Informazioni tecniche

Cos'è Ethereum?

Ethereum è una piattaforma informatica **decentralizzata**. Puoi vederla come un laptop o un PC, ma non viene eseguita su un singolo dispositivo. Invece, funziona **contemporaneamente su migliaia di dispositivi in tutto il mondo**, il che significa che non ha un proprietario.

Ethereum, come Bitcoin e altre criptovalute, ti permette di **trasferire denaro** digitale. Tuttavia, **è capace di molto altro** – puoi implementare il tuo codice, e **interagire con applicazioni create da altri utenti**. Grazie alla sua flessibilità, ogni sorta di programma sofisticato può essere lanciato su Ethereum.

In poche parole, l'idea centrale alla base di Ethereum è che **gli sviluppatori possono creare e implementare codice che viene eseguito attraverso un network distribuito**, invece di esistere su un server centralizzato. Questo significa che, in teoria, queste applicazioni **non possono essere bloccate o censurate**.

Cosa rende Ethereum prezioso?

Abbiamo accennato all'idea per cui Ethereum può eseguire codice attraverso un sistema distribuito. Per questo, i programmi **non possono essere alterati da parti esterne**. Vengono aggiunti al database di Ethereum (ovvero, la **blockchain**), e possono essere programmati in modo che il codice non possa essere modificato. Inoltre, il database è visibile a tutti, quindi **gli utenti possono verificare il codice** prima di interagire con esso.

Questo significa che chiunque, ovunque, può lanciare applicazioni che non possono essere disattivate. Ancora più interessante, dato che la sua unità nativa – ether – conserva valore, queste applicazioni possono impostare condizioni sui modi in cui il valore viene trasferito. Chiamiamo i programmi che compongono le applicazioni ***smart contract***. Nella maggior parte dei casi, possono essere configurati per operare senza intervento umano.

Comprensibilmente, l'idea di “denaro programmabile” ha attirato utenti, sviluppatori e compagnie in tutto il mondo.

Cos'è la blockchain?

La **blockchain** è al centro di Ethereum – è il database che contiene le informazioni usate dal protocollo. Possiamo paragonare la blockchain di Ethereum a un libro al quale continui ad aggiungere pagine. Ogni pagina è chiamata un **blocco**, ed è piena di informazioni sulle

transazioni. Quando vogliamo aggiungere una nuova pagina, dobbiamo includere un valore speciale in cima alla pagina. Questo valore dovrebbe consentire a tutti di verificare che la nuova pagina sia stata aggiunta *dopo* la pagina precedente, e non inserita a caso nel libro.

Essenzialmente, è un po' come un numero di pagina che fa riferimento alla pagina precedente. Esaminando la nuova pagina, possiamo dire con certezza che segue quella precedente. Per farlo, usiamo un processo chiamato hashing.

L'hashing prende un insieme di dati – in questo caso, tutto ciò che troviamo sulla nostra pagina – **e restituisce un identificatore unico** (la nostra hash). Le probabilità che due insiemi di dati restituiscano la stessa hash sono incredibilmente basse. Inoltre, si tratta di un processo unidirezionale: puoi calcolare facilmente una hash, ma è virtualmente impossibile invertire la hash per ottenere le informazioni usate per crearla. Parleremo dei motivi per cui questo è importante per il mining in un capitolo successivo.

Ora, abbiamo un meccanismo per collegare le nostre pagine nell'ordine corretto. Qualsiasi tentativo di modificare l'ordine o di rimuovere pagine renderà evidente che il nostro libro è stato alterato.

Come funziona Ethereum?

Possiamo definire Ethereum come una ***macchina a stati***. Questo significa semplicemente che, in qualsiasi momento, hai uno **snapshot di tutti i saldi dei conti e degli smart contract** come appaiono correntemente. Alcune azioni causeranno l'aggiornamento dello stato, quindi tutti i nodi aggiorneranno il proprio snapshot per riflettere il cambiamento.

Gli smart contract eseguiti su Ethereum vengono attivati da transazioni (siano queste da utenti o da altri contratti). Quando un utente invia una transazione a un contratto, ogni nodo sul network esegue il codice del contratto e registra l'output. Per far ciò utilizza la ***Ethereum Virtual Machine (EVM)***, che converte gli smart contract in istruzioni leggibili dal computer.

Per aggiornare lo stato, si usa (per ora) un meccanismo speciale chiamato ***mining***. Il mining segue un algoritmo Proof of Work, simile a quello di Bitcoin. Approfondiremo questo argomento a breve.

Cos'è uno smart contract?

Uno *smart contract* è semplicemente codice. Il codice non è né intelligente, né un contratto nel senso tradizionale. Lo chiamiamo smart in quanto **esegue sé stesso secondo determinate condizioni, e può essere considerato un contratto in quanto fa rispettare accordi tra le parti.**

L'idea, proposta a fine anni '90, viene attribuita allo scienziato informatico Nick Szabo. Ha usato l'esempio di un distributore automatico per spiegare il concetto, affermando che poteva essere visto come un precursore del moderno smart contract. Nel caso del distributore automatico, il contratto eseguito è semplice. Gli utenti inseriscono monete e, in cambio, la macchina eroga un prodotto di loro scelta.

Uno smart contract applica questo tipo di logica in un contesto digitale. Potresti specificare qualcosa di semplice nel codice come *return "Hello, World!" quando due ether vengono inviati a questo contratto.*

In Ethereum, lo sviluppatore potrebbe programmarlo in modo che possa in seguito essere letto dalla EVM. Potrà quindi pubblicarlo inviandolo a un indirizzo speciale che registra il contratto. A quel punto, chiunque può usarlo, e il contratto non può essere eliminato, a meno che lo sviluppatore abbia specificato una condizione durante la scrittura.

Ora, il contratto ha un indirizzo. Per interagirci, gli utenti devono semplicemente inviare 2 ETH a quell'indirizzo. Questo attiverà il codice del contratto – tutti i computer sul network lo eseguiranno, vedranno che il pagamento è stato effettuato al contratto e registrandone l'output (*"Hello, World!"*).

Quello che abbiamo descritto sopra è forse uno degli esempi più elementari di ciò che è possibile realizzare con Ethereum. Applicazioni più sofisticate che collegano diversi contratti possono essere – e sono state – costruite.

Chi ha creato Ethereum?

Nel 2008, uno sviluppatore sconosciuto (o un gruppo di sviluppatori) ha pubblicato la whitepaper di Bitcoin sotto lo pseudonimo di **Satoshi Nakamoto**. Questo ha cambiato in modo permanente il panorama del denaro digitale. Pochi anni più tardi, un giovane sviluppatore di nome Vitalik Buterin ha concepito un modo per approfondire questa idea e applicarla a qualsiasi tipo di applicazione. **Il concetto è stato concretizzato in Ethereum**.

Ethereum è stato proposto da Buterin in un blog post risalente al 2013 intitolato *Ethereum: The Ultimate Smart Contract and Decentralized Application Platform*. Nel suo post, ha descritto l'idea per una blockchain Turing-completa – un computer decentralizzato che, con tempo e risorse sufficienti, potrebbe eseguire qualsiasi applicazione.

Nel tempo, i tipi di applicazioni che potrebbero essere implementati su una blockchain sarebbero stati limitati **solo dall'immaginazione degli sviluppatori**. Ethereum mira a scoprire se la tecnologia blockchain ha utilizzi validi al di fuori dei limiti di progettazione intenzionali di Bitcoin.

Come funziona il mining di Ethereum?

Il mining **è fondamentale per la sicurezza del network**. Garantisce che la blockchain venga aggiornata seguendo le regole e consente al network di funzionare senza un organizzatore centrale. Nel mining, un sottoinsieme di nodi (chiamati appunto *miner*) dedicano potenza computazionale alla risoluzione di **un'enigma crittografico**.

Ciò che stanno effettivamente facendo è l'hashing di un set di transazioni in sospeso, insieme ad altri dati. Per fare in modo che il blocco sia considerato valido, la hash deve essere inferiore a un valore definito dal protocollo. Se i miner non hanno successo, possono modificare parte dei dati e riprovare.

Per competere con gli altri, i miner devono quindi riuscire a generare hash il più velocemente possibile – misuriamo la loro potenza in hash rate**. Maggiore è l'hash rate sul network, più difficile sarà l'enigma da risolvere**. Solo i miner devono trovare la soluzione – una volta trovata, è facile per gli altri partecipanti controllare che sia valida.

Come puoi immaginare, **l'hashing continuo ad alte velocità è costoso. Per incentivare i miner a proteggere il network, viene distribuita una ricompensa, composta da tutte le commissioni sulle transazioni nel blocco.** Inoltre, ricevono ether appena generato – 2 ETH al momento della stesura.

Cos'è Ethereum gas?

Ricordi il contratto *Hello, World!* che abbiamo menzionato prima? E' un programma molto semplice da eseguire, non richiede troppe risorse computazionali. **Tuttavia, non lo stai solo eseguendo sul tuo PC – stai anche chiedendo a *tutti* nell'ecosistema di Ethereum di eseguirlo.**

Questo ci porta alla seguente domanda: ***cosa succede quando decine di migliaia di persone stanno eseguendo contratti sofisticati?*** Se qualcuno imposta il proprio contratto per continuare a ripetere lo stesso codice, ogni nodo dovrà eseguirlo all'infinito. Questo richiederebbe troppe risorse.

Fortunatamente, **Ethereum introduce il concetto di *gas***. Proprio come la tua automobile non si muove senza benzina, i contratti non possono essere eseguiti senza gas. I contratti definiscono una **quantità di gas** che gli utenti devono **pagare** per eseguirli con successo. Se non c'è abbastanza gas, il contratto si bloccherà.

Queste sono dei costi che si pagano al momento della generazione dello smart contract

In sostanza, è un meccanismo di commissioni. Lo stesso concetto si estende alle transazioni: i miner sono motivati principalmente dal profitto, quindi potrebbero ignorare le transazioni con una commissione inferiore.

Ricorda che ether e gas non sono la stessa cosa. Il prezzo medio del gas fluttua e viene deciso principalmente dai miner. Quando effettui una transazione, paghi per il gas in ETH. In questo contesto, è simile alle commissioni di Bitcoin – se il network è intasato e molti utenti stanno cercando di effettuare transazioni, è probabile che il prezzo medio del gas aumenterà. Al contrario, se l'attività è scarsa, il prezzo diminuirà.

Anche se il **prezzo del gas varia**, ogni operazione richiede una quantità di gas fissa. Questo significa che i contratti complessi consumeranno molto più di una semplice transazione. Quindi, **il gas è una misura della potenza computazionale**. Garantisce che il sistema possa presentare una commissione appropriata agli utenti in base al loro uso delle risorse di Ethereum.

In genere, il gas costa una frazione di ether. Di conseguenza, usiamo un'unità più piccola (*gwei*) per indicarlo. Un *gwei* corrisponde a un miliardesimo di un ether.

In poche parole, *potresti* eseguire un programma che si ripete per tanto tempo. Tuttavia, farlo diventerà rapidamente molto costoso. Per questo motivo, i nodi sul network di Ethereum possono mitigare lo spam.

Gas e limiti di gas

Supponiamo che Alice stia effettuando una transazione verso un contratto, e che abbia calcolato quanto vuole spendere in gas (per esempio, usando ETH Gas Station). Potrebbe scegliere un prezzo più alto per incentivare i miner a includere la sua transazione il più rapidamente possibile.

Ma imposterà anche un *limite di gas* per proteggersi. Qualcosa potrebbe andare storto con il contratto, portandolo a consumare più gas di quanto ha previsto. Il limite di gas viene fissato per garantire che, una volta usata una quantità *x* di gas, l'operazione venga interrotta. Il contratto verrà bloccato, ma Alice non finirà per pagare più di quanto ha indicato inizialmente.

A primo impatto potrebbe sembrare un concetto difficile da comprendere. Non c'è da preoccuparsi – puoi impostare il prezzo che vuoi pagare per il gas (e il limite di gas) manualmente, ma gran parte degli wallet se ne occuperà al posto tuo. In breve, il prezzo del gas definisce la velocità con cui i miner includeranno la tua transazione, e il limite di gas definisce la quantità massima che pagherai.

Quanto tempo ci vuole per minare un blocco di Ethereum?

Il tempo medio necessario per aggiungere un nuovo blocco alla catena è **12-19 secondi**. Molto probabilmente questo intervallo cambierà una volta che il network effettua la transizione alla **Proof of Stake**, che mira, tra le altre cose, a rendere possibili tempi tra blocchi più rapidi.

Cosa sono i token di Ethereum?

Una buona parte dell'attrattiva di Ethereum è la possibilità per gli utenti di creare i propri **asset on-chain,** i quali possono essere **conservati e trasferiti** come ether. Le regole che li governano sono definite in smart contract, consentendo agli sviluppatori di impostare parametri specifici per i loro token. Questi possono includere il **numero da emettere, le modalità di emissione, la divisibilità, la fungibilità** e tanti altri. Lo standard tecnico più diffuso che consente la creazione di token di Ethereum finora era ERC-20 – ed è per questo che i token sono comunemente noti come token ERC-20. **Ora il nuovo standard è ERC-1155, molto migliore del precedente e con nuove funzionalità che rende Ethereum capace di moltissimi interessanti sviluppi.**

La funzionalità dei token offre agli innovatori un vasto terreno per sperimentare con applicazioni all'avanguardia nella finanza e nella tecnologia. Dall'emissione di **token uniformi che fungono da valuta in-app, alla produzione di token unici garantiti da asset fisici**, c'è una grande flessibilità nella progettazione. E' perfettamente possibile che alcuni dei migliori **casi d'uso per una creazione di token facile e lineare non siano ancora stati scoperti** !

Cos'è la Proof of Stake (PoS) di Ethereum?

La Proof of Stake (PoS) è un **metodo alternativo** alla Proof of Work per la convalida dei blocchi. In un sistema Proof of Stake, i blocchi non vengono *minati*, ma ***coniati*** (a volte indicato come *forgiati*). Invece di miner che competono con potenza computazionale, un nodo (o *validatore*) viene scelto **periodicamente a caso per convalidare un blocco candidato**. Se fatto correttamente, riceverà tutte le commissioni sulle transazioni contenute nel blocco e, a seconda del protocollo, possibilmente anche un block reward.

Dato che non viene più usato il mining, la **Proof of Stake è considerata meno dannosa per l'ambiente**. I validatori consumano una **frazione dell'energia utilizzata dai miner**, e possono invece coniare blocchi su hardware comune.

La transizione di Ethereum da PoW a PoS è programmata come parte di Ethereum 2.0, con un aggiornamento conosciuto come *Casper*. Anche se una data esatta non è ancora stata annunciata, è probabile che la prima iterazione verrà lanciata nel 2020.

Cos'è la Finanza Decentralizzata (DeFi)?

La Finanza Decentralizzata (o semplicemente, DeFi) è un movimento che punta a decentralizzare le applicazioni finanziarie. La DeFi è costruita su blockchain pubbliche e open source accessibili da chiunque con una connessione a internet (*permissionless*).

Questo è un **elemento cruciale per introdurre potenzialmente miliardi di persone** a questo nuovo sistema finanziario globale.

Nel crescente ecosistema della DeFi, gli utenti interagiscono con smart contract e tra di loro attraverso network peer-to-peer (P2P) e Applicazioni Decentralizzate (DApp). Il grande vantaggio della DeFi è che, oltre a rendere tutto questo possibile, gli utenti mantengono comunque la proprietà dei propri fondi in qualsiasi momento.

In poche parole, la Finanza Decentralizzata (DeFi) mira a creare un nuovo sistema finanziario libero dalle restrizioni di quello attuale. Grazie al suo alto grado di decentralizzazione e alla sua grande base di sviluppatori, **la maggior parte delle applicazioni DeFi sono attualmente in costruzione su Ethereum**.

Per cosa può essere usata la Finanza Decentralizzata (DeFi)?

Probabilmente lo sai già, ma uno dei principali vantaggi di Bitcoin, Ethereum e altre Cryptovalute, è che non serve un'autorità centrale per coordinare l'operazione del network. Ma cosa succede se usiamo questa caratteristica come idea centrale e realizziamo applicazioni programmabili sopra di essa? **Questo è il potenziale delle applicazioni DeFi. Nessun coordinatore centrale o intermediario, e nessun singolo punto di errore.**

Come già detto, uno dei grandi vantaggi della DeFi è il libero accesso. Ci sono miliardi di persone nel mondo che non hanno un buon accesso ad alcun tipo di servizio finanziario. Riesci ad immaginare come gestire la vita quotidiana senza la certezza delle tue finanze? Ci sono miliardi di persone che vivono così, e in ultima analisi, questo è il target demografico della DeFi.

Quali sono le applicazioni della Finanza Decentralizzata (DeFi)?

Uno dei casi d'uso più popolari per la Finanza Decentralizzata (DeFi) sono le **stablecoin**. Essenzialmente, sono **token su una blockchain** con un valore ancorato a un asset nel mondo reale, come una moneta fiat. Per esempio, **ETH è ancorato al valore dell'USD**. Ciò che rende questi token pratici da usare è la loro esistenza su una blockchain, che li rende molto facili da conservare e trasferire.

Comunque, la parte probabilmente più entusiasmante della DeFi sono le applicazioni difficili da categorizzare. Queste possono includere qualsiasi tipo di mercato peer-to-peer decentralizzato, in cui gli utenti possono scambiare **oggetti da collezione crypto unici e altri oggetti digitali**. Possono anche consentire la creazione di **asset sintetici, in cui chiunque può creare un mercato per praticamente qualsiasi cosa che abbia valore**. Altri utilizzi possono includere mercati di previsione, prodotti derivati e tanto altro.

Definire la Finanza decentralizzata (DeFi)

DeFi sta per "finanza decentralizzata" e si riferisce all'ecosistema composto da applicazioni finanziarie che vengono sviluppate su sistemi blockchain .

La DeFi può essere definita come il movimento che promuove l'uso di reti decentralizzate e software open source per creare molteplici tipi di servizi e prodotti finanziari. L'idea è di sviluppare e gestire DApp finanziarie su un framework trasparente, come blockchain senza autorizzazione e altri protocolli peer-to-peer (P2P) .

Attualmente, le tre funzioni principali della DeFi sono:

- Creazione di servizi di banca monetaria (ad es. emissione di stablecoin)
- Fornire piattaforme di prestito e prestito peer-to-peer o in pool
- Abilitazione di strumenti finanziari avanzati come DEX, piattaforme di tokenizzazione, **NFT**, derivati e mercati delle previsioni

All'interno di questi tre campi, ci sono diversi tipi di servizi DeFi. Alcuni altri esempi di prodotti e casi d'uso includono protocolli di finanziamento, strumenti di sviluppo software, costruzione di indici , protocolli di pagamento di abbonamenti e **applicazioni di analisi dei dati**. Le dApp DeFi possono essere utilizzate anche per KYC , AML e altri servizi di **gestione delle identità**.

Cosa sono i token ERC-20 ed ERC-721 e cosa è il nuovo ERC-1155

Per capire perché sono stati creati i token ERC-1155, è necessario esaminare alcuni punti intermedi che ci daranno una migliore comprensione di questo punto. Tra questi punti possiamo menzionare:

I limiti del token ERC-20

I token ERC-20 (per token fungibili) e ERC-721 (per non fungibili, NFT) di Ethereum sono ampiamente utilizzati all'interno dell'ecosistema. Basta dare un'occhiata a Etherscan per vedere l'enorme numero di token di questo tipo che esistono. Tuttavia, entrambi i token hanno dei limiti, alcuni dei quali piuttosto gravi.

Ad esempio, nel token ERC-20, una delle principali limitazioni è la mancanza di un modo per "reagire" agli eventi di trasferimento ERC-20. Ciò si traduce in token ERC-20 intrappolati per sempre nei contratti quando gli utenti inviano accidentalmente token all'indirizzo sbagliato. In questo modo, se trasferisci a un indirizzo ERC-20 errato, ciò che hai trasferito viene perso per sempre.

I limiti del token ERC-721

Da parte loro, anche i token ERC-721 hanno i loro limiti. Ad esempio, ottenere direttamente un identificatore di token è impossibile e questo rende difficili le transazioni con questi token. Infatti, se, ad esempio, hai un set di 10 NFT che vuoi trasferire ad un'altra persona, quel trasferimento ti richiederà di effettuare 10 diverse transazioni, con la loro commissione corrispondente e ciò aumenta notevolmente il costo di questo semplice funzionamento, così come le operazioni di carico della rete, con un enorme impatto sull'usabilità della rete Ethereum. In questi scenari dovrai trasferire gettone per gettone, essendo impossibile trasferire tutti e 10 contemporaneamente, cosa abbastanza assurda in realtà.

Un altro problema è attraversare i token ERC-721. Ciò richiede che tutti i token all'interno del contratto vengano attraversati allo scopo di fornire una risposta alla DApp e all'utente in questione. Immagina per un momento che un contratto ERC-721 abbia nel suo registro 1 milione di token, ciò significa che, se una persona vuole conoscere lo stato dei propri token, deve inviare una transazione alla rete che passerà attraverso questo milione di token, li abbinerà agli indirizzi dell'utente e quindi fornirà la risposta. Questa è la più grande dimostrazione di inefficienza che si possa avere in un sistema di questo tipo.

Incompatibilità tra i token ERC-20 e ERC-721

Insieme a questo, i token ERC-20 ed ERC-721 sono incompatibili tra loro. In effetti, i contratti sono così diversi che la creazione di funzionalità aggiuntive che colleghino i due è un compito arduo e probabilmente avrebbe un forte impatto sulla rete, potenziali guasti e costi di commissione elevati.

Ciò è particolarmente importante perché molte DApp utilizzano entrambi i tipi di token e, a causa di questa limitazione, la logica del loro funzionamento diventa più complessa. Se un unico smart contract potesse essere utilizzato per gestire tutto, sarebbe molto più facile da programmare, oltre ad essere più sicuro e meno complesso da progettare.

Perché sono stati creati gli ERC-1155?

ERC-1155, uno standard per la gestione di gettoni con molteplici funzioni

L'idea è semplice e cerca di creare un'interfaccia di contratto intelligente in grado di rappresentare e controllare un numero qualsiasi di tipi di token fungibili e non fungibili. In questo modo, il token ERC-1155 può svolgere le stesse funzioni di un token ERC-20 e ERC-721, e anche entrambi allo stesso tempo. E soprattutto, migliorando la funzionalità di entrambi gli standard, rendendola più efficiente e correggendo gli errori di implementazione evidenti sugli standard ERC-20 ed ERC-721. **Questo standard è stato sviluppato da Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therien, Eric Binet e Ronan Sandford.**

In questo contesto, è stato creato ERC-1155, al fine di unire i due mondi sotto lo stesso contratto, superando i limiti già descritti e rendendo più efficiente la loro gestione. Non solo, questa soluzione eviterebbe anche l'enorme frammentazione dei token che esiste oggi, consentendo allo stesso tipo di contratto di controllare entrambi i tipi di token.

Ciò, ad esempio, consentirebbe a uno sviluppatore di DApp di utilizzare l'ERC-1155 in modo che i suoi utenti possano registrare token fungibili (token che possono essere utilizzati come valute di pagamento) e token non fungibili (oggetti collezionabili, oggetti scambiabili all'interno della DApp o del gioco) utilizzando lo stesso contratto, lo stesso indirizzo e semplificando la logica delle DApp e del **smart contract** soci. Senza dubbio, è

un uso più efficiente delle risorse, qualcosa che non verrebbe più in blockchain come Ethereum e le sue risorse limitate.

Nuove funzioni e possibilità del token ERC-1155

Un attimo fa abbiamo parlato dei token ERC-20 ed ERC-721 che hanno dei limiti da superare e che ERC-1155 era la risposta. A questo punto ti chiederai **Cosa puoi fare veramente con un ERC-1155?** Bene, queste sono alcune delle possibilità:

Trasferimenti di massa come standard

Lo standard ERC-1155 consente trasferimenti di massa dei token inclusi in uno smart contract in modo nativo. In questo modo, se, ad esempio, abbiamo una serie di token NFT o token fungibili (o entrambi), possiamo trasferire più di questi token nella stessa operazione, facendo in modo che un'unica operazione renda efficace questo trasferimento.

In questo modo è possibile risparmiare sui costi di transazione, minimizzare l'impatto sulla rete e abilitare un sistema di trading (**escrow**/**scambio atomico**) utilizzando tali gettoni in un modo molto più semplice.

Gettoni multipli nello stesso contratto

Oltre a questo, **un ERC-1155 può descrivere l'esistenza e il funzionamento di più token contemporaneamente**. Cioè, un ERC-1155 può creare uno o più token fungibili (come ERC-20) e può anche descrivere uno o più token non fungibili (come ERC-721) tutti all'interno dello stesso contratto, facilitando la distribuzione e la programmazione.

Rilevamento del tipo di token integrato

Un'altra funzionalità all'interno del token ERC-1155 è la capacità di integrare la funzionalità del **ERC-165** (noto come, interfaccia di rilevamento standard), tutti all'interno dello stesso sistema. In questo modo, il token ERC-1155 è in grado di rilevare l'interfaccia del token e

adattare il suo comportamento a seconda di essa. Ciò è particolarmente utile a causa della natura multitoken dell'ERC-1155 e semplifica la progettazione dell'applicazione.

Trasferimento sicuro dei token

Forse una delle caratteristiche più promettenti del token ERC-1155 è il **trasferimento sicuro dei token**. Per questo, lo smart contract standard ERC-1155 include una funzione che verifica che la transazione sia stata eseguita e, in caso contrario, la ripristina per restituire il controllo dei token al suo emittente.

Ciò è particolarmente utile quando commettiamo un errore nella trascrizione o nella copia degli indirizzi e invece inviamo i nostri token all'indirizzo sbagliato incapace di elaborare la nostra transazione. In tal caso, il trasferimento è nullo e l'emittente recupera i token, consentendo di verificare nuovamente l'indirizzo e di ritentare l'operazione. Per evitare attacchi da **la doppia spesa:**, sono descritte una serie di regole che impediscono questo comportamento, rendendolo sicuro contro questi tipi di attacchi e altre trappole.

Man mano che le DApp diventano più complesse e con un numero maggiore di funzioni, la capacità dell'ERC-20 e dell'ERC-721 inizia ad essere più limitata. ERC-1155 è una buona risposta, perché è conforme a tutto ciò che questi due token rendono possibile, oltre ad aggiungere nuove funzioni che facilitano una migliore integrazione e usabilità per l'utente.

Mentre i token ERC-20 sono fungibili e i token ERC-721 non fungibili, ERC-1155 è uno standard multi token: lo stesso contratto token può includere qualsiasi combinazione di token fungibili, token non fungibili o token semi-fungibili.

I token fungibili funzionano come valuta. Una banconota da $ 5 può essere cambiata con un'altra banconota da $ 5 senza alcuna differenza di valore. I token non fungibili come CryptoKitties sono unici. Ogni gattino ha un valore diverso, ha tratti individuali ed è spesso trattato come un oggetto da collezione.

Un token semi-fungibile funziona inizialmente allo stesso modo dei token fungibili. Potrebbe essere scambiato con un altro dello stesso contratto token senza differenza di valore fino a quando non viene soddisfatta una condizione particolare. Da quel momento in poi, diventa non fungibile e non può essere semplicemente scambiato tra loro.

Un esempio a cui pensare è quello di un biglietto per vedere il Manchester United in una partita di Premier League. Prima dell'inizio della partita, il biglietto potrebbe essere scambiato con quello di un'altra partita di Premier League (con qualità avversaria simile) dello stesso valore. Al termine, lo stesso biglietto potrebbe avere un valore molto diverso a seconda del suo proprietario. Per alcuni può rappresentare un momento storico della loro vita ed è estremamente prezioso come memorabilia. Per altri può essere una delle tante o addirittura rappresentare un'occasione per dimenticare. In questo modo un biglietto che una volta era fungibile con altri diventa in seguito non fungibile.

In definitiva, il token ERC-1155 è un tipo di token standard che ha la capacità di immagazzinare, sotto il suo controllo, token che possono agire come se fossero un token. ERC-20 o ERC-721, o entrambi contemporaneamente allo stesso indirizzo.

Un modo più efficiente per utilizzare le risorse e la pianificazione

Cosa è Applicazione decentralizzata (DApp)

Le applicazioni decentralizzate (**DApps**) sono applicazioni eseguite su un sistema di calcolo distribuito, ovvero una rete blockchain . Sebbene esistano vari modi per definire una DApp, di solito vengono descritte come applicazioni che presentano le seguenti caratteristiche:

- **Open Source** – Il codice sorgente è intenzionalmente reso disponibile al pubblico, il che significa che chiunque è in grado di verificare, utilizzare, copiare e modificare il codice.

- **Decentralizzato** : poiché le DApp funzionano su reti blockchain, non sono controllate da una singola entità o autorità. Al contrario, sono gestiti da più utenti (o nodi).

- **Crittograficamente sicuro** : l'applicazione è protetta dalla crittografia , il che significa che tutti i dati vengono registrati e mantenuti in una blockchain pubblica. Non esiste un singolo punto di errore.

Ci sono più problemi nelle applicazioni legacy che le DApp cercano di risolvere. Il vantaggio principale della scelta di una DApp rispetto a un'app tradizionale è che quest'ultima utilizza un'architettura centralizzata archiviando i propri dati su server controllati da un'unica entità. Ciò significa che hanno un singolo punto di errore, soggetto a problemi tecnici e attacchi dannosi.

Un server centralizzato compromesso può bloccare l'intera rete dell'applicazione, rendendola temporaneamente o permanentemente inutilizzabile. Oltre a ciò, i sistemi centralizzati subiscono spesso perdite o furti di dati, mettendo a rischio le aziende e i singoli utenti.

Esiste una grande varietà di DApp, con diversi casi d'uso. Possono includere giochi , piattaforme di social media, portafogli di criptovaluta e applicazioni finanziarie (DeFi).

Le applicazioni decentralizzate alimentano la propria attività attraverso un sistema tokenizzato (token digitali creati attraverso l'uso di smart contract). I token possono essere specifici per una particolare DApp (es. il token Steem utilizzato su Steemit), oppure possono essere nativi della blockchain che ospita la DApp, come nel caso di CryptoKitties che utilizzano ether (ETH).

Riassumendo, le DApp sono progettate come progetti open source che vengono eseguiti su una rete blockchain. A sua volta, la natura distribuita di queste reti fornisce trasparenza, decentramento e resistenza agli attacchi.

La finanza decentralizzata porta numerosi vantaggi rispetto ai servizi finanziari tradizionali. Attraverso l'uso di contratti intelligenti e sistemi distribuiti, la distribuzione di un'applicazione o di un prodotto finanziario diventa molto meno complessa e sicura. Ad esempio, molte dApp vengono sviluppate sulla blockchain di Ethereum , che offre costi operativi ridotti e barriere all'ingresso inferiori.

Riassumendo, il movimento DeFi sta spostando i prodotti finanziari tradizionali verso il mondo open source e decentralizzato, eliminando la necessità di intermediari, riducendo i costi complessivi e migliorando notevolmente la sicurezza.

NFT cosa sono

Per spiegare cosa sono gli **NFT** occorre partire dal nome per esteso: **"Non-Fungible Token"**. La prima parte del concetto (ossia, ***Non-Fungible***) racchiude un po' il **succo dell'intero discorso**: si tratta di un **pezzo**, o per meglio dire un "token" se si guarda al sostantivo che compone l'intera sigla **NFT, unico nella sua individualità**. Unico perché **non fungibile, a differenza del denaro**, del Bitcoin e di qualunque altro oggetto replicabile e sostituibile. Tanto per intenderci, **una banconota da dieci euro è facilmente rimpiazzabile con un'altra banconota di analogo valore; per gli NFT, invece, vale esattamente l'opposto, riferendosi ognuno a un prodotto diverso**.

Questa **esclusività** spiega bene il significato dei Non-Fungible Token, ossia un modo per **identificare univocamente un prodotto digitale** creato su Internet. Un po' come un **certificato di proprietà**.

Gli oggetti digitali possono essere moltissimi: dai gattini in formato digitale – di fatto i precursori del mercato degli NFT – ai post sui social, passando **per video, foto, audio, testi e addirittura GIF, opere d'arte e meme**, ma si potrebbe anche proseguire con tanti altri esempi e sfaccettature. L'elemento che lega tutti questi contenuti è che**, laddove "firmati" con NFT, è come se sopra ci fosse la firma del suo autore, che ne riconosce perciò l'autenticità e l'originalità**.

L'oggetto può anche non essere necessariamente singolo: l'autore ha infatti la possibilità di riprodurne una serie in **tiratura limitata**, dove ciascun esemplare è "marchiato" dal suo **esclusivo NFT**: in questo caso si parla di standard **ERC-1155**, dove uno smart contract vale più token. È importante sottolineare che ciò che si acquista è la certificazione

NFT e blockchain

Per poter funzionare, i **Non-Fungible Token** si servono della blockchain, che può essere immaginata come una sorta di "**registro digitale**" in cui si **annotano transazioni tramite un codice inalterabile**. Questo sistema, sorretto da moltissimi terminali informatici, garantisce il carattere **autentico delle transazioni**, mediante una serie di **metadati** salvati su una moltitudine differenziata di computer. Il meccanismo è fondamentalmente lo stesso su cui si basano i Bitcoin, ma trasposto in diversi altri ambiti. È comunque **importante** ribadire la **non-fungibilità**, l'elemento che **distingue le criptovalute dagli NFT**.

Come funzionano gli NFT

Il funzionamento degli NFT è riassumibile in tre passaggi: **creazione, archiviazione sulla blockchain attraverso lo "smartcontract" e la vendita**. Per prima cosa, viene generata la **versione digitale di un'opera**, che può essere ad esempio un file immagine, una traccia audio o un file video. Non è infrequente che le piattaforme di compravendita appongano dei limiti alle dimensioni del file: ad esempio, il marketplace Open Sea pone un limite di 100 megabyte, pur consigliando ai creatori di non sforare la soglia dei 40 mb.

La versione digitale altro non è che una sequenza di numeri, compressa – attraverso un procedimento conosciuto come hashing – in una sequenza ancora più piccola, detta appunto hash. Questa tecnica garantisce alcune tipiche **peculiarità degli NFT, come l'integrità e la sicurezza, alla quale si aggiunge anche l'indistruttibilità**, caratteristica quest'ultima dettata dall'archiviazione sulla **blockchain tramite smart contract**, una sorta di **contratto redatto con protocollo informatico nel quale sono contenuti i principali termini di acquisto**. Il soggetto che possiede il documento digitale di partenza è in grado

di calcolare l'hash, mentre non vale invece l'opposto. L'hash così generato viene memorizzato su una blockchain con una marca temporale associata (che serve a documentare la data di inserimento in questo sistema informatico) e può essere poi scambiato su diversi marketplace (Open Sea è uno di questi, ma ne citeremo anche altri) a fronte di un pagamento, solitamente in criptovaluta.

Le piattaforme per investire sugli NFT

La piattaforma più accessibile è **Open Sea** ed è basata su Ethereum. Ma non mancano anche altri marketplace dove negoziare un Non-Fungible Token, come **Nifty Gateway** e altri luoghi un po' più specializzati: vedasi ad esempio **NBA Top Shot** per l'acquisto di un NFT che afferisce a un particolare momento del gioco del basket (ha guadagnato gli onori della cronaca l'immagine della schiacciata di LeBron James, in omaggio al mitico Kobe Bryan, venduta alla cifra record di 387.600 dollari), **Valuables** per l'acquisto dei tweet e **CyptoKitties** per gli amabili gattini digitali.

In breve, NFT sta per *Non-Fungible Token* e possiamo considerarla una "**certificazione**" volta ad identificare **la proprietà di un prodotto digitale**. Ogni token non fungibile viene registrato su **blockchain**, un sistema digitale che **garantisce l'integrità e la tracciabilità di ogni trasferimento di dati. NFT, metaverso e crypto-art sono un mercato in continua crescita, che si prospetta piuttosto proficuo anche nel 2022**: un motivo più che valido per investire in non-fungible token. Ecco quindi una guida su **perché investire e come comprare NFT** attraverso i canali più famosi, come OpenSea o Nifty Gateway

Cavalcare l'onda del fenomeno? **Un'ottima opportunità**. Ma sempre con la testa sulle spalle.

I vantaggi e gli svantaggi di investire in NFT

Ciò che **differenzia** principalmente un NFT da una criptovaluta è che gli NFT sono **token non fungibili**, ovvero **non ripetibili e perciò unici**. Questo è sicuramente il **vantaggio principale dell'investire in questo nuovo business**, dal momento che un NFT acquistato ora – vista la sua natura unica – potrebbe nel tempo **acquisire un certo valore** ed essere **rivenduto ad un prezzo più elevato**.

Alcuni esempi di NFT

Gli NFT più diffusi riguardano **l'arte digitale**. Dai disegni alle illustrazioni, GIF, video, fotografie e tutto ciò che potrebbe essere etichettato come "**unico**" e venduto come **oggetto (virtuale) da collezione**. In altri casi, come per le opere di **Banksy**, esiste una controparte fisica da affiancare a quella digitale. Gli **NFT**, però, hanno **un potenziale molto più vasto**. Un precedente lo ha creato **Jack Dorsey**, ex CEO di Twitter che ha venduto sotto forma di NFT il primo tweet della storia: una transazione dal valore di 2,9 milioni di dollari. Perciò ora è possibile utilizzare **NFT** per vendere **musica**, **comprare**

biglietti per eventi, regalare buoni sconto nei negozi, per la compravendita di videogiochi o addirittura come “certificazione” per possedere un documento di proprietà immobiliare.

Come investire in NFT

Ora che sai cosa è un NFT, i vantaggi e gli svantaggi, tutte le sue applicazioni e in che modo questo nuovo mercato sta fiorendo sempre più nel mondo del web – e non solo – puoi meglio capire perché le opere d’arte digitali, sono un mercato in forissima crescita.

Dove si vendono gli NFT

La compravendita di NFT avviene sui **marketplace**: **un vero e proprio mercato** in cui i token non fungibili sono disponibili a **prezzi fissi oppure all’asta**, in quantità più o meno limitate. Alcuni **market sono specializzati**, altri – invece – più focalizzati su una certa tipologia di NFT. Tuttavia, prima di avventurarvisi bisogna tenere conto di alcune cose importanti: anche se il token non fungibile prescelto è gratuito oppure economico, per far sì che la transazione avvenga è pur sempre necessario **pagare un “gas fee”**, una tassa variabile che dipende da quanto sia congestionata (o meno) la rete in quel momento.

Il **marketplace NFT di Coinbase** sarà peer-to-peer e permetterà di comprare, vendere e mettere in mostra i propri NFT. Inoltre, secondo quanto dichiarato dalla società, saranno presenti funzionalità social, così come tutti gli strumenti necessari per creare i propri NFT in pochissimi passaggi. L’obiettivo? Quello di diventare una **piattaforma user-friendly** e semplice da usare. Inizialmente il supporto sarà limitato solamente agli standard **ERC-721 e ERC-1155 di Ethereum**, ma in futuro le porte si apriranno anche a NFT basati su blockchain differenti.

OpenSea

OpenSea è la **piattaforma di riferimento** per la compravendita di NFT e criptovalute. Basata sulla blockchain di Ethereum, offre oltre 240 metodi di pagamento differenti, rendendolo così uno dei marketplace più versatili. **Comprare NFT su OpenSea** è piuttosto semplice: basta un profilo, a cui collegare un wallet virtuale. Ogni utente può visionare liberamente quanto contenuto in un portafoglio digitale e, nel caso, comprare ciò che più gli piace in base al prezzo stabilito dal venditore – oppure partecipando a una asta.

SuperRare

SuperRare è un altro marketplace particolarmente diffuso, specializzato soprattutto nella compravendita di crypto-art. Qui gli artisti mettono in vendita **opere di ogni genere** in

forma di NFT, che verranno poi acquistate in modo sicuro tramite blockchain Ethereum dai collezionisti.

Rarible

Nonostante sia fra i meno diffusi, Rarible resta uno dei marketplace più importanti: utilizza infatti un sistema di *governance* decentralizzato, in cui è la community in possesso del token RARI **a decidere su tutto** ciò che riguarda la piattaforma.

Nifty Gateway

Al contrario degli altri marketplace, Nifty Gateway collabora con artisti, marchi e brand per dare vita a **collezioni virtuali in edizione limitata** e unicamente in vendita sulla piattaforma. Possiamo dire che qui si trovano tutti gli NFT più rari, dal momento che i "lanci" sono disponibili soltanto per un periodo di tempo molto limitato, aumentandone perciò il valore.

Mintable

L'obiettivo di Mintable è quello di diventare il marketplace leader nel settore degli NFT. Costruita su blockchain Ethereum, Mintable permette ai propri utenti di creare, distribuite, comprare e vendere NFT di qualsiasi tipo. Offre, inoltre, diversi utili strumenti come – ad esempio – **il misuratore di rarità** guidato da Intelligenza Artificiale.

MakersPlace

MakersPlace è uno di quei mercati che recentemente stanno crescendo sempre più. Anche in questo caso il market è guidato dalla community ed è **accessibile solo su invito**: MakersPlace è stato infatti progettato con l'obiettivo di dar vita ad una comunità di talentuosi artisti. È proprio qui che Beeple, uno dei cripto-artisti più famosi, ha messo in vendita lo scorso anno le proprie opere NFT per migliaia di dollari.

Foundation

Anche Foundation si concentra sulla compravendita di opere in forma di NFT: sono tanti gli artisti che si affidano a questa piattaforma, che ha fatto della **community il suo cuore nevralgico**. Come dice il sito web ufficiale, *"vogliamo che tutti coloro che hanno a cuore il futuro dell'espressione digitale facciano parte di Foundation"*. Proprio su questo market è stata venduta anche la GIF che ha dato vita al celebre Nyan Cat.

NBA Top Shot

Molto diverso dagli altri marketplace, NBA Top Shot è una piattaforma basata su tecnologia blockchain e sull'**idea di collezionismo digitale**. Qui, gli utenti possono comprare, vendere oppure scambiare i "moments", ovvero video in cui vengono mostrati gli highlights delle migliori partite NBA. Il tutto in forma di token NFT.

Gli NFT legati al mondo dei giochi

Come abbiamo potuto osservare, gli NFT sono in genere legati ad **un'opera digitale**. Ma come applicare i non-fungible token al mondo dei videogiochi? Le aziende videoludiche – al momento – non sembrano particolarmente interessante, ma **qualche intraprendente c'è**. Un esempio è Ubisoft, che ha lanciato **la piattaforma "Quartz"** che si basa su blockchain Tezos. In questo caso i token non sono altro che **skin**, numerate e quindi disponibili soltanto per pochissimi, che diventano successivamente di proprietà dell'acquirente. Tuttavia le possibilità di **NFT e videogiochi sono molto più ampie** di così: esistono infatti alcuni giochi che permettono di **guadagnare denaro** grazie alle blockchain e perfino giochi in stile *Tamagotchi* dove ogni animaletto virtuale è un **NFT unico per ogni giocatore**.

Costi e commissioni

Comprare NFT, ovviamente, comporta dei **costi e delle commissioni** da affrontare. Tutto dipende dal market a cui si fa riferimento: OpenSea, ad esempio, non prevede alcun esborso per finalizzare l'acquisto, quindi solo per la vendita, ma è presente **una gas fee variabile** fondamentale per processare la transazione in corso. Bisogna tenere conto anche di eventuali costi di **gestione account, commissioni legate alle piattaforme NFT di riferimento, convertire una criptovaluta e per l'acquisto di token**.

Considerazioni conclusive

Con un 2021 proficuo alle spalle e un 2022 incerto ma molto promettente, **ha senso investire in NFT?**

Sicuramente l'anno appena iniziato vedrà un'espansione **ancora più ampia dei non-fungible token** e battere il **ferro finché è caldo** può essere una buona idea. Con il nuovo anno ci saranno **molte novità**, legate oltre che all'**espansione** del mercato delle opere d'arte, anche al **metaverso** e al mondo dei videogiochi, e sempre più settori si affideranno alle blockchain. Non mancheranno i rischi, ma valutando **l'investimento in prospettiva della continua evoluzione sia tecnologica che del settore**, è una **mossa conveniente!**

Con quali criteri si determina la qualità e il valore di un NFT?

Ci sono alcune cose da guardare nel campo degli NFT:

1. Le proprietà uniche
Gli NFT spesso si presentano sotto forma di collezioni. Queste sono costituite da singole opere che hanno tutte proprietà diverse. Se vuoi aumentare le possibilità di acquistare un NFT con una traiettoria di valore promettente controlla la proprietà dell'NFT e la **rarità** di proprietà. Dati che puoi trovare tra i dettagli dell'NFT in vendita sul marketplace. Puoi farti aiutare anche da strumenti ad hoc come **Rarity Tool**, un sito per il monitoraggio delle rarità di NFT.

2. Chi è il venditore
Così come su Instagram e Twitter, i venditori ufficiali accreditati su OpenSea hanno la **spunta blu** accanto al loro nome per dimostrare che sono veri e affidabili. Se ti interessa un NFT di un venditore non verificato controlla il suo account sui social media per vedere se ha una buona base di follower e la spunta blu, o in alternativa cerca informazioni sul suo conto e sul progetto su forum e nella community NFT.

3. I costi di commissione

Le piattaforme NFT addebitano dei costi per le transazioni, che variano a seconda della piattaforma ma che nella stragrande maggioranza dei casi sono a carico dei venditori. Ci sono però delle piattaforme che fanno pagare le commissioni anche agli acquirenti: è il caso di **Rarible**, che addebita all'acquirente una commissione del 2,5% in aggiunta al prezzo NFT per transazione. Quindi assicurati di essere a conoscenza di eventuali commissioni esistenti sulla piattaforma scelta prima di effettuare qualsiasi acquisto.

4. L'andamento del prezzo degli NFT del venditore
Se vuoi sapere se l'NFT che vuoi comprare è un buon investimento è una buona idea controllare l'account del venditore e il suo storico. Guarda le vendite precedenti e il prezzo di vendita dei suoi pezzi

Da ricordare con gli NFT

Tieni a mente che gli NFT non hanno la stessa liquidità delle criptovalute e non puoi scambiare NFT in valuta tradizionale con la stessa facilità delle cripto.

A differenza delle criptovalute gli NFT non traggono valore dalla loro utilità (come asset di investimento) ma dai media che rappresentano (arte, video, ecc). Quindi investire in NFT vuol dire investire in un oggetto da collezione e il suo valore nel tempo sarà determinato da vari fattori intangibili tra cui la qualità del pezzo, la sua unicità e il prestigio dell'artista che lo ha creato.

In questo momento la maggiore parte viene utilizzata per vendere arte digitale e oggetti da collezione (anche se sta prendendo piede il trend degli **investimenti in terreni virtuali**). Quella degli NFT è la nuova frontiera del collezionismo di oggetti e opere d'arte. Si tratta di un mercato ancora molto giovane e durerà a lungo !

Anche nel caso dei non-fungible token vale la regola base di tutti gli investimenti: non investire di più di quanto puoi permetterti di perdere.

Questo articolo non è e non vuole essere un consiglio di investimento, ma una guida a scopo informativo. Affidati sempre a un professionista debitamente autorizzato per una consulenza sugli investimenti.

Volendo fare un esempio, la prima opera **NFT** venduta dalla storica casa d'aste **Bleepe** ("**Everydays — The First 5000 Days**") è stata acquistata da un soggetto conosciuto sotto lo pseudonimo di **Metakovan** e fondatore di Metapurse, il più grande fondo **NFT** al mondo. Nel caso di specie, Metakovan ha sborsato quasi 70 milioni di dollari per comprare un file in formato JPEG collocato in un portafoglio digitale, reso unico da uno smart contract e composto da una lunga sequela di pixel e byte. Non ha dunque la disponibilità del file – che si trova altrove – ma i diritti sullo stesso, cristallizzati attraverso il possesso dei metadati. In ogni caso, grazie al metodo dell'hashing, l'**NFT** tiene in memoria tutti i dati relativi ai passaggi di proprietà, consentendo la dimostrazione semplice e immediata del possesso anche senza l'ausilio di un soggetto terzo. Almeno fintantoché la blockchain che ospiterà il token resterà attiva. E qui si inseriscono alcuni dei problemi giuridici legati al mercato dei Non-FungibleToken.