MODULO 4:

Altcoin, criptoattivi e il loro impatto, Wallets, Masternode, Staking

Cosa sono le altcoin?

Le altcoin nascono con l'obiettivo di diversificare e migliorare l'ecosistema crypto offrendo alternative oltre al bitcoin.

Si definisce "altcoin" (alternative coin) qualsiasi criptovaluta diversa da bitcoin, inglobando nel termine sia le vere e proprie criptovalute, sia i token. Il numero attuale di altcoin è difficile da determinare, data la grande quantità di token creati ogni mese per finanziare diversi progetti, ma si aggira intorno ai 37 milioni.

Lo sviluppo delle altcoin è relativamente semplice, poiché bitcoin è open source, così come molte altre criptovalute. È quindi possibile utilizzare il codice esistente e modificarlo per adattarlo a nuove idee o varianti del progetto.

Alcune criptovalute, come Ethereum, permettono di creare token senza dover sviluppare una nuova blockchain. Attraverso gli Smart Contract è possibile definire le basi di un nuovo token, riducendo i costi di sviluppo e facilitando il finanziamento dei progetti.

Cosa offrono le altcoin?

Innovazione

Bitcoin ha dato origine a un'intera industria che continua a evolversi, proponendo modelli alternativi che offrono nuove soluzioni e migliorano aspetti fondamentali della tecnologia blockchain.

Utilità

Le altcoin cercano di offrire soluzioni concrete sia per le industrie sia per gli utenti. Alcuni progetti lavorano su

tracciabilità alimentare, logistica, sistemi elettorali o gestione intelligente dell'energia.

Decentralizzazione
L'obiettivo è eliminare sistemi centrali di controllo, creando reti distribuite a cui chiunque può contribuire, ricevendo ricompense per il proprio apporto.

Trasparenza
La blockchain permette di rendere i dati verificabili pubblicamente. Poiché i blocchi non possono essere modificati, si garantisce l'integrità e la veridicità delle informazioni.

Competizione e sviluppo

L'innovazione nasce dalla competizione. Se nessuno mette in discussione un modello, questo smette di evolversi. La presenza di molte criptovalute e progetti diversi favorisce lo sviluppo dell'intero ecosistema.

Va però considerato che non tutte le altcoin apportano valore: alcune sono semplici copie con modifiche superficiali. Nonostante ciò, il contributo complessivo delle altcoin allo sviluppo del settore crypto è significativo.

Alcuni inconvenienti delle altcoin

Speculazione

Molte criptovalute hanno un ciclo di vita relativamente breve o sono create esclusivamente per fini speculativi. Solo pochi progetti dispongono realmente di un team di sviluppo solido e di una comunità attiva che li supporta.

Il livello di speculazione è aumentato con la crescita degli exchange, che permettono di negoziare criptovalute con facilità. Questo ha portato a situazioni in cui pochi guadagnano molto denaro, mentre la maggioranza subisce perdite significative in tempi molto brevi.

Duplicazione

Non è raro che progetti validi vengano copiati senza particolari modifiche, cambiando semplicemente il nome. Esistono molti progetti quasi identici tra loro, con lievi differenze estetiche, creati con l'unico scopo di favorire la speculazione e il guadagno rapido.

Criptoattivi e il loro impatto

È evidente che ogni sistema finanziario, anche il più consolidato, evolve nel tempo, spesso a causa di eventi che possono modificare radicalmente l'economia.

Un esempio emblematico è la crisi finanziaria del 2008, che ha rappresentato un vero punto di svolta. Proprio in quel contesto nasce bitcoin, come alternativa alle valute tradizionali messe in crisi dalla perdita di valore, aprendo la strada a un sistema completamente nuovo: un modello digitale in grado di offrire maggiore controllo sul proprio capitale e una possibile protezione dalle instabilità economiche.

Con l'arrivo di bitcoin e delle altre criptovalute, l'economia globale ha iniziato a cambiare. Oggi le valute digitali competono con quelle tradizionali, influenzando il sistema finanziario e proponendosi come possibili valute del futuro.

Perché le criptovalute possono mettere in discussione l'economia globale?

Come tutti sappiamo, le criptovalute si sono presentate come una perfetta alternativa alle valute tradizionali. Il motivo principale per cui le valute digitali sono sempre più popolari è perché si trovano all'interno di un sistema decentralizzato la cui attività non è regolata da alcun organismo pubblico.

Questa è la differenza più importante rispetto alle valute tradizionali, il cui valore è sempre determinato da qualche entità finanziaria.

Ma cosa succede nei periodi di crisi? In pratica, ciò che abbiamo vissuto negli ultimi anni: le valute dei diversi paesi si svalutano (alcune addirittura crollano) e, di conseguenza, anche il nostro capitale e i nostri investimenti perdono il loro valore.

In questo scenario, le criptovalute appaiono come un'alternativa fantastica:

- Il loro valore è totalmente scollegato da qualsiasi banca e si stabilisce in base alla domanda e all'offerta.
- Le valute digitali si basano su un sistema decentralizzato, in cui il controllo non è affidato a un'istituzione centrale ma direttamente agli utenti, che fanno da "banca". In questo senso, ogni individuo diventa responsabile dei propri fondi, con la possibilità di gestirli e trasferirli liberamente in base alle proprie esigenze. Nel tempo, le criptovalute si sono progressivamente ritagliate uno spazio nella società, e oggi sempre più persone le utilizzano sia per gestire il proprio capitale sia come

possibile alternativa in contesti di incertezza del sistema economico globale.
Altri vantaggi rispetto alle valute tradizionali sono:
- Ogni transazione può essere fatta direttamente al destinatario grazie al sistema peer-to-peer. Pertanto, con queste valute digitali, non abbiamo bisogno di alcun intermediario, il che facilita la realizzazione di qualsiasi operazione.
- Tutte le transazioni effettuate tramite blockchain avvengono molto rapidamente (con Bitcoin normalmente richiedono circa 10 minuti, con altre blockchain secondi) e possono essere effettuate verso qualsiasi parte del mondo, 24/7, quindi non è necessario attendere ore o giorni come accade con i trasferimenti bancari.

Si tratta quindi di operazioni molto più flessibili, che offrono grande liquidità e sono anche più sicure. Per tutto ciò, è evidente che le criptovalute hanno avuto un grande impatto sull'economia globale, sfidando le valute tradizionali e il sistema stabilito.

Alcune situazioni reali

Anche se le criptovalute esistono da relativamente poco tempo, gli esperti assicurano che il loro impatto sull'economia mondiale sarà sempre più forte con il passare degli anni. Nonostante ciò, si sono già verificate alcune situazioni reali in cui queste valute digitali hanno assunto un ruolo di particolare rilievo.

Oltre alla crisi finanziaria del 2008, di cui abbiamo già parlato in precedenza, possiamo anche citare il ruolo principale che hanno assunto in relazione al Brexit.

Quando si verificò questo evento, la sterlina si svalutò notevolmente. Quella che per gli acquirenti stranieri fu una buona notizia, non lo fu certo per i cittadini locali, che videro il loro capitale perdere valore velocemente.
Per molti, la soluzione in questo caso fu l'uso delle criptovalute: i britannici decisero infatti di puntare su queste valute digitali per mantenere intatto il valore del proprio capitale e fare in modo che non fosse influenzato dalla situazione economica generale che il paese stava attraversando.

Qualcosa di simile avvenne con lo yuan: anche il mercato della Cina si svalutò e il valore della valuta locale diminuì notevolmente; tuttavia, non accadde lo stesso con bitcoin e per questo motivo molti utenti optarono per utilizzare questa criptovaluta, che arrivò a raggiungere un valore di oltre 1 a 3.500 yuan.
Tenendo conto di queste situazioni reali, non sorprende che in futuro possano verificarsene altre e che alcune valute digitali si presentino come riserva di valore.

Custodia e usi adeguati

Come conservare le tue criptovalute in modo sicuro (Wallet)

Uno dei temi più importanti dell'universo delle criptovalute è la sicurezza e, concretamente, la sicurezza al momento di conservarle. Si tratta di uno degli argomenti più discussi a causa di alcune differenze importanti rispetto a ciò a cui siamo abituati con le valute o le azioni tradizionali.

In questo capitolo parleremo dei metodi esistenti per conservare e custodire criptovalute. Parleremo dei vantaggi e degli svantaggi di ogni metodo e degli aspetti chiave da tenere in considerazione per evitare di perdere il nostro capitale. La maggior parte delle persone che hanno perso le loro criptovalute lo ha fatto principalmente per semplice negligenza o pura ignoranza e noi cercheremo di esporli al meglio per aiutarvi ad evitare certi errori che potrebbero costare il capitale.

I principali fattori da tenere in considerazione per l'analisi saranno:

1. Sicurezza
2. Responsabilità
3. Usabilità

Prima di iniziare, ci piacerebbe chiarire che non esiste un metodo perfetto per conservare criptovalute, ma che questo dipenderà in gran parte da ogni persona e ogni diversa situazione. In generale, l'ideale è avere diversi wallet (portafogli) in funzione dell'uso che si vuole dare alla parte del patrimonio che "contiene". Così come una persona può avere il proprio patrimonio liquido tradizionale distribuito tra conti di diverse banche, una cassaforte in casa e un portafoglio fisico per il denaro che userà nella vita quotidiana, nel mondo delle criptovalute funziona più o meno allo stesso modo.

Tipi di wallet:

- Web wallet
- Desktop wallet
- Mobile wallet

• Hardware wallet
• Paper wallet

Web wallet

I wallet web (o portafogli online) sono ciò che più si avvicina a quello che possiamo trovare nel mondo tradizionale. Funzionano come il sito della tua banca. Ti registri, crei un account, crei una password, invii (o acquisti direttamente) criptovalute e loro le conservano per te.

VANTAGGI:

• Sono molto facili da usare.
• Puoi accedere da qualsiasi dispositivo.
• Di solito permettono l'uso di carte di credito.
• Se dimentichi la password, possono fornirtene un'altra.
• Generalmente, è gratis. Conservare non ha costo.

SVANTAGGI:

• Dipendi al 100% dall'azienda.
• La sicurezza si basa sulla fiducia riposta in questa azienda.
• Non controlli le chiavi private dei tuoi fondi.
• Le aziende accumulano grandi quantità di capitale, quindi sono molto appetibili per terzi.

All'interno della categoria web possiamo includere la maggior parte degli exchange, che generalmente rappresentano la porta d'ingresso all'universo cripto: lì è dove di solito si acquistano e si scambiano le prime criptovalute e, grazie al loro funzionamento molto simile a quello di una banca on-line, vengono spesso utilizzati dalla maggior parte delle persone per conservarle. All'interno della categoria web, un exchange è una delle opzioni meno sicure per conservare criptovalute a lungo termine, poiché sono spesso obiettivo di hacker. Le

grandi quantità di capitale che accumulano e il numero di movimenti che effettuano quotidianamente li rende più vulnerabili rispetto ad altre alternative. Alcuni exchanges, come Binance, garantiscono i fondi in caso di hakeraggio fino a 100.000$

Per quanto possibile, il nostro consiglio è quello di non lasciare mai grandi quantità di capitale negli exchange. Esistono molti casi di furti o perdite e spesso non possono fare nulla per recuperarlo. L'exchange dovrebbe essere utilizzato solo per ciò per cui è progettato: scambiare criptovalute. Una volta fatto, invieremo le nostre criptovalute a un altro tipo di wallet. Se fai trading, spostare il capitale su altri wallet può complicare l'operatività e aggiungere costi per le commissioni, ma non farlo implica più rischio.

Infine, ci piacerebbe ricordare che in broker come Plus500 o eToro, in realtà NON stai acquistando criptovalute e non puoi trasferirle a nessun altro wallet al di fuori della piattaforma. Quelli in cui stai investendo sono strumenti puramente speculativi, che ti permettono di ottenere rendimento (o perdita) in base al movimento del prezzo delle criptovalute, ma che in nessun caso ti danno la proprietà della criptovaluta in sé. Invece, in un exchange (Binance, Coinbase, HitBtc, etc) stai effettivamente acquistando criptovalute e quindi puoi anche inviarle fuori dalle loro piattaforme.

Desktop wallet

I desktop wallet sono la versione di applicazione scaricabile per pc. I wallet ufficiali di ogni criptovaluta sono solitamente di questo tipo. È una delle opzioni più sicure, ma presenta anche alcuni inconvenienti.

VANTAGGI:
• Tu controlli le tue chiavi (per i distratti questo può essere un problema)
• Alta sicurezza. Senza le chiavi nessuno può accedere ai tuoi fondi.
• Non hai bisogno di essere sempre connesso a internet.
• Di solito sono multi-asset. Puoi avere più di una criptovaluta contemporaneamente.
• Alcuni hanno accesso diretto alla blockchain.
• La maggior parte sono gratis. Scaricarne uno e conservare criptovalute non ha costo.

SVANTAGGI:
• Totale responsabilità sulle tue chiavi. Se le perdi, non potrai mai accedere ai tuoi fondi. (Molta attenzione, per favore!)
• Richiede l'installazione di un software.
• Occupano spazio sul tuo computer e, a volte, implica avere un nodo attivo in funzione.
• Puoi accedere solo da un computer che abbia il wallet installato.

Esempi di portafoglio desktop (desktop wallet): Exodus, Electrum, Atomic Wallet, Coinomi, etc.

Mobile wallet
I mobile wallet sono la versione mobile dei desktop wallet. Stesso concetto, ma sul tuo telefono. Scarichi l'applicazione e puoi consultare e operare con le tue criptovalute direttamente dal tuo cellulare. Infatti, alcuni esistono su entrambe le piattaforme, sia desktop che mobile.

Va chiarito che in realtà i tuoi fondi si trovano sulla blockchain e l'applicazione (mobile wallet) è semplicemente un intermediario che serve a mostrarti ciò che è presente nel tuo indirizzo blockchain.

VANTAGGI:
• Tu controlli le tue chiavi (per i distratti questo può essere un problema)
• Facile da usare e portabilità estrema. Sempre accessibile dal tuo telefono.
• Alta sicurezza, ma inferiore al desktop perché più accessibile a terzi/curiosi.
• Di solito sono multi-asset. Puoi avere più di una criptovaluta contemporaneamente.
• È gratis. Scaricarlo e conservare criptovalute non ha costo.

SVANTAGGI:
• Totale responsabilità sulle tue chiavi. Se le perdi, non potrai mai accedere ai tuoi fondi.
• Rischi nello scaricare direttamente dallo store delle app.
• Occupano spazio sul tuo telefono.
• Puoi accedere solo da un telefono che abbia il wallet installato.

Esempio di portafoglio mobile (mobile wallet): Trust wallet, Metamask, SafePal, etc.

Hardware wallet
Gli hardware wallet, o portafogli fisici, sono considerati tra le migliori opzioni in termini di sicurezza e, anche se possono sembrare semplici USB o dischi esterni, opzioni come Trezor o Ledger Nano sono state create esclusivamente per conservare criptovalute.

D’altra parte, nonostante abbiano applicazioni e software per computer, portafogli fisici come Trezor o Ledger Nano sono in realtà solo contenitori di chiavi. Ciò che conservano sono le chiavi private per accedere alla blockchain, non le criptovalute in sé.

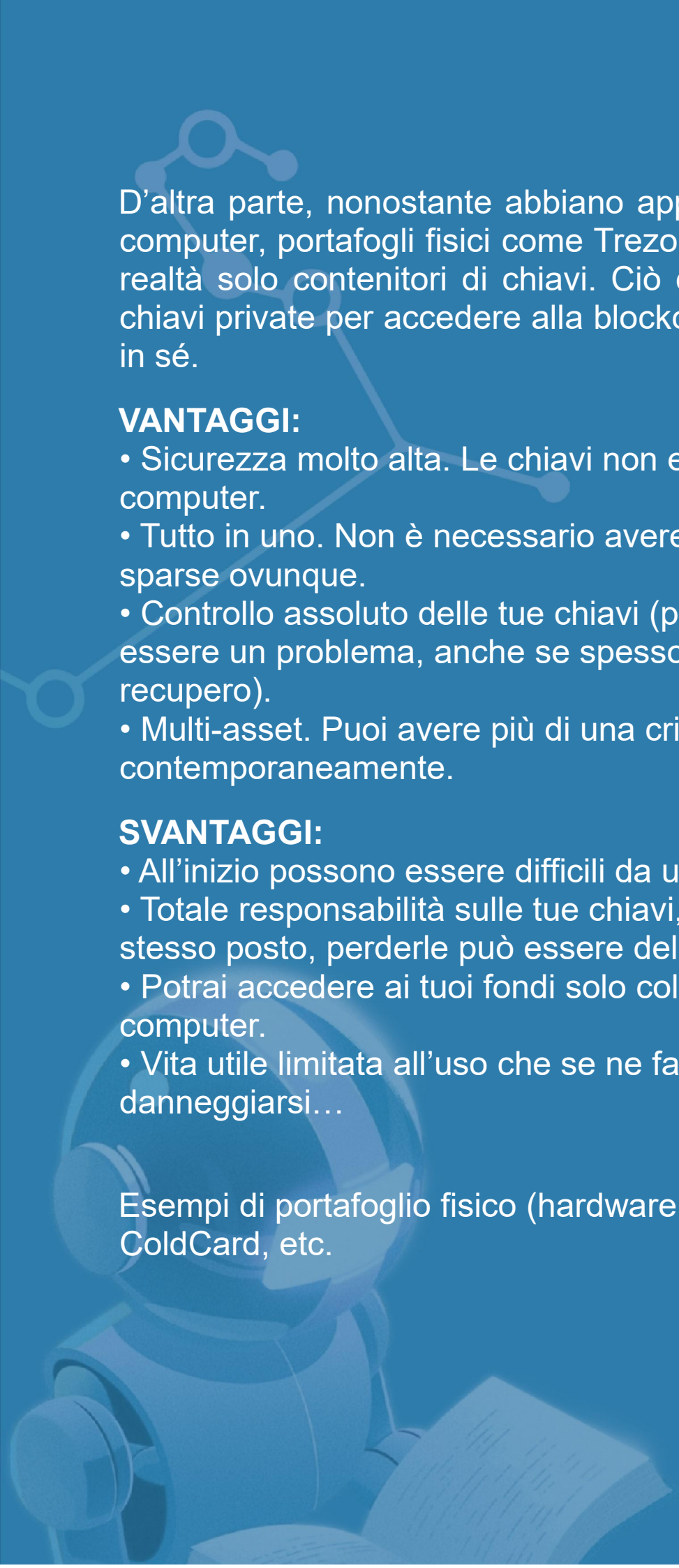
VANTAGGI:

• Sicurezza molto alta. Le chiavi non entrano in contatto con il computer.
• Tutto in uno. Non è necessario avere migliaia di chiavi sparse ovunque.
• Controllo assoluto delle tue chiavi (per i distratti questo può essere un problema, anche se spesso offrono opzioni di recupero).
• Multi-asset. Puoi avere più di una criptovaluta contemporaneamente.

SVANTAGGI:

• All’inizio possono essere difficili da usare.
• Totale responsabilità sulle tue chiavi, che essendo tutte nello stesso posto, perderle può essere delicato…
• Potrai accedere ai tuoi fondi solo collegando quel wallet al computer.
• Vita utile limitata all’uso che se ne fa. Può perdersi, bruciarsi, danneggiarsi…

Esempi di portafoglio fisico (hardware wallet): Ledger, Trezor, ColdCard, etc.



Paper wallet
Come indica il nome e per quanto semplice possa sembrare, i paper wallet sono letteralmente portafogli di carta. È il portafoglio fisico portato all'estrema semplicità. Come se fosse un cold wallet, puoi conservare tutte le tue chiavi qui, su un foglio di carta e collegarti alla blockchain senza che le chiavi tocchino il computer.

È una delle opzioni più sicure contro terzi online, ma una delle peggiori contro terzi "offline", poiché se qualcuno ottiene quel foglio, potrà accedere a tutti i tuoi fondi.

VANTAGGI:
• Sicurezza molto alta "online". Le chiavi non toccano il computer.
• Controllo assoluto delle tue chiavi (per i distratti questo può essere un problema)
• Puoi creare e avere tutti i wallet che vuoi.
• Quasi gratis. Il costo della carta.

SVANTAGGI:
• Usabilità. Non è affatto pratico.
• Totale responsabilità sulle tue chiavi.
• Limitazioni evidenti della carta: fragile, facile da rubare, rompere o perdere…
• Potrai accedere ai tuoi fondi solo usando la chiave che sarà presente su quel foglio.

Ci piacerebbe insistere sul tema delle chiavi o password, dato che è di vitale importanza comprendere bene questa parte ed è forse quella più diversa rispetto a ciò a cui siamo abituati.

Siamo abituati a usare migliaia di password nella nostra vita quotidiana: su internet, nel telefono, nell'antifurto... E siamo anche abituati ad avere sempre a portata di mano il pulsante "recupera password" che ci permette di crearne una nuova in qualsiasi momento e accedere alle nostre applicazioni preferite.

Ebbene, qui NON esiste il pulsante di recupero password. Se perdi la chiave privata, perderai l'accesso ai tuoi fondi per sempre. Per trovare un paragone che serva da esempio oggi, è come se decidessimo di conservare i nostri fondi nella cassaforte più sicura del pianeta, che può essere aperta solo con una password unica molto complicata che solo tu conosci. Se perdi quella chiave, i tuoi fondi resteranno lì. Nessuno potrà mai accedervi e nemmeno tu potrai usarli. Quindi, a effetti pratici, è come se li avessi persi.

Come anticipato prima, non esiste un wallet perfetto. Dipenderà molto da ciascuno, dalla situazione e dall'uso che vogliamo fare di quei fondi. Per chi vuole fare trading a breve termine, non ha senso usare continuamente un portafoglio fisico come Ledger Nano, né vale la pena tenere i fondi in un portafoglio online, web wallet o exchange se l'intenzione è non toccarli per parecchio tempo.

Per fare un esempio reale, noi di solito teniamo la parte stabilita come "a lungo termine" in cold wallets; la parte di capitale che usiamo per transazioni o pagamenti accessibili nella vita quotidiana è conservata in portafogli desktop o su cellulare e, infine, se vogliamo fare trading, manteniamo il capitale stabilito su un exchange.

A modo di riepilogo, se li ordiniamo in base ai 3 criteri iniziali (Sicurezza, Responsabilità, Usabilità), dal più alto al più basso, risulterebbero nel seguente modo:

Sicurezza

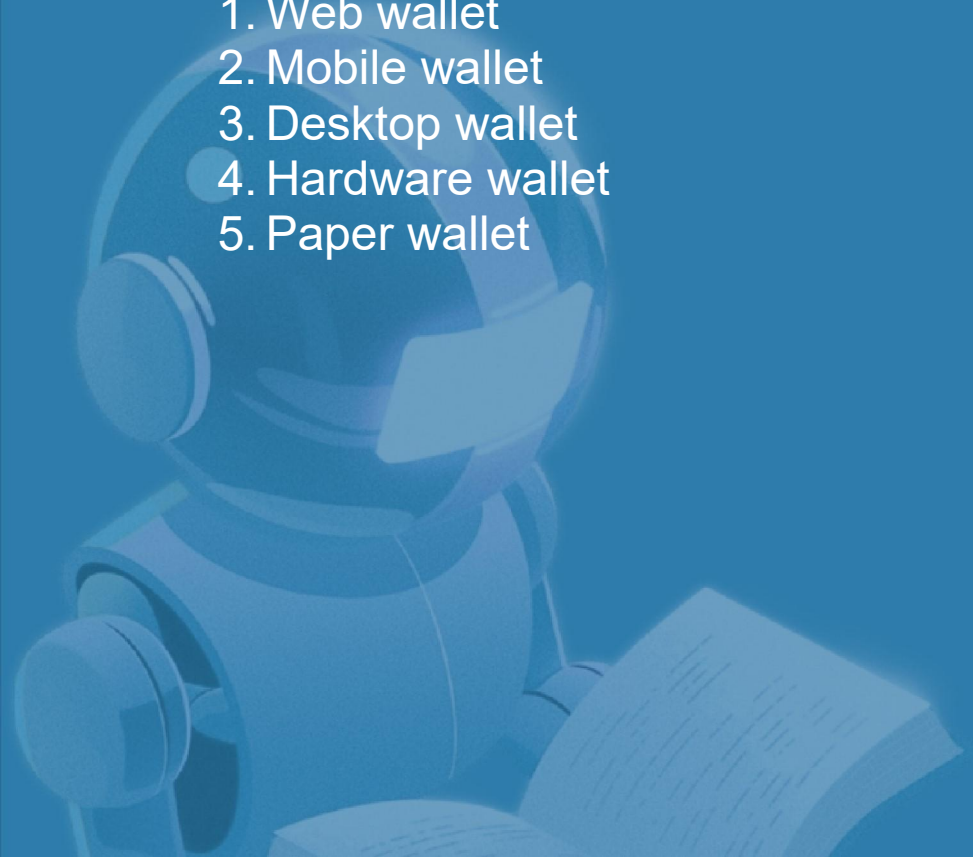
1. Hardware wallet
2. Paper wallet
3. Desktop wallet
4. Mobile wallet
5. Web wallet

Responsabilità

1. Paper wallet
2. Hardware wallet
3. Mobile wallet
4. Desktop wallet
5. Web wallet

Usabilità

1. Web wallet
2. Mobile wallet
3. Desktop wallet
4. Hardware wallet
5. Paper wallet



Che cos'è un masternode

I masternode (o nodi maestri) sono nati con la finalità di fornire servizi per abilitare una forma di governance ed economia uniche in tutto l'ecosistema blockchain. Da allora, sempre più progetti si sono orientati verso la loro implementazione cercando di offrire le migliori caratteristiche ai propri utenti.

Un masternode è un nodo avanzato di una rete blockchain che, oltre alle normali funzioni di validazione, svolge servizi aggiuntivi specifici. Per attivarlo, è generalmente necessario possedere e bloccare una certa quantità di criptovaluta come collaterale, requisito che garantisce l'affidabilità e l'impegno dell'operatore nella rete. In questo modo, queste monete vengono utilizzate come "garanzia" delle operazioni svolte dal nodo. Allo stesso tempo, l'installazione di un nodo maestro generalmente consente alla persona di partecipare alla governance o ad altre funzioni importanti della blockchain.

I masternode non esistono in tutte le blockchain e sono tipici di alcuni progetti (come Dash). Non si tratta quindi di uno standard universale come il mining o lo staking.

Chi ha creato i masternode o nodi maestri?

La storia dei masternode risale al 2014, quando lo sviluppatore Evan Duffield sviluppò un'idea che gli permise di aggiungere un secondo livello al mining. Questo design fu messo in pratica su un hard fork di Bitcoin che ricevette il nome di Xcoin e che attualmente è conosciuto come Digital Cash (Dash).

Nella sua implementazione, uno dei risultati più preziosi fu la riduzione delle commissioni o tariffe. Un'altra funzionalità aggiuntiva che Duffield implementò tramite i nodi maestri fu un sistema di governance decentralizzata e un processo di votazione tra le parti che diede origine a ciò che oggi conosciamo come DAO. Un altro progresso creato da Duffield utilizzando questo sistema fu il sistema di tesoreria, che consente alla rete di generare un budget a partire dalle ricompense. Tutto questo con la finalità di finanziare le idee presentate dalla comunità per il miglioramento della rete Dash.

Queste prime esperienze di Duffield con il concetto di nodi maestri attirarono l'attenzione di molti sviluppatori, che videro l'opportunità perfetta per implementare sistemi simili nei loro progetti blockchain.

Come funziona un masternode?

Il funzionamento di un nodo maestro dipende molto dall'implementazione del suo protocollo nella blockchain in cui viene eseguito. Ma in generale, un nodo maestro funziona tramite il protocollo di Proof of Stake (PoS). Questo perché, attraverso lo staking, il proprietario del nodo maestro può abilitare la creazione di tale nodo.

Ad esempio, in Dash è necessario possedere 1000 DASH per attivare un masternode, mentre in PIVX ne servono 10.000. Questi fondi fungono da collaterale: restano sotto il controllo del proprietario, ma devono rimanere vincolati (non spesi) per garantire il corretto funzionamento del nodo. Il collaterale non è solo una "garanzia tecnica", ma un meccanismo economico che allinea gli incentivi. Chi gestisce il nodo ha interesse a far funzionare bene la rete, perché ha capitale esposto.

Naturalmente esistono anche nodi maestri che utilizzano il protocollo Proof of Work (PoW). Un esempio di questo tipo di nodo maestro basato su PoW si può vedere nella criptovaluta MPower.

Una volta che il nodo maestro è attivo, eseguirà le funzioni per cui è stato programmato. Anche questo dipende dalla blockchain su cui viene eseguito il nodo. Tra le funzioni più comuni dei master nodes si trova l'abilitazione di pagamenti istantanei o anonimi. Vengono anche utilizzati come parte di un sistema di governance decentralizzata, in cui gli operatori dei nodi votano su temi di sviluppo legati alla blockchain a cui partecipano.

Tutte queste funzioni generano una ricompensa che consente agli operatori dei nodi maestri di ottenere guadagni. Infatti, le ricompense tendono ad essere maggiori man mano che aumenta la partecipazione nel mining PoS o PoW.

Guadagnare denaro con un masternode?

I nodi maestri sono anche oggetto di investimento, poiché possono offrire benefici interessanti. Il ROI (Return On Investment) si riferisce al valore economico generato come risultato dello svolgimento di diverse attività economiche. Con questo dato possiamo misurare il rendimento ottenuto da un investimento.

Conoscere il ROI dei nodi maestri è di fondamentale importanza, soprattutto considerando che la loro attivazione richiede un investimento elevato. Ad esempio, un nodo maestro Dash necessita di 1000 DASH per essere attivato. Al prezzo attuale, 1000 DASH corrispondono a circa 37.000

USD. Da qui l'importanza di valutare la redditività dell'installazione di un nodo maestro per una determinata criptovaluta. Tuttavia, esistono masternode per poche centinaia di euro in altre altcoin meno conosciute.

Per calcolare il ROI di un nodo maestro si devono considerare i seguenti fattori:

- Il prezzo al quale è stata acquistata la moneta.
- La ricompensa del blocco o il meccanismo di incentivo.
- Il numero di MN attivi.
- Il costo monetario di mantenimento del MN.
- Il tempo necessario per mantenere il MN.
- Le implicazioni fiscali dei guadagni del MN.
- Il prezzo a cui vengono vendute le monete.
- Il prezzo finale di vendita della moneta.

I masternode o nodi maestri sono una forma di centralizzazione della tecnologia blockchain?

A causa della loro varietà di funzioni e del loro enorme potere, i masternode sono considerati un punto centralizzato all'interno delle strutture di una blockchain. Nonostante ciò, sono una soluzione molto utile per fornire funzionalità che altrimenti sarebbero più complesse e difficili da implementare, per cui, purché la loro applicazione sia chiara, non dovrebbero rappresentare alcuna minaccia per gli utenti e la loro libertà.

Caratteristiche dei masternode

I nodi maestri si caratterizzano generalmente per quanto segue:

- Offrono miglioramenti nella privacy e nella velocità delle transazioni. I nodi maestri permettono alle criptovalute di

avere un focus sull'anonimato e di migliorare la velocità delle transazioni.

- Hanno un maggiore ritorno sull'investimento. Questo perché un master node generalmente offre margini di guadagno migliori nelle ricompense per le azioni o i servizi che fornisce.
- Permettono un meccanismo di controllo e governance più efficiente. Chi possiede un nodo maestro può partecipare alla governance della rete e prendere decisioni che la influenzano.
- Hanno una forte barriera d'ingresso. Per creare un nodo maestro è necessario possedere una quantità specifica di monete a seconda della criptovaluta. Questo rende più difficile la decentralizzazione dei masternode.

Richieste aggiuntive e costi. Per fare che un nodo maestro funzioni, è necessaria una maggior disponibilità di memoria, oltre che la connessione costante e ininterrotta alla rete.

Cos'è lo staking?

La tecnologia e lo sviluppo di ecosistemi economici intorno alle criptovalute ha portato allo sviluppo dello staking, un processo che ci permette di ottenere guadagni e diritto di voto su un progetto di criptovalute facendo qualcosa di molto semplice: risparmiarle.

Il processo di staking consiste infatti nell'acquistare criptovalute e mantenerle bloccate in un wallet con la finalità di ricevere guadagni o ricompense. È un processo molto simile all'HODL, solo che nello staking i saldi sono bloccati e non puoi usarli liberamente. Allo stesso tempo si contribuisce all'operatività e al funzionamento della blockchain di quella stessa criptovaluta.

Come ben sappiamo, la blockchain è la tecnologia che ha permesso di dare vita alle criptovalute. E ogni criptovaluta conta con una propria blockchain per registrare le transazioni effettuate. Però, anche se sono blockchain diverse, tutte hanno una relazione in comune: le transazioni devono essere validate per consenso.

Per questo, ogni blockchain adotta un protocollo di consenso; come già sappiamo, mentre Bitcoin utilizza la Proof of Work (PoW) per il mining dei blocchi (processo che richiede una grande potenza di calcolo e, di conseguenza, consuma molta elettricità), altre criptovalute, come Ether, Stellar, Algorand, utilizzano il meccanismo conosciuto come Proof of Stake (PoS).

In questo protocollo si utilizzano le criptovalute conservate come forma per verificare le transazioni all'interno delle blockchain. Per questo lo staking è un processo particolarmente adottato nelle blockchain che operano con Proof of Stake (PoS), o con alcune delle sue varianti.

Come funziona lo staking?

Nel protocollo di consenso PoS i nodi sono conosciuti come validatori. E sono quelli che si occupano, come indica il loro nome, di validare i blocchi generati.

La scelta di questi nodi validatori è un processo che avviene in modo casuale, molto simile a una lotteria. Hanno maggiore probabilità di essere scelti quei nodi che possiedono una quantità maggiore di criptovalute, così come fossero biglietti, incentivando gli utenti a mantenere i propri fondi dentro un wallet per contribuire al supporto della rete e ottenere guadagni da questo.

Quindi, per fare staking basta solo acquisire una criptovaluta che permetta questo processo e usare il wallet ufficiale per conservarla, ottenendo così ricompense dalla rete. Si può paragonare ad avere un conto di risparmio e ricevere interessi sui propri fondi e nella stessa moneta.

Tipi di staking

- **Pools di staking**

  Sono gruppi di utenti che si uniscono per incrementare le proprie possibilità come validatori di blocchi. Unificando tutti i loro fondi, infatti, hanno maggiore potere di staking. Poi, quando ricevono le ricompense, le dividono tra tutti i partecipanti in modo equivalente al contributo individuale che ognuno ha fatto.

  Questo metodo permette agli utenti piccoli o ai nuovi utenti di partecipare alla rete indipendentemente dalla quantità di asset che possiedono, contribuendo alla sua decentralizzazione.

- **Cold Staking**

  Si tratta di fare staking da un wallet “freddo”, come un hardware wallet che non ha connessione permanente a Internet. Alcune blockchain permettono questo tipo di staking, aiutando i loro utenti a mantenere i fondi offline e quindi molto più sicuri.

  È ideale per quegli utenti che possiedono grandi quantità di criptovalute, che se fossero online correrebbero un grande rischio.

- **Provider di staking**

  Questa modalità permette a molti di offrire un servizio dedicato agli utenti di monete per fare staking. Tuttavia, la redditività con questo tipo di staking dipende molto dalle commissioni che questi applicano, che possono oscillare tra il 2% e fino al 50% delle ricompense. Per questo, si otterrebbe una percentuale di guadagni minore rispetto allo staking effettuato direttamente da una piattaforma.

Vantaggi e svantaggi dello staking

Vantaggi

Il principale vantaggio di questo processo è che elimina completamente la necessità di acquisire o investire in hardware o attrezzature specializzate per il mining, e con ciò anche il fabbisogno energetico che questi richiedono. Inoltre, la generazione di blocchi attraverso lo staking permette una maggiore scalabilità della rete.

Dal lato degli utenti, mantenere una grande quantità di criptovalute in staking offre una maggiore probabilità di essere scelti come validatori e quindi poter validare e verificare i nuovi blocchi che vengono prodotti nella blockchain, ottenendo guadagni migliori e più stabili rispetto al processo di mining PoW.

Allo stesso modo, alcune criptovalute mantenute in staking non si deprezzano con il passare del tempo, come può accadere con le attrezzature di mining se ne viene progettata una migliore e più potente.

Svantaggi

Il processo di comprare criptovalute e mantenerle bloccate per ottenere ricompense può essere molto allettante, ma in realtà non si possono aspettare guadagni molto significativi. Le piattaforme e gli exchange pagano percentuali annuali molto basse, quindi le ricompense sono piuttosto scarse rispetto a quelle ottenute dal mining dei blocchi.

Inoltre, abbiamo già detto che mantenere criptovalute conservate in un wallet online può comportare rischi, poiché un hacker potrebbe sottrarre tutti i fondi. Allo stesso modo, utilizzare una piattaforma o un exchange significa mettere la propria fiducia e i propri fondi nelle mani di un terzo.

Per quanto riguarda la proprietà delle monete, è un fattore che va contro la decentralizzazione per cui sono state create le criptovalute, poiché maggiore è la quantità di asset posseduti, maggiore è la probabilità di generare blocchi e prendere decisioni. Per questo il potere può concentrarsi nelle mani di pochi, lasciando da parte i meno favoriti.

Lo staking è una buona opzione per guadagnare nel mondo crypto, poiché unisce il meglio dell'HODL insieme ai guadagni dagli interessi che genera. Inoltre, man mano che il nostro stake si rafforza, maggiore potere di voto otteniamo nella rete e maggiori guadagni otteniamo da esso.

Consigli per fare staking

Quando valuti opportunità di staking, è fondamentale adottare un approccio rigoroso e razionale. Ecco alcuni principi chiave:

- Effettua sempre una ricerca approfondita e autonoma sul progetto. Analizza la documentazione ufficiale (white paper,

tokenomics, roadmap) e verifica la credibilità del team e della tecnologia. Evita di basarti su opinioni, hype o testimonianze non verificabili.
- Prima di impegnare capitale, calcola con precisione il rendimento reale atteso (APY/APR), considerando eventuali fee, inflazione del token e condizioni di blocco. Valuta scenari conservativi, non solo quelli ottimistici, e definisci chiaramente l'orizzonte temporale dell'investimento.
- Considera attentamente i vincoli di lock-up e la possibilità di unstaking. Un rendimento elevato perde valore se il capitale è illiquido per periodi troppo lunghi o in condizioni di mercato sfavorevoli.
- Prediligi criptovalute con un caso d'uso reale, adozione concreta e una domanda potenziale sostenibile nel tempo. Molti progetti hanno una vita breve: la solidità fondamentale del protocollo è più importante del rendimento immediato.
- Diversifica le posizioni e non concentrare tutto lo stake in un unico protocollo o asset. Considera anche i rischi legati alla custodia (exchange centralizzati vs wallet personali) e alla sicurezza della rete.
- Lo staking è più efficace quando inserito in una strategia di medio-lungo termine. Evita approcci speculativi basati esclusivamente su rendimenti temporanei elevati.

In sintesi, lo staking deve essere trattato come una decisione di investimento strutturata, non come un meccanismo di rendimento passivo privo di rischi.