



UNIVERSIDAD
DE LA REPÚBLICA
URUGUAY

SCIENCE

DENSITY

Seminario de Tecnologías

Ing. Luis Azevedo

Ing. Ramiro Roselli

MSc. Ing. Roberto Kreimerman

POWER

ILLUMINATION

LIGHTING

TEAM

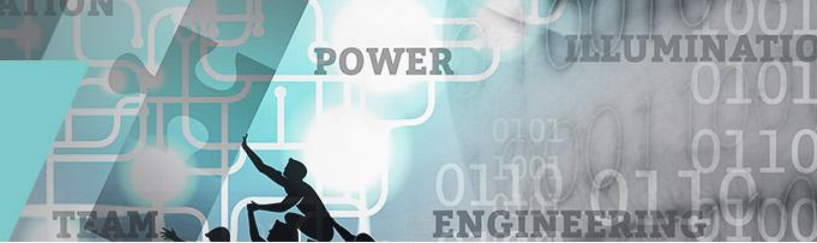
ENGINEERING



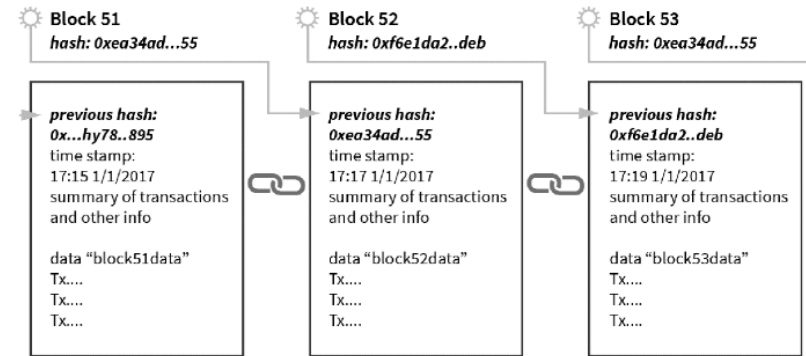
Blockchain



Introducción a *blockchain*

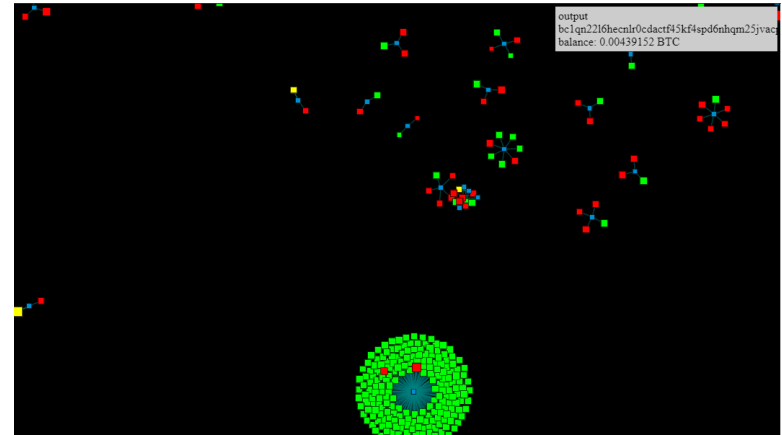


- Una cadena de bloques (*blockchain*) es una estructura de datos que permite crear un registro digital de datos (*data ledger*) y compartirlo a través de una red de participantes independientes.



Bitcoin

- Es una *blockchain* publica, una gran red distribuida que corre sobre una criptomoneda nativa. Se dice que es publica porque cualquiera puede participar y el código es abierto a la comunidad.
- Una criptomoneda (*cryptocurrency*) en un dato que puede ser intercambiado entre dos partes. Es un protocolo.
- El uso de criptografía permite que cada participante de una red administre el registro de forma segura sin la necesidad de una autoridad centralizada que dicte las reglas.



About: Visualization of bitcoin transactions (unconfirmed ones).

Node size scale: LINEAR LOG
LEGEND: Green = input, Red = output, Yellow = input+output, Blue = transaction
NAVIGATION: mouse = scroll = pan/zoom, SPACE = run/pause
TODO:

- auto remove transactions older than x min or verified
- show transaction details on hover
- connect_disconnect button

¿Qué hacen las *blockchains*?

- Una blockchain es un sistema *peer-to-peer* sin una autoridad central gestionando el flujo de datos.
- Una forma de remover el control de la autoridad central conservando la integridad de los datos es tener una gran red distribuida de usuarios independientes.
- Las computadores que componen esta red se denominan nodos completos (*full nodes*)
- Para que la red no se corrompa, no solo se utiliza blockchain sino una criptomoneda.
- Las redes de blockchain producen cripto monedas para incentivar mantener la integridad de la red.
- Básicamente el software le paga al hardware para operar, el software es el protocolo blockchain.
- Ejemplos de protocolos: Bitcoin, Ethereum, Ripple, Stellar, EOS,....
- El Hardware consiste en nodos completos que aseguran los datos en la red.

Consenso, la fuerza detrás de las blockchain.

- **Consenso** es un proceso para desarrollar un acuerdo entre un grupo común de interesados desconfiados.
- Los interesados desconfiados son los nodos (*full nodes*) de la red.
- Para lograr consenso, Bitcoin por ejemplo, usa un algoritmo llamado *proof of work*

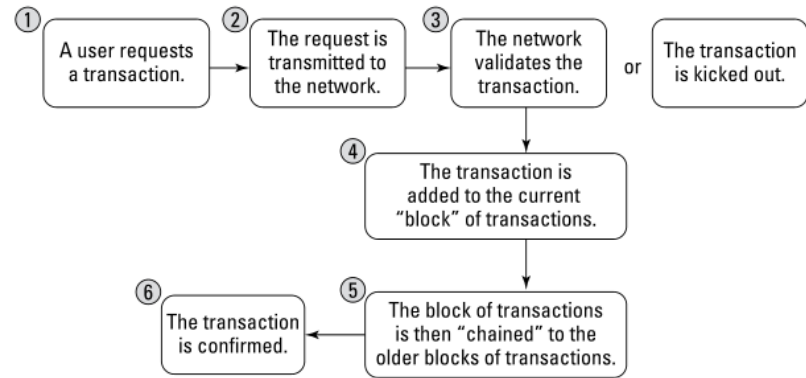
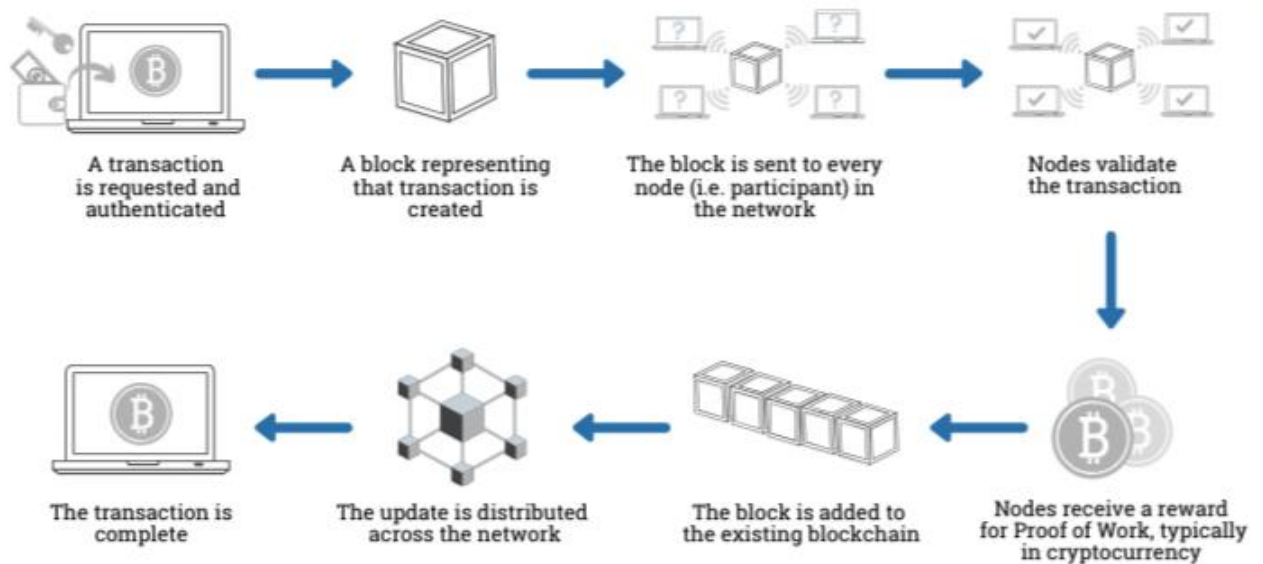


FIGURE 1-2:
How blockchains
work.

Hasta acá...



Client-Server Internet



Web2 Applications vs. Web3 Applications

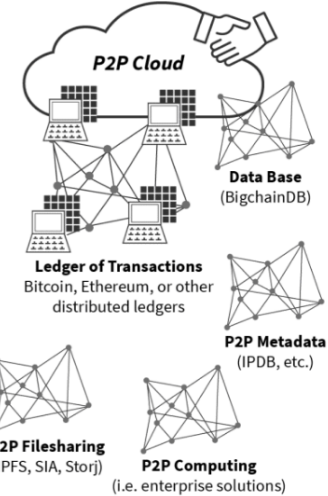
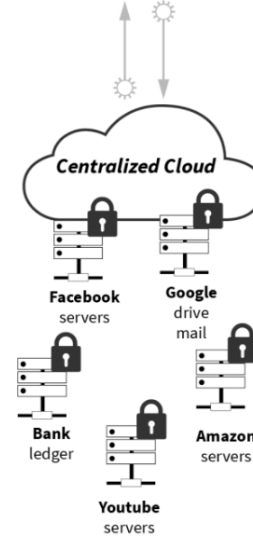
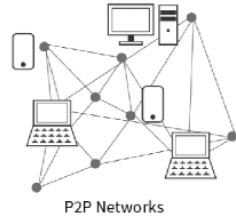
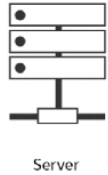
Web 2 Application (client) communicates with servers.



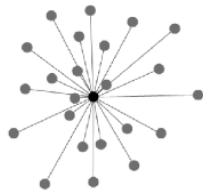
Web 3 Application (client) also referred to as "wallet" communicates with a blockchain network.



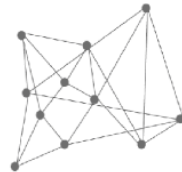
Data Monopoly vs. Data Sovereignty



Centralized vs. Distributed



Unique Point of Failure



No unique Point of Failure
=> more secure

Web2 applications run on a combination of servers owned by different organizations performing various backend operations.

Security is provided by system administrator working for those companies which act as trusted intermediary. They manage all identities (user ID & password combination) and related personal data.

Web3 applications run on a combination of public and/or private networks, performing various backend operations. The distributed ledger serves as the backbone for other the Web3 networks that are all collectively managed and are often incentivized by a token. Security is provided by a P2P network validating transactions by majority consensus.

Ethereum y redes similares



- **Smart Contracts:** Acuerdos automáticos a nivel de aplicación que definen la lógica del negocio y las reglas de comportamiento de todos los participantes
- **Registro de transacciones:** Archivo (ledger) que contiene toda la información desde el bloque de génesis, el cual es almacenada en cada nodo de la red.

Capa de aplicación

(Smart Contracts)

Capa de registro distribuido

- 1.Registro de transacciones (activos)
- 2.Reglas de conceso (infraestructura)
3. Nodos (Red distribuida de computadoras)

Capa de Internet

Enrutamiento de datos

Ethereum y redes similares

- **Reglas de consenso:** Es un conjunto de reglas codificadas de todos los derechos y obligaciones de los nodos en la red. Son las condiciones por las cuales las transacciones son creadas, enviadas y verificadas por la red, incluyendo el incentivo económico (token) & la creación/referenciación de identidades y direcciones.
- **Nodos de la red:** Son los todos los dispositivos que ejecutan el protocolo de blockchain y almacenan los registros.

Capa de aplicación

(Smart Contracts)

Capa de registro distribuido

- 1.Registro de transacciones (activos)
- 2.Reglas de conceso (infraestructura)
3. Nodos (Red distribuida de computadoras)

Capa de Internet

Enrutamiento de datos

Ethereum y redes similares



- **Enrutamiento de datos:**
Responsable del transporte de los datos. Torrent, Tor, Telehash, etc.
TCP/UDP

Capa de aplicación

(Smart Contracts)

Capa de registro distribuido

- 1.Registro de transacciones (activos)
- 2.Reglas de conceso (infraestructura)
3. Nodos (Red distribuida de computadoras)

Capa de Internet

Enrutamiento de datos

Tokens



Tokens

- Tradicionalmente representan alguna forma de valor económico o derechos de acceso.
- Siempre tienen una estructura que asegura su validez. Históricamente, los tokens han sido emitidos y administrados por entidades centralizadas, por ejemplo; bancos centrales.
- La validez y seguridad de los tokens criptográficos son administrados por los Smart Contracts que los crean, junto con el registro distribuido por mayoría consensuada en la red de nodos.

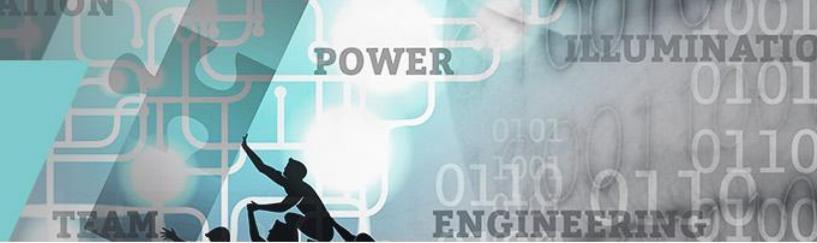


POWER

ILLUMINATION

ENGINEERING

Tokens criptográficos



- Son administrados por el registro distribuido.
- Pueden representar derechos de acceso a una propiedad o servicio.
- Representan un conjunto de reglas, codificadas en un tipo especial de Smart Contract.
- En blockchain, los tokens se representan como una entrada en el registro y son mapeadas a una dirección blockchain que representa la identidad en la blockchain del poseedor de del token

Block

```
03 01 00 00 00 01 00 00
00 00 00 00 00 00 00 00
01 04 45 54 68 65 20 54
14A 61 6E 2F 32 30 30 39
-----
02 00 00 00 00 00 00 001
00 00 00 00 00 00 00 00
00 00 00 00 3B A3 ED FD
67 76 8F 61 7F CB 1B C3
4B 1E 5E 4A 29 AB 5F 49
101 01 00 00 00 01 00 001
-----
101 00 00 00 00 00 00 001
00 00 00 00 00 00 00 00
00 00 00 00 3B A3 ED FD
67 76 8F 61 7F CB 1B C3
4B 1E 5E 4A 29 AB 5F 49
021 01 00 00 00 01 00 00
-----
1FF FF 00 1D 1D AC 2B 7C1
100 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
1FF FF 1D 04 FF FF 00 1D
69 6D 65 73 20 30 33 24
120 43 68 61 6E 63 65 6C
-----
16F 72 20 62 61 6E 6B 731
128 03 00 00 45 41 04
119 67 F1 A6 71 30 B7 10
179 62 20 EA 1F 61 DE B6
F3 55 04 E5 1E C1 12 DB
```

Author: 0xc0ffec254729296a45a38B5639AC7E10F9d54579

Smart contract address:
0xA395b25755DB8258a23eAE0ee76846a4A880888F

Smart contract's ID:
49214

Non-fungible token

getURLfromID(49214)

http://127.0.0.1:8080/protocol/
kqUMyOAGQ8Wf7iEx07H0PktuBtEtahsdxv4n15fY2
GzGrm1rAVzzzb1fkPpb1aX4eVrXr3i3U1Arad4q9v

----- Art, assets, files, etc.

Tokens criptográficos

- Los tokens son accesibles solamente con un software billetera que se comunica con la red blockchain y administra la clave relacionada a la dirección blockchain.
- Solo la persona que tiene la clave privada para esa dirección puede acceder a sus tokens.
- Se pueden crear tokens en la capa de aplicación. Por ejemplo el estándar ERC-20 de Smart Contracts define reglas comunes para tokens Ethereum.



Tokenizacion



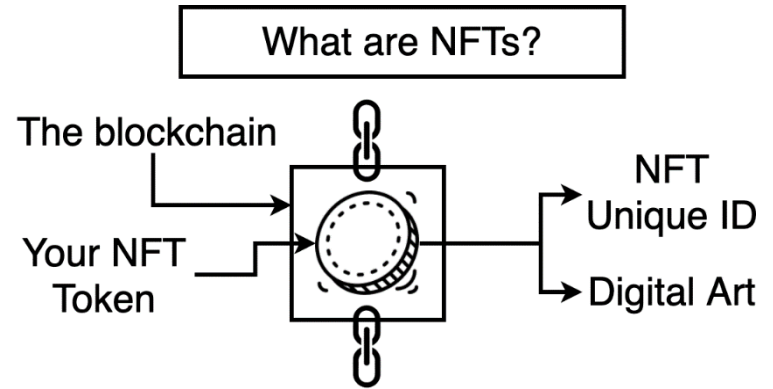
Tokenización

- La habilidad para desplegar tokens a bajo costo y sin mucho esfuerzo esta cambiando el juego.
- Hace posible representar muchos tipos de activos y derechos de acceso en una forma digital que antes no era posible.
- A esto se le llama tokenización y constituye la etapa inicial de la Web3.



NFTs

- Non-fungible tokens (NFTs) son únicos en naturaleza, que representan activos digitales únicos y escasos, como arte, coleccionables o propiedades inmobiliarias.
- Los NFTs pueden representar identidades y certificados, como licencias, títulos, llaves, pases, testamentos, derecho a voto, entradas, derechos de autor, licencias de software, datos médicos, etc.

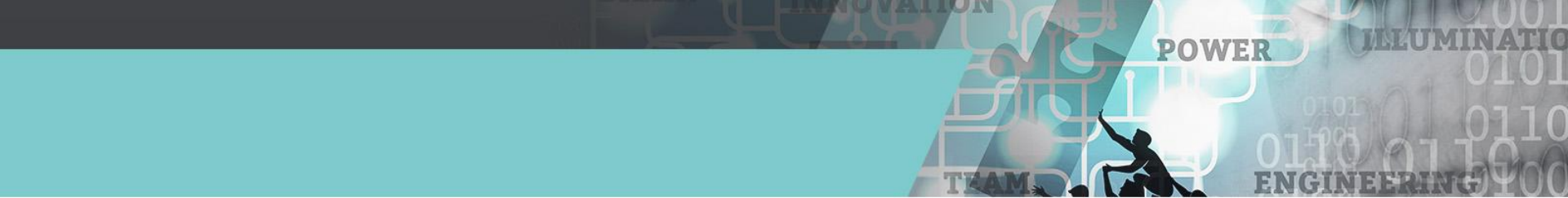


NFTs



- Cada token es único y diferente al resto de los tokens del mismo tipo. Tiene atributos únicos.
- No pueden ser remplazados con tokens del mismo tipo porque representan valores o derechos de acceso únicos. Un título universitario por ejemplo.
- NFTs están atados a una identidad y no son divisibles. No tiene sentido tener una fracción de título universitario.





POWER

ILLUMINATION

TEAM

ENGINEERING

travelX

- Tiene como objetivo acelerar la evolución de la industria de viajes a la Web3, permitiendo un modelos de capacidad de viajes mas transparente, ágil y eficiente.
- NFTickets es un proyecto para tokenizar pasajes de avión que se pueden transferir o revender.
- La plataforma para adquirir pasajes es Travel.xyz



La compañía será una de las primeras aerolíneas en convertir todos sus pasajes en tokens y ofrecerlos como NFTickets, inaugurando una nueva era de flexibilidad para sus usuarios.

26 Septiembre de 2022 16.06

Flybondi y TravelX anuncian su alianza estratégica que busca inaugurar una revolucionaria etapa en la industria de viajes: la **tokenización de los pasajes aéreos** y su evolución a NFTickets.

Business

Norwegian Air May Allow Customers to Pay With Crypto as Soon as Spring

Norwegian Air would accept cryptocurrency payments via crypto exchange NBX.

By Paddy Baker  Feb 20, 2020 at 10:00 a.m. Updated Sep 13, 2021 at 9:19 a.m.





POWER

ILLUMINATION

TEAM

ENGINEERING

