ethereum

Fundamentos de Redes

Memoria de la exposición

Pedro Bonilla Nadal
Ana Peña Arnedo

16 de noviembre de 2017

1. Introducción

Hoy en día, la información es todo. Las grandes compañias de internet han alcanzado un modelo de negocio en el cual no tienen que exigirte dinero para conseguir beneficios. Estos te cobran por una aceptación de ceder tu información para traficar con ella.

En la actualidad, con el objetivo de mantener un sistema de comercio que no tenga que ser mantenido por un organismo que, por lo tanto mantenga poder sobre sus usuarios. Este tipo de comercio 'tradicional' incluye organizaciones como, por ejemplo, amazon, que facilita la compra-venta respaldada por una compañía, o los bancos centrales, los cuales mantienen las divisas y son los responsables del cuidado y mantención de la divisa. Como sabemos que una compañia esté al cargo del cuidado del sistema, (es decir, que tenga un sistema centralizado) tiene una serie de beneficios e inconvenientes.

Por un lado el sistema centralizado con control por una compañía, como la contratación de especialistas para almacenar y proteger la seguridad, y reduce los tiempos de almacenamiento y actualización del sistema.

Por otro lado, donde hay una ventaja, hay un inconveniente. Como se ha podido ver en alguna ocasion[1]esta organización habilita a grandes compañías y estados a filtrar, robar o modificar a información sensible de los usuarios. Esta vulnerabilidad ha llegado a ser calificada como el 'pecado original' de internet, pues este siempre intento ser una plataforma de caracter descentralizado.

Satoshi Nakamoto inció en 2008 el desarrollo de bitcoin. Este hecho desencadenaria un desarrollo increible en el area de las divisas con centralizadas, es decir un sistema monetario que no necesitase de un sistema bancario o de un valor predeterminado. También sorprendió mucho a la comunidad la aplicación de la tecnología de la cadena de bloques, como una herramienta basada en la distribución del conseno. A raiz de estas surgieron otras teconologías basadas en la cadena de bloques, como namecoin, añadiendo. Lo que ethereum pretende es proveer una cadena de bloques con un leguanje turing completo integrado que pueda ser usado para el desarrollo de contratos inteligentes, permitiendo a los usarios la ceanción de proyectos solo escribiendo la logica de estos en unas pocas lineas de código. Algunos de estos poryectos, sacados del la propia web `ethereum.org` serían la creación de un crowdfounding que no sea basado en la confianza si no en un contrato que almacenará el dinero de los contribuyentes, una organización autónoma democrática.

En resumen, nuestra moneda lo que intenta es crear un 'ordenador global' que descentralice el actual cliente-servidor. Con Ethereum en lugar de tener un servidor tendríamos un conjunto de nodos, almacenados por voluntarios alrededor del mundo . Sobre este sistema, la comunidad podrá competir por ofrecer servicios, además de consumirlos.

[1] `https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order`

Ejemplifiquemos la diferencia: navegar por una app-store cualquiera nos ofrecerá una serie de aplicaciones en las cuales contactaremos con un servidor que nos proverá del servicio, generalmente gestionado por un tercero no relacionado (de manera directa) con la transacción.

Ethereum, si todo funciona, devolvería la propiedad de la información a su dueño, de modo que solo el usuario puede modificar la información, y no ninguna entidad externa.

2. Ethereum

2.1. Historia.

En 2012, un joven de 19 años propuso una nueva plataforma, con el objetivo de trasnfomar por entero internet. Vitalik Buterin, un programador de Toronto empezó su investigación en la cadena de bloques en 2011. Co-fundó el portal web Bitcoin Magazine y trabajó para compañías de la materia. En el camino pensó en una plataforma que fuera más allá de las posibilidades del bitcoin.

Con esta idea nació ethereum, una plataforma para la creación de contratos inteligentes (smart contract). Después de publicar en 2014 el white paper, otros desarrolladores se unieron al proyecto.

Para lanzar el poryecto se inició un crowdfounding en julio de 2014, donde los participantes compraban ether vinculo . Después de reunir más de 18 millones de dolares, se inició y en 2015 se lanzó una plataforma, no demasiado user-friendly, pero con comandos el linea que permitía la creación de aplicaciones descentralizadas.

Este nuevo tipo de contratos caló entre el público llamando la atención de gigantes tecnológicos como IBM y gran cantidad de desarrolladores. El dinero recaudado inicialmente está gestionado por Etherum foundaion[2], una compañía sin animo de lucro ubicada en Suiza.

2.1.1. Hardfork y el cisma de ethereum

En 2016 una organización autonoma descentralizada llamada The DAO, un conjunto de contratos inteligentes reunieron un total de USD $150 millones en una crowdsale. Al final DAO esplotó cuando en junio USD $50 millones en Ether fueron reclamados de manera anonima. El suceso inició un debate sobre si de debía hacer un hard-frok vinculo y como resutado de la disputa, la red se dividió en dos: Ethereum, el objetivo de este trabajo,que continuó la cadena modificada, y Ethereum Classic, que continuó la cadena original.

Figura 1:

[2] https://www.ethereum.org/foundation