

CONCETTI PRINCIPALI TIROCINIO(INTRODUZIONE)

Cos'è la Blockchain?

La blockchain è un **registro di contabilità condiviso e immutabile** che facilita il processo di **registrazione delle transazioni e la tracciabilità degli asset** in una rete commerciale. Un *asset* può essere tangibile (una casa, un'auto, del denaro, dei terreni) o intangibile (proprietà intellettuale, brevetti, copyright, branding). Praticamente qualsiasi cosa che **abbia un valore** può essere rintracciata e scambiata su una rete blockchain, riducendo rischi e costi per tutte le parti coinvolte. Il business si basa sulle informazioni. Più sono rapide e accurate, meglio è. La blockchain è ideale per offrirle perché **fornisce informazioni immediate**, condivise e completamente trasparenti, archiviate in un registro immutabile a cui possono accedere solo i membri di rete autorizzati. Una rete blockchain può, tra le altre cose, **tracciare ordini, pagamenti, account e produzione**. E poiché i membri condividono un'unica visione della verità, puoi vedere tutti i **dettagli di una transazione dall'inizio alla fine**, il che ti offre maggiore fiducia, oltre a nuove efficienze e opportunità.

Ethereum

Ethereum è una **piattaforma open-source basata su blockchain** che consente agli sviluppatori di creare e distribuire applicazioni decentralizzate (DApps) e contratti intelligenti. È stata proposta per la prima volta nel 2013 da Vitalik Buterin e successivamente sviluppata da un team di sviluppatori e ricercatori.

Ci sono diverse caratteristiche chiave di Ethereum:

1. ****Blockchain****: **Ethereum utilizza una blockchain per registrare e validare le transazioni**. Questa blockchain è **distribuita su una rete globale di nodi**, rendendola resistente alla censura e alla manomissione.
2. ****Contratti Intelligenti****: Ethereum **è noto per l'introduzione dei contratti intelligenti**, che sono programmi computerizzati che **eseguono automaticamente le istruzioni quando vengono soddisfatte determinate condizioni**. Questi contratti sono eseguiti sulla blockchain e possono essere utilizzati per automatizzare una vasta gamma di operazioni, inclusi pagamenti, scambi di asset e altro ancora.
3. ****EVM (Ethereum Virtual Machine)****: Ethereum include una **macchina virtuale** che consente l'esecuzione di codice di contratti intelligenti su tutti i nodi della rete. Questa EVM **consente l'esecuzione dei contratti intelligenti in un ambiente sicuro e affidabile**.
4. ****Token ERC-20 e Standard di Token****: Ethereum ha introdotto gli **standard di token ERC-20**, che hanno **reso facile la creazione e lo scambio di token su blockchain Ethereum**. Questi token possono rappresentare una vasta gamma di asset digitali, come valute, azioni, proprietà e altro ancora.
5. ****Evoluzione continua****: Ethereum è un progetto in continua evoluzione, con costanti aggiornamenti e miglioramenti. Uno dei cambiamenti più significativi è la transizione da un meccanismo di consenso Proof of Work (PoW) a Proof of Stake (PoS) con Ethereum 2.0, che mira a migliorare l'efficienza e la scalabilità della rete.

In sintesi, Ethereum è una **piattaforma blockchain** che ha introdotto molte innovazioni nel campo della **decentralizzazione e delle applicazioni decentralizzate**, consentendo agli sviluppatori di creare una vasta gamma di applicazioni e servizi decentralizzati.

Validatori

Nei sistemi blockchain basati su Proof of Stake (PoS), come Ethereum 2.0, i **validatori sono nodi che partecipano al processo di convalida delle transazioni e al consenso della rete**. Ecco una spiegazione più dettagliata su cosa fanno e come funzionano i validatori:

1. ****Convalida delle transazioni****: I validatori sono incaricati di **verificare la validità delle transazioni** inviate alla rete. Controllano se le transazioni sono formattate correttamente, se le firme digitali sono valide e se gli account che effettuano le transazioni hanno abbastanza fondi per coprirle.
2. ****Creazione di nuovi blocchi****: In molti sistemi PoS, **i validatori sono anche responsabili della creazione di nuovi blocchi sulla blockchain**. Questo avviene in un processo noto come "slotting". I validatori competono per ottenere il diritto di creare un nuovo blocco, che viene assegnato casualmente o in base a fattori come il saldo di criptovaluta che hanno bloccato come garanzia.
3. ****Staking****: I validatori **devono "mettere in gioco" una certa quantità di criptovaluta come garanzia per partecipare al processo di convalida e al consenso**. Questo serve a disincentivare comportamenti dannosi o fraudolenti, in quanto i validatori rischiano di perdere la loro criptovaluta se violano le regole del sistema.
4. ****Ricompense e sanzioni****: I validatori ricevono ricompense per il loro ruolo nella sicurezza e nella gestione della rete. Queste ricompense possono consistere in nuove unità di criptovaluta emesse come incentivo per la partecipazione al sistema. Allo stesso tempo, i validatori possono essere soggetti a sanzioni se violano le regole del sistema o se non eseguono correttamente i loro compiti.
5. ****Partecipazione al consenso****: I validatori partecipano al **processo di consenso della blockchain**, che determina l'ordine e la validità delle transazioni e dei nuovi blocchi aggiunti alla catena. In sistemi come Ethereum 2.0, il consenso può essere raggiunto attraverso un meccanismo di consenso chiamato Proof of Stake.

Complessivamente, i validatori sono **essenziali per il funzionamento sicuro e affidabile dei sistemi blockchain PoS**, poiché contribuiscono alla convalida delle transazioni, alla creazione di nuovi blocchi e alla sicurezza complessiva della rete.

Smart Contract

Gli "smart contract" (contratti intelligenti) sono **programmi computerizzati** che eseguono **automaticamente e autonomamente le istruzioni** definite al loro interno quando vengono **soddisfatte determinate condizioni**. Sono tipicamente eseguiti su una blockchain, come Ethereum, e sono progettati per automatizzare e facilitare una vasta gamma di operazioni e transazioni senza la necessità di intermediari.

Ecco alcune caratteristiche chiave degli smart contract:

1. ****Autonomia****: Gli smart contract **operano in modo autonomo una volta attivati e non richiedono intervento umano per eseguire le loro funzioni**. Ciò li rende particolarmente adatti per l'esecuzione di operazioni e transazioni in un ambiente decentralizzato come una blockchain.
2. ****Autenticità e Immutabilità****: Una volta che un smart contract è stato pubblicato su una blockchain, **diventa immutabile e sicuro**. Le informazioni e le istruzioni all'interno di uno smart contract sono crittografate e registrate sulla blockchain, garantendo l'autenticità e l'integrità del contratto.
3. ****Consenso****: Gli smart contract vengono **eseguiti e verificati dalla rete di nodi della blockchain**, che raggiunge un consenso sullo stato e sull'esecuzione dei contratti. Ciò garantisce che tutti i partecipanti alla rete concordino sulle azioni eseguite dagli smart contract.
4. ****Versatilità****: Gli smart contract **possono essere utilizzati per una vasta gamma di applicazioni**, tra cui pagamenti, scambi di asset digitali, gestione di identità digitale, sistemi di votazione e molto altro ancora. La loro flessibilità li rende uno strumento potente per la creazione di servizi e applicazioni decentralizzate.
5. ****Costi e Trasparenza****: Gli smart contract **riducono la necessità di intermediari** e le relative commissioni, poiché eseguono automaticamente le operazioni senza richiedere la supervisione umana. Inoltre, le operazioni eseguite dagli smart contract sono registrate in modo trasparente sulla blockchain, consentendo a tutti i partecipanti di verificare la loro esecuzione.

Complessivamente, gli smart contract sono **uno degli aspetti più innovativi delle blockchain**, poiché consentono la **creazione di servizi e applicazioni autonomi e decentralizzati**, riducendo la dipendenza da intermediari e aumentando l'efficienza e la trasparenza delle operazioni digitali.

Fee & Gas

Le "fee" e il "gas" sono concetti strettamente correlati nell'ambito di Ethereum e di altre blockchain. Ecco una spiegazione di entrambi:

1. ****Fee (Commissione)****:

Nel contesto di Ethereum, le fee rappresentano **la somma di denaro pagata dagli utenti per l'esecuzione di transazioni sulla rete Ethereum**. Queste commissioni vengono pagate ai miner della rete come incentivo per il lavoro svolto nel convalidare e includere le transazioni nei blocchi della blockchain Ethereum. Le fee variano a seconda della congestione della rete e della priorità assegnata dall'utente alla propria transazione. In genere, **maggiore è la fee, maggiore è la probabilità che la transazione venga elaborata più rapidamente**.

2. ****Gas****:

Il gas è un'unità di misura della **quantità di lavoro computazionale richiesta per eseguire operazioni su Ethereum**. Ogni operazione all'interno di una transazione (come l'esecuzione di un contratto intelligente o il trasferimento di fondi) richiede una certa quantità di gas per essere eseguita. Il costo totale di una transazione è **calcolato moltiplicando il prezzo del gas per l'uso di gas necessario per eseguire l'operazione**. Il prezzo del gas è espresso in piccoli incrementi di ether chiamati "gwei".

In breve, le **fee** sono il costo in ether pagato dagli utenti per eseguire transazioni su Ethereum, mentre il **gas** è l'unità di misura utilizzata per calcolare questo costo in base alla complessità e al consumo di risorse delle operazioni eseguite sulla blockchain Ethereum. Le fee vengono calcolate moltiplicando il prezzo del gas per l'uso di gas richiesto per eseguire una specifica operazione.

Inoltre è possibile anche creare dei limiti per il "gas", per evitare spiacevoli inconvenienti durante la creazione delle transazioni. E' una pratica utilizzata principalmente quando si invia una transazione ad uno smart contract, o per modificare un SC.

TestNets

Le testnet sono state create per consentire agli sviluppatori di creare applicazioni decentralizzate prima di distribuirle su blockchain principale. Nelle test Network è possibile ottenere eteri "fittizi". può essere utilizzato per la distribuzione del contratto e per pagare i costi relativi consumo di gas.

APP DECENTRALIZZATE

Le DApp, o applicazioni decentralizzate, sono **applicazioni software che operano su una rete peer-to-peer distribuita**, come una blockchain, anziché su server centralizzati. Queste applicazioni decentralizzate sono progettate per funzionare senza un'autorità centrale di controllo, **rendendole resistenti alla censura e alla manipolazione**.

Ecco alcune caratteristiche chiave delle DApp:

1. ****Decentralizzazione****: Le DApp sono costruite su una rete decentralizzata, **come Ethereum** o altre blockchain, che elimina la necessità di un'autorità centrale di controllo. **Le operazioni all'interno di una DApp sono eseguite da nodi della rete distribuita**, garantendo la trasparenza e l'immutabilità delle transazioni.
2. ****Smart Contract****: **Le DApp spesso utilizzano smart contract**, che sono contratti intelligenti eseguiti sulla blockchain e che regolano automaticamente le operazioni all'interno dell'applicazione. Questi smart contract consentono la creazione di protocolli di governance e regole che vengono eseguite in modo autonomo senza richiedere l'intervento umano.
3. ****Open Source****: Molte DApp sono open source, il che significa che **il loro codice sorgente è disponibile pubblicamente e può essere ispezionato**, modificato e distribuito liberamente da chiunque. Questa trasparenza favorisce la collaborazione e l'innovazione nella comunità degli sviluppatori.
4. ****Token Economy****: **Molte DApp utilizzano token digitali come mezzo di scambio o come incentivo per gli utenti che partecipano alle attività all'interno dell'applicazione**. Questi token possono essere utilizzati per pagare servizi, votare su decisioni di governance, o semplicemente come forma di ricompensa per il contributo degli utenti alla rete.
5. ****Interoperabilità****: Le DApp **possono interagire tra loro e con altri servizi decentralizzati**, consentendo agli utenti di combinare funzionalità da diverse fonti e creare soluzioni più complesse e innovative.

Le DApp possono essere utilizzate per una vasta gamma di scopi e applicazioni, tra cui servizi finanziari decentralizzati (DeFi), giochi blockchain, piattaforme di social media decentralizzate, mercati digitali e molto altro ancora. La loro natura decentralizzata e resiliente le rende un elemento chiave dell'ecosistema blockchain, fornendo soluzioni innovative e trasparenti per molte esigenze e settori.

Alla blockchain e ai contratti intelligenti è affidato il ruolo di gestione, verifica dei dati ed esecuzione delle funzioni che devono essere resi disponibili (e tracciabili), sicuri e incorruttibile.

WEB3

"Web3" è un termine utilizzato per riferirsi alla visione di un'Internet decentralizzata e basata su blockchain, in contrapposizione al concetto di "Web2" che si riferisce all'attuale infrastruttura centralizzata dell'Internet dominata da grandi aziende tecnologiche.

Web3 mira a creare un ecosistema Internet in cui le transazioni finanziarie, l'identità digitale, le applicazioni e i dati sono gestiti attraverso protocolli decentralizzati e blockchain anziché da intermediari centrali. Questo promuove la trasparenza, la sicurezza e l'autonomia degli utenti, riducendo la dipendenza da aziende centrali e consentendo una maggiore proprietà e controllo dei propri dati e delle proprie risorse digitali.

Alcuni dei principali componenti e concetti associati a Web3 includono:

1. ****Blockchain****: Le blockchain fungono da fondamento tecnologico per Web3, fornendo una rete decentralizzata su cui sono basate le applicazioni e le transazioni.
2. ****Smart Contract****: Gli smart contract, contratti intelligenti eseguiti su blockchain, consentono l'automazione di transazioni e accordi senza la necessità di intermediari.
3. ****Criptovalute e Token****: Le criptovalute e i token digitali sono utilizzati come mezzi di scambio e incentivi all'interno delle applicazioni e dell'ecosistema Web3.
4. ****Identità Digitale Decentralizzata (DID)****: Le identità digitali decentralizzate consentono agli utenti di controllare e gestire in modo sicuro la propria identità online senza affidarsi a entità centrali.
5. ****Applicazioni Decentralizzate (DApp)****: Le DApp sono applicazioni che funzionano su blockchain e che spesso incorporano gli smart contract. Consentono agli utenti di interagire in modo diretto e peer-to-peer senza intermediari centrali.

In sintesi, Web3 rappresenta una visione di Internet decentralizzata, basata su blockchain e protocolli decentralizzati, che promuove l'autonomia, la trasparenza e la sicurezza degli utenti.

TOKEN

I "token" sono rappresentazioni digitali di valore, spesso utilizzati all'interno di blockchain o di reti decentralizzate. Possono rappresentare una vasta gamma di asset, diritti o utilità, e vengono registrati su una blockchain per garantirne l'autenticità e la trasferibilità.

Un "utility token" è un tipo specifico di token che **conferisce agli utenti il diritto di accedere a determinati prodotti o servizi all'interno di una piattaforma o di una rete**. Questi token hanno un'utilità intrinseca all'interno dell'ecosistema che li ha emessi, e vengono spesso utilizzati per pagare le transazioni o accedere a funzionalità avanzate all'interno di una DApp (applicazione decentralizzata) o di una piattaforma blockchain.

Ad esempio, all'interno di una piattaforma di gioco blockchain, un utility token potrebbe essere utilizzato per acquistare oggetti virtuali, sbloccare livelli avanzati o accedere a funzionalità premium. In un'altra applicazione, un utility token potrebbe essere utilizzato per pagare per l'accesso a servizi di archiviazione cloud decentralizzati o per partecipare a sistemi di voto o di governance all'interno di una DAO (organizzazione autonoma decentralizzata).

In breve, mentre i token rappresentano in generale un valore digitale su una blockchain, i utility token hanno **un'utilità specifica all'interno di una piattaforma o di un ecosistema**, conferendo ai titolari il diritto di accedere a servizi, funzionalità o privilegi specifici all'interno di quella piattaforma o rete.

- I **token ERC-20** sono un tipo di **token standardizzato che si basa sulla blockchain di Ethereum**. Questo standard è stato introdotto per facilitare la creazione e l'interoperabilità di token su Ethereum, consentendo agli sviluppatori di creare facilmente token che possono essere scambiati, trasferiti e utilizzati all'interno dell'ecosistema Ethereum. Ecco alcune caratteristiche chiave dei token ERC-20:

- 1. ****Standardizzazione****: Il protocollo ERC-20 definisce un **set di regole e standard per la creazione di token su Ethereum**. Ciò consente agli sviluppatori di seguire un formato comune per la creazione e la gestione dei token, garantendo l'interoperabilità e la compatibilità tra diverse applicazioni e servizi.
- 2. ****Interoperabilità****: I token **ERC-20 sono compatibili con la maggior parte delle piattaforme e degli scambi che supportano Ethereum**. Ciò significa che possono essere facilmente scambiati, trasferiti e utilizzati su una varietà di servizi e applicazioni che supportano Ethereum.
- 3. ****Funzionalità****: I token ERC-20 **possono rappresentare una vasta gamma di asset digitali, come valute, azioni, token di utilità e altro ancora**. Possono essere utilizzati per pagamenti, scambi, votazioni e altre funzionalità all'interno di applicazioni decentralizzate (DApp) e di servizi su Ethereum.
- 4. ****Transazioni****: Le transazioni con i token ERC-20 avvengono sulla blockchain di Ethereum, utilizzando la stessa infrastruttura e le stesse funzionalità delle transazioni di Ether (ETH). Questo **garantisce che le transazioni siano sicure, trasparenti e tracciabili**.

In sintesi, i token ERC-20 sono un tipo di token standardizzato e interoperabile su Ethereum, che consente agli sviluppatori di creare facilmente e gestire token all'interno dell'ecosistema Ethereum. Questi token hanno una vasta gamma di usi e possono essere scambiati e utilizzati su una varietà di piattaforme e servizi che supportano Ethereum.

NFTs

Gli NFT (Non-Fungible Tokens) sono rappresentazioni digitali uniche e indivisibili di asset digitali, registrate su una blockchain. Contrariamente alle criptovalute fungibili come Bitcoin o Ethereum, che sono intercambiabili tra loro in modo equivalente, gli NFT sono unici e non possono essere sostituiti con altri token. Gli NFT possono rappresentare una vasta gamma di asset digitali, inclusi arte digitale, collezionabili virtuali, musica, video, giochi e altro ancora.