



Introduzione a Ethereum

Giugno 2023



WisdomTree.eu
+44 (0) 207 448 4330

L'ether è la seconda criptovaluta per capitalizzazione dopo il bitcoin. La sua attuale capitalizzazione di mercato è pari a 223 miliardi di dollari, che corrispondono all'incirca al 18% del mercato complessivo delle criptovalute¹.

Ideata nel 2013 e creata nel 2015, la rete blockchain Ethereum è cresciuta in termini di innovazione e utilità. Contrariamente alla funzione primaria del bitcoin, ovvero un sistema di moneta elettronica peer to peer e un asset anti-fiat (che potrebbe fungere da copertura qualora si manifestasse un'altra crisi del settore bancario), Ethereum sviluppa un nuovo mondo di applicazioni peer to peer.

Prima di entrare nei dettagli, è importante distinguere l'ether (ETH) da Ethereum. "Ether" si riferisce alla criptovaluta utilizzata sulla blockchain di Ethereum. "Ethereum" si riferisce alla rete blockchain.

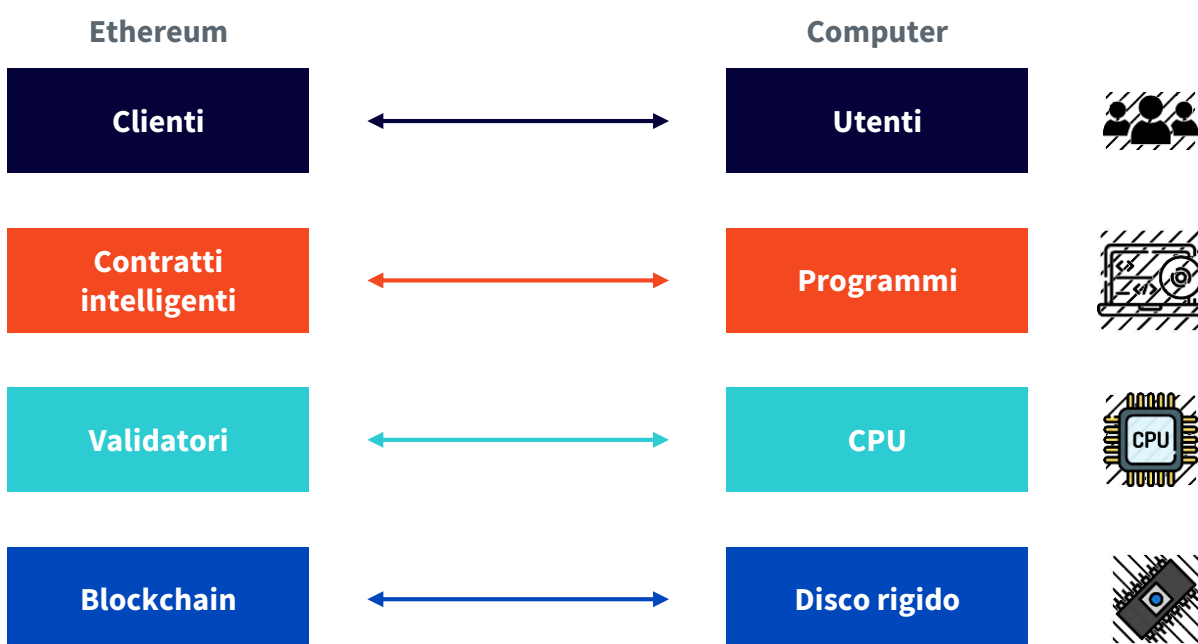
Che cos'è Ethereum?

È una blockchain modulare e programmabile che gestisce applicazioni senza affidarsi a una parte centralizzata.

La piattaforma si fonda sulla tecnologia blockchain pubblica, open source, decentralizzata e crittografica. Alimenta applicazioni decentralizzate (dApps) rese possibili da "contratti intelligenti".

Grazie alla sua potenza di calcolo aggregata sulla rete distribuita (la macchina virtuale Ethereum), Ethereum esegue transazioni peer to peer per realizzare trasferimenti automatici e condizionali di valori e informazioni, tra cui denaro, diritti di voto e proprietà.

Ethereum può essere paragonato a un "computer mondiale" su una blockchain; la tecnologia blockchain sottostante è il disco rigido della macchina virtuale, i contratti intelligenti sono i programmi, i validatori² sono l'unità di elaborazione centrale (CPU) e gli utenti pagano in ETH per utilizzare tale "computer".



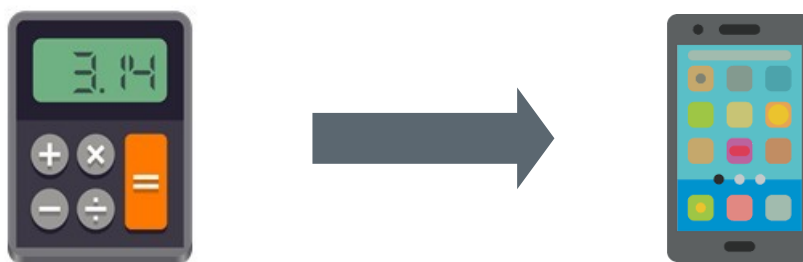
1. CoinGecko, 24 aprile 2023.

2. Un validatore è un partecipante a una blockchain proof of stake responsabile di convalidare le nuove transazioni e di mantenere la sicurezza della rete.

Risolvere il problema

L'invenzione di Ethereum si ispira al bitcoin.

Il bitcoin ha gettato le basi della tecnologia blockchain decentralizzata, ma le sue funzionalità si limitavano ai trasferimenti di moneta elettronica peer to peer. Ethereum espande le funzionalità del bitcoin alle applicazioni programmabili. In sostanza, Ethereum mira a creare una rete decentralizzata per eseguire varie applicazioni. Per dirla con la metafora del suo inventore, Vitalik Buterin: "Il bitcoin è come una calcolatrice, ma Ethereum vuole diventare uno smartphone che esegue tante applicazioni"³.



Questa rete decentralizzata automatizza le decisioni e le transazioni, affidandosi meno a una parte centrale di fiducia. Riduce la necessità di intermediari, i costi di arbitrato, le frodi e gli errori.

Come funziona Ethereum?

Contratti intelligenti

Il fulcro di Ethereum è costituito dai contratti intelligenti.

I contratti intelligenti sono pezzi di codice o programmi che dicono alla blockchain cosa fare. Nick Szabo, lo sviluppatore che li ha ideati, ha spesso paragonato i contratti intelligenti ai codici dei distributori automatici.

Un contratto intelligente viene eseguito quando attivato da una transazione. Nell'esempio del distributore automatico, il contratto intelligente viene attivato quando un utente inserisce una moneta. Una volta attivato, l'azione viene eseguita in base alle condizioni "se... allora..." incorporate nel suo codice.

Allo stesso modo, premendo una combinazione di tasti su un distributore automatico si ottiene una bottiglia d'acqua. Il prodotto specifico che viene erogato dal distributore automatico è il risultato del contratto intelligente. Sulla rete Ethereum, l'equivalente potrebbe essere un trasferimento di valore di ETH a un altro conto o una transazione che innesca un altro contratto intelligente.

Un contratto intelligente osserva una serie predefinita di norme che permettono di eseguire automaticamente il codice allo stesso modo su ciascun nodo della rete Ethereum. Così si evita che un terzo debba occuparsi dell'esecuzione del codice per conto degli utenti, decentralizzando il sistema. Il sistema consente ai programmatori di creare una vasta gamma di applicazioni che costituiscono diversi contratti intelligenti.

3. Vitalik ha utilizzato questa metafora nel discorso tenuto il 10 ottobre 2016, "Ethereum in 25 Minutes".

In un'applicazione decentralizzata in ambito assicurativo, ad esempio, i membri possono acquistare polizze direttamente sull'applicazione con il token nativo della rete. Quindi, viene istituita una riserva di denaro in cui sono aggregati i premi assicurativi di tutti i membri. Quando si verifica un sinistro, i membri interessati vengono risarciti senza dover seguire la complessa procedura tradizionale di rimborso prevista dal settore assicurativo. Un'assicurazione per i raccolti, ad esempio, pagherà automaticamente il risarcimento nel caso in cui le agenzie governative segnalino siccità o alluvioni nella zona dell'assicurato.

Gas

Per facilitare le transazioni e l'esecuzione dei contratti intelligenti è necessario pagare delle commissioni in ETH ai validatori. Tali commissioni sono chiamate "gas". Il prezzo del gas è spesso una piccola frazione di ETH, indicata in Gwei (109 Gwei = 1 ETH).

Il gas è essenziale per sostenere la rete Ethereum. Incentiva i validatori a eseguire lo staking dei loro ETH, ad aiutare nell'elaborazione e nella verifica delle transazioni e a proteggere la blockchain di Ethereum in cambio di una ricompensa monetaria. La quantità di gas necessaria per una transazione dipende dal livello di congestione della rete al momento della stessa, dalla domanda riguardante la convalida delle transazioni e dal numero di validatori che partecipano al processo. Quando la rete è congestionata e la domanda riguardante la convalida delle transazioni è elevata, anche il prezzo del gas lo sarà e viceversa. L'aggiornamento previsto, che implementa il proto-danksharding⁴, dovrebbe alleviare la congestione della rete di Ethereum.

Applicazioni

Le applicazioni di Ethereum sfruttano la natura decentralizzata e immutabile della tecnologia blockchain. Chiunque può creare e dare il proprio contributo a codice e applicazioni senza incidere sulla sicurezza del sistema. Le loro funzioni variano ampiamente. Di seguito sono riportati alcuni esempi importanti:

- + **Finanza decentralizzata (DeFi):** la DeFi mira a costruire un sistema finanziario aperto e globale accessibile a chiunque abbia una connessione a Internet. A differenza dell'industria finanziaria tradizionale, basata sulla fiducia e centralizzata, la fiducia necessaria per la DeFi è ridotta al minimo, quindi il funzionamento del sistema non si basa su una singola entità, ma è di proprietà degli utenti. Questa struttura decentralizzata permette a chiunque di accedere alla rete su richiesta. La rete è inoltre trasparente, più veloce ed economica rispetto al sistema centralizzato basato sulla fiducia. La rete decentralizzata mette in contatto domanda e offerta peer to peer, eliminando la necessità di intermediari. Gli utenti possono prendere e dare in prestito, investire, scambiare, ottenere interessi, acquistare assicurazioni e trasferire denaro in modo decentralizzato.
- + **Organizzazioni autonome decentralizzate (DAO):** per "DAO" si intende un'organizzazione che non dipende da una parte terza, creata per raggiungere un obiettivo comune. Tale organizzazione opera e collabora attraverso un protocollo condiviso, definito e automatizzato per garantire che tutti i membri del gruppo siano ascoltati e che il processo decisionale sia trasparente. Ogni DAO ha una tesoreria integrata in cui vengono conservati i fondi, poi spesi in base alle votazioni dei membri.

4. Il proto-danksharding è un modo per aumentare la scalabilità di Ethereum così da poter gestire un maggior numero di transazioni a un costo inferiore, utilizzando soluzioni layer 2.

Uno dei primi esempi di DAO è un fondo di venture capital decentralizzato chiamato "The DAO". Lanciata nel 2016, i membri potevano acquistare i token DAO per ottenere il diritto di voto sulle proposte di investimento. Se un progetto diventava redditizio, i membri ottenevano un rendimento proporzionale alle loro quote. Pur essendo un'idea innovativa, la DAO è fallita a causa di un bug nel codice del contratto intelligente che ha permesso agli hacker di rubare una parte dei fondi. Questo ha portato alla decisione di implementare un hard fork sulla rete di Ethereum, creando un ramo chiamato Ethereum Classic. Altri esempi di DAO hanno continuato a operare con successo, come MakerDAO che permette di generare Dai, una stablecoin decentralizzata.

- + **Token non fungibili (NFT):** gli NFT sono dati registrati sulla blockchain che rendono gli asset sottostanti immutabili e differenziati. Si va dai beni digitali, come foto, audio, video, azioni e certificati, ai beni fisici, come immobili e dipinti.

Poiché i file digitali sono facili da replicare, è importante avere un token non fungibile che ne dimostri la proprietà. Quando si acquista un NFT, il proprietario ottiene un documento di proprietà immutabile. Gli NFT sono particolarmente interessanti per gli asset digitali, in quanto creano un senso di scarsità, migliorando il valore collezionistico dello stesso. Agli artisti che vendono asset, gli NFT consentono la distribuzione diretta del proprio lavoro senza una piattaforma di terzi, permettendo di proteggere meglio i propri diritti d'autore e di aumentare significativamente i profitti.

Per quanto riguarda gli NFT coperti da asset fisici, la tokenizzazione fornisce la prova della proprietà digitale e preserva l'unicità degli oggetti. La tokenizzazione di asset fisici del mondo reale è diventata sempre più popolare a partire dalla fine del 2022.

Qual è il futuro di Ethereum?

La caratteristica principale della blockchain di Ethereum è il suo costante aggiornamento e il suo continuo sviluppo.

Nel settembre 2022, Ethereum è passata dal meccanismo di consenso proof of work a quello proof of stake, con un aggiornamento noto come "The Merge". Questo ha cambiato il modo in cui le transazioni vengono elaborate e convalidate e il metodo di protezione della rete di Ethereum. Sebbene la Beacon Chain⁵ proof of stake sia stata originariamente introdotta nel dicembre 2020, non è stato possibile ritirare gli ETH in staking o le ricompense accumulate fino ad aprile 2023.

Uno dei principali vantaggi del passaggio al meccanismo proof of stake è stato il significativo risparmio energetico che la rete ha ottenuto. Invece di affidarsi a miner con apparecchiature ad alto consumo energetico per risolvere complessi problemi matematici, i validatori bloccano i loro token ETH in un contratto intelligente per convalidare le transazioni e proteggere la rete, ricevendo nuovi token ETH come ricompensa.

Il prossimo importante miglioramento di Ethereum aumenterà la capacità della rete. Invece di implementare lo "sharding", dividendo la rete in "shard" più piccoli e aumentando così lo spazio, l'attenzione degli sviluppatori sembra concentrarsi sul proto-danksharding, che mira a migliorare la capacità lavorando con soluzioni di scalabilità di tipo layer 2.

5. La Beacon Chain è la blockchain proof of stake originale che ha funzionato in parallelo alla blockchain proof of work fino The Merge.

Le reti di scalabilità layer 2 spostano un gruppo di transazioni off-chain, ne effettuano il roll up e le raggruppano nuovamente in un'unica transazione, che viene protetta sulla blockchain layer 1, sfruttando la sua robustezza e sicurezza. Questo processo comporta la maggior parte del costo delle soluzioni di scalabilità layer 2, ma è essenziale per ricostruire le transazioni sulla blockchain di base se si verifica un problema sulla layer 2.

Per concludere, gli sviluppatori stanno lavorando a una soluzione che prevede un aumento temporaneo dell'archiviazione dei dati per le reti layer 2 su Ethereum. In questo modo, la rete potrebbe gestire un maggior numero di transazioni a una frazione del costo della struttura attuale.

Conclusione

La rete Ethereum è una blockchain decentralizzata, modulare e programmabile. Continua a essere la piattaforma di contratti intelligenti più adottata dagli sviluppatori di app. La blockchain continua a evolversi e aggiornarsi e offre una piattaforma interessante per creare applicazioni decentralizzate, eliminare le controparti centralizzate e fornire soluzioni più veloci e convenienti per le applicazioni finanziarie del futuro.

Informazioni importanti

Comunicazioni di marketing emesse all'interno dello Spazio economico europeo ("SEE"): Il presente documento è stato emesso e approvato da WisdomTree Ireland Limited, società autorizzata e regolamentata dalla Central Bank of Ireland.

Comunicazioni di marketing emesse in giurisdizioni non appartenenti al SEE: Il presente documento è stato emesso e approvato da WisdomTree UK Limited, società autorizzata e regolamentata dalla Financial Conduct Authority del Regno Unito.

Per fare riferimento a WisdomTree Ireland Limited e a WisdomTree UK Limited si utilizza per entrambe la denominazione "WisdomTree" (come applicabile). La nostra politica sui conflitti d'interesse e il nostro inventario sono disponibili su richiesta.

Solo per clienti professionali. Le informazioni contenute nel presente documento sono fornite a titolo meramente informativo e non costituiscono né un'offerta di vendita né una sollecitazione di un'offerta di acquisto di titoli o azioni. Il presente documento non deve essere utilizzato come base per una qualsiasi decisione d'investimento. Gli investimenti possono aumentare o diminuire di valore e si può perdere una parte o la totalità dell'importo investito. Le performance passate non sono necessariamente indicative di performance future. Qualsiasi decisione d'investimento deve essere basata sulle informazioni contenute nel Prospetto informativo di riferimento e deve essere presa dopo aver richiesto il parere di un consulente d'investimento, fiscale e legale indipendente.

L'applicazione di regolamenti e leggi fiscali può spesso portare a una serie di interpretazioni diverse. Eventuali punti di vista o opinioni espresse in questa comunicazione rappresentano le opinioni di WisdomTree e non devono essere interpretate come consulenza normativa, fiscale o legale. WisdomTree non fornisce alcuna garanzia o dichiarazione circa l'accuratezza di qualsiasi punto di vista o opinione espressa in questa comunicazione. Qualsiasi decisione di investimento dovrebbe essere basata sulle informazioni contenute nel prospetto appropriato e dopo aver richiesto una consulenza finanziaria, fiscale e legale indipendente.

Il presente documento non è, e in nessun caso deve essere interpretato come, una pubblicità o qualsiasi altro strumento di promozione di un'offerta pubblica di azioni o titoli negli Stati Uniti o in qualsiasi provincia o territorio degli Stati Uniti. Né il presente documento né alcuna copia dello stesso devono essere acquisiti, trasmessi o distribuiti (direttamente o indirettamente) negli Stati Uniti.

Benché WisdomTree si adoperi per garantire l'esattezza del contenuto del presente documento, WisdomTree non garantisce né assicura la sua esattezza o correttezza. Qualsiasi terzo fornitore di dati di cui ci si avvalga per reperire le informazioni contenute nel presente documento non rilascia alcuna garanzia o dichiarazione di sorta in relazione ai suddetti dati. Laddove WisdomTree abbia espresso dei pareri relativamente al prodotto o all'attività di mercato, si ricorda che tali pareri possono cambiare. Né WisdomTree, né alcuna consociata, né alcuno dei rispettivi funzionari, amministratori, partner o dipendenti, accetta alcuna responsabilità per qualsiasi perdita, diretta o indiretta, derivante dall'utilizzo del presente documento o del suo contenuto.

Le criptovalute sono un investimento ad alto rischio e potrebbero non essere adatte a tutti i tipi di investitori. Le criptovalute possono dimostrare una volatilità maggiore rispetto ad altre classi di attività.