



# Fundamentos técnicos y casos prácticos

9-16 diciembre 2021

Antonio Cruces Rodríguez [antonio.cruces@uma.es](mailto:antonio.cruces@uma.es)



UNIVERSIDAD  
DE MÁLAGA

| [uma.es](http://uma.es)



Trans\_UMA

# NF... ¿qué? ...ni idea de lo que significa

para entender el concepto de los **NFT** (*non-fungible token*), primero tenemos que entender que en nuestro sistema jurídico, existen **bienes fungibles** y **bienes no fungibles**

- los **bienes fungibles** son los que pueden intercambiarse, teniendo un valor en función de su número, medida o peso
- los **bienes no fungibles** son los que no son sustituibles

un ejemplo de **bien fungible** es el **dinero**; si tienes un billete de 20 euros, se trata de un bien fungible, ya que lo puedes intercambiar sin problemas por otro billete de 20 euros, no pierde valor y es exactamente igual; además, este billete se consume cuando lo utilizas

un ejemplo de **bien no fungible** sería una **obra de arte**; si tienes un cuadro en casa, este no se consume al utilizarse y tampoco puede ser sustituido por otro cuadro; una obra de arte no es equivalente a otra, y por lo tanto, no se pueden simplemente intercambiar como pasa con un billete de 20 euros

# pues tengo muchas **preguntas** al respecto

si tengo un Pollock y quiero dárselo a mi primo a cambio de su Klimt, y ambos quedamos de acuerdo, podemos hacerlo sin problemas (salvo las cuestiones de Hacienda); por tanto, serían fungibles...

puedes cambiárselo, pero ambas seguirán siendo obras diferentes, y su valor *intrínseco* (no de *cambio*) también; el valor de *cambio* varía a lo largo del tiempo, pero no el *intrínseco*

cada billete de 20 euros es diferente de otro: tienen números de serie distintos...

pero su valor no: con ambos puedes comprar bienes por un importe de 20 euros; son fungibles

...pero un NFT sería como una obra de arte única, por ejemplo, el David de Miguel Ángel; solo hay uno y está en la Galería de la Academia de Florencia; si alguien quisiese tener ese David en concreto, debería comprarlo (si estuviese a la venta) o hacerse con una copia, en cuyo caso, ya no estaríamos hablando del original, que es lo que dota de valor a la escultura



un NFT tiene un valor, y el oro o un billete, también...

# parece interesante: cuéntame **más**

al **tokenizar** un objeto no fungible (poema, vídeo, foto, dibujo, canción,...), los detalles importantes del mismo se digitalizan con el token

los tokens se guardan en carteras, que también tienen sus propias direcciones únicas

las identificaciones de los tokens apuntan a las direcciones de los monederos en la cadena de bloques, que es una gran base de datos de acceso público, por lo que cualquiera puede verificar la propiedad digital

esto también significa que las versiones falsas de los NFT nunca podrían pasar por las auténticas

token, tokenizar... ¿qué rayos es un **token**?

es una representación de un valor; y, aunque te parezca una palabra poco corriente, los usas a diario: una tarjeta de crédito, con la que te identificas ante un cajero automático, te representa a tí como persona, y por eso el cajero autoriza la operación



# vale, has captado mi atención; ¿puedo hacer un NFT?

¡pues claro! en realidad, es mucho más fácil de lo que parece; y no es necesario (aunque sí es muy conveniente) conocer los entresijos técnicos computacionales de la cuestión, porque hay servicios en la Red que facilitan la creación de NFTs

**OpenSea** y **Rarible** son las principales plataformas, y más adelante explicaremos mucho más sobre ellas, pero ahí va algún adelanto

mientras que Rarible domina en de ventas totales, OpenSea ofrece más servicios relacionados, e incluye la posibilidad de crear tu propia tienda web de NFT impulsada por la bolsa de OpenSea

ambas plataformas permiten a los usuarios subir su arte y crear colecciones sin necesidad de tener conocimientos técnicos de blockchain

también te vendrá bien la ayuda de **MetaMask**



**Rarible**



**OpenSea**



**METAMASK**

# hazme un resumen, porfa...

- el uso de blockchain no es gratuito; el acceso a la cadena tiene un coste (denominado **gas**)
- **Rarible** requiere que los artistas *acuñen* sus NFT en la blockchain durante la creación, lo que significa que han de hacerse inmodificables en ese momento; esto supone menor coste si calculas que tu NFT tendrá “buena salida” en el mercado; si planeas vender un par de NFT a precios enormes, es la mejor opción
- **OpenSea Collection Manager** permite a los usuarios pagar una cuota única para establecer una nueva colección; dentro de ella se puede crear un número ilimitado de NFT, y el equipo centralizado de OpenSea los almacenará fuera de la cadena hasta que se realice una venta; en ese momento, el comprador pagará la tasa de *gas* asociada a la transacción, y tu NFT se colocará en la cadena y se transferirá

¡más de 24  
millones de NFTs!



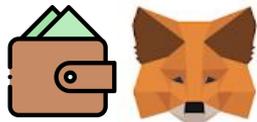
## OPENSEA

- fundada en 2018
- plataforma en línea, un mercado descentralizado que promueve y respalda la venta y la compra, incluido el comercio de NFT
- criptomoneda genérica (ETH)
- unos 20.000 usuarios

## RARIBLE

- fundada en 2020
- mercado comunitario; plataforma segura que permita a los creadores digitales intercambiar sus activos
- criptomoneda propia (RARI)
- más de 11 millones de usuarios

# y en tres simples pasos sería (con OpenSea)...



lo primero es configurar un monedero software; este monedero puede contener tus NFT y también necesitarás utilizarlo para pagar las tasas de *gas* de la cadena de bloques más adelante

dirígete a [metamask.io](https://metamask.io), descarga la aplicación o añade la extensión a Chrome (no funciona en Safari)

crear un monedero **MetaMask** es sencillo y gratuito, pero es muy importante mantener un registro de tus contraseñas en caso de que alguna vez necesites recuperar el monedero

ve a [opensea.io](https://opensea.io) y crea una colección a la que conectar tu monedero **MetaMask** para ponerte a trabajar

asigna un nombre para la colección de NFT, y añade un nuevo elemento; ahora puedes subir el archivo que quieres tokenizar y darle ciertas propiedades para distinguirlo del resto de tu colección

determina cuántas copias quieres de cada NFT y establece un precio de venta al público

para vender tu primer NFT, tendrás que habilitar **OpenSea** para realizar ventas desde tu cuenta; esto requiere una transacción de blockchain, por lo que tendrás que pagar una tarifa de *gas*;

envía un poco de ETH a tu **MetaMask**, y ya puedes empezar; sólo tendrás que pagar esta tasa la primera vez que crees una colección NFT

una vez autorizada la venta, cualquiera puede encontrar y comprar tu NFT en el mercado **OpenSea**

# pero el mundillo NFT no es Jauja

además de tácticas de trabajo con los NFT (*scalping* o reventa, o bien inversión en las propias plataformas), si eres artista o *influencer*, puede valer la pena crear tus propios NFT para tus seguidores

sin ir más lejos, la NBA está tokenizando clips de las mayores jugadas de la historia del baloncesto y vendiéndolos por una fortuna; además, se llevan un 5% de todas las transacciones del mercado secundario

pero, en realidad, lo más interesante del blockchain es que está revolucionando el arte y los objetos de colección tal y como los conocemos

algunas de las **ventajas** que ofrece este sistema de comercialización son evidentes

- un artista puede dar a conocer su obra con gran facilidad en el ámbito internacional sin apenas esfuerzo
- es un gran estímulo para la creatividad
- minimiza (pero no suprime) el papel de los intermediarios (galerías, marchantes,...)
- es un certificado de garantía automático que protege tanto al comprador como al vendedor
- prácticamente elimina el riesgo de incumplimiento contractual



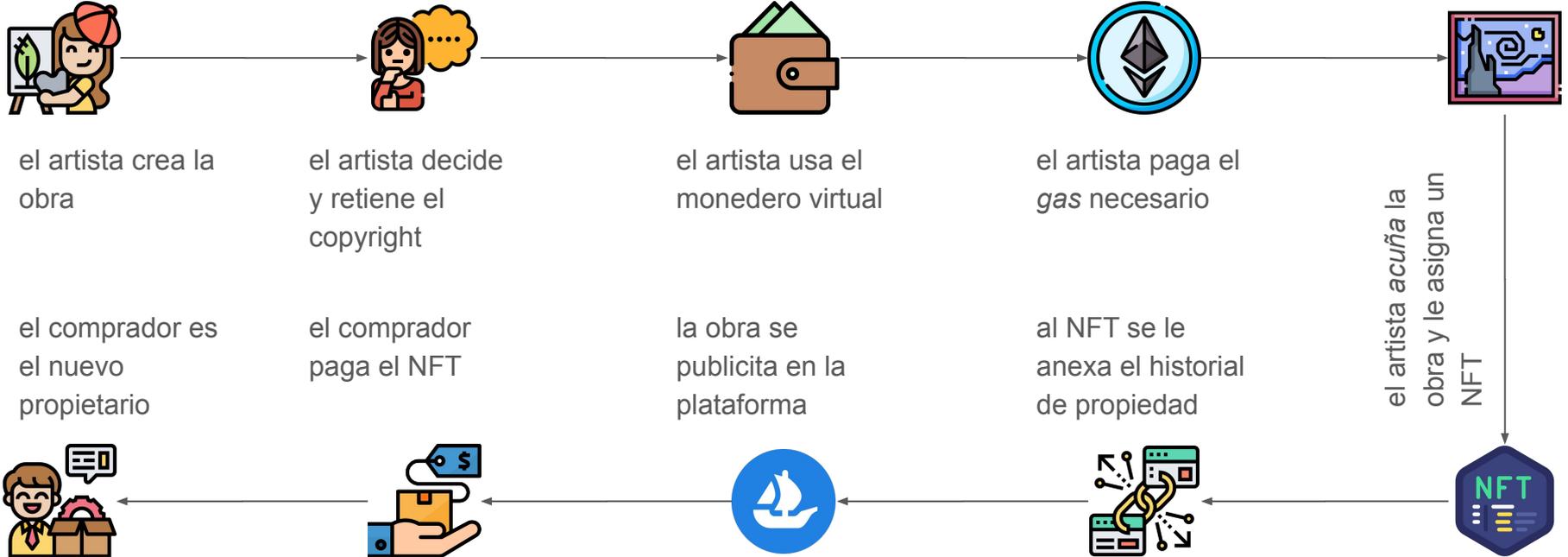
pero **no es oro todo lo que reluce**



- aunque no es imposible, cualquier memez (no “meme”) 😊 no tendrá éxito “porque sí”; en realidad, hay que demostrar calidad e imaginación para atraer al público
- algunos pueden obtener enormes beneficios; pero confiar en conseguirlos nos pinta en la espalda un enorme letrero que dice “iluso”
- se necesita espíritu emprendedor, planificación y estrategia para lograr algo
- es una burbuja, como lo fue la de los “.com” en los 80, y no durará (previsiblemente)

# y sintetizando el proceso en un **diagrama...**

una escalera de **diez peldaños** muy fácil de recorrer





## **Fundamentos técnicos**

# la importancia de la singularidad

un **NFT** (o **TNF**) se parece remotamente a una criptomoneda, pero no es lo mismo; la diferencia reside en su cualidad de único, irrepetible e invariable

característica



es único



es indivisible [\*]



es transferible



puede probar su escasez



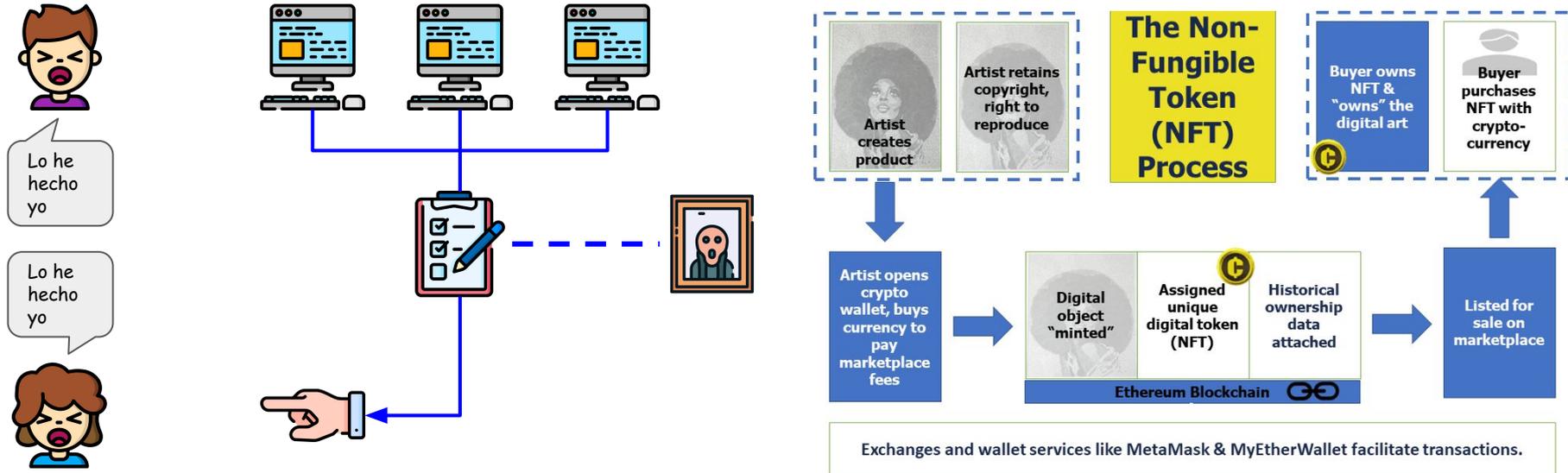
[\*] puede ser parte de una pieza mayor



# ¡eso lo he hecho yo...!

"every step you take I'll be watching you..." (*The Police*, mayo 1983)

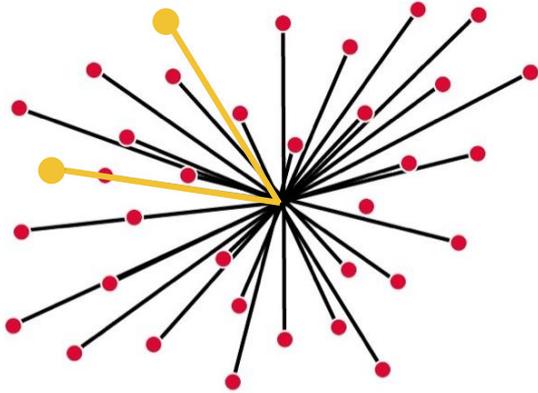
la mejor manera de garantizar la **VERACIDAD** de una afirmación es que **TODO EL MUNDO** esté de acuerdo en ella, sin discrepancias, y que dicho acuerdo esté refrendado por **DOCUMENTOS**



# la importancia de la **topología**

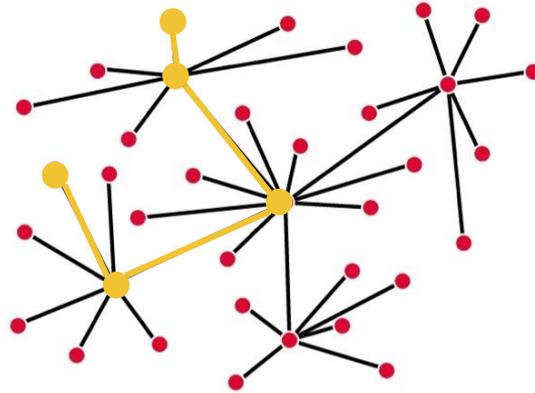
las redes distribuidas son más eficaces para **TRANSPORTAR** información entre dos puntos cualesquiera, independientemente de su ubicación

menor recorrido; si cae el centro cualquier comunicación es imposible



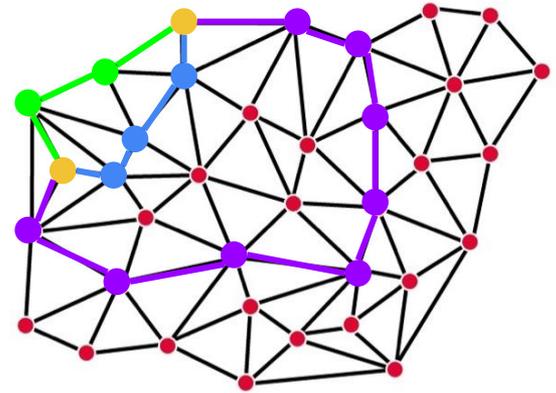
Centralizado

mayor recorrido; si cae un centro aún hay posibilidades de ruta



Descentralizado

recorrido variable; múltiples rutas posibles si el destino está activo



Distribuido

# la cola del cine y el tren

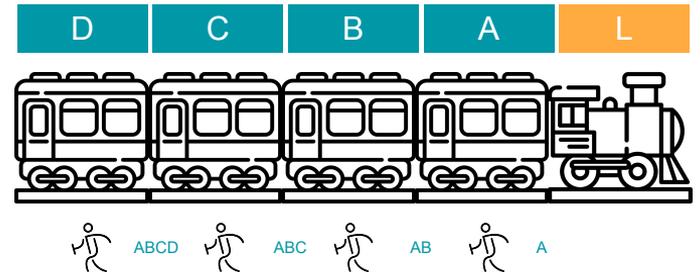
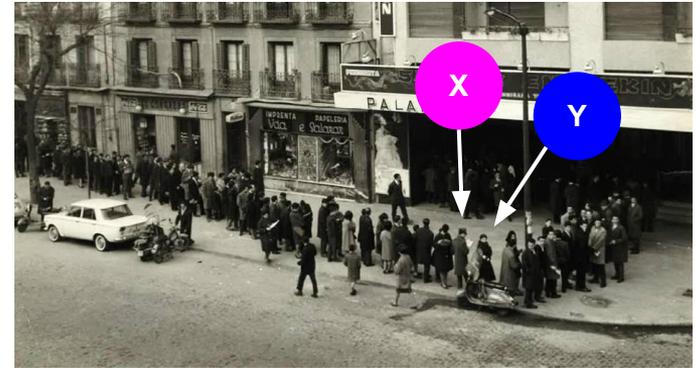
la lista enlazada es la cola de un cine; la cadena de bloques, un tren

en la **lista enlazada**, el bloque X (espectador) sabe que va detrás del bloque Y (que llegó antes), pero le da igual quién le precede (bloque Z) y quién va detrás de él

en la **cadena de bloques**, cada bloque se asemeja a un pasajero que recorre el tren desde la máquina hasta el furgón de cola; cada vez que pasa por un vagón, toma nota de su identidad; cuando llega al último, sabe exactamente por todos los vagones por los que ha pasado

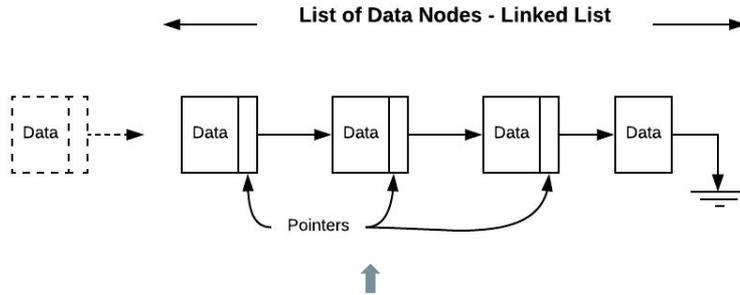


la **cadena de bloques** permite conocer la trayectoria previa de cada bloque y, en consecuencia, su estado ¿a quién pertenece? ¿lo ha obtenido legalmente? ¿su origen es el que afirma ser?; es una excelente manera de garantizar la **procedencia** de un objeto



# la procedencia y la filiación

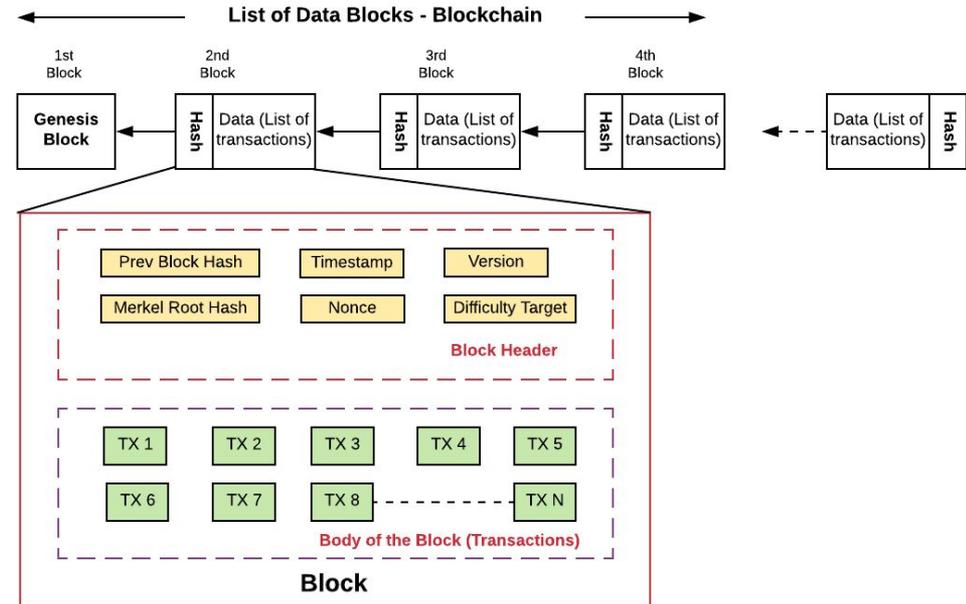
las *blockchain* (cadenas de bloques) y las listas enlazadas **no son lo mismo**



en la **lista enlazada**, cada bloque conoce a su predecesor (*procedencia*) e incluso a su sucesor, pero **NO** su *historial*; un bloque puede ser reemplazado

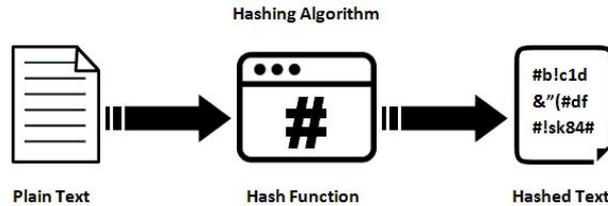


en la **cadena de bloques**, cada bloque conoce a su predecesor, puede demostrar que lo es, y contiene su historial hasta el momento (*filiación*)



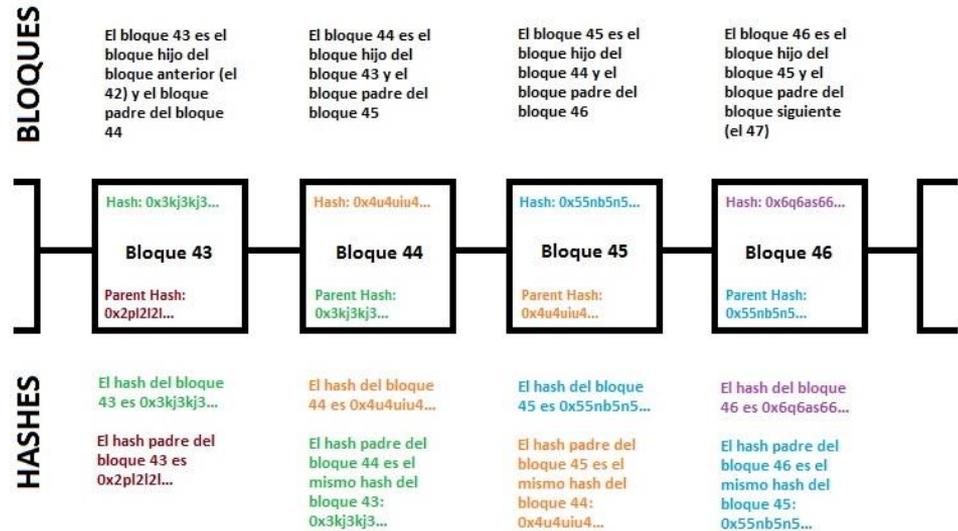
# cómo meter un **elefante** en un “seiscientos”

una función *hash* (#, “picadillo”) es una especie de “huella dactilar”



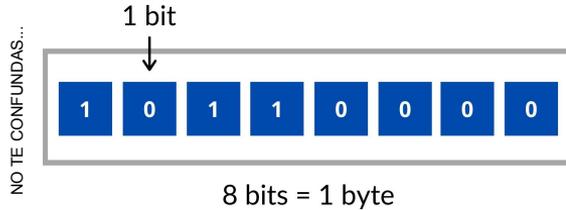
un conjunto de datos, largo y complejo, puede identificarse como único mediante una función *hash*, que dará como resultado un conjunto normalmente de longitud fija; la complejidad del algoritmo determina su fiabilidad y, en consecuencia, su veracidad

cada bloque de la cadena conoce el *hash* de su precedente, de manera que es rastreable su filiación hasta el origen; de esa manera, el último bloque puede atestiguar sobre el primero



# cómo funcionan los *hashes*

hay muchos **algoritmos**, pero suelen utilizarse aquellos más “sólidos”



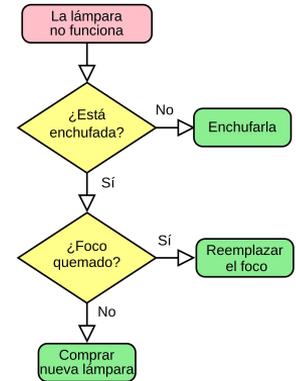
la forma más efectiva de evitar la colisión de *hash* es expandir el espacio de valores del valor de *hash*; para 16 bits binarios, la probabilidad de colisión es de uno entre 65.536; en otras palabras, si hay 65.537 usuarios, habrá una colisión; aumentar la longitud del valor hash a 32 bits binarios reduce la probabilidad de colisiones a uno entre 4.294.967.296

**debilidades** fundamentales de un hash: la **probabilidad** de una **colisión** (que dos conjuntos de datos diferentes tengan el mismo *hash*) y el **balance del costo** entre la potencia de cálculo necesaria y el beneficio (fiabilidad) obtenido; la primera se reduce notablemente usando un algoritmo que devuelva un *hash* más largo; los ordenadores actuales pueden realizar cálculos extremadamente complejos con un balance muy favorable

Diccionario de la lengua española. Edición del Tricentenario. Actualización 2020

## ALGORITMO

Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema.



# algunos ejemplos de algoritmos *hash* muy usados

SHA-256 (Bitcoin) genera un hash casi único, con 256 bits (32 bytes)

la verificación por redundancia cíclica (**CRC**) se usa para detectar errores usado en redes digitales y dispositivos de almacenamiento para detectar cambios accidentales en los datos; **MD5** es uno de los algoritmos de reducción criptográficos diseñados por Ronald Rivest del MIT (1991); poco usado desde que en 1996 se le descubrieron colisiones

algoritmo

**CRC-16**

**MD5**

**SHA256**

Antonio Cruces Rodríguez

b9ca

4a54d85114323d1e92ee5f  
61da1ce44a

5f37d612b512a54290a4d7  
683eb008760d13e33fe95  
d1687da6e3afc1e134c7

Antonio Cruces Rodríguez

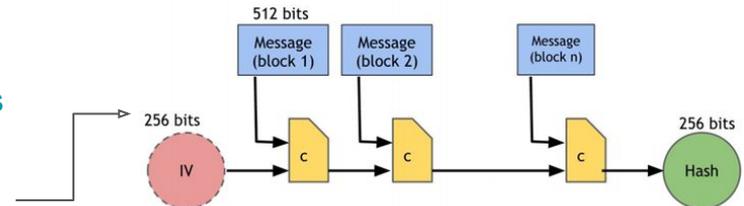
8613

5984df1f6a8f903ce41021  
e71c7b1b8f

13e75783d832de490e70e9  
befeef9c6eb0cf7d9c61c0  
b24d6e590863d0c8924e

los algoritmos **SHA** fueron desarrollados por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y el National Institute of Standards and Technology (NIST) desde 1993; **SHA-256** se considera muy seguro

IV: vector de inicialización; TEOREMA: si **c** no tiene colisiones, **hash** tampoco las tendrá



# hashing y criptografía: una pareja ideal

un hash criptográfico tiene varias propiedades que lo hacen ideal para esa tarea

**determinista**; no importa cuántas veces se aplique el hash: siempre se obtendrá el mismo resultado

**computación rápida**; la velocidad implica eficiencia

**resistencia de la preimagen**; no es imposible, pero sí inviable, obtener el original a partir del hash calculado

**efecto avalancha**; un pequeño cambio en el original se traduce en un cambio enorme en el *hash*

**compresión**; reduce mucho la cantidad de datos a utilizar

**resistencia a la colisión**; no es imposible, pero sí inviable, que dos hashes de dos entradas distintas coincidan y den lugar a errores

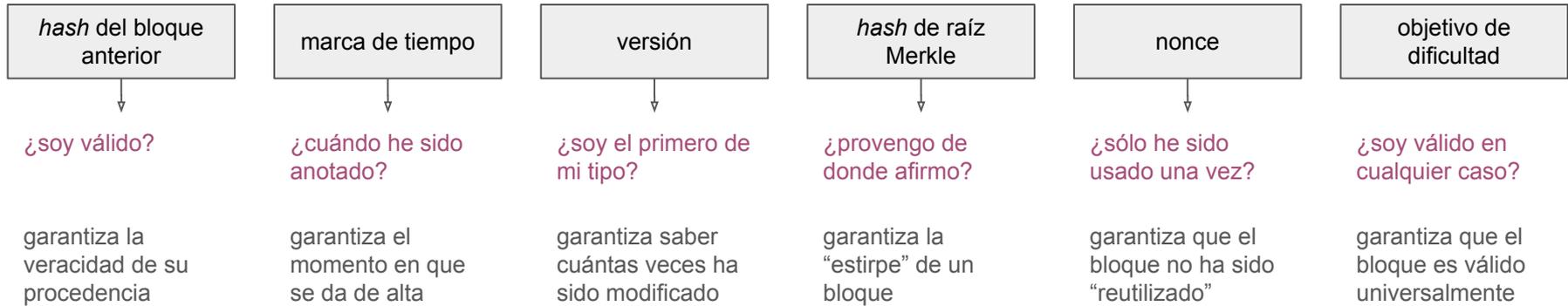
Y AÚN TIENE MÁS VENTAJAS...

en el caso de **SHA-256**, no importa cuán grande o pequeña sea su entrada, la salida siempre tendrá una longitud fija de 256 bits. Esto se vuelve crítico cuando se trata de una gran cantidad de datos y transacciones, porque, básicamente, en lugar de recordar los datos de entrada —que podrían ser enormes— el *hash* permite realizar un seguimiento

el ataque de **fuerza bruta** (ir probando originales a partir del hash) promedio requeriría alrededor de  $1,7 \times 10^{38}$  **intentos**: un número realmente enorme

# una sopa de letras para garantizar el resultado

en el tren *blockchain*, la *cabecera* es el enganche de cada *cuerpo* (vagón)



Ralph **Merkle** inventó el concepto (1979) de **árbol o raíz** que lleva su nombre; cada “hoja” aporta su *hash* para construir el *hash* de la “rama padre”; es algo así como el ADN del bloque; “**nonce**” (apócope de *number that can be only used once*) es un número arbitrario que se puede usar solo una vez en una comunicación criptográfica; garantiza que las comunicaciones antiguas no se puedan reutilizar; la red de bitcoin tiene una **dificultad de bloque global**, que se recalcula más o menos cada dos semanas; un bloque es válido si su *hash* está por debajo de este objetivo

# para resumir...

las cadenas de bloques y las listas enlazadas se parecen, pero no son iguales

## LISTA ENLAZADA

- lista conectada mediante **punteros**
- el puntero indica cuál es el siguiente (o precedente) nodo; si es nulo, no existe
- un nodo puede ser modificado (y, en consecuencia, falsificado)
- se puede añadir un nodo en cualquier punto de la lista
- si se borra un nodo y se copia su puntero al siguiente (o anterior) la lista seguirá trabajando igual

## CADENA DE BLOQUES

- lista conectada mediante **enlaces**
- el enlace es un *hash* de la cabecera del bloque anterior; así no solo apunta a él, sino que lo valida
- para modificar un bloque habría que recalcular toda la cadena completa
- un bloque solo se puede añadir al final de la cadena
- borrar un bloque implica recalcular toda la lista y sus *hashes*

## LA UNIÓN HACE LA FUERZA

para falsificar un NFT, TODAS las copias de la cadena de bloques, en una red mundial distribuida, deben estar de acuerdo y señalar exactamente lo mismo; cualquier discrepancia significativa invalida la afirmación de titularidad; ***you can fool all the people some time, you can fool some of the people all of the time, but you can not fool all the people all the time*** (atribuida a Abraham Lincoln)

# ¿y todo esto qué tiene que ver con NFT?

1 algo de **vocabulario**, para desenvolverse en un mundo (no tan) complejo

pues tiene mucho que ver; porque el sistema **blockchain** es el que asegura la veracidad de las transacciones, garantiza su integridad y actúa como una especie de “caja fuerte” que impide la falsificación y valida todas las operaciones; por eso es importante saber cómo funciona

**ERC-721** estándar o conjunto de normas que se usan para regular las transacciones NFT (2018)

**CONTRATO INTELIGENTE** eso es un NFT: una *relación* entre dos usuarios que acuerdan intercambiar un elemento único por un valor económico

**CONTRATO INTELIGENTE + TOKENID** el primero (URI<sup>[\*]</sup>) más el segundo definen un elemento único, que “apunta” al objeto

**TOKENID** número entero definido por 256 bits; puede alcanzar un valor máximo que equivale más o menos a 1.579 seguido por 74 ceros

**ETHEREUM** plataforma digital que adopta la tecnología blockchain

**ETHER (ETH)** criptomoneda nativa de Ethereum; es parte de un sistema financiero entre *pares*<sup>[\*\*]</sup> autónomo, libre de intervención gubernamental

**MINERÍA** blockchain funciona como un libro de contabilidad; los mineros verifican grupos de transacciones para formar bloques y codificarlos, enlazándolos a la cadena anterior; el minero recibe una recompensa (un número fijo de *tokens*<sup>[\*\*\*]</sup> de ether)

[\*] URI = Universal Resource Identifier; una especie de “dirección Internet” [\*\*] pares = partes con el mismo rango y las mismas atribuciones [\*\*\*] token = ficha, valor o símbolo; en este contexto, equivaldría a las fichas de los casinos, que pueden cambiarse por un valor real

# ¿un “contrato inteligente”?

(casi) nada es gratis; el uso de blockchain tiene un coste, una tasa de red llamada **gas**, que tendrás que pagar para tokenizar tu arte

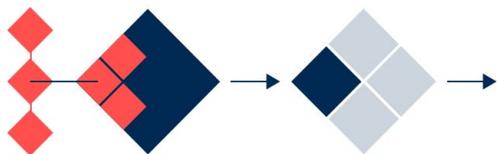
pero no  
olvides  
que...

## 2 algo de **vocabulario**, para desenvolverse en un mundo (no tan) complejo

pues sí: si un contrato tradicional describe los términos de una relación; un *smart contract* se asegura de que esos términos se cumplen escribiéndolos en código, programas que automáticamente ejecutan el contrato una vez que las condiciones predefinidas se cumplen, eliminando el retraso y el coste que existe al ejecutar un acuerdo de manera manual

POR EJEMPLO...

quieres enviar una cantidad establecida de ether a un amigo en una fecha determinada; se genera este código en la blockchain y cuando el contrato se complete (llega la fecha acordada) los ether se enviarán automáticamente



El minero agrupa transacciones de criptomoneda nuevas en un "bloque".



El bloque se codifica y se vincula a la cadena de bloques o blockchain existente.



El minero obtiene su recompensa, que puede inyectar directamente de nuevo en el mercado.



Un número fijo de usuarios anónimos acuerdan unos términos y el contrato se codifica dentro de la cadena de bloques.

El evento desencadenante se produce y el contrato se cumple.

Los términos del acuerdo se ejecutan entonces entre las partes correspondientes.

# la minería no me ha quedado clara...

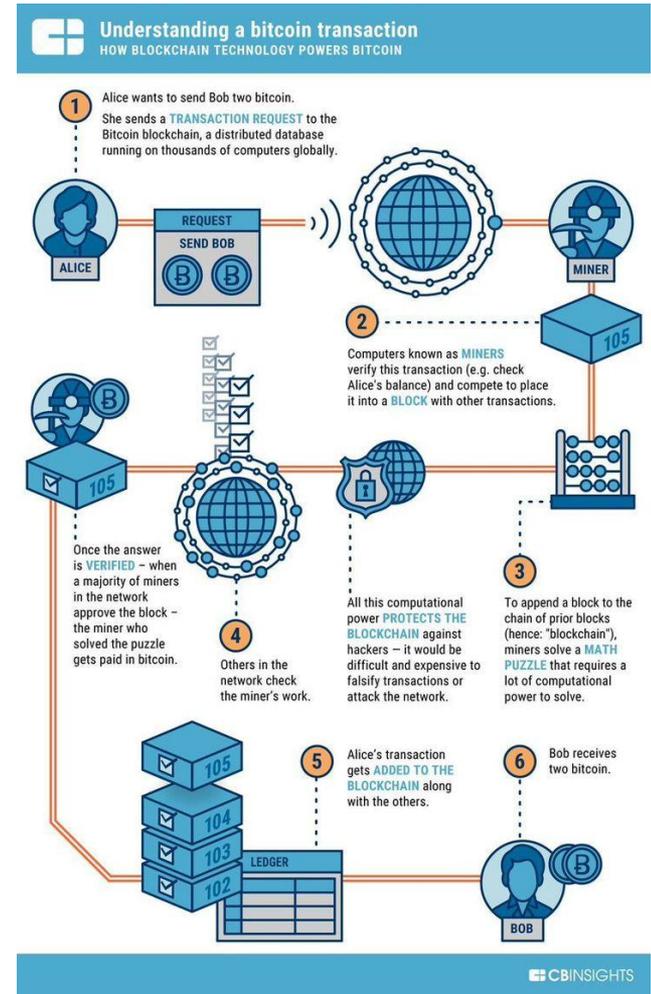
la propia página de Ethereum lo explica bastante bien

Ethereum utiliza un mecanismo de consenso llamado *prueba de trabajo*; cualquiera que quiera añadir nuevos bloques a la cadena deberá resolver un difícil rompecabezas, para el que se precisa mucha potencia computacional; resolver el rompecabezas demuestra que has invertido los recursos computacionales necesarios

este proceso se denomina **minería**; puede entenderse como un proceso de prueba y error, pero la exitosa adición de un bloque se recompensa con ETH; además, el envío de bloques fraudulentos no es una opción atractiva considerando los recursos que se invierten en producir un bloque

los nuevos bloques son transmitidos a la red, y una vez revisados y verificados, se actualiza el estado para todos; en resumen: cuando envías ETH a alguien, la transacción se debe minar e incluir en un bloque nuevo.

<https://ethereum.org/es/developers/docs/intro-to-ethereum/>; el esquema es válido también para ETH (<https://www.pinterest.es/pin/401242648043898675/>)





**Caso práctico**

# no es nada difícil, pero hay que prestar atención

para que empieces a utilizar el recurso de comercializar tus obras o tus creaciones con **NFT**, es preferible no apuntar demasiado alto; por eso la recomendación es, en tus primeros pasos, trabajes con **OpenSea**

pero antes de comenzar necesitarás un monedero virtual (*wallet*), donde guardar tus activos y tu dinero; hay muchos en la Red (**Coinbase Wallet, WalletConnect, Fortmatic, Kaikas, Bitski, Venly,...**); sin embargo, la sugerencia es **MetaMask**; es sencillo, se puede instalar tanto en móvil como en tableta o sobremesa (en este último caso, solo en Chrome)

y te recordamos que nada es “gratis total”: probablemente te hará falta una primera inyección de ETH, aunque hay algún que otro atajo...



**METAMASK**



**OpenSea**

# vayamos por partes... ¿qué tal un mapa de carreteras?

pues hay uno, y bastante bueno, que se muestra condensado aquí; los de **Criptonoticias**, un medio independiente especializado en formar en el uso de blockchain, tienen un excelente **tutorial** que recomendamos seguir

en 2020 se lanzó un nuevo tipo de arte digital NFT capaz de ser programable y mutar de apariencia; conocido como arte volátil, fue introducido por la plataforma de arte, AsyncArt y permite que un elemento digital interactúe con datos de la blockchain; la galería de arte ha vendido dos piezas que funcionan con este nuevo mecanismo, un cuadro de Bitcoin y otro de Vitalik Buterin, ambos por más de 200 ETH



**ESTO ES UN NO PARAR:** en febrero de 2021, Christie's subastó un collage de 5.000 piezas creado por el artista Mike Winkelmann

en febrero de 2021 el mercado NFT superó los 500 millones de dólares; algunas piezas digitales se venden por precios cada vez más altos por el interés que despiertan en coleccionistas e inversores, llegando a comprarse un meme NFT de Homero Simpson Pepe en 320.000 dólares y un *cryptopunk* (un coleccionable) por 7,5 millones

# pero hay que pagar, ¿no? ¡ya me parecía a mi...!

**OpenSea** funciona sobre la red de **Ethereum**, así que necesitarás una cartera de esta red que permita interactuar con **DApps**; te sugerimos **MetaMask**, aunque **Coinbase** o **Trust** también son buenas opciones

y ahora, la primera decisión...



## QUIERO VENDER YA

hay que echar al monedero algunos ETH para comenzar a *acuñar* NFTs; las **comisiones** aproximadas suelen rondar **entre los 5 y los 25 USD** (en ETH) dependiendo de la congestión de la red; la plataforma suele cobrar el **2,5% del importe** si logras vender tu NFT

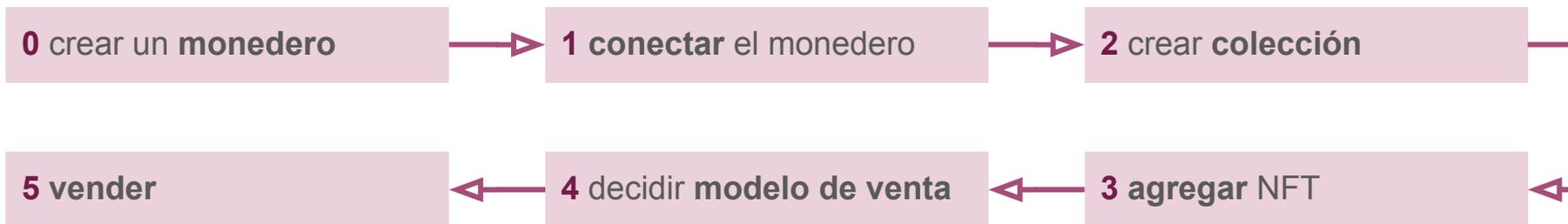
## QUIERO PROBAR ANTES

pues estás de suerte: OpenSea se encuentra disponible en distintas redes de prueba de Ethereum, como en **Rinkeby** (ahora **testnets**). Así puedes crear y poner en venta un NFT sin gastar dinero; además, también proporcionan un sistema **gas-free**, más lento pero menos oneroso para publicar NFTs

**DAPP** acrónimo de *decentralized application*, que funciona en una red *distribuida*; no hay servidores centrales; de hecho, una DApp es en realidad una **blockchain**; son muy transparentes, muy difíciles de manejar y bastante refractarias a ataques maliciosos y censura; sin embargo, su escalabilidad es un punto débil, así como el problema del **“51%”**: si una mayoría se hace con el control de los nodos, puede influir decisivamente

# vale, ya he decidido ¿qué tengo que hacer?

pues simplemente seguir unos sencillos pasos, asegurándote de que cada uno está correctamente realizado; es muy conveniente, cuando se juega con posibles gastos, ser precavido y cuidadoso



¿por qué algunos NFT son tan valiosos?

muchos NFT resultan **valiosos** para sus compradores debido a que sus características son «**deseables**» (no para todos, pero para gustos, colores); también existen series de estos activos que lo son por su **historia** o por su **utilidad**: por ejemplo, un ticket puede ser valioso porque es la oportunidad para asistir a un evento; otros, por el **origen** con el que fueron generados: un *tweet* de Jack Dorsey está en venta a precio exorbitante porque son las primeras palabras tuitadas por el mismísimo CEO de la red social; no cabe duda de que el valor de algunos tokens reside en su **inmutabilidad** y en su naturaleza **irrepetible**; y, además, no podía faltar otro punto de gran importancia que contribuye a la valoración de los NFT hoy en día: la **especulación**

# 0 crear un monedero

**recuerda:** en macOS NO puede instalarse en el navegador Safari; Chrome es una buena alternativa; en móviles Apple o Android puede instalarse sin problemas

sigue el procedimiento habitual para registrarte en cualquier plataforma y crea una nueva cartera

establece una **contraseña**

la particularidad: para evitar suplantaciones, MetaMask usa una **frase de respaldo**, que deberás conservar cuidadosamente; será tu salvaguarda ante cualquier problema



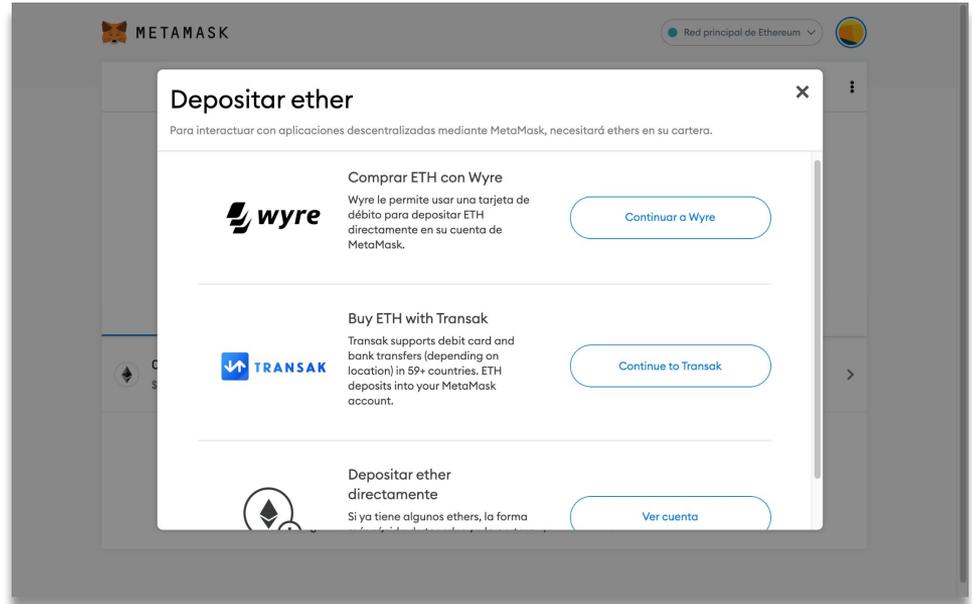
# 0 añade ETH

**recuerda:** preferiblemente hazlo justo cuando lo necesites (antes de pagar *gas*, por ejemplo); en cualquier caso, y como medida de seguridad, puedes bloquear el monedero mientras no te haga falta

puedes emplear cualquier compañía de las que MetaMask te propone

puedes añadir dinero a ETH de **forma anónima**, pero con un **límite** semanal

la mayoría de servicios de compra ETH te indicarán la **tasa de cambio**, el importe de la **transacción** (lo que cobra ese servicio) y el **pago por red** (lo que se abona a los *mineros*); de media, en 2021 **1 ETH** se cambia a unos **3.500 €**



# 0 usa cualquier compañía para añadir ETH

**recuerda:** cada compañía que realiza la transferencia entre una moneda “física” y ETH cobrará un pequeño porcentaje; las siglas **TBD** significan *to be determined*, porque se calcula según el importe

la imagen de ejemplo corresponde a la compañía Wyred, que será la que cargue el importe en la cuenta de crédito o débito que se utilice

las tasas de cambio entre divisas (por ejemplo, € y ETH) fluctúan con muchísima rapidez, y el porcentaje de transacción se fijará en el momento en que se decida efectuar la compra

The screenshot shows a payment interface with the following elements:

- A notification at the top: "Your limit is 1000. Verify your identity to increase your limit to \$28000/week!"
- A large display of "€ 100" with a red arrow pointing to it from the text "cantidad que se desea transferir a MetaMask".
- Below the amount, it shows "-0.02331561 ETH".
- Two currency selection buttons: "EUR" and "ETH", with a red arrow pointing to "ETH" from the text "divisa".
- A blurred card number field with a red arrow pointing to it from the text "datos de la tarjeta de crédito o débito".
- A dropdown menu set to "Credit / Debit".
- A summary table at the bottom:

ETH Exchange Rate	4288.97 EUR
Transaction fee ⓘ	4.35 EUR
Network fee ⓘ	9.91 EUR

# 0 ojo con los **costes** de la transacción

**recuerda:** puedes escoger entre diferentes modalidades de pago para comprar ETH; todas tienen costes añadidos

The image shows two screenshots from a payment interface. The left screenshot displays a summary of transaction costs in EUR, with a red arrow pointing to the 'Purchase Total' of 114.25 EUR, labeled 'importe total que se cargará en la tarjeta'. Below this is a checkbox for authorization, with a red arrow pointing to it labeled 'aceptar para continuar'. The right screenshot shows the 'Select payment method' screen, with a red arrow pointing to the 'Credit / Debit' option, labeled 'OJO a los costes'.

**EUR** > **ETH**

Credit / Debit

ETH Exchange Rate	4282.92 EUR
Transaction fee	4.35 EUR
Network fee	9.89 EUR
<b>Purchase Total</b>	<b>114.25 EUR</b>

**importe total que se cargará en la tarjeta**

**aceptar para continuar**

I authorize Wyre to debit my account indicated for the amount above on today's date, and I agree to [Wyre's User Agreement](#)

Next

Select payment method

This browser does not support Apple Pay

Credit / Debit

- Instant
- 3% fee
- \$500/week

**OJO a los costes**

Apple Pay

- Instant
- 3% fee, \$5 min
- \$500/week

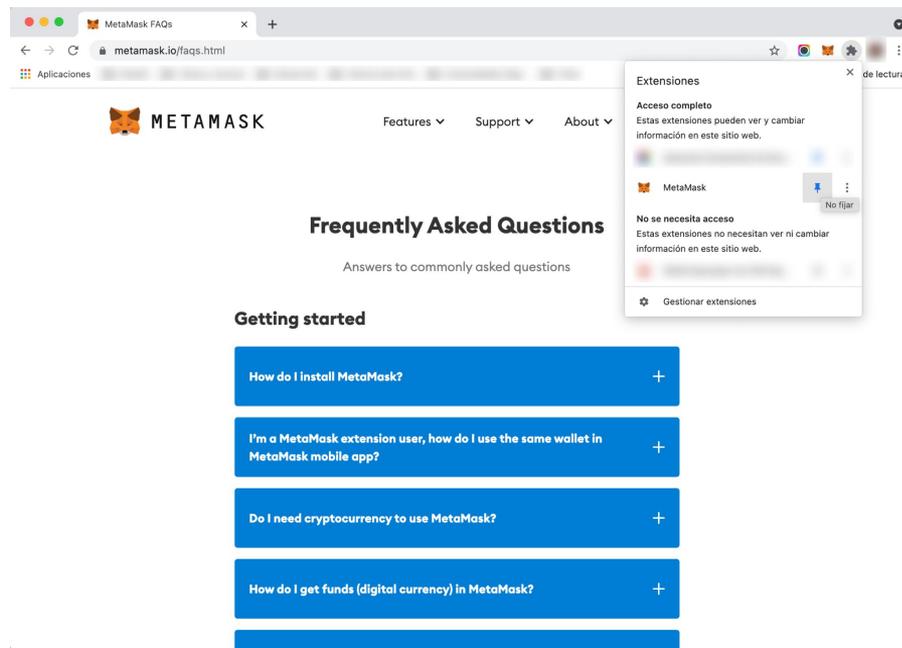
# 0 añade la **aplicación** al móvil o al navegador

**recuerda:** en los ordenadores de sobremesa o portátiles, únicamente el navegador Chrome acepta la aplicación MetaMask

en Chrome, pulsa sobre la pieza de puzzle situada en la barra de navegación para añadir la aplicación MetaMask

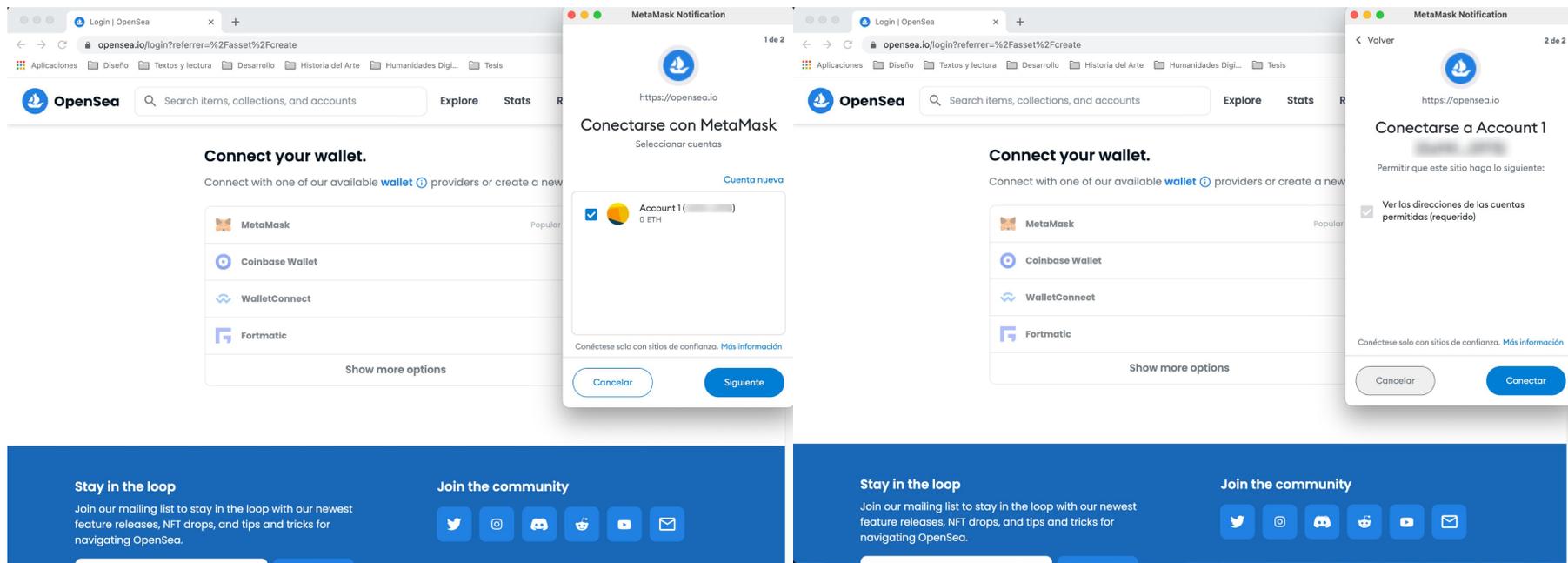
puedes fijarla de manera que se muestre permanentemente

cada cierto tiempo te pedirá reidentificarte; es una medida de seguridad



# 1 conecta el monedero con OpenSea

**recuerda:** puedes realizar transacciones desde la página de OpenSea simplemente abriendo la aplicación



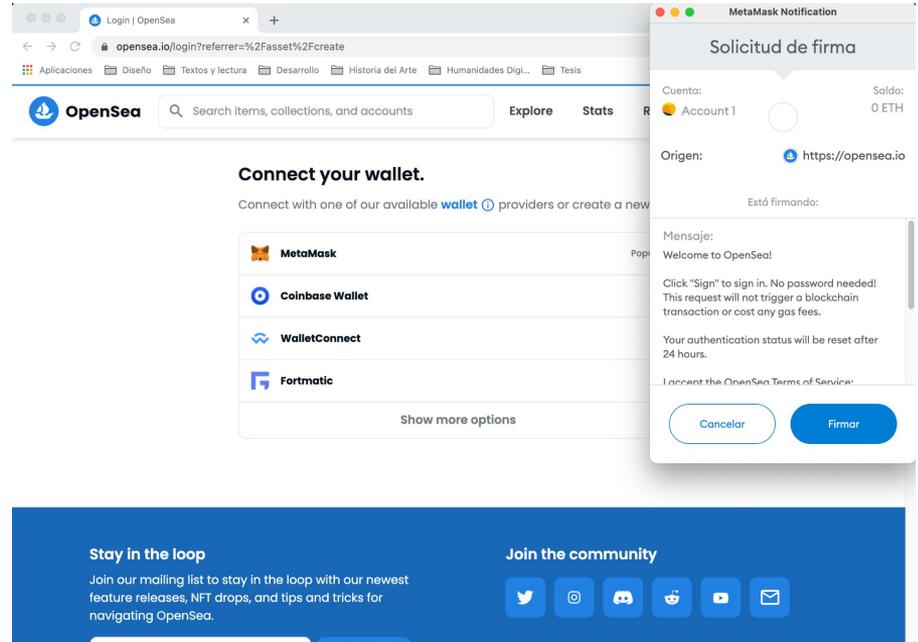
## 2 crea una colección

**recuerda:** cuando lo hagas, OpenSea te pedirá una firma; no conlleva ninguna transacción monetaria, y caduca a las 24 horas; en esa firma se vincula tu monedero y la cuenta de OpenSea

pulsa el menú de arriba a la derecha (normalmente un círculo con una imagen) para abrir tu perfil; escoge *My Collections* para crear una colección y pulse el botón *Create a collection*

cada NFT debe estar dentro de una colección; no importa si es uno solo, este debe pertenecer a una colección específica

puedes crear cuantas colecciones quieras



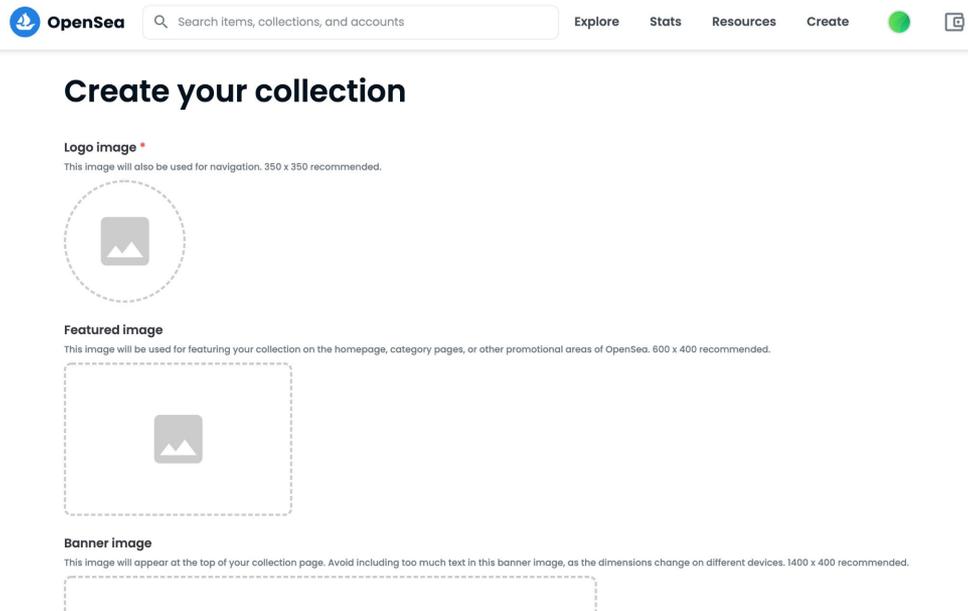
## 2 rellena el formulario de la nueva **colección**

**recuerda:** los únicos campos obligatorios son un logotipo (se sugiere de 350 x 350 píxeles) y el nombre; ambos son muy importantes, porque dan “pistas” sobre el contenido de tu colección

también son importantes los campos como la URL (que debe ser descriptiva, si es posible) y la descripción

el blockchain elegido será habitualmente Ethereum (aunque puede ser otro, como Polygon)

se puede establecer un royalty, de pago mensual, cuando un usuario revende un artículo que creaste originalmente; se paga mensualmente



The screenshot shows the OpenSea interface for creating a new collection. At the top, there is the OpenSea logo, a search bar with the text "Search Items, collections, and accounts", and navigation links for "Explore", "Stats", "Resources", and "Create". Below the navigation bar, the main heading is "Create your collection".

The form contains three main sections:

- Logo image \***: A circular dashed box containing a placeholder icon of a mountain range. Below it, the text reads: "This image will also be used for navigation. 350 x 350 recommended."
- Featured image**: A rectangular dashed box containing a placeholder icon of a mountain range. Below it, the text reads: "This image will be used for featuring your collection on the homepage, category pages, or other promotional areas of OpenSea. 600 x 400 recommended."
- Banner image**: A wide, short rectangular dashed box containing a placeholder icon of a mountain range. Below it, the text reads: "This image will appear at the top of your collection page. Avoid including too much text in this banner image, as the dimensions change on different devices. 1400 x 400 recommended."

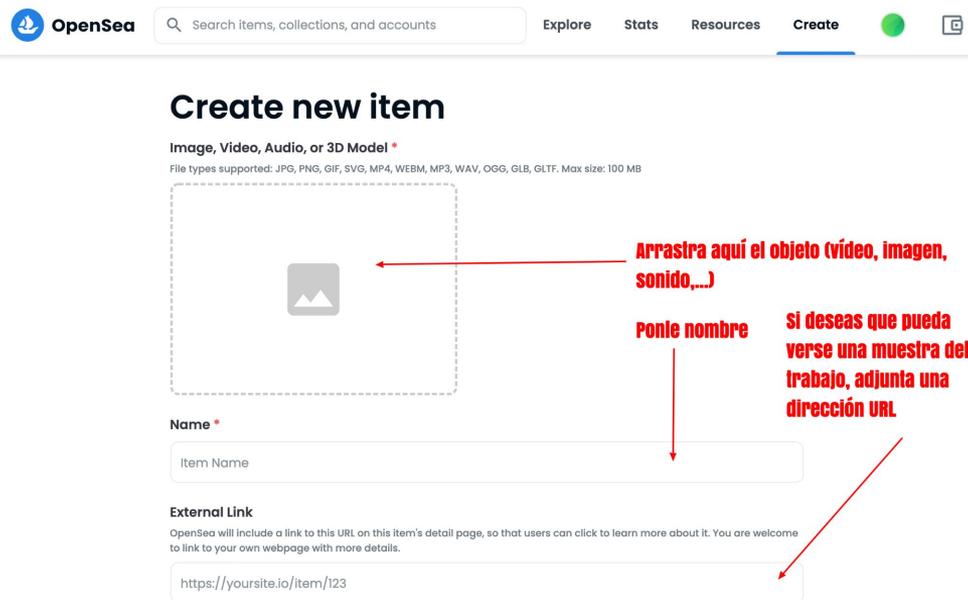
### 3 agregar NFT a la colección (1)

**recuerda:** la información que asignes será inmutable y no podrá ser modificada una vez el NFT haya sido puesto en venta; esto, en cierta manera, le presta autenticidad y colectibilidad

también son importantes los campos como la URL (que debe ser descriptiva, si es posible) y la descripción

el blockchain elegido será habitualmente Ethereum (aunque puede ser otro, como Polygon)

se puede establecer un *royalty*, de pago mensual, cuando un usuario revende un artículo que creaste originalmente; se paga mensualmente



The screenshot shows the OpenSea 'Create new item' interface. At the top, there is a search bar and navigation links for 'Explore', 'Stats', 'Resources', and 'Create'. The main heading is 'Create new item', followed by the sub-heading 'Image, Video, Audio, or 3D Model \*'. Below this, it lists supported file types: 'JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF. Max size: 100 MB'. A large dashed box contains a placeholder icon of a mountain range. A red arrow points to this box with the text 'Arrastra aquí el objeto (vídeo, imagen, sonido,...)'. Below the box is a 'Name \*' field with a placeholder 'Item Name'. A red arrow points to this field with the text 'Ponle nombre'. Below the name field is an 'External Link' field with a placeholder 'https://yoursite.io/item/123'. A red arrow points to this field with the text 'Si deseas que pueda verse una muestra del trabajo, adjunta una dirección URL.' The OpenSea logo is in the top left corner.

# 3 agregar NFT a la colección (2)

**recuerda:** la ficha del NFT es importante; piensa bien el valor que asignarás a cada elemento; los *tags* (etiquetas) ayudan a que posibles compradores encuentren lo que están buscando

**describe el objeto: sé claro pero conciso** →

**deber crearla primero** →

**Identificadores globales (tags)** →

**sólo el propietario puede desbloquear el objeto** →

**crear colecciones** →

**Description**  
The description will be included on the item's detail page underneath its image. [Markdown](#) syntax is supported.  
Provide a detailed description of your item.

**Collection**  
This is the collection where your item will appear. ⓘ  
Select a collection

**Properties**  
Textual traits that show up as rectangles +

**Levels**  
Numerical traits that show as a progress bar +

**Stats**  
Numerical traits that just show as numbers +

**Unlockable Content**  
Include unlockable content that can only be revealed by the owner of the item.

**Explicit & Sensitive Content**

**marcar contenido NSFW** →

**copias que se "acuñarán" (1 normalmente)** →

**divisa de pago**

**¡OJO! si lo marcas, no podrás volver a modificar el objeto**

**Explicit & Sensitive Content**  
Set this item as explicit and sensitive content ⓘ

**Supply**  
The number of copies that can be minted. No gas cost to you! Quantities above one coming soon. ⓘ  
[Input field]

**Blockchain**  
Ethereum **divisa de pago**

**Freeze metadata** ⓘ **¡OJO! si lo marcas, no podrás volver a modificar el objeto**  
Freezing your metadata will allow you to permanently lock and store all of this item's content in decentralized file storage.  
To freeze your metadata, you must create your item first.

**Create**

### 3 agregar NFT a la colección; **campos importantes** (1)

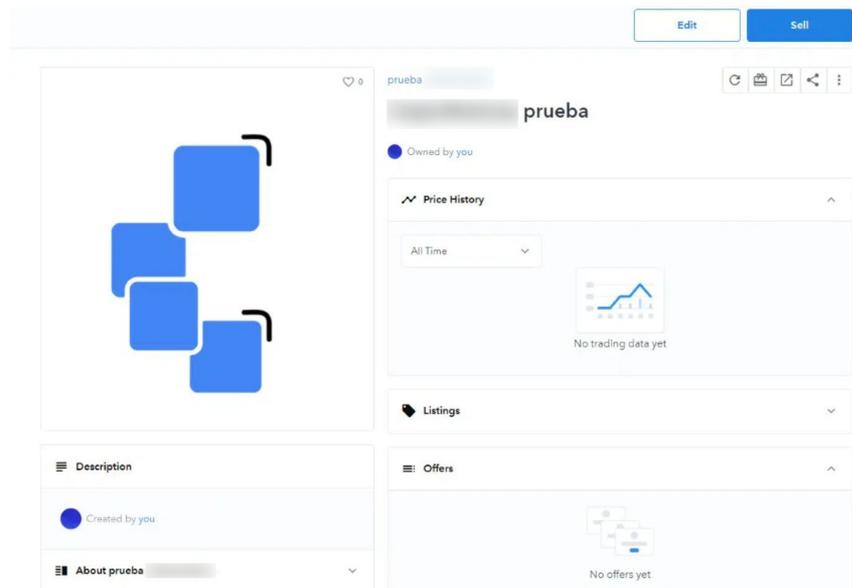
- **Image, Video, Audio, or 3D Model**; tipos de archivos disponibles: JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF, máximo 100 MB
- **Name**; no es obligatorio que sea algo único, como es el caso de los nombres de usuarios. Esto simplemente servirá para identificar tu token
- **External Link**; opcional, aunque facilita a los usuarios poder ir a una web o blog en que puedan conocer más sobre la historia de tu NFT o sobre su creador; puede ser importante
- **Description**; soporta sintaxis *markdown*, que sirve para crear descripciones personalizadas
- **Properties**; opcional, pero permite asignar personalizaciones que destaquen o diferencien al *token*; no está limitado su número
- **Levels**; similar al anterior, pero presentado en una barra más o menos larga
- **Stats**; ídem que el anterior, pero presentado con valores numéricos
- **Unlockable Content**; un texto que solo el dueño del token podrá ver, por ejemplo, una contraseña, un mensaje, etcétera

### 3 terminar la creación del NFT

**recuerda:** estas operaciones previas no son triviales; aunque parezca raro, es perfectamente posible que el creador de un NFT se prohíba a sí mismo modificarlo; sé extremadamente cuidadoso

al pulsar *Create* se abrirá una ventana de tu cartera para confirmar la operación, y ya está creado el token; puedes seleccionar la opción *Visit* para ver más detalles

se pueden visualizar los NFTs creados desde la opción *My collections* del perfil (menú de arriba a la derecha)



Detalles del token NFT creado en OpenSea. Fuente: OpenSea.

### 3 agregar NFT a la colección; **campos importantes** (2)

- **Explicit & Sensitive Content**; permite avisar que el NFT puede tener un contenido no apto para ser mostrado a menores o público sensible
- **Supply**; la cantidad que se creará del NFT; actualmente OpenSea crea un único ejemplar, pero trabaja para crear NFT múltiples; no se trata de “copias”, sino de crear varios originales
- **Blockchain**; la red en la que el NFT será publicado; en el caso de usar la red de pruebas, figurará Rinkeby, pero si se usa la red principal, aparecerá Ethereum
- **Freeze metadata**; son todos aquellos valores que no se almacenan en la blockchain; en OpenSea, la imagen y algunos valores estadísticos del NFT se almacenan en la red de archivos descentralizada IPFS y FileCoin; puesto que estos metadatos están fuera de la cadena de bloques, existe la posibilidad de que sean modificados, cambiando totalmente las características originales de un NFT; esta función «congela» los datos, que ya no podrán ser modificados ni por ti, ni por quien compre posteriormente el NFT

## 4 decidir el modelo de venta

**recuerda:** cuando hayas terminado de crear el token, pulsa el botón *Sell* para venderlo; aunque hay tres modalidades, en realidad la tercera solo sirve para vender más de un NFT a la vez

la primera modalidad (*Set Price*) es venta directa, en la que solo debes fijar el precio final

la subasta (*Highest Bid*) permite colocar un precio mínimo de venta junto con el tiempo de subasta

el paquete (*Bundle*) es una venta agrupada, en el que vendes dos o más NFT de forma conjunta

Select your sell method

**Set Price**  
Sell at a fixed or declining price

**Highest Bid**  
Auction to the highest bidder

**Bundle >**  
Group this item with others to sell

**Price**  
Will be on sale until you transfer this item or cancel it.

Amount

**Include ending price**  
Adding an ending price will allow this listing to expire, or for the price to be reduced until a buyer is found.

**Schedule for a future time**  
You can schedule this listing to only be buyable at a future date.

**Privacy**  
You can keep your listing public, or you can specify one address that's allowed to buy it.

**Instructions**

**Summary**

**Listing**

Post your listing >

**Bounties** EDIT

OpenSea rewards 1% to registered affiliates who refer your buyer.

**Fees**

Listing is free! At the time of the sale, the following fees will be deducted. [Learn more.](#)

To OpenSea	2.5%
<b>Total</b>	<b>2.5%</b>

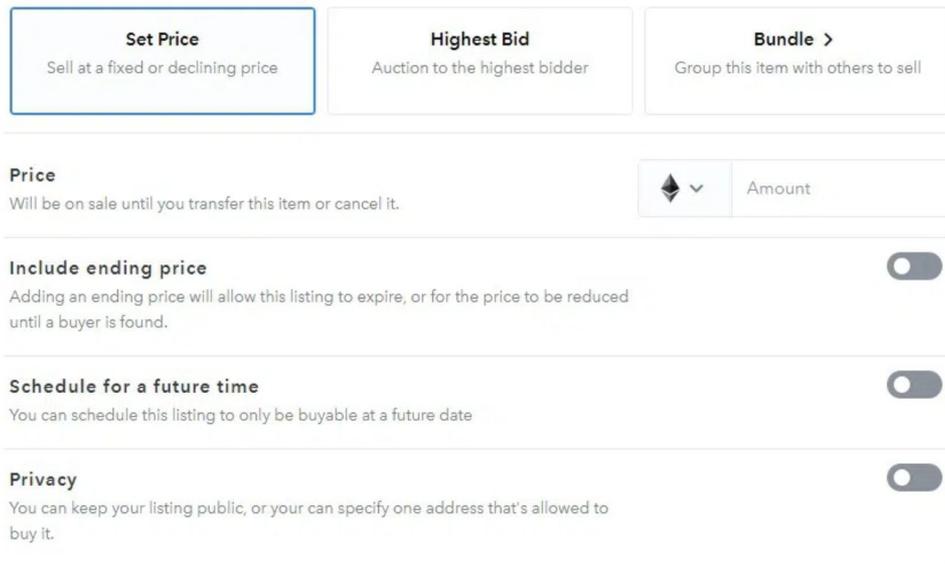
## 4 modelo de venta directa (1)

**recuerda:** es un modelo bastante utilizado; no pongas precios muy elevados (recuerda el cambio ETH/€) o te arriesgas a que nadie compre el *token*

**Price;** precio de venta; en ETH, DAI una criptomoneda propia de OpenSea) o USDC

**Schedule for a future time;** puedes establecer la fecha y hora futura en que quieres que el *token* se liste; esto es muy útil para lanzamientos programados

**Privacy;** permite mantener la venta del *token* en secreto; solo quienes posean el enlace de la venta podrán ofertar; el *token* no estará listado en el *marketplace* público



The screenshot shows the 'Set Price' option selected, with a subtext 'Sell at a fixed or declining price'. The other options are 'Highest Bid' (Auction to the highest bidder) and 'Bundle >' (Group this item with others to sell).

**Price**  
Will be on sale until you transfer this item or cancel it.

 Amount

**Include ending price**   
Adding an ending price will allow this listing to expire, or for the price to be reduced until a buyer is found.

**Schedule for a future time**   
You can schedule this listing to only be buyable at a future date

**Privacy**   
You can keep your listing public, or you can specify one address that's allowed to buy it.

## 4 modelo de venta directa (2)

**recuerda:** esta variante de la modalidad de venta directa funciona como una especie de “rebaja automática”, de forma similar a la de los productos perecederos en el mercado al final del día

**Include ending price;** sirve para reducir el precio según el paso del tiempo; se asigna una fecha de expiración y el precio final (límite de reducción); el precio se irá reduciendo cada 24 horas, de forma uniforme, hasta llegar al precio final el día establecido; si se asigna este valor, una vez se cumpla la fecha de expiración, el NFT será retirado del *marketplace*, y tendrá que ser puesto nuevamente a la venta

<b>Set Price</b> Sell at a fixed or declining price	<b>Highest Bid</b> Auction to the highest bidder	<b>Bundle &gt;</b> Group this item with others to sell
--	---	---

---

**Price** Amount

Will be on sale until you transfer this item or cancel it.

---

**Include ending price**

Adding an ending price will allow this listing to expire, or for the price to be reduced until a buyer is found.

---

**Schedule for a future time**

You can schedule this listing to only be buyable at a future date

---

**Privacy**

You can keep your listing public, or your can specify one address that's allowed to buy it.

## 4 modelo de subasta

**recuerda:** está en auge, de un tiempo a esta parte; es especialmente útil para la venta de series coleccionables

**Minimum Bid;** precio mínimo para ofertar; en ETH, DAI o USDC

**Reserve price;** quien oferte por encima de él, comprará el NFT automáticamente; algo así como un precio máximo, aunque, pueden existir ofertas superiores

**Expiration Date;** duración de la subasta; si se cumple la fecha sin venta hay que volverlo a listar

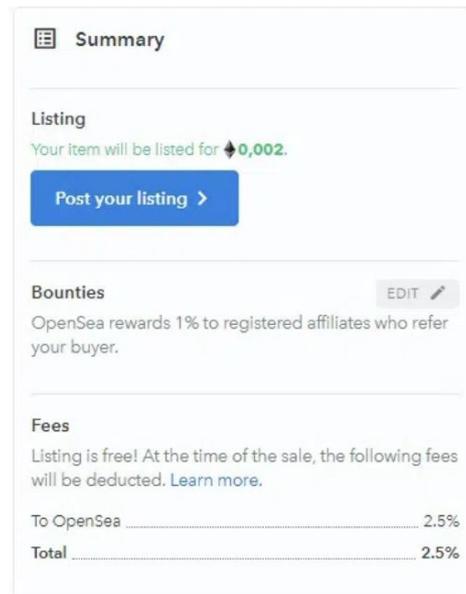
<b>Set Price</b> Sell at a fixed or declining price	<b>Highest Bid</b> Auction to the highest bidder	<b>Bundle &gt;</b> Group this item with others to sell
<b>Minimum Bid</b> Set your starting bid price. <a href="#">Learn More</a>	 2	
<b>Reserve price</b> Create a hidden limit by setting a reserve price. <a href="#">Learn More</a>	 1	
<b>Expiration Date</b> Your auction will automatically end at this time and the highest bidder will win. No need to cancel it!	in 5 days 	
	at  09 : 08 p. m.	

## 5 venta del NFT

**recuerda:** las comisiones de red (*gas*) varían según la congestión; poniendo en diferido la venta, según la experiencia personal de cada uno, pueden obtenerse mejores tasas

las **Bounties** (recompensas), de las que se ha hablado (*royalties*) se asignan a quien pueda conseguir que un NFT se venda; varían entre 0,1% y 2,5% y se descuentan del total de la venta; pueden desactivarse colocando una comisión de 0%

para finalizar, pulsar **Post your listing**; se abrirá una ventana de tu cartera para confirmar la transacción (que es gratuita, salvo el *gas*)



The screenshot shows the 'Summary' section of an OpenSea listing. It includes a 'Listing' section with a price of 0,002 ETH and a 'Post your listing' button. Below that is the 'Bounties' section, which is currently disabled (0%). The 'Fees' section shows a 2.5% fee for OpenSea.

Category	Value
Listing Price	0,002 ETH
Bounties	0%
Listing Fee (OpenSea)	2.5%
<b>Total</b>	<b>2.5%</b>

# Unas reflexiones para finalizar

Avaro es el que no gasta en lo que debe, ni lo que debe, ni cuando debe.

La inteligencia consiste no sólo en el conocimiento, sino también en la destreza de aplicar los conocimientos en la práctica.

Aristóteles (384 AC-322 AC)

El pobre carece de muchas cosas, pero el avaro carece de todo.

Séneca (2 AC-65) Filósofo latino.

No gastes tu dinero antes de ganarlo.

Thomas Jefferson (1743-1826)



Y si necesitas **saber más** o no quieres tomar apuntes...

...puedes preguntar aquí...

[antonio.cruces@uma.es](mailto:antonio.cruces@uma.es)

...o descargar esta presentación en...

<https://iasd.iarthislab.eu>

en el menú *Documentos*



UNIVERSIDAD  
DE MÁLAGA

| [uma.es](http://uma.es)



Trans\_UMA