

Álex Granados

# NFT

Qué son, para qué sirven y  
cómo van a cambiarlo todo

la esfera  de los libros

# ÍNDICE

AGRADECIMIENTOS .....	11
PRÓLOGO .....	13
<b>1. BLOCKCHAIN: CONCEPTOS BÁSICOS</b> .....	17
<i>Blockchain</i> : el origen de todo .....	18
Aprendiendo a confiar: <i>Proof of work</i> y <i>Proof of stake</i> .....	21
Criptomonedas: el nuevo dinero .....	25
<i>Wallet</i> .....	27
<i>Smart contracts</i> .....	28
<i>Gas fees</i> .....	29
<b>2. NFT: UN NUEVO PARADIGMA</b> .....	32
Las dos formas de entender los NFT .....	36
Posibilidades de los NFT .....	45
Estándares ERC .....	49

<b>3. ECOSISTEMA Y PLATAFORMAS: MARKETPLACES, METAVERSOS, JUEGOS</b> .....	54
Exploradores de bloques .....	55
<i>Marketplaces</i> .....	56
Otros <i>marketplaces</i> .....	69
Metaversos .....	70
Identidad .....	73
Juegos NFT .....	76
Dominios NFT .....	80
POAP .....	81
Libros NFT .....	82
<b>4. CÓMO EMPEZAR EN EL MUNDO NFT</b> .....	87
¿Qué <i>blockchain</i> utilizo? .....	87
<i>Wallets</i> : qué son y cómo crear una .....	88
Enviar criptomonedas a tu <i>wallet</i> .....	92
Comprar NFT .....	94
<i>Mintear</i> (crear) NFT .....	97
El mundo NFT está en Twitter y Discord .....	102
<b>5. SEGURIDAD, DESCENTRALIZACIÓN Y CÓMO EVITAR ESTAFAS</b> .....	104
La seguridad importa: cómo evitar que te roben todo .....	104
¿Cómo reconocer proyectos NFT estafa? .....	111
La importancia de la descentralización: almacenamiento de <i>metadata</i> y <i>smart contracts</i> .....	113
<i>Metadata</i> de NFT .....	114
Medios de almacenamiento .....	114
<i>Smart contracts</i> .....	118

<b>6. PROYECTOS NFT Y MARKETING</b> .....	120
Cómo crear tu propio proyecto <b>NFT</b> .....	120
Lanzar el proyecto adecuadamente .....	130
<b>7. HERRAMIENTAS NFT</b> .....	134
Etherscan .....	134
Ethereum Price .....	135
Rarity.tools .....	135
MintGate .....	135
Cyber .....	136
<i>Bots de Discord y Telegram</i> .....	136
Dune.xyz .....	137
Manifold.xyz .....	137
Studio721 .....	138
NiftyKit .....	138
Open Zeppelin .....	138
POAP .....	139
Tixit.cc .....	139
Dappradar .....	139
Github .....	140
Token Frame .....	140
CocoNFT .....	141
Linktree .....	141
Epílogo: EL FUTURO DE LOS NFT .....	143
GLOSARIO DE TÉRMINOS .....	149

## PRÓLOGO

Durante bastante tiempo había escuchado hablar de criptomonedas y parecía que todo el mundo a mi alrededor había invertido en ellas. Yo era bastante escéptico y, aunque siempre estuve interesado en invertir en general, no lo hice con cripto.

A principios de 2021, no mucho después de acabar de estudiar un grado en psicología, estaba trabajando como Digital Marketing Manager en una empresa de *packaging*. Llevaba dos años allí y estaba buscando un cambio. Un día, por casualidad, me enteré de que alguien necesitaba a una persona para un trabajo de «Community management y **NFT**».

No tenía absolutamente ni idea de qué era eso de los **NFT**, pero como soy una persona muy curiosa y no me gusta decir que no a nada, envié un correo a la persona que lo anunció.

Antes del *meeting* que tendríamos la siguiente semana, leí por encima un post en Reddit para ver de qué iba todo

esto de los **NFT**. Aunque me parecía extraño, entendí más o menos el concepto. Así que me aventuré a la entrevista.

Un chaval joven, con el que conecté bastante rápido, me estuvo contando sobre los Cryptopunks y lo que hacía en su estudio creativo y la verdad es que no entendía gran cosa, ni por qué había gente que pagaba tanto por unos monos pixelados. Más tarde descubriría que era Tox Sam, fundador de Polygonal Mind y uno de los pioneros creadores del metaverso. A la semana dejé mi trabajo y me uní a su equipo.

Así empezó mi aventura como cocreador de **NFT**esp. El objetivo era claro: crear la comunidad de referencia sobre todo lo que tuviera que ver con **NFT** en español. No había información sobre los **NFT** en nuestro idioma y alguien tenía que encargarse de explicar todo correctamente y que la gente pudiera introducirse a este mundillo sin caer en estafas ni *hackeos*.

El único problema es que al principio yo no tenía ni idea sobre todo esto, así que el primer mes en este equipo fue un proceso de pura investigación. Desde cómo crearte una *wallet* y preguntarme «¿para qué necesito una *wallet* siquiera?», «¿es gratis?», «¿por qué es gratis?», hasta entender los metaversos como Decentraland y todo sobre los **NFT** a nivel más técnico.

Fueron unos meses de no parar, explicando esta tecnología a cientos y cientos de personas hispanohablantes en distintas plataformas como Clubhouse y Twitter, yendo a eventos en lugares como la Universidad Politécnica de Va-

lencia, haciendo apariciones en la radio y en medios nacionales e internacionales y entrevistando a distintos criptoartistas y otra gente del mundillo.

Llegó un punto en que me paré a pensar, y vi que todavía nadie había escrito un libro en español sobre qué era esto de los **NFT** y cómo iniciarse en ello, así que me lancé y este es el resultado.

Mi objetivo con este libro es intentar explicarte, de manera simple, todo el mundo y ecosistema de los **NFT**, empezando por lo más básico (*blockchain*), y pasando por los distintos conceptos que necesitas saber. También quiero compartir mi experiencia y visión sobre cómo crear **NFT** y las buenas prácticas a tener en cuenta, así como la visión de distintos pioneros y referentes del mundo **NFT**. Sin humo.

Allá vamos.

#### NOTA FINAL

Aunque he intentado hacer todo lo posible por tener el contenido del libro al día, conforme lo iba escribiendo, las plataformas y el ecosistema NFT iban cambiando. Por tanto, habrá algún detalle que pueda haber cambiado cuando estés leyendo esto, pero no alterará el sentido general del libro.

# 1 : **BLOCKCHAIN: CONCEPTOS BÁSICOS**

Si estás leyendo este libro es porque en algún momento has oído hablar de los **NFT** y has querido saber de qué va todo esto. Seguramente habrás leído alguna noticia sobre cómo el artista Beeple vendió el **NFT** de su obra *Everydays: The First 5000 days*, en la que hizo un *collage* de todas las obras diarias que realizó durante 5.000 días, por 69 millones de dólares, o cómo Jack Dorsey, el fundador de Twitter, vendió el primer tuit de la historia como **NFT** por 2,9 millones de dólares.

Habrás escuchado hablar de criptomonedas y de *blockchain* sin llegar a entender realmente los conceptos. Pero no te preocupes, porque no hace tanto yo estaba como tú, y después de asimilar estos conceptos y explicarlos de forma diaria en **NFTesp** a cientos de personas en charlas de Clubhouse y Twitter y en eventos físicos, he llegado a entender por qué la gente no lo entiende. Y es porque nadie se lo explicó adecuadamente.

Por eso, para entender qué es un **NFT** (e incluso una criptomoneda), hay que conocer primero de qué va la tecnología que lo hace posible: la *blockchain*.

## **BLOCKCHAIN: EL ORIGEN DE TODO**

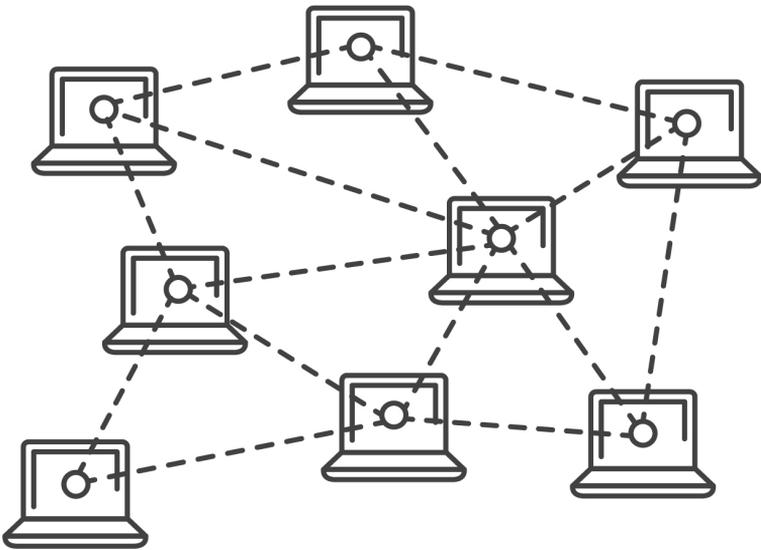
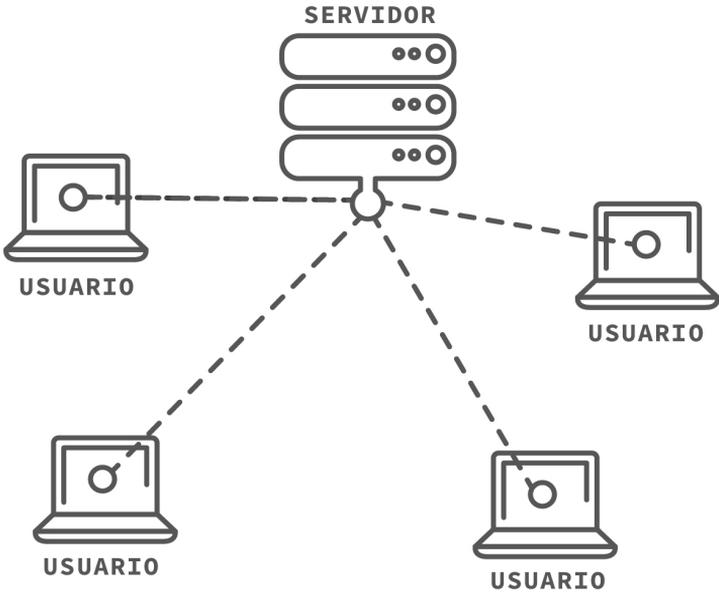
Todos sabemos lo que es un servidor informático: un ordenador que está constantemente funcionando y que está conectado a otros ordenadores, sea a través de Internet o de una red local. Este ordenador almacena información o recursos a los que podemos acceder siempre que esté conectado.

Un buen ejemplo de esto es un servidor de Gmail (o uno de los muchos que hay, al menos): te conectas a tu correo a través de una aplicación y puedes ver todos los mensajes almacenados en el espacio que se te ha cedido. Hasta aquí, bien.

Ahora imaginemos que un *hacker* decide atacar ese servidor y lo consigue. Si elimina toda la información, te quedarías sin poder acceder a tus correos, hasta que sea restaurada, en el mejor de los casos. En el peor caso, perderías esa información para siempre.

Pero, ¿qué pasaría si en lugar de estar almacenada esa información en un servidor, lo hiciera simultáneamente en cientos de ordenadores interconectados a tiempo real? Pues que tendrías que *hackear* muchísimos servidores para poder censurar o eliminar una información concreta. O también, en caso de alguna catástrofe o un apagón, la información seguiría siendo accesible por todos.

NFT



Servidor vs. Red *Blockchain*

Básicamente, esta es la idea detrás de la *blockchain*: una red de servidores interconectados y localizados en distintas partes del mundo que cooperan simultáneamente y guardan una copia exacta de toda la información. Si a eso le sumas que esa información, en lugar de añadirse en líneas infinitas (como en una hoja de Excel), se organiza en *packs* de información numerados que se van sumando entre sí (como si fuera una nueva hoja de Excel cada vez), enhorabuena, acabas de entender una gran parte de lo que es la *blockchain*.

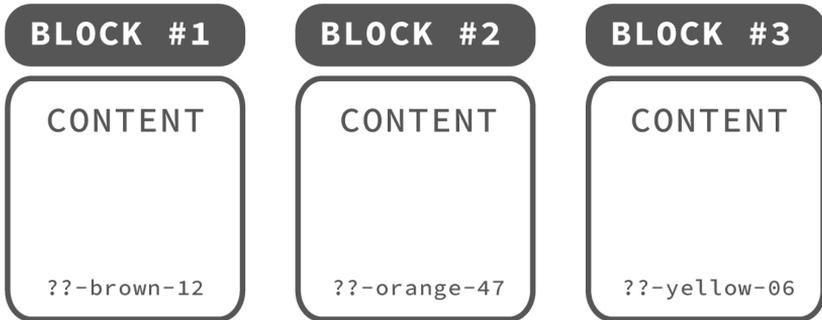


Diagrama de bloques de *blockchain*.

¿Fácil, eh?

Sin embargo, tenemos un problema: ¿cómo confiamos en que todos esos servidores (que ahora llamaremos «nodos») tienen una copia real y lícita de la información? Quizás ese mismo *hacker* que quería eliminar la información del servidor de Gmail podría montar 50 nodos y engañarnos a todos destrozando la red o cambiando la información.

**Nodo:** «servidor» que participa en la *blockchain*, almacenando una copia exacta de la misma.

Aquí es donde se pone interesante, ya que tenemos un gran problema de confianza. Pero como siempre hay alguien más listo que nosotros, no tenemos que pensar mucho porque ya se inventaron dos soluciones: *Proof of work* (PoW) y *Proof of stake* (PoS).

## **APRENDIENDO A CONFIAR: *PROOF OF WORK* *PROOF OF STAKE***

En asuntos sensibles como nuestra información o el dinero, la confianza no se da gratuitamente. Necesitamos pruebas. Así que distintos programadores y expertos llegaron a dos ideas muy buenas para validar la *blockchain*.

En la primera, *Proof of work* (PoW), se da, literalmente, una prueba de que hemos hecho un trabajo, en el sentido más físico de la palabra. Es decir, los nodos prueban que la información que añaden a la *blockchain* es válida porque han hecho un esfuerzo muy grande en forma de energía computacional (como si fuera un sacrificio para demostrar lealtad). Esta energía es usada para resolver criptogramas (es decir, ecuaciones muy complejas) cuya solución demuestra que has hecho ese esfuerzo. Es como cuando de niño enseñabas a tus padres que habías hecho los deberes y ellos te dejaban salir a la calle como recompensa. De hecho, la ra-

zón por la que las criptomonedas se llaman así es porque el sistema usa la encriptación para funcionar, basando su seguridad en la resolución de problemas criptográficos.

Este método de validación es el más conocido, ya que se utiliza en Bitcoin. Miles de ordenadores compiten para ser los primeros en llegar a la solución de cada problema criptográfico y así recibir la recompensa en forma de bitcoins. Se le llama «minar» a intentar resolver estos criptogramas, y es lo que nos ha dejado imágenes de granjas de minería con numerosos ordenadores funcionando al mismo tiempo.

Y dirás, vale, pero, ¿por qué es de fiar quien resuelve el problema criptográfico? ¿No podría un *hacker* intentar resolver el problema por su cuenta para engañar al resto?

Sí y no. Por un lado, cuantos más mineros existen en la *blockchain*, más poder computacional necesitas para resolver las ecuaciones. De hecho, el nivel de dificultad en *blockchains* como Bitcoin se va adaptando en función del número de mineros. Esto hace que necesites muchísimos ordenadores para llegar a resolver un criptograma y validar un bloque. Por esa razón se crean *pools*, que no son más que un conjunto de muchísimos ordenadores de personas que ceden su poder computacional para que, entre todos y actuando como un organismo, puedan resolver estas complejas ecuaciones. A cambio, todos se llevan una pequeña parte en criptomonedas.

***Proof of work***: muchos ordenadores compiten por resolver un desafío criptográfico antes que nadie. A cambio reciben una recompensa.

Así, cuanto más gente hay validando una *blockchain*, más segura es y más ordenadores se necesitarían para poder hacer un ataque, hasta alcanzar números imposibles. Sin embargo, este método de validación ha suscitado alguna crítica por el hecho de que haya que gastar electricidad en el proceso. Aunque es imposible conocer datos reales del consumo, de la eficiencia energética y de dónde viene esta electricidad, podría ser una crítica legítima, especialmente cuanto más crezca la *blockchain*.

Por eso, entre otras cosas, se desarrolló el método de *Proof of stake* (PoS).

En este segundo método, en lugar de dar una prueba de trabajo, se sigue una de las formas más tradicionales de validación de confianza: las apuestas.

Cuando estás muy seguro de algo (por ejemplo, de que el sol saldrá mañana), no tienes problema alguno en apostar a que va a ser así. De esta manera, ganas dinero fácil. El sistema de *Proof of stake* sigue esta misma lógica. Es decir, apuestas tu dinero en forma de criptomonedas (por ejemplo, XTZ, la moneda de la *blockchain* de Tezos) a que un validador o nodo va a actualizar la información de la *blockchain* de forma legítima.

A cambio, recibirás una recompensa también en forma de criptomonedas que varía dependiendo de la *blockchain* y la cantidad de gente que haya realizando *staking*, que es como se le llama a hacer esta apuesta. Los validadores con más dinero en juego tendrán más probabilidad de ser elegidos por la *blockchain* para validar el próximo bloque y, si se demuestra que un bloque se verificó maliciosamente, la *blockchain* te quitará una parte de las criptomonedas que apostaste. A esto se le llama *slashing*.

Este sistema es interesante porque cuanto más crece una *blockchain* y más dinero invertido hay en su criptomoneda, más dinero habría que invertir para destruirla, con riesgo de perderlo todo.

***Proof of stake:*** la gente apuesta a que distintos grupos de ordenadores van a validar la *blockchain* correctamente. Si la información no es veraz, se pierde la apuesta.

Un ejemplo: la *blockchain* de Polkadot tiene una inversión (capitalización de mercado) de 25.000 millones de dólares en el momento de escribir esto. Si quisiéramos realizar alguna operación maliciosa, tendríamos que invertir, como mínimo, un 51 por ciento de esta cantidad, es decir, 12.750 millones de dólares, y estar dispuestos a perderlo todo. Como puedes imaginar, es mucho dinero.

Aun así, este método también tiene su lado criticable, ya que aquellos con más dinero recibirán mayores recompensas, por lo que cabe la posibilidad de que acaben teniendo el monopolio sobre la *blockchain*. Sin embargo, también deberían ser los menos interesados en que ocurra algo negativo o que se destruya, ya que la criptomoneda bajaría mucho de valor.

Dicho todo esto, hay que aclarar que cada *blockchain* funciona con un método de validación distinto: Bitcoin y Ethereum funcionan con PoW, mientras otras, como Polkadot o Tezos, lo hacen con PoS.

Una vez que sabemos que podemos confiar en la *blockchain* (al menos mucho más que en un servidor de una empresa o institución), podemos usarla para guardar activos inquebrantables como criptomonedas o... **NFT**.

### ACLARACIÓN

Bitcoin es una *blockchain* y también es el nombre que tiene la criptomoneda de la propia *blockchain*, lo cual puede dar lugar a confusiones.

## CRIPATOMONEDAS: EL NUEVO DINERO

Hemos hablado de criptomonedas... pero ¿qué son exactamente? Las criptomonedas no son más que *tokens* (es decir,

activos digitales) que tienen un valor monetario y se aprovechan de la tecnología *blockchain*: es información dentro de ella, que se va actualizando como un saldo de *tokens*, de los que hay una cantidad total limitada que puede ir creciendo o decreciendo (situaciones inflacionarias o deflacionarias).

Este saldo no deja de ser información que se registra en la *blockchain* y que, como hemos explicado antes, es actualizada constantemente por los validadores, conforme se producen transacciones con uno de los dos métodos que existen (PoS o PoW). Las criptomonedas tienen valor porque ciertos grupos de personas comenzaron a darles valor. Igual que al oro, la plata o las acciones de empresas.

Si quieres entender el mundo cripto, tienes que entender algo: el valor es subjetivo. Debes empezar a preguntarte el porqué de todo lo que te rodea. Por ejemplo, ¿por qué le damos valor a un número en una cuenta bancaria para el cual invertimos 40 horas semanales? La respuesta es fácil: por convención social.

Al final, todos le damos valor a ese número en la cuenta y eso hace que a cambio podamos pagar el alquiler y recibir alimentos. Sin embargo, ¿cuánto tiempo lleva siendo así? Como hemos visto, esto puede cambiar, y, como ha sido el caso de países como Venezuela, en los que el valor percibido del dinero cambia por la política monetaria, se ha pasado de usar el dinero *fiat* (convencional) a incluso utilizar oro para pagar en ciertas tiendas. En gran medida, todo se basa en la confianza y la convención social. Por eso, la gente que cree en las criptomonedas ha

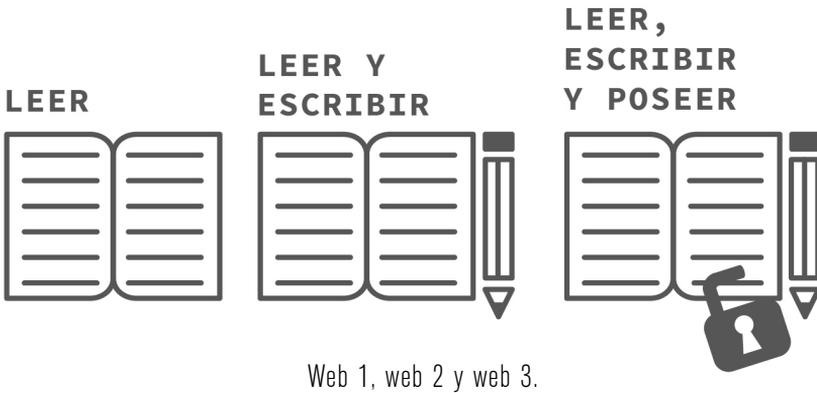
llegado a una nueva convención social en la que da valor a estas por sus características y porque confían en la *blockchain*. Y así, países como El Salvador se han unido a esta nueva convención social adoptando Bitcoin.

## **WALLET**

Cuando hablamos de *wallets* (o monederos), hablamos de «cajas fuertes» inquebrantables en la *blockchain*, donde podemos guardar nuestros activos digitales. Son algo así como cuentas bancarias para criptomonedas o **NFT**, y que, a su vez, funcionan como una cuenta de Google y un pasaporte, dándote una forma de identidad pseudónima con la que puedes *loguearte* en la Web3.

Imagina que todo lo que haces *online* con tu cuenta de Gmail estuviera asociado a tu cuenta del banco, tu nombre y correo electrónico, en lugar de ser *x@gmail.com*, fuera tu número de cuenta del banco (ES77...). Algo así ocurre con la *wallet*, que, por ejemplo en Ethereum empieza por 0x.

Esto es muy interesante porque hace que tengas un «todo en uno», a la vez que genera interoperabilidad dentro del ecosistema *blockchain* de las webs, en las cuales te puedes *loguear* con la misma *wallet* en cualquier sitio y sin necesidad de registrarte. Esto es lo que crea la base de la Web3, que al final es un tipo de Internet en el que el usuario es dueño de los distintos elementos.



## **SMART CONTRACTS**

Los *smart contracts* o contratos inteligentes son algo de lo que oirás hablar mucho en el mundo cripto. Básicamente, dentro de una *blockchain* (y dependiendo de su arquitectura y lenguaje) puede existir la posibilidad de crear programas que vivan y se ejecutan en ella. A estos programas los llamamos contratos inteligentes.

¿Recuerdas cómo la información en la *blockchain* se organizaba como un Excel pero en *packs*? Pues esto sería algo así como escribir líneas de código en las líneas de la hoja de Excel que pueden ejecutarse para hacer algo específico. Algo así como las propias funciones de Excel. Piensa que pasamos de poder usar solamente números, como en el caso de Bitcoin, a poder crear programas. ¡Un gran paso!

Su existencia es importante, ya que gracias a los *smart contracts* existen los **NFT** como tales. Ethereum fue la primera *blockchain* en introducir esta tecnología de manera

nativa, ya que Bitcoin es bastante más limitada en cuanto a programación y no tiene la posibilidad de albergar *smart contracts*. En cierto modo, en el caso de Bitcoin, intentar crear un *smart contract* sería como intentar escribir una novela con cinco palabras, en lugar de tener disponible todo el diccionario español.

## ***GAS FEES***

Las *gas fees*, por su nombre, eran algo que me confundía mucho en un principio cuando entré al mundo **NFT**. Sin embargo, es un concepto bastante fácil de entender.

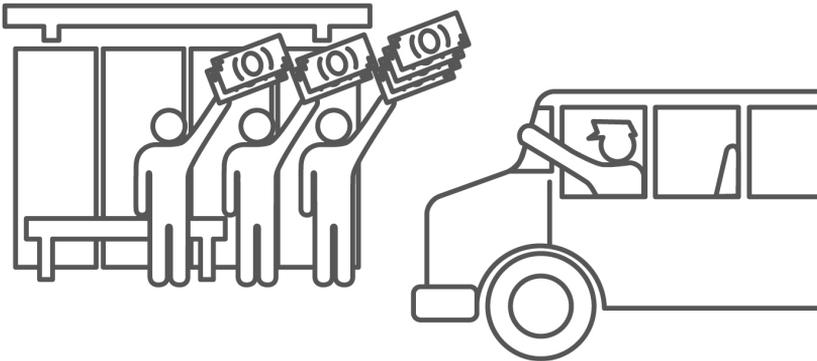
Básicamente, cada vez que realizas una transacción en la *blockchain* (como enviar o crear un **NFT**), si esa transacción lleva consigo un cambio de información en la cadena de bloques, tienes que pagar a uno de los nodos o validadores (de los que hablábamos al principio) para que añadan esa información verificada por ti.

Como esos validadores están usando sus recursos (energía computacional) para mantener la *blockchain*, se les remunera con las *gas fees* para que sigan haciéndolo.

**Gas fees:** tasas que pagamos a los nodos para que añadan información en la *blockchain*. Su precio depende de la cantidad de información añadida y de la congestión de la red en un momento determinado.

Su precio depende de varios factores, pero los más importantes son la cantidad de información cambiada y la cantidad de transacciones que se registran en un mismo momento.

Cuanta más información cambies o añadas, más tendrás que pagar. De la misma forma, las *gas fees* (al menos en PoW) se basan en un sistema de subastas que se explica con el ejemplo del autobús: Hay 100 personas esperando un autobús y solo caben 15. Pasa uno cada 10 minutos. Entonces, el conductor le dice a la gente que quien más pague, podrá montarse en el primer autobús, y los que no, tendrán que ir esperando a que vengan autobuses nuevos. De esta forma, van montándose personas hasta subir los precios a límites absurdos (si no para de llegar gente) o hasta que se reduzca el número de personas esperando la cola.



Como puedes imaginar, esto conlleva un gran problema: si queremos que mucha gente se suba al autobús de la *blockchain* (es decir, que haya adopción), tendremos que in-

crementar la frecuencia de autobuses de alguna manera. Este, de hecho, es el problema de escalabilidad de Ethereum.

Un dato: las *blockchains* que usan PoS, al ser mucho más eficientes, tienen unas *gas fees* bajísimas en comparación a las que usan PoW. Es decir, su frecuencia de autobuses es mucho mayor.

### NOTA FINAL

Además de todo esto, y a pesar de que cada *blockchain* es distinta, las más grandes y relevantes como Bitcoin o Ethereum tienen la característica de ser muy transparentes. De hecho, cada transacción que ha ocurrido en ellas, así como toda la información que hay, es accesible para cualquier persona. Así, puedes saber qué criptoactivos (como criptomonedas) tiene la *wallet* de cualquiera.

Aquí es donde viene la parte curiosa: gracias a esta transparencia, podemos confiar más en la *blockchain* y en sus usuarios, ya que todo se puede comprobar. Es más, algo que en mi opinión es muy interesante es que ocurre lo contrario que en el sistema bancario tradicional: puedes saber cuántas criptomonedas tiene una *wallet*, pero no quién hay detrás de la *wallet* (al menos fácilmente), ya que son pseudónimas.

De esta forma, comienzan a establecerse las bases para una criptoeconomía en general y para los **NFT** en particular.