**Etiquetado de tiempo confiable para Blockchain** https://github.com/gperezalba/TFM

## RESUMEN

En este TFM pretendemos desarrollar nuevas metodologías de desarrollo de la tecnología blockchain usando el tiempo como primitiva fundamental. Se pretende desarrollar una solución de etiquetado de tiempo descentralizado y trazable a referencias internacionales (tiempo UTC), que se ejecute en el procesador de forma confiable y segura. Se estudiará como esto permite desarrollar distintas aproximaciones en las pruebas de trabajo con objeto de mejorar la escalabilidad de la tecnología blockchain y su impacto en aplicaciones futuras.

## Conocimientos recomendados:

programación en c/c++, s.o. Linux.

Equipos:

Pc de proposito general + tarjetas Rasp Berry Pi

INDICE

1. Introducción
   1. Motivación del proyecto

Ganancia de popularidad de las criptomonedas

Los últimos años la popularidad se la lleva blockchain también

Actualmente existen varias limitaciones sin resolver de esta tecnología

Problema de escalabilidad (PoW)

Desperdicio de electricidad(PoW)

No descentralización por las minning pools

Etc

* 1. Objetivos

El problema que se pretende atajar es el de la escalabilidad

Blockchain con PoW es un método para ordenar transacciones con cuyo orden todos estén de acuerdo

No se usa el Timestamp ya que los actores (mineros) no son conocidos (no se puede confiar) y no se tiene la certeza de que usen el tiempo real de su reloj, y además, no se tiene la certeza de que los relojes de los mineros estén bien sincronizados.

Si se pudiera solventar lo anterior se podría hacer uso del Timestamp para un PoW más eficiente

Trustzone+Autenticación/Cifrado junto con software de trazabilidad de tiempo

* 1. Materiales y métodos

Trustzone

Autenticación y cifrado de código

R2CGGTTS

Se necesita dispositivo con ARM…RaspberryPi3

* 1. Organización de la memoria

1. Estado de la técnica
   1. Trazabilidad (código d Pascale de Fraigne)

Señal GPS

Satélites en common view

Trazabilidad a lab(k) o UTC

Fichero CGGTTS

* 1. Revisión de tecnologías blockchain

¿Qué es y cómo funciona blockchain?

Funciones hash, cifrado de clave asimétrica…

Conceptos clave?

¿Qué es minar un bloque?

Algoritmos de consenso (PoW, PoS)

Problemas

Problema escalabilidad cuando PoW por los 10 min no reducibles por incremento forks

Mala descentralización por minning pools

Problemas de PoS (reparto de la riqueza desigual, seguiría estando mal descentralizado porque elegirían los que más token tienen)

Latencia de la red

* 1. Trusted Code

1. Desarrollo de un software de análisis de trazabilidad
   1. Integración “bonita” del código de Pascale
2. Desarrollo de software confiable en Zedboard
   1. Ejemplo de referencia
3. Propuesta blockchain basado en tiempo confiable

PoW: orden de paqs en base al trusted timestamp

Se mencionó que pow era un mecanismo para ordenar txs o bloques

Lo que redacté del nº de forks

El algoritmo dicta que hay que quedarse con la cadena más larga… por tanto sólo se puede decidir en base a la longitud de la cadena. Si se hace uso del timestamp se puede hilar más fino pudiendo reducir tiempo de pow sin que aumenten los forks

PoS: Proof of Traceability (Trabajo future?????????????)

En lugar de que la probabilidad de minar el siguiente bloque dependa de tu riqueza, dependería de lo bien sincronizado con la red que estés.

1. Integración y resultados experimentales
2. Conclusiones
   1. Revisión de objetivos y conclusiones
   2. Valoración personal
   3. Trabajo futuro
3. Bibliografía
4. Apéndices (coste del proyecto, diagrama gant, .…).

## BIBLIO

- Código confiable:

https://software.intel.com/es-es/sgx/details

https://developer.arm.com/technologies/trustzone

https://forums.xilinx.com/t5/Xcell-Daily-Blog-Archived/Secrets-of-the-ARM-TrustZone-in-the-Zynq-All-Programmable-SoC/ba-p/454128

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

- "trusted-timestamp service"

- Trazabilidad de referencias GNSS

- Uso de Trustzone o SGX para el códgo de trazabilidad, etiquetado y/o sincronización (ptp/ntp??)

https://forums.xilinx.com/t5/Xcell-Daily-Blog-Archived/Secrets-of-the-ARM-TrustZone-in-the-Zynq-All-Programmable-SoC/ba-p/454128

https://developer.arm.com/technologies/trustzone

https://software.intel.com/es-es/sgx/details

- Smart contract basado en "trustedtimestmamps software".

# Introducción

## Motivación del Proyecto

En el año 1992, tras una reunión en Sillicon Valley, Timothy C. May publica el manifiesto cripto-anarquista que da origen al movimiento Cyberpunk. Este movimiento social es el origen de una revolución de carácter libertaria cuyo principal objetivo es reducir la intervención del Estado a su mínima expresión. Se consideraba que la protección birndada por el Estado en la relación y acuerdos entre individuos, podía ser brindada de una manera más libertaria y eficiente por la tecnología. Dicho movimiento siembra las premisas de un proyecto que surge años después, el proyecto Bitcoin.

[Manifiesto cripto-anarquista]

El 1 de noviembre de 2008 se publica un artículo/White-paper titulado “Bitcoin: A Peer-to-Peer Electronic Cash System”. El autor (o autores) del artículo/White-paper, que se esconde bajo el alias Satoshi Nakamoto, decide publicarlo en una lista de correo sobre criptografía. Este es uno de los primeros documentos en los que se menciona el término *Blockchain.* Se describe como una tecnología creada con el propósito de llevar a cabo el proyecto de Bitcoin. Blockchain surge de la ingeniosa combinación de distintas técnicas creadas años atrás en el campo de la informática y la criptografía. Apoyándose en los ideales del movimiento Cyberpunk, se describe al Bitcoin como una moneda digital gobernada por unas reglas criptográficas que controlan su gestión y emisión. La tecnología blockchain garantiza el correcto funcionamiento de los aspectos clave de las criptomonedas: la puesta en circulación de la moneda y el mecanismo de gasto que garantiza que una moneda no pueda ser gastada varias veces. Anteriores monedas digitales habían intentado resolver estos dos problemas sin éxito. El proyecto Bitcoin, cuya base tecnológica es blockchain, es la primera criptomoneda capaz de resolverlos de manera totalmente descentralizada.

[Whitepaper bitcoin]

El problema del mecanismo para poner en circulación la moneda digital tiene su origen en el proyecto de Adam Back llamado HashCash. El proyecto tenía como objetivo combatir el correo *spam* haciendo uso de la técnica conocida como prueba de trabajo. La prueba de trabajo consiste en un problema matemático de resolución compleja pero cuya verificación es muy sencilla. El aspecto clave de la prueba de trabajo radica en que la dificultad del problema a resolver se puede ajustar. Es vital para cualquier moneda digital que la emisión de la misma sea predecible y constante en el tiempo. La regulación de la dificultad de la prueba de trabajo es el mecanismo por el cual se consigue ajustar la puesta en circulación. Las redes blockchain que hacen uso de la prueba de trabajo permiten que el usuario que antes resuelva uno de estos problemas cree una determinada cantidad de nuevas monedas. El resto de usuarios de la red procederá a la sencilla verificación de la solución del problema antes de comenzar a buscar la solución a otro de estos problemas.

Para resolver el segundo problema se necesita que los usuarios de la red sean capaces de conocer el último estado consensuado de la blockchain. Gracias a esto, los usuarios de la red serán capaces de determinar sin un usuario de la red es el poseedor de cierta moneda. En otras palabras, los usuarios de la red pueden verificar si un usuario en concreto está realizando un doble gasto de una determinada moneda o no. El trabajo del investigador Nick Szabo sobre la tolerancia a fallos bizantinos se convierte en la pieza clave para que los usuarios de la red lleguen al consenso sobre el último estado global de la blockchain.

[Tema 1 Alberto Toribio Intro a blockchain curso UNIR]

La tecnología blockchain permite a los usuarios de la red tener un registro válido, inalterable y consensuado de todas las transacciones realizadas. Los bloques de la cadena contienen la información relativa a esas transacciones, es por esto que a menudo se denomina a la blockchain como libro contable.

El 3 de enero de 2009 Satoshi Nakamoto crea el primer bloque de la cadena de Bitcoin conocido como bloque génesis. Desde ese momento se han estado creando nuevos bloques de la cadena y nuevos bitcoins ininterrumpidamente. Sin embargo, la popularidad de Bitcoin no ha sido la misma desde entonces. Durante los primeros años sufrió varios altibajos tanto en popularidad como en el precio. No fue hasta finales de 2017 cuando su popularidad y precio comenzaron a incrementarse de manera exponencial. Entre 2009 y 2017 surgen muchas otras criptomonedas y proyectos basados en Bitcoin y blockchain.

El proyecto con mayor repercusión que hizo ver las posibilidades que ofrecía la tecnología blockchain más allá de Bitcoin fue Ethereum. El proyecto Ethereum, bajo el liderazgo de Vitalik Buterin, surge en 2014 con el objetivo de crear una nueva red blockchain. La red Ethereum, además de registrar todas las transacciones de su propia moneda digital (el Ether), registra pequeños programas informáticos llamados Smart Contracts. Los usuarios de la red, además de estar de acuerdo en las transacciones que se realizan en la red, deben estar de acuerdo en los despliegues de los Smart Contracts y de los resultados de la ejecución de los mismos. Con los resultados de la ejecución de los Smart Contracts ocurre exactamente igual que con las transacciones de monedas, si la mayoría de la red está de acuerdo el resultado pasa automáticamente a ser válido.

El nombre de Smart Contract puede llevar a equivocación. Sin embargo, los Smart Contracts no extienden todas las capacidades o características de un contrato convencional. Son programas informáticos que permiten programar una serie de instrucciones máquina propias de su máquina virtual (Ethereum Virtual Machine, EVM) para interaccionar con los datos que residen en memoria. Por lo tanto, la clase de tareas que podrán realizar los Smart Contracts será muy limitada.

Uno de los principales usos de los Smart Contracts es la creación de *tokens*. Un token es una unidad de valor que una organización crea para gobernar su modelo de negocio y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas [william mougayar, the business blockchain]. El Smart Contract asociado a un determinado token será el encargado de programar el registro y la interacción que se tenga con el token en cuestión. En definitiva, se tendría un pequeño libro contable creado sobre un gran libro contable (la blockchain) [tema 1 UNIR].

La *tokenización* de activos abre un gran abanico de posibilidades, siendo su mayor práctica las ICOs (Initial Coin Offering). Permite una nueva forma de financiación a nuevas empresas. Consiste en la preventa de su propia moneda digital o token en representación de los servicios que dicha empresa prestará en el futuro. En el 2017 la financiación obtenida por empresas que han realizado esta oferta inicial de moneda supera los 5000 millones de euros [buscar dato real].

Tras toda esta serie de puntos de inflexión que han marcado el avance de la tecnología blockchain, es necesario citar los principales problemas, aún por resolver, entre los cuales se encuentra la principal motivación de este trabajo.

La raíz de la mayoría de problemas está en la prueba de trabajo. La dificultad de los problemas de la prueba de trabajo se ajusta constantemente para hacer que el tiempo que empleará el poder computacional de todos los usuarios de la red en resolver el problema sea constante. Este tiempo tiene que ser suficiente para que la solución al problema hallada por un usuario sea difundida a la mayoría de usuarios y se adquiera el consenso. Este tiempo dependerá de las características de la red blockchain en cuestión. Cada solución a un problema permite que se añada un nuevo bloque a la cadena que contendrá la información relacionada con las transacciones realizadas. Cada bloque tiene un tamaño máximo que dependerá de cada red blockchain. Se tendrá por tanto un tiempo de creación y un tamaño máximo prefijado. Esto se traduce en una tasa máxima de transacciones por segundo (tx/s) para cada blockchain. Notar que la dificultad de la prueba de trabajo se ajusta en base al poder computacional agregado de todos los usuarios para que el tiempo sea constante. Esto significa que no por añadir más poder computacional a la red se incrementará el número de transacciones por segundo. Si un sistema no aumenta su rendimiento cuando se le añaden más recursos al mismo se dice de este que no es escalable. Es por esto que las redes blockchain basadas en prueba de trabajo son ineficientes por diseño. En base a la definición que se tiene, no se podrá conseguir que sea escalable como tal. Sin embargo, se podrán realizar cambios en el protocolo para hacer que sea lo más eficiente posible. Estos cambios en el protocolo que hagan que se consiga la máxima eficiencia posible están aún por descubrir y diseñar.

La falta de escalabilidad da paso a otro de los principales problemas, el desperdicio de energía eléctrica. La reciente popularidad de las criptomonedas y las redes blockchain ha atraído el interés de muchas personas. Cada vez son más los usuarios que suman su poder computacional a la red con el objetivo de resolver los problemas de la prueba de trabajo. Sin embargo, el protocolo define que el tiempo empleado por el poder computacional agregado de todos los usuarios sea aproximadamente el mismo siempre. En otras palabras, si se aumenta el poder computacional de la red, aumentará también la dificultad de la prueba de trabajo. Este aumento de la dificultad se traducirá en un aumento de la energía eléctrica empleada en resolver la prueba de trabajo. El resultado siempre será la creación de un nuevo bloque de la cadena cada cierto intervalo de tiempo, la consecuencia directa que cuánto más poder computacional tenga la red, más energía eléctrica se empleará en el proceso.

Cuando un usuario encuentra solución a la prueba de trabajo, este obtiene la capacidad de crear cierta cantidad de nuevas monedas que se autoasignará. Esto ha provocado la creación de grupos que aúnan todo su poder computacional en un mismo usuario para así aumentar la posibilidad de encontrar la solución a la prueba de trabajo y por ende de recibir estas nuevas monedas creadas que posteriormente repartirán entre todos. Surge así un nuevo problema que atenta contra la descentralización de la red. En redes como la de Bitcoin, casi la totalidad de los nuevos bloques son incluidos a la cadena por tres de estos grupos. Se podría decir que estos tres grupos gobiernan la blockchain de Bitcoin. A esto se le suma que, si uno de estos grupos adquiere al menos el 51% del poder computacional de la red, este podrá incluir las transacciones que desee a su antojo. Esto se conoce como el ataque del 51%.

La gran cantidad de inconvenientes aún por solventar o mejorar motivan este trabajo. En el siguiente apartado se definirá más concretamente el problema que se pretende atajar en el trabajo y los objetivos del mismo.

## Objetivos

En el apartado ANTERIOR se describen los hitos más relevantes de la historia de las criptomonedas y blockchain. Una vez se conoce el porqué de su reciente popularidad se describen los problemas entre los cuales se encuentra la principal motivación de este trabajo. En este apartado se describirá con mayor detalle el problema que se pretende atajar en este trabajo y los objetivos del mismo.

En base al protocolo actual que se tiene para las redes blockchain basadas en prueba de trabajo, ninguna de estas puede ser un sistema escalable. Si se quiere que una red blockchain basada en prueba de trabajo siga teniendo las características necesarias para sustentar una moneda digital, no se podrá conseguir que el sistema sea escalable como tal. Está diseñado para que sea ineficiente. Sin embargo, es posible hacer cambios en el protocolo para que, dentro de esa ineficiencia, el sistema sea lo más eficiente posible.

¿Por qué está diseñado para ser ineficiente? La prueba de trabajo plantea problemas matemáticos a toda la red de usuarios de manera que el primero en encontrar la solución, la distribuya, sea el creador del siguiente bloque de la cadena y se lleve una recompensa por ello. El problema viene en la distribución de la solución. Se necesita que la mayoría de la red esté de acuerdo con que un usuario en concreto ha sido el primero en encontrar la solución a la prueba de trabajo y todo lo que ello acarrea. El consenso debe llegar antes de que los usuarios de la red comiencen a buscar solución a la nueva prueba de trabajo. Los usuarios forman una red P2P, por lo que la distribución de la solución llevará su tiempo antes de que la mayoría de la red alcance el consenso. Para este tiempo es para el que se ajusta la dificultad de la prueba de trabajo, y no se puede reducir ya que sino la red no alcanzaría el consenso. En la red Bitcoin este tiempo es de aproximadamente 10 minutos. Se suele dar el caso de que, durante este tiempo de difusión de una solución, haya otros usuarios que, sin saber que alguien ya ha encontrado una solución, encuentren otra solución y comiencen a distribuirla desde otro punto de la red. Habrá usuarios de la red que reciban soluciones a la misma prueba de trabajo de distintos usuarios. Sólo una de ellas se puede considerar válida, y los usuarios deben ponerse de acuerdo en cuál de ellas. Cada vez que se encuentra una solución a la prueba de trabajo, a su vez se genera una nueva prueba de trabajo relacionada con esa solución anterior. El protocolo actual dicta que cuando un usuario recibe varias soluciones válidas a una misma prueba de trabajo, este debe elegir una de estas soluciones al azar y comenzar a buscar solución a la nueva prueba de trabajo generada. Cada usuario espera que la mayoría de la red haya elegido la misma solución que él, ya que sino estará buscando solución a una nueva prueba de trabajo distinta a la de la mayoría de la red y por ende inválida. Cuantas más soluciones se encuentren a la misma prueba de trabajo, más difícil resultará alcanzar el consenso. Por lo tanto, la dificultad de la prueba de trabajo se ajustará para que el número de soluciones concurrentes sea el mínimo posible.

A priori se podría pensar que resultaría mucho más eficiente que cada usuario sellara temporalmente su solución. Así cuando otro usuario de la red tenga que elegir entre varias soluciones, podrá hacerlo en base al sello temporal y no por azar. Esto da pie a otro de los puntos clave de las redes blockchain, y es que, al tratarse de redes P2P públicas, ningún usuario debe confiar en ningún otro. Por lo tanto, hay dos aspectos de los que ningún usuario debe fiarse:

1. No se tiene la certeza de que otro usuario selle temporalmente una solución con la hora real de su reloj. Podría hacerlo con una hora previa para sacar ventaja de ello.
2. No se tiene la certeza de que la hora real que marque el reloj de un usuario esté sincronizada con la hora UTC.

El objetivo del presente trabajo consiste en solventar estos dos puntos. De conseguirlo, se podría hacer uso de un sellado temporal distribuido y confiable para las distintas soluciones que se encuentren a la prueba de trabajo. Se considera que esto permitiría a los usuarios de la red encontrar el consenso de manera más eficiente. Así se podría reducir la dificultad de la prueba de trabajo, sin que esto afecte al consenso, lo que supondría una mejora en el número de transacciones por segundo.

## Materiales y métodos

## Organización de la memoria

# Estado de la técnica

## Trazabilidad

## Revisión de tecnologías blockchain

En el apartado de Introducción se ha dado una visión muy general de cómo surgió blockchain y de sus hitos más importantes. La explicación de las redes blockchain ha sido tan simple como ha sido posible para entender la motivación y los objetivos del proyecto. Sin embargo, es necesario conocer con más detalle el funcionamiento y las posibilidades que ofrecen los distintos tipos de redes blockchain para la correcta comprensión del trabajo. Notar que, pese a que la explicación se realizará en base a la blockchain de Bitcoin, la explicación es extensible a la gran mayoría de redes blockchain.

### Criptografía

La criptografía pese a ser prácticamente transparente para el usuario, juega un papel fundamental en la actualidad. Acciones tan cotidianas como enviar un correo electrónico o pagar con tarjeta de crédito funcionan gracias a la criptografía. La criptografía aporta seguridad a estos procedimientos. ¿Por qué se confía en la criptografía? La criptografía se basa en una ciencia exacta, como son las matemáticas, y en algoritmos muy estudiados por la comunidad científica. Varios de estos algoritmos de la criptografía son usados en la tecnología blockchain para aportar seguridad. Son esenciales para su correcto funcionamiento.

#### Funciones hash

La traducción al castellano de blockchain es cadena de bloques. En este apartado se explica la metodología que se sigue para que los bloques de información queden encadenados y cuál es el objetivo de esto.

Una función hash es una función unidireccional. Las funciones unidireccionales se definen como:

La principal característica de estas funciones es que es fácil de calcular, pero calcular es computacionalmente irrealizable. Apoyadas en esta característica, las funciones hash se aplican sobre mensajes M para proporcionar un resumen del mismo denominado m. El resumen m tendrá una longitud fija independiente de la longitud del mensaje M.

Existen numerosas funciones hash. Sin embargo, para que una función hash se considere segura y pueda ser utilizada en criptografía debe cumplir una serie de requisitos:

1. Dependencia de bits: se corresponde con la propiedad de dispersión de las funciones hash. El resumen debe depender de todos los bits del mensaje. Esto significa que, si se cambia un bit del mensaje, cambian de media la mitad de los bits del resumen.
2. Resistencia a la preimagen: dado un resumen m, debe ser computacionalmente difícil obtener M de modo que H(M) = m.
3. Resistencia a la segunda preimagen: dado un mensaje M, debe ser computacionalmente difícil encontrar otro mensaje N cuyos resúmenes coincidan, es decir H(M) = H(N).
4. Resistencia a colisiones: debe ser computacionalmente difícil encontrar una colisión. Una colisión consiste en dos mensajes M y N cuyos resúmenes coincidan.

Recordar diferencia 3 y 4, posible pregunta. Resistencia a colisiones es más débil, ya que en la 4 son 2 mensajes cualesquiera y en la 3 se trata de fijado un mensaje M encontrar otro que colisione.

En definitiva, las funciones hash permiten obtener un identificador único de un mensaje. Identificador a partir del cual no se podrá obtener el mensaje original y que garantiza la integridad del mismo. Este aspecto es lo que hace a las funciones hash indispensables para blockchain.

##### Aplicación de las funciones hash a blockchain

Una cadena de bloques se origina a partir de un primer bloque, el bloque génesis. Se pretende que todos los bloques que se vayan añadiendo a la cadena estén enlazados de alguna manera inequívoca con todos los bloques previos hasta llegar al génesis. Esto se consigue con las funciones hash siguiendo la siguiente metodología desde el bloque génesis:

1. Haciendo uso de una función hash, se obtiene el resumen o hash del bloque génesis. El hash será un código de longitud fija que identifica inequívocamente al bloque génesis.
2. Para crear el siguiente bloque de la cadena, se incluye en este un campo que contendrá el hash del bloque anterior.
3. Una vez finalizada la creación del nuevo bloque, se le calcula el hash al nuevo bloque y se vuelve al paso 2.

Con este procedimiento se consigue que el hash de un bloque N de la cadena identifique inequívocamente a toda la cadena de bloques desde el bloque génesis hasta el bloque N. Se garantiza que toda la cadena de bloques permanece íntegra y que si alguno de los bloques sufre algún cambio se alterarán los hashes de todos los bloques posteriores.

#### Criptografía de clave asimétrica

En 1976 Diffie y Hellman proponen un nuevo método para la distribución de claves. El propósito de este método era permitir a dos extremos de una comunicación establecer una clave simétrica sin que estos hayan tenido un contacto previo o usen un canal seguro. Esta propuesta daba solución al intercambio de claves simétricas, pero no permitía el cifrado. Sin embargo, este método dio origen un año después al primer algoritmo de cifrado de clave asimétrica. En 1977 nace el algoritmo RSA de la mano de Rivest, Shamir y Adleman. Este es uno de los algoritmos más utilizados incluso a día de hoy. RSA permite no sólo el cifrado sino también la firma digital.

La principal innovación que introduce este tipo de criptografía es el uso de un par de claves. Se tendrá una clave pública y una clave privada. Como su propio nombre indica, la clave pública será conocida por todos, en cambio la clave privada sólo la debe conocer su propietario. De esta manera deja de ser necesario el intercambio de una clave simétrica a través de un canal seguro.

La criptografía asimétrica se apoya en tres tipos de problemas matemáticos:

1. Problema de la factorización de enteros
2. Logaritmo discreto
3. Curvas elípticas

Al igual que ocurría con las funciones hash, las funciones matemáticas escogidas para estos problemas tienen como principal característica el fácil cálculo en un sentido, pero muy difícil computacionalmente en el sentido inverso. De nuevo se trata de funciones unidireccionales.

El cifrado de un mensaje mediante criptografía de clave simétrica sigue el siguiente esquema:

1. El emisor obtiene la clave pública del destinatario por cualquier canal (puede ser inseguro).
2. El emisor cifra el mensaje con la clave pública del destinatario.
3. El emisor envía el mensaje cifrado a través de cualquier canal ya que solamente el poseedor de la clave privada asociada a la clave pública con la que se cifró el mensaje podrá descifrarlo. En este caso el destinatario.
4. El destinatario recibe el mensaje cifrado y haciendo uso de su clave privada obtiene el mensaje en texto plano.

Este esquema explica un simple intercambio de un mensaje cifrado. Sin embargo, la criptografía de clave asimétrica abre un abanico de posibilidades a protocolos más complicados que ofrezcan distintas cosas. Un claro ejemplo es la firma digital. La tecnología blockchain también hace uso de este tipo de cifrado.

Los principales aportes que hacen al cifrado asimétrico tan interesante para blockchain son:

1. No repudio. Si un usuario firma un mensaje con su clave privada, no podrá negar haberlo hecho.
2. Identificación. Ambos extremos de una comunicación quedan identificados.

Se podría incluir aquí la firma digital

##### Aplicación de la criptografía a Blockchain

Este apartado describe el uso que la tecnología blockchain hace de la criptografía de clave asimétrica. Una red blockchain es una red P2P, por lo tanto, ninguno de los usuarios es a priori conocido o fiable. Dentro de esta red la identidad de los usuarios es pseudoanónima. No se conoce la identidad real de los usuarios, pero tampoco es necesario. Solamente es necesario un identificador único que los identifique dentro de la red. Cada usuario tiene un par de claves asimétricas (pública y privada). Este identificador único se corresponde con la clave pública del usuario (existe un proceso que transforma la clave pública en una dirección, pero no es relevante).

La mejor forma de observar el uso que se hace de este par de claves es describir los pasos que se siguen para realizar una transacción en la blockchain de Bitcoin.

1. El receptor envía su clave pública al emisor de la transacción.
2. El emisor incluye en el campo destinatario de la transacción la clave pública del destinatario.
3. La transacción, entre otros datos, incluye la cantidad de bitcoins a transferir.
4. El emisor cifra la transacción con su clave privada. En este paso el emisor está demostrando que posee una cierta cantidad de bitcoins y acepta que ahora pasan a ser propiedad del destinatario.
5. La transacción se transmitirá a todos los usuarios de la red que la validarán e incluirán en la blockchain.

El paso 4 resulta crucial ya que de él se obtiene la identificación y el no repudio de la transacción. Resulta evidente que la criptografía de clave asimétrica es idónea y totalmente necesaria para el correcto funcionamiento de cualquier red blockchain.

### Teoría de juegos

La teoría de juegos es una rama de las matemáticas aplicada que analiza la toma de decisiones en situaciones en las que la decisión no sólo se basa en el punto de vista de un jugador, sino teniendo en cuenta las decisiones tomadas por el resto de jugadores. Se entiende por juego una situación en la que un jugador podrá obtener recompensas o perjuicios según la decisión que hayan tomado él mismo y el resto de jugadores.

El concepto relacionado con la teoría de juegos más importante para blockchain es el equilibrio de Nash. Este concepto, creado por John Nash, afirma que, si todos los jugadores siguen una estrategia óptima, ningún jugador saldrá beneficiado si cambia individualmente su estrategia. El equilibrio de Nash está directamente relacionado con la expresión “Si la mayoría de los usuarios de la red actúa correctamente la blockchain funcionará correctamente”. Ciertos usuarios de la red podrían intentar hacer trampa incluyendo bloques a la cadena sin resolver la prueba de trabajo, incluir transacciones inválidas, etc. Sin embargo, blockchain está diseñada para que se mantenga el equilibrio de Nash. Si se incluye un bloque válido encima de uno inválido, este pasa automáticamente a ser inválido también. Por lo tanto, la estrategia que les interesa a los usuarios es actuar de manera correcta y elegir la situación más estable. Se mantendrá el equilibrio de Nash mientras la mayoría de los usuarios actúen de manera honesta. Si usuarios con más de la mitad del poder computacional de la red deciden actuar de manera deshonesta, el equilibrio de Nash pasará a localizarse del lado de los usuarios deshonestos y la blockchain pasará a estar corrompida.

### Aspectos clave del protocolo blockchain

#### Concepto de minado

Hasta este apartado se había descrito la red blockchain como una red P2P formada por usuarios. Se utiliza el termino usuario por simplicidad. En este apartado se explica en qué consiste la minería de bloques en blockchain y quienes son los que la realizan.

En realidad, la red blockchain la componen una serie de nodos denominados mineros. En cambio, los usuarios simplemente son los encargados de enviar sus propias transacciones a la red cuando lo deseen. La tarea de los mineros consiste en minar bloques que contengan transacciones con el objetivo de obtener una recompensa. Minar un bloque es como se denomina al acto de resolver la prueba de trabajo descrita de manera simplificada en el APARTADO XXXXXXXXXXXXXxxX.

##### Prueba de trabajo

En el apartado XXXXXXXXxx se describe la prueba de trabajo como un problema de solución muy compleja, pero de verificación muy sencilla. Existen multitud de problemas matemáticos que se podrían utilizar para la prueba de trabajo de blockchain. El problema elegido para blockchain es el cálculo de un resumen hash con una característica determinada. El hash que sirva de solución a la prueba de trabajo de un bloque debe tener una determinada cantidad de ceros (‘000…’) al principio. La cantidad de ceros estará determinada por la dificultad, que a su vez está marcada por la cantidad de poder computacional total de la red. El resumen hash se calcula al bloque que se pretende incluir en cadena de bloques.

Por lo tanto, los pasos que deberá seguir un minero que pretende resolver la prueba de trabajo y minar un nuevo bloque son los siguientes:

1. Calcular la dificultad del siguiente bloque de la cadena. Esta dificultad se calcula en base a una expresión que depende del tiempo que se ha tardado en resolver los últimos bloques de la cadena. La dificultad determina el número de ceros que debe tener el hash del siguiente bloque a incluir en la cadena.
2. Construir un bloque válido que pretenda incluir en la cadena.
3. Dentro del bloque existe un campo denominado *nonce* que será variable y que no aporta ninguna información. El minero deberá ir cambiando el campo *nonce* hasta que obtenga un hash del bloque que tenga el número de ceros que satisfaga la prueba de trabajo.
4. Dar un valor al campo *nonce*.
5. Calcular el hash del bloque con el *nonce* incluido en el punto 4.
6. Si el hash obtenido no satisface la prueba de trabajo, volver al punto 4. En caso de que el hash satisfaga la prueba de trabajo, se dice que se ha minado el bloque. El minero puede proceder a difundir este bloque minado para que los demás lo validen e incluyan a la cadena de bloques.

Este es el algoritmo que deberá seguir todo minero para minar un nuevo bloque. Notar que es en los puntos 4, 5 y 6 donde se emplea la gran parte del poder de cómputo para el minado.

##### Creación de un bloque válido

En el algoritmo que debe seguir un minero para minar un nuevo bloque se observa que el segundo paso es crear un nuevo bloque válido a incluir en la cadena. Para entender en qué consiste este paso en detalle es necesario saber de qué está compuesto un bloque.

Un bloque está compuesto por un campo que contiene las últimas transacciones realizadas, otro campo que contendrá el hash del bloque anterior y el campo nonce descrito en el apartado anteriorXXXXXXXXXXXXXXXXXXXX. Para que un bloque sea válido, todos los datos que este contenga deben ser válidos. En especial es necesario validar las transacciones que se incluyan, ya que si nuestro bloque es inválido el resto de la cadena lo rechazará para mantener el equilibrio de Nash.

La validación de las transacciones consiste básicamente en dos pasos:

1. Validar la clave con la que se ha cifrado la transacción.
2. Comprobar que esa clave privada realmente posee la cantidad de moneda digital que pretende transferir.

#### Validez de la cadena de bloques

En ninguno de los procesos seguidos en las redes blockchain se puede olvidar que se trata de una red descentralizada P2P compuesta por nodos desconocidos. No se tiene la certeza de que los nodos con los que se interactúe estén actuando de manera honesta. Se puede dar el caso de que un nuevo nodo quiera entrar a formar parte de la red blockchain. Este nuevo nodo desconoce totalmente lo sucedido en la cadena de bloques anteriormente así que debe pedirla a varios de los nodos que ya forman parte de la red. Si cada uno de los usuarios a los que solicita la cadena de bloques le proporciona una cadena de bloques distinta, este nuevo nodo deberá saber cuál elegir por sí mismo.

De entre todas las posibles cadenas, la cadena válida (y en la que se encuentra el equilibrio de Nash) se determinará llevando a cabo el siguiente procedimiento:

1. De entre todas las cadenas de bloques, se debe quedar sólo con las cadenas bien formadas. Una cadena está bien formada si todos los bloques que esta contiene son válidos (incluyendo sus transacciones) y todos los bloques están enlazados correctamente mediante hashes.
2. De entre todas las cadenas bien formadas, la cadena válida será la que más carga computacional contenga. Cada bloque añade carga computacional a una cadena de bloques, por lo tanto, la cadena válida será la más larga (en número de bloques).
3. Se puede dar el caso de que el paso 2 nos de como resultado varias cadenas posibles. En este caso el nuevo nodo deberá elegir al azar entre todas las posibilidades y esperar a que en el futuro se llegue al consenso con los dos primeros pasos del procedimiento.

La situación planteada no solamente se puede dar cuando un nuevo nodo quiere entrar a formar parte de la red. Otro caso en el que se puede dar es cuando varios mineros minan un bloque en un tiempo similar y cada uno transmite su bloque minado desde un punto de la red. Un nodo intermedio puede recibir varias cadenas de bloques distintas y deberá elegir la cadena válida en base el procedimiento planteado. Cuando se mina un bloque simultáneamente en dos puntos de la red y ambas cadenas llegan a un nodo intermedio se dice que se ha producido un *fork.* Un *fork* no es más que una cadena de bloques cuyo bloque sucesor pueden ser varios bloques durante un pequeño espacio de tiempo hasta que se consigue el consenso.