Jornada 2

WORKSHOP CRIPTOACTIVOS

CARTA FINANCIERA
IDEAS CONCRETAS

Contenidos

Segundo Día:
Key Take Aways

U4. Matriz de tokens criptográficos & Token Taxonomy
U5. DEX vs CEX + DEFI
U6. Privacidad

CARTA FINANCIERA
IDEAS CONCRETAS

4 Matriz de tokens criptográficos & Token Taxonomy

Tokens

Token	• Palabra de origen anglosajona y *poli-semántica*. • De manera generalizada, se entiende por token a **la representación de algo**
Tokens Digitales	• Los tokens digitales, son entonces representaciones digitales de algún elemento. • Si ese elemento tiene valor económico, es entonces un activo, en la medida que represente alguno o todos los derechos respecto de dicho elemento.
Tokens Criptográficos	• **SON DATOS REGISTRADOS EN UNA DLT/BC** • Pueden ser representaciones de bienes y derechos (¿*activos*? ---- ¿*always*?) programados y administrados por un Smart Contract y registrados en una DLT subyacente. • Son solamente accesibles por personas que poseen una Llave Privada asociada a una dirección de la red de Blockchain donde opera el Token.

Inside the Box

DIMENSIÓN DE ANALISIS	CARACTERIZACIÓN BINARIA
Perspectiva Técnica	Tokens de Protocolo vs Tokens de Aplicación
Perspectiva de los Derechos	Derechos de Propiedad vs Derechos de Acceso
Perspectiva de la Fungibilidad	Idénticos vs No Idénticos
Perspectiva de la Transferibilidad	Transferibles vs Intransferibles
Perspectiva de la Regulación	Fácil vs Difícil Clasificación y Regulación
Perspectiva de los Incentivos	Soportado en base a la validación de un comportamiento vs Respresentación de DDs
Perspectiva de la Oferta	Oferta Fija vs Oferta Ilimitada
Perspectiva del Flujo de los Tokens	Lineal vs Circular
Perspectiva de Vida Útil	Con fecha cierta de vencimiento vs Sin fecha de vencimiento
Perspectiva de Privacidad	Mas privacidad por Diseño vs Menos privacidad por Diseño
Perspectiva de Estabilidad	Con Mecanismo de Estabilidad vs Sin Mecanismo de Estabilidad

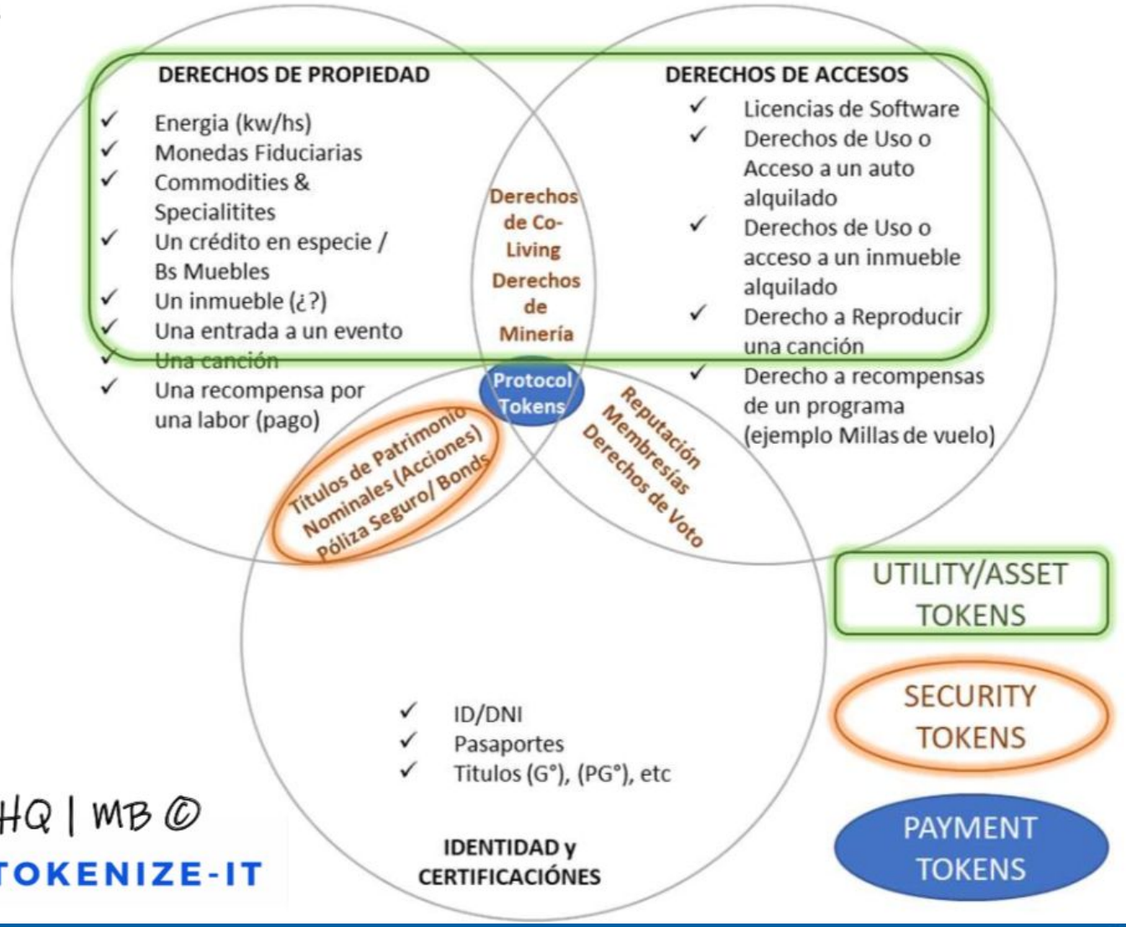
Inside the Box

TOKENS DE APLICACIÓN

Pueden representar cualquier derecho de propiedad, de acceso, de uso, de identidad o certificación. Pueden implicar simples funcionalidades hasta complejas dependiendo el espíritu que persigan.

TOKENS DE PROTOCOLO:

También llamados nativos, intrínsecos o incorporados, tienen un rol muy claro en las redes públicas: mantener segura la red de ataques actuando como incentivos para la validación de bloques (recompensa para los mineros), y para prevenir la sobrecarga de transacciones. Los tokens nativos de protocolo también pueden ser necesarios para pagar comisiones por transacción en una red y cumpliendo una finalidad de pago por diseño.



SHQ | MB ©

TOKENIZE-IT

Take a view from outside the Box…

Cryptographic Tokens

Cryptoassets

12.084
Publicly Listed

Non CryptoAssets

+1000 | *On going Projects*

Security Tokens	Utility Tokens	Assets Tokens	Payment Tokens	Identity	Certifications & Credentials	Policy Rights

Tokenized Securities

SEBA BANK

Security Tokens

Sygnum will sell 4,000 NFT shares of Picasso's Fillette au béret. Credits: Sygnum

Stable Payment Tokens

SUCOIN

PAX GOLD

Non Stable Payment Tokens

bitcoin

Polkadot.

Chainlink

Algorítmicos

DAI

Collateralized Tokens

tether

CBDC

Identity

OpenID.ee

ID Tokenizado en Estonia

Certifications & Credentials

The Learning Credential Network

Settlement, Clearing and Recording Cross Border Transactions.

r3.

Policy Rights

Ayuntamiento de ALCOBENDAS

Presupuesto Participativo y Representación Ciudadana Directa

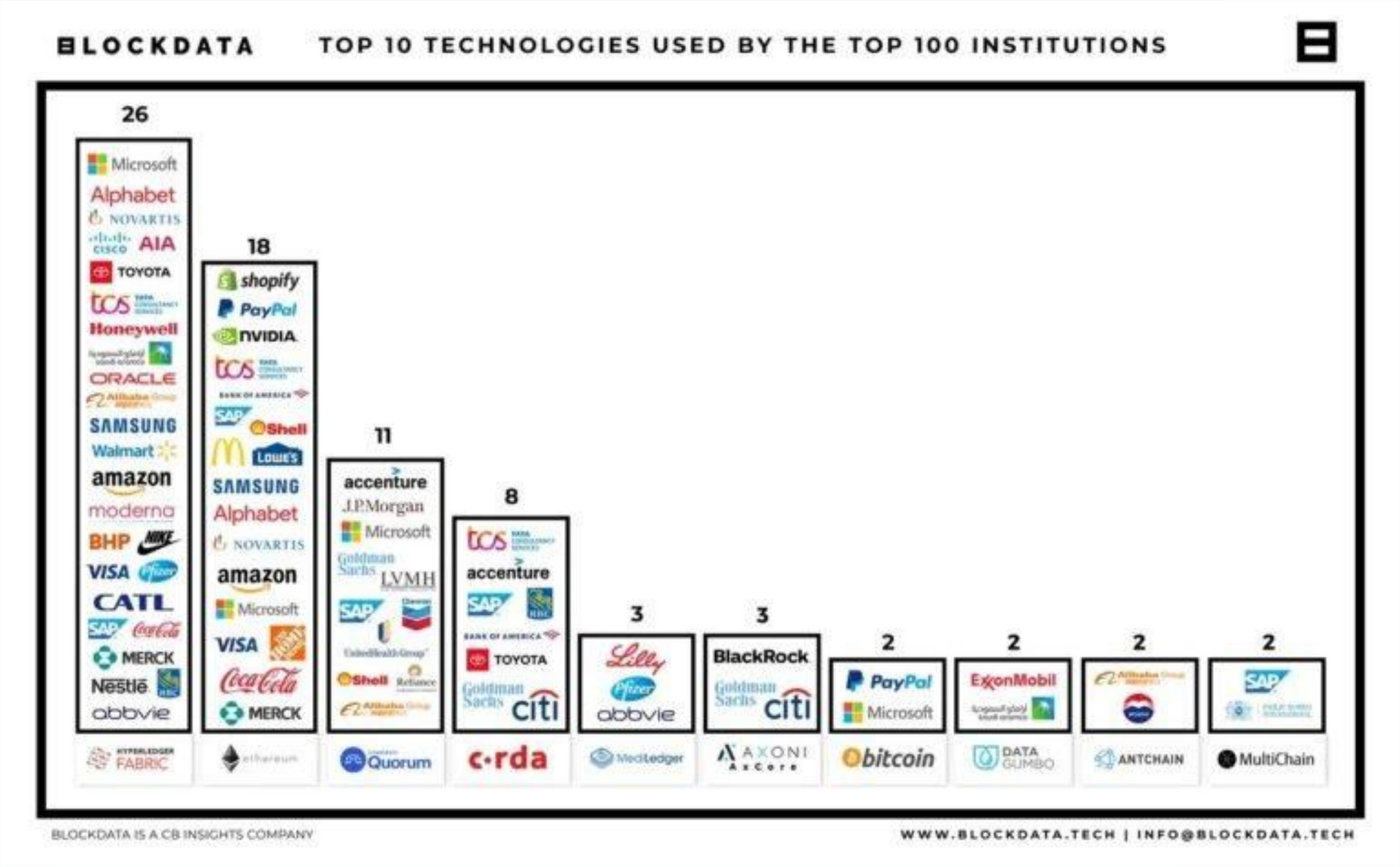
Pasaporte del Vehículo y Trazabilidad de la Cadena de Valor.

TOKENIZE-IT

SHQ | MB ©

Tokens Híbridos (CA)

Take a view from outside the Box…



Proceso de Creación

Tokens Criptográficos – Emisión y Proceso

SAFT
(Safe Agreement for Future Tokens)

Private Placement

- Iniciativa Privada de creación y colocación de Tokens*.
- Estos tokens como ya hemos visto pueden ser de diversa naturaleza, con el consecuente impacto/tratamiento tanto para emisor como adquiriente.
- Adquiriente, ¿siempre es un Inversor? , en caso de serlo, **¿debe ser "Calificado"?** (*Suitable*)

Publicly Listed

- Iniciativa privada de oferta publica y masiva de Tokens*
- El token ofertado puede crearse en (1) simultaneo con la oferta a realizar o (2) ya encontrarse creado previo a ser públicamente ofrecido
- El proceso implica listar el token en un "Exchange". Industria escasamente regulada y mucho perjuicio causado por ausencia de ciberseguridad.

Proceso de Creación

ITO

- Por su siglas refiere a “Initial Token Offering”
- El proceso implica una oferta “publica y masiva” de tokens criptográficos **cualquiera sea su naturaleza**
- Implica migrar a la WEB 3 (*back-end revolution*) un negocio, un bien o un servicio, tal que su impacto derrama no solo en la dinámica de sus finanzas sino también en las relaciones jurídicas subyacentes.
- **Impacto Critico**: **Eficiencia**

DON’T FORGET: *“Blockchains, cryptocurrencies, and related technologies — that is, crypto — will change the world, not through anarchy (as many people believe) but through sheer efficiency. They’ll have tremendous impact, but not in the way the creators intended.”* ***(1)***

ICO

- Por su siglas refiere a “Initial Coin Offering”
- El proceso implica una oferta “publica y masiva” de tokens criptográficos que se caracterizan como “Payment Tokens”
- Es el caso mas comúnmente observado en el período ya transcurrido de la joven historia de BC, dado que fue una de las metodologías de “fondeo” de la mayoría de las redes de BC creadas hasta la actualidad. (Ej. Ethereum, Bitcoin, Cardano, Polkadot, Chainlink).

Caracteres de la Moneda – Finalidad de la Moneda

STO

- Por sus siglas refiere a “Security Token Offering”.
- Se puede agregar que existe dos tipos posibles alusiones a este proceso: STO vs TSO. La diferencia alude a si el security es nativo o no de la red de Blockchain en la cual se está ofertando.
- Este proceso implica una “oferta publica y masiva” de tokens criptográficos que se caracterizan como “Security Tokens”.
- Es el proceso análogo a un IPO (Initial Public Offering) (u OPA, por sus siglas en castellano)

IEO –
Initial Exchange Token Offering

Proceso de Creación

¿Qué es IPO?

- Refiere al proceso a partir del cual una compañía abre el capital y deja de ser "privada". Implica generalmente la emisión de nuevas acciones las que se suscriben a través de un proceso de venta publica en mercados regulados a tales efectos (mercado de capital).
- El proceso permite a los inversores privados de la compañía, realizar la ganancia por la valorización de su empresa que se hace objetivo en el precio de corte y lanzamiento a mercado.

¿Para qué IPO?

- Las compañías siguen este tipo de decisiones para realizar la ganancia de los Accionistas y eventualmente para obtener fondeo. Es decir que puede perseguir dos fines disimiles: (1) objetivar el valor de la compañía en favor del inversor privado quien hace "cash in" de dicho "*value*" y/o (2) obtener fondeo vía la ampliación de capital, en este caso por suscripción y oferta publica.

¿Cuándo un IPO?

- Generalmente esto resulta oportuno al alcanzar la compañía la etapa de crecimiento maduro. Esto implica que la decisión dependerá no solo de la compañía, sino de cada industria, mercado y momento temporal.

Dato de Referencia. USA un IPO hoy tiene entidad para empresas valuadas por encima del *Billion Dólar (1.000 Millones).* Cantidad de IPO en USA últimos 12 meses = 192 / En Argentina hace mas de 30 meses que no hay IPO y los últimos 6 se realizaron entre 2015-2019 (Loma Negra, Corporación America Airports, Central Puerto, Grupo Supervielle, Laboratorios Richmond y Havanna Holding)

STO & TSO

SIMILITUDES

- Persigue idénticos propósitos al IPO.
- El activo subyacente del proceso de fondeo, es de igual naturaleza.
- Hay oferta publica de un instrumento cuyo valor depende del "*managerial effort*" (SEC and Howey Test: Inversión de Dinero, Empresa Común y Expectactiva de obentener beneficios en función de otros)

DIFERENCIAS

- No esta regulado en Argentina de manera directa……. ¿? Analogía.
- No requiere de un agente colocador. Si requiere de validar protocolos y scripts en el Exchange donde se listará.
- A la fecha, existen pocos países que han regulado cuestiones de validación preliminar de Inversores como Calificados.

Proceso de Creación: IEOs, the rising Star

→ Un Exchange con mucho prestigio, usa su goodwill para ofrecer a sus clientes un token criptográfico propio, que permite (1) participar en el negocio del Exchange propiamente dicho, o bien tener preferencia para (2) fondear algún proyecto a ser listado en el Exchange, permutando los IEOs por ICOs/STOs del proyecto

→ El Exchange actúa “como un” underwriter/colocador/estructurador, según el caso

→ El primer IEO fue en 2017 de la mano de Binance

→ PROs: (i) El Exchange se ocupa del protocolo de KYC-AML-CTF, ya que son sus clientes los eventuales compradores del token a ofrecer; y (ii) permite a las empresas que buscan fondeo apuntar/llegar a la cartera de clientes del Exchange (más profunda, conocida) con menores riesgos comparado a la emisión de un ICO o un STO de manera solitaria (stand-alone emission)

Proceso de Creación: IEOs, the rising Star

- **Until early 2019**, **IEOs** did not play any **significant role** in global crypto market / ecosystem (after first **IEOs** already took place in 2017 - e.g., Bread, Gifto)
- **IEOs experienced strong momentum** (in terms of # completed offerings and aggregate funding volume) in **beginning of 2019**; **Bitfinex** with **largest IEO** (USD 1.0 bn) in **May 2019**
- **Low level** of **completed token offerings** in **second half of 2019**; nonetheless, **IEOs** with **relatively strong / increasing adoption**, indicating a **progressive establishment** of this **crowdfunding instrument** in **Blockchain sphere**
- Looking ahead, the **development / institutionalization** of the **underlying infrastructure** (i.e. crypto exchanges) and the **clarification** of the **regulatory landscape** of associated **global crypto offerings** will further drive **market traction of IEOs**

strategy&

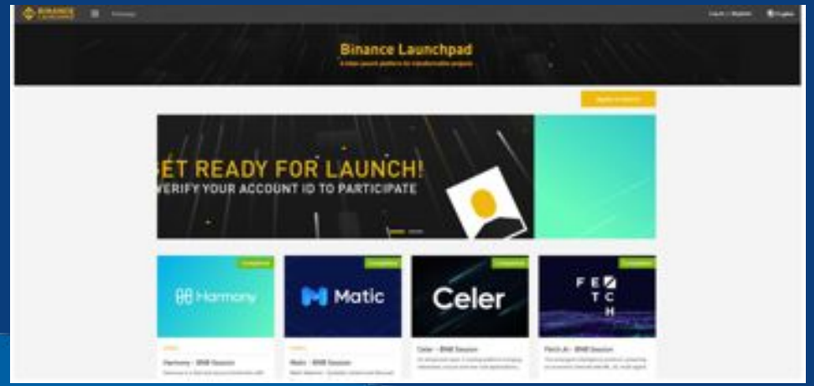
pwc

OK Jumpstart by OKEx is an excellent platform for quality blockchain projects. It offers a high-quality liquid market, top-notch exposure, and token listing opportunity in one of the most popular exchanges in the world.

OKEx introduced a subscription plus allotment approach to avoid oversubscription. This way, there's a brief 30-minute subscription window before an IEO, which closes if the max limit is reached. Then, the allotment part follows: an investor must hold a minimum of 500 OKB (OKEx exchange token) for seven days or at least 3,500 OKB at the snapshot time before the token sale. The allotment amount is based on your OKB holdings. The more OKB user has, the more significant the allotment amount one gets. OKB is the only accepted token on OK Jumpstart IEO platform.

Binance Launchpad is the pioneering IEO platform which launched in 2017 just to become mainstream in 2019. It had many successful IEOs, including Matic Network (MATIC), BitTorrent (BTT), Celer Network (CELR), Fetch AI (FET), Bread (BRD), and others. At pixel time, the average ROI for Binance IEO investors is nearly 580%.

Binance Launchpad is arguably the best token launch platform on the market. It is backed by one of the top exchange's in the world and is led by a class act Changpeng Zhao. The launchpad is powered by leading technology (capable of processing over 1,400,00 orders per second) and high-level partnerships, which bring an abundance of investors to every token sale. Hence, liquidity is rarely a problem with Binance.



Proceso de Creación en distintos países

España

Suiza

USA

Argentina

Proceso de Creación

España

España

Comisión Nacional del Mercado de Valores (CNMV) y el Banco de España (BCE), los reguladores españoles, quizás con mayor precisión que nuestra CNV, distinguieron entre la emisión propiamente dicha de criptomonedas (Initial Coin Offerings –ICOs–) y la emisión de "derechos de diversa naturaleza" denominados tokens o vales.

Además distinguen entre:

Security Token: participación en las ganancias del emisor

Utility Token: derecho a un bien o servicio futuro

ONDA SERRANO

Proceso de Creación

Suiza

Suiza

FINMA distingue entre:

Asset Token: representa un activo físico o bien la participación en flujos de fondo, instrumentos de renta fija, o en general, situaciones similares a un activo financiero que se negocia en mercados.

Utility Token: derecho a un producto o servicio digital

Payment Token: sinónimo de cryptomoneda, es decir, sirve para realizar pagos.

UK: *"same page"*

Monday, 1 February, 2021

SEBA Bank is issuing its Series B equity as security tokens

- With the adoption of the DLT law today, SEBA Bank is issuing its Series B Participation Certificates as tokenized equity securities on the blockchain
- SEBA Bank's Equity Tokens will be issued and held within SEBA Bank's banking-grade digital custody in a FINMA regulated environment
- SEBA Bank's Equity Tokens based on ERC20 Ethereum protocol are fully engineered to allow seamless connectivity for trading and liquidity on future internationally recognised digital liquidity venues

Proceso de Creación

Suiza

finma

Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Press release

Date:
29 September 2021

Embargo:
-

Contact:
Tobias Lux, Media Spokesperson
Tel. +41 (0)31 327 91 71
tobias.lux@finma.ch

Approval of first Swiss crypto fund

The Swiss Financial Market Supervisory Authority FINMA has approved the first crypto fund according to Swiss law. The fund, which is restricted to qualified investors, invests primarily in so-called cryptoassets.

For the first time, FINMA has approved a Swiss fund that invests primarily in cryptoassets, that is to say in assets based on the blockchain or distributed ledger technology. The fund concerned goes by the name of the "Crypto Market Index Fund", an investment fund according to Swiss law belonging to the category "other funds for alternative investments" with particular risks. Distribution of this fund is restricted to qualified investors.

Consideration of the particular risks

In order to facilitate serious innovation, FINMA applies the existing provisions of financial market laws in a consistently technology-neutral way, i.e. in keeping with the "same risks, same rules" principle. In doing so, it makes sure that new technologies are not being used to circumvent the existing rules and that the protective goals of financial market legislation are preserved. Since cryptoassets involve particular risks, FINMA also tied the approval to specific requirements in the present case. For instance, the fund may only invest in established cryptoassets with a sufficiently large trading volume. Furthermore, the investments must be made through established counterparties and platforms that are based in a member country of the Financial Action Task Force (FATF) and are subject to corresponding anti-money laundering regulations. Finally, there are specific requirements with regard to risk management and reporting for the institutions involved in the management and custody.

→ FINMA (29/09/2021 / HOY) aprobó el primer fondo con Oferta Publica (analogico | *"Legacy System"*) con inversiones en CRYPTOASSETS

→ Caracterizan el fondo como "Other Funds for **ALTERNATIVE INVESTMENTS"**

Proceso de Creación

USA

USA

Cuál es la importancia de diferenciar tokens de securities? Aplicación de la ley de valores negociables americana.

La SEC dijo que un token no será un security regulado si sus adquirentes no esperan razonablemente que una persona o grupo gestor preste servicios de gestión empresarial.

Howey Test: standard fijado por la Corte americana en 1946 para determinar si un contrato es de inversión. ¿los tokens se adquieren para obtener un beneficio de la actividad de un tercero o si dichos tokens darán derecho a adquirir un bien o servicio?

SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering

FOR IMMEDIATE RELEASE
2020-338

Washington D.C., Dec. 22, 2020 — The Securities and Exchange Commission announced today that it has filed an action against Ripple Labs Inc. and two of its executives, who are also significant security holders, alleging that they raised over $1.3 billion through an unregistered, ongoing digital asset securities offering.

Proceso de Creación

Argentina

Argentina

AUSENCIA DE REGULACIÓN. Algunas expresiones aisladas de CNV

DEFINIO blockchain como un “inventario de existencia electrónico no modificable” de todo el sistema de transacciones que es mantenido por varios partícipes en una red de computadoras, que almacena de forma creciente datos ordenados en el tiempo y sin posibilidad de modificación ni revisión.

La CNV se refirió también a la tokenización afirmando que comprende desde la emisión de monedas virtuales, hasta un token digital que puede representar una acción en una empresa, un bono prepago para servicios futuros o, en algunos casos, no ofrecer ningún valor discernible.

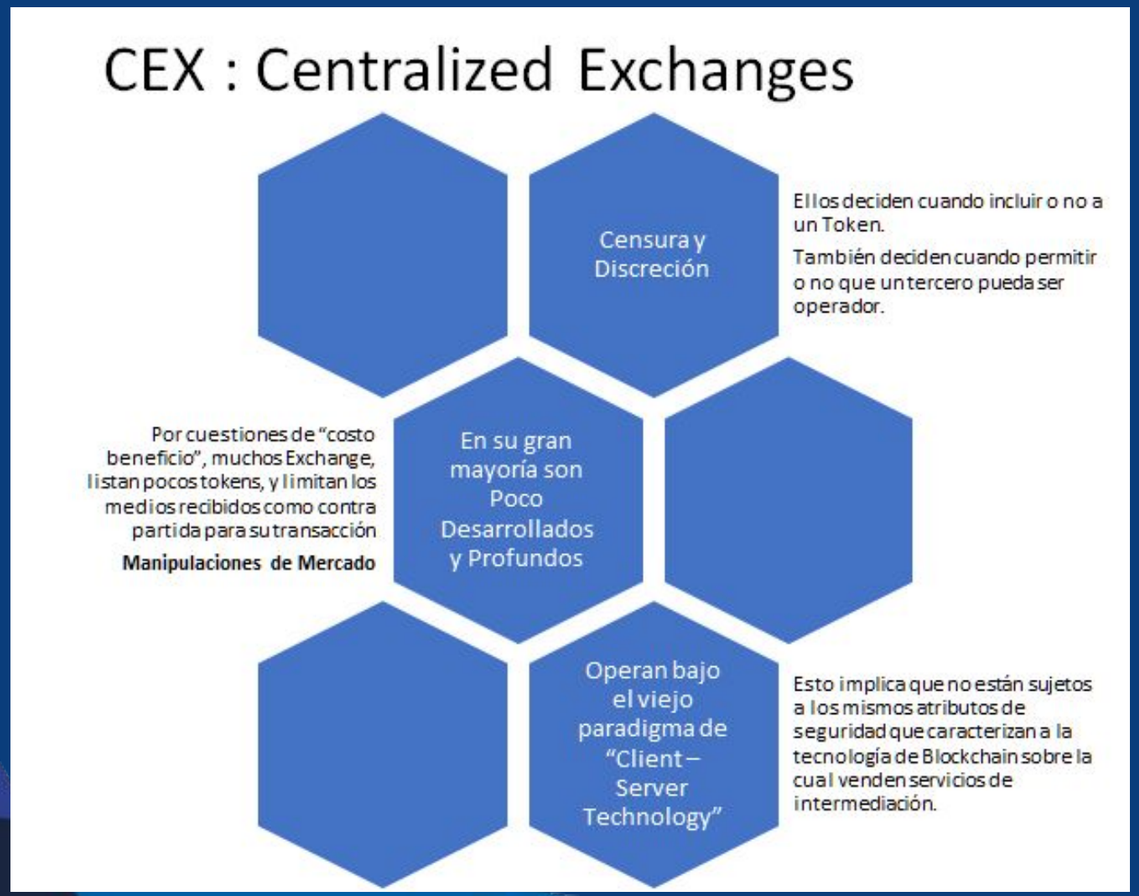
5 DEX vs CEX + DEFI

Exchange: Centralized Exchange (CEX) vs Decentralized Exchange (DEX)

La paradoja de este nuevo paradigma descentralizado …… CEX!!!

Exchange: Centralized Exchange (CEX) vs Decentralized Exchange (DEX)

La paradoja de este nuevo paradigma descentralizado ..... CEX!!!



Un caso Testigo

"Mt. Gox," which was the largest Bitcoin exchange at the time, suspended trading and filed for bankruptcy in 2014. Due to mismanagement, approximately 850,000 BTC went missing, most likely stolen. (Current Mkt Value: 32 B USD)

Fecha de Actualización	9/28/2021			
Tipo	#Cantidad	Market Cap (USD)	Total Volume (Linear) | (USD)	Relative Weight
CEX	312	$ 1,726,875,836,646	$ 142,637,972,224	91%
DEX	102	$ 173,021,096,939	$ 14,291,345,038	9%
Total	**414**	**$1,899,896,933,585**	**$ 156,929,317,262**	**100%**

Fecha de Actualización	5/19/2021			
Tipo	#Cantidad	Market Cap (USD)	Total Volume (Linear) | (USD)	Relative Weight
CEX	312	$ 1,741,405,791,644	$ 597,065,626,105	98%
DEX	64	$ 34,970,239,117	$ 11,990,041,502	2%
Total	**376**	**$1,776,376,030,761**	**$ 609,055,667,607**	**100%**

Los DEX aumentaron su volumen transaccional (en USD) un 19% en 4 meses!!!!! ..... En un contexto donde a la fecha se ralentizó la magnitud de operaciones diarias que se concentran en los CEX!

Exchange: Centralized Exchange (CEX) vs Decentralized Exchange (DEX)

La paradoja de este nuevo paradigma descentralizado ..... CEX!!!

Top 20 CEX	#Tokens	#Markets	Volume (24hsT)
Binance	386	1432	$ 18,350,600,754
Mandala Exchange	279	521	$ 16,206,481,926
BKEX	465	495	$ 6,015,127,230
OKEx	288	650	$ 5,542,982,023
ZG.com	42	46	$ 4,288,624,821
Huobi Global	356	1069	$ 4,047,158,275
ZT	566	592	$ 3,719,176,435
Upbit	147	221	$ 3,424,365,840
BiONE	173	189	$ 3,300,576,265
HitBTC	511	1071	$ 3,157,836,727
Bitcoin.com Exchange	120	252	$ 3,071,415,867
Coinbase Exchange	104	312	$ 2,898,029,337
Crypto.com Exchange	118	240	$ 2,895,288,876
Changelly PRO	41	103	$ 2,775,456,088
Ecxx	8	15	$ 2,630,954,276
WOO Network	60	59	$ 2,593,477,894
Hotcoin Global	231	251	$ 2,499,382,829
IndoEx	72	149	$ 2,116,936,738
FTX	261	522	$ 2,059,358,539
TOKENCAN	45	45	$ 2,001,134,641
20			**$ 93,594,365,381**
6%			66%

Top 20 DEX	#Tokens	Types	Volume (24hsT)
dYdX	∞	Orderbook	$ 9,807,724,328
Uniswap (V3)	∞	**Swap**	**$ 1,094,975,868**
PancakeSwap (V2)	∞	Swap	$ 717,631,616
1inch Liquidity Protocol	∞	**0**	**$ 457,218,159**
Uniswap (V2)	∞	**Swap**	**$ 286,271,896**
Sushiswap	∞	**Swap**	**$ 285,121,430**
Honeyswap	∞	Swap	$ 210,549,846
MDEX	∞	Swap	$ 179,081,727
Raydium	∞	Swap	$ 165,193,726
1inch Exchange	∞	**Aggregator**	**$ 101,887,948**
Perpetual Protocol	∞	0	$ 96,258,783
KLAYswap	∞	Swap	$ 88,833,082
Serum DEX	∞	Orderbook	$ 76,410,398
QuickSwap	∞	Swap	$ 71,687,211
Biswap	∞	0	$ 64,631,084
TraderJoe	∞	0	$ 59,191,199
BabySwap	∞	0	$ 43,673,509
DODO	∞	Swap	$ 43,487,924
Curve Finance	∞	Swap	$ 38,506,092
SpookySwap	∞	0	$ 38,071,118
20			**$ 13,926,406,944**
20%			97%

f: https://coinmarketcap.com/rankings/exchanges/dex/

Ranking	CEX	Score	Volume (24hsT)	Avg. Liquidity	#Weekly Visits	#Markets	#Tokens	#FIAT Supported
253	Ripio	0.4	$ 122,176.00	--	11,031	9	7	--
294	Bitex.la	0.7	-	18	2,909	1	2	USD

CEX mas relevantes de Argentina ....

Exchange: Centralized Exchange (CEX) vs Decentralized Exchange (DEX)

- **Binance:** Cayman Islands & Seychelles
- **Mandala Exchange:** Malta
- **OKEx:** Seychelles
- **ZG.com:** Islas Caymán
- **Huobi Global:** Seychelles & Hong Kong
- **ZT:** Seychelles
- **Upbit:** Corea del Sur
- **BiONE:** Singapur
- **HitBTC:** Hong Kong
- **Bitcoin.com Exchange:** Cayman
- **Coinbase Exchange:** San Francisco
- **Crypto.com Exchange:** Hong Kong
- **Changelly PRO:** República Checa
- **Ecxx:** Hong Kong
- **WOO Network:** Singapur
- **Hotcoin Global:** Australia
- **IndoEx:** NY & Canada
- **FTX:** San Fracisco
- **TOKENCAN:** Hong Kong

Ranking	CEX	Score	Volume (24hsT)	vg. Liquidit	#Weekly Visits	#Markets	#Tokens	#FIAT Supported
1	Binance	9.9	18,350,600,754.00	668	28,351,152.00	1432	386	AED, ARS, AUD
2	Coinbase Exchange	8.9	2,898,029,337.00	548	2,901,407.00	312	104	USD, EUR, GBP
3	FTX	8.7	2,059,358,539.00	562	3,866,226.00	522	261	USD, EUR, GBP
4	KuCoin	8.5	1,376,717,397.00	467	1,746,860.00	924	468	USD
5	Huobi Global	8.4	4,047,158,275.00	600	962,260.00	1069	356	ALL, AUD, BRL
6	Kraken	8.3	744,937,374.00	564	2,080,996.00	347	88	USD, EUR, GBP
7	Gate.io	8.2	990,858,543.00	369	2,225,432.00	1602	919	KRW, EUR
9	Bithumb	8.1	1,073,616,193.00	276	563,851.00	255	184	KRW
8	Bitfinex	8.1	753,485,544.00	502	846,579.00	319	154	USD, EUR, GBP
10	Binance.US	8	522,702,482.00	345	666,807.00	120	62	USD

Exchange: Centralized Exchange (CEX) vs Decentralized Exchange (DEX)

Atomic Swaps, DEX & P2P Lending/Borrowing

Dinámicas Inherentes a los DEX – Atomic Swaps, Agreggator and Orderbook

Atomic Swaps

- Los Atomic Swaps permiten los intercambios comerciales P2P entre redes diferentes y pueden ser directamente ejecutados entre redes de blockchain separadas, de billetera la billetera, sin necesidad de un tercero intermediario de confianza como en el caso de los mercados.
- Usan un tipo especial de smart contract llamado "hash time-locked contract" (HTLC) para asegurar la transacción del token, haciendo segura para ambas partes que el intercambio del token cumpla con todos los requisitos. HTLCs es una solución similar a la de los canales estatales que se ocupan de la liquidación de pagos "fuera de la cadena" (off-chain) a través de un contrato inteligente. Los usuarios mantienen bajo control la totalidad de sus llaves privadas, y sus tokens, cuando realizan este tipo de intercambios

Agreggator

- Los agregadores son protocolos financieros que permiten a los traders acceder a una amplia gama de grupos de negociación a través de un solo panel. Luego, a través de un SC (el agregador de liquidez") encuentra el mejor precio posible en todas las plataformas disponibles para que usted ejecute su orden.
- Ejemplos de DEX con este tipo de 1inch Exchange
- Única solución que a la fecha resuelve el problema de coincidencia de deseos. Contra: Proceso mas lento.

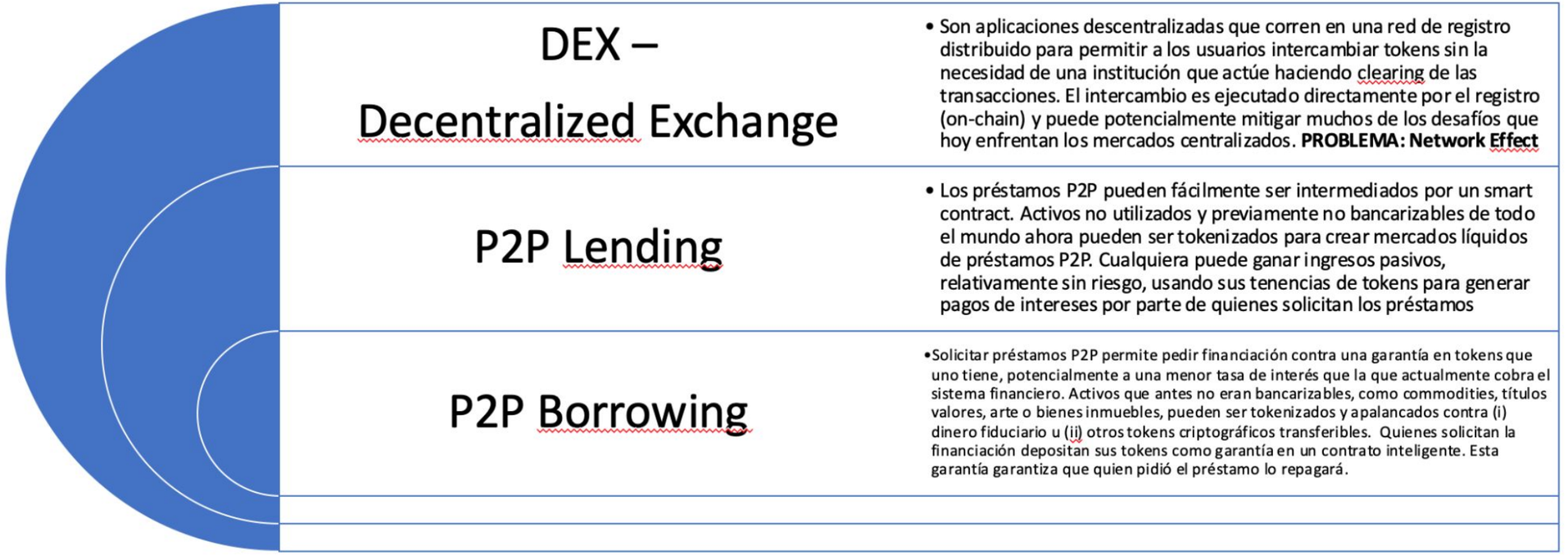
Orderbook

- Los traders ponen ordenes de compra y de venta las cuales se van agregando "on-chain" hasta matchear en orden de preferencia "precio-tiempo".
- Es empleada tanto por CEX como por DEX. La diferencia radica en si las ordenes se incorporan de manera directa ON-CHAIN (DEX) vs OFF-CHAIN en los (CEX) para luego cargarse a la Red BC.

Exchange: Centralized Exchange (CEX) vs Decentralized Exchange (DEX)

Atomic Swaps, DEX & P2P Lending/Borrowing

DEX – P2P Lending / Borrowing.



Trading Tokens & DeFi

DeFi - Concepto e Impacto: ¿Hacia una Economía de Trueque?

Implica cualquier aplicación Financiera que cumple los siguientes caracteres:	Por definición es descentralizada. Esto implica la inexistencia de intermediarios.
	Están construidas sobre la base de tecnología *"DLT"*, enfatizando la seguridad transaccional.
	Se corresponden con servicios de pago, de recaudación y de ofrecimiento de crédito y toma de prestamos.

Estas aplicaciones basadas en los servicios financieros tradicionales, tienen la potencialidad para eliminar ineficiencias de mercado.

Trading Tokens & DeFi

DeFi - Concepto e Impacto: ¿Hacia una Economía de Trueque?

→ Son *servicios financieros de-centralizados* que se brindan a través de DLTs: la mayoría de servicios DeFi corren en Ethereum (pero en expansión a otras redes: cross & side chains)

→ CeFi's pains: slow settlement cycles, price discovery ineficiente, iliquidez, incertidumbre sobre alocación del subyacente, moral hazard (sub-prime?)

Hedge funds rethink after GameStop pain

January's surprise attack by retail investors has sparked new efforts to detect emerging threats

Investors co-ordinating their purchases on Reddit's WallStreetBets message board were able to drive up the share price of Gamestop, the US video game retailer, from less than $20 at the start of the year to more than $480 by late January, while the prices of some other beaten-down stocks also soared.

**DeFi beyond the hype, the emerging world of Decentralized Finance*, Wharton Blockchain & Digital Asset Project, WEF, Kevin Warbach, 2021.

DeFi: Zoom In

→ Intermedian la transferencia e intercambio directo de valor P2P (aunque requieran servicios auxiliares como oráculos, wallets y decentralized storage) **Over-collateralization** (por volatilidad y falta de credit scoring)

→ Las transacciones se ejecutan (settlement & finality) sobre la base de **smart contracts** según las reglas de cada protocolo de DeFi, reglas que son públicas y transparentes: token holders tienen –generalmente- voting rights para decidir upgrades/updates de protocolo via DAOs

→ **Non-custodial:** los activos digitales gestionados vía DeFi son siempre gestionados sólo por sus dueños **(private key holder: non-custodial wallets/smart contract-based escrow**). Custodial-CEX no son parte del DeFi vertical

→ Source code & APIs son open source, programables, y combinables (e.g., se puede combinar un token estable, para usarlo como subyacente de un derivado, o como garantía de un préstamo con activos digitales, etc.)

Trading Tokens & DeFi

DeFi - Concepto e Impacto: ¿Hacia una Economía de Trueque?

Problemas Relevantes aún NO RESUELTOS:

1. Capacidad de billeteras con interoperabilidad (múltiples tokens)
2. Mejores soluciones de recuperación de claves.
3. El problema de la "Coincidencia de Deseos". Los intermediarios (CEX) resuelven este problema al oficiar como *matchmakers* pero con las problemáticas de la centralización previamente señaladas
4. Las externalidades y reticencias de los actuales sistemas de monetarios (analógicos en su enorme mayoría), que limitan muchas veces el acceso a este sistema.

¿Cómo podría resolverse?

Un caso Testigo

"Stefan Thomas perdió hace años el papel donde escribió la contraseña de su cartera de bitcoins. Y ahora solo **le quedan dos intentos para averiguarla o perder los 220 millones de dólares en los que están valorados sus 7.002 BTC.** Es la historia que nos cuenta el New York Times, la de un ingeniero alemán que ha visto como con el paso de los años su olvido va camino de convertirse en tragedia.

Los bitcoins los tiene almacenados en un pequeño disco duro cifrado, denominado como IronKey. Se trata de un disco flash que ofrece seguridad y privacidad. Y también 10 intentos antes de formatear y eliminar el contenido. Thomas ya ha probado ocho veces algunas de sus contraseñas más utilizadas, pero ninguna ha funcionado."
https://www.xataka.com/criptomonedas/220-millones-dolares-bitcoin-contrasena-perdida-dos-intentos-restantes-tragica-historia-ingeniero-aleman-para-recuperar-su-cartera

La tokenización de actividades económicas, desde activos reales hasta activos digitales y todo tipo de derechos de acceso, podría afectar el papel del dinero del banco central como monopolista geográfico que proporciona un medio de intercambio, una vez que se manifieste la adopción masiva de los manifiestos Web3 y los efectos de red necesarios. **La tokenización de la economía real también podría conducir a *la fusión del sector financiero con la economía real. ?***

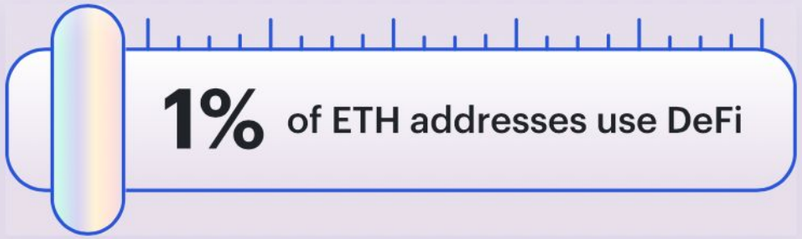
DeFi: Zoom In

→ Es un mercado que nace en la **intersección de la Blockchain, los activos digitales y los servicios financieros**

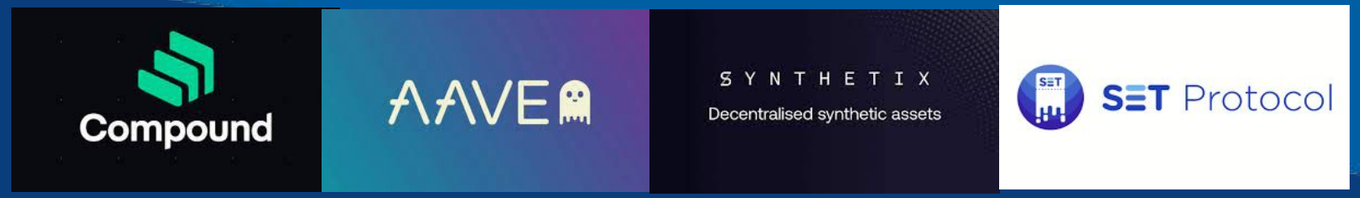
→ Crecimiento exponencial: de **1B locked en 2019 a los 53B locked in Q121:** 53X en 2Y ....

→ Todos estos nuevos servicios corren en **Ethereum,** Binance Smart Chain (hard fork de Ethereum compatible) y otras blockchains pública no permisionada, diseñada para transaccionar smart contracts

Mientras todo este crecimiento ha sido increíblemente beneficioso para todo el ecosistema de criptomonedas, el aumento de la demanda presenta algunos desafíos para la red. El precio medio del gas ha aumentado de aproximadamente 100 Gwei a principios de año a alrededor de 150 Gwei al 31 de marzo, un aumento del 50% en ETH. Este aumento se produjo durante un tiempo en el que el precio de ETH también aumentó de USD $732 a casi USD $2,000 en el mismo período de tiempo, lo que agravó el valor en dólares que los usuarios deben pagar por gas. El aumento en el precio del gas y el precio de ETH llevó a que las tarifas de transacción promedio aumentaron de USD $5.4 al comienzo del año a USD $22.9 al final del primer trimestre, un aumento de aproximadamente 4.2x.



DeFi: Servicios



1. **Stablecoins**: en tanto sean non-custodial (vs. USDC, DIEM). Cubren la volatilidad: MakerDAO & DAI.

2. **Exchanges**: DEX vs. CEX vs. Automated Market Makers (AMMs) & liquidity pools vs. bid/ask spreads: UniSawp (100B trading volumen en 2Y) & SushiSwap (fork de UniSawp + SushiToken for governance)

3. **Crédito**: Compound & Aave: agrupan tokens (pooling) y pagan un interés variable en tokens de protocolo en función de un ratio supply-to-borrowing. Tomadores también pagan un interés variable y sobre-colateralizan con tokens. Estos créditos pueden securitizarse. Flash loans (arbitraje cross-exchanges)

4. **Derivados**: Synthetix: sintético en Ethereum. SNX token: staking & collateral + 3 DAOs (protocol, grants, Synthetix)

5. **Seguros**: (new) DeFi risks: hacks, smart contracts bugs, game-theory poor design risks. NexusMutual: NXM token holders validan ocurrencia de siniestro y pago de cobertura, reciben pro rata interés generado por pago de primas

6. **Asset management:** Set Protocol. DeFiPulse Index

7. **Servicios auxiliares**: non-custodial wallets + oráculos + decentralized storage

DeFi: Agregadores de Servicios Defi

Ofrecen una combinación de todos o los principales servicios DeFi

$85.8B+	820K+	5	6.4M+
Total volume	Total users	Supported networks	Total trades
$43B+	57.40%	122	1INCH
Access liquidity sources	Aggregation share	Sources connected	Governance and utility token

1inch DAO

A decentralized autonomous organization that governs the 1inch Network, enabling 1INCH stakers to vote for key protocol parameters and take part in the network's governance.

DeFi: *On-Chain Governance*

→ La mayoría de los servicios DeFi se apalancan en una **estructura horizontal donde los tokens holders de cada protocolo DeFi pueden votar** en materias relevantes (suele existir una DAO)

→ Usuarios con X tokens los depositan (locked-up) en un pool y a cambio reciben pagos in kind (similares a intereses, tasa pasiva) y a veces tokens de gobernanza

→ Usuarios de los servicios DeFi que acceden al pool de DeFi services (e.g. préstamos, seguros, liquidez, tokens estables –DAI–, nuevos tokens) pagan fees al DeFi pool (similares a interés, tasa activa, o comisiones)

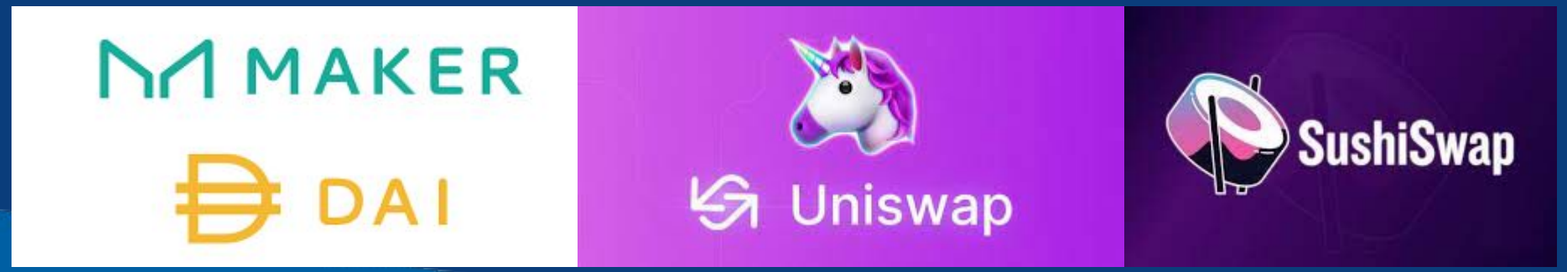
→ Mientras más liquidez tenga un pool, más valor tiene esa red/protocolo y más usuarios atraerá (network + token effect), y ese mayor valor se reparte entre quienes aportan liquidez generalmente de manera algorítmica

DeFi: *On-Chain Governance*

→ Cuando se emiten tokens a cambio de liquidez, éstos tokens de cada protocolo DeFi suelen/pueden incluir **derechos de voto sobre mejoras/actualizaciones del protocolo, o fijación/modificación de criterios de tasas de interés/comisiones/ratios de garantías/ apalancamiento**

→ Estos tokens de protocolo pueden a su vez ser intercambiados vía Exchanges, y su valor estará vinculado al nivel de actividad del servicio DeFi que los emite (pool size)

→ En el máximo nivel de descentralización, **el servicio DeFi es operado por una DAO**: los votos de los token holders sobre X materias se procesan vía smart contracts, sin que nadie puede interferir/manipular en el proceso (on-chain governance): MakerDAO y SushiSwap, etc.



DeFi: Fork it & Improve it

→ UniSwap se lanzó en Ethereum para permitir Atomic Swaps entre token holders creando liquidity pools automátizados (Automated Market Makers) via HTLCs

→ UniSwap no tenía un token de gobernanza propio. En Agosto 2020, **SushiSwap decidió forkear el protocolo de Uniswap, y agregar un token de gobernanza (SUSHI) y staking rewards para los inversores**

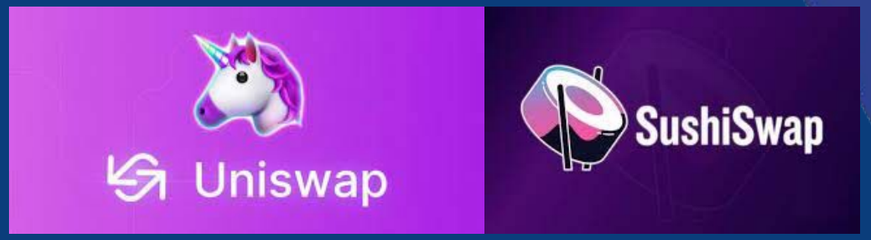
→ El creador de SushiSwap es anónimo (Chef Nomi)

→ SushiSwap permite prestar tokens para liquidity pools y, además ganar tokens y fees a cambio de hacer staking de los SUSHI tokens

→ En 24 horas, SushiSwap recaudó tokens por valor de 250M U$D (se llevó casi el 50% de la liquidez de UniSwap, que luego también creó un token de gobernanza - UNI)

Sushiswap — the appetizing fork of Uniswap

SushiSwap and Vampire Attacks in Decentralized Finance (DeFi)



6 Privacidad

Privacidad en la Web3 & *Payment Tokens**

May 12, 2021, 06:55pm EDT | 42.974 views

Vitalik Buterin Moves $1.3 Billion Worth Of Ether, But Where?

Ethereum co-creator Vitalik Buterin has moved $1.3 billion worth of ether, almost all of his holdings, from his main public address to a separate wallet.

Buterin disclosed his main ether address in October 2018, and until approximately six hours ago, the wallet held more than 320,000 ether, the blockchain's native cryptocurrency. Then, at 1:18 PM EST the ethereum inventor transferred 325,001 ether to a separate contract address created approximately 21 hours ago, leaving some $10,000 worth of ETH in his main wallet.

→ Las primeras redes de blockchain son muy transparentes: la historial del token es visible para todos

→ Esto puede comprometer la privacidad de los token holders y también vuelve menos fungibles a los tokens

→ Sistemas alternativos de tokens han nacido para crear protocolos que preservan más la identidad

→Las formas analógicas de dinero (monedas y los billetes), no dan ninguna información sobre el historial de transacciones: no hay una forma económicamente viable de trazar una lista de los anteriores dueños

→ El **papel moneda puede ser considerada la forma de dinero más anónima y más fungible** (Escocia: 1749, determinó la fungibilidad de tokens-moneda emitidos por el Estado en forma de pagaré bancarios y monedas afirmando que el historial de una moneda individual o de un pagaré eran irrelevantes)

→ Esta **fungibilidad del dinero ha sido desafiada por la creciente digitalización de nuestros sistemas financieros globales**

* Shermin Voshmgir, Token Economy, https://github.com/Token-Economy-Book/SpanishTranslation/wiki/Tokens-de-Privacidad

Privacidad en la Web3 vs. *Privacidad* en la Web2*

→ El auge de los pagos con tarjeta de crédito, los servicios de banca electrónica, y los servicios de tecnología financiera basados en la Web2 **han aumentado las posibilidades de trazar los flujos de dinero**

→ Los registros electrónicos han reducido los costos de monitoreo sobre cómo usamos nuestro dinero con simples algoritmos: regulaciones antilavado (AML) y esfuerzos por parte de entes recaudadores obligan a las instituciones financieras a monitorear y en algunos casos revelar información sobre las actividades financieras de sus clientes

→ Las regulaciones AML en los EE.UU datan de la Ley de Secreto Bancario de 1970. El auge del tráfico internacional de drogas y el lavado de activos llevó a la creación del Grupo de Acción Financiera Internacional **(GAFI)** en 1989. Luego del 11/9 en 2001, el GAFI amplió su regulación AML para combatir el financiamiento del terrorismo

---

→ Muchos países comenzaron a imponer regulaciones de KYC que requieren que las instituciones financieras establezcan la **identidad de sus clientes, mantengan registros de sus transacciones, y notifiquen a las autoridades sobre actividades potencialmente sospechosas** de sus clientes respecto de “umbrales de transacción” definidos por los gobiernos

---

→ Tales prácticas, consecuencia de imposiciones regulatorias, están gradualmente erosionando la fungibilidad del dinero (electrónico)

* Shermin Voshmgir, Token Economy,
https://github.com/Token-Economy-Book/SpanishTranslation/wiki/Tokens-de-Privacidad

Privacidad de los Tokens Criptográficos*

→ *Bitcoin y otras redes públicas no permisionadas usan* ***criptografía asimétrica para crear identidades online en la forma de direcciones de blockchain***

→ *Un usuario puede crear múltiples direcciones sin requerimientos de KYC y a la vez enviar y recibir tokens de manera totalmente confiable a través de redes públicas*

→ *Las direcciones consisten en una tira alfanumérica que no da* ***ninguna indicación sobre la identidad del usuario****, pero esto sólo provee* ***pseudonimidad***

→ *Divulgar públicamente la dirección de uno en blockchain (incluso por la actividad de uno en un Exchange) hace que el usuario pueda ser* ***des-anonimizado a través de esfuerzos usando análisis de datos:*** *la privacidad de los nodos solo puede ser garantizada mientras la identidad real del dueño de una billetera no pueda ser vinculada a una determinada dirección en la red*

** Shermin Voshmgir, Token Economy, https://github.com/Token-Economy-Book/SpanishTranslation/wiki/Tokens-de-Privacidad*

Privacidad de los Tokens Criptográficos*

→ ***La naturaleza públicamente verificable de algunas redes de blockchain vuelven trazables las transacciones***

→ *Todas las transacciones son registradas en texto plano (no encriptado) en un registro y los datos de las transacciones son visibles para cualquiera que use un explorador de bloques y pueden por ello ser vinculadas a otras transacciones hechas por el mismo tenedor del token*

→ *Tales datos* ***pueden potencialmente revelar información sensible: la dirección de quien envía, la dirección de quien recibe, el vínculo entre ambas direcciones, y la cantidad de tokens enviados***

→ *Aún más, en el proceso de transmitir transacciones, los nodos pueden revelar su dirección de IP: metadatos de las transacciones de tokens pueden ser usados para trazar la dirección de IP de un usuario, en ocasiones incluso si se utilizan servicios de anonimización como Tor o I2P.*

→ *Hacer tales vinculaciones no requiere demasiado esfuerzo, especialmente para autoridades gubernamentales*

** Shermin Voshmgir, Token Economy, https://github.com/Token-Economy-Book/SpanishTranslation/wiki/Tokens-de-Privacidad*

Privacidad de los Tokens Criptográficos*

→ *La mayoría de los usuarios hoy compran tokens en Exchanges contra dinero fiduciario usando Exchanges que están más y más sujetos a regulaciones KYC*

→ *Incluso si no lo hacen, el dinero fiduciario que es enviado a un Exchange de tokens generalmente requiere interacción con el sistema bancario, y éstos bancos están sujetos a regulaciones KYC*

→ ***Cualquiera con acceso a la base de datos de un Exchange puede, por ello, vincular las direcciones pseudónimas con nombres reales:*** *tales datos son compartidos entre los Exchanges y con agencias estatales o empresas de análisis de blockchain "Chainalysis" y "Elliptic" para detectar patrones generales de transacciones, incluyendo potenciales actividades de lavado de dinero y fraude*

→ *Dependiendo del origen de un token, tokens individuales pueden ser no aceptados por comercios debido a su* ***historial contaminado de transacciones:*** *esto reduce la fungibilidad de un token.*

US Treasury Department Blacklists 20 Bitcoin Addresses Tied to Alleged North Korean Hackers

The U.S. Treasury Department's Office of Foreign Asset Control has added two individuals and 20 bitcoin addresses to its sanctions list, accusing them of being part of the North Korea-affiliated Lazarus Group.

By Nikhilesh De · Mar 2, 2020 at 2:23 p.m. · Updated Sep 13, 2021 at 9:22 a.m. ·

The group has been accused of stealing more than half a billion dollars in crypto as far back as 2018, when cybersecurity vendor Group-IB claimed it had targeted 14 different exchange in two years. Monday's action specifically stems from the hack of an unnamed exchange in April 2018, according to a press release by the Treasury Department.

Privacy-Preserving Tokens*

→ Las redes de blockchain más recientes han sido configuradas para **mejorar el nivel de privacidad de las transacciones de tokens**

→ Estos “tokens de privacidad” **usan varios mecanismos de ofuscación** para hacer menos transparente el historial: el objetivo es **diseñar un protocolo que revele la mínima información necesaria y oculte toda otra información**

→ Dependiendo del protocolo de blockchain, varios elementos de una transacción pueden ser anonimizados en diferentes niveles:

→ Privacidad de usuario (anonimidad total): la identidad del usuario que envía o recibe un token es ofuscada de modo tal que las acciones del usuario no pueden ser vinculadas a su identidad en el mundo real

→ Privacidad de los datos de transacciones: ofuscando datos específicos de transacciones de tokens usando herramientas criptográficas, como las direcciones de quién envía y quién recibe, o el monto de la transacción

→ Privacidad del estado de la red: Si ciertos datos de transacciones pueden ser convertidos en privados, el registro sólo revela información parcial sobre el estado de la red. Diferentes atributos del estado de la red pueden ser privados para distintos usuarios

* Shermin Voshmgir, Token Economy, https://github.com/Token-Economy-Book/SpanishTranslation/wiki/Tokens-de-Privacidad

Privacy-Preserving Tokens*

→ Algunos métodos actualmente empleados:

→ Mixing Services: es una técnica de agregación usadas por servicios de mezcla: mezclan inputs y outputs de diferentes transacciones de tokens, combinándolos en una transacción colectiva y así ofuscando las conexiones entre quienes envían y quienes reciben. E.g. “Bitmixer”, “CoinJoin” y “TumbleBit”

→ La mayoría de los clientes actuales de los tokens de privacidad y de las blockchains que preservan identidad usan una variación de dichos servicios de mezclado

→ Originalmente lanzada como “XCoin”, luego rebautizada “Darkcoin” antes de ser renombrada como “Dash” es un fork del código base de Bitcoin que fue activado en 2014: es una red de Prueba-de-Trabajo con diferentes tipos de nodos, los “diggers” (mineros) y los “nodos maestro”. Nuevos bloques son creados por los mineros. Los nodos maestro se ocupan de la gobernanza y las funciones de privacidad: “PrivateSend” (privacidad financiera) y “InstantSend” (transacciones inmediatas). “PrivateSend” usa variaciones de métodos de mezcla de tokens de CoinJoin. “InstantSend” permite transacciones casi inmediatas donde los inputs son bloqueados en relación a transacciones específicas y verificadas por el consenso de los nodos maestro de la red

→ transacciones específicas y verificadas por el consenso de los nodos maestro de la red

* Shermin Voshmgir, Token Economy, https://github.com/Token-Economy-Book/SpanishTranslation/wiki/Tokens-de-Privacidad

Privacy-Preserving Tokens*

→ Monero se basaba originalmente en el protocolo de “Bytecoin”, y fue bifurcada por varios desarrolladores (algunos de los cuales siguen siendo anónimos) en “Bitmonero”, y fue bifurcada en Monero en 2014

HELEN PARTZ 24 AUG 2021

El precio de Monero sube un 20% tras la implementación de Atomic Swap

El Proyecto Monero introdujo la semana pasada una nueva forma de intercambio trustless entre Monero y Bitcoin.

→ Monero es el token de privacidad más antiguo y también la red de tokens de privacidad más difundida. A diferencia de Bitcoin, donde los tokens son enviados a direcciones públicas, los tokens en la red de Monero son enviados a nuevas direcciones anónimas creadas para un único uso (direcciones secretas). Para crear una dirección secreta y autorizar transacciones se necesita usar una “llave privada de única vez”.

→ Solo el destinatario de la transacción puede “descubrir” esta nueva dirección usando su “llave secreta para ver”.
→ El proceso de descubrimiento es realizado por la billetera Monero del destinatario, que escanea la red para encontrar estas nuevas direcciones secretas.

→ El equipo de Monero también planeaba implementar en el protocolo un enrutamiento de paquetes que preserve la privacidad con el proyecto “Kovri”, que hubiera permitido a los usuarios esconder su dirección de IP y sus ubicaciones.es inmediatas

Privacy-Preserving Tokens*

→ Zcash fue lanzada en 2016. Es un desarrollo que usa las pruebas de zero
conocimiento (ZKP), algoritmos criptográficos que permiten que los nodos de la red demuestren la posesión de ciertos datos sin revelar los datos en sí. Pueden usarse para ofuscar datos de transacciones almacenados en el registro (la dirección del remitente, la dirección del destinatario, la cantidad transferida), permitiendo a los nodos verificar la validez de los datos de transacción encriptados sin tener que conocer los datos

→ En estas configuraciones, el que "demuestra" puede demostrar al "verificador" que una aseveración es verdadera, sin revelar ninguna información más allá de la validez de la aseveración.

→ La red Zcash ofrece "privacidad opcional": usuarios pueden elegir usar "direcciones transparentes" o "direcciones protegidas". Las "direcciones transparentes" son similares a las direcciones en la red de Bitcoin. Las direcciones protegidas anonimizan los datos de la transacción.

→ En Zcash las transacciones pueden ser (i) transparente-a-transparente (igual a Bitcoin), (ii) transparente-a-protegida (protegiendo transacciones que rompen la trazabilidad), (iii) protegida-a-transparente; (iv) protegida-a-protegida (transacciones privadas donde las direcciones y los valores de transacciones son anónimos); (v) híbridas (protegiendo parcialmente las direcciones remitentes y/o destinatarias)

Privacy-Preserving Tokens*

KOLLEN POST OCT 19, 2020

US financial watchdog fines early Bitcoin mixer $60M for money laundering

FinCEN has fined the operator of early crypto mixers Helix and Coin Ninja for Bank Secrecy Act violations.

Bittrex
@BittrexExchange

#Bittrex Customers:

The $XMR, $ZEC, and $DASH markets will be removed on Friday, January 15th at 23:00 UTC.

Details: bittrex.zendesk.com/hc/en-us/artic...

2:15 p. m. · 1 ene. 2021

2 mil Compartir este Tweet

FINANCIAL CRIMES ENFORCEMENT NETWORK

Mixing services attempt to privatize cryptocurrencies by sending them through a massive series of transactions involving various wallets. The process aims to obscure the origins of coins as well as the entity in control of them when they come out of mixing. Harmon's mixers were only accessible via the dark web.

First Bitcoin “Mixer” Penalized by FinCEN for Violating Anti-Money Laundering Laws

Contact: Office of Strategic Communications, 703-905-3770
Immediate Release: October 19, 2020

MUCHAS GRACIAS POR SU TIEMPO

Sebastian Heredia Querro

Martín Bertoni