



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES



ciie

Centro de Investigación
e Innovación Educativa

Bitcoin como una organización descentralizada

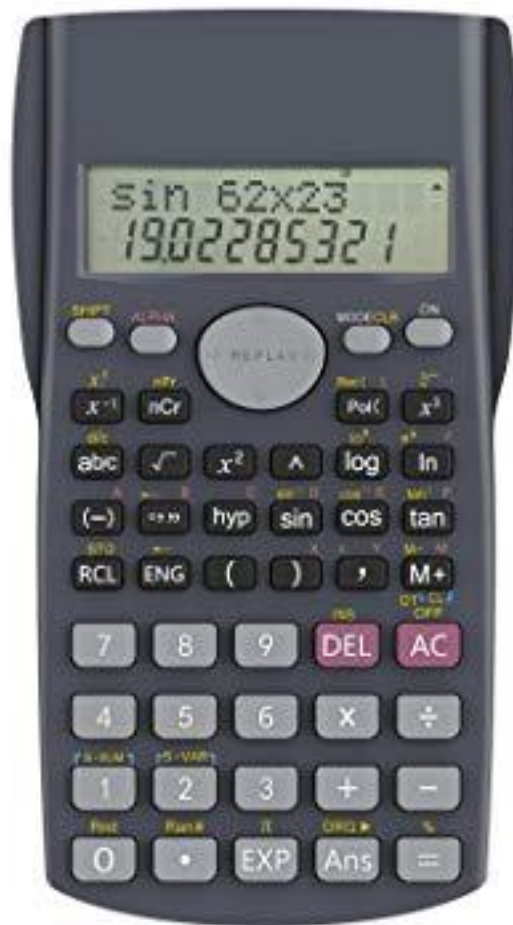
6.1 Ethereum, la otra blockchain

¿Por qué Ethereum?

- Las blockchains son útiles para hacer cosas. Útiles no quiere decir eficiente.
- ¡No solo dinero! Emisión de activos, crowdfunding, registro de dominios, registro de títulos, juegos de azar, predicción de mercado, internet de las cosas, votaciones, cientos de aplicaciones!

Problema

La mayoría de las blockchains estaba diseñada de esta forma:



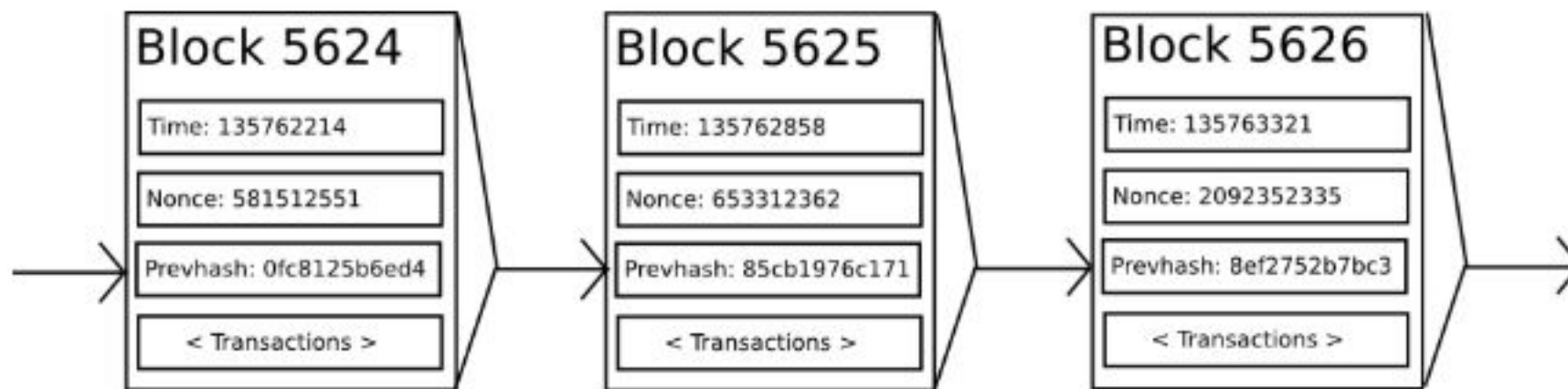
Ethereum

Ethereum está pensado para ser una computadora de propósitos generales



Ethereum – El concepto

Ethereum es una blockchain



Ethereum – El concepto

Ethereum tiene diferencias con respecto a Bitcoin:

- 1) Un lenguaje de programación Turing Complete incorporado.
- 2) Dos tipos de cuentas
 - Cuentas de usuario (controladas por claves privadas)
 - Contratos (controlados por código)
- 3) Cualquiera puede crear una aplicación con cualquier regla definiéndolo como un contrato
 - Desde la lógica matemática se entiende como $P \rightarrow Q$

Ethereum – Estado vs Historia

- 1) Estado = información “actual”
 - Saldos de cuentas
 - Nonces
 - Código del contrato y almacenamiento de contrato.
- 2) Historia = cosas que pasaron
 - Transacciones
 - Recibos
- 3) Actualmente, todos los nodos "completos" almacenan el estado, algunos almacenan la historia y algunos no almacenan historia.

Ethereum – Estado

- 1) El estado consiste en direcciones de mapeo de valores clave para los objetos de cada cuenta.
- 2) Cada objeto de cuenta contiene 4 datos:
 - Nonce
 - Balance
 - Almacenamiento de las raíces de los árboles de merkle y los árboles de patricia

Ethereum – Ejecución de código

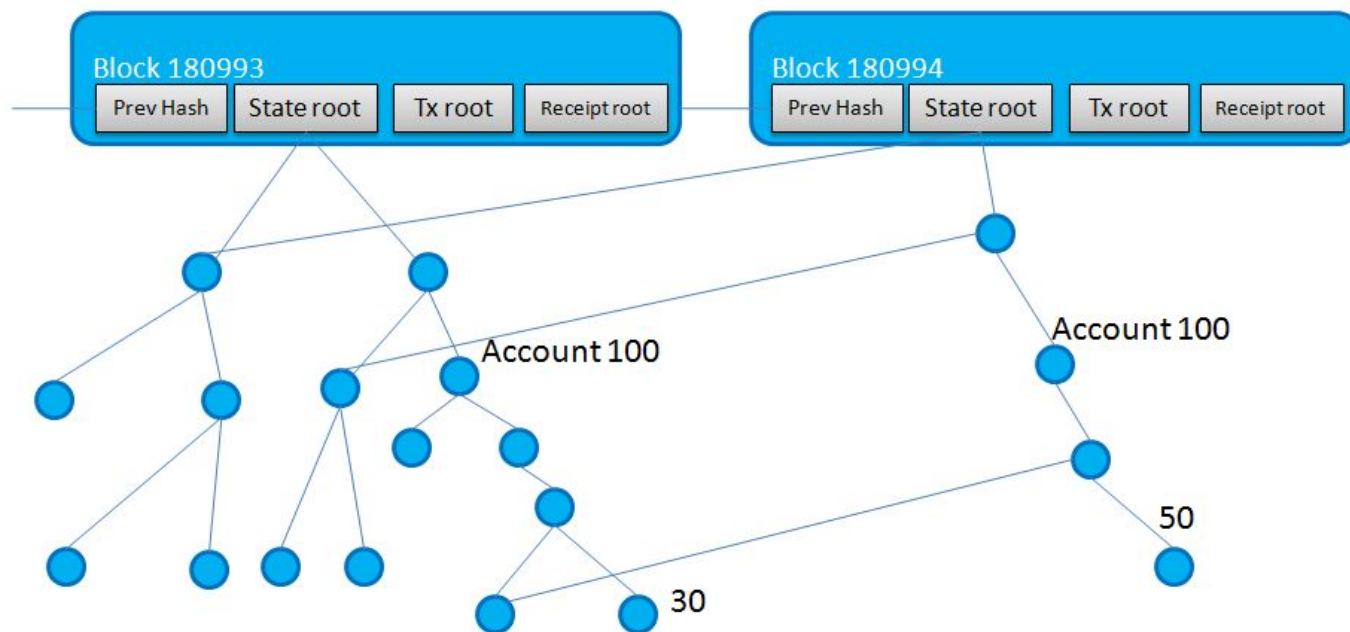
- 1) Cada transacción especifica una dirección "a quien" se envía (a menos que esté creando un contrato).
- 2) El código de la dirección "a quien" se ejecuta.
- 3) El código puede:
 - Enviar ETH a otros contratos
 - Leer / escribir en el almacenamiento
 - Llamar (iniciar ejecución) otros contratos
- 4) Cada nodo (completo) en la blockchain procesa cada transacción y calcula y almacena el nuevo el estado, al igual que Bitcoin.

Ethereum – GAS

- 1) Problema de "detenimiento":
 - No puedo decir de antemano si un programa se ejecutará o no infinitamente
- 2) Solución: es una tarifa por paso de cálculo ("gas")
- 3) Las tarifas especiales también se aplican a las operaciones que ocupan almacenamiento
- 4) Contraparte al límite de tamaño de bloque como en bitcoin
- 5) Mecanismo de votación (puede aumentar / disminuir el límite de gas por 0.0976% cada bloque)

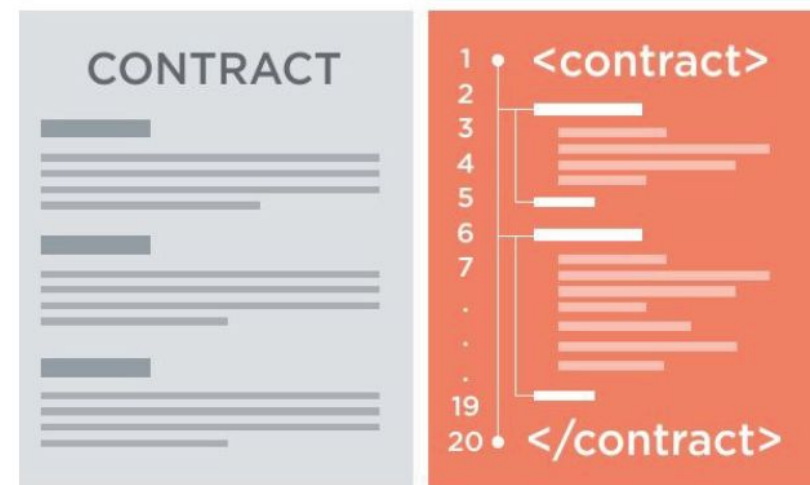
Ethereum – Árboles de Merkle y Patricia

- 1) Cada encabezado de bloque contiene tres intentos- Transacciones, Estado, Recibos
- 2) Patricia trees son usados para permitir eficientemente insertar / eliminar operaciones



Ethereum – Contratos inteligentes

1. La transacción debe involucrar más que la simple transferencia de una moneda virtual de una persona a otra (es decir, una transferencia de pago),
2. La transacción involucra a dos o más partes (como todo contrato debe).
3. La implementación del contrato no requiere la participación humana directa después de que el contrato inteligente se haya convertido en parte de la cadena de bloques. Es este último elemento que hace que estos contratos sean "inteligentes" y, por lo tanto, amerita una discusión más detallada.



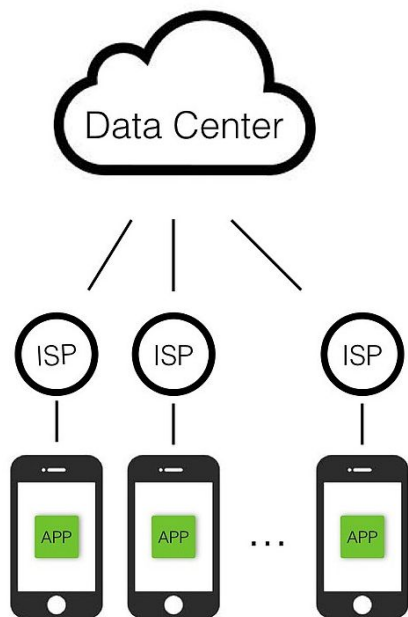
Traditional and Coded (Smart)

Ethereum – Aplicaciones descentralizadas

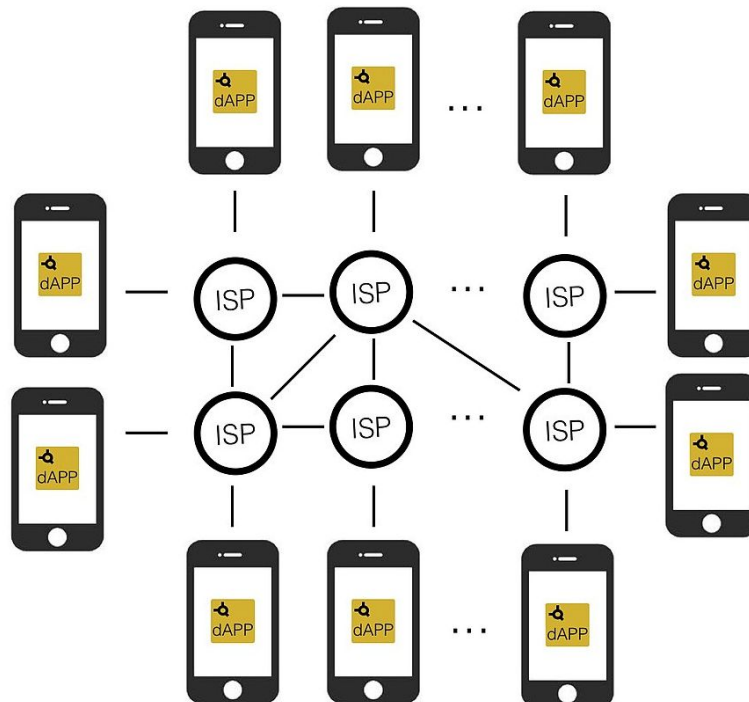
1. La aplicación debe ser completamente de código abierto, debe funcionar de forma autónoma y sin ninguna entidad que controle la mayoría de sus tokens. La aplicación puede adaptar su protocolo en respuesta a las mejoras propuestas y los comentarios del mercado, pero todos los cambios deben decidirse por consenso de sus usuarios.
2. Los datos de la aplicación y los registros de operación deben almacenarse criptográficamente en una cadena de bloques pública y descentralizada para evitar puntos centrales de falla.
3. La aplicación debe usar un token criptográfico (bitcoin o un token nativo de su sistema) que es necesario para acceder a la aplicación y cualquier contribución de valor de (mineros / agricultores) debe ser recompensada en los tokens de la aplicación.
4. La aplicación debe generar tokens de acuerdo con un algoritmo criptográfico estándar que actúa como una prueba de que los nodos de valor contribuyen a la aplicación (Bitcoin utiliza el algoritmo de prueba de trabajo).

Ethereum – Aplicaciones descentralizadas

Apps



dApps



Ethereum – Usos de las Dapps

Las aplicaciones descentralizadas pueden en un futuro tener varios casos de uso. Algunos ejemplos son:

1 - Gestión de la identidad. Dado que cada usuario en la plataforma Ethereum firma digitalmente todas sus interacciones con contratos inteligentes u otros usuarios, es posible asociar una identidad a un usuario y todas las acciones realizadas por ese usuario estarán conectadas a su identidad. - Civic y Blockstack son dos proyectos que apuntan a administrar la identidad en la cadena de bloques.

Ethereum – Usos de las Dapps

Las aplicaciones descentralizadas pueden en un futuro tener varios casos de uso. Algunos ejemplos son:

1 - Gestión de la identidad. Dado que cada usuario en la plataforma Ethereum firma digitalmente todas sus interacciones con contratos inteligentes u otros usuarios, es posible asociar una identidad a un usuario y todas las acciones realizadas por ese usuario estarán conectadas a su identidad. - Civic y Blockstack son dos proyectos que apuntan a administrar la identidad en la cadena de bloques.

Ethereum – Usos de las Dapps

2 - Confianza y transparencia. Cada vez que se puede expresar un acuerdo a través del lenguaje de programación, los contratos inteligentes se pueden usar como una forma de reemplazar (y hacer cumplir) los contratos entre las partes. También se puede utilizar para la transparencia. Por ejemplo: digamos que desea donar a una organización sin fines de lucro, pero queremos asegurarnos de que usen los fondos para apoyar proyectos de agua potable en África. Existen aplicaciones y plataformas en Ethereum que supervisan cómo se utilizan los fondos en tiempo real.

Ethereum – Usos de las Dapps

3 - Crowdfunding. Los contratos inteligentes de Ethereum nos permiten generar tokens (ERC20) que pueden venderse a cambio de "dinero real", lo que efectivamente financia los nuevos proyectos o nuevas empresas. Muy parecido a Kickstarter o Indiegogo, pero sin la necesidad de confiar en un tercero. 2017 fue el año de las ofertas iniciales de monedas (ICO son sus siglas en inglés), cualquier empresa escribía un whitepaper contando las maravillas de sus monedas y las salieron a vender al público. Durante el 2018 más del 50% de ellas ya habían fallado antes de llegar a la mitad de año.

Ethereum – Usos de las Dapps

4 - Marketplaces. Imaginemos un Airbnb donde los huéspedes puedan interactuar directamente con los anfitriones y no tener comisiones por servicios, o un Facebook donde los usuarios interactúen, sean propietarios de todos sus datos y obtengan una parte de los pagos que hacen los anunciantes para obtener su atención. O un Uber pero sin Uber. Ethereum nos permite crear marketplaces descentralizados en donde los usuarios pueden confiar entre sí sin los intermediarios y sus comisiones.

Ethereum – Usos de las Dapps











5 – Copyright . Cuando uno envía una transacción en la red Ethereum, la información se agrega permanentemente en la cadena de bloques de Ethereum. Son inmutables, tienen una marca de tiempo de cuando se han agregado y no se pueden eliminar. Por estos motivos, puede guardar prueba de propiedad, registrar su IP o los derechos de autor de una canción o un libro, en la cadena de bloques Ethereum con la certeza de que nadie puede eliminarla y siempre podrá demostrar que usted es el autor y propietario de dicho documento.

Ethereum – Usos de las Dapps

6 – Gobierno. Ethereum es una buena plataforma para manejar sistemas de votación a escala. Dado que cada usuario de esta computadora global puede interactuar con ella de una manera segura e infalsificable, Ethereum se puede utilizar para implementar sistemas de votación para elecciones, gobierno corporativo, toma de decisiones y acuerdos de consenso.

Ethereum – Estados de las Dapps

<https://www.stateofthedapps.com/rankings>

		PLATFORM		CATEGORY			
		All platforms		All categories			
# ?		Platform	Category	Users (24h) ?	Volume (7d) ?	Dev activity (30d) ?	User activity (30d) ?
1	 DrugWars The drugs are virtual, but the money is real	Steem	Games	5,421 +0.22%	938 STEEM 307 USD +15.13%	208 -6.73%	
2	 Steemit Social blogging platform	Steem	Social	3,678 -6.10%	0 STEEM 0 USD -	1,469 +194.39%	
3	 Geon App Visit locations. Get Paid.	POA	Games	1,027 +2.19%	0 POA 0 USD -	0 -100.00%	
4	 Basic Attention Token Digital advertising	Ethereum	Wallet	2,073 -1.61%	0 ETH 0 USD -	682 -25.22%	
5	 MakerDAO Where you can interact with the Dai Credit System	Ethereum	Finance	1,043 +37.24%	40,996 ETH 7,862,596 USD +108.34%	1,463 -25.24%	

El futuro de Ethereum

Ethereum es un proyecto independiente de Bitcoin pero complementario, ya que ofrece cualidades y características distintas. En su futuro tiene:

1. Prueba de arriesgo (proof of stake)
2. Soporte de privacidad (Zsnarks)
3. Alquiler de blockchain
4. Actualizaciones de la Máquina Virtual
5. Uso más flexible del almacenamiento.
6. Escalabilidad