Qué es blockchain, el ecosistema bitcoin basado en APIs

martes, 30 de noviembre de 1999

Blockchain es la tecnología en la que se basa el proceso de minado y cotización de los bitcoins, un procedimiento por el cual los usuarios de esta criptomoneda realizan pagos y transacciones de forma encriptada y autenticada en una base de datos distribuida.

Cualquier cuestión relacionada con los bitcoins va invariablemente unida a blockchain, la tecnología en la que se basa la criptomoneda. Al final es una gran base de datos distribuida en numerosos servidores por todo el mundo que acumula todas las transacciones que se producen en bitcoins. Cada una de esas operaciones, encriptada y autenticada, se suma a la cadena de bloques que es blockchain y en la que se basan los bitcoins. Ese proceso sería imposible sin APIs.

Lo cierto es que a día de hoy, la tecnología bitcoin ofrece muchas más posibilidades y despierta más interés en los desarrolladores, en comparación por ejemplo con otros sistemas de pago online como PayPal. En estos momentos existen dentro de la plataforma de desarrollo colaborativo GitHub casi 3.200 repositorios relacionados con PayPal, mientras que vinculados a bitcoin existen más de 8.000 repositorios. En este gráfico de fiebre elaborado por CoinDesk se puede observar el crecimiento anual de uno y otro sistema desde el año 2009.

La consultora Deloitte realizó recientemente una encuesta dentro de la comunidad de bitcoiners para establecer algunas perspectivas de futuro dentro del sector. Entre las preguntas más interesantes de la misma encontramos: ¿Qué campos relacionados con blockchain encontraban mayores perspectivas de penetración este 2016? El 37% respondió en el lanzamiento de nuevos productos, seguido por nuevos casos de uso. Es evidente que 2016 puede ser el año del desembarco real de blockchain en nuestras vidas.

¿Cómo funciona blockchain?

Cualquier usuario puede usar bitcoins, lo único que es necesario es la instalación de un monedero virtual en un dispositivo. No es necesario tener excesivos conocimiento técnicos para operar con esta criptomoneda, ya que funciona de forma parecida a cualquier proceso de pago online. Lo que hay que tener en cuenta es que cada transacción que un usuario haga con bitcoins, una vez que ha sido verificada, se añade a la cadena de bloques o blockchain y en ese mismo instante comienza a formar parte de una contabilidad compartida por los usuarios.

Esa cadena de bloques o contabilidad compartida es el resultado de todas la operaciones realizadas con los monederos de bitcoins de todos los usuarios de la red. Cada transacción necesita, obligatoriamente, una clave y una firma que identifica a cada usuario y encripta y verifica cada una de esas operaciones. La introducción de cada transacción dentro de la cadena de bloques se produce mediante un proceso llamado minería de bitcoins, basada en un procedimiento conocido como prueba de trabajo (sistema POW, en inglés proof of work).

Cada transacción, que siempre es pública, debe ser verificada para evitar problemas dentro de la cadena de bloques: los bitcoins tienen que ser auténticos y no estar duplicados. Si no es así, alguien pierde dinero. La idea es que un conjunto de nodos se encargue de verificar la autenticidad de cada operación, un protocolo que tarda habitualmente 10 minutos. Cada 2016 bloques se reevalúa para que el proceso siempre ronde ese tiempo de comprobación. La idea es que cada transacción se verifique por consenso y ese proceso de autenticación de las operaciones reciba una comisión por la prueba de trabajo. Es un sistema que evita vulneraciones sin depender de un árbitro de confianza (por ejemplo, un banco).

Algunas de las características fundamentales de blockchain son:

Ï Encriptado por el lado del cliente: todos los monederos virtuales usados por los bitcoiners utilizan JavaScript para su encriptado, lo que facilita una protección contra posibles vulneraciones desde el lado del servidor.

Ï Código abierto: todo el código relacionado con los monederos es de código abierto, eso facilita el trabajo conjunto de las comunidades de desarrolladores.

Ï Operaciones offline: los monederos pueden operar offline con HTML5.

Ï Conversión de bitcoins en 22 monedas internacionales.

Ï Tipos de transacciones: incluyen procesos por email, SMS y Facebook.

Ï Notificaciones de pagos: email, SMS, Skype o llamadas HTTP POST.

Ï Posibilidad de hacer backups automáticas del monedero virtual.

La importancia de las APIs de blockchain
Todo el proceso de transacciones, recepción y emisión de pagos, las operaciones con monederos virtuales o la gestión de los datos no sería posible sin la existencia de una interfaz de desarrollo de aplicaciones por cada una de estas funciones. Hoy día blockchain dispone de varias APIs para diferentes funcionalidades. Sin algunas de ellas nadie podría hacer operaciones con bitcoins en el mundo:

Receive Payments API: la versión 2 de esta interfaz está disponible desde el pasado 1 de enero de 2016. Es la forma más sencilla para que una empresa o un negocio puede empezar a aceptar pagos automatizados en bitcoins. La API se basa en peticiones HTTP GET y se encarga de la creación de una dirección única por cada uno de los usuarios y por cada emisión de factura en cada operación con bitcoins. Condición imprescindible de buena praxis.

Blockchain Wallet API: para el uso de esta API desde el pasado1 de enero es necesario la instalación de un servidor local para la gestión del monedero virtual. El método de comunicación utilizado se basa en llamadas HTTP POST o GET. El proceso por el que se crea un monedero virtual recibe el nombre de create_wallet a partir de esta url: http://localhost:3000/api/v2/create. Cada monedero va asociado a una contraseña con una longitud mínima de al menos 10 caracteres, un código de autenticación de la API, una clave privada por usuario, la carpeta donde se creó el monedero y un email.

JSON RPC API: desde marzo de 2016, la recomendación universal para los usuarios de bitcoins es utilizar la nueva Blockchain Wallet API, aunque la intefaz basada en llamadas RPC sigue siendo compatible con el antiguo protocolo Bitcoind RPpara interactuar con los monederos virtuales. Se puede instalar y utilizar a partir de librerías en numerosos lenguajes de programación: sintaxis como Python, Ruby, PHP, Node.js y .NET.

Blockchain Data API: con ella se pueden consultar los datos en formato JSON de las transacciones y operaciones dentro de la cadena de bloques.

Query API: API de texto plano para consultar datos de blockchain.

WebSocket API: esta interfaz de desarrollo de aplicaciones facilita a los programadores notificaciones en tiempo real sobre transacciones y bloques.

Exchange Rates API: gestiona la información de precios de cambio de los bitcoins y las distintas monedas internacionales en tiempo real y en JSON.