Universidad Zaragoza

Trabajo Fin de Máster

Tecnología cadena de bloques y criptomonedas. Blockchain technology and criptocurrencies.

Autor

Javier Macarrilla Bastida

Director

Jorge Rosell Martinez

ESCUELA DE INGENIERÍA Y ARQUITECTURA

2021

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

(Este documento debe acompañar al Trabajo Fin de Grado (TFG)/Trabajo Fin de Máster (TFM) cuando sea depositado para su evaluación).

TRABAJOS DE FIN DE GRADO / FIN DE MÁSTER

D./Dª. Javier Macarrilla Bastida,

con nº de DNI 76973395P en aplicación de lo dispuesto en el art. 14 (Derechos de autor) del Acuerdo de 11 de septiembre de 2014, del Consejo de Gobierno, por el que se aprueba el Reglamento de los TFG y TFM de la Universidad de Zaragoza,

Declaro que el presente Trabajo de Fin de (Grado/Máster) Máster, (Título del Trabajo) Tecnología cadena de bloques y criptomonedas.

Blockchain technology and criptocurrencies.

es de mi autoría y es original, no habiéndose utilizado fuente sin ser citada debidamente.

Zaragoza, 26 de Noviembre de 2021

Fdo:

AGRADECIMIENTOS

Agradezco a mis amigos por soportar mis quejas del trabajo. A mi familia por apoyarme, ayudarme (especialmente a mi madre) y siempre confiar en mi trabajo. Y por último, pero no menos importante, al director de este proyecto por su disponibilidad al afrontar esta propuesta y guiarme en este proyecto.

Título del resumen

RESUMEN

La tecnología Blockchain se basa en un protocolo de consenso: un algoritmo informático que proporciona un registro fiable de historiales de transacciones, haciendo que esta historia sea compartida, inmutable y abiertamente disponible para todos los participantes de la red Blockchain. Puede considerarse legítimamente una tecnología institucional que puede crear innovaciones radicales en el sistema actual de instituciones económicas del capitalismo. Además, muchos estudios [1] demuestran que debido a su estructura tokenizada, no solo conducirá a una reducción de costes, sino que también tendrá un efecto en los intermediarios, redirigiéndolos hacia la mejora de la calidad de las transacciones y la ampliación de servicios. Su fórmula de descentralización más tokenización puede causar muchas alteraciones en la organización de los procesos de negocio, que junto con los contratos inteligentes permitirán automatizar un gran número de aplicaciones como las certificaciones de un producto. También hablaremos de los Smart contracts, que pueden aportar mejoras en: negociaciones, transferencias, certificaciones y controles en distintos sectores del ámbito industrial.

Índice

Capítulo 1

Introducción y Objetivos

Durante los últimos años hemos visto como el mundo digital ha ido creciendo a un gran ritmo. El uso de internet es exponencial, cada vez se suben más fotos, se envían más mensajes y actualmente estamos incrementando el número de compras online, especialmente estos últimos años con la pandemia y esto se escenifica en que la economía digital actual esta determinada por una autoridad de confianza. Hacemos casi todo utilizando internet y cualquier transacción se basa en confiar en que al otro lado de la pantalla se lleven las acciones pactadas, puede ser un proveedor de servicios de correo electrónico que nos diga que nuestro correo electrónico ha sido entregado, puede ser una autoridad que certifique un papel etc. Esta confianza muchas veces no llega a ser del 100 %. Además, al comprador le supone una perdida de confidencialidad (cediendo datos personales e información del individuo), integridad (el servicio puede llegar a mantener esa información de forma perpetua) y no-repudio (no se puede negar a dar esta información si queremos adquirir ese servicio) [2]. Aquí es donde la tecnología Blockchain es útil y ha llegado de la mano de Bitcoin.

Blockchain es considerada una de las innovaciones más impactantes en los últimos años, hasta el punto que se compara con internet [3], llamando la atención académicamente e industrialmente. Esta tecnología tiene la capacidad de transformar los servicios financieros tal y como los conocemos, así como varios aspectos sociales. Su fórmula permite un consenso distribuido donde todas y cada una de las transacciones en línea, pasadas y presentes, que involucran activos digitales son verificables. Hace esto sin comprometer la privacidad de los activos digitales y las partes involucradas. El consenso distribuido y el anonimato o pseudo-anonimato son dos características importantes de la tecnología Blockchain de las que trataremos profundamente a lo largo de este trabajo.

La tecnología Blockchain se simplifica mucho si pensamos en un *Libro de contabilidad distribuido*, es decir, descentralizado, que permite de forma sencilla y en poco tiempo verificar y registrar transacciones. La tecnología permite a las partes

enviar, recibir y registrar valor o información a través de una red de computadoras denominadas nodos. Blockchain tiene una amplia gama de aplicaciones más allá de las conocidas *criptomonedas*, incluso como plataforma para los llamados contratos inteligentes o aplicaciones descentralizadas. Los contratos inteligentes son transacciones o contratos convertidos en código de ordenador que facilitan, ejecutan y hacen cumplir acuerdos comerciales entre dos o más partes. Los contratos inteligentes basados en Blockchain tienen el potencial de agilizar las transacciones financieras y disminuir el riesgo operacional. En este proyecto se explicará la tecnología y los conceptos fundamentales desde el ecosistema de la criptomoneda *Bitcoin*, por ser la que más efecto red genera y ser un estándar y punto de partida para el desarrollo de nuevos proyectos en el área del Blockchain. Lo que provoca que la mayoría de cadenas de bloques compartan estos conceptos. También se explicarán algunas aplicaciones no financieras de la tecnología, gracias a los ya mencionados Smart contracts. Para los *Smart contracts* (en español contratos inteligentes) nos fijaremos en la plataforma de fuente abierta *Etherum* ya que en el código de *Bitcoin*, estos son mucho más difíciles de implementar y en el caso de implementarse son demasiado simples para aplicaciones de empresas en el mundo real.

Tal y como se ha apuntado, el interés generado ha propiciado un desarrollo muy rápido de diversas propuestas. Pero en muchos casos no se han contemplado los riesgos que pueden llevar la acogida de esta tecnología, por eso en este trabajo también realizaremos una valoración de los riesgos que consideramos cruciales.

Capítulo 2

Definiendo Blockchain

¿Qué es Blockchain?

Una tecnología digital, que almacena y verifica todo el historial de transacciones entre pares de usuarios en una red propia. Estas transacciones son fácilmente verificables e inmutables, una vez se ha ingresado una transacción esta no puede ser alterada o borrada, características que generan confianza e integridad sin necesidad de un tercero. La podemos entender como una base de datos descentralizada que cumple con las siguientes características: está distribuida y compartida entre sus usuarios, utiliza métodos de encriptación para proporcionar seguridad y sirve como un depósito irreversible e incorruptible de información [3]. Desde el punto de vista técnico, es por lo tanto un libro de contabilidad distribuido *Distibuted Ledger Technology "DLT"* capaz de almacenar en paquetes, datos ordenados cronológicamente. Estos paquetes son denominados bloques, cada bloque esta ligado al anterior y al siguiente y así sucesivamente formando una cadena, por ello la tecnología es conocida como cadena de bloques.

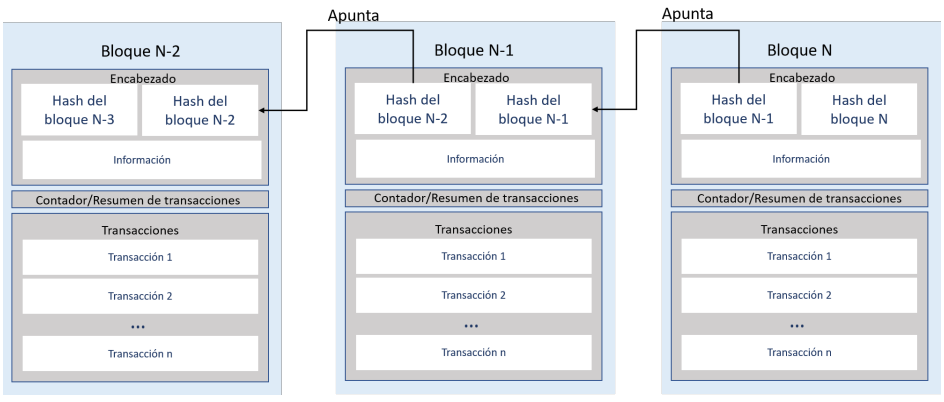

Figura 2.1: Encadenado de Bloques

2.1. Libro de contabilidad distribuido

Es la técnica para almacenar y acceder a la información a través de una base de datos compartida, capaz de operar sin la validación de un sistema centralizado. Es, por lo tanto, el historial completo de las transacciones ejecutadas en la red. Al ser un sistema distribuido, cada usuario de la red ejecutará el software para que el sistema funcione correctamente. El mantenimiento de la red lo realizan los propios participantes y la seguridad proviene con los sistemas de encriptación y minería que usará la Blockchain, para guardar información y para validar transacciones. Debido a esta distribución entre todos los usuarios, las transacciones pueden realizarse y verificarse de forma casi inmediata, aunque suelen tardar varios minutos para dar una mayor seguridad a la red. El desarrollo de esta técnica podría transformar los sistemas de pago, hacía un sistema en el que los bancos no fuesen estrictamente necesarios como intermediarios y estas transacciones funcionasen de forma descentralizada.

2.2. Conceptos Técnicos

Ahora que hemos explicado como funciona un sistema distribuido, vamos a profundizar en algunos conceptos técnicos para entender mejor las implicaciones de las diferentes arquitecturas respecto al desempeño de privacidad, seguridad e inmutabilidad.

Empezaremos por el **nodo**. Como ya se ha explicado en este capitulo, un sistema distribuido necesita de ordenadores que ejecuten el software de la Blockchain. A cada uno de estos ordenadores se les llama nodo, también denominados en inglés *peer*. Cada nodo conectado a una red Blockchain será capaz de recibir, enviar y verificar transacciones. Además, tendrá su propia copia del historial de la Blockchain sincronizada con el resto de nodos gracias a la tecnología *peer to peer* que explicaremos en el próximo capítulo. Este conjunto de nodos formará **la red**. En la actualidad las redes se dividen en tres tipos: redes públicas, híbridas (o de consorcio) y privadas (o autorizadas).

La red pública es aquella en la que cualquier persona con conexión a internet puede acceder, crear y validar nuevos bloques y participar en los procesos de votación. La capacidad de admitir tal cantidad de usuarios la hace mas descentralizada que el resto. Los procesos de votación de la red son importantes, porque necesitan una mayoría para realizar cambios en el código (funcionamiento de la red). Sin embargo, tiene un problema y es que su eficiencia es la mas baja de las tres redes. La red de consorcio tiene un sistema de votación diferente al de la red pública, ya que este proceso esta

limitado a un conjunto de nodos, los cuales son elegidos por el resto de la red o por un sistema aleatorio según el código; estos nodos serán los encargados de crear y validar los nuevos bloques. Produciendo una red más mutable, más centralizada y con una mayor eficiencia. En esta red la lectura del historial de transacciones podrá ser pública o privada. El último tipo de red es la privada, donde los permisos de escritura se mantienen centralizados, los de lectura pueden ser públicos o privados y tiene eficiencia y una mutabilidad más alta. Su uso, por el momento, se restringe a la administración de bases de datos o para auditorías internas de la empresa [4].

Las transacciones, tienen dos fases, la primera es donde un usuario de la red realiza una transacción y envía esta información a algunos nodos, estos a su vez la reenvían a otros nodos y así sucesivamente hasta que llegue a toda la red, conocida como envió de transacción (en ingles *submit transaction*). Y la segunda fase es de verificación y registro en el libro de contabilidad distribuido. Cada transacción realizada es objeto de aprobación, acción realizada por los nodos (mineros) de la Blockchain que reciben, procesan y validan criptográficamente cada transacción e ignoran las fraudulentas [5]. Actualmente asociamos que la **información** que contienen las transacciones en cualquier Blockchain es una transferencia monetaria, por ejemplo: María ha pagado a José 10 Bitcoins, pero esto es solo la punta del iceberg. La información contenida podría ser de un registro médico, certificación de un testamento, autenticar activos o propiedades...

Los nodos se encargarán de recoger aquellas transacciones validadas e incorporarlas a un **bloque**. Los bloques se dividen en varías partes encabezado , contador de transacciones y datos de las transacciones fig.2.2 (el contenido del bloque). Un bloque debe seguir un conjunto de normas predeterminadas en el propio código de la Blockchain. Normalmente, dichas normas son muy restrictivas con el tamaño del bloque ya que es importante que la información contenida en el mismo no exceda "x" bytes, por que un tamaño superior puede traer problemas cuando un nodo actualice el historial [6]. Cada bloque incorporado al historial se liga al último bloque que había sido incorporado y así sucesivamente formando la **Blockchain**.

El código es el software que ejecutan los ordenadores de la red (nodos) y que establece el conjunto de normas que rigen una Blockchain donde se especifican tamaños de bloques, las acciones que se pueden realizar, como por ejemplo, especificar si la red va a tener tokens, como es el caso de Bitcoin y especificar el número máximo de tokens que pueden existir o como se van a distribuir etc. Estos códigos en las redes públicas son abiertos, es decir, cualquiera puede acceder a ellos e incluso modificarlos. Cualquiera puede descargarse gratis el protocolo Bitcoin y tener una copia de la Blockchain. El protocolo usa la técnica del *bootstrapping*, que permite instalar el programa en el

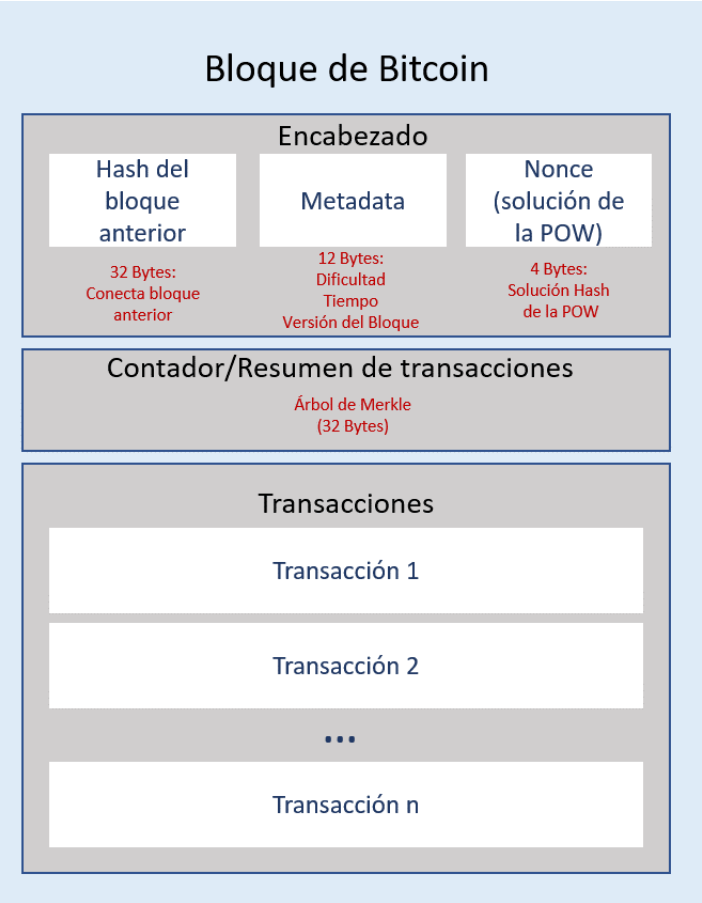

Figura 2.2: Bloque

ordenador o dispositivo móvil de un usuario siguiendo unas sencillas instrucciones que hacen funcionar el resto del programa. Técnica que ya se usaba en BitTorrent.

2.3. Principales Características

En el libro [7] se recogen una serie de principios esenciales para el correcto funcionamiento de una Blockchain. Para recoger estos puntos el libro se fija en el articulo de Satoshi Nakamoto [8] y en los foros y libros blancos que han surgido a lo largo del tiempo.

2.3.1. Integridad de la Red

Satoshi no sólo quería prescindir de la mediación de los bancos centrales, sino también eliminar la ambigüedad y las interpretaciones conflictivas de las transferencias. Que el código hable por sí mismo. Que la red busque algorítmicamente consenso sobre lo ocurrido, lo cifre y lo registre en forma de Blockchain. Todo el mundo puede ver las transacciones que se registran en el mismo momento en que se realizan. Nadie puede esconder ninguna, lo que hace que Bitcoin pueda seguirse mejor que el dinero

en efectivo. Ya hemos comentado durante este trabajo que la confianza es uno de los puntos claves a la hora de entender el Blockchain como una tecnología del futuro. Esta confianza, es proporcionada por el código de la Blockchain sin depender de cada miembro de la red, es decir, no hay que confiar en cada uno de los integrantes ya que los valores de honradez, transparencia y responsabilidad que generan la confianza están codificados gracias a estructuras de incentivos, derechos de votación y decisión.

Otra realidad que hace aumentar la integridad de la red es que mientras en internet la mayoría de información es maleable y fugaz y en muchos casos la hora y fechas exactas no son esenciales para la información pasada y futura, en la red Blockchain toda la información se guarda en bloques inmutables ordenados cronológicamente.

2.3.2. Descentralización

El sistema deberá distribuir poder por una red de iguales sin una autoridad que controle el resto de nodos. Además, esto permite que el apagón de uno o varios nodos no someta completamente la red, siempre que un nodo esté ejecutando el código, la Blockchain sobreviviría. Esta idea resuelve los problemas de bases de datos centralizadas y controladas por una institución, los poderes centrales han demostrado su voluntad y su capacidad de pasar por alto a los usuarios, almacenar y analizar sus datos, suministrar información al gobierno sin su conocimiento y realizar cambios importantes sin su consentimiento. Los principales beneficiarios serán aquellos ciudadanos de estados autoritarios o de países inestables o ante administraciones confiscatorias como la de Franklin Delano Roosevelt mediante el decreto 6102 [9] que obligaba a los ciudadanos a entregar al gobierno «monedas de oro, lingotes de oro y certificados de oro», pero también existen desventajas, como imposibilitar la capacidad de congelar cuentas a acusados en un juicio en estados democráticos.

2.3.3. EL Valor de la Red Como Incentivo

Al crearse la red de Bitcoin, Satoshi esperaba que los participantes actuaran en interés propio. Sabía que las redes sin protección eran vulnerables y habían recibido ataques llamados *Sybil*, que hacen que los nodos forjen múltiples identidades, los derechos se difuminen y el valor de la reputación se deprecie. Por eso Satoshi programó el código fuente de manera que, por muy egoístamente que actuemos, nuestras acciones beneficiarán al sistema en su conjunto. La exigencia de recursos del mecanismo de consenso, unida a la idea de premiar con bitcoins (a mayor valor mayor beneficio), podría persuadir a los participantes a comportarse correctamente y a resultar fiables en el sentido que se esperaba.

Figura 2.3: Bitcoin [10]

2.3.4. Seguridad

Está incorporada en el código fuente evitando puntos débiles. El código garantiza la confidencialidad, autenticidad y aceptación de todas las actividades realizadas, es decir, una transferencia es ejecutable sin necesidad de dar tu nombre o procedencia (al igual que cuando en un establecimiento pagamos en efectivo, nuestros datos personales no son revelados). Al realizar una transferencia monetaria, si tu dispones del crédito suficiente, nadie podrá evitar que ese pago se realice, sin importar lo que compres. Verificar, que un usuario es el poseedor de ese crédito, es muy sencillo debido a que todo queda registrado en el libro de contabilidad, visible para cualquiera en cualquier momento. Las claves para conseguir este sistema son: persistencia, anonimato o pseudoanonimato y auditabilidad (que se consigue gracias al almacenamiento público de todas las transacciones) [11].

Otra brecha de seguridad es la que surge cuando queremos acceder a cuentas digitales. Los principales problemas de este sistema son:

1. Al acceder desde un dispositivo los datos pueden ser robados.

2. El hackeo de una base de datos expondría el usuario y contraseña y por lo tanto el acceso a tu cuenta de personas que no deberían.

3. La gente repite contraseñas o estas son muy sencillas. Bitcoin resuelve este problema mediante el uso de firmas digitales.

2.3.5. Privacidad

La privacidad está definida como el ámbito de la vida personal de un individuo desarrollado en privado, con la idea de ser confidencial [12]. Esta idea debería permanecer en internet donde el sector público y privado han acumulado toneladas de información confidencial. Con la tecnología Blockchain sumado a la criptografía, nadie

tiene que proporcionar sus datos personales. Es como pagar en efectivo artículos en internet. Pese a que la red es completamente pseudoanónima, a la hora de entrar en ella se suele realizar mediante bolsas autorizadas, como puede ser *Binance*. Estas requieren cumplir unos requisitos .ªML/KYC", *Anti Money Laundering/ Know Your Costumer*, para evitar el blanqueo de capital y conocer al cliente. Esta información puede incluir tu dirección IP, información sobre el dispositivo etc. Información que los gobiernos pueden reclamar a los servicios de internet. Tradicionalmente el modelo de los bancos es ofrecer una capa de privacidad limitando el acceso de información, únicamente a las partes involucradas en una operación (Comprador vendedor y tercera parte de confianza). La necesidad de anunciar todas las transacciones públicamente es incompatible con este método, pero la privacidad aún se mantiene gracias al pseudoanonimato de las claves públicas. El público puede ver que alguien está enviando una cantidad para otra persona, pero sin información que vincule la transacción a datos personales. El riesgo es que si se revela el propietario de una clave, la vinculación podría revelar otras transacciones que pertenecían a el mismo dueño. [8]

2.3.6. Derechos e Inclusión

Es una de las ideas más importantes a la hora de entender el éxito de las redes Blockchain como Bitcoin. Permitir a todas las personas con acceso a internet pueden acceder a la red tirando barreras y obstáculos. Hoy en día hay un gran número de personas sin capacidad para tener cuentas bancarias y las grandes comisiones hacen difíciles los micropagos. El sistema Blockchain abarata los costes producidos por el giro de divisas, facilita el acceso a una cuenta bancaria, simplifica la manera de obtener crédito e invertir y fomenta el valor de las empresas y la participación en el comercio global. Además, ofrece derechos, evita el empobrecimiento de los ahorradores producto de la inflación. Tras la última pandemia vimos como los bancos centrales imprimían billetes para afrontar el gasto. Esto se esta traduciendo en la actualidad en una inflación del 5 %, en divisas como el euro o el dolar, disminuyendo el poder adquisitivo de los ahorradores. Pero en estados no tan desarrollados como Turquía esta inflación esta en el 19 %, produciendo un empobrecimiento gigantesco (en 3/4 años si se mantiene la divisa valdría un 50 % de lo que vale en la actualidad). Argentina ha visto como se deprecia su moneda nacional 1€ equivalía a 16,48 pesos en octubre del 2016; en octubre de este año cambias 115 pesos por 1€.

Capítulo 3

Fundamentos Técnicos

3.1. P2P

Si nos conectamos a la red de internet desde un dispositivo este es capaz de reproducir contenido multimedia, acceder a juegos... Esta información entra en nuestro ordenador en forma de paquetes y para recibirlos tiene que existir una fuente de almacenamiento que sea capaz de almacenarlos y luego enviarlos. Lo mas común es utilizar un modelo cliente servidor. En este método la información está centralizada en un servidor y esta no es enviada hasta que el usuario no realice una petición. En este caso un único cliente es capaz de conectarse a varios servidores. De cada servidor recibirá un tipo de información, por ejemplo, tu puedes usar los servidores de Spotify para escuchar música mientras lees un artículo digital.

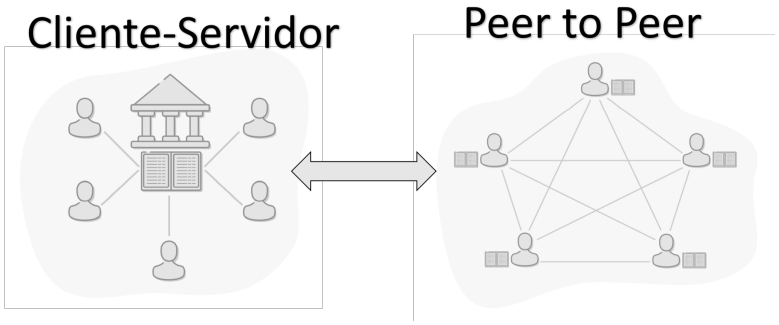

Figura 3.1: Esquema sistema centralizado y sistema distibuido

Pero esta no es la única forma de conectarse a una red y es que existe el método p2p. P2P es el acrónimo en ingles de *peer to peer* y significa " entre pares", es decir, se refiere a un sistema donde una persona interactúa con otra como iguales sin la necesidad de un intermediario. El principio de esta tecnología lo encontramos en el protocolo BitTorrent donde los usuarios descargan los archivos entre ellos directamente, divididos en pequeños fragmentos, una vez descargados permite a otros usuarios descargar de él, esos paquetes. Con este diseño, un archivo grande puede expandirse relativamente

rápido sin necesidad de grandes servidores. La idea es muy sencilla: conectar un gran número de nodos de manera aleatoria, los cuales comparten información entre sí. Por lo tanto, en este método cada dispositivo cumplirá dos funciones indistintamente la de servidor (enviando paquetes) y la de cliente (solicitando datos). Este sistema garantiza que la información pueda seguir fluyendo pese a la desconexión de algunos equipos de la red. En un sistema cliente-servidor, si un servidor se desconectara de la red las peticiones de los clientes no recibirían respuesta. Esto es lo que pasó hace poco, durante seis horas con los servidores de Facebook. Otro factor de riesgo es la perdida completa de datos si un servidor se estropea y no existe una copia actualizada en otro servidor. Este error sería menos probable en una red P2P ya que todos los nodos deberían eliminar los archivos.

3.2. Firmas digitales

Acabamos de explicar como la información circula a través de una red Blockchain, la cual se almacenará por todos los nodos de la red. Entonces: ¿cómo puede existir esa privacidad y seguridad de la que hemos hablado en el capítulo anterior? La solución que formuló el creador de Bitcoin fue el uso de dos llaves, una pública y otra privada criptadas asimétricamente. Estas claves, ligadas matemáticamente entre sí, son generadas de manera aleatoria, sin la necesidad de dar datos personales cuando se genera una nueva cuenta o dirección en la red de Bitcoin. El tamaño de estas claves es de 256 bits, aproximadamente 10 elevado a 77. Las probabilidades de adivinar una clave privada son prácticamente nulas. Para escenificar la magnitud, se estima que el número de átomos que tiene el universo es aproximadamente ese número. Las claves tienen números tan grandes para evitar que al crearse una clave coincida con una existente. La llave o clave privada debe mantenerse secreta. Sin embargo, la clave pública es la que compartiremos con el resto, la mostraremos cuando queramos recibir o enviar los tokens de la red Blockchain.

$$256bits = 2^{256} = 115,792,089,237,316,195,423,570,985,008,687,$$

$$907,853,269,984,665,640,564,039,457,584,007,913,129,639,936$$

La forma más rudimentaria de cifrar mensajes es mediante el uso de la criptografía de clave secreta. Este método es simétrico, es decir, utiliza la misma clave para cifrar como para descifrar mensajes. Entre los ejemplos más conocidos de este sistema está Enigma, un sistema empleado por Alemania durante la Segunda Guerra Mundial, en el que las claves se distribuían a diario en forma de libros de códigos [13]. Este método tiene muchas carencias y es quebrantable con tecnología de computación y si un tercero

conoce la clave puede interferir los mensajes cifrados. Satoshi Nakamoto pensó que el sistema era ineficaz para asegurar la red y diseño un cifrado para el par de claves público-privadas asimétrico. La idea es muy sencilla, con una clave podrás cifrar y con la otra descifrar. Para realizar una transacción el receptor generará un par de claves. La pública será la que pueda compartir y la utilizará el emisor para codificar la información. Una vez codificada esta información y actualizada en la cadena de bloques, el emisor no tiene acceso a ella, es decir, el envío ya se ha realizado, y solo el poseedor de la clave privada podrá usar el contenido del mensaje. Pero el emisor debe mostrar que él poseía esos datos antes del envío. Este proceso en el sistema bancario se verifica cuando das tu usuario y contraseña. Cuando mueves bitcoins, proporcionas una prueba de que eres propietario de esos bitcoins, posees la clave privada de la dirección X la cual esta representada por una clave pública. Esta prueba es la conocida como *Firma digital*[14]. Las firmas digitales llevan un proceso a la inversa. El emisor transforma el documento original a enviar, mediante la función Hash, en un conjunto de números y letras. Este conjunto se encripta con la llave privada del emisor 3.2. Cuando un nodo recibe el conjunto encriptado lo descifra usando la llave pública del remitente y si el resultado coincide con el Hash del documento original se garantiza que la dirección posee esos bitcoins y que este documento ha sido firmado por el remitente, por lo que éste no puede revertir el envío [15].

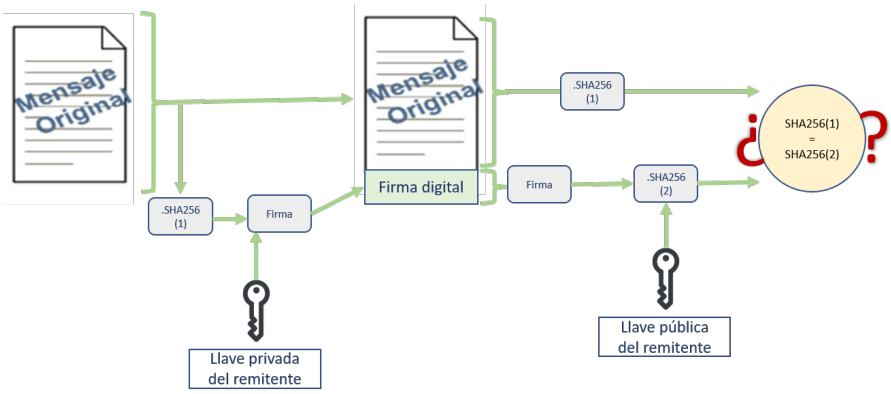

Figura 3.2: Comprobación firma digital

Resumiendo, la privacidad se adquiere gracias a la generación aleatoria de un número al crear una nueva cuenta o dirección en la red. Para realizar esta gestión, a diferencia de crear una cuenta con un banco, no revelamos ningún dato personal. La seguridad es ofrecida gracias al sistema de encriptación asimétrica y las claves privadas. Solo el poseedor de una clave privada puede gestionar los datos de una dirección ya que es la única manera de desencriptar la información del interior. Y el sistema asimétrico permite cifrar o descifrar sin revelar a nadie tu clave privada. Al contrario que en el caso de una firma en un cheque o tu contraseña de tu banco, tu firma digital es

especial para los datos de la transacción que estés firmando. Por lo tanto, no pueden ser robados y reutilizados en otra transacción diferente. Cada transacción obtiene una firma diferente, incluso si se envía desde la misma dirección pública.

3.3. Función Hash

Es un proceso capaz de tomar cualquier flujo de elementos entrantes y transformarlos en un rango de salida de longitud fija conocida como *Hash, Hashcode* o en español resumen"[16]. La función Hash es una caja negra, Bitcoin utiliza la función SHA256 desarrollada por la *National Security Administration* la cual sigue un conjunto de propiedades: es determinista, ya que se obtiene la misma salida para la misma entrada, esta salida es impredecible, el cambio de una sola letra en la entrada produce un Hashcode completamente distinto, dos entradas distintas no pueden producir la misma salida, son unidireccionales con una entrada es muy fácil obtener el Hascode pero el paso inverso no y la longitud siempre sera de 256 bits 3.3. La función Hash es esencial ya que se utiliza para firmas digitales, pruebas de trabajo, árboles de Merkle, direcciones de la Blockchain y la función Hash permite identificar un conjunto de datos públicamente sin revelar nada de los mismos.

Figura 3.3: Transformación de un Hash

Hemos explicado como las transacciones se agrupaban en bloques que se incorporan a la red en orden cronológico formando una cadena. Cada bloque es único e identificable por su Hash el cual se encuentra en el encabezado. Además, en el encabezado podemos encontrar el Hash que tenia justo el bloque anterior. En la Blockchain este proceso se conoce como (.ªpuntado.º que un bloque apunta al anterior fig.2.1). Este procedimiento se sucede hasta el conocido como bloque "genesis"que es el primer bloque. Los elementos entrantes que se utilizan para formar el Hash de cada bloque son dos las transacciones que recoge el bloque y el código Hash del bloque anterior. Esto produce una inmutabilidad en los bloque antiguos a la red, por ejemplo si nos encontramos en el bloque N (donde N es el tamaño actual de la Blockchain) y queremos cambiar una transacción del bloque N-3 tendremos que cambiar el Hashcode de ese bloque y por lo tanto el de todos los siguientes. El resto de nodos conocedores del Hash del último bloque sabrían que esa cadena ha sido modificada y la desecharían.

3.3.1. Arboles de Merkle

La Blockchain está en continuo crecimiento, siempre almacena mas datos que tampoco se pueden borrar. Este crecimiento es continuo en el tiempo y habrá un punto en el que algunos nodos se saturarían y la red dejaría de ser accesible para todo el mundo. Además, la verificación de cada transacción sería mas costosa. Por tanto, se creó un mecanismo que permita consultar de forma eficiente la red, es decir, consultar un bloque o una transacción sin la necesidad de descargarse todo el libro de contabilidad de la red. Bitcoin creo el sistema *Merkle root* traducido al español como árbol de Merkle. Formando una estructura piramidal de datos dividida en varias capas, relacionando todas las transacciones y agrupándolas entre pares. Cada capa se vincula con la inmediatamente superior mediante los códigos Hash. Y como pasaba con los bloques, el Hash de las capas superiores es el resultado de la suma de la información que contiene el nivel con el Hash del bloque anterior, de esta forma se conectan hasta formar el bloque completo que se introducirá en la cadena. Y como pasaba antes, la manipulación de un Hash invalida el resto. Este mecanismo permite generar una base de datos distribuida de forma eficiente y menos costosa. Proporciona inmutabilidad y permite la disección para realizar búsquedas más rápidas, de hecho, su uso facilita la descarga de una parte del historial.[17]

3.4. Minería

El minado explica como se generan los bloques, permitiendo el flujo de transacciones de la red. Es una competencia basada en el poder computacional y energético. Lo que deben de hacer es adivinar un número **Nonce**. Este Nonce nos permite que cada función Hash de los bloques se vea de determinada manera, es decir, que tenga una particularidad y en este caso consiste en que tenga un determinado número de ceros[18]. A mayor números de 0 menos números disponibles, por lo tanto, mayor dificultad para obtener la solución. Resumiendo, los mineros ejecutarán un algoritmo matemático prueba de trabajo (*"PoW" Proof of Work*), con la intención de adivinar la información del conjunto de transacciones que ha producido esa clave. El primero que lo consiga se llevará el premio de X Bitcoins. El numero de bitcoins que recibe el minero se reduce cada 210.000 bloques a la mitad (aproximadamente cada 4 años),actualmente es de 6.5 bitcoins por bloque minado. Hay otros sistemas de minado que permiten reducir el consumo energético como la prueba de participación (*"PoS" proof of stake*). Este sistema en vez de basarse en la capacidad computacional del minero se basa en la posesión del token. Con PoS la probabilidad de recibir la recompensa, por incorporar un bloque a la cadena, es directamente proporcional a la cantidad de monedas que uno

tiene acumuladas

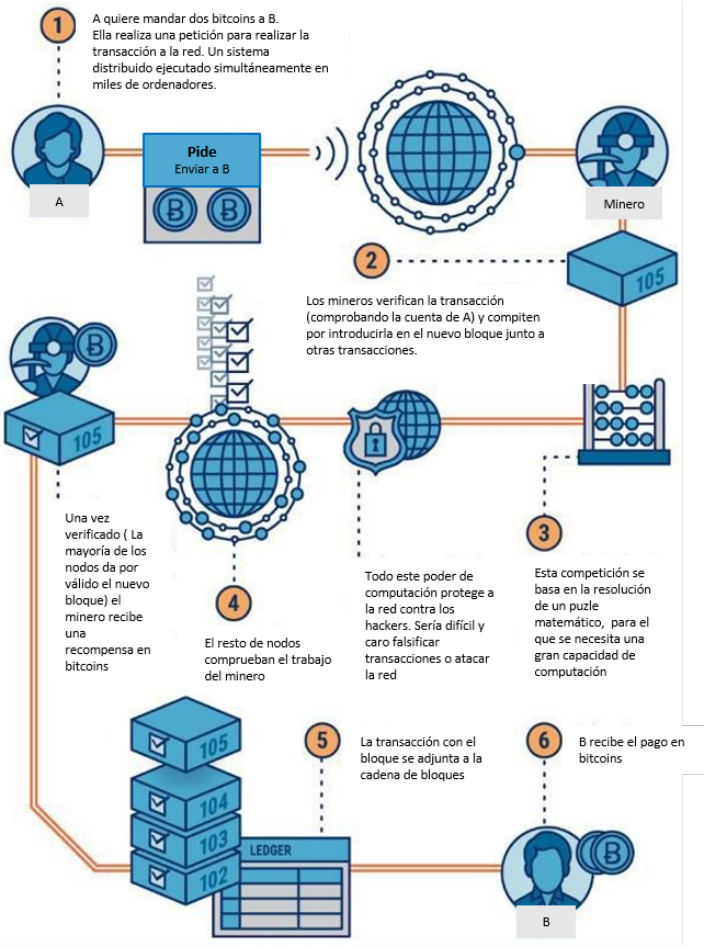

Figura 3.4: Transacción y minería [10]

Capítulo 4

Smart contracts y Aplicaciones

Hasta ahora hemos referenciado la mayoría de aspectos a la red Bitcoin por varias razones: es la red de la que suceden el resto y al ser de código abierto gran parte de ellas comparten estos aspectos. A día de hoy Bitcoin es, sin duda alguna, la realización práctica de la tecnología blockchain más conocida. Sin embargo, la lista de posibles casos de uso de la tecnología está en una fase temprana y evolucionando, un ejemplo de esta evolución es la incorporación de los contratos inteligentes *Smart contracts*. Bitcoin no se creó con la idea de ir evolucionando con el paso del tiempo, por eso para aspectos como este nos vamos a fijar en la que hoy en día es la segunda red mas popular dentro del ecosistema blockchain, Etherum.

4.1. Etherum

Una plataforma que fue efectiva tras 18 meses de trabajo de un equipo cuya figura mas representativa es Vitalik Buterin. El lanzamiento comenzó con la creación del bloque "génesis" en el año 2015 fig.4.1. En la web de Etherum se explica que es una plataforma capaz de lanzar aplicaciones de forma descentralizada (DApps), estas aplicaciones principalmente son los contratos inteligentes. Es importante saber que Etherum (La plataforma) se parece a Bitcoin en que su token (ether) motiva a una red de iguales para que validen las transacciones, protejan la red y creen consenso sobre lo que existe y lo que ha ocurrido. Pero se diferencia de Bitcoin en que incluye algunas poderosas herramientas para ayudar a los desarrolladores a crear servicios de software que van desde juegos descentralizados hasta mercados de acciones. Para entender las diferencias nos podemos remontar al inicio de su creación. Bitcoin fue diseñada como una red de ordenadores para transferir valor y Etherum fue creada para ejecutar *scripts* (códigos) . Para facilitar el uso de aplicaciones descentralizadas, Ethereum, emplea un lenguaje de programación (turing complete) denominado *Solidity*, necesario para poder alcanzar niveles de programación de aspectos muy avanzados, este sistema permite a los

desarrolladores crear aplicaciones que se ejecutan en el sistema Ethereum. Los contratos inteligentes de Ethereum residen en la máquina virtual de Etherum *Etherum Virtual Machine .EVM"*, lo que los aísla de la red Blockchain para evitar que el código que se ejecuta en el interior interfiera con otros procesos. Cuando el programador sube su programa a la red de Etherum, este se distribuye por todos los nodos (con el sistema peer-to-peer) y este código queda inmutable. Los nodos son los encargados de realizar el cálculo computacional. Esto permite que cualquiera pueda utilizar ese código. Al usar las funciones del programa tu tendrás que pagar, este pago se realiza a los nodos (que emplean sus recursos para ejecutar el código) con el token de la red, en este caso Ether. El otro sistema de financiación que tiene la red y sirve para evitar el *spam*, es el pago que realiza el programador para subir su código a la red. [19]

ethereum

Figura 4.1: etherum.org

4.2. Que es un contrato inteligente

Un contrato inteligente es un protocolo transaccional ejecutable desde un ordenador. Capaz de satisfacer condiciones contractuales normales: pagos, confidencialidad, etc, de minimizar las situaciones excepcionales, tanto accidentales como maliciosas y evitar en lo posible los intermediarios. Con el claro objetivo económico de reducir pérdidas por fraude, los costes de arbitraje y recursos legales, y otros costes transaccionales [20]. Con este formato las cláusulas son ejecutadas automáticamente cuando las condiciones pre-programadas se cumplen, (p. ej.4.2). Se pueden programar para que tengan una interfaz de usuario emulando un contrato en papel y facilitando la comprensión del mismo. Este tipo de contratos pueden soportar un elevado número de clausulas diferentes para contemplar todos los escenarios y llevar a cabo unas acciones u otras. Son dinámicos y capaces de captar mas tipos de información, como la sensorial adaptándose para ejecutar ciertas acciones [21]. Una de las características más importantes de contratos en la Blockchain es la capacidad de realizar transacciones "sin confianza". Las transacciones se pueden validar, monitorear y hacer cumplir bilateralmente a través de una red digital sin la necesidad de un tercer intermediario de confianza. Además, los contratos inteligentes se pueden ligar a una criptomoneda,

de esta forma se evitarían los pagos atrasados o los impagos. Puedes incorporar la funcionalidad firma múltiple, donde la aprobación de dos o más partes es necesaria antes de que se pueda ejecutar algún aspecto del contrato. Por ejemplo, la herencia de una casa para tres hermanos que para venderla necesiten la aprobación de los tres. Además en este caso, se podrían poner cláusulas de qué pasaría en los distintos escenarios (dos si quieren vender, uno no...). Los contratos inteligentes al igual que las redes Blockchain pueden ser públicos (donde cualquier nodo puede subir un contrato y cualquier usuario puede usarlo como ocurre en Etherum) o autorizados los cuales residen en redes Blockchain autorizadas (con permiso para participar). Estos últimos se están volviendo cada vez más populares en las colaboraciones comerciales. La principal ventaja con respecto a los públicos es que los procesos son más rápidos, eficientes y menos costosos.

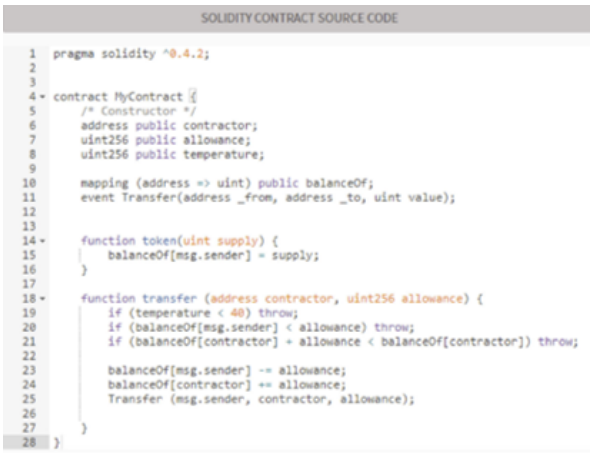

Figura 4.2: Contrato inteligente pasado a código [22]

La tecnología Blockchain ha vuelto mucho más fácil registrar, verificar y ejecutar los contratos inteligentes. En Etherum hay muchos casos de uso de estos contratos inteligentes. La red permite crear tu propia criptomoneda a modo de contabilidad propia. Por ejemplo bit2me, una empresa española que hace las funciones de cartera y *exchange* de criptomonedas, va a lanzar su propia moneda que permite a los usuarios utilizar la plataforma con una serie de ventajas, por ejemplo, comisiones más bajas, mientras la empresa adquiere financiación. Otro caso de uso son los NFTs (Non fungible tokens) y arte digital, donde tu puedes generar una representación digital de algo que se convierte matemáticamente, que por el hecho de ser únicos, algunos lo consideran arte por si solo o le puedes vincular una representación visual. En la actualidad nos encontramos en este punto de representación visual, pero puede llegar el punto que estas representaciones convivan en un mismo ecosistema en la red formando un Metaverso.

Ahora veremos algunas aplicaciones de estos contratos en el sector de la industria.

Algunos ya tienen proyectos en marcha, otros sirven para exponer el potencial de esta tecnología.

4.3. Industria de la Salud

Es una de las áreas donde más se están aplicando los contratos inteligentes, especialmente tras la pandemia. Entre sus múltiples posibles aplicaciones destacan dos: en la linea de distribución de medicamentos y en los registros médicos. Nos podríamos fijar en la morfina como un caso específico de la linea de suministro de medicamentos, gracias a los contratos inteligentes se podrían seguir el proceso de producción y distribución completo, desde la fábrica donde se produce hasta el paciente final. En este caso los lotes serían autentificados y marcados (con fecha y hora) en cada punto de entrega intermedio. Este registro se iría guardando en la red Blockchain permitiendo un seguimiento perfecto, sin errores e inmutable, por las propias características de la red fig.4.3. Esto simplifica y agiliza enormemente la gestión de la línea de distribución de medicamentos, que puede evitar que los medicamentos caigan en las manos equivocadas, asegurando la distribución del medicamento en el consumidor final, lo que en gran medida reduce la posibilidad de falsificación, manipulación de precios y entrega de medicamentos caducados. Actualmente Bayer utiliza la red VeChain para el seguimiento de medicamentos.

Figura 4.3: Control de medicamentos con Blockchain [23]

En cuanto a los registros médicos muchos profesionales del sector piensan que sería una forma segura de compartir y acceder al historial de un paciente. Con el proceso de *Firma Múltiple* el acceso a un registro estaría permitido a algunos usuarios solo si paciente y doctor lo autorizan. También permitirían la interoperabilidad entre los distintos sectores de la medicina para mantener un registro de forma mas efectiva y consistente. Los contratos inteligentes también pueden ser utilizados para otorgar a los investigadores acceso a ciertos datos personales de salud y permitir micropagos que

se transferirán automáticamente a los pacientes para su participación sin revelar la identidad de estos, es decir, autorizar parcialmente al registro médico para investigar.

4.4. Agencias Gobernamentales

Las agencias públicas pueden beneficiarse enormemente de un acceso casi instantáneo y simultáneo a una red distribuida que guarda registros públicos. Por ejemplo, los pasaportes o licencias de conducir se pueden colocar en Blockchain, lo que permite a múltiples agencias compartir, acceder y verificar la identificación en tiempo real incluso en distintos países. Esta tecnología no está todavía implantada pero hay gobiernos como el de Estonia o el Salvador que están experimentando con esta posibilidad [24]. Otro ejemplo son las aplicaciones regulatorias y tributaciones. Muchos bancos e instituciones financieras están trabajando actualmente para ubicar datos financieros personales en la Blockchain. Los reguladores pueden imponer directamente restricciones en la ejecución de transacciones en Blockchain para que se apliquen automáticamente. Grabar las transacciones en el libro de contabilidad de forma automática permite: un seguimiento de la transferencia de propiedad, que las agencias tributarias puedan realizar un seguimiento, reducir pagos por auditorías y evitar otros procesos intermedios.

Otra aplicación serian las ayudas extranjeras ante catástrofes humanas. El uso de transferencias transfronterizas se realizaría de una manera mucho más específica y eficiente y centrada en los destinatarios afectados. Estas ayudas llegarían directamente a la zona del desastre. También serían útiles en zonas de guerra. Reducirían gastos que, por ejemplo, una .ºNG"produce a la hora de enviar efectivos. Por último usando la tecnología Blockchain se puede implementar un sistema de votación completamente anónima y verificable en la que cada ciudadano pueda participar. Elimina una sobrecarga considerable del entorno de votación, desde la preparación de mesas electorales los recursos para realizar el conteo. Es una campo con un enorme potencial pero que solo se le conocen pequeños estudios experimentales

4.5. Industria de la Construcción

El primer desafío al que se enfrentan las corporaciones que se dedican a la construcción es la confianza en cada aspecto de sus actividades. Para empezar a la hora de elaborar un contrato, en este sector estos suelen ser de suma global, es decir, cotizado a un precio único para un proyecto completo basado en planos y especificaciones, donde normalmente se selecciona el que ofrece el precio más bajo. En este tipo de proyectos se

producen cambios constantes en los requisitos del proyecto que afectan a la confianza. El segundo desafío al que se enfrenta esta industria es la cadena de suministros, y pese a que muchos estudios se han centrado en mejorar la administración de suministros, este sigue siendo un problema general. En muchos casos los suministros llegan con retraso o en malas condiciones. Es un problema producido por muchos factores pero la falta de trazabilidad, transparencia y comunicación (entre las partes involucradas en el proyecto) son los principales. En un proyecto complejo y grande para conseguir transparencia en la cadena de suministros se requiere que la información de cada producto sea documentada y guardada de forma muy precisa en una base de datos, para analizar las consecuencias de cada decisión. Esto trae gastos de documentación, almacenamiento y análisis. El manejo de activos es otro punto crítico, como ya pasaba en la cadena de suministros compartir datos entre las diferentes partes es complejo, ya que en muchos casos no se quiere revelar información privada, y otras veces se obtienen datos duplicados. En proyectos de este tipo se recomienda que tales datos se encuentren distribuidos geográficamente en múltiples sitios, reduciendo riesgos de que una sola identidad posea todos los datos de los activos. En la actualidad cada entidad guarda sus propios archivos en bases de datos internas dificultando la interoperabilidad. Proporcionar datos a una plataforma de otras empresas conduce a la reticencia de los participantes.

Por los problemas relatados se puede ver el gran potencial que tendría esta tecnología en el sector de la construcción. Primero en relación a los documentos notariales. Estos documentos dejarían de necesitar verificaciones de autenticidad. Las empresas del sector emplean un gran número de recursos, trabajo y tiempo en estudiar las crecientes regulaciones de los gobiernos, aun más cuando la entidad opera en distintos países. Asimismo, tienen que preservar la integridad de cada documento durante su almacenamiento y/o retiro. El uso de redes Blockchain permitiría almacenar estos documentos en un sistema distribuido donde hay una notarización perfecta de cada creación, eliminación y actualización de documentos en el sistema. Esta aplicación puede utilizarse para registrar datos sobre calidad de la construcción, instalaciones o de las materias primas. Favorecería una mayor información sobre el progreso del proyecto y los recursos empleados.

Aplicaciones relacionadas con transacciones podrían facilitar la adquisición y el pago de manera automática. Este proceso de automatización de pagos es fácil de implementar para realizar transferencia de título de propiedad, evitando controversias típicas del sector relacionados con el pago, la transferencia de tecnología, el arrendamiento de equipamiento y la venta de casas. Con tales aplicaciones, se puede ahorrar un tiempo y un costo significativo si todos los procesos son automatizados. Obviamente, en la cadena

de suministros, las aplicaciones para conocer la procedencia de los materiales mejoraría los problemas comentados de trazabilidad y transparencia. Ya que cada transacción es visible en el ecosistema Blockchain, es fácil rastrear hacia atrás el suministro de cada producto o servicio con autenticidad de un cumplimiento o garantía de calidad. Por ejemplo, durante la operación y etapa de mantenimiento, si un defecto grave de un producto es encontrado, tendremos disponibles el historial completo desde la fabricación hasta la colocación. Encontrando la parte responsable sin necesidad de costosos y tediosos peritajes.

Otro tema comentado anteriormente es la capacidad de ligar una criptomoneda al contrato a modo de seguro. En el sector de la construcción es común encontrar disputas por el retraso de pagos, debido a la existencia de un gran número de subcontratas y pago a proveedores. Veamos el ejemplo de una constructora que compra hormigón a un proveedor. La constructora depositará una cierta cantidad de criptomonedas (100 ether) para asegurar que el pago se realizará cuando reciba correctamente el material acordado. El proveedor depositará 25 ether como garantía de calidad y cumplimiento de plazos, es decir, si no hay retrasos en las entregas y llegan en buen estado recibirá de vuelta este depósito. Estos depósitos se irán liberando según las condiciones del contrato. [22]

4.6. Industria alimentaria

El consumidor de este sector da un gran valor a como son tratatos los productos y cual es su origen, es decir, la trazabilidad es un punto clave en este sector. Actualmente, estos registros son recogidos en una base central administrada y gobernada por los propios vendedores del producto, lo que se traduce en falta de confianza en el cliente. La única excepción han sido los sistemas de trazabilidad de obligado cumplimiento, bajo el control de organizaciones gubernamentales o asociaciones independientes. La tecnología Blockchain, gracias a su registro distribuido, traería tres importantes soluciones a este ámbito. La primera es una ganancia en los costes monetarios, este sistema contribuye a la prevención de incidencias dado que facilita la ubicación exacta de lotes o productos y, en caso de surgir inconvenientes, facilita la retirada efectiva y selectiva del alimento deteriorado, sin desechar productos que no están afectados. En segundo lugar, traería beneficios a la hora de verificar la información, reduciendo el tiempo necesario para esta tarea. Ya que todos los registros quedan ordenados de manera cronológica y estos son inmutables, lo que produce una mayor auditabilidad de los productos. Y por último, generaría una cadena de confianza entre las partes involucradas, posibilitando la transparencia en el movimiento de un producto a través de sus distintas etapas,

partiendo de la producción hasta llegar al consumidor final [25]. Este sistema ya está implantado en algunos sectores. Actualmente, el del vino es el que más interés ha generado debido a su utilidad para certificar la D.O. de sus viñedos. Incluso yendo un paso más allá, ya que han integrado datos obtenidos a partir de sensores incorporados en los viñedos para dar al consumidor una mayor información sobre las condiciones de cultivo [26].

4.7. Industria Automotriz

Ya hay empresas del sector que están experimentando con esta tecnología, como Seat y otras grandes marcas como Mercedes o Ford, estudiando las ventajas de implementarla. En la cadena de suministros ya se ha comentado que permitiría al consumidor final comprobar todo el ciclo de vida del vehículo que desea adquirir: materia prima, calidad de componentes, reparaciones e incluso accidentes sufridos. Los gobiernos tendrían información veraz y actualizada sobre los vehículos en circulación, con la que plantear estrategias de desarrollo sostenible, incrementar seguridad vial o reducir emisiones. Además, gracias a los Smart contracts, se podría crear un mercado abierto para compraventa de materiales. Cuando una marca necesitase una materia mandaría una petición a la red. Los proveedores que utilicen la plataforma podrán presentar ofertas (especificando: precio, fechas de entrega...). Entonces, el fabricante elegirá la que mejor se adaptase a sus necesidades y al mejor precio. Las dos ventajas serían: la automatización y la posibilidad de establecer condicionantes. Por ejemplo, el deterioro de la mercancía o el retraso en el abastecimiento podrá ser castigado con una multa que no dependerá de valoraciones subjetivas. Facilitará la identificación de las partes que cometan infracciones contractuales reduciendo su valoración dentro de la plataforma [27].

4.8. Reestructurar la Empresa

Cuando se creo internet varios agentes pensaron que la estructura de las empresas pasaría de jerarquizada a estructuras horizontales o de innovación abierta. Sin embargo, vemos que las empresas tienen una estructura similar a la era industrial. Si que vemos cambios a la hora de comerciar. Por ejemplo, ahora hay más subcontratas y transacciones internacionales traduciéndose en abaratamiento de costes y las comunicaciones son mejores permitiendo ver multinacionales con sedes en distintos lugares del mundo. Pero la estructuras de las empresas más exitosas, incluso las más tecnológicas e innovadoras como Google o Amazon, son jerarquizadas. Las razones

por las que se sigue manteniendo la estructura, principalmente es por que en otro tipo de estructuras (como la horizontal, donde todos pueden tomar decisiones) los intereses personales podrían oponerse a los de la empresa. Los contratos inteligentes nos permiten crear organizaciones autónomas descentralizadas *Decentralized Autonomus Organizations "DAOs"*. Entornos donde todos los integrantes sin necesidad de una regulación pueden tomar decisiones de forma colaborativa y democrática en función de la cantidad de participación que tengan dentro de la "DAO". Aquí se aplica el equilibrio de Nash o la teoría de juegos, una situación en la cual todos los jugadores han puesto en práctica, y saben que lo han hecho, una estrategia que maximiza sus ganancias dadas las estrategias de los otros, por lo tanto a participación más alta más interés en que la organización crezca para obtener más beneficio [28].

Capítulo 5

Riesgos y Problemas

Blockchain es una prometedora tecnología con un gran número de aplicaciones. Estas aplicaciones no se quedan solo en el marco financiero sino que van mas allá; son capaces de realizar funciones notariales. Pero como todos los cambios de paradigma, su adopción conlleva una serie de riesgos. Por esa razón, se expondrán a continuación los que hemos considerado mas relevantes.

5.1. Despilfarro Energético

El consumo de energía que realiza la red se puede dividir en dos partes. Por un lado, existe un consumo mínimo a la hora de realizar la transferencia (sería el mismo que utilizamos al mandar un bizum mediante un banco). Por otro lado el consumo de la minería el cual si es muy relevante. Como se ha explicado en el capítulo 3 la minería es la competición entre miembros de la red por resolver problemas matemáticos, para verificar las transacciones y obtener una recompensa. Actualmente tenemos un gran número de equipos compitiendo en cada bloque, para que solo uno lo resuelva, lo que produce que todo el consumo energético de los demás equipos no adquiere una recompensa. Si crecen los equipos de minería por el propio código de Bitcoin incrementará la dificultad de minar un nuevo bloque, es decir, necesitamos más energía. Esto hace ver a Bitcoin como un enemigo energético, incluso estudios estiman que la red consume mas recursos energéticos que países como Argentina. Sin embargo, la minería es un proceso fundamental para hacer segura la red. Además, hay estudios que demuestran como Bitcoin favorece la adopción de energías renovables y su consumo es muy inferior al de los sistemas bancarios [29]. Pero esto no es todo, existen alternativas a la minería de "PoWçomo el "PoS"que reduce enormemente el consumo de la red[30]. Este término siempre tendrá una parte muy subjetiva por dos razones: no se puede conocer exactamente la energía consumida de los mineros ni su procedencia y todo depende de la visión que tengas hacia las criptomonedas, como medio para escapar de

la inflación represión monetaria y control capital o como un sistema de blanqueo de dinero o un sistema de estafa.

5.1.1. Ataque del 51 % o Control Sobre la Red

Un ataque del 51 % se produce en el instante que una persona controla el 51 % del poder computacional de la red. Es decir, dispondría de más de la capacidad de cálculo que todos los demás mineros y más participación para las "votaciones" que el resto junto. Pero en la práctica es casi imposible debido a los altos gastos para emparejar tu capacidad al de toda la red. En el caso de que se consiguiese este escenario inverosímil, empleando gigantescos recursos económicos, podría funcionar a corto plazo pero a mediano largo plazo la gente perdería la confianza en la red y su valor decrecería rápidamente, produciendo perdidas económicas para el atacante. En este artículo se relata de manera mas extensa por que actualmente este ataque no es viable [31].

5.1.2. Puertas Traseras o Hackeos

La seguridad de bases de datos en la actualidad dependen de ordenadores impenetrables ante los ataques cibernéticos. Esto suele estar ligado a tener el último sistema de seguridad actualizado, los mejores firewall, sistemas antivirus etc. Esto implica grandes costes. Bitcoin, por otro lado, está compuesto por un conjunto de ordenadores, los nodos, un ordenador que tenemos por casa con mil virus puede pertenecer a la red, por eso el protocolo Bitcoin trabaja con la hipótesis de que todos los nodos son atacantes hostiles. Deberíamos hackear gran número de equipos para controlar la red Otro posible riesgo es corromper los hardware que ejecutan el software de la Blockchain. Por ejemplo, las empresas que producen los equipos dedicados al minado podrían instalar programas maliciosos indetectables. Este equipo podría ser controlado por un agente externo favoreciendo un ataque del 51 %. También se puede colocar una puerta trasera en un ordenador o realizar hackeos a equipos que permitan acceder a claves privadas de un usuario y, por lo tanto, acceso a sus criptomonedas. Es de los riesgos mas viables que podrían dañar la imagen de Bitcoin. Además, actualmente no hay tantos fabricantes de equipos de minería pese a que este número esta creciendo, constituyendo uno de los únicos puntos débiles. [32]

5.2. Doble Gasto

Este ataque se produce cuando un usuario trata de utilizar la misma moneda varias veces. Si estuviésemos en un sistema centralizado como un banco, mirando su base de datos puede decirte rápidamente que estás intentando utilizar el dinero que ya te

has gastado. El problema del sistema descentralizado es que la información no viaja igual a todos los nodos y podemos encontrar bifurcaciones en las cadenas de bloques. Pongamos que Alicia tiene 2 btc y manda 2 btc a Bob, entonces toda la red actualiza la contabilidad y si Alicia tratase de enviar otros 2 btc, la red no aceptarían esta transacción como válida. Ahora vamos al caso en el que Alicia no da tiempo a todos los miembros a actualizar la red, se produce la bifurcación, en una rama encontraremos una transacción y en otra rama la otra transacción, dando el problema de doble gasto, en este punto se produce una carrera por conseguir la cadena más larga. Ya que por el propio protocolo de Bitcoin al descargar el libro de contabilidad lo actualizas con respecto a la cadena más larga. Escoger la cadena mas larga tiene dos razones. La cadena mas larga (5.1)es la que mas trabajo tiene y por lo tanto suele ser la más segura. La segunda razón es para obtener un consenso sobre el historial de transacciones. Imaginemos que un nuevo nodo se quiere unir a la red, primero se conectará a una serie de nodos, que le pueden mandar copias falsas o desfasadas del libro de contabilidad. Entonces, el nuevo nodo para saber cual es la copia buena, medirá la prueba de trabajo acumulada y la de mayor cantidad será considerada como la autentica.

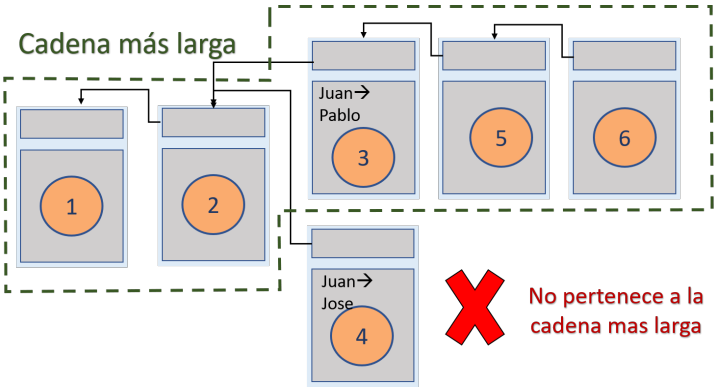

Figura 5.1: Cadena más larga

5.3. Escalabilidad

Bitcoin tiene estipulado en su código que el tamaño por bloque sean aproximadamente de un megabyte esto produce que el número de transacciones diarias que soporta la red son de 500.000 operaciones [32]. Cuando se supera este número produce un incremento en los costes de transacción. El problema vendría con la adopción masiva de esta tecnología que produciría tasas incluso más grandes que los propios pagos. Una solución sería aumentar la capacidad de cada bloque a 1 megabyte, esto debería ser sometido a consenso por todos los nodos de la red, y las veces que así ha sido se ha acabado descartando los cambios por falta de consenso. Asimismo, debido a

su naturaleza descentralizada el incremento en la capacidad de los bloques, produciría un aumento en el coste de memoria al registrar transacciones, dejando algunos equipos obsoletos.

5.4. Cierre internet

Podría ocurrir que se produjese una tormenta solar que cerrase internet o el ataque hacia las infraestructuras que provocasen la caída de internet. Producirían una desconexión de todos los equipos de la red y que dejasen de actualizar su libro de contabilidad. Pero el software seguiría funcionando en cada ordenador. Aun así Bitcoin sería capaz de sobrevivir, por que es un protocolo software capaz de seguir ejecutándose internamente en cada ordenador y hay nodos en búnkeres conectados a la red capaces de soportar estos desastres. Además, por su propio protocolo Bitcoin es muy viral y en el momento en el que los equipos se volviesen a conectar a la red el libro de contabilidad se volvería a distribuir entre todos los usuarios.

5.5. Irrupción algoritmo sha-256

Es una parte esencial del funcionamiento correcto en la red Bitcoin. Ya hemos explicado que son los hashcodes y como se forman. Con las mejoras de la capacidad de procesamiento, como la computación cuántica, podría ser factible que los ordenadores calcularan y revirtieran estas funciones hash, lo que se traduciría en que todas las direcciones de Bitcoin serían vulnerables al robo. La única solución sería realizar una bifurcación, aprobada por consenso por mas de la mitad de los nodos y cambiar a un sistema de encriptación más sólido y fiable.

5.6. Falta de adopción

Actualmente la red es lo suficientemente famosa y confiable como para dejar de lado este aspecto. Pero podría darse el caso que apareciese otra criptomoneda u otra tecnología que dejase a un lado Bitcoin. Por ejemplo, una moneda más escalable, más efectiva, que consuma menos energía proporcionando la misma seguridad, capaz de realizar más acciones... Aun así, hay que tener mucho cuidado con el resto de criptoactivos. Existen un gran número que son estafas, otro gran número están muy centralizadas y pueden cambiar las reglas en medio del juego para su propio beneficio u otras que comparten características iguales a Bitcoin pero es difícil que alcancen su fama o nivel de confianza.

Capítulo 6

Conclusiones

Frente a los sistemas centralizados que tradicionalmente han servido para guardar información especialmente tras la llegada de internet, la tecnología Blockchain supone un cambio de paradigma que se necesita estudiar en profundidad, porque permite implementar un libro de contabilidad distribuido público. En este trabajo fin de máster, se analiza desde un punto de vista técnico cómo funciona la tecnología, las características principales, que surgió como una forma de eliminar a los intermediarios y que ha abierto una gran diversidad de oportunidades para las empresas. Su reducción de costes y ser un medio de intercambio de información seguro, transparente e inmutable ofrece aplicaciones con un gran potencial, especialmente en las cadenas de suministros.

Se han estudiado los Smart contracts y las ventajas competitivas que ofrecen. Estos contratos al igual que la tecnología están ganando popularidad. Permiten la operación entre iguales y tienen el potencial de mejorar la eficiencia y la transparencia en las negociaciones. En este documento, se argumenta como pueden facilitar la colaboración en distintos sectores industriales y en que situaciones deberían integrarse. Hemos explicado como los Smart contracts ofrecen intercambio de información, trazabilidad y una automatización, que pueden permitir mejoras en colaboraciones de empresas (creando mercados abiertos), certificaciones, reestructuraciones empresariales, etc. Por ejemplo, en el sector sanitario, podrían poner fin a la falsificación de medicamentos gracias a una auditabilidad minuciosa al alcance del paciente. Actualmente, el número de empresas que utilizan esta tecnología es pequeño, pero este número podría crecer si se realizan más estudios e investigaciones sobre la tecnología y explorar las ventajas y e implicaciones. Esto contribuiría a un mayor desarrollo de la tecnología y de las empresas en la era de la industria 4.0.

Por último, no hay que olvidar que la tecnología se encuentra en una fase de exploración y que tiene algunos riesgos. Nosotros hemos expuesto los considerados mas importantes pero pueden existir otros como regulaciones que podrían poner en jaque la tecnología.

Bibliografía

[1] Daniil Frolov. Blockchain and institutional complexity: an extended institutional approach. *Journal of Institutional Economics*, 17(1):21–36, 2021.

[2] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10):71, 2016.

[3] Hossein Kakavand, Nicolette Kost De Sevres, and Bart Chilton. The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. *Available at SSRN 2849251*, 2017.

[4] Luz Parrondo. *Tecnología blockchain, una nueva era para la empresa.* 2018.

[5] Walter Iván Navas Bayona, Halder Yandry Loor Zambrano, and Cristian Ricardo Amen Chinga. La consolidación del blockchain en las empresas como método de pago para sus transacciones. *Revista Investigación y Negocios*, 13(22):135–144, 2020.

[6] Juan Carlos HERNÁNDEZ PEñA. Blockchain y el sector eléctrico. una propuesta de regulación. In *Nuevos retos del Estado garante en el sector energético*, pages 259–283. Marcial Pons, 2020.

[7] Don Tapscott and Alex Tapscott. La revolución blockchain. *Descubre cómo esta nueva tecnología transformará la economía global. ediciones deusco. séptima edición. recuperado en webdelprofesor. ula. ve/economia/oscared/materias/E_E_Mundial/Economia_ Internacional_Krugman_Obstfeld. pdf*, 2017.

[8] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.

[9] Axel Kaiser. *La miseria del intervencionismo.* Aguilar, 2012.

[10] J Frankenfield. Bitcoin. *Investopedia, Feb*, 18, 2021.

[11] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. IEEE, 2017.

[12] Wikipedia. Privacidad — wikipedia, la enciclopedia libre, 2021. [Internet; descargado 16-octubre-2021].

[13] Wikipedia. Criptografía simétrica — wikipedia, la enciclopedia libre, 2021. [Internet; descargado 28-octubre-2021].

[14] Yan Pritzker. *Inventing Bitcoin: The Technology Behind the First Truly Scarce and Decentralized*. Amazon Digital Services LLC-KDP, 2019.

[15] Carlos Zozaya, José Incera, and A Franzoni. Blockchain: Un tutorial.

[16] Wikipedia. Función hash — wikipedia, la enciclopedia libre, 2021. [Internet; descargado 28-octubre-2021].

[17] Carlos Dolader Retamal, Joan Bel Roig, and Jose Luiz Muñoz Tapia. La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía industrial*, 405:33–40, 2017.

[18] Ines Gomez Lasala. Blockchain. la revolucion en la industria. B.S. thesis, Universitat Politècnica de Catalunya, 2018.

[19] Chris Dannen. *Introducing Ethereum and solidity*, volume 318. Springer, 2017.

[20] Xiaomin Bai, Zijing Cheng, Zhangbo Duan, and Kai Hu. Formal modeling and verification of smart contracts. In *Proceedings of the 2018 7th international conference on software and computer applications*, pages 322–326, 2018.

[21] Yining Hu, Madhusanka Liyanage, Ahsan Mansoor, Kanchana Thilakarathna, Guillaume Jourjon, and Aruna Seneviratne. Blockchain-based smart contracts-applications and challenges. *arXiv preprint arXiv:1810.04699*, 2018.

[22] Jun Wang, Peng Wu, Xiangyu Wang, and Wenchi Shou. The outlook of blockchain technology for construction engineering management. *Frontiers of engineering management*, pages 67–75, 2017.

[23] Ferdinando Chiacchio, Diego D'urso, Lucio Compagno, Marcello Chiarenza, and Luca Velardita. Towards a blockchain based traceability process: a case study from

pharma industry. In *IFIP International Conference on Advances in Production Management Systems*, pages 451–457. Springer, 2019.

[24] Rainer Kattel and Ines Mergel. *Estonia's digital transformation: Mission mystique and the hiding hand*. 2019.

[25] Oscar Lage Serrano. Blockchain: Aplicaciones en la industria alimentaria. *Ponencia de la XXXIII Jornada Anual sobre Digitalizacion en el Sector Alimentario*, pages 13–16, 2019.

[26] Joaquín Jiménez-Godoy. Trazabilidad fiable del vino: Blockchain. Master's thesis, 2018.

[27] Mario Villegas Casado. Blockchain y su aplicación a la cadena de suministro. 2019.

[28] Wikipedia. Equilibrio de nash — wikipedia, la enciclopedia libre, 2021. [Internet; descargado 30-octubre-2021].

[29] Javier Pastor. Bitcoin como desastre medioambiental: que sea el mayor despilfarro energético de la historia depende de su futuro. *Xataka*, 2021. https://www.xataka.com/criptomonedas/bitcoin-como-desastre-medioambiental-que-sea-mayor-despilfarro-energetico-historia-depende-su-futuro.

[30] Mario Becedas. Goldman sachs ve en ethereum: un amazon de la información. que superará al bitcoin. *Goldman*, 2021. https://www.eleconomista.es/divisas/noticias/11233173/05/21/Goldman-Sachs-ve-en-Ethereum-un-Amazon-de-la-informacion-que-superara-al-bitcoin.html.

[31] Jonathan Chiu and Thorsten Koeppl. Incentive compatibility on the blockchain. In *Social Design*, pages 323–335. Springer, 2019.

[32] S. Ammous and M.V. Granados. *El patrón Bitcoin: La alternativa descentralizada a los bancos centrales*. Deusto. Deusto, 2018.

Lista de Figuras

Anexos

Anexos A

Un anexo

Gráfico de Gantt

	TIEMPO 12 créditos ECTS (300 horas de trabajo personal del estudiante)														
GRÁFICO DE GANNT	AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE	**TOTAL**	
ACTIVIDADES	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13		
A1- Estudio de las tecnología blockchain y conceptos o tecnologías subyacentes. **A4- Aplicaciones en la industria de la tecnología blockchain.**	10	20	25	30	35	20	10							150	
A2- Estudio del mercado de las criptomonedas **A4- Aplicaciones en la industria de la tecnología blockchain.**						5	24	21	18	15	5			88	
A3- Análisis de la información, conclusiones para la gestión.								7	7	5				19	
A3-Escritura Memoria						4	1	1	2	5	15	15	10	53	
TOTAL	10	20	25	30	35	29	35	29	27	25	20	15		300	310