Terminologia delle Criptovalute

Glossario Veloce

www.AssistenzaCriptovalute.it

Assistenza Criptovalute

Risorse Gratutite

Terminologia Delle Criptovalute

Glossario Veloce

di AssistenzaCriptovalute.it

Terminologia Delle Criptovalute

Questo glossario vuole essere un utile riferimento per familiarizzare rapidamente con i concetti fondamentali.
Ogni voce è collegata a una pagina di approfondimento.

Criptovaluta (Cryptocurrency): le criptomonete sono, come dice il nome, valute crittografate. Si tratta di risorse digitali, dislocate su una rete decentralizzata di computer, e quindi non soggette al controllo di alcuna autorità centrale. Esistono sotto forma di unità crittografiche create in blocchi, registrate in uno speciale database chiamato blockchain e gestite attraverso un consenso distribuito.

Crittografia: è la disciplina che tratta le tecniche di trasformazione di testi inizialmente leggibili in stringhe incomprensibili, mediante l'uso di algoritmi (cifratura). Usando la procedura inversa queste possono essere ricondotte al contenuto originario. E' alla base della sicurezza informatica e della protezione di dati riservati. Le criptovalute di basano sulla crittografia asimmetrica che fa uso di chiavi pubbliche e private.

Blockchain: La 'catena di blocchi' è un registro (ledger) digitale condiviso da una rete di partecipanti che, essendo distribuito in più copie costituite da blocchi immutabili, consente di registrare informazioni sicure tra le parti coinvolte garantendone l'autenticità in maniera decentralizzata (ossia tramite il meccanismo del consenso distribuito e senza l'intervento di un'autorità centrale).
I dati registrati nei blocchi includono tutte le attività che avvengono in rete (transazioni, contratti, trasferimenti).
La tecnologia, nata con Bitcoin e basata sulla crittografia, ha poi trovato applicazione in migliaia di altri progetti e nei più svariati settori, grazie all'indipendenza e trasparenza del processo di verifica.
Ci si riferisce alla blockchain, intesa come piattaforma, chiamandola anche rete o network.

Decentralizzazione: è la proprietà di un qualsiasi sistema nel quale le parti coinvolte collaborano in maniera distribuita per ottenere un obiettivo comune, mediante un meccanismo di consenso che consente la rappresentatività e l'autonomia.
Inoltre, non essendo soggette a controllo centralizzato, queste infrastrutture non hanno un singolo punto di vulnerabilità e sono quindi pressoché inattaccabili.

Bitcoin: è una valuta digitale decentralizzata ed è la prima criptovaluta, creata da Satoshi Nakamoto nel 2009. E' un sistema di pagamento, riserva e scambio di valore che funziona in maniera autonoma, su una sua rete peer-to-peer (da pari a pari), senza una banca centrale, senza intermediari, con transazioni sicure basate sulla tecnologia blockchain.

Altcoin: qualsiasi criptovaluta che non sia Bitcoin. Tutte, da Ethereum a Shiba Inu. Stando a CoinMarketCap attualmente ne esistono oltre 10.000.

Token: è una unità di valore digitale, progettata per avere una sua utilità. Sebbene ogni criptovaluta possa essere considerata un token, con questo termine, che testualmente significa gettone, si intende più comunemente una cripto che non ha una propria blockchain ma esiste su una blockchain di appoggio.
Il caso più comune è quello delle migliaia di ERC-20 tokens, criptovalute create su Ethereum usando il protocollo standard ERC-20.

Ticker Symbol (simbolo azionario): è la sigla, tipicamente una combinazione di tre lettere, che viene usata per codificare il nome di una criptovaluta e renderla riconoscibile sugli exchange o altre piattaforme di scambio. Ad esempio BTC per Bitcoin, ETH per Ethereum, ADA per Cardano.

Portafoglio (Wallet): è il dispositivo che, conservando le chiavi pubbliche e private, permette di accedere e interagire con le proprie criptovalute per spedirle, riceverle, scambiarle e in alcuni casi firmare non solo transazioni ma anche contratti.
Esistono portafogli software, hardware, online, per desktop, per smartphone, e addirittura cartacei. Alcuni sono dedicati a una sola cripto, mentre la maggior parte consente di gestire una moltitudine di monete diverse.

Frase Seme (Seed Phrase): anche chiamata recovery phrase o frase mnemonica, è una serie di 12 o 24 parole scelte da una lista di 2048 termini inglesi. Viene generata nel momento in cui si crea un portafoglio ed è il mezzo di accesso ai propri fondi, in quanto rappresenta tutte le chiavi pubbliche e private conservate nel portafoglio.
E' l'elemento più prezioso nella gestione delle proprie criptovalute perché perderla equivale a non poter in alcun modo recuperare le nostre monete.

Indirizzi: sono le stringhe di lettere e numeri, fornite dai wallet in formati specifici per ogni criptovaluta, derivate dalle chiavi pubbliche in versione abbreviata e più pratica. Possono essere pensati come username, tranquillamente condivisibili. Ognuno di questi è l'equivalente di un IBAN a cui ricevere o dal quale inviare denaro.

Chiavi Pubbliche: sono la versione estesa degli indirizzi, che il wallet usa dietro le quinte in abbinamento alle chiavi private per condurre e validare transazioni.

Chiavi Private: sono i codici personali e segreti che permettono di accedere ai fondi depositati a un certo indirizzo. E' come se fossero password necessarie a validare le nostre transazioni.
Essendo costituite da lunghe e complesse serie di numeri e lettere, una per ogni criptovaluta e corrispondente chiave pubblica, per facilitarne la custodia i portafogli codificano le chiavi private in una frase di 12 o 24 parole inglesi, la Seed Phrase.

Exchange: sono le aziende che consentono ai propri clienti di comprare e vendere criptovalute usando euro o altre monete tradizionali, e inoltre di scambiare diverse criptovalute tra loro.
A differenza di normali piattaforme di scambio di altri beni, o della Borsa, sono attivi 24 ore al giorno, 7 giorni alla settimana.

2FA (Two Factor Authentication): l'autenticazione a due fattori è un sistema di riconoscimento basato sull'utilizzo di due diversi metodi di verifica dell'identità di un utente che accede a una piattaforma o software, per garantire una maggiore sicurezza. Viene usato sia dagli exchange che da alcuni wallet.

KYC (Know Your Customer): letteralmente 'conosci il tuo cliente', è un insieme di procedure utilizzate per acquisire dati certi e informazioni sull'identità di utenti e clienti, applicate per obbligo di legge da alcuni professionisti e istituti, tra cui gli exchange di criptovalute.

Portafoglio Custodial e Non-Custodial: i portafogli custodial sono detenuti dall'exchange presso cui abbiamo acquistato le criptovalute. Questo significa che noi non abbiamo le chiavi private ma solo le password di accesso al nostro conto sull'exchange, che tecnicamente rimane il proprietario delle nostre cripto.
Nel caso dei wallet non-custodial invece abbiamo noi le chiavi private e quindi le criptovalute sono effettivamente in nostro possesso.
Affidarsi a una terza parte riduce la sicurezza ma anche le responsabilità, e per questo è una soluzione che alcuni preferiscono.

Fees: sono i vari costi che gli exchange fanno pagare per i depositi, le negoziazioni e i prelievi. Le trading fees sono le commissioni sulle operazioni di acquisto e vendita. Le withdrawal fees sono le commissioni sui prelievi. I depositi di solito sono a pagamento solo se avvengono con carta di credito anziché bonifico.

Transaction Fees: sono le quote che vengono accreditate ai miners come ricompensa per la conferma di una transazione sulla blockchain. Sulla blockchain di Ethereum queste commissioni sono chiamate 'gas fees', e sono misurate in Gwei, una piccola somma equivalente a un miliardesimo di ETH.

Mining: letteralmente 'estrazione', è il processo mediante il quale criptovalute come Bitcoin, Dogecoin, Monero, e Litecoin vengono create. Viene svolto dai miners, che mettono a disposizione del network la propria potenza di calcolo in cambio di una ricompensa in nuove monete.

Miners: i 'minatori' sono coloro i quali verificano le transazioni e partecipano alla creazione di nuovi blocchi nella blockchain, mediante la risoluzione di complessi problemi matematici con potenti calcolatori.
Il loro sforzo viene remunerato in due modi: con le transaction fees, e con le nuove monete estratte.

Network: è la rete di nodi (computer dedicati) che partecipano alla decentralizzazione, sicurezza e gestione di una blockchain. Ogni nodo possiede una copia costantemente aggiornata dell'intera blockchain.

Peer to Peer: letteralmente 'da pari a pari', si riferisce alle interazioni tra le varie parti di un network distribuito, che si dividono i compiti e il carico di lavoro. E' una struttura che può essere usata per scambi decentralizzati di qualsiasi tipo, dai file alle criptovalute.

Smart Contracts: sono protocolli software automatizzati che permettono di eseguire, convalidare e far rispettare contratti sulla blockchain, al verificarsi di determinate condizioni, senza l'intervento di terze parti.

Proof of Work: letteralmente 'dimostrazione di lavoro' è l'algoritmo di consenso sviluppato per le prime blockchain, inclusa quella di Bitcoin. E' fondamentale per la sicurezza del network, e consiste in un meccanismo che premia i miners che per primi forniscono la soluzione di complessi puzzle matematici, facendogli validare transazioni e aggiungere blocchi.

Proof of Stake: traducibile con 'dimostrazione di rischio' o, più precisamente, 'prova che si ha un interesse in gioco', è uno dei più usati meccanismi di consenso su blockchain. Si distingue per un consumo energetico molto contenuto.
In questo caso invece dei miners abbiamo i 'validators', che convalidano transazioni e creano nuovi blocchi provando di avere a disposizione una certa quota della criptovaluta in questione.

Staking: è un processo che consente ai possessori di alcune criptovalute di guadagnare ricompense sotto forma di interessi, accreditati automaticamente al proprio indirizzo a scadenze periodiche prestabilite, in base al programma/condizioni cui si aderisce.
E' una delle opportunità di guadagno con le criptovalute, in aggiunta a quelli permessi dalle oscillazioni di prezzo.

DeFi: pronunciato 'di-fai', è l'abbreviazione di Decentralized Finance, il movimento che incoraggia lo sviluppo di servizi finanziari alternativi a quelli tradizionali, accessibili a tutti e indipendenti da controlli monopolistici di terze parti.

La finanza decentralizzata ha avuto un boom nel 2020 con decine di applicazioni sviluppate su Ethereum (ad esempio Uniswap) che grazie all'utilizzo di smart contracts consentono l'esecuzione automatica di prestiti e scambi, senza la necessità di un intermediario.

Dex: significa Decentralized Exchange, e si riferisce agli exchange peer to peer che consentono di comprare, vendere e scambiare criptovalute senza bisogno di un mediatore. Le transazioni avvengono direttamente tra gli utenti, i quali si interfacciano usando applicazioni che eseguono gli ordini mediante smart contracts.

CeFi: sta per Centralized Finance, ed è l'insieme dei servizi finanziari offerti sulle criptovalute da istituzioni che operano con strutture simili a quelle del sistema bancario tradizionale, gestite da aziende e persone, anziché puramente dalla tecnologia come avviene nella DeFi.
Alcuni esempi sono gli exchange come Binance e Coinbase o le piattaforme di prestito e interessi sui depositi come BlockFi e Nexo.

Yield Farming: significa 'coltivazione di un rendimento' ed è un processo che permette di far fruttare il proprio capitale mettendolo a disposizione come liquidità o prestandolo in mercati finanziari decentralizzati, ottenendo ricompense sotto forma di criptovaluta aggiuntiva.

DApps: significa Decentralized Applications, ovvero applicazioni che girano su una rete distribuita di computer anziché su un singolo server. Sono in grado di fornire le stesse prestazioni delle applicazioni tradizionali garantendo allo stesso tempo tutti i vantaggi della decentralizzazione, come ad esempio l'assenza di un unico punto di vulnerabilità, la resistenza alla censura e il non avere un proprietario.

NFT: è l'acronimo di Non Fungible Token, ovvero 'gettoni non fungibili'. Al contrario delle criptovalute tradizionali, per le quali ogni unità è identica all'altra, non sono reciprocamente intercambiabili perché ciascuno di essi rappresenta qualcosa di unico.
Possono essere usati come attestati digitali del possesso di un bene sottostante: da un'opera d'arte a un file digitale, dai diritti d'autore a qualsiasi diritto di proprietà.

Web 3.0: il Web 3.0, o Web3 è l'internet delle DApp, le applicazioni decentralizzate che troviamo nei network che supportano smart contract.
Esistono DApp dedicate ad esempio alla finanza decentralizzata (DeFi), al gaming e all'interazione con gli NFT.
Per poter essere usate richiedono portafogli specifici come MetaMask, in grado di navigare quest'ultima versione del web e gestire smart contract.

EVM: è l'acronimo di Ethereum Virtual Machine, la rete distribuita di computer su cui girano tutti i progetti realizzati su Ethereum. Esistono moltitudini di blockchain compatibili con questa piattaforma: in pratica condividono con Ethereum gran parte del codice e sono in grado di eseguire smart contract programmati nel suo stesso linguaggio.

DAO: è l'acronimo di Decentralized Autonomous Organization, ossia una organizzazione autonoma basata su regole definite da una rete di computer e governata da smart contract eseguiti su una blockchain, che garantiscono funzionalità, trasparenza e sicurezza senza bisogno di un'entità centrale che prenda decisioni.

Trader: è colui che opera a livello professionale con le criptovalute, effettuando compravendite a scadenze regolari, anche giornaliere, con l'obiettivo di trarre profitto dalle oscillazioni di prezzo.

Volatilità: consiste nelle improvvise e sostanziose oscillazioni di prezzo che caratterizzano certi mercati, tra cui quello delle criptovalute. Misura l'intensità delle variazioni in uno specifico periodo di tempo.

Liquidità: la più o meno facile possibilità di comprare o vendere una criptovaluta (o qualsiasi bene) trasformandola rapidamente nel suo corrispettivo valore in moneta tradizionale.
Uno strumento finanziario è tanto più liquido quanto sono minori i costi di transazione e veloci i tempi necessari per la conversione.

CBDC: la Central Bank Digital Currency è una moneta digitale basata sulla stessa tecnologia delle criptovalute ma emessa da una banca centrale che ne determina la politica monetaria. E' una soluzione già operativa in Cina da fine 2020 e in arrivo in tutto l'occidente, come risposta alla velocità di adozione di massa delle criptovalute.

Valute Fiat: le valute fiat (dal latino 'sia fatto') sono le monete a corso legale stabilite da ciascun paese (euro, dollaro, sterlina), prive di valore intrinseco in quanto non coperte da riserve auree o di altro tipo.
Il loro valore si basa unicamente sulla fiducia nell'autorità delle banche centrali che le emettono. Possono esistere in forma di banconote cartacee o essere rappresentate elettronicamente.

Stablecoin: le monete 'stabili' sono criptovalute caratterizzate da una volatilità estremamente bassa, grazie al fatto di essere ancorate a riserve con prezzi pressoché costanti come il dollaro americano o l'oro.
Sono per questo molto più adatte all'utilizzo quotidiano e rappresentano un ideale punto di incontro tra valute tradizionali e cripto.

Shitcoin: letteralmente 'moneta di m....', viene definita così una criptovaluta senza potenziale in quanto non ha alcuna utilità, non risolve alcun problema, e di conseguenza non ha nessun valore.

Memecoin: sono criptovalute basate su memi, idee che si diffondono rapidamente nella cultura di massa. Il loro valore scaturisce esclusivamente dal clamore della rapida adozione da parte di una comunità che esplode di colpo sui social media, finendo spesso per consumarsi nell'arco di poche settimane.

Airdrop: è una campagna di marketing che distribuisce gratuitamente una certa criptovaluta al pubblico che vuole parteciparvi, tipicamente come premio per il fatto di possederne un'altra correlata, oppure in cambio di iscrizioni/condivisioni sui social media.

Halving: letteralmente 'dimezzo' è il processo automatizzato a causa del quale la ricompensa che i miners ricevono per l'aggiunta di blocchi alla blockchain di Bitcoin viene dimezzata.
Avviene ogni 210.000 blocchi (circa 4 anni) e l'ultimo è stato a Maggio 2020.

Whale: letteralmente 'balena', è un termine che si riferisce a investitori che detengono enormi quantità di criptovalute, spesso acquistate quando costavano pochissimo, e che hanno abbastanza fondi da poter facilmente influenzare gli andamenti del mercato.

Swap: fare swapping significa scambiare istantaneamente una criptovaluta per un'altra in maniera decentralizzata e senza che queste lascino il proprio portafoglio, mediante apposite applicazioni come i Dex citati sopra o alcuni wallet che hanno questa funzione.

APY: è l'acronimo di Annual Percentage Yield, ovvero il numero che indica il rendimento percentuale annuo effettivo pagato a un prestatore o a chi fa staking, su un exchange o in un wallet.

Trustless: letteralmente significa 'senza fiducia' o 'che non richiede fiducia'. Si riferisce a una struttura che non necessita che le parti coinvolte si conoscano perché possano fidarsi l'una dell'altra.
E' uno dei capisaldi della blockchain e delle criptovalute, le quali, grazie alla loro natura distribuita e decentralizzata, non hanno bisogno di un'autorità esterna per garantire la sicurezza delle operazioni e la fiducia tra i vari soggetti.

White Paper: il 'libro bianco' è un manifesto, rilasciato dal team di una criptovaluta, col quale si informano i potenziali investitori riguardo i concetti, l'utilità, gli obiettivi, le scadenze e gli aspetti tecnici del progetto, prospettandone la crescita e il successo.
L'esempio perfetto è il White Paper con cui Satoshi Nakamoto ha presentato Bitcoin al mondo.

IoT: è l'acronimo di Internet of Things, l'Internet delle Cose, ovvero la rete globale di dispositivi, sensori e programmi interconnessi, che possono raccogliere e scambiarsi dati in tempo reale tramite internet.
Tutto ciò che chiamiamo mettendoci uno 'smart' davanti, ne fa parte.

Open Source: termine usato inizialmente in informatica per riferirsi a software non protetti da copyright e liberamente modificabili dagli utenti, è diventata una vera e propria filosofia dove i partecipanti credono nello scambio libero e gratuito di informazioni allo scopo di perseguire un bene comune più elevato.

Permissionless: letteralmente 'senza permesso' o 'che non richiede permesso', è un termine spesso usato per descrivere la blockchain, in quanto un sistema si può definire permissionless quando non c'è nessuno che può sta-

bilire chi e come ne può fare uso. Non tutte le blockchain sono permissionless come quelle delle criptovalute, con le quali chiunque può interagire senza autorizzazioni, senza registrarsi e senza doversi identificare.

QR Code: il codice QR (Quick Response, 'risposta rapida') è un'etichetta, leggibile da un computer, che mostra informazioni codificate in una matrice in bianco e nero.
Può essere scannerizzato rapidamente e usato per effettuare accessi, pagamenti, trasferimenti, e viene usato come modo alternativo di leggere gli indirizzi a cui inviare criptovalute.
Non bisogna mai scannerizzare un QR code su un sito/app non fidati.

FOMO: la Fear Of Missing Out è il timore di perdere un'occasione, l'emozione prevalente tra gli investitori durante le fasi di mercato in forte rialzo.

FUD: è l'acronimo di Fear Uncertainty and Doubt, la paura, incertezza e dubbio che dilagano tra gli investitori durante le fasi di mercato in ribasso.

Hodl: deriva dalla parola inglese 'hold', tenere, ed è entrato nello slang delle criptovalute a seguito del frequente errore d'ortografia commesso sul primo forum di Bitcoin.
Indica un approccio all'investimento basato sul conservare le monete a lunghissimo termine, a dispetto di qualunque condizione di mercato.
Da 'hodl' derivano poi i vari termini 'hodler' (colui che detiene), 'hodling' (detenere a lungo termine) e così via.

www.AssistenzaCriptovalute.it

DISCLAIMER:

I contenuti di AssistenzaCriptovalute.it hanno scopo didattico e sono semplici opinioni della redazione.

Il sito e i booklet liberamente scaricabili contengono materiale formativo, articoli, guide, informazioni e pareri relativi a criptovalute e assistenza tecnica delle stesse. Non includono strategie di investimento o di gestione del proprio portfolio. Non costituiscono quindi consulenza finanziaria o incentivo all'investimento. Il lettore si assume la piena responsabilità delle sue azioni.

Alcuni dei link esterni di AssistenzaCriptovalute.it sono connessi a programmi di affiliazione commerciale per sostenere l'operatività del Blog e delle risorse gratuite.

Le opinioni espresse sono del tutto indipendenti e basate esclusivamente su esperienza diretta e accurata selezione dei servizi e prodotti più sicuri e affidabili.
Per garantire trasparenza e qualità dei contenuti AssistenzaCriptovalute.it non accetta sponsorizzazioni e non pubblica guide, articoli o recensioni dietro compenso e su richiesta di terzi.
Le piattaforme, exchange, wallet e strumenti citati vengono scelti sulla base di performance, sicurezza, leadership nel settore ed esperienza utente eccelsa.

Usufruendo di un servizio o acquistando un prodotto di terzi per mezzo dei link presenti sul sito o nei booklet l'utente, senza alcun sovrapprezzo, contribuisce a far ricevere ad AssistenzaCriptovalute.it una piccola commissione per poter continuare a offrire in autonomia risorse di qualità e gratuite.

Nota Informativa:

Un link di affiliazione è uno strumento che indirizza gli utenti ad un sito gestito e di proprietà di terze parti. Contiene al suo interno un codice di tracciamento (cookie) allo scopo di identificare il sito di provenienza del clic, per consentire ai programmi di affiliazione di monitorare le conversioni.
Ogni creazione di account, conversione o acquisto effettuato attraverso i link esterni presenti sul sito consente ad AssistenzaCriptovalute.it di percepire una commissione.
Tale commissione non comporta alcun supplemento di prezzo per l'utente, in quanto viene decurtata dal prezzo di vendita.

Errori e Omissioni:

I contenuti sono redatti con la massima cura e sottoposti ad un attento controllo. Ciononostante potrebbero contenere o essere soggetti a errori e imprecisioni, e potrebbero non essere completi e aggiornati. AssistenzaCriptovalute.it si riserva il diritto di correggere inesattezze, imprecisioni e omissioni, nonché di aggiornare contenuti e procedure, in qualsiasi momento e senza preavviso.
AssistenzaCriptovalute.it non si assume responsabilità per eventuali inesattezze riportate nei propri contenuti.

Esclusione di Responsabilità:

AssistenzaCriptovalute.it declina ogni responsabilità per eventuali errori commessi dall'utente nel seguire le indicazioni contenute in guide e articoli.
L'utente si assume la piena responsabilità delle sue azioni, inclusi errori che possono portare alla perdita di fondi.