

Módulo 3

Parte 3: Teoría Blockchain

Teoría Blockchain (40m)

1. **Blockchain:** Nodos, Sistema distribuido, transacción, mempool, bloque, minado, doble gasto, comunicación p2p, consenso, Ataque 51%, generales bizantinos, Merkle tree, inmutabilidad, Marco financiero para blockchain, Valor del btc. (1hs 45')
2. **Tipos de blockchain** (5')
3. **Wallets:** Aplicación, cuentas (clave privada, pública y address), Firma criptográfica asimétrica, Verificación, Metamask. Custodial vs Non Custodial (Responsabilidades), Frías vs Calientes. (30')
4. **Explorador de bloques** (10' práctico)
5. **Valor de otras criptos:** Filecoin, btt, LanguageNearYou (10')
6. **Inversión:** CEX (Binance) vs DEX (Pancakeswap), Valor tecnológico vs especulativo, HODL, TRADE, BID, ASK, spread, resistencia, soporte. Stake (pool+ PoS), Farm + protocolo de liquidez, apalancamiento, flash loan, p2p. (40')

Blockchain

Inversiones

Exchanges

- **intercambios** de token y criptomonedas.
- **CEX**
- **DEX**
- **Híbridos**

Nota: Las diferentes blockchains no pueden comunicarse entre sí por lo que existen puentes. Un CEX además de exchange actúa como puente.

CEX

- **Exchanges custodios**
- **NYK NYC**
- Únicamente te proveen la **dirección** para ingreso de dinero.
- Los **swaps** son realizados **Offchain**.
- Ejemplos: Binance, Buda, Cryptomkt, Buen Bit, Lemon Cash.

DEX

- El Usuario es el dueño de sus claves privadas
- La **interacción** es mediante **smart contracts**.
- Debemos darles permisos para que transfieran nuestros tokens.
(**transfer_from => Habilitar token**)
- **Nunca mandamos la clave privada**, sino que les **mandamos la operación firmada**.
- Ejemplos: Uniswap, Pancakeswap, QuickSwap.

Características CEX

Ventajas

- Cuentas custodias
- Multi Blockchain
- Permite efectivo
- KYC y AML
- Swap sin fee
- Extracción por sobre el gas.

Desventajas

- Hackeos de claves privadas.
- Wash trading.
- Algunos tienen seguro ante hackeos, otros no.
- Bash extractions.
- Fácilmente regulados.

Características DEX

Ventajas

- No tienen tus claves privadas
- Solo intra blockchain.
- No reciben efectivo.
- No necesitas KYC ni AML.
- Interactúas con smart contract y no con una empresa.
- Pagas gas por los swaps

Desventajas

- No pueden hackear al exchange
- Si pueden explotar smart contracts
- Ingeniería social latente
- El gobierno no puede regularlos
- Bridges para multichains.
- Farms, pools y reparten ganancias.

Pools y Farms

- Los **Pools** usados para **staking**. Los DEX comparten sus ganancias.
- Los **Farms** usados para **aportar liquidez**. (vender sin necesidad de una contraparte) en oposición a la compraventa P2P (peer to peer). El DEX te comparte las ganancias de los fees que cobran.

Farms, Automated Market Maker(AMM) e Impermanent Loss

AMM: Algoritmo que nos provee la **cotización entre 2 activos** en un DEX. Por ejemplo:

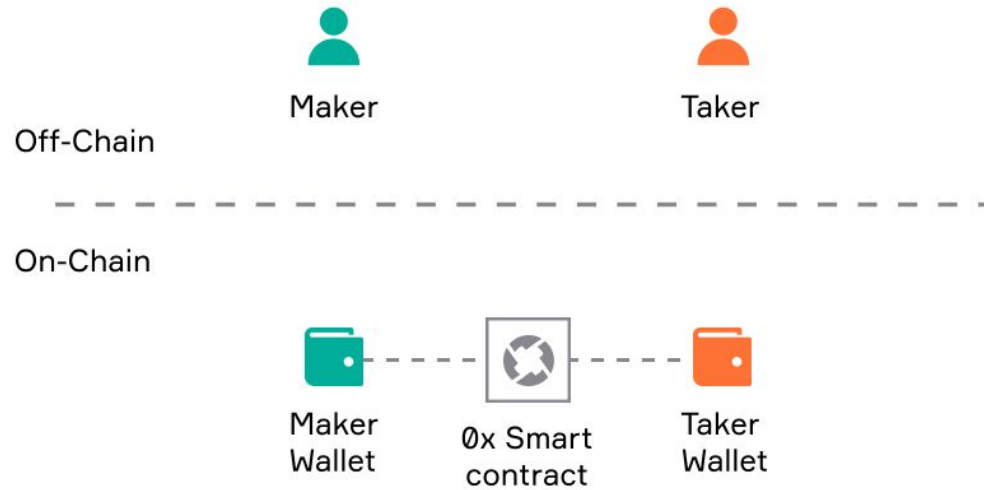
- 1) $33K \text{ USDT} / 33M \text{ Cake} = 0.001 \text{ USDT por cada Token}$
- 2) En el farm yo tengo $\Rightarrow 3.3 \text{ USDT} + 3300 \text{ Cake} \Rightarrow 0.01\%$ del farm
- 3) Alguien compra $1M \text{ Cake} \Rightarrow 1000 \text{ USDT}$
- 4) Ahora el pool tendrá $\Rightarrow 34K \text{ USDT} / 32M \text{ Cake} = 0.0010625 \text{ USDT por cada Cake}$
- 5) Con el Fee del 1% , el comprador en vez de 1000USDT habra pagado 1010USDT .
- 6) Los 10USDT de Fee se reparten el 50% para el DEX, 50% para el farm.
- 7) Yo tenía 0.01% del farm, por lo que gané $(5 \text{ USDT} \times 0,01\%) \Rightarrow 0.0005\text{USDT}$
- 8) En el farm ahora tendré $= 3.4\text{USDT} + 3200 \text{ Cake}$.

Impermanente loss= Si no hubiera puesto en el farm, tendría 3300 CAKE y 3.3USDT (6.80625 USD). Pero acumulé más del token cuyo precio bajo más (ahora tengo 6.8USDT)

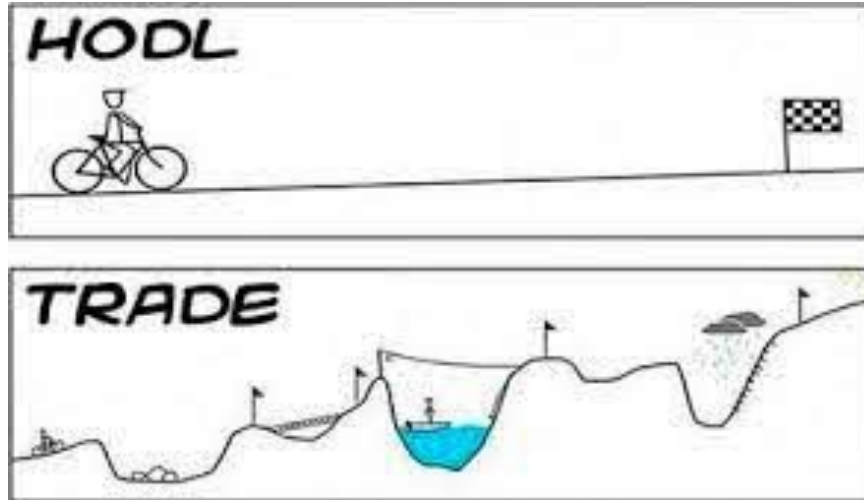
Peligro de los Farms, Pools y swaps en DEX

- Vulnerabilidades en smart contracts. Por este hecho las **Auditorías** de los contratos son muy importante. (**Reentrancy**)
- **front running**. Lectura del mempool para conocer el futuro y actual en consecuencia, ganandole de mano a ciertas transacciones.

Exchanges Híbridos



Hodl vs. Trade



BID, ASK y Spread

BID

The price a buyer
is willing to pay
for an asset

Order book			
	Bid	Ask	
20.04	18 717.28	18 727.15	2.28
2.65	18 715.41	18 729.02	5.2
17.75	18 714.91	18 730.89	12.65
0.24	18 711.91	18 732.77	25.32
10	18 706.42	18 734.64	48.9
6	18 705.92	18 735.14	12
8.28	18 704.92	18 735.64	8.04
16	18 703.92	18 743.13	9.92
9	18 702.92	18 745.01	6.75
8.96	18 701.42	18 745.51	14

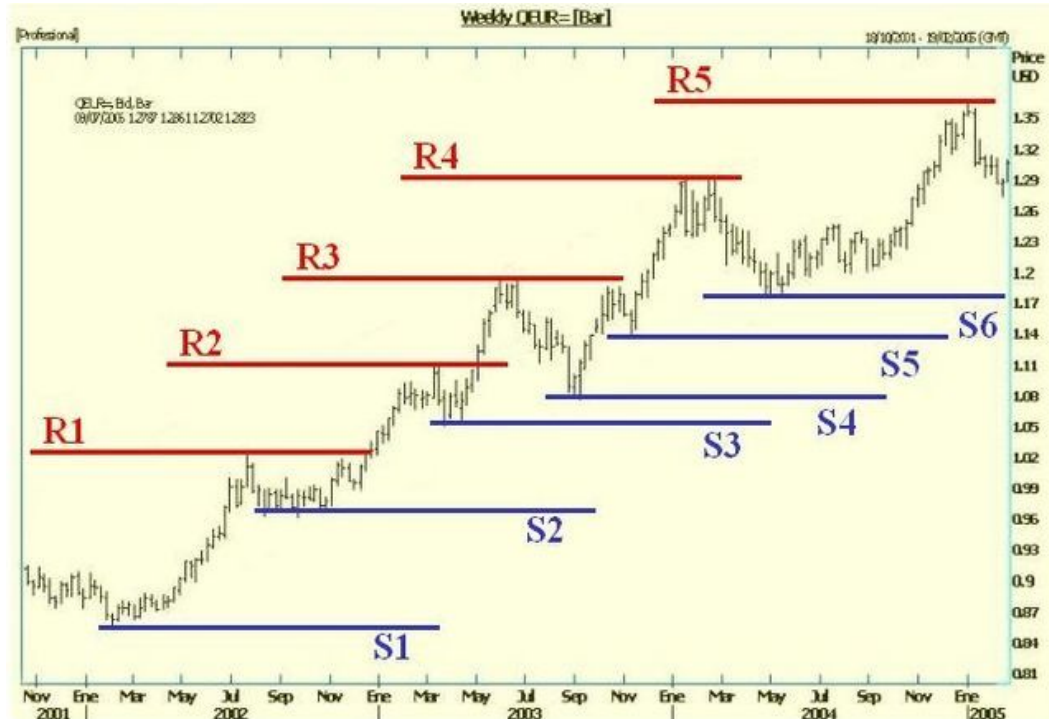
ASK

The price a buyer
is willing to pay
for an asset

SPREAD

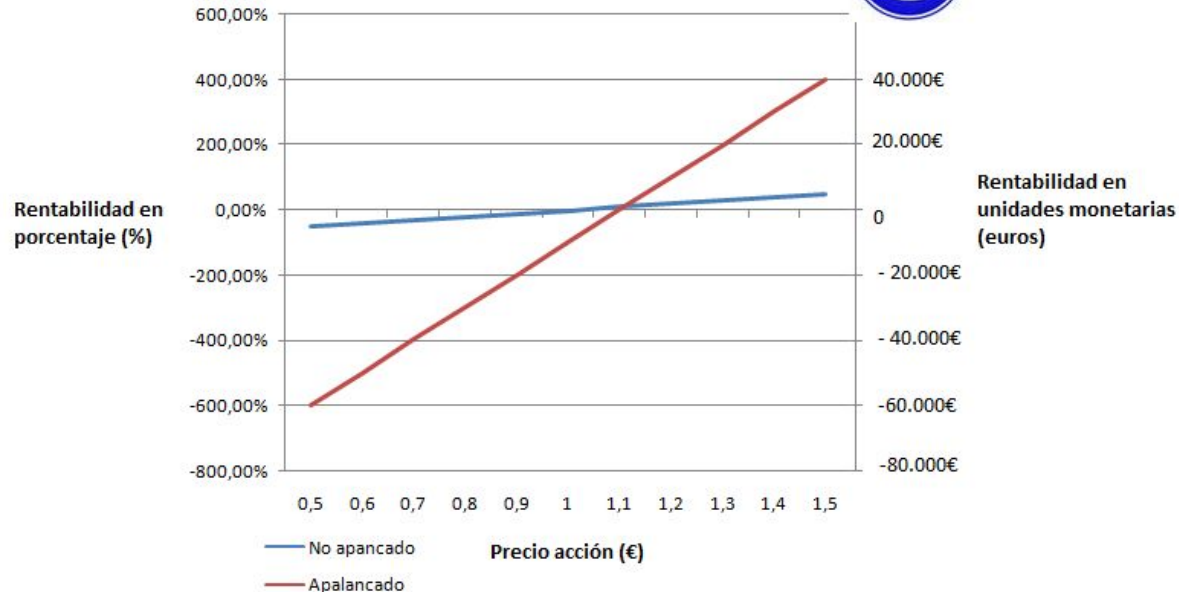
The difference between
the **BID** and **ASK** prices

Resistencias y Soportes



Apalancamiento

Ejemplo de apalancamiento financiero



Arbitraje

coinmonitor.info

FINEX USD 28.610,00 BITSTAMP USD 28.600,00 KRAKEN USD 28.588,90 COINBASE USD 28.556,02 OKCOM

coinMonitor Argentina OFFLINE 24hs visitas 3.273 365d -24.87% 01-05-23 | 00:29

Comprar				Vender			
01	Let'sBit	BTC 12.000.321,04 USDC 421,00	Bitstamp -4,15% Dolar 420,52	01	Fiwind	BTC 12.735.619,26 USDT 446,00	Bitstamp -5,05% Dolar 445,30
02	ArgenBTC	BTC 12.894.992,00 USDT 451,00	Bitstamp -3,86% Dolar 450,87	02	Bitso	BTC 12.722.454,50 DAI 444,29	Bitstamp -5,15% Dolar 444,84
03	TiendaCrypto	BTC 12.998.330,80 USDT 455,00	Bitstamp -3,09% Dolar 454,49	03	CryptoMKT	BTC 12.685.412,84 USDT 442,55	Bitstamp -5,43% Dolar 443,55
04	CryptoMKT	BTC 13.030.088,75 USDT 458,85	Bitstamp -2,86% Dolar 455,60	04	Cajeros Athena	BTC 12.624.974,42	Bitstamp -5,88% Dolar 441,43
05	Lemon	BTC 13.048.615,20 USDT 456,52	Bitstamp -2,72% Dolar 456,25	05	belo.app	BTC 12.613.826,40 USDT 446,00	Bitstamp -5,96% Dolar 441,04
06	Decrypto	BTC 13.049.094,00 USDT 456,59	Bitstamp -2,72% Dolar 456,26	06	buenbit	BTC 12.594.400,00 DAI 440,60	Bitstamp -6,11% Dolar 440,36
07	belo.app	BTC 13.070.671,20 USDT 453,00	Bitstamp -2,56% Dolar 457,02	07	ArgenBTC	BTC 12.554.961,00 USDT 439,00	Bitstamp -6,40% Dolar 438,98
08	buenbit	BTC 13.098.200,00 DAI 458,20	Bitstamp -2,35% Dolar 457,98	08	Lemon	BTC 12.485.100,80 USDT 436,81	Bitstamp -6,92% Dolar 436,54

Flashloan

- Pido dinero prestado.
- Lo uso para hacer lo que necesito (Arbitraje)
- Lo devuelvo con los intereses apropiados

Nota: Todo esto en una misma transacción. Si alguna de las partes no se ejecuta, se revierte y es como si nunca hubiera pasado. De esta forma el prestamo no necesita colateral ni garantías.

Bibliografía

Precios de bitcoin en multiples exchanges: <https://coinmonitor.info/>

Ethereum Yellowpaper, Gavin Wood: <https://www.cryptosaurio.com/ar/>

Binance: <https://www.binance.com/en>

Cryptomkt: <https://www.cryptomkt.com/es-ar/>

Buda: <https://www.buda.com/argentina>

Pancakeswap: <https://pancakeswap.finance/>

Resumen

- 1) **CEX:** exchange centralizado donde puedo comprar y vender criptomonedas y donde no soy custodio de mis claves privadas.
- 2) **DEX:** exchange descentralizados donde puedo comprar o vender tokens dentro de una misma blockchain pero no existe una empresa atrás como en un CEX sino que interactúo con smart contracts.
- 3) **Trade vs Hold:** Si intercambio para ganar por los cambios estoy haciendo trading, si compro para esperar que a largo plazo suba estoy haciendo HODL. Hodl es una deformación de la palabra inglesa Hold.
- 4) **Resistencia y soportes:** dificultad que presenta un activo para subir o bajar de un valor determinado.
- 5) **Arbitraje:** Comprar en un lado y vender en otro para obtener ganancias.
- 6) **Farms y Pools:** Lugar en donde pongo mis tokens para que sean usados por los contratos de los DEX y así recibir ganancias por contraprestación.
- 7) **Spread y Comisiones:** Spread es la diferencia entre valores de compra y venta mientras que las comisiones es lo que se paga por usar un servicio dado. Estas comisiones incluyen generalmente el gas por el uso de la blockchain en cuestión aunque en los CEX suele hacerse offchain.

Consultas

¿?

Reto

<https://cursoblockchain.com.ar/>

Enunciados

1. Crear un Farm del token creado en un DEX
2. Hacer un swap de un token usando un DEX
3. Orden limit en un DEX.
4. Uso de un bridge descentralizado
5. Agregar tokens a un Pool en un DEX.
6. Ver billeteras en un CEX
7. Cargar saldo en un CEX
8. Crear una orden limit entre 2 monedas de diferente blockchain (CEX)
9. Entender diferencia entre orden limit y market CEX
10. Retirar saldo de un CEX,