



RIDAA
Repositorio Institucional
Digital de Acceso Abierto de la
Universidad Nacional de Quilmes



Universidad
Nacional
de Quilmes

Zocaró, Marcos

Criptomonedas y blockchain



Esta obra está bajo una Licencia Creative Commons Argentina.
Atribución - No Comercial - Sin Obra Derivada 2.5
<https://creativecommons.org/licenses/by-nc-nd/2.5/ar/>

Documento descargado de RIDAA-UNQ Repositorio Institucional Digital de Acceso Abierto de la Universidad Nacional de Quilmes de la Universidad Nacional de Quilmes

Cita recomendada:

Zocaró, M. (2022). *Criptomonedas y blockchain*. *Revista Intercambios*, 7(3), 10-27. Disponible en RIDAA-UNQ Repositorio Institucional Digital de Acceso Abierto de la Universidad Nacional de Quilmes
<http://ridaa.unq.edu.ar/handle/20.500.11807/5197>

Puede encontrar éste y otros documentos en: <https://ridaa.unq.edu.ar>

CRIPTOMONEDAS Y BLOCKCHAIN



Marcos Zocaro

Contador Público por la Universidad Nacional de La Plata (UNLP), especialista en Tributación y magíster en Finanzas Públicas Provinciales y Municipales por la misma institución. Asesor, docente universitario e investigador del Centro de Estudios en Administración Tributaria. Miembro de la Asociación Argentina de Estudios Fiscales y la ONG Bitcoin Argentina. Autor de los libros *Manual de Criptomonedas* y *Una bolsa de impuestos*. Sus principales áreas de interés son la tributación de las operaciones bursátiles, las criptomonedas, la economía del conocimiento, la educación financiera y las finanzas públicas.

Buenas tardes y muchas gracias por la invitación, a vos y a las autoridades de la Universidad Nacional de Quilmes. Vamos a hablar en esta presentación sobre *criptomonedas*, *blockchain* y el origen de *bitcoin*: ¿qué vinieron a solucionar y con qué objetivo se crearon hace poco más de diez años, allá por los años 2008 y 2009?

Antes de entrar de lleno en bitcoin, sepamos que el dinero en la historia no fue siempre como lo conocemos hoy (el billete o la moneda que llevamos en la billetera). Originalmente, se trocaba; después, como medio de pago o de intercambio de valor, se utilizaban vacas o más tarde, la sal. El fenómeno del intercambio y la unidad de valor fue mutando hacia los metales como forma de intercambio. A veces se hacía una moneda de metal con menor cantidad de material que el que decía tener. Se empezó a tener desconfianza y por eso también la moneda de metal fue mutando al dinero en papel, el conocido billete (Ver: Imagen 1).

Primero en China, y siglos después en Europa, el dinero en papel como medio de intercambio facilitaba el comercio entre diferentes puntos geográficos, pues cumplía en principio tres objetivos: ser una unidad de cuenta, servir como medio de intercambio y ser una reserva de valor. Originalmente, cada billete estaba respaldado por metales. Hace unos 200 años se implementó el patrón oro, vigente hasta entrado el siglo XX.

Todo el dinero, todos los billetes (cada dólar emitido) estaban respaldados por el patrón oro (Ver: Imagen 2). Hasta que llega la primera guerra mundial, cuando se tuvo que empezar a emitir más de lo que se podía respaldar. Para solventar los gastos de la guerra, el dinero se empezó a emitir de forma descontrolada, hasta que el patrón oro se terminó de romper en la segunda mitad del siglo XX.

En la imagen se ve el dibujito de la maquinita que emite indiscriminadamente; pues, desde 1970, no existe el patrón oro. En este caso, la Reserva Federal de los Estados Unidos no requiere que por cada dólar que emita haya un respaldo de ningún tipo.

Breve historia del dinero

Principales acontecimientos

9 de junio 2021

Primer país del mundo en adoptar una criptomoneda
El Salvador aprueba el bitcoin como moneda de curso legal

14 de abril 2021

Criptomonedas en Wall Street
Salida a la bolsa de una de las mayores plataformas de intercambio de criptomonedas, Coinbase



Moneda virtual
Lanzamiento del Bitcoin como criptomoneda (descentralizada). Le siguen Litecoin, Ethereum y ZCash



Finales de los 90

Pago digital

Los pagos se realizan usando dispositivos electrónicos portátiles como teléfonos inteligentes o tabletas



El ganado es canjeado como forma de pago

Trueque

Alrededor de 9.000 aC

Peso

3.000 aC

Unidades de peso como base para el comercio (ejemplo: xx cantidad de granos = xx cantidad de oro y otros metales)

Monedas de metal

1.000 aC

Monedas de oro y plata

600 aC

Alrededor de 800 dC

Papel moneda

1.400

Bancos

Surgen conceptos de banca, deuda comercializada

1816

Patrón oro

Estandarización del valor en Inglaterra. Adaptado en EEUU en 1900, dando lugar al nacimiento del banco central

1871

Transferencia de dinero

Primera transferencia de fondos por telegrama, por Western Union

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

1930

Fin del patrón oro

La norma es revisada en EEUU y el precio del oro se devalúa. La estandarización británica también termina

Versiónes metálicas de las conchas marinas de China, consideradas como las primeras monedas



Primera moneda nacional en la actual Turquía



Primeras versiones de papel moneda impreso en China. En Europa los billetes se introducen en el siglo XVII



Fuentes: Investopedia, mint.com, Western Union, Goldtraders, PBS, Fotos AFP

AFP

Imagen 1: Breve historia del dinero.

Evolución del "respaldo" del dólar



Imagen 2: Evolución del "respaldo" del dólar. Se consignan las imágenes en dólares según circularon con y sin respaldo en oro.

Sabemos de la inflación que hay y de los inconvenientes que causa la emisión. Estados Unidos mismo, a raíz de la pandemia tuvo que emitir demasiado dinero, lo cual generó una inflación interanual del 7%. Hacía décadas que no les sucedía eso a los estadounidenses.

Entonces, una de las consecuencias de la emisión indiscriminada de dinero es la inflación; por lo tanto, se produce la pérdida de reserva de valor. Se está desvirtuando la reserva de valor incluso en el dólar. Una persona que tenía hace un año 100 dólares, hoy tiene un 7% menos de poder adquisitivo. Hablo del dólar, no del peso argentino, con muchísimo mayor pérdida (Ver: Imagen 3).

Como vemos en el gráfico (Ver: Imagen 4), en el caso del peso, no hace falta que nos vayamos 100 años para atrás. Vemos la tremenda pérdida del poder adquisitivo desde 2017: un billete de 1.000 pesos que hace menos de 5 años equivalía a 57 dólares, aquí equivale a menos de 5 dólares. Todos los billetes, no solo la moneda argentina,

sino el dólar también, pierden valor, pierden poder adquisitivo.

Es por ello que en 2008 irrumpe en la escena económica mundial el bitcoin. Un tal Satoshi Nakamoto publica ese año un *paper* de 9 páginas –se lo pueden encontrar fácilmente en internet– donde describe el sistema bitcoin, el objetivo y cómo funcionaría.

En enero de 2009 aparece la primera unidad de bitcoin. Pero uno de los objetivos de Satoshi Nakamoto, quizás el principal, fue crear un dinero inteligente, que cumpla con el objetivo principal del dinero (la reserva de valor). En el caso de bitcoin, una de las características principales es su escasez, pues no se van a emitir más de 21 millones de bitcoins. Hay incluso un modelo de emisión que ya está pautado desde el origen y no se puede modificar (Ver: Imagen 5).

Vean la importancia económica de las cripto monedas.

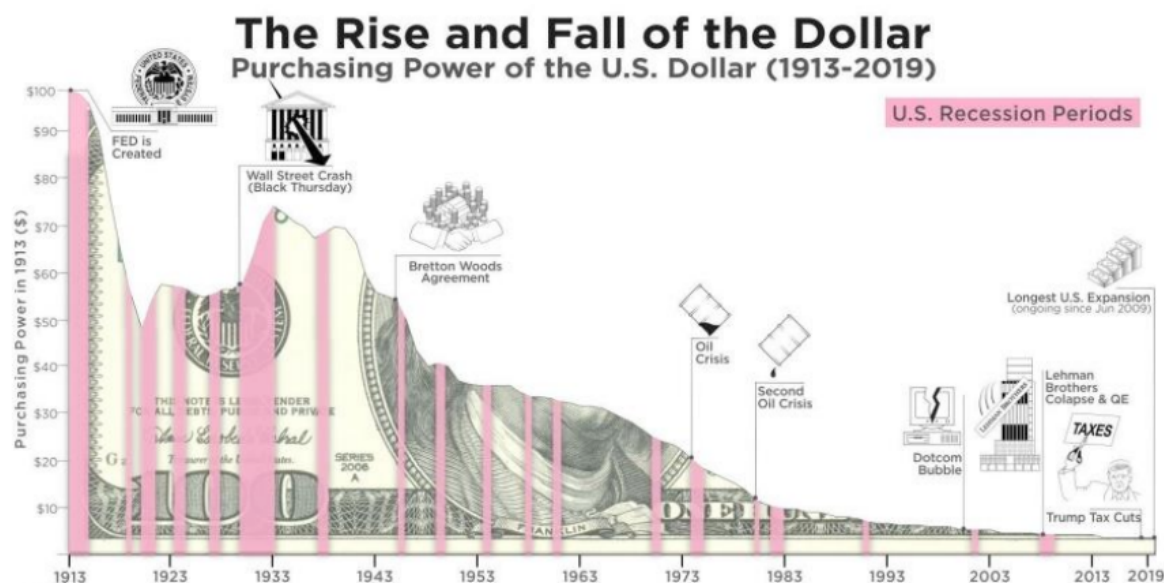


Imagen 3: The Rise and Fall of the Dollar.



Imagen 4: Desde su emisión, el billete de \$1.000 perdió 92% de su valor en dólares.

Satoshi Nakamoto y la irrupción de las criptomonedas



Imagen 5: Satoshi Nakamoto y la irrupción de las criptomonedas.

Todo arrancó con un bitcoin, pero se multiplicaron las cantidades de *tokens* y de criptomonedas diferentes. Hoy hay más de 18 mil en el mercado, la gran mayoría sin mucho sentido. Bitcoin sigue siendo la principal y la más importante del ecosistema actual. Hoy bajó un poco la capitalización del mercado, pero en el 2021, llegó a cotizar más de 3 billones de dólares. Más de 6 veces el PBI argentino, para que se hagan una idea de la magnitud (Ver: Imagen 6).

Esa imagen es de hace pocos días. El bitcoin cotizaba a 39 mil dólares. Hoy cotiza a 42 mil. En las páginas *Coin market cap* y *Eintreiben*, hay más de 18 mil criptomonedas o tokens, la gran mayoría sin demasiado sentido, reitero. Hay que tener cuidado a la hora de invertir. Bitcoin es la principal, la que acapara casi el 43% del mercado y la capitalización del mercado, en el *Market cap* es de más

de 700 mil millones de dólares –para que vean la importancia. Además, el gráfico muestra en *Circulating Supply*, en el capital de circulación que es clave, aun no llega a 19 millones de bitcoin.

En la evolución del dinero, siempre la escasez fue un problema para poder satisfacer el requisito de reserva de valor. En el caso del bitcoin, lo que lo hace muy valioso es precisamente la escasez: no se va a emitir más de 21 millones. El resto de las criptomonedas sí, hay algunas que tienen emisión ilimitada; incluso, algunas dependen de la voluntad de una empresa que las emita. No son todas descentralizadas.

En el caso del bitcoin, tenemos un dinero electrónico; digital, mejor dicho, y descentralizado. Eso es fundamental, es lo que quiso hacer Satoshi Nakamoto, además de un

Cryptos: 18.142 Exchanges: 460 Market Cap: \$1,758,275,879,484 24h Vol: \$90,823,405,339 Dominance: BTC: 42.6% ETH: 17.8%							
# ▲	Name	Price	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ	Circulating Supply ⓘ
1	 Bitcoin BTC Buy	\$39,410.11	▼ 5.82%	▼ 6.13%	\$747,990,322,634	\$30,949,108,476 785,309 BTC	18,979,656 BTC
2	 Ethereum ETH Buy	\$2,609.59	▼ 3.28%	▼ 6.96%	\$312,907,082,281	\$5,113,244 ETH	119,906,553 ETH
3	 Tether USDT	\$1.00	▲ 0.03%	▲ 0.04%	\$80,078,353,064	\$65,506,076,332 65,469,562,166 USDT	80,033,716,071 USDT
4	 BNB BNB Buy	\$371.12	▼ 5.27%	▼ 7.06%	\$61,277,481,929	\$2,092,052,104 5,637,191 BNB	165,116,761 BNB
5	 USD Coin USDC	\$0.9999	▼ 0.02%	▲ 0.01%	\$52,404,967,281	\$3,967,949,966 3,968,393,363 USDC	52,410,823,254 USDC
6	 Terra LUNA Buy	\$100.52	▲ 1.60%	▲ 18.52%	\$36,372,171,982	\$5,616,315,003 55,874,950 LUNA	361,855,289 LUNA

Clave: Escasez

Imagen 6.



Imagen 7: Where Cryptocurrency Is Most Heavily Used.

dinero que tenga reserva de valor cuya emisión sea limitada. También quiso que sea parte de un sistema descentralizado, que no dependa de bancos, ni de empresas, ni de ninguna institución, sino de personas (Ver: Imagen 7).

Aquí vemos un dato de color de hace menos de un año: los países en los que más se utilizan las criptomonedas son Argentina, Estados Unidos y parte de Europa. En América Latina va creciendo quizás a un ritmo más acelerado que en Europa. Lo cierto es que, de a poco, se va masificando el uso de criptomonedas.

¿Cómo empezó bitcoin? Como les decía, en el año 2008, el 31 de octubre, en medio de la crisis económica mundial. Justo el día de Halloween, Satoshi Nakamoto, perso-

na totalmente anónima, publica en un foro de internet, el *paper* titulado "Bitcoin, sistema de dinero en efectivo electrónico *peer-to-peer*" (Ver: Imagen 8).

Recién el 3 de enero del 2009 empieza –entre comillas– a “fabricarse” el bitcoin y en octubre de ese mismo año se hace la primera venta de bitcoin, que valía en ese entonces 0,001 dólar. Vean todo lo que aumentó hasta hoy. Un detalle de color: en mayo de 2010, un programador estadounidense produce la primera compra de un bien pagando con bitcoin.

Lazlo Hanyecz publicó en un foro de internet: a quien traiga dos pizzas a mi casa, le pagaré con 10.000 bitcoin. Nadie le llevó las pizzas hasta que, unos días después,

republicó el aviso, y el 22 de mayo alguien le llevó a la puerta de su casa las dos pizzas. Lazlo pagó con 10.000 bitcoins, que hoy representan más de 400 millones de dólares.

En ese entonces no existían pizzerías que aceptaran bitcoin. Hoy en día, sí; y se acepta cualquier criptomoneda para comprar lo que sea. Por ello, el 22 de mayo se conmemora siempre el *Bitcoin pizza day* (Ver: Imagen 8).

Además, hay mucho conocimiento acumulado. Para entender cómo funciona bitcoin, tenemos que entender en primer lugar qué es la

Lazlo Hanyecz publicó en un foro de internet: a quien traiga dos pizzas a mi casa, le pagaré con 10.000 bitcoin. Nadie le llevó las pizzas hasta que, unos días después, republicó el aviso, y el 22 de mayo alguien le llevó a la puerta de su casa las dos pizzas. Lazlo pagó con 10.000 bitcoins, que hoy representan más de 400 millones de dólares.

tecnología *blockchain*. Es tecnología de registro distribuido que se utiliza para bitcoin, pero no es ese el único uso.

Se puede utilizar para muchas otras actividades. ¿Qué es la tecnología de registro distribuido?: es una base de datos distribuida. Imaginen que hay computadoras distribuidas alrededor del mundo conectadas entre sí por internet y en cada una de ellas existe la misma base de datos. Cada vez que se incorpora información a esa base, cae en el libro *blockchain*, una cadena de hojas, y cada hoja del libro es un bloque. Cada vez que se incorpora información a uno de

Evolución del precio medio de bitcoin (valor de cierre diario)



Imagen 8: Evolución del precio medio de bitcoin (valor de cierre diario).

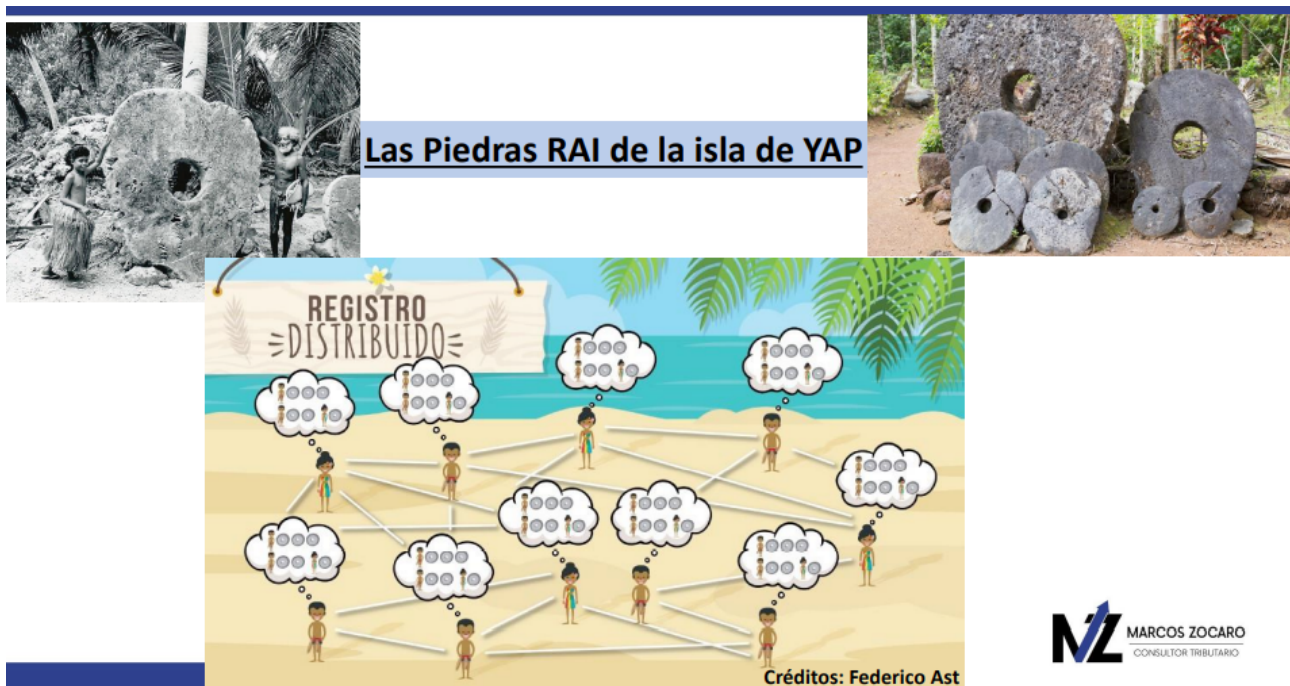


Imagen 9: Las Piedras RAI de la isla de YAP.

esos bloques, una de las hojas del libro –de la base de datos–, todas las computadoras, todos los nodos distribuidos alrededor del mundo, actualizan automáticamente la información.

Eso hace que si uno de los nodos (una de las computadoras) se apaga, la base de datos sigue viva en el resto de los nodos. Por eso, el sistema es descentralizado. Y por eso, la fortaleza del sistema no es una base de datos centralizada (si se rompe el servidor central, no tenemos más base de datos), sino la descentralización. Blockchain se puede utilizar también para –por decir algo bastante común– registrar compras públicas; porque hay diferentes tipos de blockchain, pero una de las características es que es pública y, al ser pública, cualquier persona puede ver las transacciones. Imaginen que en vez de registrar compras públicas en un expediente en papel, o en una base de datos electrónica, se utilizara la blockchain; en

ese caso, cualquier persona puede ver las transacciones por ser algo público, y una vez que está incorporada la información a la base de datos, ya no se puede alterar.

No se puede modificar, por eso es importante la tecnología blockchain, que tiene un antecedente en la isla de Yap, en Oceanía. No hace muchos siglos, los habitantes de una tribu de esa isla no tenían monedas ni billetes, y en vez de usar las vacas o la sal, como medio de intercambio utilizaban piedras gigantes de diferentes tamaños. ¿Qué pasaba?: no se podían mover de un lugar a otro. ¿Entonces, qué hacían? Tenían un registro donde “anotaban” a quién pertenecía cada piedra. Si, por ejemplo, yo le compraba un bien a Maxi pagándole con alguna piedra, tenía que “registrar” que la piedra pasaba de mi titularidad a la de Maxi (Ver: Imagen 9).

Pero la tribu de Yap no conocía la escritura, el registro se

Como les decía, Blockchain puede ser pública, como el caso del bitcoin. Cualquiera de los nodos puede bajar un *node* entero de bitcoin. Al ser pública, o sea, no impedir el acceso a nadie, es visible por cualquier persona. Pese a

Hay también blockchain privadas con acceso limitado a la visibilidad; por ejemplo, en empresas. También existen consorcios o blockchain federadas. Un ejemplo de ello es Blockchain Federal Argentina, que es donde se registra el Boletín Oficial. Puede ser pública o privada y está limitada a un número determinado de participantes. La más importante que se conoce es la de bitcoin, que es pública y cualquiera puede acceder.

Acá tenemos los mineros de bitcoin (Ver: Imagen 10). Son esos aparatitos que se encargan de registrar las transacciones. Podemos tener una pequeña red de minería,

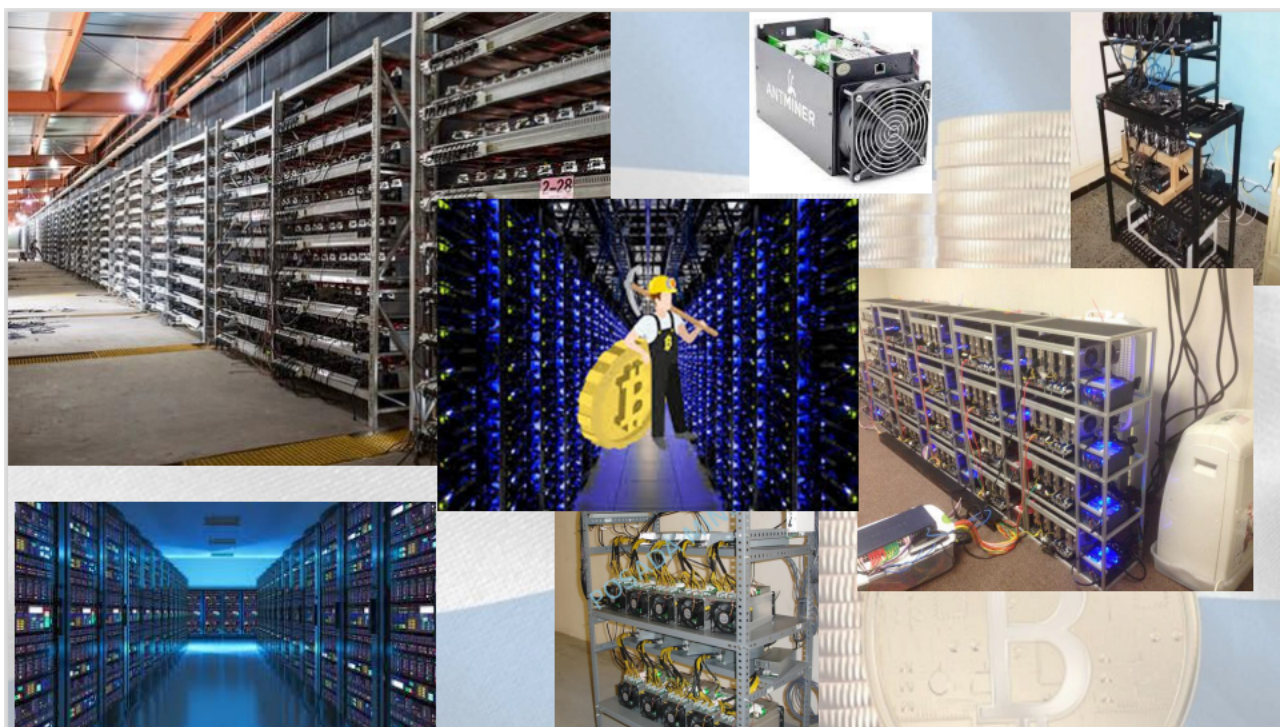


Imagen 10.

Cómo funciona la minería de Bitcoin

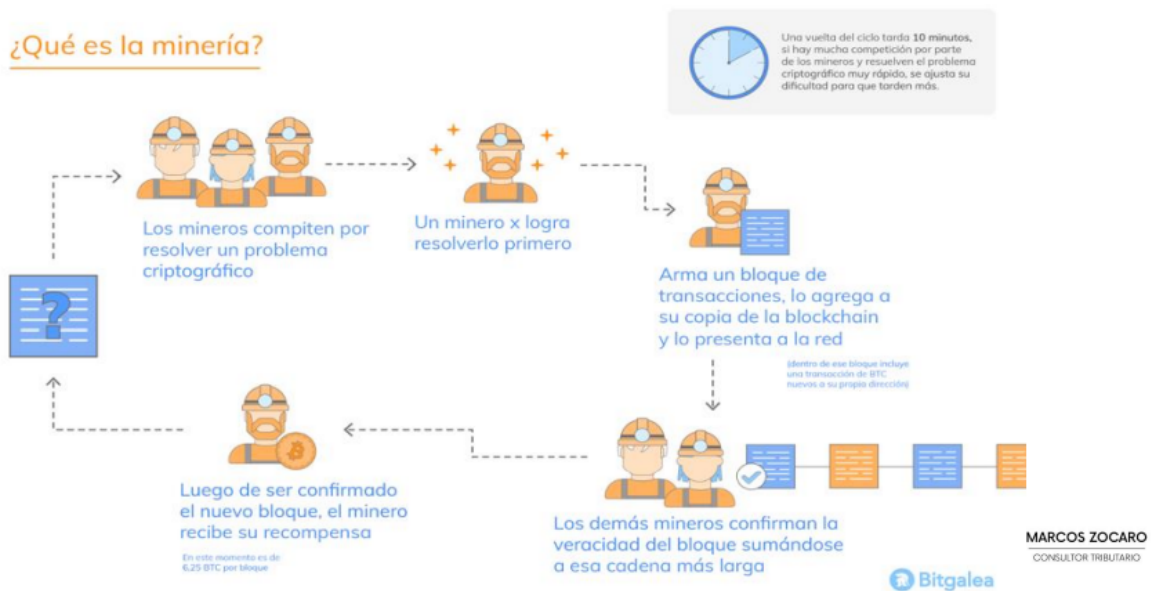


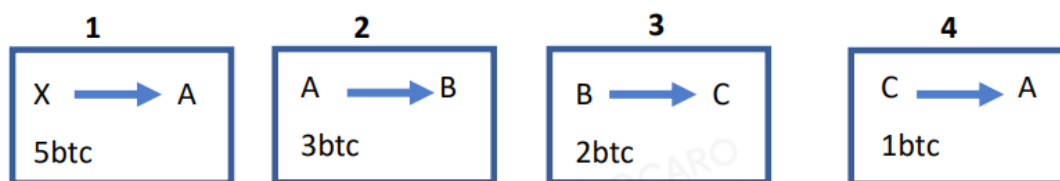
Imagen 11: Cómo funciona la minería de Bitcoin.

una pequeña granjita en nuestras casas o empresas con miles de mineros. En la Patagonia, por ejemplo, están Bit Patagonia y Bit Fan. También están llegando a Córdoba –si no me equivoco– muchas empresas grandes que tienen mineros, pero lo cierto es que cualquiera de nosotros también puede tener alguno de estos mineros en casa.

¿Cómo funciona bitcoin? (Ver: Imagen 11) Gracias a la tecnología blockchain, tenemos los mineros que están conectados a la red y que compiten entre ellos para resolver un problema matemático. Esta minería es la minería de prueba de trabajo. Para incorporar la información a la red, se necesita un mecanismo de consenso entre todos los mineros (un protocolo). En el caso de bitcoin, se utiliza la prueba de trabajo, el mecanismo más seguro. ¿Qué hace?: los mineros compiten entre sí para resolver un problema matemático; el que logra resolverlo, arma

un bloque, una hoja de la cadena de bloques del libro contable. Es una hoja con transacciones que se la muestra al resto de los mineros. Aprobado el bloque con todas las transacciones, ese minero tiene el derecho de incorporar la información a la blockchain. El minero que logró resolver el problema matemático y conformar el bloque, tiene el derecho a incorporar la información a la blockchain y a recibir recompensas en criptomonedas, pues para eso ejerce la actividad de minería.

Antes de avanzar, imaginen una transacción en la que X le quiere mandar 5 bitcoins a A. La transacción se registra y se envía a la red. Después, otra transacción: A le quiere mandar a B unos 3 bitcoin, B le quiere mandar a C 2 btc (bitcoin), y C le quiere mandar a A 1 btc. Son todas transacciones. Bitcoin no es más que el saldo contable que tiene cada persona en la red, en el libro contable. En



SALDOS:

A: 3 btc

B: 1 btc

C: 1 btc



Imagen 12.

ese sentido, A tiene 3 btc, después recibió 5 btc, después envió 3 btc y después recibió 1. A tiene 3 btc. Y si A quisiera enviar 4 btc, la red lo rechazaría, porque los mineros verifican el saldo (Ver: Imagen 12).

Bitcoin no es más que el saldo en el registro contable. B, por ejemplo, tenía 3, envió 2 y ahora le queda 1. Se pueden enviar también centavos de bitcoin. No hace falta enviar uno entero. Por cada bloque correlativo, hay miles de transacciones en cada hoja del libro. El bloque tiene un número que vendría a ser como el número de página de un libro. En el caso de bitcoin, hay alrededor de dos mil transacciones por bloque. Esto puede variar dependiendo de blockchain y de la criptomoneda que sea.

Algo que no aclaré: la blockchain de bitcoin se llama bitcoin y la blockchain de la criptomoneda ether, se llama Ethereum. En la jerga, cuando hay referencia a la cripto-

moneda, se dice *ethidium* o *etereum*. La blockchain Cardano tiene como criptomoneda, o como *token*, a Aida o Ada. Y así con cada criptomoneda que tiene su propia blockchain.

Hay criptomonedas que corren y existen en la blockchain de una criptomoneda. Por ejemplo, *Dai* es una criptomoneda, que corre sobre Ethereum, la blockchain de Ethereum. Volviendo a bitcoin, aquí tenemos un bloque con toda la información (Ver: Imagen 13). Lo importante es el número de transacciones, casi 2.000, 1809, esto se hizo el 6 de noviembre de 2021. El minero que logró incorporar este bloque en la blockchain, verificar las transacciones, que ganó la competencia al resto de los mineros, tiene dos recompensas: recompensa de bloque y recompensa de tasa.

La recompensa de tasa o de comisión en este caso son

0,07 bitcoin o dicho de otra forma, serían 7 millones 699 mil 305 centavos de bitcoin (Ver: Imagen 13). Esta recompensa de tasa es variable: es la sumatoria de todas las comisiones que pagaron esas 1809 personas. Cada una de ellas, para hacer cada transacción, pagó un *fee*; el minero ganó la totalidad de las comisiones y a su vez, ganó la recompensa del bloque, hoy es 6,25. Estos son los “bitcoins nuevos” que se emiten. Cada 10 minutos aproximadamente se confirma un bloque, se incorpora un bloque a la blockchain y se emiten 6,25 bitcoins. Así está diseñado desde el inicio.

Hoy en día, cada 10 minutos aproximadamente, con cada bloque se emiten 6,25 btc, pero no siempre es así, sino cada 4 años aproximadamente, cuando sucede el hal-

ving. El *halving* es básicamente la reducción a la mitad de la emisión. Originalmente, cuando Satoshi Nakamoto minó el primer bloque, se emitieron 50 btc por bloque. Significa que los mineros ganaban 50 btc cada vez que minaban un bloque.

Después –de vuelta de 4 años aproximadamente–, eso se reduce a la mitad. Así se redujo con el primer halving a 25 btc, después a 12,5 y hoy a 6,25. Y así se va a ir disminuyendo hasta que dentro de años no se emitan más bitcoins. Cuando se emita el bitcoin 21 millones, de vuelta tendremos escasez.

Tengan en cuenta que acá vimos el protocolo prueba de trabajo de bitcoin muy rápidamente, pero también existen otros protocolos menos seguros según la mayoría

Criptomonedas y Blockchain

Bloque

Hash	000000000000000000000000804bca44b370b70a74b036d20cb177cb71173b18c732e
Confirmaciones	1
Sello de tiempo	2021-11-06 23:24
Altura	708570
Minador	Unknown
Número de transacciones	1809
Complejidad	21.659.344.833.264.85
Raíz de merkle	c17008b675ad5d1c3040bc31690a54c95bd3fb0724eea3364257c774d990b42
Versión	0x2000e004
Bits	386.727.631
Peso	3.173.950 WU
Tamaño	1.143.481 bytes
Único	377.124.682
Volumen de transacciones	10387.19761019 BTC
Recompensa de bloque	6.25000000 BTC
Recompensa de tasa	0.07699305 BTC

Imagen 13: Criptomonedas y Blockchain.

de los expertos. Por ejemplo, el *Proof of Stake*, prueba de participación, al cual va a migrar etherium, hoy en día lo tienen las redes como por ejemplo Cardano, donde los mineros no tienen que resolver un problema matemático, sino que, básicamente varían las transacciones y los bloques de acuerdo a la participación de cada uno en la red.

Incluso acá en la foto lo vemos a Ginóbili, un *Proof of humanity*, en un sistema creado por un argentino, Santiago Siri --que vive en Europa--, para verificar la identidad de las personas y poder ver automáticamente los *ubi*, que son los *token* de la red. Solo por verificar la identidad, automáticamente te dan los *ubi*, los token de esta red, te dan esa especie de pensión básica universal. Obviamente, ya que corre por la red de Ethereum, tiene costos de

gastos y de riesgos; pero volviendo a bitcoin, todas las operaciones son visibles en la red.

Hay estafas en Twitter en nombre de famosos; por ejemplo, en el caso de la ilustración, de Obama en 2020 (Ver: Imagen 14). Todas las personas que le enviaran a esa dirección de bitcoins (que es como un CBU), por mil dólares, a "Obama" (al estafador), él les enviaría el doble en cuestión de 30 minutos. Es una estafa burda, pero si se entra a esa dirección en el momento mismo en que la estafa sucede, se podrá ver a las víctimas depositando bitcoin. Y eso, nadie lo puede detener porque es descentralizado. Efectivamente, no hay ninguna institución que pueda detener la estafa.

En fin, la billetera tuvo 378 transacciones, recibió más

Blockchain.com

Monedero

Intercambio

Explorador

Address ⓘ

Petición de pago

Botón de Donación

Estafa con robo de cuentas de Twitter 15/07/2020

Dirección	bc1qxy2kgdygjrsc
Formato	BECH32 (P2WPKH)
Transacciones	378
Total Recibidas	12.86644654 BTC
Cantidad total enviada	12.85345191 BTC
Saldo final	0.01299463 BTC

Barack Obama @BarackObama

I am giving back to my community due to Covid-19! All Bitcoin sent to my address below will be sent back doubled. If you send \$1,000, I will send back \$2,000! bc1qxy2kgdygjrsc2n0yrf2493p83kkfjhx0wih Only doing this for the next 30 minutes! Enjoy.

5:35 PM · Jul 15, 2020 · Twitter Web App

833 Retweets and comments · 1.4K Likes

Transacciones ⓘ

Hash	f8ac43a4b7d9492d499e071d951538fc54e...	3PZXptyo1RZ4yawQSQ...	0.00441612 BTC	→	bc1qxy2kgdygjrsc2n0yrf2493p83kkfjhx0wih	0.00080085 BTC	2020-07-16 05:05
					3KPqpS2RRyL19LASnc...	0.00361322 BTC	
Comisión	0.00000205 BTC (0.556 sat/B - 0.251 sat/WU - 369 bytes)						+0.00080085 BTC

Tres años de cárcel para el hacker de Twitter que promocionó estafa con bitcoin

Imagen 14: Estafa con robo de cuentas de Twitter 15/07/2020.

Herramientas de trazabilidad blockchain



Imagen 15: Herramientas de trazabilidad blockchain.

de 12 btc y el estafador, a su vez, envió más de 12 btc a otra billetera. Es posible ver el saldo final de la cuenta del estafador, la cuenta bancaria del estafado y todas las transacciones. Esas 378 transacciones explican cómo la víctima le envió btc a la dirección del estafador y cuánto pagó de comisión por cada transacción. Si ustedes entraran de vuelta a blockchain.com, o a cualquier empleador de bitcoin, podrán ver, con solo ingresar a esa dirección, las 378 transacciones (quién fue y para dónde fue).

Por eso se dice que al hacker lo terminan descubriendo, porque se encuentra quién hackeó Twitter. Por eso se dice también que bitcoin es un seudónimo. No tiene el nombre del titular, sino caracteres alfanuméricos encriptados, de ahí la criptografía y de ahí el nombre "criptomonedas".

Hay empresas como Chainalysis y Ciphertrace que son contratadas por los estados y por las grandes empresas para analizar y rastrear operaciones (Ver: Imagen 15). De esa manera, se han desbaratado bandas terroristas en Medio Oriente. Dicen que los delincuentes usan criptomonedas, pero en verdad lo último que un delincuente va a usar son las criptomonedas, porque quedan rastros por todos lados. La mayoría de los delincuentes usan efectivo.

Agregué un gráfico sobre cómo es la emisión de bitcoin deflacionaria (Ver: Imagen 16). Cada cuatro años está el *halvi*, que es cuando la emisión se reduce a la mitad. Cuando llegue, ninguno de nosotros va a estar. En ese entonces no se van a emitir más bitcoin y los mineros van a ganar, no la recompensa de bloques, ya que no se van a emitir más, sino las comisiones de la red, las comisiones

Bitcoin = deflacionario

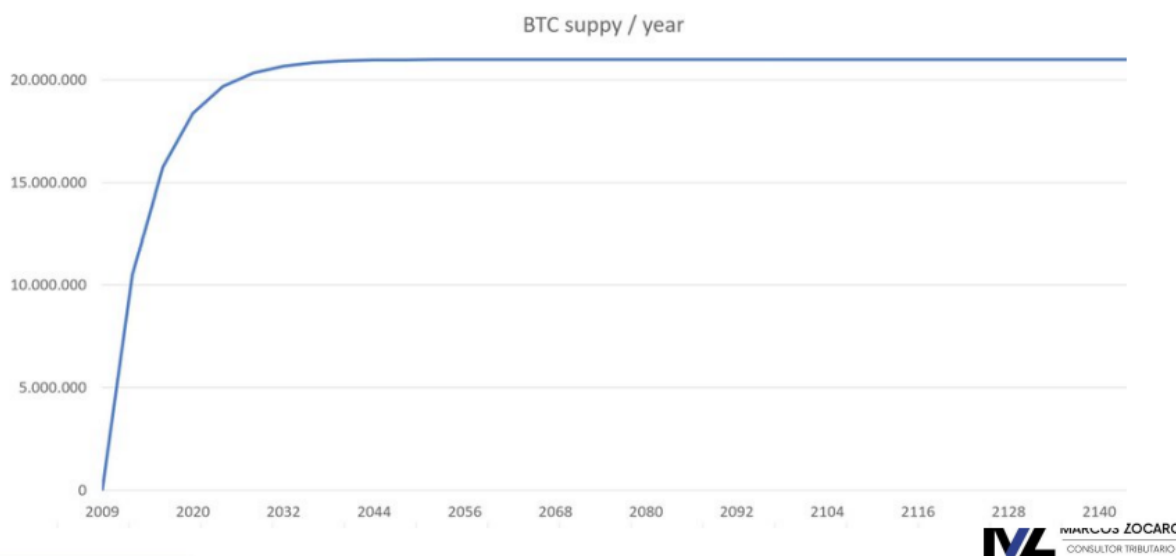


Imagen 16: Bitcoin = deflacionario

que paga cada persona para hacer transacciones.

Bitcoin, entonces, es emitida de forma descentralizada y sin intermediarios. Asimismo, por más que China prohíba la minería, en el resto del mundo se sigue minando. No puede un gobierno o una empresa bajar una perilla y acabar con la red. Justamente, la fortaleza es esa, que es un sistema descentralizado y cualquiera de nosotros puede tener una copia de la base de datos. Aparte, es imposible de falsificar. Las transacciones son pseudo-anónimas, como vimos, pero visibles en la red, y la emisión es limitada a 21 millones, como ya sabemos.

La operación de bitcoin dio inicio a nuevas criptomonedas. Con el tiempo, comenzó a desarrollarse el concepto de finanzas descentralizadas que, básicamente consiste en servicios financieros sin intermediarios, sin bancos, ni el central siquiera, ni bancos privados, sino con contratos inteligentes (smart contracts).

¿Cuáles son las formas principales de adquisición? Se pueden comprar directamente a través de un exchange o broker –en Argentina hay muchos–. Ese fue el espíritu

de Sashimi Nakamoto: poder hacer la compra directamente, cara a cara. Me junto con Maxi, le doy plata y Maxi me transfiere las criptomonedas. También se puede hacer para la prestación de servicios, incluso para pagar salarios en criptomonedas hasta un 20%.

La operación de bitcoin dio inicio a nuevas criptomonedas. Con el tiempo, comenzó a desarrollarse el concepto de finanzas descentralizadas que, básicamente consiste en servicios

financieros sin intermediarios, sin bancos, ni el central siquiera, ni bancos privados, sino con contratos inteligentes (*smart contracts*).

¿Qué es un contrato inteligente? Es un contrato que se autoejecuta. Por ejemplo: compré un boleto para viajar en avión, y el avión se retrasa cuatro horas. Debería reclamar una compensación que, en el mejor de los casos, tardaría años en llegarme. Un *smart contracts* metido en el medio de esa situación, ¿qué haría? Por ejemplo: verificaría la existencia efectiva de la demora que el reclamo menciona y, no importa por qué –si depende de la agencia de viajes, de la aerolínea o de mí–, pero automáticamente me compensaría depositándome criptomonedas. Un contrato inteligente es autoejecutable.

La principal red donde se desarrollan estas finanzas descentralizadas es en Ethereum. Hay otras en crecimiento, como Solana y Matic. También está desde hace años la red Cardano, una red blockchain para contratos inteligentes.

Tenemos, entonces, las monedas emitidas por los bancos centrales, como el peso, la libra, el euro, el yuan; tenemos finanzas descentralizadas; tenemos monedas estables algorítmicas, como la dai; tenemos el banco central europeo y la Fed norteamericana; tenemos la dai como *money exchange*. Y así, cada servicio financiero tradicional puede migrar el día de mañana a finanzas descentralizadas abaratando costos y obteniendo mayores ganancias.



Diploma de Posgrado en Gestión Integral
de Empresas Industriales y de Servicios
[https:// bit.ly/3Ffb5s0](https://bit.ly/3Ffb5s0)

PREGUNTAS DEL AUDITORIO

Maximiliano Pérez: Perfecto Marcos, impresionante. Vamos a aprovechar este espacio para hacer algunas preguntas que tienen que ver con la dinámica cotidiana de las blockchain y de las criptomonedas.

Para personas que prestan sus servicios a otros países, cuáles son las implicaciones a nivel impositivo que tienen las operaciones con criptomonedas (AFIP, Ingresos Brutos).

Marcos Zocaro: Para cobros desde el exterior, habría que evaluar las implicancias cambiarias, pero se trata de exportación, por ende, se pagaría IVA alcanzable y cuota cero de Ingresos Brutos. La gran mayoría de las provincias tampoco pagan Ingresos Brutos porque es exportación.

Te repito que hay que evaluar las cuestiones cambiarias, pero es más eficiente, rápido y económico: la resolución se hace en 5 segundos y no se paga comisión por intermediario. Por el sistema bancario, en cambio, recibís una transferencia, vas en persona al banco, firmás papeles, presentás facturas, esperás alrededor de diez días para que Comercio Exterior del Banco no ponga reparos, apruebe la transacción y te liquide las divisas al cambio oficial. Todo puede demorar dos semanas y encima el banco te cobra una comisión bastante elevada por operar.

Maximiliano Pérez: ¿Hay que facturar?

Marcos Zocaro: Sí, hay que hacer una factura, no evadir.

Maximiliano Pérez: Perfecto. También te pregunto por las tarjetas de crédito en relación a las criptomonedas.

Marcos Zocaro: Las tarjetas son de débito y prepagas lanzadas por empresas como Argentinas Lemon y otras. Se pueden recargar con criptomonedas y cualquier negocio que tenga un postnet y que acepte Mastercard o Visa puede aceptarlas. Ejemplo: compro algo en el supermercado de la esquina que tiene un postnet normal e informo que pagaré con, por ejemplo, bitcoin. Lo que

hace la empresa cuando la tarjeta ya fue tomada por el postnet es cambiar automáticamente esas criptomonedas por pesos. Puedo usar las criptomonedas para hacer compras y los comerciantes reciben pesos, no reciben criptomonedas. La transformación se hace automáticamente.

Hoy en día, la mayoría de estas tarjetas están dando un *cashback* (una promoción que por cada consumo se devuelven el 2% en criptomonedas). Es más, se puede no comprar criptomonedas, se fondea la tarjeta con pesos –como si fuese la Uala–, y se devuelve el 2% en criptomonedas. Por eso tanta gente en el mundo tiene su tarjeta en criptomonedas.

Maximiliano Pérez: Las criptomonedas pueden pegar saltos (tocar el techo o caerse al piso). Por ejemplo: en el contexto de la guerra de Rusia a Ucrania hay gran volatilidad entre las distintas criptomonedas, pero hay otras que parecen ser un poco más estables, las *stablecoin* (monedas estables).

Marcos Zocaro: Hay diferentes tipos de monedas estables, algunas más seguras que otras. Básicamente, son estables en referencia a uno de los activos que más se utiliza (el dólar). Pero tenemos las que valen siempre un dólar. Dai también es una moneda estable, es emitida en forma algorítmica y vale siempre un dólar. Usdt es una empresa que emite usdt, y por cada usdt que emite dice tener como respaldo desde depósitos bancarios hasta títulos de deuda; eso significa que tiene respaldo financiero, no es descentralizada como bitcoin. En ese caso, el día de mañana, la empresa puede cerrar o tener un faltante de respaldo; pero aun así, usdt es de las *stablecoin* y de las más usadas hoy. Hay muchas otras. Binance también es estable con respecto al activo más utilizado (el dólar).

Maximiliano Pérez: Marcos: una persona que quiere empezar a acercarse al mundo de criptomonedas, ¿qué se le puede recomendar? Por ejemplo: ¿que arranque por

las monedas estables o depende de para qué las quiere?

Marcos Zocaro: Depende de cada caso y de para qué lo quiere. Por mi parte, siempre voy a recomendar bitcoin, la mejor. Pero vamos a suponer un caso: necesitas hacer un pago para una operación importante (de salud, o de la vivienda) el mes que viene. Es bueno invertir hoy un arqueo volátil, porque dentro de un mes necesitarás ese monto sí o sí. Es riesgoso el asunto. Entonces, te conviene algo estable. Pero si es dinero que no te importa si baja en el cortísimo plazo, es otra historia...

Maximiliano Pérez: En la Argentina, ¿están reguladas las criptomonedas, o cambia de provincia a provincia?

Marcos Zocaro: A nivel nacional, esto da para tres charlas más. A nivel provincial, hay Ingresos Brutos diferentes en cada provincia. El impuesto es el mismo, pero cada una puede determinar un imponible diferencial.

Maximiliano Pérez: Por mi parte, Marcos, te agradezco muchísimo, fue una charla realmente enriquecedora. Marcaste los puntos fundamentales del tema. Obviamente, cada uno de nosotros tendrá que ir avanzando con lecturas y prácticas, pero las ideas quedaron claras y sembradas. De vuelta: gracias por tu tiempo y por la exposición.

Marcos Zocaro: Muchísimas gracias por la invitación a vos y a la Universidad.

Maximiliano Pérez: Nos despedimos, entonces, agradeciendo la participación de ustedes. Este Diploma de posgrado tiene como eje fundamental formar gerentes; por eso, a los efectos de contar con una visión integral del negocio, nos pareció súper interesante incorporar el tema de la criptomoneda.



Diploma de Posgrado en Gestión Integral
de Empresas Industriales y de Servicios

<https://bit.ly/3Ffb5s0>