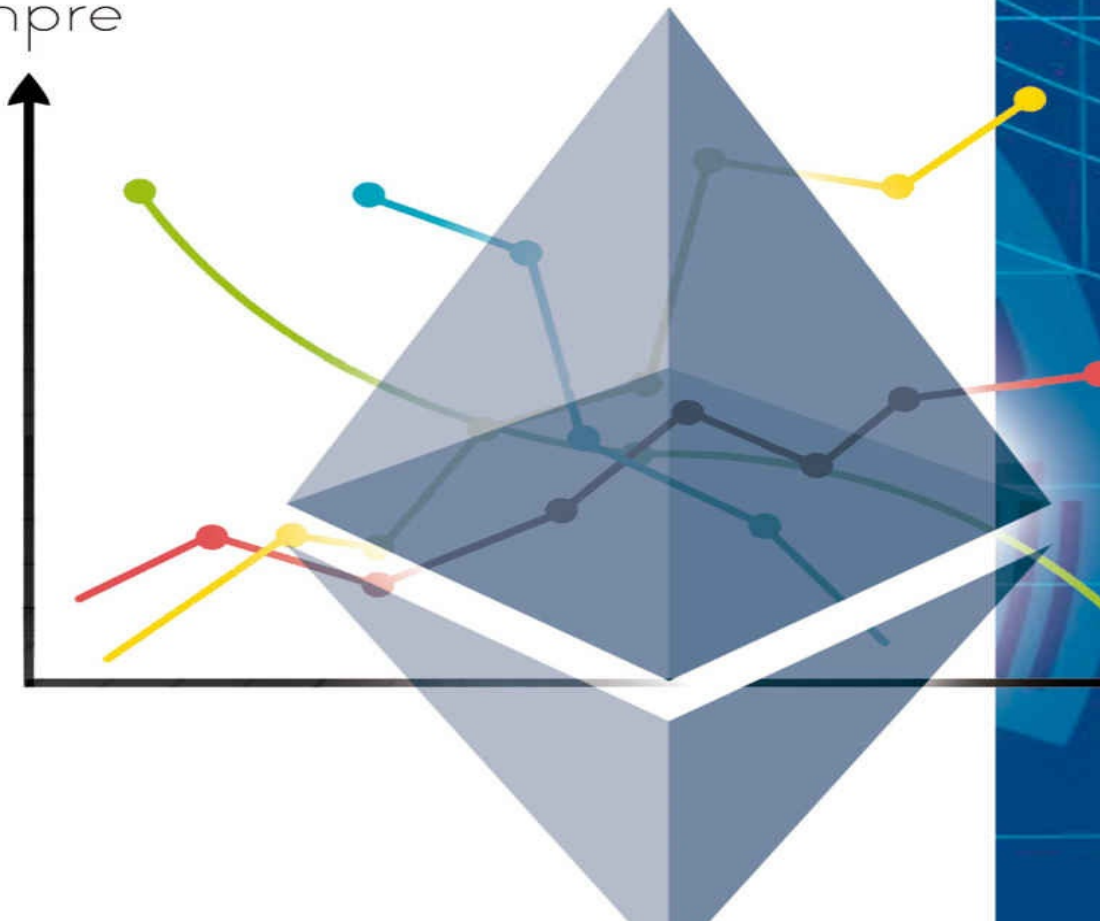
bubok
EDITORIAL

Miguel Caballero
Arnau Ramió
Marcos Carrera

# FINANZAS DESCENTRALIZADAS PARA INQUIETOS

## Cómo Blockchain y las DeFi han cambiado la industria financiera para siempre



# FINANZAS DESCENTRALIZADAS PARA INQUIETOS

Miguel Caballero
Arnau Ramió
Marcos Carrera

bubok
EDITORIAL

Miguel Caballero
Arnau Ramió
Marcos Carrera

# FINANZAS DESCENTRALIZADAS PARA INQUIETOS

## Cómo Blockchain y las DeFi han cambiado la industria financiera para siempre

Diciembre 2020

ISBN papel: 978-84-685-5457-0
ISBN ePub: 978-84-685-5458-7

Editado por Bubok Publishing S.L.
equipo@bubok.com
Tel: 912904490
C/Vizcaya, 6
28045 Madrid

*No creo que volvamos a tener alguna vez una buena moneda antes de sacar el tema de manos del gobierno, es decir, no podemos arrancárselo con violencia, lo único que podemos hacer es introducir algo de alguna forma taimada e indirecta que [el gobierno] no pueda detener.*

Friederich Hayek, 1984

*EE. UU. ha impreso más dinero en un mes que en dos siglos: con ese primer trillón de dólares que la FED acaba de emitir derrotamos a los imperialistas británicos, compramos Alaska y la Compra de Luisiana, derrotamos al fascismo, terminamos con la Gran Depresión, construimos el Sistema de Autopistas Interestatales y fuimos a la Luna.*

Dan Morehead, CEO Pantera Capital, 2020

¿Me preguntas si podremos tener una blockchain *interplanetaria en unas décadas, tras colonizar Marte y con la civilización humana asentada en la luna, para transferir valor y crear economías con monedas que no dependan de Estados? Es evidente que sí. Tan solo tendremos que forkear y modificar ligeramente Bitcoin para transmitir bloques más despacio.*

Adam Back en *Lightnite Show*, con Carlos Roldán
y Miguel Caballero, 2020

*La cotización de la acción del Banco Santander, a octubre de 2020, ha caído a los mismos niveles que en 1987. Ha sido un banco fundamental en el pasado, con más de 150 años de historia, pero… ¿de verdad creemos que representará a la banca del futuro?*

Miguel Caballero, hoy

# Índice

# AGRADECIMIENTOS

Escribir un libro es una tarea compleja. Lograr un segundo libro cuando tu actividad principal no es la escritura solo es posible si cuentas con ayuda e inspiración de tus círculos de confianza.

Mi abuelo Pepe me grabó con fuego aquello de «Es de bien nacido el ser agradecido», así que aquí van mis agradecimientos:

Gracias a mi mujer, Carmen; mi fuente de inspiración, de la que bebo a diario. A mis hijos Clara y Nacho, por hacerme feliz. A mis padres, Pilar y Paco, por haberme hecho ser quien soy y porque, en el fondo, les debo todo.

Gracias a los tutellianos de todas las promociones. Ya vamos por quince ediciones; gracias a todos vosotros nos inspiramos cada día para seguir aprendiendo. Gracias también a todos los que habéis aprendido (o enseñado) alguna vez en Tutellus, porque vosotros también sois tutellianos. Y gracias tanto a los que leísteis mi primer libro como a los que escucháis mi pódcast *Blockchain para inquietos*. ¡Que el ritmo no pare!

Gracias a mis socios y compañeros de aventuras de los diferentes proyectos en los que tengo el honor de participar: al eterno joven Javi Ortiz, alias el Sokar, con quien empecé Tutellus hace ya siete años; a mis compañeros tutellianos y *escritores* Arnau Ramió y Marcos Carrera, con quienes comparto y aprendo cada día; a toda la gente envuelta en mis últimos criptolanzamientos y colaboraciones (Criptokuántica, RentalT, Potestas Know) y muy especialmente a Turin Labs, con quienes, junto a Carlos Roldán y Carlos Borlado (de Satoshis Games) lanzamos productos de DeFi sobre Bitcoin pioneros en el mundo.

Y gracias al entorno cripto, que me inspira directamente a intentar ser mejor cada día: desde la comunidad de CryptoPlaza capitaneada por el gran Jesús Pérez y Marcela Carvajal hasta los amigos del sector y seguidores en redes. Espero seguir contribuyendo cada día, con mi humilde granito de arena, en hacer del mundo un lugar mejor.

Miguel Caballero

Siempre había tenido claro que quería publicar un libro, aunque nunca pensé que sería ni tan pronto ni sobre este tema. Aunque bueno, aquí estoy, y con ello siento que todo lo que voy consiguiendo es en parte gracias a las personas que me rodean y que han influido en mi vida. Ahora es el momento de agradecerles.

Gracias a mis padres, por confiar en mí en todo momento, incluso cuando nadie más lo hacía. A mis hermanos, por hacerme tan feliz y servirme de motivación para seguir creciendo. Y a mi familia, en especial a mis dos tíos, que junto a mi padre me han inspirado con su estilo de vida y pasión por el trabajo.

Gracias a mi grupo de amigos, por todas las experiencias que he vivido con ellos y porque se preocupan no solo de disfrutar sino también de mejorar cada día. En especial, a Raimon y Juan, quienes me introdujeron inicialmente al Bitcoin en un momento en que no entendía nada. Fue con ellos que abrí los ojos y descubrí un mundo que no quería dejar ir.

Gracias a todos mis compañeros de aventuras profesionales; a Giacomo, Marco y Marc por formarme y enseñarme. Gracias también a Rai y a Dani por confiar en mí en este último proyecto que empezamos, siempre con entusiasmo e ilusión. No podía faltar Marcos Carrera, amigo y compañero de libro, por las risas del día a día y por sus constantes consejos que me ayudan a mejorar.

A Nicolas Barilari y Nestor Kresmer, amigos y socios de un gran proyecto; Criptokuántica. A los miembros de Crypto Plaza, en especial a Jesús Perez, que sin él darse mucha cuenta ha sido mi gran inspiración para entrar con todo en el mundo DeFi.

Y, sobre todo, gracias a Miguel Caballero y a Javi *Sokar* Ortiz por confiar en mí y darme la oportunidad de participar en la que creo que es una de las empresas cripto más relevantes y con perspectiva de futuro de España. Estoy orgulloso del equipo que me rodea, no tengo dudas de que sacaremos algo muy interesante dentro de este ecosistema.

No podías faltar tú, lector. Gracias por tomarte el tiempo de leer el libro y por confiar en nosotros como fuente de conocimiento para aprender sobre Bitcoin y DeFi.

Y, para acabar, creo que me toca. Quiero agradecerme a mí. Por mi entusiasmo y ganas de aprender, por no rendirme, por seguir siempre lo que dice mi corazón sin importar las opiniones de los demás, por pedirme más continuamente, por cuidar y valorar las relaciones que tengo en mi vida y, por encima de todo, por hacer siempre las cosas a mi manera. Sigue así.

Arnau Ramió

Agradecido a ti, ¡lector inquieto! Este ecosistema solo y exclusivamente crecerá si tú crees en él y si lo compartes con otras personas inquietas.

Soy un firme creyente de que el triunfo en la vida se debe al éxito emocional, que puede llevar al logro profesional. Estoy seguro de que la libertad que genera DeFi podrá hacerte un poco más feliz, podrá empujarte a sentirte victorioso. Recuerda que el éxito es una sensación subjetiva, que no dependes de terceras personas para generarla. Así que, ya solo por haber dado este paso, siéntete orgulloso de ti mismo.

Agradezco mucho y mucho a mis compis Miguel y Javier, quienes me apadrinaron y convirtieron. Gracias también a Arnau, por ser una pila constante de conocimiento.

También agradezco a mis padres y a mi hermanote Sergio el haberme dado la oportunidad de pensar con libertad, de no juzgar mis ideas locas ni hacerme sentir juzgado mientras me acompañaban en el camino para ayudarme a levantar, por si me cayera. Lo extiendo al resto de mi familia, a los que están y a los que ya no están. Es fundamental rodearse de gente que siempre quiera sumarte.

A Alaminos, con quien escribí mi primer libro hace ya dos años, y me inspiró a seguir escribiendo una página nueva cada día de aquello de lo que quiero compartir. Muchas gracias, María José, por estar siempre conmigo en esta y otras aventuras.

También a Alberto Bernat por su paciencia y conocimiento, y por supuesto a mis amigos y círculo de amistades más cercano: Edu, Ramón, Marcos, Rubén, Beatriz, Talayer, Tiniyer y Skaleguer. ¡Y a mi gata Frida!

Marcos Carrera

# PRÓLOGO

## Seguimos creando ecosistema

Por Miguel Caballero

Hace poco más de un año terminaba de publicar mi primer libro: *Bitcoin, blockchain y tokenización para inquietos*. Tuve la necesidad de contar muchas cosas en un formato fresco y ligero, y el resultado fue un libro —quizás— demasiado superficial. De cualquier forma, su objetivo era atraer talento al ecosistema cripto y que la gente perdiese el miedo a aprender sobre Blockchain, por lo que creo que el objetivo se ha conseguido: la aceptación por parte de los lectores fue maravillosa, y mi libro llegó a estar durante una semana en el top de ventas de Amazon. Verlo rankeado varios días seguidos en primera posición, por encima de *Padre rico, padre pobre* (uno de los libros de cabecera que cualquiera debería leer), me llenó de orgullo y satisfacción y sencillamente no me lo podía creer.

Sin embargo, quedaron muchas cosas por contar. Este 2020 ha sido un año de locos en todos los sentidos, no solo por la COVID-19, sino por la explosión y crecimiento exponencial que han tenido las Finanzas Descentralizadas o DeFi (Decentraliced Finance). De ser un ecosistema de frikis a principios de año, moviendo unos pocos cientos de millones de USD, a superar la barrera de los 12 000 MUSD bloqueados en protocolos DeFi durante octubre; un ecosistema donde la mayoría está por ganar dinero en el corto plazo, pero algunos nos hemos percatado de cómo esta nueva tecnología nos abre un mundo de posibilidades que hasta ahora, incluso para los más tecnófilos, nos sonaba a ciencia ficción.

¿Es posible vivir sin bancos en países desarrollados? ¿Podemos crear nuestros propios productos financieros y obtener atractivas rentabilidades? ¿Debemos centrar nuestro patrimonio y, en definitiva, nuestra economía alrededor de las DeFi? ¿Qué riesgos (y oportunidades) conllevan estas decisiones?

A estas preguntas, querido lector, trataremos de hallar respuestas en este libro. Nosotros te daremos las herramientas y tuyas serán las conclusiones. Pero lo que parece evidente es que el mundo ha cambiado y, como aquella canción de El canto del Loco: *Ya nada volverá a ser como antes*.

Y no me refiero tan solo al efecto COVID; me muevo en un marco mucho más amplio. Las políticas económicas y monetarias de Occidente tienen los días

contados. El sistema económico mundial ha colapsado, es un anciano moribundo que en cualquier momento se desploma, y la única razón por la que no lo hace es por la continua inyección de liquidez que le hacen los bancos centrales: más y más dinero, cada año, cada mes, cada semana, cada día. Este modelo de políticas monetarias es insostenible porque hacen al ciudadano, cada día, más pobre. Y llegará un momento que el sistema tenga que cambiar si no queremos sufrir una revolución como la francesa durante 1789, porque vamos por el mismo camino. Al igual que no se puede impedir que el bitcoin alcance el precio de USD 1 000 000 (es tan solo cuestión de tiempo), es imposible evitar que el actual sistema colapse.

En Tutellus estamos poniendo nuestro granito de arena, desde 2016, para que la gente conozca qué es Blockchain y cómo puede ayudar a mejorar sus vidas. Por nuestra plataforma online han pasado ya cerca de cien mil personas haciendo cursos de esta temática; por nuestros programas presenciales o intensivos (bootcamps), cerca de trescientos alumnos.

En 2017 lanzamos el primer token educativo del mundo (TUT), viviendo todos los momentos que te puedas imaginar, acompasados al mercado: euforia, impotencia, hundimiento, recuperación y nuevas innovaciones.

Hemos creado más de diez empresas junto a alumnos de distintas promociones y lanzado más de treinta proyectos al mercado (presentados en Demo Days); hemos creado un fondo descentralizado de inversión en criptoactivos (Tutellus Fund) bajo un protocolo DeFi en el que cualquiera puede invertir, hemos lanzado el primer equity tokenizado sobre Bitcoin del mundo (Turin Labs con el TURIN token) y una plataforma de inversión en inmuebles tokenizados (RentalT); otra para tokenizar activos ubicados en Latinoamérica con tokens líquidos (Criptokuántica) y otra para la gestión tokenizada de las prácticas laborales de universitarios (Potestas Know). En 2019 publiqué uno de los libros más leídos en español de la industria cripto, y ahora escribimos uno nuevo (Arnau Ramió, Marcos Carrera y un humilde servidor) para seguir demostrando con el *learning by doing* que nuestra industria está abierta a todos, y que no debemos tener prejuicios en función de nuestra formación, experiencia laboral o sector de actividad.

Con este humilde libro, querido lector, te traemos herramientas para que puedas salirte de esta espiral sin sentido basada en «la economía en manos de los Estados», y aprendas así a organizar, sin depender de nadie, tus finanzas, tus ahorros y tu patrimonio. Te demostraremos que no solo es posible, sino

altamente probable que, en unos pocos años, el ciudadano de a pie, incluso el no bancarizado, comience a utilizar este tipo de servicios en su día a día.

Y es la última razón que hay detrás de estos planteamientos es muy sencilla y, a la vez, apasionante: las personas buscamos la felicidad. Hemos nacido para disfrutar de la vida y, aunque a veces suframos, la mayor cualidad que tenemos como especie es la consciencia de poder ser felices. Nacemos, vivimos y morimos para ser felices.

Y para ser feliz hay que ser libre.

Las DeFi, Bitcoin y las blockchains públicas nos ayudan a ser más libres, a evitar seguir encadenados a las órdenes del poder. Aunque resulte paradójico, las cadenas de Blockchain nos ayudan a desencadenarnos del sistema. Pongamos nuestro granito de arena para ayudarte a encontrar el camino hacia esta libertad y felicidad.

Comencemos.

# Mi primer contacto

Por Arnau Ramió

Como muchos en el espacio cripto, mi primer contacto con Bitcoin llegó demasiado pronto, tanto que no le di la importancia que merecía. Me acuerdo perfectamente cómo en la cena de Navidad de 2013: mi tío me habló de una moneda digital que «no paraba de subir». En aquel momento yo tenía 15 años, mucha inmadurez y poca atención como para ver el trasfondo de esa moneda digital. Para aquellos que hayan vivido una situación similar, empatizo con vuestras reflexiones de medianoche: «¿Y si hubiera comprado en aquel momento?».

No fue hasta finales del 2017 cuando volví a coincidir con Bitcoin, y esta vez para engancharme completamente. Un amigo me propuso invertir en él, aunque mi conexión plena llegó gracias a un chico de León que me contagió su entusiasmo. Por primera vez vi que una persona *amaba* Bitcoin no porque pudiera ganar dinero, sino porque creía en lo que representaba, veía en él una revolución, algo que cambiaría el mundo. En cinco minutos de charla quedé enamorado para siempre.

Desde aquel momento, mi vida pasó a moverse alrededor de Bitcoin. Me leí y estudié todo lo que encontraba del tema, desde Antonopoulos a *El patrón Bitcoin*. Quería saberlo todo y comprenderlo bien. Esta curiosidad loca me llevó finalmente a cursar la segunda promoción del Máster en Blockchain de Tutellus. Desde febrero de 2019 cogía un tren cada viernes de Barcelona a Madrid para formarme en algo que nadie parecía entender realmente. Era el mejor día de la semana, allí me sentía como en casa. Había dado con gente con quien podía compartir mi entusiasmo por Bitcoin y Blockchain, aunque todavía sabía poco. Quizá fue gracias a eso que, meses después de terminar la formación, empecé a trabajar en la empresa. Ahora, un año después, puedo mirar atrás y comprobar que fue de las mejores decisiones que he tomado.

Enero de 2020 también fue un momento importante en mi recorrido cripto. Con Tutellus, estábamos trabajando ya en algunos de los proyectos más innovadores de Europa en cuanto a tokenización de activos, pero es que además estábamos siguiendo en primera persona el nacimiento de las Finanzas Descentralizadas o DeFi. Por aquel entonces, las DeFi acumulaban poco más de 150 MUSD, y la mayoría eran protocolos que nadie utilizaba; aunque también había algo en el ambiente que te decía que esto era revolucionario, que era cuestión de tiempo. Desde el minuto uno me tiré a la piscina; me leí cada

whitepaper de cada protocolo, los empecé a usar, a mover mis criptoactivos por todas partes y a buscar todo tipo de estrategias de inversión. Casi un año después, las DeFi acumulan más de 13 000 MUSD bloqueados y es seguramente el ecosistema más relevante en Blockchain.

Creo que la mayoría de la gente entra en contacto con este mundo por motivos especulativos, sobre todo justo antes de un ciclo alcista. De los que entran, una pequeña parte se queda porque ha llegado a comprender la tecnología y el trasfondo del mundo cripto. Espero que este libro tenga el mismo efecto contigo, querido lector.

En las próximas páginas te verás inmerso en un mundo apasionante, desde Bitcoin a Ethereum y, finalmente, profundizando en DeFi y estrategias de carteras de inversión. Te aseguro que en algún momento llegarás al punto de pensar que te va a estallar la cabeza, pero te aseguro que, al acabar, entenderás que Bitcoin ha llegado para quedarse, y que lo que se está construyendo sobre Blockchain cambiará el mundo como pocas tecnologías lo han hecho nunca. Con esto espero que te sientas afortunado de poder participar en los años iniciales de esta revolución. Y, quién sabe, acabes siendo uno de los protagonistas. Esto es solo el principio.

# SuperAcción: porque superarte es hacer una acción mejor que la anterior

Por Marcos Carrera

Sin duda, 2020 ha sido y está siendo la ratificación de muchas tendencias que ya se estaban cocinando a fuego lento. Me refiero a modelos de negocio y de generación de valor que ya estaban obsoletos o zombies. Ha tenido que venir una fuerza mayor, como una pandemia global, para darnos cuenta de que hay líneas rojas y elementos básicos sin los cuales no existirá progreso en las empresas y en la sociedad: libertad digital, conservación de los ahorros y del patrimonio, transparencia de los modelos, etc., y, fundamentalmente, modelos de confianza.

¿Y por qué hablo de confianza? Porque el ser humano necesita ver para creer, necesita que las cosas sean sencillas, evitar fricciones que generen una pérdida de interés. Necesitamos modelos de negocio y organizaciones transparentes, sin partes oscuras en una transacción, sin partes difusas en comisiones de compra-venta, sin propiedad del dato por parte del usuario.

Quizás en el modelo de negocio bancario también ha sucedido esto: una erosión de la confianza por parte del cliente, e incluso una falta de comprensión de por qué, para un organismo central o gubernamental, tenía prioridad una entidad bancaria frente al ciudadano (que es realmente la unidad de ahorro).

Cierto es que el entorno bancario ha hecho un esfuerzo de frescura y digitalización para acercarse mejor a un cliente distinto, con carácter milenial, para ofrecerle velocidad y usabilidad, pero quizás haya sido tarde.

En este punto y no por casualidad, Blockchain viene a sustituir modelos de negocio que ya no aportan valor al usuario. Y es que Blockchain es más, mucho más que el Internet del valor. Es la nueva referencia para todas las empresas, marcas y organizaciones.

Como en aquel momento, allá por el 2000, aquella empresa que no tuviera una web no existía, ahora en 2020, aquella empresa que no sea digital, con un modelo de negocio en base digital, no existe. Y en menos de cinco años, la empresa digital que no use blockchains (bien como medio de pago, bien aplicando tokenomics), no tendrá sitio en el mercado. ¡No hay vuelta atrás!

Mi reflexión, por tanto, es que empieces desde hoy a tener algo más de cultura financiera DeFi. Y no te hablo solo de rentabilidad y análisis de inversiones, sino de entender, desde una visión más global, qué significa el dinero y el valor, de entender qué propósito tiene tu empresa ¿Crea o destruye valor? O quizás lo transforma..., como la energía.

Y entender que somos partes activas de la sociedad, que esta no cambiará si no cambiamos nosotros de manera individual.

Termino haciéndote una petición: conviértete en un criptobeliever, sé parte activa de este ecosistema de valor, hazte embajador de un cambio de paradigma donde todos tenemos la posibilidad de aportar nuestra visión, aunque sea desde una perspectiva lejana a lo técnico.

Blockchain no es solo para programadores, Blockchain **es para inquietos**; así que espero haberte generado inquietud al final de estas páginas.

# GLOSARIO DE TÉRMINOS DEFI

Creado de forma altruista y descentralizada por los alumnos de la 13ª edición del Bootcamp en DeFi de Tutellus (ordenados alfabéticamente)

| **Término** | **Descripción** | **Alumno** |
|---|---|---|
| AML | Anti-money laundering (prevención de blanqueo de capitales). Es un método que se utiliza para aclarar la procedencia del dinero de un inversor. | Saül Salcedo |
| 2FA | 2 factor authentification. Verificación a través de la cual el sistema comprueba con un segundo método el acceso a un elemento protegido (cuenta exchange/wallet) | Alejandro San Nicolás |
| Apalancamiento - Leverage | Relación entre el capital propio y el invertido en operaciones financieras. Por capital invertido se entiende capital propio más el crédito recibido. | Nicolás Barilari |
| AMM | Automated market maker. Se llama así a los creadores de mercados automáticos (pools de liquidez) como Uniswap. | Nicolás Barilari |
| Asset | Activo. Cualquier bien (ya sea del mundo digital o del mundo físico) con capacidad para ser tokenizado, y que tenga interés o valor para los demás. | Nicolás Barilari |
| Atomic loans | Empresa centrada en la creación de préstamos en stablecoins respaldados por Bitcoin sin custodia. | José Luis Lorente |
| AuM | Assets under management. Valor de mercado total de los activos e inversiones gestionados por un inversor, entidad o fondo en nombre de sus clientes. | Sergi Nieves |
| Blockchain | Registro donde, para cada uno de sus bloques, se almacena una serie de transacciones únicas, así como información concerniente a dicho bloque y su relación unívoca con los bloques precedente y | José Manuel Flomesta |

| | | |
|---|---|---|
| | posterior. Dicha relación se establece por medio del hash. | |
| Barbell | Se trata de dividir la cartera de inversión en dos partes: una, con un riesgo muy reducido, sin volatilidad; y la otra, con un nivel de riesgo elevado, aunque siempre dentro de cierta ponderación, sin arriesgar en exceso. | José Manuel Flomesta |
| Bonding curve | Curva matemática que establece una relación positiva directa entre el precio de un token y su oferta (supply), actuando como un automated market maker (AMM). De esta manera, el precio del token aumenta automáticamente cuando hay una compra, y disminuye al haber una venta, y los tokens son destruidos. | Sergi Nieves |
| Bot | Programa informático que efectúa automáticamente tareas repetitivas a través de Internet. Puede estar diseñado en cualquier lenguaje de programación, funcionar en un servidor o en un cliente. | Enric Martínez |
| Bóveda | Antiguamente conocida como CDP (posición de deuda colateralizada), es un smart contract donde depositas un colateral y tienes a cambio derecho a generar un préstamo contra dicho colateral. | Miguel Caballero |
| CeFi | Centralized finance. Hace referencia al mercado de finanzas donde las operaciones están custodiadas por un tercero (normalmente una empresa), en oposición a DeFi (Decentralized Finance). | José Manuel Flomesta |
| Clave privada | Clave que permite la total propiedad y manejo de un wallet (monedero de criptomonedas). | Enric Martínez |
| Clave pública | Identificador de una cuenta de Blockchain. Es como el número de una cuenta bancaria o el nombre de usuario de cualquier cuenta de una página web. Cualquier persona puede tener esta | Enric Martínez |

| | | |
|---|---|---|
| | información, pero para acceder necesita la clave privada. | |
| Colateralizar | Aportar una cantidad de criptomonedas como fondo de reserva para pedir un préstamo. | Mariano Rubio |
| DAO | Organización autónoma descentralizada. Se trata de una nueva forma de asociar los intereses de los participantes en un proyecto, cambiando la gobernanza centralizada habitual (en una empresa, CEO o similar) a un conjunto de smart contracts gobernados por token holders. | José Luis Lorente |
| DeFi | Conjunto de aplicaciones y protocolos que permiten generar productos y servicios financieros sin la necesidad de un intermediario o agente mediador. | Miguel Caballero |
| Derivados | Producto financiero cuyo valor depende de otro activo. En DeFi existe la versión tokenizada de los derivados a través de los assets sintéticos. | Miguel Caballero |
| Desarrolladores | Profesionales dedicados a implementar software de aplicaciones o de sistemas. Cualquier aplicación que utilicemos ha sido programada por desarrolladores. | José Luis Lorente |
| DEX | Mercado de criptodivisas descentralizado (decentralized exchange). Aplicación descentralizada que se ejecuta en una blockchain específica. | Enric Martínez |
| Dificultad de minado | Dato utilizado para aumentar o disminuir la complejidad de la minería de bloques. Si la dificultad es alta, se necesita más poder de cómputo para extraer la misma cantidad de bloques y la red es más segura. | José Luis Lorente |
| | Prueba de participación delegada. Protocolo de consenso diseñado para blockchains altamente escalables. Los participantes de la red eligen, por votación, «delegados» que permiten implementar | |

| | | |
|---|---|---|
| DPOS Delegated proof of stake | el protocolo. No se utilizan equipos para minar de alta computación y gasto energético. La participación en la red para confirmar bloques depende de la cantidad de tokens que tiene cada usuario. | José Luis Lorente |
| Dump | Vender a un precio inferior al de mercado. | Alfonso Martínez |
| Ecosistema | Sistema formado por un conjunto de elementos, el medio en que se desarrollan (hábitat) y las relaciones que se establecen entre ellos. | Saül Salcedo |
| ERC20 | Estándar de Ethereum que rige la creación de un smart contract con una tipología concreta de tokens, estandarizando la interfaz de creación y emisión de nuevos tokens en dicha red. Garantiza la interoperabilidad entre tokens. | Enric Martínez |
| Estrategia de farming | Aportación de liquidez a un protocolo y, a cambio, generación de tokens como recompensa (rewards) en un marco de tiempo limitado. | Mariano Rubio |
| Estrategia de pool | Aportación de liquidez a un protocolo de cambio entre dos o más tokens y, a cambio, recibir una parte proporcional de las fees que se generan en dicho pool. | Mariano Rubio |
| ETH2 beacon-chain | Será la nueva cadena de bloques del núcleo de ETH2 para la blockchain Ethereum. Garantizará que toda la red esté sincronizada con los mismos datos. | José Luis Lorente |
| ETH2 validator | Es un cambio importante en la validación de bloques en la blockchain de Ethereum. La validación se realizará por proof of stake (prueba de participación) en la que no se necesita potencia de hardware, sino un mínimo de 32 ETH para ser validador. | José Luis Lorente |
| | | |

| | | |
|---|---|---|
| Etherscan | Motor de búsqueda de la blockchain de Ethereum. Su objetivo es hacer que la cadena de bloques de Ethereum sea transparente, mostrando información clara e inequívoca sobre sus actividades. | Enric Martínez |
| EVM Ethereum Virtual Machine | Máquina virtual que forma parte del ecosistema blockchain de Ethereum. Puede ejecutar variedad de instrucciones, por lo que tiene gran flexibilidad para realizar diferentes operaciones basadas en el lenguaje Solidity. | Enric Martínez |
| Fake | Corresponde al hecho que, relatado, da apariencia de verdad o de certeza, pero que analizado desde ojos expertos resulta ser falso. | Alejandro San Nicolás |
| Fee | Coste de la ejecución de una transacción en la red: satoshis para Bitcoin (BTC), Gwei para Ethereum (ETH). | Enric Martínez |
| EWMA | Exponentially weighted moving average - Media móvil ponderada exponencialmente. | Alfonso Martínez |
| Exchange | Empresa necesaria para cambiar fiat a criptomonedas, y al revés. | Mariano Rubio |
| Fiat | Dinero que existe «por decreto», impreso por alguna entidad central con competencias para ello (dólares, euros, otros). | Javier Masfarré |
| Flash loan | Préstamo sin colateral a través de un smart contract con varias partes estructuradas. Por un lado, se solicita un préstamo, se hacen las operativas deseadas con él y, finalmente, se devuelve dicho préstamo en la misma transacción (en el mismo bloque de Ethereum). | José Manuel Flomesta |
| FOMO | Fear of missing out - Ansiedad que lleva a compras no razonadas por temor a perderse lo que pueda ocurrir. | Alfonso Martínez |
| Fud | Diseminar información negativa. | Alfonso Martínez |
| | | |

| | | |
|---|---|---|
| Fully dilluted market cap o FDMC | Proyección futura de la oferta circulante de un token en base a las emisiones e inflación previstas para el mismo. | Alfonso Martínez |
| Gas | Comisión pagada a los mineros para que funcione el ecosistema. En Bitcoin la llamamos fee. | Saül Salcedo |
| Gwei | 10^9 wei es un Gwei. Gwei es la unidad más común cuando se habla de gas (costes de transacción). En vez de decir que el coste de gas de una operación es 0.000000001 ETH, se puede decir 1 Gwei. | Enric Martínez |
| Hash | Algoritmo matemático para convertir bloques de datos arbitrarios en nuevas cadenas de longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida siempre tendrá la misma longitud. Habitualmente trabajamos en Blockchain con la versión SHA-256. | Enric Martínez |
| Health factor | Parámetro que mide la calidad (riesgo) de una posición de deuda en un protocolo DeFi. Un health factor bajo provocará que la posición se liquide. | Miguel Caballero |
| Hodl | Mantener una criptomoneda/token en tu cartera, en vez de venderla | Alfonso Martínez |
| Holdear | Mantener en cartera los tokens sin hacer ninguna operación con ellos. Su precio variará en función de las variaciones que sufra el mercado. | José Manuel Flomesta |
| Impermanent loss | Factor de medición que determina la variación porcentual negativa asumida respecto a la decisión de aportar ciertos tokens a un pool de liquidez, comparada con el resultado que hubiéramos obtenido si hubiéramos optado por holdear dichos tokens. Este indicador mide el costo de oportunidad al optar por estrategias de liquidity provider o LP. | José Manuel Flomesta |

| | | |
|---|---|---|
| Invariante de un pool | Fórmula que permite calcular los precios de los tokens de un pool, en función de su oferta y demanda. La siguiente fórmula permite el cálculo. Invariant = Nº de tokens A x Nº de tokens B. El invariant se ha de mantener constante en el pool, de manera que el aumento o disminución de precio de uno de los tokens hace que el otro token realice la operación contraria para que el Invariant se mantenga estable. | José Luis Lorente |
| KYC | Know your customer. Proceso para registrar e identificar a usuarios o inversores en un activo. | Saül Salcedo |
| Lending | Prestar o depositar tokens en un pool y recibir interés por prestar esta liquidez. | Javier Masfarré |
| Liquidity mining | Estrategia a través de la cual un inversor añade liquidez a un protocolo a cambio de token nativos del mismo. | Alejandro San Nicolás |
| LP - Liquidity provider | Aquella persona que proporciona liquidez a un pool a fin de recibir fees por cada uno de los intercambios que se realicen en él (swaps). | José Manuel Flomesta |
| Market cap | Es el valor de las acciones en circulación de una empresa. En el mundo cripto es el valor en dólares de los tokens en circulación de una criptomoneda. | José Luis Lorente |
| Mineros | Hardware especializado en la resolución de algoritmos sobre los que se basa y mantiene segura una blockchain. | Enric Martínez |
| MOFO | Término empleado cuando sucede lo contrario al FOMO y existe ansiedad por realizar ventas no razonadas por temor a desplomes. | Alfonso Martínez |
| Nodos | Red de computadoras interconectadas que comparten información de forma segura y descentralizada en una blockchain. Todos los nodos tienen el mismo peso y operan de la misma manera. Los nodos ejecutan un software determinado, como es el caso de Bitcoin, y se | José Luis Lorente |

| | | |
|---|---|---|
| | sincronizan entre ellos. Todos los nodos siguen las mismas reglas, aunque pueden desarrollar distintas funciones. | |
| Nonce | Número de un solo uso utilizado en los algoritmos de prueba de trabajo (PoW) para determinar el minero que se lleva la recompensa de cada bloque minado. El nonce se determina por esfuerzo computacional y forma parte de la información crítica de cada bloque minado al estar incorporado en la cabecera de cada bloque. | Miguel Caballero |
| Oferta circulante - circulating supply | Cantidad total de tokens que están en el mercado. | José Manuel Flomesta |
| Open source | Código abierto. Cualquier persona o entidad tiene capacidad para acceder al código de un protocolo, programa, contrato, etc., y modificarlo para adaptarlo a sus necesidades. | Enric Martínez |
| Oráculo | Conexión existente entre un smart contract y el mundo real para obtener información necesaria para su ejecución (precios, horarios, etc.). | Francisco Sánchez |
| Pool DeFi | Nueva versión del concepto clásico de exchange pero descentralizado, donde en vez de fijar los precios de los activos por libros de órdenes utilizamos algoritmos; en función del tipo y cantidad de tokens inyectados al pool obtenemos precios por los assets. Cualquier pool necesita de LP, pero no tanto de compradores o vendedores. | Miguel Caballero |
| | Sistema que se utiliza para determinar qué usuarios son elegibles para realizar los cálculos necesarios para agregar un nuevo bloque de datos a una cadena de bloques y recibir el pago asociado. Prioriza los mineros en función tanto del staking como del número de transacciones en la | |

| | | |
|---|---|---|
| Proof of importance (POI) | criptomoneda correspondiente que realizan. Cuantas más transacciones se realicen hacia y desde la billetera de criptomonedas de una entidad, mayores serán las posibilidades de que la entidad reciba proyectos mineros. | Enric Martínez |
| Proof of stake (POS) | Protocolo de consenso para redes distribuidas que protege el sistema al solicitar prueba de posesión de la moneda. Con POS la probabilidad de encontrar una transacción y recibir el bono correspondiente es proporcional a la cantidad de monedas acumuladas (evitando así que la confianza se determine por la cantidad de trabajo invertido). | Enric Martínez |
| Proof of work (POW) | Protocolo de consenso que mide el esfuerzo computacional que aporta cada minero a la red para recompensar al que encuentre la prueba matemática que le permita recibir la recompensa por minar el bloque. El POW defiende la red frente a ataques a través del hash rate. | Miguel Caballero |
| Protocolo | Son las reglas que forman un lenguaje codificado con una sintaxis, semántica y procedimientos definidos, para que se entiendan, comuniquen y sincronicen dispositivos conectados a una red. | José Luis Lorente |
| Proof of adress | Prueba de domicilio. En wallets se aplica a la prueba de residencia del país del titular de cuentas de exchange o wallets custodiados. Habitual en un proceso de KYC y AML. | Alejandro San Nicolás |
| Pump | Hinchar el precio de un activo (para que suba). | Alfonso Martínez |
| Ratio de Sharpe | Una relación creada en 1966 y que los inversores y economistas utilizan para evaluar el retorno potencial de la inversión (ROI). | José Luis Lorente |

| | | |
|---|---|---|
| Ratio de Treynor | Mide el exceso de rentabilidad ganado por unidad de riesgo sistemático. | José Luis Lorente |
| Rekt | Que ha perdido todo lo invertido por un movimiento brusco del mercado | Alfonso Martínez |
| Riesgo sistémico | Riesgo del mercado independiente del activo activo en cuestión. Es decir, riesgo no diversificable entre activos del mismo conjunto. | Nicolás Barilari |
| ROI | Return on investment - retorno de la inversión | Nicolás Barilari |
| Satoshi | Unidad más pequeña (hasta la fecha) de la criptomoneda bitcoin. Lleva el nombre de Satoshi Nakamoto, el creador del protocolo. La proporción de satoshi a bitcoin es de 100 millones de satoshis por bitcoin. | Enric Martínez |
| SC - smart contract | Contratos realizados sobre la BC de Ethereum. Conjunto de algoritmos ordenados de manera que ejecuten funciones determinadas en un entorno blockchain de Turing complete | Saül Salcedo |
| Scam | Estafa realizada a través de medios electrónicos. Se usa esta palabra para definir los intentos de estafa a través de modelos de blockchains que incorporan esquemas Ponzi del tipo *network marketing*, asegurando altas tasas de rentabilidad a cambio de custodiar tus criptoactivos. Suelen estar asociados a bots de arbitraje. | Enric Martínez |
| Security token | Es un tipo de token criptográfico vinculado a valores financieros. Otorga a los propietarios derechos y obligaciones. | José Luis Lorente |
| SHA-256 | Función hash que ha sido elegida para el funcionamiento de muchas criptomonedas (bitcoin entre ellas). Ofrece un alto nivel de seguridad, las protege y codifica de forma segura la información y garantiza la integridad de la información almacenada en un bloque, entre otras cosas. | Enric Martínez |

| | | |
|---|---|---|
| | Desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y el National Institute of Standards and Technology (NIST). | |
| Shorting | Estrategia de vender un token que va de bajada por una stablecoin y volver a comprarlo antes de que se vuelva a recuperar. | Mariano Rubio |
| Sidechains | Una cadena lateral es una cadena de bloques basada en una blockchain matriz principal. El uso de cadenas laterales permite la creación de varios tipos de contratos inteligentes, acciones, derivados, etc. Mejora las prestaciones de una blockchain ya existente al permitir funcionalidades no viables en la nativa. | Enric Martínez |
| Sintéticos | Activos que copian el movimiento de precio otro asset, pero sin estar vinculados, permitiendo la exposición a dicho activo y cubriendo el riesgo con distintos tipos de colateral. | Miguel Caballero |
| Skin in the game | Tomar verdadero riesgo. | Mariano Rubio |
| Slippage | Valor en % de cambio permitido del valor de los tokens durante un proceso de swaping. | Mariano Rubio |
| Stablecoin | Cripto ligada a un activo financiero real (oro, dólar, etc.). Token de valor estable colateralizado con assets del propio ecosistema blockchain o del sistema tradicional. | Saül Salcedo |
| Stake | Mantener fondos bloqueados en bóvedas, smart contracts o protocolos, como depósito para recibir recompensas. | José Luis Lorente |
| Stress de un pool | Nivel de liquidez disponible respecto a los activos depositados. Se dice que un pool está estresado cuando tiene poca liquidez al haber realizado operaciones en las que se ha producido una gran | Miguel Caballero |

| | | |
|---|---|---|
| | descompensación de tokens, por lo que el precio que devuelve el pool por cada token es malo en términos de eficiencia. | |
| Swap | Intercambio de un token por otro dentro de un pool, que conlleva un gasto de gas. | José Manuel Flomesta |
| Token holder | Poseedor de un token. | Alejandro San Nicolás |
| Token | Representación digital de un asset con unas características determinadas según su funcionalidad. | Saül Salcedo |
| Token de gobernanza | La gobernanza son las reglas que permiten el desarrollo y mantenimiento de una red o de un protocolo. El poseedor de tokens de gobernanza participa en las votaciones que propone la comunidad y así se toman las decisiones. La gobernanza puede ser descentralizada totalmente, parcialmente, o centralizada. | José Luis Lorente |
| Tokenización de activos | Representación digital de todo aquello que tenga un valor que alguien esté dispuesto a pagar. | Francisco Sánchez |
| Tokenomics | Reglas que rigen el funcionamiento de un token entre todos sus participantes (cantidad, proporción del total, características, etc). | Javier Masfarré |
| TPS (transacciones por segundo) | Cantidad de transacciones por segundo que es capaz de procesar una red blockchain. | José Luis Lorente |
| Tutelliano | Adicto e incondicional de Tutellus y sus grupos. Inquieto por naturaleza, dícese del que aporta valor al ecosistema de forma desinteresada. Suele presentar alguna tara mental, pero es buena gente. | Alejandro San Nicolás |
| txn | Transacción. | Alfonso Martínez |
| | | |

| | | |
|---|---|---|
| Utility token | Token cuya utilidad reside en tener un derecho de acceso a productos o servicios sobre futuros desarrollos del proyecto. Suelen estar destinados a financiar un negocio, aunque también se pueden emitir en un contexto de no buscar financiación. | Alejandro San Nicolás |
| UTXO | Salida de transacción no gastada o unspent transaction output | Alfonso Martínez |
| VFA | Virtual financial asset. La ley define un activo financiero virtual como cualquier forma de registro en un medio digital que se utiliza como medio de intercambio, unidad de cuenta o depósito de valor y que no es dinero electrónico, un instrumento financiero o un token virtual. | José Luis Lorente |
| Volatilidad | Mide la rapidez de la variabilidad o fluctuaciones del precio de un activo y su rentabilidad. | José Luis Lorente |
| Volatilidad histórica | Se expresa en porcentaje y se calcula como la desviación que registra un activo con respecto a su media de cotización histórica en un periodo determinado. | José Luis Lorente |
| Wallet | Programa o accesorio que almacena criptodivisas. | Enric Martínez |
| Whitepaper | Documento que explica con detalle un proyecto de lanzamiento de un token o protocolo. En él se detalla el proyecto, financiación, tokenomics, problemas que resuelve y la hoja de ruta de su puesta en marcha. | José Luis Lorente |
| Yield farming | Uso de las criptomonedas que hacen los titulares de estos activos para invertir y obtener el mayor retorno de la inversión. | Enric Martínez |

# PRIMERA PARTE:
# BITCOIN Y EL DINERO

# 1. ¿Qué es el dinero?

Cada vez que comparto a qué me dedico y cómo mi profesión está directamente relacionada *con eso del Bitcoin*, suelo obtener siempre la misma respuesta: «Lo he escuchado, pero la verdad es que no entiendo nada». Pero siendo sincero, Bitcoin no es difícil de comprender; simplemente su comprensión implica familiarizarse con muchos conceptos, la mayoría de ellos completamente nuevos. Me pregunto lo difícil que fue, en su momento, comprender cómo funciona Google, por ejemplo. Es por eso que vamos a ir por partes, empezando desde el principio de todo. Si Bitcoin es una forma de dinero, quizá antes deberíamos empezar por comprender qué es el dinero, ya que por muy absurdo que suene, es un tema bien desconocido.

## 1.1. Una primera definición de dinero

El dinero es uno de los elementos más importantes de nuestras vidas. Siempre existirá la visión que defiende que el dinero no es importante, que lo que realmente importa es la felicidad y las personas con las que acabas compartiendo tu vida. Y aunque esto tenga parte de verdad, la realidad es que no significa que el dinero no sea importante. Nuestras vidas giran en torno al dinero; por ejemplo, estudiamos para conseguir un buen trabajo y así ganar un buen dinero.

Si dejáramos de hacer uso del dinero, quedaríamos fuera del sistema, ya que no podríamos transferir valor los unos a los otros. Por ejemplo, si no tengo dinero, no puedo plantearme adquirir un coche, ir al cine o comprarme una casa. Todos estos productos o servicios están a nuestra disposición porque alguien ha dedicado tiempo y esfuerzo, y es lógico que esperen algo a cambio. Así, de alguna forma podemos decir que el dinero es como un lenguaje, más bien una metalenguaje, ya que sirve de apoyo a la lengua normal para podernos coordinar en sociedad con más facilidad.

No hay duda de que el dinero es fundamental. Sin él no podríamos mantener estructuras sociales como las que tenemos hoy. Por tanto, el siguiente paso es preguntarnos por qué hay materiales que se usan como dinero y otros no. O directamente: ¿cuándo surgió el dinero? Para responder estas cuestiones tendremos que viajar en el tiempo hacia nuestros orígenes.

## 1.2. El ser humano y el dinero

Los seres humanos somos una especie surgida tras millones de años de evolución. A nivel fisiológico no somos muy distintos de otras especies, pero seguramente una de nuestras más notables diferencias es nuestra «preferencia temporal» es decir, nuestra capacidad para pensar en el futuro.

Pongamos un ejemplo. Cuando un animal tiene hambre, su reacción automática es ponerse en busca de comida. Piensan y actúan. Su cerebro se enfoca principalmente en el presente, no está en sus preocupaciones si en dos semanas tendrá comida, eso queda demasiado lejos. Los humanos, en cambio, si tenemos hambre, es cierto que tenemos la opción de ponernos a buscar comida de forma automática, pero también tenemos la opción de dedicar tiempo para construir alguna herramienta para aumentar nuestra productividad. Por ejemplo, podríamos dedicar tiempo a construir una caña de pescar para así sacar más peces en menos tiempo. Invertimos tiempo hoy para recibir algo después. En otras palabras, tenemos la capacidad de pensar en el futuro.

De alguna forma esto nos permite entender el proceso de civilización que hemos vivido como especie. En un principio, cuando nuestra preferencia temporal era más alta, valorábamos menos el futuro y vivimos más al día. Con el tiempo, nuestra preferencia temporal empezó a bajar, lo que nos permitió, por ejemplo, cazar más de lo necesario para así almacenar alimento y comer en momentos difíciles. Por primera vez empezamos a acumular más de lo que necesitábamos. El aumento de productividad permitió a los seres humanos generar un excedente, lo que a su vez ayudó a que naciera el primer sistema económico de la historia; un sistema basado en el intercambio.

## 1.3. Los sistemas basados en el intercambio: el trueque

Con este sistema, las pequeñas comunidades que habitan en las mismas zonas ya no se ven como rivales, sino como posibles colaboradores. Intercambiando diferentes excedentes podían mejorar sus vidas y obtener cosas que necesitaban a cambio de otras que les sobraban.

Este sistema, a pesar de originar un punto de inflexión muy relevante en nuestra civilización, tenía muchas limitaciones:

1. Solo era viable el trueque en pequeños círculos, no permitía la creación de grandes economías.

2. Era necesario que hubiera una coincidencia de deseos. Yo no puedo hacer un trueque con una persona que no está interesada en hacer el trueque conmigo.
3. Era difícil determinar el valor de las cosas ya que muchas veces los objetos no eran divisibles, o eran difíciles de comparar.
4. Se hacía uso de elementos perecederos, es decir, que se estropean con el tiempo. Era difícil acumular valor si tu riqueza desaparecía en cuestión de semanas.

## 1.4. Una gran solución: el dinero moderno

A raíz de estas limitaciones, las comunidades se vieron obligadas a innovar y generar así una de las tecnologías más antiguas y relevantes que existen: el dinero.

Este no es más que un material que permite un intercambio indirecto entre dos personas. A pesar de su simpleza, el potencial de esta tecnología es enorme. Ahora, por ejemplo, ya no importa si no hay coincidencia de deseos porque existe un material intermedio con el que puedes acceder después a cualquier otro producto. El dinero es el elemento más líquido en una economía y es un elemento indispensable para vivir una expansión económica.

En definitiva, el dinero es una tecnología que aparece de forma natural entre los seres humanos para facilitar el intercambio de valor entre individuos, lo que a su vez permite generar comunidades más grandes, hasta llegar a construir pueblos o ciudades. Nacido hace más de quinientos mil años, el dinero es uno de los elementos clave en nuestro proceso evolutivo.

Aun así, configurar y desarrollar una forma de dinero no es tan sencillo. ¿Cómo se llega a un acuerdo entre diferentes comunidades sobre cuál va a ser el material que se usará como dinero? Durante la historia ha habido muchas formas de dinero: conchas, plumas, piedras preciosas… ¿Cómo se escoge qué material se va a utilizar? ¿Hay alguien que sea el elegido para escogerlo? Es decir, ¿se impone o se establece de forma natural?

La respuesta la encontramos en el nivel de vendibilidad de un material.

## 1.5. Vendibilidad de un material usado como dinero

Este concepto nos permite valorar cómo un material puede cumplir la función de dinero teniendo en cuenta tres aspectos. En función de lo eficiente que sea un

material en relación con estos aspectos, se determinará que una forma de dinero sea «buena» o «mala».

Los tres aspectos utilizados para determinar la vendibilidad de un material son los siguientes:

### 1ª característica: valor reserva

Un material es un buen valor reserva cuando es capaz de conservar su valor durante el tiempo. Este rasgo viene dado por varios factores. El primero es que no se deteriore. Por ejemplo, la comida es un mal valor reserva porque tiene fecha de caducidad y, por tanto, no me permite acumular valor a lo largo del tiempo.

Una vez confirmamos que perdura en el tiempo, dicho material actuará como buen valor reserva en función de lo escaso que sea. Por ejemplo, las piedras comunes no son deteriorables, pero son abundantes, por lo que no es un buen valor reserva. Algo que existe en abundancia no puede ser nunca una buena opción para guardar valor. Esta conclusión lógica empieza a generar ciertas dudas sobre el dinero actual, ya que, como veremos más adelante, los bancos centrales tienen el poder de imprimir infinitas cantidades de dinero.

Una vez tenemos un material no deteriorable y escaso, ¿cómo comparamos cuál cumple mejor la función de valor reserva? La respuesta la obtenemos a través de una ratio conocida como stock-to-flow-ratio, que vendría a ser la ratio entre el material existente y el nuevo material introducido en la economía anualmente. Un ejemplo:

Pongamos que tenemos un material muy escaso, pero que anualmente, si invertimos tiempo y dinero para generar más de ese material, podemos llegar a encontrar un 10 % del total ya existente. Este material, por tanto, no es óptimo para conservar valor en el tiempo, porque estará sujeto a un nivel de inflación anual del 10 %. Cuando aparece más cantidad de un material, el mismo pierde valor. Hace cincuenta años, una Coca Cola costaba 0,10 USD y hoy cuesta 2 USD, pero no es que la Coca Cola valga veinte veces más, sino que el material que usamos como dinero vale veinte veces menos.

Por lo tanto, para que un material funcione de forma óptima como valor reserva, debe tener una stock-to-flow-ratio alta, o, lo que es lo mismo, que la cantidad anual de ese material que se introduce en la economía sea muy inferior al material ya existente. No es una coincidencia que durante miles de años el valor reserva por excelencia haya sido el oro. El oro ha demostrado durante miles de años que, aunque invirtamos el doble que el año anterior en extraerlo,

vamos a sacar siempre alrededor del 1 % - 1,5 % del total existente. Esto permite que la gente pueda confiar en este material como valor reserva, ya que la historia demuestra que no es posible que su valor caiga por un aumento inesperado de la oferta total.

**2ª característica: medio de cambio**

Este aspecto determina cómo de aceptado está en una sociedad ese tipo de dinero. Cuanto más aceptado esté, más podré comerciar con él.

El nivel de aceptación de una forma de dinero tiene una relación directa con el grado de especialización y, por tanto, complejidad económica y comercial de una sociedad. Si yo puedo confiar en que el oro es una buena forma de dinero y que está altamente aceptada, puedo estar tranquilo con que siempre podré satisfacer mis necesidades con ese dinero. En consecuencia, será menos arriesgado especializarme en una actividad concreta: si yo no puedo confiar en una moneda o esta es poco aceptada, es difícil que me especialice en zapatos y me haga zapatero, porque el tiempo invertido en dominar esta actividad será tiempo que no habré invertido en aprender otras prácticas necesarias para sobrevivir (criar animales, cultivar vegetales, coser ropa…).

**3ª característica: unidad de cuenta**

Este rasgo de una forma de dinero determina si es capaz de dar una orientación del valor de las cosas. Por ejemplo, hoy en día podemos entender el valor de algo en función de su precio: los euros, dólares u otras monedas nos permiten calcular fácilmente el valor de los productos o servicios.

Esta característica va ligada a una baja volatilidad y, además, al nivel de desarrollo económico de una sociedad, ya que permite a los emprendedores calcular beneficios y pérdidas. Es decir, saber si la actividad ha sido rentable o no, algo complicado si se usa como dinero un activo muy volátil.

## 1.6. Resultados de un material vendible

Una vez entendemos qué es lo que hace que un material sea vendible, podemos también entender cuándo una moneda es «sólida» o «débil».

Una moneda es sólida cuando cumple correctamente los tres aspectos que determinan su vendibilidad. De estos, el más importante es su capacidad de guardar valor en el tiempo, es decir, su capacidad de actuar como valor reserva. Esto es debido a que los otros aspectos suelen nacer como consecuencia de que

ese material sea un buen valor reserva (antes debe haber un proceso evolutivo). Inicialmente, el oro no se aceptaba en todas partes; fue demostrando su capacidad para guardar valor, lo que generó confianza entre la población para aceptarlo como método de cambio y, una vez adoptado, el valor de las cosas empezó a calcularse respecto al oro.

Una sociedad con una moneda sólida es aquella en que la población comprende que lo que ahorra hoy tendrá más valor en un futuro y hay incentivos para ahorrar e invertir en proyectos estables a largo plazo. Esto crea el escenario perfecto para el florecimiento de economías estables basadas en el ahorro y en las inversiones prudentes, y no en la deuda y las malas inversiones. Esto tiene consecuencias a nivel psicológico, ya que estas sociedades empiezan a adoptar comportamientos propios de personas con una baja preferencia temporal (valoran más el futuro que el presente), lo que se ve reflejado no solo en el consumo, sino en las relaciones o incluso en el arte.

Por otro lado, una moneda débil es aquella que es incapaz de guardar valor en el tiempo, lo que genera inestabilidad y bloquea el progreso económico y social. En algunos casos, estas monedas también son grandes impulsoras de una economía basada en el gasto y en la deuda. Esto es bastante lógico ya que, si una moneda pierde valor cada año, el mejor momento para gastar es hoy mismo. En definitiva, son monedas que van ligadas a la inestabilidad; es impensable vivir en una sociedad estable y que progresa cuando su forma de dinero pierde un 50 % de su valor de un año para otro.

Y con esto no estoy poniendo ejemplos hipotéticos. Sin ir más lejos, en peso argentino tuvo un nivel de inflación del 53 % durante 2019. En otras palabras, el gobierno empobreció a su población sin que los ciudadanos pudieran evitarlo. Esto sucede con todas las monedas débiles, monedas poco escasas y con un stock-to-flow muy baja.

# 2. Evolución del dinero

A lo largo de la historia ha habido muchas formas de dinero, algo normal ya que, como hemos visto, este es necesario para desarrollar grandes sociedades. Como la calidad de una forma monetaria depende de lo bien que cumpla ciertas características, es lógico que haya una competición sana entre diferentes formas de dinero. Con el tiempo, aquellas más vendibles se imponen sobre otras que aportan menos valor al ciudadano.

Por poner algunos ejemplos, ha habido sociedades que han utilizado conchas, sal, piel o vidrio, aunque con el tiempo fue el oro lo que se acabó imponiendo en la mayor parte del mundo como forma de dinero más aceptada. Simplemente era más sólido, conservaba mejor el valor.

Una moneda débil, que genere inestabilidad y en la que no se pueda confiar a largo plazo porque es susceptible de perder su valor fácilmente, acaba desapareciendo. Una moneda que constantemente pierde valor, acaba valiendo nada.

Este elemento es muy crítico dentro de una sociedad porque puede conllevar momentos de expropiación y empobrecimiento masivo de una población. Durante el imperialismo, los europeos se dirigieron a África cargados de vidrio, porque allí este material se utilizaba como dinero. Sin ninguna dificultad pudieron controlar a la población africana y sus sistemas de producción. Básicamente, los africanos vendían su riqueza real obtenida con tiempo y esfuerzo (recurso limitado) a cambio de un material que para los europeos era exageradamente fácil de conseguir (recurso ilimitado). En definitiva, debido a que la población africana utilizaba una forma débil de dinero, les expropiaron todas las tierras y propiedades a cambio de un material que no valía nada.

## 2.1. Descubrimiento del oro y la plata

Como hemos visto, un material es una buena forma de dinero cuando es altamente vendible. Claramente, el oro no fue vendible desde el primer momento, sino que pasó por muchos años de evolución. Primero convenció a la gente por su escasez, ya que permitía conservar valor en el tiempo de forma segura. Más tarde se empezó a utilizar como medio de cambio, ya que la gente confiaba en el valor de ese material. Finalmente, las cosas se podían valorar en relación con el oro. Es a partir de este momento cuando se impuso de forma

clara sobre las otras formas de moneda y se posicionó como el dinero por excelencia.

Al utilizar oro, las sociedades vivieron muchos años consecutivos de estabilidad. Básicamente, el oro se impuso de forma natural por su vendibilidad.

El oro es un buen material para conservar valor, no se puede falsificar, es resistente, difícil de destruir y mantiene una stock-to-flow ratio alta gracias a su escasez y su dificultad de extracción. Una vez los tres aspectos principales se cumplen, se empiezan a valorar otros aspectos como la divisibilidad, la portabilidad, la facilidad de transferirlo y guardarlo o la facilidad para detectar falsificaciones.

## 2.2. El dinero durante el Imperio romano

En un mundo donde el oro ya se posicionó como material principal para conservar valor, surgieron períodos de estabilidad y expansión comercial que dieron lugar, en parte, al nacimiento de grandes imperios. Un ejemplo es el romano.

El gobierno creó una moneda basada en oro que era más vendible que el oro en sí mismo. Era más fácil de reconocer, transportar, facilitaba el intercambio… La gente confiaba más, estaba estandarizada y hacía más fácil el comercio. Esta —creada por Julio César— fue la primera moneda sólida de la historia. Se llamaba áureo y constaba de ocho gramos de oro por unidad.

Figura 1. Primera moneda sólida de la historia: el áureo de Julio César

El caso del Imperio romano nos ayuda entender la importancia de una moneda sólida en una sociedad y los perjuicios que conlleva que haya alguna entidad con el poder de manipularla y hacerla cada vez más débil.

El caso es que, con los años, los diferentes césares fueron devaluando la moneda. Si inicialmente tenía ocho gramos de oro por, el gobierno empezó a emitirlas reemplazando este por metales de menos valor. Llegó el punto en que la moneda se devaluó tanto —siempre con el fin de financiar los caprichos de la

nobleza y las guerras— que la sociedad simplemente se derrumbó. Los precios subieron y la población pasó de tener monedas para poder comprar y comerciar, a tener trozos de metal con el que no podían comprar nada, principalmente porque era solo eso: metal.

La situación era tan crítica que a los productores ya no les salía rentable producir, haciendo que el comercio se colapsara y que los productores adoptaran economías más de subsistencia, rompiendo todo el comercio que se había creado durante muchos años de prosperidad.

El resultado fue la separación del Imperio romano y la entrada en la Edad Media, un periodo de más de mil años de baja prosperidad. Y no es que la población no fuera capaz de generarla, sino que no existía ninguna forma de dinero sólida, como fue el áureo, que permitiera a la sociedad prosperar y expandirse económica y comercialmente.

La realidad es que las verdaderas causas del fin del Imperio romano como civilización conectada comercial y económicamente fueron estas recetas económicas que hoy nos resultan muy familiares.

## 2.3. El dinero durante el Renacimiento

La suerte cambió a partir del Renacimiento cuando, en Florencia, la familia Medici (los primeros banqueros del mundo) crearon la segunda gran moneda sólida de la historia: el florín. En aquella época surgieron los primeros bancos, que básicamente ofrecían un servicio de custodia. La población guardaba de forma segura su oro en las bóvedas de los bancos a cambio de un coste. Con el tiempo, los bancos empezaron a crear «papeles» o letras que representaban aquel oro depositado en sus cajas fuertes. El papel, respaldado por oro, era más vendible que el oro en sí mismo, era más fácil de transportar y de intercambiar, y era más divisible. Aunque tardó unos cuatrocientos años en establecerse, finalmente el papel moneda respaldado en oro se acabó imponiendo sobre las propias monedas de oro.

Figura 2. Monedas acuñadas en Florencia durante la Edad Media

Este evento impulsó la aparición del sistema que más prosperidad y expansión económica ha generado: el patrón oro. Los gobiernos terminaron creando bancos centrales que acumulaban el 100 % del oro y después emitían el papel moneda estatal correspondiente. El proceso por el que los bancos centrales se fueron imponiendo y expropiando el valor de los bancos comerciales fue de lo más interesante. Básicamente el gobierno se dio cuenta del poder que representaba tener el control sobre la moneda. Hay un libro que te recomiendo, si quieres profundizar sobre el tema, que me dejó fascinado: *¿Qué ha hecho el dinero con nuestro dinero?*, de Ludwig von Mises.

La vendibilidad de esta nueva forma de dinero no tenía precedentes. Era mucho más fácil de transferir y transportar y seguía siendo sólida porque mantenía las características del oro. En pocos años, las sociedades occidentales vivieron el momento de máxima expansión económica y comercial. Esta época, liderada por Gran Bretaña, se conoce como la *belle époque* y duró desde 1871 hasta 1914. Estuvo caracterizada por el libre comercio, importantes inventos y el nacimiento de una economía global. Esto dio paso a grandes inversiones y a la creación de enormes empresas que permitieron el inicio de la industrialización y la urbanización.

## 2.4. La Primera Guerra Mundial y el fin del patrón oro

En 1914 el mundo se vio inmerso en el inicio de la Primera Guerra Mundial, que terminó provocando la abolición del patrón oro en la mayoría de países.

Esta guerra, por primera vez mundial, es diferente a muchas otras, y ahora entenderemos por qué. Más que una guerra de armas, fue una guerra monetaria. En los años anteriores las guerras duraban hasta el punto en que la casa real o el gobierno de uno de los países se quedaba sin dinero para financiar las batallas. Esta guerra, en cambio, fue diferente a las anteriores ya que por primera vez los gobiernos, a través de los bancos centrales, tenían el control no solo de su riqueza, sino de la riqueza de toda la población.

El tipo de dinero que utilizaban los ciudadanos eran papeles respaldados por el oro que el banco central tenía guardado en sus cajas fuertes, y los gobiernos podían ir imprimiendo tanto dinero como quisieran aunque no estuviera respaldado por oro, y así financiar la continuación de la guerra. Esto, lógicamente, obligó a los países a abandonar el patrón oro.

| | 1913 | 1914 | 1915 | 1916 | 1917 | 1918 |
|---|---|---|---|---|---|---|
| Royaume-Uni | 8,1 | 12,7 | 33,3 | 37,1 | 37,1 | 35,1 |
| France | 10,0 | 22,3 | 46,4 | 47,2 | 49,9 | 53,5 |
| Allemagne | 9,8 | 23,9 | 43,8 | 50,3 | 59,0 | 50,1 |
| | | | | | | |
| Etats-Unis | 1,8 | 1,9 | 1,9 | 1,5 | 3,2 | 16,6 |
| Australie | 5,5 | 5,7 | 9,6 | 14,0 | 17,2 | 17,2 |
| Canada | 7,0 | 10,0 | 13,1 | 16,5 | 15,7 | 16,9 |

Figura 3. Porcentaje del PIB correspondiente al gasto estatal. Broadberry & Harrison, 2005, p. 15

Tal fue el nivel de impresión de dinero por parte de los gobiernos, que hasta que uno de los bandos (Alemania principalmente) no llegó a la hiperinflación —empobreciendo así a toda su población—, la guerra no terminó. Durante los siguientes años, Alemania se vio inmersa en un momento de crisis e inestabilidad absolutas: habían generado tanto dinero que este, en sí mismo, ya no tenía valor.

| | 1914 | 1916 | 1918 |
|---|---|---|---|
| Grande-Bretagne | 100 | 160 | 227 |
| France | 100 | 189 | 340 |
| Allemagne | 100 | 153 | 217 |
| États-Unis | 100 | 127 | 194 |

Figura 4. Variación de la tasa de inflación. Broadberry & Howlett, 2005

Una de las pocas economías europeas que no renunció al patrón oro y que se abstuvo de aplicar políticas monetarias altamente inflacionarias fue Suiza. En consecuencia, el franco suizo vio como todas las otras monedas estatales se devaluaron a velocidades alucinantes.

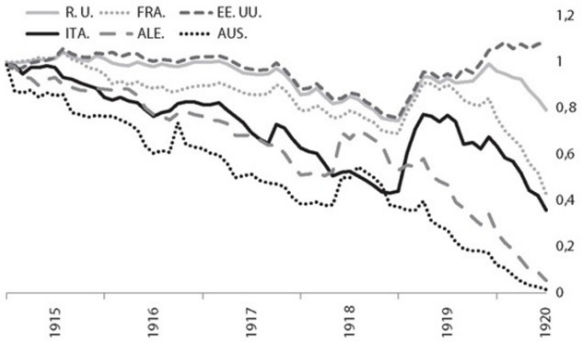



Figura 5. Depreciación de las monedas nacionales frente al franco suizo durante la Primera Guerra Mundial - George Hall, «Exchange Rates and Casualties During the First World War», Journal of Monetary Economics, vol. 51

Si reflexionamos sobre este hecho, creo que lo podemos definir como una de las acciones más graves e injustas que pueden existir: un gobierno había empobrecido completamente a toda la población del país sin que las personas pudieran hacer nada para evitarlo. Esto solo es posible en modelos monetarios

donde el control sobre el dinero recae en una entidad centralizada como es un gobierno. La historia demuestra que la tentación de crear dinero de la nada es demasiado tentadora. Tanto el Imperio romano como muchos otros imperios y países hicieron mal uso del poder de manipular la masa monetaria.

Este hecho generó tal inestabilidad que, unos años más tarde, vivimos la Segunda Guerra Mundial, impulsada principalmente por el malestar generalizado de la población, sobre todo de Alemania, causado por el derrumbe del tipo de dinero que se utilizaba.

## 2.5. Final de la II GM y acuerdo de Bretton Woods

Al finalizar la Segunda Guerra Mundial, las principales potencias se congregaron en una reunión conocida como Acuerdo de Bretton Woods. El objetivo fue definir un nuevo sistema comercial, económico y monetario que garantizase estabilidad y evitase otras guerras.

Figura 6. Sede de la reunión para establecer el Acuerdo de Bretton Woods

Durante la reunión de Bretton Woods se acabó adoptando un modelo que beneficiaba claramente a Estados Unidos (la potencia más fuerte en ese momento) y que se basaba en las teorías económicas de John Keynes (keynesianismo). Esta teoría nace con la hipótesis de que es imposible garantizar la estabilidad si no hay una entidad central (banco central) que tenga el control de la oferta monetaria. Estos eran responsables de aumentar la masa monetaria a través de la inflación y, según Keynes, esto promueve la inversión y el gasto, componente clave para que una economía genere prosperidad y evite momentos de crisis.

Se trata de una idea muy controvertida, ya que hay decenas de estudios que demuestran que las hipótesis planteadas por Keynes son incorrectas, sobre todo por la correlación —evitada por los keynesianistas más radicales— entre las políticas económicas y las monetarias. Sin ir más lejos, hemos vivido momentos donde los niveles de inflación e inyección han sido altos pero, al contrario de lo

que afirma Keynes, no ha habido una mejora de la situación económica y no se ha podido evitar la pérdida masiva de puestos de trabajo. Recuperando el tema y partiendo de esta idea, se implementó un sistema llamado «el patrón dólar».

Este sistema consistía en lo siguiente: Estados Unidos pasaba a ser el centro del sistema ya que el dólar estadounidense cumplía la función de moneda de reserva global. El dólar pasaba a ser la única moneda respaldada por oro (con un tipo de cambio fijo) lo que, al mismo tiempo, le dio derecho a tener el control de todas las reservas de oro del mundo. De alguna manera, era un intento fallido de volver al patrón oro, pero Estados Unidos aprovechó la ocasión para generar más dinero del que tenía respaldado en este material, rompiendo el cambio fijo del dólar-oro.

Este hecho dio lugar al «déficit sin lágrimas». Básicamente, Estados Unidos podía generar dinero de la nada sin vivir períodos de inflación. Como todo el mundo utilizaba los dólares como moneda reserva, los daños se repartían entre todos los países del mundo; Estados Unidos podía imprimir dinero y beneficiarse de ello, repartiendo las consecuencias negativas entre todos los países. No es de extrañar que en aquella época las empresas estadounidenses se comieran el mundo y se convirtieran en las más grandes del planeta: financiación ilimitada a un tipo de interés muy bajo.

La inflación se empezó a notar y países como Francia y Alemania quisieron recuperar sus reservas de oro dando, a cambio, dólares. Ante esta situación, en la que Estados Unidos veía cómo sus reservas de oro se iban reduciendo, el presidente de ese momento, Nixon, anunció la suspensión temporal de la paridad dólar-oro. Este evento se conoce como «Nixon Shock» y tuvo lugar en 1971.

## 2.6. El dinero actual: un sistema basado en deuda

Este conjunto de eventos ha acabado dando lugar a la consolidación del sistema monetario actual. Hoy en día el dinero no está respaldado por un valor real como lo es el oro, sino en leyes políticas y en la «fe» en el país: simplemente es papel basado en la deuda y en la promesa de devolverla gracias capacidad de generar valor en el futuro. O, dicho de otro modo menos sutil: esclavizando a las generaciones futuras, ya que son estas las que deberán pagar esa deuda a través de los impuestos.

Si recuperamos lo que determina que una moneda sea sólida, el dinero fiat (nombre con el que se define el tipo de moneda actual o dinero fiduciario) es la forma de dinero más débil que hemos tenido nunca: un sistema donde la

capacidad de imprimir es ilimitada y donde los países pueden gastar más de lo que tienen pidiendo préstamos a bancos centrales que lo único que tienen que hacer para generarlo es inyectar dinero creado de la nada. Claramente, una moneda controlada por una entidad y que no cumple la función principal, que es conservar valor en el tiempo, no es una moneda sólida.

## 2.7. Conclusiones del dinero fiat

Tras años de evolución monetaria, el poder sobre la moneda fue cayendo progresivamente sobre los Estados. Estos han acabado monopolizando el control sobre el dinero, lo que genera un problema grave. La historia nos confirma con cientos de ejemplos —desde el Imperio romano o el chino— que la posibilidad de sacar provecho del control de la moneda es demasiado tentadora. ¿Quién no quiere dinero gratis? ¿Quién no quiere «aprovecharse» poco a poco de su población en beneficio propio sin que esta se dé cuenta?

Al final, lo más conflictivo de estas políticas donde se manipula la oferta total de dinero disponible a través de la inflación son los efectos negativos que tienen sobre la sociedad. Progresivamente los ciudadanos se vuelven cada vez más pobres, no en cantidad de dinero, pero sí en poder adquisitivo. Es decir, seguirán teniendo 1000 EUR, pero con los años con estos 1000 EUR podrán adquirir menos cosas. El valor de las cosas se mantiene, pero el valor del dinero baja. Los precios suben y, pasados los años, nos damos cuenta de que ahora una Coca-Cola ya no vale 0,10 USD sino 1,50 USD. La Coca-Cola no vale quince veces más, sino que nuestro dinero vale quince veces menos.

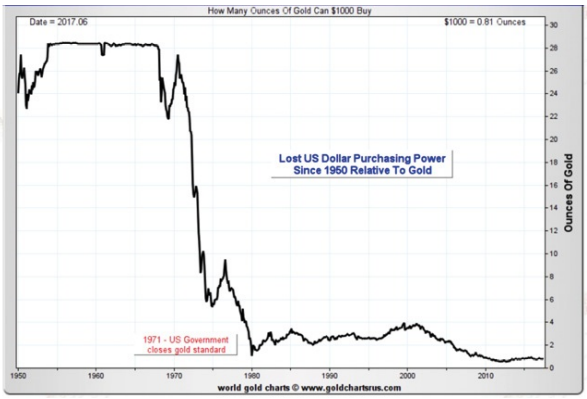



Figura 7. Poder de compra del dólar calculado en oro. Fuente: *Goldchartsrus*

Teóricamente, este efecto se contrarresta a través del aumento de sueldos. Y aunque esto solo se aplica a una pequeñísima parte de la población (trabajadores

con un contrato salarial antiinflacionario que aumenta cada año proporcionalmente a la inflación del periodo), no es del todo cierto.

La realidad es que la inflación beneficia a los ricos a costa de los más pobres y provoca que a lo largo del tiempo la diferencia entre ricos y pobres se vaya agravando. Pongamos que el Banco Central Europeo emite 1000 MEUR, estos se inyectan en la economía para darle un impulso y reactivarla, promover el gasto, incentivar la producción y así aumentar los puestos de trabajo. Ahora bien, los primeros en recibir este dinero suelen ser las grandes empresas, aquellas con suficiente capital para poder comprar «dinero barato». Por lo tanto, los ricos son los que mejor financiación obtienen. En segundo lugar, debido a que ha habido un aumento de la oferta monetaria, los precios de las cosas comienzan a subir, pero estas empresas gastan ese dinero en momentos donde los precios aún no han variado. Es difícil competir justamente con esto.

Como conclusión, vivimos en un sistema inflacionario que beneficia a los ricos a costa de los pobres y provoca que, con el tiempo, se agrave la separación entre los adinerados y la gente más necesitada. Además, la base del sistema es una de las formas monetarias más débiles que hemos tenido nunca: completamente ilimitada y por tanto mal valor reserva, controlado por una entidad central que toma decisiones centralizadas sobre esta moneda sin que la población pueda interferir y que se utiliza para financiar —muchas veces— barbaridades como guerras o aeropuertos innecesarios. Al ser una moneda débil, esta va perdiendo valor progresivamente en el tiempo. Es decir, el sistema basado en monedas fiat incentiva el endeudamiento y el gasto en vez del ahorro y la inversión a largo plazo. No es de extrañar que actualmente algunos países estén en tipos de interés negativos para penalizar el ahorro e incentivar a gastar más. Este cambio nos afecta el comportamiento, aumenta nuestra preferencia temporal, nos enfocamos más en el corto que en el largo plazo, y esto tiene consecuencias en la mayoría de las áreas de nuestra vida; desde el arte, la cultura, la economía o en el hecho de emprender.

Si mis 1000 EUR de hoy tendrán menos valor en un año, tiene más sentido gastarlos hoy en vez de guardarlos; una empresa está más incentivada a endeudarse y buscar crecimiento a corto plazo que a construir pilares sólidos y crecer mirando el largo plazo. Si me endeudo hoy, lo que tendré que devolver mañana representará menos valor porque las monedas se habrán devaluado. Las monedas fiat han construido una sociedad consumista que busca gastar en vez de ahorrar, con una visión más cortoplacista y de hacer «dinero rápido», en vez de

una visión más largoplacista y por tanto construir organizaciones sólidas, nacidas después de años de esfuerzo.

## 2.8. Houston, tenemos un problema (y una solución)

Algo que está claro es que en un mundo donde la mayoría de los países tienen una deuda superior al 100 % del PIB, donde la pobreza es cada vez más común y la sensación de crisis e inestabilidad es constante, un cambio es más necesario que nunca.

Bitcoin nació por estos motivos: para ofrecer una alternativa. En un principio nadie lo vio así, ni sus creadores iniciales. De hecho, Hal Finney, uno de los máximos aportadores a su protocolo durante los primeros años, lanzó un tweet anunciando el lanzamiento de Bitcoin:


Figura 8. Tweet comunicando el lanzamiento de Bitcoin. Hal Finney

Si hubiera sabido que estaba creando lo que Bitcoin es hoy, lo habría publicado en un contexto más trascendental. El tiempo lo ha fortalecido y actualmente son muchos los argumentos y las personas que ven en Bitcoin un escape a ese sistema. En el próximo capítulo entenderemos Bitcoin, primero qué es y cómo funciona, y después veremos por qué es relevante a nivel monetario.

# 3. El nacimiento de Bitcoin

El 3 de enero de 2021 Bitcoin cumplirá exactamente doce años. Podemos decir que estos primeros años no han sido fáciles: ha sido tasado de estafa, de inútil y de fracaso incontables veces, y, aun así, hoy en día la red de Bitcoin sigue en pie, acumulando más de 300 000 MUSD de capitalización y surgiendo como una posible alternativa al sistema monetario actual.

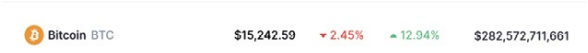



Figura 9. Capitalización de Bitcoin, coinmarketcap.com

Seguramente la pieza más importante para empezar a considerar Bitcoin como algo más que simplemente un juego es que podamos tener la certeza de que es seguro. Es decir, que podamos confiar en que esta red de dinero digital es segura y nos permite guardar y transmitir valor. Es por esto que empezaremos familiarizándonos con su funcionamiento más técnico. Entender cómo esta red consigue posicionarse como la más segura que ha existido nunca nos permitirá darle un voto de confianza para que nos podamos plantear si algún día puede reemplazar al sistema actual, o, al menos, surgir como una alternativa para todos.

## 3.1. Algunos conceptos previos

- **Red P2P o red de pares.** Es una red donde los participantes se conectan de forma directa. De tú a tú, sin intermediarios.
- **Protocolo**. Software informático que funciona como «lenguaje de la red» y permite a los participantes comunicarse y entenderse.
- **Descentralizada.** Sin una entidad central.
- **Criptografía.** Ciencia que permite encriptar información. «Cripto» proviene de ´secreto´, y «grafía» proviene de ´texto´. Hacer que un texto sea secreto.
- **Hash.** Función criptográfica que cifra una información y además permite crear una secuencia alfanumérica única; crea como una huella digital única de la información.

## 3.2. ¿Qué es Bitcoin?

Empecemos por el principio. Bitcoin es un protocolo, es decir, un programa que permite una comunicación entre ordenadores. Este protocolo está abierto a todos,

es tan fácil como descargarse el software de Bitcoin. Una vez instalado el software, pasas a formar parte de una red de ordenadores descentralizados, porque ninguna tiene más poder que otro, y que usan este protocolo para comunicarse entre ellos. El objetivo principal es permitir transacciones a través de un activo digital (bitcoin) dejando registrado todos los movimientos monetarios en un libro de contabilidad compartido por todos los ordenadores de la red conocido como Blockchain.

Aquí entran varias ideas. La primera es que los nodos son descentralizados, es decir, todos estos ordenadores que componen la red de Bitcoin son independientes. No confían entre ellos y por tanto verifican individualmente todos los movimientos de esta red. Ninguno tiene poder sobre el otro, sino que toman decisiones poniéndose de acuerdo a través de mecanismos que veremos más adelante. En segundo lugar, vemos que realmente Bitcoin es un protocolo informático. Todos estos ordenadores se descargan el software de Bitcoin, esto les permite conectarse en esta red mundial de nodos diseñada para hacer transacciones. Por último, vemos que hay una diferencia entre Bitcoin y bitcoin. Para evitar posibles confusiones, Bitcoin hace referencia a la red de nodos descentralizados y conectados gracias al protocolo, y bitcoin hace referencia al activo digital que utiliza esta red para transferir valor de un lugar a otro.

Como hemos comentado, esta innovación tecnológica se introdujo por primera vez en 2008 por Satoshi Nakamoto en un blog de ciberanarquistas de diferentes matemáticos y criptógrafos que veían en la tecnología y la criptografía una forma de empoderar al ciudadano y hacerlo más libre. Dicho de otro modo, de reducir la dependencia de entidades centrales como los gobiernos u otras instituciones.

Lo más interesante de Bitcoin es que es el primer activo que utiliza la criptografía como mecanismo para verificar las transacciones y asegurar la red a través de un hash (tecnología criptográfica) y que utiliza métodos para llegar a un acuerdo entre ordenadores descentralizados. El concepto de hash lo iremos viendo a menudo: consiste en un algoritmo matemático que transforma cualquier conjunto de datos en una serie alfanumérica de longitud fija, independientemente del mensaje. El algoritmo usado por Bitcoin se lo conoce como SHA-256.

Figura 10. Desempeño de la función hash SHA-256

El resultado siempre será una serie alfanumérica de cuarenta cifras. El objetivo del hash no es cifrar o esconder información, sino generar una especie de «huella digital» de un conjunto de datos. Por lo tanto, el objetivo del hash es validar información más que cifrarla. Otro punto interesante es que una función hash es unidireccional: es muy fácil obtener el resultado, pero es imposible saber los datos previos al hash. Por ejemplo, encontrar el hash de las palabras «Buenos días» es sencillo, pero es imposible saber que del hash «21aebc48383652046150c3663a57b1cb5bf957b5ece024deb9cbc087478cdf80» la palabra de origen es «Buenos días». Este concepto es importante porque se utilizará en muchos de los mecanismos de protección del protocolo.

## 3.3. ¿Por qué existe Bitcoin?

> *La raíz del problema del dinero convencional es toda la confianza que se requiere para utilizarlo. Debemos confiar en que el banco central no devalúe la moneda, pero la historia de todas las monedas fiduciarias está llena de violaciones de esta confianza. Debemos confiar en los bancos para guardar nuestro dinero y hacer transacciones electrónicas, pero ellos lo prestan en oleadas de burbujas crediticias con apenas una fracción en las reservas. Debemos confiarles nuestra privacidad, confiar en que no dejarán que ladrones de identidad vacíen nuestras cuentas. Sus enormes costos generales hacen que los micropagos sean imposibles.*
>
> Satoshi Nakamoto
> Cypherpunks BLOG 2009

La mejor forma de entender Bitcoin es hablar del motivo por el que se creó, compartido por su creador Satoshi Nakamoto.

En esta cita de una de sus intervenciones en el blog de cyberpunks durante la creación de Bitcoin, quedan muy claros los problemas del sistema actual y ofrece Bitcoin como una posible alternativa. Los problemas son dos:

**1. Valor del dinero**

Desde hace más de un siglo, el control de la moneda ha estado en manos de los gobiernos, completamente monopolizado. Algo cuanto menos extraño es que en un mercado libre el elemento más importante (el dinero) esté controlado por los gobiernos. Estamos en contra de los monopolios empresariales, pero ni nos planteamos el hecho de que el dinero está completamente monopolizado. Probablemente si no fuera por Bitcoin hoy seguiríamos sin conocer ni comprender qué significa esto, ya que su existencia nos ha hecho cuestionar cosas tan fundamentales como qué es realmente el dinero. Cada día, los bancos centrales —porque así se ha decidido— generan más oferta monetaria sin consentimiento alguno de la población, provocando lo que se conoce como

inflación. La realidad es que, cada año, cada español se hace un 2 % más pobre, ya que el poder adquisitivo del dinero que utilizamos para guardar la riqueza se ha devaluado. Y eso ocurre en España, un país que utiliza el euro, una moneda con políticas inflacionistas «responsables». Cuando pasamos a escenarios más caóticos como Venezuela, el poder adquisitivo de la población puede llegar a reducirse a la mitad en una semana. Las teorías monetarias predominantes actualmente defienden que una inflación moderada (2 %) es buena para la economía. Una forma de obtener financiación «robando» de manera indirecta a todos los ciudadanos de una región nunca será algo que podrá considerar bueno ni legítimo.

**2. Intermediarios**

Desde hace años la tecnología ha permitido que el dinero se encuentre principalmente en formato digital. Debido al problema del «doble gasto», para evitar que yo pueda copiar mi dinero digital y pagar dos veces con la misma moneda, ha sido necesario contar con un tercero de confianza responsable de actualizar las cuentas de cada uno y evitar este problema. Esto, a pesar de ser la única solución (antes de Bitcoin y Blockchain) nos genera una gran dependencia respecto a los bancos, dándoles un poder incalculable. Cobran altísimas comisiones, les damos acceso a toda nuestra información económica, abandonando nuestro derecho de privacidad, y, además, tampoco sabemos si están haciendo su trabajo correctamente: simplemente confiamos en ellos. Siempre estaremos expuestos a censura, bloqueo de transacciones, congelaciones de cuentas o incluso que no se nos permita retirar nuestro propio dinero.

Bitcoin se presenta como un mecanismo para transmitir valor entre personas, de forma P2P (de persona a persona) sin intermediarios, y con una política monetaria propia. Esto permite que a partir de ahora ya no tengamos que depender de los bancos comerciales para guardar o transferir dinero por el mundo y en segundo lugar que lo podamos hacer a través de un activo que no está manipulado y controlado por gobiernos o bancos centrales.

## 3.4. Bitcoin: una moneda digital única

Si volvemos a definir Bitcoin, podríamos decir que es una moneda digital, criptográfica y descentralizada que nace con el propósito de ofrecer un sistema alternativo que no requiere que confiemos a nadie los derechos de manipular las propiedades del activo que utilizamos como dinero ni la capacidad que tenemos

para guardarlo y transferirlo, ya que nadie tiene el poder de alterar las normas inicialmente establecidas.

Si le damos una perspectiva histórica, hace más de quinientos mil años que la tecnología del dinero apareció, y aunque ha pasado todo ese tiempo y las formas de dinero no han parado de evolucionar, su función principal no ha cambiado: ser un activo que permita transmitir valor entre personas y a lo largo del tiempo. Bitcoin se presenta como la última versión de este proceso evolutivo. Podríamos comparar este hecho con la industria de las telecomunicaciones.

Las tecnologías de telecomunicaciones han ido evolucionando a lo largo de los años: mensajes enviados con palomas, el telégrafo, el teléfono y finalmente internet. El objetivo ha sido siempre el mismo: transmitir información de forma eficiente entre personas. El internet se ha acabado imponiendo simplemente porque es la tecnología que mejor cumple el objetivo inicial. Además, estas tecnologías tienen un componente conocido como *network effect*.

El *network effect* se entiende a la perfección si ponemos Facebook como ejemplo. Si solo una persona tiene Facebook, la utilidad de esta red social es nula, pero si ahora son mil personas las que tienen cuenta, las conexiones posibles se disparan, crecen de forma exponencial. El internet se ha extendido tan rápidamente porque el valor que puede aportar esta red es proporcional a la cantidad de gente que la utiliza. De la misma forma, cuando más gente adopte Bitcoin como alternativa, el valor que aportará la red a cada uno de nosotros aumentará exponencialmente.

## 3.5. ¿Cómo podría Bitcoin sustituir al sistema actual?

El sistema actual nos permite poder enviar dinero (con sus condiciones) a cualquier lugar del mundo, y nos asegura que si yo tengo 1 EUR, no lo podré enviar dos veces. Este trabajo lo llevan a cabo los bancos comerciales, son los que se encargan de llevar las cuentas de todos y de establecer quién tiene qué.

Bitcoin es una red descentralizada, no hay ningún banco o ningún órgano central que determine el saldo de sus participantes o que se asegure de que las transacciones están bien hechas. Ahora veremos cómo lo consigue.

Hemos quedado en que Bitcoin es una red descentralizada; por lo tanto, para poder estar seguros de que no hay fallos y que nadie utiliza dos veces el mismo bitcoin, o que alguien diga que tiene más bitcoins los que realmente posee, la única opción es que todos estos nodos repartidos por el mundo lleven las cuentas. Es decir, ahora ya no tenemos un banco que se encargue de establecer

las cuentas y balances de cada individuo, sino que todos los ordenadores (nodos) son los que llevan las cuentas de todos los individuos, y todos registran a la vez todas las transacciones de la red. Todos tienen una copia completa de la blockchain de Bitcoin o libro contable descentralizado donde se anotan todos estos movimientos y saldos.

Ahora vemos cómo se efectuaría una transacción en este nuevo modelo. Imaginemos que Juan quiere enviar 1 BTC a Marta. Ahora Juan no debe solicitar a su banco y que este, asumiendo el control sobre su dinero, lleve a cabo la operación. Con Bitcoin, Juan deberá anunciar en la red su deseo de hacer esta transacción; a continuación, todos los nodos de la red verificarán que esta transacción es correcta, y si todos están de acuerdo, todos anotarán el movimiento y actualizarán que ahora Juan tiene 1 BTC menos en su balance y que Marta tiene 1 BTC más. Este apunte contable se producirá actualizando la blockchain, donde se ha anotado este movimiento. Bitcoin tiene valor porque sus usuarios confían en este mecanismo descentralizado, que, por cierto, no ha fallado nunca en sus casi doce años de historia.

De alguna manera, Bitcoin quita el control del dinero al banco comercial y a los bancos centrales y se lo entrega a la gente. Hace libres monetariamente a todas las personas del mundo.

> Bitcoin es al dinero lo que el internet es la información.

## 3.6. Utilizando criptografía asimétrica

Antes de seguir, haré un par de aclaraciones para poder comprender el funcionamiento de Bitcoin. Todas las personas que participan son anónimas, y esto se debe a la tecnología criptográfica de Bitcoin.

Los participantes tienen dos claves:

- **Clave pública.** Esta vendría a ser como el IBAN de tu cuenta. Consiste en un conjunto de números y letras únicos que permite a los usuarios enviar bitcoins a la dirección de algún otro usuario. Esta dirección es completamente anónima, o, mejor dicho, pseudoanónima. La blockchain es pública, por lo tanto, otros usuarios pueden ver que la cuenta X ha recibido X bitcoins, pero no podrán saber que aquella cuenta pertenece a Juan a no ser que él lo haga público. De todas formas, el número de direcciones que uno se puede crear es ilimitado, así que Juan siempre podrá asegurarse de que su privacidad sea respetada.

- **Clave privada.** Esta clave es la contraseña que permite a la red saber que Juan es el verdadero propietario de los bitcoins que quería utilizar. Esta contraseña se debe guardar correctamente, ya que en caso de perderla dejarías de tener control sobre tus bitcoins y probablemente quedarían perdidos para siempre. De nuevo, tener el poder sobre tus finanzas está ligado a una gran responsabilidad. En este sistema no hay bancos que se encarguen de todo, sino que tú eres el responsable de guardar bien tu riqueza. Como dice la famosa cita del tío de Spiderman: «Un gran poder conlleva una gran responsabilidad».

Además, cuando decimos que los nodos certifican, estos no son personas, sino ordenadores. Por lo tanto, la acción de verificar y actualizar cuentas es completamente automática. Las normas sobre cómo deben actuar estos nodos están programadas en el protocolo de Bitcoin diseñado por Satoshi Nakamoto.

Por último, necesitamos diferenciar los tipos de nodos que existen en la red:

- **Nodos que no verifican.** Estos son básicamente todas las personas que utilizan Bitcoin pero que no se han descargado el software y no tienen la copia de la blockchain guardada para acceder a la red los usuarios se descargan un wallet o billetera digital. Un wallet es básicamente un lugar digital donde una persona puede guardar sus bitcoins. Este wallet tiene una clave pública (para poder recibir bitcoins) y una clave privada (la contraseña que debe guardar el usuario y que le permite transferir estos bitcoins).
- **Nodos que verifican o full-nodos.** Estos son los ordenadores, repartidos por todo el mundo y que funcionan de forma descentralizada, que verifican todas las transacciones y que tienen una copia de la blockchain, la cual se va actualizando constantemente. Estos nodos pueden ser públicos o privados, la mayoría de ellos son privados y por tanto no se conoce con exactitud la cantidad de nodos en el mundo.
- **Nodos que verifican y archivan o nodos mineros.** Estos son los famosos mineros de la red de Bitcoin. A diferencia de los full-nodos, estos nodos, además de verificar y guardar una copia actualizada de la blockchain, son los encargados de anotar los movimientos. Es decir, primero se verifican las transacciones para todos los nodos, pero la anotación del movimiento de bitcoins a la blockchain es responsabilidad de los mineros. Una vez un minero anota un movimiento nuevo en la blockchain, todos los demás nodos actualizan este libro contable descentralizado.

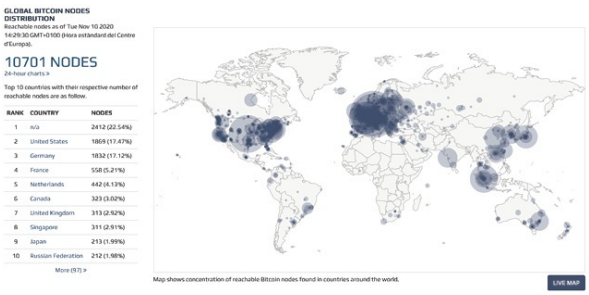


Figura 11. Distribución de nodos de Bitcoin en el mundo. bitnodes.io

## 3.7. Tecnología detrás de Bitcoin

Ya lo hemos definido, pero básicamente la blockchain es aquel libro contable donde se anotan todos los movimientos y saldos de los participantes de la red y que guarda cada uno de los nodos. Este libro contable es muy importante para que todos los nodos puedan saber si un usuario está mintiendo; por ejemplo, querer utilizar bitcoins que no tiene para hacer un pago. El nodo solo debe consultar la blockchain donde ha quedado todo registrado desde el 3 de enero de 2009.

El algoritmo de consenso es el mecanismo utilizado entre los nodos para determinar de forma descentralizada quién será el encargado de anotar las transacciones consolidadas en la blockchain (siempre un nodo minero). Como hemos dicho, en esta red no hay ningún órgano central que ponga orden, por lo tanto, el nodo minero encargado de apuntar a la blockchain se tiene que elegir de forma descentralizada y siguiendo un mecanismo con el cual podamos estar seguros de que no está mintiendo, o anotando movimientos que no se han realizado. Un ejemplo podría ser que el nodo minero anote una transacción hacia él mismo de 1000 BTC. El mecanismo de consenso debe asegurarse de que esto no sea posible.

Volvamos a repasar la vida de una transacción entre en Juan y Marta. Para hacer la transacción, Juan debe avisar a toda la comunidad y a continuación todos los nodos del mundo irán comprobando que esta transacción es correcta. Con esto me refiero a que Juan sea realmente Juan (se podrá saber a través de su firma digital hecha con la clave privada que solo él posee), que contiene las instrucciones necesarias (enviar 1 BTC a Marta) y que se demuestre, revisando la blockchain, que Juan realmente tiene 1 BTC para enviar.

Cuando todos los nodos dan por buena la transacción, esta aún no se anota en la blockchain y por tanto aún no se lleva a cabo oficialmente. Antes, irá a parar a un pool de transacciones verificadas. Un pool es un lugar digital donde se guarda

algo, en este caso, transacciones pendientes de ser anotadas en la blockchain. Es a partir de este momento cuando entran los mineros, encargados de ir agrupando estas transacciones y anotarlas en la blockchain.

Los mineros, también repartidos por todo el mundo, agrupan las transacciones en bloques de transacciones. Blockchain o cadena de bloques tiene el nombre que tiene porque este libro contable realmente está formado por bloques de transacciones relacionados matemáticamente (criptográficamente) entre ellos. Los mineros en este momento competirán entre ellos para ser los elegidos y poner su bloque en la blockchain. De nuevo hay que tener en cuenta que, aunque los mineros sacan las transacciones del mismo pool, no todos los bloques propuestos serán iguales, ya que hay muchas transacciones cada minuto.

Esta competición es muy sencilla: básicamente deberán dedicar «fuerza computacional» para encontrar un número aleatorio. El primero en encontrar este número tendrá el privilegio de anotar un nuevo bloque en la blockchain y recibirá una recompensa a cambio. Actualmente, la recompensa es de 6,25 BTC. Estas inscripciones en la blockchain tienen lugar cada diez minutos, por lo tanto, la nueva oferta de Bitcoin no depende de cuántas máquinas estén extrayendo como ocurre con el oro, o de un órgano central que puede emitir tanto nuevo dinero como quiera.

La nueva oferta monetaria está dictada por un protocolo informático defendido por cientos de miles de ordenadores repartidos por el mundo. Esto aporta una propiedad única a Bitcoin: la nueva oferta monetaria es pública y se puede prever. Todo el mundo puede estar seguro de que mañana no habrá 1000 BTC más, como puede ocurrir con las monedas fiat o el oro. Bitcoin muestra características que lo pueden convertir en el mejor mecanismo de valor reserva del mundo.

## 3.8. El halving de Bitcoin

Algunas aclaraciones antes de continuar. Estos bloques tienen una capacidad máxima de un mega, que equivale a unas 2700 transacciones. Cada bloque tiene un identificador único, su hash. Los bloques se generan cada diez minutos y la recompensa que da la red se va reduciendo a la mitad cada cuatro años. Por tanto, los primeros bloques de Bitcoin confirmados por los mineros permitían a estos últimos obtener una recompensa de 50 BTC por bloque. En 2012, tuvo lugar el halving, momento en el que la recompensa pasó a ser de 25 BTC por bloque. En 2016 tuvo lugar el segundo halving, reduciendo la recompensa a 12,5

BTC por bloque. Finalmente, este 2020 tuvo lugar el tercer halving, haciendo que, hoy en día, la recompensa por bloque sea de 6,25 BTC.

Este evento suele estar ligado a momentos de grandes subidas en el valor de Bitcoin. Al final, esto es comprensible: si un activo digital limitado tiene un precio en función de la oferta y la demanda, si la oferta de nuevos bitcoins se divide en dos y en cambio la demanda se mantiene o aumenta, el precio sube.

Figura 12. Ciclos de halving de Bitcoin. Tradingview

Dejando de lado la parte especulativa y recuperando la idea de Bitcoin como mecanismo para guardar valor, volvemos a ver cómo realmente Bitcoin puede convertirse en unos años en el mejor activo que hemos visto nunca. No se pueden crear más bitcoins de los que determina el sistema (x bitcoins por cada bloque confirmado). Estos nuevos bitcoins que reciben los mineros como recompensa se reducen a la mitad cada cuatro años. Si hacemos los cálculos, la cantidad de bitcoins generados llegará a 0 aproximadamente el 2140, cuando se llegue exactamente a la cantidad máxima de bitcoins (también determinado por el sistema), que son 21 000 000 de unidades.

Cada cuatro años, la inflación de Bitcoin irá bajando, siendo inferior que el oro (el mejor activo en términos de stock-to-flow) a partir de 2024, con el cuarto halving. Tocaremos estos aspectos cuando analicemos Bitcoin con un punto de vista monetario.

## 3.9. El algoritmo de consenso: proof-of-work

Volvamos revisar la forma en que se registran las transacciones. Hemos dicho que para determinar cuál será el minero responsable de anotar el nuevo bloque, este tendrá que encontrar un número aleatorio y el primero de todos los mineros del mundo que lo encuentre, lo anunciará a los demás, el resto confirmará si están de acuerdo y, en caso afirmativo, el minero tendrá derecho a anotar el nuevo bloque y recibir la recompensa. Este proceso se conoce como proof-of-work y ahora profundizaremos un poco más sobre cómo funciona.

El proof-of-work es un sistema que surgió durante los años 90, inventado por Adam Back, para evitar el spam. Algunos años después, Satoshi Nakamoto utilizó esta innovación desconocida para hacer de Bitcoin una red extremadamente segura y robusta. La idea era la siguiente: para evitar correos spam, cada vez que una persona envía un correo, el ordenador tiene que resolver un cálculo matemático que le consume energía (y por lo tanto dinero). De esta manera no se envían muchos mensajes seguidos a modo de spam porque debería gastar demasiado tiempo y dinero (ya que la fuerza de cálculo del ordenador consume energía). El sistema desincentiva a los usuarios a enviar mensajes spam.

Aplicado a Bitcoin, tiene el mismo objetivo: como hay que gastar energía para resolver estos problemas, un minero que quiera «verificar transacciones falsas» simplemente solo conseguirá perder dinero. Es decir, desincentiva querer manipular la red. Primero, porque encontrar este número aleatorio tiene un alto coste energético; y segundo, porque antes de verificarlo todos los mineros deben aprobar el bloque; y, si este bloque está manipulado, sencillamente no lo aceptarán. Por tanto, el proof-of-work consigue que solo tenga sentido participar en hacer la red de Bitcoin más segura si no quieres engañar, ya que es la única forma de obtener una recompensa y para contrarrestar los costes que tiene el querer participar. Por otro lado, el resto de los mineros aceptarán rápidamente cualquier bloque que sea correcto porque así no pierden tiempo ni dinero en aportar capacidad de cálculo para intentar minar el siguiente bloque. **El proof-of-work consigue que un minero obtenga el máximo rendimiento cuando actúa de la forma más justa y honesta, por la red**.

Veamos cómo está formado un bloque de la blockchain de Bitcoin para así comprender cómo se aplica el proof-of-work:

- Primero tenemos el hash del bloque anterior.
- Después el timestamp, para determinar la hora exacta en la que se ha creado el bloque.
- A continuación, la raíz de Merkle de las transacciones, es decir, todas las transacciones del bloque se encuentran hasheadas y representados en un árbol de Merkle, incluyendo en el bloque el hash resultante.
- Ahora aparece el nonce, que es simplemente aquel número que los mineros tienen que descubrir para poder anotar el bloque y recibir la recompensa.
- Y, por último, tenemos el HASH del bloque, que sale hacia al siguiente. De aquí el término de que los bloques están encadenados: están unidos siempre por un hash de entrada y salida.

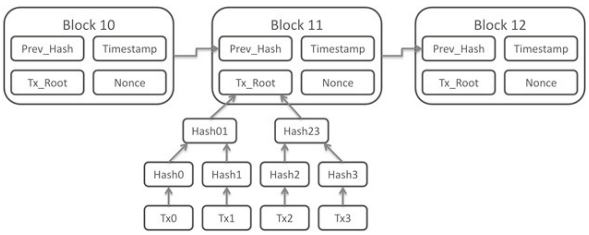


Figura 13. Incorporación de transacciones (hasheadas) en bloques y configuración de cabeceras

Para entender mejor el último término introducido, el nonce, debemos introducir el concepto de dificultad. El protocolo de Bitcoin dice que los bloques se deben pasar por un hash siempre, y este hash debe comenzar por un número X de ceros. Por lo tanto, los mineros tendrán que encontrar el número (nonce) que, haciendo el hash del bloque, dicho bloque empiece con el número de ceros necesarios. Antes hemos visto que la función hash es unidireccional, así que la única forma de encontrar tal número es por fuerza bruta. Gastar enormes cantidades de energía para probar números de forma aleatoria hasta encontrar el correcto.

El número de ceros va cambiando para aumentar la dificultad del problema y asegurar que los bloques se minen siempre cada diez minutos. Por ejemplo, si hoy hay cinco mineros y entre los cinco tardan diez minutos en descubrir el nonce, y por tanto en anotar un nuevo bloque, si el día siguiente hay diez mineros, la lógica nos dice que ahora tardarán cinco minutos en encontrar el nonce. Para evitar esto y asegurar que siempre se tarde de media diez minutos por bloque, y así hacer de Bitcoin un sistema monetario con una inflación programada y controlada, se utiliza la dificultad. Esta se basa en modificar el número de ceros con lo que debe comenzar el hash cada nuevo bloque. Si hay muchos mineros, aumentará el número de ceros para hacer más difícil el cálculo, y si hay menos, se reducirá ese número de ceros, siempre asegurando que todos los mineros juntos tarden de media diez minutos en descubrir el nonce.

El hash es como nuestra huella dactilar, es muy fácil encontrarla cuando tenemos nuestro dedo, pero es muy difícil saber a quién pertenece si solo tenemos la huella. El hash funciona igual, es muy fácil para los otros mineros ver si el nonce descubierto por uno de los mineros es correcto. La parte complicada es encontrar el número (nonce) con el cual el hash del bloque empiece con los ceros necesarios. Otra comparación son los sudokus, revisar si está bien no es complicado, pero resolverlos sí lo es.

Figura 14. Aplicación práctica de la función hash aplicando algoritmo SHA-256.
https://www.keycdn.com/support/sha1-vs-sha256

Por otro lado, hemos visto que cada bloque empieza anotando el hash del bloque anterior. Esto permite que los bloques estén vinculados matemáticamente. De nuevo por eso se conoce como cadena de bloques, porque estos están ligados como una cadena. Cambiar un dato de la blockchain es prácticamente imposible ya que, cambiando un pequeño dato, el resultado del hash del bloque cambia y por tanto no coincide con el anotado en el bloque siguiente.

## 3.10. Bitcoin: la red más segura del mundo

Hemos visto cómo funciona técnicamente Bitcoin, ahora iremos viendo cómo cada uno de los mecanismos que hemos comentado sirve como barrera de seguridad de la red. Vamos a poder determinar que Bitcoin es una red segura y que podemos confiar en ella para guardar y transmitir valor.

**Caso 1. Realizar una transacción falsa, por ejemplo, enviar bitcoins que no tenemos**

Este problema se soluciona en la primera capa de seguridad, los full-nodos. Estos serán los primeros en recibir la transacción y deberán revisar que sea correcta. Al revisar la blockchain y ver que este agente no tiene los bitcoins que dice que quiere enviar, la transacción se cancela. Además, aunque un nodo la dé por buena, no es suficiente, deben ser todos (un 70 % de la red aproximadamente) los que afirmen que la transacción es correcta. Al ser una red descentralizada, las transacciones las revisan todos individualmente; por mucho que un nodo afirme que la transacción es correcta o falsa, cada nodo se asegurará él mismo. Primer posible ataque solucionado.

**Caso 2. Cambiar información de bloques pasados**

Otro intento por falsificar información y dañar la reputación de Bitcoin (debemos tener en cuenta que el mínimo error del sistema conllevaría una pérdida absoluta de la confianza que la gente ha depositado en Bitcoin) es el hecho de cambiar la información de bloques pasados.

Imaginemos que puedo acceder a la blockchain de Bitcoin y hacer un cambio referente al número de bitcoins que recibí hace una semana. Cada bloque tiene incorporado el hash del bloque anterior. Por tanto, el mínimo cambio provocaría que el hash dejara de coincidir y automáticamente toda la red detectaría y desaprobaría el cambio que se está intentando hacer. En segundo lugar, si se quisiera sacar adelante, antes se debería manipular prácticamente la mayoría de los nodos de la red (aproximadamente unos cuarenta mil). Además debería superar en fuerza computacional a todos los mineros, ya que tendrían que volver a minar todos los bloques para poder conseguir el nuevo hash.

Como aclaración, la red de Bitcoin es, con muchísima diferencia, la red más grande, más segura y con más fuerza computacional del mundo. Podríamos llegar a afirmar que es más factible hackear la NASA, la CIA y la Reserva Federal a la vez de intentar cambiar bloques de la red de Bitcoin.

### Caso 3. La red se satura porque hay muchos mineros intentando mentir

Este podría ser uno de los grandes problemas, que la red se saturara porque hay demasiados individuos poniendo freno a las confirmaciones de los bloques, demasiados agentes malignos que buscan atacar el sistema.

El algoritmo de consenso y los incentivos económicos nativos de la red hacen tan poco atractivo a nivel económico la existencia de este tipo agente, que consigue que todos los mineros sean honestos. Si recordamos, un minero maligno estaría continuamente gastando grandes cantidades de electricidad solo para frenar la red, sin recibir nada a cambio. Realmente, si este agente existe, en pocos días acabaría actuando de forma honesta y ayudando a la red a ser más segura, porque al menos actuando así recibe bitcoins a cambio y podría compensar los enormes gastos de estar compitiendo con otros mineros para encontrar el nonce.

### Caso 4. Ciertos mineros controlan más del 51 % de la red

Este es uno de los problemas más grandes de todas las blockchains: que un solo individuo o grupo controle más del 51 % y, por lo tanto, tenga suficiente fuerza como para manipularla o cambiar las normas. En el caso de Bitcoin, este ataque podría haber sido posible durante sus primeros años de vida, cuando la red era muy débil y no estaba defendida por miles de ordenadores repartidos por el mundo. Hoy, un ataque del 51 % a Bitcoin significa lo siguiente:

Primero, controlar más de la mitad de los nodos y superar por mayoría a gran parte de los mineros del mundo, lo que equivale a millones de ordenadores funcionando día y noche y gastando barbaridades en electricidad. Además, esto

tampoco garantizaría su éxito. Realmente, un ataque así solo podría darse por parte de un gobierno o la unión de varias potencias. El hecho es que, si sucede, sería una gran confirmación de que Bitcoin es útil y que es necesario para tener un mundo más justo; y segundo, este agente solo tendría poder sobre la red durante diez minutos, ya que después, si toda la comunidad está de acuerdo, se puede actualizar el código, romper la cadena en una nueva y expulsarlo. Bitcoin se habría visto muy debilitado por el ataque, pero seguiría existiendo y seguiría creciendo de nuevo. Este fenómeno se conoce como hard fork.

**Caso 5. Los mineros pueden cambiar las normas y modificar una nueva política monetaria**

Aquí nos volvemos a encontrar en un escenario prácticamente imposible. Los mineros no tienen poder por sí solos para elegir el futuro de Bitcoin. De hecho, esto quedó demostrado con el caso Segwit.

En el caso de Segwit (una actualización que permitía aumentar el número de transacciones en un bloque sin cambiar su tamaño) los nodos anunciaron que a partir de ese momento no aceptarían ningún bloque que no tuviera incorporado Segwit. Se comportaron así porque ciertos mineros se negaban a actualizar el software, ya que no ganaban nada haciéndolo (aunque tampoco perdían). No obstante, los mineros vieron cómo de un día para otro toda su actividad productiva podría desaparecer si no aceptaban los requisitos que plantearon los nodos. Terminaron aceptando la actualización de Segwit porque corrían un grave riesgo de que los nodos dejaran de aceptar sus bloques en la cadena.

Además, tenemos que recuperar el concepto de teoría de juegos: todos tienen intereses diferentes (nodos, desarrolladores, usuarios y mineros) y ninguno puede imponer sus condiciones, ya que suelen ser contradictorias con respecto al beneficio generado en cada grupo. Esto hace de Bitcoin una red sólida, robusta y muy difícil de cambiar. Algunos verán este hecho como algo negativo de Bitcoin, ya que lo hace menos flexible y seguramente más lento. Pero seguramente es de lo más valioso de esta red. El pilar más importante de algo que se utiliza como dinero es la confianza, y esta robustez te asegura que puedes confiar que las normas de Bitcoin no van a poderse cambiar así como así.

**Caso 6. Se puede crear un nuevo bitcoin y «ya está»**

Revisemos este concepto. ¿Es cierto que la devaluación de la moneda de Zimbabwe o de Venezuela afecta el dólar? No. De hecho, solo demuestra que el dólar y el bitcoin son más valiosos que las otras dos. Como ya se ha comentado, los forks (nuevas monedas nacidas de una anterior, por ejemplo: Bitcoin Cash) y

altcoins (monedas alternativas) ayudan a Bitcoin a demostrar que es mucho más sólido y seguro, aunque esto no imposibilita la existencia de otras blockchains con otros sistemas monetarios. De hecho, siempre habíamos tenido diversas formas de valores reserva en función de su utilidad. El oro se utilizaba para guardar grandes cantidades de mucho valor, pero para pagos más pequeños y diarios se usaba o bien la plata o el bronce. También hay que tener en cuenta que estas nuevas formas de dinero programable no solo permiten crear políticas monetarias, sino también lógicas de negocio y de distribución de riqueza, así que es difícil creer que existirá solo una moneda digital. Eso sí, tengo la creencia de que es difícil que ninguna de ellas supere a Bitcoin como valor reserva.

## 3.11. ¿Supone Bitcoin una revolución monetaria?

Una vez analizada desde una perspectiva técnica, podemos decir con conocimiento de causa que Bitcoin es una red segura y robusta en la que podemos confiar para transmitir y guardar valor.

La siguiente pregunta es si resulta inteligente hacerlo; que sea segura no significa que sea atractiva como valor reserva, o que tenga unas características propias de una moneda sólida, en la que no solo podamos confiar porque sus mecanismos de seguridad son indestructibles, sino que además podamos ver Bitcoin como una buena opción para guardar nuestra riqueza a largo plazo.

Este punto de vista lo analizaremos en el siguiente capítulo, donde también aprovecharemos para comparar las características monetarias de Bitcoin con las de las monedas fiat.

Por último, simplemente remarcar que, de todo lo que hemos visto de Bitcoin, lo más relevante no es que esta moneda podría llegar a aumentar mucho su valor, o que ahora nos deberíamos preocupar porque hay una moneda descentralizada que se puede usar para financiación ilegal. Lo más importante de todo es que por primera vez en la historia tenemos a nuestra disposición una tecnología que nos permite guardar y mover valor por todo el mundo, de forma digital y al instante, de manera privada y segura, que está abierta a todo el mundo sin discriminar a nadie y que funciona sin intermediarios ni agentes centrales con el poder de manipular la red y el activo de circula sobre ella. Esto es, sin lugar a dudas, una revolución.

# 4. Bitcoin como alternativa a los bancos centrales

## 4.1. Repasando las características del dinero

El dinero es una herramienta que nos permite mover valor a través del tiempo y el espacio. Muchos materiales pueden servir para ello, por eso nos encontramos que el dinero establecido en una sociedad evoluciona de forma natural dentro del libre mercado. El mercado escoge, en función de lo bien que esa mercancía cumpla su función final, cuál es el material más intercambiable para acceder a productos y servicios dentro de la economía.

Para valorar la efectividad del dinero, nos fijamos en su vendibilidad; determinada a su vez por tres aspectos:

- Valor reserva.
- Medio de cambio.
- Unidad de cuenta (consecuencia de los dos primeros).

| Traits of Money | Gold | Fiat (US Dollar) | Crypto (Bitcoin) |
|---|---|---|---|
| Fungible *(Interchangeable)* | High | High | High |
| Non-Consumable | High | High | High |
| Portability | Moderate | High | High |
| Durable | High | Moderate | High |
| Highly Divisible | Moderate | Moderate | High |
| Secure *(Cannot be counterfeited)* | Moderate | Moderate | High |
| Easily Transactable | Low | High | High |
| Scarce *(Predictable Supply)* | Moderate | Low | High |
| Sovereign *(Government Issued)* | Low | High | Low |
| Decentralized | Low | Low | High |
| Smart *(Programmable)* | Low | Low | High |

Figura 15. Comparativa de tipos de dinero

Por tanto, el propósito del dinero nunca cambió. Lo que cambia es la tecnología que utilizamos, la cual vive en un proceso evolutivo constante impulsado por el libre mercado. Cuanto más resistente sea una moneda a su dilución en el tiempo a través de, por ejemplo, la inflación, el deterioro o la falsificación, mejor valor reserva será. Una vez que una nueva forma de dinero pasa el umbral del valor reserva y su adopción empieza a aumentar, compite teniendo en cuenta otras características secundarias:

- **Escasez.** Permite ser resistente a la manipulación de la oferta.
- **Divisibilidad**. Fácilmente separable y combinable.
- **Portabilidad**. Capacidad de poder llevar mucho valor en poco espacio.
- **Durabilidad.** Su resistencia al deterioro.

- **Reconocibilidad**. Fácilmente verificable.

Como hemos visto, el tipo de dinero utilizado ha estado en constante cambio a lo largo de la historia. Desde conchas, sal, piedras preciosas, hasta llegar al papel moneda gubernamental. Bitcoin se presenta como la última evolución en los sistemas monetarios.

Las tecnologías monetarias también evolucionan a lo largo del tiempo en función de sus características. El aspecto más importante de estas es su solidez o escasez. En inglés, este término se conoce como sound money. Esta propiedad determina la capacidad del dinero de actuar como valor reserva, cuantificable a través de la *stock-to-flow-ratio*. El cálculo consiste en dividir el stock total de un material con la nueva oferta que entra en la economía anualmente. Cuanto más alto sea la ratio, más «dura» o «sólida» será la moneda.

La solidez de alguna forma describe la dificultad o el coste de producir una nueva unidad monetaria. El oro ha sido una moneda de referencia durante miles de años porque su solidez se ha basado siempre en el coste de extracción por unidad monetaria. Como la extracción funciona siempre que el coste de extraer una onza sea inferior al valor de esa onza, esto permite que la nueva oferta de oro introducida en la economía siempre ronde entre el 1 % y el 1,5 %, convirtiéndolo en una moneda sólida.

El dinero es un tipo de tecnología fiel al concepto de *winner takes all*. Aquellos que fracasan en adoptar la moneda más sólida disponible (la que mejor actúa como valor reserva) ven cómo, cada año, su valor se devalúa en comparación a aquellos que han adoptado una mejor versión de dinero. Esto ha sucedido a lo largo de la historia constantemente, sucede hoy entre monedas estatales (inevitable porque el gobierno de cada país hace obligatorio, por ley, usar su moneda. Aunque el dólar sea más sólido que el peso, muchos países siguen usando el peso por cuestiones legales y de anti libre mercado), pero también ha sucedido cuando algunos países adoptaron el patrón oro y otros el patrón plata. Este fue el caso de China y la India, que no quisieron introducir un patrón basado en oro y después de varios años el valor del país se había devaluado casi un 50 % respecto a aquellos que sí usaban oro como moneda principal. Por eso el oro se ha posicionado siempre arriba de todo durante la historia, simplemente por su superioridad en solidez y gracias a su alto stock-to-flow.

| | Stock (tn) | Flow (tn) | SF | Price $/Oz | Market Value |
|---|---|---|---|---|---|
| Gold | 185,000 | 3,000 | 62 | $1300 | $8,417,500,000.000 |
| Silver | 550,000 | 25,000 | 22 | $10 | $308,000,000.000 |
| Bitcoin (BTC) | 15,200,000 | 656,250 | 23 | $11,500 | $174,800,000,000 |
| Palladium | 244 | 125 | 1.1 | $1400 | $11,956,000.000 |
| Platinum | 86 | 229 | 0.4 | $800 | $2,400,000.00 |

Figura 16. Comparativa en la capitalización de distintas formas de dinero

El oro es el valor reserva referente en el mundo, con el que hemos podido vivir expansiones económicas y comerciales que nos han permitido llegar a donde estamos hoy. Al ser físico, tiene muchas ventajas; precisamente esta propiedad lo convierte en «dinero soberano». Tenemos una tecnología monetaria que permite almacenar valor y transaccionar de forma segura y confiable sin riesgo de tener que contar con una contraparte.

Su propietario es el poseedor de ese oro, y, por tanto, no hacen falta bancos ni intermediarios de pagos que puedan censurar o revertir transacciones dentro del mercado libre; no necesitas confiar en nadie para poder utilizarlo.

Si lo comparamos con las monedas fiat como el USD, estas tienen, de forma implícita, el riesgo de una contraparte asociado. Esta contraparte tiene el poder de diluir la moneda a través de la inflación, además del de desautorizar el valor de ese dinero. No hace mucho, la India prohibió todos los billetes de quinientas rupias sin ni siquiera pedir permiso. Es un sistema repleto de intermediarios de pago, todos ellos con el poder de censurar, revertir y vigilar nuestras transacciones.

Por otro lado, la fisicalidad del oro también tiene ciertas desventajas asociadas. Lo físico hace que las propiedades como la divisibilidad y la portabilidad no sean muy buenas (este fue un motivo por el cual el papel moneda respaldado por oro era mucho más vendible). Esta tecnología era un híbrido del oro, una tecnología de segunda capa. Su intención era buena, pero de nuevo quedó demostrado que la tentación de los gobiernos de manipular la moneda es superior a ellos. ¿A quién no le gustaría tener una máquina de hacer dinero en casa?

El patrón oro nos condujo a la centralización del oro por parte de los bancos centrales, y estos aprovecharon la ocasión para emitir su propio dinero, respaldado por nada, simplemente por fe y promesas de capacidad de devolución de la deuda en el largo plazo. Desde ese momento, el libre mercado del dinero desapareció: solo existía un tipo de dinero y era el que el banco central controlaba. Y a pesar de que hoy en día esto sea algo «normal», nada otorga más poder a una organización que el hecho de controlar la moneda en circulación. Hoy, la inflación es la gran solución a todo, aumentando cada vez más la diferencia entre ricos y pobres.

Este sistema de reserva fraccionaria acabó estallando con el Nixon Shock en 1972, donde se eliminó de forma «temporal» el patrón oro. A partir de entonces llegamos a la era de un dinero basado en deuda y política, respaldado por los

futuros cash flows generados por las autoridades. Estos «esclavizan» (disculpas por la agresividad del término, pero creo que lo define de forma muy acertada) a las futuras generaciones, ya que estas deberán devolver, a través de impuestos, las barbaridades de los gobernantes anteriores. Sin ir más lejos, hoy España debe más del 100 % del PIB, y son los jóvenes los que tendrán que saldar esta deuda.

## 4.2. Bitcoin como activo soberano y digital

Bitcoin es el primer activo soberano en forma digital. Con él las transacciones son incensurables, irreversibles e imparables; su propietario es el poseedor de las claves privadas que le dan acceso a mover X cantidad de bitcoins almacenados en un wallet digital pseudónimo.

Es el primer activo con una escasez absoluta. La stock-to-flow-ratio que nos ayuda a medir la solidez de una moneda aumenta inevitablemente cada cuatro años, con cada halving, que reduce a la mitad la cantidad de bitcoins generados por cada bloque. A partir de 2024, con el cuarto halving, su ratio será el doble que la del oro, convirtiéndose, en tan solo quince años desde de su aparición, en el activo con mayor capacidad de transferir valor en el tiempo y el espacio que hemos tenido nunca. Será el dinero más sólido que haya existido. Esta capacidad para aumentar la robustez de la moneda se consigue gracias a «la dificultad»; método que permite aumentar la complejidad de minar un bloque para que este siempre tarde diez minutos de media en confirmarse. Este proceso requiere energía debido al proceso del proof-of-work. De alguna forma, no es casualidad que este proceso se conozca como mining, ya que su funcionamiento es muy similar a la extracción del oro.

Gracias a este sistema deflacionario, con una emisión controlada y previsible, Bitcoin representa el primer activo con una oferta perfectamente inelástica, es decir, los cambios en el precio no tienen ningún impacto en el nivel de emisión de nuevo dinero. Con el oro, cuando este sube, el margen para extraer oro aumenta, ya que será más rentable extraer más oro, y por tanto su oferta aumentará cuando esto suceda. Esto no solo es increíble por la robustez que aporta a la moneda, sino también por la transparencia que ofrece al sistema. Hoy, los bancos centrales son opacos y para nada transparentes. Con Bitcoin, cada movimiento, cada transacción, es visible, y conocemos la cantidad de dinero en circulación y emitido en cada momento, cada año e incluso cada década. Bitcoin es el rey de la transparencia; sin duda el dinero más confiable y predecible que ha existido.

Todos los tipos de monedas han seguido este proceso natural que les ha llevado a perder valor, algunos de una forma más exagerada y algunos menos:

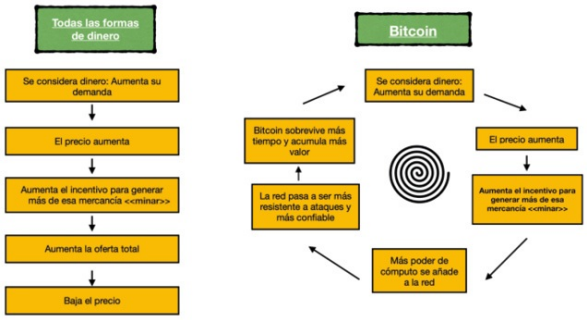



Figura 17. Ciclos del dinero en Bitcoin vs. otras formas. Elaboración propia

Al contrario que cualquier otra forma de dinero, con Bitcoin no se puede aumentar la masa monetaria más de lo que lo rige el protocolo. Ninguna otra moneda ha conseguido cumplir la función de conservar valor en el tiempo tan óptimamente como Bitcoin. Esto permite que no solo podamos depositar una confianza sin precedentes en la moneda como valor reserva, sino que convierte Bitcoin en una especie de agujero negro: siempre habrá alguien a quien le será rentable alimentarlo y hacerlo más seguro. Es prácticamente irónico pensar que desaparecerá o dejará de crecer en valor. Aunque ahora el precio de Bitcoin baje mucho y que a la mayoría de los mineros ya no les fuera rentable aportar seguridad a la red, la dificultad bajaría y nuevos mineros entrarían en busca de rentabilidad. Ello volvería a provocar que la red fuera más segura y volvería a promover el uso y la adopción. Es un círculo virtuoso muy difícil de romper.

Con el tiempo, una vez Bitcoin alcance los 21 000 000 de tokens generados (alrededor del año 2140), la stock-to-flow habrá llegado a infinito. Será la primera forma de dinero en conseguirlo, convirtiéndose, sin lugar a dudas, en el activo con la política monetaria más confiable y sólida del mundo, además de ser totalmente transparente e incambiable. En la blockchain todo es permanente. Esta idea rompe, por ejemplo, con un tratado económico publicado por Julian Simon llamado *El último recurso*[1], donde especifica que no hay forma de saber cuánto hay de una mercancía concreta, ya que nunca en la historia hemos dado con algo que fuera finito al 100 %. Incluso el oro, uno de los elementos más escasos de nuestro planeta, sigue aumentando su oferta monetaria entre 1 % y 1,5 % anualmente. Según Simon, la única forma de medir la cantidad de algo era comparar cuánto tiempo teníamos para extraerlo. Bitcoin, por primera vez, ha creado la escasez real, solo van a existir 21 000 000 de bitcoins. Ni uno más.

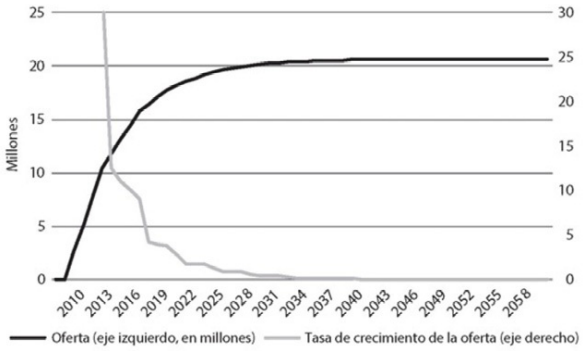


Figura 18. Oferta de Bitcoin y tasa de crecimiento de la oferta

# 4.3. Bitcoin frente a dinero fiat

Fiat hace referencia a todas aquellas monedas emitidas «por decreto» por un banco central (*fiat*, en latín, es ‘hágase’). Tales monedas siguen unas políticas monetarias independientes escogidas centralizadamente por instituciones gubernamentales. Estas son inciertas (no sabes de antemano cuáles van a ser las variaciones para el próximo año) y opacas (ya que es prácticamente imposible saber qué movimientos concretos de dinero han llevado a cabo), y siempre estarán sujetas a cambios por parte de sus dirigentes. Con el tiempo las sociedades deberán decidir en quién confiar, si en burócratas con intereses propios o en las matemáticas.

| Halving Date | Halving Year | Flow/Block | Flow/Day | Flow/Year | Flow/Halving | Total Stock | Stock-to-Flow Ratio | S2F Multiple of 2020 |
|---|---|---|---|---|---|---|---|---|
| 2020-05-15 | 2020 | 6.250000000 | 900.000000000 | 328,725.00 | 1,314,900.00 | 19,673,337.50 | 59.85 | 1.00 |
| 2024-05-15 | 2024 | 3.125000000 | 450.000000000 | 164,362.50 | 657,450.00 | 20,330,787.50 | 123.69 | 2.07 |
| 2028-05-15 | 2028 | 1.562500000 | 225.000000000 | 82,181.25 | 328,725.00 | 20,659,512.50 | 251.39 | 4.20 |
| 2032-05-15 | 2032 | 0.781250000 | 112.500000000 | 41,090.63 | 164,362.50 | 20,823,875.00 | 506.78 | 8.47 |
| 2036-05-15 | 2036 | 0.390625000 | 56.250000000 | 20,545.31 | 82,181.25 | 20,906,056.25 | 1,017.56 | 17.00 |
| 2040-05-15 | 2040 | 0.195312500 | 28.125000000 | 10,272.66 | 41,090.63 | 20,947,146.88 | 2,039.12 | 34.07 |
| 2044-05-15 | 2044 | 0.097656250 | 14.062500000 | 5,136.33 | 20,545.31 | 20,967,692.19 | 4,082.22 | 68.21 |
| 2048-05-15 | 2048 | 0.048828125 | 7.031250000 | 2,568.16 | 10,272.66 | 20,977,964.84 | 8,168.67 | 136.49 |
| 2052-05-15 | 2052 | 0.024414063 | 3.515625000 | 1,284.08 | 5,136.33 | 20,983,101.17 | 16,340.94 | 273.04 |
| 2056-05-15 | 2056 | 0.012207031 | 1.757812500 | 642.04 | 2,568.16 | 20,985,669.34 | 32,685.87 | 546.15 |
| 2060-05-15 | 2060 | 0.006103516 | 0.878906250 | 321.02 | 1,284.08 | 20,986,953.42 | 65,375.74 | 1,092.37 |
| 2064-05-15 | 2064 | 0.003051758 | 0.439453125 | 160.51 | 642.04 | 20,987,595.46 | 130,755.48 | 2,184.81 |
| 2068-05-15 | 2068 | 0.001525879 | 0.219726563 | 80.26 | 321.02 | 20,987,916.48 | 261,514.96 | 4,369.70 |
| 2072-05-15 | 2072 | 0.000762939 | 0.109863281 | 40.13 | 160.51 | 20,988,076.99 | 523,033.92 | 8,739.46 |
| 2076-05-15 | 2076 | 0.000381470 | 0.054931641 | 20.06 | 80.26 | 20,988,157.24 | 1,046,071.85 | 17,478.98 |
| 2080-05-15 | 2080 | 0.000190735 | 0.027465820 | 10.03 | 40.13 | 20,988,197.37 | 2,092,147.70 | 34,958.06 |
| 2084-05-15 | 2084 | 0.000095367 | 0.013732910 | 5.02 | 20.06 | 20,988,217.44 | 4,184,299.39 | 69,916.14 |
| 2088-05-15 | 2088 | 0.000047684 | 0.006866455 | 2.51 | 10.03 | 20,988,227.47 | 8,368,602.79 | 139,832.35 |
| 2092-05-15 | 2092 | 0.000023842 | 0.003433228 | 1.25 | 5.02 | 20,988,232.48 | 16,737,209.57 | 279,664.76 |
| 2096-05-15 | 2096 | 0.000011921 | 0.001716614 | 0.63 | 2.51 | 20,988,234.99 | 33,474,423.14 | 559,329.59 |
| 2100-05-16 | 2100 | 0.000005960 | 0.000858307 | 0.31 | 1.25 | 20,988,236.25 | 66,948,850.28 | 1,118,659.24 |

Figura 19. Bitcoin es transparente y predecible por cálculos matemáticos

La superioridad de Bitcoin en cuanto a robustez simplemente se impondrá. La historia nos demuestra que un dinero sólido no puede ser ignorado. ¿Qué pasará cuando cada persona, desde las usuarias del dólar a los pesos, los euros o cualquier otra moneda, presencie cómo cada año su moneda va perdiendo valor respecto al bitcoin? Todas y cada una de esas monedas, por su funcionamiento intrínseco, tienden a perder valor. En cambio, el bitcoin, también por su funcionamiento intrínseco, tiende a aumentar de valor. En ese momento deberemos decidir en qué activo queremos conservar y almacenar nuestra riqueza: ¿en uno que pierde valor cada año, o en uno que tiende a aumentar su valor?

| Año | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 |
|---|---|---|---|---|---|---|---|---|---|
| Oferta total de Bitcoin (millones) | 17.415 | 18.055 | 18.527 | 18.855 | 19.184 | 19.512 | 19.758 | 19.923 | 20.087 |
| Tasa de crecimiento anual (%) | 3,82 | 3,68 | 2,61 | 1,77 | 1,74 | 1,71 | 1,26 | 0,83 | 0,82 |

Figura 20. Inflación anual en bitcoins. Fuente: *El patrón Bitcoin*

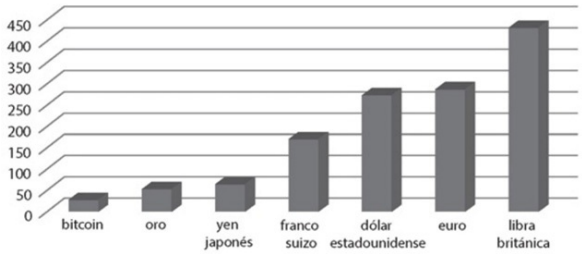



Figura 21. Proyección del incremento anual de la masa monetaria en 25 años. *El patrón Bitcoin*

Al fin y al cabo, tenemos una realidad frente a nosotros. Tenemos a Bitcoin, que representa la forma de dinero más sólida y robusta que hemos tenido nunca, compitiendo directamente con las monedas fiat, quizás el tipo de moneda más débil de la historia. Mientras Bitcoin siga existiendo, este seguirá superando en el libre mercado al oro y a las monedas fiat, del mismo modo que también su capitalización seguirá aumentando. Todos aquellos que holdeen* versiones más débiles de dinero como las fiat o incluso el oro, verán cómo gradualmente se van depreciando respecto al bitcoin.

La moneda más sólida siempre había sido escogida por el libre mercado. Por ejemplo, el oro, que se proclamó valor reserva por excelencia por sí solo, estuvo durante más de cinco mil años manteniendo su posición. La entrada de bancos centrales acabó desplazando al oro. Parece que estamos a punto de presenciar cómo surge, de nuevo, una moneda sólida escogida por el mercado. De hecho, no hay nada que encaje mejor en un mercado libre que una moneda nacida en este mismo mercado. La idea de un mercado libre que usa como sangre del sistema una moneda monopolizada simplemente no tiene sentido.

Antes de la intervención del gobierno en las políticas monetarias, la oferta de una moneda no seguía ninguna política, estaba anclada a las leyes naturales. Los gobiernos impusieron sus políticas a través de bancos centrales, ya que se dieron cuenta de que había pocas cosas que aportaban tanto control y poder sobre una sociedad como el control de su dinero. La confianza en el dinero desapareció. Este pasó a ser sumiso a leyes cambiables que debilitaban cada vez más su valor, y, por ende, su capacidad para cumplir sus funciones más básicas.

Bitcoin se presenta, seguramente, como el sistema monetario más creíble y confiable de la historia, disrumpiendo a su vez el sistema monetario menos

confiable que ha existido. Apostar en Bitcoin es apostar porque las políticas de una moneda deben depender del libre mercado y no de los bancos centrales.

## 4.4. Una economía centralizada

Las grandes empresas nacidas en los últimos años han sido capaces de innovar en su sector, ya sea en productos o servicios. Una de estas innovaciones de hecho es muy común y se basa en el concepto de aplicar un «libre mercado de ideas». Ya no vivimos en métodos empresariales donde un «jefe» determina todo de forma centralizada. El concepto *startup* suele también implicar una metodología de dirección donde se premia a las ideas y no a la posición, un lugar donde las mejores ideas ganan sin importar de quien vengan.

De alguna forma, igual que un mercado libre de las ideas es más eficiente, también lo es un mercado libre capitalista en contra un mercado socialista centralmente controlado. El problema económico central en una sociedad es la distribución del conocimiento. Este se encuentra en un cambio constante, y la prioridad de un sistema económico es poder permitir un flujo continuo, eficiente y rápido de esa información, y así poder dar los conocimientos necesarios a todos los emprendedores para tomar decisiones acertadas.

Seguramente son las señales de precio los grandes diseminadores del conocimiento. Pongamos un ejemplo. Rodrigo es un granjero que vive en el norte de España y trabaja a diario cultivando cereales. Rodrigo es muy consciente de sus costes (tierra, agua, fertilizantes...) y sabe que su actividad es rentable porque sus ingresos finales son superiores a sus costes totales. Ahora bien, Rodrigo, que vive montaña abajo, quizá no sabe que a varios kilómetros de allí, montañas arriba, hace más de nueve meses que no llueve. Este periodo de sequía provoca un aumento del precio del agua. Frente al aumento en costes, Rodrigo decide aumentar el precio de su cereal para así poder mantenerse en beneficio. Rodrigo ha tomado una decisión eficiente sin quizás ser consciente que había sequía, simplemente gracias a la información que le han aportado las señales de precio. Este ejemplo sencillo nos permite entender cómo un mercado libre con señales de precio no manipuladas, que representan fielmente la realidad económica, nos permite tomar acciones eficientes de forma descentralizada.

El libre mercado nos asegura que solo aquellos que están añadiendo valor a la sociedad podrán sobrevivir y prosperar. En esencia, la no interferencia permite crear un equilibrio natural. El gobierno es importante, pero no debe intentar ser

el señor todopoderoso y protector de todos. Más bien debe asegurarse en mantener la no violencia y el derecho a la propiedad.

Por contra, el sistema actual dirigido centralizadamente por bancos centrales es más similar a un capitalismo socialista. La economía se dirige desde un despacho privado, donde son lo suficientemente arrogantes como para pensar que disponen de todo el conocimiento para tomar decisiones económicas que beneficien a todos. Creen que las decisiones centralizadas son mejores, más eficientes y que van acorde con las realidades económicas. Esta idea me recuerda cuando la URSS intentó planificar centralizadamente la producción de patatas. Surrealista, ya que se dieron cuenta que un año había demasiadas y otro demasiado pocas. La oferta y la demanda son los mejores indicadores para la toma de decisiones, una institución centralizada nunca podrá competir contra eso. Esta interferencia de las instituciones en el mercado, dada por la fijación de precios, las restricciones y los monopolios legales en torno al dinero, ha dañado directamente la economía y el dinero que circula en esta. El dinero es como la sangre de una economía, que permite un intercambio fácil de bienes, servicios y conocimiento. Representa la mitad de todos los intercambios económicos, así que seguramente es el mercado más grande del mundo, y, actualmente, está completamente centralizado. Sin competencia, sin necesidad de innovar ni de mejorar su eficiencia en la toma de decisiones. Irónico ver cómo nuestra posición contra los monopolios energéticos es sólida, pero en cambio contra el monopolio más grande y peligroso del mundo no tenemos nada que decir. Aunque con lo poco que forman a los jóvenes sobre «el dinero» tampoco es sorprendente, ¿verdad?

Cuando un sector elimina la competencia también elimina la necesidad de avanzar hacia la mejora en su eficiencia, ya que no tiene nada que perder. Un sector que vive en el libre mercado está incentivado a buscar beneficios y a desincentivar las pérdidas simplemente porque vendrá otro que lo pasará por delante. Un banco central tiene la capacidad de emitir dinero atacando directamente el corazón del sistema (el dinero) sin verse afectado por sus decisiones. De alguna forma, privatizan los beneficios y democratizan las pérdidas.

La impresión de dinero no tiene ningún beneficio social, contrario a cualquier otro elemento. Más de la mayoría de los productos suele ser siempre una buena señal. Más oferta monetaria no lo es de ningún modo, porque su función principal es actuar como medio de cambio y valor reserva sólido en una economía, y la impresión solo consigue diluir su capacidad para cumplir esta

función. Sin contar, además, que suele beneficiar a unos pocos mientras la gran mayoría de la población pasa a ser más pobre porque su poder adquisitivo se ve reducido; representa una forma de redistribuir la riqueza de las manos de muchos a las manos de unos pocos.

> «Inflation is the surest way to fertilize the rich man's fieldwith the sweat of the poor man's brow».

En una economía centralmente planeada, las señales de precio y, por tanto, el flujo del conocimiento, también se ven afectados. Pongamos a Rodrigo como ejemplo de nuevo. Este granjero ha visto la oportunidad de pedir un crédito, ya que, según sus cálculos, un préstamo al 3 % le permitirá obtener 2,5 veces más beneficios, mientras que sus costes solo aumentarán 2,2 veces.

Delante de estos números, Rodrigo decide pedir un préstamo y aumentar su capacidad productiva. Por otro lado, Rodrigo no sabe que todos los otros granjeros de la zona han tenido la misma visión y, como la disponibilidad de dinero en una economía de bancos centrales es barata e ilimitada, estos también han pedido un préstamo. El aumento de dinero en circulación ha provocado un aumento de precios, lo que ha aumentado los costes totales a 2,8. Ahora la estrategia de Rodrigo ya no es rentable, así que deberá escoger entre aumentar sus precios, pedir otro préstamo o declararse en bancarrota.

Este ejemplo sencillo es una metáfora para ver los efectos de los grandes estímulos y los tipos de interés por los suelos. Aquí no hay un beneficio directo en la economía, sino una distorsión en los precios. Una economía basada en las inyecciones y la devaluación de la moneda como método de crecimiento incentiva a los emprendedores a tomar decisiones de inversión de muchísimo más riesgo.

Con tipos de interés negativos, lo que el banco central está haciendo es incentivar a todos los ahorradores a que dejen de ahorrar y empiecen a gastar. Y cuando gastan, encima lo tendrán que hacer en un entorno de mucho más riesgo y menos estable. Una economía saludable y próspera no basa su crecimiento en el endeudamiento y el gasto en inversiones de alto riesgo, sino en el ahorro en las inversiones premeditadas.

> *«Central Banks, via printing press, have spent over a century enjoying a perpetual "free lunch" where control over assets in continuously reallocated from the many to the few: Bitcoin is a (relatively) sudden monetary phenomenon and an economically violent force against banking cartels that is restoring equilibrium to the global economic order».*

Las monedas fiat son una herramienta para restringir libertades y confiscar la riqueza de las masas, además, de una forma muy disimulada y taimada como es la inflación. Espero que nos demos cuenta de que el sistema actual premia a unos

pocos, que gracias a esto acumulan cada vez más parte del pastel. Y es cierto que hay muchos problemas en el mundo, aunque estoy seguro de que parte de la pobreza y el incremento de la diferencia entre ricos y pobres nace en parte de esta situación. De hecho, Tomas Jefferson ya nos lo advirtió:

> «If the American people ever allow private banks to control the issue of their currency, first by inflation, then by deflation, the banks and corporations that will grow up around them will deprive the people of all property until their children wake up homeless on the continent their Fathers conquered… I believe that banking institutions are more dangerous to our liberties than standing armies… The issuing power should be taken from the banks and restored to the people, to whom it properly belongs».

## 4.5. Un poco de historia

Cuando hablamos de dinero, el concepto más relevante que le podemos asociar es la confianza. Lo más importante de una moneda es que pueda generar confianza a sus usuarios. La población debe poder confiar en que esa moneda no va a perder valor, que otros van a quererla y aceptarla, que no van a poder confiscarle la riqueza… El dinero debería ser aquel instrumento en el que pudieras conservar 1 000 000 USD durante cien años y no tener que preocuparte. Solo por si alguien no lo sabe, hoy por hoy este tipo de activo no existe en el mundo tradicional.

Dicho esto, *el track-record* es importante, ya que demuestra la solidez de algo en el tiempo. El oro hace más de cinco mil años que tiene valor y se ha mantenido escaso. De hecho, una onza de oro hoy te permite comprar algo muy parecido a lo que podías comprar con una onza de oro durante el Imperio romano. Esto aporta confianza. Por otro lado, las monedas fiat tienen un track-record contrario. Todas y cada una han demostrado ser pésimas en cumplir con la función del dinero, sobre todo porque la mayoría de ellas simplemente ha desaparecido. Es lo que pasa cuando sus políticas hacen que su valor tienda a 0. Seguramente la moneda más respetable y con mejor track-record es la libra esterlina. Este activo es la moneda estatal con mejor actuación: 317 años de historia en los que ha perdido el 99,5 % de su valor. Algo triste si concluimos que es la mejor moneda hasta la fecha, la que mejor ha sabido mantener el valor a lo largo del tiempo.

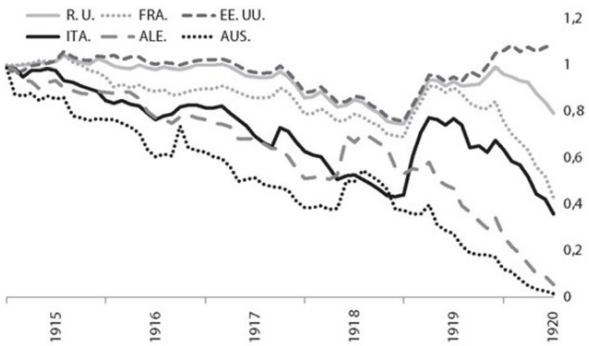


Figura 22. Como muchas monedas cayeron durante la primera guerra mundial. *El patrón Bitcoin*

Es fácil entender cómo el sistema financiero ha ido creciendo exponencialmente hasta convertirse en el sector más capitalizado de toda la economía, quizá, de forma desproporcionada. Lo cierto es que cuando disponemos de un tipo de moneda que no conserva nuestra riqueza, nos vemos obligados a buscar formas alternativas para luchar contra esto. Hoy, gran parte del dinero está invertido en los mercados financieros simplemente porque no hay ninguna otra alternativa. El dinero no sirve para guardar valor, por lo que las grandes fortunas ven en los mercados la forma de protegerse ante este «robo legal». Aquí tenemos otro motor de la desigualdad, ya que suelen ser los adinerados los que conocen el juego y crean portafolios diversificados para protegerse de la inflación. Por otro lado, la mayor parte de la población mantiene su riqueza en fiat. Cada año son más pobres y, muy tristemente, no lo saben.

Es triste también ver que sea este el indicador de bienestar económico de una sociedad. Durante la pandemia de la COVID-19, la mayor parte de las inyecciones de la FED han ido directamente a los mercados. Los pobres se han hecho más pobres y los ricos más ricos. Hoy, después del peor periodo económico a nivel mundial en décadas, con unos niveles de desempleo que han llegado a más del 20 %, las bolsas americanas están en máximos históricos. ¿Realmente esto es sostenible?

Figura 23. Evolución del S&P500 durante 2020

Quizás sea este uno de los factores que ayuden a Bitcoin a la adopción masiva. Desde siempre, la teoría básica en las inversiones ha sido la misma: una vez llegada a cierta edad, buscar un portfolio con un 60 % de renta variable y un 40 % de renta fija. Esta idea ya no es posible, porque las inversiones seguras con una renta fija ya no existen. Gracias a los bancos centrales y sus políticas impulsoras de gasto y deuda a través de tipos de interés negativos, se ha provocado que los bonos estatales sean negativos incluso a diez años. Por tanto, tenemos un 40 % presente en la mayor parte de los portfolios de inversión en busca de assets alternativos. Creo firmemente que el gran beneficiado de este pastel será Bitcoin.

Volviendo al tema de la confianza de una moneda, Bitcoin ofrece una seguridad muy robusta a sus usuarios que mediante este activo podrán protegerse de la confiscación, de la censura o bloqueo de transacciones y, sobre todo, de la inmutabilidad de la oferta monetaria. Bitcoin, al ser open source y completamente transparente, permite que sus normas sean verificables y resistentes a cambios. Sin duda, es la política monetaria más confiable que hemos visto.

Si en un mercado libre el gobierno decidiera de forma centralizada el precio de los coches, ¿cómo reaccionaríamos? Entonces, ¿por qué confiamos en los bancos centrales para escoger el precio del dinero, el mercado más grande e importante del mundo? La historia nos demuestra que el 100 % de las monedas fiat que han existido han tendido a valer 0. La idea de monedas controladas por bancos centrales para mantener un control de precios y un nivel de desempleo bajo ha fracasado. El sistema cada vez es más frágil y dependiente de grandes inyecciones. Con cada una de estas, la bola de deuda es más grande, y la moneda menos valiosa. Estamos en una calle sin salida y pocas alternativas ofrecen mayores soluciones que Bitcoin.

Bitcoin es un activo nacido en el libre mercado, para el libre mercado. De la misma forma que Bitcoin consigue alinear la avaricia y los intereses personales con el objetivo de la red, así también lo hace el mercado. En Bitcoin, si los mineros quieren aumentar al máximo sus rendimientos, la mejor forma para hacerlo es alinearse con Bitcoin y proveer de máxima seguridad a la red. El libre mercado lo consigue porque transforma este interés personal en una mejora colectiva gracias al aumento de la productividad, la reducción de precios y la aparición de ideas innovadoras.

## 4.6. Es el momento de abrir los ojos

Desde principios de la década, Bitcoin es considerado el best performing asset, a años luz del segundo, con un rendimiento del 60 000 000 %. Contra la mejor acción, Netflix, es más rentable en un 3700 %. En tan solo diez años se ha convertido en la red de ordenadores más potente y segura que hemos tenido nunca, ha conseguido capitalizar hasta cuatrocientos billones de dólares sin ninguna ronda para levantar capital, con 0 USD gastados en *marketing*, ninguna oficina y ningún equipo pagado. El mercado le ha dado valor. Y en ningún momento durante todos estos años ha habido fallos o errores críticos. Es aquí cuando ves, querido lector, que quizás falta un poco más de apertura por parte de todos.

Figura 24. Días no rentables para comprar BTC (2 % su existencia). Fuente: www.lookintobitcoin.com

Hay una anécdota de lo más interesante sobre cómo Inglaterra dejó perder el potencial de la industria automovilística cuando esta estaba naciendo a finales del siglo XIX. Inglaterra era el líder indiscutible en ese momento, pero, como sucede ahora, la gente no era capaz de concebir un nuevo modelo de transporte que no fuera a base de carros y caballos. La mayoría despreciaba la innovación y la consideraban algo inútil. ¿Cómo va a funcionar algo que en X kilómetros tiene que repostar? Tal fue el desprecio hacia esta innovación que se creó una de las leyes más absurdas que he visto. Las personas que se comprasen un coche deberían ir con un conductor profesional, y a 20 m – 30 m, una persona con una bandera roja debería ir avisando que llegaba un coche. Esto hizo que en cuestión de años la industria automovilística se desarrollara en Estados Unidos, donde empresas como Ford y General Motors explotaron.

Esta situación me recuerda Bitcoin y cómo muchos países están bloqueando su entrada. La cuestión es que no puedes evitar que Bitcoin llegue a tu país, pero con políticas antiinnovadores sí puedes evitar que tu país llegue a Bitcoin. El futuro demostrará que países con políticas cerradas y que no promuevan la innovación en tecnologías como Bitcoin o Blockchain se verán penalizados con el tiempo.

De nuevo, Bitcoin nos puede servir como ejemplo para aprender a tener una visión más abierta. Bitcoin es una tecnología open source, lo que significa que es absolutamente transparente, auditable y donde cualquiera puede contribuir a mejorarla. Por contra, las monedas fiat son más tecnologías closed source que están legalmente protegidas de auditorías y de competir en el libre mercado contra otras tecnologías monetarias; y como hemos visto, esto hace que sus decisiones no les pasen facturas, lo que las convierte en malas innovadoras y poco eficientes.

El programa open source de Bitcoin está soportado por todos los nodos de la red que ayudan a mejorar sus funcionalidades y promover así su crecimiento. Al ser transparente, todas las visiones están sobre la mesa y se discuten libremente para llegar a un acuerdo. Recordemos que dentro de la red hay muchos participantes, todos ellos con visiones e intereses diferentes. Esta apertura y transparencia es la clave para conseguir una superioridad competitiva contra otras formas de dinero. Los programadores, encargados de mejorar el protocolo, no pueden cambiar estas normas hasta que todos estén de acuerdo. Las monedas fiat han estado protegidas de la competencia y por tanto no han vivido prácticamente ninguna innovación desde su nacimiento.

La antifragilidad y robustez de Bitcoin también viene dada por esta transparencia absoluta. Cada vez que Bitcoin ha sido atacado, se ha hecho más fuerte. Con cada situación hostil, ha mejorado su reputación, su seguridad, su fiabilidad y su inmutabilidad. Bitcoin ha ido adquiriendo cada vez más valor —y seguirá haciéndolo— gracias a su constante mejora en la credibilidad que tiene como dinero. Ha persistido hasta hoy por sus propios méritos, contrario a las monedas fiat, que han persistido gracias a que ha sido impuesta a través de regímenes aplicados por los gobiernos.

Este último halving, cuando las recompensas por bloque pasaron de 12,5 BTC a 6,25 BTC, tuve la suerte de presenciarlo en vivo. Estaba conectado a la blockchain de Bitcoin para presenciar la creación del primer bloque con una recompensa de 6,25 BTC. Esta transparencia no tiene precedentes. Ningún sistema monetario permite a cualquier persona del mundo ver por sí misma cuando el dinero se está creando hoy, o cuánto dinero se habrá creado en diez años. Y no solo eso, sino que todos los movimientos son públicos. Cada año más y más bancos son denunciados por blanqueo de dinero de cárteles de droga, financiar guerras o manipular sus balances. En Bitcoin esto no sería posible, todos deberían actuar de forma justa y honesta, porque no hay otra opción.

Como curiosidad, compartiré lo sucedido en el último bloque minado antes del mencionado halving. Este bloque fue publicado por el grupo de minería F2Pool e incluyó un mensaje muy propio de la filosofía Bitcoin que recordó a muchos el motivo por el cual creemos en esto. En memoria al primer bloque de Bitcoin, cuando Satoshi publicó en él la portada del *The Times* de ese día, F2Pool hizo lo mismo:

> *NYTimes* 09/Apr/2020 *With $2.3T Injection, Fed's Plan Far Exceeds 2008 Rescue*.

Y para los que no conocen la portada del primer bloque:

> *The Times* 03/Jan/2009 *Chancellor on brink of second bailout for banks*.

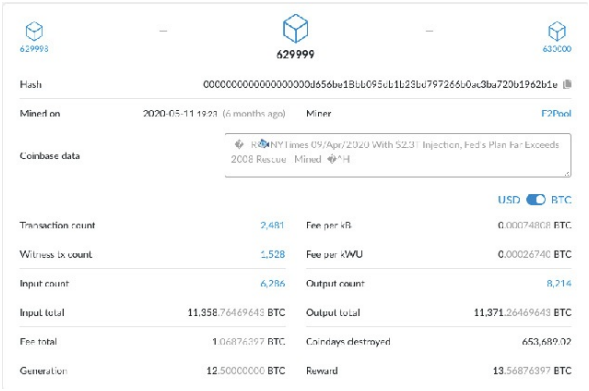



Figura 25. Primer bloque minado tras el halving de 2020, con un «mensaje especial»

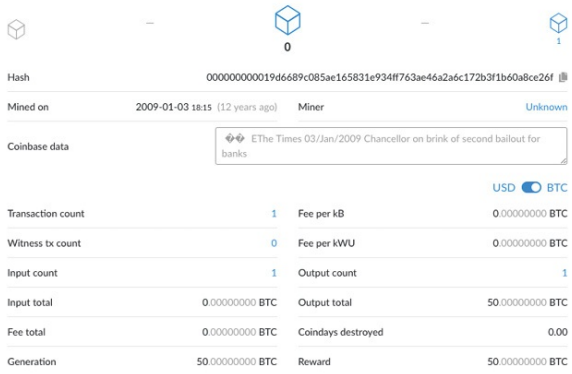



Figura 26. Primer bloque minado de Bitcoin (bloque Génesis)

## 4.7. Toda causa tiene un efecto

Lo que está claro es que reacciones distintas llevan a resultados distintos. Causas distintas tienen efectos distintos. Lo mismo sucede con el dinero: formas de dinero distintas consiguen resultados distintos.

Después de todo lo que hemos visto, debemos ser más conscientes de lo importante que es el dinero en una sociedad. Cada forma de dinero tiene fuertes

consecuencias en nuestros hábitos, ya que es capaz de promover comportamientos concretos. Sin ir más lejos, los bancos centrales establecen tipos de interés negativos para promover de forma masiva el gasto. Las características del dinero tienen efectos en nuestro comportamiento.

Las monedas fiat tienen integrado en su diseño un sistema de control y de devaluación constante. Es decir, cada año valen menos por naturaleza. Esto tiene efectos en cómo nos comportamos. Si usamos una forma de dinero que nos incentiva a gastar hoy —ya que si ahorro para el futuro ese total de dinero tendrá menos poder de compra—, el Estado conseguirá el objetivo y gastaré el dinero ahora, y seguramente en cosas que no necesito. Este efecto no solo es visible en el gasto y el consumo excesivo de nuestra sociedad, sino también en la cantidad de préstamos concedidos por la banca. Tendemos a endeudarnos porque en el sistema actual es de lo más inteligente. Gasto hoy para devolverlo mañana; lo que ocurre es que mañana ese dinero valdrá menos, por lo que habré podido gastar más gracias al préstamo. Este sistema penaliza el ahorro y las inversiones prometidas e incentiva el gasto precipitado, el endeudamiento y las inversiones de alto riesgo; es un pilar poco sólido para construir una sociedad próspera a largo plazo. Vemos el futuro como algo en lo que invertir y no en lo que tomar prestado. Me pregunto qué sentido tendría endeudarse de por vida para comprar un coche en un mundo dominado por una moneda sólida; seguramente, muy poco.

En el mundo empresarial esto también se ve reflejado cuando empresas que ya no son eficientes y que no generan valor suficiente para mantenerse, siguen funcionando gracias a la habilidad del gobierno para imprimir dinero. Esto distorsiona el mercado, bloquea su naturaleza competitiva y reduce la innovación y la eficiencia. Al menos en un mundo donde el dinero es sólido y donde el gobierno no tiene poder para imprimir, quizá las guerras y los conflictos bélicos se reducirían. Desde la primera guerra mundial, las grandes potencias han creado un vínculo amoroso con las guerras, y es que financiarlas permite generar enormes ingresos. Desde la guerra de Vietnam se creó ante nuestros ojos el concepto de «guerra contra el terror», una guerra contra nadie y contra todos a la vez, que permitió a los países aumentar brutalmente sus despensas en armamento militar.

| Período | Los conflictos se cobran cada vez más vidas humanas | | |
|---|---|---|---|
| | Muertes en conflictos (millones) | Población mundial a mediados del siglo (millones) | Muertes en conflictos como proporción de la población mundial (%) |
| **Siglo XVI** | 1,6 | 493,3 | 0,32 |
| **Siglo XVII** | 6,1 | 579,1 | 1,05 |
| **Siglo XVIII** | 7,0 | 757,4 | 0,92 |
| **Siglo XIX** | 19,4 | 1.172,9 | 1,65 |
| **Siglo XX** | 109,7 | 2.519,5 | 4,35 |

Fuente: «Informe sobre Desarrollo Humano 2005», Programa de las Naciones Unidas para el Desarrollo.

Figura 27. Relación entre muertos en guerras sobre porcentajes de población

En definitiva, nuestro comportamiento está orientado al presente y no al futuro. Es decir, el dinero débil aumenta nuestra preferencia temporal, y esto se ve no solo en nuestro comportamiento económico sino también en otros ámbitos. Hace un siglo, un pintor dedicaba años a una obra; hoy, el arte es más negocio que otra cosa. La forma de enfocar las relaciones, de comportarnos con el medioambiente, la forma en que queremos «hacernos ricos rápido y además sin esfuerzo», no son más que reflejos del tipo de dinero predominante. Y es que este es la sangre del sistema, la mitad de cada acción comercial, y no es difícil entender que las características del dinero tienen un impacto enorme en nuestro comportamiento.

Por otro lado, las monedas sólidas son aquellas que promueven comportamientos más a largo plazo, más enfocados en la verdadera prosperidad y no en los beneficios a corto plazo. En este sistema, gracias a la imposibilidad de crear dinero de la nada, se mantiene la relación básica de ahorro-inversión: no se podrá invertir más de lo que se ha ahorrado, incentivando al ahorro, reduciendo así la necesidad de gastar ahora y en cosas innecesarias. Es definitiva, tendríamos una preferencia temporal más baja, lo que se reflejaría no solo en una reducción del consumismo, el gasto sin sentido y el endeudamiento sin control. También se reflejaría en nuestras relaciones, nuestra cura del medioambiente, nuestras pasiones. Estaríamos dispuestos a dedicar tiempo hoy por tener un mejor futuro mañana.

## 4.8. Todo cambia, todo evoluciona

Si algo es seguro, es que lo único que no cambia es el cambio en sí mismo. Cuando algo deja de cambiar, deja de crecer y de mejorar y es señal de que ha acabado. Todo lo que existe, o está evolucionando o está devolucionando.

Históricamente, el dinero más sólido es aquel con las mejores características monetarias. Esa forma de dinero supera a aquellas que son fáciles de producir para convertirse en el dominante del libre mercado. La mejor tecnología es escogida por una selección natural impulsada por el libre mercado.

El nacimiento y posicionamiento de las monedas fiat ha sido el resultado de la centralización del oro por parte de los gobiernos. El papel moneda solucionó en su momento la poca portabilidad y baja divisibilidad del oro. El problema llegó cuando este dejó de ser redimible por oro. Este golpe contra la escasez del dinero ha generado una moneda que se va debilitando con el tiempo.

Bitcoin es un paso adelante para la tecnología del dinero. Combina su escasez absoluta con propiedades como la divisibilidad, la durabilidad, la portabilidad y el fácil reconocimiento. Es hora de dejar de tener dinero controlado por gobiernos y dejar paso a dinero controlado por unas normas establecidas por todos. Utilizando la analogía darwiniana, el Bitcoin y el oro son el resultado de una selección natural, mientras que las monedas fiat son el resultado de una selección artificial. La solidez de Bitcoin tiende a superar en el mercado las otras formas de dinero, ya que la única explicación de que el dinero gubernamental siga existiendo es el monopolio establecido, que impulsa esta selección artificial. Gracias a la trascendencia legal de Bitcoin, este no tiene nada que temer ante este monopolio, haciendo que sea cuestión de tiempo que su mayor solidez acabe superando las monedas fiat.

Desde la crisis del 2008, los bancos centrales se han visto obligados a inyectar cantidades sin precedentes de dinero causando mayor desequilibrio entre ricos y pobres y generando un importante riesgo sistémico. Hoy, después de la crisis de la COVID-19, los gobiernos han vuelto a tener que decidir entre parar la bola de deuda o seguir imprimiendo, y han seguido imprimiendo. En 2020 se creó el 22 % de dólares en circulación. La bola es cada vez mayor, y, en consecuencia, el sistema financiero actual, moribundo, necesita cada vez mayores inyecciones de dinero para parecer que sigue gozando de buena salud.

Este riesgo sistémico ha provocado que valores seguros, como los bonos, dejen de ser seguros, impulsando aún más las inversiones con alto riesgo; una gran contradicción al «estándar de inversión», donde debe haber un equilibrio entre inversiones en renta variable y renta fija. Bitcoin, en cambio, se presenta como alternativa y nuevo activo seguro a largo plazo. El dinero actual es dependiente de inyecciones artificiales para mantenerse a flote y, cada vez más, estos flujos de dinero van a ir entrando a Bitcoin.

Los bancos centrales inyectan dinero a través de la compra de bonos, aumentando el precio de estos y reduciendo a la vez el tipo de interés que ofrecen. El sistema fiat es una trampa que depende de las inyecciones y de la devaluación de la moneda para mantener una economía sana. Ahora, los inversores de bajo riesgo se ven obligados a entrar en inversiones de alto riesgo

como los mercados de equity. ¿Qué pasará con los *portfolios* de retiro o los fondos de pensiones? Quizá estos sean los primeros en explorar nuevas alternativas.

Estamos delante del end game de las monedas fiat, ya que, si los bancos centrales dejan de emitir dinero, viviremos el mayor crack económico que hayamos visto, pero si mantienen las inyecciones, las monedas seguirán perdiendo valor, haciendo que el golpe tarde más en llegar, pero que sea más fuerte cuando llegue.

Y la verdad es que las opiniones tienen poco valor —ya que el resultado vendrá dado por el mercado— y la tendencia que muestra este es bastante obvia. Bitcoin es una alternativa muy atractiva en un mercado libre para poder limpiar el desastre creado por los bancos centrales y los gobiernos durante las últimas décadas. En pleno 2020, es ya monetariamente irresponsable ignorar este activo; como dijo Einstein:

> *«Significant problems from our time cannot be solved by the same level of thinking that created them».*

Bitcoin es una protesta pacífica contra este sistema institucionalizado y gobernado por bancos centrales. Es un símbolo de libertad para todos los habitantes del planeta y un pilar sólido sobre el que crear una sociedad justa donde construir la economía del futuro.

Y aquí, sin nada más que añadir, cierro el tema de Bitcoin para ahora profundizar en blockchain y en las Finanzas Descentralizadas o DeFi. Quiero diferenciarlo porque, a pesar de que Bitcoin es una blockchain, para mí tiene poco que ver. Bitcoin es una nueva forma de dinero sólido y, por tanto, tiene poco que ver con las posibilidades de las blockchains. Espero haber transmitido correctamente mi visión optimista sobre este activo, y cómo, desde ahora, tenemos la oportunidad de hacer las cosas bien desde la raíz. Y si Bitcoin nos abre las puertas a un mundo así, más abierto, transparente, justo e interconectado, no cabe duda de que es un símbolo de libertad.

Y para concluir, quiero agradecerte personalmente a ti, lector. Espero de verdad que haya enriquecido tu conocimiento y opinión respecto a Bitcoin, y que esta vez, sin posponer, cambiéis el número de 0 % de vuestro capital guardado en Bitcoin. No hay ningún número correcto, solo uno incorrecto, y este es 0. Me despido con una cita de Friederich Hayek, uno de los economistas austríacos más reconocidos que en 1984 nos dejó un mensaje que hoy parece una profecía a punto de cumplirse:

> «No creo que volvamos a tener alguna vez una buena moneda antes de sacar el tema de manos del

gobierno, es decir, no podemos arrancárselo con violencia, lo único que podemos hacer es introducir algo de alguna forma taimada e indirecta que [el gobierno] no pueda detener».

Friederich Hayek, 1984

1. https://en.wikipedia.org/wiki/The_Ultimate_Resource

# SEGUNDA PARTE:
# DE LAS FINANZAS CLÁSICAS AL DEFI

# 5. Tradición y cultura financiera

## 5.1. Evolución de la inversión en España

En este capítulo hablaremos de lo que significa este término tan de moda: inversión financiera. Lo asociamos a lo *cool* que resultaría trabajar en Wall Street con los traders más famosos. Pero antes, hagamos un breve paso por la historia reciente.

La inversión financiera no comienza a consolidarse en España hasta los años 80. ¿Por qué? Fundamentalmente porque no se primaba el ahorro a medio plazo y mucho menos a largo plazo. Es decir, el banco te daba un interés muy alto por tener el capital en tu cuenta, y en cambio cualquier tipo de inversión que no fuera en el corto plazo rentaba a un valor mucho menor.

En aquellos momentos, el fomento del consumo y no del ahorro era la tendencia prioritaria. Nadie hablaba de riesgo de inversión o pérdida de valor adquisitivo, o incluso de inflación (que llegó a ser del 20 % en 1983). La manera más rentable de generar plusvalías era mantener tus ahorros en la cuenta corriente, obteniendo entre un 10 % – 20 % (como se observa en la gráfica anexa). Es lo que se denomina «curva invertida del ahorro».

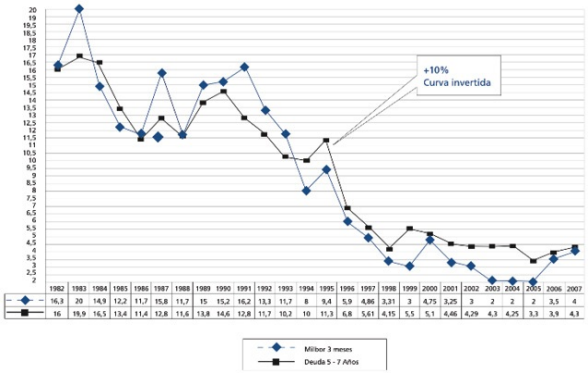



Figura 28. Evolución de los tipos de interés en España 1982-2007

A la vista de estos rendimientos a corto plazo, no era ni atractivo ni rentable plantearse otro tipo de inversión. De ahí viene el término cuenta corriente o cuenta de ahorro. Es decir, te presto mi liquidez a cambio de un interés o remuneración mensual/anual.

Con ello, aparecieron posibilidades y oportunidades de inversión que hoy nos harían saltar las alarmas: inversiones en sellos, monedas de internacionales y coleccionables.


Figura 29. Cuentas de ahorro y productos de inversión en España durante los años 80

No se permitía la inversión fuera de España ni que capitales extranjeros invirtieran en este país. Esto conviene recordarlo porque, aunque hoy damos por hecho que todo es global y que puedes a comprar o invertir en cualquier parte del mundo con relativa facilidad, hasta hace poco más de treinta años esto era ciencia ficción. La fecha exacta a partir de la que se permite invertir fuera de España es el .

## 5.2. Curvas de crecimiento y ciclos económicos

Históricamente, una curva de rendimiento invertida ha sido vista como un indicador de una recesión económica pendiente. Cuando las tasas de interés a corto plazo exceden las tasas a largo plazo, el sentimiento del mercado sugiere que la perspectiva a largo plazo es pobre y que los rendimientos ofrecidos por el ingreso fijo a largo plazo continuarán cayendo.

Las curvas de rendimiento invertidas, aunque las consideramos como situaciones excepcionales, no lo son tanto debido, en gran parte, a periodos más largos que el promedio entre recesiones desde principios de los años 90. Por ejemplo, las expansiones económicas que comenzaron en marzo de 1991, noviembre de 2001 y junio de 2009 fueron tres de las cuatro expansiones económicas más largas desde la Segunda Guerra Mundial. Durante estos largos períodos, a menudo surgió la pregunta de si una curva de rendimiento invertida puede volver a ocurrir.

Los ciclos económicos, independientemente de su duración, históricamente han pasado del crecimiento a la recesión y han regresado al crecimiento, iniciando un nuevo ciclo. Las curvas de rendimiento invertido son un elemento esencial de estos ciclos, que preceden cada recesión desde 1956. Considerando

la consistencia de este patrón, es probable que se vuelva a formar un rendimiento invertido si la expansión actual se desvanece hasta la recesión, por lo que puede considerarse como un indicador de advertencia.

A medida que el ciclo económico comienza a desacelerarse, la curva de rendimiento tiende a aplanarse, aumentando las tasas a corto plazo y manteniéndose estables los rendimientos más largos. En este entorno, los inversionistas ven los rendimientos a largo plazo como un sustituto aceptable del potencial de rendimientos más bajos en acciones y otras clases de activos, que tienden a aumentar los precios de los bonos y reducir los rendimientos.

Si analizamos el impacto en los consumidores y en el negocio hipotecario (donde las tasas de interés se actualizan periódicamente en función de las tasas de interés a corto plazo), una recesión impactaría en que los pagos de intereses tienden a aumentar, con lo que los consumidores deben dedicar una mayor parte de sus ingresos al servicio de la deuda existente. Esto reduce el ingreso fungible y tiene un efecto retroalimentado negativo en la economía en su conjunto.

Una curva invertida elimina la prima de riesgo (al arriesgar más tiempo obtienes más interés) para las inversiones a largo plazo, lo que permite a los inversores obtener mejores rendimientos con inversiones a corto plazo. Cuando el diferencial entre los bonos (una inversión sin riesgo) y las alternativas corporativas de mayor riesgo se encuentra en mínimos históricos, a menudo es una decisión fácil invertir en vehículos de menor riesgo.

Otro punto interesante es que los márgenes de ganancia caen para las compañías que piden préstamos a tasas a corto plazo y que prestan a tasas a largo plazo, como los bancos comerciales. Del mismo modo, los fondos de cobertura a menudo se ven obligados a asumir un mayor riesgo para alcanzar el nivel de rendimiento deseado.

A pesar de sus consecuencias para algunas partes, las inversiones en la curva de rendimiento tienden a tener menos impacto en los consumidores de alimentos básicos y en las compañías de atención médica, que no dependen de la tasa de interés. Cuando esto ocurre, los inversionistas tienden a recurrir a acciones defensivas, como las de las industrias de alimentos, petróleo y tabaco, que a menudo se ven menos afectadas por las desaceleraciones de la economía.

Si bien los expertos cuestionan si una curva de rendimiento invertida es o no un indicador sólido de la recesión económica pendiente, hay que tener en cuenta que la historia está llena de carteras que fueron devastadas cuando los inversionistas siguieron ciegamente las predicciones de «esta vez es diferente». Más recientemente, los inversionistas de capital que lanzaron este supuesto

participaron en el «choque de tecnología», adquiriendo acciones en compañías tecnológicas a precios inflados, aunque estas empresas no tenían ninguna esperanza de obtener alguna ganancia.

¿Y si la historia volviera a repetirse?

Sin duda ninguna, la historia siempre se repite. Los ciclos comienzan de nuevo y las políticas económicas y monetarias de los Estados nos están llevando a la mayor recesión que vayamos a conocer. Tardará más o menos, pero llegará y todos los que estamos leyendo estas líneas la vamos a tener que sufrir. La clave es, precisamente, organizar nuestra vida —financieramente hablando— para sacarle provecho y poder surfear la ola en vez de que nos aplaste. Pero solo podremos surfearla si nos preparamos para estar en el lugar adecuado, en el momento adecuado y con la forma física adecuada.

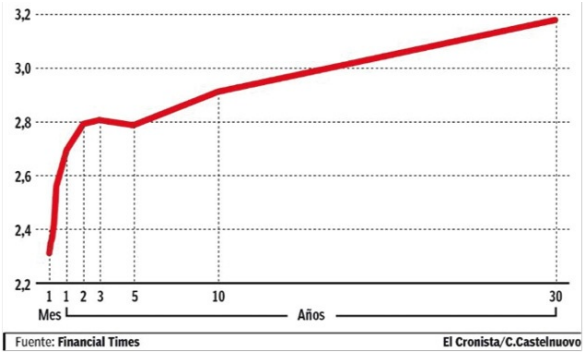



Figura 30. Rendimiento de los bonos de Estados Unidos (en %).

La economía no sigue una línea recta que sube o baja de manera constante, sino que sigue un patrón de ciclos. Y en función del punto que nos encontremos en el ciclo, tendremos que actuar con una estrategia diferente.

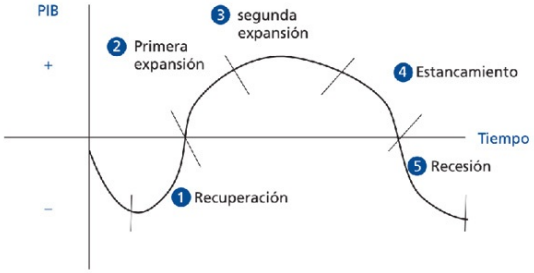



Figura 31. Evolución de los ciclos económicos

El mejor indicador para evaluar en qué fase estamos del ciclo es el PIB o Producto Interior Bruto. Es el agregado que se utiliza para medir el crecimiento de una economía, habitualmente medido en trimestres. En resumen, es el valor añadido generado por todos los factores de producción, tanto nacionales como de titularidad extranjera, creados en su interior. Es un indicador que suele

demorarse un mes en aparecer, con lo que no se puede trabajar en tiempo real con él (excepto con previsiones).

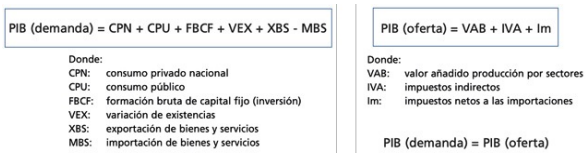
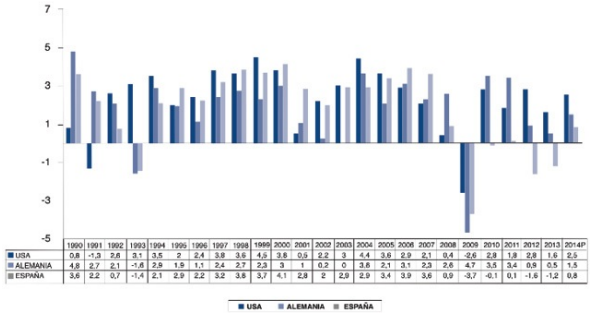



Figura 32. Definición del PIB (de oferta y demanda)




| | 1990 | 1991 | 1992 | 1993 | 1994 | 1995 | 1996 | 1997 | 1998 | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| USA | 0,8 | -1,3 | 2,6 | 3,1 | 3,5 | 2 | 2,4 | 3,9 | 3,6 | 4,3 | 3,8 | 0,9 | 2,2 | 3 | 4,4 | 3,6 | 2,9 | 2,1 | 0,4 | -2,9 | 2,8 | 1,8 | 2,8 | 1,6 | 2,5 |
| ALEMANIA | 4,8 | 2,7 | 2,1 | -1,6 | 2,9 | 1,9 | 1,1 | 2,4 | 2,7 | 2,3 | 3 | 1 | 0,2 | 0 | 1,6 | 2,1 | 3,1 | 2,3 | 2,6 | 4,7 | 3,5 | 3,4 | 0,9 | 0,5 | 1,5 |
| ESPAÑA | 3,6 | 2,2 | 0,7 | -1,4 | 2,1 | 2,9 | 2,2 | 3,2 | 3,8 | 3,7 | 4,1 | 2,8 | 2 | 2,9 | 2,9 | 3,4 | 3,9 | 3,6 | 0,9 | -3,7 | -0,1 | 0,1 | -1,6 | -1,2 | 0,8 |

Figura 33. Comparativa del crecimiento del PIB entre USA, Alemania y España 1990-2014

Los órdenes de crecimiento del PIB suelen estar entre el -1 % y el 4,5 % anual.

Hay otros muchos indicadores que sirven para testar cómo están yendo las cosas, pero no quiero que os parezca más complicado de lo que realmente es. En todo caso os recomiendo leer sobre indicadores de sentimiento, indicadores de oferta, indicadores de demanda e indicadores compuestos. Hay un mundo de psicología y estadística detrás de todos estos datos.

Para simplificar un poco todo este enredo de datos y concluir cómo los indicadores afectan el crecimiento o recesión de la economía, adjunto esta tabla:

| **Recesión** | **Crecimiento** |
|---|---|
| **PIB** = Dos trimestres consecutivos en signo negativo | **PIB** = En signo positivo |
| **Indicadores:** | **Indicadores:** |
| Paro ↑ | Paro ↓ |
| Demanda ↓ | Demanda ↑ |
| Oferta ↓ | Oferta ↑ |
| Sentimiento ↓ | Sentimiento ↑ |
| Compuestos ↓ | Compuestos ↑ |
| **Inflación** ↓ | **Inflación** ↑ |
| **Tipos de Interés** ↓ | **Tipos de Interés** ↑ |
| **Bolsa** ↑ | **Bolsa** ↓ |

Figura 34. Indicadores macroeconómicos en ciclos de recesión y crecimiento

Uno de los aspectos más importantes de las finanzas descentralizadas es la independencia con respecto a las políticas de los bancos centrales, con lo que no estarás supeditado a estrategias globales aplicadas en un ámbito local (país), sino tan solo a un mercado internacional global (aunque sin perder de vista las grandes ballenas).

Retomando el hilo principal sobre la poca historia en materia de asesoramiento financiero en nuestro país, entendemos que treinta años puede parecer poco tiempo para hacer entender a los ciudadanos la relevancia no solo de la educación financiera, sino, en el sentido más amplio, de la economía. Pero como nunca debemos esperar que el Estado nos eduque en estos términos, precisamente porque por influencias keynesianas nos enseñarán solo «su verdad», debemos ser nosotros mismos, como ciudadanos libres, los que nos ocupemos y preocupemos por difundir esta educación en nuestro más amplio entorno.

## 5.3. Ahorro, inversión e inflación

En este capítulo nos acercaremos a términos como tasa de interés, inflación, rentabilidad, volatilidad y palabras que debieran ser parte principal de nuestro día a día porque, al final, trabajamos por dinero y trabajamos más de lo necesario para poder tener un ahorro o dinero futuro.

**¿Qué es el ahorro? ¿Es el ahorro un invento de la sociedad capitalista?**

No hay mejor manera de explicar esto que con el ejemplo de un sector productivo primario: un agricultor produce para poder recuperar su inversión durante la época de cultivo (agua, gasoil, semillas, productos fertilizantes, amortizaciones de la maquinaria, etc.). Pero también produce con el objetivo de generar un excedente.

Antiguamente se producía para autoabastecimiento, es decir, para consumir lo que uno mismo generaba. Y si eras capaz de generar más, lo almacenabas e incluso lo llevabas al mercado para canjearlo por otro producto que necesitaras. Aquí enlazamos conceptos como necesidad, producción e intercambio.

En términos netos, si producías más de lo necesario, estarías ahorrando. Imaginemos que cultivas patatas y consigues tener un excedente del 50 %. Dada la naturaleza efímera de la patata, solo podrías disfrutar de tu excedente durante un tiempo limitado.

Era un ahorro inseguro seguro y poco usable. Por esta razón nacen los mercados: para acudir a ellos con tu excedente y poder cambiarlo por algo que cubra tu necesidad actual o futura. En nuestro ejemplo, podríamos comprar el equivalente al 20 % de nuestra producción en semillas de otra especie. Podríamos decir que es una inversión futura, dado que estaríamos esperando incrementar la producción en un 20 % aproximadamente.

Por ello, el ahorro es un concepto arraigado a la seguridad futura, a mantener su valor a fecha futura, y a tener una disponibilidad rápida para hacer frente a un imprevisto o a una situación excepcional. Sin embargo, el concepto de **inversión** está arraigado a un valor futuro más cercano pero de mayor cuantía, es decir, generar una plusvalía llevando implícito un riesgo asociado al éxito (en nuestro ejemplo, podrían ocurrir diferentes acontecimientos para que dicho 20 % de semillas adicionales no produjera la producción deseada).

Ahora bien, en la actualidad el concepto de riesgo no se ha transmitido con veracidad: 10 000 EUR ahorrados hoy es seguro que valdrán menos dentro de diez años debido a la emisión de dinero público (e inflación). ¿Por qué entonces la banca y todo el sistema tradicional nos impulsa a ahorrar en dinero fiat?

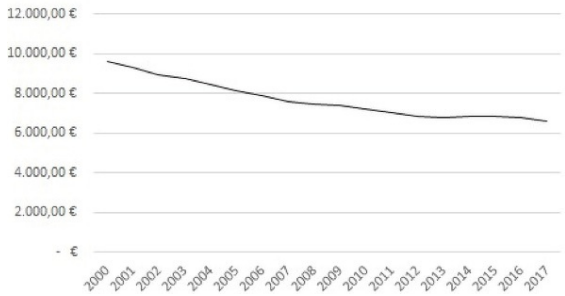


Figura 35. Evolución del valor del dinero fiat (EUR) en función de la inflación

Como se puede ver en la gráfica anterior, la pérdida de valor en siete años ha sido aproximadamente del 40 %, y seguramente cercana al 50 % en diez años, con lo que el término ahorro aplicado a mantener el dinero fiat no tiene sentido; debemos usar el término inversión. Entendamos que existe riesgo, pero entendamos también que si solo dejamos el dinero en una cuenta, al cabo de diez años valdrá la mitad.

> El mundo financiero actual nos obliga a no ahorrar, sino a invertir. Necesitamos invertir nuestros ahorros para que con el tiempo genere plusvalías y crezca así nuestro patrimonio. Lo peor que podemos hacer es «dejar el dinero quieto».

Aunque debiera estar en boca de todos, nadie verbaliza este tipo de pronósticos de manera directa. Solo mencionan inflación o PIB de manera aislada, pero no se habla del impacto que tiene en los ciudadanos esta pérdida de poder adquisitivo.

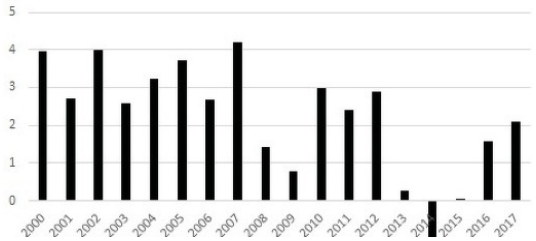


Figura 36. Evolución de la inflación en España desde el año 2000

Otro de los términos que solemos asociar a un futuro incierto es la **inflación**, que es el incremento de los precios de consumo o, visto de otra manera, la pérdida de poder adquisitivo.

Desde que una persona comienza a ahorrar dinero, este empieza a perder poder adquisitivo fruto del sistema inflacionario por el que todos los países se rigen. Cuando hablamos de poder adquisitivo nos referimos al poder económico del dinero. El objetivo no es tener 10 000 EUR y mantenerlos durante diez años, el objetivo es tener al menos 10 000 EUR y, con el paso de los años, con esa misma cantidad poder seguir comprando, al menos, lo mismo que al inicio.

Como hemos visto en la gráfica anterior, la inflación ha sido constante a lo largo de los años, provocando que los ahorros de los ciudadanos hayan ido perdiendo poder adquisitivo; es decir, cada año valen menos.

Dice Murray R. Rothbard en su libro *What has the government done to our money?:*

> «Si el gobierno encuentra alguna manera de dedicarse a falsificar dinero creándolo de la nada, podría ganar dinero sin molestarse de vender sus productos o extraer oro. De esta manera se apropia astutamente de recursos de manera sutil, sin provocar la hostilidad que levantan los impuestos».

Es importante tener clara la idea sobre lo que provoca la inflación, que nada tiene que ver con los impuestos establecidos como IRPF, IVA, IS, IE, etc.

Si comparamos el impacto de la inflación sobre los ahorros con el que tienen los impuestos sobre nuestros beneficios, comprobamos que, con la media inflacionaria de los últimos veinte años, para un ahorrador el dinero que desaparece por causa de la inflación está a años luz del que desaparece por causa de los impuestos establecidos.

Pero no todos salen perjudicados con la inflación. Esta beneficia a los endeudados, que reducen su deuda a medida que el dinero va perdiendo valor. ¿Y quién es el mayor endeudado que conocemos?

Efectivamente, el Estado. ¿Te das cuenta, querido lector, cómo vivimos en un sistema financiero centralizado, orquestado por unos pocos, donde los ciudadanos somos cada vez más pobres sin darnos cuenta?

En una definición más completa, podemos definir inflación como el incremento del precio que pagamos por los bienes y servicios, pero también es el incremento de masa monetaria en el sistema. Este acto supone un impuesto oculto para los consumidores y es la causa principal por la que se produce inflación. Quizás ahora, después de entender este fenómeno, no veamos de manera tan positiva las noticias que salen sobre inyección de liquidez en los mercados a través de impresión y creación de dinero por parte de los bancos centrales.

En la siguiente imagen vemos que el volumen de euros en circulación se ha duplicado en veinte años.

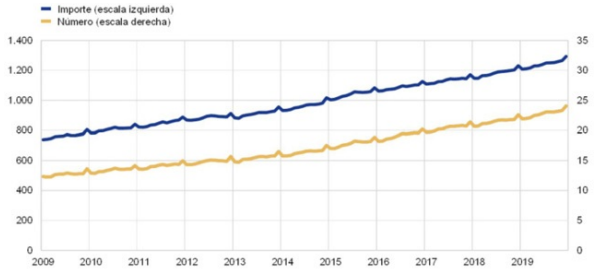



Figura 37. Volumen de euros en circulación los últimos veinte años

Como decíamos en el prólogo del libro: «Nosotros te damos las herramientas y tuyas serán las conclusiones». Lo que parece evidente es que el sistema financiero mundial y actual no está orquestado para beneficiar a los ciudadanos, sino a unos pocos privilegiados dentro de los círculos de confianza del *establishment* y la clase política del más alto nivel.

Lo bueno es que conforme profundicemos en capítulos posteriores, aprenderás a tomar las riendas de tu vida financiera por fuera del sistema tradicional, adentrándote en protocolos DeFi que te permitirán crear productos financieros en función de tu nivel de riesgo y expectativas de rentabilidad.

## 5.4. Mercados tradicionales y su antesala evolutiva a cripto

En este apartado expondremos una introducción básica a los productos más comunes del mundo tradicional financiero y su conversión o equivalente en el mundo cripto.

La base del mercado financiero es la existencia de oferta y demanda de productos financieros, llamémosles liquidez, préstamos a corto/largo, renta a corto/largo, etc.

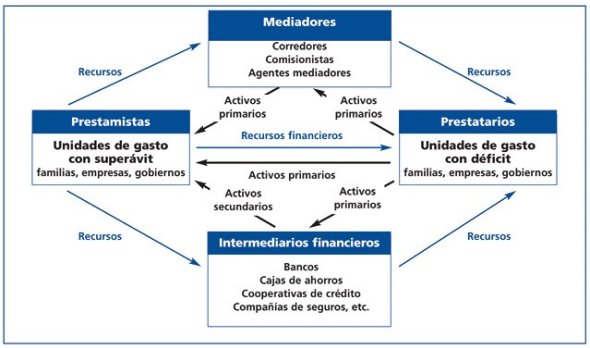



Figura 38. Flujos de un sistema financiero y agentes operativos

Dado que se trata de un mercado no controlado, los precios y productos se irán adaptando a la oferta y la demanda, excepto los intereses de préstamo de dinero, que vendrán influenciados por el interés marcado por los bancos centrales. Para que el flujo descrito funcione es muy importante que las unidades de ahorro (empresas y familias) sigan generando plusvalías para poner ese beneficio a disposición de las unidades que lo necesitan; la rueda no puede parar.

En la tabla anterior hemos resumido los productos financieros históricos que han ido ocupando el mercado financiero español desde los años 80, repasados en el capítulo anterior. Como podemos comprobar, se trata de un mercado regulado y que además dispone de un sistema de compensación para el caso de momentos excepcionales (como quiebras).

Estos mercados están sujetos a la oferta y demanda de manera natural, con lo que su equilibrio depende de sí mismos. Esta es una de las características que debemos llevar a los nuevos mercados financieros descentralizados, donde la regulación y la gestión está repartida en toda la comunidad de usuarios.

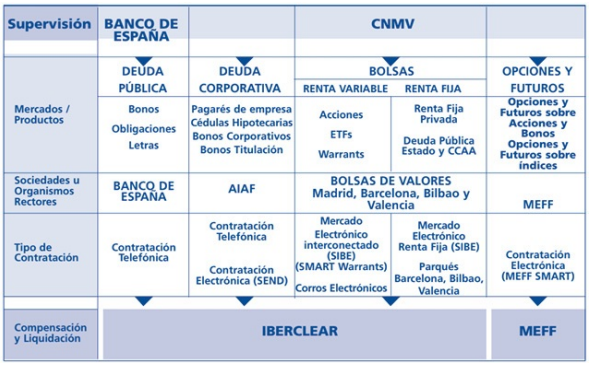



Figura 39. Agentes participantes en los mercados financieros españoles

Si hacemos el recorrido completo de un criptoactivo, como por ejemplo Ethereum o Bitcoin, podemos entender la función relevante del mercado. Este sería el recorrido:

1. Los tokens —en este caso— se minan, es decir, se usan equipos informáticos específicos que necesitan de energía eléctrica para generar un esfuerzo computacional que produce una recompensa en forma de monedas digitales/tokens.
2. *A priori,* el único valor que pudieran tener dichos tokens sería el del propio consumo eléctrico más la amortización de la inversión en los equipos informáticos.
3. Sin embargo, el mercado, a través de su oferta y demanda, otorga un precio mayor a estos criptoactivos. Hablamos del mercado primario.
4. Además, y dado que existe una liquidez limitada, algunos de los propietarios de esos criptoactivos deciden prestar a un tercero a cambio de una renta, o incluso revenderlos a un precio mayor. Nos referimos al mercado secundario.

Partimos de la premisa de que se compra/vende aquello que tiene valor para un tercero. En esta parte entran en juego las características específicas de cada token: por ejemplo, si es deflacionario y tiene un número limitado de unidades es muy posible que dicha escasez digital genere un incremento de su valor a lo largo del tiempo.

La razón de analizar los mercados y adaptarlos a los criptoactivos se debe a que para la emisión, compra o venta de cierto tipo de tokens que representan instrumentos financieros (los security tokens) será necesario conocer qué actores intervienen en los mercados para cumplir con la legislación vigente. Así, en el sistema financiero participan los siguientes agentes:

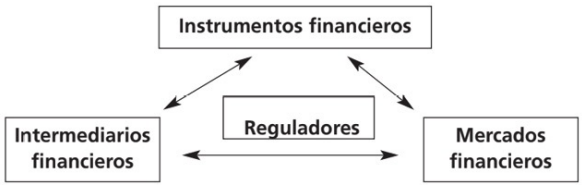



Figura 40. Agentes participantes en la comercialización de productos financieros en España

Hasta hace pocos años, los intermediarios financieros no tenían un papel relevante dado que las inversiones más complicadas a medio y largo plazo (en España) no tenían sentido. Pero recientemente, y dado que la cantidad de productos financieros se ha multiplicado, los intermediarios financieros se han hecho más que necesarios (con un perfil que aporte transparencia y sobre todo que permita adaptar los productos a los clientes finales).

Lo más habitual es que asociemos los intermediarios financieros a las entidades bancarias, pero, como recalcamos, cada día aparecen nuevos entes que

asesoran de manera independiente y desvinculada de los productos de inversión del propio banco.

Desde Tutellus siempre recomendaremos entrar en el mundo de inversión de la mano de un asesor financiero profesional o formaros específicamente en esta materia para, al menos durante los primeros pasos, tener alguien con quien consultar e ir aprendiendo sobre errores y éxitos en un mercado tan novedoso como es el de los criptoactivos.

En nuestro sector cripto hay mucho FOMO y también mucho intento de *spam*, con lo que contar con un perfil experto os dará seguridad y garantía. Siempre recomendaremos huir de sistemas Ponzi y plataformas que aseguran rendimientos a través de bots de arbitraje y esquemas muy similares al *network marketing*; tal y como decimos en nuestros programas formativos tutellianos: «¡Huid, insensatos!».

Volviendo al gráfico anterior y antes de cerrar el capítulo, los intermediarios financieros son los agentes necesarios para una correcta emisión de un instrumento financiero *(security token)* frente al regulador antes de que dicho token se dirija hacia los mercados.

Según el epígrafe 35.2 de la Ley del Mercado de Valores, cierto tiempo de intermediario financiero (EAF) será quien supervise la emisión de un security token (haciendo una especie de fronting con CNMV) cuando dicha emisión cumple ciertas características, como por ejemplo que puedan acudir inversores no profesionales para emisiones de hasta 5 MEUR (la más habitual utilizada en España). En nuestra experiencia y tras haber presentado bastantes STO al regulador, contar con un buen EAF y presentar una correcta documentación (whitepaper, tokenomics, etc.) es una primera garantía para asegurar el éxito de la emisión, aunque no la única.

# 6. Del FinTech al Open Finance y al DeFi

Una de las conclusiones de la pasada década es que la innovación digital fue transformadora, pero no llegó a jugar un papel disruptivo, no generó ningún efecto wow. El ecosistema financiero se limitó a copiar y pegar los esquemas de un sistema financiero diseñado para el mundo analógico, superponiendo las interfaces digitales para hacerlo más accesible a un público con la mirada centrada en su móvil y su PC.

Con una mirada crítica, incluso alguien podría decir que, aunque ha habido progreso, nada ha cambiado. Nuestros intentos de banca centrada en el cliente siguen siendo torpes, los no bancarizados siguen excluidos del sistema y todavía tenemos un sistema altamente concentrado y que depende de acciones políticas de gobiernos.


Figura 41. Distribución de la población no bancarizada en el mundo

## 6.1. Funcionamiento de los flujos de capitales

Los bancos centrales moderan la **oferta monetaria** de una nación (o conjunto de naciones) para alcanzar los objetivos de inflación (y a veces de empleo). Para hacerlo, toman acciones como establecer tasas de interés, realizar operaciones de mercado abierto y prescribir regulaciones de capital bancario y liquidez.

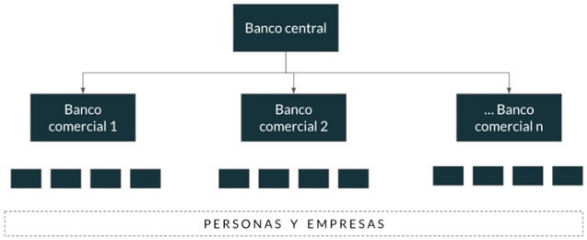



Figura 42. Distribución de productos financieros desde los bancos centrales

En primer lugar tenemos a los **bancos centrales**, encargados de definir y modelar la política monetaria dentro de una nación o conjunto de naciones. Es decir, ellos tienen el poder de manipular la oferta monetaria disponible, donde

los criterios son siempre intentar estimular la economía y evitar momentos de crisis con grandes pérdidas de trabajo. Algunos de los mecanismos son modificar los tipos de interés (el precio del dinero; cuanto más bajo, más barato es pedir prestado) o inyecciones de capital directas al sistema para promover el gasto e impulsar la economía.

En una segunda capa encontraríamos a los **bancos comerciales**, que actúan como intermediarios entre los ciudadanos y el banco central. A través de estos podemos guardar y transferir dinero, en formato digital, alrededor del mundo. Estos compiten entre ellos para acumular el máximo número de clientes y por tanto de dinero depositado, lo que les da el poder para generar un modelo de negocio basado en préstamos y comisiones por estos. De hecho, algo asombroso de estos bancos es que tienen el derecho legal de prestar un dinero que no tienen, algo que se conoce como reserva fraccionaria. Es decir, tan solo tienen la obligación de tener depositado un X % del dinero que prestan (2 % en la UE), lo que asombrosamente los convierte en la única empresa en el mundo que tiene el derecho legal de estar en una bancarrota permanentemente (ya que, si en algún momento tuvieran que devolver ese dinero, simplemente no podrían hacerlo).

Por último tenemos, siempre mirando este sistema tradicional a grandes rasgos, los **bancos de inversión**, que más que bancos son organizaciones con poder de generar vehículos de inversión como OPI, bonos corporativos, etc. que sirven para «poner a trabajar tu dinero». Consiguen trasladar los ahorros de los ciudadanos a estos activos de inversión, cosa que les pone en una situación de mucha responsabilidad, ya que si generan vehículos de inversión de mala calidad —y no informan correctamente de ello— pueden hacer desaparecer los ahorros de miles de personas, algo similar a lo que sucedió en 2008 con la crisis de las preferentes. Estas prácticas poco éticas han hecho que algunos bancos de inversión tengan que desconstituirse y constituirse de nuevo como bancos comerciales, para así recibir los privilegios que los hacen inmunes a prácticas como dar préstamos con dinero que no tienen.

En definitiva, analizando muy *a grosso modo* el sistema financiero, vemos que se trata de un sector altamente centralizado, con fuerza para desestabilizar una sociedad entera y que acumula mucho poder. Imagina la capacidad de controlar y manipular el activo más importante y esencial en una economía: el dinero.

Actualmente, formar parte de este sistema implica riesgos, como el hecho de estar obligado a confiar, primero, en que los bancos centrales no devalúen la moneda y te quiten parte de tu poder adquisitivo sin que tú puedas hacer nada —situación que se produce constantemente con cada nueva emisión monetaria

como estímulo a la economía—; y segundo, en que los bancos comerciales hagan un uso lícito de tu dinero: lo guarden sin perderlo, no te bloqueen transacciones o te congelen cuentas. En definitiva, nuestros derechos financieros cuelgan de un hilo.

En cuanto a cómo fluye el dinero desde su propia emisión hasta que deriva en productos financieros sofisticados, la siguiente gráfica nos muestra una aproximación:

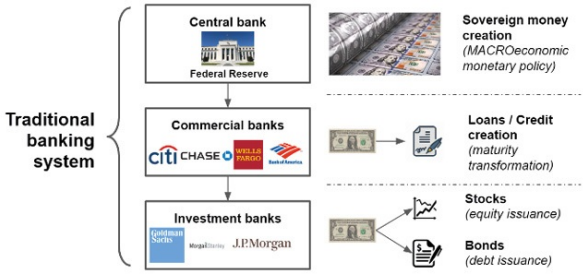



Figura 43. Flujos de agentes que participan en la creación de productos financieros

Los bancos comerciales operan bajo el banco central para agrupar el dinero de su país compitiendo para acumular depósitos de sus ciudadanos. Luego prestan estos **depósitos agregados** sobre una base de reserva fraccionaria para crear préstamos (crédito), en un proceso conocido como transformación de vencimientos. Esto expone a los bancos a un riesgo estructural de endeudamiento a corto plazo y préstamos a largo plazo. Para compensar los riesgos de este desajuste estructural de activos y pasivos, los bancos comerciales tienen dos privilegios especiales que nadie más obtiene: el acceso directo al banco central y la liquidez generada en una emergencia.

Los bancos de inversión (que técnicamente no son bancos) emiten varios tipos de activos (por ejemplo, OPI, bonos corporativos, etc.). Al hacerlo, **canalizan los ahorros bancarios** de las personas hacia estos activos. Algunos bancos de inversión también realizan actividades similares a las de los bancos comerciales, como préstamos y préstamos de valores, también conocidos, por ejemplo, como rehipotecas. Esta práctica a menudo crea el mismo riesgo estructural que enfrentan los bancos comerciales. Después de la crisis de 2008, la mayoría de los bancos de inversión, al borde del fracaso debido a las crisis de liquidez, se vieron obligados a volver a constituirse en bancos comerciales, para poder obtener los privilegios de la banca comercial.

## 6.2. FinTech: finanzas + tecnología digital

A finales del siglo XX, aparece la denominada FinTech (tecnología financiera) que a lo largo de los años —y con más fuerza en la última década— ha integrado soluciones innovadoras para expandir el alcance de servicios financieros, reducir barreras de acceso y educar a más personas sobre las finanzas personales. El impacto de la FinTech ha sido enorme, impulsando la inclusión de millones de personas alrededor del mundo a los servicios financieros.

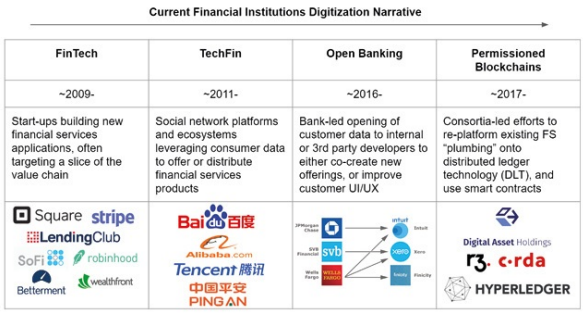


Figura 44. Evolución de empresas FinTech 2009-2017

No obstante, esta corriente aún deja varios problemas por resolver relacionados con obstáculos físicos y técnicos. Para personas de bajos recursos que habitan en zonas lejanas sin conexión adecuada a banda ancha, su acceso todavía resulta un desafío. Asimismo, la FinTech todavía funciona sobre sistemas centralizados donde se requiere confiar en los intermediarios, con programas informáticos pueden tener alta vulnerabilidad a ataques.

## 6.3. Open Banking u Open Finance

Por primera vez existe la posibilidad de mover la liquidez de un mundo analógico a un mundo digital, con una dependencia mínima de la infraestructura existente (como los bancos). La liquidez puede agruparse y agregarse de diferentes maneras, no limitadas por las huellas físicas de los bancos comerciales y las redes de distribución (por ejemplo, sucursales y cajeros automáticos).

Esto erosiona una ventaja a largo plazo que los bancos comerciales han tenido durante mucho tiempo: un monopolio sobre la financiación barata frente a los depósitos.

De esta manera, la Open Finance —la infraestructura de servicios financieros de código abierto construida sobre blockchains públicas— puede ser el próximo reto de digitalización después de la FinTech. Impulsada por la transformación de la liquidez analógica (depósitos en una cuenta bancaria) a liquidez digital (tokens en billeteras digitales), el campo de juego puede nivelarse hacia el valor digital para ofrecer servicios financieros exclusivamente digitales.

Al intentar redefinir los servicios financieros desde el núcleo, cambiarán las antiguas creencias convencionales sobre cómo funciona la banca. El resultado es la posibilidad de que surja algo fundamentalmente nuevo. Es por eso que Open Finance puede resultar una alternativa de digitalización más disruptiva de lo que hemos visto en el pasado.

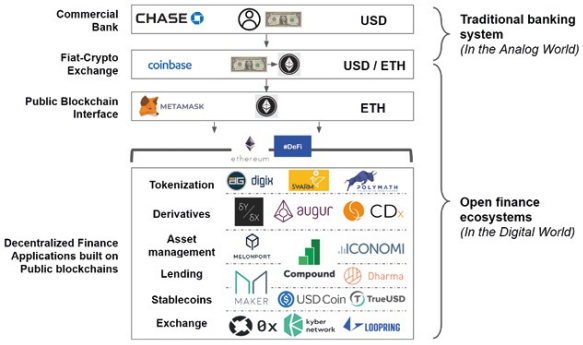



Figura 45. Flujos de dinero cripto en cuanto a la creación de productos financieros

El humo y la opacidad que generaron los clásicos modelos económicos se empezaron a diluir en 2017: los bancos —con los intereses por los suelos— buscaban nuevos productos, comisiones y clientes cautivos; ya no les valía con tener solo una web basada en UX. Pero en aquel momento, las FinTech ya habían cobrado mucha fuerza, por lo que el crecimiento de estas en nuevos clientes (fagocitando a la banca tradicional) fue tremendo.

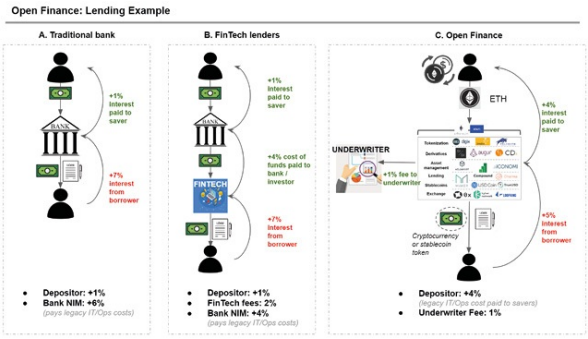



Figura 46. Diferencias entre banca tradicional, FinTech y Open Finance

## 6.4. Mecanismos de transmisión bancaria en open finance

En un mundo donde la transmisión de dinero no está controlada por una red de bancos, el valor puede transmitirse de nuevas maneras, no limitadas por las fronteras físicas. Con la infraestructura de Open Finance es posible diseñar un sistema donde el dinero se agregue y fluya de diferentes maneras.

Los intercambios de cifrado fiduciario se convierten en las rampas de entrada que transforman la liquidez analógica (por ejemplo, dinero fiduciario en una cuenta bancaria) en liquidez digital (por ejemplo, tokens en una billetera digital). Los nuevos participantes como Coinbase, Binance, 2gether, Bit2me o los propios individuos (con DeFi) se convierten en los bancos de facto en estos nuevos ecosistemas.

Podemos decir que se trata de un movimiento social que aprovecha las redes descentralizadas para transformar productos financieros antiguos en protocolos transparentes sin requerir de confianza de terceras partes, ejecutándose sin intermediarios. Lo denomino social porque está moviéndose de boca a oído. Está siendo difundido por gente inquieta para gente inquieta. Y, lo más importante, DeFi no requiere que los bancos o las instituciones financieras incorporen la tecnología, pues son protocolos independientes —lo más parecido a un ente vivo — que ofrecen servicios independientes como intercambios descentralizados, billeteras, mercados de predicción y protocolos de liquidez.

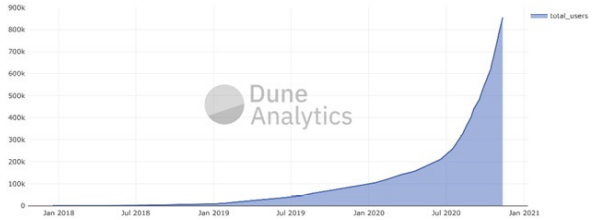


Figura 47. Usuarios totales de DeFi

La entrada a este mundo digital es posible a través de las interfaces blockchain e Internet (como, por ejemplo, MetaMask). Desde aquí, los consumidores pueden acceder directamente a los servicios financieros sin tener que tocar un banco.

Los diferentes ecosistemas públicos de blockchain tendrán su propio conjunto de aplicaciones y protocolos de servicios financieros, dependiendo de sus creencias e ideologías de gobernanza. Por ejemplo, el ecosistema de Bitcoin es generalmente más conservador y se centra en ofrecer servicios a través de segundas capas o cadenas laterales, sin tocar el *core* (que siempre será la seguridad, inmutabilidad y reserva de valor); mientras que en el ecosistema de Ethereum existe un enfoque prioritario en la creación de aplicaciones en la propia red, de forma nativa. Pero incluso, en el extremo más conservador, el dinero fiat se puede convertir en monedas estables respaldadas por dichos activos fiduciarios (USDC, TrueUSD, etc.) o criptomonedas digitales no soberanas (BTC, ETH, DAI, etc.). El abanico de opciones es enorme.

## 6.5. Diferencias entre FinTech, Open Finance y DeFi

Las diferencias principales entre FinTech y DeFi son muchas, pero las más importantes son dos: DeFi implica una descentralización completa de todos y cada uno de los procesos, incluso la gobernanza. Existe una versión menos purista conocida como Open Finance (protocolos financieros programados sobre una blockchain pero que funcionan de forma centralizada, como los sistemas actuales). La segunda gran diferencia es que los protocolos DeFi funcionan en un sistema nuevo, al margen del tradicional. Una FinTech, en última instancia, sigue dependiendo de bancos centrales y comerciales, además de no ofrecer ninguna mejora en cuanto a las políticas monetarias y de forma de dinero utilizado.

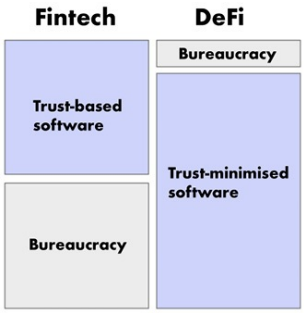



Figura 48. Diferencias conceptuales entre FinTech y DeFi

Al contrario que la mayoría de las plataformas actuales, el valor de los sistemas descentralizados retorna al protocolo, que a su vez está dividido en pequeñas porciones de gobernanza (conocidas como **tokens de gobernanza**) que son transferibles y con derechos de voto. Este concepto es revolucionario, porque por primera vez el éxito de un proyecto como un protocolo DeFi beneficia a todos sus usuarios y no solo a los accionistas. Claramente el incentivo es crear productos para la gente y no para los accionistas, ya que esto hará que el valor total del protocolo aumente aún más. Estamos delante no solo de unas finanzas abiertas al mundo, sino con un core-design pensado para aportar valor al usuario, no a los accionistas. Esto es, sin duda, una revolución.

Por otro lado, podemos detectar un elemento crítico en estos sistemas, y es en el diseño de estos tokens de gobernanza. Si un usuario acumula los suficientes tokens podría llegar a tomar el control de un protocolo, e incluso quedarse con los activos que el mismo esté gestionando. De hecho, cuando un protocolo acumula más valor que el coste que conlleva hacer un ataque de gobernanza, nos encontramos delante una situación peligrosa. Para evitar esto, los tokens siguen una lógica conocida como los tokenomics del token. Cuanto mejor sea el token

en capturar valor de la plataforma y distribuir este valor entre sus participantes, mayores posibilidades tendrá no solo de evitar ataques de gobernanza, sino también de convertirse en un pilar sólido para el protocolo.

A continuación, analizaremos algunos de los protocolos más relevantes que existen en DeFi y entenderemos cómo funcionan para poder hacer uso de ellos. Las DeFi ofrecen oportunidades no solo de inversión sino también para generar nuevos productos financieros y proyectos. Estamos presenciando el mismísimo nacimiento de un nuevo sistema financiero, más accesible, abierto y transparente que el actual; y si este puede, con el tiempo, llegar a competir con el tradicional, estamos sin duda delante de uno de los ecosistemas con más potencial de crecimiento que hemos visto.

## 6.6. Ethereum y su adaptabilidad al Open Finance y DeFi

Para echar un vistazo a un posible futuro de los servicios financieros digitales, un lugar interesante para mirar es el ecosistema de finanzas descentralizadas que se está construyendo en la blockchain de Ethereum. Las aplicaciones de DeFi creadas sobre Ethereum utilizan su blockchain como un libro de contabilidad global, universalmente accesible 24/7, inmutable, transparente y de código abierto. Simplemente se necesita el uso de un mecanismo de consenso de prueba de trabajo (PoW) para realizar esas entradas en el libro de contabilidad.

El ecosistema DeFi de Ethereum comienza con una cuenta bancaria tradicional. El dinero fiduciario (por ejemplo, EUR, USD) se intercambia por la moneda correspondiente utilizada en la economía de Ethereum (por ejemplo, ETH) a través de casas de cambio. Es la misma operación que se realiza cuando alguien viaja de un país a otro, sin más.

¿Qué tipo de servicios financieros podemos realizar sin intervención de terceros?

- **Intercambios.** Canjear tokens de mercados globales que representan reclamos a diferentes tipos de monedas y activos. Por ejemplo: 0x, Kyber Network, Loopring.
- **Stablecoins.** Acceder a un índice de valor estable garantizado por fiat u otras formas digitales de valor, especialmente útil en países con alta depreciación de su moneda local. Por ejemplo: DAI, USDC.
- **Préstamos.** Solicitar préstamos prometiendo garantías digitales, dejando colateralizado otro activo digital. Por ejemplo: Maker, Compound.

- **Gestión de activos.** Acceder a fondos/carteras rastreando una variedad de elementos subyacentes nuevos y tradicionales (tokens de servicios públicos, activos inmobiliarios, valores tokenizados, bitcoin envuelto, etc.). Por ejemplo: Melonport, Iconomi.
- **Derivados.** Acceder a los mercados de derivados para crear posiciones largas/cortas en varios resultados, incluso en especulación apalancada. Por ejemplo: dYdX, CDX, Augur.
- **Emisión de activos.** Emitir activos tokenizados (sobre activos físicos o no) que representen tanto utilities como securities.
- **Arbitraje.** Aprovechar las diferencias de precios entre mercados para obtener ganancias haciendo aumentar la liquidez y reduciendo la disparidad de precios de un activo en diferentes mercados. Por ejemplo: Oasis, Uniswap y Kyber.

En la práctica, tratar de adivinar exactamente qué nuevos jugadores y modelos de negocios surgen y ganan, será difícil. Es muy posible que los modelos de negocio innovadores provengan tanto de los titulares (bancos, gestores de patrimonio y activos) como de nuevas empresas y otros. Los impulsores subyacentes del cambio son los mismos: nosotros, los inquietos.

A medida que tanto los titulares como las nuevas empresas se sientan cada vez más cómodos con el nuevo paradigma, junto con los reguladores y los formuladores de políticas que comienzan a comprender la teoría del juego económico asociada con las blockchains públicas, las condiciones para la innovación inspirada en DeFi florecerán.

Recordando la cita anterior: *«S*olo haciendo algo diferente uno puede esperar un resultado diferente». Será emocionante ver las nuevas innovaciones, muchas de las cuales ni siquiera podemos imaginar, basadas en este nuevo mundo de DeFi.

# 7. Ethereum como puerta de entrada al DeFi

Seguramente para hablar sobre Ethereum (o Bitcoin) necesitaríamos un libro entero. Bitcoin, por su revolución sobre las tecnologías monetarias; y Ethereum por representar el primer sistema computacional descentralizado que permite a cualquier persona del mundo ejecutar y crear aplicaciones sin pasar por intermediarios, que hace uso de un activo digital (Ether o ETH) para usarse no solo como medio de pago sino también como control de seguridad para la red.

Esta complicada definición quedará más que clara una vez hayamos roto en pedazos la segunda red descentralizada más relevante y capitalizada después de Bitcoin. Para que sea entendida por todos, veremos Ethereum desde una perspectiva fundamental y poco técnica.

## 7.1. Orígenes de Ethereum

El concepto de Ethereum nació en 2013 en la cabeza de un joven genio de diecinueve años llamado Vitalik Buterin. A través de su padre, Vitalik había entrado en contacto con Bitcoin durante sus primeros años de vida, y desde sus inicios esta tecnología le dejó perplejo. De hecho, en 2013 ganó sus primeros bitcoins redactando artículos para la revista *Bitcoin Magazine*.

Según Vitalik, la idea de Ethereum le llegó cuando se topó con un problema nacido directamente de la centralización. Uno de sus juegos favoritos era WoW (World of Worldcraft) y, de un día para otro, el equipo de desarrollo eliminó del juego un elemento que él usaba mucho y que además le gustaba. Allí se dio cuenta de la virtud de una red como Bitcoin, que elimina a estos terceros de confianza de manera que las transacciones son incensurables. Ahora bien, Bitcoin no permitía crear un WoW descentralizado donde no hubiera nadie que pudiese cambiar las normas del juego, y que estas solo pudiesen cambiar mediante votaciones en la comunidad. Fue durante este pequeño pensamiento cuando Vitalik dio con una de las ideas más rompedoras e innovadoras de nuestro siglo: usar la tecnología detrás de Bitcoin (la blockchain, los algoritmos de consenso…) para crear una red que permita ejecutar código.

¿Qué significa esto? Que los nodos de la red no solo incorporan la funcionalidad de libro contable distribuido donde se anotan todas las transacciones, sino que además incorporan una máquina virtual (llamada Ethereum Virtual Machine) que puede ejecutar código. Esto permite que

cualquier persona del mundo cree una aplicación y que esta no dependa de servidores centralizados, sino que sea una red de ordenadores global y descentralizada la que se encargue de ello.

Esta definición es técnica y compleja, así que, al igual que hicimos con Bitcoin, vamos a analizarla por partes.

## 7.2. Por qué existe Ethereum

Hoy en día, esta red de información que conocemos como Internet está soportada por un montón de servidores alrededor del mundo, la mayoría de ellos controladas por grandes empresas como Google, Amazon o Microsoft. Es decir, para poder programar una aplicación, ya sea una app móvil o una web, necesitamos un servidor que se encargue de ejecutar todas mis líneas de código.

Por tanto, cualquier aplicación puede ser modificada por sus creadores, que asumen el 100 % del control, y todas tus interacciones con esta aplicación quedarán guardadas y almacenadas en estos servidores: toda tu información personal, desde tus datos, correos, balances bancarios, fotos, videos, registros de pagos en tarjetas de crédito… Si cada empresa, gobierno y aplicación acaba usando servidores propios, imagina lo fragmentada y distribuida que puede llegar a estar tu información personal en Internet.

Esto en cierta manera es muy eficiente, pero tiene algunos puntos en contra. Primero, usar estos servicios es costoso, y esto lo acaba pagando el usuario. Hay algunas aplicaciones que tienen valor gracias al uso que de ellas hacen los usuarios; no obstante, es la empresa la que recibe todo ese beneficio. Por ejemplo, Facebook vale lo que vale y es importante porque nosotros hacemos uso de ella. Si nadie la usara, no valdría nada. Entonces, ¿no sería justo que parte de ese enorme valor que ha generado Facebook retornara al usuario que está generando dicho valor?

Otro inconveniente de los modelos centralizados es que el control para establecer cambios y normas recae sobre una entidad centralizada; esto puede causar situaciones como las que vivió Vitalik jugando al WoW.

Por último, este tipo de sistema vulnera de forma directa nuestros derechos de privacidad. Todos estos servidores guardan continuamente información sobre los usuarios, que después utilizan para ofrecer servicios de *marketing*, o directamente venden los datos a otras empresas. Hoy, la información que generamos en Internet tiene más valor que el propio petróleo, y este beneficio acaba en manos de grandes empresas y no en las de sus propietarios, los

ciudadanos. Esto sin tener en cuenta los hackeos constantes a estas empresas, que descargan muchísimos de estos datos para hacer un uso poco lícito de ellos. Por ejemplo, Dropbox, Walmart, Facebook, Google, Starbucks, LinkedIn, JPMorgan, Uber, Hilton Hotels y Adobe han sido hackeados y no sabemos quién tiene ni qué hace con nuestros datos.

La idea de Vitalik permite crear una red de ordenadores descentralizados que se comunican y llegan a un acuerdo sobre el estado de la red usando blockchain, con la capacidad de eliminar este tercero de confianza a la hora de guardar y transferir información, así como crear aplicaciones.

Esto, en primer lugar, permite crear aplicaciones al margen de la censura de gobiernos y empresas, además de que tales aplicaciones sean accesibles a todo el mundo y desde cualquier lugar: no dependen de ser aprobadas y publicadas por Amazon, Google Play o Apple Store. Permite que los datos personales se transfieran con mucha más privacidad gracias a la criptografía y, por último, el coste de desarrollar aplicaciones no solo cae, sino que además es mucho más accesible. Con Ethereum cualquier persona del mundo puede crear aplicaciones sin tener que pedir permiso a nadie; sin duda esto es una autopista para la innovación y no tengo duda de que pronto veremos una explosión de aplicaciones descentralizadas creadas por personas de todas las edades.

## 7.3. Características de Ethereum

Ahora hemos visto para qué nos puede servir una red como Ethereum y cómo esta pretende ser el «cerebro descentralizado del mundo»: permite programar y ejecutar aplicaciones sobre una red que nadie controla. Ahora todos podemos crear aplicaciones desde casa, sin pagar a grandes empresas por sus servidores ni tener que depender de terceros.

Intentemos entonces definir Ethereum y darle más sentido a todo esto. Ethereum es software open source accesible a todos con el cual se crea una red de ordenadores descentralizados y conectados que integra una máquina virtual en todos estos equipos (nodos) para que la red puede también ejecutar código de forma descentralizada. Estos programas que la red ejecuta se llaman smart contracts. Usa blockchain para sincronizar y guardar los datos del sistema, junto con su criptomoneda nativa, el Ether, que permite transferir valor y aportar una segunda capa de seguridad a la red. Es decir, sustituimos los servicios de servidores o cloud de las grandes empresas por una red descentralizada formada por muchos ordenadores pequeños alrededor del mundo.

Hoy en día, casi todas las aplicaciones dependen de estas grandes corporaciones. Por ejemplo, toda app para móvil depende de AppStore o GooglePlay (Apple y Google). Estas empresas no solo controlan qué aplicaciones están o no disponibles, sino que además las hacen más costosas y les ponen condiciones y restricciones. Ethereum desplaza estas empresas por la comunidad.

La gran idea detrás de Ethereum es que esta red de ordenadores se use para la creación de apps (ahora denominadas dapps o decentralized applications) y estas pasen a estar controladas por la comunidad y no por entidades centralizadas. De alguna forma, Ethereum cambia la manera en que funciona Internet y aporta al mundo una tecnología con la que podemos desintermediar industrias enteras y hacerlas más abiertas, transparentes y justas.

## 7.4. Cómo funciona Ethereum

Ethereum funciona de modo muy similar a Bitcoin, pero con algunas diferencias:

- Los bloques se minan en quince segundos y contienen no solo transacciones sino también smart contracts (líneas de código que los nodos ejecutan de la misma forma que lo hace un servidor).
- La cantidad de ETH es ilimitada, se crean dos ETH por cada bloque minado, pero no está establecida la cantidad máxima de ETH que habrá (es un token inflacionario).

La diferencia principal, que separa las blockchains de primera generación de las de segunda generación, es su capacidad de programar smart contracts y, con ellos, crear dapps o aplicaciones descentralizadas. El término smart contract ha generado mucha confusión, ya que estos ni son contratos ni son inteligentes. Smart contract hace referencia a un programa computacional inmutable que se ejecuta de forma determinista a través de la Ethereum Virtual Machine de cada nodo de la red de Ethereum. Se la llama **ejecución determinista** porque el resultado de la ejecución del contrato será siempre el mismo; y también son inmutables porque los contratos se guardan en la blockchain, lo que hace que sea imposible cambiar un contrato una vez deployado.

Este tipo de entornos usa un lenguaje de programación único llamado Solidity, creado por el equipo fundador de Ethereum, que sirve para explotar al máximo las posibilidades que ofrecen los smart contracts. De hecho, la Ethereum Virtual Machine tiene la característica de que es Turing complete. Esto significa que es

capaz de ejecutar cualquier operación o función. Es decir, en Ethereum se puede programar cualquier tipo de cosa, sin ningún límite, solo el de la imaginación. El potencial es prácticamente ilimitado.

## 7.5. Definición de gas

Veamos con tranquilidad el término *gas*, ya que aparte de ser crucial para entender Ethereum, también es algo que nos encontraremos constantemente cuando operemos con cualquier protocolo DeFi.

El gas es seguramente una de las más grandes genialidades de Ethereum y se usa para solucionar uno de los problemas que puede generar el Turing complete: la recursividad. Un sistema basado en Turing complete puede ejecutar cualquier tipo de código, pero es imposible conocer cuánto tiempo o energía va a necesitar para hacer correr un programa sin antes ejecutarlo. Es decir, la Ethereum Virtual Machine (EVM) no es capaz de saber el tiempo y los recursos que va a tener que usar para ejecutar un smart contract hasta que no lo haga, incluso podría ser que este no terminase nunca. Esto sucede con una función recursiva que, por su diseño, se mantiene en ejecución infinitamente. Por ejemplo:

El siguiente smart contract determina que si Juan es un hombre debe pagar 1 ETH a María, y que si María recibe 1 ETH y además es una mujer, debe pagar 1 ETH a Juan. Este contrato nunca pararía de ejecutarse, ya que las dos condiciones son ciertas.

Esto plantea dos problemas para Ethereum: el primero es que haya gente que cree contratos recursivos para saturar la red, ya que esta quedaría bloqueada ejecutando un contrato infinito. El segundo problema está en la imposibilidad de calcular el coste de ejecutar un smart contract sin saber cuántos recursos va a consumir, ya que habrá algunos que usarán más recursos que otros.

Cuando la EVM ejecuta un smart contract tiene en cuenta cada instrucción que se debe ejecutar (cálculos, transferir, pedir datos, condiciones...). Cada instrucción tiene un coste determinado por gas y, cuanto más largo y complejo es un contrato, más gas necesitará para ejecutarse. Cuando una transacción desencadena la ejecución de un contrato, se deberá incluir el gas limit o la cantidad máxima de gas que puede usar este contrato. Si el gas necesario para ejecutarlo es superior al gas limit la EVM terminará la ejecución. De esta forma, aunque un contrato esté mal hecho y sea recursivo, la EVM dejará de ejecutarlo cuando la cantidad de gas usada supere el gas limit.

Paralelamente y aunque suene extraño, el gas no existe: es una forma de medir la cantidad de recursos que necesitamos (el esfuerzo computacional por unidad de tiempo) para ejecutar un contrato. La cantidad de gas no varía, lo que sí varía es el coste en ETH por unidades de gas. Por lo tanto, al hacer una transacción estándar o una transacción que ejecute un smart contract, esta deberá incluir la cantidad máxima de gas que se está dispuesto a usar, así como el coste (gas price). El resultado de estas dos variables determina el coste de cada movimiento hecho en Ethereum (transaction fee).

| Opcode | Name | Description | Extra info | Gas |
|---|---|---|---|---|
| 0x00 | STOP | Halts execution | - | 0 |
| 0x01 | ADD | Addition operation | - | 3 |
| 0x02 | MUL | Multiplication operation | - | 5 |
| 0x03 | SUB | Subtraction operation | - | 3 |
| 0x04 | DIV | Integer division operation | - | 5 |
| 0x05 | SDIV | Signed integer division operation (truncated) | - | 5 |
| 0x06 | MOD | Modulo remainder operation | - | 5 |
| 0x07 | SMOD | Signed modulo remainder operation | - | 5 |
| 0x08 | ADDMOD | Modulo addition operation | - | 8 |
| 0x09 | MULMOD | Modulo multiplication operation | - | 8 |

Figura 49. Un ejemplo del coste (en gas) de ejecutar distintos tipos de funciones

Cuando las comisiones son altas es porque hay mucha gente que quiere usar la red al mismo tiempo, mucha gente que reclama unidades de gas ya que estas representan tiempo de ejecución. Como hay más demanda que gas disponible el precio de este sube, y las transacciones son más caras (las que estén dispuestas a pagar más por unidad de gas serán las primeras en ejecutarse). De allí también la importancia de optimizar al máximo los contratos, ya que de esta forma se reducirá la cantidad necesaria de gas para ejecutarlos.

El coste del gas se determina en Gwei. En las siguientes imágenes verás los nombres asignados a cada unidad monetaria en Ethereum. El Ether tiene, máximo, dieciocho decimales, siento la unidad más pequeña el wei.

| Unit | Wei Value | Wei |
|---|---|---|
| wei | 1 wei | 1 |
| Kwei (babbage) | 1e3 wei | 1,000 |
| Mwei (lovelace) | 1e6 wei | 1,000,000 |
| Gwei (shannon) | 1e9 wei | 1,000,000,000 |
| microether (szabo) | 1e12 wei | 1,000,000,000,000 |
| milliether (finney) | 1e15 wei | 1,000,000,000,000,000 |
| ether | 1e18 wei | 1,000,000,000,000,000,000 |

Figura 50. Distribución de unidades económicas en la red de Ethereum

Como curiosidad, el nombre a la unidad monetaria más pequeña (wei) se debe a Wei Dai, el conocido criptógrafo en el que se apoyó Satoshi para diseñar el paper de Bitcoin. Wei Dai es el único profesional activo de primera línea completamente desconocido (se vanagloria de que no existen fotos suyas en Internet) y que ha pasado a la historia porque tanto su nombre como su apellido representan dos activos continuamente utilizados en el mundo de Ethereum y en DeFi.

## 7.6. Definición y taxonomía de tokens

La palabra *token* deriva del inglés antiguo «tācen», que significa signo o símbolo. Se usa comúnmente para referirse a artículos similares a monedas emitidas de forma privada sin ningún valor intrínseco, como fichas de transporte, de lavandería y de juegos online o de póquer.

Hoy este término se está redefiniendo gracias a Blockchain. Un token en Ethereum o en cualquier blockchain hace referencia a una unidad digital única diseñada dentro una cadena (por tanto, inmutable, transferible, divisible…) que puede representar cualquier tipo de activo físico, digital o moneda.

Hoy en día, los tokens administrados en blockchains están redefiniendo la palabra para referirse a abstracciones que pueden ser de propiedad y que representan activos, moneda, instrumentos financieros o derechos de acceso. Existen dos grandes tipos de tokens: aquellos que no tienen ningún valor si no es marcado a través de la oferta y la demanda que se lo otorgan (utility tokens) y aquellos que por el activo que representan tienen un valor intrínseco (security tokens). La separación entre los utility y security tokens puede ser a veces confusa, ya que la flexibilidad de la blockchain permite moldear los usos y funcionalidades de estos, haciendo que en algunos casos sea difícil determinar su naturaleza.

Veamos algunos ejemplos de tipos de tokens:

- **Criptomonedas.** Son los tokens destinados a ser usados como monedas y que su valor es determinado por el libre mercado. Todas las blockchains tienen una moneda nativa usada como criptomoneda para incentivar a los que aportan seguridad a la red. Algunos ejemplos son BTC (Bitcoin), Ether (Ethereum), XMR (Monero) o ZEC (Z-cash).

  Con esto ya podemos detectar que aquellas blockchains que no incluyen un token no deberían considerarse como tales porque no están descentralizadas

ni son públicas y abiertas a todo el mundo. Es más, podríamos pensar que son una versión camuflada de los servidores y bases de datos tradicionales que no aportan descentralización ni accesibilidad como lo hacen las blockchains públicas. Aunque, por otra parte, también existen blockchains públicas y abiertas con tokens que no son descentralizadas, ya que alguna entidad mantiene tanto poder que pueden cambiar las normas de la red.

- **Recursos.** Son unidades usadas para medir la aportación u obtención de recursos en una economía colaborativa. Por ejemplo, la moneda GLM (golem) sirve para determinar la cantidad de CPU que has aportado a la red.
- **Acceso.** Este tipo de token otorga derechos de entrada para acceder a sitios como foros de discusión, páginas exclusivas o incluso habitaciones de un hotel.
- **Votación o gobernanza**. Este modelo sirve para descentralizar la gobernanza de una plataforma, empresa o comunidad y darle el poder a dicha comunidad para determinar los cambios a través de votaciones.
- **Coleccionable**. Se trata de tokens únicos que permiten crear activos digitales singulares e indivisibles. Por ejemplo, un autógrafo en formato digital o una obra de arte.
- **Identidad.** Este token sirve para representar tu identidad en formato digital, ya sea para un videojuego o una identidad legal como tu DNI o pasaporte.
- **Equity.** Representa acciones reales de una empresa, pero con características de un *token* (más líquido, más vendible, fácil de transferir, sin intermediarios…). Este es un claro ejemplo de un security token.
- **Propiedad.** Este token representa los derechos de propiedad de un activo físico como, por ejemplo, un edificio. En este caso, lo que determina la propiedad de un activo como un inmueble no está en el certificado de propiedad sino en el token. Esto aporta características únicas a este derecho, ya que ahora es más líquido, más fácil de transferir y no depende de entidades centralizadas, lentas y costosas. Otro ejemplo de un security token.

Estos son tan solo algunos ejemplos de los tipos de tokens que hay en circulación. Todos ellos se crean a través de un smart contract que siguen estándares aceptados por la comunidad, para que sean más interoperables entre ellos.

Desde 2017, en Tutellus hemos estado trabajando en la creación de tokens, desde utilities a securities. Tokenizar es, sin duda, unos de los casos de uso más potentes y disruptivos de las blockchains.

# 7.7. Dapps o aplicaciones descentralizadas

Las dapps son aquellas aplicaciones que están total o parcialmente descentralizadas. La creación de un ecosistema de dapps es una de las visiones que Vitalik más remarcaba, y se conoce como Web3. Estas dapps usan los smart contracts para descentralizar el control sobre la lógica de estas aplicaciones y sus funcionalidades implícitas, aunque la idea de Web3 es ir más lejos y descentralizar también el almacenamiento, la mensajería y la capacidad de cómputo.

Básicamente una dapp es muy similar a una aplicación tradicional; la diferencia es que toda la lógica de back end no se encuentra en servidores, sino que está en una blockchain programada a través de smart contracts.

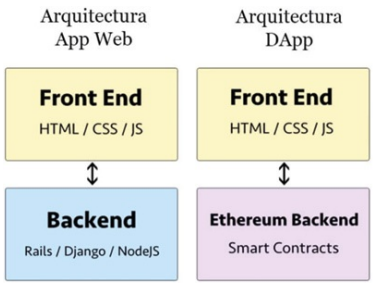



Figura 51. Arquitectura básica y diferencias entre apps y dapps

Aplicado a DeFi, cualquier protocolo de los que analizaremos está basado en dapps, es decir, en uno o varios smart contracts que ejecutan una lógica concreta. Cada vez que interactuemos con un protocolo estaremos transaccionando contra smart contracts. Por tanto, una dapp tiene algunas características únicas respecto a las aplicaciones normales:

- **Resiliencia.** Las dapps estarán en funcionamiento constante ya que dependen de la blockchain y no de servidores.
- **Transparencia.** Todos los programas y contratos de la dapp serán públicos y abiertamente auditables. No habrá funcionalidades desconocidas como pasa hoy con las aplicaciones, donde no sabemos realmente qué está pasando por detrás.
- **Resistente a la censura.** Como el back end estará dentro de una blockchain, será completamente imposible eliminar ese programa, cambiarlo o censurarlo. Blockchain descentraliza y esto hace que ninguna de sus dapp pueda censurarse.
- **Abiertas a todos.** Algo asombroso de las dapps es que si, por ejemplo, Twitter se descentraliza en un futuro (algo ya mencionado por Jack Dorsey,

su CEO), la lógica de Twitter estará programada con smart contracts y deployada en una blockchain. Eso significa que quizá habrá muchas aplicaciones diferentes que harán uso de su protocolo. Es decir, la visión front end de Twitter será la propuesta por la empresa, pero cualquier persona podrá crear un nuevo front end enfocado solo en temas políticos en Twitter (por ejemplo), y que por debajo esté usando también el protocolo. Habrá miles de formas de interactuar en Twitter, ya que la lógica de este será pública.

En definitiva, las *dapps* son parte esencial del ecosistema DeFi y la base de negocio de este nuevo sistema financiero.

## 7.8. Escalabilidad en Ethereum

Esta idea de la Web3 y un ordenador que haga de «cerebro del mundo» es increíble y apasionante, pero la realidad es que de momento es solo ciencia ficción.

Las ventajas de descentralizarse son muchas, pero también tiene sus limitaciones. Una red descentralizada es mucho más lenta que una red centralizada, por lo que, hasta que la escalabilidad de las blockchains no aumente, es difícil pensar en un mundo repleto de dapps.

A esto se lo conoce como el trilema de la blockchain, según el cual esta puede ser descentralizada y segura, pero no escalable y rápida; puede ser rápida y descentralizada, pero no segura; y puede ser segura y rápida, pero no descentralizada.

Figura 52. El trilema de la blockchain

Hoy por hoy, Ethereum está trabajando en el lanzamiento de Ethereum 2.0, una actualización del protocolo donde se migrará de un algoritmo de consenso basado en la fuerza de trabajo (proof of work) a un algoritmo basado en la cantidad de monedas bloqueadas (proof of stake).

Esta actualización podría marcar un antes y un después en Ethereum, ya que solo un sistema PoS (proof of stake) que incorpore otras innovaciones tecnológicas puede hacer que Ethereum no solo mantenga la seguridad y la descentralización, sino que también sea altamente escalable.

Por el momento esto es solo un proyecto y debemos esperar algún tiempo antes de sacar conclusiones al respecto.

# 8. Introducción a DeFi y a las stablecoins

Como acabamos de ver, DeFi hace referencia a un nuevo ecosistema financiero donde somos capaces de crear nuestros productos financieros de forma completamente descentralizada.

## 8.1. Introducción al ecosistema DeFi

Hablamos de ecosistema porque DeFi es el conjunto de protocolos y capas que nacen dentro de una blockchain. De hecho, muchas veces se habla de DeFi como un money lego por este mismo motivo. Estos protocolos se pueden combinar entre ellos para generar nuevos productos, e incluso nosotros mismos podemos hacer uso de varios protocolos a la vez para crear estrategias de inversión únicas.

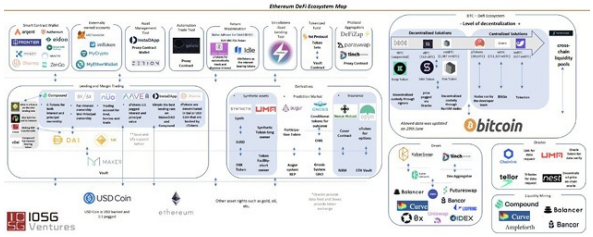



Figura 53. Agentes en el ecosistema DeFi, octubre 2020

Esta imagen nos muestra el mapa del ecosistema DeFi actual en Ethereum. Claro está que no lo veremos todos, pero sí veremos los proyectos más relevantes del ecosistema para así poder entender su funcionamiento. DeFi ha nacido principalmente sobre Ethereum, aunque seguramente sea una industria que acabe interoperabilizándose con todo el ecosistema. Sin ir más lejos, proyectos como Cosmos o Polkadot pretenden ser el puente entre diferentes ecosistemas para no limitar las finanzas descentralizadas a una cola blockchain. Después de que DeFi explotó sobre Ethereum, otras blockchains como BinanceChain o Tron han empezado a crear sus propios protocolos DeFi, aunque muy lejos del tamaño y volumen que se mueve en Ethereum.

Un tema interesante será ver cómo evoluciona este mismo ecosistema DeFi sobre Bitcoin, que, aunque este no tiene la capacidad de ejecutar smart contracts, existen redes paralelas como RSK que permiten ejecutar dichos smart contracts usando como capa de seguridad la red de Bitcoin. Actualmente hemos visto proyectos (como Money on Chain o AtomicLoans) desarrollados para el ecosistema de Bitcoin, pero a pesar de las ventajas y posibilidades que ofrece

este protocolo a las finanzas, parece que no puede seguir el progreso que hay en Ethereum. Por eso mismo, durante este libro nos centraremos en los proyectos DeFi nacidos en Ethereum y dejaremos para un tercero el DeFi alrededor de Bitcoin, la madre de todas las blockchains.

## 8.2. Introducción a las stablecoins

Antes de empezar, es importante introducir el concepto de stablecoin. Aunque muchos ya las conocéis, este tipo de monedas aportan un valor enorme y son un pilar básico de un ecosistema financiero.

Las criptomonedas, a pesar de todas sus ventajas, también tienen grandes inconvenientes, y uno de ellos es la volatilidad. Crear productos financieros con activos volátiles o usar las criptomonedas para transferir dinero y que este se vea devaluado es un problema. Las stablecoins ofrecen una solución porque son monedas pegadas 1:1 con las monedas fiat, la mayoría con el dólar. Es decir, es una versión criptográfica de las monedas tradicionales. En cierto sentido es maravilloso porque puedes mantenerte en el sistema tradicional y aprovechar a la misma vez las ventajas de la blockchain: transparencia, que no haya intermediarios, transacciones al momento con bajo coste, sin comisiones.

**¿Cómo se genera una *stablecoin*?**

Hay varias formas de generar monedas estables. La más usada es a través de un peg centralizado. Es decir, una empresa emite una moneda estable, y por cada moneda en circulación, hay un dólar real que lo respalda y que está depositado en una cuenta bancaria. De las monedas que usan este sistema, las más fiables son las que han pasado por un proceso de auditoría que certifica que realmente lo que tienen en circulación está respaldado por dinero real (USDC, TUSD o BUSD). De hecho, la moneda estable más líquida y antigua del ecosistema se llama theter (USDT) y nunca ha habido una auditoría que confirme al 100 % que disponen de un colateral real. Es decir, podría ser que Tether estuviera generando más dinero del que tiene, manipulando directamente el mercado.

**¿Por qué son necesarias las stablecoins?**

Utilizamos stablecoins cuando queremos tener un dinero tokenizado (con sus ventajas implícitas) evitando los riesgos de la volatilidad inherente al mercado cripto. En una industria con altibajos constantes, ciertos negocios necesitan tener garantizada una estabilidad para ser rentables. Por ejemplo, si creamos un

préstamo en una stablecoin vinculada al BTC el prestatario queda sujeto a su volatilidad; si hoy recibo un préstamo de 100 EUR en BTC y este mes baja un 30 %, a cierre de período deberé 130 EUR más los intereses generados. Sencillamente hay modelos que necesitan de una estabilidad que el propio mercado cripto, por su propia inmadurez y naturaleza, no le puede proporcionar.

Tener dinero en una stablecoin me garantiza dos cosas:

- **Una revaloración si la moneda fiduciaria de mi país es inflacionaria.** Si vivo en Venezuela (depreciación del bolívar = 99 % en 2019) o Argentina (depreciación del peso: 40 % anual en 2020) me interesaría más cobrar en una stablecoin que en mi moneda, ya que mi dinero sería capaz de mantener un valor frente al USD.
- **Una privacidad para mi dinero y mis transacciones** de forma que, al menos aparentemente, no estaría controlado por los bancos y sería un ciudadano más libre. Más adelante veremos que en la mayoría de las ocasiones esto no es cierto.

## 8.3. Taxonomía de stablecoins

Podemos dividir las stablecoins en función de varios parámetros:

**A. En función del colateral que las garantizan**

a.1. En función del tipo de colateral

- Dinero fiat.
- Commodity (oro, petróleo).
- Cripto.
- Una combinación de los anteriores (DAI).

a.2. En función de la cantidad de colateral

- Colateralizado (100 %).
- Sobrecolateralizado (> 100 %).
- Parcialmente colateralizado (< 100 %).

**B. En función de los mecanismos usados para crear el token**

- Activo colateralizado en depósito (la mayoría de los casos).
- Préstamos apalancados (DAI).
- Algoritmia.

- Monedas duales cripto-fiat.

**C. En función de los mecanismos usados para estabilizar el precio**

- Trading (la mayoría de los casos).
- Oráculos (DAI).
- Votaciones.

**D. En función de la naturaleza del activo apalancado**

- Fiat (la mayoría de los casos).
- Commodity.
- Índices.
- Una combinación de los anteriores.

## 8.4. Una visión más técnica de las stablecoins

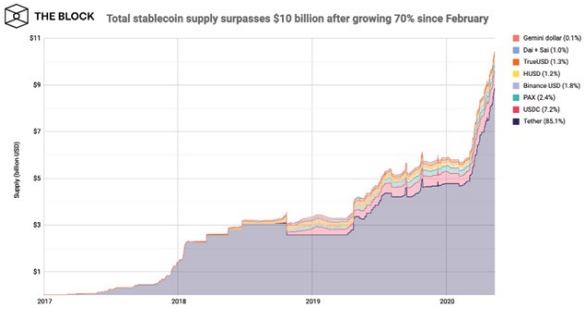



Figura 54. Principales stablecoins por marketcap, escala logarítmica. Fuente: *The Block*

Vamos a centrarnos en analizar las stablecoins descritas en la gráfica anterior, con cifras a 22 de noviembre de 2019:

- **Tether (USDT).** Es la stablecoin de mayor volumen. También es la que se encuentra operativa en más blockchains (Ethereum, EOS, Tron, Liquid y Omni sobre Bitcoin).
- **USD coin (USDC), true USD (TUSD), paxos (PAX) y la recién creada de binance (BUSD).** Todas ellas guardan similitudes: operan sobre Ethereum (salvo BUSD, que además lo hace sobre Binance).
- **DAI/SAI.** Separamos esta última del resto de stablecoins porque tiene una naturaleza distinta: su emisión está sobrecolateralizada (SAI en relación de 2/3 sobre ETH) y utiliza mecanismos de deuda colateralizada (los famosos CDP) en vez de un simple depósito asociado. La analizaremos detenidamente en el capítulo de Maker.

## 8.5. Riesgos asociados a las stablecoins

Aunque tienen aspectos de lo más disruptivos, para no caer en la espiral bullshit debemos conocer los riesgos inherentes al manejo de stablecoins, para tratar de mitigarlos en función de nuestra aversión al mismo.

- Las stablecoins, aunque son dinero, no son usadas como medios de pago. No existen merchants o tiendas físicas que las acepten. Si ya es poco habitual pagar con bitcoin, imagínate hacerlo con PAX o USDT. Así que no pienses en negocios donde el usuario tenga que operar con ellas porque te estamparás contra un muro.
- Las stablecoins dejan trazabilidad, por lo que una postura libertaria de utilizarlas para no depender de los bancos y del sistema no es del todo correcta: ninguna requiere de KYC para su holdeo, pero sí para ser redimidas (salvo DAI/SAI, ya que la tenedora es un smart contract sobre Ethereum).
- Los wallets que holdean las stablecoins pueden llegar a ser congelados si entran en listas negras: todas, salvo DAI/SAI y USDT sobre Liquid (sidechain de Bitcoin que incorpora anonimidad en el propio protocolo), tienen esta función activada en su contrato, y los propios exchanges te avisan de ello. De momento se han congelado unos 40 MUSD, lo que es poco (1 % sobre el total) siempre y cuando no nos toque a nosotros.
- Las stablecoins, como cualquier cripto, nos obligan a ser extremadamente responsables a nivel de seguridad. Si perdemos las claves privadas de nuestro wallet perderemos los fondos depositados.
- Por otro lado, al ser la mayoría de los proyectos open source, su código y contratos están disponibles para ser auditados y trazados, y ya existen empresas (como Chainalysis) que ofrecen sus servicios de trazabilidad a gobiernos. Tan solo algunas variantes de USDT (sobre EOS, Tron y por supuesto Liquid) no son trazables. Los dos primeros casos porque los contratos no son open source y en Liquid por lo ya explicado en cuanto a anonimidad en el propio protocolo.

Como conclusión podemos decir que las stablecoins solucionan problemas de volatilidad y son capaces de mantener el valor de nuestros activos en países con dinero fiduciario inflacionario, pero al mismo tiempo generan otras responsabilidades que tener en cuenta. Sin duda se trata del elemento necesario para que el mundo DeFi despegara, ya que gracias a ellas evitamos la volatilidad para construir productos financieros.

# 9. Plataformas y aplicaciones donde obtener análisis de datos

Antes de empezar a ver protocolos DeFi, nos debemos familiarizar con los principales servicios de análisis de datos con los objetivos tanto de hacer una correcta toma de decisiones para nuevas inversiones, como de realizar el seguimiento de las que estén en marcha.

Lo más importante es que conozcas y pruebes varias plataformas hasta sentirte cómodo con una o dos, y que sean las que siempre uses. Básicamente, la diferencia entre unas y otras es la UX y la interfaz; casi todas ofrecen los mismos datos, pero como bien dice el refrán: «Para gustos, los colores».

Para introducirte en ellas, te recomiendo que bucees con un objetivo concreto para que entiendas correctamente los datos que aportan. Por ejemplo:

- Quiero saber la evolución del token LINK en los dos últimos meses.
- Quiero conocer el volumen máximo diario del token REN.
- Quiero detectar la influencia de BTC sobre el mercado.
- Quiero saber la composición de cartera de mi wallet.

Este es nuestro particular resumen de aplicaciones y plataformas que más valor aportan al ecosistema. Para facilitarte el acceso a todas ellas, introducimos un QR de acceso directo.

## 9.1. Etherscan

**https://etherscan.io**

Es la plataforma donde se centraliza la información de la blockchain Ethereum. En ella podemos encontrar información de todas las transacciones que se realizan en DeFi ERC-20 y ERC-721, de los wallets y tokens que la componen.

Tiene un *look & feel* muy técnico, pero, una vez que llevas tiempo accediendo, te resulta amigable. Es la plataforma más completa.

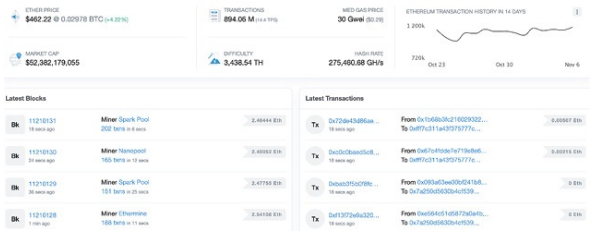


Figura 55. Detalle de la interfaz de Etherscan

# 9.2. Coinmarketcap

**https://coinmarketcap.com**

Es otra plataforma que resume gran cantidad de datos y donde además puedes analizar el volumen de capitalización tanto del mercado global como de cada token. Aunque no es necesario, te recomiendo que te crees una cuenta. Puedes usar contenidos gráficos de evolución y otras métricas globales al estar registrado. La app nativa móvil funciona muy bien.

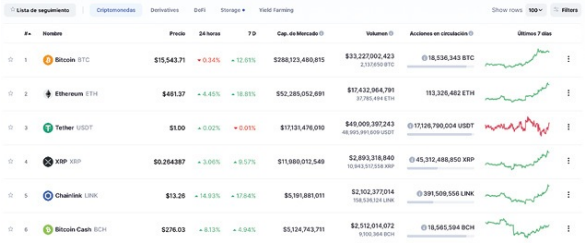


Figura 56. Detalle de la interfaz de Coinmarketcap

# 9.3. Coingecko

**https://www.coingecko.com/**

Es otra plataforma similar a Coinmarketcap; de hecho, la página inicial es casi idéntica. En la parte de mercados/derivados tienes mucha información relevante, así como en la sección de mercados/índice de cripto y en la de riesgos externos. También dispone de más criptomonedas que Coinmarketcap.

Figura 57. Detalle de la interfaz de Coingecko

# 9.4. Coinarbitragebot

**https://coinarbitragebot.com**

Esta plataforma hace un análisis en tiempo real de las posibilidades de arbitraje entre las distintas plataformas de intercambio (exchanges).

Su buscador de tokens en la parte superior derecha te permite encontrar oportunidades de buen precio y arbitraje, y además un gráfico de tendencia de precio y un resumen de los puntos de soporte y resistencia.

Figura 58. Detalle de la interfaz de Coinarbitragebot

# 9.5. Defipulse

**https://defipulse.com**

Esta página resume todos los proyectos y su ranking en el mundo DeFi. Además, incluye sus links de acceso en el apartado de DeFi list.

Accede a la parte donde enumera los tipos y versiones de wallets descentralizados y la parte de interfaces o aglutinadores, que son aplicaciones

que simplifican la información de tu wallet y activos, expresándolo de una manera gráfica y visual muy sencilla.

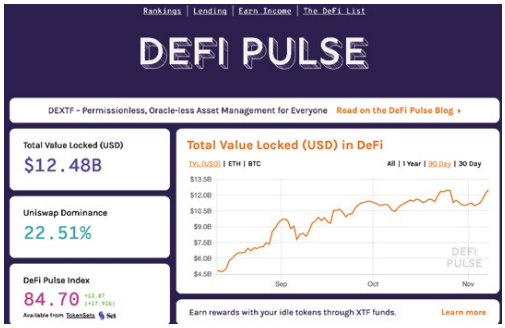


Figura 59. Detalle de la interfaz de DefiPulse

# 9.6. Loanscan

**https://loanscan.io**

Esta plataforma es un excepcional resumen de los productos DeFi que están en marcha en el mercado, con categorización y priorización por interés, volumen, etc.

Es la puerta de entrada al mundo DeFi, pasando del simple trading a préstamos cripto, colaterización de activos, rentas de liquidez y otros productos.

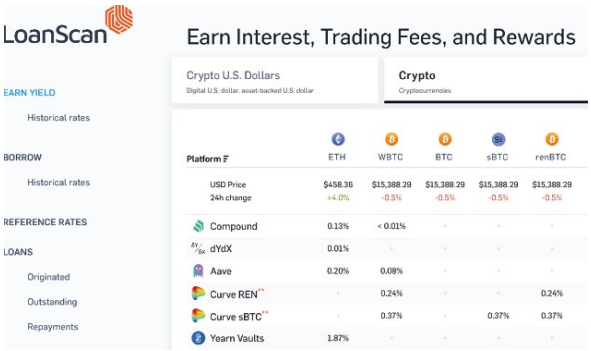


Figura 60. Detalle de la interfaz de LoanScan

# 9.7. DeFiscore

https://defiscore.io

Es otra de las plataformas más completas del ecosistema DeFi. Tiene la opción de conectar con tu wallet (MetaMask y otros).

Muy interesante la evaluación que hacen de los protocolos DeFi con el DeFiscore.

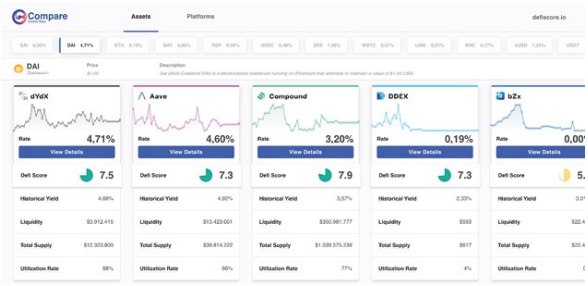



Figura 61. Detalle de la interfaz de Defiscore

# 9.8. Comparativa de herramientas

En resumen, los datos que debes tener en cuenta son los siguientes:

| Aproximación inicial | Precio histórico | Volumen | Indice cripto | Tendencia | Características |
|---|---|---|---|---|---|
| Etherscan | | | | | ● |
| Coinmarketcap | ● | ● | | | |
| Coingecko | ● | ● | ● | | |
| Coinarbitragebot | ● | ● | | ● | |
| DeFipulse | ● | | | | |
| Loanscan | | | | | |
| DeFiscore | | | | | ● |

| Aproximación avanzada | Holding | Staking | Lending | Cobertura | Trading |
|---|---|---|---|---|---|
| Etherscan | ● | | | | |
| Coinmarketcap | ● | | | | ● |
| Coingecko | ● | | | | ● |
| Coinarbitragebot | ● | | | ● | ● |
| DeFipulse | | ● | ● | | |
| Loanscan | | ● | ● | | |
| DeFiscore | | | | | ● |
| Dy/Dx / Binance | | | | ● | ● |

Figura 62. Comparativa de herramienta de análisis de datos

En función de tus intereses, ya sabes qué plataforma puedes manejar en cada momento.

Con este capítulo cerramos el bloque actual y nos empezamos a sumergir en los principales protocolos DeFi del mercado.

# TERCERA PARTE:
# ANÁLISIS DE PROTOCOLOS DEFI

# 10. Introducción a los protocolos DeFi

A estas alturas del libro ya deberíamos empezar a tener claro que el nuevo sistema económico y financiero nacido alrededor de las finanzas descentralizadas parece que no va a ser una moda pasajera. Hemos pasado en 2020 de ver cómo protocolos (como Uniswap) empezaban el año acumulando 10 MUSD y lo van a terminar con más de 3000 MUSD bloqueados, es decir creciendo un 3 000 % en tan solo doce meses.

Los protocolos DeFi nos están ayudando a comprender que existe una nueva forma de relacionarnos con el dinero sin depender de terceros o intermediarios, realizando operaciones directamente entre usuarios. Cómo alineando intereses de ambas partes del modelo (los que tienen dinero o prestamistas o los que quieren dinero o prestatarios) podemos crear un conjunto de incentivos que beneficie a todos y, lo que es más interesante, podemos crear productos estilo Lego, es decir, apilando unos protocolos sobre otros. Tranquilo, querido lector, que esto lo iremos entendiendo durante los próximos capítulos.

Es fundamental que entendamos la diferencia básica entre un protocolo y una empresa: mientras que el objetivo de esta última es ganar dinero (generar muchas ventas para que, con unos costes optimizados, consigamos beneficios), el objetivo de un protocolo es captar el máximo de liquidez para así dinamizar sus tokenomics internos. Los protocolos pueden ser desarrollados por empresas, DAO o simplemente desarrolladores, pero no buscan ganar dinero sino aumentar su TVL, es decir, el apalancamiento en el protocolo con la liquidez de terceros: un protocolo con mucha gente dispuesta a interactuar con él (de cualquiera de las formas posibles) atraerá, por defecto, a nuevos usuarios.

De alguna manera, un protocolo funciona de forma similar a una plataforma. Cuando lanzamos Tutellus tuvimos que iniciar una etapa de crecimiento que nada tenía que ver con un e-commerce, SaaS o similar: en una plataforma debes trabajar los dos lados de la balanza: la oferta y la demanda. No debíamos crecer mucho en usuarios si no teníamos suficiente oferta como para «saciarlos»; y no podíamos buscar excesivos profesores de golpe porque si no disponíamos de alumnos interesados en consumir sus contenidos, los profesores terminarían por abandonar la plataforma.

Los protocolos DeFi me recuerdan esta etapa vivida hace siete años, ya que tienen que alimentar su interés tanto en la oferta (por simplificar: depósitos) como en la demanda (por simplificar: préstamos).

Durante los próximos capítulos vamos a profundizar, a veces demasiado, en el funcionamiento de los protocolos DeFi más importantes segmentados por funcionalidad. Hemos configurado este libro como una «guía de cabecera», para que profundices en el aspecto que más te interese cuando lo necesites.

Si intentas entender todos de golpe, seguramente te estallará la cabeza. Y si necesitas ayuda o *mentoring*, recuerda que desde Tutellus tenemos bootcamps y programas formativos continuos para acompañarte.

# 11. Protocolos para stablecoins descentralizadas: Maker

Empezamos nuestra profundización en protocolos DeFi hablando de Maker, uno de los primeros protocolos en aparecer y que hoy en día sigue siendo uno de los mayores players en el ecosistema. De hecho, fue el primer protocolo en llegar a una capitalización de 1000 MUSD.

La importancia de Maker en el ecosistema DeFi es enorme, ya que ha conseguido crear una base sólida que ha ayudado al desarrollo de otros protocolos financieros. Si retrocedemos en el tiempo, antes de la aparición de las DeFi tal y como las conocemos, vivíamos un momento en el que era impensable generar productos financieros sobre tokens extremadamente volátiles; había una gran necesidad de tener monedas estables en las que se pudiese confiar. En aquel momento existía theter (USDT), pero esta era una moneda que rompía con la idea de la descentralización, ya que la emite una empresa privada que supuestamente mantiene un colateral en una cuenta bancaria. Y digo supuestamente porque no hay forma de comprobarlo, sino que debes confiar en la empresa y en sus auditorías de que así ocurre.

Maker propuso un protocolo capaz de generar una moneda estable descentralizada y respaldada por criptoactivos cuyo valor está referenciado 1:1 por el dólar. Parece obra de magia: ¿cómo puede un activo volátil dar estabilidad a otro activo? El sistema de Maker usa un conjunto de smart contracts para conseguir dicha estabilidad, y ahora veremos cómo lo consigue.

## 11.1. El protocolo de Maker

Maker es un protocolo que une varios smart contracts que permiten generar la moneda DAI junto a algún otro componente. Este protocolo está descentralizado a través de su token de gobernanza, llamado maker. Es a través de este que se toma la mayoría de las decisiones sobre el protocolo: los stakeholders votan lo que consideran más adecuado, y en función del resultado se aplican unos cambios u otros.

Para entender cómo se crea el DAI, antes debemos poner como ejemplo las casas de cambio tradicionales. Imaginemos que dispongo de una obra de arte muy antigua que no solo tiene un alto valor económico, sino también emocional. Yo necesito dinero, pero no quiero vender la obra para conseguirlo. Lo que sí puedo hacer es pedir un préstamo y poner la obra de arte como colateral. Si la

obra tiene un valor de 100 000 EUR, la casa de cambio quizá concederá un préstamo de 50 000 EUR y, a cambio, se quedará la obra. En el momento que yo devuelva los 50 000 EUR más los intereses acordados, podré recuperar el cuadro. Me he podido apalancar sobre mi obra de arte para pedir un préstamo; y obviamente, si no devuelvo el préstamo, habré perdido el colateral.

Con esto en mente, ya podemos entender cómo funciona Maker. A través de unos smart contracts conocidos como CDP (posición de deuda colateralizada), el sistema de Maker permite crear DAI a través de un préstamo. Por ejemplo, yo dispongo de 10 000 USD en ETH, si deposito mis ETH en un CDP de Maker (ahora llamadas bóvedas de Maker o Maker’s vaults), puedo pedir un préstamo contra esos ETH en forma de DAI, una moneda estable con paridad 1:1 con el dólar. Existe otro smart contract llamado DSR (tasa de interés en DAI) que sirve para depositar tus DAI y ganar un interés sobre ellos gracias a las comisiones generadas en el protocolo.

Gracias a este sistema, conseguimos crear una moneda estable y descentralizada. Esto es muy relevante, ya que esta moneda, a pesar de ser estable y aportar cierta solidez en un mundo muy volátil, no depende de ningún banco ni de ningún colateral fiat guardado de forma centralizada. Aquí todo funciona por smart contracts y criptocolaterales. Todo es descentralizado.

Inicialmente, la única forma de generar DAI era poniendo ETH como colateral. Hoy en día, se pueden usar otros muchos activos:

| COLLATERAL TYPE | STABILITY FEE | LIQ RATIO | LIQ FEE | YOUR BALANCE | DAI AVAILABLE |
|---|---|---|---|---|---|
| ETH-A | 2.00 % | 150.00 % | 13.00 % | 0,1956 ETH | 195.00M |
| ETH-B | 6.00 % | 130.00 % | 13.00 % | 0,1956 ETH | 19.53M |
| BAT-A | 4.00 % | 150.00 % | 13.00 % | 0,00 BAT | 6.62M |
| USDC-A | 4.00 % | 101.00 % | 13.00 % | 0.00 USDC | 78.43M |
| USDC-B | 50.00 % | 120.00 % | 13.00 % | 0.00 USDC | 30.00M |
| WBTC-A | 4.00 % | 150.00 % | 13.00 % | 0,00 WBTC | 13.72M |
| TUSD-A | 4.00 % | 101.00 % | 13.00 % | 0,00 TUSD | 78.28M |
| KNC-A | 4.00 % | 175.00 % | 13.00 % | 0,00 KNC | 4.92M |
| ZRX-A | 4.00 % | 175.00 % | 13.00 % | 0,00 ZRX | 4.92M |
| MANA-A | 12.00 % | 175.00 % | 13.00 % | 0,00 MANA | 559.39K |
| USDT-A | 8.00 % | 150.00 % | 13.00 % | 0,00 USDT | 10.00M |
| PAXUSD-A | 4.00 % | 101.00 % | 13.00 % | 0,00 PAXUSD | 76.98M |
| COMP-A | 3.00 % | 175.00 % | 13.00 % | 0,00 COMP | 6.99M |
| LRC-A | 3.00 % | 175.00 % | 13.00 % | 0,00 LRC | 2.48M |
| LINK-A | 2.00 % | 175.00 % | 13.00 % | 0,00 LINK | 100.97K |

Figura 63. Tipos de colaterales en Maker con sus características

Como vemos en la imagen, cada activo tiene unos parámetros de colateralización y de liquidación diferentes en función de la solidez y volatilidad del activo usado como colateral. Uno de los límites de Maker y DAI es que la cantidad de DAI disponible en el mercado dependerá siempre de cuántas

bóvedas se hayan creado. Es por esto que la oferta de DAI es incapaz de seguir la demanda del mercado. Para facilitar la creación de más bóvedas y promover la creación de DAI, se han añadido más activos que se pueden usar como colaterales.

Esta fue una decisión difícil para Maker y sus token holders, ya que usar activos muy volátiles puede suponer mucho riesgo para el sistema. De hecho, uno de los objetivos a largo plazo de Maker es poder usar activos físicos tokenizados en, por ejemplo, Real Estate, y usar estos activos como colaterales para generar DAI.

La tokenización es un tema asombroso y fascinante. Sin duda, una buena forma para introducirse es a través del libro *Bitcoin, Blockchain y tokenización para inquietos*, de Miguel Caballero.

## 11.2. El colateral y otros parámetros

El colateral consiste en aquellos activos que se bloquean en una bóveda y que permiten generar DAI. Esto es algo muy delicado, porque se deben seguir unas normas que aseguren que nunca se va a prestar más dinero del que se ha depositado como colateral. De ser así, el protocolo entraría en pérdidas y podría hacer fallar todo el sistema.

Para esto, cada bóveda tiene una ratio de liquidación. Por ejemplo, para bóvedas en ETH, en el momento que el DAI prestado llegue a valer igual o más que el 75 % del valor colateralizado (o, dicho de otro modo, si la ratio del colateralización llega al 150 %), el colateral se va a vender a un precio de descuento en el mercado; de este modo, Maker se asegura de que el sistema no entre en pérdidas.

Cada activo tiene una ratio de colateralización diferente en función de su riesgo y volatilidad. Las liquidaciones suelen ocurrir cuando el valor del activo puesto como colateral cae. Para evitar que esto suceda, puedes añadir más colateral (poner más ETH en la bóveda) o devolver parte del préstamo, minorando tus posiciones de riesgo.

Otros parámetros a tener en cuenta, los cuales todos son votados por los stakeholders de Maker, son la stability fee (comisión es estabilidad) y la liquidation fee (comisión de liquidación). La stability fee es el coste que tiene generar un préstamo, es decir, el tipo de interés anual que hay que pagar para generar el préstamo.

Si pido un préstamo de 100 DAI con una stability fee del 1 % gracias a un colateral de 1000 USD en ETH, al cabo de un año deberé devolver 101 DAI para recuperar el colateral.

Por otro lado, la liquidation fee es la penalización del sistema por haber dejado liquidar tu bóveda. Cuando tu préstamo deja de ser seguro porque sobrepasa la ratio de colateralización, este se pone en venta en el mercado para poder recuperar el préstamo y así evitar que el sistema entre en pérdidas. Además, el sistema te cobra un 13 % como penalización. Si después de recuperar el préstamo y de haberse cobrado la penalización sobra colateral, este se deposita automáticamente en tu wallet.

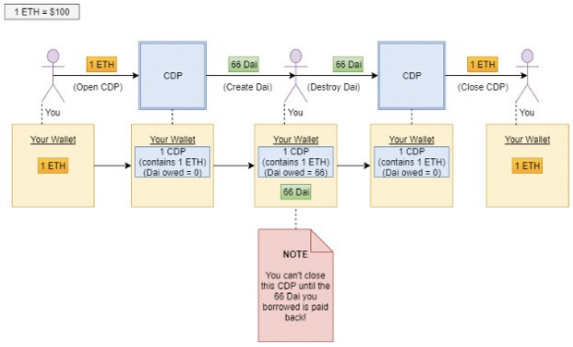


Figura 64. Ciclo de vida de una bóveda (CDP) en Maker

## 11.3. Casos de uso con Maker

Como vemos, DAI no solo sirve como base del sistema DeFi, sino que además cuenta con un sistema descentralizado que asegura que la moneda siempre estará respaldada por otros activos. De alguna forma, DAI representa la primera stablecoin descentralizada y la primera solución para poder apalancarse sobre tus propios activos.

Actualmente, las bóvedas se usan por motivos especulativos. Por ejemplo, yo dispongo de mucho ETH pero no quiero vender nada para comprar otras monedas. Por tanto, uso mi ETH como colateral y pido un préstamo para invertir en otros proyectos, aunque también puedo hacerlo por estrategias de trading o simplemente para hacer frente a pagos sin vender mis activos. Quizá necesito un coche pero no quiero vender nada de mi ETH porque confío que valdrá más en un futuro. Una opción es pedir un préstamo en Maker usando mi ETH como colateral y así comprarme un coche sin haber vendido nada de ETH.

Eso sí, mi recomendación es siempre utilizar Maker usando posiciones muy seguras. Es decir, si mi ratio de colateralización es del 150 %, voy a pedir un

préstamo para tener un ratio del 350 %, de este modo, aunque haya fuertes caídas del ETH, es muy poco probable que me liquiden la posición, ya que está muy sobreapalancada.

## 11.4. El Jueves Negro de 2020

El Jueves Negro no fue un día importante solamente en el mundo cripto, sino en todos los mercados financieros.

Se conoce como Jueves Negro el día en que, debido al confinamiento de muchos países a consecuencia de la COVID-19, los mercados de todo el mundo cayeron en picado, y, con ellos, también el mercado cripto.

Tanto Bitcoin como Ethereum cayeron más de un 50 % en cuestión de horas, lo que provocó grandes problemas en todo el ecosistema, sobre todo en DeFi. El más afectado fue Maker, que no consiguió recuperar los préstamos a través de la venta de los colaterales porque el precio del ETH estaba cayendo a demasiada velocidad. A pesar de liquidar las posiciones, al momento de vender el precio había caído tanto que no conseguía ni siquiera recuperar el préstamo que había generado en DAI.

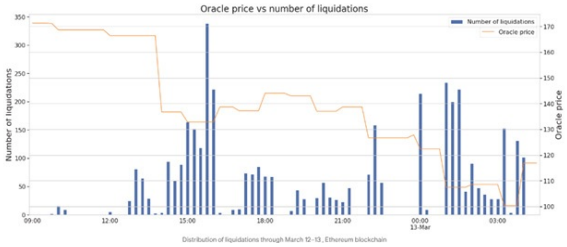



Figura 65. Evolución del número de liquidaciones en Maker durante el jueves negro (marzo 2020)

En definitiva, Maker acumuló unas pérdidas de más de 2 000 000 MUSD, que consiguió recuperar gracias a la emisión de nuevos tokens de Maker puestos a la venta en subasta. El gran problema fue que quedó demostrado que uno de los grandes pilares de DeFi no era tan sólido como se pensaba. A partir de ese momento, han empezado a aparecer otros proyectos que buscan trabajar en esta primera capa de stablecoins descentralizadas para darle más solidez y seguridad y evitar situaciones como las que se vieron ese día.

# 12. Protocolos para stablecoins descentralizadas: mStable

## 12.1. Introducción a mSTABLE

Uno de los proyectos que han aparecido para dar más solidez y seguridad al mundo de las stablecoins es mStable. Este no intenta competir con Maker, sino que es un protocolo que busca crear una segunda capa de seguridad al mundo de la stablecoins.

El problema detectado es que el mundo DeFi depende de unos pilares creados por las stablecoins que hacen de base de todo este lego de protocolos. De momento, estas stablecoins siguen teniendo riesgos asociados: DAI por fallos del sistema, y otras monedas como USDT, USDC y TUSD porque están centralizadas, podrían no estar respaldadas o sufrir ataques regulatorios.

Una de las piezas claves a mejorar es, de hecho, esta primera capa, ya que si los fundamentos de DeFi no son sólidos, la cantidad de protocolos que podremos crear encima serán limitados. Es por eso que mStable propone crear canastas de activos estables diferentes y usar esa canasta como colateral para crear una nueva moneda estable mucho más segura y sólida que las otras.

Vayamos más despacio; mStable es un protocolo que permite unir, gobernar y asegurar grupos de activos tokenizados. Todas las stablecoins son activos tokenizados, ya que son tokenizaciones de monedas convencionales, y si las agrupamos y generamos una nueva moneda, conseguiremos que esta nueva sea más segura y más sólida.

Es decir, mStable cuenta con unos contratos en los que puedes depositar stablecoins u otros activos tokenizados (pensado para futuras versiones) para así crear una canasta de activos donde todos representan al mismo, en este caso, el dólar. Entonces, se usa como colateral esta canasta llena de assets fragmentados y se crea una nueva moneda estable llamada mUSD. Esta nueva moneda, al estar creada con activos diferentes, es más sólida que los fragmentos usados como colaterales.

De este modo, yo puedo guardar mi dinero directamente en monedas estables y usar algunos protocolos DeFi que me permiten generar intereses mucho mayores que los que ofrecen las DeFi sin tener que preocuparme porque esta moneda pueda «irse a cero». Aunque nunca ha pasado, no significa que sea imposible. Con mUSD te aseguras de mantenerte estable aunque haya eventos como el que tuvo DAI durante el Jueves Negro.

## 12.2. Fragmentación de stablecoins vs. mStable

Actualmente, en DeFi hay muchas opciones de stablecoins. Por un lado, este es un hecho muy positivo porque es un signo del cambio revolucionario que estamos viviendo. Gracias a Blockchain hemos privatizado la creación de dinero y existen muchas opciones, todas ellas con propuestas de valor diferentes (en el mundo tradicional existe una moneda obligatoria generada por un Estado y nada más). Y aunque esto hace que el ecosistema sea más competitivo y tienda a mejorar su eficiencia más rápidamente, también supone un problema: hace que la experiencia de usuario sea complicada (muchas stablecoins por escoger) y fragmenta la liquidez.

mStable intenta mantener esta diversificación y crear un activo que agrupe estos assets tokenizados para lograr uno optimizado (al igual que en la trilogía de J.R. Tolkien: «Un anillo para gobernarlos a todos»).

## 12.3. El proyecto Meta

Meta es el token de gobernanza del protocolo y también el pilar que le da lógica a todo el sistema. Sirve para participar en la gobernanza y también como garantía de seguridad.

Los holders de meta pueden depositar sus tokens en la plataforma, recibiendo a cambio todas las comisiones que genera el protocolo y también pueden votar en las mejoras que se vayan a aplicar. Por contra, en caso de fallo de alguno de los activos dentro de las canastas, se usará este token para recompensar el valor perdido y asegurar que el mUSD sigue siendo estable.

Por ejemplo, pongamos que la canasta usada como colateral del mUSD está compuesta de USDT, USDC y DAI en proporciones iguales. Si USDT falla y acaba valiendo cero, el 33 % del valor de la canasta se recuperará a través de los metas depositados, garantizando así que el mUSD siempre será más estable que las otras stablecoins. Este evento se conoce como recolateralización y es votado por los holders de metas.

Tal proceso no está automatizado por un smart contract, porque las stablecoins, a pesar de que pueden perder valor por algún fallo o evento extraordinario, tienden a recuperarlo 1:1 con el dólar. Es por esto que, en casos donde una stablecoin se despega de su relación 1:1 con el dólar, hay que valorar si es porque el proyecto ha fallado, o solo porque ha pasado algo fuera de lo normal y que fácilmente volverá a recuperar su estabilidad. Esta decisión subjetiva no la

puede llevar a cabo un smart contract, y por ello depende de las votaciones de los stakeholders.

mStable, además, cuenta con algunos otros productos, como un smart contract para ahorradores, que permite que estos puedan generar un interés de sus mUSD dentro de la plataforma. Por último, también ofrece un servicio de intercambio entre stablecoins. Esta acción de cambiar un token por otro se conoce como swap y en mStable es posible porque la canasta tiene varios activos dentro. Si todos valen lo mismo, yo puedo usar la canasta para meter DAI y sacar USDC: habré cambiado el token gracias a la liquidez disponible en las canastas de mStable.

# 13. Exchanges descentralizados: Uniswap

## 13.1. Introducción a Uniswap

Uniswap es un proyecto DeFi nacido en noviembre de 2018 y desarrollado gracias a una financiación de 100 000 USD otorgado a los desarrolladores por la Fundación Ethereum. En poco tiempo se ha consolidado como uno de los protocolos más potentes en el mundo DeFi, además de ser el primer DEX (exchange descentralizado) en acumular un valor considerable. Un dato curioso es que este superproyecto ha sido impulsado por solo dos desarrolladores, que, además, no han generado ningún modelo de negocio alrededor de él. Es decir, no hay una fundación o un token interno que acumule el valor generado en el protocolo para poder financiar futuras mejoras en el desarrollo. Es algo que Vitalik Buterin define como «public pools»: sistemas descentralizados que benefician a todos aquellos que los usan. Aquí entra la discusión si estos proyectos son rentables a largo plazo, ya que, si tienen problemas, solo podrían financiarse a través de donaciones. Aunque pensándolo mejor, Bitcoin es al final algo muy similar a los «public pools» y, de momento, sigue siendo la blockchain más consolidada e importante.

El objetivo de Uniswap es permitir a los usuarios ejecutar swaps entre tokens generados en la red de Ethereum (principalmente tokens ERC-20). ¿Qué significa esto? Es como hacer un cambio de cromos. Ahora, cuando quieres cambiar un token, estás obligado a pasar por un exchange centralizado, pagar comisiones y comprometer cierta privacidad y seguridad, sin contar el hecho de que normalmente, para cambiar un token ERC-20 por otro (pongamos por ejemplo Chailink por BAT), tienes que comprar ETH con tu token LINK, y con ese ETH comprar BAT. Un doble gasto en gas y comisiones.

El swap ofrece otra solución: poder hacer cambios directos a nivel atómico sin pasar por ninguna entidad centralizada, todo a través del protocolo. Y a pesar de lo maravilloso que suena esto, lo más revolucionario de Uniswap no es el swap en sí mismo, sino la lógica que se ha integrado en el protocolo para que esto sea posible.

Para poder valorar el cambio que ofrece Uniswap, debemos primero entender cómo funcionan los mercados tradicionales.

## 13.2. Cómo funcionan los mercados tradicionales

Los mercados tradicionales funcionan todos de la misma manera: utilizan un libro de órdenes u order book para determinar el precio de un activo; son software algorítmico que conecta a compradores con vendedores. Con este software tienes dos posibilidades de entrar al mercado: comprando/vendiendo a precio de mercado, o comprando/vendiendo a un precio que tú determinas. Esto genera un libro de órdenes de compras y de ventas que permite al software identificar el precio del activo, ya que este siempre será el valor en el cual haya gente dispuesta a comprar y gente dispuesta a vender.


ORDER BOOK BTC USD

| COUNT | PRICE | AMOUNT | TOTAL | TOTAL | AMOUNT | PRICE | COUNT |
|---|---|---|---|---|---|---|---|
| 5 | 2,810 | 983 | 983 | 46 | 46 | 2,820 | 39 |
| 12 | 2,800 | 2,919 | 3,903 | 109 | 62 | 2,830 | 28 |
| 12 | 2,790 | 33 | 3,937 | 200 | 90 | 2,840 | 21 |
| 6 | 2,780 | 16 | 3,953 | 237 | 37 | 2,850 | 22 |
| 11 | 2,770 | 28 | 3,982 | 283 | 45 | 2,860 | 24 |
| 10 | 2,760 | 50 | 4,033 | 698 | 415 | 2,870 | 26 |
| 16 | 2,750 | 99 | 4,132 | 844 | 145 | 2,880 | 37 |
| 10 | 2,740 | 19 | 4,152 | 980 | 135 | 2,890 | 64 |
| 18 | 2,730 | 141 | 4,293 | 1,139 | 158 | 2,900 | 88 |
| 15 | 2,720 | 14 | 4,308 | 1,261 | 122 | 2,910 | 43 |
| 36 | 2,710 | 31 | 4,339 | 1,328 | 66 | 2,920 | 39 |
| 72 | 2,700 | 187 | 4,526 | 1,429 | 101 | 2,930 | 38 |
| 21 | 2,690 | 51 | 4,578 | 1,508 | 79 | 2,940 | 33 |
| 33 | 2,680 | 54 | 4,633 | 1,661 | 152 | 2,950 | 66 |
| 27 | 2,670 | 30 | 4,663 | 1,789 | 128 | 2,960 | 26 |
| 33 | 2,660 | 73 | 4,737 | 1,860 | 70 | 2,970 | 18 |
| 56 | 2,650 | 230 | 4,967 | 1,921 | 60 | 2,980 | 24 |
| 19 | 2,640 | 22 | 4,990 | 2,034 | 113 | 2,990 | 29 |

Figura 66. Libro de órdenes BTC/USD de Bittrex

Este método es el utilizado en cualquier exchange clásico, y permite acudir a estrategias de inversión como el uso bots algorítmicos capaces de predecir el comportamiento del precio a futuro analizando las órdenes registradas en el mercado. Se puede incluso simular niveles, o intentar posicionarse para ser el primero en liquidar la operación.

Este sistema también tiene ciertos problemas. Por ejemplo, en mercados con poco volumen, el precio puede ser muy manipulable, además del hecho de que en momentos de pánico, cuando nadie quiere comprar, el precio puede caer a cero a pesar de que el activo representado (las acciones simbolizan la propiedad de las empresas reales) sea mucho mayor. Sin ir más lejos, la crisis del COVID-19 ha provocado caídas de más del 80 % en algunas aerolíneas, a pesar de que estas sigan siendo las mismas que hace dos meses. Es por esto que las bolsas se cierran cuando hay caídas bruscas: para evitar este pánico que se extiende por todo el mundo y que provoca que nadie quiera comprar, dando lugar a una caída libre del precio, que seguirá su curso hasta encontrar un nivel donde haya gente dispuesta a comprar.

Otro problema es que muchas veces, para conseguir que la oferta y la demanda se encuentren, hace falta la intervención de los market makers, profesionales con

mucha liquidez que manipulan el libro de órdenes para asegurar que la oferta y la demanda se encuentren y, por tanto, haya movimiento de activos. En definitiva, se trata de mercados poco eficientes donde «la banca siempre gana», ya sea por una manipulación directa de precios o por las acciones de market making.


Figura 67. Acciones United Airlines (caída del **~ 80 %**) tras el efecto COVID-19

## 13.3. Análisis de la lógica de Uniswap

Uniswap funciona de modo completamente distinto a los modelos de mercado tradicionales, y esta es la parte más fascinante de su protocolo. Primero, la idea de que necesitamos dos partes (comprador y vendedor) dispuestas a hacer el swap y que un software las junte, ya no existe. En vez de esto, se crea un pool que aportará liquidez para que se puedan hacer swaps en cualquier momento. Esto a su vez implica que haya gente incentivada para bloquear sus tokens en un pool para dar liquidez a los swaps, como veremos más adelante. En segundo lugar, el precio no se determina por las órdenes de compra/venta, sino por una fórmula que mueve el precio cada vez que hay una orden para hacer un swap. Algo complejo que mejor lo vemos con ejemplos.

La idea es la siguiente: tenemos un pool con dos tipos de tokens que se pueden swapear. Cada pool está compuesto por dos tokens (por ejemplo, ETH y DAI), y habrá un pool diferente por cada par que se pueda swapear. Cuando una persona quiere swapear 1 ETH por su valor en DAI, el precio al que se pague el DAI que se quiere adquirir dependerá de la situación del pool. Cuanto más ETH se quiera swapear, más se va a encarecer el precio. El precio queda determinado por esta fórmula:

(ETH_Pool*XXX_Pool=Invariant)

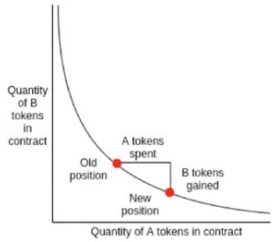



Figura 68. Algoritmo de fijación de precios de Uniswap

Pongamos el caso de que una persona quiere hacer un swap por valor de 1 ETH y recibir BAT a cambio. El precio del swap está directamente relacionado con la liquidez del pool y el total en valor del swap que se quiera realizar, ya que cuanto más presión de le pone al pool (en términos técnicos se le denomina «estrés»), más coste tendrá el swap. Esto permite desincentivar los swaps cuando hay poca liquidez en el pool, e incentivar los swaps en el caso contrario. De hecho, existen profesionales que se dedican a sacar rendimiento de estos desequilibrios con oportunidades de arbitraje.

Antes de la solicitud del swap, el pool tiene la siguiente situación: consta de 10 ETH y de 500 BAT. A partir de allí se calcula el invariant, un número que no puede variar y que se calcula multiplicando la cantidad de ETH * la cantidad de BAT. Al solicitar el swap, el pool pasa a tener más ETH que antes (11), así que el smart contract debe ejecutar un cálculo para saber cuánto BAT sobra en el pool para poder mantener el invariant a 500:

Es decir: 500 - (5000/11) => el resultado será la cantidad de BAT que va a recibir por 1 ETH.

Si en el ejemplo el swap fuera de menos valor (pongamos 0,1 ETH) la cantidad recibida cambiaría y pasaría a ser 4,9 BAT. Como ves, el valor adquirido es proporcionalmente superior al de antes, ya que al pedir menos al pool, este no ve tan comprometida su liquidez y ofrece un mejor precio por el swap. ¡Increíble!

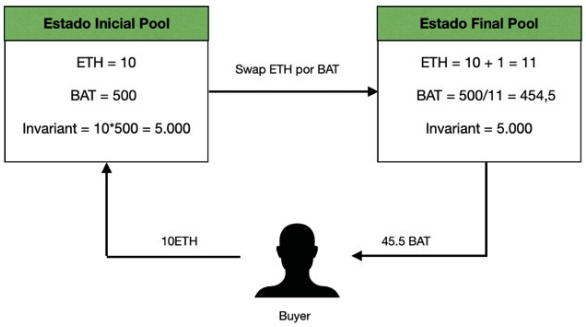



Figura 69. Swap de ETH por BAT en Uniswap

Pongamos un último ejemplo para dejarlo más claro. Una persona quiere hacer un swap en el pool de (ETH-MKR) para swapear 10 ETH por la cantidad correspondiente de MKR. Recordemos que la cantidad de MKR dependerá de Uniswap, en función de la liquidez del pool y de la presión que le pongamos (cuánto más valor queramos swapear, más presión ponemos al pool). Este pool consta de 1000 ETH y 470 MKR. Hagamos los cálculos:

- **Invariant** = 1000 * 470 = 470 000

La situación del pool ahora ha cambiado, tenemos 1010 ETH, y acto seguido debemos calcular la cantidad de MKR que va a recibir el solicitante del swap, ya que debemos mantener el invariant estable.

- 470 000 / 1010 = 465,34
- 470 - 465,34 = 4,675 MKR

El solicitante va a recibir 4,675 MKR. Si repetimos el ejemplo, pero solicitando un swap de 100 ETH, la cantidad de MKR recibida sería 42,72, un precio porcentualmente más caro que el anterior ya que hemos estresado (solicitado más liquidez) al pool, y este ha movido el precio del swap en consecuencia.

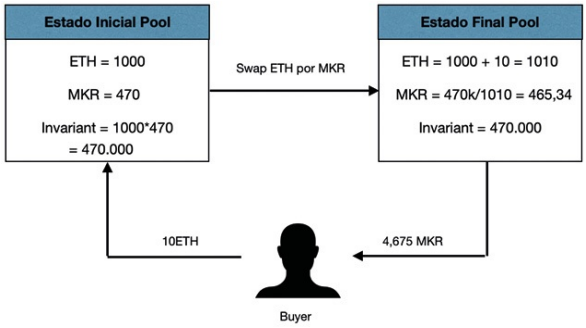


Figura 70. Swap de ETH por MKR en Uniswap

# 13.4. Pools de liquidez en Uniswap

La pregunta que deberíamos hacernos es: ¿De dónde sale esta liquidez en los pools? ¿Qué incentivo hay para congelar tus activos en un pool de Uniswap para permitir que la gente los pueda realizar?

Aquí entra el juego de las comisiones por swap, las cuales oscilan entre el 0,3 % en los swaps donde uno de los tokens sea ETH, y 0,6 % cuando ninguno de los tokens swapeados sea ETH.

Estas comisiones se reparten, como recompensa, entre todas las personas que están dando liquidez al pool. Este tema resultará interesante a los inversores, ya que podemos llegar a ver rendimientos de hasta + 90 % anual. La rentabilidad vendrá dada por la combinación de dos variables: la liquidez del pool y el volumen diario.

- **Poca liquidez - mucho volumen.** Esta es la combinación perfecta, ya que no solo habrá mucho volumen y por tanto muchas comisiones, sino que además el precio de los swaps será alto, ya que el pool se verá estresado cada vez.
- **Mucha liquidez - mucho volumen.** Esta también es una combinación acertada, ya que seguramente el valor movido en el pool no será tan alto como en casos de poca liquidez (el pool no estará muy estresado y permitirá swaps a buenos precios) pero habrá mucho volumen para generar rentabilidad con las comisiones.
- **Poca liquidez - poco volumen.** Al haber poca liquidez, seguramente los precios serán altos, pero no habrá mucho rendimiento porque el volumen será bajo.
- **Mucha liquidez - poco volumen.** Esta es la peor combinación, ya que no solo los precios serán bajos (al igual que las comisiones) sino que además habrá poco volumen para cobrar las mismas.

Este es el motivo por el cual Uniswap seguramente ha crecido tanto, siendo el primer exchange descentralizado que realmente ha sido capaz de acumular mucho valor bloqueado en sus pools de liquidez. Para poder conocer la liquidez y rentabilidades de los pools en Uniswap podemos visitar: www.pool.fyi, la herramienta analítica de Uniswap: https://info.Uniswap.org/home o también una herramienta externa como https://www.Uniswaproi.com/#. Y, si queremos añadir liquidez y sacar rendimiento a nuestro capital cripto, lo podemos hacer desde https://www.Uniswap.com.

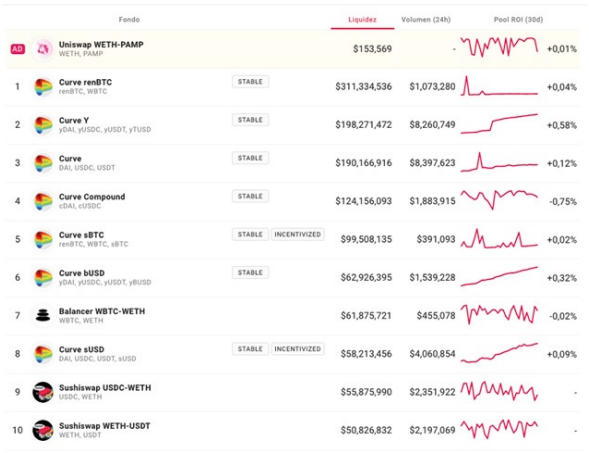


Figura 71. Principales pools de liquidez en Uniswap. Fuente: pools.fyi

No menos importante es también comentar los riesgos, que aunque no los hay (ya que no vas a perder dinero, solo generar ingresos a través de las comisiones de los swaps) sí puede ocurrir que obtengas un interés negativo debido a la caída del precio de los tokens depositados, y no debido al protocolo. El riesgo —o, mejor dicho, la característica de los pools— es que siempre se deben depositar dos tokens (ETH-DAI/ETH-MKR/ETH-BAT…) y por tanto, en función de la demanda de los swaps, acumularás más de un token que del otro. Este desbalance es más exagerado cuando uno de los tokens pierde mucho valor, ya que, debido al protocolo, suele ser este el que más acumulamos.

Unas aclaraciones para cuando queremos añadir liquidez: debemos guardar dos tokens en ese pool en función del par con el que queramos participar, y el valor de los dos debe ser el mismo. Por ejemplo, si quiero poner liquidez en el pool de ETH-DAI, al poner 1 ETH (ej. valor actual 400 USD), estaré obligado a poner 400 DAI (1 USD). Una vez en el pool, la proporción entre estos dos variará en función de la demanda de los swaps. Generalmente, debido al protocolo se acumulará más del token que haya bajado más de valor. Tus rentabilidades las adquirirás a través del token del pool llamado UNI-V1 (ver en etherscan), que representará la proporción del pool de la cual tú eres propietario y que, a su vez, irá acumulando las rentabilidades que genere el pool. Será a través de ese token con el que podrás recuperar tu inversión y cobrar las rentabilidades que hayas ido generando.

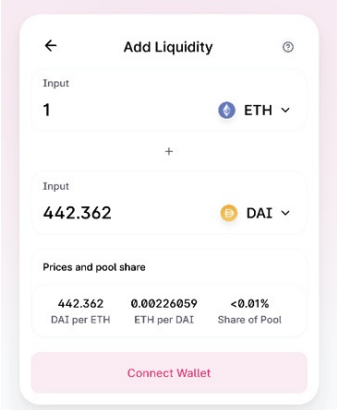



Figura 72. Añadiendo liquidez en Uniswap (LP o Liquidity Provider). Uniswap.exchange/add-liquidity

## 13.5. Uniswap: conclusiones

Una vez hemos visto cómo funciona Uniswap y todas las posibilidades que nos brinda, dediquemos un momento a reflexionar sobre qué representa esta innovación en el campo de las finanzas y porqué es revolucionario.

El primer punto está claro: es una forma nunca vista de calcular el precio y de generar mercados. Por primera vez, el precio no se regula por las órdenes de compra, sino a través de un algoritmo que mueve el precio por cada swap que se realiza en el pool. Ahora ya no hace falta tener órdenes de compra para poder mantener el precio de un activo. **Adiós a las fortunas gastadas en market makers para mantener el precio de un activo.**

Otra cosa maravillosa es la posibilidad de crear mercados de la nada y de dar liquidez a un token (o a un activo tokenizado) sin necesidad de listarlo en un exchange, donde tampoco te aseguran liquidez, ya que esta dependerá de las órdenes de compra venta que haya. Con Uniswap tú puedes dar un valor y liquidez a tu token creando un pool con ETH que le otorgue un valor. Si le damos un par de vueltas, crear un pool con 100 ETH y 100 de nuestros tokens implica que nuestro token pasará a tener un valor de 1 ETH. Como veis, acabamos de dar liquidez, valor y mercado a un nuevo token y no hemos necesitado cientos de miles de dólares para listarlo en un exchange, donde probablemente necesitaremos market makers para generar órdenes de compra para que su valor no caiga a cero.

Otro dato sorprendente es que en Uniswap se pueden swapear security tokens. Actualmente ya hay algunos disponibles, aunque no lo podremos ver desde nuestro MetaMask, ya que, para transaccionar con securities, debemos

acreditarnos con la empresa emisora del token del que somos inversores acreditados.

Aun así, la idea detrás es fascinante: puedo vender mi 0,1 % de un bloque de pisos en Madrid en cualquier lugar y en cualquier momento. Esto sí es dar liquidez a mercados no líquidos.

El primer proyecto en usar pools de Uniswap para dar liquidez a STO ha sido RealT, aunque cada vez son más los que se adentran en este espacio. De hecho, dos proyectos que hemos lanzado junto a nuestros alumnos de los másters y bootcamps son RentalT y CritptoKuantica, los cuales también aportarán liquidez a los inversores mediante pools de security tokens en Uniswap.


Figura 73. cryptokuantica.com y rentalt.co incorporan liquidez en Uniswap para cada uno de sus assets

Esta innovación también permite nuevos modelos de negocio como el caso de los Unisocks, calcetines limitados que solo se pueden comprar con el token unisock, solamente disponible en Uniswap. Esto significa que cada vez que alguien adquiera un token para comprar los calcetines, el valor del token aumentará, dando cada vez más valor a los calcetines en función de su escasez: el pool tendrá menos liquidez y por tanto el precio del swap será más alto.

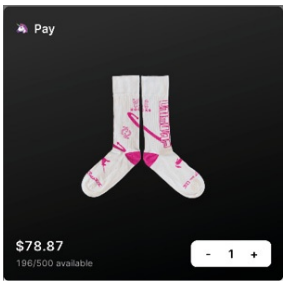



Figura 74. Unisocks y su modelo de liquidez basada en Uniswap

Sin duda alguna estamos en un momento de cambios e innovaciones. Las puertas que nos abre el mundo DeFi son ilimitadas y cada vez se abrirán nuevas. En los próximos años veremos cómo la tecnología Blockchain conectará al mundo financieramente de la misma forma que Internet nos conectó socialmente. Y es, de hecho, esta característica la que más me fascina de los protocolos DeFi: no hay restricciones, cualquier persona del mundo puede participar y acceder a servicios financieros que anteriormente solo eran accesibles para una minoría.

# 14. Exchange Descentralizados: Sushiswap

Vale la pena comentar el caso de Sushiswap porque, a pesar de que ha acabado siendo un proyecto con menos éxito de lo que se pretendía, ha provocado un cambio de pensamiento en el mundo DeFi.

Sushiswap es un hard fork de Uniswap (al ser todo open source, los proyectos pueden ser copiados) que nació con el objetivo de reemplazar a Uniswap como DEX principal en DeFi. Lo curioso es que su plan para conseguirlo era nada más y nada menos que migrar (o también podríamos decir «robar») toda la liquidez que había en Uniswap hacia Sushi. Es decir, quería copiar Uniswap y añadirle algunos cambios para dar más valor a la comunidad y a los proveedores de liquidez para que estos prefiriesen llevar sus activos de Uniswap a Sushiswap.

Sushiswap llegó después de la aparición del concepto de yield farming y liquidity mining que veremos más adelante en profundidad. Aun así, esto no supondrá un problema para entender el protocolo y cómo evolucionó.

## 14.1. Sushiswap y la filosofía de la descentralización

Como hemos dicho, Sushiswap es un hard fork de Uniswap. La única diferencia es que ha añadido un token de gobernanza con el cual el poder sobre el protocolo se reparte entre la comunidad.

Para ponernos en contexto, durante ese momento Uniswap había cambiado su política de fees y subieron las comisiones por swap del 0,25 % al 0,3 %. Los proveedores de liquidez seguían obteniendo el 0,25 % como recompensa, pero este nuevo 0,05 % iba directo al equipo de Uniswap y a sus inversores. Uniswap era y sigue siendo uno de los protocolos más rentables, así que estamos hablando de beneficios de cientos de millones de dólares por mes. Esta fue la principal motivación detrás de Sushi, eliminar a estos inversores que centralizaban el valor generado por miles de usuarios y distribuir este valor entre la comunidad.

Como vimos en el capítulo de Uniswap, la idea de «pool público» acabó fracasando ya que el equipo de desarrollo necesitaba financiación para seguir mejorando el protocolo si quería seguir compitiendo en el mundo DeFi. Subir las fees era la única solución para capitalizarse.

Aquí es donde veo que **Sushiswap representa algo exageradamente disruptivo para DeFi**. Básicamente pretendieron dar a la comunidad el poder de un proyecto financiado y dirigido —el original— por VC. Por tanto, en

Sushiswap los poseedores del token sushi serán los propietarios del protocolo, participarán en la gobernanza y además recibirán el 0,05 % de cada swap realizado. ¿Cómo de revolucionario es esto, ya que no solo es algo «tecnológicamente posible» sino que, además, Uniswap quizá no podía hacer nada para evitarlo? Ahora bien, con esto no estoy alabando el trabajo de Sushiswap, ya que surgió como proyecto no auditado y que fácilmente podría haber sido un scam con el que se habrían perdido miles de millones, aunque el *hype* y el alboroto que generó Sushi en DeFi y en el ecosistema cripto fue tal que incluso algunas grandes firmas empezaron a auditar el protocolo prácticamente a cambio de nada. Lo nunca visto.

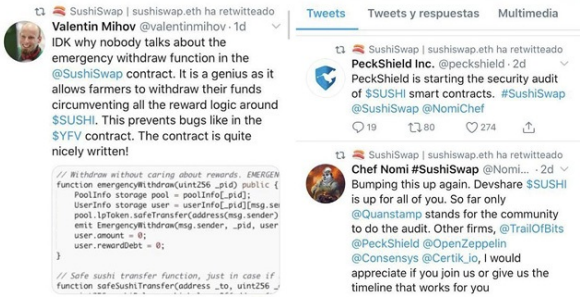


Figura 75. Tweets sobre auditorías «descentralizadas» hechas por la comunidad en Sushiswap

Esta situación en la cual un hard fork consigue llevarse todo el negocio del proyecto forkeado se ha denominado *vampire mining*. A través de incentivos y un sistema que retribuya mejor a la comunidad, un protocolo forkeado puede llegar a comerse al original. Dicho a la ligera parece poco…, pero ¿qué representa esto a nivel filosófico?

Pues básicamente que gracias a Sushiswap existe la opción de forkear proyectos y dar más poder a la comunidad a cambio de que sus miembros traspasen sus fondos a estos nuevos protocolos. Ahora no hay dudas: en Blockchain, el poder está en la comunidad y no en los VC. Por otro lado, **hemos comprobado cómo el dinero rompe el amor**: la fiel comunidad de Uniswap le dio la espalda cuando vio que había una forma mejor de monetizar sus aportaciones.

Para que te hagas una idea del *boom* que tuvo Sushi en el ecosistema, Uniswap superó por primera vez a Coinbase Pro en volumen movido, unos 500 000 000 USD diarios. Esto se debe a que, antes de migrar a Sushiswap, debías haber participado en Uniswap, entonces entró mucho capital en Uniswap que, acto seguido, quedaba vinculado a Sushiswap, pendiente de que los activos se migraran al nuevo protocolo. Si el 0,05 % de este volumen se reparte entre la comunidad, estamos diciendo que ese mismo día se hubieran repartido más de

2 500 000 USD entre los 100 000 000 de sushi tokens que iban a emitir. Sin duda, esto era MUY atractivo.

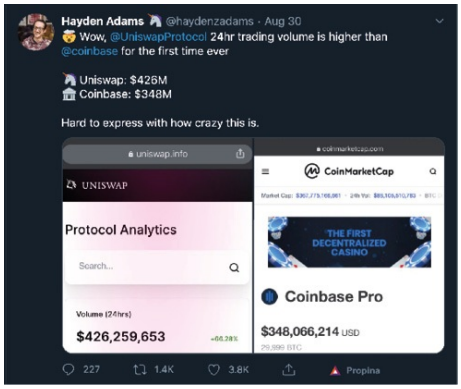


Figura 76. Hayden Adams sobre Uniswap, superando a Coinbase Pro en volumen

## 14.2. Comparativa de Sushiswap con el mundo tradicional

Para poder dar más peso y comprensión a este suceso, compararemos la jugada de Sushiswap aplicándola al mundo tradicional. Aunque no sea posible, ya que en el sistema tradicional los proyectos no son open source y no son «copiables», haremos una excepción para demostrar la magnitud de lo sucedido.

Pongamos que somos clientes del mayor banco español. En él, millones de clientes tienen depositados sus ahorros, que suman un total de más de 6 000 millones EUR en cuentas. Un día, una persona anónima, vamos a llamarle igual que al responsable de Sushiswap, Master Chef, publica un *post* donde avisa que va a forkear este banco y que a todos los que certifiquen que tienen dinero allí depositado y confirmen que quieren migrar al nuevo banco una vez se haga el fork, les va a repartir durante dos semanas (y de forma muy agresiva) las acciones de este nuevo banco. Finalmente, tal día, el fork se genera y todas estas personas que han estado recibiendo acciones del nuevo negocio pasan a formar parte del banco más importante de España; y no solo eso, sino que además ahora son los propietarios.

Esto es un ataque en toda regla a Wall Street.

## 14.3. Funcionamiento de Sushiswap

En el momento inicial, Sushiswap era un conjunto de smart contracts que te permitían hacer farming (ya veremos qué significa) de los futuros tokens de

gobernanza Sushiswap a cambio de depositar en tal smart contract los liquidity tokens (LP) de Uniswap. Los LP tokens de Uniswap te permiten recuperar la liquidez que hayas añadido a algún pool (UNI-V1, UNI-V2, etc.).

Ahora entendemos por qué Uniswap vio multiplicado su TVL: porque si querías participar en el farming de sushis debías primero depositar liquidez en Uniswap. Y la verdad, no era de extrañar si vemos las rentabilidades que se ofrecían en sushis:

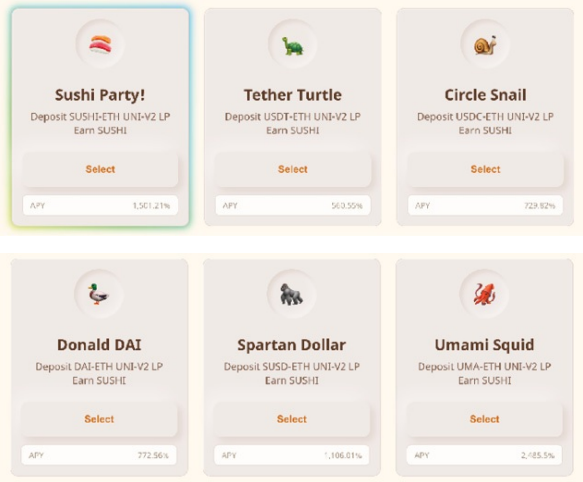



Figura 77. Rentabilidades (TAE o APY) en Sushiswap al momento de postear, pagadas en sushis

Estos smart contracts servían para después hacer una migración completa, ya que si quieres llevarte todo el negocio de Uniswap, no puedes hacerlo poco a poco, debe ser un golpe directo. Sobre todo porque el valor y usabilidad que aporta un exchange descentralizado está directamente relacionado con su liquidez. Si Sushiswap no conseguía tener mucha liquidez al principio no podría atraer a usuarios para usar su protocolo. Entonces esto era lo que se pretendía con esta primera fase de farming, además de repartir el poder de voto del futuro protocolo.

En cuanto a consecuencias, además del incremento de valor de Uniswap, también podemos entender por qué Uniswap superó en volumen a Coinbase Pro: porque las fees subieron de forma tan exagerada esos últimos días y porque algunos tokens subieron en cotización. Esto último fue debido a que, si querías participar pero no tenías tokens suficientes, los tenías que adquirir, haciendo subir la demanda.

En definitiva, un *post* de *Medium* consiguió que, en solo cinco días, el 67 % del valor depositado en Uniswap estuviera bloqueado en smart contracts de un protocolo no auditado que ofrecía una promesa a futuro. Sin lugar a dudas esto es una locura, y demuestra la inmadurez del ecosistema DeFi actual, porque a

pesar de «tener sentido», el riesgo que se estaba asumiendo seguía siendo demasiado alto. Y, por si el *hype* generado no fuese ya bastante, el token sushi se listó al cabo de pocos días en Binance.

## 14.4. Distribución de los sushi tokens

Los sushi tokens se distribuyeron a través de liquidity mining o yield farming (programa de incentivos que veremos más adelante en detalle). Estarían minando (generando) sushis quienes depositaran los LP tokens de Uniswap de estos pares en los contratos de Sushiswap:

- USDT-ETH
- USDC-ETH
- DAI-ETH
- sUSD-ETH
- COMP-ETH
- LEND-ETH
- SNX-ETH
- UMA-ETH
- LINK-ETH
- BAND-ETH
- AMPL-ETH
- YFI-ETH
- SUSHI-ETH

Aunque los pares pueden cambiar a través de votaciones de la comunidad, estos son los que inicialmente se remuneraban. Estos incentivos se iniciaron en el bloque 10 750 000 de Ethereum y se reducían después de 100 000 bloques (en dos semanas). Durante esas dos semanas, se generaron más de 1000 tokens por bloque (cada 15 segundos) que se repartían entre la comunidad.

## 14.5. El futuro de Sushiwap

Al ver este suceso solo me viene a la mente que estos tipos de protocolo pueden seguir apareciendo. Y aunque diluyen la liquidez y por tanto el valor ofrecido por algunos protocolos, también pueden llegar a mejorar sus tokenomics y modelos de gobernanza para dar más poder y retribuciones a la comunidad. Quizá los protocolos DeFi tendrán que adoptar nuevas estrategias para fidelizar

más a su comunidad y distribuir mejor el valor que generan y así evitar casos de vampire mining.

Como siempre, esto tampoco tiene por qué ser bueno, ya que seguimos en medio del conflicto entre pura descentralización o media descentralización. **Dejar la evolución del protocolo y su gobernanza íntegramente en manos de la comunidad quizá no sea la mejor opción.** Solo el tiempo lo dirá.

Por otro lado, en ese momento nadie podía predecir cómo acabaría todo. Teníamos posibles escenarios:

- El primero era que todo esto quedara en una broma, que la mayoría de los fondos no se hubieran migrado y que Uniswap hubiese mantenido el liderazgo.
- La segunda era ver cómo Sushiswap conseguía nacer como nuevo protocolo (y con fuerza) ya que se quedaría con un poco más o un poco menos de liquidez que la que había en Uniswap.
- La última opción era que Sushiswap se llevase prácticamente toda la liquidez de Uniswap y que hubiéramos clasificado el ataque de vampire mining como un éxito rotundo, dejando perplejos a todos el ecosistema DeFi.

En cuestión de semanas veríamos el resultado y, mientras tanto, todo el ecosistema andaba loco. Yo personalmente miné algunos sushis, sobre todo porque la idea detrás del proyecto me fascinó. Confiaba más en Uniswap como proyecto, principalmente por el equipo que había detrás, pero también creía que los fundadores acumulaban demasiado poder y que era inteligente intentar descentralizar, a la vez que así se repartía parte del valor generado por el protocolo directamente a la comunidad.

Esta fascinante historia acabó quedándose solo como una anécdota ya que aunque en un momento inicial Sushiswap se posicionó rápidamente como uno de los mayores protocolos por capitalización —quedándose con casi la mitad de los fondos que había en Uniswap— fue perdiendo fuerza hasta que a día de hoy prácticamente no dispone de liquidez y por tanto no tiene sentido hacer uso de él.

El problema principal fue que su fundador anónimo aprovechó el momento para deshacerse de gran parte de los tokens sushi que tenía, haciendo caer el precio y abandonando la credibilidad que la comunidad le había depositado. Esto fue un duro golpe para la moral de los que creían en el proyecto. Primer problema.

Como segundo problema, en cuestión de semanas, Uniswap presentó su plan para descentralizar el protocolo y crear el token UNI, que se repartiría a todos aquellos que hubieran usado al menos una vez el protocolo. Es decir, mágicamente un día todos los usuarios de Uniswap recibimos mínimo 400 UNI gratuitamente, fue un día maravilloso. Ese mismo día llegó a valer 7 USD cada token. Los UNI tienen unos tokenomics muy bien diseñados, además de contar también con la propuesta de valor de Sushiswap: dar a la comunidad ese 0,05 % de cada swap. Al final, por errores de uno y virtudes del otro, Uniswap ha conseguido mantener su posición y mantenerse líder de los DEX en Ethereum. Aunque también es importante destacar el peso del equipo, ya que aunque Sushiswap fuera en su momento atractivo, el peso de conocer quién está detrás del proyecto es muy relevante para la comunidad, y en esto Uniswap era claramente superior.

De todos modos es importante conocer este evento por las implicaciones filosóficas que trajo con él. En el mundo DeFi el poder está en la comunidad, y en caso de que un protocolo de forma centralizada tome decisiones que la comunidad no comparta fácilmente, puede ver cómo todos sus fondos desaparecen para irse a un competidor que hace lo mismo pero que aporta más valor a los usuarios y a la comunidad del proyecto.

# 15. Exchanges descentralizados: Balancer

Los exchanges descentralizados nacen para solucionar un problema latente en el mundo cripto: la dependencia en casas de cambio centralizadas que generan fricción, costos y pérdida de tiempo. La idea era crear una plataforma descentralizada donde pudieses tradear tus assets sin perder el control sobre ellos, y con comisiones y tiempos mínimos.

El primer DEX que ganó tracción —analizado en el capítulo anterior, Uniswap — es un protocolo que actúa como exchange descentralizado en la red de Ethereum y que ofrece transacciones de intercambio o swaps a través de liquidez bloqueada en pools, aportada por usuarios que buscan generar una rentabilidad a sus activos.

Después de dos años liderando el mercado, Uniswap empezó a tener los primeros rivales con un nuevo DEX llamado Balancer. Este proyecto nace con el objetivo, similar a Uniswap, de permitir AMM (automated market making) para así generar ingresos a través de esos activos parados que generan rendimiento. Es decir, como ocurre en Uniswap, los proveedores de liquidez (LP) pueden depositar sus activos en pools existentes para poder ofrecer swaps a los traders que compensan a los proveedores generando un rendimiento a sus activos a través de unas fees. Balancer te permite crear todo tipo de pools, incluso convertir todo tu portfolio en uno. Con más de ocho tokens y con una distribución más interesante que Uniswap, no estás obligado a mantener una proporción del 50 % entre dos tokens. Sin duda existía una gran demanda para proveer liquidez de forma flexible e independiente nativamente en un protocolo, y Balancer la ha sabido aprovechar.

Por todo ello, Balancer es un protocolo multitoken que permite market making automático con la posibilidad de crear infinidad de pools con diferentes proporciones entre tokens, número de tokens y con fees que pueden moverse entre el 0,0001 % y el 10 %.

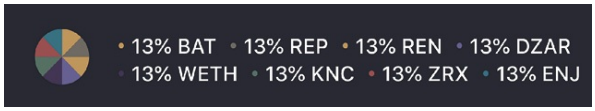



Figura 78. Pool en Balancer con 8 tokens con un peso del 13 % cada uno

## 15.1. Balancer y sus innovaciones

La misión de Balancer es ofrecer un protocolo financiero que permita, de forma flexible y descentralizada, aportar liquidez programable, y mediante esta, ofrecer a todo el ecosistema swaps instantáneos on chain con costes de gas eficientes.

A primera vista puede parecer que Balancer no es más que un Uniswap con la posibilidad de crear pools con más tokens y con proporciones entre tokens diferentes al 50/50, pero si estudiamos bien el protocolo, nos daremos cuenta de que es mucho más que esto.

En las finanzas tradicionales encontramos los denominados index asset managers o fondos de inversión indexados que mantienen constante la distribución entre los diferentes assets. Aquí, a los inversores se les cobra una comisión no solo por participar en el fondo, sino también por los rebalanceos entre assets que se van actualizando por los asset managers. Balancer ha invertido completamente la lógica económica de estos fondos. Ahora, no solo no tienes que pagar fees por participar en los pools actuando como proveedor de liquidez, sino que además generas ingresos a través de fees por conseguir este rebalanceo. Te pagan por participar en un protocolo con una función de asset management integrada de forma nativa. Esto se debe a que el protocolo vende parte de sus assets y cobra una comisión por la venta para así poder reequilibrar las proporciones entre los tokens.

Este rebalanceo tiene lugar a través de arbitraje, ya que los inversores están incentivados a tradear con pools donde el precio ha subido o bajado hasta zonas donde es rentable hacer una operación, y reequilibrarlos. Ello permite que los pools cobren comisiones por estos trades y por tanto generan rendimiento a los proveedores de liquidez, además de que permiten rebalancear de nuevo el portfolio.

De alguna forma, Balancer ha descentralizado completamente el concepto de market making, no solo por lo que hemos comentado anteriormente, sino porque además siempre tienes la opción de convertir todo tu portfolio en un pool nuevo. Es decir, puedes escoger la distribución entre tokens que prefieras y usar Balancer para rebalancear esas proporciones, además de cobrar fees por hacerlo. ¡Simplemente asombroso!

Hasta aquí tampoco estamos teniendo en cuenta la contribución de Balancer al ecosistema, ya que actúa como una especie de *sandbox* que nos permite innovar e investigar en relación a pools con proporciones y fees desiguales y así encontrar soluciones a problemas que aún no hemos encontrado.

## 15.2. Funcionamiento del protocolo

A nivel de protocolo, el funcionamiento para determinar el precio de los swaps es muy similar a Uniswap. El framework matemático es más complejo debido a que debe calcular precios en pools con proporciones diferentes al 50/50, manteniendo también el equilibrio porcentual entre los tokens.

En Balancer podemos encontrar dos usuarios: los proveedores de liquidez y los traders. Los **proveedores de liquidez** son aquellos que actúan como propietarios de los pools, y que aportan sus assets en ellos para ofrecer swaps eficientes y baratos a los traders. Generan un rendimiento de su capital a través de fees, además de tener un servicio remunerado de asset management, ya que puedes participar o crear en todo tipo de pools, con tokens y distribuciones completamente distintas. Por otro lado, tenemos a los traders que «usan» los pools como servicio de exchange para hacer swaps entre tokens. Estos, además, pueden usar el protocolo para generar oportunidades de arbitraje. Un tipo de trader que hace uso de los pools podrían ser también smart contracts que usan Balancer como proveedor de liquidez para ejecutar sus funciones previamente programadas.

Cuando un trader hace una solicitud para un swap, el protocolo calcula el precio con un sistema similar al que usa Uniswap, aunque no 100 % igual. Es decir, los criterios básicos para determinar el precio sí coinciden: la liquidez de los pools y la cantidad solicitada. Cuanto más se estresa al pool, más slippage (movimiento del precio) habrá.

Analicemos la primera diferencia. En Uniswap, los cálculos para determinar precios son más sencillos ya que cada par de tokens tiene un pool propio. En Balancer, en cambio, podemos encontrar un mismo par en muchos pools diferentes, todos ellos con liquidez diferente, número de tokens diferente y diferente distribución de esos tokens. Es por eso que en Balancer se integra un optimizador de precios off chain conocido como SOR (Smart Order Router). Consiste en un routing que en función del par de tokens que se quiere swapear y la cantidad, busca entre todos los pools con ese par para aportar el mejor precio posible. Este «mejor precio» puede implicar usar varios pools e incluso swaps con diferentes cantidades en función del pool.

Pongamos un ejemplo: imagina que quieres hacer un swap de 3 ETH por AAVE. En el momento en que hagas la solicitud del swap, el protocolo usará el SOR para buscar, entre todos los pools que contengan ETH y AAVE, cuál es la mejor combinación para obtener el mejor precio. El resultado podría ser hacer un swap de 1 ETH en el pool X, que contiene ETH, LINK, AAVE y MKR; hacer un

swap de 1,5 ETH en el pool Y que contiene LEND y DAI, y un último swap de 0,5 ETH en pool Z que contiene AAVE, DAI, USDC, SNX y KNC.

Este routing, que estará disponible on chain en futuras actualizaciones, es realmente asombroso. Te permite usar varios pools para evitar que el slippage te perjudique y así conseguir precios muy competitivos. Con esta lógica, los precios de Balancer deberían ser los más económicos del ecosistema, y, aunque es así, en algunas ocasiones tiene un pequeño problema: interactuar con un pool implica ejecutar un smart contract en la red de Ethereum, lo que implica pagar un gas fee. Esto hace que muchas veces la mejor opción no sea posible debido al aumento del coste del gas, cosa que el SOR también tiene en cuenta. Esto, además, crea desbalanceos y por tanto oportunidades de arbitraje. Veámoslo a continuación.

Como el gas fee aumenta, el protocolo no puede usar todos los pools disponibles para conseguir el mejor precio, así que por lo general usará el que más liquidez tenga y quizás alguno más. Esto hace que los precios establecidos entre pares concretos sean distintos entre los diferentes pools, provocando que parte del valor que el trader ha dejado atrás se lo acabe llevando una operación de arbitraje que buscará reequilibrar los precios entre pools. Esto es normal cuando hay cambios en los precios de los activos, pero son también una muestra de ineficiencia cuando sucede por desequilibrios de los pools no generados por cambios en el valor de los tokens del portfolio.

El caso idóneo (quizá posible en un futuro) será tener costes de gas tan mínimos que un trade pueda hacer uso de tantos pools como sea necesario, consiguiendo así que el precio de intercambio entre dos tokens se mueva de forma exacta entre todos los pools que contienen ese par.

## 15.3. Pools desiguales

Una particularidad de Balancer, como hemos ido viendo durante el post, es la posibilidad de crear pools con varios tokens y con proporciones diferentes. En Uniswap, por ejemplo, solo existe un pool por cada par, y este contiene una proporción del 50/50 entre los dos tokens.

Vamos a dedicar unas líneas para investigar posibles casos de uso, además de comentar las consecuencias que pueden tener estos tipos de pools.

## 15.4. Pools disparadores de liquidez

Este concepto es para mí de los más interesantes de Balancer. Uno de los casos de uso más atractivos de Uniswap era la posibilidad de generar mercados de la nada, ya no tenías que pasar por un exchange para dar liquidez a tu propio token. Gracias al market making descentralizado y a la posibilidad de establecer un precio a los tokens sin un libro de órdenes, podías crear un mercado a tu propio token sin casi ninguna fricción.

Aunque suene muy interesante, este caso de uso tenía algunas limitaciones, siendo la más importante el hecho de que para poder crear un pool de tu propio token debías poner en ETH o en un ERC20 el equivalente al 50 % del valor que quisieras depositar, haciendo esta opción poco atractiva para aquellos que no disponen de fondos. De hecho, si lo comparamos con una alternativa a financiación clásica de una ICO, resulta paradójico que necesites la mitad del capital que querrías obtener durante dicha ICO.

En Balancer ahora puedes usar pools con proporciones tan radicales como 95/5: 95 % del valor en tu propio token y el 5 % en otro token como ETH o DAI. Esto te permite dar liquidez a tu token sin necesidad de contar con muchos recursos. Y cada vez que la proporción entre tokens varía, estás perdiendo tokens propios en retorno a ETH o DAI. Simplemente magnífico para ICO, STO, e incluso proyectos que simplemente buscan dar liquidez a su propio token, lo cual es bueno; les beneficia no solo porque hace el token más atractivo, sino porque además genera un rendimiento de su capital a través de las fees que va generando continuamente.

Por ejemplo, muchos fundadores o advisors suelen recibir grandes cantidades de tokens sobre el proyecto que han desarrollado. Obviamente esto les pone en una situación donde no quieren venderlo todo y derrumbar su precio, ya que están incentivados a hacer que el precio aumente y que el futuro del proyecto sea bueno. En este caso, estas «ballenas» pueden aportar sus tokens en pools de Balancer desiguales; primero, para dar más usabilidad al token que holdean; segundo, para ir rebalanceando su portfolio hacia tokens más sólidos como ETH o DAI sin perjudicar su valoración de mercado, y por último, para generar un rendimiento a su capital en forma de fees.

## 15.5. Bullish portfolios o pools desiguales

A menudo es recomendable diversificar tu portfolio de inversión, aunque también hay casos donde se apuesta por un proyecto concreto. Estos inversores en general no tienen un incentivo para proveer liquidez en Uniswap, ya que eso

implica que tengan que depositar el 50 % del valor en otro token que quizás no tienen, además de que asumen el riesgo de perder exposición al token que holdean.

Con los pools desiguales de Balancer, ahora estos inversores pueden generar fees de su capital sin necesidad de perder exposición a su token, simplemente pueden participar en pools con distribuciones del 90/10 - 95/5.

## 15.6. Impermanent loss en Balancer

El concepto de **impermanent loss** es de vital importancia a la hora de convertirte en proveedor de liquidez, y suele ser frustrante ver cómo tu capital ha disminuido a pesar de recibir ingresos en forma de fees. Básicamente se refiere a la pérdida de valor de tus assets cuando inviertes en pools de liquidez en comparación con, simplemente, holdear dichos criptoactivos.

Para que quede claro, ya que es una pregunta que me hacen con mucha frecuencia, pondré un ejemplo para entender bien cuándo sucede y por qué, usando como ejemplo un pool en Uniswap.

Pongamos el caso de que quiero depositar en un pool de Uniswap 10 ETH y 1000 DAI y dicho depósito representa el 1 % del pool, ya que este contiene 1000 ETH y 100 000 DAI. La primera conclusión es que el precio de 1 ETH = 100 DAI ya que una de las condiciones de Uniswap es que el pool debe tener una proporción de 50/50. Ahora imaginemos que el precio del ETH ha cambiado a 120 DAI (un 20 % de revalorización); en este momento el protocolo debe hacer uso de su asset management nativo para recuperar la distribución 50/50 entre los dos tokens, manteniendo así el invariant en la misma cantidad (10 000 de valor, en este ejemplo):

- ETH = 910,2871
- DAI = 109 540,45

Como somos propietarios del 1 % del pool, significa que ahora tenemos el derecho de recuperar un total de 9,128 ETH y 1095,4 DAI. Para entender mejor si hemos salido ganando en la operación, lo más práctico es transformar todo en DAI, ya que este es un token estable y nos permitirá comparar el valor depositado inicialmente con el valor retirado. Haciendo el cambio, tenemos un valor total de 2190,09 DAI, y si nos fijamos a cuánto depositamos inicialmente, el total equivale a 2200 DAI. Es decir, **hemos dejado de ganar 9,1 DAI por haber participado en un pool de liquidez.**

Como es lógico, se debe al rebalanceo, lo que hace que **poco a poco vayas perdiendo exposición en los tokens que se van revalorizando**. La primera conclusión entonces es que, si eres largoplacista en un token, el mejor momento para usar ese asset para proveer liquidez es durante mercados bajistas, ya que cuando el precio sube pierdes exposición, pero cuando el precio baja, la ganas. Esta pérdida de valor viene representada a través del siguiente gráfico:

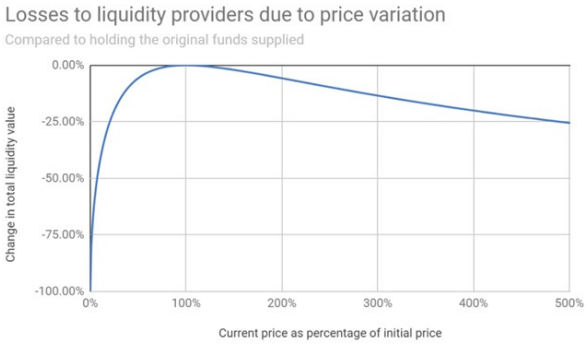
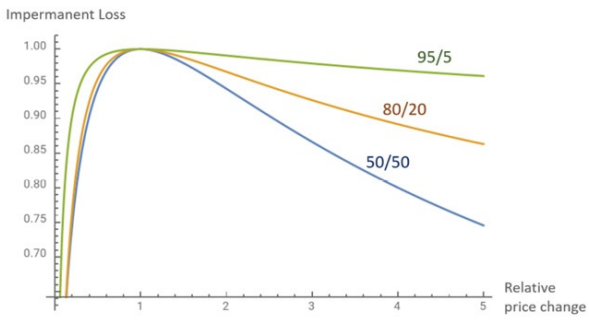



Figura 79. Modelización del impermanent loss en Balancer en función de la liquidez

- Un x 1,25 del precio da como resultado una pérdida del 0,6 % en comparación con hacer holding.
- Un x 2 del precio da como resultado una pérdida del 5,7 % en comparación con hacer holding.
- Un x 4 del precio da como resultado una pérdida del 20 % en comparación con hacer holding.
- Un x 5 del precio da como resultado una pérdida del 25,5 % en comparación con hacer holding.

Ahora veamos esto aplicado en los pools de Balancer. El concepto de impermanent loss también lo encontramos en este protocolo, aunque de una forma mucho más flexible. Para exponerlo, nos referiremos solo a pools con dos tokens, aunque también es aplicable a pools con incluso ocho tokens.

La posibilidad de crear pools desiguales hace que el impermanent loss pueda ser mayor o menor en función de las proporciones. Veamos el gráfico:




Impermanent Loss for different combinations of Balancer pool weights

Figura 80. Modelización del impermanent loss en Balancer en función de la configuración de los pools en cuanto a peso (porcentaje) de tokens

Anteriormente hemos visto que un pool 50/50, donde tenemos un incremento de x5, el impermanent loss es del 25,5 %, pero en pools 95/5, esta pérdida se reduce a 3,88 %, es 6,5 veces menor. Es decir, aquellos inversores que tengan gran confianza en un token, pueden mantener una exposición muy alta mientras van generando fees al mismo tiempo.

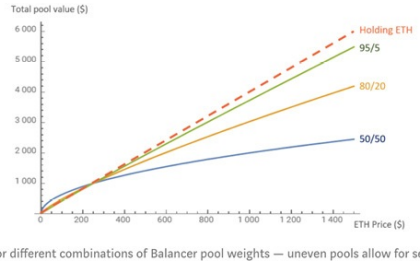



Figura 81. Efecto del impermanent loss en Balancer (en función de la configuración de los pools en cuanto a peso —porcentaje— de tokens) respecto al holding de Ethereum

Los pools de Balancer son mucho más flexibles y se adaptan mejor a las necesidades concretas de cada proveedor de liquidez. De alguna forma, este protocolo está verdaderamente descentralizando el market making.

## 15.7. Slippage en el precio y APR (anual percentage rate)

El concepto de slippage consiste en cuánto puede variar el precio del swap en función del estrés que está asumiendo el pool. Es decir, si yo quiero swapear 1 ETH por DAI y el pool es muy líquido, si 1 ETH = 100 DAI, seguramente el swap me aportará 100 DAI. Ahora bien, si queremos swapear 1000 ETH seguramente no vamos a recibir 100 000 DAI, ya que habremos puesto demasiado estrés al pool y este estará cobrando un precio de cambio más alto.

Por tanto, los pools más eficientes en cuanto a slippage son los pools 50/50. Lo podemos demostrar mediante el siguiente gráfico:

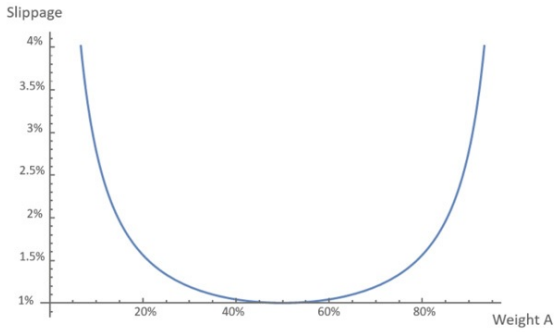


Figura 82. Efecto del slippage en función de la configuración del pool en cuanto a tokens (porcentaje)

Pools desiguales provocan un slippage mayor, dando como resultado menos volumen tradeado y por tanto un ARP o retorno anual inferior. Esto podría ser una desventaja para Balancer en comparación con Uniswap mientras los costes de gas sigan siendo tan altos. Debido a que el SOR no puede utilizar muchos pools a la vez, en ciertos swaps Uniswap podría estar ofreciendo un mejor precio.

## 15.8. Swing- trading y pool con altas fees

Otra particularidad de Balancer es la opción de manipular las fees del pool. Ahora bien, esto solo es posible en pools «privados» donde solo existe un owner (propietario) y este tiene el poder de hacer cambios en el funcionamiento del pool constantemente. Los pools «públicos» o abiertos, donde cualquier persona puede invertir, no pueden modificar este aspecto.

La premisa inicial es muy lógica: cuanto más altas sean las fees de un pool, con menos frecuencia vas a recibir solicitudes de swaps y, por tanto, menos fees o rendimiento vas a poder generar con tus activos. Por ello, estos se van a utilizar cuando haya desequilibrios en los precios de los pools (generados por variaciones en los precios de los assets subyacentes) que permitan compensar estas altas fees.

Pongamos un ejemplo: 1 ETH = 100 DAI, y este es el precio que esperas obtener al hacer un swap. Un pool con un 10 % de comisión solo se usará cuando, debido a desequilibrios de pools, este ofrezca un swap donde 1 ETH = 110 DAI. A partir de ese precio hay incentivos para posiciones de arbitraje o incluso traders para swapear en dicho pool.

Conclusión: cuanto más alto sea el fee, menos operaciones habrá y por lo tanto el rebalanceo entre los tokens será menos frecuente. Esto es asombroso: de alguna forma los pools con un 10 % en fee actúan como una estrategia de holding, ya que sus balances no se van a mover hasta que haya trades, y estos no sucederán hasta que el slippage compense la comisión. Como vemos en la siguiente imagen, si el precio de ETH no se mueve hasta llegar a puntos de compra/venta el pool no tendrá operaciones de arbitraje y por lo tanto no se va a rebalancear, actuando más como una especie de holding.

Figura 83. Efecto de una «volatilidad estable» en el rebalanceo de pools en Balancer

Mientras el precio de ETH se mantenga entre las zonas donde comprar/vender sea rentable, no entrarán operaciones de arbitraje que rebalancearán el portafolio.

En esta imagen, en cambio, el precio se ha colocado en zonas donde tanto comprar/vender han sido rentables. Es en estas zonas cuando entran los trades que permiten rebalancear el portfolio y volver a mover los precios de ETH para generar oportunidades de compra/venta.

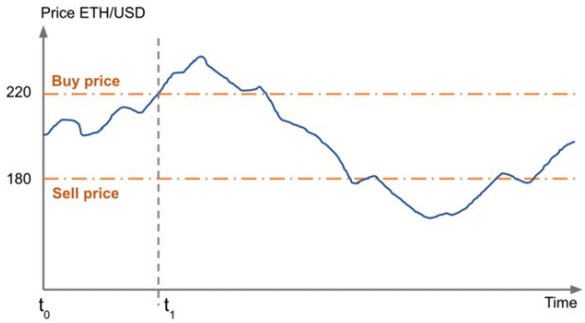


Figura 84. Efecto de una «volatilidad extrema» en el rebalanceo de pools en Balancer

Como vemos en la imagen anterior, esto cambia cuando el precio se mueve de forma considerable, ya que es a partir de ese momento cuando los trades y las operaciones de arbitraje empiezan a ser rentables. En la imagen siguiente podemos ver cómo el pool con fees del 10 % —el que más se acerca a una posición de holding— se ve menos afectado por el impermanent loss, e incluso ha sido más rentable mantener pools del 10 % en comparación con hacer puramente holding.

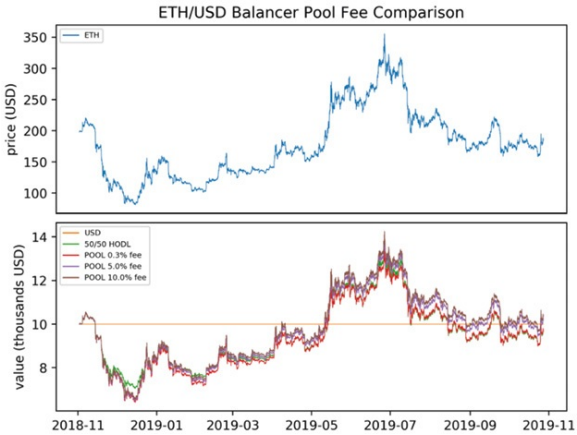


Figura 85. Efecto del precio del ETH sobre pools en Balancer con diferentes fees

**Como vemos, los pools de Balancer ofrecen muchísimas posibilidades y por lo tanto diferentes estrategias de inversión**. Escoger un pool con fees altas te permite rebalancear comprando barato y vendiendo caro, algo muy atractivo. En contra, el pool es mucho menos activo y por lo tanto genera un rendimiento mucho menor. Por otro lado, puedes escoger pools con fees muy bajas, lo que generará un volumen tradeado enorme (tanto por trades en busca de un buen precio como por oportunidades de arbitraje para compensar variaciones en el precio), aunque también generan menos ingresos por trade y verás tu portfolio más afectado por el impermanent loss.

Un pool con fees altas podría verse como un sustituto a los fondos indexados convencionales con estrategias de asset management, donde solo se rebalancea el portfolio cuando se llega a variaciones significativas del x %. Es decir, el pool permitirá al portfolio fluctuar hasta que no lleguen las operaciones de arbitraje debido a fuertes fluctuaciones en los assets.

## 15.9. Balancer: conclusiones

Después de una buena lectura, creo que podemos afirmar que Balancer no es simplemente un Uniswap 2 que solo permite hacer pools con proporciones diferentes. **Más bien es una disrupción en toda regla que descentraliza por primera vez y da la posibilidad a cualquier usuario de participar en fondos indexados de asset management sin pagar comisiones**. De hecho, es al contrario: generas rendimiento en forma de fees por hacerlo.

Sin duda, Balancer será protagonista en los próximos meses ya que sirve como sandbox para ir probando y diseñando nuevas estrategias de inversión, altamente

variadas gracias a la posibilidad de manipular muchos aspectos técnicos del pool (número de tokens, su distribución, las fees, etc).

Cada vez hay más oportunidades de convertirse en proveedor de liquidez y generar rendimientos a nuestros criptoactivos. Un límite muy importante que veía en Uniswap es la alta posibilidad de perder parte del rendimiento generado por el activo que holdeas en un bull market debido al impermanent loss. Ahora, con pools con fees altas y con proporciones desiguales (90/10 o 95/5), este escenario es completamente distinto.

# 16. Exchanges descentralizados: Curve

Curve es otro protocolo que actúa como proveedor de swaps gracias a la creación de pools de liquidez. Hemos profundizado bastante en Uniswap y Balancer, así que no repetiremos conceptos con Curve.

Este vendría a ser como una segunda versión de Uniswap que busca ofrecer swaps exclusivamente para assets tokenizados como stablecoins o tokenizaciones de Bitcoin como RenBTC, wBTC o tBTC. En caso de querer swapear este tipo de monedas, Curve es la mejor opción, ya que aplica un modelo similar a Uniswap pero con mucha más profundidad. Veámoslo en detalle.

La fórmula que permite determinar el precio de los swaps en Curve es menos sensible que en Uniswap porque está pensada para evitar al máximo el movimiento de precio cuando se estresa el pool.

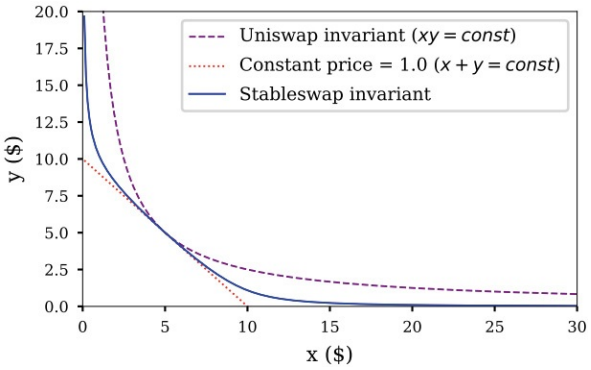



Figura 86. Algoritmo de fijación de precios de Curve

Eso permite que el protocolo de Curve pueda dar mejores cambios cuando se trata de swaps entre stablecoins. De hecho, Curve solo funciona con stables y tokenizaciones de Bitcoin porque este tipo de curvas solo tienen sentido cuando los activos que se intercambian tienen el mismo valor.

En Curve por ejemplo, como los pares de tokens de los pools tienen el mismo valor, no hay posibilidad de sufrir impermanent loss, cosa que hace estos pools muy atractivos como vehículos de inversión.

## 16.1. Integraciones de Curve

Otro aspecto interesante de Curve es que se integra con otros protocolos para ofrecer más rendimiento a sus proveedores de liquidez.

Por un lado, les ofrece las comisiones de cada swap (que son del 0,04 %), y, por otro lado, les da los intereses generados en otros sistemas como Compound (ya que cuando los activos no se están usando, Curve los deposita en otros protocolos para sacarles un interés). De hecho, existen unos pools en Curve que integran el protocolo Yearn, y este permite que los fondos no solo se depositen en Compound sino que se transfieran en el protocolo más rentable en cada momento. En caso de que Compound deje de ser el más rentable, el smart contract del pool deposita los fondos en el nuevo protocolo más beneficioso para así maximizar los rendimientos.

Por otro lado, Curve también se integra con otros protocolos, ya que en algunos pools de Curve no solo obtienes rendimientos por las fees de los swaps sino que te recompensan con tokens como el SNX tokens, el REN token o el CRV token (token de gobernanza de Curve). Esto es un poco complejo, así que lo volveremos a repasar más adelante.

# 17. Mercados de dinero: Compound

Compound es un protocolo que a través de un tipo de interés generado de forma algorítmica y dinámica en función de la oferta y demanda permite crear un mercado de dinero. Pensemos por un momento la disrupción tecnológica y financiera de este modelo: mientras que en los mercados tradicionales los tipos de interés los fijan los bancos centrales, estos varían con una frecuencia muy baja, cada año. En Compound, los tipos de interés se recalculan en cada bloque de Ethereum (cada quince segundos), 24x7x365. Ahora entendamos el porqué y el cómo.

Compound se empezó a escuchar durante 2017, año en que tuvieron su primera ronda de inversión de 8 000 000 USD de forma cerrada, seguida por otra, que llegó más adelante, de 25 000 000 USD.

El proyecto lo fundó Robert Leshner. El apoyo de las inversiones privadas no es de extrañar, ya que Leshner cuenta con un gran recorrido en el mundo financiero y una visión a tres años vista de lo que DeFi puede aportar al mundo.

**La idea del protocolo es generar mercados de dinero donde cualquier persona pueda pedir prestado capital (dando un colateral como garantía) a un tipo de interés calculado de forma algorítmica según la oferta y demanda que se actualizada cada 15 segundos (cada bloque de Ethereum).**

Esto es realmente interesante, sobre todo si lo comparamos con lo que estamos acostumbrados a ver, no solo en el mundo tradicional, sino incluso en otros protocolos lending en cripto.

## 17.1. Los préstamos en el sistema tradicional

En los mercados de dinero del mundo tradicional estamos acostumbrados a que **el coste del dinero lo fijen los bancos centrales**. Estos tipos de interés no suelen ser nada elásticos ni proporcionales a la oferta y demanda del mercado. De alguna manera usan estos tipos para «dirigir», de forma centralizada, el desarrollo económico. Sinceramente, creo que algún día esta idea será tan absurda como que en la Unión Soviética se intentara controlar de forma centralizada la cantidad de patatas a producir. Un movimiento libre de precios entre oferta y demanda, en mi opinión, aportará siempre un mejor equilibrio en la economía. Solo hace falta ver dónde están los tipos de interés ahora mismo: la mayoría muy cerca al 0 %.

| Central Bank | Current Rate | Next Meeting | Last Change |
|---|---|---|---|
| Federal Reserve (FED) | 0.00%-0.25% | Apr 29, 2020 | Mar 15, 2020 (-100bp) |
| European Central Bank (ECB) | 0.00% | Apr 30, 2020 | Mar 10, 2016 (-5bp) |
| Bank of England (BOE) | 0.10% | May 07, 2020 | Mar 19, 2020 (-15bp) |
| Swiss National Bank (SNB) | -0.75% | Jun 18, 2020 | Jan 15, 2015 (-50bp) |
| Reserve Bank of Australia (RBA) | 0.25% | May 05, 2020 | Mar 19, 2020 (-25bp) |
| Bank of Canada (BOC) | 0.25% | Jun 03, 2020 | Mar 27, 2020 (-50bp) |
| Reserve Bank of New Zealand (RBNZ) | 0.25% | May 13, 2020 | Mar 15, 2020 (-75bp) |
| Bank of Japan (BOJ) | -0.10% | Jun 16, 2020 | Jan 29, 2016 (-20bp) |
| Central Bank of the Russian Federation (CBR) | 5.50% | Apr 24, 2020 | Apr 24, 2020 (-50bp) |
| Reserve Bank of India (RBI) | 4.40% | May 03, 2020 | Mar 27, 2020 (-75bp) |
| People's Bank of China (PBOC) | 4.35% | | Oct 23, 2015 (-25bp) |

Figura 87. Tipos de interés actuales de los bancos centrales

De hecho, es gracias a estos mecanismos que en algunos momentos hemos tenido «barra libre de dinero», etapas de máxima inflación que lo único que aportan es la dilución de la eficacia del dinero, desestabilizando la economía. A raíz de esto aparecen las empresas zombie o QE *(quantitative easing);* que no son competitivas pero se mantienen a flote gracias al acceso barato a financiación, rompiendo una ley sagrada del mercado: penalizar a las empresas ineficientes y premiar a las eficientes.

En cuanto a los créditos bancarios, podemos ver tipos de interés fijos, variables y correlacionados con algunos índices, que van cambiando de forma gradual en el tiempo. En el caso de los préstamos personales, también hay diferencias, ya que en función del uso que quieras hacer del dinero puedes pagar más o menos interés.

En definitiva, el acceso al dinero está centralizado, es lento, depende de intermediarios que generan ficción al proceso y que tienen el poder de manipular las condiciones contractuales.

## 17.2. Plataformas de lending en Blockchain

Por otro lado, tenemos las plataformas de lending del mundo cripto. Estas disponen de un sistema que pone en contacto a los borrowers con activos específicos, reduciendo la liquidez y la disponibilidad inmediata del dinero, ya que este no estará disponible hasta que se hayan establecido los términos como el tiempo o el tipo de interés.

Por ejemplo, yo dispongo de 1 BTC y lo quiero dejar prestado para obtener un rendimiento de mi activo sin desprenderme de él. El sistema conectará mi BTC con un borrower que quiera pedirlo prestado: esto significa que debemos llegar a un acuerdo en cuanto a condiciones, haciendo que el proceso sea lento y lleno de fricciones. Además, como lender tengo que renunciar a la disponibilidad de mis activos hasta el vencimiento del contrato, provocando tipos más altos para el borrower. La lógica financiera nos dice que cuanto más tiempo ponga a

disposición mi dinero, más rentabilidad voy a obtener, o lo que es lo mismo, más caro va ser el tomar prestado ese dinero.

## 17.3. Compound Money Market

La propuesta de Compound, en cambio, es diferente, innovadora y disruptiva. Genera un mercado de dinero donde gente con exceso puede prestar su excedente a gente con usos productivos e inversiones rentables para ese dinero, pagando un interés a cambio. La diferencia es que en este protocolo no existen intermediarios, sino que los usuarios pueden prestar sus activos añadiéndolos a un pool compartido y descentralizado, permitiendo que todos los lenders y borrowers puedan depositar y retirar sus activos cuando lo deseen. Es decir, en Compound, un borrower no toma prestado un activo concreto y llega a un acuerdo con el lender, sino que solicita un préstamo de un pool compartido entre todos los lenders. Esto permite que estos últimos puedan retirar sus activos cuando lo deseen, y que el proceso de pedir un préstamo sea mucho más rápido ya que no hay que fijar términos y condiciones. No hay fricciones.

El tipo de interés se fija y se actualiza cada quince segundos en función de la oferta y demanda que haya en un activo concreto. Esto permite crear un sistema de incentivos automático; es decir, si existe mucha demanda para pedir prestado un activo pero hay poca oferta, la tasa de interés subirá, incentivando a los lenders a depositar activos para generar un rendimiento. En cambio, si existe mucha oferta pero poca demanda, la tasa de interés será más baja, incentivando la creación de crédito. Podríamos decir que es un mercado de dinero propio de la economía austríaca, que va cambiando en función del mercado, no de intereses centralizados.

Algo asombroso también es que podríamos estar hablando de los préstamos más baratos de todo el ecosistema. Si el lender no está obligado a retener sus activos durante X tiempo, sino que puede depositar y retirar cuando lo desee, provoca que el coste de pedir prestado sea mucho más bajo ya que en ningún momento priva de la disponibilidad de capital a sus tenedores. Por otro lado, hay que tener en cuenta que los tipos se actualizan en cada bloque de Ethereum, y a pesar de que probablemente variarán de forma suave (ya que dependen de la liquidez del protocolo) tenemos que esperar cambios graduales en el coste del dinero. La contrapartida es que en caso de que se haya tomado prestado en exceso, el protocolo no te permite retirar tu capital, aunque, como recompensa,

seguramente estarás obteniendo rentabilidades del 20 % anual, ya que la ratio oferta y demanda es tan alto que el tipo de interés se dispararía.

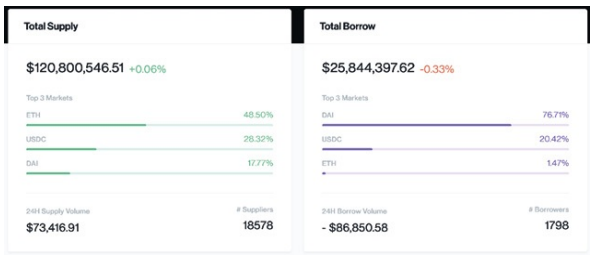



Figura 88. Métricas generales en compound.finance (mayo 2020)

Algo interesante de la imagen es cómo lo más común es colateralizar ETH y pedir prestado stablecoins. Esto es lógico, ya que no quieres pedir un préstamo en un activo volátil, ya que estarías asumiendo un riesgo muy alto en comparación a la adquisición de una moneda estable.

## 17.4. Compound: los lenders (prestamistas)

Contrario a otros tipos de plataformas P2P, cuando un usuario suministra activos para poner a disposición de los prestatarios, estos los añaden a un pool común, haciendo el activo más líquido que con lending directo.

En el momento de suministrar los activos, Compound generará un token (cToken) que representa el balance del token depositado más el interés acumulado en cada bloque, obtenido a través del aumento del valor de los cTokens. Así pues, acumular interés es tan fácil como holdear cTokens, que la vez son transferibles, tradeables y programables. Para recuperar tus activos más el interés adquirido es tan fácil como redimir los cTokens en Compound. Actualmente hay a disposición cZRX, zREP, cBAT, cUSDC, cwBTC, cSAI, cDAI y cETH.

La forma en que se obtiene rentabilidad a través de los cTokens es a través de los intereses pagados por los préstamos generados, que se acumulan y permiten que los cTokens vayan aumentando de valor. Los cETH, por ejemplo, tienen un valor de salida de 0,020 ETH, una proporción que va aumentando a medida que van acumulando intereses. Si por ejemplo dejas prestado 1 ETH (190 USD) recibirás 50 cETH a cambio debido a que valen 0,020 ETH (esto fue en el momento del lanzamiento, ahora equivalen a 0,020062 ETH ya que han aumentado de valor por la acumulación de intereses). **Los intereses no los ganas porque aumenta el número de tokens sino porque aumenta el valor del token**.

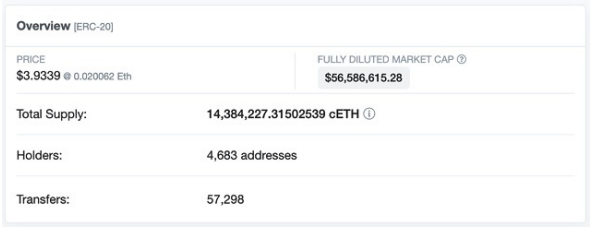


Figura 89. cETH en Etherscan: Compound Ethereum Token (mayo 2020)

Los casos de uso más evidentes son los inversores long term de Ethereum, que pueden usar Compound como otra fuente de ingresos sin perder su ETH. Por otro lado, esto también está a disposición de dapps, máquinas, exchanges o incluso protocolos que, gracias a la flexibilidad de Compound (que permite depositar y retirar tus activos en todo momento), pueden aumentar sus ingresos en caso de tener activos parados, aunque sea durante un corto periodo de tiempo (recordemos que obtienes rendimiento del protocolo por cada bloque de Ethereum, aproximadamente cada quince segundos). Este hecho, sin duda, permite la creación de nuevos modelos de negocio para el ecosistema Ethereum. Incluso puede llegar al día en que los activos disponibles de empresas se depositen en protocolos de mercados de dinero de Compound o similares aprovechando periodos en que ese capital disponible estaría «parado».

Por último, estamos viendo una tendencia creciente en adoptar cDAI como moneda estable. Resulta algo curioso, ya que estamos hablando de un DAI que, además, va acumulando interés. Esta capacidad de generar DAIs con intereses va a generar competencia entre monedas estables, ya que al final la gente quiere usar la forma de dinero más rentable. Para mí, un caso de uso de lo más interesante.

Existen incluso otras formas de DAI como el rDAI, un token que separa el rendimiento de Compound a otra cuenta, pudiendo reinvertirlo para generar interés compuesto en el protocolo. Además, ofrece nuevos casos de uso como, por ejemplo, que las empresas acepten solo rDAI, permitiendo que el tiempo que ellos tienen el control de ese dinero, le saquen un rendimiento enviado a otra cuenta. Imagina intermediarios que tienen control momentáneo de dinero y mueven cantidades enormes de capital, pero no consiguen sacarle provecho. Desde luego, disruptivo.

## 17.5. Compound: los borrowers (prestatarios)

En cuanto a los borrowers, estos deben depositar un colateral para poder pedir prestado. Este colateral de hecho se consigue bloqueando los fondos que han

añadido en el pool compartido de Compound, privándote de la posibilidad de retirarlos hasta que devuelvas el capital que has tomado prestado. Es decir, colateralizas tus cTokens, así que ya no puedes transferirlos o redimirlos por tus activos prestados. Eso sí, ¡sigues obteniendo rentabilidad por ellos!

Como comentábamos, este proceso no tiene fricciones, solo tienes que especificar el activo que quieres tomar prestado y ya estará hecho, no hay que negociar términos ni condiciones; el borrowing es instantáneo.

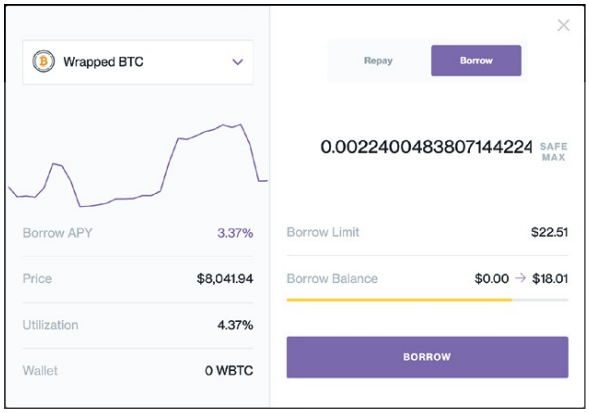



Figura 90. Ventana para tomar prestado wBTC - 22,51 USD = 75 % del colateral (mayo 2020)

Puedes tomar prestado hasta un 74,99 % de tu capital, ya que cuando llega al 75 %, tu posición se liquida para que el protocolo pueda recuperar el capital prestado. Este es un tema muy curioso del protocolo de Compound.

En el caso de Maker, las liquidaciones son automáticas, ya que se vende el ETH colateralizado con un descuento del 3 % en el mercado para recuperar los préstamos en DAI. En el caso de Compound, se ofrece una tool para los liquidadores, que son usuarios dispuestos a devolver el préstamo a cambio de recibir el colateral con un incentivo del 5 % (sin contar fees de las transacciones). Estas acciones suelen ser muy rápidas y es difícil acceder a liquidaciones muy rentables porque suelen desaparecer rápidamente.

Así que podemos identificar otro participante en el protocolo: **los liquidadores**. Estos tienen la posibilidad de liquidar una vez la función health: {“value” : “1.0” } es menor que 1. Para entender cómo se liquida, hace falta una versión práctica del proceso, ya que está más enfocado a profesionales que buscan rentabilidades. Analizamos las liquidaciones en profundidad tanto en el Máster Blockchain como en el Bootcamp DeFi que impartimos en Tutellus.

Figura 91. Cuentas *unsafe* susceptibles a ser liquidadas

En cuanto a los casos de uso, los motivos para tomar préstamos en Compound son bastante lógicos: tomar prestado al momento sin depender de entradas de capital off chain y así disponer de liquidez inmediatamente, o para realizar inversiones sin desprenderte de tu ETH. Aunque el caso más interesante está en darle un uso especulativo y poder realizar *shorts* en el precio.

Imaginemos que Bob es un gran creyente de ETH y ya tiene algunas inversiones en ese activo. Ahora, Bob estima que el token BAT va a caer comparado con el ETH, así que colateraliza ETH (200 USD) y pide prestado BAT (100 USD) que venderá al mercado inmediatamente por ETH. Cuando el precio del BAT cae un 50 % respecto al ETH, Bob vuelve a adquirir BAT con el ETH que adquirió antes de la caída (esta vez mantiene un 50 % en ETH, ya que en precio del BAT ha caído) para recuperar su colateral con ese BAT. Utilizando un mercado de dinero, Bob ha sido capaz apalancarse en su predicción económica y así acabar con 250 USD en ETH.

## 17.6. Compound: los oráculos

Para realizar estos procesos —como siempre— debemos usar oráculos que determinen los precios de los activos y garanticen así el correcto funcionamiento del protocolo. En el caso de Compound, los datos llegan de exchanges con grandes volúmenes como Coinbase Pro, Bittrex, Poloniex y Binance. Algo que sí es realmente interesante es la variación máxima de precio que acepta el protocolo; un máximo de variación del 10 % por hora. Esta medida de seguridad es realmente buena en caso de desplomes en el mercado, ya que da un pequeño margen de tiempo a los borrowers de asegurar sus préstamos y evitar liquidaciones.

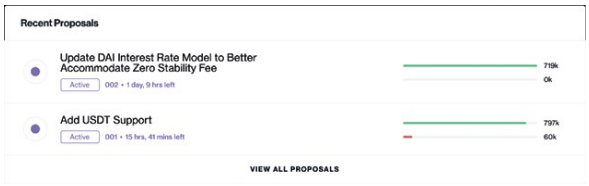
## 17.7. Compound: el sistema de gobernanza

A mediados del 2020, Compound hizo público su plan para descentralizar la gobernanza, que hasta entonces había estado en manos del equipo de Compound.

Se creó el token COMP que sirve para participar en la gobernanza del protocolo y que se ha repartido entre todos los participantes. Gran parte de los tokens han ido en manos del equipo fundador, los advisors y los venture capitals que financiaron el proyecto inicialmente. Otra parte se ha repartido entre la comunidad y otra se ha puesto como mecanismo de incentivo a la plataforma. Esto lo veremos en el próximo capítulo, con el liquidity mining, pero

básicamente es que se reparten tokens COMP a todos aquellos que usen el protocolo. Por tanto, lenders y borrowers se benefician del protocolo en sí por los intereses que genera y las posibilidades que otorga, y además reciben COMP cada quince segundos. Esto es un mecanismo que permite incentivar aún más el uso de la plataforma y, por tanto, la entrada de liquidez.

Todos aquellos que dispongan de estos tokens tendrán una ventana en Compound.finance para poder hacer votaciones y proposals para el protocolo. La siguiente imagen es una captura de la primera propuesta: para añadir USDT como activo disponible en Compound, donde la comunidad acabó votando a favor.




Propuestas activas para ser votadas

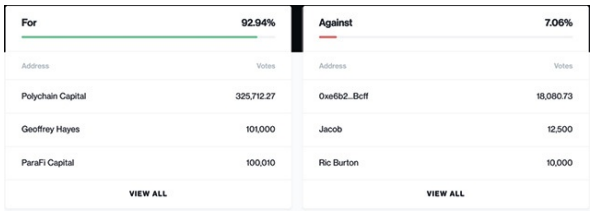



Figura 92. Votaciones para añadir USDT en Compound (mayo 2020)

Un reto que veo en el token COMP y cualquier otro token de gobernanza es la necesidad de hacer que sea atractivo para sus holders. Un token poco atractivo podría provocar escaso interés en la gobernanza, y sus holders podrían también vender ese poder por valores muy reducidos.

**Considero que los tokens de gobernanza deben disponer de unos tokenomics que incluyan un mecanismo de revalorización futura del token;** en parte para aumentar el coste de un ataque a la gobernanza, y en parte para incentivar su holdeo y evitar centralizar el token en pocas cuentas. Recordemos que lo más valioso de un protocolo es su gobernanza. Por ejemplo, si en Compound hay 1000 MUSD colateralizados, y su ataque de gobernanza es de 100 MUSD, tendríamos un problema.

A pesar de los retos que deben afrontar este tipo de tokens, el COMP está diseñado de una forma muy correcta y atractiva. Es suficientemente sólido como para evitar riesgos de ese tipo (aunque nada es seguro al 100 %), sin contar el hecho de que grandes corporaciones tienen mucho interés en tener poder de voto para así impulsar cambios hacia su propio interés. Uno de los inconvenientes

más grandes de Compound es la gran participación de inversores privados, que han hecho que gran parte de los tokens se entreguen a corporaciones y VC, y no a la comunidad. Esto lo hace menos descentralizado, aunque es demasiado pronto para afirmar que dicha semicentralización sea algo bueno o malo. Quizá no lo sea a nivel filosófico, pero contar con equipos profesionales —que además tampoco podrán conseguir el control total del protocolo— podría ser algo bueno a largo plazo.

Otra reflexión que quiero compartir es la creciente tendencia de los protocolos a descentralizarse y a dejar sin poder, e incluso eliminar, las fundaciones que suelen acumular gran poder de decisión. En un principio puede parecer que es debido a la gran consciencia del ecosistema de la importancia de descentralizar, pero desde la demanda a Maker debido a las liquidaciones provocadas por el Jueves Negro —donde muchos perdieron sus colaterales debido a una fuerte caída del precio del ETH, como ya vimos en el capítulo de Maker— más y más protocolos optan por descentralizarse para evitar conflictos legales y de responsabilidad subsidiaria. **Podría ocurrir que las grandes fundaciones cripto con fuerte poder de decisión se conviertan en algo del pasado**. Solo el tiempo lo dirá.

Veremos más en profundidad este token y sus tokenomics en el capítulo de liquidity mining.

## 17.8. Compound: funcionamiento del protocolo

Vamos a entender primero los conceptos que rigen el funcionamiento del mismo:

- **Equilibrio de los fondos.** Como hemos visto, Compound dispone de un pool de liquidez compartido donde se pueden realizar préstamos colateralizados. En un lado tenemos los fondos depositados por los prestamistas, y al otro los fondos prestados, que nunca serán equivalentes ya que un mínimo del 10 % de los fondos disponibles se mantienen como reservas líquidas para poder garantizar liquidez al pool; es decir, permitir depósitos y retiros de los fondos en cualquier momento.

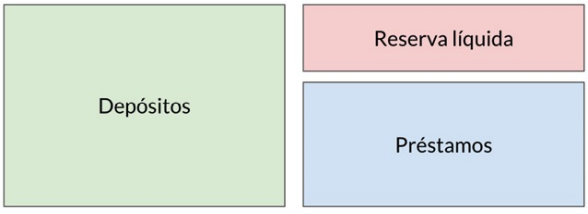



Figura 93. Estructuración general de depósitos y préstamos en Compound

- **Ratio de utilización.** El precio del dinero (tipo de interés) se determina en función de la oferta y demanda, entrando así en el sistema de incentivos de liquidez automático que comentábamos antes. Si hay mucha demanda y poca disponibilidad para prestar, el tipo de interés aumenta y por tanto también lo hace el rendimiento de los prestamistas, incentivando la entrada en estos al pool compartido. En caso contrario, si hay mucha liquidez y poca demanda, el precio del dinero es muy bajo y hay un incentivo para pedir prestado. Este cálculo se consigue primero calculando el ratio de utilización, es decir, qué parte de los fondos disponibles se ha tomado prestada.

Ratio de utilización = reserva líquida/depósitos

Una vez que tenemos la ratio de utilización, podemos calcular el tipo de interés al cual se va a pagar el préstamo de un activo:

Interés = 2,50 % + ratio * 20 %

Esta es la fórmula del protocolo de Compound, con la cual podemos entender que el coste del capital rondará entre el 2,5 % al 20 %, en función de la relación entre la oferta y la demanda.

- **Interés del lending.** A la hora de calcular el interés generado por el protocolo para los prestamistas, este se calcula repartiendo el total adquirido en intereses en préstamos entre todos los prestamistas. Para conocer el interés que obtendrías a día de hoy, puedes consultar aquí.


Figura 94. Situación del pool de Ethereum en Compound un día cualquiera

En este caso tenemos que el capital prestado es de 386 000 USD con un interés del 2,09 % (borrow APY). Este tipo de interés generará un beneficio de 8 067,40 USD (gross borrow) que se reparte entre el capital disponible para prestar 55,88 MUSD (gross supply), lo que equivale a un interés del 0,01 % (supply APY).

El aumento del 0,02 % del gross supply y la reducción del 1,48 % del gross borrow hacen referencia al crecimiento o decrecimiento del total puesto para prestar y del total prestado.

Llegados a este punto, solo me queda comentar que las fórmulas ofrecidas son ejemplos de cómo funcionan los cálculos, **pero estos son bastante más complejos.** Es por eso que, si llevamos a la práctica estos cálculos, nos encontraremos con que no se consigue nunca un valor exacto del tipo de interés.

Para esto deberíamos seguir los cálculos reales, disponibles **aquí**. Pongamos un ejemplo:

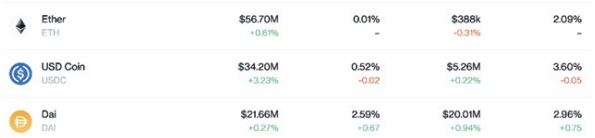



Figura 95. Situación de pools varios en Compound para análisis de costes y rentabilidades

- Tipo interés ETH = (2,5 % + ratio de utilización * 20 %) —> 2,636 %
  Valor en Compound = 2,09 %
- Tipo interés USDC = (2,5 % ratio de utilización * 20 %) —> 5,576 %
  Valor en Compound = 3,60 %
- Tipo interés DAI = (2,5 % + ratio de utilización * 20 %) —> 19,976 %
  Valor en Compound = 2,96 %

El caso más crítico lo tenemos con DAI, ya que funciona particularmente diferente. Los DAI que aún no han sido prestados se envían al DSR de Maker, influyendo en el tipo de interés que deben pagar los que piden prestado. Además, el tipo también está influenciado por el stability fee de Maker.

## 17.9. Compound: conclusiones

Sin lugar a dudas estamos delante de un protocolo con un potencial enorme. No solo porque permite la creación de un mercado de dinero en el ecosistema DeFi de Ethereum, sino porque replantea cómo funciona el hecho de prestar y pedir prestado. Recalcular el tipo de interés cada quince segundos y disponer de un pool descentralizado y compartido (y no un sistema que conecta activos concretos entre prestamistas y prestatarios) abre un nuevo mundo de posibilidades.

En primer lugar, consigue ofrecer los préstamos más baratos del ecosistema, ya que el lender siempre podrá disponer de su capital cuando quiera, puede sacar rendimiento por sus activos aunque sean solo durante un bloque. Esto no había pasado nunca. En segundo lugar, no hay ningún tipo de fricción e intermediario, es completamente descentralizado, incluso puedes prestar y pedir prestado sin necesidad de identificarte; solo necesitas una cuenta en MetaMask.

Por último, un tema interesante es la aparición de los cTokens, ya que ahora estamos viendo cómo la comunidad prefiere utilizar cDAI y no DAI, que al final son lo mismo, solo que los cDAI mantienen un interés integrado. Esto saca a la luz posibles rivalidades entre monedas estables, ya que al final cada uno buscará

hacer uso de la moneda más rentable. Compound marcó un hito en la industria DeFi y nos hizo entender que un nuevo concepto de mercados de dinero y tipos de interés era posible.

# 18. Mercados de dinero: Aave

El protocolo de Aave (muy similar a Compound) representa el nacimiento de las plataformas de lending del mundo cripto. En 2017, con un proyecto conocido como ETHLend, el equipo actual de Aave trabajaba en el primer protocolo descentralizado para lending P2P. El protocolo básicamente permitía que los prestamistas creasen un smart contract donde incluían las condiciones del préstamo, para que luego un depositante valorase la oferta y decidiese aceptar el contrato de lending y prestarle lo que solicitaba. El prestatario debía depositar una garantía, y según Stani Kulechov, fundador de ETHLend y Aave, fue difícil de hacer entender; poner más dinero en garantía del que pedías prestado era confuso; ¿porque deberías hacerlo si ya tienes el dinero que buscas?

La clave está en entender el valor futuro que una persona otorga a cierto asset: pedir prestado te posibilita no perder tu posición, lo que te permitirá beneficiarte de revalorizaciones del asset en un futuro.

A pesar de avanzar correctamente y haber ejecutado con éxito la ICO del token LEND en 2017, donde recaudaron más de 600 000 USD a cambio de 1 000 000 000 de tokens de los 1,3 billones existentes, las fricciones del lending P2P y la aparición de protocolos como Compound provocaron que en septiembre de 2018 ETHLend volviera con el nombre de Aave, con mucho más que aportar al ecosistema del lending descentralizado.

## 18.1. Aave: funcionamiento del protocolo

Aave nace como un protocolo de lending descentralizado a través de liquidity pools compartidos, que calculan los tipos de interés para pedir prestado a través de la oferta y demanda, exactamente igual que Compound. No obstante el equipo, ambicioso, quiso ir un poco más allá. **Definen Aave como un protocolo de mercados financieros**, siendo el lending descentralizado el primero de sus mercados. Ya disponen de dos mercados, aunque esto lo veremos más adelante.

Como hemos dicho, la parte principal de Aave en estos momentos se centra en su función para ofrecer servicios de lending. Similar a Compound, hay unos depositantes que ponen a disposición sus assets para ofrecerlos a terceros a cambio de un interés. Este interés se calcula según la oferta y demanda, es decir, según la ratio de utilización del pool. Si hay 10 000 000 disponibles y 9 000 000

millones se han pedido prestados, el tipo de interés a pagar seguramente será alto, debido a la alta ratio de utilización del pool.

Los prestamistas deberán bloquear una garantía superior al valor que están pidiendo prestado. En caso de que el prestamista no devuelva su préstamo, o si su colateral pierde más valor de lo permitido para poder considerar que su préstamo no supone riesgo, este se liquidará para evitar pérdidas en el protocolo.

Hasta aquí, nada ha cambiado respecto a Compound. Pero el equipo de Aave sabía que no podía entrar a competir con uno de los protocolos con más relevancia del ecosistema sin ofrecer nuevos servicios y propuestas de valor diferenciadas, y no se quedó corto.

## 18.2. Primer mercado de Aave: lending

### 1. Los Aave tokens (aTokens)

Una vez depositas assets en el protocolo de Aave, recibes a cambio una representación de cantidad aportada a través de los aTokens. Estos, a diferencia de Compound, no muestran los intereses generados por tu activo depositado a través de la revalorización del token, **sino por el aumento de número de tokens de los que dispones**. Es decir, los aToken tienen un peg 1:1 con los depósitos aportados; si yo ingreso 100 DAI en el pool para lending de DAI, recibo 100 aDAI a cambio. Los DAI van aumentando cada quince segundos (cada bloque de Ethereum) debido a los intereses generados, así que el número de aTokens de los que dispones también suben.

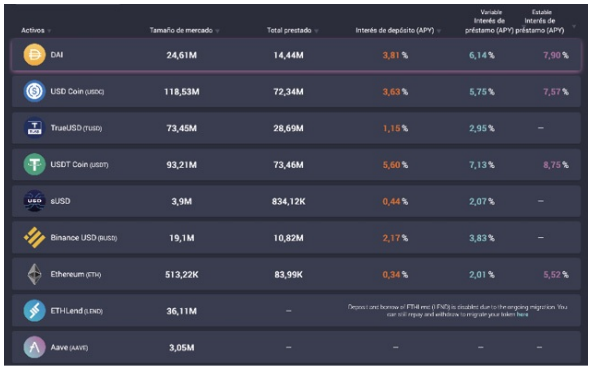
La innovación en este punto es considerable. Primero, porque la facilidad de uso es mucho mayor, ya que es fácil conocer la cantidad que están representando los aDAI gracias a su peg 1:1. Segundo, porque el aumento del número de tokens significa que recibes nuevos assets cada quince segundos, algo poco viable debido al coste del gas. Esto no es realmente así, ya que el propio smart contract del token tiene integrada la función de consultar el interés generado y actualizar las cuentas de los aToken. El cambio prácticamente no tiene coste, ya que está integrado en el propio smart contract y no transaccionalmente en la blockchain.

Algo curioso también es la imposibilidad de transferir el 100 % de los aTokens en una sola transacción, ya que durante el tiempo de confirmación se siguen generando intereses, así que siempre tendrás (aunque sea algo mínimo) una

cantidad de aTokens pendientes de retirar. Aquí tienes la opción de realizar dos transferencias o redimir los tokens en Aave.

## 2. Número de assets disponibles

Algo particular y a remarcar de Aave es que dispone de veintidós assets con los que prestar y pedir prestado.



| Activos | Tamaño de mercado | Total prestado | Interés de depósito (APY) | Variable Interés de préstamo (APY) | Estable Interés de préstamo (APY) |
|---|---|---|---|---|---|
| DAI | 24,61M | 14,44M | 3,81 % | 6,14 % | 7,90 % |
| USD Coin (USDC) | 118,53M | 72,34M | 3,63 % | 5,75 % | 7,57 % |
| TrueUSD (TUSD) | 73,45M | 28,69M | 1,15 % | 2,95 % | – |
| USDT Coin (USDT) | 93,21M | 73,46M | 5,60 % | 7,13 % | 8,75 % |
| sUSD | 3,9M | 834,12K | 0,44 % | 2,07 % | – |
| Binance USD (BUSD) | 19,1M | 10,82M | 2,17 % | 3,83 % | – |
| Ethereum (ETH) | 513,22K | 83,99K | 0,34 % | 2,01 % | 5,52 % |
| ETH Lend (LEND) | 36,11M | – | Deposit and borrow of ETH and LEND is disabled due to the ongoing migration. You can still repay and withdraw to migrate your token here | | |
| Aave (AAVE) | 3,05M | – | – | – | – |

Figura 96. Principales tokens en el mercado de Aave

Esto es posible porque cada asset, antes de estar disponible, sigue un proceso de valoración de riesgo donde se determina si es apto para ser prestado y el porcentaje que se puede tomar prestado por cada 100 tokens puestos como garantía. Es decir, se le otorgan ciertas funcionalidades en función de su valoración de riesgo. Vamos a verlo.

| | Smart contract Risk | Counterparty Risk | | | Market Risk | | | |
|---|---|---|---|---|---|---|---|---|
| | | Centralization | Trust | Diversified average | Market Cap | Liquidity | Volatility | Diversified average |
| BUSD | C+ | D+ | A | B- | B+ | B- | A | B+ |
| DAI | B- | B- | C- | C+ | B+ | B- | A | B+ |
| SUSD | C | D+ | C- | C- | C+ | C- | B+ | B- |
| TUSD | B | C- | B- | C+ | B | C+ | A+ | B+ |
| USDC | B+ | C | A | B | B+ | B- | A+ | A- |
| USDT | A- | C | D+ | C- | A+ | A+ | A+ | A+ |
| AAVE | D+ | C- | B+ | B- | B | C+ | C | B- |
| BAT | B+ | B+ | B+ | B+ | B | B- | B- | B |
| ENJ | B+ | B | B+ | B+ | B- | C | B | B- |
| ETH | A+ | B | A+ | A+ | A+ | A- | B | A- |
| KNC | B+ | B | B+ | B+ | B- | C+ | B- | B- |
| LEND | B | B+ | B+ | B+ | C+ | C+ | C- | C+ |
| LINK | B+ | B+ | B+ | B+ | B+ | B+ | C | B |
| MANA | B | C | C | C | C+ | C+ | C+ | C+ |
| MKR | B | C | C- | C | B+ | C+ | B- | B |
| REN | B | C+ | B+ | B | B | C+ | C- | C+ |
| REP | B | C+ | B+ | B | C+ | C | B- | C+ |
| SNX | C+ | C- | C | C | B | C+ | C | B- |
| UNI | B- | B | B+ | B+ | B+ | B- | D- | C+ |
| WBTC | B | D+ | B- | C | B+ | C+ | B+ | B |
| YFI | B- | C+ | B+ | B | B | B- | D- | C+ |
| ZRX | B+ | B+ | B+ | B+ | B | C+ | C+ | B- |
| Risk scale from **lowest** to **highest** : | | | | A+ | D- | | | |

Figura 97. Resultados del análisis de riesgo de los tokens en Aave

Cada asset es calificado y, en función de dicha calificación, dispone de ciertos parámetros a la hora de servir como colateral, así como de las penalizaciones que

recibe en caso de ser liquidado, generando, como siempre, un sistema de incentivos para reducir el riesgo en la plataforma.

Un ejemplo es USDT, que a pesar de poderse depositar, generar intereses y pedirse prestado, no se puede usar como colateral, ya que Aave considera que su centralización es demasiado elevada y, por tanto, es demasiado arriesgado usarlo como colateral para pedir préstamos.

### 3. Liquidaciones

Estos parámetros de riesgo sirven también para determinar el estado de salud de un préstamo. Igual que en Compound, una vez el health factor es inferior a 1, el préstamo es susceptible a ser saldado por los liquidadores, que reciben un interés por su acción. En función del riesgo del asset, la penalización por ser liquidado puede aumentar, rondando valores de entre el 5 % y el 15 %.

Algo interesante de Aave es la integración, en la propia plataforma, de un servicio de liquidación para dar más equilibrio al protocolo. Gracias a esta integración, cualquiera puede liquidar préstamos y recibir «dinero gratis» por ello; aunque también es cierto que estas oportunidades no suelen estar disponibles para el usuario normal porque los bots se encargan de liquidar cualquier préstamo rentable en el momento que aparece. Hay gente que se dedica profesionalmente a esto. Ahora bien, en casos como el Jueves Negro, donde tuvimos enormes cantidades de préstamos liquidados debido a la bajada de más del 60 % del valor del ETH, había tantos préstamos a liquidar que los liquidadores no podían con todos, así que cualquier persona pudo aprovechar para obtener rentabilidad. Esto es algo genial ya que aumenta el equilibrio y seguridad del protocolo.

Figura 98. Configuración de una liquidación en Aave

Los flash loans (préstamos flash que veremos más adelante) no están disponibles para ser usados dentro del mismo protocolo; esto para evitar riesgos y posibles ataques. Así que, a pesar de que se suelen usar para operaciones de este tipo, no pueden utilizarse para liquidar préstamos dentro de Aave. Para esto, se podrían utilizar flash loans de otros protocolos como dY/dX.

Además, como Aave es un protocolo abierto, se pueden generar aplicaciones que integren sus funcionalidades. Un ejemplo es un servicio que permite a los

usuarios acceder a las liquidaciones de Aave sin pasar por su plataforma (iliquidate.finance).

### 4. Tipo de interés e interest swaps

Debido a la actualización constante del tipo de interés en cada bloque generado en Ethereum, el precio del dinero que se ha pedido prestado puede variar en el tiempo. Cuanta más liquidez haya en el protocolo, menos bruscos serán estos cambios, pero es cierto que, en casos excepcionales, el tipo de interés puede llegar a dispararse.

Para algunos borrowers, este riesgo es alto, y están dispuestos a asumir un tipo de interés más elevado pero fijo en el tiempo. Esto significa que, a la hora de pedir prestado, tienes la opción de pagar un interés variable o un interés fijo en el tiempo, que a pesar de que pueda variar, una vez escogido se mantendrá fijo y al precio al que lo tomaste.

Esto también genera cierta vulnerabilidad en el protocolo. Imagina que el interés variable es del 2 % y el fijo es del 5 %. En este momento, la rentabilidad generada por los depositantes es del 1 %. El interés fijo solo se mantendrá siempre que no se llegue a tomar prestado el 95 % de los fondos disponibles o, si el interés generado por los depositantes es mayor que el interés fijo a pagar por los prestamistas. Si esto sucediera habría un bug en el sistema para depositar y pedir prestado continuamente, aprovechando que el interés generado por prestar es mayor que el precio a pagar para pedir prestado.

Los interest swaps consisten en hacer un swap de préstamos fijo a variable o al revés. Esto suele ser una opción para proteger tus préstamos en caso de subidas bruscas en el tiempo del interés variable de la plataforma.

### 5. Flash loans o préstamos sin colateral

Los flash loans son la gran innovación que presentó Aave en su lanzamiento. Por increíble que parezca, los flash loans son préstamos sin colateral. ¿Cómo? Lo que oyes, puedes pedir prestado —por ejemplo— 7 500 ETH sin ofrecer ninguna garantía.

Un flash loan es un préstamo que puedes pedir al protocolo de Aave sin necesidad de poner nada como colateral, siempre que el préstamo se devuelva (más un 0,09 % de comisión) durante la misma transacción (es decir, en el mismo bloque). Por otro lado, si el préstamo no se devuelve durante esa misma transacción, es cancelado, no llegándose a emitir.

Este producto financiero no era posible con el sistema tradicional, pero gracias a Blockchain y a la posibilidad de revertir transacciones antes de su

confirmación, ahora podemos utilizar este tipo de préstamos. Se ha creado una forma de democratizar la liquidez, ya que todo el mundo puede acceder a crédito sin necesidad de disponer de un colateral. Esta innovación también tiene sus riesgos. Imaginemos que se puede pedir un flash loan, usar este préstamo para votar en alguna decisión de gobernanza y justo después devolver el préstamo. Me explico:

Por ejemplo, se puede estar votando en Maker qué hacer con unos fondos que se han generado. Si yo pido un flash loan de Maker, puedo usar este préstamo para votar (podré pedir prestado muchos tokens y manipular la votación a mi favor) y realizar así un ataque de gobernanza. Algunas barreras para evitar estas situaciones podrían ser que para votar debas depositar los tokens durante X horas, y así evitar votaciones a través de flash loans.

Este servicio es principalmente usado por desarrolladores que integran esta liquidez en sus aplicaciones para ofrecer servicios con ellos, que suelen tener el objetivo de generar dinero a través del arbitraje o de ahorrar dinero autoliquidando préstamos obtenidos.

Un ejemplo es DefiSaver: estos te dan la opción de liquidar tu bóveda en Maker para recuperar tu colateral devolviendo a través de un flash loan la cantidad adeudada. Pongamos un ejemplo:

Imagina que has depositado 100 ETH en una bóveda de Maker y a cambio has pedido prestado 10 000 DAI (ejemplo: 50 % del valor de los ETH). Este préstamo no tiene fecha límite y lo estás usando para pagar impuestos evitando vender tu ETH. Al cabo de tres meses, el precio del ETH empieza a bajar bruscamente y te encuentras que no tienes suficiente DAI para devolver el préstamo más los intereses, y que tu bóveda podría ser liquidada asumiendo una penalización del 13 %. Con DefiSaver puedes usar un flash loan de 10 000 DAI más los intereses a devolver en Maker, recuperar tus 100 ETH, llevar 50 ETH en Uniswap, swapearlos por 10 000 DAI más el interés pagado en Maker, y devolver esa cantidad a Aave, cerrando así el flash loan (para saber más sobre MakerDAO, clica aquí).

Gracias a un préstamo sin colateral, has ahorrado un 12,75 % de los 100 ETH depositados en Maker, ya que DefiSaver añade una comisión de 0,14 % al 0,09 % de Aave. Asombroso.

Otro caso de uso lo tenemos con ColateralSwap, que te permite, a través de un flash loan, cambiar el colateral usado en Maker. Tomemos el ejemplo anterior:

Dispones de un préstamo de 10 000 DAI en Maker, que has obtenido colateralizando 100 ETH en una bóveda. Imagina que prevés una caída del ETH

y una revalorización del BAT. Con ColateralSwap puedes usar un flash loan para cambiar el colateral que estás usando (DAI por BAT) en una sola transacción, sin necesidad de disponer de los DAI.

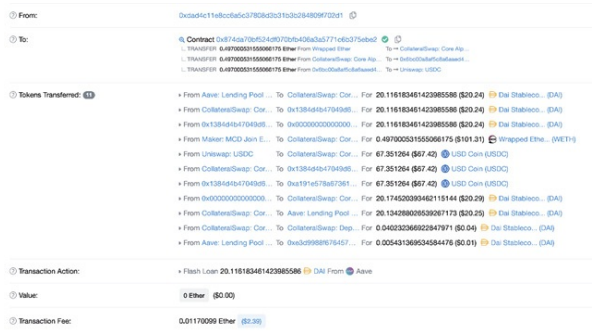



Figura 99. Análisis en Etherscan de un flash loan en Aave

Esta es una transacción utilizando CollateralSwap para cambiar el colateral de Maker de ETH a USDC. Vamos a analizarla:

- Flash loan de DAI para liberar el colateral.
- Recuperas el ETH y lo swapeas por USDC en Uniswap.
- Abres otra bóveda en Maker con USDC.
- Recuperas los DAI en forma de préstamo.
- Devuelves el DAI prestado a Aave.

Por último, comentaré **furucombo**, una aplicación descentralizada todavía en estado beta que te permite encadenar transacciones seguidas, consiguiendo el primer arbitraje a través de un flash loan de un usuario sin haber tenido que desarrollar o programar nada.

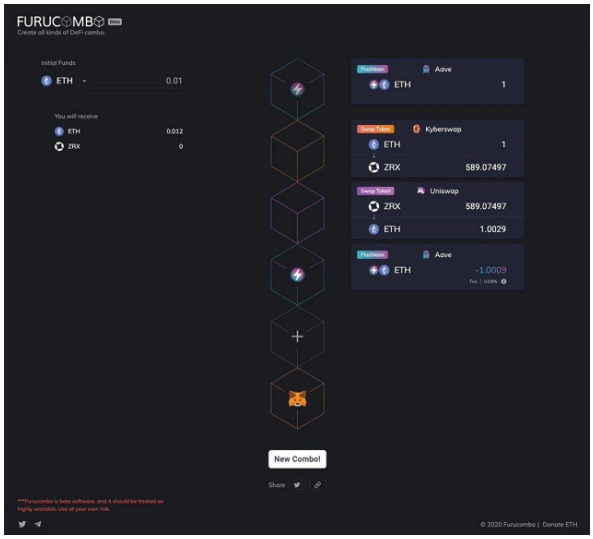



Figura 100. Furucombo en acción (configurador visual de operaciones en DeFi)

Para una explicación más extensa y detallada de los flash loans, aquí tenéis un artículo de Miguel Caballero donde se tratan estos préstamos de forma individual: «Flash loans, DeFi 2.0 y killer-apps».

**6. Intereses generados**

Algo curioso de Aave es que regularmente ofrece mejores retornos que otros protocolos de lending con pools de liquidez compartidos. Esto se debe a las integraciones extras del protocolo. En primer lugar, una cantidad de los préstamos se toman con un interés fijo, dando un retorno mayor a los depositantes, además del 0,09 % de comisión por generar flash loans, donde el 70 % se destina a los depositantes, y, del 30 % restante, 80 % se quema para promover el incremento de valor del token AAVE y un 20 % se destina a los desarrolladores que integren los flash loans. En cuanto a las comisiones de los préstamos normales, estos se usan en un 80 % para quemar tokens AAVE y el 20 % por ciento restante para los depositantes, algo que podría cambiar con la gobernanza descentralizada a través del token nativo.

Un ejemplo del efecto de los flash loans se ve en el interés generado a los depositantes del ETH. Un asset que teóricamente debería ofrecer (comparando el asset en Compound) un retorno del 0,01 % anual, está dando un 0,16 %. Y de este 0,16 %, aproximadamente un 0,1 % lo generó en cuestión de días cuando muchas bóvedas de Maker se intentaron cerrar haciendo uso de los flash loans, generando intereses para todos los depositantes.

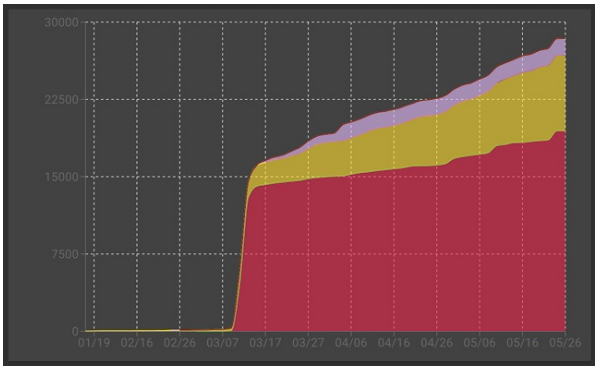


Figura 101. Flash loans durante el Jueves Negro (marzo 2020)

## 18.3. Segundo mercado de Aave: Uniswap liquidity tokens

Como hemos comentado al iniciar el capítulo, Aave no se limita a ser un protocolo de lending, sino es más bien un protocolo de mercados financieros,

donde la opción de depositar y pedir prestado es solamente uno de los mercados disponibles.

Recientemente hemos visto introducido el segundo mercado, que consiste en usar como colateral los liquidity tokens de Uniswap. Si hacemos un repaso, Uniswap es un protocolo para swapear tokens ERC20 gracias a un pool entre dos tokens depositados por los usuarios que reciben un interés a través de las comisiones por cada swap realizado (ver Uniswap aquí).

Hasta ahora, los que añadían liquidez a los pools de Uniswap recibían intereses y un token que representaba esos activos para, más adelante, poder retirarlos o transferirlos a un tercero sin necesidad de retirar la liquidez. Con esta integración de Aave, ahora puedes usar como colateral los liquidity tokens y tomar un préstamo. Este mercado es más arriesgado que el de lending por el tipo de token usado para colateralizar, además del hecho de que Uniswap tiene un riesgo intrínseco debido al rebalanceo entre los dos tokens depositados en el pool.

Por lo tanto, se trata de un mercado nuevo independiente del anterior. Los usuarios podrán depositar sus assets para el mercado de los Uniswap tokens o para el mercado de lending. Esto significa que veremos oportunidades de arbitraje dentro del mismo protocolo, cosa que aún no se había visto.

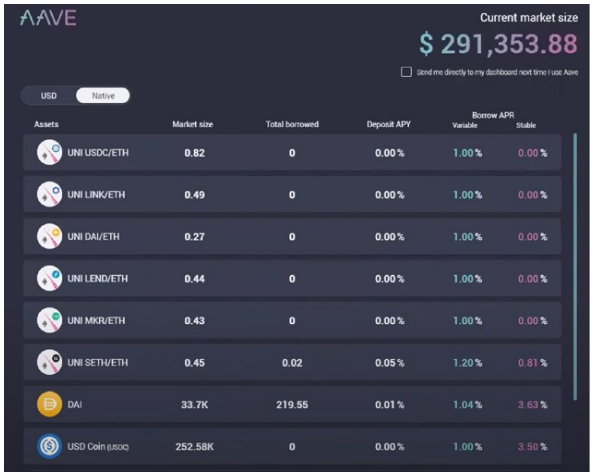


Figura 102. Mercado de Uniswap en Aave

## 18.4. Oráculos en Aave

Otro de los retos de Aave es asegurar que los precios reflejen las condiciones del mercado en tiempo real. Esto conlleva tener en consideración y conocer los precios de las principales plataformas descentralizadas y centralizadas. Estos datos se encuentran principalmente off chain, así que se necesita hacer uso de oráculos para llevar los datos dentro de la blockchain.

Conectar los datos on chain no es suficiente, ya que necesitan ser incorporados utilizando un framework que minimice el riesgo y promueva la descentralización. Esta es seguramente la información más crítica del protocolo, así que es necesario que los datos se obtengan de forma segura y descentralizada.

Con el objetivo de cumplir con estas condiciones, Aave ha usado Chainlink para inyectar los resultados en los smart contracts. Chainlink es una red descentralizada de oráculos que proporciona a los smart contracts acceso seguro y confiable a proveedores de datos, API y muchos otros datos externos.

Seguramente la forma más eficiente es obtener los datos directamente on chain. La nueva versión de Uniswap, por ejemplo, ofrece la opción de usar el protocolo de swaps para proveer datos de precios a tiempo real y on chain. A pesar de la clara mejora de este servicio para el ecosistema DeFi en general, el riesgo asumido es demasiado alto, y quizás veamos adoptados los precios de la versión 2 como oráculo on chain más adelante. Sin ir más lejos, hemos visto protocolos ser atacados y perder millones de dólares por usar Kyber como oráculo de precios. Los atacantes modificaban el precio ofrecido por Kyber añadiendo estrés al pool de liquidez y, justo en ese momento, atacaban al protocolo. También es cierto que la nueva versión de Uniswap ofrece mejoras para evitar este tipo de manipulaciones.

## 18.5. Características del AAVE token

Uno de los elementos que más me fascinan del protocolo de Aave es, sin duda, su token nativo: AAVE. Dispone de unas funcionalidades y unos tokenomics que pueden servir de ejemplo para todo el ecosistema DeFi. Como hemos comentado en varias ocasiones, la gobernanza de un protocolo es la parte más crucial, ya que si un protocolo tiene 1000 MUSD bloqueados y el ataque de gobernanza tiene un coste de 500 MUSD, tenemos un gran problema.

Es por esto que el token debe tener un modelo de tokenomics que incentive a sus tenedores a holdearlo para así beneficiarse de revalorizaciones futuras. De este modo, evitas que se quieran desprender de él, provocando bajadas continuas de precio.

El token AAVE es complejo ya que, además de tener muchas funcionalidades, ha pasado por un proceso de migración. Empecemos por el principio. Cuando ETHLend empezó (proyecto anterior a AAVE), este hizo una ICO con un token llamado LEND. En la ICO se vendieron aproximadamente el 78 % de los tokens disponibles (un billón de los 1,3 billones disponibles). Con la remodelación del

modelo de negocio y la aparición del AAVE, este token adquirió nuevas funcionalidades. En primer lugar, usarlo en la plataforma te otorga ciertos beneficios como pagar menos comisiones, usar el token como garantía, recibir comisiones de otras transacciones y usar esas comisiones para comprar (y quemar) tokens LEND, incrementando el precio del propio token.

Ahora bien, el token no estaba preparado para adoptar el rol de token de gobernanza que quería AAVE para su protocolo. Es por esto que en octubre de 2020 el equipo hizo público un plan para reconvertir el token de LEND a AAVE. Esta migración reduciría cien veces la cantidad de tokens (1 AAVE = 100 LEND), aunque también se crearía un total de tres millones de tokens (una inflación de alrededor del 20 %). Esto, a pesar de ser perjudicial a primera vista, ya que diluye el valor del token, es una estrategia beneficiosa para AAVE y sus holders en el largo plazo. El equipo pretende usar estos nuevos tokens para generar incentivos a sus participantes, y así promover algunas acciones concretas que hacen la plataforma más segura y usable.

El objetivo principal del token AAVE es gobernar todos los mercados financieros de Aave y crear un sistema de incentivos donde el crecimiento, la sostenibilidad y la seguridad del protocolo tengan prioridad sobre los objetivos individuales de las partes interesadas. Este proceso de descentralización de la gobernanza que está viviendo Aave se encuentra a mitad de camino. Actualmente se acaba de hacer la migración y pronto veremos los sistemas de incentivos activados para así finalmente conseguir un token con la gobernanza total del protocolo. Estos incentivos vendrán dados a través de un pool de reserva que incentivará a los proveedores de liquidez y a los que aportan seguridad al sistema.

Uno de los cambios más importantes en el token AAVE es que se puede depositar en un smart contract para que dé seguridad a los fondos de la plataforma. Funcionará como una segunda capa de defensa en caso de que las garantías no sean suficientes para afrontar las deudas generadas dentro del protocolo. A cambio, en caso de generar nuevos tokens (como sucedió en Maker para poder recuperar los fondos perdidos durante el Jueves Negro) dichos tokens los recibirán los depositantes de la garantía como recompensa por proveer seguridad al protocolo. Otros incentivos es que reciben parte de las comisiones del protocolo y forman parte de un sistema de incentivos alimentado por los nuevos tokens creados. Estas comisiones vendrán de todos los mercados disponibles en Aave, desde el lending a los colaterales con Uniswap, y un futuro mercado de préstamos colateralizados con SetTokens.

De alguna forma, Aave está creando una capa de seguridad con una funcionalidad muy similar a los protocolos de seguros como Nexus Mutual. Recibes incentivos por aportar seguridad al sistema, permitiendo una relación win-win para el protocolo.

La última capa de seguridad será la denominada backstop, que permite que los usuarios depositen activos para servir como garantía del protocolo con assets estables o ETH, sin necesidad de que sea AAVE.

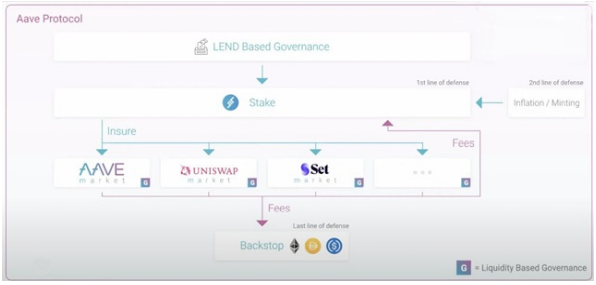



Figura 103. Funcionamiento básico del Aave Protocol

En definitiva, Aave ha conseguido crear un token que actúa realmente como corazón y motor del ecosistema. La gobernanza del protocolo estará en manos de los holders de AAVE, aunque deberán lidiar con unas políticas de mercado y políticas del protocolo fijas y difíciles de mover. Es decir, los holders de AAVE tendrán poder de voto para las decisiones y cambios del protocolo, pero siempre respetando políticas grabadas en Aave.

Están las políticas que se definen en el contexto de cada mercado, y las específicas para los participantes del ecosistema Aave (que implican operar de modo que no se violen las políticas de seguridad del protocolo).

En segundo lugar, las políticas de Aave son las encargadas de gobernar el comportamiento general del sistema y las entidades que pertenecen a él. Regulan aspectos específicos del protocolo relacionados con la seguridad, la economía y la expansión.

Esta es la imagen final de los tokenomics del token:

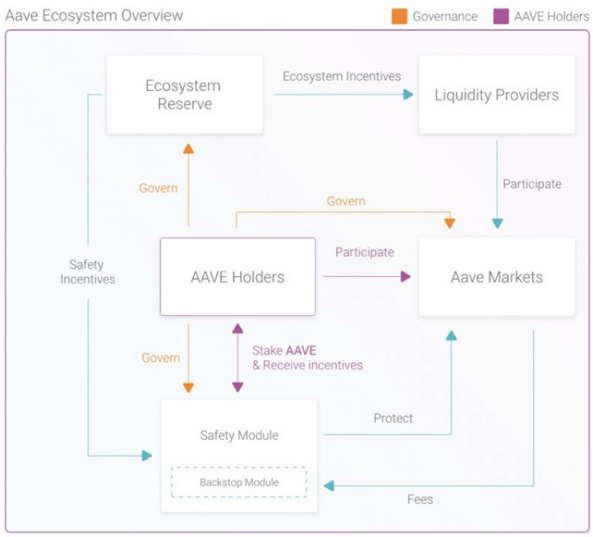


Figura 104. Tokenomics básicos del Aave Protocol

# 18.6. Conclusiones de Aave

No hace ni diez meses que se lanzó el protocolo DeFi de Aave y en este poco tiempo se ha convertido en uno de los proyectos líderes, tanto por sus aportaciones innovadoras como por las mejoras continuas y constantes que van añadiendo.

Uno de los puntos clave es la transparencia que ofrecen sobre los datos y funcionalidades del protocolo. Aunque no serlo resultaría absurdo (ya que todo es público y revisable al ser open source), trabajan para que esta transparencia sea aún más visible. Aquí, por ejemplo, puedes ver todos los datos del protocolo en tiempo real, junto a las estadísticas de cada asset.

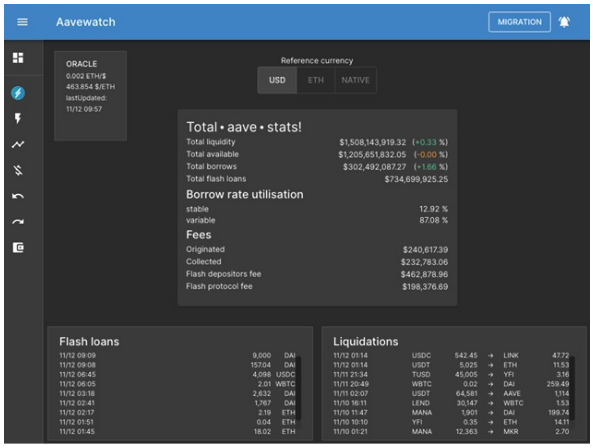


Figura 105. Estadísticas de Aave a tiempo real. https://aavewatch.com/

En poco tiempo, Aave se ha convertido en la principal amenaza de Compound. Este tweet me sorprendió bastante en su momento:

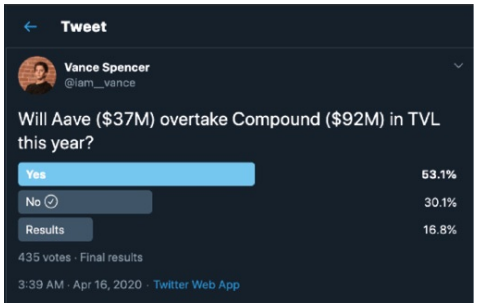



Figura 106. Abril 2020, polémica entre Aave y Compound. Fíjate en el TVL (37 MUSD)

En el momento del tweet, Aave aún disponía de un token nativo (AAVE) con unos tokenomics muy mejorables, además de que tampoco había anunciado el nuevo mercado financiero de Uniswap. Este *post* se hizo en abril, en un momento donde Aave tan solo empezaba. Hoy, es el protocolo líder en mercados de dinero con una capitalización de más de dos billones de dólares. Incluso en ese momento, algunos ya lo tenían claro:


Figura 107. Respuesta de un usuario al tweet anterior

Sin duda, algo a tener en cuenta es la parte de less captured by VC. Compound se financió principalmente por rondas privadas, lo que hace que el token esté mucho menos distribuido, todo lo contrario que el token de Aave. En general, los tokens capturados por VC suelen tardar en aparecer y revalorizarse debido a su falta de liquidez. Aave representa una gran amenaza en este sentido: su amplia distribución hará que las interacciones con el token sean mucho mejores.

Sin duda espero lo mejor para Aave, no solo por el equipo de detrás, siempre atentos y con ganas de mejorar para ofrecer DeFi a un sistema financiero tradicional que lo necesita, sino también por todas las innovaciones que están trayendo al ecosistema.

# 19. Liquidity mining y yield farming

## 19.1. Introducción al LM y YF

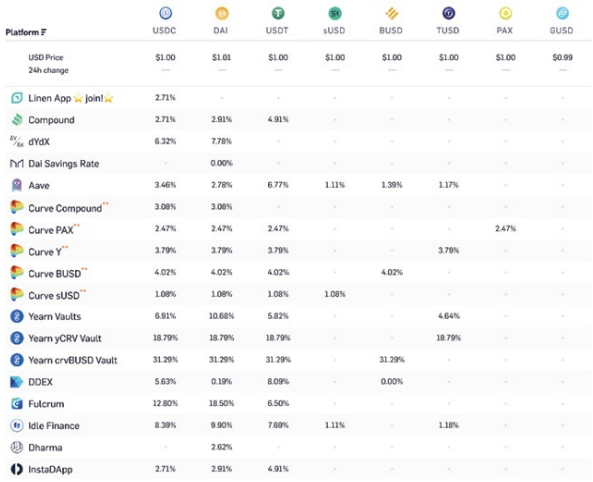
A mediados de junio y principios de julio (2020), DeFi vivió el boom definitivo, llegando por primera vez a los 10 000 MUSD bloqueados en protocolo financieros. Esto fue gracias a la llegada de dos nuevos conceptos que hoy ya son un día a día en este ecosistema: el yield farming y el liquidity mining. Antes de analizarlos, haremos un repaso general para anclar definitivamente conceptos sobre DeFi y así seguir avanzando.

Como hemos visto muchas veces, DeFi hace referencia a un conjunto de aplicaciones descentralizadas que nos permiten operar de la misma forma que en las finanzas centralizadas, solo que en un sistema donde siempre mantienes en control de tus activos, sin intermediarios (peer-to-peer network) y en el que puedes utilizar criptoactivos.

Muchos de estos protocolos necesitan liquidez para aportar esos servicios financieros que, al ser descentralizados, son los mismos usuarios los que depositan sus activos actuando como proveedores de liquidez a cambio de unos intereses. Es decir, pones tu dinero a trabajar sin la necesidad de comprar o perder tu posición en ese activo.

Los protocolos DeFi suelen ser muy atractivos ya que sus rendimientos en comparación con las finanzas tradicionales son muy altos. Solo si vamos a los bonos americanos, una posición a diez años con suerte puede darte un 0,68 %. En cambio, posiciones con stablecoins en protocolos DeFi pueden generarte hasta más de un 5 % - 10 % anual, creando un mercado maravilloso para mucha gente alrededor del mundo. Este matiz es importante: **alrededor del mundo.**

DeFi no está limitado a una zona geográfica o a un cierto nivel adquisitivo, está abierto a todo el mundo sin ningún tipo de restricción. Pongamos como ejemplo el caso de Argentina, donde por políticas monetarias mal gestionadas por parte del Estado, sus ciudadanos usan el concepto de dolarizarse para luchar contra la inflación. Este cambio ahora es de lo más complicado, ya que el Estado pone trabas para evitarlo. Aquí podemos ver cómo todo un país no solo se beneficiaría de la dolarización a través de stablecoins, sino que además podrían usar esos activos para generar unos rendimientos muy altos en comparación a las posiciones que podría haber adoptado en las finanzas tradicionales.



| Platform | USDC | DAI | USDT | sUSD | BUSD | TUSD | PAX | GUSD |
|---|---|---|---|---|---|---|---|---|
| USD Price 24h change | $1.00 | $1.01 | $1.00 | $1.00 | $1.00 | $1.00 | $1.00 | $0.99 |
| Linen App join! | 2.71% | - | - | - | - | - | - | - |
| Compound | 2.71% | 2.91% | 4.91% | - | - | - | - | - |
| dYdX | 6.32% | 7.78% | - | - | - | - | - | - |
| Dai Savings Rate | - | 0.00% | - | - | - | - | - | - |
| Aave | 3.46% | 2.78% | 6.77% | 1.11% | 1.39% | 1.17% | - | - |
| Curve Compound** | 3.08% | 3.08% | - | - | - | - | - | - |
| Curve PAX** | 2.47% | 2.47% | 2.47% | - | - | - | 2.47% | - |
| Curve Y** | 3.79% | 3.79% | 3.79% | - | - | 3.79% | - | - |
| Curve BUSD** | 4.02% | 4.02% | 4.02% | - | 4.02% | - | - | - |
| Curve sUSD** | 1.08% | 1.08% | 1.08% | 1.08% | - | - | - | - |
| Yearn Vaults | 6.91% | 10.68% | 5.82% | - | - | 4.64% | - | - |
| Yearn yCRV Vault | 18.79% | 18.79% | 18.79% | - | - | 18.79% | - | - |
| Yearn crvBUSD Vault | 31.29% | 31.29% | 31.29% | - | 31.29% | - | - | - |
| DDEX | 5.63% | 0.19% | 8.09% | - | 0.00% | - | - | - |
| Fulcrum | 12.80% | 18.50% | 6.50% | - | - | - | - | - |
| Idle Finance | 8.39% | 9.90% | 7.69% | 1.11% | - | 1.18% | - | - |
| Dharma | - | 2.62% | - | - | - | - | - | - |
| InstaDApp | 2.71% | 2.91% | 4.91% | - | - | - | - | - |

Figura 108. APY para distintos protocolos en Loanscan

Claro está que también encontramos factores de riesgo. Todas las inversiones con grandes retornos nacen debido a que asumimos un riesgo. El principal seguramente está en la poca madurez del mercado, haciendo posible errores o bugs en los smart contracts que gestionan los fondos de los protocolos. Aunque si este riesgo disminuye con el tiempo, dudo que los rendimientos lo hagan también de forma proporcional.

Una diferencia entre el mundo cripto y las finanzas tradicionales es la descentralización de las políticas monetarias. Es decir, en un entorno DeFi no se pueden bajar los tipos para promover el gasto ni manipular los rendimientos que generan los ahorros. A día de hoy, el sistema tradicional desincentiva claramente el ahorro y promueve el gasto. Es más inteligente gastar hoy que ahorrar para mañana, ya que este dinero ahorrado tendrá menos valor. Es más: lo mejor es pedir prestado y endeudarse, ya que el dinero es barato (nunca se acaba) y el total a retornar cada año representa menos valor. En un mundo DeFi esto no es posible —al menos en la misma magnitud que existe ahora—, lo que incentiva mucho más el ahorro en la mayoría de la gente, ofreciendo rendimientos dignos por su capital y promoviendo la mejora de la calidad de vida de la población en general.

## 19.2. Liquidity mining

Ahora que hemos hecho un repaso sobre las finanzas descentralizadas, podemos introducir los conceptos de yield farming y liquidity mining. Aunque hacen referencia a prácticamente lo mismo, tienen algunas diferencias.

El concepto de liquidity mining se refiere a una mecánica que han implementado algunos protocolos para incentivar a los usuarios a proveer liquidez. Como muchos de estos sistemas dependen de la liquidez para poder aportar más valor a los usuarios, se ha creado un mecanismo que compensa con tokens nativos o de gobernanza del protocolo a aquellos que están añadiendo liquidez. Es decir, el sistema remunera a aquellos que gracias a su aporte están ayudando a mejorar el protocolo.

El concepto de minería es algo bastante familiar en el mundo cripto. Repasando, es básicamente el sistema que utilizan blockchains como Bitcoin o Ethereum para dar seguridad a la red. Los llamados mineros aportan fuerza computacional a la red, con la cual luchan por tener el privilegio de anotar el siguiente bloque a la cadena. Con esta aportación, los mineros hacen que la cadena sea más segura y por tanto más confiable como red de transmisión de valor.

La seguridad es la clave y la característica más valiosa de la red de Bitcoin. Es por eso que Bitcoin nació con un sistema natural de incentivos para recompensar a aquellos que proveen seguridad, a la vez que anima constantemente a que este aporte de seguridad continúe creciendo. Este sistema ha sido utilizado por la gran mayoría de blockchains públicas; de hecho, Ethereum sigue utilizando el mismo mecanismo hasta que llegue la actualización ( Ethereum 2.0), donde acogerá un sistema con finalidades similares pero con procesos distintos.

DeFi, en cambio, es una estructura de protocolos financieros creados sobre la red de Ethereum (principalmente) que aportan servicios como derivados, lending, trading… Como ocurre con la red de Bitcoin, el factor clave para el mercado DeFi es la disponibilidad de capital, es decir, la liquidez. Cuanta más liquidez haya bloqueada en los protocolos, mayor eficiencia y valor para los usuarios tiene. Por este motivo, algunos protocolos han empezado a ofrecer sistemas de incentivos a los proveedores de liquidez, ya que de alguna forma esto genera una relación win-win (ambas partes ganan).

**En definitiva, liquidity mining consiste en ofrecer incentivos a los proveedores de liquidez de protocolos DeFi a través de la emisión de tokens de gobernanza, algo muy similar al equity o las participaciones de una empresa.**

Y este incentivo suele repartirse, en general, de forma proporcional a la liquidez y al valor que genera ese capital dentro del protocolo. La relación win-win viene dada por un círculo virtuoso generado en el protocolo:

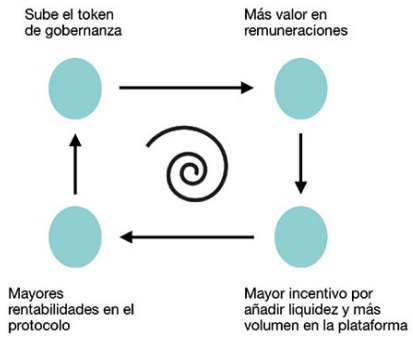


Figura 109. Círculo virtuoso del liquidity mining con token de gobernanza

Veámoslo con más detalle. La emisión de tokens de gobernanza incentiva la entrada de liquidez en el protocolo. Esta liquidez permite al protocolo ofrecer sus servicios financieros de forma más eficiente. Este aumento de eficiencia atrae a más usuarios, ya que el protocolo ahora es más competitivo dentro del mercado. Este aumento de usuarios aumenta los beneficios del protocolo (por comisiones o intereses), lo que comporta un aumento de precio del token de gobernanza que captura el valor generado en el protocolo. Finalmente, los proveedores de liquidez, al haber un aumento en el precio del token que reciben como incentivo, están interesados en aportar aún más liquidez.

Este modelo win-win no es para nada curioso. De hecho, Bitcoin ha generado también un círculo virtuoso alrededor de su protocolo gracias al sistema de incentivos:

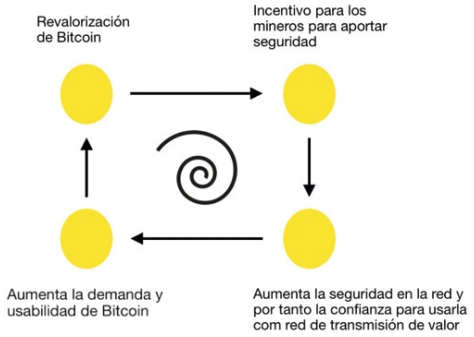


Figura 110. Círculo virtuoso en los incentivos de Bitcoin

Como vemos, el incentivo de minar (recibir BTC por cada bloque generado) impulsa a los usuarios a convertirse en mineros, aportando fuerza computacional y por lo tanto haciendo la red más segura. Al hacerla más segura, la usabilidad de Bitcoin aumenta, y con ello el número de usuarios. Este aumento conlleva una revalorización del precio de Bitcoin, lo que incentiva aún más la aparición de nuevos mineros que hacen todavía más segura la red.

De nuevo confirmamos cómo un sistema de incentivos bien generado es un elemento crucial para crear ecosistemas sanos, descentralizados y con valor en el

largo plazo. Se trata de un método que aprovecha las características naturales de las blockchains para redistribuir el valor generado dentro de los protocolos por parte de todos sus usuarios, y darle una lógica a esta distribución en forma de incentivos para promover aún más el crecimiento y el futuro a largo plazo de este ecosistema. Sin duda es algo apasionante. Estoy impaciente por ver cómo estos mecanismos de incentivos se van a llevar a plataformas tan conocidas como YouTube, Amazon o Facebook, o si realmente van a ser estos los que aprovecharán estos mecanismos o se verán superados por otros precisamente gracias a la opción de dar parte del valor generado a sus usuarios. Sin ir más lejos, Balancer superó en cuestión de semanas a Uniswap al lanzar un sistema de incentivos basado en liquidity mining. Esto fue algo previsible, ya que Uniswap no tenía —en ese momento— un modelo de negocio claro ni un token que acumulase parte del valor generado, lo que se convirtió en una gran debilidad para ellos en caso de que aparecieran protocolos similares, con tokens nativos y modelos de incentivos mucho más claros.

## 19.3. Gobernanza a través de liquidity mining

Como hemos visto, los protocolos que usan liquidity mining suelen dar, como incentivo al aporte de liquidez, el token de gobernanza del protocolo. Estos tokens son de lo más interesantes, así que dedicaremos unas líneas a comprenderlos mejor.

Seguramente la parte más valiosa de un protocolo son sus tokens de gobernanza, ya que con estos tienes el poder de utilizar fondos bloqueados en el protocolo en su propio beneficio, de forma que el valor del token puede considerarse proporcional al valor de los recursos que gobierna. Este concepto es muy claro en los casos de equity empresarial: con ellos tienes derecho a una parte de la empresa. En cambio, en los tokens de gobernanza su precio puede ser modificado por el libre mercado, lo que provoca que dichos tokens tengan que diseñarse con mucho cuidado, ya que pueden convertirse en la causa del fracaso de un gran proyecto. Me remito al ejemplo puesto en capítulos anteriores: imagina que un protocolo acumula 100 MUSD y que el coste del ataque de gobernanza es de 25 MUSD. Claramente el ataque está muy incentivado, por lo que el riesgo es extremo.

Un buen diseño se consigue combinando unos buenos tokenomics y un buen modelo de gobernanza. **Los tokenomics vendrían a ser las normas del sistema y el modelo de gobernanza definiría quién tiene el poder de cambiar dichas**

**normas y en qué condiciones.** En el caso de que estos dos modelos se hayan diseñado correctamente, el token puede servir como valor añadido de la plataforma porque, al contrario que el equity, un token de gobernanza representa capital a la vez que actúa como moneda. Es decir, es una fusión entre un utility token y un token de gobernanza que genera una nueva forma de capital; el **network capital**.

Un claro ejemplo del poder de un token de gobernanza es el incremento de valor del token COMP, nativo del protocolo de Compound. Su modelo de gobernanza determina que solo aquellos con un 1 % (propio o delegado) de los COMP en circulación, tienen el derecho a hacer propuestas de mejora en el protocolo. Este *poder* sobre el capital bloqueado tiene muchísimo valor, lo que ha provocado una avalancha de compras del token por individuos, grandes carteras e incluso fondos de inversión, para así tener una posición privilegiada a la hora de determinar el futuro de Compound.

Desde el nacimiento de liquidity mining hay dos proyectos que lo han explotado de forma espectacular y que vamos a comentar a continuación: Compound y **Balancer**. No obstante, estos no son los únicos que han adoptado estrategias de liquidity mining. De hecho, hay otros como RenVM, Sinthetix, mStable… Vamos a analizarlos en detalle.

## 19.4. Liquidity mining en Compound

Como ya analizamos en capítulos anteriores, Compound es un protocolo que funciona como un mercado de capital, con servicios de lending y borrowing, a tipos de interés generados por oferta y demanda y en tiempo real (en cada bloque, es decir, cada aproximadamente quince segundos). Así que podemos identificar dos usuarios: los que prestan dinero al protocolo y los que después piden préstamos a partir del capital que han depositado los prestamistas. Compound incorpora el liquidity mining para incentivar a estos dos usuarios de forma igual: el 50 % de los tokens destinados a cada asset irá a los prestamistas y el 50 % a los que piden prestado (prestatarios).

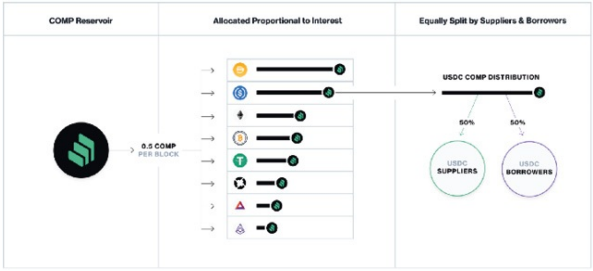


Figura 111. Liquidity mining en Compound

El token de gobernanza, denominado COMP, da poder de voto a las propuestas generadas por aquellos que disponen de más de un 1 % de los tokens, ya sean propios o delegados. Vendría a ser un token que representa el equity del protocolo, aunque con algunas diferencias. De hecho, actualmente el COMP ofrece dividendos, algo que podría cambiar si los stakeholders aprueban un cambio en el protocolo donde este genera unos ingresos que después reparte en forma de dividendos.

Este sistema de incentivos, de nuevo, crea un círculo virtuoso tanto para Compound como para sus usuarios. El hecho de haber más capital hace que los préstamos sean más baratos, lo que a su vez promueve generar más préstamos, haciendo de nuevo muy atractivo depositar capital; como ves, genera una rueda que no para de retroalimentarse.

Dentro de Compound existe la opción de comprobar cuáles son las direcciones (wallets) con mayor fuerza de voto, y es de lo más interesante, ya que no solo tenemos algunos de los fundadores sino también otros protocolos como Kyber Network, InstaDapp o fondos de inversión muy conocidos en la industria:

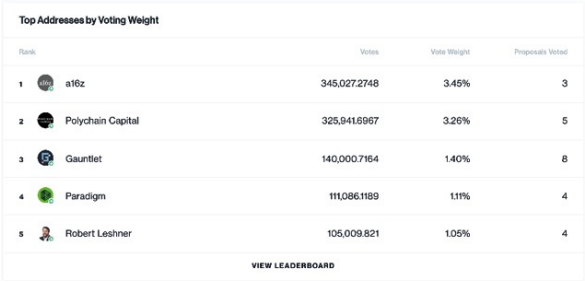



Figura 112. Top 5 COMP adress

La distribución inicial propuesta por Compound fue la siguiente:

| Party | Tokens | Percentage |
|---|---|---|
| **Shareholders** | 2,396,307 | 24.0% |
| **Founders & Team** | 2,226,037 | 22.3% |
| **Option Pool** | 372,707 | 3.7% |
| **Users** | 5,004,949 | 50.0% |
| **Compound Labs, Inc** | 0 | 0.0% |
| **Total** | **10,000,000** | **100.0%** |

Figura 113. Propuesta inicial de distribución de los COMP tokens

Aunque finalmente este modelo ha cambiado un poco, en total se van a emitir diez millones de tokens, de los cuales cuatro millones se van a repartir como incentivos a los borrowers y a los lenders durante cuatro años; lo que equivale a unos 2880 tokens al día, distribuidos en cada bloque minado en Ethereum. Estos

se reparten proporcionalmente a la demanda de préstamos de cada activo, y luego se divide 50 % a los borrowers y 50 % a los lenders. Es decir, en función de la demanda de cada asset, este recibirá más o menos tokens. Por ejemplo, si el activo más demandado es BAT, este seguramente recibirá la mayor compensación en tokens COMP, aunque si con el tiempo la demanda de DAI supera a la de BAT, los borrowers y lenders de DAI son los que recibirán los mayores incentivos. Aquí tenemos una imagen actual de la distribución por assets de los COMPS distribuidos:

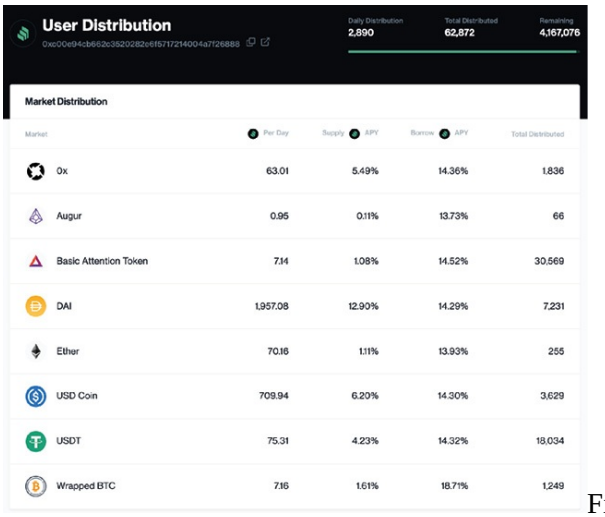



Figura 114. Distribución actual en función de la demanda de préstamos

Los tokens que se van minando se acumulan dentro de la plataforma y pueden retirarse a partir del momento en que hayas acumulado un mínimo de 0,001 COMP.

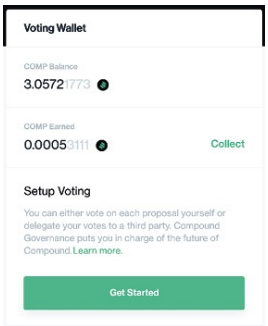



Figura 115. Wallet interno de Compound

Algo muy interesante a nivel de inversión que podemos desarrollar en este protocolo es la opción de utilizar el leverage (apalancamiento) de la plataforma o el leverage de smart contracts especialmente diseñados para aumentar la cantidad de COMP que puedes llegar a generar.

Compound, al ser un mercado de dinero, te da la opción de pedir un préstamo en función de la cantidad de activos que hayas depositado. Esto significa que si depositas 1000 DAI, tomas prestado después 300 DAI y los vuelves a depositar en Compound, tendrás una posición apalancada con la que serás capaz de generar más COMP de los que podrías solo con tu propio capital. Esto de hecho explica que el marketcap de DAI sea (en el momento de escribir estas líneas) de 157 MUSD y, en cambio, la cantidad de DAI depositada en Compound sea de 500 MUSD.

De hecho, existen también smart contracts que te permiten generar cuatro veces más COMP de los que generarías con tus activos en propiedad. Eso sí, recuperamos de nuevo el concepto de riesgo. **Cuanto más rentabilidad, más riesgo.**

Estas posiciones de leverage pueden llegar a ser desastrosas en caso de caídas fuertes del mercado, ya que se liquidarían muchas posiciones de golpe poniendo el capital depositado en un riesgo altísimo. Es por estas prácticas por las que han aparecido críticas a algunos protocolos DeFi, clasificándolos como burbujas que están repitiendo el *hype* de las ICO de 2017, pero esta vez en 2020 y en torno a DeFi.

Como opinión personal, creo que estas prácticas son correctas simplemente porque son posibles gracias a Blockchain. **Quizás la solución esté en trabajar mejor los sistemas de seguridad a través de pools como ha hecho Aave**, que además ha conseguido dar más funcionalidad y valor a su token nativo. Por otro lado, también hay que recordar que existen protocolos que nos permiten asegurar nuestro capital, como Nexus Mutual. Así que en caso de que estés manteniendo posiciones de leverage con gran riesgo, podrías también generar una garantía de tu capital y así estar cubiertos en caso de situaciones bajistas del mercado.

## 19.5. Liquidity mining en Balancer

Otro protocolo que analizamos en capítulos anteriores es Balancer, un exchange descentralizado similar a Uniswap aunque con diferencias en cuanto a la forma de construcción de los pools: en Balancer tienes la opción de participar en diferentes pools con distintas proporciones de tokens y políticas de fees de entrada y salida. Cada pool puede tener fees diferentes y los usuarios hacen trading contra estos smart contracts (pools) para así hacer swaps entre tokens de forma eficiente y poco costosa.

Ahora analizaremos cómo Balancer ha aplicado el liquidity mining en su protocolo, ya que gracias a esto ha sido capaz de colocarse entre los diez primeros protocolos en cuanto a dinero bloqueado.

Como vamos a ver, aplicar liquidity mining en Balancer tenía todo el sentido del mundo. **La competitividad y eficiencia de un DEX recae sobre todo en la liquidez de la que disponga**. Cuanta más liquidez tenga el DEX, los usuarios podrán gozar de swaps más económicos y eficientes, lo que aumenta el volumen diario en el protocolo, que a su vez aumenta la rentabilidad generada a través de las fees, que de nuevo incentiva aún más a otros usuarios a añadir más liquidez. Este círculo virtuoso se ha iniciando gracias a otro incentivo que es la emisión de los tokens de gobernanza de BAL, que han sido los que han empujado la rueda para que esta pueda girar sola.

Teniendo esto en mente, a su vez Balancer busca incentivar con más fuerza a aquellos proveedores de liquidez más iniciales, es decir, los que participan desde hace más tiempo, ya que son los que asumen más riesgo, tanto por posibles fallos en los smart contracts como por costes de oportunidad. Por ello, los proveedores van a recibir rendimientos de sus assets no solo a través de las fees generadas en el protocolo, sino también a través de la distribución de tokens BAL, para que así ganen más peso a la hora de definir la evolución futura del protocolo.

El total de tokens BAL emitidos es de cien millones: veinticinco millones colocados ya desde el inicio entre los fundadores, core developers, advisors e inversores; y los setenta y cinco millones restantes, distribuidos en forma de incentivos a los proveedores de liquidez. Un dato interesante es cómo la distribución es más justa en Balancer que en Compound, sobre todo porque este está menos capturado por venture capital llegados a través de inversiones privadas en las primeras etapas del proyecto. Actualmente se distribuyen 7 500 000 tokens al año (145 000 por semana), lo que significa que habrá una inflación del 30 % el primer año respecto a los veinticinco millones de tokens emitidos inicialmente. En un futuro, la distribución anual puede cambiar, ya que se va a discutir y decidir entre la comunidad de stakeholders de BAL.

Un objetivo de Balancer es hacer esta distribución de la forma más justa posible, de manera que se distribuya de forma proporcional a la liquidez aportada por cada adress, teniendo en cuenta también el valor que aporta esa liquidez al protocolo. Por ello, hay algunos factores que influyen en la cantidad de token BAL que reciben los proveedores de liquidez.

Factores que influyen en la distribución:

Primero tenemos el **feeFactor**. Los pools con fees más bajos contribuyen con más fuerza al valor y la usabilidad del protocolo, y por tanto, reciben más compensación:

$$feeFactor = e^{-\left(\frac{fee}{2}\right)^2}$$

Figura 116. Fórmula del feeFactor en Balancer

Esta fórmula crea un gráfico en forma de curva donde, por ejemplo, un pool con un fee de 0,5 % tiene un feeFactor de - 0,94; y un pool con un fee del 1 %, tiene un feeFactor de - 0,78

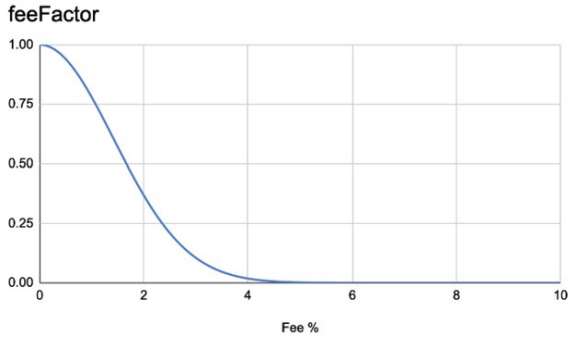



Figura 117. Curva del feeFactor en Balancer

Otro elemento que influye en la distribución es el **ratio factor**, que busca dar una retribución más elevada a los pool con proporciones más equilibradas, ya que consiguen dar precios más estables. Por ejemplo, un pool con un 10% de DAI y un 90% ETH, al tener proporciones poco equilibradas, los movimientos del precio de los swaps son muy bruscos, aportando peores precios y por tanto menos valor al protocolo. Por ello, este factor sirve para retribuir más a aquellos pools con balances más equilibrados.

Por último, tenemos el **wrapped factor**, que busca dar menos peso a la hora de recibir BAL a aquellos pools de tokens con poco volumen, ya que son más específicos o diferentes. Estos pares que vienen ahora tienen diez veces menos peso a la hora de recibir BAL:

```
[WETH, aETH, cETH, iETH (iearn), iETH (Fulcrum), PETH], // ETH group
[DAI, aDAI, cDAI, dDAI, iDAI, yDAI, rDAI, CHAI] // DAI group
[USDC, aUSDC, cUSDC, dUSDC, iUSDC, yUSDC] // USDC group
```

Figura 118. Tokens con wrapped factor aplicado en Balancer

Una vez se calcula y actualiza la liquidez aportada por cada adress en relación a la liquidez total de acuerdo con los factores comentados, se distribuyen los tokens. Algo curioso es que estos se reparten en cada snapshot block, es decir, cada sesenta y cuatro bloques o bloques generados durante quince minutos,

donde se reparten 230 BAL (145 000 tokens por semana/630 snapshot blocks por semana).

| Address | % Balancer liquidity ($) | BAL token received |
|---|---|---|
| 0xaaaaa... | 1% | 2.3 |
| 0xbbbbb... | 0.8% | 1.84 |
| 0xccccc... | 1.5% | 3.45 |
| 0xddddd... | 0.1% | 0.23 |
| 0xeeeee... | ... | ... |
| 0xffffff... | ... | ... |
| ... | ... | ... |
| **Total:** | **100%** | **230** |

Figura 119. Tokens distribuidos y con los factores aplicados

## 19.6. Yield farming

Ahora que entendemos en qué consiste el liquidity mining, podemos ver que si escogemos estrategias de inversión inteligentes que combinan varios protocolos a la vez, podemos llegar a hacer mining de liquidez de varios protocolos y, por tanto, recibir más de una recompensa.

Esta variedad de protocolos DeFi y de modelos de incentivos para proveer de liquidez provocó que muchos usuarios buscaran estrategias para obtener el máximo retorno de su inversión. Estos son los llamados farmers o granjeros, que teniendo en cuenta los intereses, las comisiones y los modelos de incentivos, buscan las mejores opciones de inversión para así maximizar los retornos económicos.

Estas estrategias no son fijas, sino que van cambiando con el tiempo, tanto porque la rentabilidad que ofrecen algunos protocolos cambia como porque los modelos de incentivos también pueden ir variando, y donde antes generaban dos tipos de tokens a través de liquidity mining ahora solo generan uno porque el modelo de incentivos de uno de los tokens ha dejado de funcionar. Es por esto que es difícil presentar estrategias concretas de yield farming, ya que estas suelen cambiar constantemente. Y esto sin contar la complejidad de algunas estrategias, que incluso pueden involucrar más de un protocolo a la vez.

Solo por poner un ejemplo concreto, una estrategia podría ser la siguiente: un granjero podría depositar ETH y DAI en Compound y a cambio recibiría cETH y cDAI. Estaría recibiendo un interés de sus dos activos además de beneficiarse del liquidity mining de COMP, que también recibiría.

La estrategia podría continuar, ya que ahora el granjero podría llevar sus cDAI y cETH y depositarlos en un pool de Balancer, donde estaría generando un interés gracias a los swaps y estaría recibiendo BAL gracias al sistema de incentivos de Balancer.

Y lo podríamos complicar aún más si parte de los cDAI o cETH los usamos para pedir un préstamo de USDC en Compound y llevarnos después el USDC a Uniswap, lo swapeamos por sUSD, llevamos el sUSD a Curve y lo depositamos en un pool para así recibir intereses y tokens CRV (Curve token) y SNX (Synthetix token) gracias a los modelos de incentivos de cada protocolo.

Como veis, las estrategias pueden ser tan complejas como queramos, pero también hay que entender que cuanto más las compliquemos, más costosas serán en gas, más difíciles de gestionar (como los rendimientos son cambiantes deberemos revisar la rentabilidad de la estrategia regularmente) y más riesgo estaremos asumiendo. Estas prácticas se han hecho muy populares durante la segunda mitad del 2020; tanto que han aparecido proyectos de altísimo riesgo con sistema de incentivos muy agresivos.

Siempre debemos recordar que participar en los protocolos de farming o diseñar estrategias de farming es algo complejo y arriesgado. Sin duda, muchas pueden ser altamente rentables, pero siempre recomendaría formarse antes, aprender sobre DeFi y después destinar una parte minoritaria de tu portfolio a este tipo de inversión. Digo una pequeña parte porque un buen portfolio es aquel que equilibra inversiones de bajo y alto riesgo, así que está bien hacer uso del yield farming, pero siempre con una estrategia que nos asegure que, si algo falla, no perdamos todo nuestro dinero.

# 20. Protocolos para gestión de fondos: Melon Protocol

## 20.1. Introducción a Melon

Melon es un protocolo que, a pesar de estar poco capitalizado y bastante penalizado por el mercado, forma parte de las mayores innovaciones del ecosistema. Básicamente Melon es un protocolo de gestión de activos, lo que en finanzas tradicionales definimos como fondos de inversión. De alguna manera, Melon sirve como plataforma base para la creación de los fondos de inversión del futuro (o los criptofondos).

La industria de los fondos de inversión es de las más tediosas de todo el mundo financiero, estando exageradamente regulada. No digo que esto sea malo, ya que estas regulaciones tienen el objetivo de garantizar la transparencia en la operativa de estos fondos para evitar grandes estafas (como ya ha habido) o que los gestores de los fondos actúen mirando por su propio interés y no el interés de los socios participantes. Al final, esto es crítico ya que otra persona tiene el poder sobre fondos de muchas personas, y es fácil ver que es necesaria dicha regulación.

Esta muralla regulatoria, aunque necesaria, hace que toda la industria sea lenta, poco ágil y muy poco eficiente, sin contar que, para crear un fondo, los tiempos suelen ser largos (mínimo seis meses) y que los costes asociados a su creación y la gestión son exageradamente altos. Esto provoca que solo unos pocos privilegiados puedan acceder a esta industria, que esta sea poco accesible para la mayoría de gente. Es más, la mayor parte de los clientes de los fondos de inversión suelen ser gente adinerada.

Melon llega entonces para revolucionar para siempre este sector, ya que por primera vez existe la opción de crear un fondo en aproximadamente diez minutos y con unos costes de creación y gestión insignificantes en comparación con los que se necesitan para crear un fondo tradicional. De hecho, este coste está directamente asociado al coste del gas en cada momento, ya que no hay ninguna comisión por crear un fondo, sino que lo único que hay que hacer es deployar sobre la red de Ethereum un conjunto de contratos.

Estos contratos son los que permiten crear unas normas de transparencia absoluta, además de limitar la operativa de los fondos para dar absoluta seguridad al inversor sobre dónde está invirtiendo. Melon pretende convertir los fondos de inversión en algo accesible a todo el mundo, ya que ahora es posible

participar en un fondo con 10 EUR o menos, además de entrar y salir de él cuando quieras. Hoy esto es impensable, ya que no solo tus acciones dependen siempre de un tercero o un intermediario, sino que son muy poco flexibles, y siempre vas a necesitar pasar por un lento y tedioso proceso de verificación.

Con Melon, los gestores de fondos no necesitan saber quién eres, puedes invertir usando solamente MetaMask. Y si esto fuera poco, debemos recordar que está construido sobre Blockchain así que todo, y cuando digo todo es todo, es auditable al 100 %, aportando un nivel de transparencia sin precedentes. Melon ha revolucionado de una forma espectacular una de las industrias con más peso del mundo financiero.

## 20.2. Operativa para inversores

El proceso para los inversores que quieren participar en un fondo es muy sencillo. Entrando en la plataforma de Melon puedes analizar cada uno de los fondos, ver sus portfolios, qué tokens tienen comprados y en qué proporciones/cantidades, cuáles son sus comisiones por el *performance* (es decir, cuánto te cobra el fondo por los beneficios que te genere) y cuáles son las rulesets aplicadas.

Las rulesets son unos smart contracts que permiten limitar la operativa del fondo. Por ejemplo, hay una ruleset que imposibilita al fondo exponer su portafolio en un solo token. Analizando las normas que ha aplicado el fondo, un inversor puede estar más tranquilo y seguro a la hora de invertir, porque esas normas están integradas al fondo por defecto.

Por ejemplo, analicemos el Alchemy Fund:


Figura 120. Características de un fondo en Melon

En la primera imagen podemos ver la evolución del fondo durante un periodo de tiempo, el nombre y el precio de cada participación. Al invertir, el gestor del fondo habrá determinado anteriormente los tokens que puedes usar, que

normalmente son: DAI, MLN, ETH, wBTC y USDC. En la barra lateral puedes también obtener información sobre la performance del fondo.


Figura 121. Rentabilidad mensual de un fondo en Melon

Aquí podemos ver cuáles han sido los resultados del fondo (mensualmente).

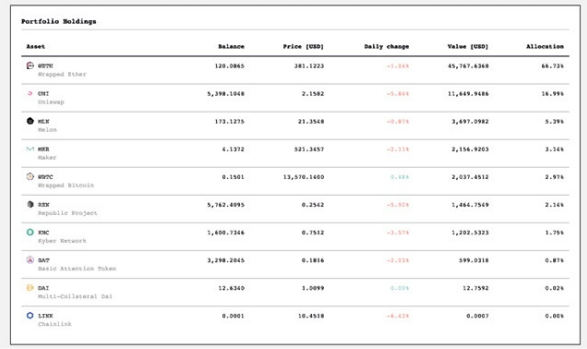



Figura 122. Distribución del portfolio de un fondo en Melon

La distribución del portfolio, tanto en porcentaje como en capital invertido, también está disponible. De hecho, el nivel de transparencia es tal que también podemos conocer su historial de inversión, todos los movimientos de tokens y del portfolio que han realizado o incluso las ruleset que han aplicado (en este caso, este fondo no ha aplicado ninguna ruleset).

## 20.3. Operativa para gestores de fondos

Para ser un gestor de fondos, tan solo debes crear un fondo de inversión a través de Melon y usar MetaMask para pagar los costes de gas al deployar cada contrato. Antes deberemos dar un nombre al fondo, determinar el management fee (cuánto queremos cobrar a los participantes del fondo por los beneficios) y el período de tiempo en el que se cobrarán las performance fees, que suele ser cada noventa días. Estas fees se cobran por *gota de agua*, es decir, si he invertido 100 USD y ahora tengo 110 USD, me cobrarán una comisión sobre esos 10 USD de beneficio. Pero si el mercado cae y ahora dispongo de 101, y el mes siguiente subo a 109, no me cobrarán nada: hasta que no supere los 110 USD en beneficio, no se cobrará ninguna otra performance fee.

Acto seguido debemos deployar nueve contratos, lo que nos puede llevar entre diez minutos y una hora, y los costes de creación siempre van a depender del coste del gas en cada momento. Y quiero remarcar que, aunque el gas esté alto y

tardemos una hora en crear un fondo, el coste total rondará los 300 USD (comparado con el funcionamiento del mercado tradicional, sigue siendo insultantemente barato). No debemos olvidar que estos nueve contratos están creando un framework que nos permite operar como fondo de inversión, algo que en el mundo tradicional necesita de cientos de miles de euros y muchos meses de trabajo, burocracia y papeleo.

Una vez consolidado, habrá que determinar el ruleset del fondo —si es que hay — y finalmente ya estará listo para invertir. Los inversores comprarán participaciones del fondo, cuyo precio dependerá del capital total depositado y el rendimiento del fondo.

## 20.4. Tutellus Fund

En Tutellus empezamos nuestro fondo de inversión[2] hace unos meses. Nuestra intención es crear una cartera de inversión muy estable pero que también pueda sacar partido de grandes subidas del mercado, sobre todo las generadas por protocolos DeFi.

El objetivo de nuestro fondo es aportar a nuestros alumnos —y a todo aquel interesado en invertir, es un fondo abierto y público— una forma de estar expuesto a la tendencia DeFi a la vez que contar con un portfolio seguro y diversificado, con estrategias de rebalanceo. De hecho, para la v2 (versión 2) del protocolo de Melon se podrá también aplicar modelos de inversión más complejos, como añadir liquidez en pool o participar en estrategias de yield farming. Esto nos permitirá ofrecer un portfolio con mejor rendimiento e, incluso, minimizar el riesgo de solo hacer holding de criptoactivos.

Figura 123. Rentabilidad y métricas principales del Tutellus Fund en Melon

Empezamos el Tutellus Fund a finales de octubre de 2020, y desde entonces la rentabilidad obtenida ha sido del 20,33 %, consiguiendo un 0,24 % en ese mes y un 20,03 % en noviembre. Hoy, el fondo acumula una pequeña cantidad de 1463 USD y un precio por acción del fondo de 467,085 USD.

Hoy en día, Melon tan solo nos permite generar un portfolio diversificado, aunque no podemos aprovechar nuestros conocimientos en estrategias de inversión relacionadas con la creación de pool o yield farming. No obstante, en las próximas versiones podremos generar portfolios más sólidos y con mucho más rendimiento gracias a la posibilidad de aplicar estrategias con yields optimizados en el pool.

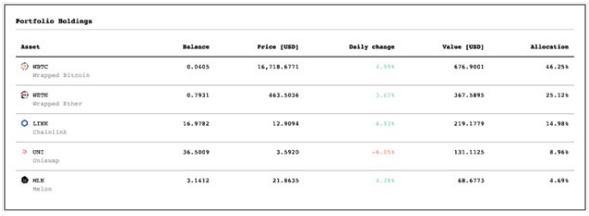


Figura 124. Estructura de la cartera del Tutellus Fund en Melon

En el momento de escribir estas líneas, el portfolio actual es el siguiente: WBTC (46,25 %), WETH (25,12 %), LINK (14,98 %), UNI (8,96 %) y MELON (4,69 %). A medida que podamos diversificar más y adoptar estrategias más complejas, podremos mejorar el fondo y ofrecer así una forma fácil y accesible a todos los inversores para participar de forma segura en el cambiante mundo DeFi, reduciendo también exposiciones en el momento de grandes pérdidas.

2. https://2tel.us/35CdH10

# 21. Protocolos para gestión de fondos: Set Protocol

## 21.1. Funcionamiento del protocolo

Set es otro proyecto interesante relacionado con el mundo del asset management, aunque ofrece algo diferente a Melon.

Set es un protocolo que te facilita la compra y creación de los set tokens. Estos son una tokenización de canastas de activos que no solo pueden tener portfolios diversos (en cuanto a número de activos) sino también incluyen estrategias de rebalanceo y de trading automatizadas. Es decir, un token set no solo te aporta un management y un rebalanceo automático, sino que además te permite adoptar estrategias de trading de tu portfolio de forma automatizada. De aquí el nombre: strategy enabled tokens (SET).

Dentro del protocolo hay muchos tipos de set tokens en los que invertir. Para saber qué set encaja mejor con el tipo de inversión que buscas, debes fijarte en las variables: el número de assets que habrá en la canasta, si quieres que esa canasta además genere intereses y si tu sentimiento de mercado es muy alcista, alcista, neutral, bajista o muy bajista. En función de estas variables, podrás seleccionar el token set que se adapte mejor a ti: cada set representa un portafolio de activos que, además, cuenta con estrategias de management, rebalanceo y trading. Dichas estrategias están programadas en el smart contract, por lo que no dependen de ningún gestor de fondos.

Por último, existen dos grandes tipos de set tokens: aquellos que tokenizan una estrategia de trading algorítmico que permite gestionar tus activos de forma automática 24/7 (son los set robo), y los social trading set, que te permiten copiar estrategias de traders especializados.

Aunque los rendimientos de algunos set han sido muy positivos, e incluso ha habido algunos que han superado el mercado, hay que usarlos con responsabilidad. Como dice el dicho, los resultados del pasado no indican resultados en el futuro.

## 21.2. Ejemplos de set tokens

**1. DeFi Pulse Index**

Este token set representa la tokenización de una cartera de inversión en protocolos DeFi diseñada por DeFiPulse, la web de referencia para medir la evolución del sector DeFi. En este caso, el token set solo tokeniza una canasta de activos sin que estos generen intereses ni tengan estrategias de trading.

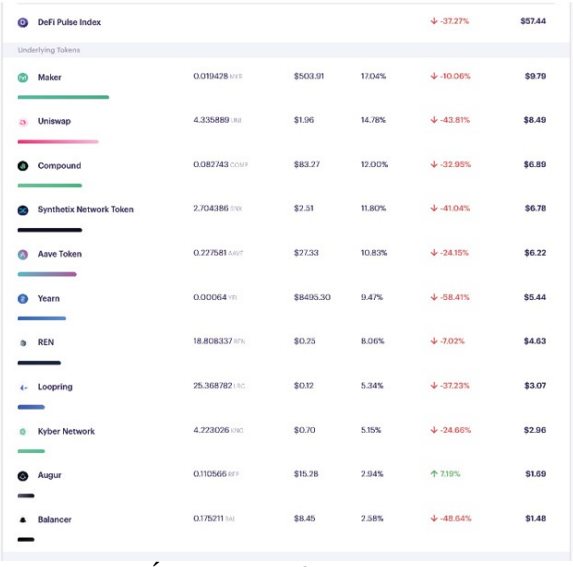


Figura 125. Índice de Defipulse en Set protocol

## 2. Holistic BTC Set

Este token set es uno de los más interesantes, sobre todo si queremos aprovechar al máximo las subidas de Bitcoin y también minimizar al máximo las bajadas. El Holistic BTC Set representa una tokenización de una estrategia de trading que funciona de la siguiente manera: cuando el mercado es alcista y la línea de tendencia también lo es, la canasta de activos que representa el token set será 100 % bitcoin, pero cuando la línea de tendencia se rompe y pasa a ser bajista, el BTC disponible se va a vender progresivamente por cDAI. De esta forma, cuando el mercado sube aprovechamos al máximo la subida, pero cuando baja buscamos perder exposición de mercado y reducir nuestras pérdidas con una stablecoin que además nos genera un interés.

Este token también tiene su versión en ETH (Holistic ETH Set) donde la estrategia aplicada es exactamente la misma, pero cambia el activo subyacente. Ahora no usamos Bitcoin sino que usamos Ethereum.

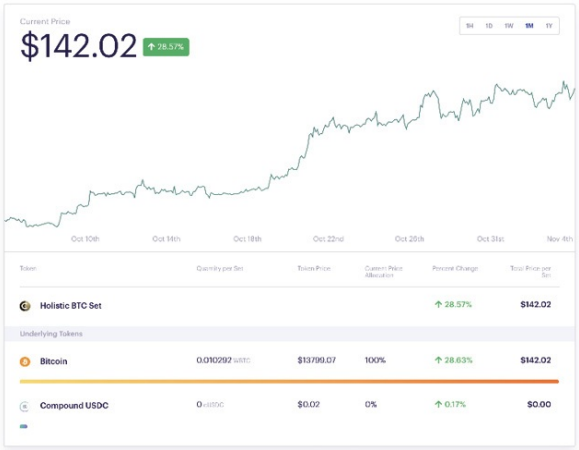



Figura 126. Índice de Holistic BTC en Set protocol

## 3. ETH 20 MA Crossover Yield Set II

Este set es una tokenización de una estrategia muy bajista. La idea del token es que la canasta a la que está representando va a mantener todo su capital en cDAI y va abriendo posiciones en ETH para sacar rendimiento de las tendencias.

Este token es para inversores con un sentimiento muy bajista, o cuando realmente el mercado está bajista: te permite mantenerte al margen de las caídas mientras además generas un interés, pero a la vez recapitalizarte aprovechando las pequeñas tendencias positivas que se van generando. El propio token automatiza la estrategia para sacar el máximo rendimiento durante mercados bajistas.

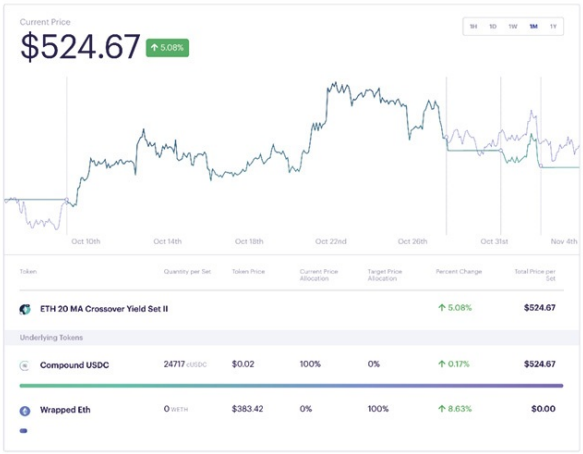



Figura 127. Índice de ETH 20 MA Crossover Yield en Set protocol

# 22. Mercados predictivos: Augur

## 22.1. Introducción a Augur

Augur es uno de los proyectos más antiguos de la blockchain de Ethereum: fue la primera ICO lanzada en Ethereum durante 2015, donde recaudaron unos 5 MUSD de dólares (al precio de ETH de aquel momento). Augur es un protocolo que permite la creación de mercados predictivos descentralizados y usa su token nativo REP como pilar del sistema. Sirve para la gobernanza del protocolo y como oráculo descentralizado encargado de dar el resultado final de cada mercado. Veámoslo con más calma.

Dentro de Augur yo puedo generar un mercado en el que cualquier persona pueda votar a través de la compra de acciones. Por ejemplo, voy a crear el siguiente mercado: «¿Llegará Bitcoin a los 100 000 USD en 2021?», donde las respuestas posibles son SÍ y NO. Cada respuesta será una acción, el precio de la cual empezará siempre a 0,50 USD por el SÍ y 0,50 USD por el NO. A medida que la gente vaya participando en este mercado, el precio de la acción se irá moviendo, ofreciendo una imagen clara de la probabilidad que un evento suceda. Eso sí, siempre basado en lo que cree la multitud.

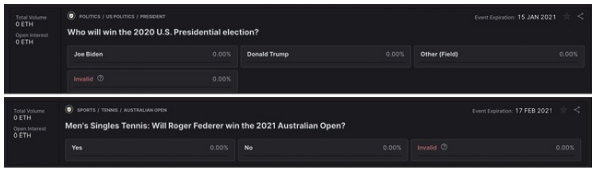


Figura 128. Ejemplo de mercado en Augur

## 22.2. Ejemplo en Augur: un partido Barça-Madrid

Pongamos que soy una persona amante del fútbol español, sigo la Liga y la Champions y no me pierdo ningún partido. En mi opinión, está clarísimo que el Barça va a ganar al Madrid, así que me dirijo a Augur para poder comprar acciones a favor del Barça. El mercado ya está creado así que no hará falta que lo cree de cero.

A pesar de mi convencimiento, resulta que las acciones a favor del Barça están más baratas que a favor del Madrid, lo que significa que la mayoría de gente considera que el Madrid es el favorito. Al iniciar el partido, el Barça es el primero en anotar, sorprendiendo a la mayoría. Debido a esto, el mercado

reacciona, y ahora es la acción del Barça la más cara, ya que el sentimiento del mercado ha cambiado. En este momento los que han comprado la acción de Madrid siguen teniendo la opción de vender, una opción que ya no estará en el momento que acabe el partido.

Finalmente, el partido termina con una victoria del Barcelona. Es en ese momento cuando los token holders de REP van a actuar como oráculos descentralizados e informar al sistema del resultado final: se dará por bueno lo que vote la mayoría. Si alguien de los que ha votado ha intentado mentir y el sistema lo ha detectado porque su respuesta no coincide con la de la mayoría, pierde los tokens REP que ha usado para votar y se reparten entre los que han dado el resultado correcto. Estos, además, también se llevan las comisiones que ha recaudado el sistema. El mercado finalmente confirma que el Barcelona ha sido el ganador, así que reparte todo el dinero de las acciones a favor del Madrid entre todos los que hayan comprado acciones a favor del Barça.

Con todo ello, Augur es simplemente un protocolo descentralizado donde se pueden crear mercados sobre eventos futuros. En este mercado, yo puedo comprar acciones sobre lo que creo que va a pasar, y en caso de estar en lo cierto, llevarme unas ganancias. El resultado final de cada mercado lo determinarán los holders de REP, que están interesados en decir la verdad para llevarse las comisiones y para no dañar la reputación del protocolo y el valor de su token.

## 22.3. La sabiduría de la multitud

Lo mejor de los mercados de Augur no es que permiten ganar dinero a través de la especulación o servir como entretenimiento, sino que permite aprovechar la sabiduría de la multitud para crear un mercado predictivo completamente descentralizado.

Los mercados predictivos consisten en que la opinión de las masas puede dar una visión mucho más fiable de la realidad que un especialista. Este concepto no es nuevo; de hecho y por ejemplo, Google tiene una capacidad predictiva muy importante sugiriendo búsquedas en función precisamente de cómo usa la gente el servicio. Augur es la primera versión descentralizada en un mercado predictivo donde en un futuro podría servir como motor de búsqueda para determinar eventos futuros.

## 22.4. Augur, un seguro frente a imprevistos

En función de cómo evolucione el protocolo y el uso que de él se haga, también podría servir como una especie de garantía o seguro ante eventos no deseados. Por ejemplo, imagina que soy un granjero; si este año hay sequía, no voy a poder cultivar, y seguramente pasaré una etapa económica muy complicada. Podría crear un mercado en Augur sobre si habrá o no sequía y comprar acciones a favor del SÍ. Esta acción puede servir como seguro frente a este suceso, ya que es cierto que no podré cultivar nada, pero al mismo tiempo mis pérdidas se verán reducidas gracias a las acciones compradas en el mercado de Augur.

# 23. Protocolos de seguros: Nexus Mutual

## 23.1. Análisis del protocolo

Las compañías de seguros forman parte de una de las industrias más interesantes y también más reguladas del sector financiero. Estas empresas han existido desde hace siglos, aunque en los últimos años hemos visto cómo los primeros modelos basados en comunidades que acumulaban recursos para protegerse de los riesgos que los afectan se han convertido en una industria centralizada por enormes corporaciones.

De hecho, esta industria ha ido empeorando con el tiempo debido al aumento de costes y la reducción de la flexibilidad y la eficiencia. Ello se debe a la gran confianza que debemos depositar en tales entidades, y cómo esta confianza se soluciona a través de un proceso regulatorio muy exhaustivo que consigue «garantizar» confianza a un coste muy elevado; se estima que el 35 % de las primas de seguros se pierden en costes debido a las altas fricciones del sistema. Es decir, solo el 65 % de las primas se devuelven a los clientes a través de reclamaciones. El resto se pierde en distribución, gastos operativos (incluidos los regulatorios), costos de capital y ganancias.

Gracias a Blockchain, proyectos como Nexus Mutual han visto la posibilidad de recuperar los objetivos iniciales de las mutuas, donde todas las contribuciones son enteramente en beneficio de sus miembros. Este es un proyecto con un modelo complejo que, a pesar de considerarse un proyecto DeFi, no está completamente descentralizado. Para poder participar en el fondo de mutual, debes ser miembro, lo que requiere pasar por un proceso de verificación y pagar una comisión de 0,002 ETH. El protocolo está liderado por una empresa británica que cumple con las regulaciones necesarias para incluir «Mutual» en su nombre comercial y debe, por tanto, operar acorde con tales regulaciones. Por otro lado uno de sus objetivos es avanzar hacia la descentralización y ofrecer así a todos sus miembros una forma más simple, transparente, accesible y menos costosa la protección financiera contra sus riesgos.

Como hemos dicho, Nexus es una alternativa descentralizada a las compañías de seguros que usa Blockchain para crear una mutua (grupo que comparte los mismos riesgos) y así retornar la industria de los seguros a la gente.

Cualquiera puede ser miembro de la mutua, y de esta forma comprar contratos de cobertura para riesgos concretos (de momento, solo para bugs en los smart

contracts de algunos protocolos DeFi), además de poder participar en el sistema y beneficiarse de su modelo de incentivos. Este hecho es muy relevante, ya que debe procurar alinear los intereses de los miembros y asegurarse de que les obliga a mantener una visión a largo plazo.

## 23.2. Cubrirse de un bug con el protocolo

El primer paso es hacerte miembro de Nexus Mutual, pasando por un proceso de verificación que puede llegar a tardar de veinticuatro a cuarenta y ocho horas y pagar una pequeña comisión (de 0,002 ETH). Una vez verificado, ya eres miembro y puedes acceder a todos los servicios del protocolo.

Es posible crear una cobertura para cualquier smart contract en la red de Ethereum. La única condición es que este contrato de cobertura debe estar protegido con suficientes fondos para poder hacer frente al coste si realmente hay un bug. Los encargados de depositar este colateral son los holders del token NXM, que reciben un interés por aportar su capital como garantía. En función de la garantía, el tipo de interés que deberá pagar el usuario que quiera protegerse de un bug será más alto o más bajo. Esta cobertura tiene un tiempo de expiración, con un mínimo de treinta y un máximo de 365 días. En función de cuánto capital se quiera cubrir, del capital disponible puesto en garantía y del riesgo del protocolo, se hace un cálculo que determinará cuánto debe pagar el usuario para mantener esa posición de cobertura.

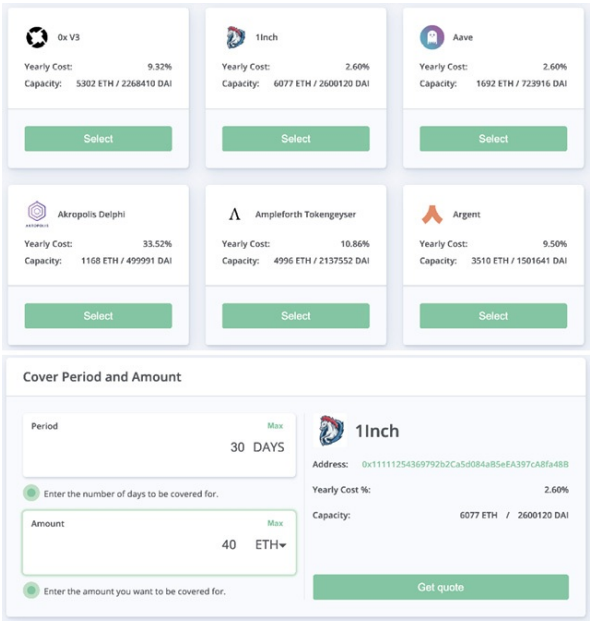



Figura 129. Seguros varios en Nexus Mutual y detalles del contrato de 1Inch

## 23.3. Proceso de reclamación de una cobertura

Imaginemos que hemos creado una posición de cobertura ante un posible bug en el smart contract del protocolo de 1Inch (un DEX o exchange descentralizado). ¿Cómo conseguimos hacer la reclamación?

El usuario debe pasar por el proceso de claiming, donde los miembros de Nexus Mutual votarán si se debe pagar la cobertura o no. Los primeros en votar son aquellos miembros que han depositado NXM para poder votar en este proceso. Para incentivar a estos a decir lo correcto, se premiará a aquellos que actúen justamente y penalizará a los que lo hagan de forma contraria. Cada vez que un miembro vota en contra, sus NXM quedan bloqueados durante noventa días, incentivando así a que tengan una visión a largo plazo. Esto es sumamente importante, ya que pagar una cobertura les penaliza, pero no hacerlo penaliza la imagen del protocolo. Un protocolo de seguros que no paga ningún seguro no tiene ningún valor.

Si los miembros con derecho pleno no acaban con una decisión votada por más del 70 %, todos los miembros de la red pasan a votar para que se pueda llegar a una decisión final.

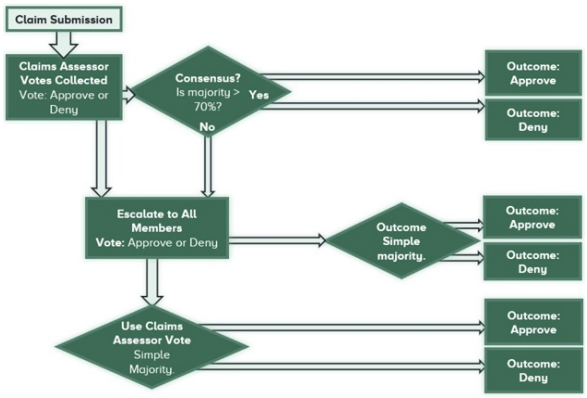



Figura 130. Proceso de reclamación de una cobertura de seguros en Nexus Mutual

## 23.4. Tokenomics del NXM token

Con lo visto hasta ahora podemos entender el funcionamiento base del protocolo: cómo este consigue dar cobertura a ciertos bugs en smart contracts de Ethereum, y qué proceso se requiere para poder reclamar tal cobertura.

Por último, indagaremos en el modelo del NXM token, ya que, a diferencia de muchos otros, este usa un sistema llamada continuos token model, lo que significa que su precio fluctúa no por especulación sino por adopción y

rendimiento del protocolo. El movimiento de precio sirve para incentivar la entrada de capital cuando no hay fondos suficientes para hacer frente a todos los contratos de cobertura, y sube de precio cuando hay mucho más capital del necesario.

Por otro lado, este token solo se puede comprar y vender en la plataforma de Nexus, tanto por el complejo modelo que sigue como porque solo los miembros que hayan pasado el proceso de verificación pueden tener acceso al token. Para aquellos que quieran formar parte del futuro crecimiento de Nexus Mutual existe la opción de comprar NXM token wrappeados en Uniswap (representaciones de NXM tokens reales).

Las variables que determinan el precio son las siguientes:

- **Minimum capital requirement (MCR).** Mínimo capital requerido para poder devolver con tranquilidad todas las reclamaciones.
- **Capital pool**. Total de fondos disponibles en la plataforma
- **Ratio MCR %.** Ratio entre los fondos necesarios y los fondos disponibles. Este valor tiene un efecto directo en el precio del token.

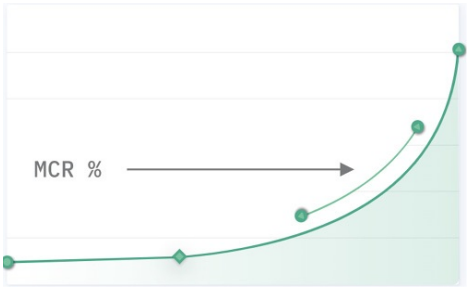



Figura 131. Evolución del ratio MCR en Nexus Mutual.

NXM sube de precio cuando:

- El fondo tiene dinero suficiente para hacer frente a las reclamaciones.
- Aumenta el número de coberturas y por tanto el capital mínimo disponible.
- El aumento del capital pool hace incrementar el valor del NXM token.

NXM baja de precio cuando:

- El capital pool se reduce, incentivando la entrada de más fondos para hacer frente a las reclamaciones de forma segura.
- Cuando se reduce el número de coberturas ya que hace falta menos capital para hacer frente a las reclamaciones.

El valor clave que determina el precio es la relación entre el capital necesario (MCR) y el capital disponible (capital pool). Si la relación entre estos dos

valores hace que la ratio MCR baje, el token baja de valor; si el ratio MCR sube, el token sube de valor.

Por tanto, a corto plazo el token facturará en función del ratio entre fondos necesarios y fondos disponibles, ahora bien, a largo plazo serán los fondos necesarios MCR que irán aumentando el valor del token de forma progresiva.

# 24. Protocolos de seguros: Opyn

Opyn es otro proyecto que pretende ofrecer seguros ante fallos de smart contracts o incluso altas volatilidades. Actualmente sus funciones de seguro son limitadas, ya que permiten protegerse ante fallos en Compound y grandes volatilidades o eventos como un flash crash en Uni, wBTC, YFI y DFI (Defi Pulse Index).

Los seguros de Opyn están 100 % garantizados, descentralizados y funcionan de forma automática. Esto lo consiguen gracias a la creación de opciones de call y put.

## 24.1. ¿Qué es un call/put?

Una opción es un derivado financiero que te permite crear opciones de call u opciones de put. Una call option representa el derecho, pero no la obligación, de comprar un asset concreto a un precio ya establecido durante un periodo determinado. En cambio, una put option te otorga el poder contrario: el derecho, pero no la obligación, de vender un activo específico a un precio concreto durante un periodo determinado.

Estos productos derivados son muy abundantes en las finanzas tradicionales; de hecho existen opciones en función de qué país los genere. Por ejemplo, las opciones derivadas generadas en Estados Unidos pueden ejecutarse en cualquier momento del periodo establecido; en cambio, en Europa debe ser en una fecha concreta.

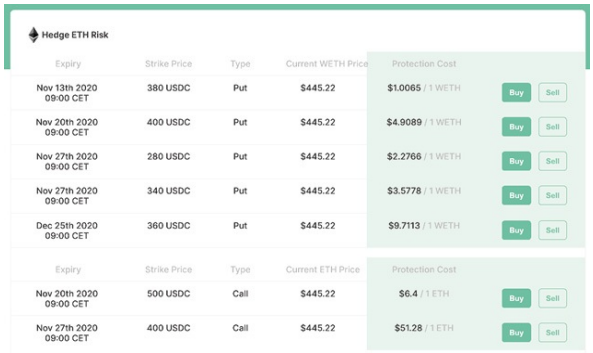


Figura 132. Detalle de coberturas de seguros en Opyn.

## 24.2. Funcionamiento de Opyn

El funcionamiento de Opyn es de lo más curioso ya que, a través de los oTokens Opyn, consigue tokenizar los propios seguros.

Por ejemplo, en el caso de que yo quisiera cubrirme de un fallo en el protocolo de Compound, podría comprar una opción put para poder vender mis cDAI a cambio de DAI en caso de que el protocolo fallara.

Por tanto, aquí vemos que, para que alguien pueda cubrirse comprando una opción put, debe haber alguien que genere una opción call y que esté dispuesto a asumir el riesgo a cambio de un interés. Esto es exactamente lo que hacen los generadores de los oTokens.

Depositando ETH a una ratio de colateralización del 160 %, tienes la opción de generar oTokens, que son tokenizaciones de seguros, ya que esos tokens están 100 % respaldados por un colateral. Esto, a cambio de generar estos tokens y venderlos en el mercado, lo que está haciendo es crear una call option para que alguien pueda comprarla y usarla como una put option.

Este protocolo es de lo más interesante en cuanto a rendimiento ya que los yields anuales pagados por depositar ETH son de los más altos de todo DeFi. Ahora bien, claro está que este interés generado no viene solo, ya que debes estar dispuesto a asumir el riesgo de tener que garantizar tus activos a terceros que hagan uso de la put option si el protocolo de Compound (en este caso) fallase. Lo interesante es que este fallo no solo tiene que ver con fallos del smart contract sino también con fallos financieros.

Otra estrategia interesante para los creadores de oTokens no es solo vender los tokens a aquellos que quieran cubrirse, sino añadir liquidez a un pool de Uniswap y así generar otra APR anual. Aunque el APR variará en el tiempo, puede llegar a ser muy rentable en función de la demanda de oTokens.

## 24.3. Diferencias con Nexus

Hay varias diferencias, pero me centraré en las más relevantes.

En primer lugar, Nexus ofrece cobertura en fallos de cualquier smart contract (con suficiente liquidez dentro de Nexus) y, en cambio, Opyn protege no solo de fallos en smart contracts sino de otros riesgos (de protocolos y tokens concretos).

La cobertura en Opyn no pasa por ninguna votación, sino que es automática y su liquidez está 100 % garantizada gracias a los dos participantes: los que depositan el colateral y generan los oTokens y los que hacen uso de ellos.

Por último, y seguramente sea la diferencia más interesante, es el coste de crear una posición de cobertura para un protocolo concreto. En Nexus esto se

determina a través de un algoritmo de precio que tiene en cuenta tanto el riesgo y el capital disponible para hacer frente a las coberturas. En Opyn, en cambio, se determina en el propio mercado por oferta y demanda, sobre todo debido a que estos token están disponibles en Uniswap.

# 25. Protocolos de margin trading (dYdX)

## 25.1. Análisis del protocolo

El protocolo de dYdX nace con el objetivo de solucionar la falta de herramientas de trading avanzadas disponibles en un ecosistema descentralizado. En el mundo cripto, este tipo de operaciones como margin trading o derivados perpetuos no han parado de crecer, pero tan solo han estado disponibles dentro de plataformas centralizadas como Binance, Kraken o Bitmex. dYdX pretende ofrecer estos productos a través de su exchange descentralizado, y aunque puede parecer limitado por el número de assets disponibles, realmente estamos hablando de un gran paso para el ecosistema DeFi.

En definitiva, dYdX es un protocolo que permite servicios de lending y borrowing a un tipo de interés determinado dinámicamente por la oferta y la demanda (similar a Compound y Aave,) pero que además consta de un exchange descentralizado donde operar con operaciones spot, de margin y con perpetuos.

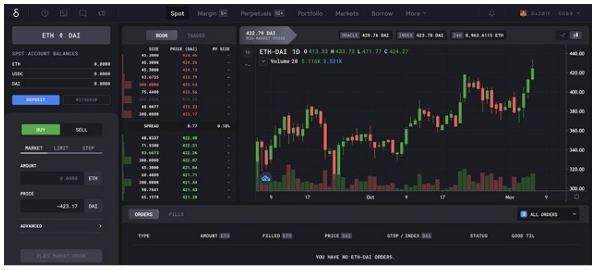


Figura 133. Detalle de la interfaz del protocolo dYdX.

## 25.2. Funcionalidad básica como DEX

A diferencia de otros DEX que hemos visto que funcionan como pools de liquidez, dYdX usa como base el protocolo 0x Relay para permitir un intercambio directo (atómico) entre diferentes usuarios. Es decir, para hacer uso de él debemos depositar un colateral en la plataforma y este después va a usar un libro de órdenes off chain sin poder de custodia para ofrecer estos intercambios. Aquí podemos ver que dYdX no ha completado aún su fase de descentralización ya que depende de este libro de órdenes off chain para ofrecer los intercambios. Una ventaja es que no hace falta pagar ningún coste de gas dentro de la plataforma, pero, por contra, existe la posibilidad de censura por parte del equipo del proyecto. A pesar de esto, los smart contracts hacen que los fondos sean no

custodiados, así que nunca tendrán control sobre los fondos, tan solo podrán censurar ciertas acciones.

Este exchange descentralizado permite operar de tres formas distintas: con operaciones spot, operaciones de margin trading y con productos perpetuos.

## 25.3. Funcionalidad de Spot Trading

Este servicio es la funcionalidad más simple de un exchange, ya que permite intercambiar tokens de forma directa con otros usuarios usando como base protocolos como 0x Relay. Los pares disponibles son ETH-DAI, ETH-USDC y DAI-USDC y permite usar opciones de compra como market orders (acción de compra o venta precio de mercado), limit orders (acciones de compra o venta a precios determinados) y stop orders (acciones de cierre de operaciones).

Antes de usar esta funcionalidad debemos depositar los fondos en dYdX para después tradearlos.

## 25.4. Funcionalidad de margin trading

Este es el servicio estrella del protocolo, ya que permite a sus usuarios operar en los mercados con un apalancamiento de hasta un x5 de forma totalmente descentralizada.

En las finanzas tradicionales, los trades de margin se llevan a cabo gracias a un préstamo de la casa (entidad centralizada) para que puedas hacer operaciones con más dinero del que dispones y así aumentar tus posibles beneficios (pero también aumentar tus posibles pérdidas).

El margin es el colateral que usa el trader para poder tomar prestado, ya que estos fondos deberán devolverse con un tipo de interés. Entonces, el apalancamiento es el aumento del poder de compra sobre venta (lo que equivale también a un aumento de riesgo) que depende directamente del margin usado como colateral.

Por ejemplo, si mi portfolio consta de 1000 USD y quiero hacer una operación apalancada a un 5x, mi depósito de margin va a ser 100 USD, poniendo en riesgo el 10 % de la cuenta. Si quiero tener un apalancamiento de 2x, debo depositar como margin 500 USD, el 50 % de la cuenta. Cuanto más leverage, menos capital necesito, pero también estoy más cerca del precio de liquidación. Es decir, que con caídas del precio mucho más pequeñas puedo ver cómo mi capital depositado desaparece.

En dYdX, este dinero prestado que usamos para apalancarse proviene de los usuarios que han depositado sus fondos para generar intereses, ya que esos fondos los podrán utilizar otros usuarios para tomar prestado y para hacer trading apalancado. Es por eso que el precio de liquidación y el colateral siempre van a ser altos, para minimizar o anular el riesgo que asumen los lenders. Este sistema es el usado en Compound o Aave, en los que existe un pool compartido desde donde todos pueden entrar y salir en cada momento y que en función de la relación entre los fondos depositados y los fondos prestados se determinará un tipo de interés que beneficiará directamente a los lenders.

A través de este dinero que se toma prestado usando un colateral como garantía, existen dos tipos de margin trades:

- **Isolated margin trade.** Este es un tipo de trade en el que solo se pone en riesgo un total determinado y no toda la cuenta. Yo puede tener depositado en el protocolo 1000 USD pero usar solo 100 USD para mi trade. Estoy aislando el capital que quiero arriesgar para cada operación.
- **Cross margin trade.** Este tipo de trade usa toda la cuenta como colateral. El resultado es que es mucho más flexible y permite a los traders sacar el máximo provecho de estos productos. Por otro lado, el riesgo es mucho mayor, ya que a pesar de que el precio de liquidación será más bajo porque hay más colateral, si este se liquida, el trader perderá todo el capital depositado en el protocolo.

Algo asombroso en dYdX es que el capital depositado como colateral generará intereses en todo momento, ya que estará depositado en el pool compartido desde donde lenders y borrowers interactúan.

## 25.5. Funcionalidad de productos perpetuos

Los perpetuos son productos sintéticos muy similares a los futuros, aunque se diferencian en que no tienen una fecha de liquidación. Mientras el colateral aguante, el producto sintético puede seguir operando.

Este es un servicio integrado muy recientemente en dYdX y en el que se mantienen muchas expectativas, ya que es la forma más eficiente para ganar exposición al precio de ETH o BTC de forma descentralizada. Esto último es relevante sobre todo por las sanciones y problemas que están teniendo algunos exchanges centralizados. Por ejemplo, Bitmex, el exchange más relevante en operaciones apalancadas, está pasando por un mal momento por cuestiones

regulatorias. Este duro golpe puede ser un gran disparador para que protocolos como dYdX empiecen a concentrar la liquidez que hasta ahora estaba depositada en estas plataformas centralizadas.

El contrato de perpetuos es un producto complejo de por sí, y lo es aún más cuando se crea en un ecosistema descentralizado. Básicamente, usa oráculos para determinar el precio real de los activos y de esta forma calcula el funding rate: un tipo de interés que se paga entre las posiciones apalancadas a largo y las posiciones apalancadas a corto para mantener el precio del contrato lo más cercano al precio real del activo.

El apalancamiento asumido en estos productos será también proporcional al colateral depositado, llegando a ser de hasta un 10x. Hay muchas estrategias de inversión que usan los perpetuos, ya sea para cubrir riesgos, para generar ingresos pequeños gracias al fund rate o simplemente por motivos especulativos con altos rewards (pero también altísimos riesgos).

## 25.6. Funcionalidad de lending y borrowing

Como hemos visto, dYdX también permite depositar y tomar fondos prestados. La diferencia es que estos fondos depositados no solo se usan para préstamos normales, sino también para poder abrir posiciones apalancadas.

Esto hace que depositar activos en dYdX sea muy atractivo, ya que abrir posiciones apalancadas suele ser algo costoso. Esto permite a los lenders obtener unos buenos rendimientos anuales.

Los depósitos se realizan en dos tipos de cuentas: las de margin o las de spot, en función de qué servicio de trading queramos usar.

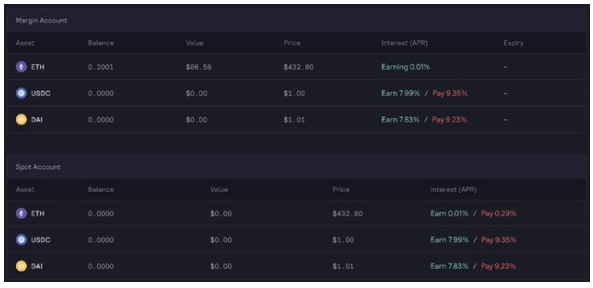


Figura 134. Detalle del mercado de lending en dYdX

# 26. Protocolos para assets sintéticos: Synthetix

## 26.1. La gran disrupción de Synthetix

El último protocolo que analizaremos es Synthetix. Lo he dejado para el final, primero, por su complejidad, pero también por lo innovador que es.

Actualmente gran parte de los protocolos DeFi ofrecen réplicas adaptadas a Blockchain de productos financieros que ya existen en las finanzas tradicionales. Aunque teniendo en cuenta que Blockchain es una plataforma global, abierta a todo el mundo y capaz de cargar con dinero programable, no tengo duda de que **en menos de lo que esperamos empezaremos a ver protocolos DeFi que presentarán instrumentos completamente únicos y exclusivos de Blockchain**. La aparición de estos protocolos podría ser también uno de los grandes triggers de adopción, ya que solo estarán disponibles a través de Blockchain.

Uno de estos instrumentos serán los assets sintéticos, los cuales tienen un potencial enorme. Es por esto que nos dedicaremos a comprender cómo funciona Synthetix Protocol, uno de los primeros en intentar disrumpir el mercado financiero más grande de todos: el de los derivados. Existen tres tipos de instrumentos financieros:

- Los activos basados en deuda, como los bonos.
- Los que representan equity, como las acciones.
- Los productos derivados. Estos representan el segmento más grande y extenso del mundo financiero. Protocolos DeFi enfocados en este segmento pueden realmente ser revolucionarios.

## 26.2. El mercado de los derivados y los assets sintéticos

Un producto derivado consiste en un asset financiero que en sí mismo es un contrato entre dos o más participantes —los cuales toman posiciones a corto o a largo para dicho asset— y que copia el movimiento de precio de un activo subyacente. El derivado (por ejemplo, puede representar el movimiento de precio de cinco empresas tecnológicas) no contiene en sí mismo acciones de tales empresas, simplemente imita el movimiento de precio para permitir exposición en dichos assets sin realmente comprarlos. Por tanto, un producto

derivado debe mantener un colateral que respalde su valor (ya que no mantiene la propiedad del subyacente que representa), que podrá ser cualquier tipo de activo, o incluso diferentes activos a la vez.

| Category | Value ($ Billions, USD) | Source |
|---|---|---|
| Silver | $44 | World Silver Survey 2019 |
| Cryptocurrencies | $244 | CoinMarketCap |
| Global Military Spending | $1,782 | World Bank |
| U.S. Federal Deficit (FY 2020) | $3,800 | U.S. CBO (Projected, as of April 2020) |
| Coins & Bank Notes | $6,662 | BIS |
| Fed's Balance Sheet | $7,037 | U.S. Federal Reserve |
| The World's Billionaires | $8,000 | Forbes |
| Gold | $10,891 | World Gold Council (2020) |
| The Fortune 500 | $22,600 | Fortune 500 (2019 list) |
| Stock Markets | $89,475 | WFE (April 2020) |
| Narrow Money Supply | $35,183 | CIA Factbook |
| Broad Money Supply | $95,698 | CIA Factbook |
| Global Debt | $252,600 | IIF Debt Monitor |
| Global Real Estate | $280,600 | Savills Global Research (2018 est.) |
| Global Wealth | $360,603 | Credit Suisse |
| Derivatives (Market Value) | $11,600 | BIS (Dec 2019) |
| Derivatives (Notional Value) | $558,500 | BIS (Dec 2019) |
| Derivatives (Notional Value - High end) | $1,000,000 | Various sources (Unofficial) |

Figura 135. Valor total por mercado. El mercado de derivados asciende a un cuatrillón USD

Así que, básicamente, **un asset sintético vendría a ser la tokenización de uno de estos instrumentos financieros.** Es decir, un token que actúa como representación digital única de un derivado, lo que a su vez lo convierte en un instrumento completamente nuevo y con multitud de ventajas:

## 26.3. Ventajas de un token sintético

- Creación sin restricciones. Gracias a Blockchain puedes crear tokens sintéticos de forma descentralizada y sin depender de ningún intermediario.
- Facilidad de acceso a estos productos y simplicidad para transferirlos. Esto los convierte en instrumentos mucho más líquidos (ya que dependerían únicamente de la creación de pools de liquidez de dichos assets) y que al ser abiertos no están restringidos a inversores sofisticados, sino a cualquiera que quiera comprarlos.
- Exposición en precios de activos reales dentro una blockchain. Blockchain nos permite trabajar con productos financieros con ventajas únicas, como la descentralización y la imposibilidad de censura. Con assets sintéticos podemos exponernos a movimientos del precio de activos reales manteniendo estas características únicas de una blockchain.
- Estos tipos de tokens pueden presentar una solución al estancamiento tecnológico en cuanto a los cross swap, ya que podemos mantener posiciones en Ethereum de tokens no compatibles, como Bitcoin u otros.

Básicamente los tokens sintéticos pueden permitirnos introducir activos reales en una blockchain para que traders e inversores puedan estar expuestos a cambios en los valores de tales activos sin realmente comprarlos, manteniendo así las maravillosas ventajas de una blockchain. Cualquier persona podrá comprar exposición de precio de la mayoría de activos de forma descentralizada, e incluso después podrá usar ese token como colateral en protocolos como Maker, Compound o Aave. Estos tokens pueden representar desde commodities, equity e incluso instrumentos de deuda como los bonos.

Este modelo, aunque interesante y entusiasmante, sigue siendo un resultado lógico si pensamos qué nos podrían permitir los assets sintéticos. Pero podemos ir más allá: imagina un nuevo tipo de instrumento que te permita especular en mercados culturales, tokens de marcas personales o incluso cambios en las condiciones climatológicas.

**Todo es tokenizable a través de un asset sintético.**

Podríamos invertir en el rendimiento de Leo Messi a través de sus tokens sintéticos (sin necesidad de haber realizado un contrato real de cesión de derechos con el deportista), cuyo precio estará determinado por el rendimiento del jugador.

El potencial es ilimitado; solo pensando en que el volumen anual tradeado en el mercado de equity superó los 32,5 trillones USD, y que todos estos activos pueden ser reemplazados por su versión sintética en una blockchain para ofrecer aún más versatilidad en el trading, es increíble. Este activo tokenizado pasaría a ser global, abierto a todo el mundo y con liquidez disponible gracias a pools globales de liquidez, o incluso con liquidez ilimitada como sucede en Synthetix.

## 26.4. Análisis del protocolo de Synthetix

Una vez analizado y entendido qué son los instrumentos derivados, podemos ya meternos de lleno en Synthetix. Sin duda, un proyecto que vale la pena comprender, ya que incluso en una versión muy inicial y con mucho trabajo por hacer, su propuesta de valor en DeFi es clara, lo que le ha permitido acumular un total de 730 MUSD en el momento de escribir estas líneas, ocupando así la sexta posición por dinero bloqueado en DeFipulse.

| DEFI PULSE | Name | Chain | Category | Locked (USD) ▼ | 1 Day % |
|---|---|---|---|---|---|
| 1. | Aave | Ethereum | Lending | $1.48B | -3.77% |
| 2. | Maker | Ethereum | Lending | $1.26B | 1.19% |
| 3. | Curve Finance | Ethereum | DEXes | $1.02B | 0.29% |
| 4. | Uniswap | Ethereum | DEXes | $904.0M | -8.36% |
| 5. | Balancer | Ethereum | DEXes | $769.0M | 18.88% |
| 6. | yearn.finance | Ethereum | Assets | $734.9M | -3.23% |
| 7. | Synthetix | Ethereum | Derivatives | $718.0M | -4.59% |
| 8. | Compound | Ethereum | Lending | $672.5M | 5.37% |

Figura 136. Ranking DeFipulse, con Synthetix en 7ª posición (septiembre 2020)

Synthetix es un protocolo que te permite acceder a assets sintéticos (llamados synths) y después tradear con ellos en su plataforma de exchange. Los synths son tokens ERC20 con los que puedes tener exposición de precio de otros assets reales. El protocolo, para poder emitir estos tokens sintéticos que imitan el valor de otros activos a través de price feeds de oráculos descentralizados, usa un colateral para mantener sus precios. Los responsables de dar este colateral son los SNX holders, el token de gobernanza del protocolo que además sirve para ponerlo en marcha, ya que es a través de este con el que se pueden llegar a crear los synths.

Como veremos, los stakers (SNX holders) asumen el riesgo del derivado, ya que si los activos subyacentes aumentan en valor, ellos deberán responder asumiendo más deuda de la que inicialmente tenían, y por esta razón reciben grandes recompensas por stakear. Primero reciben todas las fees generadas entre el intercambio de synths dentro del Synthetix Exchange (0,3 % por cada operación) y, segundo, reciben unos rewards en SNX gracias a una política inflacionaria enfocada a incentivar a los stakers. Por tanto, podemos decir que el valor del token SNX está directamente relacionado con el valor creado y la usabilidad del protocolo. Como resultado, el colateral permite la creación de unos assets sintéticos que son intercambiables al instante, sin fricción y sin ningún tipo de slippage entre ellos. No cambias el colateral, simplemente quemas y creas nuevos tokens, eliminando así el problema de la liquidez y del price slippage propio de los pools con AMM disponibles para swaps.

Parece confuso, así que mejor vamos por partes.

## 26.5. Derivative contract & debt pool

Hemos dicho que un derivado viene a ser un contrato entre dos a varios participantes que compiten entre ellos, unos a corto y otros a largo. En Synthetix los participantes del contrato son los SNX holders y los SNX stakers.

Pongamos un ejemplo. Yo soy poseedor de SNX tokens, y, como tal, estoy incentivado a stakear y ofrecer como colateral mis tokens para poder ganar fees y rewards, e incluso beneficiarme de la revalorización de los synths, aunque esto lo veremos más adelante. Una vez he puesto mis SNX como colateral, el protocolo va a generar sUSD, que representarán mi deuda total con el sistema (para poder retirar mi colateral). ¿Por qué deuda total? Porque solo podré retirarme del sistema y recuperar mis SNX cuando devuelva el total de sUSD que he generado. Algo similar a Maker con DAI.

La deuda que he generado se añade al total debt pool, representado en USD y responsable de calcular en cada momento la deuda que tienen los SNX stakers con el protocolo. Lo curioso es que esta deuda puede variar, es decir, puede ser que tengas que devolver más de lo que retiraste para poder salir del sistema. Esto sucede porque, cuando generas sUSD a través de tu colateral y este pasa a conformar tus obligaciones de deuda, tienes tres opciones: holdearlo, swapearlo por activos reales como ETH o swapearlo por otros synths. Los otros synths como sBTC o sETH también están respaldados por el mismo colateral, lo que quiere decir que si BTC sube un 10 %, los traders que estén holdeando los sBTC podrán hacer líquidas sus ganancias gracias a que la deuda total del pool habrá aumentado.

La deuda total está representada en sUSD, pero como mi sUSD es intercambiable por otros assets como sBTC, y además todos los synths comparten el mismo colateral, si estos synths suben de valor, la deuda total del sistema aumentará también. Esto significa que si quiero salir de sistema, la cantidad de sUSD a devolver puede variar en función de las fluctuaciones de precio de los synths.

## 26.6. Staking SNX como colateral

Podemos ver que es importante mantener una ratio de colateralización segura; así, en caso de grandes subidas, los traders pueden asegurarse de que podrán recaudar sus ganancias. Si esto no fuera así, la confianza con los sTokens sería muy baja, y no habría incentivo en crear pools de liquidez entre tokens sintéticos y tokens reales como sucede en Curve, Uniswap, Sushiswap o Balancer.

Es por esto que el sistema incentiva a los stakers a mantener una **ratio de colateralización del 750 %** (si no es así, estos no tienen derecho a reclamar fees y rewards). Esto hace que semanalmente, en el momento de recibir los incentivos, los stakers paguen parte de su deuda o aumenten la cantidad de SNX

para poder aumentar su ratio de colateralización y tener derecho a recibir los incentivos. El mecanismo de incentivos ayuda al protocolo a estar siempre en una ratio de colateralización muy alta, haciendo del protocolo un sistema muy seguro y confiable. En parte esto explica que repentinamente, en protocolos de lending, el APR de SNX se dispare incluso a valores del 60 % anual.

Por otro lado, estar en una c-ratio inferior del 750 % no es motivo de liquidación, simplemente significa que no tienes derecho a recibir tus recompensas por ser staker. Las liquidaciones solo entran en vigor cuando tu c-ratio es inferior al 200 %

Por último, como todos los synths están colateralizados por el mismo pool de deuda, y en consecuencia esta deuda total a la que deben hacer frente los stakers de SNX puede cambiar en función de las variaciones de precio de los assets reales, los swaps entre ellos son simples. Swapear un sBTC por un sETH es muy fácil: el protocolo simplemente cambia la representación de esa cantidad de deuda; quema los sBTC y genera sETH, nada ha cambiado dentro del pool de deuda. Esto aporta unos beneficios muy atractivos para los traders. Los problemas habituales de AMM como Uniswap —la falta de liquidez y el price slippage— no existen dentro del Synthetix Exchange. Esto solo nos afecta si queremos swapear sETH por ETH real, entonces sí deberemos usar pools de liquidez en Uniswap u otros protocolos.

Podríamos ver a los stakers como una especie de compañía de seguros. Ellos van recibiendo fees y rewards muy atractivos, pero alguna vez se ven obligados a pagar las ganancias de los traders de synths.

## 26.7. Pool neutral (neutralizar la debt pool)

Actualmente existen tokens sintéticos para commodities (oro o plata), criptoactivos (sETH o sBTC), criptoactivos a la baja (iETH o iBTC), monedas convencionales (sUSD) y algunos índices de un conjunto de tokens DeFi y de un conjunto de tokens CEX (exchanges centralizados).

Esto significa que podría ser que la deuda del pool se mantuviera estable. Imagina que hay 1000 USD en sUSD creados, y estos se usan para generar 500 USD de sETH y otros 500 USD de iETH. Como son posiciones contrarias, la deuda total del pool se mantendrá estable. Este tipo de posiciones hacen que el riesgo de los SNX stakers baje.

| | Step | Alice | Bob | Debt Pool |
|---|---|---|---|---|
| 1. | Starting sUSD | 50,000 | 50,000 | 100,000 |
| 2. | Debt Pool Percentage | 50% | 50% | |
| 3. | Alice and Bob both buy sBTC | 50,000 (in sBTC) | 50,000 (in sBTC) | 100,000 |
| 4. | sBTC goes up 50% | 75,000 | 75,000 | 150,000 |
| 5. | Asset Value | 75,000 | 75,000 | 150,000 |
| 6. | Debt Owed | 75,500 | 75,500 | 125,000 |
| 7. | Profit or Loss (Asset minus Debt) | 0 | 0 | |

Figura 137. Neutralización del debt pool en Synthetix

## 26.8. Un ejemplo real de funcionamiento en Synthetix

Recordemos: los synths son contratos de derivados dentro del protocolo de Synthetix, deployados sobre la red de Ethereum. Estos tokens siguen el movimiento de precio de sus activos subyacentes. Para Bitcoin el sBTC y para Ether el sETH, con algunas opciones para ir a corto como sería el iBTC o el iETH (los traders sacan rendimiento cuando el precio baja).

Para generar estos tokens necesitamos tener un colateral aportado a través de SNX por parte de los stakeholders del token.

Imaginemos que Alice tiene 7500 USD de tokens SNX. Ella quiere poner sus tokens en stake para beneficiarse de las fees/rewards del protocolo a pesar del riesgo que supone, ya que ahora va ser propietaria y responsable de una parte de la debt pool de Synthetix. Alice pone en stake 7500 USD y mintea 1000 USD en sUSD con el que puede tradear o holdear. De este modo, su c-ratio es del 750 % y por tanto tiene ahora derecho a recibir retribuciones.

A partir de ese momento, Alice puede ver su c-ratio subir o bajar en función de ciertas variables. Por ejemplo, si el valor del token SNX aumenta, su c-ratio aumentará, pero sucederá lo contrario si el valor se reduce. Por otro lado, si los traders de synths han obtenido rentabilidad debido a que los precios de los activos reales han subido, la deuda total del protocolo a la que los SNX stakers hacen frente con su colateral habrá aumentado; por tanto, Alice verá cómo sus obligaciones de deuda han subido, o, lo que es lo mismo, su c-ratio ha bajado. Para poder recuperar su posición de 750 % de colateral, deberá aumentar la cantidad de SNX stakeado o comprar sUSD para reducir su deuda. Este caso podría darse también de forma contraria: los synths han visto su valor total reducido, y en ese momento la c-ratio de los stakers habrá subido, ya que la debt

pool se habrá reducido y por tanto las obligaciones de deuda de cada uno habrán bajado también.

También es posible que Alice haya tomado una posición para cubrirse del riesgo. Imaginemos que con sus 1000 USD de sUSD minteados al inicio, Alice compró sBTC. Si este ha subido un 10 %, Alice, al swapear en el exchange de Synthetic (con zero slippage y máxima liquidez) sus sBTC por sUSD, habrá compensado el aumento de sus obligaciones de deuda. Aquí cada staker puede adoptar estrategias muy diferentes para minimizar el riesgo.

Veámoslo en números reales: si Alice ha minteado 1000 USD de sUSD y en total existe 100 000 USD en SNX, Alice es responsable del 1 % de la deuda. Si después de un día de intensa volatilidad, los SNX en conjunto han tenido una revalorización del 100 %, ahora la deuda total es de 200 000 USD y, por tanto, el 1 % de Alice ha aumentado a 2 000 USD. Como hemos dicho, Alice podría haber mitigado el riesgo swapeando sus sUSD por algún otro token como sBTC. Si el sBTC ha tenido un aumento del 120 %, Alice no solo habrá recuperado su obligación de deuda inicial (1000 USD), sino que incluso la habrá reducido.

| | Step | Alice | Bob | Debt Pool |
|---|---|---|---|---|
| 1. | Starting sUSD | 50,000 | 50,000 | 100,000 |
| 2. | Debt Pool Percentage | 50% | 50% | |
| 3. | Alice buys sBTC | 50,000 (in sBTC) | 50,000 (in sUSD) | 100,000 |
| 4. | sBTC goes up 50% | 75,000 | 50,000 | 125,000 |
| 5. | Asset Value | 75,000 | 50,000 | 125,000 |
| 6. | Debt Owed | 62,500 | 62,500 | 125,000 |
| 7. | Profit or Loss (Asset minus Debt) | +12,500 | -12,500 | |

Figura 138. Hedging strategy en Synthetix

Como resumen de todo el ecosistema podemos ver su funcionamiento a través de este gráfico.

Los SNX stakers dejan sus SNX como colateral y mintean sUSD, que luego pueden holdear, vender al mercado a través de pools o cambiar por otros SNX.

Estos nuevos SNX se van a usar en Synthetix Exchange, donde el protocolo va a generar fees que van a recibir los SNX stakers.

El mercado determinará si el valor de los SNX sube o baja. Si baja, la deuda de los SNX stakers bajará; si sube, aumentará.

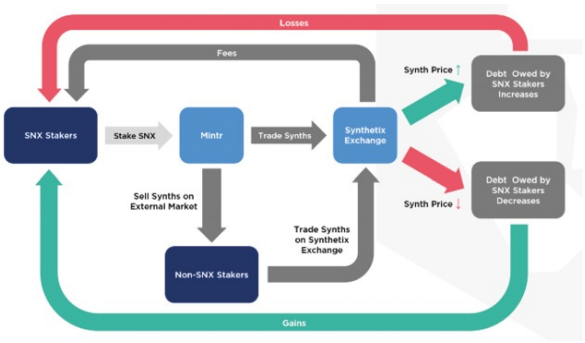


Figura 139. Modelo tokenómico de Synthetix

# 26.9. Política inflacionaria en Synthetix

En los últimos meses, los rendimientos de los stakers han sido muy positivos, y seguramente lo sean más cuando el volumen tradeado en el exchange de Synthetix aumente. Como actualmente el volumen no es muy elevado, el protocolo ha adoptado una política inflacionaria para poder compensar con SNX tokens a los stakers y asegurar que estén bien incentivados; primero, para ofrecer liquidez para generar SNX; y segundo, para que constantemente quieran mantener una c-ratio superior al 750 % y asegurarse las retribuciones.

Esta política inflacionaria empezó en marzo de 2018 y terminará en agosto de 2023. El total supply de SNX aumentará un 40 %, de 184 a 260 millones. A partir de ese momento habrá una inflación anual del 2,5 % (a no ser que haya un cambio por votaciones en el sistema de gobernanza). Otra aclaración: estos rewards quedan bloqueados en escrow durante un año, para que no se vendan una vez se reciban. El sistema de incentivos diseñado permite crear una comunidad que busque beneficiarse del protocolo a largo plazo. Esto les convierte en believers, lo que da más fuerza y seguridad a Synthetix.

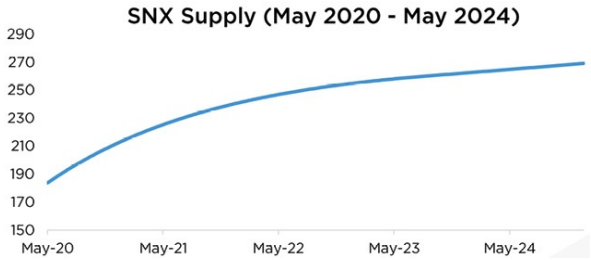


Figura 140. Política inflacionaria SNX Token

Este sistema inflacionario, aunque quizás conflictivo, ha resultado ser de gran ayuda para el protocolo. Recordemos que, sin colateral, los SNX no pueden crearse, por lo que había una gran necesidad de liquidez inicial. También una prioridad era mantener el SNX token como colateral para convertirlo en una

pieza clave del protocolo y ofrecerlo como token de gobernanza, ya que otra opción habría podido ser usar ETH como colateral. Al introducir los incentivos, el 84 % del SNX se puso en staking, un éxito increíble, permitiendo que una gran cantidad de SNX salieran a circulación.

Al final, este tipo de incentivos se podría ver como la primera aplicación de liquidity mining de la historia, muy anterior a Compound u otros protocolos comentados: incentivos en el token nativo para promover el crecimiento orgánico del protocolo y buscar la generación del famoso círculo virtuoso.


Figura 141. Círculo virtuoso del SNX

## 26.10. Necesidad de liquidez e incentivos secundarios

Uno de los puntos críticos de Synthetix es asegurar que los participantes puedan confiar plenamente en que el peg de sUSD es estable y garantizado. Primero, porque los stakers cobran las fees en sUSD, y si esta no es fácilmente intercambiable con otras stablecoins, básicamente no tendrá valor fuera la plataforma.

Por otra lado están los traders, que en caso de profits quieren poder intercambiar los synths por otros tokens sintéticos o por activos reales. Esta paridad líquida entre synths y tokens reales a su vez permite que nuevos participantes puedan entrar en el sistema simplemente comprando synths con activos reales en un pool de liquidez como Uniswap.

Para mantener el peg y garantizar liquidez hacen falta dos cosas: primero una buena ratio de colateralización (garantizando así confianza), acción que además se *corrige* gracias al sistema de incentivos, y, en segundo lugar, pools de liquidez profundos. Estos pools permiten hacer swaps de synths a activos normales y al revés, y están disponibles en los principales protocolos de liquidez: Uniswap, Curve y Balancer. Con el objetivo de que haya liquidez en los pools de estos protocolos, Synthetix tiene un sistema de incentivos secundario para ayudar a que esto suceda. Estos incentivos varían periódicamente, y van cambiando de

protocolo. Por ejemplo, anteriormente en Uniswap estabas incentivado a través de SNX tokens para añadir liquidez al pool sETH/ETH, sXAU/USDC y SNX/USDC.

Para asegurar la liquidez e incentivar a los token holders a mantener pools con synths, parte de los tokens emitidos por la política inflacionaria de Synthetix se destinan como incentivos secundarios que buscan garantizar liquidez de los sTokens.

1. DAI:USDC:USDT:sUSD

En este pool, Synthetix destina unos incentivos de 48 000 SNX semanales para incentivar la creación de liquidez entre stablecoins.

2. renBTC:wBTC:sBTC

En este pool se destinan 10 000 SNX semanales, además de 25 000 REN también semanales. Este pool a principios de septiembre dejó de incentivar a través de REN tokens, pero mantiene los incentivos secundarios de SNX.

3. iETH - iBTC

Este es un modelo de incentivos diferente, pero pretende estimular la compra de token iETH (bajista a Ethereum) para compensar la fuerte demanda de sETH y mitigar el riesgo asumido por los SNX stakers. Sucede lo mismo con el sBTC y el iBTC.

Para poder aprovechar este tipo de incentivos, los LP tokens o el token correspondiente deben stakearse a través de Synthetix.

Generar pools de liquidez, además de hacer más útiles los synths, ayuda a mantener un peg estable gracias a oportunidades de arbitraje.

## 26.11. Usando ETH como colateral en SNX

Otra opción para participar en el protocolo es usar ETH como colateral. Al contrario que con SNX, stakeando ETH no participas en la debt pool y por tanto no recibes retribuciones a través de fees y rewards. Simplemente es una forma de generar sETH usando ETH como colateral, a una c-ratio del 150 %.

## 26.12. xSNX Token Strategy

El modelo tokenómico del SNX token, a pesar de ser una genialidad, es complejo de entender y tiene grandes costes asociados en caso de querer adoptar posiciones para mitigar el riesgo del aumento de las obligaciones de deuda. Está directamente bloqueada la entrada a un gran número de inversores que no tienen suficiente conocimiento como para entender la dinámica del modelo.

Es por eso que próximamente va estar a disposición el xSNX, el cual te permitirá participar en el protocolo de Synthetix y recibir fees y rewards sin ningún tipo de complejidad, simplemente comprando o vendiendo los tokens. Con el xSNX puedes aprovechar los retornos de stakear tus tokens e incluso recibir tokens que representan las posiciones de staking para usar en otras operaciones y en ningún momento tendrás que mintear, reclamar fees, adoptar posiciones de hedging para reducir el riesgo de las obligaciones de deuda, ni tendrás que manejar activamente tu ratio de colateralización.

La idea es la siguiente: un usuario podrá generar xSNX a través del protocolo usando ETH o SNX, aunque también podrá usar un pool de Balancer para obtenerlo. Al obtener este xSNX, por detrás, el smart contract del token estará minteando sUSD, el cual adoptará la estrategia ETHRSI6040 que consiste en mantener el 25 % en ETH real y un 75 % en ETH cuando la tendencia sea alcista, y si la tendencia es bajista, se haría un swap automático a USDC. Como vemos, es un token que se encarga de hacer el proceso de creación de sUSD y además aplica una estrategia para mitigar el riesgo de las obligaciones de deuda de forma nativa.

Por el momento solo está disponible esta estrategia, aunque habrá más en el futuro, como por ejemplo LINKETHRSI, ETHBTCRSI y iETH20SMACO.

Las fees se reclamarán automáticamente en el momento de hagas redeem en la plataforma. Algo interesante del token es que en caso de librarte de los xSNX a través de un swap en Balancer, el smart contract del token te permite que el swap tenga en cuenta las fees que has acumulado y por tanto puedas recuperar las fees incluso a través de un swap.

El cuanto al pool de Balancer, estará compuesto por xSNX/ETH/SNX en una proporción del 50/25/25. El pool estará inicialmente capitalizado por VC como RedRock Capital e Infinite Capital, fondos muy vinculados al proyecto y participantes de la comunidad de SNX.

Por último, los xSNX tokens tendrán integrado un rebalanceo automático para asegurar las posiciones. Cuando haya un outperform del portfolio, se venderá parte del beneficio en ETH (cuando supere un 5 %) para aumentar las posiciones

de staking de SNX a través de xSNX. Por otro lado, en caso de caídas del 5 %, el movimiento será contrario: vender SNX para quemar parte de la deuda generada.

## 26.13. ¿Es sUSD rival para DAI?

La stablecoin descentralizada por excelencia en DeFi es sin duda DAI. Esta moneda generada a través de las bóvedas en Maker ha sido una de las grandes innovaciones en Ethereum y una de los precursores e iniciadores del ecosistema DeFi. Hoy, su dominio se ha visto cuestionado, sobre todo después de demostrar que el sistema de respaldo no era perfecto y que podía fallar, como ocurrió el Jueves Negro. Estas dudas han generado un gran interés por parte de otros proyectos de buscar opciones estables más sólidas (mStable, Ampleforth…). Y, entre todos ellos, también tenemos al sUSD de Synthetix, un token que podría representar una gran amenaza para DAI.

Si analizamos DAI en Maker y sus inconvenientes, podemos identificar dos:

- El primero es que su forma para mantener el peg es a través de oportunidades de arbitraje donde teóricamente muchos de los usuarios con bóvedas estarán interesados en comprar DAI a bajo precio para reducir la cantidad de deuda a devolver. El problema es que la mayoría de estos son holders de ETH y confían en su valor a largo plazo, por lo que este incentivo no es suficiente para que aquellos equilibren constantemente el token. De hecho, hemos visto cómo DAI ha estado rondando incluso por los 96 - 98 céntimos varias veces.
- En segundo lugar destacaría que no hay una forma de incentivar la generación de DAI. Esto hace que el token no sea escalable en función de la demanda. El motivo principal por el cual se genera es para ofrecer posiciones de leverage a los ETH holders.

Por otro lado, sUSD tiene características diferentes. Primero, tiene un mecanismo para incentivar el aumento de sUSD a través del incremento de la demanda. Imaginemos que hay un total market de synths de 15 M, 2,5 M en sUSD y 12,5 M en otros SNX. Si la demanda total de los synths sube un 10 %, será claro que el precio del SNX token (usado como colateral) no estará respondiendo correctamente a la demanda de synths, y por tanto podríamos decir que el token estará devaluado. Los inversores verán atractiva la compra de SNX haciendo que este suba de precio tras haber aumentado suficientemente el colateral del sistema para generar más sUSD y compensar el aumento de demanda (exactamente SNX token habrá subido un 2 %).

Esto a su vez sirve como mecanismo para incentivar la generación de sUSD en momentos críticos, cosa que DAI no pudo hacer durante el Jueves Negro. De hecho, la idea de poner USDC (u otros assets) como colateral en Maker era buscar una forma de aumentar colateral y generar más DAI en esos momentos.

Claro está que Synthetix no compite ni de lejos con Maker en cuanto a ofrecer posiciones de leverage a través de ETH. Primero, porque si se usa ETH para generar sETH en Synthetix, si el trader usa esos synths para adquirir sLink, aunque Link suba de valor, si no sube más que ETH, el trader seguirá estando en pérdidas en términos de coste de oportunidad; sin contar con que, con ETH como colateral, no tienes derecho a recibir fees y rewards. En el momento que este tipo de colateral sea válido en Synthetix y se pueda generar sUSD con ETH, el token estable sUSD podría tener más ventajas: ser más líquido, con un modelo de incentivos mejorado y con muchas oportunidades ancladas (como comprar otros synths u obtener leverage en la plataforma).

Esta es una idea que ha surgido con fuerza después del problema que vivió Maker durante la caída de este año. Aunque pueda tener cierto sentido, sigue siendo algo muy teórico. A día de hoy, Maker es el líder indiscutible y la cantidad de DAI en comparación a sUDC en el mercado es tremendamente superior.

## 26.14. El gran valor diferencial de Synthetix

Sin duda alguna, el mayor potencial que tiene un asset sintético es el poder traer a una blockchain la posibilidad de tener exposición de precio de activos reales, manteniendo así todo lo bueno de blockchain. A día de hoy, no hay forma de utilizar los criptoactivos para especular en los mercados. Los assets sintéticos pueden hacerlo posible.

Por otra parte, las ventajas que pueden traer estos tipos de assets a los traders son enormes, aunque también lo son sus riesgos. Así que vamos a comparar los pros y contras, para así poder decidir de forma objetiva si queremos o no participar en el protocolo:

Ventajas:

- **Leverage.** Protocolos como Synthetix te permiten abrir posiciones con leverage e invertir en todo tipo de activos.
- **Hedge risk.** Los token sintéticos pueden permitirte buscar posiciones de cobertura a tus inversiones. Imagina que tenemos 50 000 USD en Bitcoin;

para evitar grandes pérdidas si este cae de precio, puedo abrir posiciones en tokens sintéticos inversos (en caso de Synthetix, es iBTC).

- **Trading para grandes volúmenes.** Como hemos visto, tradear con sintéticos no tiene nada que ver con hacerlo con activos normales, porque tan solo te dan exposición de precio, pero en ningún momento compras el asset real. Esto nos permite poder mover dinero de un asset al otro sin tener que preocuparnos de la liquidez o del price slippage durante el cambio.
- **Portfolio.** Gracias a swaps exageradamente económicos a través de tokens de Synthetix, tenemos la posibilidad de crear un portafolio con re-locations constantes. Esto aumenta mucho el rendimiento final del portfolio.
- **Creación de sintéticos únicos.** Gracias a Blockchain y los assets sintéticos podemos crear tokens que nos den exposición de precio a miles de cosas. Como hemos comentado, podemos crear assets sintéticos de jugadores de fútbol, y que su fluctuación de precio esté sujeta a un montón de variables donde se tenga en cuenta su rendimiento, los minutos jugados, la opinión pública, los goles… Este sintético nos permitiría apostar por el rendimiento de un jugador concreto. A diferencia de un proceso de tokenización, no estarías comprando derechos reales sobre el jugador, simplemente te expones a su precio, ya que el valor de ese movimiento no está respaldado por el jugador, sino por puro colateral.
- **Proyecto open source** y con la intención de descentralizarlo progresivamente durante los próximos años.
- **Buenos tokenomics**: el token SNX ha sido integrado al sistema de forma central, generando un sistema que permita al token una revalorización a largo plazo y que también sea capaz de absorber el valor generado dentro del protocolo.

Inconvenientes:

- **Tecnológico.** El primer riesgo, presente también en todos los otros protocolos, es el tecnológico. No solo por posibles bugs en sus smart contracts, sino por posibles fallos de la plataforma base (Ethereum) o fallos de otros protocolos asociados. Al final, el concepto de money lego hace que los protocolos dependan unos de otros, para lo bueno y para lo malo.
- **Poca madurez.** Hoy en día, Synthetix sigue siendo un protocolo que se encuentra en fases iniciales. De hecho, no se pretende incentivar la entrada de nuevos usuarios hasta que se reduzca la complejidad y haya una mejora de la

plataforma. Esto evitaría generar malas experiencias a los nuevos usuarios y que no utilizasen más el protocolo.

- **Price oracles.** Recordemos que los swaps entre synths se hacen a través de smart contracts, no hay límite de liquidez ni problema de slippage. Esto hace que el precio del swap lo dicte un oráculo. Aquí está uno de los puntos más críticos del protocolo, los price feeds. Por el momento estos están asegurados y ofrecidos de forma descentralizada a través de ChainLink.
- **Centralización.** Synthetix a día de hoy sigue siendo uno de los protocolos más centralizados del ecosistema. El CEO del proyecto defendió públicamente que prefería mantener un control centralizado durante el desarrollo y buscar la descentralización en etapas futuras. SNX será el token de gobernanza, aunque por el momento no tiene mucho poder.
- **Riesgos del protocolo.** La posibilidad de iniciar un círculo vicioso en el protocolo. Usar SNX como colateral del sistema, aunque sea muy bueno para el diseño del token y su valor a largo plazo, podría ocasionar grandes problemas a la plataforma si hubiera caídas del precio; incluso, puede llegar a provocar la pérdida de todo el TVL. Además, debes contar con un nivel de colateralización muy alto, lo que te obliga a perder usabilidad de tus activos. Por último, destacar la complejidad del sistema y la gran cantidad de factores a tener en cuenta para poder usar Synthetix de forma muy rentable si eres un staker.

## 26.15. Conclusiones de Synthetix

Como resumen, Synthetix es un protocolo que te da acceso a comprar y tradear tokens sintéticos completamente on chain. A pesar de ser complejo, el diseño en general está muy bien logrado y podríamos considerar el token SNX como uno de los mejores —en cuanto a diseño— tokens de gobernanza en protocolos DeFi.

Sin duda, el potencial de los assets sintéticos es enorme y aún está por verse. Veremos si Synthetix acaba siendo una pieza clave en la emisión y evangelización de este tipo de activos.

Estamos presenciando el nacimiento de lo que algún día será uno de los ecosistemas con más valor de todo Blockchain, y, sin exagerar, creo que podemos llegar a ver trillones de dólares bloqueados en protocolos de este tipo. Poder participar y aprovechar esta expansión no tiene precio.

# 27. Protocolos para optimizar yields (rendimientos): Yearn Finance

Sin duda, Yearn es uno de los grandes proyectos del ecosistema DeFi. No solo por su elegancia y aporte al ecosistema, sino por cómo se ha desarrollado y por ser un fiel ejemplo de lo que se está intentando construir en el mundo descentralizado. Desde el principio hemos dejado claro que entramos en un nuevo paradigma financiero, donde el valor generado no se lo llevan unos pocos sino que se reparte entre una comunidad, la misma que conjuntamente ,y aplicando los principios de consensos de las blockchains, actúan como gobernantes de tales protocolos.

Yearn ha sido llamado, en muchas ocasiones, el «Bitcoin de DeFi», y no solo porque ha alcanzado los precios más altos conseguidos por un token hasta la fecha, sino por cómo se ha distribuido y entregado a la comunidad. La mente detrás de este proyecto es Andre Cronje, «el Satoshi de DeFi», quien no generó ningún preminado para él mismo, sino que lo entregó a la comunidad de la misma forma que lo hizo Satoshi. Así que Yearn es seguramente el protocolo más descentralizado que existe, con la comunidad más activa y que más rápido ha crecido.

## 27.1. Análisis del protocolo de Yearn

Yearn es básicamente un protocolo que se enfoca en optimizar yield o el rendimiento de inversiones en protocolos DeFi. Con esta definición ya queda claro que es un protocolo flexible y en constante cambio, ya que continuamente la forma más rentable de mover tu capital en DeFi va variando.

Curiosamente, Yearn nació como un proyecto personal de Andre, quien estaba cansado de mover a diario su capital (y el que gestionaba de amigos y familiares) entre los diferentes protocolos, buscando siempre el máximo rendimiento. De allí nació su idea de crear un smart contract que continuamente consultase a protocolos como Compound, Aave o dYdX qué rendimiento estaban ofreciendo, y en función de cuál fuese el más rentable, el smart contract movería los fondos a ese protocolo de forma automática. Para dar una aclaración, los activos que se movían eran siempre stablecoins.

En ese momento, Andre se dio cuenta de que no había ningún motivo por el cual no debiera abrir ese servicio al público y permitir a otros usuarios usar el mismo smart contract. De hecho, esta fue una estrategia incluso más inteligente, ya que más capital hacía dicha estrategia todavía más rentable: un smart contract solo consulta y realiza una acción cuando alguien lo activa pagando un gas, por lo que cuantas más interacciones haya con ese smart contract (depósitos y retiros de capital) más veces este consultará las mejores opciones a otros protocolos, por lo que más movimientos de capital generará, lo que su vez producirá un mejor rendimiento a ese capital.

Esta fue la primera versión de Yearn, lanzada a principios de 2020 sin ningún tipo de auditoría y con muy poco volumen. Andre siempre había dejado claro que los productos que él creaba eran para él mismo y que, por tanto, la gente tenía que invertir con precaución ya que podía haber bugs en los contratos.

## 27.2. Segunda versión de Yearn

La popularidad de Yearn como optimizador de inversión en protocolos DeFi estaba aumentando, hasta el punto en que los smart contracts usados también debían mejorar su complejidad. En la segunda versión, Andre creó un sistema que permitiese al smart contract valorar el riesgo y tomar decisiones en función de este. Claro está que esta acción es relativa y subjetiva; incluso en las finanzas tradicionales es imposible tener un medidor exacto del riesgo. Lo que hacía el smart contract era consultar no solo el rendimiento del protocolo sino también el volumen y la liquidez, ya que debía también calcular cómo afectaría la entrada de 2 MUSD de dólares al protocolo y al rendimiento que este ofrecía.

De nuevo, el protocolo continuó buscando y encontrando la forma más optimizada para invertir tus stablecoins y, por tanto, la popularidad de Yearn seguía creciendo.

## 27.3. Lanzamiento de Curve.fi

El lanzamiento de Curve presentó nuevas oportunidades de optimización en cuanto a inversiones de stablecoins en DeFi. Como hemos visto ya, Curve es un protocolo con AMM (automated market making) que crea un mercado extremadamente eficiente para swapear stablecoins.

Después del lanzamiento, Curve lanzó el yPool, que consistía en un pool para swapear stablecoins con un yield maximizer. Es decir, cuando tú depositas

stablecoins (y ahora también otros activos) en el protocolo de Yearn, recibes a cambio yTokens, que son tokens que están viendo sus rendimientos optimizados constantemente. Desde ese momento, con tus inversiones en Yearn no solo aprovechabas al máximo los rendimientos de los protocolos de lending, sino que además generabas rendimiento a través de las fees acumuladas en Curve. Concretamente el 0,04 % de cada swap realizado.

A partir de ese momento las oportunidades para maximizar los rendimientos se estancaron, así que Andre se dedicó a crear más productos que buscaran incrementar mínimamente los APR actuales.

Uno de los productos fue el yTrade y el yLeverage, que consistían en una estrategia donde a través de un flash loan generado en dYdX de USDC hacías una operación de arbitraje. La idea era la siguiente:

- Pedías un flash loan de USDC de dYdX,
- te llevabas el USDC a Maker y creabas un CDP para generar DAI,
- vendías este DAI en Curve por USDC, y
- devolvías así el préstamo original en USDC.

Si la operación había ido exitosa, ganabas un interés. Esto no solo ofrecía oportunidades de arbitraje, sino que además aumentaba el volumen de trades en Curve, lo que mejoraba el APR del yPool en Curve.

Otra innovación fue la integración de Zapper.fi con Yearn, para ofrecer así el zap service, que te permitía entrar en cualquier optimización usando el token de entrada que quisieras. Este automáticamente se intercambiaba por otro (DAI, USDC, USDT) y se optimizaba.

Al final, el objetivo siempre era el mismo: manteniendo un nivel de riesgo bajo (por ejemplo, los productos de leverage no ofrecían todo el leverage posible por precaución) maximizar los retornos de inversión. Una de las leyes en Yearn (dejando de lado la integración con zapper) es buscar la mejor optimización sin cambiar el activo subyacente; es decir, si tengo DAI y quiero invertir DAI, no voy a cambiarlo por USDC porque dé un mejor APR, sino que voy a buscar la inversión más optimizada usando DAI.

## 27.4. Compound, liquidity mining y la gran revolución

A partir de julio de 2020, la propuesta de Compound de incentivar con COMP a los liquidity providers y dar origen así al concepto de liquidy mining cambió completamente las reglas del juego, no solo para Yearn sino para todo DeFi.

La realidad es que esta innovación nació realmente por el sistema de rewards que creó Syntehtix para disparar la liquidez disponible de su stablecoin nativa en Curve: depositando sUSD en Curve y haciendo staking de ese LP curve token en Synthetix, podías obtener unas rewards semanales en token SNX.

Con la llegada del liquidity mining, buscar la inversión más optimizada era mucho más complicado, ya que encima ahora podías también hacer farming de otros tokens, lo que aumentaba tu APR final. Esta estrategia la adoptaron después otros protocolos como Balancer, mStable, Curve, Ren y Aave (recientemente) y, por tanto, había que redefinir por completo la forma de optimizar los rendimientos a través de Yearn.

## 27.5. La llegada de las vaults y el YFI token

Ese cambio traía consigo algunos problemas. Ahora, con las nuevas estrategias de liquidity mining —que además cambiaban sin cesar— era prácticamente imposible optimizar las inversiones de stablecoins de la forma que se estaba haciendo. Primero surgió un problema de oráculos, ya que no había forma on chain y segura de acceder a los datos sobre rendimientos de liquidity mining de todos los protocolos; y además, las estrategias se habían vuelto demasiado complejas como para que solo Andre dedicase tiempo a programar los smart contracts.

Lo que estaba claro es que en Yearn participaban los farmers (optimizadores de inversión) más comprometidos y conocedores del ecosistema, y que Yearn podía apalancarse en estos para crear continuamente nuevas estrategias. Esta idea permitió el nacimiento de la yVaults y el YFI token.

Los vaults (bóvedas) son smart contracts que optimizan la inversión de un token (por ejemplo DAI) siguiendo una estrategia compleja que incluso usa diferentes protocolos a la vez. Estas estrategias necesitan que se estén mejorando y cambiando continuamente.

Este era el objetivo del YFI token: crear un modelo de incentivos que alinease a estos farmers iniciales no solo a dar con estrategias rentables, sino también a codificarlas y crear vaults con esas estrategias; y que obviamente se voten por la comunidad antes de aplicarse. El YFI token serviría como token para gobernar el protocolo, el cual con un modelo de comisiones incentivaría a sus holders a participar en la gobernanza y a los strategy writers a buscar continuamente nuevas estrategias optimizadas y programarlas. De hecho, el modelo de fees para las vaults consiste en un 0,5 % por cada retiro para el protocolo, y un 5 % de

performance fee, donde un 90 % va destinado como incentivo al proceso de gobernanza y un 10 % al creador de la estrategia (strategy hero).

Los YFI, por tanto, se repartieron entre la comunidad (un total de 30 000 tokens) a través de un sistema de rewards. Aquellos que depositaran sus stablecoins en Yearn (usando por debajo los yPools de Curve) recibirían los YFI tokens. Estos primeros farmers minaron los primeros YFI tokens a 3 USD, y este ha llegado a los 43 000 USD en sus máximos históricos, y en muy pocos meses. No es de extrañar que Yearn tenga una de las comunidades más participativas y entregadas de todo DeFi.


Figura 142. Evolución en la cotización del YFI token agosto-noviembre 2020.

Al final, este tipo de distribución fue de lo más justa y descentralizada que se ha visto, ya que se entregó el 100 % a la comunidad, sin dejar que ningún VC participara. Ni tan solo Andre minó algunos YFI previamente para sí mismo. El objetivo era realmente dar el token a aquellos que participaban, entendían y estaban comprometidos con el proyecto para crear una comunidad de gobernanza potente. El carácter especulativo que se le ha dado a YFI siempre ha sido algo que no ha gustado a su fundador, ya que él ya avisó que el token no tenía ningún valor desde un principio, y que solo servía para la gobernanza. La realidad es que podría ser que un día los tokenholders decidiesen repartir dividendos a la comunidad y transformar el token de gobernanza a un capital asset que diera rendimiento, así que no me extrañan tanto estas subidas extremas en el precio del token.

## 27.6. Algunas estrategias en vaults de Yearn

Este capítulo puede llegar a ser poco trascendente al paso de los días, ya que comentaremos estrategias usadas al momento de escribir el libro, lo que significa que pueden quedar fácilmente desactualizadas. Para revisar las estrategias podéis visitar el **site de gobernanza de Yearn**, donde se votan y discuten las próximas estrategias que se van a aplicar.

## yETH Vault

Esta vault es de lo más interesante, ya que por primera vez consiguió ofrecer un rendimiento atractivo al ETH, que en general siempre ronda el 0,1 % - 1 % de APR en la mayoría de protocolos de lending. Estrategia actual: **StrategyMKRVaultDAIDelegate**

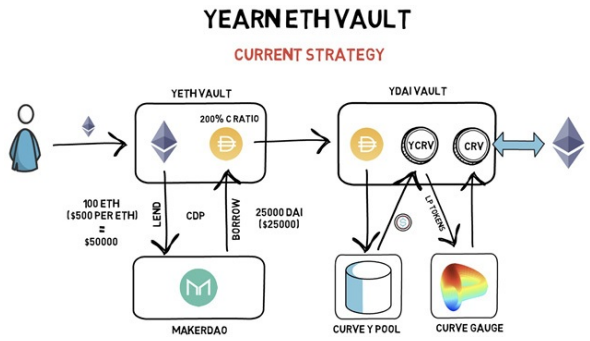



Figura 143. Estrategia con vaults de yETH en Yearn

Como vemos en la imagen, el ETH se usaba como colateral en Maker para generar DAI. Este DAI se llevaba al yPool de Curve, donde a cambio se recibía el liquidity pool token de yCRV. Con este token se abría una posición de staking, que generaba rewards en CRV. Finalmente este se cambiaba por ETH y se devolvía al usuario en forma de APR. ¡Para que te explote la cabeza!

El APR de este vault había llegado a valores del 17 % durante sus inicios. No obstante, ahora se ha visto reducido hasta un APR del 0,71 %

## yVault YFI

Esta vault usa la estrategia **StrategyYFIGovernance,** que funciona de la siguiente manera:

En primer lugar, depositar tus YFI tokens que, inmediatamente, se depositan en el contrato de staking para gobernanza de Yearn. Este contrato te permite generar Curve-Y que inmediatamente se convierte en USDT usado para comprar más YFI y así aumentar tu posición en el yVault.

Actualmente esta estrategia está dando un APR del 8,15 %.

## Curve y pool yVault

Estrategia usada para el vault: **StrategyCurveYVoterProxy**

El token usado en esta estrategia en el yPool, liquidity provider de Curve, que se deposita en Curve.fi en forma de staking para hacer farming del token CRV. El 10 % de estos CRV se bloquean en Curve para multiplicar hasta por 2,5x la cantidad de CRV generados (política de incentivos aplicada en Curve que se

mantendrá durante un periodo determinado). El 90 % restante se convierte en DAI, que automáticamente se deposita en un yPool de Curve para después usar el LP token en Yearn y empezar con el mismo proceso de nuevo.

Esta estrategia, compleja sin duda, está generado un APR del 9,99 %.

**Curve sBTC Pool yVault**

Estrategia usada: **StrategyCurveBTCVoterProxy**

En esta vault se aplica la misma estrategia que en la vault anterior (Curve y pool yVault), solo que este caso el token depositado en el smart contract de la bóveda es el Curve-sBTC, el token de liquidity provider del pool de sBTC de Curve.

El rendimiento actual de la estrategia es un APR del 4,7 %.

## 27.7. Conclusiones y últimas innovaciones

Antes de finalizar este fascinante protocolo, mencionaremos el último servicio de yinsusance.finance, un sistema que te permite crear opciones de cobertura en algunos protocolos DeFi usando Nexus Mutual por debajo pero sin tener que pasar por un KYC. Es decir, servicios de cobertura sin necesidad de identificarte.

Yearn tuvo un éxito tan enorme, que muchos protocolos nacieron con la idea de copiarlo, algunos son DEFI.money, DEFI.Finance o YFIII. Ninguna de ellas ha resultado tener la capacidad de superar ni lo más mínimo a Yearn, ya que al final el valor más alto de su protocolo es la comunidad y los strategy writers que continuamente modifican y descubren las mejores estrategias para ofrecerlas a la comunidad. Al final, los sistemas de incentivos funcionan. Es cierto que los votos en Yearn se han reducido, sobre todo por la entrada (o salida) de muchos especuladores, pero aun así la participación de los stakeholders sigue siendo de las más altas en todo DeFi.


Figura 144. Votaciones en Yearn de agosto a noviembre 2020

Concluiremos Yearn simplemente mostrando y admirando cómo ha crecido y aportado al ecosistema. Sin duda es uno de los grandes players de esta revolución y lo demuestra cada día con sus constantes innovaciones. Buscar

optimizar los APR no es trabajo sencillo, ya que te obliga a ser flexible y a estar en cambios constantes. No tengo duda de que Yearn seguirá cambiando cuando el mercado lo requiera y es una opción sólida y fiable para quien busca maximizar sus inversiones en DeFi.

# 28. Protocolos para tokenizar Bitcoin: wBTC

El ecosistema DeFi se ha desarrollado prácticamente en su totalidad sobre la blockchain de Ethereum. Es cierto que ya hay y se están desarrollando algunos protocolos directamente sobre Bitcoin, pero en ningún caso podemos comparar la cantidad de usuarios y desarrollo que hay en Ethereum con lo que existe en Bitcoin.

Esto genera algunos problemas, ya que el claro límite de DeFi es que nunca podrá acumular más valor que el que hay en la red de Ethereum, además de que esta última se usa por muchos otros motivos que únicamente DeFi. Ante este límite se empezaron a estudiar opciones para traer Bitcoin dentro de Ethereum, sobre todo porque la capitalización de Bitcoin es tan alta que podría llevar consigo mucha liquidez, además de solidez y seguridad no solo a DeFi sino a Ethereum en general.

De esta idea nació la primera propuesta para tokenizar Bitcoin sobre Ethereum (wBTC), y la cantidad de proyectos que pretenden ofrecer soluciones a este problema no ha parado de crecer. El primero que veremos será wBTC, que de hecho es el que actualmente acumula más valor.

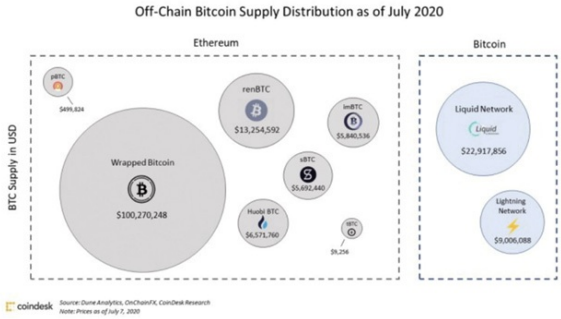



Figura 145. Diferentes formas de tener Bitcoin en el ecosistema DeFi

wBTC es un proyecto impulsado inicialmente por BitGo (plataforma de inversión en criptoactivos especializada en inversores institucionales), Kyber Network (exchange descentralizado) y RenVM (protocolo de interoperabilidad que busca generar BTC tokenizados sobre Ethereum de forma descentralizada). Este proyecto sigue un modelo gobernado por un consorcio y un modelo de seguridad basado en custodia. Es decir, con wBTC podemos dejar nuestro BTC custodiado y recibir wBTC a cambio en la red de Ethereum. El ratio siempre será 1:1 y habrá tantos wBTC en circulación como BTC bloqueados en custodia. De alguna forma, este es un modelo muy similar al que sigue USDT.

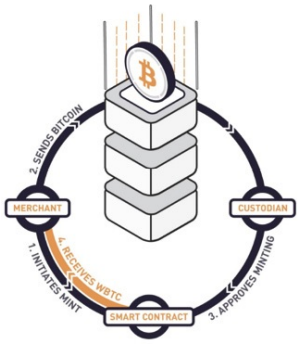



Figura 146. Workflow general de wBTC

Ahora bien, para poder generar wBTC, antes debes pasar por un proceso de validación de KYC y convertirte en un merchant. Estos tienen la capacidad de generar y eliminar wBTC del mercado, apoyándose en una entidad que les custodie los activos, como es el caso de BitGo.

Mints/Burns for Top 10 wBTC Merchants

| merchant | wbtc_minted | wbtc_burned | difference |
|---|---|---|---|
| Alameda Research | 43,606.00 | 0.00 | 43,606.00 |
| Coinlist | 41,216.10 | 0.00 | 41,216.10 |
| Grapefruit Trading | 15,764.70 | 1,694.60 | 14,070.10 |
| Three Arrows | 6,638.60 | 0.00 | 6,638.60 |
| Kyber | 669.90 | 0.00 | 669.90 |
| Maker | 231.10 | 0.00 | 231.10 |
| DDEX | 99.90 | 0.00 | 99.90 |
| Airswap | 87.60 | 30.40 | 57.10 |
| Native Gaming | 23.60 | 1.80 | 21.80 |
| Prycto | 12.20 | 0.00 | 12.20 |

Figura 147. Consorcio de minteadores de wBTC, por relevancia

El consorcio está formado por varios líderes del ecosistema DeFi como Maker, Airswap, Set Protocol, Radar Relay y Gnosis, que se encargan de auditar los balances de BTC y wBTC disponibles y gobernar el consorcio a través de votaciones y propuestas de mejora. Además también se comprometen a dar liquidez, estabilidad y seguridad al proyecto.

Sin duda, la entrada de Bitcoin en Ethereum ha sido muy relevante para el ecosistema. De hecho, en cuestión de meses wBTC se puede usar en la mayoría de protocolos DeFi y fue de los primeros assets en ser aprobados por Maker con los que podrías generar DAI usándolo como colateral.

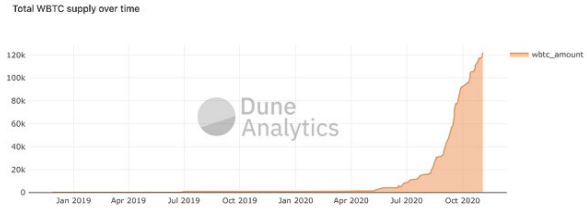



Figura 148. Entrada de wBTC a Ethereum desde su creación.

La adopción no ha parado de crecer desde su introducción, y al final es más que comprensible. A pesar de que el bitcoin tokenizado nunca será bitcoin, ya que ahora lo estamos moviendo a través de una red mucho menos segura (en comparación a Bitcoin) disponer de BTC en Ethereum aporta liquidez y mucha seguridad a los protocolos.

Claro está que el proyecto de wBTC es contrario a la visión de descentralización que existe en DeFi y es por eso que cada vez hay más proyectos que buscan ofrecer la posibilidad de trasladar BTC sobre Ethereum pero de una forma completamente descentralizada. De hecho, para poder generar wBTC hay que pasar por un proceso de KYC, algo que estos nuevos protocolos no requieren. En concreto veremos RenVM y Keep Network, las dos opciones más interesantes actualmente.

# 29. Protocolos para Tokenizar Bitcoin: Keep Network

Keep es uno de los protocolos más recientes que pretenden crear un puente de interoperabilidad entre Bitcoin y Ethereum para ofrecer un servicio descentralizado para wrappear tus bitcoins.

Ofrecer un protocolo que tokenize Bitcoin sobre la red de Ethereum de forma descentralizada es una tarea compleja. La clave en estos sistemas es conseguir un modelo donde, en primer lugar, sea prácticamente imposible para los participantes del protocolo acceder y mover los bitcoins custodiados (cada bitcoin tokenizado debe estar respaldado por un bitcoin real), y generar al mismo tiempo un modelo de incentivos que evite que estos usuarios quieran quedarse con estos bitcoins.

En el caso de Keep Network, esto funciona de la siguiente manera: el protocolo está formado por los llamados signers, que son los encargados de generar los tBTC (bitcoins tokenizados por el protocolo de Keep) y custodiar los bitcoins reales. Estos signers están obligados a mantener siempre un 150 % de colateral en ETH. Es decir, si tokenizan 1 BTC tienen que mantener 1,5 BTC en ETH como colateral. Esta es la primera capa de seguridad con la que se desincentiva por completo a los signers de intentar *robar* los bitcoins custodiados, ya que automáticamente perderían su colateral.

En segundo lugar, los bitcoin enviados por el usuario que quiere migrar sus tokens a la red de Ethereum se guardan en un wallet con unas claves privadas especiales que se rompen en pedacitos para que cada signer guarde una pequeña parte, y este la mantendrá custodiada durante seis meses. De esta forma, no solo están desincentivados a robar los bitcoins, sino que además es algo muy complicado, porque nunca un signer tendrá el control total de las claves privadas del wallet de bitcoins.

Debido al funcionamiento interno del protocolo, Keep solo permite generar migraciones de lotes predeterminados de bitcoins, es decir, si quieres generar más de 1 BTC o 0,75 tBTC estarás obligado a realizar más de una transacción.

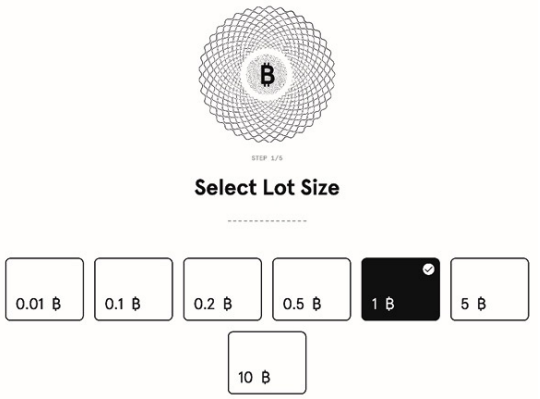


Figura 149. Creación de tBTC bloqueando BTC (vía EWTH) por distintos tamaños de lotes

# 30. Protocolos para tokenizar Bitcoin: RenVM

El último protocolo para tokenizar Bitcoin que veremos es RenVM, seguramente el protocolo de interoperabilidad entre Bitcoin y Ethereum para la tokenización de BTC más importante hoy en día.

A nivel funcional, la forma en que Ren y Keep Network afrontan el problema de la descentralización es muy similar, aunque cada uno lo hace de una forma diferente, con sus ventajas y desventajas.

En el caso de RenVM, el token usado como colateral y que aporta seguridad al sistema es su token nativo (ren). Es decir, los participantes del protocolo, en este caso llamados darknodes, deben depositar un mínimo de 100 000 rens y mantener siempre un nivel de colateralización del 300 %. Esto implica que el valor del token ren esté directamente relacionado con la usabilidad y el crecimiento del protocolo. Esta característica hace que ren sea más eficiente en cuanto al uso del capital bloqueado, ya que en caso de caídas de token, el protocolo automáticamente ajusta las comisiones (que benefician directamente el valor del token) para volver a equilibrar el sistema.

Otra característica es que la forma en que los darknodes custodian diferentes partes de las claves privadas del token de bitcoin es diferente, ya que están cambiando constantemente de nodo. Esto significa que, en primer lugar, tienes un modelo que desincentiva claramente el ataque; y, en segundo lugar, coordinar un ataque es prácticamente imposible, porque una vez has localizado todos los nodos que custodian una clave privada, esta ya ha cambiado de darknode y, por tanto, se hace muy difícil un ataque.

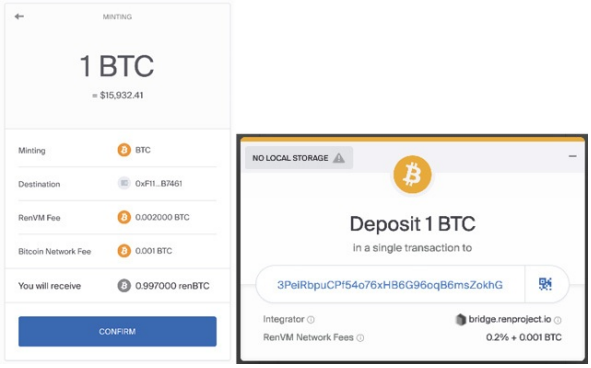



Figura 150. Interfaz general de RenVM para generar renBTC

## 30.1. Comparación RenVM y Keep Network

Si hay algo claro es que un modelo descentralizado siempre aportará más valor a la comunidad que uno que no lo sea, sin tener en cuenta que con wBTC hay que pasar por un proceso de validación que muchos usuarios prefieren ahorrarse.

La siguiente pregunta es ver qué protocolo es más seguro y sólido: Keep o RenVM. Aunque es una pregunta difícil, vamos a comprar los dos sistemas y sacar las ventajas y desventajas de cada uno.

**a) Seguridad del protocolo**

Siempre que se construye algún tipo de protocolo de interoperabilidad, este tiene por defecto cierta cantidad de valor bloqueado dentro. En este caso, los dos protocolos disponen de un custodio descentralizado que está almacenando una gran cantidad de valor. Si el valor bloqueado en el protocolo llega a niveles demasiado altos, los incentivos para atacar y llevarse los fondos custodiados son enormes. Por tanto, se debe crear un sistema donde estos custodios deban mantener un colateral superior al dinero que pueden llegar a robar. La forma de garantizar este colateral es seguramente la diferencia más grande entre los protocolos.

Keep Network usa ETH como colateral con un sistema de liquidación clásico, como los que hemos visto en Maker u otros protocolos. Los signers se comprometen a mantener una ratio de colateralización del 150 % en ETH respecto al valor total custodiado. En caso que esta ratio sea inferior al 150 %, se verán liquidados y perderán su colateral, el cual se usará para recomprar los tBTC a los usuarios (con una prima) y quemar el token.

RenVM, en cambio, usa un sistema diferente. Los darknodes en RenVM deben estar constantemente rebalanceando su colateral en tokens ren (debe ser siempre del 300 %), algo similar a lo que sucede en Synthetix, en función de la demanda de renBTC. Esto hace que el valor del ren dependa exclusivamente de la usabilidad y el valor del protocolo, con lo que, en caso de que el protocolo esté a punto de llegar a niveles de colateralización muy bajos, se puedan reajustar las comisiones para aumentar el valor del token y evitar situaciones de peligro. Esto no solo aumenta el valor, sino que hace que se reduzca la demanda y por tanto suaviza el peligro porque ahora el coste de tokenizar bitcoins es mayor. En definitiva, como el valor del token está ligado a la plataforma y este sirve como colateral, en caso de fluctuaciones del protocolo o del propio token, el hecho de poder modificar las fees permite volver a equilibrar el sistema, dándole más seguridad y estabilidad en situaciones de riesgo. Un sistema muy similar a Synthetix, que usa su token nativo SNX como colateral del protocolo.

Con todo ello, parece que Keep es claramente más sólido a corto plazo, pero a su vez también menos flexible, lo que le puede salir demasiado caro en situaciones críticas como lo sucedido durante el Jueves Negro con la caída catastrófica del ETH.

**b) Capacidad del sistema**

El mercado total al que puede acceder cada protocolo es muy diferente. En este caso, Keep es claramente superior, ya que su potencial depende de la capitalización de Ethereum. En cambio, RenVM depende del valor del token ren, y solo podrá generar un total de ⅓ de ese valor, ya que debe mantener un colateral del 300 %.

La ventaja de Keep Network aquí es que necesita poco tiempo para conseguir que su sistema esté plenamente operativo. ETH es un activo muy maduro, con mucha liquidez, los usuarios en DeFi están más acostumbrados a usarlo como colateral y los mecanismos de liquidación deberían funcionar correctamente. En el caso de RenVM esto es contrario, ya que dependen de un mercado que, encima, hoy en día es pequeño.

Esta misma situación es muy diferente a largo plazo. En el día uno es imposible que RenVM acumule 500 MUSD, pero, con el tiempo, con el aumento continuo de la demanda de renBTC, la valoración de ren se incrementa, igual que su market cap. Esto loop positivo es muy interesante para los darknodes, ya que ellos no deben hacer nada, y no solo van a recibir fees sino que van generar ingresos por el aumento del valor del ren.

Con Keep, esta relación entre el aumento de la demanda y el aumento de la capacidad de generar tBTC no existe, ya que podría pasar que, aunque la demanda aumente, la demanda para ETH baje, no solo por una bajada en el precio, sino también porque aparezcan oportunidades de inversión alternativas más interesantes que mantenerlas en Keep. Por ejemplo, usar el ETH para añadir liquidez en Uniswap o generar préstamos en Maker.

**Conclusiones**

La realidad es que los protocolos son muy similares y cada uno tiene sus ventajas y sus desventajas. Mi objetivo es dar a conocer estas diferencias y dar valor a RenVM , que a pesar de parecer *peor* a primera vista, ya que no usa un colateral tan sólido como Keep, su potencial a largo plazo es de lo más interesante.

# GESTIÓN DE CARTERAS DE INVERSIÓN CON PROTOCOLOS DEFI

# 31. Encuadre temporal de cualquier inversión

En esta última parte del libro introduciremos las herramientas y metodologías para que, habiendo ya analizado los principales protocolos DeFi, puedas diseñar tú mismo tus propios productos financieros y carteras de inversión.

Invertir no es otra cosa que poner a producir un valor, un dinero y tener una expectativa de incremento en un periodo. Recalco: valor, incremento y tiempo.

Ninguna inversión tiene sentido si no la encuadramos en un marco temporal: minutos, horas, días o años. Lo primero que debes plantearte es cuánto tiempo puedes dejar bloqueada una inversión esperando su rentabilidad: ¿necesitas ese dinero o activo para otra cosa?

No debes tener prisa a la hora de entrar a comprar un token o cualquier tipo de producto financiero, debe ser una decisión lo más analítica posible y en base a un posible rendimiento.

Y digo posible (y no seguro), porque puede cumplirse en un porcentaje, o no. Imaginemos que compras un token al valor de 1 con la expectativa de que llegue a 2 en un marco temporal de un año, pero finalmente llega a 1,2. Has conseguido un 20 % de tu objetivo.

De igual manera debemos medir el riesgo, que es la posibilidad de que se cumpla mi expectativa: en este caso, incrementar el valor un 100 %.

El análisis completo sería:

Estoy en la posición de adquirir 100 unidades del token A, cuyo valor hoy es de 1, con la expectativa de que llegue a 2 en un año, sabiendo que tengo una incertidumbre o probabilidad aproximada del 70 % (la probabilidad no es sí o no: será más cercana al 100 % si estamos en una tendencia alcista, o cercana a 0 % si estamos en tendencia bajista). En este caso, estaríamos asumiendo un riesgo mínimo del 30 %.

Otro análisis es obtener la probabilidad estimada y el riesgo analizando cómo se comporta ese activo respecto al mercado y su evolución histórica.

En todo caso debes entender que las predicciones se pueden cumplir (o no), por lo que debes medir y entender la posibilidad de pérdida aceptándola como parte de la evolución de tu cartera; eso sí, protegiéndola en la medida de lo posible.

Como las inversiones cripto invitan mucho al gaming, te recomiendo que te hagas estas **preguntas poderosas** antes de darle al clic de comprar, swapear o vender:

- ¿Qué puedes ganar/perder?
  Me refiero a un valor concreto, a que incluso esboces un número de cabeza.
- ¿El token que adquiero, qué blockchain o proyecto representa?
  Especialmente con proyectos emergentes, debes entender muy bien sus tokenomics.
- ¿Es inversión o es probar suerte?
  Esta es la pregunta clave. Si quieres probar suerte (probabilidad de éxito) sé consciente de que solo el 2 % de las inversiones de especulación consiguen tener una rentabilidad jugosa.
- ¿Con ese dinero, en qué otro token podrías invertir?
  De alguna manera se trata de medir el coste de oportunidad.

Hay muchas maneras de enfocar un proceso de inversión. Cada cual tiene sus propios hábitos, pero mi principal consejo es que tengas claro un objetivo concreto de ganancia en un tiempo concreto. Y que este porcentaje de ganancia o pérdida no suponga un valor representativo más allá del 3 % - 5 % sobre el total, de tal manera que las ganancias vengan de un proceso reiterativo y no de operaciones aisladas.

De esta manera tendréis el riesgo mejor controlado y diversificado en inversiones adecuadamente estructuradas.

# 32 Conceptos útiles sobre inversión

Quizás ya conozcas la mayoría de estos conceptos, así que vamos a enfocarlos en cripto para que sean útiles en tu día a día. Recuerda que es una aproximación sencilla a un área de conocimiento muy amplio: se trata de una simplificación para acelerar el proceso de aprendizaje.

## 32.1. Tasa de descuento o coste de oportunidad

Con este concepto me gustaría introducir la visión desde lo macro a lo micro, es decir, cómo será de buena nuestra inversión si la comparamos con otra inversión de características similares que esté disponible en el mercado o incluso con la propia tendencia del mercado.

Imaginemos que queremos comprar 100 tokens X, y dicho token tendrá, en un año, un aumento de precio del 100 %. Pero sabemos, además, que el mercado tenderá a incrementarse en un 200 % de media al final de ese año. Lo que *a priori* podría parecer una buena oportunidad de inversión, al compararlo con la tendencia global no lo es.

Por ello, una muy buena recomendación es que siempre tengas en la cabeza cómo está evolucionando el mercado de manera objetiva y aritmética (es decir, haciendo números con lápiz y papel) para tener datos concisos y al menos poder construir una predicción básica.

La tasa de descuento además, es la corrección de la tasa de interés: poner en perspectiva un valor futuro y traerlo al presente para verificar su viabilidad. De una manera más precisa, la tasa de interés sirve para aumentar el valor (o añadir intereses) al dinero actual. La tasa de descuento, por el contrario, resta valor al dinero futuro cuando se traslada al presente, al menos que sea negativa. En caso de que la tasa de descuento fuera negativa, se entendería que, contrario a lo que indica la teoría, el dinero futuro vale más que el actual.

Por ello, para que las comparaciones entre distintos proyectos de inversión sean homogéneas, debemos considerar el riesgo de cada uno, y esto se resuelve incorporando su efecto en la tasa de descuento.

Así, podemos afirmar que la tasa de descuento tiene dos componentes:

- El **coste de los recursos financieros** utilizados o rentabilidad mínima que debemos exigirle a la inversión.

- **La prima de riesgo.** Si la nueva inversión que estamos analizando presenta más riesgo que la que estamos tomando como referencia, debemos exigir más rentabilidad a la nueva; es decir, deberíamos aumentar su tasa de descuento.

## 32.2. Coeficiente beta (β)

El coeficiente beta es muy similar a la tasa de descuento, dado que compara la rentabilidad de una inversión (en nuestro caso, token) con la del índice sectorial al que pertenece la acción y la rentabilidad del índice del mercado general.

A mí me gusta la expresión contribución al riesgo; es decir, si nos hemos marcado un objetivo, ¿el token/activo/inversión nos acerca o nos aleja al objetivo?

Este coeficiente indica la sensibilidad histórica (dado que nos basamos en datos históricos) de la evolución de la cotización de una determinada acción ante la evolución del índice de referencia del mercado al que pertenece la acción. Es decir, cuánto sube o baja la cotización de una determinada acción ante variaciones del 1 % en el índice de referencia del mercado.

En el caso de los criptoactivos, la tendencia es seguir en un porcentaje elevado a BTC y ETH: si estos suben o/y bajan, el mercado general lo hará también en mayor o menor medida.

De esta manera, si la beta es positiva, ante subidas del índice del mercado se producirían subidas en la cotización de la acción. En cambio, si la beta es negativa, ante subidas del índice del mercado se producirían subidas en la cotización de la acción.


Figura 151. A mayor coeficiente beta, más riesgo

Una nota: los coeficientes beta solo tienen sentido en el momento histórico de la fecha de su cálculo, no tienen vigor en otro momento, incluso en el actual.

Si quieres avanzar más en este tema, investiga sobre el modelo CAPM, que explica cómo el riesgo de una acción se descompone en dos tipos: el **riesgo sistemático**, que deriva del riesgo del mercado al que pertenece, y el **riesgo asistemático**, que deriva de las características concretas de la acción o token del proyecto. El coeficiente beta mide este riesgo asistemático, es decir, el riesgo individual de la acción mitigado en su totalidad por el riesgo de mercado.

Mientras que el riesgo sistemático se mide por la prima de mercado (que sigue la tendencia de los tokens más potentes: BTC, ETH, etc.), el cociente beta es una

medida del riesgo inherente a un valor, tomando como referencia un indicador representativo del mercado; es decir, el coeficiente beta determina la volatilidad de un activo.

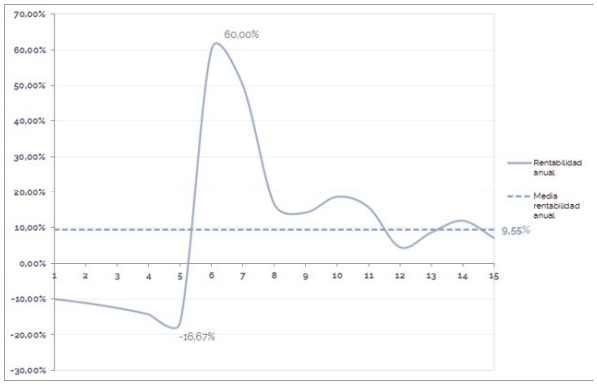
De esta manera, puede decirse que beta es directamente proporcional a la variación del mercado; es decir, el valor de un activo se moverá con el mercado en la medida de lo grande o pequeña que sea su beta; pero (siempre hay un pero) hay activos que tienen un comportamiento extraño; su beta es negativa, lo cual significa que van a moverse de manera inversamente proporcional al mercado.

El rendimiento esperado de un activo depende solo del riesgo sistemático de ese activo.

De ahí viene esa famosa frase en finanzas: «Mayor riesgo, mayor rentabilidad».

## 32.3. Volatilidad de un activo

Este es otro de los términos que escucharás con frecuencia, habitualmente con una connotación negativa. En realidad **no es algo negativo**, puesto que la volatilidad genera movimiento de precio y volumen, lo que a su vez genera oportunidades de inversión. Enlazándolo con el término anterior, podemos decir que el coeficiente beta determina en cierta manera la volatilidad de un activo si lo referimos al mercado.




La volatilidad es lo que varía la rentabilidad de un activo respecto a su **media** en un periodo determinado. Por tanto, la volatilidad es un concepto que referencia exclusivamente al activo o token. Es su propiedad intrínseca.

Para muchos, en especial para los académicos, cuando se dice que un activo tiene una alta volatilidad, se está haciendo referencia a que sus rentabilidades en el periodo analizado han sido muy diferentes entre sí, considerando al activo en cuestión como un activo de alto riesgo.

## 32.4. Riesgo de una inversión

La palabra riesgo la escucharás muchas veces y en multitud de entornos: inversión de riesgo, cartera de riesgo, protocolo DeFi con mucho riesgo, etc. No lo asocies a una connotación negativa. El riesgo realmente es la probabilidad de cumplir un objetivo de inversión, con lo que, cuando hablemos de un activo de riesgo, nos referiremos a que dado que su volatilidad es alta, podemos llegar a nuestro objetivo de beneficio, o no, con un % de incertidumbre. La mejor manera de cuantificar un riesgo y evitar el término alto riesgo, es darle un valor; por ejemplo: BTC llegará a 20 000 USD en abril de 2021 con una probabilidad del 70 %.

En otras palabras, podríamos hablar de riesgo de pérdida, es decir, qué porcentaje de nuestro capital podemos perder si nos afectara la volatilidad del activo en un porcentaje concreto.

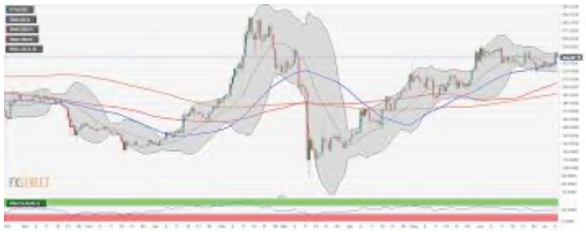


Figura 152. Riesgo de pérdida en una inversión en función de la volatilidad del activo

Del gráfico anterior podríamos decir que el riesgo de pérdida puede ser la diferencia entre el punto en que el valor del activo está más bajo y el valor de entrada (izquierda).

La volatilidad, como hemos visto previamente, es la diferencia entre el valor más alto y el valor más bajo, en términos generales.

## 32.5. Medias móviles y aritméticas

Aunque parezca una obviedad, muchas veces analizar el valor medio de una evolución de valores nos permite ver un panorama objetivo (un valor concreto) en un tiempo futuro. Especialmente en el mundo cripto, debido a la variación de los precios por día —o incluso por hora— no es intuitivo predecir en qué valor podemos fijar nuestra predicción futura pues puedes seleccionar el valor máximo o mínimo del día, o cualquier otro, y en función del que analices te saldrá una rentabilidad distinta.

Por eso te recomiendo que uses el dato del **valor medio** para esa primera aproximación de tu predicción. En la mayoría de las plataformas puedes seleccionar el modo de visualización incluyendo la media.

Figura 153. Cotización de BTC con indicadores de precio, volumen y volatilidad (Huobi)

Habitualmente puedes completar la vista con una gran variedad de indicadores, aunque no te recomiendo que lo hagas en una primera fase de detección de oportunidad.

En el gráfico anterior, extraído de Huobi, puedes ver, en la parte superior, el precio, la media móvil y la media; en la parte media, el volumen y la volatilidad, y, la parte inferior, el canal de precio.

Un inicio sencillo es analizar precio, volumen y media. Con esos tres valores puedes ver posibles entradas/salidas de operación, para posteriormente analizarlos con otros indicadores más complejos con la idea de crearte un panorama o proyección.

## 32.6. Capitalización de mercado (market cap)

Este indicador debes tenerlo siempre en la cabeza, dado que indica la salud del criptoactivo. El mercado cripto es mucho más dinámico que el mercado tradicional y los volúmenes de movimiento tienen más variación.

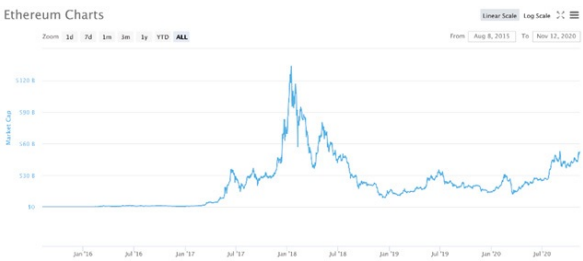



Figura 154. Precio de ETH en escala lineal 2016-2020. Coinmarketcap

Para determinados momentos es recomendable usar la escala logarítmica, especialmente cuando la evolución del precio se vea influenciada por el interés compuesto, de tal manera que podremos ver la evolución de una manera más descargada.

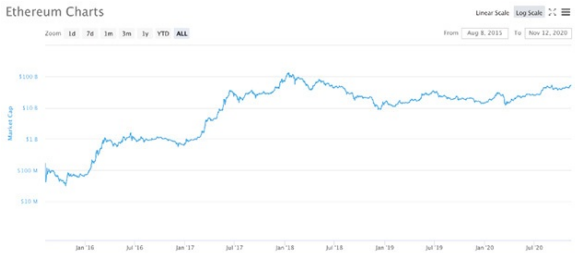
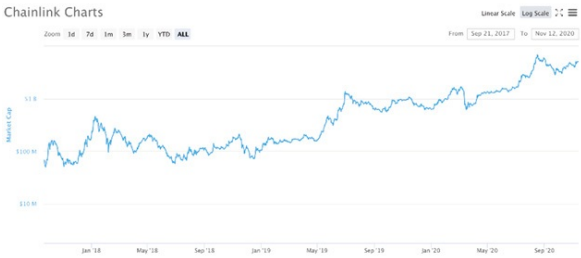



Figura 155. Precio de ETH en escala logarítmica 2016-2020. Coinmarcketcap

Con esta simplificación eliminamos ruido de la gráfica y entendemos la salud de su crecimiento. La recomiendo usar también en los momentos iniciales de capitalización de los proyectos, que es cuando los incrementos son más elevados frente a la media diaria o semanas.




Cuando diseñes una estrategia de inversión, ten en cuenta el volumen de capitalización (hora/día) como un elemento de confirmación del precio, es decir, si el volumen es alto, es que el mercado la está dando por buena tanto si es una bajada o una subida, y se consolidará.

Precio y volumen es la constatación de una tendencia. Sería como precio = velocidad, y volumen = aceleración. Así, el precio de tu activo puede estar a velocidad constante y subir o bajar por efecto de la aceleración (volumen de mercado).

## 32.7. Bandas de Bollinger

Es una herramienta visual para detectar tendencias en oportunidades de mercado. Recuerda que una oportunidad es tanto subida como bajada de precio, y viene generada siempre por un movimiento de mercado en volumen de transacciones.

Se representa mediante dos líneas, por encima y por debajo de una media móvil central que abarca el precio. Es, por lo tanto, una banda muy intuitiva. De una manera muy sencilla, cuando las bandas de Bollinger se desvían, la pendiente de las bandas seguirá a la de la media móvil central y, por lo tanto, irá hacia arriba y hacia abajo.

Las fases de tendencia se inician cuando una vela sale de una de las dos bandas externas, muy por encima o por debajo de los movimientos recientes. Es importante conocer que, cuando las bandas se expanden (en anchura), va a haber un movimiento del precio en alguna dirección.

Figura 156. Bandas de Bollinger en el precio de ETH

Si trabajas con estas bandas, recuerda que la información relevante que aportan es sobre volatilidad. Los precios pueden exceder la banda superior e ir por debajo de la banda inferior. En todo caso, el cierre de velas fuera de las bandas de Bollinger son señales de continuidad y no de inversión, simplemente determina si los precios están altos o bajos en relación con la base, que es la media móvil.

## 32.8. Bandas de Bollinger + RSI

Una muy buena combinación de indicadores es usar las bandas anteriores con el indicador RSI (índice de fuerza relativa), que mide la relación entre los movimientos ascendentes y descendentes y normaliza el cálculo para que el índice fluctúe en un rango de 0 a 100.

Debes tener en cuenta que:

Un indicador RSI alrededor del nivel 30 se trata de una situación en la que los precios han caído bruscamente y ahora el movimiento podría perder fuerza. Y al revés: alrededor del nivel 70, indicaría sobrecompra y tendencia a que el movimiento se debilite. Como último apunte, cualquier cruce de los niveles de 30, 50 y 70 da señales de trading.

Figura 157. Bandas de Bollinger + RSI en el precio de ETH

No es el método más preciso, pero es muy intuitivo y visual. Con algo de práctica, puedes detectar zonas de inversión usando las bandas superior e inferior.

Las señales de trading pueden ser de esta manera: **señal de compra** si el precio rompe por debajo de la banda inferior de Bollinger (pero solo si el RSI es inferior a 30), y **señal de venta** si el precio supera la banda superior (solo si el RSI es superior a 70).

# 33. Plataformas de visualización de estados de cartera

Una vez que des el paso de gestionar de una manera profesional tu cartera de criptoactivos y portfolio de inversión, debes contar con una herramienta de visualización que te permita detectar de un vistazo cómo está configurada.

Para un primer acercamiento, hay varias plataformas gratuitas que te permiten tener un encuadre visual simplemente con conectar tu wallet a la plataforma. Incluso puedes ver el avance histórico, la composición en peso y porcentaje de la cartera, transacciones pasadas, etc. En este capítulo vamos a revisar las más utilizadas.

## 33.1. Zerion

**https://app.zerion.io/**

Zerion es una plataforma que permite entrar en tu wallet de manera activa (entrando por MetaMask o wallet frío) o pasiva, simplemente en modo visualización de una dirección de wallet.

En modo visualización (sin conectar tu wallet), tan solo puedes ver la evolución histórica, las transacciones realizadas, y luego datos del mercado, pero no puedes realizar operaciones. Puedes dejar en watchlist cualquier wallet, no solo el tuyo.

Representa de una manera muy sencilla la composición de la cartera, estimando el porcentaje en peso de la misma. Además, si el activo ha aumentado de precio en las últimas veinticuatro horas, se coloca en color verde, y, si ha bajado, en color rojo.

Te aconsejo entrar en su blog[3] para leer sus últimas features y noticias relevantes.

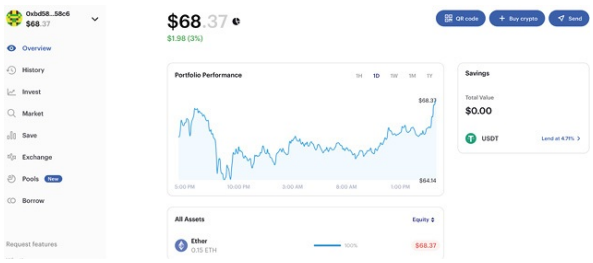



Figura 158.Interfaz principal de Zerion

En el apartado «Market» puedes encontrar la evolución de la mayoría de los tokens ERC-20 con su incremento en uno, treinta y noventa días, así como su market cap.

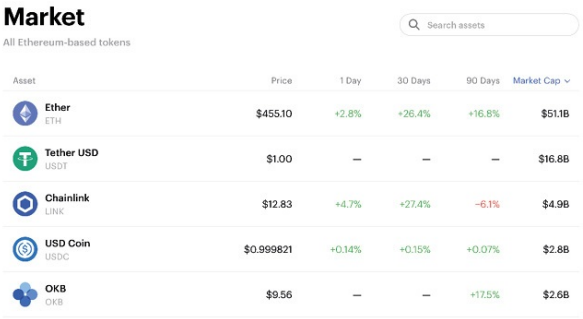



Figura 159. Interfaz «Market» en Zerion

# 33.2. DeFiSaver

**https://defisaver.com**

Esta es una aplicación más orientada a funcionalidades DeFi y no tanto a la evaluación de la cartera. Sin embargo, te permite acceder de una manera muy sencilla a los principales protocolos en la parte de la izquierda: Aave, Compound, Maker. También a tres apartados más: «Smart Savings», «Exchange», y «Loan Shifter».

En la parte superior derecha tenemos el símbolo del gas, que nos indica a qué precio se encuentra en tiempo real. Muy útil.

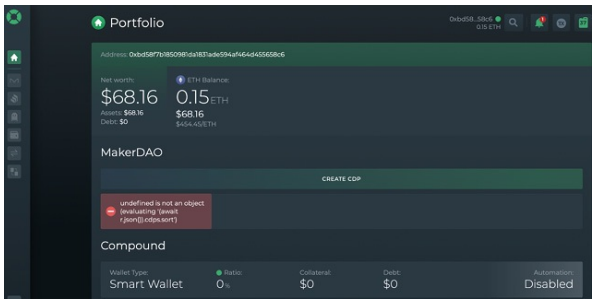


Figura 160. Interfaz principal de DeFiSaver

Una de las funcionalidades más interesantes es la posibilidad —una vez tengas alguna posición de préstamo y colateral— de cambiar de protocolo, activo colateralizado o reducir/ampliar la deuda, todo ello de una manera unificada y rápida.

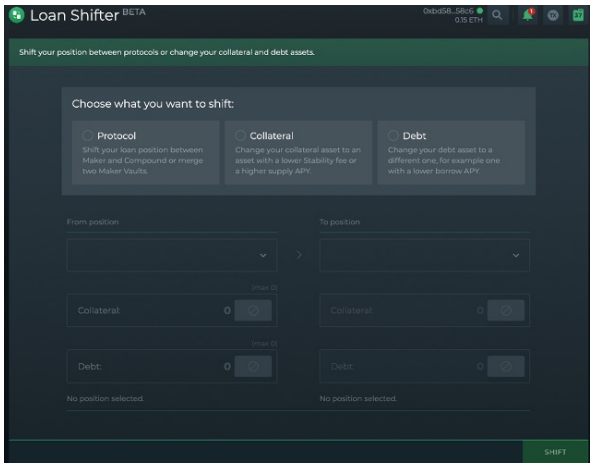


Figura 161. Detalle de la Interfaz de DeFiSaver

# 33.3. DeBank

**https://debank.com**

Es una plataforma muy intuitiva que analiza tu cartera y la composición de la misma, similar a Zerion. En la landing nos muestra los tres proyectos de la semana y un gráfico de la evolución de la capitalización del mercado DeFi.

En la parte de dashboard resume la posición de tu cartera, con la evaluación de tus posiciones de deuda y las posiciones de tus activos, asignando un valor total al conjunto. No lo representa de manera gráfica, solo en valor actual.

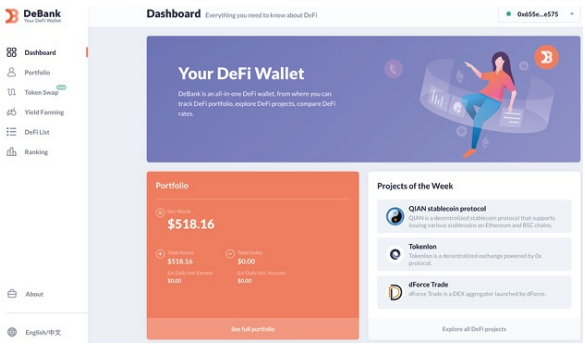



Figura 162. Interfaz principal de DeBank

3. https://blog.zerion.io/zerion-community-update-october-2020-c02bbf6a6fe2

# 34. Trading. Análisis fundamental y análisis técnico

## 34.1. Diferencias y similitudes AF/AT

Hay dos partes fundamentales y dependientes entre sí en cuanto a técnicas de análisis, que son el **análisis fundamental** (alto nivel e influencia de mercado) y el **análisis técnico** (análisis visual y gráfico).

Una vez que entres en el mundo de inversión cripto, pasarás a trabajar el trading, que es básicamente invertir en criptoactivos de manera autosuficiente y autónoma sin depender de intermediarios financieros.

El **análisis fundamental** se usa para tener en cuenta todos los factores que afectarán a los activos digitales, desde variables macro y microeconómicas, aspectos de demanda y oferta, así como los comportamientos del mercado.

El uso de este método para el análisis a corto plazo rara vez es rentable y representará pérdidas, dado que estos factores requieren tiempo para mostrar su efecto en el mercado. Como se vio en la década pasada, desde la llegada de Bitcoin las criptomonedas cambian de precio en períodos cortos, lo que ha generado interrogantes sobre el uso del análisis fundamental para predecir los precios futuros. Sin embargo, es muy útil para el análisis de otras criptomonedas que se ven influenciadas por los movimientos de Bitcoin (que son todas en mayor o menor porcentaje).

A diferencia del análisis fundamental, el **análisis técnico** se centra en los movimientos de precios a corto plazo de los activos digitales: un minuto, una hora, un día o una semana. Esto implica utilizar los gráficos de precios para identificar tendencias y patrones a partir de los cuales el trader hace una predicción del precio.

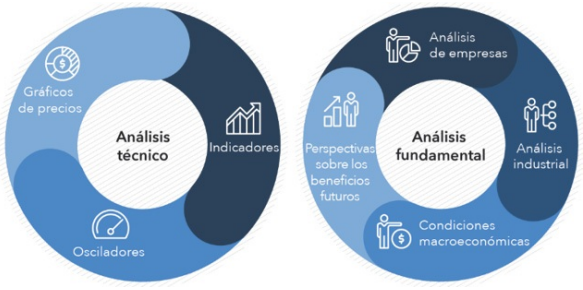



Figura 163. Diferencias entre análisis fundamental y técnico

La mayoría de los operadores de monedas virtuales (y algunos otros traders de activos individuales) se centran en el análisis técnico, ya que ofrece la

oportunidad de hacer dinero rápido. Dada la alta volatilidad experimentada en las criptomonedas en los últimos años, el análisis técnico se está convirtiendo en la disciplina favorita de los que esperan obtener ganancias en los mercados cripto. Mi consejo es que huyas de la mera especulación, o al menos, que esta no sea tu centro geométrico de la cartera.

Sin embargo, el análisis fundamental en relación a las monedas digitales y nuevos proyectos DeFi es único en comparación con la forma tradicional, ya que nuevos factores son añadidos al estudio constantemente, por considerar los inversores que los mismos ejercen algún tipo de influencia en el precio de los activos digitales, de impacto social, de usabilidad, de cambio de paradigma, etc. Algunos de estos factores son:

**a) Capitalización de mercado**

La capitalización de mercado permite conocer el valor en efectivo de las criptomonedas en circulación. Este valor se obtiene al multiplicar el número total de monedas en circulación por el precio de cotización que muestra la moneda digital. El valor lo puedes encontrar en www.coinmarketcap.com.

Este indicador ofrece una imagen clara de la cantidad de monedas actualmente en uso en comparación con otras. Una gran capitalización de mercado señala un mayor valor en el uso de la moneda y viceversa, además de influencia sobre otras criptomonedas.

Por otro lado, puedes además bucear en www.etherscan.io para analizar qué porcentaje de tokens tienen los inversores (la rich list de cada proyecto), número de wallets que posee el token y transacciones sobre el activo; y entender si el proyecto está vivo o no.

**b) Análisis de desarrollo**

Una de las áreas clave que los usuarios deben verificar es el progreso del desarrollo de la criptomoneda. Una forma clara de medir esto sería a través del número de revisiones aprobadas agregadas en la página de GitHub, e incluso revisar en etherscan.io si los smart contracts están auditados y por quién.

**c) Posición de gobiernos frente a las criptomonedas**

Desde la fuerte caída en los precios de la criptomoneda a principios de 2018, ciertos gobiernos han emitido una postura firme contra los activos digitales. La regulación en la industria está dando pasos cautelosos, pero continuos, a medida que las jurisdicciones de todo el mundo diseñan una transición sin fricciones a esta nueva clase de activos. Una postura positiva sobre un activo digital muestra

que el futuro de la criptomoneda es más confiable a medida que las instituciones de gobierno las integren, lo que también constituye un fuerte soporte para su adopción entre el público general.

Otro aspecto muy favorable es que El BCE esté pensando en un euro digital, no por el hecho de que funcione dicha cripto, sino porque quiera sumarse a la tendencia cripto, aunque bajo mi criterio es un paso extraño: no es descentralizado, no está desligado de las políticas de BCE, y, por lo tanto, no es afectado por las políticas expansivas o contraccionarias.

**d) Posición social**

Los proyectos de monedas digitales también cobran vida a través de foros comunitarios que ofrecen una gran oportunidad para comprender mejor la propuesta y evaluar los puntos de vista de sus seguidores. Los sentimientos positivos y las relaciones en torno a los miembros de la comunidad ejercen un efecto beneficioso en el precio de la moneda.

Podemos ser capaces de detectar y medir este sentimiento si revisamos etherscan.io en su parte casilla de social, dado que recoge los mensajes y comunicaciones que emiten las empresas en Twitter, Facebook, etc.

**e) Evolución de los índices de bolsa en USA**

No podemos olvidar que las bolsas americanas tienen un gran movimiento y condicionan al resto de las bolsas mundiales. El mundo cripto no va a ser menos, sufre su influencia. Os recomiendo seguir whalealert en Twitter o en versión web. Es un bot que te avisa de grandes movimientos de cripto en el mercado.

**f) Estrategia de adopción**

Otro aspecto muy relevante cuando analizas el proyecto y su token asociado, es tener claro si dicho proyecto tiene un camino de ruta que genere tracción. La estrategia de adopción es el puente entre las ideas y los resultados. Muchos proyectos cripto mueren porque no son capaces de seguir un plan y pivotar sobre él.

## 34.2. Trading técnico: soportes y resistencias

Una vez que entres en el mundo de inversión, pasarás a trabajar el trading de activos cripto, que trata, en esencia, de invertir de manera autosuficiente y autónoma sin depender de intermediarios financieros.

El trading técnico está basado en los análisis gráficos y creación de escenarios. El primer paso será entender qué son los soportes y resistencias, para entender cómo evoluciona el mercado y cómo te pueden permitir entrar o afectar a tu cartera.

Los soportes y resistencias son aquellos niveles donde el precio se detiene. Y se detiene porque es el punto donde las fuerzas alcistas y bajistas se oponen (oferta y demanda) de manera más intensa, generando una reacción o movimiento contrario a la tendencia:

- Soporte. Nivel en el que el precio frena su descenso para volver a subir.
- Resistencia. Nivel en el que el precio deja de subir para comenzar con su descenso.

Cuantas más veces en el tiempo el precio haya realizado ese comportamiento en dichos niveles, más *sencillo* será predecir el movimiento del precio en el futuro, dado que son considerados niveles psicológicos; es decir, los traders tienden a comprar o vender en esos puntos, lo que ayuda a fortalecerlos. Un punto tipo de soporte y resistencia es cuando el precio termina con varios 0. Estos se denominan «niveles psicológicos».

La manera más fácil de empezar a trastear es que escojas una buena plataforma, me refiero a usable y sencilla, y mediante pantallazos y usando el mismo Paint o programa de dibujo, tires líneas.



Realiza estas primeras tareas para entender cómo se construyen los análisis técnicos:

- Pinta y señala máximos y mínimos históricos = soportes y resistencias horizontales.
- Une los distintos máximos y los distintos mínimos = tendencias alcistas o bajistas, uniendo los máximos y mínimos con líneas de tendencia o canales.

- Señala los soportes y resistencias en los niveles psicológicos.
- Cuando hayas realizado esta primera parte puedes confirmar con otros indicadores si, efectivamente, los puntos son relevantes o no (¿coinciden los indicadores con tus dibujos?).

Acostúmbrate a pensar dibujando antes de tomar decisiones sobre compra o venta. Gran parte del movimiento del mercado es fomo, y tiene una componente psicológica muy importante. Evita realizar cualquier acción coaccionado por el miedo, el pánico o el ansia. Dibuja, calcula y actúa.

Recuerda que no hay una herramienta perfecta, así que prueba varias y decide cuál es la que mejor se adapta a ti, no en complejidad y opciones de cálculo sino en sencillez. El aprendizaje es un camino, ve poco a poco. A continuación comienza a dibujar y testar, a hacer pruebas y ver si se cumplen tus tendencias, de manera global. Porcentúa qué grado de éxito has tenido.

El camino formativo debe ser a través de estas etapas:

**a) Fase de prueba**

Abre y prueba todas las herramientas e indicadores de soportes y resistencias que desees. No hay límites aquí, ya que puedes probar y trabajar con los diferentes niveles. Hay muchos indicadores disponibles, así que tómate tu tiempo para revisarlos todos y anota los que te parezcan más interesantes. Te he indicado cúales son los habituales y más sencillos, pero aplica todos y luego descarta.

**b) Fase de investigación**

Una vez que hayas realizado una breve lista de las herramientas e indicadores que te parezcan más interesantes, tómate un tiempo para comprenderlas con mayor profundidad.

**c) Fase de práctica**

Una vez que hayas reducido la lista a solo unos pocos y comprendas las herramientas y los indicadores de soportes y resistencias a un nivel más avanzado, es hora de la siguiente fase, que es practicar y probar estas herramientas.

Trata de adquirir un mejor entendimiento y comprensión de los métodos que funcionan bien con esos niveles de soportes y resistencias.

**d) Fase de decisión**

Elige las herramientas de soporte y resistencia que mejor se adapten a tu estrategia de trading, psicología de trading y tiempo disponible. Comienza a elaborar pronósticos y a tenerlos registrados, siempre con la triple variable: precio/volumen/tiempo.

**e) Fase de Integración**

Después de que se complete la fase de prueba, asegúrate de que la herramienta para determinar soportes y resistencias esté totalmente integrada en tu plan de trading. Integrar significa que de manera automática analizas con un gráfico, esbozas un número y decides si entrar o no.

# 35. Gestión de carteras

## 35.1. Introducción a la gestión de carteras

La gestión de la cartera es la organización profesional y analítica de los activos financieros, incluyendo una evaluación sistemática para reducir el riesgo y maximizar la rentabilidad.

Dado que estamos en el entorno cripto y DeFi, serás tú quien va a gestionar tu cartera de valores. Esto equivale a tener el control de tus inversiones bursátiles en todo momento, decidiendo dónde y cuándo invertir, controlando rigurosamente el riesgo y optimizando el tiempo que dedicas a administrar tu cartera.

Debes mantener una actitud activa, es decir, implica tomar decisiones de inversión calculadas y utilizar estrategias de mejora, balanceo, etc.

La gestión de cartera comienza con estas tres fases principalmente:

1. **Selección estratégica de valores.** Establece unos criterios para reconocer lo que consideramos valores buenos y cuándo entrar.
2. **Seguimiento de la evolución de la cartera.** Tener KPI o elementos de medición que te permitan ver la subida o bajada de tus activos. Piensa que unos activos bien diversificados reducirán tu riesgo de exposición frente a las tendencias de mercado.
3. **Valoración de resultados. Estimar si estás alcanzando los objetivos a corto plazo para plantear estrategias diferentes en caso necesario.**

## 35.2. Gestionando tu primera cartera

Cuando gestiones tu primera cartera, tendrás que autoanalizarte para entender cómo quieres gestionar tu posición. Te recomiendo que te hagas un plan o análisis detallado de tus ingresos, deudas y posibles contingencias a un año vista, para que así puedas tener claro qué porcentaje económico puedes dedicar de manera independiente a la inversión.

En el entorno cripto tenemos una velocidad mucho mayor a la de los mercados tradicionales, con lo que debes ser capaz de adaptarte a este nivel de información y, sobre todo, tener resiliencia ante los movimientos impredecibles.

Algunos conceptos importantes sobre carteras son:

- **Tolerancia al riesgo.** Normalmente a mayor riesgo, mayor rentabilidad. La cartera ideal debería lograr un equilibrio del riesgo dependiendo de la tolerancia al mismo del inversor. Esto incluye activos con más riesgo o probabilidad de ganancia. Invertimos para sacar rentabilidad, pero también debemos protegernos.
- **Medición del rendimiento.** Establecer métricas diarias, referencias y objetivos te permite realizar un seguimiento de los posibles errores y conocer la ratio riesgo/rentabilidad. Te permitirá adquirir conocimiento.
- **Asignación de activos.** Los distintos activos avanzan en direcciones diferentes y tienen diferentes niveles de estabilidad. Elegir una mezcla de activos puede ayudar a reducir el riesgo y maximizar la rentabilidad ponderando la volatilidad e invirtiendo como corresponda.
- **Diversificación.** La volatilidad de los mercados y el riesgo es algo medible, con lo que puedes hacer cálculos que te permitan reducir exposición. Tendrás que entender que hay activos muy vinculados a la tendencia del mercado y otros que no, y debes incluirlos como estrategia de seguridad. Así, si un mercado se desploma, no perderás todo tu dinero.
- **Reestructuración.** El precio de los valores en el mercado cambia con el tiempo, afectando la rentabilidad de tus inversiones y la ponderación de las mismas en tu cartera. Reestructurar habitualmente tu portfolio te asegura que mantienes un buen equilibrio entre el riesgo y la rentabilidad, al devolver la ponderación de los activos a su nivel inicial.
- **Objetivo único.** Recomiendo que cada cartera tenga solo un objetivo de ganancia en un espacio temporal concreto, de manera que puedas tener varias carteras a la vez, diversificando aún más tu riesgo. Una vez llegado al objetivo, debes salir y mantener la ganancia en activos de menos volatilidad.

## 35.3. Estrategias globales de inversión DeFi

A nivel general te recomiendo plantearte estas cinco opciones de estrategias generales con los criptoactivos que tengas. Significa que frente a un criptoactivo puedes usar la estrategia que mejor encaje en tu balance de objetivos.

Un mensaje un poco agresivo sería: holdear no es gestionar una cartera de criptoactivos. Gestionar una cartera es conseguir que siempre estés obteniendo rendimientos, a pesar de la volatilidad del mercado mediante acciones y estrategia. Por lo tanto, comprar y mantener a ver qué ocurre en cinco años... no es una estrategia activa.

También se debe tener en cuenta que Bitcoin lo considero como un valor refugio y reserva de valor, por lo que no se incluye en estrategias DeFi.

Resumiendo: gastamos en dinero fiat, ahorramos en Bitcoin e invertimos en estrategias DeFi.

| | Velocidad entrada salida | Canal | Rentabilidad | Dificultad | Seguimiento |
|---|---|---|---|---|---|
| **Holding** | Muy rápida | Exchange / swap | Depende de la tendencia alcista / bajista | Nula | Bajo |
| **Staking** | Rápida | Maker / compound | Entre el 1 y el 7% | Baja | Bajo |
| **Pool** | Rápida | Uniswap | Holding + rendimientos de la liquidez | Baja / Media | Medio |
| **Bóveda** | Lento | Maker dao / aave | Holding colateral + trading del préstamo | Media | Medio |
| **Farming*** | Lento | Instadapp | Rendimiento holding + préstamo | Media | Alto |

Figura 165. Distintas estrategias globales de inversión DeFi

1. **Holding.** Ya lo hemos mencionado. Tiene sentido como estrategia complementando al resto. En función de nuestro nivel de riesgo tendrá más o menos peso respecto a las estrategias siguientes.
2. **Staking.** Es la segunda estrategia que te recomiendo, dado que adquirir y dejar depositado el criptoactivo en distintos protocolos te permite obtener un rendimiento con un riesgo limitado (solo la bajada de precio del criptoactivo).
3. **Pool.** Te permite compensar un criptoactivo volátil con otro menos volátil, habitualmente una stablecoin, lo que te da un porcentaje de protección en caída, pero también te limita el rendimiento en caso de momentos alcistas del criptoactivo volátil (impermanent loss).
4. **Bóveda.** Dado que es un préstamo en el que depositas un colateral, te recomiendo gestionarlo bien para momentos alcistas cuando puedes swapear a un activo con más crecimiento. O bien en momentos de caída para adquirir una posición de deuda con un ether más barato.
5. **Farming.** Ya vimos en capítulos anteriores la posibilidad de apalancarnos en incentivos aplicando complejas estrategias de inversión dirigidas a obtener el máximo rendimiento de cada protocolo y en tiempo real. La ponemos en último lugar porque solo es recomendable para carteras de mucho riesgo y en una proporción baja.

Entendiendo lo que hemos propuesto en este punto, cuando decidas adquirir un activo tendrás que pensar cómo obtener el mejor rendimiento del mismo usando estas cinco estrategias. El ejemplo más claro lo tienes en las stablecoins, que tienen que estar incorporadas en cualquier cartera: ¿por qué adquiero DAI o USDC si no tienen rendimiento? Porque estabilizan tu cartera ante fluctuaciones de mercado (aprovechando acciones en corto para apalancarte) y porque si las utilizas en bóvedas y pools sí obtienes rendimientos interesantes.

Otra variable que pongo sobre la mesa es la madurez del token; es decir, en qué estado está el proyecto dado que su crecimiento en las primeras fases es exponencial y posteriormente hace correcciones más drásticas, para luego continuar con una muerte lenta o una ascensión más o menos continua.

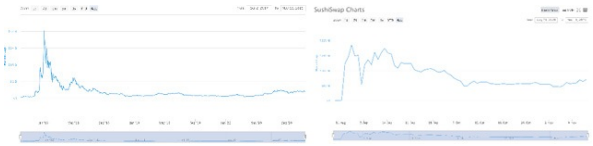


Figura 166. Cardano y Sushiswap como ejemplos de evolución clásica del precio del token

En base a este último argumento —contrastable con la mayoría de los tokens— debes reflexionar sobre lo que esperas al entrar en un token: ¿especular y coger toda la ola de subida, o esperas rendimiento moderado? Por ello es tan importante la diversificación.

Y siempre piensa sobre esta afirmación: lo que inviertas en un token de riesgo debe ser una cantidad que, llegado al punto de perder un 50 %, no te genere «una muerte en vida», y que lo que hayas ganado haya merecido la pena con el incremento conseguido.

## 35.4. Tendencias de mercado (criptoíndices)

En este apartado quiero hacer énfasis en que el mercado es quien marca la tendencia: ir contra el mercado en una posición de long te generará pérdidas a corto plazo. No ir contra el mercado es una buena estrategia para todo inversor no muy experimentado.

Aunque ir contra el mercado no es incompatible con aplicar técnicas de short para tener acciones de ganancia en el corto plazo frente a eventuales bajadas, recuerda que ir siempre en línea con el mercado disminuye el riesgo.

Te recomiendo que sigas estos cripto índices:

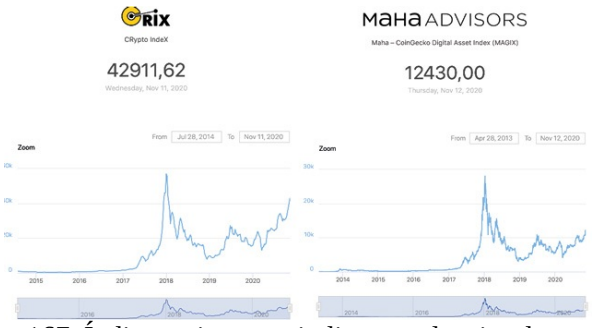



Figura 167. Índices cripto que indican tendencias de mercado

Como ya sabes, querido lector, bitcoin es el token más influyente en el mercado. Una posible cartera a desarrollar podría tener esta composición (ejemplo):

- Bitcoin 71.48%
- Ethereum 12.48%
- XRP 2.76%
- Chainlink 1.17%
- Bitcoin Cash 1.15%
- Binance Coin 0.98%
- Polkadot 0.97%
- Litecoin 0.93%
- Cardano 0.77%

Con esto quiero decir que siempre estés pendiente de noticias y evolución de los primeros cinco criptoactivos más importantes, lo que te permitirá adelantarte a posibles movimientos del mercado.

## 35.5. Panorama y objetivos

Una vez que tengas afinados números con respecto a tokens, cantidades y plazos de inversión, debes marcar el objetivo de ganancia. Es importante que te marques objetivos realistas con respecto a un token y no te veas influenciado por otros tokens o solo por casos de éxito. Recuerda que solemos hablar de las operaciones en las que ganamos, pero no en las que perdemos; así que echa un ojo a los históricos y entiende bien por qué puede subir un token y, al contrario, cuánto puede no subir y por qué.

Tu cartera siempre será activa, es decir, las ganancias que vayas obteniendo tendrás que sacarlas para reinvertirlas en otro token o en otra estrategia global (de las analizadas en el capítulo 34.3).

Así podrás conseguir un interés compuesto (con intereses varios). Estarás, por tanto, obteniendo interés de un primer incremento de valor, interés de nuevo en una segunda ola (si sigue subiendo), y además conseguirás interés de los beneficios obtenidos de la primera ola. Y, por supuesto, obtendrás rentabilidad compuesta con diversificación de riesgo.

Gráficamente se ve muy bien: mientras que el interés simple es lineal, el interés compuesto consigue finalmente bastante más margen.

Ten en cuenta que tus activos deben estar produciendo siempre: haz que tus beneficios también trabajen.

En DeFi el tiempo va mucho más de prisa, así como los rendimientos. Es fundamental que entiendas que un capital parado unos días podría haber generado un 1 %. Este interés, te lo podría dar un banco por mantener tus activos un año, así que los órdenes de magnitud en DeFi son muy superiores.

La salud de tu cartera tendrá mucho que ver con los ahorros y rentabilidades que vayas teniendo, así como la cantidad de stablecoin que puedas tener.

Por otro lado, debes mantener una posición mínima de ETH, dado que es la herramienta de trabajo con la que pagarás gas, harás colateralizaciones, etc., con lo que tendrás una posición de holdeo. Intenta tener siempre ETH disponible para oportunidades que detectes.

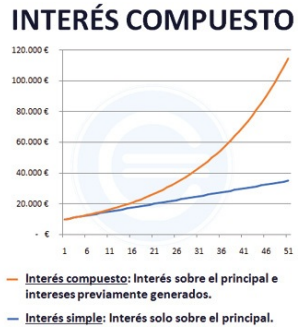



Figura 168. Características de las distintas estrategias de inversión

En la gráfica anterior puedes ver una propuesta de acción bastante moderada, donde añadimos el plan de contingencia que debes tener en caso de alarma.

Es fundamental saber qué debes hacer en caso de bajada drástica o de no cumplir con los objetivos proyectados. Solo te digo: piensa previamente para actuar lo más rápidamente, no pienses sobre la marcha y en estado de ansiedad. La estrategia se madura, la acción se hace.

## 35.6. Rebalanceo de carteras

Como hemos estudiado anteriormente, la gestión de carteras requiere de dedicación diaria o semanal, y, sobre todo, de planificación. Huye de improvisar.

El rebalanceo no es otra cosa que guardar tus beneficios y reequilibrar el peso de la cartera. Imagina que tienes un 50 % en wBTC y un 50 % en DAO, y en un mes has conseguido que wBTC haya subido un 50 %. Rebalanceo sería retirar el

porcentaje correspondiente a ese 50 % y pasarlo a DAI, de tal manera que tu cartera tiene consolidados sus beneficios y sigues teniendo el mismo valor total en wBTC.

Es una modificación de los porcentajes de holdeo, pero no una variación del precio porcentual de los activos con respecto al resto.

También puedes hacer un rebalanceo sobre otro tipo de activos, pero implicaría volver a hacer los análisis previos y volver a definir una estrategia global. Esto lo puedes hacer una vez cada dos meses, pero no cada día.

Por tanto, rebalancear consiste en devolver una cartera de inversión a su asset allocation inicial después de un ciclo de inversión donde los mercados hayan sufrido variaciones. El motivo más importante para rebalancear la cartera es para mantenerse fiel a las razones por las que se eligió el asset allocation. Son la base de cualquier plan de inversión. Y el asset allocation es la herramienta para ejecutarlo.

No rebalancear puede ser el detonante de que la inversión acabe en fracaso. Si cambian las condiciones del mercado, sería como estar invirtiendo con el asset allocation elegido por otro inversor que no tiene nada que ver contigo.

Yo te recomiendo que realices el rebalanceo de cartera según porcentajes, dado que tendrás los números hechos y será más fácil tu control. De esta manera sabrás cuándo realizar rebalanceo: cuando la distribución de los activos se ha ido por encima o por debajo de un porcentaje establecido de antemano. Los más utilizados son el 5 % - 10 %.

Existen algunas plataformas que automatizan, pero trabajarlas con lápiz, papel y calculadora es una buena idea.

## 35.7. Una cartera eficiente

Y ya para terminar este acercamiento a la gestión de activos, gestión de carteras y libertad financiera con productos en un entorno libre, autónomo y transparente, traemos un concepto demoledor: la cartera eficiente.

No es otra cosa que trasladar el modelo de Markowitz a nuestro mundo cripto y entender que siempre podremos mejorar nuestra cartera hasta un límite. Sería como la capacidad de estresar nuestros activos o el límite elástico de un material.

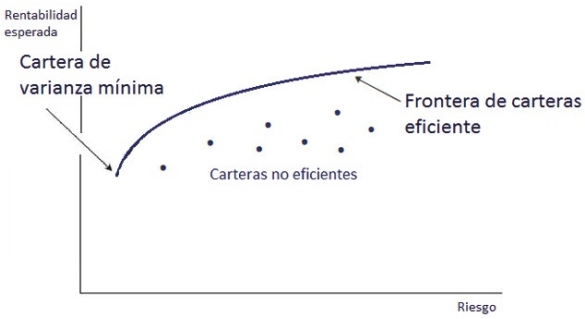


Figura 169. El modelo de Markowitz de cartera eficiente

Ya sabemos que las dos variables relevantes son rentabilidad y riesgo, con lo que para un determinado riesgo deberé obtener un porcentaje de rentabilidad y viceversa.

La teoría de formación de carteras se compone de tres etapas:

1. Determinación del conjunto de carteras eficientes.
2. Determinación de la actitud del inversor frente al riesgo.
3. Determinación de la cartera óptima.

Además, se apoya en los siguientes supuestos de partida:

- La rentabilidad de una cartera viene dada por su esperanza matemática o media.
- El riesgo de una cartera se mide a través de la volatilidad (según la varianza o desviación típica).
- El inversor siempre prefiere la cartera con mayor rentabilidad y menor riesgo. Hay que estudiar la relación rentabilidad, riesgo y liquidez.

Por lo tanto, la técnica de la cartera eficiente persigue calcular de manera conjunta las probabilidades de rentabilidad de cada activo de manera porcentual y cruzarlas con el porcentaje de riesgo (volatilidad) de los mismos.

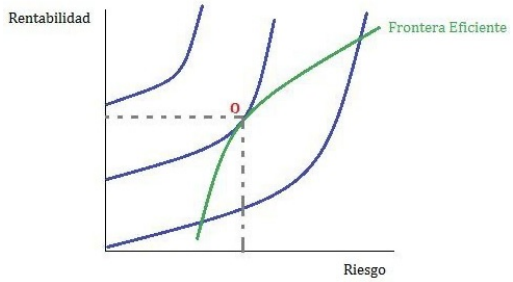


Figura 170. El modelo de Markowitz de cartera eficiente (2)

Te recomiendo echar un vistazo a las teorías de Markowitz y carteras eficientes así como CML (capital market line). En palabras sencillas, la diferencia entre

una cartera eficiente y no eficiente sería el porcentaje de éxito que puedas tener asumiendo un riesgo concreto.

No te recomiendo otra cosa que práctica; que apuntes números y hagas predicciones, y que pruebes con dinero real una vez tengas clara tu posición y hayas confirmado alguna de tus predicciones. A estas alturas, deberías saber que las inversiones cripto no hay que entenderlas como gaming, sino con análisis, comprensión de los protocolos y los productos financieros asociados y toma de decisiones en frío. Mi expectativa contigo es que seas capaz en un futuro a medio plazo de controlar tus activos y conservar y ampliar tu patrimonio.

DeFi es un mundo apasionante que permitirá hacer líquidos muchos mercados y activos que no lo eran. Bienvenido a una nueva era, una era en la que el valor lo pone el usuario.

# 36. Fiscalidad y regulación cripto

## 36.1. Taxonomía de impuestos en España

Este último capítulo del libro lo centraremos en el «apasionante» mundo de los impuestos y la regulación fiscal en cuanto a criptoactivos. Es importante que entiendas qué son los impuestos y en qué te afectan como criptoinversor. Como siempre, la primera recomendación —a cumplir a rajatabla— es que una vez empieces a generar operaciones, tengas a tu lado alguien que te asesore a nivel fiscal de manera profesional.

En España tenemos estupendos asesores tributarios con amplísimo conocimiento sobre la materia, como José Antonio Bravo, Cristina Carrascosa y muchos otros. Contratar a un buen asesor tributario es tan importante como tener un buen médico o abogado: no debemos acordarnos de ellos solo ante los problemas. No hay dinero mejor invertido que en ellos. Nosotros, sin llegar a la suela de sus zapatos, te daremos una serie de recomendaciones y guía básica a seguir para iniciarse en la materia pisando terreno sólido.

Así que, empezando por lo más sencillo, los impuestos o tributos pueden ser de dos tipos:

- **Los de naturaleza directa.** Son aquellos que gravan la obtención de renta: IRPF, IP, ISyD, IRNR, IIVTNU.
- **Los de naturaleza indirecta.** Son los que gravan la mera circulación de bienes y servicios: IVA, ITPyAJD.

En detalle, estos acrónimos serían:

- **IRPF (Impuesto sobre la Renta de las Personas Físicas).** Grava la renta que obtiene una persona física de forma onerosa.
- **IS (Impuesto sobre Sociedades).** Grava la renta (beneficio) que obtiene una sociedad.
- **IP (Impuesto sobre el Patrimonio).** Grava la mera tenencia de bienes por parte de las personas físicas.
- **ISyD (Impuesto sobre Sucesiones y Donaciones).** Grava la renta o ganancia que obtiene una persona física de forma gratuita.
- **IRNR (Impuesto sobre la Renta de No Residentes).** Grava la renta obtenida en territorio español por las personas físicas o entidades no residentes en el mismo.

- **IVA (Impuesto sobre el Valor Añadido).** Grava, entre otras operaciones, la transmisión de bienes cuando el transmitente es un empresario o un profesional.
- **ITPyAJD (Impuesto sobre Transmisiones y Actos Jurídicos Documentados)** en sus distintas modalidades:
  - **TPO (Transmisiones Patrimoniales Onerosas).** Grava, entre otras operaciones, la transmisión de bienes cuando el transmitente es un particular.
  - **OS (Operaciones Societarias).** Grava la realización de determinadas operaciones por sociedades y entidades asimiladas.
  - **AJD (Actos Jurídicos Documentados).** Grava, entre otras operaciones, la formalización de actos en escrituras públicas.
- **IIVTNU (Impuesto sobre el Incremento de Valor de Terrenos de Naturaleza Urbana).** grava la obtención de un incremento de valor experimentado por los terrenos de naturaleza urbana como consecuencia de la transmisión de su propiedad por cualquier título.

En la siguiente tabla podemos ver un poco más claro cómo se vincula el tipo de impuesto con el tipo de fiscalidad, objeto y el tipo de persona jurídica;

| | IRPF | IS | IVA | ITPyAJD | IP | ISyD |
|---|---|---|---|---|---|---|
| **Denominación común** | Renta | Sociedades | IVA | ITP | Patrimonio | Sucesiones |
| **Objeto** | Ganancia de renta | Ganancia de renta | Circulación bienes | Circulación bienes | Tenencia de bienes | Ganancia de renta gratuita |
| **Tributación** | Máximo 45 % | 25 % | 21 % 10 % 4 % | TPO 6-4 % OS 1 % AJD 0,5 % | Hasta 2,5 % | Según escala progresiva y CCAA |
| **Sujetos** | Personas físicas | Personas jurídicas | Todos | Todos | Personas físicas | Personas físicas |

Figura 171. Características y afección de los principales impuestos en España

# 36.2. Los criptoinversores y el IRPF

El IRPF es uno de los impuestos más conocidos y odiados. Como hemos comentado, es de carácter directo y de naturaleza personal; grava la obtención de renta de las personas físicas residentes en España.

El objeto del IRPF está constituido por la totalidad de la renta: rendimientos, ganancias y pérdidas patrimoniales e imputaciones de renta con independencia del lugar donde se hubiesen producido y cualquiera que sea la residencia del pagador.

¿Cuál es su ámbito de aplicación?

Concretamente a las personas físicas que tienen su residencia habitual en el territorio español. Los residentes en España, sean nacionales o extranjeros, son los contribuyentes del IRPF y son gravados por la totalidad de la renta que

obtengan, por su renta mundial. Este hecho es muy relevante ya que en estos últimos años puede que algunos de nuestros queridos lectores hayan estado residiendo un número de meses al año fuera de España. Si fuera tu caso, revisa bien esta parte de la tributación.

¿Qué constituye el hecho imponible del IRPF?

El hecho imponible u objeto de la tributación del IRPF lo constituye la obtención de renta (en lo que atañe a nosotros, a las plusvalías obtenidas por la venta de criptoactivos). Dicha renta se cuantifica y califica en función de su actividad ha desarrollado:

- Rendimientos del trabajo.
- Rendimientos de capital inmobiliario.
- Rendimientos de capital mobiliario.
- Rendimientos de actividades económicas.
- Ganancias y pérdidas patrimoniales.

Entre las rentas mencionadas en el IRPF, los rendimientos del capital mobiliario (RCM) y las ganancias o pérdidas patrimoniales (GP) derivadas de la transmisión de elementos patrimoniales, son las que afectan a la fiscalidad de los productos financieros y, en nuestro caso a los criptoactivos. Aclaremos simplemente que las ganancias o pérdidas patrimoniales son las que provienen de transmisiones de bienes, como la venta de acciones, el reembolso de fondos de inversión, la venta de inmuebles, etc.

Enlazando estos regímenes impositivos y su estructura fiscal con el mundo cripto, desde enero de 2018 el Ministerio de Hacienda utiliza unas directrices especiales para las criptomonedas, dado que las considera como medios de pago y son operaciones financieras siempre y cuando esas monedas hayan sido aceptadas como medio de pago por todas las partes de una transacción. Por lo tanto, las operaciones con monedas virtuales están exentas del IVA tanto para el comprador como el vendedor, ya que se trata de medios de pago y no de bienes o servicios.

Por ello, cualquier ingreso o gasto derivado de la compraventa de criptomonedas debe incluirse en la declaración de la renta de igual forma que si se tratara de otras inversiones, ya que tienen la consideración de ganancia o pérdida de patrimonio. El resultado de esta actividad se incluirá en la compensación de ganancias o pérdidas patrimoniales de la base imponible del ahorro.

Recuerda que el método que se usa para la valoración neto de patrimonio es el

FIFO

(first in first out), es decir, la cotización la calculas mediante el precio al que adquiriste el primer criptoactivo restándolo del precio del mismo criptoactivo que ha salido de tu cartera.

Para ello, se debe integrar la diferencia entre los precios de compra y venta de las criptomonedas, en el apartado del patrimonio, al igual que sucede con las acciones de empresas cotizadas y otro tipo de productos financieros.

Los tipos impositivos para las ganancias obtenidas mediante criptomonedas son los mismos que los de otros productos de inversión y ahorro:

- Si la cantidad es menor a 6000 EUR, un 19 % del IRPF.
- Si se encuentra entre los 6000 y los 50 000 EUR, un 21 %
- Cuando sea superior a 50 000 EUR, el IRPF será del 23 %.

En todo caso es importante que te asesores por un abogado o experto en tributación.

Otra de las grandes cuestiones que siempre salen a debate es qué ocurre si no saco dinero de mi monedero virtual de criptomonedas. Su respuesta, sin entrar en detalles y de manera general, sería: dado que las criptomonedas se consideran como un medio de pago, los monederos virtuales tienen la misma consideración que las cuentas bancarias. Por lo tanto, la retención para ellos es del 19 % sobre las ganancias que se obtengan al operar con cualquier tipo de moneda virtual.

Sin embargo, si el dinero en criptodivisa se mantiene en el monedero sin realizar ningún movimiento con él, no tendrá un valor real, ya que no se ha convertido a una divisa nacional como el EUR. Por lo tanto, en caso de que no se opere con ellas, no será necesario pagar impuestos a Hacienda. En resumen: solo habrá que declararlo en caso de que se realicen operaciones con estas criptomonedas.

Como ves, todavía quedan muchas lagunas, como por ejemplo qué ocurre con los cold wallets, o si afectan de manera similar a los wallets en exchange o en wallets personales. Todo esto poco a poco se está regulando, y te recomendamos estar actualizado para que puedas planificar el pago de tus futuros impuestos.

El nuevo proyecto de ley que el Gobierno ha aprobado el día 13 de octubre de 2020 intenta acercar dichos conceptos fiscales hacia las Medidas de Prevención y Lucha contra el Fraude Fiscal, motivando la modificación de la Ley 7/2012 que introdujo la obligación de informar sobre bienes y derechos situados en el extranjero. En este proyecto se introduce la obligación de informar sobre la tenencia y operativa de monedas virtuales, afectando tanto a las criptomonedas

situadas en España como en el extranjero (curiosa apreciación), siempre y cuando afecte a contribuyentes españoles. Así, a partir de ahora se va a exigir información sobre saldos y titulares de las monedas en custodia a los diversos exchanges que realicen servicios en España y a los profesionales que trabajen como asesores activos (no así de los assets mantenidos en cold wallets).

Pero además de ello, se va a tener obligación de suministrar información sobre las operaciones de criptomonedas (adquisición, transmisión, permuta, transferencia, cobros y pagos). Como novedad, también se va a tener obligación de informar en el modelo 720 de la tenencia de monedas virtuales en el extranjero.

Otra de las dudas que siempre aflora es cómo tributar en el caso de pagar con cripto un producto o servicio. En este caso, al usar como medio de pago criptomonedas, se generará una ganancia o pérdida patrimonial con respecto al precio que las adquiriste, con lo que deberás declarar simplemente esta ganancia en el IRPF.

En nuestro caso, suponiendo que pagaste con parte de un bitcoin (X satoshis) tomarás como valor el de adquisición de los primeros que compraste.

Otro apunte importante es que el Impuesto sobre el Patrimonio se aplica en todo el territorio nacional, aunque su rendimiento está cedido en su totalidad a las comunidades autónomas. Cada comunidad autónoma puede asumir competencias normativas sobre el mínimo exento, el tipo de gravamen y las deducciones y bonificaciones de la cuota.

No obstante, tendrás que superar el mínimo exento aprobado por cada comunidad autónoma para ver si tienes la obligación de tributar por el IP o no. Por ejemplo, para el caso de la Comunidad Valenciana, el mínimo exento actual en el Impuesto sobre el Patrimonio son 600 000 €. En caso de que superes el mínimo exento de este impuesto, deberás declarar el valor de las criptomonedas.

Por otro lado, debes analizar el tipo de gravamen. En este ejemplo para la Comunidad Valenciana se establece que la cuota íntegra del impuesto se conseguirá aplicando a la base liquidable los tipos de la siguiente escala:

| Base liquidable Hasta € | Cuota € | Resto Base liquidable Hasta € | Tipo aplicable % |
|---|---|---|---|
| 0,00 | 0,00 | 167.129,45 | **0,25** |
| 167.129,45 | 417,82 | 167.123,43 | **0,37** |
| 334.252,88 | 1.036,18 | 334.246,87 | **0,62** |
| 668.499,75 | 3.108,51 | 668.499,76 | **1,12** |
| 1.336.999,51 | 10.595,71 | 1.336.999,50 | **1,62** |
| 2.673.999,01 | 32.255,10 | 2.673.999,02 | **2,12** |
| 5.347.998,03 | 88.943,88 | 5.347.998,03 | **2,62** |
| 10.695.996,06 | 229.061,43 | En adelante | **3,12** |

**Base Liquidable x Tipo de Gravamen según Escala = Cuota Íntegra**

Figura 172. Escalas del Impuesto de Patrimonio (IP) en la Comunidad Valenciana

## 36.3. Prescripción de la deuda tributaria

Otra cuestión que suele salir a debate es si existe la prescripción de una deuda (deuda, no delito). Como norma general, la prescripción general sucede a los cuatro años, según se establece en el artículo 66 de la Ley 58/2003 General Tributaria.

Pero para ser más concretos, en cuatro años puede prescribir:

- El derecho de la Administración para determinar y exigir el pago de las deudas tributarias e imponer sanciones.
- El derecho del contribuyente a solicitar y obtener las devoluciones derivadas de la normativa de cada tributo.
- El derecho del contribuyente a solicitar las devoluciones de ingresos indebidos y el reembolso del coste de las garantías.

Por otro lado, la excepción por prescripción a diez años, donde la Ley 34/2015 modificó parcialmente la Ley General Tributaria, entre otras cosas, en materia de prescripción con respecto a la comprobación de ejercicios prescritos con trascendencia, en ejercicios no prescritos y las obligaciones tributarias que estén vinculadas a los anteriores.

Se introdujo así un periodo de diez años para comprobar determinadas bases imponibles o cuotas pendientes de compensar, computadas desde la finalización del plazo voluntario establecido para presentar la declaración o autoliquidación por parte del obligado tributario.

Como has podido observar hay mucho por hacer en el entorno cripto, y, como suele pasar en los ámbitos de innovación, la normativa y la regulación suele ir por detrás de la innovación, usabilidad y comunidad.

En el caso concreto de DeFi, tenderá a ser más restrictiva, dado que la libertad financiera va en contra de muchos principios de la centralización monetaria,

inflación y demás términos macroeconómicos. Por eso te recomendamos que estés al tanto de las noticias o que sigas nuestro criptoblog para recibir píldoras de actualización.

Blockchain y su usabilidad en DeFi está removiendo el tablero de juego y está recolocando a todos los actores financieros en posiciones distintas. El actor que no aporte valor a la comunidad será apartado del juego. Por lo tanto, la comunidad será la directora de orquesta de este nuevo ciclo y sistema económico basado en el Internet del valor.

# EPÍLOGO

A estas alturas del libro, querido lector, imagino que te habrá estallado la cabeza no una, sino decenas de veces. Como decíamos a mitad del mismo, hemos intentado hacer una guía, un libro de cabecera para consultar cada vez que necesites reforzar ideas sobre la materia.

Quizás lo que viene a continuación lo tendríamos que haber contado al inicio del libro, pero lo he querido hacer así porque, al cerrar estas últimas líneas, el libro se convierte en un paso más en esta criptoaventura en la que no sabemos a dónde nos llevará ni nos importa, porque lo hacemos para disfrutar durante el viaje aprendiendo y compartiendo lo que aprendemos con la comunidad, y especialmente contigo.

Fue en 2014 cuando el Sokar y un humilde servidor intentamos añadir Bitcoin como forma de pago en Tutellus. Lo enfocamos más como una herramienta de *marketing* y promoción que otra cosa, ya que no entendimos qué significaba Bitcoin ni dónde residía su valor. El proyecto, como tantos otros, quedó a medio camino.

En 2016 vi cómo surgían las primeras ICO y empecé a investigar y a aprender sobre tokens, aunque no terminé de ver la aplicación práctica en Tutellus. Una vez más, abandoné esta línea de trabajo; pensaba que por mucho que me atrajese, esto no iba con Tutellus, y, siendo responsable, yo me debía a mi compañía y a mis socios.

No fue hasta 2017 cuando conocí Steemit y comencé a verle sentido al proyecto de tokenizar Tutellus como medio para aumentar el valor aportado a los usuarios y, en definitiva, a la comunidad: si éramos capaces de devolver al usuario parte del valor que generaba con sus hábitos en Tutellus (en la forma de un token) crearíamos un modelo diferenciador capaz de «pagar por aprender». Durante todo ese año y el siguiente estuve viajando e introduciéndome en el ecosistema cripto a nivel mundial, y tuve la suerte de visitar países, conocer gente y establecer vínculos en cuatro continentes.

A finales de 2018 vimos la oportunidad de empezar a enseñar, de una forma más seria y profesional, todo lo que habíamos aprendido los últimos dos años en la forma de másteres y bootcamps. Creamos como experimento el Primer Máster de Blockchain Práctico, y el resultado es que ya vamos por la 15ª edición. El formato no ha sido un éxito porque yo lo diga, sino por la evolución de los alumnos, los proyectos y startups que han surgido a nuestro alrededor y la comunidad que hemos creado entre todos.

Fue en esa época, a finales de 2018, cuando conocí a un chaval de veinte años que venía en AVE de Barcelona a Madrid todas las semanas con el único

objetivo de aprender sobre cripto. Se llama Arnau Ramió. Cuando terminó el máster le vi tan comprometido con la causa que empezó a trabajar en Tutellus, desarrollando negocio y ecosistema desde Barcelona. Hay que recordar que en esa época DeFi no existía ni siquiera como ecosistema.

A principios de 2019, en otro programa de Blockchain conocí a otra persona que me sorprendió gratamente: Marcos Carrera. Era el único que venía siempre una hora antes de empezar —nos pillaba comiendo y refunfuñábamos cada día— para comentar ideas de proyectos para tokenizar. Marcos, como muchos otros, me confesó poco después que Blockchain le había cambiado la vida y su perspectiva de los negocios y, al igual que Arnau, estaba tan comprometido con la causa que empezó a trabajar junto al equipo core de Tutellus desde entonces.

Entre 2019 y 2020 el área de formación de la compañía creció mucho, no solo en alumnos sino en proyectos y en posicionamiento en el mercado. A principios de 2020 arrancaron los primeros protocolos DeFi más allá de Maker, y fuimos conscientes, al haber vivido la industria desde dentro, que algo muy grande se avecinaba. Creamos un primer bootcamp específico de DeFi con un resultado espectacular (veinte alumnos) y nos animamos con un segundo (cuarenta alumnos) recibiendo a compañeros no solo de España sino de Estados Unidos, Argentina, Venezuela y Chile. La voz se estaba corriendo: «Estos de Tutellus están a otro nivel». Recuerdo cómo un alumno nos comentaba que había tomado un café con un compañero de trabajo que estaba haciendo un Máster en Blockchain en una conocida universidad y, literalmente, a los cinco minutos de conversación aquel no entendía nada de lo que hablaba *nuestro hombre*.

Debido al cambio de vida que todos hemos sufrido consecuencia de la COVID-19, el modelo de formación en remoto empezó a consolidarse y, de alguna manera, la corriente del río era ya tan fuerte que nos llevaba hacia abajo con un esfuerzo relativamente pequeño: los alumnos de promociones anteriores hablaban tan bien de nosotros que eran ellos mismos los que llenaban, directa o indirectamente trayendo a gente cercana, los nuevos programas.

2020 ha sido además el año de consolidar otros proyectos más allá de la plataforma educativa. Iniciamos —como comenté en el prólogo— diferentes empresas con socios del sector y alumnos de distintos programas con el objetivo de seguir contribuyendo al ecosistema con algo más que palabras y una buena formación: con productos, con tecnología, con STO bien estructuradas, con tokens líquidos, con fondos de inversión propios, con network real, sin bullshit.

Y en esta tesitura nos encontramos ahora, a finales de 2020; a pesar de vivir en un contexto incierto, somos afortunados al poder estar saturados de proyectos y

nuevas ideas, creando productos y con las mismas ganas de aprender y de hacer cosas nuevas que el primer día. Me considero una de las personas más afortunadas del mundo, ya que trabajo en lo que me gusta y rodeado de la gente que quiero, aprecio y me enriquece.

2021 será el año que consolidaremos algún protocolo DeFi propio y muy probablemente sea sobre Bitcoin. Pretendemos seguir contribuyendo al ecosistema, atraer más talento y seguir desarrollando productos que nos hagan la vida más fácil.

Porque ya sabes, querido lector, que todo esto va de felicidad. De vivir siendo más felices. Y como el ser humano es más feliz cuando es libre, en la búsqueda de esa libertad las DeFi juegan un papel fundamental. Si has entendido cómo funciona este ecosistema y, sobre todo, que hay futuro más allá de los bancos, nosotros ya nos damos por satisfechos.

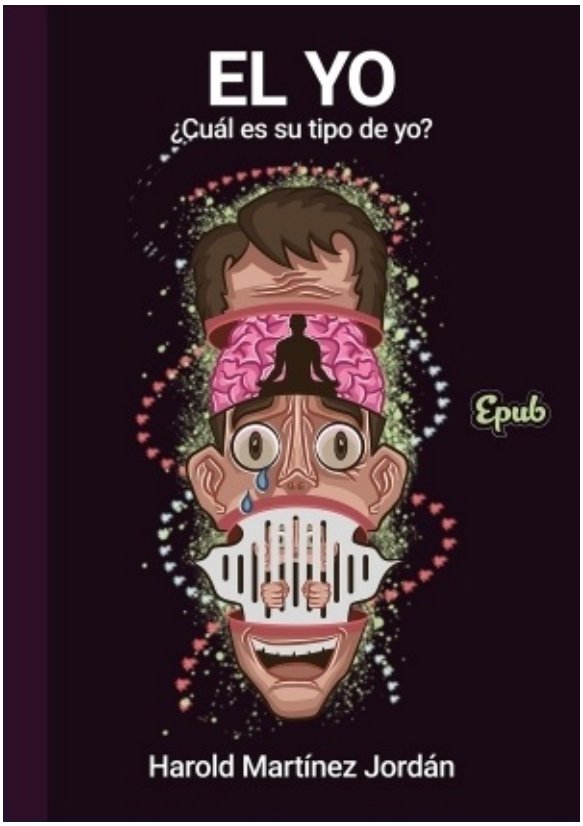
Lo único que me queda recalcar es que esperamos tener la suerte de conocerte personalmente algún día: en algún evento, bootcamp, webinar o, quién sabe, durante el próximo libro, presentando alguna de tus innovaciones o proyectos.

Las empresas y los proyectos las hacemos las personas, las relaciones humanas. Detrás de toda descentralización tenemos pares, personas de carne y hueso con las que compartir protocolos, tokens e historias. Tenemos la suerte de poder escribir la historia en primera persona.

Ten en cuenta que la persona más sabia del mundo en cripto apenas nos saca unos pocos años. Todos estamos a tiempo de subirnos a este tren y de mejorar nuestras vidas. Todos estamos a tiempo de reconvertirnos profesionalmente, de formarnos en Blockchain, de iniciar nuevos proyectos. Porque uno nunca es demasiado viejo para seguir aprendiendo, sino que nos hacemos viejos porque dejamos de aprender.

Mientras tanto, sigamos disfrutando del camino.

Miguel Caballero
Madrid, noviembre de 2020.


EL YO
¿Cuál es su tipo de yo?
Epub
Harold Martínez Jordán

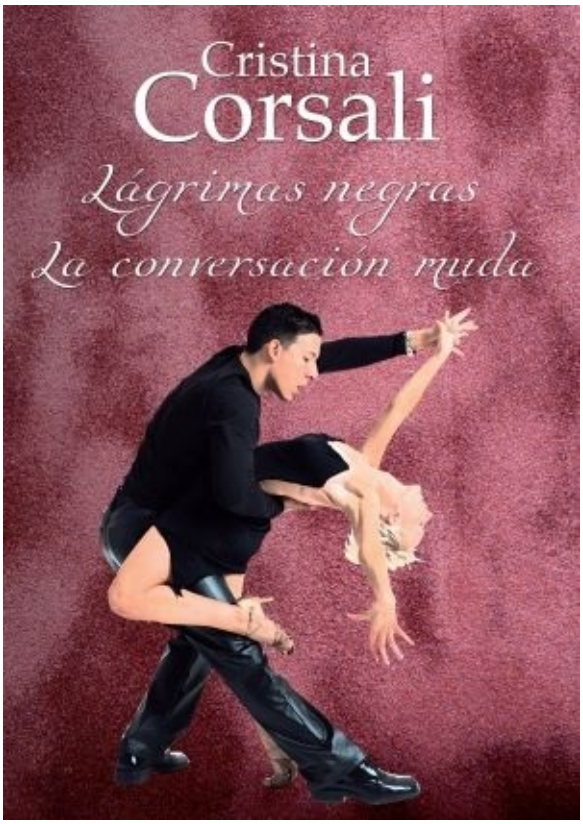
# El yo

Martínez Jordán, Harold
9788468532431
118 Páginas



En este libro, el lector encontrará la nueva teoría del Yo de acuerdo al resultado de una indagación de varios años, en cuya visión se expone su conocimiento moderno. En él se incluye su historia desde sus concepciones esotéricas, su mecanismo con relación a sus cinco inteligencias, sus ciclos y los tipos de Yo o signos psicológicos, como parte de su nueva estructura general.
Robert Bissonnette, psicólogo Canadiense, afirma:
"Harold Martínez Jordán hace una prueba de audacia y de originalidad presentando una nueva tipología del yo. Su trabajo es el resultado de una reflexión filosófica y psicológica. Este libro está inscrito dentro de la corriente contemporánea de la psicología de la espiritualidad entre otras descrita por Eckhart Tolle, que hace hincapié en la importancia de conocer los diversos "yo" con el fin de poder liberarlo."

Cómpralo y empieza a leer


Cristina
Corsali
Lágrimas negras
La conversación muda

# Lágrimas negras. La conversación muda

Corsali, Cristina
9788468527031
246 Páginas



Erotismo, esperanza, acento canario y sabor latino. Lágrimas negras. Esther y Marcelo llevan meses chapoteando torpemente en un matrimonio donde ya llovía sobre mojado desde hacía mucho tiempo. La paciencia de Esther se agota cuando, en lugar de celebrar su aniversario juntos, Marcelo decide quitársela de en medio unos días y enviarla con doña Asunción, su madre, a un lujoso crucero. Pero el destino tiene una sorpresa preparada para ella… Omar, cantante de salsa y viejo amor de juventud, se cruza de nuevo en su camino. A pesar de años de separación tras un final abrupto, Esther siente todavía una fuerte atracción por el cubano, pero un secreto de aquella época la atormenta… "Pase lo que pase, el domingo, salsa". La conversación muda Invisible. Así se siente María Eugenia después de que su marido pusiera punto y final a años de relación y de que su hijo se mudara al extranjero. Decidida a recuperar las ganas de vivir, retoma su pasión por la pintura y descubre el baile como terapia. María Eugenia no imagina que su primer boceto será el del hombre que la enseñará a caminar por una jungla de gente insensibilizada, de sexo sin amor, de la conversación breve y muda del Messenger… Sin embargo, de su mano se agudizarán también miedos e inseguridades. ¿Será capaz de reinventarse y dejar atrás los apegos que la paralizan? En su lucha, la salsa será lo único que la mantenga a flote. Cristina Corsali regresa después de Todos los caminos con dos nouvelles sobre el amor, las segundas oportunidades y la satisfacción que da el tiempo cuando pone a cada uno en su lugar.

Cómpralo y empieza a leer


bubok
EDITORIAL
Miguel Caballero
BITCOIN.
BLOCKCHAIN
Y TOKENIZACIÓN
PARA INQUIETOS
BITCOIN·DIGITAL·DECENTRALIZED·PEER TO PEER
TROY OZ 999 FINE COPPER MONETARY METALS

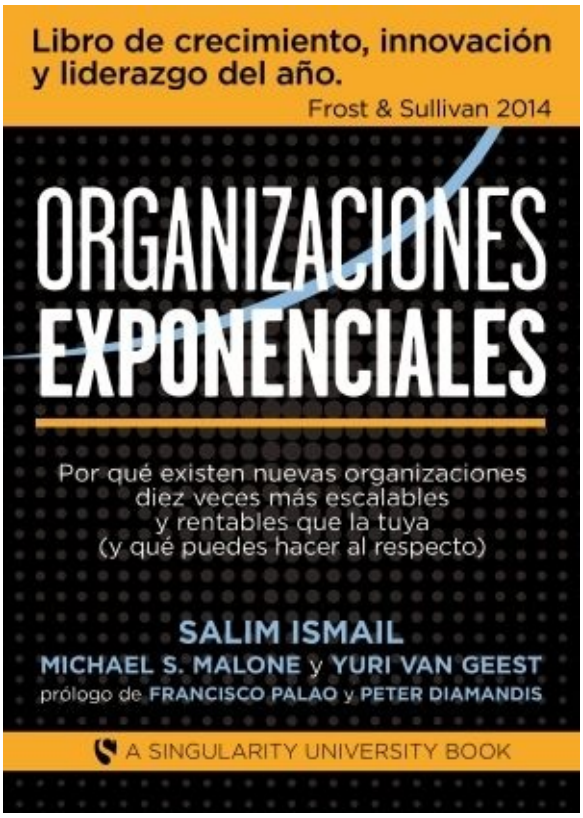
# Bitcoin, Blockchain y tokenización para inquietos

Caballero, Miguel
9788468543215
218 Páginas



¿Cómo funciona Bitcoin y qué valor aporta a la sociedad? ¿Qué significa y cómo funciona Blockchain? ¿Cómo podemos aplicar la tokenización en nuestras empresas? El lector encontrará las respuestas en esta obra de Miguel Caballero, CEO DE Tutellus, la mayor plataforma educativa online en habla hispana del mundo. El autor ha querido elaborar un ensayo donde expone casos reales de los problemas que resuelve la tecnología para ayudar así a que los lectores a comprender las implicaciones que ésta tiene en su día a día, tanto a nivel personal como profesional. La gran parte de las publicaciones realizadas hasta la fecha sobre esta materia están dirigidas al público especializado. Sin embargo, esta obra pretende lanzar una lanza en favor de los que todavía no conocen Blockchain desde dentro. Cualquier persona familiarizada con innovación entenderá este libro. Únete a la comunidad usando el hashtag #BlockchainParaInquietos

Cómpralo y empieza a leer


Libro de crecimiento, innovación y liderazgo del año.
Frost & Sullivan 2014
ORGANIZACIONES EXPONENCIALES
Por qué existen nuevas organizaciones diez veces más escalables y rentables que la tuya (y qué puedes hacer al respecto)
SALIM ISMAIL
MICHAEL S. MALONE y YURI VAN GEEST
prólogo de FRANCISCO PALAO y PETER DIAMANDIS
A SINGULARITY UNIVERSITY BOOK

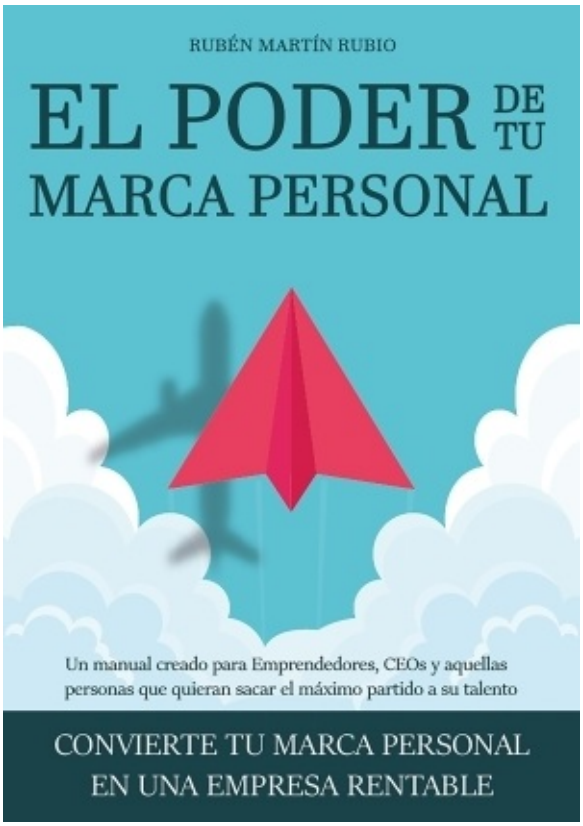
# Organizaciones Exponenciales

Ismail, Salim
9788468686387
414 Páginas



Durante los últimos cinco años, el mundo empresarial ha sido testigo del surgimiento de una nueva generación de empresas – las Organizaciones Exponenciales (ExO) – que han revolucionado la forma de acelerar su crecimiento mediante el uso de la tecnología. Una ExO puede transformar el modo lineal e incremental en que las empresas tradicionales crecen, mediante el uso de activos como su comunidad, personal bajo demanda, Big Data, Inteligencia Artificial y otras nuevas tecnologías, hasta alcanzar un rendimiento diez veces superior al de empresas similares. Tres visionarios del mundo de los negocios – Salim Ismail, Yuri van Geest y Mike Malone – han investigado este fenómeno y han documentado diez características de las Organizaciones Exponenciales. En este libro, Organizaciones Exponenciales, acompañan al lector en su viaje para conocer cómo, cualquier compañía, desde una startup a una gran multinacional, puede convertirse en una ExO, mejorando su rendimiento y evolucionando al siguiente nivel.

Cómpralo y empieza a leer


RUBÉN MARTÍN RUBIO
EL PODER DE TU MARCA PERSONAL
Un manual creado para Emprendedores, CEOs y aquellas personas que quieran sacar el máximo partido a su talento
CONVIERTE TU MARCA PERSONAL EN UNA EMPRESA RENTABLE

# EL PODER DE TU MARCA PERSONAL

Martín, Rubén
9788468543093
400 Páginas

Cómpralo y empieza a leer

Manual práctico sobre estrategias de implementación de tu **Marca Personal** en el mercado, orientado a emprendedores, CEOs y aquellas personas que quieran sacar el máximo partido a su talento.

"*Rubén ha desarrollado un método muy efectivo para potenciar la marca personal. Consigue que cada persona pueda desarrollar sus fortalezas y convertirlas en una empresa rentable.*" - Pilar Jericó, Empresaria, Conferenciante y Escritora.

**Convierte tu Marca Personal en un negocio rentable.**

En este momento te estarás preguntando:
¿Cómo conseguir más ingresos dedicándome a mi pasión?
¿Cuál es la manera de sacar mayor potencial a mi imagen y comunicación?
¿De qué manera podría ofrecer nuevos productos y servicios con un público que esté deseando comprar?

Si te ves reflejado, entonces, ***El Poder de tu Marca Personal***es para ti.

El libro es un viaje a través de una **metodología práctica** y te dará las claves para **generar ingresos con aquello que te hace único** y puedes ofrecer al mercado.
**El poder de tu marca personal te enseñará cómo:**
• Encontrar tu propósito vital para ponerlo al servicio de los demás.
• Construir los pilares de tu Marca Personal posicionándote como autoridad y generando una comunidad de seguidores.
• Ser la opción preferida del mercado en tu sector.
• Convertir tu Marca Personal en una empresa rentable.
• En definitiva: crear tu mejor versión en el ámbito personal, social y de negocios.

**Sobre el autor**

Rubén Martín, empresario con más de 16 años de experiencia, conferenciante, formador y uno de los mayores referentes en España en cuanto a Marca Personal. Trabaja en la marca de escritores, deportistas y personajes públicos de primer nivel ayudando a mejorar sus resultados.

Se considera producto de su propio producto al crear un negocio rentable a través de su Marca Personal, empezando desde cero. Actualmente es uno de los grandes divulgadores de Marca Personal con miles de seguidores en sus redes y constantes apariciones en medios de comunicación.

**Testimonio de lectores**
"*Lectura muy recomendable para aquellos que quieran aprender a monetizar y optimizar su marca personal, llevándola al siguiente nivel. Sólo apto para valientes que quieran realmente despegar*". **- Laura López Basulto**. Cofundadora de *InfluSpeakers*

"*He podido experimentar todas esas herramientas que se exponen en el libro en mi persona y la mejora en mis habilidades. Sencillamente excelente, limpio, claro y definido*". **Héctor J. Stezano Colares**, Consultoría y formación en Ventas.

"*El libro es un viaje fascinante en el proceso de creación de una marca personal. Rubén Martín nos acompaña desde su experiencia para que el camino sea fácil y no nos asuste demasiado mirar hacia adentro.*". **Manuela Ortiz**, Asesora y formadora en Comunicación.

Cómpralo y empieza a leer