CURSO
BLOCKCHAIN

Modulo 4

Smart Contracts (Parte 1)

CURSO BLOCKCHAIN

Lo visto

Estudiamos:

- Conceptos informáticos: bits, bytes, hexadecimales, algoritmos, seguridad.
- Historia: Criptografía y cypherpunks hasta la invensión de la blockchain y criptomonedas.
- Teoría blockchain: Que es, como funciona, características, casos de uso y como usarla para transferir valor, las wallets y las cuentas.
- Inversiones: Vocabulario que se usa en el mundo cripto y algunas inversiones con las cuales nos podemos encontrar, algunos riesgos y como es que funcionan para ganar capital.

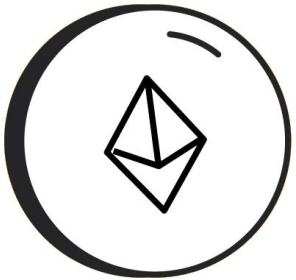
Lo visto

Hoy Estudiaremos:

- **web**: dApps, Web1, Web2, Web3. (15')
- **Oraculos** (5')
- **Smart Contract:** Ethereum, EVM, patriccia merkle tree, variables de estado, programa (codigo), transacciones, gas, caracteristicas, casos de ejemplo, canal de pagos, DAO (Governanza y votacion -> España) (1hs)
- Programación de uno en tiempo real (ERC20 + con contrato legal). (10’)

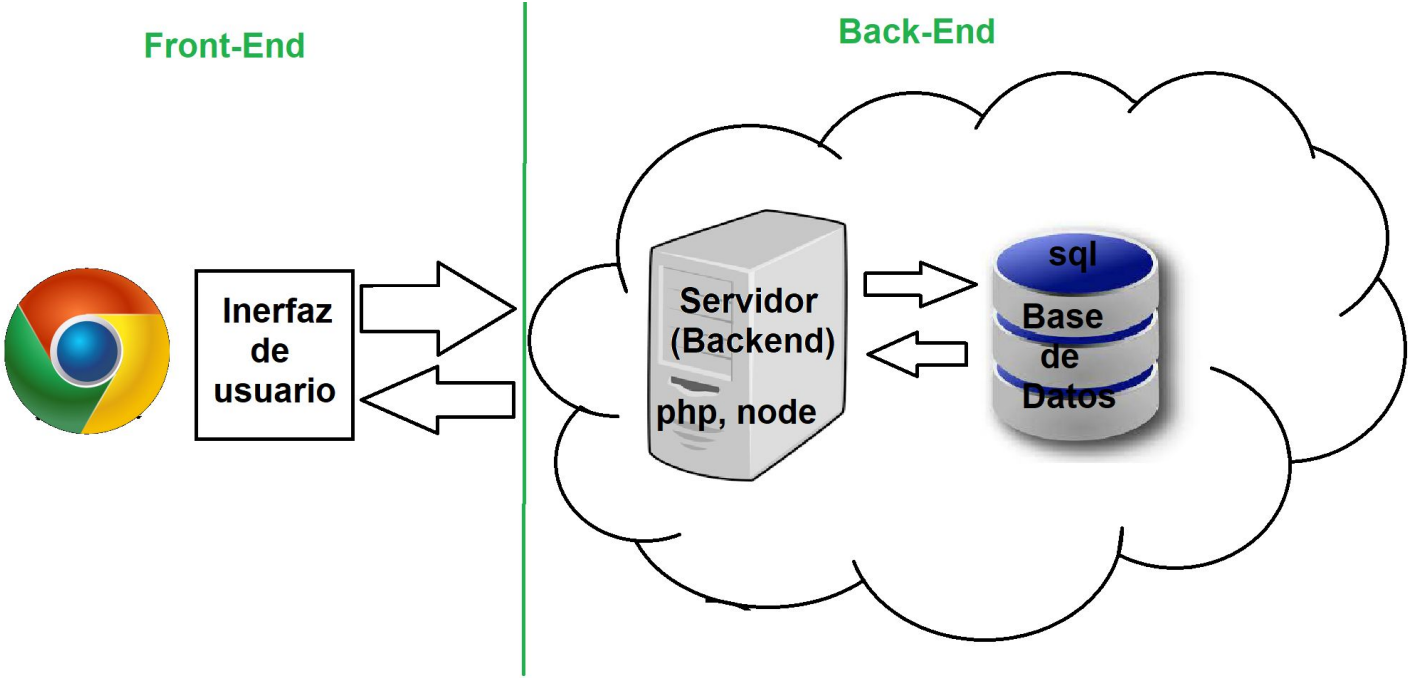
CURSO BLOCKCHAIN

WEB 1, WEB2 y WEB3

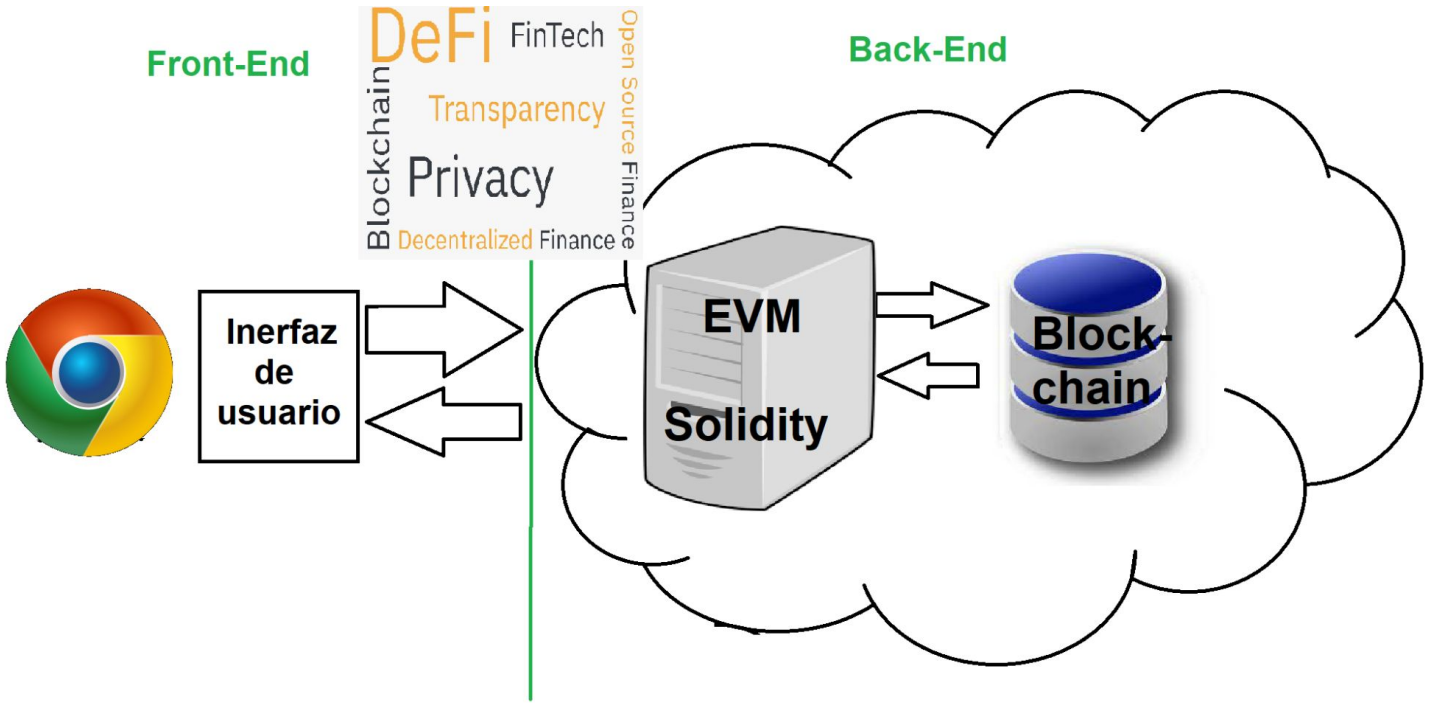
WEB1	WEB2	WEB3
		
Información	Plataformas	Propiedad

CURSO BLOCKCHAIN

WEB2

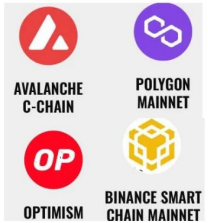


WEB3


Front-End
Back-End
DeFi
FinTech
Transparency
Privacy
Decentralized Finance
Blockchain
Open Source Finance
Inerfaz de usuario
EVM
Solidity
Block-chain

CURSO BLOCKCHAIN

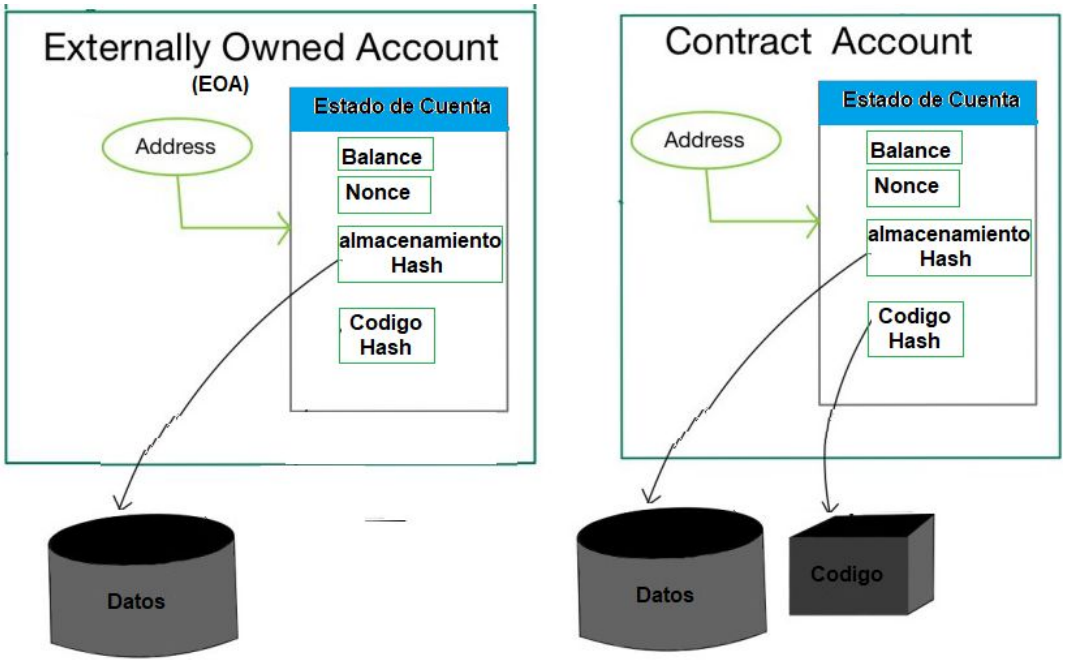
Problema web3



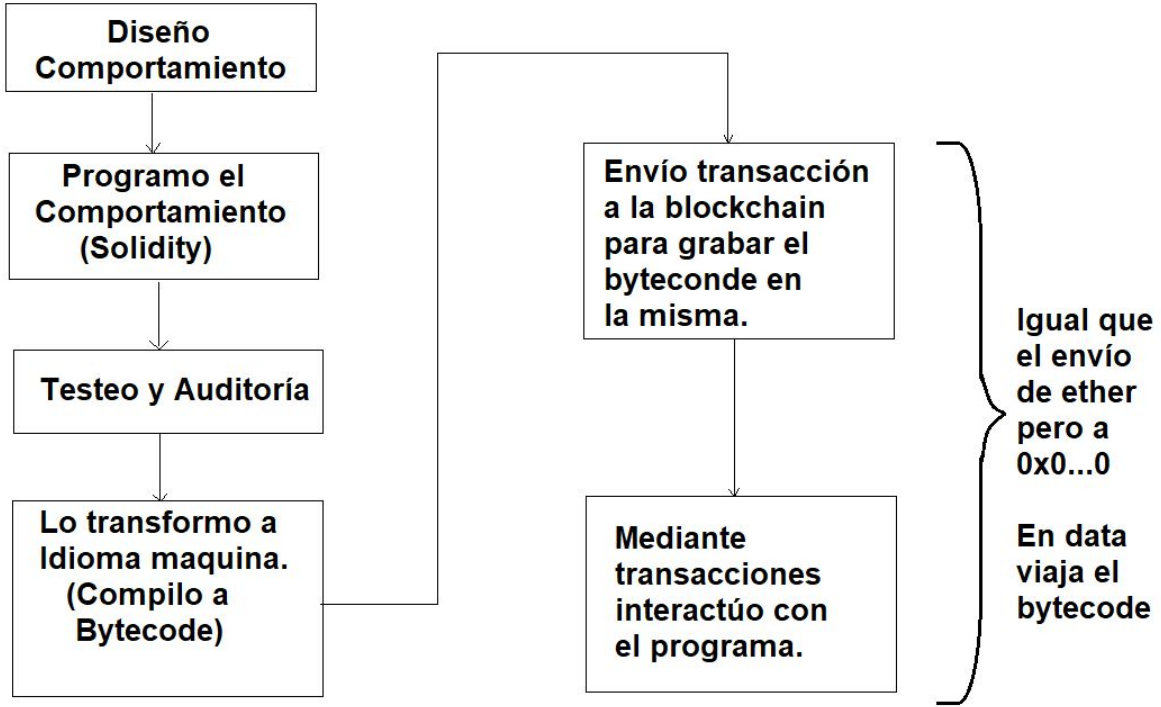
Solución: Oráculos

Chainlink

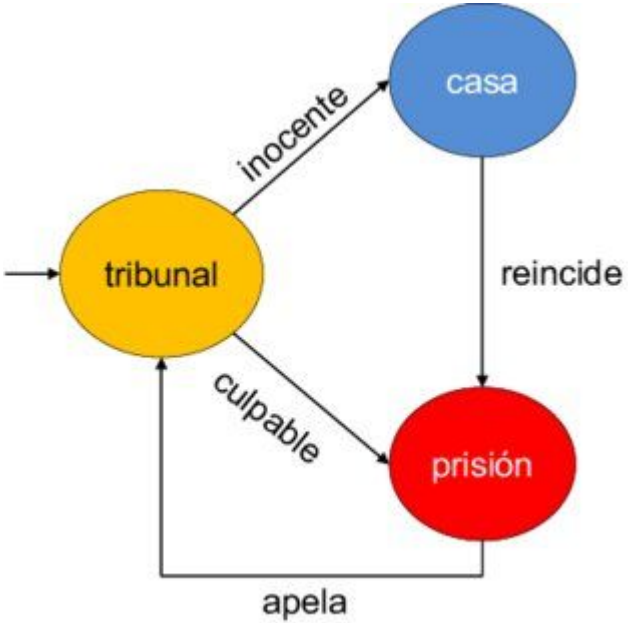
Cuentas e integridad



Diseño y deploy de smart contract



Programando el comportamiento



CURSO BLOCKCHAIN

Smart Contract (solidity)

Características de Smart Contracts

1. **Programables**
2. **Determinísticos**
3. **Ejecución automática de lo establecido. Aunque alguien debe iniciarla.**
4. **Transacciones transparentes y seguras**
5. **Descentralización**
6. **Almacenamiento permanente**
7. **Integridad de datos**
8. **Acceso irrestricto**
9. **Touring completos**

CURSO BLOCKCHAIN

Casos de uso

Almacenamiento de registros

Actividades comerciales

Cadenas de suministro

Hipotecas

Mercado inmobiliario

Contratos de trabajo

Protección de copyright

Servicios de salud

Procesos electorales

Reclamaciones a aseguradoras

Canal de pagos

Tokenización de Activos

Contrato: Este Contrato de Token de Tenencia es para confirmar que la posesión de este Token es para representar el 100% de acciones de una LLC. Solo se emitirán 100 tokens y todos los derechos, beneficios y responsabilidades serán igualmente repartidos entre los poseedores de los tokens.

Token ERC20: https://github.com/DigiCris/EasyERC20/blob/main/ERC20.sol

Votaciones

- Snapshot
- DAOs
- Agora

Algunas elecciones ya hechas utilizando blockchain:

https://cointelegraph.com/public/index.php/news/blockchain-and-elections-the-japanese-swiss-and-american-experience/amp

https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/

https://es.cointelegraph.com/news/blockchain-technology-used-in-ecuadors-national-electoral-process

CURSO BLOCKCHAIN

Bibliografía

Mastering Ethereum, Andreas Antonopoulos

https://cointelegraph.com/public/index.php/news/blockchain-and-elections-the-japanese-swiss-and-american-experience/amp

https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/

https://es.cointelegraph.com/news/blockchain-technology-used-in-ecuadors-national-electoral-process

https://www.youtube.com/watch?v=KqGz3W05trg

https://eips.ethereum.org/EIPS/eip-20

https://github.com/SecurityTokenStandard/EIP-Spec/blob/master/eip/eip-1400.md

https://soliditylang.org/

Resumen

1) **Smart Contract:** Programa determinista que sirve para correr cláusulas predeterminadas ante un flujo establecido que no puede ser alterado. Su proceso es transparente e incensurable. Sus usos pueden ser amplios pero hay que evaluar muy bien si tiene sentido en cada caso ya que su ejecución implica dinero.
2) **WEB=** tenemos 3 etapas divisibles de los ciclos web, la 1, 2 y 3. La uno era estático de solo lectura, en la 2 existe interacción y dominan las grandes plataformas, en la 3 predomina lo descentralizado y cada uno es dueño de su contenido e información.
3) **Oráculos**: Conectan la blockchain con el mundo exterior ya que por si sola no puede. Estos comenzaron siendo centralizados pero ahora existen descentralizados como chainlink.
4) **DAO**: Organismos de gobernanza descentralizados. Pueden usar snapshot para sus votaciones y smart contracts para que sigan los casos de uso que la comunidad haya escogido sin que nadie pueda alterar su curso de acción.
5) **Agora**: blockchain especializada en sistemas electorales. El principal problema de esto será lograr la identidad electrónica de los ciudadanos.

Consultas

¿?

Reto

https://cursoblockchain.com.ar/

Actividad

a) Sin necesidad de programarlo. Plantear un caso de uso de un smart contract y diseñar el flujo que este debería seguir.
b) Por qué usaría un smart contract para eso y no un sistema de programación convencional como los ya existentes en una página web o un programa de escritorio?