

Crypto wallet

Nel mondo digitale delle criptovalute, il crypto wallet è la chiave per la gestione e la custodia sicura di questi valori patrimoniali digitali. Ma di cosa si tratta esattamente, e come funziona? In questo articolo vengono spiegati in parole semplici i vari tipi di crypto wallet, il loro funzionamento e la gestione delle criptovalute.

Punti importanti:

- Il wallet è mio, la responsabilità pure! Il codice d'accesso a un portafoglio è l'unico modo per accedere al patrimonio ivi contenuto. Se perdete il codice d'accesso, perdete anche il denaro.
- Il modo migliore per proteggere il vostro crypto wallet è utilizzare un wallet hardware offline e conservare l'ID del wallet e i codici d'accesso con estrema attenzione e in modo sicuro – anche offline, p. es. su carta nella cassaforte.
- Non condividete mai l'ID del vostro wallet e i codici d'accesso via e-mail o in altro modo e non inseriteli mai su una piattaforma o un'app di origine sospetta.

Con i crypto wallet potete conservare in modo sicuro le vostre chiavi private – praticamente le password con cui potete accedere alle vostre [criptovalute \(https://www.ebas.ch/it/criptovalute/\)](https://www.ebas.ch/it/criptovalute/) – e comunque averle a disposizione in qualsiasi momento per inviare e ricevere criptovalute come Bitcoin ed Ethereum.

A differenza di un normale portafoglio in cui si conserva denaro reale, i crypto wallet tecnicamente non contengono le criptovalute in quanto tali, ma solo le chiavi d'accesso (chiamate anche codici d'accesso). Il deposito effettivo di criptovalute si trova nella blockchain su Internet e per accedervi è necessaria una chiave privata. Le chiavi sono la prova della proprietà della moneta digitale e consentono di effettuare transazioni. Se perdete le vostre chiavi private, perdete anche l'accesso al vostro denaro. Ecco perché è essenziale conservarle e gestirle in modo sicuro.

In quali modi si possono gestire le criptovalute?

Esistono diversi approcci alla gestione delle criptovalute. Il primo è la custodia personale (self-custody), con la quale avete pieno controllo sulle vostre chiavi private e sul crypto wallet. Questo metodo offre la massima sicurezza, perché soltanto voi avete accesso alle vostre criptovalute. L'altro lato della medaglia è il doversi occupare personalmente di ogni aspetto riguardante il backup e la gestione delle chiavi.

Il secondo approccio è la custodia delle criptovalute da parte di un fornitore di servizi terzo (custodial services). Può trattarsi di una soluzione più comoda, perché è il fornitore di servizi a occuparsi della gestione e della sicurezza delle vostre chiavi. Tuttavia, c'è il rischio che il fornitore subisca un attacco hacker o fallisca. Esempi di tali fornitori di servizi sono gli exchange di criptovalute come Coinbase o Binance.

Come funziona un crypto wallet?

Un crypto wallet è composto da una chiave pubblica e una privata. La chiave pubblica (public key) si può paragonare al codice IBAN dei conti bancari: è come un indirizzo che gli altri utenti possono utilizzare per trasferirvi criptovalute. La chiave privata (private key), invece, è un codice segreto che consente l'accesso alle criptovalute memorizzate nel wallet. Questa chiave deve essere conservata in modo sicuro e non va mai condivisa con nessuno.

Un crypto wallet permette di memorizzare e conservare queste chiavi in modo sicuro. Potete ricevere criptovalute fornendo il vostro indirizzo pubblico e potete inviare le vostre criptovalute ad altri indirizzi utilizzando la vostra chiave privata.

Che tipi di crypto wallet esistono?

Per i crypto wallet esiste una vasta gamma di opzioni, dalle app semplici e di facile utilizzo alle soluzioni più complesse ed estremamente sicure. I tipi più comuni di wallet sono:

Wallet software

I wallet software sono applicazioni o app installate su un computer o un dispositivo mobile. Esempi sono i wallet desktop come Electrum o Exodus e i wallet mobili come Trust Wallet o Mycelium.

Vantaggi:

- Le chiavi private sono memorizzate localmente sul vostro dispositivo e voi avete il pieno controllo su di esse.
- Alcuni wallet software possono essere utilizzati anche senza connessione a Internet.

Svantaggi:

- Avete il pieno controllo, ma anche la piena responsabilità: se il dispositivo viene perso o danneggiato e non avete una copia di sicurezza (backup), l'accesso al wallet può andare perso in modo irrecuperabile.
- I dispositivi connessi a Internet possono essere vulnerabili al malware.

Wallet online

I wallet online, noti anche come web wallet, sono wallet accessibili tramite un browser Web e i cui dati vengono memorizzati nel cloud da un fornitore di servizi. Questo tipo di wallet consente di accedere alle criptovalute da qualsiasi dispositivo con accesso a Internet. Esempi noti di wallet online sono Coinbase e Blockchain.info.

Vantaggi:

- Accesso da qualsiasi dispositivo dotato di connessione a Internet.
- Adatto ai principianti per la facilità di configurazione e utilizzo.
- I dati vengono memorizzati nel cloud, quindi la perdita del dispositivo non comporta la perdita del wallet.

Svantaggi:

- Le chiavi private vengono memorizzate online, il che comporta un maggiore rischio per la sicurezza e una maggiore esposizione agli attacchi.
- La dipendenza dal fornitore rende necessaria una certa fiducia nelle misure di sicurezza che esso adotta.

Wallet hardware

Un wallet hardware è un dispositivo fisico (in genere con porta USB) appositamente progettato per conservare le criptovalute in modo sicuro. Offre uno dei modi più sicuri per gestire i valori patrimoniali digitali memorizzando le chiavi private offline e proteggendole così dalle minacce online. Esempi comuni di wallet hardware sono Ledger e Trezor.

Vantaggi:

- Sicurezza elevata grazie alla memorizzazione offline delle chiavi private.
- Alcuni wallet hardware possono interfacciarsi con i wallet software.
- Compatibilità con numerose criptovalute.

Svantaggi:

- Soluzione più costosa dei wallet software od online per via dell'hardware specifico.
- Rischio di perdita irreversibile della criptovaluta se il dispositivo viene smarrito e non è stata impostata una frase di ripristino.
- Utilizzo più complicato rispetto ai semplici wallet software od online.

Wallet cartaceo

Un wallet cartaceo è un metodo fisico per conservare le criptovalute. In sostanza, si tratta di un pezzo di carta su cui sono stampate le chiavi pubbliche e private di una criptovaluta. Questo metodo offre un modo sicuro per archiviare le criptovalute offline, riducendo al minimo il rischio di attacchi online e malware.

Vantaggi:

- Sicurezza elevata contro le minacce online come gli attacchi hacker.
- Molto economico e facile da usare.
- Particolarmente adatto per la conservazione a lungo termine della criptovaluta.

Svantaggi:

- Se il wallet cartaceo viene perso o danneggiato e la chiave privata risulta illeggibile, le criptovalute memorizzate vengono irrimediabilmente perse.
- Scarsa facilità d'uso per transazioni regolari. Ogni transazione richiede la digitazione manuale delle chiavi.

In conclusione: il wallet è mio, la responsabilità pure!

Le criptovalute sono memorizzate in formato digitale nei cosiddetti wallet (portafogli) e protette da codici d'accesso. Il codice d'accesso a un portafoglio è l'unico modo per accedere al patrimonio ivi contenuto. Se perdetevi il codice d'accesso, perdetevi anche il denaro.

Protegetevi il vostro crypto wallet così:

- Meglio utilizzare un hardware wallet offline.
- Conservate l'ID del wallet e i codici d'accesso con estrema attenzione e in modo sicuro – anche offline, p. es. su carta nella cassaforte.
- Non condividete mai l'ID del vostro wallet e i codici d'accesso via e-mail o in altro modo e non inseriteli mai su una piattaforma o un'app di origine sospetta.

Un crypto wallet (chiamato anche portafoglio per criptovalute o semplicemente wallet) è un portafoglio digitale con il quale si possono archiviare, ricevere e inviare in modo sicuro criptovalute come Bitcoin, Ethereum e non solo. È uno strumento indispensabile per la gestione e l'uso sicuro delle criptovalute.