e el presente proyecto. Las conclusiones se dividirán en cuatro secciones: tres secciones se corresponden con las dimensiones de seguridad fundamentales(confidencialiad, integridad y disponibilidad) y finalmente la última sección se centrará en el rendimiento ofrecido por la tecnología de blockchain en nuestro escenario.

Para evaluar los resultados, se realizarán verificaciones sobre las 2 direcciones utilizadas:

- Cuenta privilegiada, con la dirección 0x3Fc0aD7B4b64a2F8d47dA09dC6934B31B92cD320.
- Cuenta no privilegiada, con la dirección 0x7ceFE9e80eF1076C087eD1515a995AC3d220143F.

En las siguientes secciones se hará referencia a la figura 9.1, que muestra los detalles de una de las transacciones ejecutadas durante la configuración de las políticas de las pruebas.

8.1. Confidencialidad

En la figura 8.1 se han resaltado varios campos con cuadros de color verde:

- Hash de transacción.
- Método ejecutado.
- Datos de entrada.
- Origen de la ejecución.
- Destino de la ejecución.

Atendiendo a los valores de todos los campos, se puede observar que toda la información se encuentra cifrada; además, ya que conocemos la solución empleada, sabemos que el cifrado se ha realizado mediante criptografía asimétrica de cúrvas elípticas.

Haciendo un análisis básico de alguno de los campos cifrados, como por ejemplo los datos de entrada de la ejecución, podemos realizar una evaluación fundamental de la confidencialidad. Para ello, se pueden emplear la popular herramienta criptográfica , y entre los múltiples operadores disponibles, se empleará el operador *'Magic'*, que analiza la entrada y ofrece distintas posibilidades para su decodificación. En la figura 8.2 se aprecia cómo ninguno de las alternativas ofrece una decodificación exitosa.

A pesar de que esta comprobación no es un análisis criptográfico en profundidad, sirve para descartar que se trate de criptografía básica o algoritmos fundamentales.

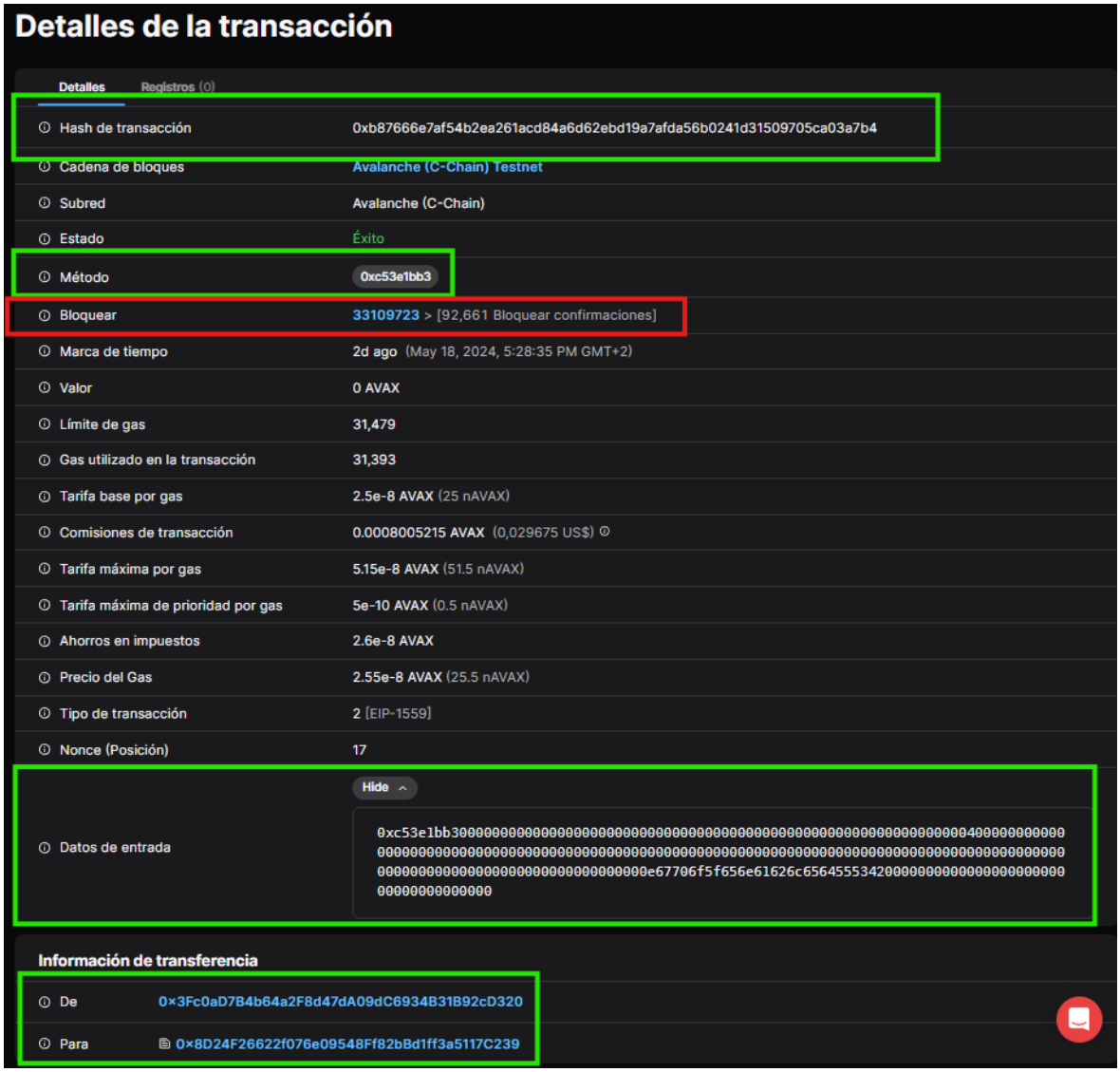


Fig. 8.1. Detalles de transacción.

Sin embargo, como se puede apreciar en figuras anteriores, como la 7.17, 7.19 o 7.20, si el usuario que ejecuta las transacciones es un usuario legítimo, sí podrá acceder a los datos decodificados.

Por lo tanto, al asegurar la confidencialidad del sistema, se aseguran también distintas dimensiones de seguridad derivadas de la misma, como la anonimización de los datos personales de los usuarios(la identificación del origen y el destino).

Fig. 8.2. CyberChef.

8.2. Integridad

Avalanche, al igual que otras tecnologías Blockchain, emplea mecanismos de criptografía asimétrica para la firma y *hasheado* de las transacciones, asegurando así la integridad de las transacciones y ejecuciones. En la figura 9.1 puede observarse en el primer campo que incluso el identificador de la transacción se encuentra *hasheado* para asegurar que sea un identificador único.

Además, dada la naturaleza del *'proof-of-stake'* de Avalanche, la transacción se ha validado por una cantidad determinada de bloques, como se aprecia en el campo resaltado en rojo en la figura 8.1. Por ello, incluso si un atacante fuese capaz de vulnerar la integridad de la transacción, aún debería replicar su ataque en otros nodos para vulnerar la integridad general del sistema.

8.3. Disponibilidad

Nuevamente nos referimos a la validación por los bloques del sistema destacada en color rojo en la figura 8.1. Gracias a la propia naturaleza del blockchain, los datos se encuentran disponibles repartidos en los nodos del sistema. Aunque eventualmente uno de ellos pierda la conexión, el resto de nodos continuará validando las operacioens realizadas en la blockchain, y tras la reconexión del nodo desconectado, éste podrá volver a disponer de los datos.

Cabe destacar que si el nodo que pierde la conexión es el que trata de ejecutar las operaciones y no un validador de las mismas, sí podría acarrear falta de disponibilidad del sistema, ya que requiere que el nodo tenga comunicación con la dirección en la que esté desplegada el contrato.

8.4. Rendimiento

Las diferentes plataformas de blockchain presentan sus propios problemas de rendimiento y escalabilidad, a menudo propiciado por su mecanismo de consenso. En el caso de la red Avalanche, el diseño del mecanismo de consenso basado en tolerancia a fallas bizantinas ofrece un gran rendimiento y una alta escalabilidad al sistema[62].

8.5. Líneas futuras

En esta sección se explora las posibilidades que ofrece este proyecto y la prueba de concepto que supone para la gestión de los servicios de forma descentralizada en una coalición federada.

8.5.1. Entorno real

La prueba de concepto de este proyecto se ha desarrollado en diferentes entornos, pero todos los entornos explorados tienen en común que son soluciones blockchain públicas y/o de terceros. Al trasladar esta propuesta a un entorno real, lo apropiado para una red de coalición federada sería, tal y como se mencionó en el capítulo 6 del presente documento, una red blockchain privada.

El despliegue que se realizado debiera atender a una configuración específica que atienda a las necesidades de escalabilidad, gestión de usuarios y rendimiento del sistema; dado que la propuesta se ha probado sobre redes basadas en Ethereum y los resultados han sido apropiados, el método de consenso basado en *'Proof-of-Stake'* sería válido para un despliegue federado.

8.5.2. Tecnologías *'Quantum-safe'*

Uno de los pilares fundamentales para asegurar las dimensiones de seguridad en las redes blockchain es el modelo criptográfico que implementa el sistema; actualmente, es común encontrar sistemas asiméricos basados en curvas elípticas, como en Avalanche o en la red Ethereum.

En este contexto, y dado que se espera desarrollar redes que puedan ser confiables a lo largo de los años, resulta conveniente atender a las futuras amenazas tecnológicas, siendo las tecnologías cuánticas [1] un tema bastante discutido en la actualidad. Dentro de estas tecnologías existen dos grandes grupos, cada uno con una amenaza para la seguridad de los sistemas [63]:

- **Comunicaciones cuánticas**: las comunicaciones cuánticas se basan en el envío de fotones polarizados como elemento de comunicación en distintos tipos de redes. Dentro de este grupo se halla la **criptografía cuántica**, que desarrolla distintos algoritmos de consenso para destilar claves que aseguren las comunicaciones gracias a las propiedades físicas de los fotones, como por ejemplo el protocolo BB84.
- **Computación cuántica**: la computación cuántica es un modelo disruptivo de computación que, se espera, facilite y optimice enormemente la resolución de diferentes problemas matemáticos; dentro de los problemas que se espera que pueda solucionar, se encuentran los fundamentos matemáticos en los que se basa la criptografía asimétrica actual.

  Por eso, surge la **criptografía post-cuántica**, que no es más que criptografía basada en modelos matemáticos que un computador cuántico no podría resolver. En la actualidad, se propone el uso de **modelos criptográficos híbridos**, que usan de manera conjunta modelos actuales y modelos post-cuánticos para asegurar la confidencialidad y la integridad de las comunicaciones en cualquier caso.

En consecuencia, y restringiéndonos a la naturaleza de blockchain, se propone el uso de modelos criptográficos híbridos para hacer frente a la amenaza de la computación cuántica. Los esquemas de comunicación cuántica quedan fuera del alcance de la propuesta.

8.5.3. Desarrollo de funciones

Como se ha visto en el capítulo 4, la función desarrollada no es la única identificada. En futuros desarrollos, la dApp de gestión de servicios debiera incluir más funciones como las planteadas, entre otras.

8.5.4. Integración con otras dApp descentralizadas

Como se introdujo en el capítulo 4, este proyecto se enmarca, junto al trabajo de Ana María Saiz García [54], en el desarrollo de una capacidad operativa. La integración de las funciones de ambas propuestas, además de otras aún no exploradas, habilitaría dicha capacidad de gestión descentralizada ofrecida por Blockchain descrita en la sección 5.1. La integración con este tipo de app es idónea para el despliegue de Smart Cities junto con la tecnología blockchain como en [64].

8.5.5. Automatización

Múltiples funciones se beneficiarían de la integración con un *front-end* que automaticase ciertos procesos como la selección de directivas o su configuración. Un desarrollo más avanzado de esta propuesta debería integrarse en un *front-end* que facilitase el uso de la aplicación para distintos tipos de usuario.

BIBLIOGRAFÍA

[1] M. I. Garcia Cid, J. Álvaro González, L. Ortíz Martín y D. Del Río Gómez, "Disruptive quantum safe technologies," en *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1-8.

[2] V. M. Baeza y L. C. Salor, "New horizons in tactical communications: An overview of emerging technologies possibilities," *IEEE Potentials*, vol. 43, n.º 1, pp. 12-19, 2024. DOI: 10.1109/MPOT.2023.3297326.

[3] L. Concha Salor y V. Monzon Baeza, "Harnessing the Potential of Emerging Technologies to Break down Barriers in Tactical Communications," *Telecom*, vol. 4, n.º 4, pp. 709-731, 2023. DOI: 10.3390/telecom4040032.

[4] L. C. Salor y V. M. Baeza, "Análisis y casos de uso de las comunicaciones 5G para entornos tácticos," Tesis doct., Universidad Carlos III de Madrid, 2021.

[5] J. Morillo Osuna, "ATDTEM. Aplicación de la tecnología Digital Twin en entornos militares," Tesis doct., Universitat Oberta de Catalunya, Barcelona, Spain, 2024.

[6] V. O. Gómez y V. M. Baeza, "Desarrollo de una aplicación para mejorar la interoperabilidad en escenarios tácticos," Tesis doct., Universidad Carlos III de Madrid, 2019.

[7] E. J. Alcántara Suárez y V. Monzon Baeza, "Evaluating the Role of Machine Learning in Defense Applications and Industry," *Machine Learning and Knowledge Extraction*, vol. 5, n.º 4, pp. 1557-1569, 2023. DOI: 10.3390/make5040078.

[8] E. J. Alcántara Suárez, "Análisis de la aplicación de machine learning en sistemas de defensa," Tesis doct., Universitat Oberta de Catalunya, Barcelona, Spain, 2023.

[9] H. Aden, "Information sharing, secrecy and trust among law enforcement and secret service institutions in the European Union," en *Secrecy in European Politics*, Routledge, 2020, pp. 157-178.

[10] F. T. Johnsen y M. Hauge, "Interoperable, adaptable, information exchange in NATO coalition operations," *Journal of Military Studies*, vol. 11, n.º 1, pp. 49-62, 2022.

[11] N. Jansen et al., "NATO Core Services profiling for Hybrid Tactical Networks—Results and Recommendations," en *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, IEEE, 2021, pp. 1-8.

[12] O. Evsyukova, "Political digitalization for Ukrainian society–challenges for cyber security," *Cybersecurity and Law*, vol. 5, n.º 1, pp. 139-144, 2021.

[13] N. Myers, "Cyber Security: Cyber Crime, Attacks and Terrorism," *ODU UN Day 2020 Issue*, pp. 1-13, 2020.

[14] R. Dávila Álvarez, *El Nuevo Arte de la Guerra*. La esfera de los libros, 2022.

[15] H. Halpin y M. Piekarska, "Introduction to Security and Privacy on the Blockchain," en *2017 IEEE European symposium on security and privacy workshops (EuroS&PW)*, IEEE, 2017, pp. 1-3.

[16] C. Villar Miguelez, V. Monzon Baeza, R. Parada y C. Monzo, "Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks," *Smart Cities*, vol. 6, n.º 2, pp. 728-743, 2023. DOI: 10.3390/smartcities6020035.

[17] C. Tarazona Lizarraga, "Análisis de las necesidades de una Smart City en el marco de un desarrollo sostenible," Tesis doct., Universitat Oberta de Catalunya, Barcelona, Spain, 2020.

[18] G. Assembly, "sustainable Development goals. SDGs," *Transforming our world: the*, vol. 2030, 2015.

[19] D. Upadhyay, N. Gaikwad, M. Zaman y S. Sampalli, "Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications," *IEEE Access*, vol. 10, pp. 112 472-112 486, 2022. DOI: 10.1109/ACCESS.2022.3215778.

[20] W. W. Widiyanto, D. Iskandar, S. Wulandari, E. Susena y E. Susanto, "Implementation Security Digital Signature Using Rivest Shamir Adleman (RSA) Algorithm As A Letter Validation And Distribution Validation System," en *2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC)*, 2022, pp. 599-605. DOI: 10.1109/IIHC55949.2022.10060839.

[21] S. Haber y W. S. Stornetta, *How to time-stamp a digital document*. Springer, 1991.

[22] S. Shanaev, A. Shuraeva, M. Vasenin y M. Kuznetsov, "Cryptocurrency value and 51 % attacks: evidence from event studies," *The Journal of Alternative Investments*, vol. 22, n.º 3, pp. 65-77, 2019.

[23] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[24] V. Buterin et al., "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, n.º 37, pp. 2-1, 2014.

[25] Y. Gilad, R. Hemo, S. Micali, G. Vlachos y N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," en *Proceedings of the 26th symposium on operating systems principles*, 2017, pp. 51-68.

[26] M. Caprolu y R. Di Pietro, "Account Clustering in the Polkadot Network: Heuristic, Experiments, and Insights," en *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1-4. DOI: 10.1109/ICBC56567.2023.10174938.

[27] K. Wrona y M. Jarosz, "Does NATO Need a Blockchain?" En *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 2018, pp. 667-672. DOI: 10.1109/MILCOM.2018.8599845.

[28] P. Woitschig, G. S. Uddin, T. Xie y W. K. Härdle, "The energy consumption of the ethereum-ecosystem," *Available at SSRN 4526732*, 2023.

[29] H. Li, D. Meng, H. Wang y X. Li, "Knowledge Federation: A Unified and Hierarchical Privacy-Preserving AI Framework," en *2020 IEEE International Conference on Knowledge Graph (ICKG)*, 2020, pp. 84-91. DOI: 10.1109/ICBK50248.2020.00022.

[30] C. A. Lee, "Cloud Federation Management and Beyond: Requirements, Relevant Standards, and Gaps," *IEEE Cloud Computing*, vol. 3, n.º 1, pp. 42-49, 2016. DOI: 10.1109/MCC.2016.15.

[31] Q. Li et al., "A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, n.º 4, pp. 3347-3366, 2023. DOI: 10.1109/TKDE.2021.3124599.

[32] R. Hull, B. Kumar y D. Lieuwen, "Towards federated policy management," en *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, 2003, pp. 183-194. DOI: 10.1109/POLICY.2003.1206972.

[33] J. Jensen, "Federated Identity Management Challenges," en *2012 Seventh International Conference on Availability, Reliability and Security*, 2012, pp. 230-235. DOI: 10.1109/ARES.2012.68.

[34] I. G. Niemegeers y S. H. De Groot, "FEDNETS: Context-aware ad-hoc network federations," *Wireless Personal Communications*, vol. 33, pp. 305-318, 2005.

[35] R. Hoencamp et al., "Systematic review of the prevalence and characteristics of battle casualties from NATO coalition forces in Iraq and Afghanistan," *Injury*, vol. 45, n.º 7, pp. 1028-1034, 2014.

[36] 2012. [En línea]. Disponible en: https://c2coe.org/download/afghanistan-mission-network-future-mission-network/.

[37] F. T. Johnsen y M. Hauge, "Interoperable, adaptable, information exchange in NATO coalition operations," *Journal of Military Studies*, vol. 11, n.º 1, pp. 49-62, 2022.

[38] J. M. Pullen, F. Corona y C. Zamponi, "NATO Federated Mission Networking Standards for CAX," *EasyChair Preprint*, vol. 4511, pp. 2-17, 2020.

[39] A. Saini et al., "A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System," *IEEE Internet of Things Journal*, vol. 8, n.º 7, pp. 5914-5925, 2021. DOI: 10.1109/JIOT.2020.3032997.

[40] K. Singh, P. K P, S. Benakatti y V. Srivatsa, "Revolutionizing Digital Banking: Harnessing Blockchain Smart Contracts for Enhanced Security and Efficiency," en *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, 2023, pp. 1-5. DOI: 10.1109/SMARTGENCON60755.2023.10442642.

[41] A. Mbiriki, "A Consortium Model for Managing Nodes in Smart Factories Based on Blockchain and Smart Contracts," en *2023 International Conference on Innovations in Intelligent Systems and Applications (INISTA)*, 2023, pp. 1-4. DOI: 10.1109/INISTA59065.2023.10310595.

[42] M. de Defensa, *Transformación digital de las FAS para el combate multidominio*. 2024.

[43] N. Petersen, "Bargaining power among potential allies: negotiating the North Atlantic Treaty, 1948–49," *Review of International Studies*, vol. 12, n.º 3, pp. 187-203, 1986.

[44] E. Konacakli y E. Karaarslan, "Blockchain-Based Secure Recognized Air Picture System Proposal for NATO Air C2 Capabilities," en *Artificial Intelligence and Applied Mathematics in Engineering Problems: Proceedings of the International Conference on Artificial Intelligence and Applied Mathematics in Engineering (ICAIAME 2019)*, Springer, 2020, pp. 758-765.

[45] K. Wrona y M. Jarosz, "Use of blockchains for secure binding of metadata in military applications of IoT," en *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, IEEE, 2019, pp. 213-218.

[46] B. RUMELIOGLU, "Blockchain: Transformation of NATO Logistics Capabilities," en *North Atlantic Treaty Organization: Science and Technology Organization symposium. Available at: Link*, 2022.

[47] A. Aytaç y S. Çakir, "AN ANALYSIS OF THE FEASIBILITY OF BLOCKCHAIN TECHNOLOGY IN THE NATIONAL DEFENSE INDUSTRY," *Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, vol. 14, n.º 27, pp. 525-541, 2023.

[48] K. Wrona, F. M. Scharf y M. Jarosz, "Security Accreditation and Software Approval with Smart Contracts," *IEEE Communications Magazine*, vol. 59, n.º 2, pp. 56-62, 2021. DOI: 10.1109/MCOM.001.2000802.

[49] C. Tselios, I. Politis y S. Kotsopoulos, "Enhancing SDN security for IoT-related deployments through blockchain," en *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, 2017, pp. 303-308. DOI: 10.1109/NFV-SDN.2017.8169860.

[50] S. Van Rossem et al., "Deploying elastic routing capability in an SDN/NFV-enabled environment," en *2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, 2015, pp. 22-24. DOI: 10.1109/NFV-SDN.2015.7387398.

[51] S. Shin y G. Gu, "Attacking software-defined networks: a first feasibility study," en *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking*, ép. HotSDN '13, Hong Kong, China: Association for Computing Machinery, 2013, pp. 165-166. DOI: 10.1145/2491185.2491220. [En línea]. Disponible en: https://doi.org/10.1145/2491185.2491220.

[52] P. Fonseca, R. Bennesby, E. Mota y A. Passito, "A replication component for resilient OpenFlow-based networking," en *2012 IEEE Network operations and management symposium*, IEEE, 2012, pp. 933-939.

[53] D. Kreutz, F. M. Ramos y P. Verissimo, "Towards secure and dependable software-defined networks," en *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, 2013, pp. 55-60.

[54] A. M. S. García, "Gestión descentralizada de la red en un despliegue de coalición federada mediante blockchain," Trabajo de fin de máster, Universitat Oberta de Catalunya, Barcelona, Spain, 2024.

[55] Í. Foto et al., "Ejército de Tierra Español, oct 2010,"

[56] W. B. Weinrod y C. L. Barry, *NATO Command Structure: Considerations for the Future*. Center for Technology y National Security Policy, National Defense University, 2010.

[57] C. Clausewitz, *On war*. Penguin UK, 2003.

[58] D. Thibault, "Commented APP-6A-Military symbols for land based systems," *NATO's current military symbology standard [Electronic resource]/Defence R&D Canada–Valcartier.–mode of access: http://www. mapsymbs. com/APP-6ADRDCValcartierEdition121 (Mod). pdf*, 2005.

[59] *Blockchain garantiza la integridad y autenticidad de los datos con la máxima seguridad digital | SEIDOR*. [En línea]. Disponible en: https://www.seidor.com/blog/blockchain-garantiza-la-integridad-y-autenticidad-de-los-datos-con-la-maxima-seguridad-digital.

[60] W. Han, Z. Zhao, A. Doupé y G.-J. Ahn, "Honeymix: Toward sdn-based intelligent honeynet," en *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, 2016, pp. 1-6.

[61] "NATO ARCHITECTURE FRAMEWORK Version 4 Acknowledgments for NAFv4 Publication,"

[62] Y. Jiang y Z. Lian, "High performance and scalable byzantine fault tolerance," en *2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC)*, IEEE, 2019, pp. 1195-1202.

[63] J. Á. González, "Análisis de seguridad de protocolos criptográficos 'Quantum Safe'," 2022.

[64] G. Á. Domínguez Camarero, "Desarrollo de una aplicación descentralizada basada en blockchain para el gobierno de una ciudad inteligente," Tesis doct., Universitat Oberta de Catalunya, Barcelona, Spain, 2024.