

laSalle

UNIVERSITAT RAMON LLULL

Escola Tècnica Superior d'Enginyeria La Salle

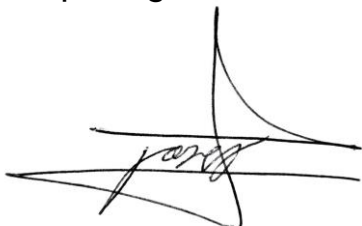
Treball Final de Grau

Grau en Enginyeria en Organització de les TIC

Estudio de la tecnología blockchain y su aplicación en sistemas NAC

Alumne

Josep Selga Vilalta



Professor Ponent

Dr. Daniel Amo Filvà

ACTA DE L'EXAMEN DEL TREBALL FI DE CARRERA

Reunit el Tribunal qualificador en el dia de la data, l'alumne

D.

va exposar el seu Treball de Fi de Carrera, el qual va tractar sobre el tema següent:

Acabada l'exposició i contestades per part de l'alumne les objeccions formulades pels Srs. membres del tribunal, aquest valorà l'esmentat Treball amb la qualificació de

Barcelona,

VOCAL DEL TRIBUNAL

VOCAL DEL TRIBUNAL

PRESIDENT DEL TRIBUNAL

Resumen

Actualmente podemos encontrar la tecnología blockchain en muchos ámbitos, puesto que su uso puede reportar varios beneficios, como pueden ser un aumento de eficiencia, eliminación de una autoridad central, más transparencia, trazabilidad, seguridad y menores costes en determinados casos.

Por otra parte, las tecnologías de Network Access Control están obteniendo cada vez más importancia en cualquier red donde se pretenda tener un buen sistema de seguridad. Esta tecnología nos permite controlar el acceso a la red para limitar el acceso a recursos y proteger activos críticos en las redes informáticas.

En este trabajo se pretende hacer un análisis global de ambas tecnologías, ver cómo funcionan y qué elementos intervienen en el desarrollo y en el uso de estas. Posteriormente se realizará una propuesta de aplicación de la tecnología blockchain en un sistema NAC. Se expondrá como se puede desarrollar esta tecnología y se valorará qué ventajas y desventajas puede tener respecto al sistema actual para hacer una comparativa y ver el valor añadido que nos puede aportar el uso de la blockchain.

Resum

Actualment podem trobar la tecnologia blockchain en molts àmbits, ja que el seu ús pot reportar diversos beneficis, com poden ser un augment d'eficiència, eliminació d'una autoritat central, més transparència, traçabilitat, seguretat i menors costos en determinats casos.

D'altra banda, les tecnologies de Network Access Control estan obtenint cada vegada més importància en qualsevol xarxa on es pretengui tenir un bon sistema de seguretat. Aquesta tecnologia ens permet controlar l'accés a la xarxa per a limitar l'accés a recursos i protegir actius crítics en les xarxes informàtiques.

En aquest treball es pretén fer una anàlisi global de totes dues tecnologies, veure com funcionen i quins elements intervenen en el desenvolupament i en l'ús d'aquestes. Posteriorment es realitzarà una proposta d'implementació de la tecnologia blockchain en una aplicació de sistema NAC, s'exposarà com es pot implementar aquesta tecnologia i es valorarà quins avantatges i desavantatges pot tenir respecte al sistema actual per a fer una comparativa i veure el valor afegit que ens pot aportar l'ús de la blockchain.

Abstract

Currently we can find blockchain technology in many areas, since yours can bring you several benefits, such as an increase in efficiency, deletion of a central authority, more transparency, traceability, security, and lower costs in certain cases.

On the other hand, Network Access Control technologies are gaining more and more importance in any network where a good security system is intended. This technology allows us to control network access to limit access to resources and protect critical assets on computer networks.

The aim of this work is to make a global analysis of both technologies, to see how they work and what elements are involved in their development and use. Subsequently, a study will be carried out a proposal of making use of blockchain technology in a NAC system application, it will be exposed how this technology can be implemented and it will be assessed what advantages and disadvantages it may have with respect to the current system to make a comparison and see the added value that the use of the blockchain can bring us.

Agradecimientos

Me gustaría agradecer a todas aquellas personas que de forma directa o indirecta han contribuido a la realización de este Trabajo de fin de grado.

A mi familia por todo su apoyo, no solo a lo largo del Trabajo de fin de grado, sino durante todo el transcurso de mis estudios, gracias a ellos he podido llegar hasta aquí.

A mis compañeros de *Open Cloud Factory* por brindarme la posibilidad de trabajar con ellos y por estar siempre dispuestos ayudarme cuando me ha surgido cualquier duda, brindándome todo el conocimiento que fuera necesario.

A mis amigos, por sus ánimos y el apoyo que me han dado dentro y fuera de la universidad, sin ellos la carrera no hubiera sido lo mismo.

Finalmente, a la universidad, La Salle URL y a mi tutor y cotutor de TFG, Dr. Daniel Amo y Eduard Céspedes, por guiarme durante la realización de este trabajo de fin de grado.

Índice de contenido

Resumen.....	1
Acrónimos	8
Listado de tablas.....	9
Listado de ilustraciones.....	9
1 Introducción	11
2 Objetivos	15
3 Metodología	16
4 Planificación del proyecto	17
5 Organización del documento	18
6 Estudio de la tecnología Blockchain.....	19
6.1 La tecnología blockchain	19
6.1.1 Como funciona la blockchain	20
6.1.2 Criptografía de la blockchain y firmas digitales.....	22
6.1.3 Funciones hash y Árbol de Merkle	24
6.1.4 Nodos de la blockchain	27
6.1.5 Algoritmos de consenso	27
6.1.6 Tipos de blockchain	29
6.1.7 Estructura de los bloques.....	31
6.2 Problemas y vulnerabilidades	35
6.2.1 Doble Gasto.....	35
6.2.2 Ataque del 51%	36
6.2.3 Ataque Sybil.....	36
6.2.4 Ataque Erebus	37
6.3 Aspectos legales	37
7 Network Access Control	38
7.1 Tecnología NAC	38
7.2 Protocolos AAA.....	40
7.2.1 Authentication.....	40
7.2.2 Authorization.....	41

7.2.3	Accounting.....	41
7.3	Protocolo 802.1x	41
7.3.1	Autenticación con suplicante	43
7.3.2	Autenticación por Mac Address Bypass	44
7.3.3	Flujo del protocolo 802.1x en sistemas NAC.....	45
7.4	Protocolo EAP	47
7.4.1	EAPOL	47
7.4.2	Tipos de EAP	48
7.5	Protocolo RADIUS.....	49
7.6	Soluciones NAC: openNAC	51
7.7	Ejemplarización de un flujo NAC (Laboratorio).....	52
7.7.1	Autenticación	53
7.7.2	Autorización	55
7.7.3	Contabilidad (<i>Accounting</i>).....	58
8	Aplicación Blockchain en sistemas NAC	59
8.1	Trazabilidad de activos en la red	59
8.2	Propuesta de aplicación blockchain - NACTrack	60
8.2.1	Arquitectura del sistema	60
8.2.2	Estructura de datos	61
8.2.3	Estructura de bloques y transacciones.....	62
8.2.4	Algoritmo de consenso.....	63
8.2.5	Flujo de funcionamiento	63
9	Análisis de la propuesta	66
10	Previsión del proyecto de desarrollo	68
10.1	Ciclo de vida del proyecto	68
10.2	Definición del alcance	69
10.3	Roles y responsabilidades	70
10.4	Estructura de Desglose de Trabajo.....	71
10.5	Previsión Temporal del desarrollo	72
10.5.1	Listado de tareas	72
10.5.2	Diagrama Gantt	74
10.6	Presupuesto	76
10.6.1	Presupuesto de recursos humanos	76
10.6.2	Presupuesto de recursos no humanos	77

10.6.3	Presupuesto total	79
11	Validación externa de la propuesta	80
12	Estudio del coste del TFG en horas de trabajo.....	81
13	Conclusiones y líneas futuras	83
13.1	Líneas Futuras	84
14	Referencias.....	85
Anexo A –	Encuesta NACTrack	89
	Estructura y preguntas de la encuesta.....	89
	Resultados de la encuesta.....	93

Acrónimos

ACL: *Access Control List*

AP: *Access Point*

BYOD: *Bring Your Own Device*

DHCP: *Dynamic Host Configuration Protocol*

DLT: *Distributed Ledger Technology*

EAP: *Extensible Authentication Protocol*

EAPOL: *Extensible Authentication Protocol Over Lan*

IT: *Information Technology*

LAN: *Local Area Network*

MAB: *Mac-Address-Bypass*

MAC: *Media Access Control address*

MVP: *Minimum Viable Product*

NAC: *Network Access Control*

NAS: *Network Access Server*

P2P: *Peer-to-peer*

RADIUS: *Remote Authentication Dial-In User Service*

SIEM: *Security information and event management*

TFG: *Trabajo Final de Grado*

VLAN: *Virtual LAN*

WSB: *Work Breakdown Structure*

Listado de tablas

Tabla 1 Estructura de un bloque de Bitcoin	32
Tabla 2 Cabecera de un bloque de Bitcoin.....	32
Tabla 3 Estructura de datos aplicación NACTrack.....	61
Tabla 4 Estructura de un bloque de la aplicación NACTrack.....	62
Tabla 5 Roles del proyecto de desarrollo.....	70
Tabla 6 Tareas Fase Project Management	72
Tabla 7 Tareas Fase Investigación	72
Tabla 8 Tareas Fase Definición de requisitos	73
Tabla 9 Tareas Fase Diseño	73
Tabla 10 Tareas Fase Desarrollo.....	73
Tabla 11 Tareas Fase Test	74
Tabla 12 Tareas Fase Producción	74
Tabla 13 Diagrama Gantt NACTrack.....	75
Tabla 14 Presupuesto Recursos Humanos	76
Tabla 15 Presupuesto de hardware	77
Tabla 16 Presupuesto de software.....	77
Tabla 17 Presupuesto recursos genéricos.....	78
Tabla 18 Presupuesto total	79

Listado de ilustraciones

Ilustración 1 Crecimiento del mercado de la transformación digital en Estados Unidos	13
Ilustración 2 Diagrama Gantt de la previsión en días de trabajo.....	17
Ilustración 3 Funcionamiento básico de la blockchain	20
Ilustración 4 Modelos de arquitectura P2P.....	21
Ilustración 5 Sistema de criptografía de clave asimétrica.....	23
Ilustración 6 Arquitectura del Árbol de Merkle	26
Ilustración 7 Enlace de bloques de una blockchain	33
Ilustración 8 Árbol de Merkle contenido en los bloques de una blockchain	33
Ilustración 9 Información contenida en un bloque de Bitcoin.....	34
Ilustración 10 Arquitectura del modelo AAA	40
Ilustración 11 Arquitectura 802.1x.....	42
Ilustración 12 Tráfico 802.1x en un puerto de Switch	43
Ilustración 13 Diagrama de secuencia autenticación con suplicante	43
Ilustración 14 Tráfico MAB en un puerto de Switch	44
Ilustración 15 Diagrama de secuencia autenticación por MAB	45
Ilustración 16 Diagrama de flujo del protocolo 802.1x.....	46
Ilustración 17 Trama del protocolo EAP.....	47
Ilustración 18 Trama del protocolo EAPOL	48
Ilustración 19 Trama del protocolo RADIUS.....	50

Ilustración 20 Funcionalidades sistema openNAC	51
Ilustración 21 Arquitectura de pruebas NAC	53
Ilustración 22 Captura Wireshark del flujo 802.1x.....	54
Ilustración 23 Captura tcpdump del flujo RADIUS	55
Ilustración 24 Captura Wireshark del flujo RADIUS	55
Ilustración 25 Política de autorización de openNAC.....	56
Ilustración 26 Paquete Access-Accept	57
Ilustración 27 Aplicación de VLAN en el switch	57
Ilustración 28 Captura tcpdump de paquetes Accounting	58
Ilustración 29 Arquitectura de ejemplo del sistema NACTrack	63
Ilustración 30 Flujo de NAC Y transacciones en NACTrack.....	64
Ilustración 31 Ciclo de vida del proyecto NACTrack.....	68
Ilustración 32 Diagrama WBS NACTrack	71
Ilustración 33 Diagrama Gantt Coste Real en horas de trabajo.....	82

1 Introducción

1.1 Servicio de registros de certificación basados en sellos de tiempo

Aunque la atribución de la invención de blockchain y su actual éxito pertenece a Bitcoin y a su creador Satoshi Nakamoto, las bases que componen esta tecnología ya habían sido ideada muchos años antes.

En 1991, Stuart Haber y W. Scott Stornetta, buscaban crear un sistema para evitar que los documentos no pudieran ser modificados y/o alterados mediante el uso de un sello de tiempo digital o *timestamp* (Haber y Scott Stornetta, 1991). La teoría que desarrollaron fue, posteriormente, una parte fundamental en la característica de inmutabilidad de Bitcoin. La teoría de Stuart Haber y W. Scott Stornetta proponía un sistema de validación mediante criptografía a través de un servidor central de confianza. Aunque el funcionamiento era correcto, Satoshi Nakamoto llevo más allá esta verificación mediante los algoritmos de consenso que permitían una descentralización del sistema.

1.2 Evolución de la idea del *time-stamp service*: criptomonedas

En 1998, el criptógrafo Wei Dai publico la propuesta del dinero digital denominado b-money. En este documento se detallaban algunos de los que posteriormente fueron pilares fundamentales de la tecnología, como la necesidad de aportar trabajo computacional con el fin de generar las monedas (W. Dai, 1998).

El último que diseñó un mecanismo o arquitectura similar al Bitcoin antes de este, fue Nick Szabo en 1998. Este modelo llamado Bit Gold nunca se llegó a implementar, pero es considerado el precursor directo de la arquitectura en la que se basa Bitcoin. Bit Gold contenía las características que posteriormente también formaron parte de Bitcoin tales como su estructura descentralizada, el uso de la criptografía y las funcionalidades de prueba de trabajo (Szabo, 2005).

1.3 Confianza en entornos de desconfianza

Uno de los aspectos clave de la tecnología blockchain es su modelo de confianza en un entorno de desconfianza. En este punto, aparece David Chaum quien en 1983 presento su trabajo "*Blind signatures for untraceable payments*". En dicho trabajo, se exponía un método, basado en criptografía, para realizar transacciones seguras manteniendo la privacidad de los participantes, verificar la validez de los pagos y controlar el fraude en las transacciones (Chaum, 1983). En 1990, David Chaum creo una empresa llamada DigiCash, mediante esta empresa desarrollo un sistema de dinero digital llamado ecash (DigiCash, 1994). Ecash facilitaba las transacciones económicas privadas, seguras y difíciles de rastrear. La empresa no fue capaz de crecer hasta que en 1998 se declaró en bancarrota (Smith, 2017).

Una de las principales diferencias entre el sistema ecash ideado por Chaum y Bitcoin es la necesidad de intermediarios en la operativa del protocolo. Mientras que ecash necesita una entidad centralizada para controlar las transacciones (Van Wirdum, 2018), Bitcoin no necesita dicho intermediario gracias a su sistema de red P2P (Satoshi Nakamoto, 2008).

Estas teorías marcarían las bases de lo que posteriormente Satoshi Nakamoto desarrollaría en su *White paper* ("Bitcoin: A Peer-to-Peer Electronic Cash System") donde explicaba un nuevo modelo de moneda digital P2P basada en una arquitectura de bloques encadenados entre sí (Satoshi Nakamoto, 2008).

En esta tesis, Satoshi Nakamoto describe un modelo de dinero digital basado en el P2P, es decir, en el que no existen instituciones intermediarias para el intercambio de este dinero digital. Estas transacciones se almacenan en una cadena formada por bloques, los cuales contienen un conjunto de estas transacciones, esta es la llamada blockchain.

Hasta la fecha nadie sabe quin o quienes son Satoshi Nakamoto y aunque varias personas hayan autoproclamado el serlo, la verdad es que es y probablemente seguirá siendo un misterio sin resolver.

En 2009 se minó el primer bloque de bitcoin, el nominado *Genesis Block*, a partir de este momento esta tecnología se convirtió en una realidad y a medida que pasaban los años el valor de la moneda crecía a la par que lo hacía el interés por ella.

1.4 Automatización de contratos

En poco tiempo empezaron a surgir multitud de proyectos basados en blockchain, muchos de ellos sin un valor real o con propósitos muy específicos. Fue en 2014 cuando Vitalik Buterin, un joven ruso-canadiense, y su equipo de desarrollo publicaron el *White paper* de *Ethereum*, ("A Next Generation Smart Contract & Decentralized Application Platform"). Ethereum es una tecnología de Smart Contracts basada en blockchain y la tecnología donde muchos dicen que reside el verdadero potencial de blockchain. A grandes rasgos, los *Smart Contracts* son, como su nombre indica, contratos inteligentes que se programan con código y se ejecutan sobre una red blockchain.

1.5 La importancia de la blockchain como evolución tecnológica

Blockchain y los proyectos relacionados con ella han supuesto un cambio muy grande en la forma en que entendemos muchos de los procesos que hasta ahora veíamos eficientes, no solo en el ámbito tecnológico sino en sectores y aplicaciones más tradicionales. Es por esto por lo que esta tecnología ha recibido muchísima atención estos últimos años y mucha gente ha comprendido el potencial que tiene en un futuro no muy lejano.

En 2017 el mercado de criptodivisas empezó a crecer de forma exponencial, todo el mundo hablaba de bitcoin y de las proezas de esta tecnología. Esto generó un sentimiento de especulación en muchísima gente que a pesar de no tener claro lo que bitcoin era o representaban ellos también querían formar parte del fenómeno.

Algunos empezaron a considerar al Bitcoin y al mercado de criptodivisas una burbuja financiera y en parte, con razón. A principios del 2018, el precio del bitcoin cayó un 65% y se calcula que las pérdidas del mercado en general fueron del 80%. Fueron muchas las compañías que desaparecieron de la noche a la mañana dejando a los inversores con unos tokens con valor cero.

Estas bajadas tan pronunciadas en la valorización de esta criptomoneda se convierten en eventos que se repiten a lo largo del tiempo como se vio en el mes de abril de 2021 donde el valor se redujo aproximadamente un 23%. Dado que el precio de bitcoin es propenso a realizar grandes subidas en periodos cortos, existe la posibilidad de que estas devaluaciones sean correcciones en el precio, insignificantes pasados unos años.

Esto refleja el hecho de que más allá de la especulación de los propios inversores, se generó una especulación en las aplicaciones de la tecnología y fueron muchos que quisieron fundar compañías que a priori mejoraban tecnologías actuales o solucionaban problemas mediante blockchain, pero que en la práctica no tenían sentido alguno.

Es importante entender que blockchain puede mejorar muchísimas cosas, pero es erróneo pensar que puede suponer una mejora para cualquier cosa. Actualmente esta tecnología tiene sus puntos fuertes como lo es la fiabilidad y confianza de la información que almacena, pero también tiene sus puntos débiles como la velocidad, haciéndola de difícil uso en aplicaciones donde sea esta característica un punto fundamental.

1.6 Sistemas NAC

La otra tecnología o sistema del que se hablara en este TFG y posteriormente se le buscaran posibles implementaciones de la tecnología blockchain en ella, son los denominados sistemas NAC. En términos generales, los sistemas NAC, son aplicaciones informáticas encargadas de controlar el acceso a las redes y que, a pesar de ser un sistema que lleva muchos años en la industria de la ciberseguridad, está empezando a convertirse en una pieza clave en la ciberseguridad de empresas y organismos gubernamentales.

Nos encontramos en una época de cambio respecto a cómo las empresas y organizaciones estructuran su forma de trabajar. Estas empresas confían cada vez más en los sistemas informáticos y las redes con el fin de optimizar y agilizar flujos de trabajo a la vez que se optimizan costes.

Tal y como podemos observar en el siguiente gráfico, el mercado de la transformación digital en Estados Unidos aumenta año tras año, impulsado en parte, por la necesidad de las compañías de adaptarse a estos nuevos tiempos (Grand View Research, 2020).

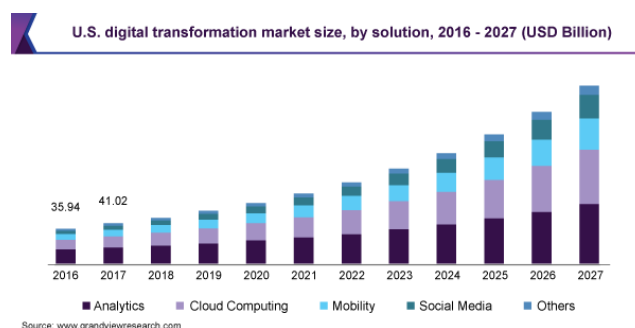


Ilustración 1 Crecimiento del mercado de la transformación digital en Estados Unidos

Esta transformación digital supone un gran avance para dichas organizaciones, pero también pueden devenir riesgos de ciberseguridad o privacidad de datos, entre otros, si no se realizan estableciendo un modelo seguro.

En ocasiones podemos pensar que la ciberseguridad es un tema complicado y más en las grandes empresas las cuales disponen de grandes cantidades de sistemas, redes, usuarios, etc. Es evidente que el trabajo de mantener segura toda la infraestructura de la empresa no es simple, pero en ocasiones se focaliza más en grandes proyectos de ciberseguridad y se olvidan los aspectos básicos como, por ejemplo, mantener los equipos actualizados. Un caso con mucha repercusión fue el ataque que sufrió Telefónica en mayo de 2017, el llamado *malware* de WanaCry, este *ransomware* aprovechaba una vulnerabilidad de los equipos Windows (ya solucionada mediante parches en el momento del ataque) por la que era capaz de secuestrar los datos del equipo donde se encontraba, cifrándolos y manteniéndolos secuestrados hasta que se realizara un pago a una cuenta de bitcoins. Este ataque afectó a más de 200.000 máquinas Windows que no estaban actualizadas.

Otras prácticas que se están extendiendo en la forma que se trabaja en las empresas son los fenómenos de *Bring Your Own Device* (BYOD) y el trabajo remoto, esta segunda muy extendida a causa de la pandemia de la COVID-19.

El BYOD es el permitir a los empleados de una empresa, estudiantes en una universidad, etc. acceder a los recursos de esta mediante sus dispositivos personales como el portátil, *smartphone*, etc. Esto quiere decir que la seguridad de estos dispositivos cliente recae sobre el usuario y no sobre el propietario de la red donde se conectan.

El otro fenómeno es el del trabajo a distancia o remoto, esta forma de trabajo ya existía en muchas organizaciones, pero a causa de los acontecimientos sucedidos en 2020 a causa de la pandemia de la COVID-19, muchos trabajadores y estudiantes se han visto obligados a realizar sus tareas desde casa. Esto obliga a estas organizaciones a disponer de una infraestructura para que esto sea posible y estas personas sean capaces de acceder a recursos de la organización de forma remota.

En ambos casos estas organizaciones tienen la responsabilidad de elevar la seguridad de sus redes y sistemas informáticos, ya que están apareciendo factores clave para la seguridad que antes no tenían que controlar.

Los sistemas NAC cubren una necesidad básica de cualquier red privada, controlar quien o que se conecta a nuestra red, autorizando o denegando el acceso a estos siguiendo un listado de políticas de acceso, como por ejemplo tener instalado un cierto parche de un sistema operativo o contar con un antivirus. Estos sistemas NAC hacen uso de diferentes protocolos de seguridad que nos permiten realizar las autenticaciones, transportar la información entre los clientes y los servidores de forma segura, etc.

La tecnología blockchain ha demostrado tener multitud de aplicaciones en sectores y ámbitos en los que nunca se hubiera imaginado que pudiera aportar características como mayor seguridad, transparencia o confianza en la información. Es por esto por lo que en este TFG se teorizará sobre posibles aplicaciones de la tecnología blockchain sobre sistemas NAC para con el objetivo de explorar las posibilidades de mejora de estos sistemas.

2 Objetivos

El objetivo principal de este TFG es realizar un estudio profundo sobre la tecnología blockchain y la tecnología de Network Access Control, ambas tecnologías, pese a llevar mucho tiempo en nuestro entorno, están cogiendo cada vez más importancia debido a los cambios por los que atraviesa la sociedad.

Dicho estudio perimirá realizar una investigación con la que, dentro de un marco teórico, se desarrollaran posibles aplicaciones de la tecnología blockchain en sistemas NAC para aprovechar las ventajas que esta nos ofrece.

De forma más específica, podemos resumir los objetivos y subobjetivos de este trabajo de fin de grado en los siguientes puntos:

- Obtener una visión profunda del entorno y las tecnologías con las que se va a fundamentar el trabajo:
 - Conocer el funcionamiento de la tecnología blockchain y como esta puede revolucionar multitud de sectores y metodologías tradicionales con las que blockchain puede optimizar y mejorar procesos.
 - Conocer con mayor profundidad las bases teóricas y de funcionamiento de los sistemas de Network Access Control. Entendiendo el funcionamiento general y los protocolos que lo componen.
- Dentro de un marco teórico, realizar una propuesta de posible aplicación de la tecnología blockchain en sistemas NAC:
 - Desarrollar una propuesta teórica sobre posibles aplicaciones de blockchain en sistemas NAC.
 - Validar la propuesta de aplicación de forma externa a partir de los beneficios que esta puede aportar.
- Definir una previsión organizacional y económica relativa al desarrollo de la aplicación de la tecnología blockchain.
- Realizar un análisis de resultados que permitan entender las ventajas e inconvenientes de la blockchain aplicada a los sistemas NAC y el posible potencial que estas aplicaciones pudieran tener.

Así pues, después de realizar el estudio de la tecnología blockchain y los sistemas NAC, se profundiza sobre qué aplicaciones puede tener el uso de blockchain sobre estos sistemas, que ventajas e inconvenientes puede tener y la viabilidad del uso.

Debido a la gran variedad de posibilidades que blockchain nos ofrece, se escogerán varias propuestas de aplicaciones por las que se elegirá una de ellas para un posterior análisis y comparación más profunda respecto al modelo actual de funcionamiento.

3 Metodología

La metodología para la realización de este trabajo de fin de grado se ha basado en el estudio dentro de un marco teórico, de dos tecnologías concretas. Una de ellas es la blockchain, de la que se pueden extraer una gran cantidad de aplicaciones en diferentes ámbitos de sectores muy diversos, la segunda, es la tecnología de control de acceso a la red (NAC).

Tras haber realizado el estudio teórico se procederá a analizar posibles aplicaciones blockchain a sistemas NAC.

Así pues, la metodología se basa en tres puntos clave:

1. Estudio del contexto tecnológico actual.
2. Marco teórico de la tecnología blockchain.
3. Marco teórico de los sistemas NAC.
4. Propuesta teórica de una posible aplicación de la tecnología blockchain sobre un sistema NAC.
5. Previsión del desarrollo de la propuesta.
6. Validación externa de la propuesta.
7. Conclusiones definitivas.

En el marco teórico de ambas tecnologías se detallarán los conceptos básicos con el fin de obtener un conocimiento global de cada una de ellas, entender cómo funcionan y que aportan es sus respectivos campos.

Habiendo realizado el estudio de estas tecnologías determinamos que tenemos conocimiento suficiente para realizar una teorización sobre una posible aplicación que la tecnología blockchain podría tener en sistemas NAC. Se realizará un estudio sobre la viabilidad e impacto que puedan tener las aplicaciones propuestas.

Con dicha propuesta teórica se establecerá una previsión donde se definirá el proceso para el desarrollo de esta nueva aplicación. Este proceso se realizará desde una aproximación al *Project Management*.

Dado que se propondrá una aplicación de tecnología, se considera oportuna la validación externa de dicha aplicación.

Finalmente, se definirán las conclusiones obtenidas en el global del trabajo y se valorarán los aspectos relativos al estudio de la posible aplicación.

Durante el transcurso del trabajo será necesario realizar consultas a diferentes fuentes con el fin de obtener el conocimiento necesario. Estas fuentes podrán proceder de libros, artículos científicos o webs, intentando siempre contrastar la información consultada y validando la reputación de la fuente de procedencia.

4 Planificación del proyecto

Para la planificación del desarrollo del trabajo de fin de grado, se establecen fases correspondientes a los objetivos y metodología del propio trabajo.

Estas fases son:

- Definición de concepto.
- Documentación.
- Estudio Blockchain.
- Estudio sistemas NAC.
- Propuesta de aplicación blockchain.
- Previsión organizacional y económica del desarrollo.
- Validación externa de la propuesta.

En la siguiente ilustración podremos observar el diagrama de Gantt con la distribución temporal de estas fases:

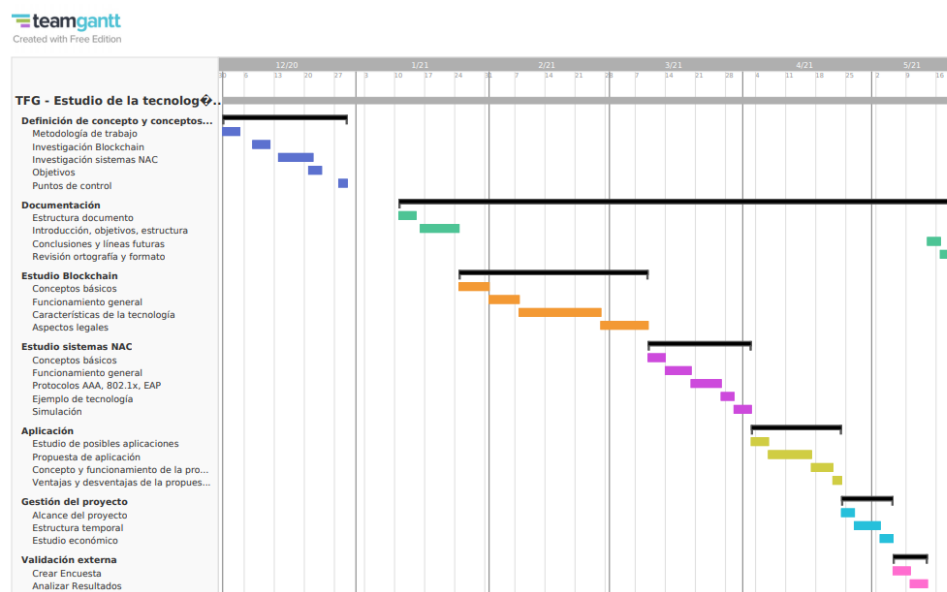


Ilustración 2 Diagrama Gantt de la previsión en días de trabajo

Las horas estimadas para cada una de las fases son:

- Definición de concepto → 35h
- Documentación → 60h
- Estudio Blockchain → 100h
- Estudio sistemas NAC → 50h
- Aplicación blockchain → 35h
- Estudio del proyecto de desarrollo → 50h
- Validación externa de la propuesta → 10h

Se estima un total en horas de dedicación de: **340h**

5 Organización del documento

Este proyecto se ha estructurado partiendo de un estudio teórico de todas aquellas tecnologías que componen el caso de estudio, para que a partir de dicha base teórica sea posible estudiar las posibles aplicaciones y casos donde estas tecnologías puedan ser combinadas de forma efectiva.

En una primera parte (Apartados 1, 2, 3, 4 y 5) se describen los aspectos generales del proyecto donde podremos entender que se pretende con la realización de este y cuál ha sido la metodología utilizada.

En los apartados 6 y 7 se desarrollará la base teórica de las dos tecnologías que componen el caso de estudio, la tecnología *blockchain* y la tecnología de *Network Access Control* (NAC).

En ambas tecnologías se parte de una base profunda para ir completando en términos más generales el funcionamiento de estas tecnologías. El apartado 6 corresponde a la tecnología *blockchain*.

En el apartado 7 se tratarán los aspectos de los productos NAC, su funcionamiento y estructura general, así como los protocolos, en un marco teórico, de los que hace uso para su funcionamiento.

Llegados al apartado 8 y con una base teoría de ambas tecnologías, se realizará una propuesta de un posible uso de la primera tecnología (*blockchain*) aplicada a los productos de tecnología NAC. En el apartado 9 se realizará un análisis de la propuesta.

En el apartado 10 se realizará una previsión temporal y económica del posible proyecto de desarrollo de la propuesta descrita en el apartado 8.

Con el fin de validar la propuesta de aplicación se realizará una encuesta a varios participantes y se expondrán los resultados en el apartado 11.

En la última sección de este documento se realizará un análisis de los resultados obtenidos en los estudios que se han llevado a término. Se realizará un breve resumen del costo económico y temporal del proyecto y finalmente, se desarrollarán unas conclusiones y líneas futuras a seguir.

6 Estudio de la tecnología Blockchain

En este apartado se analizará y detallará el funcionamiento de la tecnología blockchain desde su base y desde un punto de vista técnico. Posteriormente se analizarán aquellos problemas ya solucionados gracias a blockchain, así como las posibles vulnerabilidades que existen actualmente para esta tecnología. En última instancia se hablará brevemente de los Smart Contracts, su estructura, funcionamiento y beneficios de esta tecnología basada en blockchain.

6.1 La tecnología blockchain

A grandes rasgos podemos definir blockchain como una base de datos distribuida con algunas particularidades como la inmutabilidad de los datos y la falta de necesidad de una tercera parte de confianza para el intercambio de datos ya que se trata de un protocolo *Peer-to-Peer* (P2P) por lo que las transacciones se realizan entre dos partícipes con la misma condición.

Estos datos conforman un registro distribuido por todos los partícipes del sistema llamado blockchain o cadena de bloques. En estos registros se almacenan transacciones entre dichos participantes sin la necesidad de tener una tercera parte de confianza para validar dicha transacción.

Aunque no fue hasta 2008 cuando Satoshi Nakamoto definió e implemento la primera blockchain en su *WhitePaper* "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2008) anteriormente ya se habían realizado varios estudios que definían una idea básica de lo que posteriormente sería la blockchain. Una de las aproximaciones más próximas a Bitcoin fue el estudio de Nick Szabo que realizó en 1998 donde se define un protocolo en el cual no eran necesarios intermediarios de confianza para el intercambio de datos y donde ya se abordaba el problema del doble gasto que trataremos más adelante (N. Szabo, 2005).

Mediante el uso de cifrado, la información es protegida para garantizar que no se viole la privacidad del usuario y que los datos no puedan ser alterados. A diferencia de las instituciones financieras existentes, la información en una red Blockchain no está gobernada por una autoridad centralizada. Los miembros de la red conservan los datos y tienen la autoridad democrática para autorizar cualquier actividad que pueda surgir en una red Blockchain. Una red Blockchain tradicional, por lo tanto, es una Blockchain pública.

Blockchain es un mecanismo de registro de información que hace que modificar, manipular o engañar el sistema sea complejo e improbable. Blockchain es esencialmente una base de datos de transacciones que es duplicada y distribuida a través de toda la red informática Blockchain.

Cada bloque de la cadena contiene varias transacciones y se añade una anotación al registro de cada participante siempre que se genera una nueva transacción en la Blockchain. La infraestructura de blockchain es una red descentralizada dirigida por varias personas llamada *Distributed Ledger Technology* (DLT).

6.1.1 Como funciona la blockchain

Para conocer en detalle el funcionamiento de blockchain podemos separar esta tecnología en los siguientes aspectos principales:

1. Sistemas P2P.
2. Criptografía y cifrado de información.
3. Bloques, Almacenamiento y Transacciones.

En la mayoría de los casos, las claves criptográficas se componen de una clave privada y de una clave pública. Estas claves ayudan a ejecutar de forma efectiva y segura las transacciones entre dos partes. Cada individuo tiene las dos claves que usa para crear una fuente segura para la identificación digital. Una de las características principales de la tecnología Blockchain es esta identificación protegida.

Esta identificación, que es considerada una "firma digital" en el área de la blockchain, es utilizada para la autorización y regulación de las transacciones que se producen en la red.

La firma digital se combina en una red P2P. Cuando el acuerdo o transacción es validado, un cálculo matemático certifica que los dos participantes conectados a la red han completado con seguridad la transacción. Por lo tanto, para resumirlo, los usuarios de Blockchain utilizan claves encriptadas para comunicarse en la red P2P de diferentes maneras.

La siguiente imagen muestra cómo trabaja la blockchain de Bitcoin de forma resumida:

Qué es la Blockchain?

y, cómo funciona?

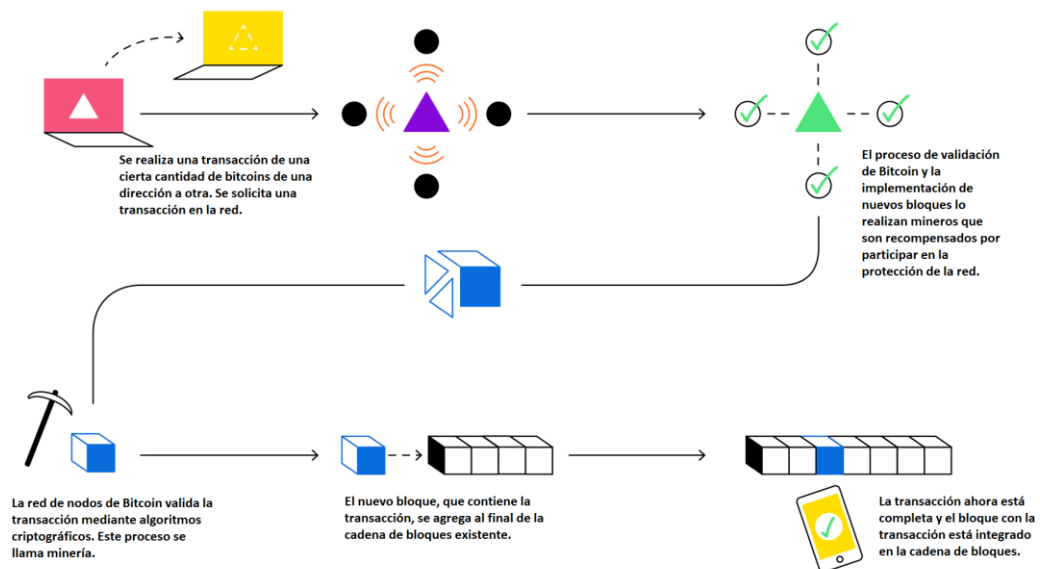


Ilustración 3 Funcionamiento básico de la blockchain

En una primera instancia se genera una nueva transacción en la red, las transacciones son la información principal almacenada en la red Bitcoin y corresponden a un traspaso de valor

entre un usuario A y un usuario B. Se informa a todos los nodos de la red de esta nueva transacción y seguidamente los nodos de la red proceden a la validación. Las transacciones se agrupan en bloques que posteriormente al proceso de minado serán añadidos a la blockchain momento en el cual la transacción se completa.

Red P2P:

Las redes peer-to-peer mantienen una estructura descentralizada, estas están formadas por nodos pudiendo ser estos, por ejemplo, ordenadores ubicados en zonas geográficas dispares. Todos estos nodos existen bajo un mismo protocolo de comunicación con el objetivo de crear una red donde sea posible compartir información de cualquier tipo.

El hecho de que se trate de una red descentralizada indica que no existe un nodo o punto central de conexión o control y las partes partícipes de esta red actúan de forma autónoma y con métodos para determinar un consenso común.

Dadas las características de este tipo de protocolo es posible la creación de redes descentralizadas de uso libre y difícilmente censurables.

Las redes P2P por definición suelen interconectar todos los partícipes de la red eliminando los conceptos de “centro” y “periférico” característicos de las redes centralizadas y descentralizadas.

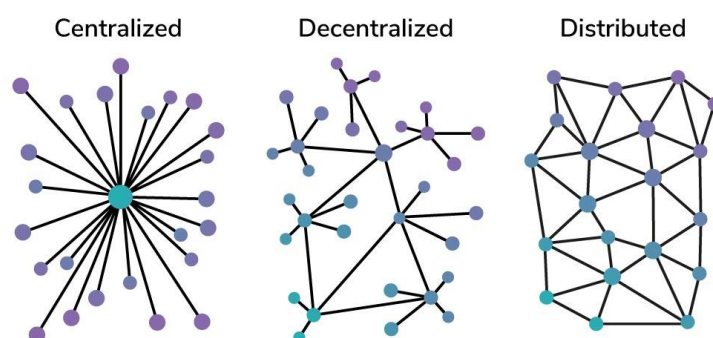


Ilustración 4 Modelos de arquitectura P2P

Tal y como podemos observar en la imagen anterior, en una red centralizada, todos los nodos de la red son periféricos de un único nodo central lo que provocaría que ante un fallo o cambio de este nodo central toda la red se vería afectada. En una red descentralizada existen diversos puntos de conexión (nodos centrales) y varios periféricos unidos a estos nodos. Finalmente, en una red distribuida al no existir nodos centrales ni periféricos, todos los nodos se conectan entre sí por lo que el flujo de información en la red es libre y la desconexión de uno de los nodos no afectaría al resto (Qureshi, 2020).

Funciones hash:

El cifrado de información mediante funciones hash nos permite crear una identificación única de forma cifrada para la información almacenada en la blockchain. Estas funciones reciben una entrada X pudiendo ser esta en formato de texto plano y, mediante funciones matemáticas, obtenemos un resultado alfanumérico de longitud fija. Cualquier modificación en la entrada X resultará en variaciones en la salida de la función. Esto permite que pueda detectarse cualquier alteración de la información de forma rápida.

Transacciones:

La transacción es un tipo de información almacenada en la blockchain como por ejemplo la de Bitcoin, esta determina la transferencia entre un usuario A y un usuario B de la red.

En el momento en el que una transacción es validada, esta se añade a un “pool” de transacciones junto a otras, las cuales posteriormente a su selección, formaran un bloque que será añadido a la red.

Bloques:

Los bloques de una blockchain son aquellos elementos que contienen la información que se almacena en la propia blockchain. Estos pueden ser de tamaño variable y almacenan, por ejemplo, en el caso de Bitcoin, transacciones realizadas entre usuarios de la red. Dependiendo del caso de uso de la blockchain, estos bloques podrán ser más simples como en Bitcoin donde solo se realiza una transferencia de valor entre usuarios o más complejos como el caso de Ethereum y sus Smart Contracts.

En el apartado 6.1.7 veremos con más detalle la composición de los bloques.

6.1.2 Criptografía de la blockchain y firmas digitales

La criptografía es una forma de diseñar técnicas y protocolos que previenen a terceros acceder y sensibilizar datos de comunicaciones privadas durante la fase de comunicación o almacenamiento. La criptografía se compone principalmente de dos palabras griegas; Kryptos, que significa oculto y Graphine, que significa "escribir". El modelo criptográfico representa un elemento fundamental para la tecnología blockchain dado que en un sistema donde la información se comparte de forma pública, es esencial mantenerla protegida.

En este apartado se profundizará sobre los aspectos básicos de la criptografía y de cómo la blockchain hace uso de esta.

Los siguientes términos pueden ser importantes para entender la criptografía:

1. **Encriptado:** Un método para convertir texto sin formato (texto plano) en texto cifrado (secuencia aleatoria de bits).
2. **Desencriptado:** El método opuesto de encriptado, transformando el texto cifrado en texto sin encriptar.
3. **Clave:** Se necesita una cantidad limitada de información para inducir la función del algoritmo criptográfico.

6.1.2.1 Tipos de criptografías:

Básicamente, existen tres tipos o maneras principales en las que podemos realizar criptografía y desarrollar e implementar sus algoritmos (Sectigostore, 2020).

- **Criptografía de clave simétrica**

En este método de encriptado, se utiliza una sola clave (k). Esta clave estándar se utiliza tanto para el encriptado como para el desencriptado. El uso de una clave única común presenta un problema debido a la necesidad de transferir la clave entre el remitente y el receptor. También llamada criptografía de clave secreta.

- **Criptografía de clave asimétrica**

Este método de encriptado utiliza varias claves, una clave privada (de encriptado), una clave pública (de desencriptado). El par de claves generado por este algoritmo consta de una clave privada y una clave única pública generada por el mismo algoritmo. A menudo se conoce como criptografía de clave pública.

El proceso de transmisión de datos cifrados entre A y B se realiza de la siguiente manera:

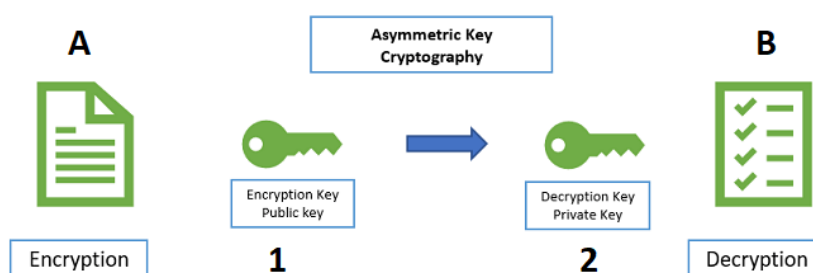


Ilustración 5 Sistema de criptografía de clave asimétrica

1. La información se encripta en A mediante la clave pública de B.
2. La información cifrada se envía a B y mediante la clave privada de B esta se desencripta.

En una red blockchain, como Bitcoin, el par de claves público-privada se utiliza para administrar la gestión de usuarios en la red y las transacciones entre ellos. La clave pública se utiliza como la dirección criptográfica de la persona dentro de la blockchain. La clave pública puede ser accesible a terceros, es decir, puede ser visible para todos los miembros, aunque normalmente esta se utiliza después de haber pasado por una función hash, ya que obtenemos una clave pública más corta y con una capa extra de seguridad. La clave privada es un valor secreto que se utiliza para tener acceso a los datos de dirección y para permitir todas las acciones de "dirección", normalmente transacciones salientes.

La clave privada de forma simple, un número generado de forma aleatoria. A partir de esta clave privada, mediante funciones matemáticas, se genera la clave pública, no es posible obtener la clave privada a partir de la clave pública. Algunos algoritmos para la generación

de estas claves públicas son el RSA (*Rivest Shamir Adleman*) o el ECDSA (*Elliptic Curve Digital Signature Algorithm*) utilizado por Bitcoin.

6.1.3 Funciones hash y Árbol de Merkle

Tal y como hemos visto en el apartado 6.1.1, las funciones o algoritmos de hash son elementos matemáticos donde dada una entrada X obtendremos una salida codificada de forma alfanumérica y única.

La función hash es una función unidireccional, una función unidireccional se define como aquella que solo es posible calcular el resultado hacia una dirección por lo que nos asegura que, una vez obtenido el hash de una serie de datos, difícilmente podremos obtener dicha información a partir del hash.

Una función hash debe constar de una serie de propiedades para determinar que esta es segura. Estas propiedades son (Wikipedia, 2020):

- **Determinista**

Una función hash determinista es aquella que dada una entrada X el valor de salida Y siempre será el mismo mientras no se modifique X. Para lograr mantener esta propiedad la función debe operar solamente sobre los datos de entrada, sin depender de datos externos que podrían variar modificando así la salida de la función.

- **Computacionalmente eficiente**

Que una función hash sea computacionalmente eficiente hace referencia a la facilidad o rapidez en que es posible calcular el resultado de una función. Esto se debe a que, si el cálculo del resultado de la función consumiera mucho tiempo y recursos, las aplicaciones que hacen uso de estos serían ineficientes.

- **No reversible o resistente a preimage**

No debe existir una forma de obtener el conjunto de datos original a partir del código hash. Así pues, dado una salida Y a una función $h(x)$ no debe ser posible obtener x de forma directa. Algunos ataques de fuerza bruta podrían obtener el valor original de la cadena, pero el coste computacional sería más alto que la recompensa obtenida.

- **Resistente a colisión**

La resistencia a colisión se establece como la improbabilidad de que dadas dos entradas más a la función hash se obtenga una salida igual. Dado que las salidas de las funciones hash tienen una longitud fija independientemente de la longitud de entrada las posibilidades de salida son finitas por lo que no hay función hash cien por cien resistente a colisiones. El objetivo es reducir la posibilidad de colisión al máximo.

Dentro de la tecnología blockchain el uso de funciones hash es ampliamente utilizado para:

- **Creación de direcciones públicas**

Las direcciones públicas de la red Bitcoin son representaciones de las claves públicas de los usuarios de la red. Estas claves públicas suelen ser complejas y extensas, por esta razón, mediante el uso de una función hash es posible generar esta representación de la clave pública más corta a la vez que añadimos una capa extra de seguridad.

- **Proceso de minería**

Redes blockchain como las de Bitcoin utilizan el proceso de minería para añadir nuevos bloques a la red. Este proceso, en la mayoría de los casos, es básicamente el cálculo de un acertijo matemático mediante un proceso de prueba y error donde los nodos de minado calculan el hash necesario para añadir el bloque a la red.

- **Smart Contracts**

Dentro de las blockchain enfocadas al uso de los Smart Contracts, las funciones hash son utilizadas para proteger información sensible dentro de una red pública tales como nombres, direcciones, datos de terceros, etc.

Otra funcionalidad de los hashes dentro de las aplicaciones de Smart Contracts es el versionado de estos, dado que cualquier modificación del contrato generara un cambio en el hash por lo que se anula el contrato previo dando por válido el nuevo.

Finalmente, el uso de los hashes para dar validez y autenticidad a los contratos ejecutados, siendo estos los testigos de la ejecución del contrato por ambas partes.

El Árbol de Merkle (Binario)

El Árbol de Merkle, también llamado árbol de hash es básicamente una estructura de datos ordenados y ligados entre ellos, tal y como indica su nombre, en forma de árbol invertido formado por nodos. Estas estructuras están creadas con el objetivo de facilitar la verificación de grandes cantidades de datos organizados por medio de diversas técnicas criptográficas.

Este árbol resume todas las transacciones incluidas en un bloque, formando la siguiente estructura (Brilliant, 2016):

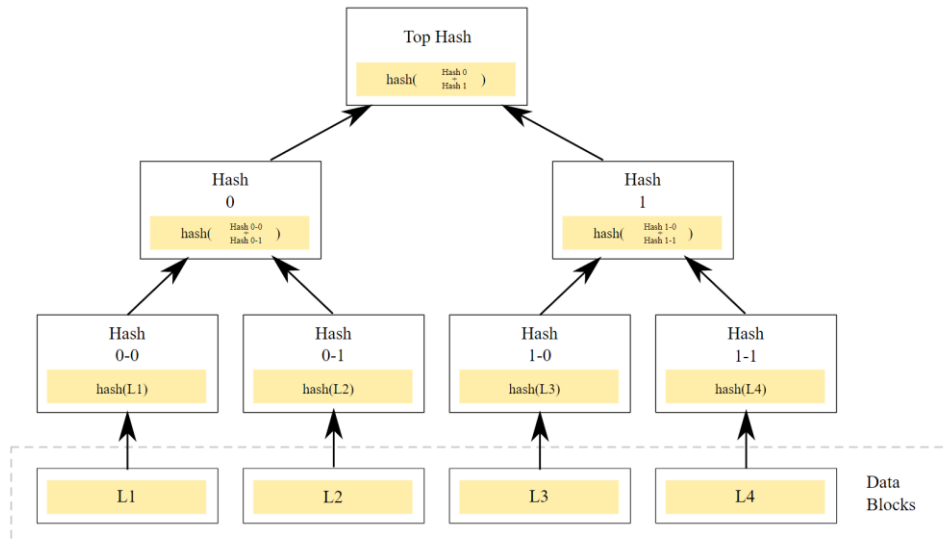


Ilustración 6 Arquitectura del Árbol de Merkle

Tal y como podemos observar en la parte inferior de la estructura tenemos la información base que compone el árbol, en este caso todas las transacciones incluidas en un bloque. Cada una de estas transacciones pasa por una misma función hash. Estos nuevos hashes se agruparán de forma binaria, de dos en dos, para formar un nuevo hash a partir de la combinación de ambas, esto reducirá por dos el número de hashes hasta llegar al punto donde todos los nodos del árbol se agruparán en uno solo el Top Hash o Merkle Root.

Dado que se utilizan funciones hash que dependen de la entrada y que siempre tienen el mismo resultado para una misma entrada, cualquier modificación en la base de la información provocaría un cambio en todos los hashes superiores hasta llegar al Merkle Root, que se vería modificado dando el bloque por inválido.

Más allá de la consistencia y validez de los datos, los árboles de Merkle nos aportan eficacia en cuanto a la verificación de la existencia de ciertos datos. Esto se debe a que, a pesar de que los datos estén “enterrados” bajo un mismo hash, no es necesario comprobar todas las transacciones para determinar la existencia de una en concreto.

En la Ilustración anterior, en caso de querer verificar la existencia de los datos L1 simplemente necesitaríamos el Hash de L1 (Hash 0-0), el Hash 0-1, el Hash 0, el Hash 1 y el Top Hash.

Aunque la mayoría de blockchain utilizan la tecnología del árbol de Merkle, no todos lo utilizan de forma binaria dado que la información almacenada puede ser más compleja que las transacciones como en el caso de Bitcoin.

6.1.4 Nodos de la blockchain

Los nodos de una red blockchain son aquellos que mantienen el registro e información de la red. Tienen entre sus funciones la validación o verificación de los bloques que se añadirán a la red. Estos nodos son aquellos que a través de software se interconectan mediante la red P2P, así pues, todos los nodos operan de forma equivalente entre ellos. Los nodos deben mantenerse actualizados entre sí por lo que tienen el encargo de almacenar y compartirse la información que se almacena en la blockchain.

En una red blockchain pueden existir varios tipos de nodos dependiendo de las características, aunque todos ellos deben ejecutar las mismas funciones, en el caso de Bitcoin, estos nodos son (Khan, 2020):

- **Nodos Completos**

Estos nodos son aquellos que almacenan una copia exacta, completa y actualizada de la información almacenada en la red blockchain a la par que realizan el proceso de minado, son nodos llamados Mineros.

- **Nodos Ligeros**

Los nodos ligeros mantienen un registro parcial de la red blockchain por lo que es factible ejecutarlos en dispositivos de menores recursos de hardware. Estos no son capaces de validar transacciones de la red y deberán recibir la información a través de un supernodo.

- **Supernodos**

Los supernodos son un tipo de nodo completo que aparte de mantener una copia completa de la información almacenada, actúa como un punto de comunicación con otros nodos de la red de forma abierta y pública para que cualquiera que desee conectarse a la red pueda hacerlo.

- **Nodos de Minería**

Los nodos de minería son nodos completos que aparte de almacenar la información completa de la red, ejecutan de forma paralela el proceso de minería por lo que serán los encargados de procesar y añadir nuevos bloques a la blockchain.

Dependiendo de las necesidades o tipo de la red blockchain pueden existir otros tipos de nodos con funciones afines al objetivo final de la blockchain.

6.1.5 Algoritmos de consenso

Blockchain es una red autónoma y distribuida que proporciona autenticidad, confidencialidad y transparencia. No hay ningún organismo central que esté presente para comprobar y verificar las transacciones, sin embargo, cada transacción está totalmente protegida y monitoreada.

Esto es posible gracias a los algoritmos de consenso, que son un aspecto fundamental de cualquier red Blockchain. El algoritmo de consenso es un proceso en el que todos los participantes del sistema Blockchain dan su consentimiento sobre el estado del registro público. Por lo tanto, los algoritmos de consenso logran proveer confianza a la red Blockchain y crean consenso entre participantes anónimos en una red distribuida.

El algoritmo de consenso determina que cualquier modificación de la blockchain, como el proceso de añadir un nuevo bloque en la red debe ser aceptada por todos los nodos de Blockchain.

Así pues, un algoritmo de consenso busca alcanzar un entendimiento compartido que sea válido para toda la red.

Los principales mecanismos de consensos son los siguientes:

- **Proof of Work (PoW)**

Proof of Work fue el primer mecanismo de consenso en una red blockchain, utilizado por la red Bitcoin. Este mecanismo se basa en el esfuerzo computacional de los nodos de minería de la red, este esfuerzo es al cálculo de numerosas operaciones matemáticas que, posteriormente, serán validadas por la red.

En el caso de Bitcoin, para cada nuevo bloque se deberá resolver un problema matemático mediante intentos de prueba y error por parte de los nodos de minería, la resolución del problema dará como resultado la creación del nuevo bloque, la confirmación de las transacciones incluidas en él y finalmente la liberación de una cantidad determinada de bitcoins como recompensa por el minado de dicho bloque.

La prueba o problema que deben resolver es descubrir los parámetros de entrada de un determinado hash. Como hemos visto anteriormente las funciones hash son unidireccionales por lo que la determinación de la entrada solo puede ser calculada mediante un ejercicio de prueba y error (Wikipedia, 2020).

Uno de los principales inconvenientes que presenta este mecanismo es que, dado que es necesaria gran cantidad de potencia computacional, el consumo energético de la red puede ser muy elevado y aumentar a medida que lo hace la red por lo que puede resultar contraproducente para el medio ambiente.

- **Proof of Stake (PoS)**

El algoritmo de prueba de participación (PoS) nace como alternativa más eficiente, escalable y ecológica al PoW.

En este mecanismo de consenso a diferencia de PoW, no se requiere potencia computacional, sino que será necesario mantener valor dentro de la red. Los nodos que realizan el PoS, son aquellos llamados validadores.

El procedimiento de validación es simple, de forma aleatoria se escoge un nodo para que realice la validación de un bloque, a más cantidad de valor depositada en la red mayor probabilidad de ser elegido para la validación (Ethereum, 2020).

Las principales ventajas respecto a un sistema PoW son el ahorro energético y el menor impacto medioambiental, la proporcionalidad entre nodos validadores dado su carácter de aleatoriedad y una mayor escalabilidad por la falta de un trabajo computacional que consume una cierta cantidad de tiempo. Estos delegados serán los responsables de realizar la validación de los bloques.

Cada partícipe tiene una cantidad de votos relacionada directamente con la cantidad de valor almacenada en la red. Los nodos delegados se repartirán las tareas de validación y ante un comportamiento erróneo de sus funciones, este puede perder su reputación y retirarle la condición de delegado.

- **Delegated Proof of Stake (DPoS)**

Este algoritmo de consenso es una derivación del anterior, el PoS y por ende el concepto y funcionamiento es similar con algunas modificaciones. En el PoS todos los nodos de la red podían ser validadores si de forma aleatoria eran elegidos para la validación, en el DPoS una cantidad limitada de delegados de la red son elegidos mediante la votación de los partícipes de la red (Binance, 2020).

- **Proof of Authority (PoA)**

El algoritmo de consenso PoA se consolida como una alternativa con mayor escalabilidad a los mecanismos PoS consiguiendo un mayor número de transacciones por segundo. Este mecanismo hace uso de la identidad y reputación real de los nodos como garantía de transparencia.

El uso de este algoritmo aumenta la centralización de la red dado que son pocos los nodos con autoridad dentro de la red (bit2me, 2020).

Este mecanismo suele utilizarse en blockchain privadas (Apartado 6.1.6) dado que en estas redes los participantes suelen ser entidades conocidas y la renuncia a cierta cantidad de descentralización no es un gran problema.

6.1.6 Tipos de blockchain

Hay dos tipos principales de Blockchain; blockchain privadas y blockchain públicas. Sin embargo, también se utilizan varias versiones, como los consorcios de Blockchain y las blockchain híbridas. Si consideramos Bitcoin como el precursor de la tecnología blockchain,

podemos afirmar que la blockchain pública fue la primera dado que bitcoin utiliza este tipo de blockchain.

A continuación, se detallarán las características de cada uno de los diferentes tipos de blockchain (Peh, 2018):

- **Blockchain Pública**

Una blockchain pública es una tecnología de tipo DLT, en este tipo de blockchain no existen permisos de ningún tipo y cualquiera es libre de unirse y realizar transacciones dentro de la red. No existen restricciones en cuanto la distribución de la información almacenada en la propia blockchain y cualquiera es libre de hacer copias de dicha información.

Algunos de los beneficios de Blockchain pública son:

- **Acceso libre:** Cualquiera puede unirse a la red y participar en ella.
- **Confianza y transparencia:** El hecho de que los datos almacenados sean públicos y accesibles aporta confianza y transparencia dado que estos no pueden ser modificados.
- **Datos de libre lectura y escritura:** cualquier individuo puede interpretar los datos de Blockchain, componerlos y manipularlos.
- **Mejora de la red:** Al tratarse de una red pública, los partícipes están más involucrados en la mejora de la red.

Algunas de las desventajas que tiene este tipo de red residen en la eficacia y escalabilidad de esta. Las blockchain públicas suelen ser más lentas, esto es debido a que, a mayor número de partícipes, mayor complejidad para llegar al consenso.

- **Blockchain Privada**

A diferencia de la blockchain pública, una blockchain privada se ejecuta en un entorno restrictivo, en una red cerrada. Así mismo esta estará bajo el control de una entidad autorizada.

Este tipo de blockchain está pensada para empresas u organizaciones que deseen utilizar esta tecnología de forma interna, en casos de uso donde se requiera mantener un control sobre la información y la red. En este caso dentro de la red pueden existir niveles de permisos para diferentes usuarios, controles de accesibilidad, autorización, etc. Esta es la principal diferencia, dado que se mantienen las características fundamentales de la blockchain, la confianza, transparencia y seguridad, pero solamente para los usuarios con permisos.

Es posible que, debido a las necesidades del caso de uso, una blockchain privada esté centralizada dado que existe una autoridad que supervisa y controla la red.

- **Velocidad:** Las blockchain privadas son más rápidas que las públicas dado que existe un número menor de nodos por lo que el consenso se alcanza antes.
- **Privacidad mejorada:** Solamente pueden acceder a los registros de blockchain los miembros verificados.
- **Escalabilidad mejorada:** Existe una mayor escalabilidad, ya que pueden existir un número limitado de nodos validadores y por tanto la red no se vea afectada por un aumento del tamaño de la red.

El aspecto clave y diferenciador entre la blockchain pública y la privada reside en el aspecto centralizador y de control mediante permisos por parte de una organización. En este mismo punto encontramos las principales desventajas, la falta de descentralización precede una mayor desconfianza. Por otro lado, la seguridad también se puede ver afectada por el hecho de que existe un menor número de nodos y la red será más susceptible a ciertos ataques como el del 51%.

- **Blockchain Híbrida**

Una blockchain pública pretende combinar aspectos de la blockchain pública con los de la blockchain privada.

En la mayoría de los casos en este tipo de blockchain se mantiene la propiedad de la accesibilidad a los datos que contiene la red al igual que en una blockchain pública, por otro lado, el acceso a la red, las propuestas de mejora o validaciones son realizadas por individuos autorizados para mantener el control de la red. Con esta combinación obtenemos una mayor transparencia y confianza de los datos sin renunciar al control de la red. Esto puede ser útil, por ejemplo, en casos de uso relativos a la administración pública.

- **Consortio Blockchain**

Un consorcio blockchain (también llamada blockchain federada), es un tipo de blockchain en la que los principales participantes o autoridades son distintas organizaciones que colaboran con un objetivo común (Binance, 2021). Estas suelen ser blockchain privadas o híbridas donde estas organizaciones mantienen el control. Este tipo de blockchain es útil cuando varias empresas en un mismo sector pretenden desarrollar una blockchain que aportara un beneficio al sector como puede ser en ámbitos de banca, energía, salud, etc.

6.1.7 Estructura de los bloques

Dependiendo de la blockchain los bloques pueden contener diferentes informaciones, pero de forma general, suelen tener estructuras similares,

En este apartado vamos a analizar la estructura y contenido de un bloque de la red Bitcoin.

Los bloques están formados por 4 grupos de información principales, estos son (Antonopoulos, 2014):

Tabla 1 Estructura de un bloque de Bitcoin

Campo	Descripción
Tamaño del bloque	Tamaño del bloque en <i>bytes</i> .
Cabecera del bloque	Datos correspondientes a la información del bloque.
Contador de transacciones	Número de transacciones incluidas en el bloque.
Transacciones	Registro de transacciones incluidas en el bloque.

La información relevante para el entendimiento de la tecnología blockchain reside en la cabecera del bloque. La información que contiene esta cabecera es la siguiente:

Tabla 2 Cabecera de un bloque de Bitcoin

Campo	Descripción
Versión	Versión del bloque.
Hash anterior	Este corresponde al hash (identificador) del bloque anterior al actual.
Raíz Merkle	Hash de la raíz del árbol de Merkle del bloque.
Timestamp	Hora aproximada de la creación del bloque.
Target Difficulty	Dificultad establecida para el bloque.
Nonce	Contador aleatorio usado para el proceso de minado.

Ahora vamos a realizar una explicación más detallada de cada uno de estos campos que forman la cabecera de un bloque:

- **Versión**

A lo largo del tiempo los bloques de la red han ido evolucionando con el fin de obtener mejoras en la red. Este campo indica la versión del bloque.

- **Hash anterior:**

Este corresponde al hash (identificador) del bloque anterior al actual. Este también suele definirse como “*Parent Hash*” o Hash padre. Este elemento es quien mantiene el orden dentro de la blockchain y como es lógico el hash anterior de un bloque siempre corresponderá al hash del propio bloque anterior. Tal y como podemos apreciar en la siguiente imagen este campo corresponde al enlace entre bloques de la cadena:

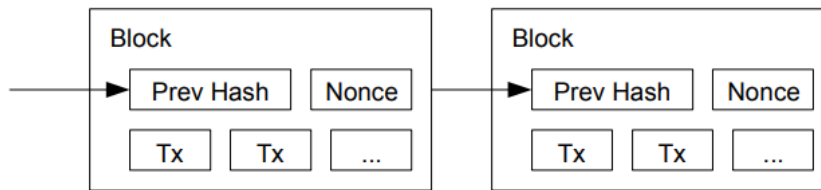


Ilustración 7 Enlace de bloques de una blockchain

- **Raíz Merkle**

Valor de hash que resume todas las transacciones incluidas en el bloque mediante un árbol de Merkle.

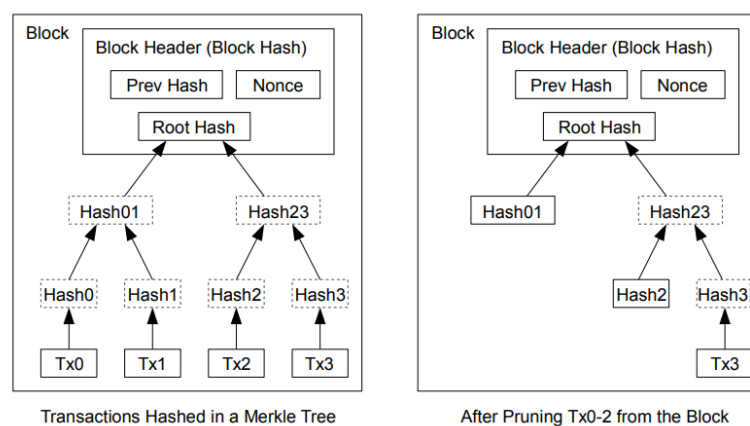


Ilustración 8 Árbol de Merkle contenido en los bloques de una blockchain

- **Timestamp (hora):**

El *timestamp* de un bloque hace referencia al momento en que este es minado o incluido en la cadena. Este campo tiene ciertas utilidades, una de ellas es la identificación única del bloque, ya que dos o más bloques no pueden tener un *timestamp* igual.


- **Target Difficulty:**


Dificultad que habrá en el proceso de minado del bloque. La dificultad se calcula a partir de ciertos parámetros como, por ejemplo, el número de mineros dispuestos a realizar la prueba de trabajo (PoW) para ese bloque, a mayor cantidad de nodos intentando minar, mayor dificultad. A mayor dificultad menor valor tendrá este campo, a menor valor de este campo más difícil será para los nodos mineros encontrar la solución al problema.

- **Nonce:**

Finalmente tenemos el campo "*nonce*", este campo es de vital importancia para el proceso de minado. Como hemos visto en el Apartado 6.1.5, el mecanismo de consenso PoW

En la siguiente imagen podemos observar un bloque de la red Bitcoin utilizando un explorador de bloques de la red:


Explorar >  Bitcoin Explorer > Bloque

 Busque su transacción, una dirección o un bloque

USD ▾

Bloque 672013 ⓘ

USD BTC

Hash	0000000000000000000000063e88cd06633ad4cff8d0284dd1121e20c7a4ee36a7bd 
Confirmaciones	2
Fecha y hora	2021-02-24 19:32
Altura	672013
Minero	Unknown
Número de transacciones	2076
Dificultad	21.724.134.900.047,27
Dirección de raíz Merkle	0be6bf969dc5e657f0c42deccbd80527b616c12209cd883a59e7db537172736b
Versión	0x2000e000
Bits	386.725.091
Peso	3.993.590 WU
Tamaño	1.218.581 bytes
Nonce	1.425.574.119
Volumen de la transacción	2802.05696558 BTC
Recompensa de bloque	6.25000000 BTC
Remuneración por comisión	1.27649733 BTC

Podemos observar que aparecen campos que no hemos visto anteriormente, estos campos no se incluyen en los bloques de manera directa, pero son calculados de forma dinámica por cada nodo. Algunos de ellos son el número de bloque o altura (*Height*) y el hash del bloque , el primero corresponde al número de bloque asignado en orden ascendente desde que se inició la cadena de bloques. También puede definirse como la distancia del bloque con respecto al bloque 0. El segundo corresponde al identificador único de cada bloque, este se calcula con base a la información almacenada en la cabecera y se añade al siguiente bloque en el campo de “Hash anterior”.

6.2 Problemas y vulnerabilidades

La tecnología Blockchain ha atraído una atención significativa debido a sus múltiples casos de uso y su potencial de disrupción. Surgió por primera vez como la tecnología detrás de Bitcoin.

La base de blockchain es una de las explicaciones clave de por qué es tan segura: utiliza redes P2P para almacenar transacciones, se organiza como un archivo de registro digital y se administra como una serie de grupos relacionados o bloques. Todos y cada uno de los bloques están criptográficamente unidos con el bloque anterior y la cadena solamente se puede modificar para agregar un bloque.

Aun siendo blockchain una tecnología segura y resistente, esta no está libre de posibles ataques en determinadas condiciones. Algunos de estos ataques o vulnerabilidades han sido mitigados en versiones o modificaciones posteriores al inicio de Bitcoin.

A menudo la mitigación de una vulnerabilidad de la red mediante nuevos enfoques puede desencadenar nuevas vulnerabilidades que no existían anteriormente por lo que no es extraño observar combinaciones de metodologías entre blockchain de antigua generación con las más modernas.

A continuación, veremos algunos de los problemas que la tecnología blockchain ha mitigado, así como algunos tipos de ataques maliciosos que pueden afectar al funcionamiento e integridad de una blockchain.

6.2.1 Doble Gasto

En los sistemas de dinero digital existe un problema conocido llamado doble gasto. Este proceso consiste en el envío simultáneo de los mismos fondos a diferentes direcciones. Esto puede dar como resultado que un usuario reciba unos fondos que ya han sido gastados en otra parte, por lo que estos no serían válidos. Es por ello por lo que en un sistema como este deben existir medidas para que los usuarios no tengan la capacidad de copiar o replicar fondos para mandarlos de forma simultánea a otros usuarios (Binance, 2021).

En un sistema centralizado esta tarea puede resultar sumamente simple dado que todas las transacciones deben pasar por un mismo nodo supervisor y este puede detectar y anular transacciones de doble gasto.

Desde un enfoque descentralizado, este problema requiere mecanismos más complejos debido a esta falta de la existencia de un nodo central.

En el *White Paper* de Satoshi Nakamoto el doble gasto se aborda como un objetivo primordial, la blockchain resulta ser una tecnología que en sí misma se protege, en parte, de este tipo de vulnerabilidad (Nakamoto, 2008).

La forma en que se evita el doble gasto en una red blockchain como la de Bitcoin es, básicamente, mediante las confirmaciones de los bloques minados por los nodos de la red.

Cuando un nodo es minado este se añade a la red, pero aun así no debemos dar por válidas las transacciones que se incluyen en el bloque y debemos esperar a que los otros nodos confirmen la validez del bloque dando por válidas las transacciones que contenga.

Ponemos por ejemplo una tienda que acepte pagos en Bitcoin, un cliente llega a la tienda y decide comprar un cierto producto, a la hora de pagar decide hacerlo con Bitcoin y manda la cantidad de Bitcoin requerida a la dirección pública de la tienda para hacer el pago. Dado que hacer esperar al cliente a que se confirme la transacción no es una opción dado el tiempo que puede suponer el cliente se va de la tienda con el producto. Una vez fuera el cliente realiza una transacción de los Bitcoins a una de sus direcciones públicas con una comisión mayor para que esta sea aceptada antes que la de la tienda e incluida en la red, invalidando la transacción anterior. Este tipo de ataque se llama ataque de carrera.

6.2.2 Ataque del 51%

El ataque del 51% es quizás el más famoso debido a que se focaliza en los pilares fundamentales de la blockchain como son las redes p2p de libre acceso o los mecanismos de consenso. Como hemos visto anteriormente la validación de los bloques la realizan los nodos de minería de la red aportando un esfuerzo computacional para resolver problemas. Dada la posibilidad de que cualquier usuario de la red pueda participar en el proceso de minado la potencia total se distribuye entre estos usuarios. El ataque del 51% es básicamente la centralización de la potencia de minado por parte de una sola organización, en caso de que esto ocurriera, esta organización sería capaz de excluir, modificar o revertir el orden de las transacciones de la red pudiendo desencadenar problemas de doble gasto maliciosos.

Este tipo de ataques resultan improbables en redes muy grandes dado que el poder llegar a poseer el 51% de la potencia resultaría muy difícil y económicamente desincentivador.

6.2.3 Ataque Sybil

Un ataque Sybil es aquel donde distintos nodos en principio, independientes, actúan bajo el control de un único usuario. Así pues, un ataque Sybil se realiza cuando un usuario trata de obtener el control de la red mediante la creación de múltiples cuentas o nodos de la red a la vez que este intenta ocultar que estos nodos son propiedad del mismo usuario (Wikipedia, 2020).

Este tipo de ataques busca principalmente conseguir cierta influencia sobre las decisiones que se toman en una red.

Si mediante este ataque un usuario consigue una gran cantidad de identidades falsas en la red este podría manipular votaciones o incluso superar el 51% de la red pudiendo realizar un ataque del 51%.

Los protocolos de consenso como por ejemplo el PoW, suponen una capa de seguridad ante estos tipos de ataques al requerir que por cada identidad o nodo deba aportarse una cierta

cantidad de potencia computacional lo que requiere de un desembolso económico por parte del atacante.

Otra posible forma de prevención contra ataques Sybil es el uso de un sistema de reputación por el cual se entrega poder en la red a aquellos usuarios más respetables.

6.2.4 Ataque Erebus

El ataque Erebus es un ataque basado en la denegación de servicio (DDoS) y tiene la capacidad de obtener el control de una red hasta volverla inutilizable.

El objetivo de este ataque es interrumpir el funcionamiento de una red haciéndola inaccesible para los usuarios. Esto se realiza mediante la partición o división de la red P2P que compone la blockchain, esto se realiza mediante la manipulación de las conexiones de los nodos de la red mediante el uso de técnicas de tipo *man-in-the-middle*. El atacante se va haciendo con el control de las conexiones de la red hasta llegar a un punto donde le sea posible realizar cualquier acción maliciosa en la red como un ataque del 51%.

Este tipo de ataques son factibles dado que aun tratarse de una red P2P, esta hace uso de Internet para intercomunicar todos los nodos de la red. Esto hace que las conexiones puedan manipularse suplantar identidades y aislar nodos de la red haciéndoles creer que siguen en ella (Tran et al., 2020).

6.3 Aspectos legales

Los negocios basados en Blockchain están viviendo un crecimiento exponencialmente en los últimos años. Una empresa que aplica tecnologías Blockchain a procesos/metodologías o sistemas mejora su valor y confianza. La blockchain es una tecnología por lo que su uso no se puede regular, no obstante, si se pueden regular las actividades relacionadas o que hacen uso de esta tecnología.

Durante los últimos años, debido a la popularización de los proyectos basados en blockchain las regulaciones han sido un tema de debate en este ámbito. En este punto es importante diferenciar blockchain como tecnología de las llamadas criptomonedas. Las criptomonedas son tokens pertenecientes a una blockchain tal y como lo son los bitcoins, estos tokens suelen intercambiarse por dinero fiduciario como puede ser el euro o el dólar estadounidense. Estas criptomonedas tienen distintas regulaciones dependiendo de los gobiernos llegando incluso a considerarse activos prohibidos en países como, por ejemplo, Bolivia (The Law Library of Congress, 2018). Al tratarse de un fenómeno relativamente novedoso puede ser difícil determinar un ámbito jurídico o regulatorio tradicional.

En el marco internacional ningún país reconoce ninguna criptomoneda como una moneda fiduciaria o de curso legal al igual que tampoco son considerados de forma explícita como activos financieros.

7 Network Access Control

En este apartado se realizará el estudio de la tecnología NAC y los protocolos que la componen, se realizará un enfoque técnico en el que se tratarán todos los aspectos relacionados con el acceso a la red. Se establecerá un orden de estudio por niveles, empezando por una explicación generalizada de los sistemas NAC para posteriormente explicar los protocolos tanto del nivel más bajo como a los niveles superiores.

7.1 Tecnología NAC

El control de acceso a la red es el proceso de control de acceso a la red, cuando hablamos de un sistema NAC, nos referimos al sistema que implementa esta funcionalidad y que tiene la capacidad, mediante el uso de varios protocolos, aplicar un conjunto de políticas para decidir quién y quien no puede acceder a la red. Estas políticas pueden aceptar o rechazar el acceso de un usuario y/o decidir que puede y que no puede hacer este usuario dentro de la red. Esto es posible asignando una VLAN al usuario o aplicándole ACL.

Muchos de los grandes fabricantes de electrónica de red disponen de sus propias soluciones NAC como Cisco ISE, Aruba Clearpass o FortiNAC. Existen otras empresas especializadas en productos NAC como pueden ser openNAC o PacketFence.

Una solución NAC, aunque no sea necesario, puede hacer uso de protocolos ya existentes en el mercado como el IEEE 802.1x. Esto nos aporta facilidad y estandarización en los flujos de trabajo del sistema NAC. Algunos de los casos o escenarios donde la implantación de un sistema NAC resulta de gran utilidad pueden ser:

- **Acceso de usuarios:** Controlar que usuarios pueden acceder a la red y a que recursos pueden acceder, este es el caso de uso básico de cualquier implantación de sistema NAC.
- **Acceso a usuarios invitados:** Cuando los usuarios invitados quieren acceder a la red, es importante controlar que estos estén limitados a ciertos recursos y se les bloquee el acceso a recursos críticos de las organizaciones.
- **Acceso Remoto:** Una herramienta NAC nos permite la autenticación y autorización de usuarios que estén accediendo a través de, por ejemplo, una VPN corporativa.
- **Segmentación de red:** La capa o proceso de autorización de un NAC nos permite el poder mejorar la segmentación de la red mediante, por ejemplo, la asignación dinámica de VLAN a los clientes de la red.
- **Cumplimiento:** Una de las utilidades de los sistemas NAC es la verificación de ciertos aspectos que los clientes deben cumplir para poder acceder a la red, por ejemplo, el tener instalado un antivirus o el firewall activado.
- **BYOD:** Cada vez más las organizaciones permiten a sus empleados utilizar sus propios dispositivos en las redes corporativas, estos equipos no están controlados por las organizaciones por lo que es importante tener un control de aquellos que se conectan y que estos cumplan ciertos requisitos antes de brindarles acceso a ciertos recursos.

- **Uso de dispositivos IoT:** Los dispositivos de internet de las cosas son cada vez más utilizados en todos los ámbitos y pueden convertirse en un riesgo de ciberseguridad al pasar por alto algunos controles de seguridad tradicionales.

Como ya hemos comentado, los sistemas NAC pueden apoyarse en el uso de protocolos estandarizados para la implementación, aunque no sea necesario. Podemos determinar los tipos de NAC (Bradford Networks, 2013, p. 8,9) basados en la arquitectura que estos usan:

- **Basados en 802.1x:** Una gran cantidad de soluciones NAC se basan en el uso del protocolo IEEE y agregan capas para complementar la solución como reglas de cumplimiento para los dispositivos. Esta implementación es muy corriente dado la gran extensión que tiene el protocolo 802.1x en la mayoría de los equipos implicados en las organizaciones que requieren el uso de un NAC.
- **Out-of-band:** Esta arquitectura es similar a la 802.1x con la diferencia de que este sistema no depende de la necesidad que los dispositivos finales deban tener compatibilidad con protocolos 802.1x.
- **Inline:** Una implementación NAC *Inline*, conlleva que el sistema NAC se encuentre en medio de la ruta que los dispositivos tienen para acceder a los recursos de red. De esta forma todo el tráfico debe pasar por el sistema NAC bloqueando o permitiendo el tráfico. Esta arquitectura conlleva problemas de escalabilidad debido a que es necesario procesar todo el tráfico que se genere entre los dispositivos y los recursos a los que se les brinda acceso.
- **Client-side:** Las arquitecturas basadas en el cliente las funcionalidades NAC se desplazan al lado del cliente a través del uso de agentes que se ejecutan en los dispositivos finales. La aplicación de políticas se realiza en el propio dispositivo al igual que las comprobaciones de cumplimiento. Esta arquitectura se ve limitada por la necesidad imperativa del uso de un software que actúa como agente en los dispositivos.
- **Híbrida:** La necesidad del uso de varias de las arquitecturas expuestas anteriormente constituye una arquitectura híbrida en la que por ejemplo en una parte de la red es necesario implementar una arquitectura *Inline* y en otra zona una arquitectura *Out-of-band*. Estas son las más complejas de implementar.

En un sistema NAC, el uso de Agentes nos permite conocer mucha más información relativa a los dispositivos que se conectan a la red a través de la realización de escaneos del sistema que nos reportaran información sobre estos dispositivos finales. Esta información puede utilizarse para realizar políticas de cumplimiento para el acceso a la red. Aunque el escaneo de información no es la única funcionalidad, esta suele tener un peso importante como funcionalidad. Existen dos tipos principales de agentes (Bradford Networks, 2013, p. 9):

- **Agentes Instalables:** Un agente instalable se mantiene activo en el equipo final como servicio después de ser instalado. Este se ejecuta en segundo plano recopilando información y cambios en el equipo a medida que va notificando dichos cambios entre el usuario final y el servidor de autenticación.

- **Agentes Solubles:** Los agentes solubles suelen funcionar a través de una ejecución única posterior al acceso a la red la cual escaneara la información del equipo y la mandara al servidor para las comprobaciones de cumplimiento.

Una vez detallado el concepto de un sistema NAC detallaremos los protocolos usados para la implementación de estos sistemas en la mayoría de los casos.

7.2 Protocolos AAA

AAA no se trata de un protocolo en sí, más bien representa un conjunto o tipos de protocolos que controlan ciertos aspectos sobre el acceso a recursos informáticos. Estas tres A se describen como:

- **Authentication** (Autenticación)
- **Authorization** (Autorización)
- **Accounting** (Contabilidad)

Cada uno de estos procesos representa un paso para el acceso a un recurso o recursos específicos y se desencadenan de forma sucesiva tras completar el proceso previo.

El esquema del modelo AAA en una red es el siguiente (Meb & Cisco Systems, 1999):

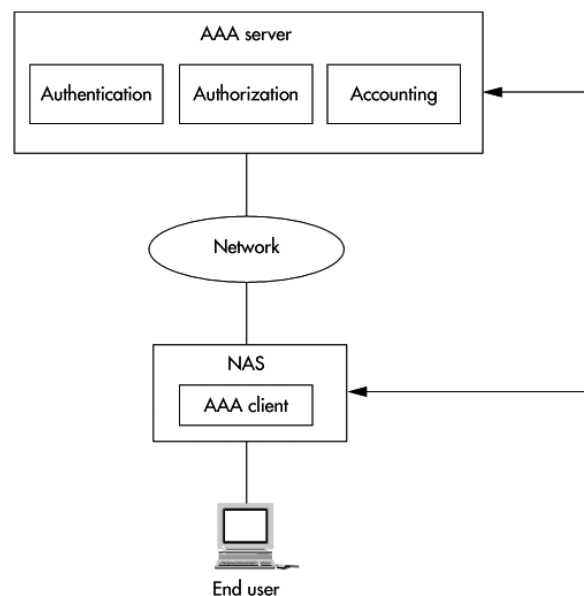


Ilustración 10 Arquitectura del modelo AAA

El usuario final se conecta a un NAS, este es un dispositivo de red, normalmente un *switch*. Este actúa como autenticador de los dispositivos finales, recopila la información de autenticación y se comunicará con el servidor AAA, normalmente un servidor RADIUS, al que redirigirá dichas peticiones a través de la red.

7.2.1 Authentication

El primer paso corresponde a la Autenticación, este es el proceso por el cual se identifica a un

usuario. Este proceso suele realizarse a través de una petición de credenciales por parte del autenticador, posteriormente, el usuario manda dichas credenciales al autenticador para que este las valide mediante el sistema que convenga en cada caso, puede realizarse mediante una base de usuarios local, un directorio activo, etc. En caso de que las credenciales no sean validadas, a este usuario se le deniega el acceso a la red, en caso contrario, se realizaría el siguiente proceso, la autorización.

El servidor AAA, procesa la petición y comunica al NAS si el dispositivo final se autentica (*Accept*) o no (*Reject*). Finalmente, el cliente AAA notificará el resultado al dispositivo final.

7.2.2 Authorization

Una vez hemos verificado que el usuario está habilitado para acceder a la red, es decir, que sus credenciales son válidas, debemos determinar que puede y que no puede hacer o a que recursos puede acceder dentro de esa red, este es el proceso de autorización.

Esta autorización suele ejecutarse mediante políticas que dependiendo de ciertas condiciones determinaran a que recursos puede acceder el usuario. En el caso de las redes y sistemas NAC, la autorización suele determinar de la asignación a una VLAN concreta o la asignación de ACL que restringen el tráfico del dispositivo.

Cuando el dispositivo se ha autenticado, el servidor AAA comunicara al NAS los parámetros de conexión que se deben asignar al dispositivo final.

7.2.3 Accounting

El paso final del proceso de AAA la contabilidad, este proceso se inicia una vez se ha autorizado al usuario y no finaliza hasta que se termina la sesión de dicho usuario. Durante una sesión, los usuarios acceden a los recursos permitidos y generan tráfico tanto de recepción como de transmisión. Toda esta información se recopila y se puede almacenar en varios formatos como *logs* o estadísticas, este es el proceso de contabilidad. En el entorno de red, la contabilidad nos aporta información variada como, por ejemplo, la IP que recibe un dispositivo por DHCP, el fin de una sesión (*logout*), etc.

Esta contabilidad será recopilada por el servidor NAS y posteriormente enviada al servidor AAA.

7.3 Protocolo 802.1x

El protocolo IEEE 802.1x es el protocolo más extendido para la autenticación en redes. Este protocolo está basado en la autenticación por puertos y nos permite bloquear de la transmisión y recepción de paquetes de dispositivos no autenticados. 802.1x nos permite definir una capa intermedia entre el protocolo RADIUS y EAPOL los cuales encapsularan los paquetes de tipo EAP.

EAP es el protocolo que nos permite la transmisión de la información que contiene los datos de identificación de los usuarios.

Este protocolo es válido tanto para redes cableadas como inalámbricas. Una red con 802.1x implementado dispone de un servidor RADIUS, esta comprueba que las credenciales de los usuarios son válidas y abre los puertos de un dispositivo de red para el acceso a la red. El servidor RADIUS suele tener comunicación con el directorio corporativo mediante LDAP o SAML para autenticar dichos usuarios.

El protocolo 802.1x requiere la existencia de 3 elementos básicos para su implementación, estos son(Data Network Resource, 2009):

- **Suplicante:** Los dispositivos finales que quieran acceder a la red mediante 802.1x deben poder ejecutar un software o servicio llamado suplicante que se encarga de mandar las tramas EAPOL/EAP para la autenticación. Este es quien inicia el flujo de autenticación.
- **Autenticador:** El autenticador es el dispositivo de red donde los dispositivos finales se conectan (generalmente switch o APs). Este se encuentra entre el suplicante y el servidor de autenticación y actuará de intermediario entre los dos.
- **Servidor de autenticación:** Este servidor (generalmente un servidor RADIUS) es quien recibe y responde a las peticiones para acceder a la red.

En la siguiente figura podemos observar la arquitectura básica de una implementación 802.1x:

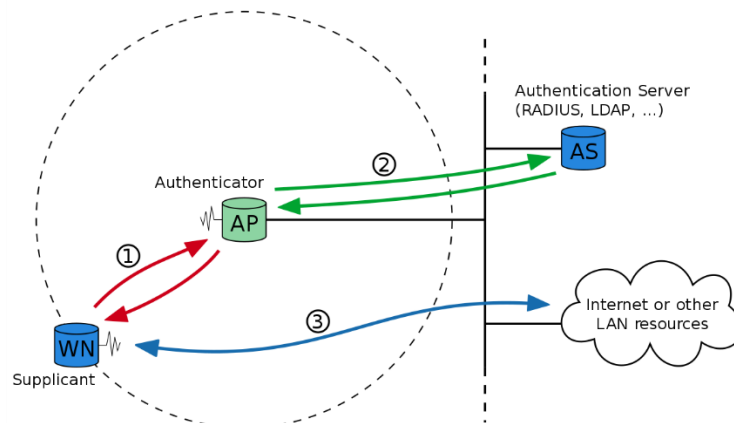


Ilustración 11 Arquitectura 802.1x

En la anterior imagen podemos observar el flujo generalizado del protocolo 802.1x este se compone de tres pasos:

1. El suplicante se comunica con el autenticador, el autenticador le pregunta las credenciales al suplicante y este se las entrega con un paquete EAP encapsulado en EAPOL.
2. El autenticador recibe las credenciales del suplicante y las redirige hacia el servidor de autenticación, los paquetes son EAP encapsulados en RADIUS. El servidor de autenticación verifica las credenciales a través de una base de datos local o mediante otro método compatible como un directorio activo.
3. Si la autenticación es válida se le concede acceso a la red al dispositivo final.

7.3.1 Autenticación con suplicante

Como hemos visto anteriormente, para que sea posible una autenticación mediante 802.1x, es necesario el uso de un suplicante por parte del dispositivo final. En este apartado veremos más profundamente todos los pasos que se ejecutan al realizar la autenticación por suplicante.

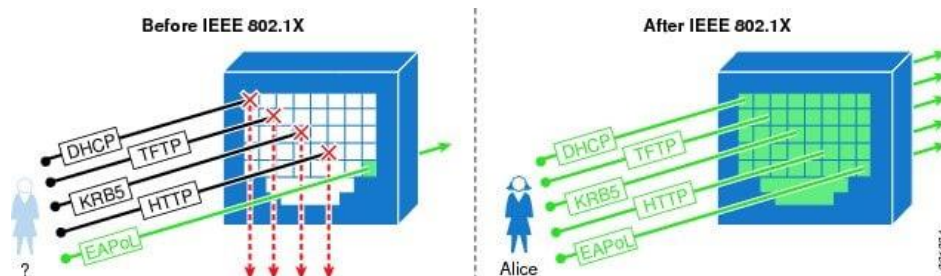


Ilustración 12 Tráfico 802.1x en un puerto de Switch

Cuando un nuevo dispositivo se conecta a un puerto del dispositivo de red, en un principio el dispositivo no es conocido y se bloquea todo el tráfico, solo se permiten los paquetes encapsulados en EAPOL para realizar la autenticación. Una vez se ha realizado el proceso de autenticación el puerto se libera permitiendo todo el tráfico que se haya autorizado.

En el siguiente diagrama de secuencia muestra el proceso de autenticación con suplicante (Cisco Systems, 2018):

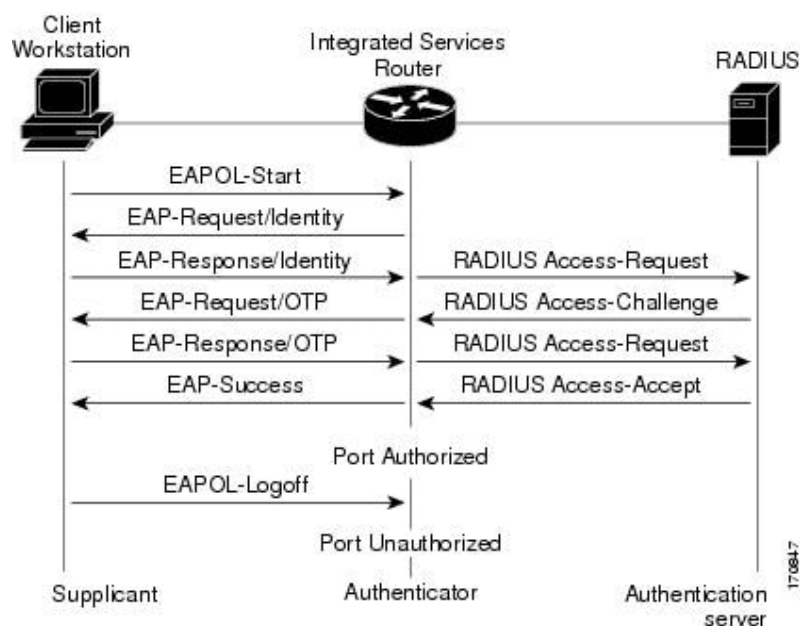


Ilustración 13 Diagrama de secuencia autenticación con suplicante

Al conectar el dispositivo final o cliente, este inicia la autenticación cuando el suplicante manda un (*EAPOL-Start*), el dispositivo de red (actuando como autenticador) le pregunta al suplicante la información para acceder a la red (*EAP-Request/Identity*) y este después de introducir dicha información la mandara hacia el autenticador (*EAP Response/Identity*). El autenticador redirige la información al servidor de autenticación para que este las valide (*RADIUS Access-Request*), se realiza un *challenge* en caso de requerirse más información y

posteriormente se responde a la petición con un *RADIUS Access-Accept* en caso de ser una autenticación válida o un *RADIUS Access-Reject* en caso de no serlo.

7.3.2 Autenticación por Mac Address Bypass

Es probable que en cualquier implantación de red existan dispositivos finales los cuales no disponen o no son capaces de ejecutar un servicio de suplicante como, por ejemplo, impresoras, dispositivos VoIP, etc. Estos dispositivos no podrán acceder a la red si no existe la opción de realizar un acceso por MAB.

Cuando un dispositivo se conecta a un puerto, el autenticador espera a que se inicie una autenticación al recibir una trama EAPOL. En caso de no ser así y excedido un cierto tiempo, el autenticador iniciará una autenticación por MAB.

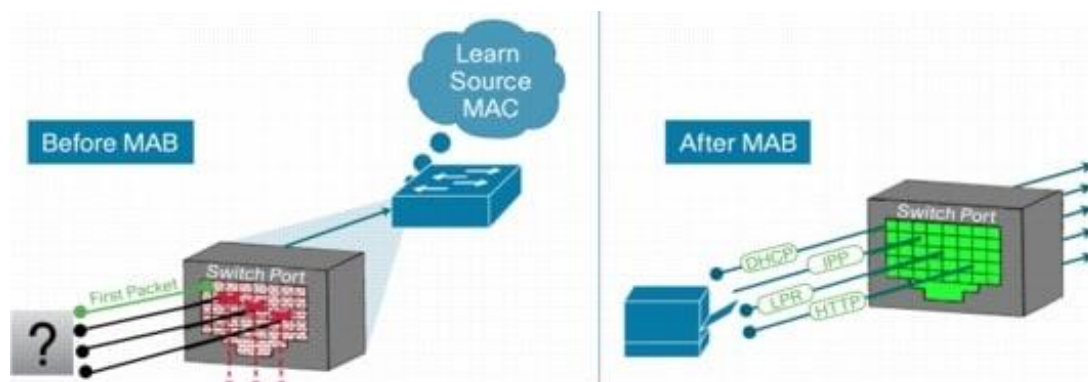


Ilustración 14 Tráfico MAB en un puerto de Switch

En un principio, cuando el dispositivo no es conocido, se bloquea todo el tráfico. El autenticador analiza un paquete enviado por el dispositivo final en busca de una MAC. Una vez se ha aprendido la MAC, el puerto se abre y se permite el tráfico con un filtrado para dicha MAC.

Las autenticaciones por MAB siempre resultarán válidas, es decir, un dispositivo siempre tendrá una autenticación satisfactoria.

En el siguiente diagrama de secuencia muestra el proceso de autenticación por MAB (Cisco Systems, 2018):

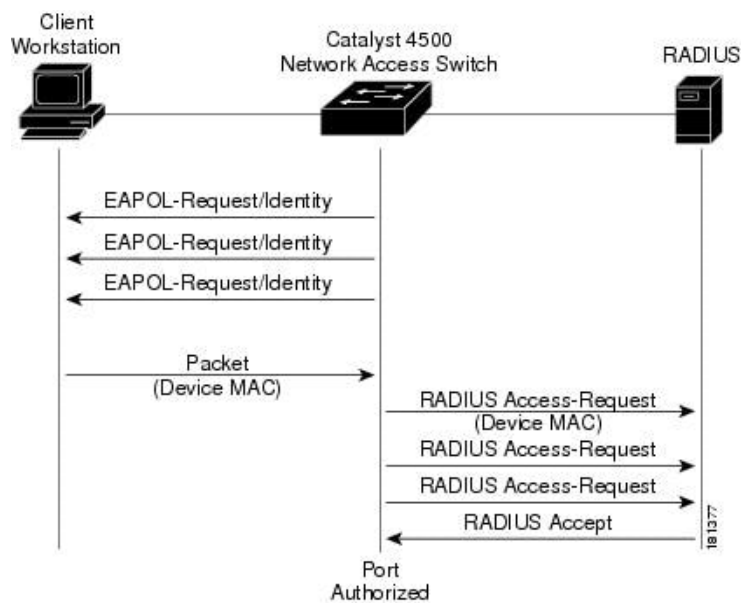


Ilustración 15 Diagrama de secuencia autenticación por MAB

Como podemos ver, en un principio, el dispositivo de red (autenticador) intenta iniciar una autenticación por 802.1x mediante la petición de identidad (*EAPOL-Request*). Dependiendo de la configuración del dispositivo de red mandará una cierta cantidad de peticiones antes de determinar que no existe suplicante en el dispositivo por lo que debe realizarse un MAB. Pasados estos intentos, el dispositivo de red cojera un paquete que contenga la MAC de dispositivo final o cliente, este mandara la MAC al servidor de autenticación (*RADIUS Access-Request*) y el servidor responderá con la aceptación de dicha MAC (*RADIUS Accept*) por lo que el puerto de dispositivo de red empezara a permitir el tráfico a la red.

7.3.3 Flujo del protocolo 802.1x en sistemas NAC

Anteriormente hemos visto el flujo de las autenticaciones en el protocolo 802.1x, en este diagrama de flujo podremos observar con más detalle el proceso completo de 802.1x en una implementación de sistema NAC:

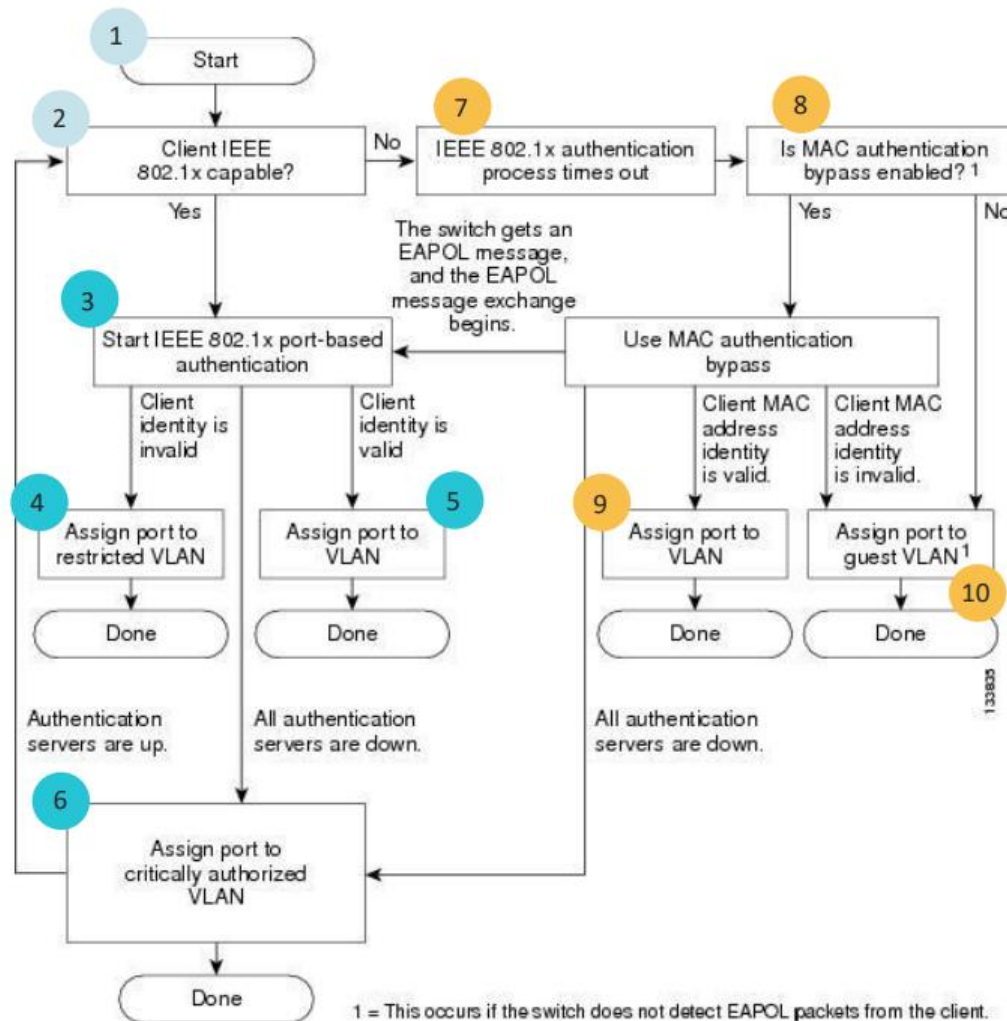


Ilustración 16 Diagrama de flujo del protocolo 802.1x

1. Al conectar un dispositivo a la red, se produce el inicio de la ejecución del protocolo 802.1x.
2. La primera tarea que realizan los dispositivos de red es comprobar que el dispositivo conectado dispone de un servicio de suplicante. Esto se comprueba viendo si se recibe un paquete de tipo EAPOL.
3. En caso de que exista un suplicante configurado en el dispositivo, se inicia el proceso de autenticación. El autenticador (switch) enviara una petición de autenticación al servidor de autenticación y se validaran en este servidor contra el *back-end* de autenticación (base de datos local, *Active Directory*, etc.)
4. En caso de que las credenciales no sean válidas, es posible asignar por defecto ciertos parámetros a dicha conexión, como, por ejemplo, una VLAN restringida.
5. Una vez validada la autenticación, se ejecuta el proceso de autorización donde mediante políticas, se determinarán los parámetros aplicables a dicha conexión y serán devueltos al dispositivo de red mediante RADIUS para que los aplique.
6. En caso de no ser posible la validación de autenticación debido a que no existe o no sea posible la comunicación con el servidor de autenticación, es posible asignar por

defecto ciertos parámetros a dicha conexión, como, por ejemplo, una VLAN restringida.

7. En caso de agotarse el tiempo o el máximo de solicitudes EAPOL, el autenticador concluye que no existe suplicante configurado en el dispositivo final.
8. Al no existir un suplicante en el cliente, se procede a realizar una autenticación por MAB (siempre que esté configurada en el autenticador).
9. Como ya hemos visto, las autenticaciones por MAB siempre obtendrán una respuesta válida por lo que se asignarán los recursos correspondientes.
10. Anteriormente hemos dicho que las autenticaciones por MAB siempre se dan por válidas, esto nos genera un problema, ya que cualquier dispositivo podría acceder a la red por lo que debemos controlar que recursos asignamos a una autenticación por MAB, esto lo podemos realizar con la autorización denegando el acceso dependiendo de la MAC.

7.4 Protocolo EAP

El EAP es el protocolo que se utiliza para el intercambio de información entre el autenticador y el dispositivo final (suplicante). Este protocolo se establece en la capa 1 a través de PPP (Point-to-Point Protocol) y, por tanto, para poder realizar una comunicación, EAP debe encapsularse en EAPOL (EAP Over Lan) para transmitirse a nivel de enlace (capa 2).

Las tramas EAP tienen el siguiente formato (Lee, 2017):

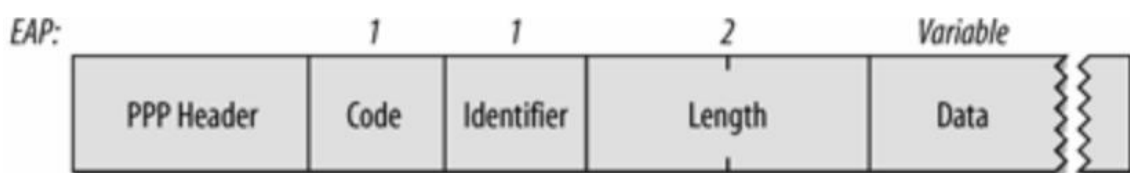


Ilustración 17 Trama del protocolo EAP

Como ya hemos comentado EAP se ejecuta en PPP por eso la cabecera de la trama corresponde a este protocolo. Los otros campos de la trama son (Father, 2017):

- **Código** (1 byte): Corresponde al tipo de paquete EAP, este puede ser *Request*, *Response*, *Success* o *Failure*.
- **Identificador** (1 byte): Identificador que relaciona las peticiones (*Requests*) y respuestas (*Responses*)
- **Longitud** (2 bytes): Longitud total del paquete EAP en bytes.
- **Datos** (variable): El campo de datos tiene un formato variable que depende del tipo de trama (código)

7.4.1 EAPOL

Como ya hemos comentado, para poder transmitir los paquetes EAP sobre una red LAN necesitamos encapsular los paquetes en una trama que permita la transmisión en capa 2.

Las tramas EAPOL tienen el siguiente formato (Lee, 2017):

a) EAPOL on Ethernet

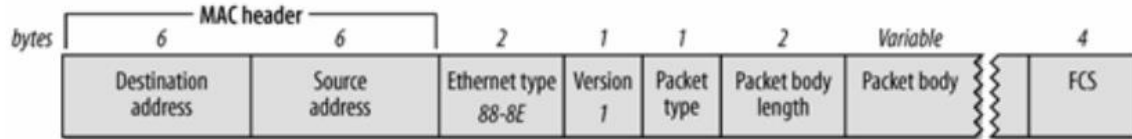


Ilustración 18 Trama del protocolo EAPOL

Los campos que componen esta trama EAPOL son los siguientes:

- **Cabecera MAC:** contiene la dirección de destino (6 bytes) y la dirección de origen (6 bytes) del paquete.
- **Tipo de Ethernet** (2 bytes): Código que hace referencia al tipo de paquete Ethernet, en el caso de EAPOL: 88-8e.
- **Versión** (1 byte): Existen dos versiones en 802.1x por lo que el valor puede ser 1 o 2.
- **Tipo de paquete** (1 byte): Tipo de paquete EAPOL, estos pueden ser EAP-Packet, EAPOL-START, EAPOL-Logoff, EAPOL-Key o EAP-Encapsulated-ASF-Alert.
- **Longitud de la trama**(2 byte): Longitud total de la trama EAPOL.
- **Cuerpo de la trama**(variable): Este es campo es el que encapsula el paquete EAP.

7.4.2 Tipos de EAP

El protocolo EAP dispone de varias opciones de ejecución del proceso de autenticación. Estos tipos han ido evolucionando y se han creado nuevos tipos que mejoraban vulnerabilidades de anteriores por lo que actualmente muchos de ellos no se usan de forma frecuente. Algunos de los métodos que podemos encontrar en la actualidad son (Intel Corporation, 2021):

- **EAP-MD5:** Uno de los métodos de autenticación más sencillos es el EAP-MD5. Esta autenticación se produce de forma unidireccional, es decir, solo el suplicante debe enviar las credenciales al autenticador encriptadas en MD5.
- **EAP-TLS:** A diferencia del anterior, el EAP-TLS requiere de una autenticación mutua entre el suplicante y el autenticador. Esta autenticación mutua se realiza mediante certificados en ambos lados.
- **EAP-TTLS:** El método EAP-TTLS consta de dos partes, primero se establece una autenticación mutua entre ambas partes a través de la CA del servidor, para, posteriormente crear un túnel seguro para la segunda parte, la autenticación contra el servidor.
- **PEAP:** PEAP no es un método propiamente dicho, es más bien una encapsulación. Al igual que EAP-TTLS, PEAP consta de dos partes, la primera es de igual forma el establecimiento de un túnel seguro entre autenticador y suplicante a través de la clave pública del servidor, se crea un túnel TLS entre ambos y se realiza el intercambio de información.
- **EAP-FAST:** A diferencia de EAP-TTLS o PEAP, EAP-FAST realiza la autenticación mutua a través de una PAC (credencial de acceso protegido), estas pueden generarse de forma manual o automática y no requiere que el servidor utilice certificados.

7.5 Protocolo RADIUS

La comunicación entre autenticador y servidor de autenticación se realiza mediante el protocolo RADIUS. RADIUS es un protocolo para la autenticación y autorización basado en una arquitectura cliente-servidor. En el caso de NAC, el cliente es el NAS que suele ser un dispositivo de red de tipo switch el servidor es el servidor de autenticación RADIUS, este puede implementarse de distintas formas, por ejemplo, una máquina servidor corriendo un servicio de RADIUS como, por ejemplo, FreeRADIUS.

Cuando un autenticador recibe una petición de un cliente final, este viene encapsulada en EAPOL, el autenticador reencapsula esta petición en el protocolo RADIUS y la redirige al servidor de autenticación para su validación.

RADIUS no solo ejecuta la autenticación de clientes, sino que también puede realizar la autorización y contabilidad de dichos clientes durante su sesión. Por eso, podemos decir que RADIUS es un protocolo de tipo AAA.

Los tres pasos AAA que implementa RADIUS son (Data Network Resource, 2009):

- **Autenticación:** El cliente envía una solicitud de acceso a la red en la capa de enlace como un paquete EAP encapsulado en EAPOL. Esta solicitud contiene unas credenciales o un certificado. El autenticador empaqueta el EAP en formato RADIUS y lo envía a un servidor RADIUS. El servidor RADIUS valida dichas credenciales y decide si autentica o no al usuario. Los mensajes utilizados son *Access Reject*, *Access Challenge* (más información) o *Access Accept*.
- **Autorización:** El servidor RADIUS determina los parámetros de acceso a la red para dicho cliente, es decir, lo que el usuario puede hacer en la red. Esta autorización se puede realizar mediante el establecimiento del dispositivo en una determinada VLAN o aplicación de ACL, estos parámetros se enviarán al autenticador o dispositivo de red para que los aplique a la conexión.
- **Contabilidad:** Cuando un usuario se autentica y autoriza correctamente, se inicia una sesión de contabilidad donde el dispositivo red o cliente RADIUS realizara un seguimiento de esta sesión como por ejemplo la duración de esta hasta recibir finalizador de sesión.

Una trama de tipo RADIUS tiene el siguiente formato:

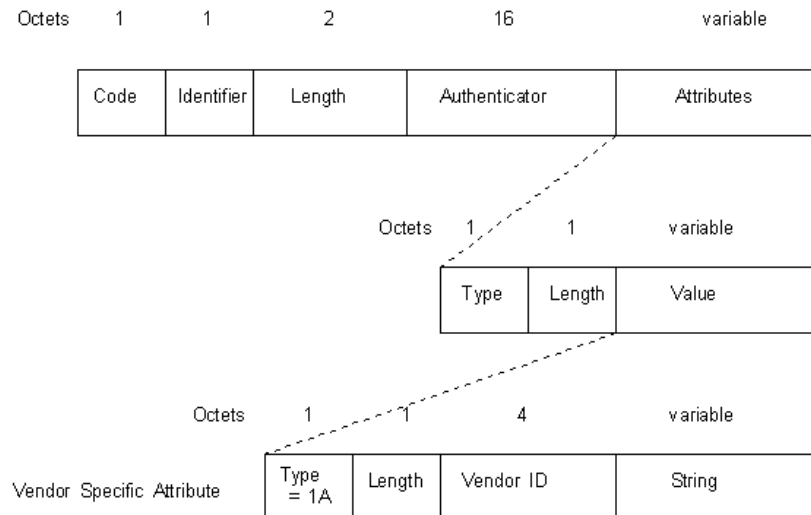


Ilustración 19 Trama del protocolo RADIUS

La trama se compone de los distintos paquetes, estos son:

- **Código** (1 byte): Este indica el tipo de paquete RADIUS, estos pueden ser:
 - 1 - *Access-Request*
 - 2 - *Access-Accept*
 - 3 - *Access-Reject*
 - 4 - *Accounting-Request*
 - 5 - *Accounting-Response*
 - 11 - *Access-Challenge*
 - 12 - *Status-Server*
 - 13 - *Status-Client*
- **Identificador** (1 byte): Identificador que relaciona las peticiones (*Requests*) y respuestas (*Responses*).
- **Longitud** (2 bytes): Longitud total de la trama RADIUS.
- **Autenticador** (16 bytes): Información que se utiliza para la autenticación entre cliente-servidor del protocolo RADIUS.
- **Atributos** (variable): Este contiene la información relacionada con los atributos de tipo RADIUS que se intercambian entre cliente-servidor.
 - Tipo (1 byte): Indica el tipo de atributo que se está mandando, estos pueden ser varios como *NAS-Port* para indicar el puerto del cliente NAS, *Filter-ID* para asignar filtros como ACL a la conexión u otros. En estos también se incluyen los mensajes EAP cuando estos se encapsulan en RADIUS (*EAP-Message*) (Podemos ver una lista completa de atributos RADIUS en la documentación de FreeRADIUS).
 - Longitud (1 byte): Longitud total de la Trama de Atributos.
 - Valor (variable): En este paquete se encapsula la información específica del paquete, este puede ser por ejemplo el paquete EAP encapsulado (*EAP-Message*) o un atributo específico de *Vendor*, cada *Vendor* tiene su propia forma de tratar estos atributos, por lo que debe indicarse el *Vendor ID* correspondiente en la trama. Esta trama incluye el tipo, la longitud de la trama, el *Vendor ID* y el *String* correspondiente al valor del atributo.

7.6 Soluciones NAC: openNAC

En el mercado existen multitud de productos de tipo NAC muchos de ellos corresponden a grandes fabricantes de electrónica de red como Clearpass de Aruba o FortiNAC de Fortinet. Además de las grandes empresas existen proyectos especializados en productos NAC como el caso de PacketFence u openNAC.

En este apartado hablaremos del producto openNAC que es un producto *open source* de la empresa OpenCloud Factory.

openNAC es un control de acceso a la red de código abierto que proporciona acceso seguro para LAN/WAN. Permite la aplicación de políticas de acceso flexibles basadas en reglas. Funciona con una amplia gama de clientes (Windows, Mac, Linux, otros ...) y dispositivos de red (Extreme Networks, Cisco, Alcatel y 3Com). Se basa en componentes de código abierto bien probados y en nuestro propio desarrollo. Extensible y muy flexible, es fácil incorporar nuevas funcionalidades. Está abierto a integrarse con plataformas actuales como contabilidad, gestión de activos, autenticación, sistemas de detección de intrusiones en la red, ...

Además del control de acceso a la red principal, openNAC tiene servicios de valor agregado como configuración y descubrimiento de red, respaldo de la configuración de dispositivos de red y monitoreo de la red. (openNAC, 2014)

OpenNAC nació como una simple aplicación NAC y a lo largo de los años se han ido integrando diferentes funcionalidades tanto para cumplimentar la base fundamental de NAC como para expandir sus aplicaciones en otras aplicaciones sobre el control de redes. Este es un sistema modular por lo que se permite desplegar solamente alguna de sus funcionalidades una combinación o el total de ellas.

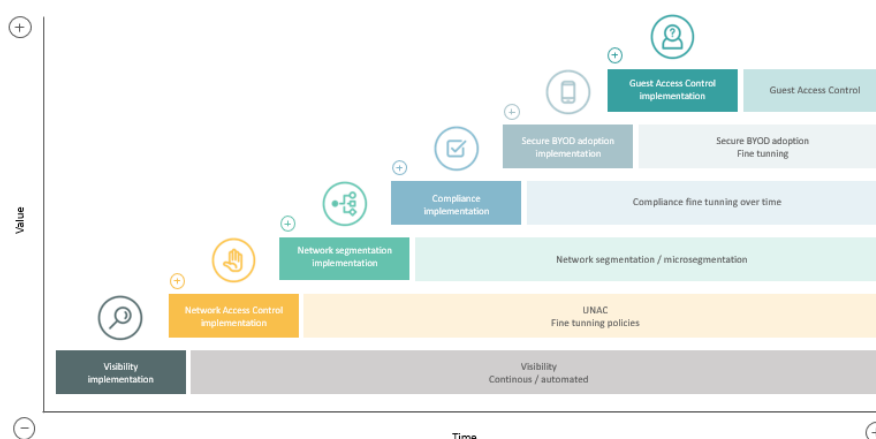


Ilustración 20 Funcionalidades sistema openNAC

En la anterior imagen observamos algunas de las funcionalidades de openNAC con el correspondiente valor que estas pueden aportar al control de la infraestructura de red. Estas funcionalidades son:

- **Visibilidad:** openNAC nos permite descubrir y perfilar todos aquellos dispositivos que se encuentran conectados a la red a través de diferentes métodos de descubrimiento.
- **Control de acceso:** La funcionalidad básica del sistema es la de NAC que nos ayuda a controlar quien puede y quien no acceder a la red.
- **Segmentación de red:** La segmentación de red nos permite separar los diferentes activos de la red de forma modular teniendo en cuenta las necesidades de la red.
- **Conformidad de dispositivos:** openNAC nos permite comprobar que los dispositivos (tanto de usuario como de red) cumplen una serie de requisitos definidos en el sistema.
- **BYOD:** La herramienta o sistema openNAC nos permite una rápida adopción del fenómeno BYOD donde se permita los usuarios de la red utilizar sus dispositivos personales.
- **Acceso a invitados:** El tener un control total de acceso a la red nos permite facilitar el despliegue de el acceso a la red para usuarios invitados.

Estas son algunas de las funcionalidades base que nos aporta openNAC y aunque existen otras, representan casos de uso más específicos que complementan las ya definidas anteriormente o que no aplican al caso de uso de control de acceso a la red.

En openNAC el control de acceso se realiza mediante AAA:

La autenticación se puede realizar mediante la base de datos local de openNAC donde tendremos que añadir los usuarios o bien mediante el directorio activo o LDAP que ya esté implementado en la infraestructura con el fin de agilizar la implementación.

La autorización se realizará mediante políticas, estas políticas se componen de precondiciones y postcondiciones. Las precondiciones son toda aquella información que se conoce de la conexión del dispositivo, por ejemplo, el tipo de suplicante utilizado (estas precondiciones serán las que determinaran si el dispositivo entra o no en la política) y las postcondiciones serán aquellas acciones que se aplicaran a la conexión en caso de entrar en la política, por ejemplo, la aplicación de una VLAN.

Finalmente, la contabilidad se realizará mediante los paquetes que los dispositivos de red manden al sistema openNAC con la información relativa a la conexión del dispositivo.

7.7 Ejemplarización de un flujo NAC (Laboratorio)

En este apartado realizaremos una simulación de autenticación de un cliente mediante un equipo Windows 10 actuando de cliente, un switch Cisco con la función de autenticador y un servidor openNAC basado en CentOS Linux que realizara la función de AAA.

El esquema siguiente muestra la arquitectura implementada para la prueba:

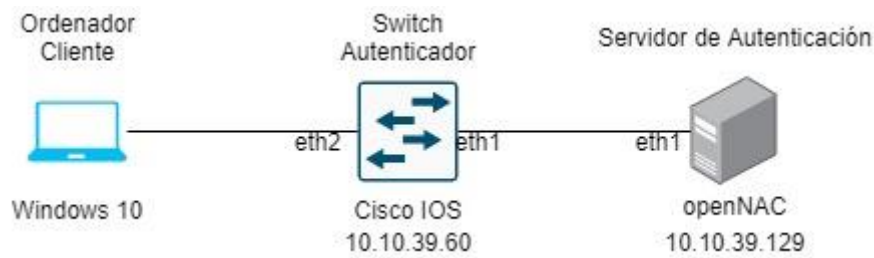


Ilustración 21 Arquitectura de pruebas NAC

Como podemos observar se trata de una arquitectura simple, completamente válida para replicar todos los pasos que conforman el proceso de acceso a la red.

Antes de empezar el proceso recordemos de forma breve y resumida los pasos que se van a realizar internamente:

1. El equipo cliente se conecta a la red e inicia el proceso de autenticación
2. El switch autenticador pedirá al equipo cliente las credenciales para el acceso
3. Una vez el cliente le devuelva las credenciales, el switch las redirigirá a través de RADIUS al servidor de autenticación.
4. El servidor de autenticación evaluará las credenciales para autenticar al dispositivo, en este caso las credenciales estarán almacenadas de forma local en el servidor.
5. En caso de que las credenciales sean correctas se evaluará la autorización del dispositivo mediante políticas.
6. Una vez se haya evaluado y determinado la autorización para el dispositivo cliente, se mandarán los paquetes RADIUS correspondientes al switch autenticador para que este aplique las características al puerto del dispositivo cliente.
7. En este punto el puerto debería abrirse y permitir el acceso a la red del equipo cliente.

A continuación, analizaremos todo el tráfico procedente del protocolo AAA por cada una de sus partes, Autenticación, Autorización y Contabilidad.

7.7.1 Autenticación

En este caso se realizará una autenticación PEAP mediante el uso de credenciales de tipo usuario/contraseña.

En la prueba realizada analizaremos dos flujos de comunicación, la comunicación EAPOL entre el cliente y el autenticador (Switch) mediante el uso de Wireshark en el equipo cliente y la comunicación RADIUS entre el autenticador y el servidor de autenticación mediante un *tcpdump* al puerto 1812 ejecutado en el servidor de autenticación el cual se guardará en un archivo .pcap para analizar posteriormente en Wireshark.

Una vez conectemos el equipo cliente al puerto del SW se inicializará el proceso de autenticación tal y como podemos ver en la siguiente captura de Wireshark (Flujo 802.1x):



Por el otro lado, una vez el autenticador recibe las credenciales (*Response, Identity*), este iniciará la comunicación RADIUS con el servidor de autenticación tal y como podemos ver en la siguiente imagen (Flujo RADIUS):

54


```
[root@on-dc-dev ~]# tcpdump port 1812 and host 10.10.36.48
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
19:14:47.936898 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x44 length: 218
19:14:47.941373 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x44 length: 64
19:14:47.949097 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x45 length: 233
19:14:47.951151 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x45 length: 64
19:14:47.964039 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x46 length: 353
19:14:47.969856 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x46 length: 1090
19:14:47.980514 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x47 length: 233
19:14:47.981868 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x47 length: 1086
19:14:47.991151 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x48 length: 233
19:14:47.992424 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x48 length: 740
19:14:48.001842 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x49 length: 371
19:14:48.004372 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x49 length: 123
19:14:48.012286 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x4a length: 233
19:14:48.013456 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x4a length: 101
19:14:48.025093 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x4b length: 270
19:14:48.026002 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x4b length: 117
19:14:48.033398 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x4c length: 270
19:14:48.036005 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x4c length: 117
19:14:48.044079 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x4d length: 318
19:14:53.078606 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Request (1), id: 0x4d length: 318
19:14:53.990913 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Challenge (11), id: 0x4d length: 149
19:14:53.998961 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x4e length: 270
19:14:54.002001 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Challenge (11), id: 0x4e length: 101
19:14:54.009604 IP 10.10.36.48.datametrics > 10.10.36.40.radius: RADIUS, Access Request (1), id: 0x4f length: 270
19:14:54.690964 IP 10.10.36.40.radius > 10.10.36.48.datametrics: RADIUS, Access Accept (2), id: 0x4f length: 183
```

Ilustración 23 Captura tcpdump del flujo RADIUS

En la siguiente imagen, observamos el mismo flujo de RADIUS analizado utilizando la herramienta de Wireshark donde podemos ver en más detalle cada uno de los paquetes que se han transmitido:

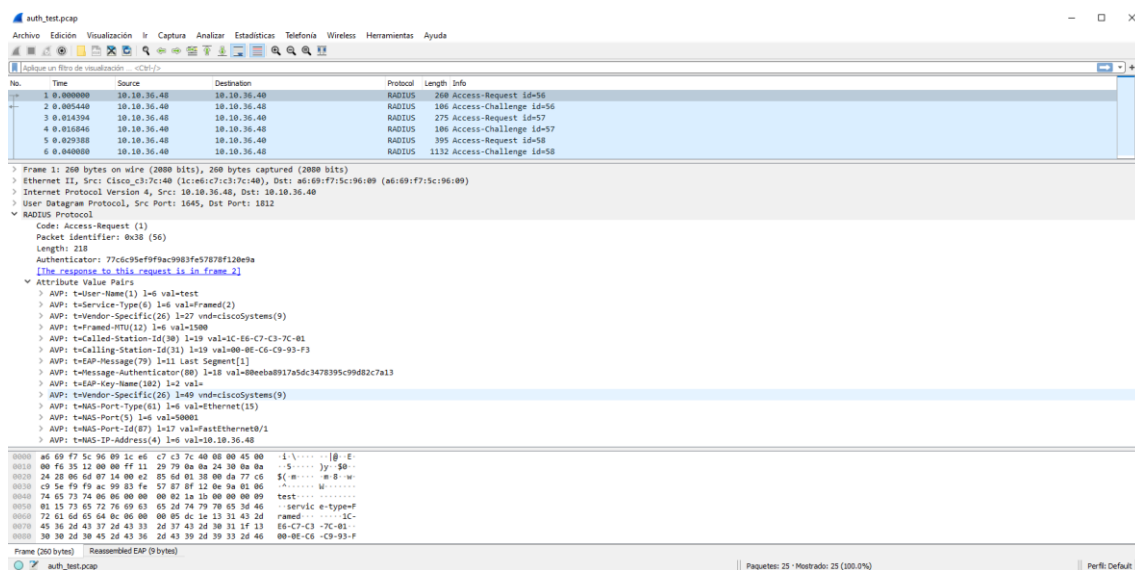


Ilustración 24 Captura Wireshark del flujo RADIUS

En ambas capturas de tráfico vemos que se realizan varios retos de autenticación (*Access-Request* → *Access-Challenge*) por los cuales el servidor RADIUS recibe las pruebas de autenticación generadas por el switch con la información recibida por parte del host.

Estas capturas nos confirman la teoría analizada en el apartado 7.3.2 relativa a la autenticación de host mediante solicitante.

7.7.2 Autorización

Una vez se ha autenticado el cliente, se inicia la evaluación de la política de openNAC, que a través de todos los datos de autenticación decidirá las características de la conexión de este

cliente. A continuación, veremos la implementación de una política simple la cual aplicara al dispositivo que se ha autenticado en el paso anterior:

The screenshot shows the 'Edit [Test_dot1x_CISCO]' configuration window. It has a 'General' section with fields for 'Name' (Test_dot1x_CISCO), 'Enabled' (Yes), and 'Comment'. Below this are four expandable sections for 'Preconditions': 'Time', 'Users', 'User Devices', and 'Network Devices'. The 'Sources' section is expanded, showing a grid of checkboxes for various authentication methods: MAB (No), MAC discover (No), Supplicant User (Yes), Supplicant User Certificate (Yes), Supplicant Host (Yes), Supplicant Host Certificate (Yes), VPN (No), User (No), Visibility (No), and SNMP Trap (No). Below the preconditions is the 'Postconditions' section, which includes a 'Set VLAN' button, a table for VLAN configuration, and a 'Set Security Profile' button.

	Vlan ID	Type	VLAN by default	Name
<input type="checkbox"/>	330	Service	false	v330

Ilustración 25 Política de autorización de openNAC

Como podemos observar existen diversos apartados que se resumirán brevemente a continuación:

General

Se define un nombre un comentario y el estado de la política (activada o desactivada).

Precondiciones

Las precondiciones son aquellas características por las que se decide si una conexión hace *match* con la política. Tenemos varios tipos de precondiciones:

- Tiempo: periodo del día en que se realiza la conexión
- Usuarios: usuario que realiza la conexión.
- Dispositivos de usuario: Dispositivo de usuario que realiza la conexión.
- Dispositivo de red: Dispositivo de red del cual proviene la conexión.

- Fuente: Tipo de fuente de la conexión, en nuestro caso activaremos “Suplicant User”, ya que es el tipo de suplicante que hemos configurado en el cliente Windows.

Así pues, en caso de cumplirse las precondiciones, la conexión se establecería en esta política y se procedería a aplicar las Postcondiciones.

Postcondiciones

Las postcondiciones son aquellas características que se aplicaran a la conexión del cliente autenticado, las dos principales pueden ser, la asignación de una VLAN o la aplicación de un *Security Profile* (ACL). En este caso, en caso de cumplir las precondiciones, la conexión del cliente Windows se asignará a la VLAN 330.

Los parámetros de la conexión se mandarán al Switch autenticador mediante paquetes RADIUS, podemos ver los paquetes que recibiremos en el debug del Switch CISCO.

En la siguiente imagen observamos el paquete *Access-Accept* recibido en el switch desde el servidor Radius después de la validación de las credenciales (autenticación) donde se determina la VLAN que se asignara al host mediante el atributo “*Tunnel-Private-Group* [81]”, en este caso, la VLAN 330:

```
*Mar 4 10:06:51.551: RADIUS: Received from id 1645/110 10.10.36.40:1812, Access-Accept, len 183
*Mar 4 10:06:51.551: RADIUS: authenticator B1 2F 93 B3 CB A9 1D B7 - 1A C1 EC 05 AE C8 29 1B
*Mar 4 10:06:51.551: RADIUS: User-Name [1] 6 "test"
*Mar 4 10:06:51.551: RADIUS: Vendor, Microsoft [26] 58
*Mar 4 10:06:51.551: RADIUS: MS-MPPE-Recv-Key [17] 52 *
*Mar 4 10:06:51.551: RADIUS: Vendor, Microsoft [26] 58
*Mar 4 10:06:51.551: RADIUS: MS-MPPE-Send-Key [16] 52 *
*Mar 4 10:06:51.551: RADIUS: EAP-Message [79] 6
*Mar 4 10:06:51.551: RADIUS: 03 0C 00 04
*Mar 4 10:06:51.551: RADIUS: Message-Authenticato[80] 18
*Mar 4 10:06:51.551: RADIUS: 0E 1D 26 D5 E7 35 E9 C8 7A 4E E2 57 0E F4 21 E8 [ &5zNW!]
*Mar 4 10:06:51.551: RADIUS: Tunnel-Type [64] 6 00:VLAN [13]
*Mar 4 10:06:51.551: RADIUS: Tunnel-Medium-Type [65] 6 00:ALL 802 [6]
*Mar 4 10:06:51.551: RADIUS: Tunnel-Private-Group[81] 5 "330"
*Mar 4 10:06:51.551: RADIUS(0000009E): Received from id 1645/110
*Mar 4 10:06:51.551: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 4 10:06:51.567: %DOT1X-5-SUCCESS: Authentication successful for client (000e.c6c9.93f3) on Interface Fa0/1
```

Ilustración 26 Paquete Access-Accept

Y podemos comprobar que se aplican estos parámetros en el listado de conexiones autenticadas en la interfaz donde se encuentra el host en el Switch:

```
MiniCiscoPoe#show authentication sessions interface fastEthernet 0/1
Interface: FastEthernet0/1
MAC Address: 000e.c6c9.93f3
IP Address: 1.2.3.4
User-Name: test
Status: Authz Success
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: 330
Session timeout: 3600s (local), Remaining: 1520s
Timeout action: Reauthenticate
Idle timeout: N/A
Common Session ID: 0A0A2430000000791177E721
Acct Session ID: 0x00000067
Handle: 0xAA00007A

Runnable methods list:
Method State
dot1x Authc Success
mab Not run
```

Ilustración 27 Aplicación de VLAN en el switch

Aquí podemos ver los detalles de la conexión del cliente, como podemos ver se ha aplicado la VLAN 353 a dicho cliente.

7.7.3 Contabilidad (*Accounting*)

Los mensajes de contabilidad se mandarán del autenticador al servidor de autenticación durante el periodo de tiempo que durara la conexión del cliente, estos mensajes mantendrán actualizada la información relativa a la conexión. Estos mensajes también se encapsulan en RADIUS, pero a diferencia de los mensajes de autenticación y autorización, estos se mandan a través del puerto 1813. Para ver uno de estos mensajes realizaremos un tcpdump al puerto 1813 del servidor de autenticación.

```
[root@on-dc-dev ~]# tcpdump port 1813 and host 10.10.36.48
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
20:07:29.731152 IP 10.10.36.48.sa-msg-port > 10.10.36.40.radius-acct: RADIUS, Accounting Request (4), id: 0x24 length: 298
20:07:30.385667 IP 10.10.36.40.radius-acct > 10.10.36.48.sa-msg-port: RADIUS, Accounting Response (5), id: 0x24 length: 20
```

Ilustración 28 Captura tcpdump de paquetes Accounting

Cuando el host se desconecta del puerto, el switch manda un paquete (*Accounting-Request*) al servidor Radius para informarle de la desconexión, si el paquete se recibe correctamente el servidor Radius responderá al switch con un paquete de confirmación (*Accounting-Response*).

8 Aplicación Blockchain en sistemas NAC

Una vez realizado el estudio de ambas tecnologías, en este apartado, se propondrá una posible aplicación de la tecnología blockchain en un sistema NAC.

Como se ha visto anteriormente, blockchain nos puede aportar multitud de beneficios en diversos ámbitos. Así pues, el uso correcto de esta tecnología puede aportar un valor añadido a productos o servicios ya existentes. Un ejemplo de esto sería la mejora en la trazabilidad de activos dentro de la red.

8.1 Trazabilidad de activos en la red

La propuesta de aplicación de la tecnología blockchain en un sistema NAC viene impulsada por la posibilidad de ataques a infraestructuras de red y a sus recursos desde un punto de vista interno.

Los sistemas NAC nos aportan gran cantidad de información relativa al estado de la red, quien ha accedido a ella o quien ha sido rechazado. Toda esta información nos aporta visibilidad de la red. En ocasiones, en entornos críticos o donde se realizan auditorias exhaustivas, es importante mantener un registro constante y actualizado del estado de la red y los activos conectados a ella. Blockchain nos permite mantener este registro actualizado en forma de transacciones incluidas en bloques que contengan la información recopilada por el sistema NAC.

Otro aspecto para tener en cuenta, relativo al registro de actividad, es el análisis forense de red en caso de sufrir algún tipo de ataque interno. Un ataque interno es aquel que se realiza desde el interior de la propia red. En la mayoría de los casos un ataque interno se realiza por alguien que ya sea de forma legítima o ilegítima ha obtenido acceso y autorización a la red. Una vez la persona se encuentra dentro de la red, puede causar grandes perjuicios a la infraestructura de la red o sus sistemas, robar información, obtener permisos administrativos, etc. una vez realizado el ataque eliminar o modificar todo registro que pudiera determinar las acciones y/o origen del ataque y salir de la red.

El uso de blockchain como registro de eventos nos permite tener una base de datos inmutable, persistente y de confianza que mantenga una integridad completa de los datos almacenados.

En el siguiente punto se propondrá una posible implementación de un registro blockchain para el almacenamiento de esta información. La propuesta se realizará a nivel teórico, detallando los aspectos técnicos sin llegar a realizar una implementación práctica.

La aplicación de blockchain a un sistema NAC dará como resultado la conceptualización de un nuevo sistema conjunto al que, desde este punto, nos referiremos como NACTrack como la integración entre ambas tecnologías.

8.2 Propuesta de aplicación blockchain - NACTrack

La propuesta de implementación se basa en una blockchain que actúe como registro de eventos generados en la red. La principal fuente de información de este registro serán los eventos generados por un sistema NAC, estos incluyen los accesos a la red, autorizaciones, actividad de red y comportamiento del activo.

Al tratarse de un sistema interno a las organizaciones, la propuesta se basará en una blockchain de tipo privada. El uso de una blockchain privada nos ofrecerá mayor velocidad, escalabilidad y control. Dado que los datos, principalmente, serán internos a una organización, este tipo de blockchain nos ofrecerá una mayor privacidad y control de los datos almacenados en ella.

La blockchain será permissionada, eso significa que no será de libre acceso. Existirá un control sobre quien puede participar en la cadena de bloques y que permisos tiene cada uno de los nodos.

Por otra parte, dado que no es necesaria la transferencia de valor dentro de la blockchain, esta no hará uso de tokens o monedas.

8.2.1 Arquitectura del sistema

Una de las principales características de blockchain, es su arquitectura P2P. Esta arquitectura nos permite descentralizar el control de la información lo que ayuda a mantener una integridad en los datos y evitar comportamientos maliciosos por parte de los partícipes de la red.

En el sistema NACTrack se plantea la existencia de dos tipos de nodos dentro de la red blockchain.

El sistema constará de dos tipos de nodos dentro de la red, estos son:

- **Nodos Administradores**

Los nodos administradores serán los responsables de verificar y generar nuevos bloques dentro de la cadena. También son los encargados de transmitir los nuevos bloques añadidos. En una implementación real en, por ejemplo, una empresa, estos nodos administradores podrían establecerse por departamentos.

- **Nodos Participantes**

Los nodos participantes serán los nodos que recopilaran la información y la transmitirán a los nodos administradores para que estos la validen y la incluyan en la cadena de bloques. Estos nodos también mantienen una copia de la cadena de bloques.

En una primera instancia se plantea una infraestructura donde los nodos administradores actúen de forma aislada, es importante mantener una seguridad muy elevada en cuanto a estos nodos dado que son un punto crítico en el sistema. Ellos son quienes validan los nuevos bloques por lo que son susceptibles a ataques.

Los nodos participantes serán aquellos que a la vez actuaran como servicio NAC por lo que por ellos pasaran la mayoría de los eventos. Estos eventos se almacenarán en forma de transacciones y se enviarán a los nodos administradores para su verificación.

En entornos donde exista el uso de agentes (Apartado 7.1) sería posible que los propios dispositivos con agente instalado tuvieran también el rol de nodo participante para transmitir información a los nodos administradores.

8.2.2 Estructura de datos

Los datos almacenados en el registro de blockchain de NACTrack se basan principalmente en eventos de red relativos a los activos conectados. Es importante seleccionar y estructurar de forma correcta la información que se almacenará en la blockchain.

Estos datos componen las transacciones que posteriormente serán añadidas a los bloques que conformarán la cadena. Las transacciones se compondrán por los siguientes datos:

Tabla 3 Estructura de datos aplicación NACTrack

Campo	Descripción
Activo	Identificador del activo.
Usuario	Identificador del usuario
Tipo de Evento	Tipo de evento registrado.
Datos de Evento	Detalle de los datos del evento registrado.
Nodo	Nodo que ha procesado los datos (generación de la transacción).
Origen	Punto en el que se han originado los datos.
Timestamp	Marca temporal correspondiente a la generación del evento

- **Activo:** Información identificativa del activo de red al que corresponde el evento. Se utilizará la MAC del dispositivo como identificador de este.
- **Usuario:** Esta es la información del usuario al que corresponde el evento. Puede corresponder al nombre de usuario en caso de utilizar credenciales de acceso o a la MAC en caso de haber realizado un MAB.

- **Tipo de Evento:** corresponde al detalle del evento registrado, este puede ser, por ejemplo, el acceso a la red (*login*).
- **Datos de Evento:** En este campo se añadirá la información detallada relativa al evento. Por ejemplo, en un evento de tipo *login*, el tipo de acceso que se ha realizado, 802.1x por credenciales, certificado, MAB...
- **Nodo Participante:** Identificador del nodo participante que ha transmitido la transacción.
- **Origen:** Este campo hace referencia al elemento que ha originado o detectado el evento. Este identificador se establecerá como la MAC del elemento de red. Este podría ser, por ejemplo, la MAC del switch que ha generado un paquete de *Accounting*.
- **Timestamp:** Esta marca de tiempo determinará el momento exacto en que se ha generado el evento. Esta información será de gran utilidad a la hora de marcar la temporalidad de los eventos en la trazabilidad de un activo dentro de la red.

Esta será la información almacenada en la blockchain y con la que se realizará la trazabilidad de los activos.

8.2.3 Estructura de bloques y transacciones

Los datos vistos en el apartado anterior serán tratados como transacciones que se almacenarán en los bloques de la blockchain.

Los bloques de la blockchain de nuestro sistema tendrán una estructura similar a los de Bitcoin, o cualquier blockchain basada en registro de transacciones, como se ha visto en la parte teórica del trabajo.

Los bloques tendrán el siguiente formato:

Tabla 4 Estructura de un bloque de la aplicación NACTrack

Campo	Descripción			
<div>Cabecera del bloque</div> <table><tr><td>Hash anterior</td></tr><tr><td>Raíz Merkle</td></tr><tr><td>Timestamp</td></tr></table>	Hash anterior	Raíz Merkle	Timestamp	Datos correspondientes a la información del bloque.
Hash anterior				
Raíz Merkle				
Timestamp				
Contador de transacciones	Número de transacciones incluidas en el bloque.			
<div>Transacciones</div> <table><tr><td>Tn01</td></tr><tr><td>...</td></tr><tr><td>TnNN</td></tr></table>	Tn01	...	TnNN	Registro de transacciones incluidas en el bloque.
Tn01				
...				
TnNN				

Como podemos observar, se eliminan los puntos de “*Target Difficulty*” y “*Nonce*” de la cabecera del bloque (Apartado 6.1.7) esto es debido al algoritmo de consenso utilizado no hará falta el uso de esta información como veremos en el siguiente apartado.

8.2.4 Algoritmo de consenso

Dadas las características de NACTrack, por tratarse de un sistema interno y una blockchain privada, es necesario establecer un control en el proceso de consenso de los nodos. Es por esto por lo que se decide utilizar un algoritmo de consenso que permita un mayor control sacrificando algunas de las características de la blockchain como lo es la descentralización.

Esta implementación se basa en un entorno cerrado, donde la arquitectura es conocida y está bien definida. El nivel de seguridad es alto y no se requiere un perfil descentralizado por ser la propia organización la consumidora principal del sistema. Esto nos permite poder no utilizar un algoritmo de consenso preestablecido como puede ser PoW o PoS que permiten una descentralización y un incentivo a la participación.

En este caso se utilizará un algoritmo basado en la selección de nodos mediante números aleatorios. El sistema generará un numero aleatorio que corresponderá al encargado de generar el nuevo bloque. Dado que no hay prueba de trabajo, el nodo seleccionado incluirá el bloque a la blockchain de forma directa provocando la sincronización de la cadena en todos los nodos partícipes.

8.2.5 Flujo de funcionamiento

El flujo de funcionamiento del sistema NACTrak es relativamente simple. Para explicar el funcionamiento y el flujo de datos se propone la siguiente arquitectura como ejemplo de implementación:

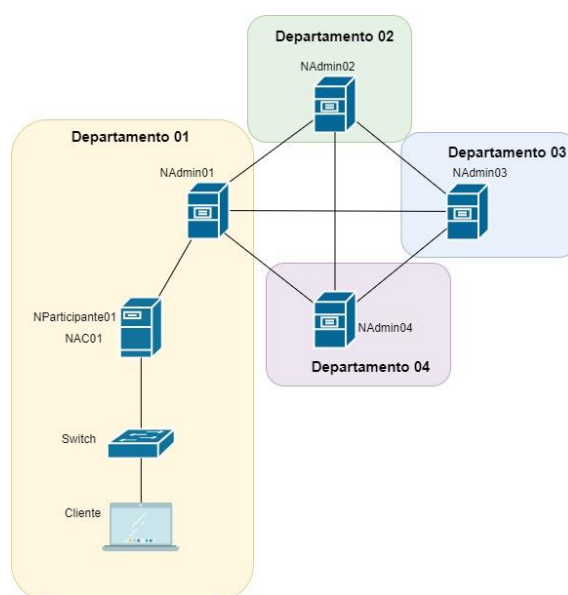


Ilustración 29 Arquitectura de ejemplo del sistema NACTrack

Ta i como podemos observar existen diversos elementos en la arquitectura propuesta. A nivel de sistema NAC los elementos principales son, el cliente, en este caso un equipo de escritorio, un switch con el rol de autenticador y finalmente el servidor de autenticación (NAC01). En cuanto a la parte blockchain, primeramente, tenemos la red de nodos Administradores (NAdminNN), estos se desplegarán por departamentos. En segundo lugar, encontráramos los nodos participantes (NParticipante01), estos existirán dentro del propio departamento.

Para detallar el flujo del sistema dividiremos este en dos fases. La primera fase consta del proceso NAC y de creación de las transacciones, como ya hemos visto las transacciones estarán compuestas por los datos obtenidos del NAC. La segunda fase es la correspondiente a la transmisión de la transacción a la red y la posterior encadenación del bloque a la blockchain.

8.2.5.1 Flujo NAC y creación de transacciones

En el siguiente diagrama de actividad podremos observar la primera parte del flujo del sistema:

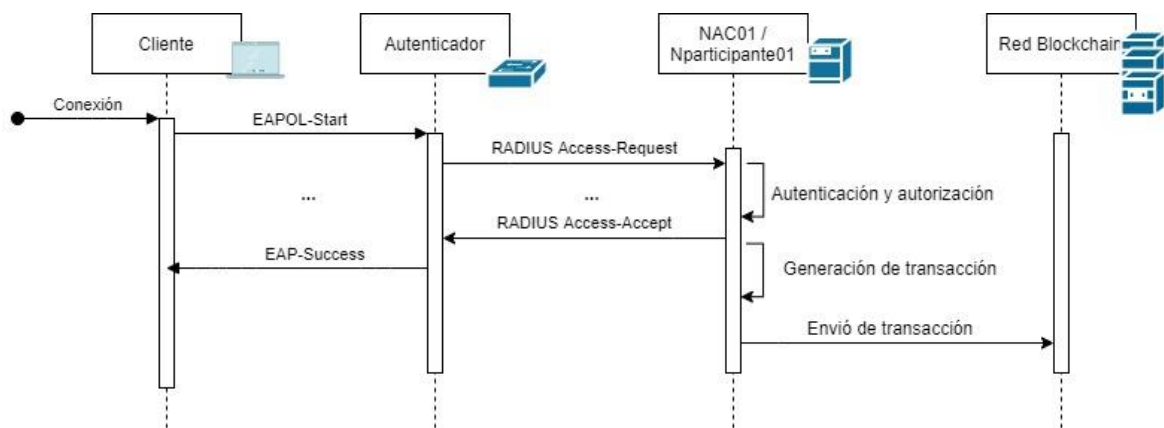


Ilustración 30 Flujo de NAC Y transacciones en NACTrack

El inicio del proceso se establece en el momento en que un cliente intenta acceder a la red (conexión). Una vez este cliente se conecta, se inicia el proceso de autenticación y autorización mediante el protocolo EAP entre cliente y Switch (Autenticador) y el protocolo Radius entre el switch y el servidor de autenticación (NAC01). Podemos encontrar el flujo completo de autenticación y acceso en el apartado 7.3. y 7.4.

Una vez se ha realizado todo el flujo de autenticación y autorización, el nodo participante (Nparticipante01), que ha recopilado toda la información necesaria, genera la transacción que contendrá los datos vistos en el apartado 8.2.2. Una vez generada la transacción, este nodo participante la mandará a la red para que sea verificada y añadida a la blockchain.

8.2.5.2 Flujo validación y encadenación de bloques

El segundo flujo del sistema corresponde a la recepción de las transacciones en la red blockchain, la verificación y el encadenado de bloques.

Los pasos para la realización de este proceso son:

1. Las transacciones se envían por parte de los nodos Participantes a la red.
2. Las transacciones entrantes son verificadas por la red y añadidas a un *pool* de transacciones pendientes de ser añadidas a los bloques.

De forma paralela:

1. Mediante el algoritmo de consenso establecido (Apartado 8.2.4) se selecciona el nodo Administrador encargado de generar el nuevo bloque.
2. El nodo seleccionado agrupa las transacciones que encuentra en el *pool* de transacciones y las empaqueta en un nuevo bloque.
3. El nuevo bloque se añade a la red comunicándolo al resto de partícipes de la red.
4. Los otros nodos de la red verifican el nuevo bloque y se sincronizan con la nueva entrada en la cadena.

Verificación de transacciones

Para que una transacción sea añadida al pool de transacciones, esta debe ser verificada por los nodos.

9 Análisis de la propuesta

Una vez realizada la propuesta de implementación de la aplicación blockchain en sistemas NAC (NACTrack), se procede a realizar el análisis de dicha propuesta.

Los dos principales beneficios que nos aporta el uso de una tecnología blockchain para el almacenamiento de los datos de trazabilidad en un sistema NAC son:

- **Integridad de los datos (inmutabilidad):** De forma predeterminada, una blockchain nos permite la posibilidad de leer y escribir datos en ella. Una vez se han introducido datos en ella no se permite la modificación de estos de forma simple.
- **Sistema parcialmente descentralizado:** Aunque desde un punto de vista lógico el sistema propuesto está claramente centralizado por una organización concreta, la implementación física está completamente descentralizada. Esto nos permite una mayor seguridad en caso de que uno de los nodos se viera manipulado y actuara de forma maliciosa.

Estas características pueden acontecer elementos clave en ciertas infraestructuras de red. En determinados entornos críticos como infraestructuras empresariales de grandes dimensiones u organismos gubernamentales, la veracidad e integridad de los datos resulta de suma importancia. Por otra parte, estas organizaciones suelen estar controladas por auditorías exhaustivas que requieren de un control muy exacto del entorno de red. Contar con datos confiables puede ser un criterio para seguir.

Otra casuística donde este sistema pueda resultar de ayuda es en el caso de que se produzca un ataque interno a la organización, este sistema no nos aporta más seguridad en cuanto a la posibilidad de que se produzca, pero sí que nos puede ayudar posteriormente. Es de esperar que un atacante que realice un ataque interno desee eliminar todo rastro posible. En caso de que dicho atacante consiguiera eliminar su rastro, supondría una dificultad añadida al posterior análisis forense para recopilar evidencias. El uso de la blockchain para almacenar los datos de registro y trazabilidad añade una capa de seguridad ante este fenómeno debido a la dificultad de modificación de la cadena de bloques.

Debido a la arquitectura de las transacciones y bloques, el sistema permite una escalabilidad al almacenar el tipo de datos de cada transacción. Esto hace que puedan integrarse nuevos sistemas de red que aporten información para la trazabilidad de activos. Un ejemplo podría ser la integración de un sistema de información de seguridad y gestión de eventos (SIEM) que nos permitiría obtener información de la red (actividad de aplicaciones, vulnerabilidades de equipos, configuraciones, etc.) para la identificación de ataques. De la misma manera que la información de los sistemas NAC se añade a la blockchain, sería posible añadir la información de los otros sistemas, indicando el origen en el campo de las transacciones “Tipo de Evento” (Apartado 8.2.2).

En el análisis de la propuesta se determinan algunos puntos desfavorables a la aplicación. El primero de ellos es la necesidad de contar con varios nodos para formar la blockchain. Esto

puede llegar a ser un problema, ya que, aun siendo posible desplegar una blockchain con pocos nodos, una cantidad reducida puede convertirse en un punto de ataque. Si el sistema cuenta con pocos nodos resulta más fácil realizar un ataque del 51% con las repercusiones que esto implicaría, destrucción de datos, modificación ilícita de datos, etc.

Cabe destacar que la implementación de esta funcionalidad no representa una mejora en las funcionalidades tradicionales de un sistema NAC, pero se presenta como un valor añadido en el global del sistema.

10 Previsión del proyecto de desarrollo

En este apartado se realizará una previsión sobre el coste organizacional, temporal y económico relativo al desarrollo del producto NACTrack. Este se enfoca como una aproximación al *Project Management*. Se determinarán los aspectos organizativos, de planificación y de recursos necesarios para el desarrollo de un producto funcional.

La previsión se basa en la creación de un MVP (Producto Mínimo Viable) que permita una funcionalidad y estabilidad suficiente para lanzar al producto. A partir de este MVP se realizaría un posterior desarrollo continuo para la mejora del sistema basado en el *feedback* que se reciba por parte de los clientes.

10.1 Ciclo de vida del proyecto

Para determinar de forma global la trayectoria y recorrido del proyecto se utilizará el siguiente modelo de ciclo de vida. En este modelo podremos apreciar las fases que componen el proyecto ordenadas de forma secuencial relativo al flujo de ejecución.

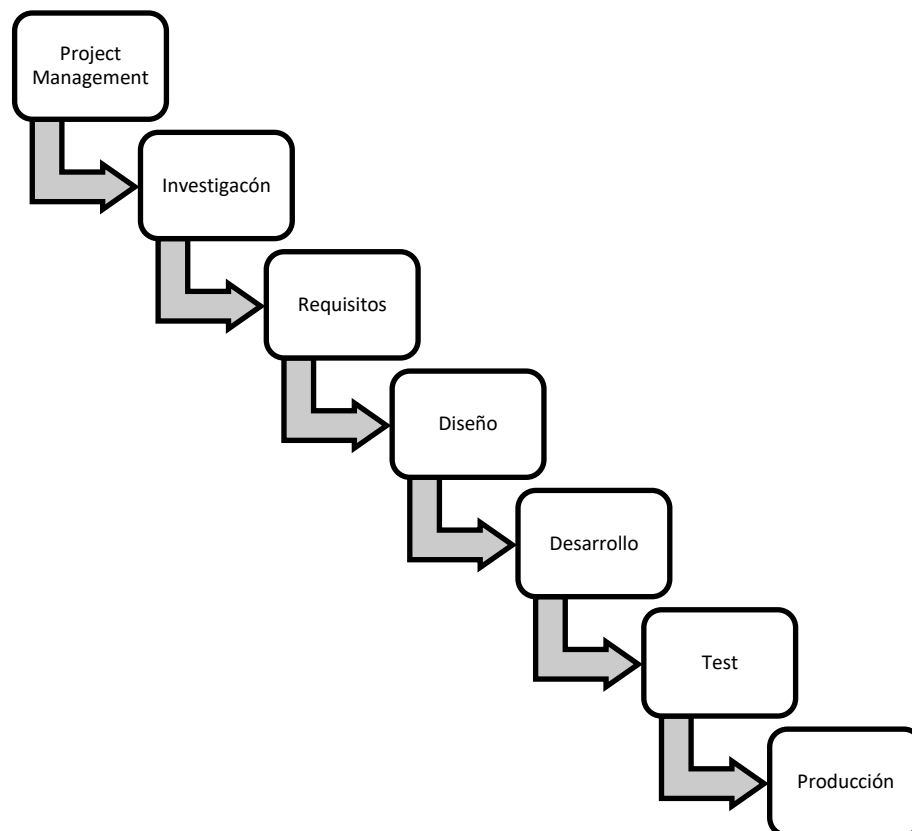


Ilustración 31 Ciclo de vida del proyecto NACTrack

Estas fases del proyecto se definen como:

- **Project Management:** Esta primera fase se establece como punto inicial donde se definirán las características del proyecto, como se gestionará, la metodología de trabajo y los aspectos relativos a la organización del proyecto de desarrollo.
- **Investigación:** En esta fase se propone fundamentar una base de conocimiento sólida sobre los dos conceptos claves (blockchain y NAC). De esta forma todos los integrantes del proyecto parten de una misma mínima base de conocimiento.
- **Definición de requisitos:** La definición de requisitos que debe cumplir el producto final se realiza como primera fase para fundamentar las bases del posterior diseño y desarrollo.
- **Diseño:** Se determina el diseño funcional del producto, la arquitectura de sistema (software) y la arquitectura de red blockchain.
- **Desarrollo:** En la fase de desarrollo se realizarán las actividades de desarrollo del software tanto del *back-end* como del *front-end* de la aplicación. El desarrollo ese constantemente pasando por procesos de control de calidad.
- **Test:** En esta fase se realizan las pruebas pertinentes a la validación y verificación del correcto funcionamiento del producto. También se realizan pruebas para determinar la correcta usabilidad y facilidad de uso por parte del usuario final.
- **Producción:** La fase de producción pretende dejar el producto listo para sacar al mercado. Empaquetar el software para facilitar el despliegue en las infraestructuras del cliente, y generar el material para que sea posible la instalación y la operación de forma autosuficiente.

10.2 Definición del alcance

NACTrack es un sistema de software, el desarrollo del producto no incluye hardware dado que se utilizará hardware genérico donde se ejecutará la aplicación.

NACTrack es una aplicación de la tecnología blockchain sobre un sistema NAC que se considera desarrollado y estable. NACTrack pretende ser un añadido a este producto con una funcionalidad no-intrusiva. Es por ello por lo que en el desarrollo de NACTrack no se incluyen cotes de recursos, tiempo o desembolso económico en el desarrollo o mejora del sistema NAC.

El alcance del proyecto se define con los siguientes puntos:

- Includo:
 - Formación interna
 - Diseño del prototipo
 - Desarrollo del software

- Control de calidad (QA)
- Desarrollo de documentación técnica
- No incluido:
 - Mantenimiento de los sistemas
 - Comercialización
 - Marketing
 - Patentes

Por otra parte, el alcance del producto se define con:

- Incluido:
 - Sistema de infraestructura
 - Software
 - Manual de uso (implementación y operación)
- No incluido:
 - Formación externa sobre el producto

10.3 Roles y responsabilidades

Para el desarrollo de la implementación del sistema NACTrack se requiere la definición de un equipo de trabajo encargado del desarrollo del producto.

Se estipula el siguiente equipo necesario para el desarrollo de NACTrack:

Tabla 5 Roles del proyecto de desarrollo

Cantidad	Rol	Responsabilidad
1	Project Manager	<ul style="list-style-type: none">• Planificación recursos.• Organización del equipo.• Control de tiempos de entrega.• Seguimiento del progreso.
1	Arquitecto Blockchain	<ul style="list-style-type: none">• Diseño de la arquitectura del sistema blockchain.• Diseño de la arquitectura de red (distribución de nodos).
1	Arquitecto de sistemas	<ul style="list-style-type: none">• Diseño de la arquitectura del sistema.• Compatibilidad SW-HW.• Seguridad del sistema.

3	Desarrolladores <i>Full-Stack</i>	<ul style="list-style-type: none"> • Desarrollo <i>back-end</i>. • Desarrollo <i>front-end</i>.
1	Ingeniero de control de calidad (QA)	<ul style="list-style-type: none"> • Pruebas de calidad. • Pruebas de rendimiento. • Control de cargas de trabajo • Pruebas de estrés.
1	Responsable de documentación	<ul style="list-style-type: none"> • Realizar la documentación del producto.

10.4 Estructura de Desglose de Trabajo

Con el fin de separar el global del proyecto en fases o elementos de menor envergadura, para afrontar de manera más rápida y obtener una visión en conjunto de los trabajos necesarios para completar el proyecto, se realiza un diagrama de Estructura de Desglose de Trabajo (*Work Breakdown Structure*).

En el siguiente diagrama de árbol, podremos observar cómo se desglosan las fases de desarrollo del producto NACTrack:

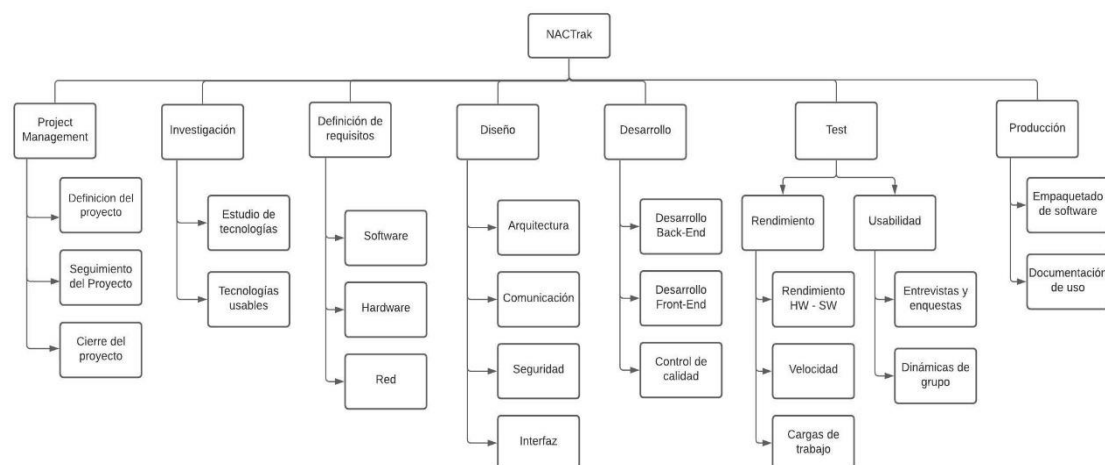


Ilustración 32 Diagrama WBS NACTrack

Como podemos observar, las fases de primer nivel del diagrama WBS corresponden a las ya definidas en el apartado 10.1 (Ciclo de vida del proyecto). En el segundo nivel se detallan o desglosan estas fases en bloques de trabajo más concretos.

10.5 Previsión Temporal del desarrollo

En este apartado se detallarán las tareas que deberían realizarse a lo largo del proyecto de desarrollo del sistema NACTrack. En una primera parte se realizará un listado de dichas tareas. Posteriormente se realizará el diagrama PERT (Técnica de Revisión y Evaluación de Programas) donde se verá el flujo de dichas tareas.

10.5.1 Listado de tareas

A continuación, se detalla el total de las tareas, divididas por fases, a realizar durante el transcurso del proyecto de desarrollo:

- **Project Management:**

Tabla 6 Tareas Fase Project Management

Referencia	Recursos Humanos	Descripción	Coste (en días)	Dependencias
A	PM	Definición del proyecto.	10	-
B	PM	Seguimiento del proyecto.	35	A
C	PM	Cierre del proyecto.	5	B;Z

- **Investigación:**

Tabla 7 Tareas Fase Investigación

Referencia	Recursos Humanos	Descripción	Coste (en días)	Dependencias
D	PM Arq. de sistemas Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 2</i> Des. <i>Full-Stack 3</i> Ing. QA Responsable de documentación	Estudio de la tecnología blockchain.	4	A
E	PM Arq. de sistemas Arq. blockchain Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 2</i> Des. <i>Full-Stack 3</i> Ing. QA Responsable de documentación	Estudio de la tecnología NAC.	3	D
F	PM Arq. de sistemas	Investigación sobre tecnologías usables	2	E

	Arq. blockchain Des. <i>Full-Stack 1</i>	al desarrollo.		
G	Arq. de sistemas Arq. blockchain Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 2</i> Des. <i>Full-Stack 3</i>	Aprendizaje de tecnologías de desarrollo.	5	F

- Definición de requisitos:

Tabla 8 Tareas Fase Definición de requisitos

Referencia	Recursos Humanos	Descripción	Coste (en días)	Dependencias
H	PM	Definición del plan de proyecto.	5	G
I	Arq. de sistemas Arq. blockchain	Definición de requisitos de hardware.	3	H
J	Arq. de sistemas Arq. blockchain	Definición de requisitos de red.	1	I

- Diseño:

Tabla 9 Tareas Fase Diseño

Referencia	Recursos Humanos	Descripción	Coste (en días)	Dependencias
K	Arq. de sistemas Des. <i>Full-Stack 1</i>	Diseño de arquitectura de sistema.	15	J
L	Arq. blockchain	Diseño de arquitectura blockchain.	15	J
M	Arq. de sistemas	Diseño sistema de comunicación.	3	K;L
N	Arq. de sistemas Arq. blockchain	Establecimiento de la seguridad del sistema.	4	M
O	Des. <i>Full-Stack 3</i>	Diseño interfaz gráfica.	5	K
P	Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 2</i>	Diseño Sistema back-end.	12	K

- Desarrollo:

Tabla 10 Tareas Fase Desarrollo

Referencia	Recursos Humanos	Descripción	Coste (en días)	Dependencias
	Arq. de sistemas Arq. blockchain	Implementación del entorno de		

Q	Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 2</i> Des. <i>Full-Stack 3</i>	desarrollo.	12	P
R	Arq. blockchain Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 2</i>	Desarrollo sistema blockchain.	50	Q
S	Arq. de sistemas Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 2</i>	Desarrollo <i>back-end</i> .	45	Q
T	Des. <i>Full-Stack 1</i> Des. <i>Full-Stack 3</i>	Desarrollo <i>front-end</i> .	35	Q

- **Test:**

Tabla 11 Tareas Fase Test

Referencia	Recursos Humanos	Descripción	Coste (en días)	Dependencias
U	Ing. QA	Implementación del entorno de QA.	10	R
V	Ing. QA Arq. de sistemas Arq. blockchain	Pruebas rendimiento HW-SW.	15	U
W	Ing. QA Arq. de sistemas Arq. blockchain	Pruebas de cargas de trabajo.	7	V
X	Ing. QA Arq. de sistemas Arq. blockchain	Pruebas de velocidad.	10	W

- **Producción:**

Tabla 12 Tareas Fase Producción

Referencia	Recursos Humanos	Descripción	Coste (en días)	Dependencias
Y	Arq. de sistemas Des. Full-Stack 1	Empaquetado de software.	15	X
Z	Responsable de documentación	Documentación de uso.	15	Y

10.5.2 Diagrama Gantt

Habiendo definido ya las actividades que deberán realizarse para el desarrollo del producto mínimo viable, se realiza la implementación el diagrama de Gantt.

Con el diagrama de Gantt obtenemos una visión organizativa de las fases, así como de las tareas que las componen. También determinamos el coste temporal total.

Nombre de tarea	Duración	Comienzo	Fin	Predic	Nombre de los recursos
Project Management					
Definición del proyecto.	5 días	lun 10/01/22	vie 14/01/22		Project Manager
Seguimiento del proyecto.	180 días	vie 14/01/22	vie 26/08/22	2	Project Manager
Cierre del proyecto.	5 días	vie 26/08/22	jue 01/09/22	3	Project Manager
Investigación					
Estudio de la tecnología blockchain.	4 días	vie 14/01/22	jue 20/01/22		Arquitecto de sistemas; Des. Full Stack 1Des. Full Stack 2C
Estudio de la tecnología NAC.	3 días	jue 20/01/22	lun 24/01/22	6	Arquitecto Blockchain;Arquitecto e
Investigación sobre tecnologías usables al desarrollo.	2 días	lun 24/01/22	mié 26/01/22	7	Arquitecto Blockchain;Arquitecto de sistemasDes.
Aprendizaje de tecnologías de desarrollo.	5 días	mié 26/01/22	mar 01/02/22	8	Arquitecto Blockchain; Arquitecto de sistemasDes.
Definición de requisitos					
Definición del plan de proyecto.	5 días	mié 02/02/22	mar 08/02/22	9	Project Manager
Definición de requisitos de hardware.	3 días	mar 08/02/22	vie 11/02/22	11	Arquitecto Blockchain; Arquitecto de sistemas
Definición de requisitos de red.	1 día	vie 11/02/22	vie 11/02/22	12	Arquitecto Blockchain;Arquitecto e
Desarrollo					
Diseño de arquitectura de sistema.	15 días	lun 14/02/22	jue 03/03/22	13	Arquitecto de sistemas; Des. Full Stack 1
Diseño de arquitectura blockchain.	15 días	lun 14/02/22	jue 03/03/22	13	Arquitecto Blockchain
Diseño sistema de comunicación.	3 días	jue 03/03/22	lun 07/03/22	16	Arquitecto de sistemas
Establecimiento de la seguridad del sistema.	4 días	jue 03/03/22	vie 11/03/22	17	Arquitecto Blockchain; Arquitecto de sistemas
Diseño interfaz gráfica.	5 días	jue 03/03/22	mié 09/03/22	15	Des. Full Stack 3
Diseño sistema back-end.	12 días	jue 03/03/22	jue 17/03/22	15	Des. Full Stack 1Des. Full Stack 2
Desarrollo					
Implementación del entorno de desarrollo.	12 días	vie 18/03/22	vie 01/04/22	20	Arquitecto Blockchain; Arquitecto de sistemasDes.
Desarrollo sistema blockchain.	50 días	vie 01/04/22	vie 03/06/22	22	Arquitecto Blockchain;Arquitecto e
Desarrollo back-end.	45 días	vie 01/04/22	vie 27/05/22	22	Des. Full Stack 1Des. Full Stack 2
Desarrollo front-end.	35 días	vie 01/04/22	lun 16/05/22	22	Des. Full Stack 1Des. Full Stack 3
Test					
Implementación del entorno de QA.	10 días	vie 03/06/22	mié 15/06/22	23	Ing. Control de calidad
Pruebas rendimiento HW-SW.	15 días	jue 16/06/22	mar 03/07/22	27	Arquitecto Blockchain;Arquitecto e
Pruebas de cargas de trabajo.	7 días	mar 03/07/22	mié 13/07/22	28	Arquitecto Blockchain;Arquitecto e
Pruebas de validez.	10 días	mié 13/07/22	mar 26/07/22	29	Ing. Control de calidad
Producción					
Empaquetado de software.	15 días	mar 26/07/22	vie 12/08/22	30	Arquitecto de sistemasDes. Full St
Documentación de uso.	15 días	vie 12/08/22	jue 01/09/22	32	Responsable de documentación

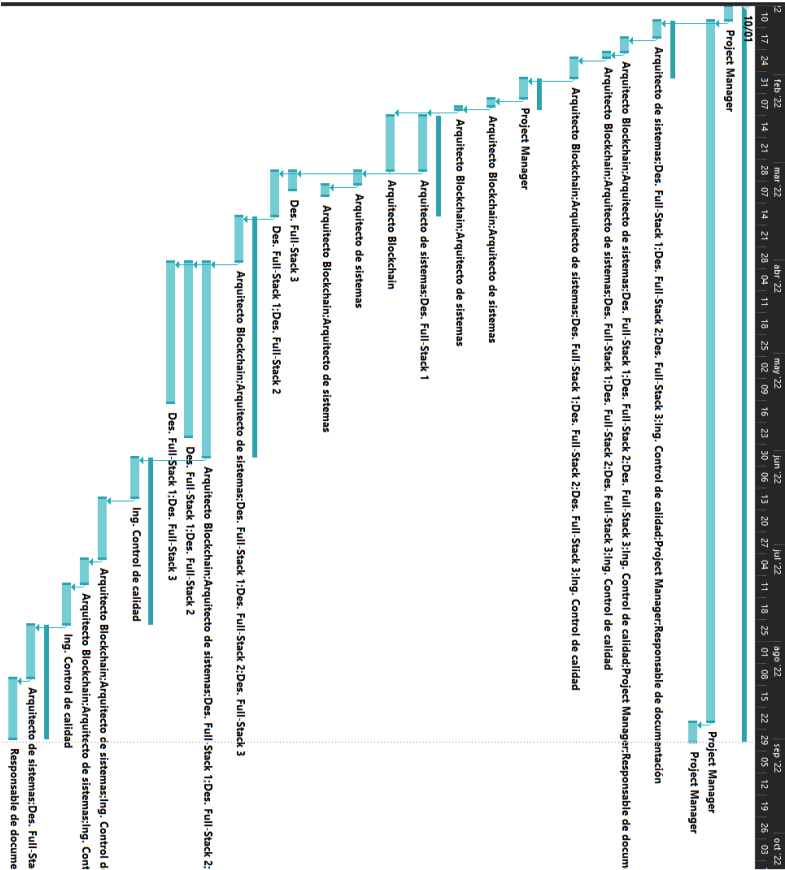


Tabla 13 Diagrama Gantt NACTrack

A partir de la información desarrollada en este y los anteriores apartados, se estipula un tiempo para el desarrollo del producto mínimo viable de NACTrack de 8 meses.

10.6 Presupuesto

Teniendo ya una definición de producto, equipo y tiempo es el momento de realizar una planificación económica o presupuesto.

En este apartado se determinará el coste de realización del proyecto de desarrollo de NACTrack. En primera instancia, estos costes se calcularán por las fases y tareas previamente definidas. Posteriormente se realizará una estimación de costes por fases y los costes directos. Y, finalmente, Se realizará el estudio total del Proyecto con los costes directos e indirectos.

10.6.1 Presupuesto de recursos humanos

A partir de las tareas que se han definido en el apartado 10.5.1, extraemos el total de horas que cada uno de los roles realizará. Se considera que todos los roles realizan una jornada laboral a tiempo completo (8 h/día). Se toman como referencia los datos del Informe de Tendencias Salariales 2021 (Randstad, 2021)

En la siguiente tabla podemos ver el coste de cada desglosado por el coste del recurso humano:

Tabla 14 Presupuesto Recursos Humanos

Rol	Horas	Coste (€/h)	Coste total
Project Manager	211	25	5275 €
Arquitectos Blockchain	936	22	20592 €
Arquitecto de sistemas	1112	20	22240 €
Desarrollador <i>Full-Stack 1</i>	1584	17	26928 €
Desarrollador <i>Full-Stack 2</i>	1064	17	18088 €
Desarrollador <i>Full-Stack 3</i>	928	17	15776 €
Ingenieros de control de calidad (QA)	448	15	6720 €
Responsable documentación	176	10	1760 €

El presupuesto total de recursos humanos se calcula en: **117379 €**

10.6.2 Presupuesto de recursos no humanos

Una vez detallados los costes relativos a los recursos humanos, es necesario detallar los costes de recursos no humanos. Estos recursos incluyen hardware, software y gastos genéricos.

10.6.2.1 Presupuesto de hardware

Los costes de hardware son aquellos relacionados con las herramientas de hardware que el equipo necesitará para realizar las tareas. Estos se desglosan en dos principales recursos:

Para el desarrollo durante el proyecto se estima oportuno el uso de una infraestructura de desarrollo y ordenadores personales con características que cumplan con los requisitos del desarrollo. Se considera que con el presupuesto asignado será suficiente para cubrir las necesidades.

Los costes asociados a estos recursos son:

Tabla 15 Presupuesto de hardware

Recurso	Unidades	Coste por unidad (€)	Coste total
Infraestructura de desarrollo	1	15000	15000 €
Equipos de usuario para desarrollo	8	1200	9600 €

El presupuesto total de recursos de hardware se calcula en: **24600 €**

10.6.2.2 Presupuesto de software

Los costes de software son aquellos relacionados con las herramientas de software que el equipo va a necesitar para llevar a cabo el proyecto. Esto incluye licencias por uso, herramientas de desarrollo, etc. En el mercado se encuentran multitud de herramientas y software *Open Source* y de uso libre, por lo que el software que cumpla estas características no se incluirá en el presupuesto.

El desglose de costes de software es el siguiente:

Tabla 16 Presupuesto de software

Recurso	Unidades	Coste por unidad	Coste total
Sistema de chat (Slack)	8	6,25 €/mes	400 €

Herramientas de ofimática (Office 365)	8	10,50 €/mes	672 €
Recursos Cloud	1	2000 €	2000 €

El presupuesto total de recursos de software se calcula en: **16500 €**

10.6.2.3 Presupuesto recursos genéricos

Los costes genéricos son aquellos no incluidos en los anteriores apartados. Estos incluyen principalmente los gastos de oficina y de servicios para la operativa del proyecto.

Se considera un alquiler de una oficina de tamaño medio para los participantes del proyecto (dimensiones de 100 m2), a un coste medio por m2 de 25,25 €/m2 (Digital, 2020) en Barcelona.

A nivel de costes eléctricos, se establece un consumo medio de 52,5 KWh/m2 por año (*Energía en edificios de Oficinas.*, 2015), con las dimensiones de oficina anteriores de 100 m2. El precio medio por KWh en el año 2020 se establece en 12,14 céntimos (Facua.org, 2020). Con estos datos obtenemos el consumo medio mensual es de 437,5 KWh, es decir 53,11 €/mes.

Finalmente, los costes de internet se estipulan en una media de 53 €/mes (Kelisto, 2020).

Estos costes se calculan de forma mensual, teniendo en cuenta la duración del proyecto, establecida en 8 meses (Apartado 10.5.2).

Tabla 17 Presupuesto recursos genéricos

Recurso	Unidades (meses)	Coste por unidad (€)	Coste total
Gastos de oficina	8	2525	20200 €
Gastos de electricidad	8	53,11	424,88 €
Conexión Internet	8	53	424 €

El presupuesto total de recursos genéricos se calcula en: **21048,88 €**

10.6.3 Presupuesto total

Habiendo calculado ya el presupuesto de los costes humanos y no humanos, se procede a calcular el presupuesto total como la suma de ambos:

Tabla 18 Presupuesto total

Recursos	Coste
Recursos humanos	117379 €
Recursos no humanos	48720.88 €
TOTAL	166099.88 €

El presupuesto total de se calcula en: **175279 €**.

11 Validación externa de la propuesta

Con el fin de determinar la aceptación del mercado del producto NACTrack, se realizará un proceso de validación externa de la propuesta.

Para la realización de dicha validación se utilizará una encuesta (Anexo A) a diferentes personas del sector con el fin de obtener unas conclusiones relativas a la aceptación del producto NACTrack.

Esta encuesta se divide en 4 apartados. El primero nos servirá para determinar un perfil de los participantes, que responsabilidades tienen y las características de la empresa. El segundo apartado nos sirve para saber el conocimiento que tienen de la tecnología blockchain. Seguidamente se comprueba el conocimiento sobre los sistemas NAC. Finalmente se realizan preguntas relativas al producto NACTrack y la aceptación que podría tener.

Después de la realización de la encuesta y a partir de los resultados obtenidos (Anexo A) se determina que la muestra esta mayormente formada por gente con responsabilidades técnicas y que forman parte de pymes y grandes empresas. Estas empresas, en la gran mayoría (83,3 %), disponen de departamento de IT y un 58.3% de estas, ofrecen servicios IT a otras empresas.

En el apartado de blockchain, la familiarización con la tecnología blockchain podemos ver que está bastante igualada decantándose en mayor parte por el desconocimiento y no habiendo nadie con un conocimiento sólido en el ámbito. Aunque la mayoría de los participantes consideran que la tecnología blockchain no es suficientemente madura, creen que, en un futuro puede ser una tecnología revolucionaria. Respecto a los sectores, el 90% de los participantes creen que puede tener futuro en el sector financiero y el 80% en el sector logístico. Respecto al sector de ciberseguridad, un 50% cree la blockchain puede tener repercusión.

Respecto a la seguridad de las empresas de los participantes, la mitad afirman que han sufrido algún tipo de ataque informático. La mayoría de estas empresas (58,3%) no cuenta con un sistema de control de acceso a la red y la mayoría de los participantes no están familiarizados con dicha tecnología.

El cuarto y último apartado nos ayuda a conocer la opinión de nuestros participantes frente nuestra propuesta de aplicación (NACTrack).

La mayoría (58,3%) creen que la funcionalidad de NACTrack de mantener un registro de los accesos de los usuarios en la red interna sería de utilidad. Respecto a la característica de que los datos de registro almacenados fueran inmutables y plenamente confiables, la mayoría de los participantes opinan que tendría una importancia relevante.

Respecto a la característica de infraestructura descentralizada, no se obtiene un resultado concluyente dado que la mayoría no se decantan ni por un sí ni por un no.

Finalmente, ante la posibilidad de llevar a cabo la implementación, una vez detallado y explicado nuestro sistema a los participantes, estos valoran positivamente nuestra propuesta para mejorar su infraestructura.

12 Estudio del coste del TFG en horas de trabajo

Este TFG se inició en diciembre de 2020 y se dio por finalizado el mayo de 2021. Para la realización del trabajo se dividió este en bloques con el fin de realizar el proyecto de forma secuencial y ordenada.

Los bloques de trabajo son los siguientes:

- **Definición de concepto:** Antes de empezar la realización del trabajo se dedicaría un periodo de tiempo a la concepción y definición del proyecto. Aquí se incluiría la metodología del trabajo, los objetivos y una breve investigación sobre las tecnologías que se querían estudiar.
- **Documentación:** En este bloque se agruparán todas esas tareas relacionadas con la realización de la documentación del trabajo. Se incluye la estructura que se seguirá durante el trabajo, así como las tareas genéricas de toda documentación tales como la introducción, conclusiones o la revisión de formato y ortografía.
- **Estudio Blockchain:** El estudio de la blockchain incluye tanto la parte de investigación y estudio como la realización de la documentación relativa a esta tecnología de forma paralela.
- **Estudio sistemas NAC:** Al igual que el estudio anterior, el de los sistemas NAC también se basa en una investigación y estudio continuo a la par que se realiza la documentación relativa a este campo.
- **Propuesta de aplicación blockchain:** El bloque de aplicación incluye la investigación, concepción y propuesta de la solución de la tecnología blockchain sobre un sistema de tipo NAC.
- **Estudio organizacional y económico del desarrollo:** Este bloque agrupa los aspectos relacionados con la organización y gestión del proyecto de desarrollo del sistema NACTrack.

A continuación, podemos observar el diagrama Gantt correspondiente a los meses de trabajo de este TFG:

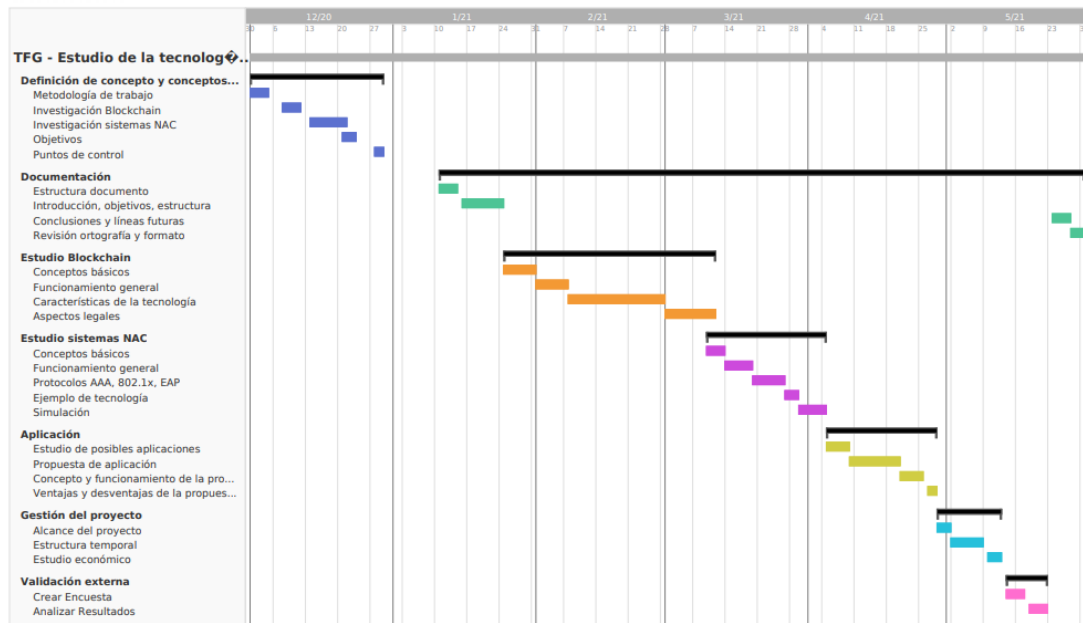


Ilustración 33 Diagrama Gantt Coste Real en horas de trabajo

Al final del trabajo se calcula un total de 152 días desglosados en los siguientes bloques:

- Definición de concepto → 20 días
- Documentación → 28 días
- Estudio Blockchain → 40 días
- Estudio sistemas NAC → 24 días
- Aplicación blockchain → 21 días
- Previsión del proyecto de desarrollo → 15 días
- Validación externa de la propuesta → 4 días

Se calcula que de media se han destinado 2,5 h por día dedicado al TFG por lo que el coste total en horas corresponde a:

$$152 \text{ días} * 2,5 \text{ h/día} = \mathbf{380 \text{ h}}$$

De esta forma el coste total ha sido de 380 h repartidas entre el mes de diciembre de 2020 y el mayo de 2021, es decir, 6 meses.

13 Conclusiones y líneas futuras

En este trabajo se ha realizado el estudio teórico de la tecnología blockchain y los sistemas NAC. Una vez se ha desarrollado una base de conocimiento sobre ambas tecnologías se ha realizado una propuesta teórica de aplicación de tecnología blockchain sobre sistemas NAC.

Los objetivos establecidos se han alcanzado de forma satisfactoria. Se aporta una visión clara de ambas tecnologías, sus usos, características y funcionamiento interno. Gracias a los conocimientos que se obtienen en la parte de estudio, se realiza una propuesta de aplicación de trazabilidad de activos de red mediante sistemas NAC. Esta propuesta mantiene una arquitectura extrapolable a muchos casos de uso en diferentes ámbitos.

La propuesta se fundamenta sobre una base sólida y aunque no cubre una necesidad explícita o un requisito indispensable en el mercado, la implantación de esta aplicación aporta un valor añadido al sistema NAC.

La propuesta de implementación no supone tampoco un gran beneficio en usuarios pequeños y es en grandes empresas u organismos gubernamentales donde sería de utilidad el uso de un sistema de trazabilidad como el expuesto.

En la previsión del desarrollo de NACTrack hemos observado que tendríamos una duración de desarrollo de 8 meses. Por otra parte, se ha establecido un presupuesto basado en los gastos de 166099,88 €.

Dados los resultados de la validación externa de la propuesta, se concluye que NACTrack puede ser un producto de utilidad y de interés. Por tanto, su desarrollo estaría justificado.

Aun siendo el principal objetivo el estudio de la tecnología y la consiguiente propuesta de aplicación de forma teórica, se considera que una implementación real del sistema a pequeña escala hubiera sido de interés para el desarrollo del trabajo. También hubiera permitido obtener datos reales para determinar la viabilidad del sistema propuesto, detallar que beneficios y que desventajas nos aporta desde un punto de vista empírico.

Otro aspecto que debería haber sido afrontado con mayor profundidad, ampliando la muestra de participantes, es la evaluación de la propuesta por parte de potenciales usuarios de la solución para validar si, a nivel de mercado, el producto sería aceptado.

La ciberseguridad está viviendo un crecimiento importante debido, en parte, a la transformación digital de las empresas. Esto hace que sea cada vez más importante contar con sistemas que ayuden no solo a prever ataques, sino a contar con información confiable para estudiar, desde un punto de vista forense, los ataques que se puedan sufrir.

La tecnología blockchain puede aportar grandes beneficios en multitud de sectores o productos, aun así, hay que determinar en cada caso su utilidad de uso dado que el uso de esta tecnología por simplemente tendencia puede acarrear mayores desventajas que beneficios.

13.1 Líneas Futuras

En líneas futuras se plantea la posibilidad de una implementación práctica de la aplicación propuesta modo de *Proof-of-Concept*. Finalizada la implementación práctica, sería conveniente un análisis de rendimiento para verificar la viabilidad del sistema.

Dadas las características de la propuesta definida, se considera oportuna la posibilidad de utilizar el registro blockchain para almacenar otro tipo de datos que pudieran ser de utilidad. Estos pueden incluir datos de red generados por sistemas como IDS, SIEM, Firewall o Antivirus. A mayor cantidad de datos mayor exactitud y detalle en la trazabilidad de activos de la red.

14 Referencias

- [1] Antonopoulos, A. M. (2014). *Mastering Bitcoin* (First Edition). O'Reilly Media, Inc.
- [2] Aruba Networks. (2015, octubre). *What is AAA?* Recuperado el 14 de marzo del 2021 de https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm
- [3] Binance. (2020, 10 diciembre). *Delegated Proof of Stake Explained*. Binance Academy. Recuperado el 16 de febrero del 2021 de <https://academy.binance.com/en/articles/delegated-proof-of-stake-explained>
- [4] Binance. (2021a). *Double Spending Explained*. Academy Binance. Recuperado el 18 de febrero del 2021 de <https://academy.binance.com/en/articles/double-spending-explained>
- [5] Binance. (2021b, abril 29). *Private, Public, and Consortium Blockchains - What's the Difference?* Academy Binance. Recuperado el 12 de febrero del 2021 de <https://academy.binance.com/en/articles/private-public-and-consortium-blockchains-whats-the-difference>
- [6] bit2me. (2020a). *What is a 51% Attack?* bit2me Academy. Recuperado el 19 de febrero del 2021 de <https://academy.bit2me.com/en/que-es-un-ataque-del-51/>
- [7] bit2me. (2020b, noviembre 10). *¿Qué es PoA (Proof of Authority - Prueba de Autoridad)?* Bit2me Academy. Recuperado el 16 de febrero del 2021 de <https://academy.bit2me.com/en/what-is-proof-of-authority-poa/#:%7E:text=PoA%2C%20is%20the%20acronym%20for,who%20participate%20in%20a%20blockchain.>
- [8] Bradford Networks. (2013). *802.1X and NAC: Best Practices for Effective Network Access Control*. https://cipherwire.net/wp-content/uploads/2013/06/802.1X_and_NAC___Best_Practices_for_Effective_Network_Access_Control.pdf
- [9] Brilliant. (2016, marzo). *Merkle Tree*. Recuperado el 14 de febrero del 2021 de <https://brilliant.org/wiki/merkle-tree/>
- [10] Chaum, D. (1983). *Blind signatures for untraceable payments*. Department of Computer Science, University of California.
- [11] Cisco Systems. (2018, 11 septiembre). *Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE*. Cisco. Recuperado el 10 de marzo del 2021 de https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/sw8021x.html

- [12] Dai, W. (1998). *b-money*. <http://www.weidai.com/bmoney.txt>
- [13] Data Network Resource. (2009, 21 marzo). *802.1X*. rhyshaden. Recuperado el 15 de marzo del 2021 <http://www.rhyshaden.com/8021x.htm>
- [14] DigiCash. (1994). *World's first electronic cash payment over computer networks*. https://www.chaum.com/ecash/articles/1994/05-27-94%20-%20World_s%20first%20electronic%20cash%20payment%20over%20computer%20networks.pdf
- [15] Digital, C. (2020, 17 abril). *¿Cuáles son los precios medios por el alquiler de oficinas?* Confidencial Digital. Recuperado el 9 de mayo del 2021 de <https://www.elconfidencialdigital.com/articulo/negocio/cuales-son-precios-medios-alquiler-oficinas/20190117174132120527.html#:~:text=Precios%20medios%20para%20alquilar%20oficinas&text=El%20precio%20de%20medio%20de,encontraba%20en%2025%20%E2%82%AC%2Fm%C2%B2>.
- [16] *Energía en edificios de Oficinas*. (2015, 17 junio). Enectiva. Recuperado el 9 de mayo del 2021 de [https://www.enectiva.cz/es/blog/2015/06/ideas-energia-edificio-de-oficinas/#:~:text=El%20valor%20medio%20\(el%20cual,\)%20es%20169%20kWh%2Fm%C2%B2](https://www.enectiva.cz/es/blog/2015/06/ideas-energia-edificio-de-oficinas/#:~:text=El%20valor%20medio%20(el%20cual,)%20es%20169%20kWh%2Fm%C2%B2).
- [17] Ethereum. (2020). *Proof-of-stake (PoS)*. Ethereum.Org. <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/>
- [18] Facua.org. (2020). *El precio del kWh en 2020 ha bajado un 14,5% con respecto a 2019*. Recuperado el 9 de mayo del 2021 de <https://www.facua.org/es/noticia.php?Id=16315#:~:text=En%20cuanto%20al%20precio%20del,14%2C20%20c%C3%A9ntimos%20de%202019>.
- [19] Grand View Research. (2020, febrero). *Digital Transformation Market Size, Share & Trends Analysis Report*. <https://www.grandviewresearch.com/industry-analysis/digital-transformation-market>
- [20] Haber, S., & Scott Stornetta, W. (1991). *How To Time-Stamp a Digital Document*. Bellcore.
- [21] Intel Corporation. (2021, 21 marzo). *Descripción general de 802.1X y tipos de EAP*. Intel LA. Recuperado el 15 de marzo del 2021 de <https://www.intel.la/content/www/xl/es/support/articles/000006999/wireless/legacy-intel-wireless-products.html>

- [22] Kelisto, R. (2020, 14 julio). *Los españoles pagan más por Internet que la media europea*. Kelisto. Recuperado el 9 de mayo del 2021 de <https://www.kelisto.es/internet/actualidad/los-espanoles-pagan-un-27-4-mas-por-internet-que-la-media-europea-6431#:~:text=Los%20consumidores%20espa%C3%B1oles%20pagan%20m%C3%A1s,de%20un%2027%2C4%25>.
- [23] Khan, R. (2020, marzo). *What is a Bitcoin Node?* Medium. Recuperado el 14 de febrero del 2021 de <https://medium.com/sazmining/what-is-a-bitcoin-node-b1106b050ace#:~:text=In%20the%20case%20of%20the,perform%20a%20different%20function%20entirely>.
- [24] Lee, J. (2017, 31 enero). *IEEE 802.11 Security*. junyeelee. Recuperado el 19 de abril del 2021 de <https://junyeelee.blogspot.com/2017/01/ieee-80211-security.html>
- [25] Meb, C. & Cisco Systems. (1999, diciembre). *AAA PROTOCOLS: Authentication, Authorization, and Accounting for the Internet*. IEEE INTERNET COMPUTING.
- [26] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org.
- [27] openNAC. (2014, noviembre). *openNAC Solution*. Recuperado el 25 de abril del 2021 de <http://www.opennac.org/opennac/en/solution.html>
- [28] Peh, B. (2018, 10 noviembre). *What are Public, Private and Hybrid Blockchains?* - Bernard Peh. Medium. Recuperado el 28 de marzo del 2021 de <https://medium.com/@blockchain101/what-are-public-private-and-hybrid-blockchains-e01d6e21eb41>
- [29] Qureshi, H. (2020, 9 junio). *P2P Networking*. NAKAMOTO. Recuperado el 31 de enero del 2021 <https://nakamoto.com/p2p-networking/#:~:text=A%20P2P%20network%20is%20a,the%20load%20of%20the%20network.&text=If%20a%20single%20node%20is,of%20the%20system%20chugs%20on>.
- [30] Randstad. (2021). *Informe de Tendencias Salariales 2021*. <https://www.randstadresearch.es/wp-content/uploads/2021/02/Randstad-Research-Informe-Tendencias-Salariales-2021.pdf>
- [31] Sectigostore. (2020, abril). *Types of Encryption: What to Know About Symmetric vs Asymmetric Encryption*. Recuperado el 19 de enero del 2021 de <https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/>
- [32] Smith, E. (2017, 5 diciembre). *Before There Was Bitcoin, There Was DigiCash*. Medium. Recuperado el 11 de febrero del 2021 <https://shortformernie.medium.com/before-there-was-bitcoin-there-was-digicash-fc2668c1d457>

- [33] Szabo, N. (2005, 29 diciembre). *Bit Gold*. nakamotoinstitute.
<https://nakamotoinstitute.org/bit-gold/>
- [34] The Law Library of Congress. (2018). *Regulation of Cryptocurrency Around the World*. Global Legal Research Center.
- [35] Tran, M., Choi, I., Jun Moon, G., Vu, A. V., & Suk Kang, M. (2020). *A Stealthier Partitioning Attack against Bitcoin Peer-to-Peer Network*. Japan Advanced Institute of Science and Technology.
- [36] Van Wirdum, A. (2018, 24 abril). *The genesis files: How David Chaum's ecash spawned a cypherpunk dream*. Bitcoin Magazine. Recuperado el 20 de enero del 2020 de <https://bitcoinmagazine.com/culture/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream>
- [37] Wikipedia contributors. (2020a). *Cryptographic hash function*. Wikipedia. Recuperado el 7 de febrero del 2020 de https://en.wikipedia.org/wiki/Cryptographic_hash_function
- [38] Wikipedia contributors. (2020b). *Proof of work*. Wikipedia. Recuperado el 21 de febrero del 2020 de https://en.wikipedia.org/wiki/Proof_of_work
- [39] Wikipedia contributors. (2020c). *Sybil attack*. Wikipedia. Recuperado el 5 de marzo del 2021 de https://en.wikipedia.org/wiki/Sybil_attack

Anexo A – Encuesta NACTrack

Estructura y preguntas de la encuesta

NACTrack - Trazabilidad de activos en la red

Esta encuesta forma parte del estudio de la aceptación de un producto de ciberseguridad para la realización de un Trabajo de Fin de Grado.

NACTrack es un sistema blockchain que se implementa junto a sistemas de Network Access Control y almacena eventos sobre la actividad de los usuarios en la red.

Indique que cargo tiene de su trabajo

- ☐ CEO
- ☐ CIO
- ☐ CTO
- ☐ Director
- ☐ Ingeniero de redes
- ☐ Consultor
- ☐ Profesor / Investigador
- ☐ Gestor de proyectos
- ☐ Desarrollador
- ☐ Comercial
- ☐ Otros: _____

Indique el tamaño de la empresa en la que trabaja

- ☐ Autonomo
- ☐ PYME
- ☐ Gran empresa

¿Existe departamento de IT en su empresa?

- ☐ Si
- ☐ No

¿Ofrece su empresa servicios de IT a otras empresas?

- ☐ Si
- ☐ No

Blockchain

¿Está familiarizado con la tecnología blockchain?

1 2 3 4 5

No la conozco ☐ ☐ ☐ ☐ ☐ Entiendo que es la blockchain y como funciona

¿Considera que blockchain es una tecnología madura?

☐ Sí

☐ No

☐ No lo se

¿Consideras que blockchain va a ser una tecnología revolucionaria?

☐ Si

☐ No

☐ No lo se

¿En qué sectores crees que puede tener mayor repercusión el uso de blockchain?

☐ Finanzas

☐ Alimentario

☐ Logístico

☐ Ciberseguridad

☐ Gubernamental

☐ Cultural

☐ Industria

☐ Altres: _____

Seguridad en la red

¿Crees que el sector de la ciberseguridad puede beneficiarse de la aplicación de tecnologías blockchain?

- ☐ Sí
- ☐ No
- ☐ Tal vez

¿Ha sufrido su empresa algún tipo de ataque informático?

- ☐ Sí
- ☐ No
- ☐ No que yo sepa

¿Existe en su empresa algún tipo de control de acceso a la red?

- ☐ Sí
- ☐ No
- ☐ No lo se

¿Está familiarizado con la tecnología NAC (Network Access Control)?

- | | 1 | 2 | 3 | 4 | 5 | |
|---------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-------------------------------------|
| No la conozco | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | Entiendo que es y su funcionamiento |

NACTrack

NACTrak es un producto que permite almacenar datos de trazabilidad relacionados con el acceso y comportamiento de los usuarios de la red. Estos datos se almacenan de forma segura en una red blockchain.

¿Crees que puede ser importante mantener un registro de los accesos de los usuarios en la red interna?

- ☐ Sí
- ☐ No
- ☐ Tal vez

¿Cómo valoraría el poder tener un registro completo relativo a los accesos a la red de su empresa?

- | | 1 | 2 | 3 | 4 | 5 | |
|----------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------|
| Negativo | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | Positivo |

¿Qué importancia le darías a que los datos de registro de acceso a la red fueran inmutables y plenamente confiables?

- | | 1 | 2 | 3 | 4 | 5 | |
|------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-------|
| Poca | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | Mucha |

¿Crees que la implantación de un sistema de infraestructura descentralizada puede aportar beneficios de seguridad respecto a un sistema centralizado?

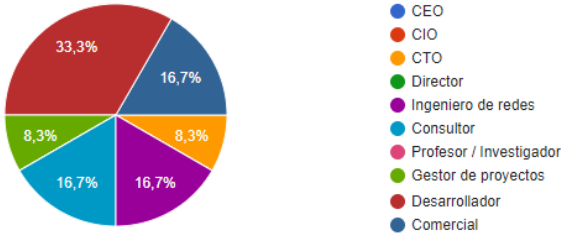
- ☐ Sí
- ☐ No
- ☐ Tal vez

¿Valoraría la posibilidad de implementación de un sistema con infraestructura descentralizada para almacenar el registro de actividad de los activos de la red?

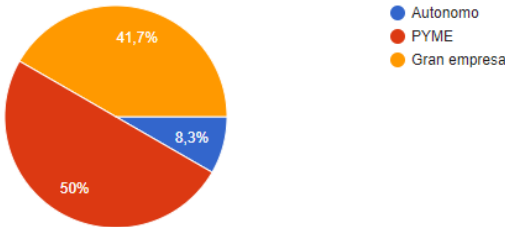
- ☐ Si
- ☐ No
- ☐ Tal vez

Resultados de la encuesta

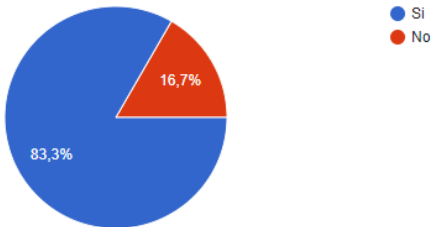
¿Que cargo se asimila más a su posición de trabajo actual?



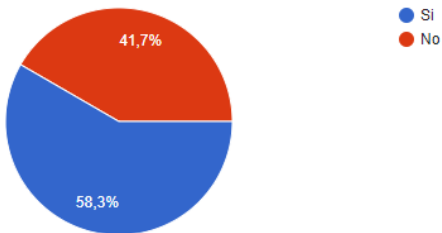
Indique el tamaño de la empresa en la que trabaja



¿Existe departamento de IT en su empresa?

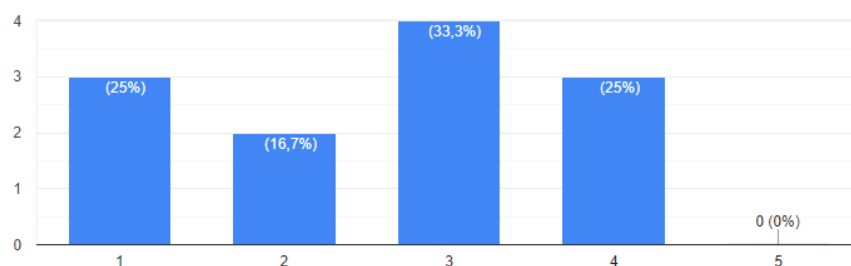


¿Ofrece su empresa servicios de IT a otras empresas?

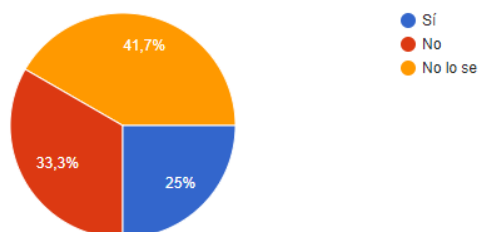


Blockchain

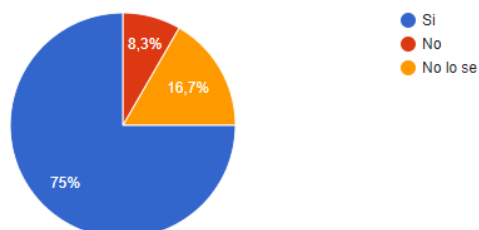
¿Está familiarizado con la tecnología blockchain?



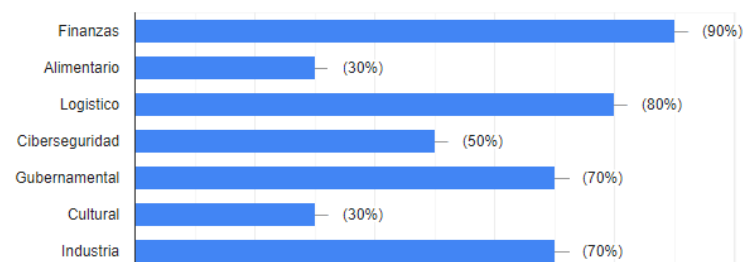
¿Considera que blockchain es una tecnología madura?



¿Consideras que blockchain va a ser una tecnología revolucionaria?

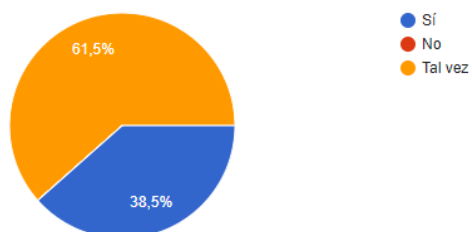


¿En qué sectores crees que puede tener mayor repercusión el uso de blockchain?

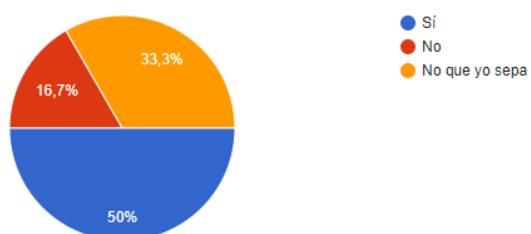


Seguridad en la red

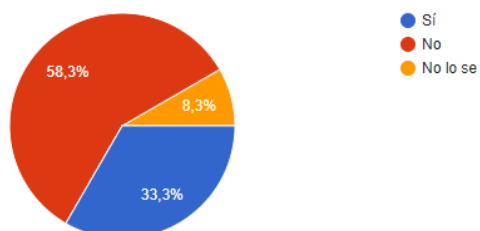
¿Crees que el sector de la ciberseguridad puede beneficiarse de la aplicación de tecnologías blockchain?



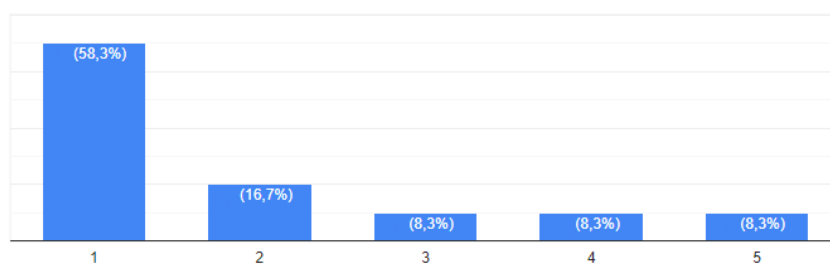
¿Ha sufrido su empresa algún tipo de ataque informático?



¿Existe en su empresa algún tipo de control de acceso a la red?

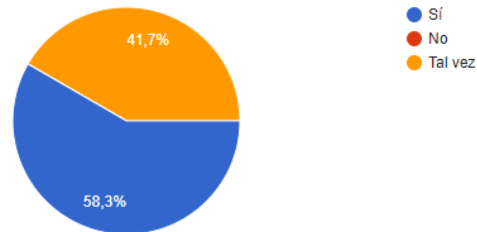


¿Está familiarizado con la tecnología NAC (Network Access Control)?

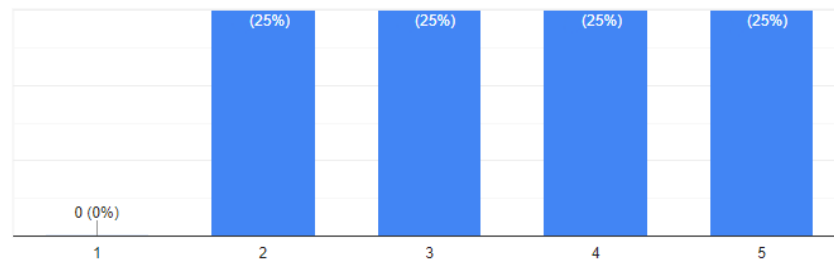


NACTrack

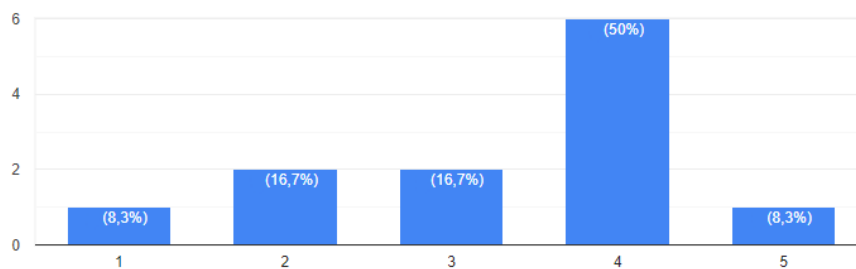
¿Crees que puede ser importante mantener un registro de los accesos de los usuarios en la red interna?



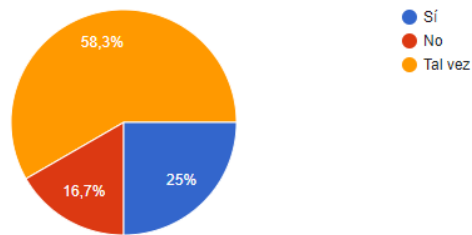
¿Cómo valoraría el poder tener un registro completo relativo a los accesos a la red de su empresa?



¿Qué importancia le darías a que los datos de registro de acceso a la red fueran inmutables y plenamente confiables?



¿Crees que la implantación de un sistema de infraestructura descentralizada puede aportar beneficios de seguridad respecto a un sistema centralizado?



¿Valoraría la posibilidad de implementación de un sistema con infraestructura descentralizada para almacenar el registro de actividad de los activos de la red?

