Universidad Zaragoza
1542

Trabajo Fin de Grado

PERSPECTIVA DE USO DE LA TECNOLOGÍA DE LIBRO MAYOR DISTRIBUIDO (DLT) EN LAS TRANSMISIONES DEL FUTURO

D. Juan Manuel Pérez Campanario

Directora académica: Dña. Lacramioara Dranca

Director militar: D. Gonzalo de La Torre Díaz

Centro Universitario de la Defensa-Academia General Militar

2022

Agradecimientos

¨Un poco más de persistencia, un poco más de esfuerzo, y lo que parecía irremediablemente un fracaso puede convertirse en un éxito glorioso¨. -Elbert Hubbard.

Me gustaría comenzar agradeciendo a mi director Militar, el Teniente de Transmisiones D. Gonzalo de la Torre Díaz, por su ayuda en el proceso de elaboración de este trabajo, aun estando involucrado en unas maniobras. También añadir al Teniente D. Aurelio Vidal Fernández, por su ayuda desinteresada en todo momento.

Por otro lado, agradecer a todas las personas que han sido participes durante mi recorrido por la Academia General Militar, desde profesores civiles, militares hasta Capitanes Jefes de Sección, sin poder olvidar a todos mis compañeros, en especial a mi camareta de primer curso y sobretodo, a mi familia, sin ellos nada de esto hubiese sido posible.

Por último, pero no menos importante, agradecerle a mi Tutora Académica, Dña. Lacramioara Dranca, su interés por el tema, su generosa ayuda desde el primer momento y todas las reuniones que hemos tenido, en las que siempre me aportaba ideas nuevas para la realización del trabajo.

RESUMEN

El Trabajo de Fin de Grado ‘’Perspectiva de uso de la tecnología de libro mayor distribuido (DLT) en las transmisiones del futuro'' ha sido realizo durante el periodo de prácticas de seis semanas encuadrado en la Compañía 33 del III Batallón del Regimiento de Transmisiones 21, ubicada en Burgos. Este trabajo es un estudio que surge motivado por el creciente interés de la tecnología del libro mayor distribuido (DLT), en concreto con la blockchain en el ámbito de la defensa.

Con la finalidad de implementar la tecnología de la cadena de bloques (blockchain) y mejorar los sistemas de información, se han identificado en el trabajo tres posibles casos de uso a través de la técnica de grupo nominal, los cuales podrían introducir en el Ejército de Tierra y posteriormente propagarse al Ejército del Aire y del Espacio y a la Armada.

Para la realización del trabajo, se ha llevado a cabo una investigación de los sistemas actuales a través de entrevistas con el personal especializado de la unidad que es el que mejor los conoce, ya que trabaja diariamente con ellos. Durante estas entrevistas de destacó la dependencia de una figura centralizada lo que conllevaba que el sistema estuviese caído algunos días y le imposibilitase realizar su trabajo.

Con la tecnología de la blockchain, que es reconocida como una de las innovaciones más disruptivas desde Internet, se puede dar solución al problema planteado. Tras el estudio de los tres casos de uso y llegar a unas posibles soluciones teóricas con el consorcio de Alastria, se observa que en todos los casos de uso se podría llevar a cabo una mejora del sistema actual y además añadir características que aportan seguridad a los sistemas como confidencialidad, integridad, disponibilidad, trazabilidad, autenticación y no repudio.

Aunque de forma teórica la implementación de la tecnología en el Ejército de Tierra puede no ser complicada, la dificultad una futura implementación de las soluciones propuestas se verá reflejada con la necesidad de encontrar personal cualificado para el mantenimiento de los nodos en los distintos acuartelamientos donde se tendrán que instalar.

PALABRAS CLAVE

Cadena de bloques, Alastria, mensajería, cadena de suministro y gestión de identidades.

ABSTRACT

The End of Degree Project "Perspective of Use of Distributed Ledger Technology (DLT) in Future Transmissions" has been carried out during the six-week internship period under the 33th Company of the III Battalion of the 21st Transmission Regiment, located in Burgos. This work arises from the study motivated by the growing interest of distributed ledger technology (DLT), specifically with the blockchain in the field of defense.

In order to implement blockchain technology (blockchain) and improve information systems, three possible use cases have been presented throughout the project by means of the Nominal Group technique, which could be introduced into the Army and then spread to the Air and Space Force and the Navy.

To carry out the work, an investigation of the current systems has been performed through interviews with specialized unit personnel who best knows the systems and operate them on a daily basis. During these interviews the dependence of a centralized figure has been highlighted, which meant that the system was down for a few days making impossible fulfilling its job.

With the blockchain technology, which is recognized as one of the most disruptive innovations since Internet, we can provide a solution to the issue raised. After studying the three use cases and reaching possible theoretical solutions with the Alastria consortium, we note that in all cases of use, an improvement of the current system could be conducted and also adding features that provide security to the systems such as confidentiality, integrity, availability, traceability, authentication and non-repudiation.

Although theoretically, the implementation of technology in the Army may not be complicated, the difficulty of a future implementation of the proposed solutions will be reflected on the need to find qualified personnel for the nodes maintenance in the different quartering where they will have to be installed.

KEYWORDS

Blockchain, Alastria, email, Supply Chain Management and identity management

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

AC	-	Autoridad de certificación
AIDC	-	identificación automática y captura de datos
BOD	-	Boletín Oficial de Defensa
BON	-	Batallón
Cap	-	Capitán
CESTIC	-	Centro de Sistemas y Tecnologías de la Información y Comunicaciones
Cía	-	Compañía
DID	-	Identificador descentralizado
DLT	-	Libro mayor distribuido
DNI	-	Documento Nacional de Identidad
EDT	-	Estructura de Desglose de Trabajo
ET	-	Ejército de Tierra
HF	-	High frecuency
IBFT	-	Instambul Byzantine Fault Tolerant
IoT	-	Internet of Things
LF	-	Baja frecuencia
NGT	-	Nominal Group Technique
OAM	-	Órgano auxiliar de mando
OCR	-	Reconocimiento óptico de caracteres
PCAMI	-	Parque y Centro de Abastecimiento de Material de Intendencia
PKI	-	infraestructura de clave pública
PoA	-	Proof of Authority
PoS	-	Proof of Stake
PoW	-	Proof of Work
RA	-	Registration Authority
Red B	-	Red Besu
Red T	-	Red Telsius
RPoW	-	Reusable Proof of Work
RT	-	Regimiento de Transmisiones
SCM	-	Supply Chain Management
SIGLE	-	Sistema Integrado de Gestión Logística del Ejército de Tierra
SIMENDEF	-	Sistema de Mensajería Oficial y Gestión Documental
SSI	-	Self Sovereign Identity
TFG	-	Trabajo Fin de Grado
TIM	-	Tarjeta de identificación militar
TSA	-	TimeStamp Authority
Tte	-	Teniente
UHF	-	Frecuencia ultra alta
UME	-	Unidad Militar de Emergencias

UE	- Unión Europea
VA	- Validation Authority
VTHO	- VeThor
WSN	- Red de sensores inalámbricos

1. INTRODUCCIÓN

1.1. Reseña histórica

A lo largo de la historia, se ha podido asistir a como las tecnologías disruptivas han acabado siendo aceptadas e incorporadas de completo a nuestras vidas. Ejemplo de ello es la irrupción del ordenador personal en el año 1971, el cual se comenzó a vender de forma masiva a partir del año 1984 (*JJ Velasco*, 2011). Otro caso similar es lo que ocurrió con los teléfonos móviles allá por el año 1984. Pero si se puede destacar una revolución, esta ha sido la popularización de Internet. Aunque Internet naciese en los años sesenta, fue en la década de los noventa cuando se empezó a introducir en los hogares (*Master Marketing*, 2019), y con el paso de los años se ha convertido en una herramienta imprescindible.

De la blockchain se puede esperar algo parecido a los casos de los ordenadores o teléfonos móviles. En sus inicios no le faltaron los detractores a esta tecnología, pero tras algo más de una década de vida ha demostrado que ha llegado para quedarse.

La tecnología blockchain aborda de un modo revolucionario de manejar datos de manera descentralizada. Se puede definir la blockchain o cadena de bloques, como una base de datos basada en la tecnología de contabilidad distribuida y resistente a las manipulaciones en una red, donde todos los participantes pueden enviar nuevos registros, pero que ninguna autoridad central controla. Estos registros sólo se añaden a la base de datos en función del acuerdo o consenso de la mayoría del grupo. De la misma manera, una vez introducido un registro, este no ser modificado ni borrado. (Barnas, 2016)

Se puede pensar que esta tecnología se origina con el nacimiento de la red Bitcoin, pero ya en 1991 W. Scott Stornetta junto a Stuart Haber, fueron los pioneros en hacer mención a la arquitectura blockchain, en un estudio que pretendía hacer una marca de tiempo en un documento digital. Este trabajo consistía en la creación de una cadena de bloques la cual estaba protegida por la criptografía. En el año 1992, con la incorporación de los árboles de Merkle, se hizo más eficiente el proyecto, debido a que ahora se permitía que varios documentos se reunieron en tan solo un bloque. Empero, la patente de esta técnica caducó en 2004. (*Binance Academy*, no date)

En 2004 Harold Thomas Finney II, resolvió el problema de doble gasto[1] a la vez que mantenía la propiedad de los bloques registrados en un servidor de confianza, que les permitía a los usuarios verificar la exactitud e integridad en tiempo real. Este avance fue gracias al sistema RPoW (Reusable Proof of Work) (*Binance Academy*, no date)

En 2008 una persona o grupo de personas bajo el seudónimo de Satoshi Nakamoto, publicó un artículo titulado *Bitcoin: A Peer-to-Peer Electronic Cash System*, creando así un sistema de efectivo electrónico descentralizado, el cual no necesita de una autoridad central para su emisión y validación de las transacciones. (*Bit2Me Academy*, no date)

El 3 de enero de 2009 nace oficialmente Bitcoin (*Bitcoin - Dinero P2P de código abierto*, no

[1] El problema de doble gasto es el riesgo que corre una moneda digital de ser duplicada y gastada en más de una ocasión.(*¿Qué es el doble gasto?*, no date)

date), cuando el primer bloque fue creado por Satoshi Nakamoto, obteniendo una recompensa de 50 bitcoins.(*Binance Academy*, no date)

En 2015 Vitalik Buterin crea Ethereum (*ethereum*, no date),plataforma con la que pretendía mejorar Bitcoin añadiendo la creación de aplicaciones descentralizadas e incluso la creación de tu propia moneda virtual. Pero la mayor novedad de esta red fue la implementación de los Smart Contracts (contratos inteligentes), entendiéndose como tal un programa informático que hace que se cumplan los acuerdos entre las partes.(*IG España*, no date)

1.2. Motivación

La llegada de Internet cambió por completo nuestras vidas y la tecnología blockchain puede llegar a tener un impacto similar. Conforme se va avanzando en el estudio de la cadena de bloques, se descubren nuevas soluciones a casos de uso en el ámbito civil, como puede ser el mercado de la energía, los cuidados de la salud, los bienes raíces o el notariado (*Nelson Rodriguez*, 2019) entre otros. Estas soluciones pueden ser trasladadas a un entorno militar.

Dos grandes naciones como China y Rusia han invertido millones de dólares en investigar y desarrollar está tecnología para sus ejércitos a fin de estar a la vanguardia tecnológica mundial. Por este motivo, el ejército de Estados Unidos también ha invertido millones de dólares y el Departamento de Defensa de este país lo situó como prioridad en sus investigaciones. (Bilyana Lilly & Sale Lilly, 2021). La Unión Europea (UE) no se queda atrás en la carrera por el uso de la tecnología blockchain, así que a través de su Agencia Europea de Defensa está también investigando la incorporación de la tecnología a sus medios militares. (*Blockchain technology in defence*, no date). España, miembro de la UE desde el año 1986, está involucrado en los proyectos que la EDA desarrolla al ser esta una organización de integración.

Este Trabajo Fin de Grado (TFG) se ha realizado en la 33 Compañía (Cía.) del III Batallón (BON) del Regimiento de Transmisiones (RT) 21 ubicado en Burgos. Este Regimiento es el pionero en las pruebas tecnológicas que se realizan en el seno del Ejército de Tierra (ET) y que posteriormente se propagan al resto de las Fuerzas Armadas.

1.3. Estructura

El presente trabajo está estructurado en seis apartados. Primero una introducción al tema, seguido de unos conceptos básicos para poder entender en que consiste la tecnología blockchain y cómo funciona. Un desarrollo donde se analizarán los resultados y para finalizar unas conclusiones del trabajo realizado.

2. OBJETIVOS Y METODOLOGÍA

2.1. OBJETIVOS Y ALCANCE

Este trabajo tiene como objetivo principal, el análisis de las posibilidades del uso de la tecnología de la cadena de bloques en el ET. Para poder lograr este objetivo, se han llevado a cabo unas tareas para poder lograr el objetivo principal:

- Identificar y seleccionar los posibles casos de uso de aplicación en defensa.
- Análisis de la situación actual de los casos de uso identificados.
- Proposición de posible implementación de la cadena de bloques en el Ejército.
- Análisis comparativo de las soluciones propuestas.

Con la finalidad de facilitar la planificación de este proyecto, se ha realizado una estructura de Desglose de Trabajo (EDT) (Anexo I), que ha sido refleja gráficamente mediante un Diagrama de Gantt (Anexo II), en el que se especifican las tareas a realizar, duración y fecha de inicio prevista.

2.2. METODOLOGÍA

Desde el punto de la vista de la metodología, para llevar a cabo este trabajo y la obtención de los objetivos, se ha realizado primeramente una revisión bibliográfica de numerosa documentación de carácter técnico y artículos de opinión enfocados en la tecnología blockchain en el ámbito de defensa y civil.

En segundo lugar, se ha utilizado la técnica de grupos nominales, en ingles conocida como nominal group technique (NGT), para poder lograr que un grupo de expertos en la materia llegase a un acuerdo sobre cuáles serían los casos de uso que más posibilidades tienen de ser implementados en el ámbito del Ejército de Tierra. Además, se utilizó además la escala Likert para determinar esta decisión.

Seguidamente, se continuó con un proceso de investigación y entrevistas al personal del III BON del RT 21, sobre los sistemas actuales en los que se solucionan los casos de uso seleccionados.

Se ha obtenido una posible implementación de los casos de uso ganadores en la tecnología blockchain. Esta solución se ha basado en otras implementaciones que ya se han llevado a cabo en el ámbito civil.

Por último, la tarea de la comparación de los casos de uso, se ha utilizado el método cuantitativo de la matriz de Pugh.

3. CONCEPTOS BÁSICOS

Para poder entender que es la blockchain y cómo funciona, se necesita conocer una serie de conceptos básicos. Estos abarcan desde qué es el libro mayor distribuido hasta los contratos inteligentes.

3.1. Libro mayor distribuido

La tecnología de libro mayor distribuido o Distributed Ledger Technology (DLT), nos permite diseñar una estructura de sistemas que funciona como una base de datos no centralizada. Esto quiere decir, que no existe la figura de un servidor u ordenador central que se encargue de almacenar la información, si no que cada nodo[2] de la red almacena una copia del libro mayor donde se almacena la información. Esta descentralización proporciona mayor seguridad, transparencia y confianza entre las partes que la utilizan. (Dolader, Bel and Muñoz, 2017)

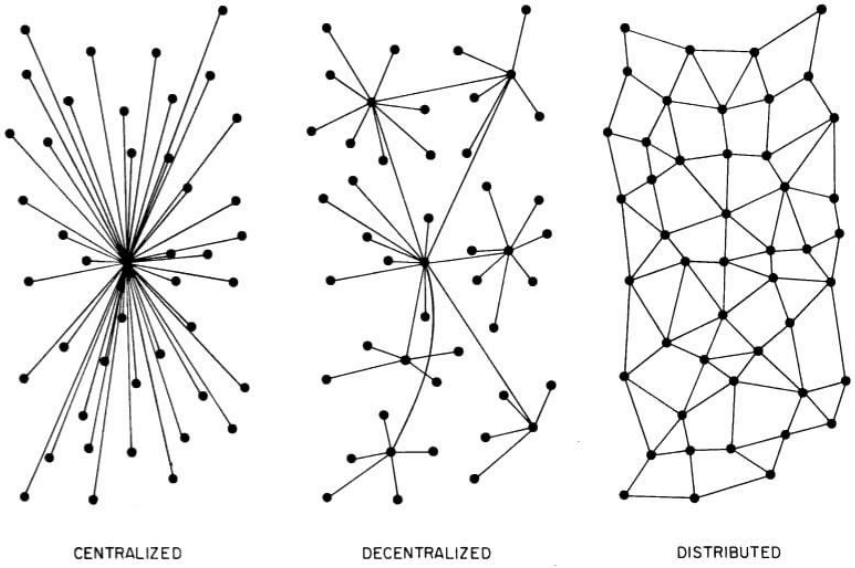


Figura 1: tipo de redes. (Baran, 1964)

Por lo tanto, la blockchain es una base de datos distribuida y su funcionamiento se basa en la creación de bloques[3] donde se almacena la información. Estos, después son enlazados entre sí, creando la blockchain, lo cual genera un registro enlazado

La estructura de la blockchain está formada por una sucesión de bloques ordenados, que están relacionados entre sí a través del hash[4], también conocido como la huella digital. Debido

[2] Un nodo es un ordenador/chip que se conecta a la red que almacena y distribuye una copia actualizada en tiempo real de la cadena de bloques (*Bit2Me Academy*, no date)

[3] Un bloque es un conjunto de transacciones confirmadas e información adicional que se incluye en la blockchain (*Bit2Me Academy*, no date)

[4] Un hash es una función criptográfica que transforma datos en una serie de caracteres con una longitud fija independientemente de la longitud de entrada. En el Anexo III se puede ver un

a que todos los bloques están relacionados entre sí por el hash del bloque anterior. Esto hace que, si alguien modificase la información de un bloque, la cadena detectaría que ha sido modificada. En el Anexo IV, se puede ver un ejemplo.

Las características de la cadena de bloques son: (*Nelson Rodriguez*, 2019)

- Inmutable: la blockchain es una red inalterable y permanente
- Distribuido: todos los participantes de la red tienen una copia del libro mayor, lo que proporciona transparencia completa, proporcionando información completa sobre los participantes de la red y las transacciones
- Descentralizado: no existe una autoridad central que se encargue de tomar las decisiones. Este proceso es llevado a cabo por un grupo de nodos.
- Seguro: todos los registros de la cadena de bloques están encriptados de manera individual.
- Consenso: en una red en la que es posible que los nodos no confíen entre sí, estos interaccionan gracias a que confían en el algoritmo de consenso[5] que se ejecuta para tomar las decisiones.
- Unánime: cuando un nodo quiere agregar un registro a la red, debe obtener un resultado favorable, es decir, que, si la mayoría de los nodos vota en contra de la propuesta, esta es rechazada.

3.2. Tipos de blockchain

Se pueden diferenciar cuatro tipos de cadenas de bloques: (*IBM Blockchain* , 2022)

- Pública: es el primer tipo de blockchain que existió, y son aquellas que se encuentra el acceso de manera pública desde internet. Este tipo de blockchain mantiene abierto los datos, software y desarrollo, de forma que cualquier persona puede auditar y desarrollar mejoras para la red. Además, este tipo de red permite que se mantenga la red descentralizada, democratizada y sin la figura de una autoridad que defina lo que está o no permitido. Ejemplos son la blockchain de Bitcoin o Ethereum.(*Bitcoin - Dinero P2P de código abierto*, no date) (*ethereum*, no date).
- Privada: con la evolución de la tecnología, las empresas empezaron a verse interesadas en la implementación de la misma. Esta blockchain cuenta con los mismos elementos que una blockchain pública, pero con la diferencia de que dependen de una unidad central, que controla las acciones dentro de la misma. Esta unidad central es la encargada de dar acceso a los usuarios, controlar sus funciones y los permisos que estos tienen dentro de la blockchain. No se puede considerar como una red descentralizada, ya que la autoridad de la misma puede modificar o eliminar cualquier bloque u operación. Se destaca el desarrollo por software libre de Hyperledger(*HyperledgerBlockchain Technologies*, no date) de la fundación Linux.

ejemplo

[5] Un algoritmo de consenso es un mecanismo que permite a los usuarios o máquinas coordinarse en un entorno distribuido. (*¿Qué es un Algoritmo de Consenso?* | *Binance Academy*, 2018)

- Consorcio: se le conoce también como permisionada privada, y es la unión entre la blockchain pública y privada en un intento de aprovechar lo mejor de ambos tipos, buscando la descentralización y la eficiencia. Se le conoce también como permisionada privada. Está gobernada por un grupo de organizaciones, en contraposición de la blockchain privada que solo es gobernada por una organización. En este tipo de cadena de bloques, la participación en red es privada, es decir, que el acceso a la red es controlado por una unidad central.Se puede destacar Global Shipping Business Network Consortium.(*GSBN*, no date)
- Híbrida: también conocida como permisionada pública. Este modelo de cadena de bloques es controlado solo por una organización al igual que la blockchain privada, pero se le añade un cierto nivel de supervisión ya que la información que se sube a la cadena es pública. De este tipo de blockchain, se puede resaltar la cadena de bloques híbrida creada por la empresa IBM, en concreto Food Trust. (IBM, 2021)

En la siguiente tabla se muestra un resumen de los tipos de blockchain anteriormente descritas

Tabla 1: clasificación de tipos de blockchain. Elaboración propia

Tipo de blockchain	Acceso	Participantes	Velocidad de transacción	Tipo de registro
Pública	Cualquiera	Anónimos	Lenta	Público
Privada	Única organización	Identidades conocidas	Rápida	Privado
Consorcio	Organizaciones seleccionadas	Identidades conocidas	Rápida	Privado
Híbrida	Única organización	Identidades conocidas	Rápida	Público

3.3. Árbol de Merkle

Dentro de la blockchain, el concepto de los hashes toma especial relevancia debido a, como se ha mencionado anteriormente, forma la huella digital del bloque. El árbol de Merkle toma importancia en este aspecto ya que se consigue aunar los hashes de todas las transacciones en uno solo.

El árbol de Merkle, el cual fue creado por Ralph Merkle en el año 1979, consiguiendo agilizar el proceso de verificación de las grandes cantidades de datos. El árbol, cobra vital importancia en el bloque, ya que se evita que se pueda cambiar las transacciones, con lo que ello conlleva.

El diseño que planteó Merkle, es una estructura de datos compuesta por hashes de los diferentes bloques de datos, y que consigue resumir todas las transacciones de un bloque en un solo hash.

Esta herramienta se caracteriza por:

- Ser un medio eficiente para generar una estructura de datos distribuida.
- Proveer gran seguridad y resistencia a la alteración de datos
- Permitir un gran nivel de rendimiento en la transmisión de datos en las redes distribuidas,

disminuyendo la cantidad de datos necesarios para el correcto funcionamiento.

- Computacionalmente son poco costosos y eficientes cuando se va a crear, procesar y verificar la información.
- Poseer una gran capacidad de adaptarse a los diferentes sistemas como pueden ser bases de datos, estructuras de llaves públicas, redes p2p o sistemas de versionamiento.
- Permitir búsquedas de verificación de manera rápida a través de ´´disección´´ sin llegar a comprometer la seguridad y trazabilidad de las transacciones que se realicen.

En la Figura 2, se puede observar la forma en la que se estructura un árbol de Merkle. Las transacciones están ligadas a sus respectivos hashes (hash0, hash1, etc). Estos hashes (TXO y TX1 respecto a hash0 y hash1) se vuelven a codificar para dar lugar a un hash que envuelve a los dos anteriores, dando lugar al Hash01. Este proceso se repetirá hasta que todas las transacciones del bloque estén ligadas a un solo hash.

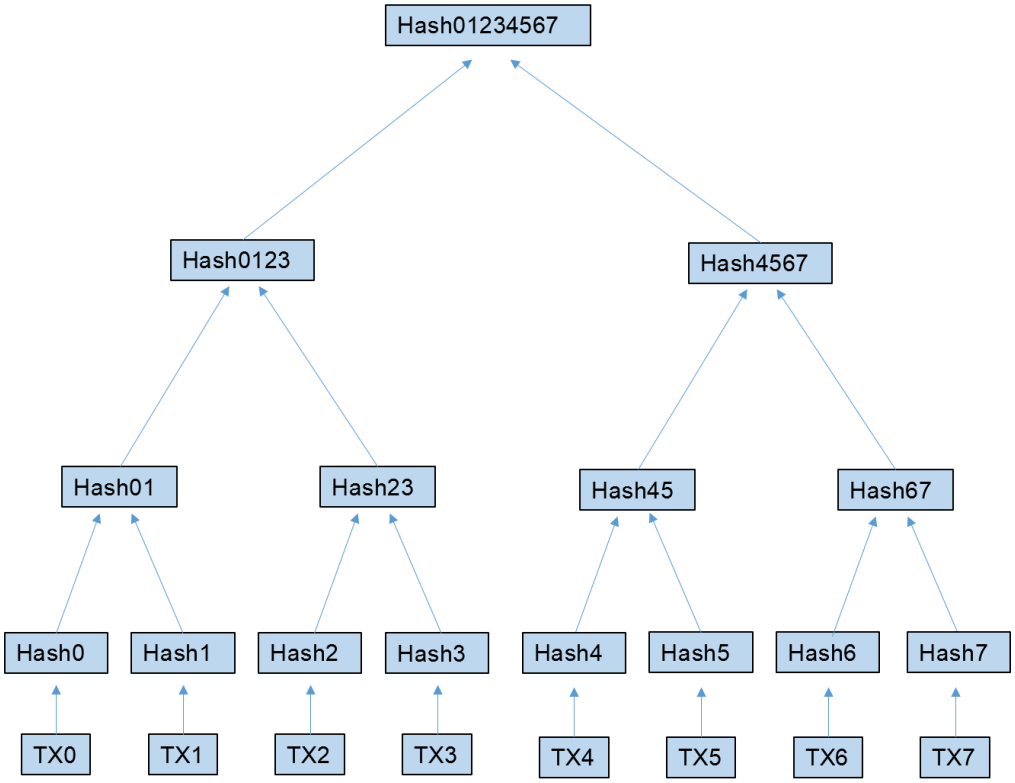


Figura 2: árbol de Merkle. Elaboración propia

3.4. Composición de un bloque

Dentro de la blockchain, cada bloque está compuesto por una serie de parámetros que se definen a continuación y que se pueden ver de manera gráfica en la figura 3.

- Hash del bloque previo: campo de 32 bytes que contiene la información que enlaza el bloque con el anterior. Al bloque anterior se le conoce como bloque padre, y al bloque de origen se le denomina génesis. Se utiliza el algoritmo de hashing SHA-256, consiguiendo evitar que se reviertan las transacciones, ya que, para llevar a cabo dicha tarea, habría que cambiar todos los hashes de los todos los bloques, lo que conllevaría gran cantidad de recursos computacionales.
- Timestamp: campo de 4 bytes que indica la fecha y la hora del bloque medida en tiempo

de Unix[6]

- Nonce: campo de 4 bytes. Es un número aleatorio que se emplea en la criptografía en los denominados protocolos de autenticación
- Hash árbol de Merkle: campo de 32 bytes. Se obtiene de los hashes de todas las transacciones que son incluidas en el bloque. Con este método nos aseguramos de que ninguna transacción haya sido modificada.
- Información: contiene todas las transacciones[7] que se quieren incluir dentro del bloque.

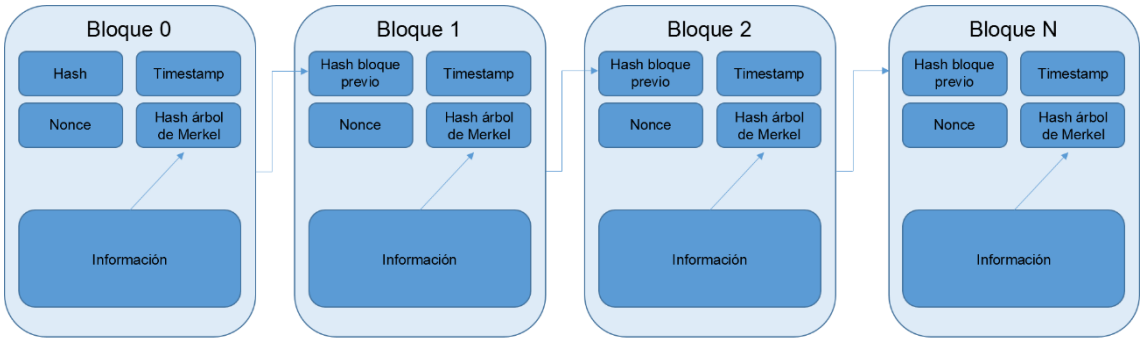


Figura 3: composición de la blockchain. Elaboración propia

3.5. Mecanismos de consenso

Los mecanismos de consenso en las blockchains son procesos de toma de decisión en grupo. Cada individuo de la red construye y apoya la decisión que sea mayoritaria, les guste o no. Un ejemplo puede ser en un grupo de 10 personas en una determinada empresa, donde quieren tomar una decisión que más fortalezca a la entidad, aunque cada participante pueda tener su propuesta, se acabará eligiendo la que mejores beneficios tenga. Este proceso, pero con miles y miles de personas se complica, pero gracias a este tipo algoritmo, se puede garantizar que todos los nodos estén sincronizados entre sí y que se establezcan una serie de normas sobre qué transacciones se pueden realizar y agregar a la cadena de bloques. (Miers *et al.*, 2019)

La importancia de los algoritmos de consenso viene de que, toda transacción en una blockchain debe ser validada. (Amores, 2020)

Los mecanismos de consenso más importantes son: (Miers *et al.*, 2019)

- Proof of work (PoW): este algoritmo fue de los primeros en implementarse en las cadenas de bloques, y es el más famosos porque es usado por Bitcoin y hasta el día 15 de septiembre de 2022 también por Ethereum.

  Definiendo la función Hash como y=H(x), donde por sus características es muy fácil de obtener y dada una x cualquiera. En cambio, dada una y cualquiera, el proceso de hallar

[6] segundos que han transcurrido desde enero de 1970 hasta el momento de creación del bloque

[7] Una transacción constituye las operaciones que se realizan para agregar información a una cadena de bloques

x es muy complicado, ya que no existe una definición de H^-1(x). La única forma de poder lograr un valor de x es a través de probar valores.

Este proceso se le conoce como minar, y consiste en que los nodos compiten por hallar el valor lo más rápido posible, para lo cual utilizan su capacidad de computación. El nodo que consigue averiguar la x que resuelve la función y=H(x), se le premia con una recompensa en forma de criptomoneda[8].

- Proof of Stake (PoS): el fundamento de este algoritmo consiste en que los nodos que minan son elegidos de manera previa de forma aleatoria. Los nodos, son seleccionados bajo el criterio de la tenencia de criptomonedas de estos nodos. En otras palabras, los nodos que posean mayor cantidad de criptomonedas tienen una mayor posibilidad de ser seleccionados. Para mantener la participación en la red de forma general, aquellos nodos que poseen menos activos también pueden ser elegidos, pero con una probabilidad menor.
- Proof of Authority (PoA): algoritmo basado en la reputación siendo una solución eficiente para las blockchain privadas. Los nodos validadores ponen su identidad real, y usan la reputación como la garantía de la transparencia de la red. Los nodos validadores son limitados, y se eligen de forma arbitraria dentro del grupo de nodos validadores confiables. Al ser reducido el número de nodos validadores, este algoritmo se vuelve preferente en los casos en los que se busque velocidad de generación de bloques.

3.6. Smart Contracts

Los Smart Contracts o contratos inteligentes, son programas que residen en la cadena de bloques y de los cuales los nodos tienen una copia. Para poder comprender totalmente se va a recordar lo que significa un contrato, siendo este un acuerdo entre dos o más partes, donde se define lo que se puede hacer, lo que no y qué sucederá si se incumple. En otras palabras, unas reglas del juego que permiten entender a las partes que interaccionan en que va a consistir la interacción. (Echabarría, 2017)

Estos contratos, son capaces de ejecutarse y hacerse cumplir de manera autónoma, sin la necesidad de intermediarios ni mediadores, cuando se cumplan las condiciones programadas en ellos y de manera totalmente descentralizada. Al ser contratos digitales hechos a través de lenguaje de programación, no cabe la posibilidad de malas interpretaciones. El lenguaje en el que están programados normalmente es Solidity. Cuando un Smart Contract se compila, este se convierte en código máquina conocido como bytecode. (Echabarría, 2017)

3.7. Dimensiones de la seguridad

Uno de los aspectos más relevantes que aporta la blockchain, es la seguridad. Pero ¿cómo se mide la seguridad de un equipo?

Las dimensiones de la seguridad, que se definen sobre un sistema con cómo de seguro es. Estas dimensiones tomarán importancia cuando se llegue a la comparación de los sistemas

[8] es un activo digital que emplea un cifrado criptográfico para garantizar su titularidad y asegurar la integridad de las transacciones, y controlar la creación de unidades adicionales. (Jiménez, 2022)

actuales con la blockchain.

Tal y como se recoge en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, las definiciones de las dimensiones de la seguridad son las siguientes:

- Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados, tienen acceso a los mismos cuando lo requieren.
- Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso), pueden ser trazadas de forma indiscutible hasta dicha entidad.
- Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

Pese a que el Esquema Nacional de Seguridad no recoge la dimensión de seguridad de no repudio o irrenunciabilidad, este sí que se considera a la hora de diseñar un sistema y se puede definir como un servicio de seguridad que permite probar la participación de las partes en una comunicación. (*CCN-CERT*, no date)

3.8. Criptografía asimétrica: clave pública y privada

En la actualidad, la criptografía en uno de los pilares más fundamentales en los que se sustenta la tecnología blockchain. Esta permite el funcionamiento de la red, garantizando el funcionamiento de los mecanismos de consenso entre los usuarios y la integridad de la cadena de bloques. (Bit2me Academy, 2022)

La criptografía asimétrica es un tipo de criptografía informática, y a su vez una de las técnicas más potentes. Este procedimiento está diseñado a partir del uso de una fórmula matemática compleja, para crear un par de claves: la privada y la clave pública. Por medio de estas claves, se establece un canal de comunicación seguro entre las partes, en el cual tanto el emisor como el receptor deben usar criptografía asimétrica, con el mismo algoritmo definido lo que permitirá crear un juego de clave único para cada uno. (*Grupo Atico34*, 2022)

Los sistemas de cifrado con claves asimétricas nos permiten garantizar la confidencialidad del mensaje o la autenticación del mismo. Para lograr la confidencialidad del mensaje, se debe cifrar con la clave pública de la persona a la que se le va a enviar el mensaje, de esta forma solo ella con su clave privada podrá descifrar el mensaje. En la figura 4 se puede observar el esquema de confidencialidad. (Granado Paredes, 2006).

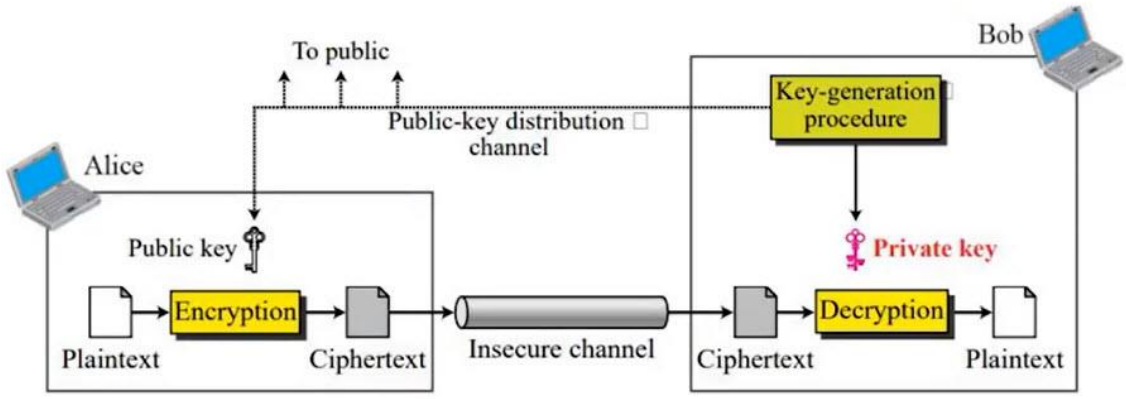


Figura 4: esquema de confidencialidad. (Abubakar Idris, Awwalu and kamil, 2016)

Mientras que para la autenticación el remitente firmará con su clave privada, de forma que la persona a la que se le envía el mensaje use la clave pública, para descifrar el mensaje y verificar que es el remitente. Este proceso se conoce como firma digital. En la figura 5 que se muestras a continuación, se puede ver el esquema de autenticación (Granado Paredes, 2006).

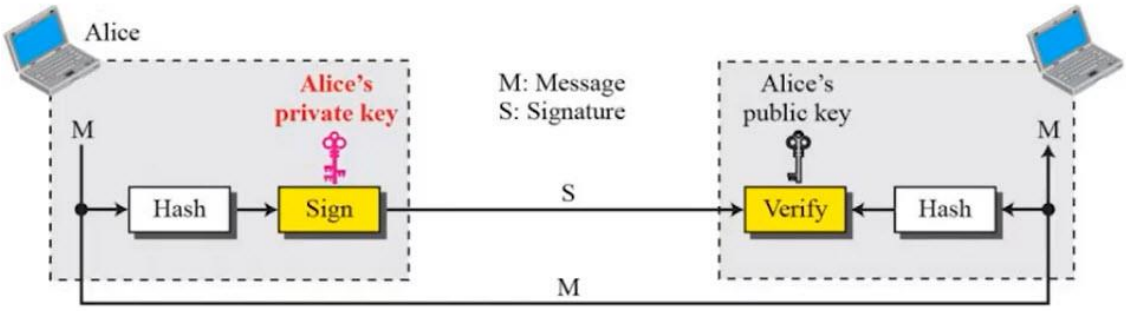


Figura 5: esquema de autenticación. (Abubakar Idris, Awwalu and kamil, 2016)

3.9. Alastria

Hogaño, Alastria es referencia nacional en el desarrollo de la economía digital, ya que, a través de sus métodos innovadores, promueve la adaptación de servicios usando la red de blockchain como plataforma de desarrollo. Esto le está sirviendo para que algunas empresas, vean en ella una oportunidad de aprovechar los beneficios que aporta la tecnología de la cadena de bloques, sin la necesidad de desembolsar grandes cantidades de dinero. Se puede destacar empresas como Indra, Telefónica o Repsol a la vez que diversas universidades, las cuales se han unido a esta asociación. (*Europa Press,* 2021)

Alastria es una asociación sin ánimo de lucro, fundada en 2017 bajo el nombre de Red Lyra, que fomenta la economía digital a través del desarrollo de tecnologías del libro mayor, distribuido y que actualmente cuenta con el apoyo del Ministerio de Ciencia e Innovación. Esta organización es usada en proyectos de carácter institucional, y es sinónimo de cumplimiento normativo con sistemas de información y la protección de datos de carácter personal. (Ecosystem, 2019)

Dentro de esta plataforma, existen dos redes distintas sobre las cuales los socios pueden desplegar sus nodos. Esto es debido a que los socios de Alastria, decidieron que se tenía que

mantener una organización “Blockchain agnostic“ [9]. Esta decisión, está determinada porque distintas redes pueden adaptarse mejor a las necesidades de cada situación, asimismo pudiera pasar que un protocolo de Blockchain perdiese soporte, debido a que no prosperase. En la actualidad, Alastria está conformada por dos redes, Red Telsius (Red T) y Red Besu (Red B) y una tercera red que está en desarrollo, la Red H. Respectivamente, usan las tecnologías de Quorum (ConsenSys, 2021), Hyperledger Besu e Hyperledger Fabric.(*Hyperledger*, 2022) (Ecosystem, 2021)

Tanto la Red T y la Red B están desarrolladas a partir de Ethereum, implicando que se posibilite la utilización de Smart Contracts. Alastria, está trabajando en ambas redes. Sin embargo, la Red B ha tenido una menor aceptación a la hora de desarrollar proyectos. (Garcia Joga and Arahuetes, 2019)

3.9.1. Red T

Su actual Red T está basada en la tecnología Quorum. Esta red fue creada a partir de un fork[10] de Ethereum, compartiendo la pluralidad de sus propiedades (De la Vega Sánchez, 2020). Esta red se puede enmarcar dentro de la clasificación que se recoge en la tabla 1 como una red de consorcio, ya que está controlada por varias organizaciones y el registro de transacciones que se llevan a cabo dentro de la blockchain en privado.

De las características de Quorum se puede destacar que se trata de una blockchain de consorcio, que nos permite la implementación y el uso de Smart Contracts de manera privada. El fork provocó cambios en la cadena, haciendo que esta se orientase hacia otros ámbitos. (Baliga *et al.*, 2018)

Se pueden destacar las siguientes características de Quorum:

- No se necesita una criptomoneda nativa como es el caso de los ethereums en la de Ethereum, ya que las acciones que se ejecuten en esta red no conllevan un coste asociado.
- Permisionado de la red: esta faceta hace que esta tecnología sea interesante para el marco empresarial. Esto quiere decir que, los nodos van a decidir qué nodos se incorporan a la red y cuales están conectados, protegiendo de esta forma el acceso a la red.
- Apoyo de privacidad: permite la realización de transacciones sin que estas sean públicas para otros miembros del consorcio. La privacidad se habilita en Quorum, al dividir el libro mayor en un libro mayor público y un libro mayor privado, este último solo visible para las partes que realizan las transacciones. Solo un hash de la transacción privada aparecerá en el libro mayor público, siendo las partes de la operación los poseedores de las claves para decodificarla y visualizarla. Los Smart Contracts, del mismo modo también pueden ejecutarse de forma privada, siendo solo visible para las partes que realizan la transacción.

La descentralización de la red viene determinada por el algoritmo de consenso de

[9] No se confía el desarrollo en una sola plataforma

[10] bifurcación de la cadena de bloques principal debido a las modificaciones del código base

Tolerancia, a Faltas Bizantinas de Estambul o Instambul Byzantine Fault Tolerant (IBFT). Este mecanismo de consenso es del tipo de PoA, en el que se selecciona de manera arbitraria un nodo validador para proponer un bloque, y el resto de los nodos, votarán sobre su validez. Si hay consenso, se añadirá el bloque a la red, si no, un nuevo nodo será seleccionado para que proponga otro bloque. (Baliga *et al.*, 2018)

Este protocolo es de los más usado en las redes de consorcio, ya que permite a diferencia de los algoritmos de las redes públicas como PoW, ahorrar costes. Además, permite que la red funcione con un número reducido de nodos validadores, traduciéndose esto en una mayor eficiencia en comparación con las redes públicas, tanto a niveles de velocidad de transacciones como de energía. (Baliga *et al.*, 2018)

La arquitectura de esta red está compuesta por distintos tipos de nodos; validadores, permisionadores y observadores.(Ecosystem, 2019)

Los nodos validadores son los que ejecutan el algoritmo de consenso IBFT, y a su vez, responsables de generar la confiabilidad y neutralidad al crear los bloques. Por su parte, los nodos permisionadores se encargan de dar los permisos a los nodos observadores. Finalmente, los nodos observadores son los responsables de aceptar las transacciones, verificarlas y entregarlas a los validadores. En la figura 6 se puede ver la relación ya mencionada de forma gráfica.

En la actualidad, el esquema de la red consta de: (*Alastria*, no date)

- 9 nodo validadores
- 3 nodos permisionadores
- 126 nodos observadores

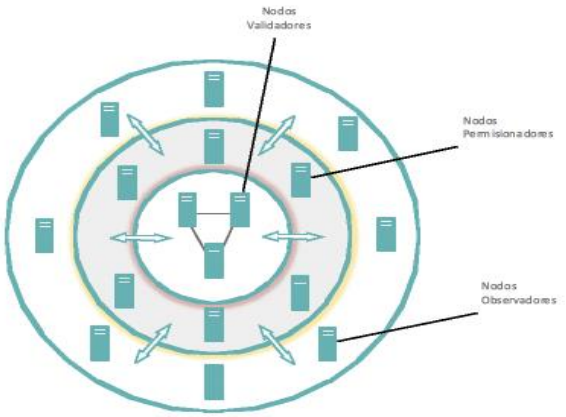


Figura 6: esquema de los nodos de la Red T (Guillermo Araujo, 2019)

Los requisitos mínimos de un nodo cualquiera de la Red T son los siguientes:

- CPU's: 2 cores (4 cores recomendado)
- Memoria: 4 Gb (8 Gb recomendado)
- Disco duro: 100 Gb SSD (1 Tb recomendado)
- Sistema operativo: Ubuntu 16.04, CentOS7.4 o Red Hat Enterprise Linux 7.4 Con 64 bits.

Estos requisitos mínimos son importantes, ya que cuanto más rápidas sean las máquinas de cada nodo de la red, más rápido se puede ejecutar el algoritmo de consenso y aumentar así el rendimiento. También, es importante el disco duro, debido a que, por las características de la cadena de bloques, se quedará guardada una copia del libro mayor en cada nodo.(Yang *et al.*, 2021)

Alastria en la actualidad cuenta con más de cuarenta proyectos en su red, en los que se destaca las facetas de sostenibilidad, tercer sector, industrias culturales y creativas, marketing, participación ciudadana, facturación, educación, veterinaria, agrifood, banca y finanzas, legal, salud, recursos humanos, real estate, transporte y logística e identidad digital.

4. DESARROLLO: ANÁLISIS Y RESULTADOS

4.1. Selección de casos de uso

Uno de los objetivos del trabajo es identificar y seleccionar los casos de uso de interés para el ET y esto se ha realizado a través de la técnica NGT. Este, consiste en un método estructurado para el intercambio de ideas en grupo, donde se fomentan las contribuciones de todos, y facilita un acuerdo rápido sobre la importancia relativa de los problemas o soluciones. (*LAEDU*, no date)

El grupo estaba compuesto por tres participantes. El número de integrantes estaba limitado por el personal que tenía conocimiento del tema dentro de la base militar. En concreto, el grupo estaba formado por un Capitán (Cap) y dos Tenientes (Ttes) de la Cía 33 del III BON del RT 21, ubicado en la ciudad de Burgos. Este proceso, se dividió en cuatro fases que fueron realizas en común en una sala con la ayuda de una pizarra.

- Generación de ideas: se lanzó una pregunta al grupo, ¿Qué posibles casos de uso tiene la blockchain en el ejército? Los componentes del grupo apuntaron sus ideas en un papel.
- Presentación de las ideas: cada persona salía a la pizarra y escribía una idea de su lista, y así hasta que se escribieron todas las propuestas.
- Discusión de las ideas: este paso fue el más laborioso, ya que se tuvieron que defender las ideas, y explicar porque si pudieran ser posible para una implementación en el ejército.
- Votación: cada participante le asignó una puntuación a cinco de las ideas puestas en común, de forma que el valor de cinco es el máximo y uno el mínimo.

Tabla 2: votación sobre los casos de uso del grupo. Elaboración propia

Puntuación (5-1)	Cap	Tte 1	Tte 2
5	Mensajería	Cadena de suministro	Gestión de identidades
4	Gestión de identidades	Gestión de identidades	Mensajería
3	Cadena de suministro	Internet of Things (IoT)	Sistemas autónomos
2	Sistemas autónomos	Logística	Cadena de suministro
1	Almacenamiento y transmisión de datos	Impresión 3D	Almacenamiento y transmisión de datos

Tras la votación, se procedió a la suma de la puntuación y la elección de los tres primeros clasificados.

Tabla 3: clasificación de los casos de uso. Elaboración propia

Clasificación	Caso de uso	Puntuación
1	Gestión de identidades	13
2	Cadena de suministro	10
3	Mensajería	9
4	Sistemas autónomos	5
5	IoT	3
6	Almacenamiento y transmisión de datos	2
7	Impresión 3D	1

Después de la realización del NGT, los casos de uso ganadores fueron la gestión de identidad, la cadena de suministro y la mensajería. La puntuación se recoge en la tabla 3.

4.2. Análisis de la situación actual de los casos de uso seleccionados

A continuación, se va a proceder a analizar como están implementados estos casos de uso actualmente en el ET.

4.2.1. Gestión de identidades

El primer caso de uso que se analizará será la gestión de identidades. En la actualidad vivimos en un mundo que está cada día más interconectado, donde la privacidad y el acceso a los datos personales está lejos de ser dictaminados por su propietario. Las empresas en las que nos registramos o las redes sociales entre otras, venden nuestros datos personales, sin que se tenga ningún control sobre la decisión sobre ello. Un ejemplo de esto es el uso de las cookies de algunas páginas web, donde se utilizan las cookies propias y de terceros para mostrarnos una publicidad relacionada con nuestras preferencias, las cuales están determinadas por el análisis de nuestros hábitos de navegación.

Además de lo descrito anteriormente, la gestión de identidades centralizadas experimenta problemas con la seguridad, ya que, al contar solo con una base de datos centralizada, pueden ser atacadas por hackers, pudiendo robar la información y los datos privados. Facebook en 2021 sufrió una brecha de seguridad, en la que la información de 500 millones de personas se filtró, incluyendo en esta información número de teléfono, nombre completo, ubicación, fecha de nacimiento entre otras. (*Andrew Thurman*, 2021)

Se define la identidad como “conjunto de los rasgos propios de un individuo o de una comunidad“ (*t-Formas*, *2020*). Estos rasgos pueden ser fisiológicos o no físicos. Las cualidades fisiológicas que definen una identidad son; el ADN, el rostro, la voz, las huellas dactilares, el habla, el olor etc. Mientras que los atributos no físicos que nos definen, se crean de manera mayoritaria en nuestro cerebro, como los conocimientos, habilidades, recuerdos, sentimientos, etc.

Para confrontar la identidad, se compara los rasgos con los datos almacenados previamente. Por ejemplo, cuando en un control rutinario en la carretera, la Guardia Civil nos para y nos piden el carnet de conducir, se está comparando nuestra apariencia y datos

biométricos con la fotografía del documento acreditativo. Otro ejemplo, puede ser el inicio de sesión en nuestras redes sociales, donde se nos solicita una contraseña y se coteja el conocimiento del individuo.

En la actualidad, el caso de uso de la gestión de identidades está solucionado en el ET a través de una infraestructura de claves públicas (PKI) en la que el personal hace uso de ella para firmar documentos. La PKI está gestionada en los acuartelamientos militares por los Puntos Oficiales de Contacto para los Sistemas de Información y Telecomunicaciones (CISPOC), de forma que cuando una persona llega nueva a la unidad, el personal del CISPOC registra los datos y confirma la veracidad de los mismos. Un ejemplo de este caso de uso es cuando un Tte realiza una orden de tiro, este documento se realiza cuando se va a llevar a cabo un ejercicio de fuego real en los campos de tiro habilitados y son importantes ya que en caso de que hubiese algún accidente, están recogidas las medidas a adoptar para solucionarlo. Este documento, se firma a través de la PKI para poder acreditar que ha sido realizado por el Tte y que se hace responsable de ello.

El proceso de toma de información sobre personal destinado en otras compañías de la misma base militar o incluso de otra plaza es algo tedioso, ya que en la actualidad se realiza de manera manual y en ocasiones son necesarias muchas llamadas telefónicas para poder llegar a los datos correctos.

Una PKI es un sistema de recursos, políticas y servicios que da soporte al uso del cifrado de claves públicas para autenticar a las partes que participan en una transacción (*IBM*, no date).La PKI está compuesta por los diferentes actores que se definen a continuación y que se pueden ver en la figura 7. (Castro Martínez Francisco Javier, 2015)

- La autoridad de certificación (AC): encargada de emitir y revocar certificados. Es la entidad de confianza, que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
- La autoridad de registro (RA, Registration Authority): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.
- La autoridad de validación (VA, Validation Authority): es la encargada de comprobar la validez de los certificados digitales.
- La autoridad de sellado de tiempo (TSA, TimeStamp Authority): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo. Esta última no será implementada.
- Los usuarios y entidades finales, son aquellos que poseen un par de claves (pública y privada), y un certificado asociado a su clave pública. Utilizan un conjunto de aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.)
- Servidor de certificados: componente encargado de expedir los certificados aprobados por la autoridad de registro. La generación de la clave pública para el usuario, está formada por los datos del usuario y finalmente se firma digitalmente con la clave privada de la autoridad de certificación.

Figura 7: componentes de una PKI y sus relaciones. (Bohorquez, Guzman and Naranjo, 2013)

4.2.2. Cadena de suministro

El segundo caso de uso que se analizará será la cadena de suministro. El término gestión de la cadena de suministro, acuñado en la década de 1990, ha ganado popularidad en los últimos años en gran parte debido a su importancia en el sector logístico en términos de eficiencia y costo para los clientes, tanto con la industria civil como en la militar.

La cadena de suministro actualmente se controla en el ejército a través de Sistema Integrado de Gestión Logística del Ejército de Tierra (SIGLE). Este sistema es utilizado por más de 10.000 usuarios repartidos en más de 1.000 Unidades, Centros u Organismos y por donde se gestionan más de 500.000 distintos materiales.(MALE, 2014)

El sistema de SIGLE es una aplicación web basada en el estándar J2EE[11]. En la figura 8, se puede observar como el cliente, el usuario final de la aplicación se conecta a través del navegador web de la WANPG a una web que nos provee de los servicios que a su vez está enlazada con la capa de acceso a los datos. Esta capa es la que muestra por pantalla una interfaz del almacenamiento de datos, en nuestro caso una base de datos Oracle.

[11] J2EE: es una plataforma para el cómputo empresarial a partir de la cual es posible el desarrollo profesional de aplicaciones empresariales distribuidas sobre una arquitectura multicapa, que son escritas con el lenguaje de programación Java y son ejecutadas desde un servidor de aplicaciones.) (*¿Qué es J2EE?*, 2016)

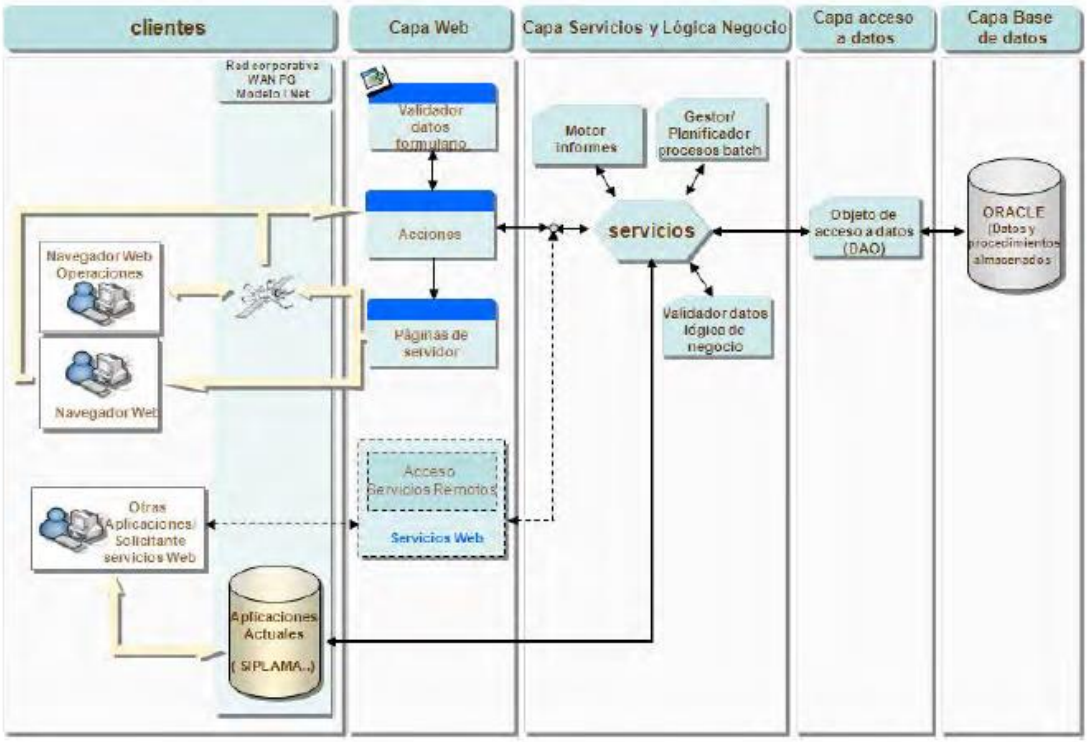


Figura 8: estructura de SIGLE. (MALE, 2014)

SIGLE está estructurado por las siguientes aplicaciones:(MALE, 2014)

- SIGLE Aplicación web. Aplicación web para la gestión integrada de la actividad logística del Ejército. El SIGLE está dividido en 7 subsistemas, 6 subsistemas para la gestión logística y 1 subsistema de administración:
    - abastecimiento
    - mantenimiento
    - transporte
    - adquisiciones
    - planificación
    - datos básicos
    - administración sistema.
- SIGLE Dispositivos Móviles. Aplicación cliente-servidor, que extiende la funcionalidad del subsistema de transporte a dispositivos móviles lectores de códigos de barras utilizados para la gestión logística del transporte en los puntos de recogida y distribución (PRD).
- SIGLE Visor GIS. Aplicación web que extiende la funcionalidad del subsistema de transporte del SIGLE, dotando al sistema de consulta y gestión de información logística georreferenciada.
- SIGLE Planificador GIS. Aplicación cliente-servidor que extiende la funcionalidad del subsistema de transporte del SIGLE, permitiendo la planificación del transporte mediante el empleo de algoritmos de optimización de costes.

- Interfaces con otros Sistemas:
- El sistema SIGLE intercambia diariamente información con múltiples sistemas, tanto del MALE como externos a él. El intercambio de información es bidireccional, y se realiza mediante el intercambio de ficheros (modalidad diferida) y mediante servicios web (modalidad en tiempo real).

SIGLE, cuenta actualmente en su sistema con bases de datos. Por aplicativo se puede cuantificar el número de tablas y procedimientos/funciones PL/SQL de las bases de datos de SIGLE:

Tabla 4: número de tablas y procedimientos de SIGLE. Elaboración propia

Bases de datos

Aplicativo	Elemento	Cantidad
SIGLE web	Tablas de BD	524
	Procedimientos/funciones PLSQL	4.680
SIGLE PRD	Tablas de BD	13
SIGLE visor GIS	Tablas de BD	29
SIGLE planificador GIS	Tablas de BD	27

En la actualidad, la trazabilidad de los envíos consta de dos fases. Por un lado, la infraestructura civil que por ejemplo la empresa El Corte Inglés tiene montada en su red, que está integrada con una empresa de mensajería externa, en este caso se realiza a través de Correos y Celeritas. La siguiente fase, se inicia cuando el Parque y Centro de Abastecimiento de Material de Intendencia (PCAMI) recibe el pedido y posteriormente, lo envía a las unidades.

El seguimiento de un pedido es actualizado de forma manual por un operario que con un lector de códigos de barras o QR y se actualiza su posición en una base de datos. (*El código postal,2020).* En la figura 9, se puede observar cómo se registra la segunda fase del proceso, pero la primera parte del proceso no es accesible para el usuario final. En lo que concierne a la trazabilidad del PCAMI, el personal encomendado para el pedido se encarga de actualizar los datos en una base de datos y esta se sincroniza con su programa informático, permitiendo que el usuario que ha hecho el pedido pueda ver la trazabilidad del pedido a través de un entorno web.

AGM

FASE	DESCRIPCION	PERIODO	FECHA
SOLICITUD PEDIDO	Periodo estipulado para que el individuo solicite el/los pedidos	01/01/2022 |A| 31/01/2022	29/01/2022
PREPARACION DE PEDIDO	Fecha de preparación para que la E. Logística prepare el pedido		15/03/2022
INTERVENCIÓN	Acto en el que la Comision Receptora da la conformidad al pedido para su envio		23/03/2022
ENVÍO	Fecha en la que el pedido es enviado al destino		04/04/2022
RECEPCIÓN AGRUPACIÓN PEDIDO	Periodo de entrega en la Agrupación del pedido del individuo	04/04/2022 |A| 05/04/2022	21/04/2022
RECEPCIÓN UCO PEDIDO	Periodo de entrega en la UCO del pedido del individuo	04/04/2022 |A| 04/05/2022	21/04/2022
ENTREGA PEDIDO	Periodo de entrega del pedido al individuo	21/04/2022 |A| 01/05/2022	20/04/2022
CONFORMIDAD ENTREGA	Periodo estipulado para que el individuo dé la conformidad a la entrega	19/05/2022 |A| 03/06/2022	04/06/2022

Figura 9: captura de pantalla del programa informático utilizado por el PCAMI.

4.2.3. Mensajería

Finalmente, el caso de uso que se analizará será la mensajería. El desarrollo del correo

electrónico interpersonal y su rápida extensión a través de internet puso de manifiesto la eficacia de esta tecnología en la tramitación de mensajes con datos adjuntos entre dos o más usuarios de correo. Pero la deficiencia de esta tecnología en cuanto a la validez jurídica de los documentos tramitados, y la falta de aclimatación al procedimiento administrativo, hicieron que no se pudiese autorizar el uso del correo electrónico interpersonal como correo oficial. (Academia Básica del Aire, 2022)

Esto ha hecho, que dentro del entorno del ET se cree la necesidad de dotar con la firma digital a la mensajería, para poder dotarla de un carácter oficial, implicando que el documento que tiene validez es el documento electrónico y no la copia impresa. Esto obliga a establecer un sistema de gestión documental, donde quede archivada y custodiada la documentación de forma digital.

Sistema de Mensajería Oficial y Gestión Documental (SIMENDEF), contribuye a dar una solución en el ámbito corporativo para la información de carácter oficial, y sin clasificar que requiera registro con la construcción, circulación por conducto reglamentario, firma electrónica, registro, transporte y gestión documental. (Academia Básica del Aire, 2022)

Surge con la necesidad de unificar los sistemas de mensajería y gestión documental existentes en el Ministerio de Defensa y las Fuerzas Armadas, a la vez que se mejora la coordinación de los trabajos conjuntos.

En la actualidad, SIMENDEF se establece como un modelo cliente servidor. Este procedimiento se basa en que los clientes realizan peticiones a un servidor central, que es el encargado de dar las respuestas. Esta arquitectura genera una total centralización del servicio.

Dentro de SIMENDEF, se encuentra con diferentes tipos de perfiles:

- Usuario de célula: puede crear y recibir oficios
- Responsable de célula: aparte de crear y recibir oficios, tiene acceso a la mensajería del resto de usuarios de su célula.
- Órgano Auxiliar del Mando (OAM): usuario encargado de la preparación de los documentos de salida, gestión del portafirmas para la firma de documentos oficiales y/o de la gestión de los de la entrada de una autoridad.
- Autoridad: usuario con la facultad de firma de oficio o documento. Es la dirección telegráfica capaz de recibir información oficialmente
- Registrador: usuario responsable del registro de entrada y/o salida de toda la documentación de ámbito registral
- Administrador local: usuario responsable de configurar y mantener las tablas de autoridades, ámbitos registrales, portafirmas y células, así como de administrar los permisos de acceso al sistema.

4.3. Verificación de los casos de uso

Una vez seleccionados los casos de uso y descrito como están solucionados en la actualidad, se usará para validarlos el diagrama de flujo titulado: Do you need a Blockchain? (Emmadi *et al.*, 2019).La primera decisión que se encuentra en el diagrama se recoge si se necesita almacenar la información. Después se encuentra si hay múltiples escritores, es decir, si más de una persona tienen que tener la capacidad de añadir datos al sistema. Se sigue el camino con la respuesta afirmativa a la anterior decisión y se localiza siguiente toma de decisión en la que pregunta si todos los escritores son conocidos. Seguidamente surge la pregunta de si todos

los escritores son conocidos, esto quiere decir si se puede verificar sin posible fallo que la persona es quien dice ser. Otra cuestión es si la información es verificable de forma pública, esto significa que si alguien externo a nuestra red puede ver los movimientos que se hacen dentro de ella. Finalmente, hay otra decisión en la que se recoge si los datos críticos deben ser a pruebas de manipulaciones.

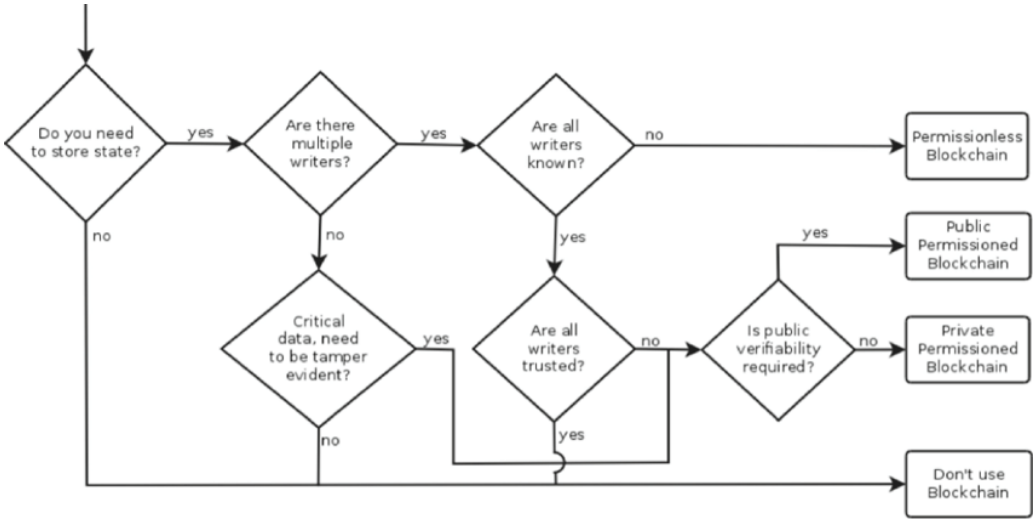


Figura 10: diagrama de flujo para la elección del tipo de blockchain. (Emmadi *et al.*, 2019)

Siguiendo el diagrama de flujo de la figura 10, se podrá deducir si nuestros casos de uso son adecuados para la implementación a través de la tecnología de la blockchain.

- Gestión de identidades: en este caso de uso, se necesita un lugar en el que estén almacenadas las claves públicas de los usuarios. Hay múltiples escritores porque nuestro sistema está centralizado y los diferentes gestores de las unidades acceden a él para añadir datos. Todos los escritores son conocidos, ya que el personal que accede al sistema se ha identificado previamente, pero no todos los nodos son de confianza debido a que, aunque los escritores inicien sesión en el sistema, no se puede verificar que sean ellos. Finalmente, la información sólo debería ser accesible al personal que esté dentro de la red, no siendo pública. Se puede deducir a través del diagrama de flujo, que este caso de uso si es compatible con la implementación de la tecnología de la cadena de bloques, y en concreto con un modelo de blockchain permisionada privada.
- Cadena de suministro: se necesitará un almacén donde guardar la información sobre los envíos, habiendo múltiples escritores, debido a que el sistema está centralizado en Madrid y se usa en todas las unidades de España. Todos los escritores son conocidos, ya que para acceder al sistema se tienen que identificar, pero no todos los nodos son de confianza debido a que, aunque los escritores inicien sesión en el sistema, no se puede verificar que sean ellos. Para concluir, la información no es pública, sólo debería tener acceso a ella el personal que está dentro del sistema. Se puede deducir a través del diagrama de flujo, que este caso de uso si es compatible con la implementación de la tecnología de la cadena de bloques, y en concreto con un modelo de blockchain permisionada privada.
- Mensajería: En concreto, para este caso de uso, se necesita almacenar un registro del flujo, con datos como que se ha enviado, cuando se ha enviado o quien lo ha enviado. Además, en el sistema hay más de un escritor, ya que el sistema está creado de manera

centralizada y es usado en todas las unidades del ET. Para poder acceder al sistema, el usuario necesita iniciar sesión con sus datos, por lo que los escritores son conocidos. Por su parte, no todos los nodos son de confianza ya que, aunque los escritores inicien sesión en el sistema, no se puede verificar que sean ellos. La información no será publica, ya que sólo debería ser accesible para el personal que pertenezca a la red. Se puede deducir a través del diagrama de flujo, que este caso de uso si es compatible con la implementación de la tecnología de la cadena de bloques, y en concreto con un modelo de blockchain permisionada privada.

4.4. Plataforma a utilizar

Tras la realización de un estudio de las posibles plataformas para la implementación de nuestros casos de uso, se pueden destacar las siguientes opciones:

4.4.1. Gestión de identidades: Sovrin

Para la implementación de la gestión de identidades, se centrará el uso de la blockchain de Sovrin, líder en este sector (Modelo de negocio y plan de marketing de la start- up “LinKple”, 2020). Esta es una organización internacional sin fines de lucro. Esta blockchain es pública, de forma que todas la personas u organizaciones pueden obtener una identidad en Sovrin. Además, esta red está autorizada, es decir, que la infraestructura para garantizar el consenso sobre las transacciones de la identidad se proporciona por los administradores que son examinados y autorizados. (de la Torre, 2022)

Esta organización está formada por una unión entre varias empresas a lo largo del mundo, siendo su misión proporcionar la infraestructura necesaria para hacer posible que la identidad soberana sea accesible para cualquier individuo.(*Bit2me Academy*, 2022). Se puede destacar la colaboración de Sovrin con empresas como International Business Machines o la Fundación de Identidad Descentralizada (DIF) (Escobar Moleiro, 2018)

La arquitectura de Sovrin está dividida en 4 capas básicas:

- La capa kernel, la cual es la primera capa, está formada por nodos validadores con la capacidad de escritura, es decir, tiene permiso para añadir bloques a la cadena. Estos nodos deben estar autorizados por los órganos responsables del sistema.
- La segunda capa la conforman los nodos conocidos como observadores, que solo pueden a leer información de la cadena. Dado que las operaciones de escritura consumen más recursos que las operaciones de lectura, la finalidad de los nodos observadores es resolver solo las solicitudes de lectura lanzadas por los clientes.
- La tercera es conocida como capa de clientes. Esta capa actúa como agentes o distribuidores autorizados. Estos clientes actúan efectivamente como clientes de los nodos, pero al mismo tiempo como servidores de los clientes finales. Actúan como un portal permanente para los usuarios finales de la Red Sovrin, a pesar de depender de los nodos para las funciones del servidor. Los clientes de esta capa representan a los clientes finales y distribuyen sus demandas a través de la Red Sovrin. El uso de múltiples aplicaciones en un cliente no requiere que los usuarios sincronicen manualmente sus datos. En su lugar, utiliza un servicio en la nube que permite que todas las aplicaciones del lado del cliente almacenen de forma segura información vinculada a la identidad y copias de seguridad criptográficas.
- La última capa que hay es la capa más periférica, la cual se ejecuta sobre los dispositivos finales. Estos clientes son la interfaz directa con los usuarios, y son aplicaciones

aplicaciones que se conectan con Sovrin a través de una interfaz directa.

Figura 11: logo de la empresa Sovrin. (Sovrin, 2022)

4.4.2. Cadena de suministro: VeChain

Para la implementación de la cadena de bloques en este caso de uso, se puede destacar la blockchain de VeChainTor.

VeChain fue creado en 2015, centrando su esfuerzo en el concepto de Internet de las cosas, en inglés IoT que, combinado con la tecnología de la cadena de bloques, permitió la gestión de la cadena de suministros. (*VeChainThor Blockchain* , no date)

VeChain tiene dos pilares; tecnología del mundo real y criptomoneda.

Con la tecnología del mundo real se hace referencia a los sistemas como RFID, códigos QR o NFC que se añaden a los productos o al envoltorio, junto a una serie de sensores que almacenan la información de las etapas de la cadena de suministro, y que vinculan la identidad del producto. La franqueza de estos datos se garantiza mediante la blockchain, ya que una vez los datos se almacenan en un bloque, resulta casi imposible modificarlos. (*Cointelegraph*, no date)

VeChain cuenta con su propia criptomoneda llamada VET, la cual es un token de utilidad dentro de su propia blockchain. Por otra parte, existe otro token denominado VeThor (VTHO), que nos permite acceder a la tecnología de la cadena de suministro, utilizándose para agregar la información a la blockchain durante el proceso de transporte. La criptomoneda cobra importancia a la hora de querer establecer un nodo, ya que desde la empresa se nos exige tener comprada un mínimo que oscila desde los seiscientos mil tokens hasta los veinticinco millones para un nodo validador (Alfonso Martínez, 2020). El precio de esta criptomoneda ha alcanzado un pico de precio 0.25 $.

Algunas empresas internacionales que trabajan con esta plataforma como Grupo BMW, Grupo Renault, Walmart o DB Schenker entre otros

Figura 12: : logo de la empresa Sovrin. (ZenLedger, 2022)

4.4.3. Mensajería: LedgerMail

Una posible solución para la mensajería es LedgerMail, que nos ofrece un correo electrónico descentralizado, con el motivo de proteger los derechos digitales a través del uso de la tecnología blockchain. Esta plataforma nos facilita el uso de un correo electrónico inmutable, privado y seguro y dejando de lado los protocolos de correo electrónico tradicionales, los cuales están desfasados, ya que los protocolos se desarrollaron en 1982 y su última actualización fue en 2008 (Montero, 2020) .En esta blockchain, cada email se trata como una transacción y a través del mecanismo de consenso de XDPoS se valida.(Ledgermail - Web3 Email, no date)

La plataforma se ejecuta sobre una cadena de bloques de tercera generación. Cuenta en la actualidad con 108 nodos encargados de la validación y tiene en espera otros 192 nodos.(Rita Aguado, 2021)

Figura 13: logo empresa Ledgermail. (*Ledgermail - Web3 Email*, no date)

4.4.4. Decisión plataforma

La elección de la plataforma ha sido laboriosa, ya que hay diferentes opciones y siendo cada una totalmente distinta a la anterior. En la tabla 5, en la cual se han recogido las alternativas vistas para cada caso de uso y además la Red T de Alastria. Dentro de la tabla se puede destacar que la Red T de la blockchain de Alastria está diseñada con un tipo de registro privado, algo que resulta necesario para nuestro proyecto, debido a que se va a trabajar con el Ministerio de Defensa. También mencionar que se permite la implementación de todos los casos de uso en una misma plataforma. Este motivo y el de la elección de una red de consoricio en vez de una privada, es motivada por los costes que supondría la creación de una red privada desde cero. Estos motivos son los decisivos para la toma de la decisión, siendo la opción ganadora la del consorcio español de Alastria, en concreto su Red T.

Tabla 5: comparación de blockchains. Elaboración propia.

	Sovrin	**VeChain**	**Ledgermail**	**Alastria (Red T)**
Tipo de blockchain	Híbrida	Pública	Pública	Consorcio
Mecanismo de consenso	Zero Knowledge	PoA	XDPoS	IBFT
¿Necesitamos algún token?	No	Si	No	No
Contratos inteligentes	Si	Si	Si	Si
¿Compatible con todos los casos de uso?	No	No	No	Si

La importancia de compatibilizar todos los casos de uso con una misma red, en este caso la Red T de Alastria, viene determinada por el ahorro de costes, debido a que los nodos que se van a instalar servirán para las tres propuestas. Asimismo, la Red T es una red de consorcio, que es similar a una red privada permisionada, lo que se compagina bien con la posible solución que nos ha aportado el diagrama de flujo.

Con esta elección, se sigue los principios en los que se basa las acciones del Ministerio de Defensa, con la fomentación de la industria nacional. Además de seguir la línea de inversión que se propone desde el ministerio, Alastria es sinónimo de cumplimiento de la normativa vigente, como puede ser la protección de datos de carácter personal, que se materializa en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, que en España se nos integra a través de la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales. (Consorcio *et al.*, no date)

4.5. Solución

Para la puesta en marcha de nuestros casos de uso, se necesitará la creación de 1 nodo validador a nivel Ministerio de Defensa. El montaje de este nodo no es imprescible, pero al tratarse del único tipo de nodo que permite la escritura en la cadena de bloques, se recomienda para poder proporcionar una mayor seguridad de la red, debido a que se está ampliando el número de nodos complicando así el ataque del 51%[12]. Este se ubicará en el Centro de Sistemas y Tecnologías de la Información y Comunicaciones (CESTIC). 17 nodos permisionadores, uno por cada comunidad autónoma y ciudades autónomas donde existen bases militares, y 38 nodos regulares, que coincide en número con las provincias en las que se puede encontrar al menos, una unidad del Ejército de Tierra. Estos nodos serán compatibles con los tres casos de uso.

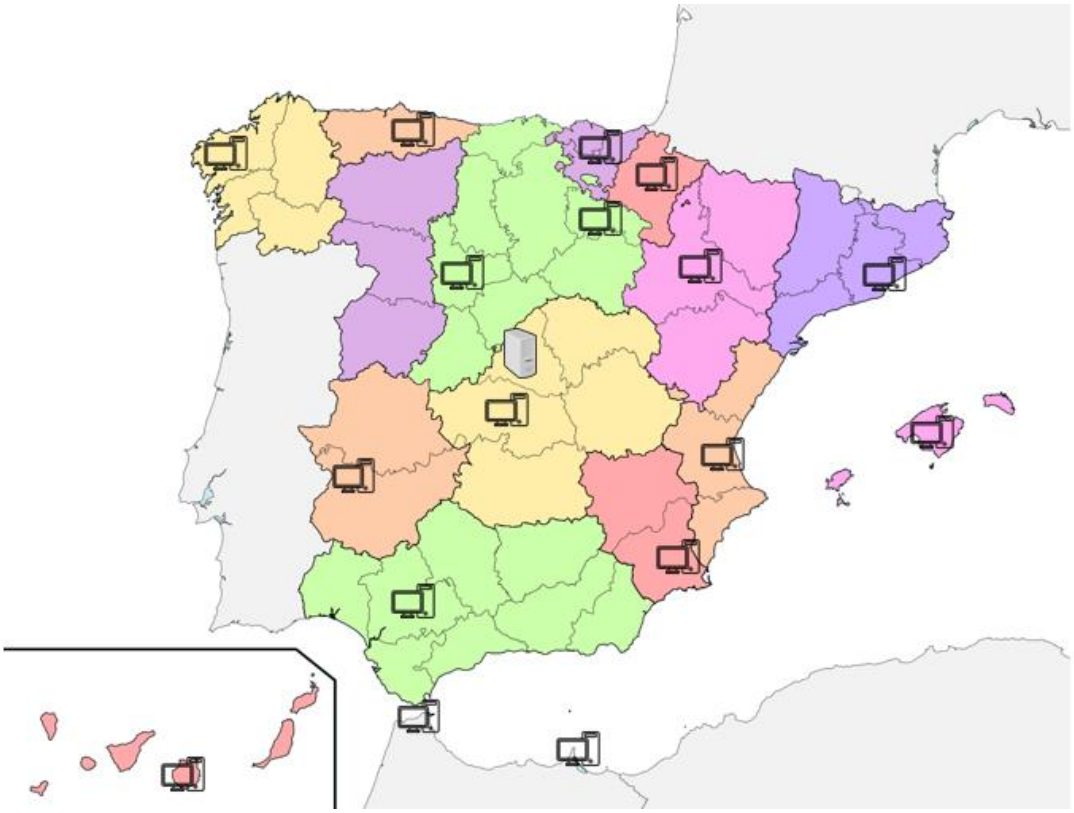


Figura 14: distribución del validador y los permisionadores pertenecientes al Ministerio de Defensa.

[12] El ataque del 51% se produce cuando una persona o grupo controla el 51% del poder computacional de la red.(*Bit2Me Academy*, no date)

Elaboración propia.

4.5.1. Gestión de identidades

Para la implementación de nuestro caso de uso, se puede mejorar los servicios que se desarrollan en la actualidad con la PKI, ya que con esta solo se están firmando documentos. Mientras que, al añadir la tecnología blockchain al ET, se estaría añadiendo de forma innata la firma digital gracias a la criptografía asimétrica, como ya se ha explicado en el apartado 3.8

Además de tener la opción de la firma digital con la blockchain, al implementarla, se está añadiendo posibles trámites que en la actualidad no están resueltos de ninguna forma concreta y en la que cada unidad actúa de forma particular como puede ser la solicitud de información sobre personal de forma automatizada.

Para mejorar este caso de uso, Alastria dispone de una plataforma centrada en la gestión de identidades, en concreto Alastria ID, el cual es un modelo de identidad digital, propuesto por el Consorcio para su uso en servicios digitales, incluso más allá de la propia tecnología blockchain e inspirado en el concepto de Self Sovereign Identity (SSI).(*ID Alastria*, no date) AlastriaID está desplegado en la Red T.

AlastriaID es referente a nivel español en el mundo de la blockchain, y también lo es a nivel europeo, a nivel de identidad digital, siendo la base del actual proyecto de la Unión Europea EBSI-ESSIF (*Inetum*, 2021)

El concepto de SSI, consiste en que la identidad está descentralizada y proporciona a los titulares de la identidad la plena propiedad, control y gestión de ellas. Esto se consigue con la independencia de cualquier autoridad centralizada, lo que se consigue con la implementación de la blockchain.

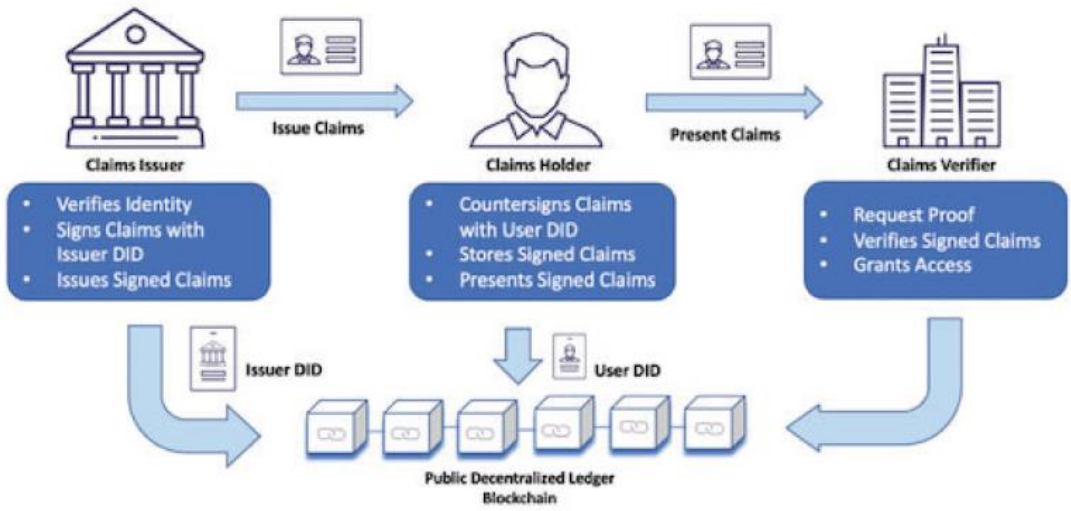


Figura 15: esquema de funcionamiento de SSI (Cuadrado Saez, 2020).

Christopher Allen, en el año 2016 escribió un artículo que estableció los 10 principios para SSI, que se ha convertido en referencia y son:

- Existencia: "*Los usuarios deben tener una existencia independiente*"; quiere decir, que

la identidad digital tiene que establecer a los usuarios la capacidad de existir en un mundo digital

- Control: "*Los usuarios deben controlar sus identidades".* El uso y destino de los datos privados debe quedar en manos de sus titulares, ya que son la autoridad soberana sobre su identidad digital, sin necesidad de un tercero intermediario.
- Acceso: "*Los usuarios deben tener acceso a sus propios datos*", es decir, que le sea posible a los usuarios acceder y recuperar la información personal que se haya aportado.
- Transparencia: "*Los sistemas y algoritmos deben ser transparentes*", esto quiere decir, que la red que se encarga de la gestión de las identidades, digitales tiene que ser abierta y pública.
- Persistencia: "*Las identidades deben ser duraderas*". Este principio defiende que la identidad digital, debería ser duradera salvo por decisión del usuario.
- Portabilidad: "*La información y los servicios sobre identidad deben ser transportables*". Allen, defiende que la información y los servicios deben ser fácilmente transportable, y no estar en manos de forma exclusiva de una tercera entidad centralizada.
- Interoperabilidad: "*Las identidades deberían ser lo más ampliamente utilizadas posible*". El fin de la identidad digital, es que sea posible usarla en todos los ámbitos posibles creando así identidades globales.
- Consentimiento: "*Los usuarios deben aceptar el uso de su identidad*". Este tipo de sistema exige que el intercambio de datos personales se realice únicamente con el consentimiento del usuario.
- Minimización: "*La divulgación de reclamos debe ser minimizada*". Cuando un usuario releva información sobre su identidad, lo hará de la forma que muestre la menor información posible.
- Protección: "*Los derechos de los usuarios deben ser protegidos*". En caso de disputa, los derechos y libertades del usuario prevalecen sobre los requisitos de la plataforma.

Figura 16: 10 principios de SSI (Domilabs, 2021).

En este caso de uso se tiene que incorporar tres actores:

- Sujeto: persona (física o jurídica) que dispone de información certificada por un emisor, y la envía a un proveedor de servicios, por lo que recibe credenciales y crea presentaciones. Es el propietario de la información y se controla desde una billetera.[13]
- Administración: identidad que implementa los contratos inteligentes, y también tiene la función de crear la primera entidad, el resto será creada por los emisores.
- Entidad: empresa u organización que puede ser:
    - Proveedor de servicios: entidad que solicita la información a un sujeto, por lo que crea solicitudes de presentación y recibe presentaciones.
    - Emisor: puede ayudar a cualquier persona a crear una nueva identidad. Además, esta entidad puede emitir información certificada, sobre un tema, creando así credenciales.

Para la implementación de nuestro caso de uso, se puede mejorar los servicios que se desarrollan en la actualidad con la PKI, ya que con esta solo se están firmando documentos. Mientras que, al añadir la tecnología blockchain al ET, se estaría añadiendo de forma innata la firma digital gracias a la criptografía asimétrica, como ya se ha explicado en el apartado 3.8.

Dentro de los sujetos, se tendrá al personal militar y también la de las unidades. Dentro de cada wallet de los individuos, se puede almacenar información como: su nombre, apellidos, documento nacional de identidad (DNI), tarjeta de identificación militar (TIM), fecha de nacimiento, domicilio, ciudad de nacimiento, estudios, datos familiares donde se incluirá nombre, apellidos, DNI y teléfono de sus familiares de primer grado. A su vez, se almacenará el expediente con la fecha de incorporación, antigüedad en la promoción, empleo actual, destinos previos, cursos realizados y nivel de inglés. A su vez, en la identidad de la unidad se almacenará el nombre de la unidad, ciudad donde se encuentra el acuartelamiento, coordenadas del acuartelamiento, ID de la unidad y su estandarte.

La administración estará recogida en la S-1 del CESTIC en Madrid.

Además de los actores definidos anteriormente, se necesitará un identificador descentralizado (DID) y una wallet (Maria del Mar Peguero, 2022). Esto es necesario debido a que es parte principal de los estudios en los que se ha basado esta solución.

Se puede definir DID según W3C (*Self Sovereign Identity*, no date) como un nuevo tipo de identificador: no es más que una cadena alfanumérica que identifica un recurso. Por recurso se entiende cualquier objeto que pueda ser identificado, desde una página web hasta una persona o un planeta.

Por otro lado, una wallet o billetera es un almacén privado que permite al propietario de la misma depositar y administrar las credenciales de identidad. Tiene que cumplir con las siguientes propiedades: (*Bit2me*, *2020*)

- Acceso seguro para el propietario.
- Asegurar que solo accedan a ella las personas autorizadas.

[13] La billetera o wallet, es una aplicación que se instala en nuestro teléfono móvil y que permite almacenar credenciales relacionada con la persona.

- Estar conectado a la blockchain donde se registró el DID.
- Facilitar procedimientos para que los individuos puedan borrar los datos asociados con ellos.
- Facilitar procedimientos para que los individuos cambien el estado de sus credenciales.

La wallet donde se almacenarán las credenciales, estará instalada en los dispositivos móviles del personal militar.

Finalmente, proveedores de servicios serán las secciones S-1[14] de las distintas compañías de forma que puedan solicitar la información. Por ejemplo, la S-1 de la Cía[15] 33 quiere saber cuántos soldados tienen el carnet de conducir tipo C de la Cía. 32, para poder agregarlos a su compañía en las siguientes maniobras. La S-1 solicitará la información a los Soldados y estos, les responderán con una presentación, donde se recoge el nombre y los tipos de carnet que tiene, de forma que no se incluya en la presentación datos que correspondan con la solicitud, como su TIM[16]. De igual forma, los emisores serán las S-1 de las distintas Cias. En la figura 17, se puede ver un diagrama del flujo de datos de las distintas S-1 y el personal.

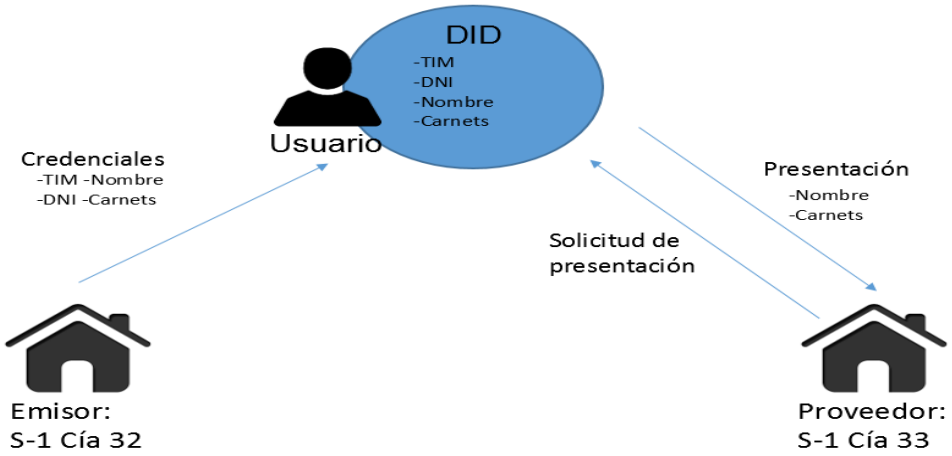


Figura 17: flujo de datos entre los diferentes actores. Elaboración propia

Otro ejemplo real para este caso de uso es la solicitud de una vacante de libre designación para un puesto en la Unidad Militar de Emergencias (UME) en Madrid. El Teniente de la Torre, quiere solicitar la vacante que ha visto en Boletín Oficial de Defensa (BOD), para ello la S-1 de la Cía. que tiene en su plantilla la vacante, le solicitará al usuario una solicitud de presentación de los datos relevantes, para la asignación de la plaza, como su expediente militar y el nivel de

[14] La S-1 son las Secciones encargadas del personal dentro las planas de mando de los acuartelamientos.

[15] Entidad militar que generalmente consta de 70 a 250 soldados.

[16] Esta presentación incluye solo los datos que se han solicitado, evitando así dar información que no aporta valor como podría ser en este caso la fecha de nacimiento o su estado civil.

inglés, para acreditar que cumple con los requerimientos de la plaza y no añadiendo su nombre, para evitar que pueda ser elegido por amiguismos. El Tte, que ya tiene en su wallet las credenciales cargadas, gracias a que el emisor se las ha certificado, crea una presentación en respuesta a la solicitud anterior y la envía a la S-1 de la UME.

Los flujos de información entre los actores quedan registrados en la blockchain, gracias a diferentes Smart Contracts. Por ejemplo, un emisor al emitir una credencial usa un Smart Contract para registrar la emisión, por otro lado, el usuario para crear la presentación con las diferentes credenciales usa otro Smart Contract para crear ese ´´paquete de información´´. El solicitante, utiliza otro contrato inteligente para comprobar que las credenciales estén vigentes, y además registra que ha recibido la presentación.

4.5.2. Cadena de suministro

Para la implementación de la blockchain en la cadena de suministros, se necesita una tecnología que sea capaz de vincular el espacio físico con el espacio de la información, es decir, que se pueda relacionar los objetos que hay en un almacén con una base de datos. Esta técnica se encuentra a partir de la tecnología de las etiquetas de identificación, por radiofrecuencia más conocidas por sus siglas en inglés RFID (Radio Frequency Identification), que las se puede definir como una comunicación inalámbrica, que se puede usar como entradas del sistema para detectar identificar, rastrear y monitorizar múltiples objetos de una manera sencilla. (Tan and Sidhu, 2022)

En la actualidad, empresas como Inditex, El Corte Inglés o Decathlon son ejemplos de uso de esta tecnología. En el caso de la empresa Decathlon, las etiquetas son usadas de forma que cuando el cliente deposite los artículos sobre la cesta de autoservicio, se detectan de manera automática y este se añade al ticket. (Expansión, 2019)

Figura 18: etiqueta RFID (Grupo SIM, 2019)

La tecnología RFID, se enmarca dentro de la identificación automática y captura de datos (AIDC). En comparación con otro tipo de soluciones AIDC, como el reconocimiento óptico de caracteres (OCR) o el sistema que actualmente se usa en el Ejército, el código de barras. En esta solución se propone implementar RFID junta a la tecnología blockchain ya que, gracias a su capacidad de leer fuera de la línea de visión y su bajo coste, es muy adecuado para su uso en la cadena de suministro.

RFID está compuesto principalmente por tres componentes; lector, antena y etiqueta. Unas ondas eléctricas de radiofrecuencia que son lanzadas desde el lector, se usa para activar y alimentar a las etiquetas, la antena convierte la onda eléctrica gracias a una bobina en flujo eléctrico, y finalmente la etiqueta adjunta una respuesta mediante el envío de otra información de ondas eléctricas al lector.

Las etiquetas se pueden clasificar en dos tipos; activas y pasivas. Las etiquetas pasivas no

necesitan una fuente de alimentación externa, ya que se alimenta de la energía de radiofrecuencia que emite el lector. Mientras que las etiquetas activas, si necesitan una fuente de alimentación externa. La tecnología pasiva es de menor coste, pero la activa nos permite que se nos proporcione datos en tiempo real, de forma continua y a una mayor distancia, debido a que es la propia etiqueta la que se activa cada cierto periodo de tiempo establecido, y envía la onda al receptor.

Para el estudio de este caso de uso, se va a poner el ejemplo de un pedido a la empresa El Corte Inglés. Esta compañía suministra al ejército vestuario y calzado de manera personalizada. Esta sociedad fabrica la ropa en fábricas ubicadas en España, por lo que se podría describir una línea temporal desde su creación, hasta que llega a las instalaciones del ejército de la siguiente forma:

- Producción de la ropa
- Transporte de la mercancía
- PCAMI

La tecnología que se va a implementar será las etiquetas RFID, en su configuración de etiqueta activa, ya que de esta forma se nos va a facilitar la información del artículo en tiempo real, y de forma continua durante todo el proceso de la cadena de suministro.

Todos los artículos estarán dotados de una etiqueta RFID activa, ya que parte de nuestra mercancía viene en contenedores, y si se usa etiquetas pasivas, no se tendría suficiente alcance para abordar todos los productos.

La configuración de las etiquetas estará de forma que repliquen su posición. Esta información será recogida por los lectores que disponen de una antena y que pasarán la información a un ordenador que estará fuera de la red de la cadena de bloques, por lo que este ordenador no puede acceder a su contenido ni tampoco subir información a la misma. Es por esto que a lo que respecta al ordenador, este se conectará con el nodo observador más cercano a través de internet, y enviará la información de la mercancía, de forma que se conozca en todo momento la localización y trazabilidad del producto. Se puede ver el flujo de información en la Figura 19.

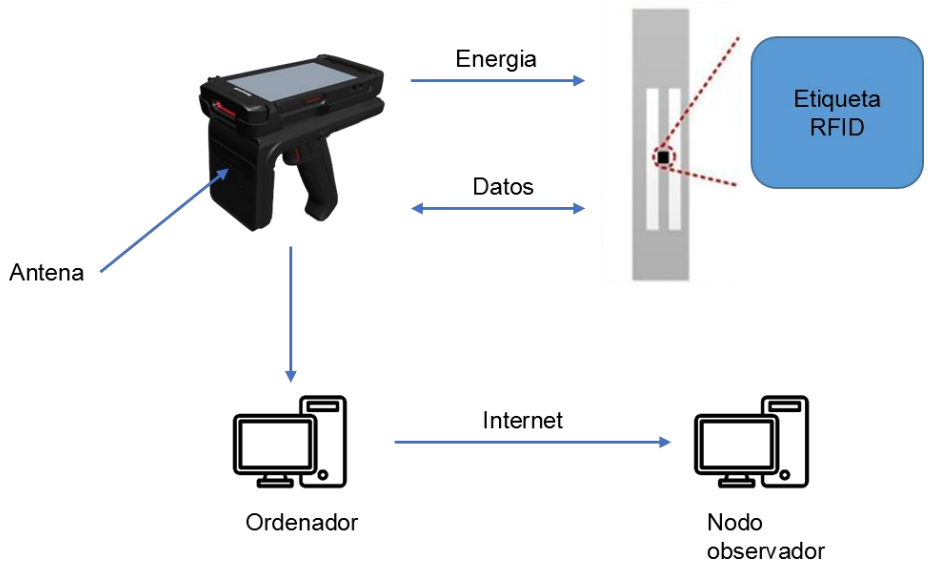


Figura 19: esquema de flujo de datos de la cadena de suministro con la tecnología blockchain. Elaboración propia

Los nodos observadores al recibir la información ejecutarán un Smart Contract de forma que, toda la información que viene desde el ordenador civil se organice dentro de la blockchain, de tal manera que cuando un operador del PCAMI o militar que no sea de este parque, quiera comprobar la trazabilidad del pedido, pueda acceder a la blockchain, buscar las transacciones que están asociadas.

Estos nodos se comunicarán con los nodos validadores los cuales posteriormente serán los responsables de subir la información a la cadena de bloques. Este proceso será realizado a través del mecanismo de consenso IBFT, el cual corresponde con la Red T de Alastria.

4.5.3. Mensajería

En este apartado se va a proponer un modelo de mensajería sobre la tecnología de la cadena de bloques, con la finalidad de mejorar la seguridad y trazabilidad. Para ello, se va a describir las aplicaciones, herramientas y la estructura necesaria para una posible implementación.

Para el usuario diario de SIMENDEF como plataforma para la solución del caso de uso de la mensajería, no habría cambios sobre la interfaz del programa, que pueda conllevar un nuevo proceso de aprendizaje del sistema.

A cada persona que esté habilitada para el uso de SIMENDEF, se le asociará una clave pública y otra privada. Con este juego de claves, el usuario podrá tanto enviar correos electrónicos como recibirlos. La clave pública tiene un formato que dificulta que los usuarios pueden recordarla17, de forma que la clave pública se asociará a la cuenta actual del correo institucional, es decir, si un usuario A enviase un correo a un usuario B, a la dirección de correousuarioB@minisdef.es, lo que estaría realmente haciendo, sería enviar el correo a la clave pública de B. Un símil de esta pareja de contraseñas sería tal que la clave pública es un buzón de correos, al que todo el mundo puede acceder y dejar en él una carta, mientras que la clave privada es la llave que nos da acceso a retirar la mensajería que se ha recibido de los usuarios de la red.

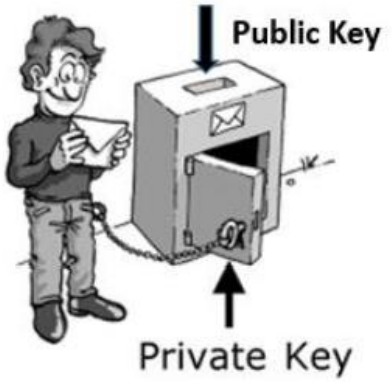


Figura 20: metáfora entre criptografía asimétrica y el buzón de correos. (Graeme L. Cohen, 2013)

El proceso de envío de un correo electrónico de A hasta B seguiría los siguientes pasos:

1. A escribe el correo electrónico que quiere enviar a B. Cuando quiere enviarlo, A usa la

[17] Ejemplo de clave pública GBR2yofwPrZnGHnzX8TqvzzEZRFkBjQ5joNNDtTqSTcy

dirección institucional de B, la cual está asociada a la clave pública de B como destinatario, consiguiendo que este correo llegue al buzón de B.

2. El ordenador de A, se conecta al nodo observador menos saturado de la red.
3. El nodo observador será el encargado de cifrar este mensaje a través del algoritmo SHA-256, que a su vez ejecutará un Smart Contract, sirviendo para que posteriormente el receptor del email pueda acceder a la información que se le ha enviado, de manera focalizada y no tener que examinar toda la cadena de bloques, y finalmente enviar este hash al nodo validador.
4. El nodo validador ejecutará el algoritmo de consenso IBFT, y agregará el bloque con la información (correos electrónicos) a la cadena de bloques. El proceso de agregación de bloques se ejecutará con cierta periodicidad.
5. El usuario B al abrir su sesión en su ordenador personal con su clave privada, se conectará con un nodo observador y se ejecutará el Smart Contract. Este nodo al ejecutar el contrato inteligente hace una búsqueda en la cadena de bloques de todo el historial de correos electrónicos que se han enviado al usuario B.
6. El usuario B accede a su buzón de entrada y puede leer el email que el usuario A le ha enviado

4.6. Análisis comparativo

Para poder comparar los sistemas actuales y las posibles implementaciones con la tecnología blockchain, en concreto con la Red T del consorcio de Alastria, primero se va a exponer las ventajas de los sistemas actuales y sus desventajas. Seguidamente se procederá de igual forma con la blockchain y finalmente para poder confrontar los sistemas, se usará el método cuantitativo de la matriz de Pugh.

Se podría pensar, que a raíz del cambio de sistema actual a la tecnología blockchain se ralentizaría el proceso, pero esto no es así. A raíz del estudio “Performance Evaluation of the Quorum Blockchain Platform“ de los autores Arati Baliga, Subhod I, Pandurang Kamat y Siddhartha Chatterjee, definiendo el rendimiento de las transacciones como el número de transacciones por segundos procesadas con éxito por la red, y siendo procesada con éxito cuando se incluye en un bloque y este se confirma como parte del libro mayor, Quorum es capaz de alcanzar una tasa de 900 transacciones por segundo.

4.6.1. Gestión de la identidad

Como se explicó anteriormente, en el ET la solución para la gestión de la identidad está basada en PKI. Este sistema, no se diferencia en cuanto a su composición o forma de actuación respecto a la infraestructura que puede tener una empresa civil para sus trabajadores.

Respecto a las ventajas de este sistema se destaca: (*Public Key Infrastructure*, 2019)

- Flexibilidad y control: al depender de una figura centralizada que está gestionada por la empresa, esta mantiene el control de las claves públicas y las modificará para que cumplan sus requisitos
- Rentabilidad: el coste inicial de la inversión puede llegar a ser alto dependiendo de la escala de la empresa. Sin embargo, a la larga el algoritmo de PKI hace que las cosas sean más baratas a las organizaciones
- Amplio soporte: el sistema de PKI es una solución comúnmente aceptada en las

empresas. Por esta razón tiene gran cantidad de soporte en los diferentes sistemas operativos como; Windows, Linux o UNIX.

Por otro lado, se puede recalcar las siguientes desventajas:(*Paso a paso*| *ComputerWorld*, 2002)

- Uso de algoritmos antiguos: el uso de algoritmos obsoletos puede ser problemático y que se permitan ataques donde se comprometan los certificados.
- Requiere copia de seguridad en caso de pérdida de datos: sin tener un sistema de respaldo y estar todo almacenado de forma centralizada, los datos pueden perderse de forma permanente.
- Personal dedicado: dada la complejidad del sistema, es necesario el uso de personal dedicado en la creación, administración y gestión de las PKIs. Es necesario el nombramiento de un responsable de seguridad, que estará encargado de establecer y administrar la política de seguridad.
- Procesos tediosos: los procesos para la recopilación de información son inexistentes, haciendo que lo que se podría hacer de forma mucho más rápida con procesos automatizados, lleve al personal militar mucho tiempo de su jornada laboral.

4.6.2. Cadena de suministro

En la actualidad, SIGLE es la solución al caso de uso de la gestión de la cadena de suministro dentro del Ejército.

Del sistema, se puede destacar las siguientes ventajas:

- El mando puede conocer en tiempo real la operatividad de sus medios y los niveles de almacenaje de los que dispone la unidad.
- SIGLE, abarca todos los escalones de mantenimiento haciendo que la comunicación entre estos sea más fluida.

Respecto a las desventajas:

- Es un sistema totalmente centralizado, con lo que conlleva que el servidor central puede caer y se paralice el servicio.
- Los datos son actualizados de forma manual y en ocasiones estos datos no se cargan a la base de datos de forma correcta.

4.6.3. Mensajería

Como se vio en el apartado 4.2.3 de esta memoria, el caso de uso de la mensajería está solucionado en el ET en la plataforma de SIMENDEF.

De este sistema, se puede destacar las siguientes ventajas:

- Ahorro de tiempo: se reduce el tiempo de generación y tratamiento de los diferentes documentos soportados. Mejora los procesos relacionados con la mensajería oficial.
- Ahorro de costes: se produce un ahorro en el gasto de papel, al estar todo el flujo de información generado por medios electrónicos, desde la creación pasando por el envío hasta su recepción, registro y archivado.
- Seguridad: proporciona la transmisión de documentos por vía electrónica y la distribución de la misma hasta llegar a la sección destinataria de la documentación. Esto permite, la

tramitación y validación de documentación oficial con firma electrónica en los documentos, y que durante el transporte se garantice la integridad e identidad del emisor del documento.

Por otro lado, la desventaja que se destaca de SIMENDEF:

- Centralización de los datos: esto conlleva que los servidores son susceptibles de ser bloqueados, y que se paralice el servicio y facilitando que hackers accedan a los servidores y roben nuestros datos.

4.6.4. Blockchain

Ventajas: (*Indra*, 2018)

- Consenso: la cadena de bloques triunfa gracias a los algoritmos de consenso, con el que llegan los nodos a un acuerdo de forma sencilla. Cada uno de estos, tiene una copia del libro mayor. Para agregar una transacción, cada nodo necesitará comprobar su validez. De forma que, si la mayoría de los nodos de la red piensan que es válida, se agregará la transacción al registro.
- Inmutabilidad: esta característica está ligada a que una vez una transacción está agregada a la cadena de bloques no puede ser cambiada o alterada. Si alguien pretende corromper la red, este deberá modificar todos los datos almacenados cada nodo de la red. Por lo que acceder a la red y modificar los libros de registro de todos los nodos es casi imposible.
- Descentralizada: la red no está controlada por ninguna autoridad que gobierne o una sola persona, sino que este control es llevado a cabo por el grupo de nodos. Esta forma es útil porque evita fallos, ya que previene los fallos humanos. Además, es menos propenso a las averías o parada del sistema, ya que, aunque un nodo caiga, se podrá seguir usando la red.
- Seguridad mejorada: la blockchain está basada en la criptografía que añadida a la descentralización de la red impone una capa de seguridad extra a los usuarios. Toda la información de la cadena de bloques se cifra criptográficamente, es decir, la información se encuentra oculta en la red gracias a los hashes.

Desventajas:

- Complejidad: esta tecnología, no es de fácil comprensión para todo el mundo (Restrepo & Ocampo, 2019).
- Almacenamiento: al crecer el número de usuarios, transacciones y bloques, el tamaño de la copia del libro mayor irá ocupando más espacio y los requerimientos técnicos de los nodos deberán ser ampliados. (*Ventajas y Desventajas del Blockchain | Binance Academy*, 2018)
- Claves privadas: debido a la excesiva seguridad, si un usuario perdiese la clave privada, se vuelve casi imposible que pueda volver a acceder a su cuenta. (*Ventajas y desventajas del Blockchain | BBVA Suiza*, 2021)
- Altos costes de implementación: la implementación de esta tecnología requiere un gran desembolso iniciales, lo que está retrasando la adopción masiva por parte de las empresas. (*Blockchain: ¿Cuáles son sus ventajas y desventajas?*, 2018)
- Con el desarrollo de los ordenadores cuánticos. los ataques a la blockchain podrían

incrementar de manera agresiva debido a la gran capacidad de computación que tendrían estos dispositivos pudiendo llegar a descifrar la criptografía asimétrica.

4.6.5. Matriz de Pugh

Para la realización de la matriz de Pugh, los inputs de comparación son los recogidos durante el periodo de entrevistas que se desarrolló durante las prácticas de mando en el RT 21. Estos inputs son: integridad, confidencialidad, trazabilidad, disponibilidad, rapidez, práctico y moderno. La valoración se calcula a partir del sistema de referencia, de forma que negativo quiere decir que la solución empeora a la referencia, normal cuando ambos sistemas son iguales en ese aspecto y positivo si la propuesta mejora a la referencia. (Julián Gómez, 2021)

Se comenzará con el caso de uso de la gestión de identidades. Se ha comparado el sistema de PKI, en la matriz aparece como REF, con la tecnología blockchain. Se puede observar en la figura 21 que la tecnología de la cadena de bloques puntúa de forma positiva en los aspectos de integridad, trazabilidad, disponibilidad, rapidez y modernidad. De la misma forma, se ha obtenido como normal los aspectos de confidencialidad y lo práctico del sistema.

Una vez ponderado los resultados, se puede comprobar que la blockchain resulta ganadora con una mejora de cinco puntos. Es decir, la cadena de bloques mejora el sistema de PKI en función de los conceptos demandados por el personal especializado en los sistemas.

		Peso/ Grado de relevancia	Productos	
			Referencia	Blockchain
Conceptos/Categorías	Integridad	10	REF	1
	Confidencialidad	7	REF	0
	Trazabilidad	6	REF	1
	Disponibilidad	9	REF	1
	Rapidez	8	REF	1
	Práctico	5	REF	0
	Moderno	4	REF	1
	TOTAL			5

Figura 21: matriz de Pugh para la comparación de PKI con la blockchain. Elaboración propia

Seguidamente, se analizará el caso de uso de la cadena de suministro. En esta comparativa, se analizará SIGLE y la blockchain. Por una parte, la blockchain destaca positivamente en integridad, confidencialidad, trazabilidad, disponibilidad, rapidez y modernidad. Mientras que se elige como normal en el aspecto práctico.

Una vez sumados los resultados, se puede comprobar que la blockchain resulta ganadora con una diferencia de seis puntos respecto a SIGLE, es decir, la cadena de bloques es mejor en función de los conceptos demandados por el personal especializado en los sistemas.

		Peso/ Grado de relevancia	Productos	
			Referencia	Blockchain
Conceptos/Categorías	Integridad	10	REF	1
	Confidencialidad	7	REF	1
	Trazabilidad	6	REF	1
	Disponibilidad	9	REF	1
	Rapidez	8	REF	1
	Práctico	5	REF	0
	Moderno	4	REF	1
	TOTAL			6

Figura 22: matriz de Pugh para la comparación de SIGLE con la blockchain. Elaboración propia

Para concluir, se analizará el caso de uso de la mensajería. En esta última matriz, se compara SIMENDEF y la blockchain. De este último, se puede destacar positivamente la integridad, confidencialidad, trazabilidad, disponibilidad y la modernidad. Mientras que se analiza como normal la rapidez y lo práctico del sistema.

		Peso/ Grado de relevancia	Productos	
			Referencia	Blockchain
Conceptos/Categorías	Integridad	10	REF	1
	Confidencialidad	7	REF	1
	Trazabilidad	6	REF	1
	Disponibilidad	9	REF	1
	Rapidez	8	REF	0
	Práctico	5	REF	0
	Moderno	4	REF	1
	TOTAL			5

Figura 23: matriz de Pugh para la comparación de SIMENDEF con la blockchain. Elaboración propia

Una vez ponderado los resultados, se puede comprobar que la blockchain resulta ganadora con una diferencia de cinco puntos. Es decir, la cadena de bloques mejora el sistema de SIMENDEF, en el caso de uso de la mensajería, en función de los conceptos demandados por el personal especializado en los sistemas.

Si se analiza las matrices, se puede observar que hay conceptos como son la integridad, trazabilidad, disponibilidad y modernidad que tienen un resultado positivo común en los tres análisis. Esto es debido a que son características inherentes a la blockchain. Por otro lado, se destaca la rapidez en la comparación de PKI porque se automatizan los procesos que son manuales en la actualidad y en la gestión de las cadenas suministro porque la lectura de RFID es automática, dejando el sistema actual de código de barras. Finalmente, la confidencialidad que se acentúa en los sistemas de gestión de la cadena de suministro y SIMENDEF por la seguridad que añade la blockchain gracias a la criptografía.

4.6.6. Discusión

Una vez se ha realizado un método cuantitativo para comparar los sistemas, se ha

comprobado que la tecnología de la blockchain mejora a los sistemas actuales en los requerimientos demandados por el personal que trabaja a diario con ellos.

La implementación de la blockchain no solo mejora los aspectos demandados por los entrevistados, sino que también añade seguridad al trabajo que se realiza en el ET, siendo esto un aspecto muy importante, debido a que se manejan diariamente información que no debe salir del ámbito de la defensa. Esta tecnología es sinónimo de confidencialidad, integridad, disponibilidad, trazabilidad, autenticación y no repudio, lo que nos ayuda a mejorar nuestra seguridad.

Durante la realización de la matriz de Pugh, no se ha tenido en cuenta el concepto de los costes, debido a que los encuestados no lo demandaron. Pero si se llevase a cabo una posible implementación de la tecnología de bloques, uno de los pilares fundamentales en los que habría que realizar un estudio exhaustivo es en el aspecto económico, ya que al no disponer de los medios ni la infraestructura el ET, habría que hacer un gran desembolso inicial.

5. CONCLUSIONES

Tras la realización del trabajo con el que se buscaba el objetivo principal de analizar las posibilidades de uso de la tecnología de la cadena de bloques en el ET se ha llegado a la conclusión de que es una idea que es factible y que, aunque hoy en día no se cuenta con el material necesario para ello, con los procedimientos que marca el consorcio de Alastria, se puede lograr.

En este estudio se han identificado a través de la herramienta de NGT los tres casos de uso que los expertos decidieron que serían más provechosos dentro del ET, siendo la ganadora la opción de la gestión de identidad por su capacidad para automatizar procesos que se hacen en la actualiad de manera manual. Sin embargo, el campo que más se está desarrollando en el mundo civil en la actualidad es el de la gestión de la cadena de suministro.

En este trabajo solo se han desarrollado tres casos de uso, pero las posibilidades que la blockchain facilita son múltiples y cada día a medida que se está estudiando y sacando más partido a la tecnología nacen nuevas iniciativas que pueden ser trasladas al ámbito de la defensa.

El Ministerio de Defensa está ya trabajando en esta tecnología para su implementación en el nuevo concepto de ejército conocido como Brigada 2035 o Fuerza 35. Si el ministerio decidiese llevar a cabo la implementación de la tecnología blockchain para dar solución a algunos casos de uso, surge la necesidad de contratar o formar personal en la tecnología para que se hagan cargo del mantenimiento de los nodos.

REFERENCIAS BIBLIOGRÁFICAS

¡6 Características clave de la tecnología blockchain que debes conocer! (2019). Available at: https://101blockchains.com/es/caracteristicas-tecnologia-blockchain/ (Accessed: 22 October 2022).

Abubakar Idris, U., Awwalu, J. and kamil, B. (2016) 'User authentication in securing communication using Digital Certificate and public key infrastructure', International Journal of Computer Trends and Technology, 37(1), pp. 22–25. doi: 10.14445/22312803/ijctt-v37p105.

Academia Basica del Aire 'MÓDULO DE GESTIÓN ADMINISTRATIVA Unidad didáctica III: SIMENDEF', Academy, B. (2019)

Ahlgren, M. (2022) Estadísticas, tendencias y hechos de ciberseguridad que importan para 2022. Available at: https://www.websiterating.com/es/research/cybersecurity-statistics-facts/ (Accessed: 19 October 2022).

Alastria (2020) 'Alastria Id Privacy Rational'.

Alastria (no date) Alastria ID estará disponible en la nueva red de producción | Inetum. Available at: https://www.inetum.com/es/prensa/alastria-id-estara-disponible-en-la-nueva-red-de-produccion (Accessed: 19 October 2022).

Alastria Consort. - ID (no date) ID Alastria - Alastria. Available at: https://alastria.io/id-alastria/ (Accessed: 19 October 2022).

Alastria, R. T. (2020) 'Políticas de Gobierno y Operación de', pp. 1–30.

Amores, A. (2020) 'Blockchain, algoritmos de consenso', p. 46. Available at: http://hdl.handle.net/10609/127926.

Antonopoulos, A. M. (2010) 'Mastering Bitcoin', Journal of World Trade, 50(4), pp. 675–704. Available at: https://www.bitcoinbook.info/.

Armero, F. (2006) 'La Oficina Sin Papel Y El CorreoElectrónico Oficial En ElMinisterio De Defensa'.

Baliga, A. et al. (2018) 'Performance Evaluation of the Quorum Blockchain Platform'. Available at: http://arxiv.org/abs/1809.03421.

Barnas, N. B. (2016) 'Blockchains in National Defense: Trustworthy Systems in a Trustless World', Blue Horizons Fellowship Air University, (June), pp. 34–40.

BBVA (2019) ¿Qué es la tecnología Blockchain?

IBM Blockchain | IBM, 1 de agosto. Available at: https://www.ibm.com/es-es/topics/what-is-blockchain (Accessed: 22 October 2022).

Binance Academy (2017) ¿Qué es un Algoritmo de Consenso Blockchain? | Binance Academy. Available at: https://academy.binance.com/es/articles/what-is-a-blockchain-consensus-algorithm (Accessed: 22 October 2022).

Binance Academy (2019) Ventajas y Desventajas del Blockchain, Binance Academy. Available at: https://academy.binance.com/es/articles/positives-and-negatives-of-blockchain (Accessed: 24 October 2022).

Bit2me (2020) Qué es una wallet o monedero de criptomonedas, bit2me Academy. Available at: https://academy.bit2me.com/wallet-monederos-criptomonedas/ (Accessed: 22 November 2022).

Bit2me (no date a) '¿Cómo funciona la Cadena de Bloques (Blockchain)?| Bit2Me Academy'. Available at: https://academy.bit2me.com/como-funciona-blockchain-cadena-de-bloques/ (Accessed: 22 October 2022).

Bit2me (no date b) ¿Qué es el ataque del 51% en Bitcoin? - Bit2Me Academy. Available at: https://academy.bit2me.com/ataque-51-bitcoin/ (Accessed: 24 November 2022).

Bit2me Academy (2020) Qué es SHA-256, Bit2me Academy. Available at: https://academy.bit2me.com/sha256-algoritmo-bitcoin/ (Accessed: 22 October 2022).

Bit2me Academy (2022) ¿Qué es la criptografía? Available at: https://academy.bit2me.com/que-es-criptografia/ (Accessed: 25 October 2022).

Bit2Me Academy (no date) ¿Qué es el doble gasto? Available at: https://academy.bit2me.com/que-es-doble-gasto/ (Accessed: 24 October 2022).

BITCOIN (2018) 'Bitcoin - Dinero P2P de código abierto', BITCOIN. Available at: https://bitcoin.org/es/ (Accessed: 24 October 2022).

Blockchain (II): Conceptos básicos desde la protección de datos | AEPD (no date). Available at: https://www.aepd.es/es/prensa-y-comunicacion/blog/blockchain-II-conceptos-basicos-proteccion-de-datos (Accessed: 22 November 2022).

Bloques y transacciones - Blockchain Federal Argentina (no date). Available at: https://bfa.ar/blockchain/bloques-y-transacciones (Accessed: 22 October 2022).

BOHORQUEZ, A. L., GUZMAN, N. E. C. and NARANJO, J. A. V. (2013) IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA - PKI.

Cámara Valencia (2019) '¿Cuándo nació internet? Historia y evolución', 2 De Agosto De 2019. Available at: https://www.mastermarketing-valencia.com/marketing-digital/blog/internet-historia-evolucion/ (Accessed: 22 October 2022).

Capocasale, V. et al. (2021) 'A blockchain, 5G and IoT-based transaction management system for smart logistics: An hyperledger framework', Proceedings - 2021 IEEE 45th Annual Computers, Software, and Applications Conference, COMPSAC 2021, pp. 1285–1290. doi: 10.1109/COMPSAC51774.2021.00179.

Castro Martínez and Francisco Javier (2015) 'Gestor de Certificados Digitales con PKI'.

Choudhary, G. and Shandilya, S. K. (2022) 'Tecnologías en Fabricación y Gestion de logistica'.

ConsenSys (2021) ConsenSys Quorum | ConsenSys, Online. Available at: https://consensys.net/quorum/ (Accessed: 25 October 2022).

Consorcio, E. et al. (no date) 'Condiciones de uso de la red alastria para nodos regulares 1.'

Consorcio, L. D. E. and Alastria, R. E. D. (2020) 'Comité legal de consorcio red alastria *', 2020.

Coronel, T. (no date) Héctor Reyes Campaña.

D. De la Vega Sánchez, I. (2020) 'Interoperabilidad Entre Nodos Geth Y Besu En Redes Ethereum Permisionadas. Aplicación En La Red T De Alastria'.

Dolader, C., Bel, J. and Muñoz, J. (2017) 'La blockchain : fundamentos, aplicaciones y relación con otras tecnologías disruptivas.', Economía industrial, (405), pp. 33–40.

Donohue, B. (2014) ¿Qué Es Un Hash Y Cómo Funciona? | Blog oficial de Kaspersky, kaspersky daily. Available at: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/ (Accessed: 22 October 2022).

Echabarría, M. (2017) 'Revista de Estudios Europeos CONTRATOS ELECTRONICOS AUTOEJECUTABLES (SMART CONTRACT) Y PAGOS CON TECNOLOGÍA BLOCKCHAIN 1', Revista de Estudios Europeos, 70(Julio-Diciembre), pp. 69–95.

Ecosystem, A. B. (2019) '¿ Qué es Alastria ?', pp. 1–20.

Ecosystem, A. B. (2020) 'Beneficios de ser socios de Alastria', pp. 1–15.

Ecosystem, A. B. (2021) 'Asociación de Tecnologías Descentralizadas / Blockchain', pp. 1–14.

Editorial Office CVJ.CH (2020) VeChain and BMW are developing a car security platform. Available at: https://cvj.ch/en/focus/blockchain/vechain-and-bmw-are-developing-a-car-security-platform/ (Accessed: 25 October 2022).

Emmadi, N. et al. (2019) Practical deployability of permissioned blockchains, Lecture Notes in Business Information Processing. Springer International Publishing. doi: 10.1007/978-3-030-04849-5_21.

Emprendices (2016) Blockchain: ¿Cuáles son sus ventajas y desventajas? Available at: https://www.emprendices.co/blockchain-cuales-ventajas-desventajas/ (Accessed: 24 October 2022).

España IG (2022) '¿Qué es Ethereum y Cómo Funciona?', IG España, (¿Que es el Ethereum y como funciona?), pp. 1–8. Available at: https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona (Accessed: 22 October 2022).

Expansión (2019) RFID: así es la tecnología que usan Inditex, El Corte Inglés o Mango, Expansión. Available at: https://www.expansion.com/economia-digital/innovacion/2019/10/16/5da0a62ee5fdea9b6d8b46d7.html (Accessed: 25 October 2022).

Francisco Jesús Millán Granado (no date) 'Red Segura para la Defensa basada en Tecnología Blockchain'.

Garcia Joga, I. and Arahuetes, A. (2019) 'El papel transformador del Blockchain en los servicios financieros'.

García Moreno, C. (2018) Descentralización, inmutabilidad y seguridad de los datos, las claves de Blockchain, Indra, Blog Neo. Available at: https://www.indracompany.com/es/blogneo/descentralizacion-inmutabilidad-seguridad-datos-claves-blockchain (Accessed: 24 October 2022).

Garcia, J. (2019) 'Blockchain y su aplicación práctica al marketing digital Blockchain', p. 37. Available at: http://zaguan.unizar.es/TAZ/EUCS/2014/14180/TAZ-TFG-2014-408.pdf.

González, J. C. et al. (2020) 'Replacing email protocols with blockchain-based smart contracts', Cluster Computing, 23(3), pp. 1795–1801. doi: 10.1007/s10586-020-03128-9.

Graeme L. Cohen (no date) Criptografía de clave pública, 2013. Available at: http://blog.kleinproject.org/?p=1618&lang=es (Accessed: 24 October 2022).

Granado Paredes, G. (2006) 'Introducción a La Criptografía', Revista Digital Universitaria, 7, pp. 2–17. Available at: http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf.

GSBN | Here to simplify trade for all (no date). Available at: https://www.gsbn.trade/ (Accessed: 21 November 2022).

Guillermo Araujo (2019) Cómo poner en marcha un nodo validador en la red Telsius de Alastria | by Guillermo Araujo Riestra | Babel — go2chain | Medium. Available at: https://medium.com/babel-go2chain/cómo-poner-en-marcha-un-nodo-validador-en-la-red-telsius-de-alastria-676bdccc253a (Accessed: 24 October 2022).

Hellani, H., Sliman, L. and Samhat, A. E. (2021) 'logística'.

Historia de la tecnología: El Kenbak-1, el primer ordenador personal (no date). Available at: https://hipertextual.com/2011/08/el-kenbak-1-primer-ordenador-personal (Accessed: 22 October 2022).

Hyperledger (2019) 'Hyperledger – Open Source Blockchain Technologies', Hyperledger. Available at: https://www.hyperledger.org/ (Accessed: 24 October 2022).

IBM (2021a) IBM Food Trust, IBM. Available at: https://www.ibm.com/es-es/blockchain/solutions/food-trust (Accessed: 21 November 2022).

IBM (2021b) Infraestructura de claves públicas (PKI) - Documentación de IBM. Available at: https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009900--htm (Accessed: 19 October 2022).

Identidad digital | t-Formas (no date). Available at: https://ci2.ual.es/comunicar-la-informacion/identidad-digital/ (Accessed: 19 October 2022).

IDENTIDAD DIGITAL SOBERANA Y TECNOLOGÍA BLOCKCHAIN . Modelo de negocio y plan de marketing de la start- up " LinKple " .' (2020).

Ingenier, C. S. D. E. and Ingenier, G. E. N. (2018) 'Implementación y despliegue de una solución de gamificación en la empresa sobre redes públicas y privadas blockchain'.

Inicio | ethereum.org (no date). Available at: https://ethereum.org/es/ (Accessed: 24 October

2022).

Introducción a los Decentralised Identifiers (DID) | Self Sovereign Identity (no date). Available at: https://www.selfsovereignidentity.it/introduccion-a-los-decentralised-identifiers-did/ (Accessed: 19 October 2022).

Jiménez, J. (2022) ¿Qué son las criptomonedas y cómo funcionan?, Santander. Available at: https://www.santander.com/es/stories/guia-para-saber-que-son-las-criptomonedas (Accessed: 24 November 2022).

Jiménez, J. I. and Puig, Á. (2017) 'La primera" blockchain" española y su impacto en la eficiencia de las empresas', Economistas, 2017(155), pp. 45–53.

Julián Gómez (2021) Matriz de Pugh: Cómo tomar una decisión de forma objetiva. Available at: https://www.laboratorioti.com/2021/09/27/matriz-de-pugh-como-tomar-una-decision-de-forma-objetiva/ (Accessed: 26 October 2022).

Khacef, K. and Pujolle, G. (2019) 'Secure Peer-to-Peer Communication Based on Blockchain', Advances in Intelligent Systems and Computing, 927(July), pp. 662–672. doi: 10.1007/978-3-030-15035-8_64.

La Historia de Blockchain, Binance Academy. Available at: https://academy.binance.com/es/articles/history-of-blockchain (Accessed: 22 October 2022).

La historia de la identidad auto soberana (2022). Available at: https://es.validatedid.com/post-es/la-historia-de-la-identidad-auto-soberana (Accessed: 25 October 2022).

Lilly, B. and Lilly, S. (2021) 'Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia', RUSI Journal, 166(3), pp. 46–56. doi: 10.1080/03071847.2021.1886871.

Liu, Y. et al. (2020) 'Blockchain-based identity management systems: A review', Journal of Network and Computer Applications, 166. doi: 10.1016/j.jnca.2020.102731.

Los datos de Facebook de 500 millones de personas se acaban de filtrar (no date). Available at: https://es.cointelegraph.com/news/half-a-billion-people-just-had-their-facebook-data-leaked (Accessed: 19 October 2022).

Maldonado, J. (2020) ¿Qué es la criptografía asimétrica? Available at: https://academy.bit2me.com/que-es-criptografia-asimetrica/ (Accessed: 24 October 2022).

MALE (no date) 'Cuartel general del ejército mando de apoyo logístico del ejército sección de sistemas de información.', p. 39.

Maria del Mar Peguero (2022) What is an SSI digital wallet? Available at: https://knowledge.wealize.digital/en/blog/ssi-digital-wallet (Accessed: 24 November 2022).

Massart, P. (2017) 'European Defence Matters', Eda.Europa.Eu. Available at: https://eda.europa.eu/docs/default-source/eda-magazine/edm-issue-14_web.pdf.

Miers, C. et al. (2019) 'Análise de mecanismos para consenso distribuído aplicados a Blockchain',

Minicursos do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, pp. 91–139. doi: 10.5753/sbc.8589.4.3.

Mondragon, E. (2021) Ventajas y desventajas del Blockchain | BBVA Suiza. Available at: https://www.bbva.ch/noticia/ventajas-y-desventajas-del-blockchain/ (Accessed: 24 October 2022).

Montero, R. (no date) 'Correo IMAP', pp. 9–20. Available at: www.imap.org.

Montul Cereceda, L. (2019) 'Trabajo Fin de Grado', Zaguan.Unizar.Es, pp. 0–43. Available at: http://zaguan.unizar.es/TAZ/EUCS/2014/14180/TAZ-TFG-2014-408.pdf.

Morgera, D. (2021) 'Implementación de Alastria ID en Hyperledger Fabric', p. 51.

Mühle, A. et al. (2018) 'A survey on essential components of a self-sovereign identity', Computer Science Review, 30, pp. 80–86. doi: 10.1016/j.cosrev.2018.10.002.

Mvp, P. (2020) 'Alastria ID'.

Núñez, M. A. (2016) 'Graduado en Ingeniería Informática'. Available at: http://oa.upm.es/43538/1/TFG_MARCO_ARJONA_NUNEZ.pdf.

ORACLE (no date) Enterprise blockchain for dummies.

Padilla, C. dominguez (2016) 'La Revolución Blockchain Y Los Smart Contracts En El Marco Europeo the', 16, pp. 1088–1109.

Palomo, R. (2018) '«Blockchain»: la descentralización del poder y su aplicación en la defensa', Instituto Español de Estudios Estratégicos , pp. 1–20. Available at: file:///C:/Users/viejo/OneDrive/Escritorio/Art. Drone/Dialnet-Blockchain-6555546.pdf.

Para, P. and Reconocimiento, E. L. (2010) 'En Materia De', pp. 1–19.

Paso a paso | | ComputerWorld (2002). Available at: https://www.computerworld.es/archive/paso-a-paso (Accessed: 23 October 2022).

PKI - The Pros and Cons - Cogito Group PKI | Public Key Infrastructure (2019). Available at: https://cogitogroup-net.translate.goog/blog/2019/11/29/pki-the-pros-and-cons/?_x_tr_sl=auto&_x_tr_tl=es&_x_tr_hl=es (Accessed: 23 October 2022).

Rahayu, S. B. et al. (2021) 'Military Supply Chain Management and Blockchain Development', 7th International Conference on Software Engineering and Applications (SOFEA 2021), October 23~24, 2021, Sydney, Australia, 11(December), pp. 93–105. doi: 10.5121/csit.2021.111608.

Retamal, C. D. and Roig, J. B. E. L. (2017) 'APLICACIONES Y RELACIÓN CON'.

Rita Aguado (2021) LedgerMail: ¡La primera solución de correo electrónico segura descentralizada del mundo a bordo de 500.000 usuarios! - CriptoPasion. Available at: https://criptopasion.com/ledgermail-la-primera-solucion-de-correo-electronico-segura-descentralizada-del-mundo-a-bordo-de-500-000-usuarios/ (Accessed: 25 October 2022).

Roberto Solé (2021) VeChain (VET): Qué es y para qué sirve esta criptomoneda. Available at: https://www.profesionalreview.com/2021/07/24/que-es-vechain/ (Accessed: 25 October 2022).

Rodriguez, N. (2019) Uso de Blockchain: lista de 20+ casos de uso de la tecnología Blockchain. Available at: https://101blockchains.com/es/uso-de-blockchain/ (Accessed: 22 October 2022).

Sánchez, D. O. (2019) 'Deployment of Blockchain technology in Serverless infrastructure'.

Sanchez, S. (2017) 'Blockchain technology in Defence', European Defence Agency, p. 17. Available at: https://eda.europa.eu/webzine/issue14/cover-story/blockchain-technology-in-defence (Accessed: 22 October 2022).

Sección Historia: Repasamos el inicio de las criptos - Bit2Me Academy (no date). Available at: https://academy.bit2me.com/historia/ (Accessed: 22 October 2022).

Sharif, A. et al. (2021) 'Making assembly line in supply chain robust and secure using UHF RFID', Scientific Reports, 11(1), pp. 1–18. doi: 10.1038/s41598-021-97598-5.

Sheva, B. (2016) 'Blockchain para la gestión de identidades'.

Sirikupt, C., Wauters, G. and Kaloudiotis, T. (2020) 'AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN The Future of Biosensors in European Defence', (September).

Source, O. (no date) 'Condiciones de operación de la red t alastria por parte de nodos críticos 1.'

Tan, W. C. and Sidhu, M. S. (2022) 'Review of RFID and IoT integration in supply chain management', Operations Research Perspectives, 9. doi: 10.1016/j.orp.2022.100229.

Técnica de grupo nominal – Estudia en línea (no date). Available at: https://laedu.digital/2020/12/26/tecnica-de-grupo-nominal/ (Accessed: 19 October 2022).

Telefónica y Alastria firman un convenio para impulsar una red blockchain basada en Hyperledger Fabric (no date). Available at: https://www.europapress.es/economia/noticia-telefonica-alastria-firman-convenio-impulsar-red-blockchain-basada-hyperledger-fabric-20210205111841.html (Accessed: 24 October 2022).

The Value Technology Foundation (2020) 'Potential-Uses-of-Blockchain-Technology-In-DoD', Potential Uses of Blockchain By The U.S. Departement of Defense, Washington(March), pp. 1–39.

thoth38 (2016) '¿Qué es J2EE?'

Universidad Politécnica de Madrid Trabajo Fin de Grado Desarrollo de una Aplicación Web del Modelo de Identidad Soberana Alastria Autor : Antonio Ruiz García' (2022).

VeChain | Cointelegraph (no date) 2022. Available at: https://es.cointelegraph.com/tags/vechain (Accessed: 25 October 2022).

Vega, S. B. (2018) 'electricidad basado en Blockchain para comunidades de vecinos'. Available at: https://dspace.uib.es/xmlui/bitstream/handle/11201/151207/Memoria_EPSU1225.pdf?sequence

=1&isAllowed=y.

What is VeChain & How Does It Work? | Exchanges | ZenLedger (no date). Available at: https://www.zenledger.io/exchanges/vechain-vet (Accessed: 24 November 2022).

Yang, Z. P. et al. (2021) 'An accelerating approach for blockchain information transmission based on ndn', Future Internet, 13(2), pp. 1–14. doi: 10.3390/fi13020047.

ZAMORANO, F. J. T. (2020) 'DESARROLLO DE UNA APLICACIÓN BASADA EN LA TECNOLOGÍA BLOCKCHAIN PARA EL APOYO LOGÍSTICO A LAS MISIONES DE LA UNIDAD MILITAR DE EMERGENCIAS', pp. 1–9.

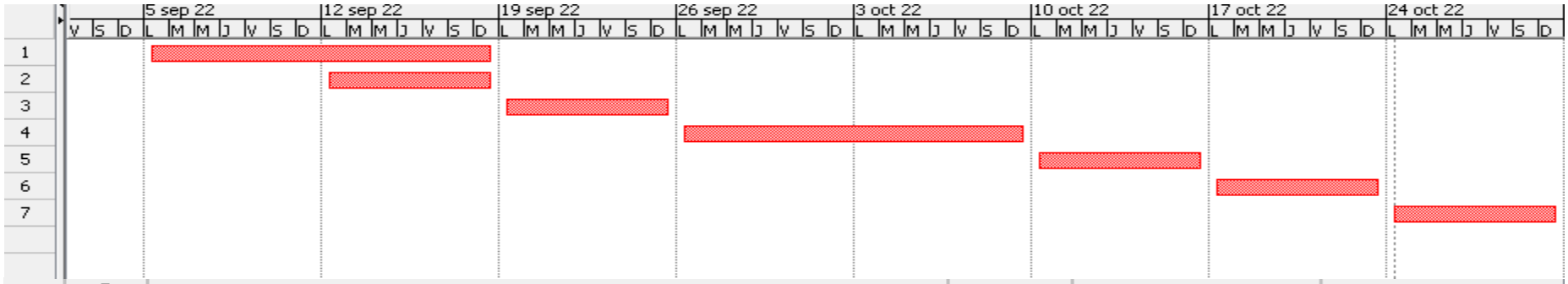
Zhu, Y. et al. (2020) 'A study of blockchain technology development and military application prospects', Journal of Physics: Conference Series, 1507(5). doi: 10.1088/1742-6596/1507/5/052018.

Anexo I EDT

Proyecto: Perspectiva de uso de la tecnología del libro mayor distribuido (DLT) en las transmisiones del Project manager: Juan Manuel Pérez Campanario		Equipo de proyecto		Fecha:	06/11/2022 15:36	
ID	**Nombre tarea**	**Descripción**	**Responsable**	**Fecha inicio**	**Fecha fin**	**Status**
1	**Lanzamiento del proyecto**		Campanario	05/09/2022	30/10/2022	Cerrada
1.1	Project Kick-off meeting	Reunión de definición y autorización del proyecto	Campanario	05/09/2022	06/09/2022	
1.2	Generación de la agenda	Definición de hitos y fechas de relevancia	Campanario	05/09/2022	06/09/2022	
2	**Identificación de posibles casos de uso**		Campanario	06/09/2022	18/09/2022	Cerrada
2.1	Investigación	Investigación sobre la tecnología de blockchain	Campanario	12/09/2022	18/09/2022	
2.1.1	Recopilación de información	Recopilación sobre la tecnología de blockchain	Campanario	12/09/2022	18/09/2022	
2.1.1.1	Revisión bibliográfica	Sobre la tecnología blockchain	Campanario	12/09/2022	18/09/2022	
2.1.1.2	Entrevistas	Al personal destinado en el III BON del RT 21	Campanario	12/09/2022	18/09/2022	
3	**Selección de los casos de uso en los que la blockchain pueda suponer una mejora**		Campanario	19/09/2022	25/09/2022	Cerrada
3.1	NGT	Reunión para seleccionar los casos de uso	Campanario	19/09/2022	25/09/2022	
3.2	Validación de los casos de uso	Comprobar los casos de uso con el diagrama de bloques	Campanario	19/09/2022	25/09/2022	
4	**Proposición de posible implementación de la cadena de bloques en el Ejército**		Campanario	26/09/2022	30/10/2022	Cerrada
4.1	Desarrollo de caso de uso de la gestión de identidades		Campanario	10/10/2022	16/10/2022	
4.1.1	Investigación sistema actual	Investigación de PKI	Campanario	26/09/2022	09/10/2022	
4.1.2	Investigación posible implementación blockchain	Investigación de Alastria ID	Campanario	26/09/2022	09/10/2022	
4.2	Desarrollo de caso de gestión de la cadena de suministro		Campanario	17/10/2022	23/10/2022	
4.2.1	Investigación sistema actual	Investigación de SIGLE	Campanario	26/09/2022	09/10/2022	
4.2.2	Investigación posible implementación blockchain	Investigación de Alastria	Campanario	26/09/2022	09/10/2022	
4.3	Desarrollo de caso de uso de gestión de la mensajería		Campanario	24/10/2022	30/10/2022	
4.3.1	Investigación sistema actual	Investigación de SIMENDEF	Campanario	26/09/2022	09/10/2022	
4.3.2	Investigación posible implementación blockchain	Investigación de Alastria	Campanario	26/09/2022	09/10/2022	

Figura 24: EDT. Elaboración propia

Anexo II Diagrama de Gantt



	Nombre	Duracion	Inicio	Terminado
1	Identificación de posibles casos de uso	13 days	6/09/22 8:00	18/09/22 17:00
2	Recopilación de información y planificación de tareas	7 days	12/09/22 8:00	18/09/22 17:00
3	Realización de NGT y recopilación de información	7 days	19/09/22 8:00	25/09/22 17:00
4	Análisis de la situación actual de los casos de uso seleccionados e investigación de implementación	14 days	26/09/22 8:00	9/10/22 17:00
5	Desarrollo caso de uso 1	7 days	10/10/22 8:00	16/10/22 17:00
6	Desarrollo caso de uso 2	7 days	17/10/22 8:00	23/10/22 17:00
7	Desarrollo caso de uso 3	7 days	24/10/22 8:00	30/10/22 17:00

Figura 25: Diagrama de Gantt

Anexo III Ejemplo de hashes con SHA256

La función criptográfica SHA256 que viene de su nombre en inglés Secure Hash Algorithm fue desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y el National Institute of Standards and Technology (NIST).(¿Qué es SHA-256?, 2022)

La entrada del algoritmo no es vinculante a la longitud del hash resultante, que siempre será una cadena de 64 letras y números (codificación de 256 bits). No hay dos hashes iguales, si la entrada cambia en una letra o número, ya el hash será totalmente distinto.

La primera entrada será Regimiento de Transmisiones 21 con una solución de ae4694ec1951090ecd20e0eac6cf4a53df7f5eb52738f90abc9ea85d88ec2590

Figura 26: ejemplo 1 de obtención del hash a través de SHA256

Por otro lado, si se añade a los datos Nº, se verá que cambia y es totalmente distinto. Con la entrada de Regimiento de Transmisiones N.º 21 la salida es e1497f6d3b0d4ffc69a8ff0a41025f4d1b80426b442335aa1ec322509fdf38e6

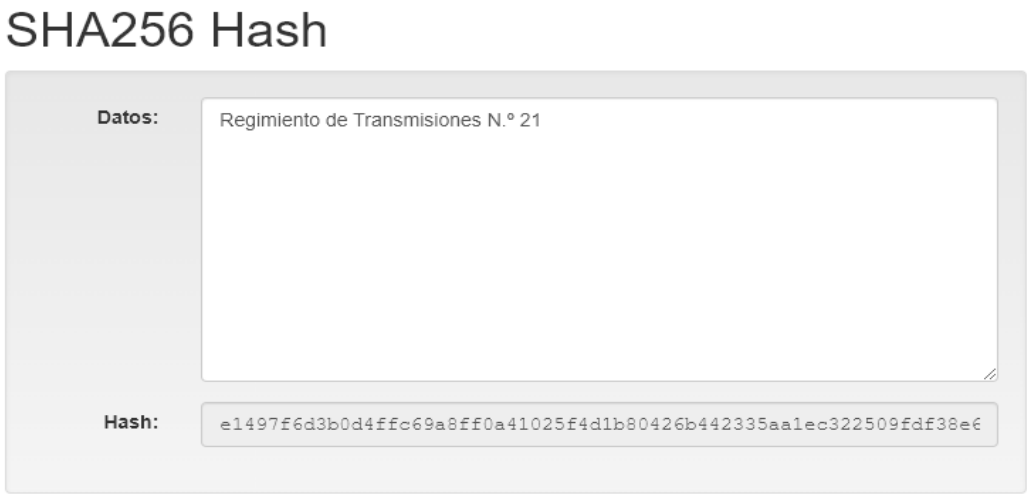


Figura 27: ejemplo 2 de obtención del hash a través de SHA256

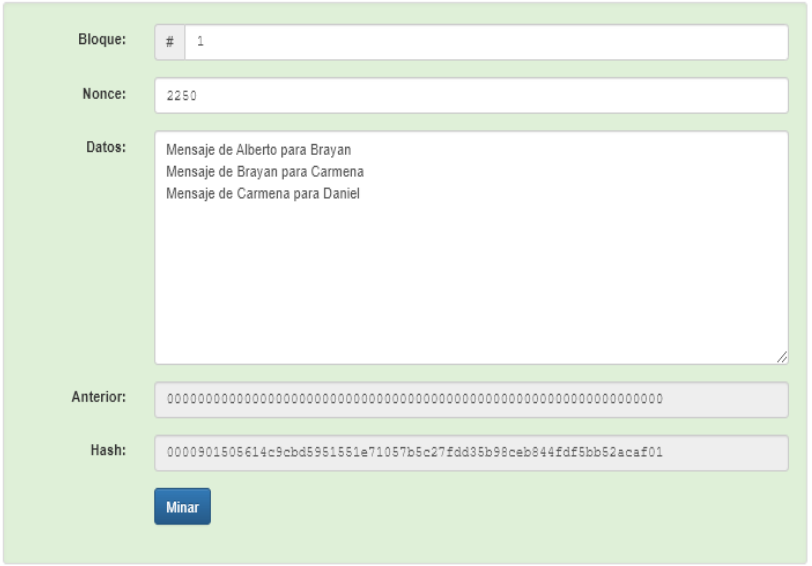
Estas pruebas, se han llevado a cabo en la web https://andersbrownworth.com/blockchain/hash , en la que se integra una calculadora de hashes.

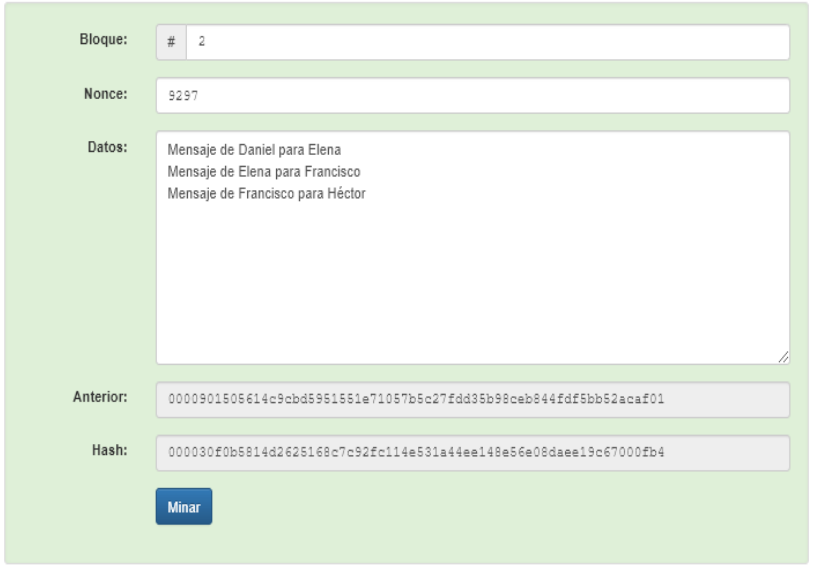
Anexo IV Funcionamiento de blockchain

Para esta práctica, se va a partir de una cadena de bloques en la que se recoge unos mensajes entre personal del ET.

Estas pruebas, se han llevado a cabo en la web https://andersbrownworth.com/blockchain/hash , en la que se integra una demo de blockchain

Se puede observar que la blockchain está compuesta por cuatro bloques relacionados entre sí con el hash del bloque anterior.





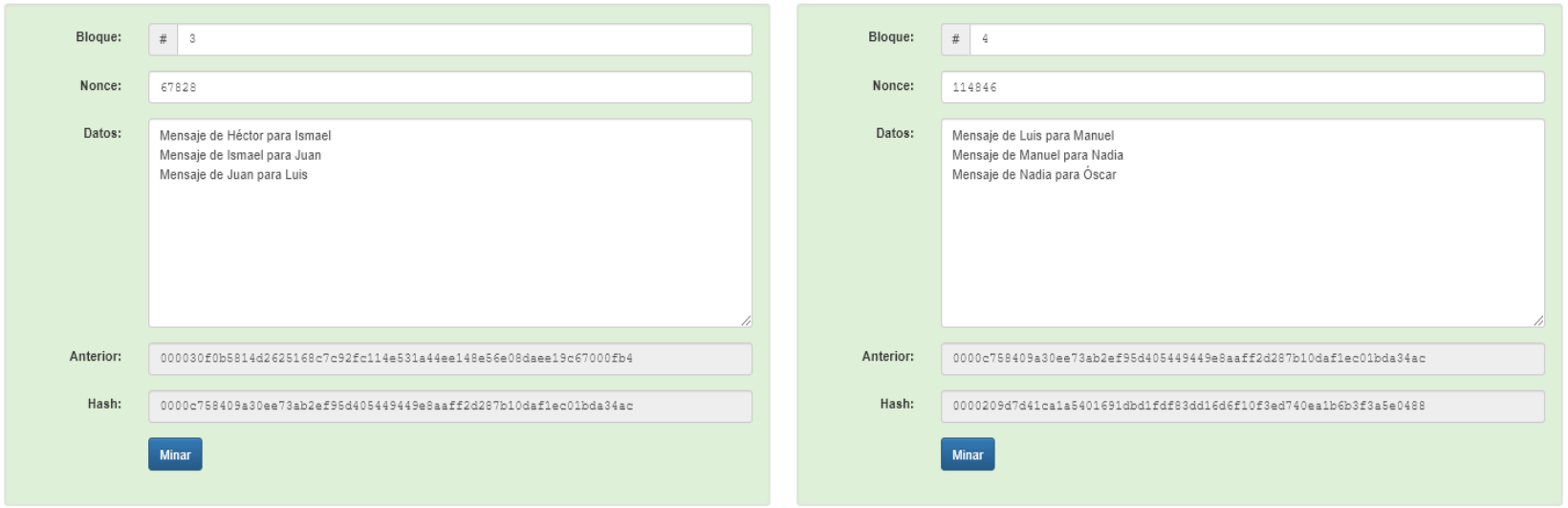


Figura 28: ejemplo de una cadena de bloques. Elaboración propia.

Este sería un ejemplo donde la blockchain está funcionando bien. A continuación, se va a suponer que un hacker consigue entrar en la red y modificar el bloque número dos y que el mensaje que envió Daniel para Elena le llegue a Pedro. Una vez el atacante modifica el nombre de Elena por Pedro en el bloque, el hash es totalmente distinto al anterior debido al algoritmo SHA256. Por esta razón, los bloques siguientes, se dan cuenta de que algo no está bien en la cadena al no corresponder el actual hash del bloque dos con el que el bloque tres conocía.

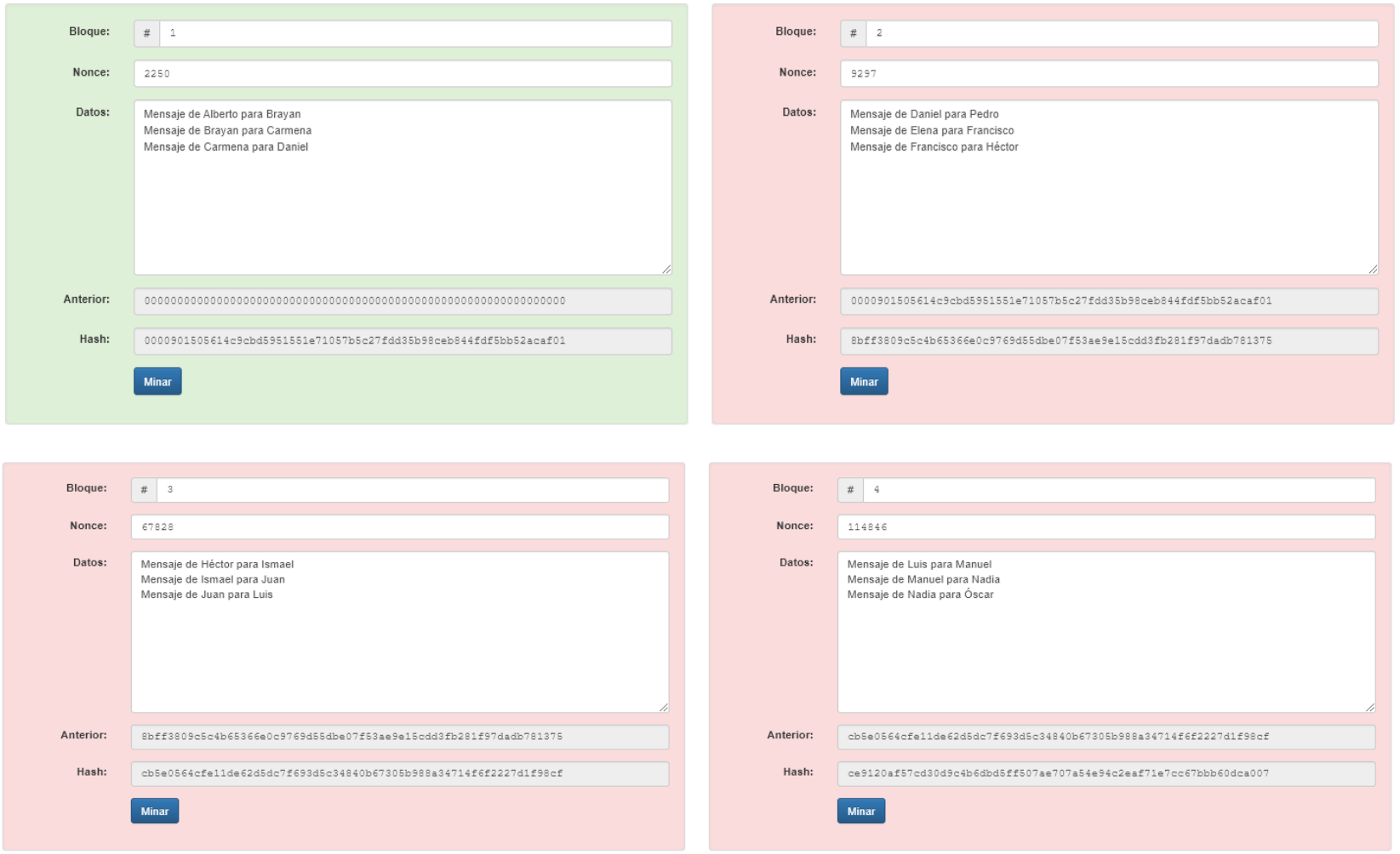
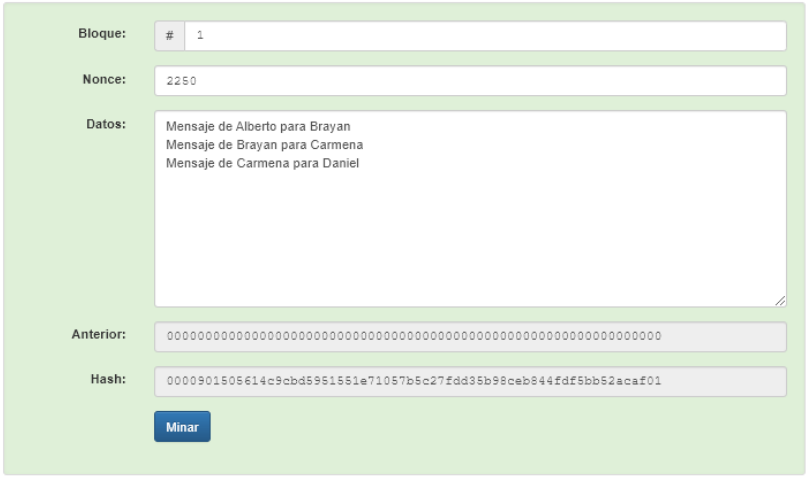
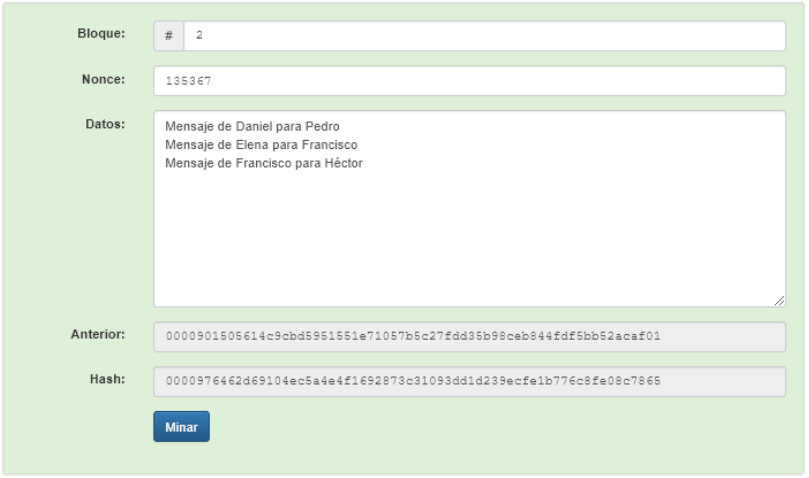


Figura 29: ejemplo 2 de una cadena de bloques. Elaboración propia.

El hacker, una vez ha conseguido modificar el bloque dos, deberá conseguir más capacidad computacional que toda la red para poder minar los bloques dos, tres y cuatro para conseguir que el mensaje original de Daniel le llegue a Pedro en vez de a Elena. Si llegase a conseguir esto, la cadena tendría de nuevo una relación correcta entre los hashes y habría sido atacada con éxito.





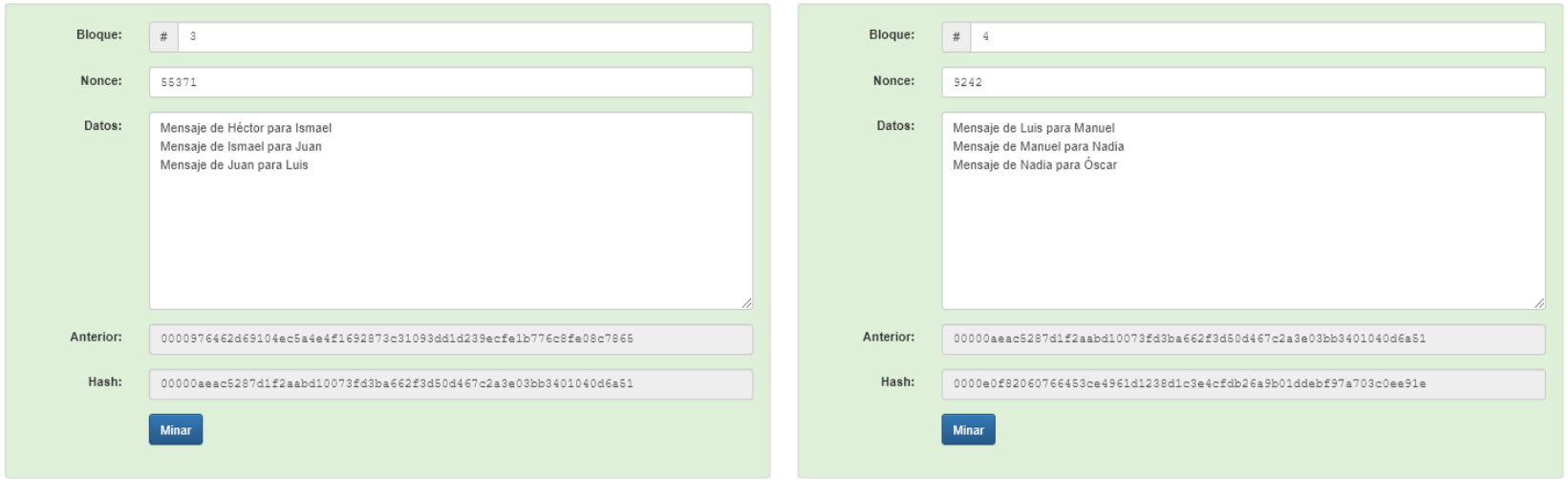


Figura 30: ejemplo 3 de una cadena de bloques. Elaboración propia.

Anexo V Entrevista

Seguidamente se muestra el guion que se ha seguido en las diferentes entrevistas realizadas al personal del III BON del RT 21 en Burgos. Estás preguntas han estado dirigidas a personas especializadas en los sistemas del ET.

- Gestor de identidades:
    - ¿Hay algún sistema militar que solucione el caso de uso de gestionar las identidades?
    - Si existe, ¿Cuál es y cómo funciona?
    - ¿Existe la dependencia de una figura centralizada?
    - ¿El sistema suele presentar el fallo de estar caído?
    - ¿Cree que el sistema se podría mejorar? ¿Cómo?
    - ¿Sabe que es la blockchain? ¿Y cómo funciona?
    - Después de conocer que es y cómo funciona, ¿piensa que podría mejorar los sistemas actuales?
    - ¿Cree que es posible su implementación en el ET? ¿Por qué?
    - ¿Hay alguna pregunta que quiera añadir?
    - En su opinión, ¿quién podría aportarnos más información sobre el tema?

- SIGLE
    - ¿Hay algún sistema militar que solucione el caso de uso de la cadena de suministro?
    - Si existe, ¿Cuál es y cómo funciona?
    - ¿El sistema actual da la posibilidad de conocer la trazabilidad de los productos?
    - ¿Existe la dependencia de una figura centralizada?
    - ¿El sistema suele presentar el fallo de estar caído?
    - ¿Cree que el sistema se podría mejorar? ¿Cómo?
    - ¿Sabe que es la blockchain? ¿Y cómo funciona?
    - Después de conocer que es y cómo funciona, ¿piensa que podría mejorar los sistemas actuales?
    - ¿Cree que es posible su implementación en el ET? ¿Por qué?
    - ¿Hay alguna pregunta que quiera añadir?
    - En su opinión, ¿quién podría aportarnos más información sobre el tema?

- SIMENDEF
    - ¿Hay algún sistema militar que solucione el caso de uso de la mensajería?
    - Si existe, ¿Cuál es y cómo funciona?
    - ¿Existe la dependencia de una figura centralizada?
    - ¿El sistema suele presentar el fallo de estar caído?
    - ¿Le ha llegado alguna vez algún correo que no supiese cuál era su remitente?
    - ¿Cree que el sistema se podría mejorar? ¿Cómo?
    - ¿Sabe que es la blockchain? ¿Y cómo funciona?
    - Después de conocer que es y cómo funciona, ¿piensa que podría mejorar los sistemas actuales?
    - ¿Cree que es posible su implementación en el ET? ¿Por qué?
    - ¿Hay alguna pregunta que quiera añadir?
    - En su opinión, ¿quién podría aportarnos más información sobre el tema?