



# 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 compañías 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 compañía 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<sup>1</sup> 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 inició en 2008 el desarrollo de bitcoin. Este hecho desencadenaría un desarrollo increíble 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 consenso. A raíz de estas surgieron otras tecnologías basadas en la cadena de bloques, como namecoin, añadiendo. Lo que ethereum pretende es proveer una cadena de bloques con un lenguaje turing completo integrado que pueda ser usado para el desarrollo de contratos inteligentes, permitiendo a los usuarios la creación de proyectos solo escribiendo la logica de estos en unas pocas lineas de código. Algunos de estos proyectos, sacados de la propia web [ethereum.org](https://www.ethereum.org) serían la creación de un crowdfunding 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.

---

<sup>1</sup><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 proveerá 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 transformar 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 proyecto se inició un crowdfunding 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 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 Ethereum foundation<sup>2</sup>, una compañía sin ánimo de lucro ubicada en Suiza.

#### 2.1.1. Hardfork y el cisma de ethereum

En 2016 una organización autónoma descentralizada llamada The DAO, un conjunto de contratos inteligentes reunieron un total de USD \$150 millones en una crowdsale. Al final DAO explotó cuando en junio USD \$50 millones en Ether fueron reclamados de manera anónima. El suceso inició un debate sobre si se debía hacer un hard-fork [vinculo](#) y como resultado 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. Desde entonces se generó un conflicto entre ambas comunidades.

Figura 1:



---

<sup>2</sup><https://www.ethereum.org/foundation>

## 2.2. Funcionamiento.

Una vez sabemos lo que es ethereum, profundizamos en el funcionamiento de la plataforma. Al usar ethereum, la ‘app’ no requiere ninguna entidad para almacenar y controlar sus datos. Para conseguirlo, ethereum hace uso del protocolo de bitcoin y su diseño de la cadena de bloques, aunque lo ajusta de manera que puede respaldar aplicaciones además del dinero. Sin embargo, ethereum persigue abstraerse del diseño de bitcoin con el fin de que los desaprobadores puedan crear aplicaciones o acuerdos que incluyan medidas adicionales, nuevas normas de propiedad, formatos alternativos de transacciones o diferentes maneras de transferir estados.

El objetivo del lenguaje de programación ‘Turing-completo’ de ethereum es permitir a los desarrolladores escribir más programas (que los que permite la línea de comandos de bitcoin) en los que las transacciones en la cadena de bloques puedan gobernar y automatizar resultados específicos. Tengamos en cuenta que un lenguaje turing-completo es capaz de generar (en teoría) los mismos programas que son desarrollables c++. Esta flexibilidad que ofrece ethereum es la innovación fundamental de ethereum sobre otras plataformas basadas en protocolo bitcoin.

### 2.2.1. Bitcoin como sistema de transición de estados

Aquí van la página 5 y 6 del pdf que te pasé (el whitepaper) [http://www.the-blockchain.com/docs/Ethereum\\_white\\_paper-a\\_next\\_generation\\_smart\\_contract\\_and\\_decentralized\\_application\\_platform-vitalik-buterin.pdf](http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf)

### 2.2.2. Cadena de Bloques de Ethereum

La estructura de la cadena de bloques de ethereum es muy similar a la de bitcoin, dado que se trata de un registro compartido de la historia de transacciones completa. Cada nodo en la red almacena una copia de este historial.

La gran diferencia con ethereum es que sus nodos almacenan también el estado más reciente de cada contrato inteligente, además de todas las transacciones de ether. Para cada aplicación de ethereum, la red tiene que mantener un seguimiento del ‘estado’ o información actual de todas estas aplicaciones, incluyendo el saldo de cada usuario, todo el código del contrato inteligente y dónde se almacena todo. Bitcoin usa salidas de transacción no utilizadas para rastrear quién tiene cuánto bitcoin. Aunque suena complejo, la idea es bastante simple. Cada vez que se hace una transacción de bitcoin, la red ‘rompe’ la cantidad total como si fuera dinero impreso, emitiendo bitcoins de vuelta de una forma que hace que la información manejada se comporte como las monedas o cambio físico.

Para efectuar futuras transacciones, la red de bitcoin tiene que añadir todas las piezas de cambio, que se clasifican en ‘gastadas’ o ‘no gastadas’. Ethereum, por otro lado, utiliza cuentas. Como en fondos de cuentas bancarias, las ‘fichas’ de ether aparecen en una cartera, y pueden ser portados (por así decirlo) a otra cuenta. Los fondos siempre están en algún sitio, pero no tienen lo que podría llamarse una relación continua. **Extender.**

### 2.2.3. Máquina Virtual de Ethereum

Con ethereum, cada vez que se usa un programa, una red de miles de computadores lo procesa. Los contratos escritos en un lenguaje de programación específico de contrato inteligente se compilan en ‘bytecode’, lo que una prestación llamada ‘ethereum virtual machine’ (EVM) puede leer y ejecutar. Todos los nodos ejecutan este contrato usando sus EVMs. Cada vez que un

usuario realiza alguna acción, todos los nodos de la red tienen que estar de acuerdo en que ese cambio se ha efectuado. El objetivo aquí es que la red de mineros y nodos tomen la responsabilidad de transferir el cambio de estado a estado, en lugar de cualquier autoridad como PayPal o un banco. Los mineros de bitcoin validan el cambio de propiedad de bitcoins de una persona a otra. La EVM ejecuta un contrato con las reglas que el desarrollador programó inicialmente.

El cálculo real en la EVM se consigue mediante un lenguaje ‘bytecode’ basado en pilas, pero los desarrolladores pueden escribir contratos inteligentes en lenguajes de alto nivel como Solidity o Serpent, más fáciles de leer y escribir para las personas, dado que bytecode es un lenguaje poco legible, pero mmás interpretable a un ordenador, análogo al lenguaje máquina. Los mineros son los que evitan un mal comportamiento. A diferencia de en bitcoin, la cantidad de nodos es escalable, por lo que la ausencia de mineros no será un problema a largo plazo. Por ejemplo, deben asegurarse de que nadie gasta dinero más de una vez, y rechazar contratos inteligentes que no se han pagado. Existen varios miles de nodos de ethereum ahí fuera, y cada uno de ellos está compilando y ejecutando el mismo código.

Podemos pensar que todo esto tiene un coste mucho mayor al de cálculos ordinarios, lo cual es cierto. Por ello la red solo debe usarse para casos de uso particular. El tutorial oficial de desarrollo de ethereum reconoce esta ineficacia, declarando: <sup>A</sup> grandes rasgos, una buena heurística para usar es que no podrás hacer nada en la EVM que no puedas hacer en un teléfono inteligente de 1999”.

#### **2.2.4. mensajes, transacciones y estado de transición de ethereum**

leer y resumir secciones del whitepaper

#### **2.2.5. Contratos inteligentes.**

[https://en.wikipedia.org/wiki/Smart\\_contract](https://en.wikipedia.org/wiki/Smart_contract) Meter fotito por aquí para amenizar la lectura

#### **2.2.6. Minería**

<https://www.coindesk.com/information/ethereum-mining-works/> <https://www.coindesk.com/information/how-to-mine-ethereum/>

#### **2.2.7. Hardfork**

<https://es.cointelegraph.com/news/hard-fork-y-soft-fork-en-qu%C3%A9-consisten-y-cu%C3%A1les-son-sus-diferencias>

### **3. Aplicaciones.**

En general, hay tres tipo de aplicaciones montadas encima de ethereum. La primera categoría es aplicaciones de financiación, las cuales habilitan una vía más amplia de gestionar los contratos. La segunda categoría son aplicaciones semifinancieras, donde el dinero está involucrado pero hay una gran parte de importancia en valores no monetarios. Por último estarían las plataformas para organizaciones de gobiernon descentralizado y voto, no monetarias en ningún sentido.

### 3.1. Sistemas de Token.

Los sistemas de tokens basados en cade de bloques tienen multitud de aplicaciones, desde representar alguna divisa o materia relacionada con el mundo real como el precio del venta de oro o intercambio de USD. Otros usos serían tokens en relación a conceptos como propiedad intelectual o sistemas no relacionados en ningún punto, no financieros en ningún aspecto.

Los sistemas de token son muy fáciles de implementar con ethereum. El punto clave para entender el funcionamiento es darse cuenta de que cualquier sistema de token es, fundamentalmente, una base de datos con una operación: Quita  $x$  unidades a  $A$  y dáselas a  $B$ , con condición de que:

- $A$  tiene al mmenos  $X$  unidades antes de la transacción.
- La transacción está aprobada por  $A$ .

Todo lo restante sería implementar esta lógica en un contrato. Un código básico sería:

---

**Algorithm 1** Contrato de Tokens.

---

```
1: procedure TOKEN( $msg, contract$ )           ▷  $msg$  contiene la información de la comunicación
2:                                           ▷  $contract$  contiene información del contrato
3:    $from = msg.sender$ 
4:    $to = msg.data[0]$ 
5:    $value = msg.data[1]$ 
6:   if  $contract.storage[from] \geq value$  then
7:      $contract.storage[from] = contract.storage[from] - value$ 
8:      $contract.storage[to] = contract.storage[to] + value$ 
9:   end if
10: end procedure
```

---

Esto sería una implementación en pseudo-código de la lógica básica del sistema bancario ya descrito.

### 3.2. Sistema de comprobación de identidad y reputación.

INVESTIGAR Y DESARROLLAR

### 3.3. Decentralized File Storage

### 3.4. Decentralized Autonomous Organizations

## 4. Particularidades.

### 4.1. Ether.

AQUÍ VA LA PAGINA QUE HAY QUE TRADUCIR.

<https://www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency/>  
si pinchas aquí te lleva.

### 4.2. DoS attack.

Dado el incidente del DAO, hemos de explicar en que consiste este ataque hecho a la red.

[https://en.wikipedia.org/wiki/Denial-of-service\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)

Esto se solvento hipotéticamente a finales de 2016 al mejorar la denfensa en este tipo de ataques.  
investigar como lo han hecho

**4.3. Escalabilidad**

**4.4. Minería centralizada**



## Índice

<b>1. Introducción</b>	<b>1</b>
<b>2. Ethereum</b>	<b>2</b>
2.1. Historia. . . . .	2
2.1.1. Hardfork y el cisma de ethereum . . . . .	2
2.2. Funcionamiento. . . . .	3
2.2.1. Bitcoin como sistema de transición de estados . . . . .	3
2.2.2. Cadena de Bloques de Ethereum . . . . .	3
2.2.3. Máquina Virtual de Ethereum . . . . .	3
2.2.4. mensajes, transacciones y estado de transición de ethereum . . . . .	4
2.2.5. Contratos inteligentes. . . . .	4
2.2.6. Minería . . . . .	4
2.2.7. Hardfork . . . . .	4
<b>3. Aplicaciones.</b>	<b>4</b>
3.1. Sistemas de Token. . . . .	5
3.2. Sistema de comprobación de identidad y reputación. . . . .	5
3.3. Decentralized File Storage . . . . .	5
3.4. Decentralized Autonomous Organizations . . . . .	5
<b>4. Particularidades.</b>	<b>5</b>
4.1. Ether. . . . .	5
4.2. DoS attack. . . . .	5
4.3. Escalabilidad . . . . .	6
4.4. Minería centralizada . . . . .	6