Ethereum

Una nueva visión de la cadena de bloques

Ana Peña
Pedro Bonilla

28 de noviembre de 2017

Universidad de Granada

Contenidos.

Introducción.

Objetivo.

Tras el boom de las cadena de bloques, las criptodivisas simples quedaban cortas y, con el objetivo de dar más funcionalidad a esta tecnología, nació ethereum.

Historia.

- 2014 • WhitePaper de Vitalik Buterin.
- 2014 • Crowdfounding.
- 2015 • Lanzamiento de la plataforma.
- 2016 • Desastre de la DAO.
- 2016 • Nace Ethereum classic.
- 2016 • Dos hard-fork más.
- 2017 • Refuerzo de la seguridad.
- 2017 • Prohibición de las ICO en China.
- 2017 • Exposición de Fundamentos de Redes

Ethereum.

Una vez vemos el objetivo que tiene este sistema, vamos a profundizar en detalles de su funcionamiento,

Bitcoin como sistema de transición de estados.

Podemos ver el la cadena como un sistema de transición de estados. Esto Seá importante para ver las posibilidades de esta entidad.

- Los estados serían el conjunto de la información escrita en cada bloque.
- Tendríamos una función de transicion:
  $APPLY(S, TX) \rightarrow S'$ o $ERROR$

Bitcoin como sistema de transición de estados.

Ejemplifiquemos el uso de este sistema.

- $APPLY(\{Ana : 50, Pedro : 50\}, \text{"enviar 20 de Ana a Pedro"})$
  Ana: 30 , Pedro: 70
- $APPLY(Ana : 50, Pedro : 50, \text{"enviar 70 de Ana a Pedro"})$
  ERROR

Cadena de bloques.

Una cadena de bloques es una base de datos distribuida, formada por cadenas de bloques diseñadas para evitar su modificación una vez que un dato ha sido publicado usando un sistemabasado en el tiempo y el consenso de los usuarios de esta.

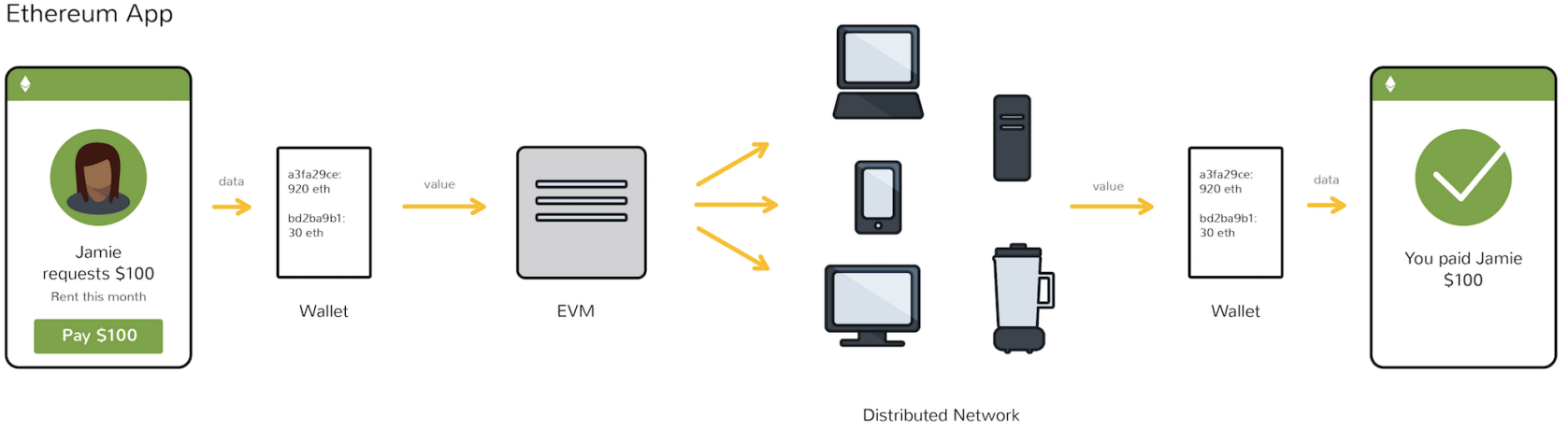
Cuentas.

Las cuentas son las entidades base de ethereum, y contiene 4 campos:

- Nonce.
- Valor.
- Código de Contrato.
- Almacenamiento.

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.

Mensajes, Transacciones y estado de transición.

Los mensajes en ethereum son parecidos de cierto modo a las transacciones de en otros sistemas de cadena de bloques, pero con algunas caracteristicas llamativas. Un mensaje puede ser creado tanto por una entidad externa como por un contrato, los mensajes pueden contener datos o, si el mensaje es recibido por un contrato, este tiene la opcion de responder. Esto implica que un mensaje en etherum puede toar el aspecto de función.

Contratos inteligentes.

Un contrato inteligente (en inglés Smart contract) es un programa informático que facilita, asegura, hace cumplir y ejecuta acuerdos registrados entre dos o más partes (por ejemplo personas u organizaciones). Como tales ellos les ayudarían en la negociación y definición de tales acuerdos que causarán que ciertas acciones sucedan como resultado de que se cumplan una serie de condiciones específicas.

Minería y Prueba de Trabajo.

La minería juega un papel importante en asegurarse como funciona ethereum, pero de forma subliminal. Además del objetivo de generar nuevos ether sin la necesidad de un banco, pero esta no es su único rol. Normalmente, es la compañía que centraliza las operaciones (como un banco) la que se asegura de mantener resgistros adecuados de los datos. Sin embargo, los sistemas de cadena de bloques introducen una nuevo modo de mantener el resgistro de acciones, cuando es la red entera la que se asegura de mantener el registro de transacciones, en lugar de un intermediario, y las anota en un registro público.

Hardfork y Sotfork.

el término fork hace referencia al despliegue de cambios en el código de la cadena de bloques. La bifurcaión sucede cuando el equipo detras de ethreum quiere implantr cambios en la estructura por diversos motivos. Como la cadena de bloques es una estructura de datos descentralizada, hay diferentes, esto provoca que estas situcaciones generen cadenas de bloques alternativas. Es lo que se conoce como bifurcación de la Blockchain, y aquí es donde entran en juego los conceptos de hardfork y softfork.

Aplicaciones.

Sistemas de Token.

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] >= value then
7:          contract.storage[from] = contract.storage[from]  value
8:          contract.storage[to] = contract.storage[to] + value
9:      end if
10: end procedure
```

Sistema de identidad.

Algorithm 1 Sistemas de identidad.

```
1: procedure IDENTIDAD(msg, contract)                ▷ msg contiene la información
2:     if contract.storage[tx.data[0]] ≠ 0 then
3:         contract.storage[tx.data[0]] = tx.data[1]
4:     end if
5: end procedure
```

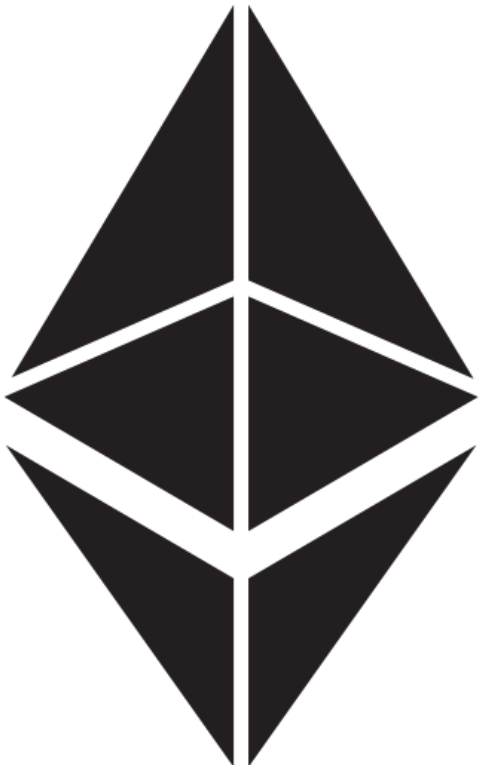
Más aplicaciones.

¡En el github `https://github.com/pedrobn23/Ether` tenemos más, mirenlo para profundizar vuestro saber!

Particularidades.

Ether.

Aunque nadie sea dueño de ethereum, el sistema que respalda esta funcionalidad no es gratis. Mejor dicho, la red necesita el 'ether', una pieza única de código que puede usarse para pagar por los recursos computacionales necesarios para ejecutar una aplicación o programa. El ether no es más que la divisa utilizada en ethereum para las transacciones.



DoS attack.

En el pasado se han visto problemas con la capacidad de ethereum para soportar este tipo de ataques, por ejemplo en la compañía bancor. Estos problemas están relacionados con la capacidad de escalabilidad de ethereum. Por ello, vamos a explicar en que consiste este tipo de ataques.

`https://motherboard.vice.com/en_us/article/newk7m/the-ethereum-network-is-ddos-ing-itself`

Escalabilidad.

Una preocupación común acerca de Ethereum es el tema de la escalabilidad. Ethereum sufre el defecto de que cada transacción tiene que ser procesada por cada nodo en la red.

Minería centralizada .

Actualmente, las dos mining pools principales indirectamente controlan aproximadamente el 50 % del poder de procesamiento en la red de Bitcoin, aunque esto está mitigado por el hecho de que los mineros pueden cambiarse a otras mining pools si una pool o coalición pretende llevar a cabo un **ataque del 51 %**. El propósito actual en Ethereum es usar un algoritmo de minería basado en generar aleatoriamente una única función hash por cada 1000 'nonces', usando un rango de computación lo suficientemente amplio para eliminar el beneficio del hardware especializado.

Conclusiones

¡Muchas gracias!