



NFT per SPIAGGIATI

DEODATO SALAFIA

STATEMENT

Nei primi mesi del 2021 il mondo dell'arte è stato sollecitato ad occuparsi di una tecnologia innovativa e già in sperimentazione da diversi anni, la blockchain. Il successo di tale tecnologia nel contesto delle criptovalute e la creazione di nuovi protocolli nella blockchain Ethereum per identificare anche stringhe uniche o in edizione limitata, nonché la possibilità di associarle ad un file digitale, ha indotto gli investitori e speculatori di criptovalute a valutare questo come il nuovo, e principale, contesto per acquistare arte. Nel mentre della stesura di questo documento il mondo si sta interrogando come arte, tecnologia e mondo finanziario dovrebbero sfruttare al meglio le nuove opportunità date dalla blockchain.

Questo breve testo è veramente un testo da spiaggia: semplice, irriverente, diretto, spero anche divertente. Affronta il tema tecnologico principalmente, ma visto dal punto di vista di chi, oltre che ad essere un informatico esperto di algoritmi, è anche un gallerista d'arte.

BIO

Autore del libro "Le tue prime cinque opere d'arte contemporanea", Deodato Salafia è laureato in Informatica ed in Teologia, nel 2021 ha fondato la start up per la creazione di un social su ambienti virtuali chiamato lieu.city, nel 2019 ha fondato la start up deodato.tech per la ricerca e sviluppo di metodologie digitali nel contesto dell'arte contemporanea. Nel 2014 ha lanciato deodato.com come negozio di eCommerce a supporto delle sue gallerie fisiche e nel 2010 ha aperto la sua prima galleria d'arte contemporanea fisica. Dal 1996 al 2001 è stato uno dei protagonisti di un delirio collettivo chiamato "new economy", mentre dal 2001 al 2010 ha svolto consulenza su processi e marketing per imprese private e pubbliche. Deodato ama definirsi nerd e monaco contemporaneo.

Opera in copertina di Mr. Savethewall
Immaginazione: Augusto Ozzella

Milano, 29 marzo 2021

NFT (tetemi)

*Un NFT può essere usato per “ricordare un fatto” non per descriverlo!
Possiamo ricordare che avevi un’opera...ma non certo che opera fosse!*

Cosa è un NFT?

Un NFT è un token (appunto Non FungibleToken), diciamo una sequenza di BIT, che all’interno di un circuito predefinito è unica. Detta così...signori, qualunque record di qualunque database che sia definito univoco è un NFT, per intenderci lo è il vostro numero di passaporto, lo è la vostra partita iva, lo è il numero del biglietto del cinema dell’ultimo film che avete visto. Ha questa sequenza di bit un valore? Beh, se qualcuno glielo dà lo ha, altrimenti no. La parte “NF” significa “non scambiabile senza perdere valore”, quindi per esempio il vostro numero di passaporto è NF in quanto se scambiate il vostro passaporto con quello del vostro amico... scordatevi di andare alle Maldive appena finisce il COVID. Mentre non è NF il codice di un biglietto di un dollaro, in quanto anche se scambiate il vostro dollaro con quello del vostro amico...beh non avete perso nulla. Anche il biglietto del cinema è NF in quanto se permettete, sedersi di lato in prima fila è molto peggio che sedersi al centro della sala, quindi i biglietti non sono interscambiabili senza perdita di un qualche valore.

Ma cosa intendono i giornali quando parlano di NFT?

Bene, in modo più restrittivo rispetto a quello che ho scritto sopra, intendono questo: un NFT è una sequenza di BIT univoca all’interno del circuito della blockchain Ethereum (che è una delle tante blockchain, che puoi immaginare come un grosso foglio excel distribuito e copiato su tanti computer in modo che tutti possano avere la stessa copia).

Ma quindi posso avere NFT su altre blockchain?

Sì, certo, e sarebbero comunque NFT veri e propri, anzi non servirebbe tecnicamente neppure una blockchain per definire un NFT, come detto.

Cosa c’entra un NFT, banale sequenza di BIT, con le opere d’arte?

Non sono molto correlate a dire il vero, possiamo correlarle in due modi, se proprio dobbiamo farlo.

1. L’NFT, rappresenta in modo univoco un’opera (fisica o digitale); in pratica la sequenza di BIT descrive l’opera (ma l’opera è sempre fisicamente fuori dall’NFT, l’NFT la definisce secondo una convenzione e basta)
2. L’NFT è l’opera digitale, sì, quella stupida e apparentemente insignificante sequenza di zeri e uno...diventa l’opera.

Il primo caso è il più usuale. Un server, come lo sono i ben conosciuti Rarible, Super Rare, Cryptokitties o Opensea, contiene delle immagini o delle informazioni digitali associate ad un NFT, come lo è il numero del tuo passaporto alla tua faccia. Il secondo caso è inusuale, ma di fatto è in questo caso che risiede la vera innovazione; se infatti parrebbe da super stupidi spendere soldi per una insignificante sequenza di bit la verità è che, quella sequenza di BIT, è l’unica cosa concreta che ha la speranza di sopravvivere nel tempo. Ne parliamo sotto.

Non ho capito come è il discorso dell’NFT che è o rappresenta l’opera, mi fai un esempio?

Nel 2009 seguii un seminario di tre giorni presso la facoltà Valdese di Teologia a Roma sulla questione se la particola consacrata (l’ostia) è, o solo rappresenta, il corpo di Cristo. Per i cristiani cattolico romani, a seguito del processo di transustanziazione, la particola è il corpo di Cristo, mentre per i cristiani protestanti la particola rappresenta il corpo di Cristo. Ecco per gli NFT è la stessa cosa, il “cristo” sarebbe l’opera, l’NFT l’ostia. Certo se la particola è Cristo...Cristo si riduce fisicamente a un poco di farina e di acqua, lo stesso è per l’NFT, se è un’opera d’arte...essa si riduce a pochi, anzi pochissimi, semplici BIT.

Non vado in Chiesa, mi spieghi meglio tecnicamente?

Allora, abbiamo detto che l’NFT è una sequenza di BIT. Tu sai bene che anche una fotografia sul tuo computer o un audio che arriva da Spotify o un film che vedi da Netflix, che ti fa piangere magari, sono sequenze di BIT. Ci sono tre casi e te li dico bene ed in modo chiaro.

Caso 1. L’NFT contiene solo un numero, che una certa azienda o galleria d’arte associano a una immagine digitale (o video o file musicale o altro). Se si brucia il database che crea questa associazione... hai perso l’opera.

Caso 2. L’NFT contiene oltre al numero anche una sequenza più lunga di BIT, che sarebbe l’opera vera e propria. Non serve alcun database esterno. Questo appare il caso migliore, sebbene queste sequenze non possano essere troppo lunghe, purtroppo. Vedi una delle domande seguenti dove ti spiego il perché.

Caso 3. L’NFT contiene sempre il nostro bel numero identificatore, ma contiene anche altre informazioni, per esempio “colore barba= giallo”, “colore capelli= rosso). Poi esiste un programma sul web, di una azienda o galleria, che sa leggere quelle informazioni e restituire come risultato un file più complesso, di solito una immagine o video, che usa quelle informazioni, per esempio un CryptoPunk con la barba gialla e i capelli rossi.

C’è il caso 2 bis. È il caso in cui l’NFT contiene un codice descrittivo che opportunamente interpretato genera l’opera. Siamo quasi nel caso 3 ma è un caso 2 in quanto nel caso 3 se brucia il database che genera l’opera allora si perde anche per sempre la fruizione dell’opera. Mentre in questo caso 2 bis il codice è un programma o eseguito nella blockchain stessa o comunque possiamo immaginare sia un programma scritto in un linguaggio di programmazione la cui semantica (interpretazione delle istruzioni) sia di conoscenza comune, come ad esempio il linguaggio C. Se non hai capito non importa...il caso 2 bis è una roba davvero da super nerd, invero è il caso che a me piace più di tutti!

Aspetta, aspetta! Cosa significa che un NFT non può contenere un file troppo lungo?

Un NFT può contenere teoricamente un file lungo, ma accade che più lungo è il file più costa inserirlo nella blockchain, c’è un costo chiamato GAS. Il costo è di circa 100 dollari per un piccolissimo file, se si dovesse conservare un file ad alta risoluzione, diciamo un’ immagine riproducibile anche su stampa, si salirebbe a molte migliaia, o decine di migliaia, di dollari. Teniamo presente che nella blockchain Ethereum, quella che tutti conoscono per gli NFT, una sequenza base è 256 bit, ovvero 32 byte...ecco 32 byte sono una frase di 32 lettere (non parole, lettere), diciamo il vostro nome e cognome o poco più. Un contratto si registra (mina) con 20.000 GAS e ogni GAS costa circa 150 Gwei (un Gwei è un milionesimo di ETH, infatti un ETH sono un miliardo di miliardi di wei, ovvero 10 alla 18), in pratica per registrare 32

lettere al momento che scrivo servono 0,0032 ETH, che sono 5,75 dollari veri. Per registrare un mega byte servono 104,8576 ETH ovvero quasi 200.000 dollari veri, per registrare una immagine HD, diciamo di 100mb serve 100 volte tanto, ovvero quasi 20 milioni di usd. Insomma il concetto è che un NFT può essere usato per “ricordare un fatto” non per descriverlo! Possiamo ricordare che avevi un’opera...ma non certo che opera fosse!

Perché gli NFT di cui parlano i giornali valgono di più del mio numero del passaporto, visto che infine sono la stessa cosa?

Per due motivi.

Il primo è che il numero del passaporto è associato al tuo viso perchè lo dice “solo” il database della Polizia del tuo paese, mentre che un NFT sia di proprietà di una persona o un’altra lo dice una comunità di database sparsi per il mondo (blockchain).

Il secondo è che nella “mente” di qualcuno, anzi sarebbe meglio dire nel “database” di qualcuno, quel numero NFT è associato ad una immagine, ovvero un’opera.

Ma seguimi bene. Che l’NFT sia di proprietà di una persona è un’informazione conservata in tanti database diffusi per il mondo e coerenti tra loro (appunto la blockchain) ma che quel numero NFT sia associato ad un’opera specifica (un Punk senza barba coi capelli rossi) questo è certificato da solo un database, né più né meno come il passaporto che è certificato dalla Polizia.

Ma quindi se si brucia il database che associa il mio NFT alla mia opera...a me cosa resta?

Nulla. Proprio nulla, se non un bel numero unico..che un tempo identificava una qualche opera.

Allora posso dire che il mio NFT “è” la mia opera?

Sì, in fin dei conti puoi dire così. E quindi...hai comprato un numero!

Ma se il database che associa il mio numero all’opera che ho visto quando l’ho comprato non si brucia...sono salvo!

Sì, se nessun database brucia, nessuno perde nulla, come nel mondo dei passaporti e dei biglietti del cinema.

Ma allora che cosa è interessante degli NFT?

La tracciabilità, ovvero, finalmente, nessuno può essere più anonimo nei passaggi. Tutte le volte che qualcuno passa l’NFT ad un altro, tutti lo sanno! E volendo una parte dei ricavi del passaggio possono essere ripartiti tra alcuni dei soggetti precedenti, come per esempio a chi lo ha creato (che poi è quello che fa la SIAE ad esempio con i diritti musicali).

Lo so che me lo hai spiegato, ma puoi ripetere? Perché e come potrei perdere la mia opera d'arte NFT?

Allora, un NFT è un token con un bel numero unico, questo token ha dei metadata, dei BIT per intenderci. Questi BIT possono contenere totalmente l'intera opera (on-chain metadata), caso rarissimo perché un'opera che sta in 32 byte o è brutta o è un'opera "concettuale", oppure questi metadata possono contenere, più probabilmente, un URI (Uniform Resource Identifier), immaginalo pure come un normale URL (Uniform Resource Locator) che metti nel tuo web browser. Quindi il tuo bel token si limita a dire dove c'è la tua opera (off-chain metadata). Se il sito o il database che risponde a quell'URI si spegne (perché fallisce l'azienda o per qualunque altro motivo), ti rimane il ricordo che avevi qualcosa, ma non hai più quel qualcosa. Un poco come quando i ladri ti rubano un orologio di valore ma ti rimane il certificato di proprietà.

Cosa è un 'oracolo'? Mi è stato detto che questo risolve il problema di avere contenuti off-chain?

Un oracolo nelle blockchain è un nodo di cui tutti si fidano e che è autorizzato a dare informazioni dal mondo reale, appunto off-chain. Gli oracoli sono nati per dare a tutti gli altri nodi della blockchain informazioni variabili in continuazione, quali il valore del cambio di una valuta, che si vorrebbe fissare in un certo istante, piuttosto che la temperatura meteo in un certo luogo e data, o qualunque altra informazione che può potenzialmente cambiare: l'oracolo fissa in modo deterministico ciò che di base non lo è. L'oracolo si basa sul mondo reale, quindi diciamo che può sbagliare tanto quanto pensiamo che possa sbagliare il TG della sera quando ci dice il cambio euro/dollaro del giorno. Se ci fosse un database delle opere d'arte di cui tutti ci fidassimo...allora sarebbe facile costruire un oracolo capace di identificare un'opera off-chain in modo deterministico. Ma ci sono due problemi: il primo è che tale database non c'è; il secondo è che se tale database esistesse...sarebbe detenuto da una banca, o da uno stato, o da una importante istituzione privata, ciò quindi vanificherebbe in buona parte lo sforzo di vedere la blockchain come strumento di decentralizzazione. Insomma ancora una volta dobbiamo capire che la blockchain conserva i contratti, non l'oggetto del contratto stesso!

A parte la perdita dell'anonimato e che finalmente il riciclaggio di denaro illecito è perseguibile più facilmente dalle autorità...non ci sono altri vantaggi? Ho sentito dire che non puoi duplicare l'opera...

Non ci sono altri vantaggi. Opera? Se parliamo dell'opera associata all'NFT la puoi duplicare e come! Anzi puoi tranquillamente creare due NFT (due diversi numeri unici) associati alla stessa opera, lo puoi fare su blockchain diverse, ma anche sulla stessa blockchain. Oltre al fatto che puoi duplicare l'opera e basta, fregandotene di associarla ad alcun NFT. Se invece l'opera è l'NFT, quindi scordati di avere immagini associate (o se ci sono non è in essa che riponiamo speranze e valore), allora il vantaggio è alto, infatti il vantaggio è che non dipendi da un database di uno solo ma da una rete distribuita di database (blockchain).

Come fai a dire che posso associare la stessa opera a due NFT diversi nella stessa blockchain! Ho letto che non è possibile!

Non hai letto bene. Se io ho 10.000 immagini di Punk diversi e dico che una certa parte della sequenza dell’NFT definisce il colore della barba del punk (diciamo i bit dal numero 5 al numero 10) e un’altra parte il colore dei capelli (bit numero 11 al numero 16), certamente non posso duplicare quell’NFT. Ma nulla mi vieta di modificare il protocollo predefinito e io dico che i bit dal numero 5 al 10 definiscono i capelli e i bit dall’11 al 16 la barba. In tal caso posso generare NFT diversi (con due lanci diversi) per la stessa opera.

Infatti le piattaforme di lancio NFT, contrattualmente, ti chiedono di non fare quello che ho appena descritto. Te lo chiedono perché sanno che lo puoi fare, altrimenti che te lo chiederebbero a fare? Se la blockchain, che servirebbe per evitare le fregature del mondo normale basato su contratti, ha bisogno di un contratto per non essere violata... ragazzi, capiamo che qualcosa non quadra!

In pratica la non clonabilità degli NFT è basata sulla fiducia?

Se per NFT intendiamo l’opera d’arte associata, l’immagine del punk per intenderci, la risposta è sì, è solo sulla fiducia.

Ma se io copio una immagine e creo un altro NFT...qualcuno se ne accorge? Si può risalire al primo proprietario?

Intanto se tu copi qualcosa, fai un illecito quasi certamente. A meno che tu non sia il proprietario dei diritti dell’immagine, ovvero l’artista.

Secondo, gli NFT hanno un timestamp, tecnicamente sarebbe possibile risalire al primo NFT, ma ciò non significa nulla. Se io faccio l’NFT della Gioconda non significa che il mio NFT abbia alcun valore, diverso sarebbe se lo facesse Leonardo Da Vinci.

Che differenza c’è tra i token normali, come i BITCOIN, e i Non Fungible Token?

I Bitcoin hanno un valore nominale, il numero associato non è importante, quindi due Bitcoin possono essere scambiati senza perdita di valore, sebbene abbiano numeri diversi. Mentre, per convenzione, e solo per convenzione si intenda, due NFT contengono il valore ed il significato nel numero stesso o nella immagine che in un certo database è associata (sempre finché non brucerà il database).

Quindi tutto l’impianto NFT che punti di debolezza ha?

Ne ha molti, due i più importanti.

Primo: qualunque numero univoco è un NFT. L’opinione pubblica ritiene che però un vero NFT sia definito nella blockchain, ma c’è da dire che vi sono molti diversi tipi di blockchain.

Secondo: se ad un NFT vi è associata una immagine, tale immagine è in un normalissimo database, che prima o poi brucerà, o si spegnerà, o sarà cancellato, o comunque vi sarà il rischio che accada.

Devo comprare un'opera in NFT?

Puoi farlo o non farlo, io in questo momento storico lo farei. Ma attenzione...non è vero che se un'opera è definita da un NFT è più sicura o che “resterà per sempre”. Essa sarà soggetta a potenziali danneggiamenti e perdite, come tutte le cose che ci circondano, a partire dalla nostra stessa vita.

Le opere NFT che sono lanciate in questo momento storico potrebbero nel breve e medio periodo, e quasi certamente anche nel lungo, rivalutarsi, ma non perché sono particolarmente belle o sicure, ma solo perché sono le prime ad essere create con questo protocollo.

Per comprare un NFT devo avere criptovaluta?

No, per nulla. Diciamo che i primi NFT sono nati nella blockchain che definisce la criptovaluta ETH e quindi i primi si sono scambiati in ETH, ma io posso comprare da te un NFT in cambio di 3 banane. Tra l'altro in ETH sono scambiati gli NFT definiti in quella blockchain, come ci siamo detti ci sono molte blockchain.

Ma quindi cosa faccio, compro o non compro?

Se vuoi speculare, compra. Se vuoi essere alla moda, compra. Se vuoi comprare un'opera immaginando che entri in un mondo super sicuro, super protetto e dove le fregature non ci sono....lascia stare! Gli NFT sono sequenze di BIT. Molte persone sono certe di entrare in comunione con Cristo mangiando l'ostia in chiesa, altre non ritengono che questo possa avvenire. È la tua intelligenza a decidere, come nella metafisica. Se vogliamo, l'arte è la metafisica più terrena che ci sia!

Posso avere un NFT che non sia solo una banale sequenza di BIT ma invece che contenga una “vera” opera d'arte?

Sì è possibile ma per opere di bassa risoluzione. Per opere ad alta risoluzione si può associare il file all'IPFS (Inter Planetary File System), in pratica non dipendi da un solo database ma da molti database. Sempre meglio di un pugno in un'occhio...ma nulla di super sicuro per ora.

Deodato, come pensi che sia intelligente usare gli NFT?

Gli NFT sono un ottimo certificato di proprietà, da associare ad un'opera fisica o digitale. Se l'opera è digitale, a bassa risoluzione, non fruibile fisicamente e registrata su un database proprietario...allora presumibilmente siamo di fronte ad una speculazione, come quando uno compra valuta nel Forex, senza in effetti sapere come funziona il mercato monetario.

Che differenza c'è quindi tra un NFT (inteso come Token che identifica un'opera digitale “bella”, e non un numeraccio insomma) e un'opera digitale non-NFT, insomma come era intesa fino a prima degli NFT?

Nessuna! Ripeto, nessuna! Infatti l'NFT serve per certificare opere, quindi non per certificare l'autenticità ma solo chi l'ha venduta a chi. Certo se il primo a venderla è lo stesso autore

allora è evidente che certifica anche l'originalità; sempre che l'autore ad un certo punto non disconosca il suo "ID", ma questa è un'altra storia. Quindi NFT non significa opera vera necessariamente.

Mi spieghi l'operazione del Banksy bruciato?

Semplice, i ragazzi hanno bruciato un Banksy vero per generare un NFT di un Banksy falso. Infatti non basta prendere una qualunque foto di un'opera di un artista terzo e creare un NFT pensando di aver creato un NFT vero. Insomma è come prendere il marito di un'altra, farlo fuori, e dire che quello era tuo marito per averne l'eredità. Non funziona così ecco. [Disclaimer, sennò Annarita mi cazzia: puoi scambiare uomo e donna se vuoi]

Non ho capito molto, ma che cosa sono questi NFT?

Sono sequenze di bit che con qualche trucco arcano lasciano traccia su internet quando qualcuno se li scambia! Inoltre questa sequenza di bit può essere opzionalmente associata ad un altro file, sia esso immagine, file musicale, video, contratto o altro.

Ricordami perché tutti sono impazziti per gli NFT quindi?

Sono impazziti per due motivi: il primo è che il mondo si è rotto le scatole di chi fa le cose "a umma a umma", il mondo si è rotto le scatole dei paradisi fiscali, dei farlocconi, di quelli che hanno qualcosa da nascondere...NFT è una tecnologia che guarda il futuro, alla trasparenza, alla tracciabilità. Dall'altra la gente è impazzita perché era già pazza, infatti non vi è alcun ragionevole motivo di comprare una sequenza di bit per migliaia di euro! Ma a dire il vero forse non vi è motivo di pagare una giacca 25.000 euro o una borsetta da donna 40.000...o forse sì vi è motivo...in fondo sono anche io confuso a riguardo!

Un'opera d'arte in NFT è davvero Arte?

Intanto secondo la mia definizione è arte qualunque cosa che metta d'accordo due persone sul fatto che sia arte e che almeno una delle due abbia speso risorse personali per possederla senza alcuno scopo utilitaristico se non per emozionarsi, senza aspettative di speculazione. Infatti è arte il vasino di Duchamp, la merda d'artista di Piero Manzoni e una tela tagliata di Lucio Fontana; sebbene non tutti i cessi, le merde o le tele tagliate siano arte. È arte ciò che si vuole che sia tale. A mio personale avviso i primi NFT erano arte. Tutti gli NFT prodotti e venduti, ma soprattutto quelli acquistati per essere rivenduti con scopo di lucro...non sono arte per nulla, quindi la maggior parte, direi il 99.999% non sono Arte. Ma qualcuno lo è!

Quindi tra 20 anni che relazione ci sarà tra NFT e l'Arte?

Una qualche forma di NFT sarà ancora utilizzata per certificare le opere d'arte, gli NFT saranno utilizzati solo per questo, per certificare, come i francobolli. Le opere saranno opere, gli NFT saranno NFT. Come detto possono collassare ed un NFT potrà essere anche un'opera, questa sarà cosa buona e giusta, senza che però ci sia un motivo perché valga di più.

Sono confuso, mi è stato detto che un NFT è unico, raro ed indivisibile, mi sembrano bellissime caratteristiche!

Unicità, rarità e indivisibilità sono alla base dell'amore, sono bellissime caratteristiche di sicuro.

Tieni presente che per un NFT l'unicità è basata su una sorta di numero seriale, tutto il resto NON è unico, a meno che non capiti che lo sia, ma certo non dipende né dagli NFT né dalle blockchain. L'opera "indicata" dal numero unico dell'NFT sarà unica fintanto che il sistema di fiducia è in piedi, come nel mondo fisico. Quando compri un quadro olio su tela e chiedi "è unico?" ed il gallerista ti risponde "certamente!", invero tu ti stai fidando, non è per nulla detto che lo sia o che l'artista sia onesto in questo.

Riguardo la rarità ancora una volta ci si basa sull'onestà di chi crea gli NFT. Certamente possiamo sapere se i certificati NFT associati ad una certa immagine sono pochi o tanti, sappiamo esattamente quanti sono. Tuttavia nulla vieta all'autore di aggiungere un pixel e riproporre all'infinito lo stesso soggetto. Insomma non cambia nulla in confronto al mondo reale, se c'è dietro gente seria...tutto ok, altrimenti...tutto a rotoli.

Riguardo la indivisibilità ci si riferisce al fatto che mentre un decimo di Bitcoin ha sempre un qualche valore, qui un decimo di un NFT non ha valore, anzi non può neppure esistere. Ancora una volta è il caso delle opere fisiche. Personalmente ritengo che in futuro i protocolli NFT permetteranno una "cartolarizzazione" della proprietà, sebbene qui si apra una tematica sul concetto di utilizzo dell'asset sottostante. Ad ogni modo sì, attualmente un NFT è indivisibile.

Gli NFT causano un problema ambientale per via della energia elettrica che serve per generarli?

Sì, certamente. Come lo causano le fiere d'arte fisiche, o andare alle Maldive o semplicemente...vivere. Qualcuno sta cercando di capire se questo consumo è "accettabile" o no.

Se non compro gli NFT proprio adesso...sono sfigato?

No, secondo me sei uno che ha qualcosa di meglio da fare che seguire mode in modo superficiale.

Se compro NFT sono sfigato?

No, se lo fai dopo aver letto questo documento...significa che sai cosa stai facendo!

Deodato, tu entrerai nel mondo NFT, come operatore? E se sì, perché lo fai?

Sì, sia come ideatore della piattaforma Lieu.city, sia come gallerista. Ci entro per due motivi: il primo è che amo un bellissimo passo del Vangelo: Matteo 18, 19 "In verità io vi dico ancora: se due di voi sulla terra si metteranno d'accordo per chiedere qualunque cosa, il Padre mio che è nei cieli gliela concederà", se Dio si butta nella mischia...non ho motivi per non farlo io.

Secondo, vedo molta confusione, ho la fortuna di comprendere sia il mondo scientifico delle blockchain, sia il mondo del mercato dell'arte; penso di poter dare un contributo!

Quindi non sei contro gli NFT.

Certo che no. È come essere sposati, io non sono sposato perché avendo analizzato chi mi circonda so cosa significa, ma non ritengo assolutamente che essere sposati sia un errore! Sapere è potere!

NFT per SPIAGGIATI

Un montagna di energia elettrica si potrebbe risparmiare (i Bitcoin ne consumano tanta quanta ne consuma l'Argentina in un anno) solo se si accettasse di avere un database centralizzato! Ma Satoshi Nakamoto ha la testa dura ed ha voluto regalare un sogno: basta banche centralizzate, basta poteri centralizzati. Verrebbe da dire: “vabbé Sato...abbiamo capito, mo basta, spegni la baracca che ci stiamo squagliando!”

Cosa è una blockchain?

La chiave della blockchain è un concetto vecchio come il cucù ed è la funzione di hash. Ascolta bene, perché la funzione di hash la usi certamente alcune migliaia di volte al giorno, senza neppure saperlo, anzi se sparisse...sarebbe fantastico perché non pagheresti più le tasse! Una funzione di hash è una funzione deterministica (che banalmente significa che con lo stesso input darà sempre lo stesso output) e che fa in modo che partendo da una grande informazione si determini una sequenza di caratteri (un numero o una sequenza alfanumerica, o anche solo una sequenza di bit) che ha una lunghezza decisa a priori. Per esempio la funzione SHA256 trasforma qualunque cosa in una sequenza di 256 byte, non importa se gli date in pasto la Divina Commedia o la foto di vostro figlio, sempre una sequenza di 256 caratteri vi restituisce. In pratica è una specie di firma, diciamo un qualcosa che certifica se un'altra cosa era quella che avevamo deciso che fosse. Esempio: ipotizziamo che ci sia il pericolo che Whatsapp possa modificare i file inviati da un utente, prima che arrivino al destinatario. Se io ti invio la Divina Commedia, di certo io e te non possiamo metterci a leggere cento canti al telefono per essere sicuri che nessuno l'abbia manomessa, fosse anche solo per una lettera. Allora ecco che l'hash ci salva. Io faccio SHA256 del file prima di inviartelo e tu, quando ti arriva, fai SHA256 del file, poi ci sentiamo al telefono e ci diciamo se lo SHA256 corrisponde. Geniale!

Lo so cosa stai pensando: ma se un file lungo si “comprime” in un file piccolo, certamente ci saranno delle collisioni, ovvero magari due file grandi potrebbero avere lo stesso SHA256. Vero, ma ci sono due fatti che ti mettono al riparo: il primo è che tale probabilità è infinitesimale su file grandi; la seconda è che la probabilità che il dipendente di Whatsapp becchi un'altra versione della Divina Commedia che abbia lo stesso SHA256 è impossibile, faremmo in tempo ad estinguerci prima che ci riesca, anche utilizzando i più potenti computer (chissà forse i computer quantici potrebbero farcela, ma non sono ancora stati completamente inventati). Il tuo codice fiscale è una funzione di hash, banalissima, ma almeno è abbastanza facile da ricordare, pensa se tu dovessi andare in giro con un tesserino di plastica lungo 256 caratteri! Giusto per tua curiosità, ma ci sarai arrivato da solo, la funzione di hash non

è reversibile, non è che dallo SHA256 della Divina Commedia posso risalire alla Divina Commedia: no way.

La blockchain è basata su due caratteristiche:

1. ogni record (qualsiasi cosa che desidero conservare) è legato, tramite un hash, al record precedente;
2. ogni record che scrivo viene in modo sicuro distribuito a tanti nodi, ognuno dei quali contiene una copia di tutti i record. Un nodo è un computer che qualcuno mantiene acceso.

Due informazioni chiave:

1. per violare una blockchain, ammesso di saperlo fare e di riuscire a farlo, si deve manipolare almeno il 50%+1 dei nodi della blockchain;
2. mantenere un nodo costa soldi, visto che devo comprare un potente computer e consumare energia elettrica, quindi il sistema è stato inventato in modo che chi mantiene un nodo sia remunerato in qualche modo (mining) attraverso dei soldi (gas).

La prima blockchain è stata creata da un anonimo chiamato Satoshi Nakamoto, in occasione dell'invenzione dei Bitcoin. La blockchain alla fine è un complesso database, la complessità sta nel fatto che l'informazione è certificata da molte persone e non da una sola istituzione.

Per eseguire il processi di validazione, sono necessari complessi calcoli matematici, per questo il processo è chiamato “proof of work” e per questo viene consumata parecchia energia elettrica. Il Cambridge Bitcoin Electricity Consumption Index (cbeci.org), dell'Università di Cambridge, fornisce una stima in tempo reale del consumo totale di elettricità della rete Bitcoin. Al momento in cui scrivo la sola blockchain dei Bitcoin (la principale, ma a cui vanno aggiunte le altre, come quella Ethereum degli NFT) consuma annualmente 133.4 Thw (therawatt per ora). Considerando che tutta la Svezia ne consuma 131.80, l'Olanda 110 e tutta l'Argentina 125.04, il “paese” bitcoin in questo momento è il 27esimo nella classifica mondiale delle Nazioni.

Chi lavora con le blockchain si sente un poco in colpa e sono stati inventati nuovi protocolli, basati sul “proof of stack”, invece che sul “proof of work”. Te la spiego semplice: chi ha più soldi comanda (articolo quinto: chi ha più soldi ha vinto), però se cerca di fare il furbo, tutti i soldi spariscono per sempre!

Notate come tutta questa montagna di energia elettrica si potrebbe risparmiare (immaginate che cifra) solo se si accettasse di avere un database centralizzato! Ma Satoshi Nakamoto ha la testa dura ed ha voluto regalare un sogno: basta banche centralizzate, basta poteri centralizzati. Verrebbe da dire: “vabbé Sato...abbiamo capito, mo basta, spegni la baracca!”

Come si fa una blockchain

Per fare una blockchain ti serve:

- una rete peer-2-peer di nodi che siano interconnessi con un protocollo condiviso;
- transazioni (messaggi) che vengono propagate e che sono in effetti definizioni di cambiamenti di stato
- un insieme di regole che definisca cosa è o non è una transazione e come si considera validata;

- una macchina a stati finiti (formalismo matematico per descrivere un processo) che processa le transazioni utilizzando le regole di cui sopra;
- una sequenza di blocchi informativi legati da una sequenza hash che contiene le informazioni relative alle transazioni effettivamente validate;
- un algoritmo che governi le regole in modo che i partecipanti siano costretti a cooperare per validare le transazioni;
- un sistema di “gaming” che consenta ai partecipanti di guadagnare dal fatto di partecipare al sistema;
- delle implementazioni software (stavolta reali e non matematiche) che siano i clienti o i nodi in modo da far funzionare quanto sopra.

È tutto un modello matematico...che poi viene implementato con dei software piuttosto semplici.

ETHEREUM in confronto con BITCOIN

Ethereum è un'altra blockchain, quella che ha permesso al mondo di scoprire gli NFT. Ha molte cose in comune con la blockchain dei Bitcoin, compreso il fatto che ha una sua moneta, ETH, ovvero un ether, che si parcellizza in wei: come un dollaro è fatto da cento cents, un ETH è fatto da un miliardo di miliardi di wei (se fossero di metallo ti sfonderebbero senz'altro le tasche). Le due blockchain hanno molto in comune: possiamo affermare che tutto quello che è stato detto finora appartiene ad entrambe le blockchain. Tuttavia Ethereum è un passo avanti, del resto arriva circa 10 anni dopo, per tre peculiarità:

1. la moneta ETH è utilizzata per far funzionare la blockchain stessa in modo nativo
2. è molto più predisposta a gestire contratti, di qualunque tipo e...udite, udite, udite
3. è un computer vero e proprio!

Infatti Ethereum è una Macchina di Turing completa, ne parliamo sotto, ma quello che è importante capire è che un token in Ethereum può contenere un programma scritto in un linguaggio di programmazione, che può fare qualunque cosa possa fare una Macchina di Turing, che in pratica fa quello che può fare qualunque computer che sarà mai inventato dall'uomo (ad eccezione probabilmente dei computer quantici, nei quali c'è il tocco di Dio, a quanto pare). Invero lo scopo principale degli ETH non è quello di far speculare o di essere utilizzato come moneta per pagare beni e servizi (come lo era per i Bitcoin) piuttosto gli ETH sono stati pensati come la moneta per far funzionare il più distribuito computer del mondo: l'Ethereum. Il computer Ethereum (attenzione parliamo sempre di formalismi matematici, come del resto per la Macchina di Turing) può essere programmato per fare qualunque cosa!

Il mondo era in fermento in quanto si sarebbe voluto dai Bitcoin molto di più di quello per il quale erano stati creati. Nel 2013 un ragazzo di nome Vitalik Buterin cominciò a fantasticare su un'estensione dei Bitcoin con automi a stati finiti (tra poco ti dico di cosa si tratta), ma il team di Bitcoin non aveva tempo di ascoltarlo. Nel dicembre 2013 Vitalik aveva già creato un più potente modello di blockchain che includeva una intera Macchina di Turing: wow! Nasceva Ethereum.

Cosa è una macchina di Turing?

Intanto cosa non è: non è quel computerone che si vede nel film di Alan Turing con il quale gli inglesi decryptarono i messaggi dei tedeschi, sebbene sì, l'Alan Turing è lo stesso uomo.

Un “automa a stati finiti” devi immaginarlo come uno schema di cerchietti collegati da archi, con dei pallini dentro: i cerchietti sono lo stato, gli archi le azioni, i pallini delineano quale stato è attivo. Ad esempio, un cerchio definisce “uomo seduto”, un altro “uomo in piedi” e due archi che li collegano sono “alzati” e “siediti”, il pallino sta in uno dei due cerchi e identifica se l'uomo è seduto o in piedi. La macchina di Turing è la stessa cosa, solo che è dotata di un formalismo che rappresenta un nastro infinito diviso per caselle, su cui è possibile annotare degli zeri e degli uno, essa ha la possibilità di leggere le caselle del nastro, di cambiare la casella (da 0 a 1 o da 1 a 0) e di far scorrere il nastro avanti o indietro.

Una curiosità, nel 1928 Hilbert pone una domanda: “Esiste sempre, almeno in linea di principio, un metodo meccanico (cioè una maniera rigorosa) attraverso cui, dato un qualsiasi enunciato matematico, si possa stabilire se esso sia vero o falso?” Nell'articolo “On computable numbers with an application to the Entscheidungsproblem”, pubblicato nel 1936, Turing gli risponde, formalizzando così il suo automa; emerge che alcuni enunciati matematici non possono essere definiti veri o falsi da alcun computer o metodo di calcolo. Invero la cosa che ci interessa è la Tesi di Church-Turing (1936): Ogni algoritmo che può essere eseguito da un umano o da un computer può essere eseguito da una macchina di Turing.

Per cui la rete Ethereum può fare qualunque cosa!

Pensate che il primo blocco in Ethereum nasce il 30 luglio del 2015, oltre due anni dopo la prima formalizzazione matematica.

Nota chiave.

Puoi pensare alla blockchain come un enorme automa a stati finiti. La differenza è che mentre la blockchain Bitcoin può registrare lo stato di chi possiede i Bitcoin, Ethereum può registrare qualunque generico tipo di stato.

La troppa potenza che potrebbe bloccare la rete e la benedetta invenzione del gas!

Una delle cose che Alan Turing ha dimostrato con la sua macchina è che nessun calcolatore che sarà mai programmato può capire se un certo programma da eseguire andrà in blocco oppure no. In pratica un computer non può predeterminare se un certo programma che sta per eseguire lo farà bloccare o no. Una delle sfide degli hacker sarà programmare un programma che mandi in blocco la blockchain (attacco DoS, Denial of Service). L'ho un poco romanzata...ma non troppo!

Cosa hanno pensato i nostri matematici? Semplice: hanno inventato il gas. Ogni istruzione che un nodo deve eseguire per completare il programma scritto in un token, richiede un gas. Se vogliamo, il gas è il costo per eseguire un'istruzione. Quando si chiede ad un nodo di verificare un contratto, il richiedente, deve indicare il numero massimo di gas che è disposto a pagare, appena il nodo consuma tutti i gas...molla il colpo e non valida.

Il gas è il trucco usato per non mandare in blocco la rete. Quando mandi un contratto per la validazione devi mandare un poco di gas. Il gas si compra in rete con gli Ether ed il prezzo

del gas oscilla, più gente vuole computare e validare, più costa il gas!

Cosa è un Wallet

Un wallet è in fin dei conti una chiave che abilita altre chiavi al fine di vedere cosa vi è associato nella rete ed abilita a fare transazioni, in particolare attivare contratti, tipo acquisto o vendita. Nella rete Ethereum un wallet non contiene un bel niente: è la rete a ricordarsi cosa contiene, come vedremo ci si riferisce ai Token. Un wallet anche se è perduto può essere ricreato, se si possiede un codice mnemonico, diciamo una password, ad esso associata. Materialmente è un software, senza il quale non si può far nulla nella rete.

Cosa è una transazione Token e cosa è un contratto nella rete Ethereum.

Una transazione è un messaggio originato da qualcuno e trasmesso e registrato nella blockchain. Le transazioni sono il modo per far scatenare la macchina di Turing sottostante ed eseguire i contratti, che come vedremo, sono dei veri e propri pezzi di codice software, mentre i Token...sono i dati. Potete immaginare come: i contratti sono le applicazioni del vostro computer, i Token sono l'hard disk o i fogli excel, mentre le transazioni sono la vostra tastiera ed il vostro mouse. Ho semplificato un poco a essere sincero, invero i Token sono particolari tipi di contratto, diciamo qualcosa tipo "contratto di possesso", quindi ogni Token è anche un contratto, strettamente parlando, ma non è vero il contrario, se non hai capito, tira una riga su questa ultima frase, non importa.

Una transazione contiene di base:

- Nonce, un numero
- Gas price, il prezzo che il mittente vorrebbe pagare
- Gas limit, il prezzo massimo che è disposto a pagare
- Recipient, il destinatario o il contratto
- Value, i soldi che si vogliono mandare in relazione al contratto da attivare
- Data, dati vari necessari
- Firma

Se recipient è un destinatario...starete solo trasferendo il value, se invece è un contratto, allora esso verrà eseguito e come input gli sarà passato quanto contenuto in data. Abbastanza semplice. Se mandate informazioni dentro data a un destinatario di solito vengono ignorati, a meno che esso abbia un wallet programmato apposta per capire queste informazioni, ma in tal caso non è un protocollo di Ethereum.

Come si fa a creare un nuovo contratto quindi?

Semplice, si manda una transazione allo zero address, il codice del nuovo contratto deve essere inserito in Data.

I contratti sono detti anche smart contract e ricordiamolo, non sono su carta ma sono pezzi di software che fanno qualcosa. È interessante notare come un contratto ne possa richiamare un altro a catena. I contratti non possono essere modificati, ma possono essere distrutti.

Sopra ho accennato che alcuni contratti sono chiamati Token. Un Token in fin dei conti rappresenta un diritto, in ultimo è una informazione. Il caso più usuale è che un token definisca un valore economico, come un bitcoin o un ether. Ma vediamo le casistiche, perché sono interessanti:

- Currency, ovviamente rappresenta un valore economico
- Resource, potrebbe essere un asset da usare, come dello spazio, energia, gas.
- Asset, un bene, tangibile o intangibile, come un'opera d'arte, dell'oro o un'automobile
- Access, il diritto di accedere a una risorsa, come una rappresentazione teatrale, un file, o un servizio
- Equity, le quote di una società
- Voting, il diritto di voto
- Collectible, si sovrappone con Asset, più appropriato per opere d'arte, memorabilia o altre cose da collezionare
- Identity, identificativo di identità, come un passaporto digitale
- Attestation, il fatto che qualcuno di autorevole abbia dato una certificazione, come una laurea
- Utility, accesso ad un servizio, in sovrapposizione con Access

Alcuni token sono scambiabili senza perdere valore, detti Fungible, altri non possono essere scambiati, perché rappresentano un qualcosa di unico, questi sono detti Non Fungible. Per esempio un diritto di voto potrebbe essere fungible, mentre potrebbe non esserlo una attestazione.

Token e parolacce

Come abbiamo visto i token sono programmi e possono rappresentare più cose. Ecco quindi che sono nati degli standard per fare in modo che token della stessa natura possano essere condivisi. Il primo standard noto è ERC20, che è lo standard che definisce il token della valuta Ether, una sorta di libro mastro. Ma perché "ERC" e perché "20"? Dovete sapere che i nerd e i programmatori si parlano in rete e quando qualcuno sviluppa qualcosa lo mette in delle basi dati e chiede agli altri nerd di verificare se ha fatto bene o male. La maggior parte di questi nerd lavorano gratis e si scambiano i favori. Ecco, ERC significa Ethereum Request for Comments, ovvero: "per favore aiutatemi a capire se ho fatto bene questa cosa e commentatela". Il numero 20 è il numero progressivo, ovvero il nerd di turno aveva già fatto altre 19 richieste simili.

Avrete sentito anche parlare di ERC-721 ed ERC-1155, che sono i due standard per gli NFT di cui tutti parlano (nel marzo del 2021) e sono rispettivamente i protocolli per le i collectibles unici o multipli. Ora sapete per cosa stanno i numeri 721 e 1155...ore di lavoro dei nerd.

Gli NFT

Beh, ormai abbiamo capito tutto! Un NFT è un token il cui contenuto è qualcosa di unico. Tecnicamente è un contratto che sancisce un diritto. Nulla di più facile.

Filosofia degli NFT

“I tempi sono tre: presente del passato, presente del presente, presente del futuro. Questi tre tempi sono nella mia anima e non li vedo altrove. Il presente del passato, che è la storia; il presente del presente, che è la visione; il presente del futuro, che è l’attesa.”

Sant’Agostino

Nel febbraio 2021 molte persone esperte e amanti delle criptovalute, anche e forse soprattutto per motivi speculativi, hanno immaginato che se normali Token (i token fungibili) crescono di valore, certamente potrebbero salire ancor più di valore i token non fungibili, ovvero quelli correlati a contratti unici e meglio ancora se correlati ad una qualche forma di opera d’arte. Apriti cielo! Arte? Investimento? Guadagno? Bomba micidiale.

Non ho mai capito perché chi non compri arte abitualmente abbia in testa che l’arte è una forma di investimento. Chi la compra sa benissimo che comprare arte è una forma di disinvestimento non di investimento! È disinvestimento perché si toglie un asset usabile come il denaro per comprare qualcosa di effimero, in effetti un’emozione o al massimo un poco di cultura. L’arte non si compra per guadagnare soldi, ma anzi per celebrarne la sua utilità ultima, ovvero tornare al nulla che siamo e consumarci in ciò che più di inutile ci sia: la bellezza.

Solo chi non compra arte e chi non l’ha ancora scoperta è fissato con la speculazione sull’arte.

Allora le opere non si rivalutano? Sì, accidentalmente e purtroppo si rivalutano. Ma se questo fosse un fatto a priori allora non si rivaluterebbero. Mi spiego: quando nell’arte le cose sono fatte a tavolino...hanno le gambe corte. Quanti cercano di pompare le aste, di pompare gli artisti e di inventarsi fatti e personaggi dal nulla. Non dura. Al contrario ci si può impegnare per fare in modo che un artista non emerga, personalmente ho seguito quanto il mondo dell’arte che conta(va) abbia cercato di ostacolare artisti come Banksy o Mr.Brainwash nell’entrare nel sistema, ma hanno fallito. L’arte vince sempre e decide sempre lei, no matter what.

Quindi, dicevo, che chi non ha di norma comprato arte, nel primo Q del 2021 ha cercato di speculare, facendo lievitare il prezzo di immagini a bassa risoluzione fino a prezzi di norma riservati a fini capolavori. È come se la gente tutta ad un tratto andasse in massa alle partite di calcio del Nocera Inferiore e le televisioni volessero comprare i diritti delle partite. Certamente il Nocera dovrebbe costruire uno stadio importante, gli sponsor si mobiliterebbero. Va bene tutto, ma con questo...il Nocera Inferiore vincerà davvero lo scudetto? La risposta è semplice: se i calciatori sono forti sì, altrimenti no. Non funziona che siccome le televisioni riprendono il Nocera allora il Nocera vince lo scudetto. Ecco con gli NFT è accaduto questo.

Poi....come detto sopra, possiamo anche dire che alcuni primi cripto artisti (che io reputo artisti a tutti gli effetti) abbiano prodotto opere, per lo più da annoverarsi come opere concettuali, che a tutto diritto devono entrare nella storia. Ma, appunto sono opere concettuali, come lo è il vasino di Duchamp, la merda d’artista di Manzoni o gli stracci di Pistoletto. Ma i primi, stop.

Vogliamo speculare un poco? Va bene, speculiamo un poco e aggiungiamo che possano avere un valore artistico anche i primi NFT di artisti già affermati, giusto per ricordare questo

momento. Ma non andrei oltre. Compriamoci i primi NFT di Koons, di Hirst, di Murakami ammesso che li facciano. Ma poi conterà l'opera, non il media.

Gli NFT sono opere concettuali, come tali vanno visti, se sono in chain, se invece sono off chain non sono neppure opere d'arte, ma meri certificati.

Sapete cosa è davvero un'opera d'arte? I protocolli. Il protocollo della blockchain è un'opera d'arte che è stata regalata alla umanità. È un'opera d'arte la rete Ethereum, la potenza teorica che ha. Certo il tema ambientale non è secondario e va affrontato con grande serietà. Ad ogni modo come nell'anno 2000 l'esplosione della new economy fu eccessiva ma premonitrice, lo stesso sono certo si dirà degli NFT tra 20 anni.