Trazabilidad de tiempo UTC y Time Stamp en Blockchain

Guillermo Pérez Alba

ETSIIT - Universidad de Granada

Estudio previo al comienzo de Trabajo final de Máster

1 de julio de 2018

1. Introducción

1.1. El Trilema

En el entorno Blockchain es muy habitual escuchar hablar de "El Trilema". Se trata de 3 aspectos clave en toda Blockchain: seguridad, descentralización y escalabilidad. Se denomina Trilema por el hecho de que los protocolos actuales de Blockchain ofrecen 2 de estos 3 aspectos clave, poniendo en compromiso el restante.
Blockchains públicas como la de Bitcoin o Ethereum ofrecen seguridad y descentralización (aunque la descentralización empieza a ser un problema que se trata más adelante) a costa de no ser sistemas escalables.
Blockchains permisionadas como las de Alastria o IBM ofrecen seguridad y escalabilidad a costa de perder un gran porcentaje de descentralización.
Actualmente no existe protocolo Blockchain alguno que no comprometa alguno de estos 3 aspectos clave. Conseguir solucionar el problema de la escalabilidad en las blockchains públicas es lo deseado, ya que la descentralización en una blockchain permisionada es imposible.

1.2. De la descentralización a la centralización

Pese a presumir de ser descentralizadas, otro de los problemas que comienza a ser preocupante es el de la descentralización en blockchain públicas. Los algoritmos más usados (Proof of Work (PoW) y Proof of Stake (PoS)), están provocando que se pierda la descentralización al depender la capacidad de minado del poder computacional o del stake que cada nodo posea.

1.3. Proof of Work

Se denomina PoW a la resolución, por parte de todos los nodos (mineros) de la red, de un reto o problema matemático. El primer minero que resuelve el reto es el creador del siguiente bloque de la cadena (habrá minado el siguiente bloque) y se llevará la recompensa asociada al minado. El reto consiste en conseguir un Hash (para el bloque que se quiere minar) con un número de ceros al principio. El número de ceros se ajusta en base al poder computacional de la red en cada momento. Se consigue así adaptar la complejidad del reto al poder computacional de la red para que toda la red tarde un cierto periodo de tiempo en resolver el reto y que la cadena no crezca de manera descontrolada. El poder computacional de cada minero va a marcar la probabilidad que este tiene de minar un bloque y llevarse la recompensa. Se crean por tanto las denominadas Mining Pools con el objetivo de sumar mucho poder computacional y aumentar la probabilidad de minar bloques. Lejos de parecer un sistema descentralizado la mayoría del poder computacional se centra en tres de ellas. En ambos casos, más del 51 % del Hashrate se concentra en 3 de estas mining pools.

1.4. Proof of Stake

El algoritmo PoS se crea como alternativa al PoW ya que es un algoritmo que no requiere un costoso hardware específico ni desperdicia energía eléctrica como PoW. La idea básica que sustenta PoS consiste en que cada nodo validador demuestre que tiene cierta cantidad de stake que se arriesga a perder en caso de no validar correctamente el siguiente bloque. En lugar de competir todos los nodos de la red por minar el siguiente bloque, este algoritmo asigna de manera aleatoria qué nodo será el encargado de validar el siguiente bloque. Sin embargo, no lo asigna de manera completamente aleatoria, ya que la probabilidad de que un nodo sea elegido como el siguiente validador está ligada al stake que este tiene. Al no existir "competición" cualquier hardware (no tan costoso) permitiría validar un bloque además de que no se desperdicia energía eléctrica en absoluto haciendo que descienda el coste (fee) asociado a cada transacción.
Pese a mejorar en cierto grado la descentralización con respecto a PoW, no deja de ser un algoritmo que da más a quien más tiene. Se trata de crear un sistema duradero y estable en el tiempo y PoS no asegura que esas diferencias no puedan acentuarse en el futuro.

1.5. El papel del TimeStamp en Blockchain

Una situación que a menudo confunde de blockchain es la puntual falta de orden del Time Stamp de los bloques. En repetidas ocasiones un bloque posee un timestamp menor al timestamp de un bloque previo. En base a la mayoría de los protocolos blockchain actuales, esta situación es totalmente válida.
Blockchain no posee una autoridad central que informe del tiempo UTC. Por lo tanto, asumir que el tiempo UTC de cada nodo es preciso o está sincronizado al resto es un error.
Cada nodo está conectado a la red a través de una serie de peers. Cada nodo posee un tiempo UTC local con un offset marcado por la media del tiempo UTC local de cada peer a los que está conectado. El tiempo global de la red está marcada por la media de los timestamps emitidos por todos los nodos de la red. Esto provoca que la sincronización en estas redes no sea óptima, provocando situaciones en las que el orden de timestamps no sea correcto.
El protocolo de Bitcoin únicamente rechaza un timestamp si es menor a la media de los timestamps de los 11 bloques anteriores o 2 horas superior al tiempo global de la red. De manera parecida se realiza en Ethereum, provocando que un nodo pueda falsear su timestamp en unos 900 segundos sin repercusión alguna.

2. Objetivo

2.1. Introducción

El trabajo consta de una primera parte en la que se desarrollará un sistema de registro confiable de trazabilidad de tiempo. Una vez conseguido, se proponen diferentes líneas de trabajo a seguir haciendo uso de este primer sistema desarrollado.

2.2. Registro confiable de la trazabilidad del tiempo

El método seguido para realizar la trazabilidad del tiempo consiste en obtener la diferencia de tiempo UTC local de un reloj con el tiempo UTC de un laboratorio encargado tal fin. Esta diferencia será almacenada en un registro seguro, distribuido e inalterable como es la Blockchain. Este sistema permitirá que en caso de ser necesario se pueda disponer de trazabilidad del tiempo.

2.3. Software R2CGGTTS

Se hace uso del software desarrollado por Pascale Defraigne (GNSS-Royal Observatory of Belgium) para calcular estas diferencias de tiempo UTC. El software hace uso de los datos proporcionados por los satélites GPS en common-view. Proporcionando como entrada los ficheros RINEX, el software da como salida el fichero CGGTTS (Common GPS Glonass Time Transfer Standard). El fichero CGGTTS contiene una columna que informa de la diferencia de tiempo UTC deseada.

2.4. API a Blockchain

El resultado final de esta primera parte del trabajo consistirá en una API que permita obtener los datos deseados del fichero CGGTTS y almacenarlos en Blockchain.

3. Propuestas de aplicación

3.1. Time Stamp como mecanismo de decisión para mejorar la escalabilidad

El consenso en Blockchain se consigue haciendo que todos los nodos elijan como válida la cadena más larga de entre todas las que reciba. El mecanismo de decisión usado es el número de bloques de la cadena, de manera que al recibir dos cadenas se toma como válida la que más bloques tenga. Cada bloque tiene un tiempo asociado, el tiempo que ha tardado en minarse debido al PoW, unos 10 minutos en Bitcoin, por ejemplo. Se establece este tiempo ya que, si se decide disminuir el tiempo de PoW, varias cadenas de la misma longitud se crearían en distintos puntos de la red. Sería costoso que alguna de ellas adelante a las demás y se establezca como la cadena válida, esto además provocaría que se tengan que revertir cadenas muy largas (cadenas muy largas dejarían de ser válidas cuando alguna las adelante).
La explicación de que sea costoso que alguna cadena adelante a las demás en el caso de que se disminuya el tiempo de PoW es que se minaría el siguiente bloque en varios puntos de la red en un tiempo "similar". Al transmitirse dichas cadenas por la red, se daría el caso en el que a un nodo le lleguen varias cadenas de la misma longitud a la vez teniendo que elegir una de ellas al azar para seguir minado sobre ella. El número de cadenas de igual longitud que le llegarían a este nodo crecería a medida que desciende el tiempo de PoW.
La propuesta consiste en un segundo método de decisión basado en el Time Stamp. En el punto "El papel del Time Stamp en la Blockchain" se mencionan todas las limitaciones por las que no se tiene un timestamp preciso. Sin embargo, haciendo uso del sistema que se desarrollará en el presente trabajo se dispondría de un timestamp más preciso y trazable. El método de decisión propuesto hace uso de este timestamp como segunda variable a tener en cuenta para un nodo.
Si de nuevo se disminuye el tiempo de PoW, se vuelve al caso en el que a un nodo le llegan varias cadenas de la misma longitud. Sin embargo, en este caso el nodo no tiene que elegir al azar con qué cadena quedarse ya que dispone de un segundo método de decisión basado en el time stamp respaldado por el sistema de trazabilidad de tiempo. Elige por tanto la cadena con el timestamp menor, al igual que harán el resto de los nodos de la red llegando al consenso deseado. Cuanto más preciso sea el timestamp, más se podrá reducir el tiempo de PoW resultando en una mejora considerable de la escalabilidad.

3.2. Proof of Traceability

El registro de trazabilidad de tiempo informaría del nivel de sincronización de cada nodo. Lo idóneo para blockchain sería disponer de una sincronización entre nodos óptima que favorezca la comunicación de la red. Una manera de incentivar esa sincronización de los nodos sería el algoritmo propuesto, Proof of Traceability (PoT). PoT funciona de manera similar al algoritmo PoS, con la diferencia de que la probabilidad de que un nodo sea el siguiente nodo validador es mayor cuanto mejor sincronizado está en base a su trazabilidad del tiempo. De esta forma se premiaría a los nodos mejor sincronizados. Debe existir un requisito de stake al igual que en PoS para poder penalizar al nodo en caso de mal comportamiento, con la diferencia de que ahora este stake no está relacionado con la probabilidad de ser el siguiente nodo validador.

4. Otros proyectos relacionados

4.1. Chronologic

El Proyecto Chronologic ofrece un sistema que permite facilitar los préstamos entre pares de manera descentralizada de manera que no es necesaria la confianza entre pares. El prestatario publica un Smart Contract en el que solicita una cantidad de token A. Para ello debe poseer una cantidad de token B (del que no está interesado en desprenderse y por eso solicita el préstamo) cuyo valor debe ser el doble del valor de la cantidad de token A que solicita.
En el momento en que un prestador accede al préstamo, la cantidad de token A solicitada llega al prestatario a través del Smart Contract. El prestador recibe en ese momento una cantidad de token DAY (propio del proyecto Chronologic) que se irá autominando en la cuenta del prestador a modo de interés. Cuanto más tarde el prestatario en devolver el préstamo, más interés se habrá acumulado en la cuenta del prestador.
En caso de que el prestatario no devuelva la cantidad de token A solicitada en el préstamo, el prestatario recibirá la cantidad de token B que se habían depositado en el Smart Contract a modo de fianza.

4.2. Ethereum Alarm Clock

El propósito de este proyecto es proporcionar un sistema para programar la ejecución de una determinada transacción en un determinado tiempo o nº de bloque futuro.
Un Smart Contract no puede ejecutar una transacción ya que no posee clave privada, por lo tanto, se necesita que la transacción la ejecute un usuario.
En resumen, todas las transacciones que se programan para el futuro se almacenan en un Smart Contract propio del proyecto para que un conjunto de nodos que trabajan para el proyecto ejecuten esa transacción en el tiempo o nº de bloque deseado a cambio de una recompensa.

4.3. OpenTimeStamp y OriginStamp

El objetivo de este proyecto es realizar un Time Stamp de un determinado fichero o información de manera que se posea una prueba de que existía en un determinado momento. Básicamente ambos proyectos incluyen el hash de la información que se quiera sellar en una de las transacciones de blockchain. Se necesita para ello realizar una transacción en blockchain con su coste asociado y esperar los tiempos de inclusión de una transacción en la cadena, por lo tanto no dota al timestamp de precisión.