# HD Wallet

Davide3011

January 2025

## 1 Introduzione

Gli **HD Wallets (Hierarchical Deterministic Wallets)** rappresentano un'innovazione fondamentale nella gestione delle chiavi crittografiche nel mondo delle criptovalute, in particolare Bitcoin. Introdotti con il **BIP 32** nel 2012, questi wallet hanno risolto molte delle limitazioni dei primi sistemi di gestione delle chiavi, fornendo un approccio deterministico e organizzato per la generazione e l'utilizzo delle chiavi crittografiche.

Prima dell'introduzione degli HD Wallets, ogni chiave privata doveva essere generata casualmente e indipendentemente, rendendo complesso il backup e la gestione di più chiavi. Inoltre, la perdita di una singola chiave privata comportava l'inaccessibilità permanente dei fondi associati. Gli HD Wallets superano queste limitazioni attraverso un sistema deterministico che consente di generare un numero illimitato di chiavi figlie da una singola *chiave master* o *seed phrase*. Questo approccio semplifica notevolmente il backup, poiché è sufficiente salvare la chiave master per ripristinare l'intero portafoglio.

Gli HD Wallets non solo migliorano la sicurezza e l'efficienza nella gestione delle chiavi, ma introducono anche una struttura gerarchica che permette di organizzare le chiavi in base a specifici scopi. Ad esempio, è possibile generare chiavi diverse per ricevere fondi, gestire pagamenti o creare account separati, il tutto mantenendo un unico punto di origine sicuro.

La loro introduzione è stata resa possibile grazie alla standardizzazione proposta dal **BIP 32**, che definisce l'algoritmo per la derivazione delle chiavi e la struttura gerarchica. Gli HD Wallets hanno posto le basi per ulteriori miglioramenti, come il **BIP 39** (seed phrase mnemonica) e il **BIP 44** (gestione multi-asset e multi-account), consolidando il loro ruolo come strumento indispensabile nell'ecosistema delle criptovalute.

## 2 Cosa sono gli HD Wallets

Gli **HD Wallets (Hierarchical Deterministic Wallets)** utilizzano un sistema deterministico per generare e gestire una gerarchia di chiavi private e pubbliche. Questo sistema si basa su una singola **chiave master** o **seed phrase**, dalla quale è possibile derivare in modo prevedibile un numero illimitato di chiavi figlie. Grazie a questa struttura, gli HD Wallets offrono una gestione avanzata delle chiavi crittografiche, garantendo al contempo sicurezza, flessibilità e facilità d'uso.

La chiave master funge da punto centrale per la generazione di tutte le chiavi figlie, mentre la struttura gerarchica consente di organizzare le chiavi in base a categorie o scopi specifici. Questo approccio è stato definito nel **BIP 32**, che stabilisce le regole per la derivazione deterministica delle chiavi e la loro organizzazione gerarchica.

Inoltre, grazie all'introduzione del **BIP 39**, la chiave master può essere rappresentata attraverso una **seed phrase** composta da 12, 18 o 24 parole. Questa rappresentazione mnemonica semplifica il backup e il ripristino del wallet, rendendo più accessibile l'uso delle criptovalute anche a utenti meno esperti.

### 2.1 A cosa servono

Gli HD Wallets sono progettati per risolvere molti problemi legati alla gestione tradizionale delle chiavi crittografiche e per offrire una serie di vantaggi pratici agli utenti. Tra i principali scopi di un HD Wallet

troviamo:

- **Semplificare i backup:** Salvando un'unica seed phrase, l'utente può ripristinare l'intero wallet, evitando la necessità di eseguire backup individuali per ogni chiave privata.

- **Organizzare le chiavi:** Ogni chiave figlia può essere generata e utilizzata per scopi specifici, come ricezione di fondi, pagamenti o gestione di account multipli, mantenendo un alto livello di ordine e tracciabilità.

- **Migliorare la sicurezza:** La derivazione delle chiavi pubbliche direttamente dalla chiave master elimina la necessità di esporre le chiavi private, riducendo il rischio di compromissione dei fondi.

- **Multi-asset e multi-account:** Grazie agli standard successivi come il **BIP 44**, è possibile gestire più criptovalute e account all'interno dello stesso wallet, rendendo gli HD Wallet una soluzione universale e versatile.

Grazie a queste caratteristiche, gli HD Wallets si sono affermati come una delle innovazioni più importanti nel settore delle criptovalute, migliorando significativamente l'esperienza dell'utente e la sicurezza nella gestione dei fondi digitali.

# 3 Vantaggi degli HD Wallets

Gli **HD Wallets** offrono una serie di vantaggi significativi rispetto ai metodi tradizionali di gestione delle chiavi private. Grazie alla loro struttura gerarchica e al funzionamento deterministico, rappresentano una soluzione avanzata per la sicurezza e l'usabilità nel contesto delle criptovalute. I principali vantaggi includono:

- **Backup unico:**
  La **seed phrase**, una sequenza mnemonica composta da 12, 18 o 24 parole generate da un'entropia casuale, rappresenta una soluzione rivoluzionaria per il backup dei portafogli. Questa singola frase consente di ricostruire completamente il wallet e tutte le chiavi ad esso associate. Rispetto ai metodi tradizionali, in cui ogni chiave privata richiedeva un backup individuale, la seed phrase semplifica notevolmente la gestione, riducendo i rischi di errore umano. In caso di smarrimento o danneggiamento del dispositivo, l'utente può recuperare rapidamente l'accesso ai fondi semplicemente inserendo la seed phrase in un wallet compatibile. Inoltre, la seed phrase è compatibile con standard internazionali come il **BIP 39**, garantendo interoperabilità tra diversi software e hardware wallet.

- **Compatibilità multi-asset:**
  Gli HD Wallets supportano la gestione di diverse criptovalute contemporaneamente grazie a standard come il **BIP 44**, che definisce un percorso gerarchico specifico per ogni blockchain. Questo approccio consente di organizzare gli asset digitali in modo efficiente, evitando confusione e migliorando l'accessibilità. Ad esempio, è possibile gestire Bitcoin, Ethereum e altre monete all'interno dello stesso portafoglio, con percorsi separati che garantiscono una gestione chiara e sicura. Questa compatibilità multi-asset rende gli HD Wallets una soluzione universale, ideale per utenti che operano su più blockchain.

- **Gestione avanzata delle chiavi:**
  La struttura gerarchica degli HD Wallets permette di organizzare e isolare le chiavi per scopi specifici, offrendo un alto livello di flessibilità e controllo. Ad esempio:
  - **Chiavi per ricezione:** Generate esclusivamente per ricevere fondi, garantiscono una maggiore sicurezza eliminando la necessità di riutilizzare gli indirizzi.
  - **Chiavi per pagamenti:** Dedicate alle transazioni in uscita, facilitano la gestione separata dei pagamenti personali e aziendali.
  - **Account multipli:** Ogni account può avere una propria gerarchia di chiavi, rendendo più semplice la gestione di portafogli personali, aziendali o familiari.

Questo livello di organizzazione non solo migliora l'efficienza operativa, ma riduce anche il rischio di perdita accidentale dei fondi, poiché le chiavi figlie sono indipendenti e possono essere rigenerate in modo selettivo.

- **Sicurezza migliorata:**
  La derivazione delle chiavi pubbliche direttamente dalla chiave master garantisce che le chiavi private non vengano mai esposte durante le operazioni quotidiane. Gli HD Wallets supportano inoltre la generazione di **chiavi hardened**, che offrono una protezione aggiuntiva contro attacchi crittografici avanzati. Le chiavi hardened impediscono che una chiave figlia venga derivata dalla chiave pubblica del genitore, eliminando il rischio che un attaccante possa risalire all'intera gerarchia delle chiavi. Questo livello di sicurezza, combinato con l'uso della seed phrase, rende gli HD Wallets uno dei sistemi più robusti per la gestione dei fondi crittografici.

Grazie a questi vantaggi, gli HD Wallets rappresentano lo standard per la gestione dei portafogli di criptovalute. La loro capacità di combinare sicurezza, flessibilità e facilità d'uso li rende una scelta ideale sia per utenti esperti che per neofiti, migliorando significativamente l'interazione con le blockchain in termini di affidabilità e praticità.

# 4 Come funzionano gli HD Wallets

Gli **HD Wallets (Hierarchical Deterministic Wallets)** si basano su una **seed phrase** per generare una **chiave master** e un **chain code**. Questi due elementi costituiscono la base per derivare in modo deterministico tutte le chiavi successive, secondo quanto definito nel **BIP 32**. Questo approccio garantisce che ogni chiave figlia sia derivabile solo dalla chiave padre e dal relativo chain code, offrendo un sistema sicuro e scalabile per la gestione delle chiavi crittografiche.

## 4.1 Generazione della seed phrase (BIP 39)

La **seed phrase** è una rappresentazione mnemonica dell'entropia utilizzata per creare la chiave master. Questo sistema, definito dal **BIP 39**, permette di rendere il backup delle chiavi semplice e intuitivo. Ecco i passaggi principali:

- Si genera una sequenza di **128-256 bit di entropia casuale**.
- Questa sequenza viene suddivisa in gruppi di 11 bit, ognuno dei quali è mappato a una parola da una lista predefinita di 2048 parole (ad esempio la lista inglese del BIP 39).
- Il risultato è una frase composta da **12, 18 o 24 parole**, che rappresenta un backup leggibile e facilmente memorizzabile.
- Una checksum, derivata dall'entropia originale, viene aggiunta per garantire l'integrità della seed phrase.

## 4.2 Creazione della chiave master

La seed phrase viene trasformata in una **chiave master** utilizzando l'algoritmo **PBKDF2 (Password-Based Key Derivation Function 2)**:

- La seed phrase è usata come input principale.
- Una passphrase opzionale può essere aggiunta come secondo parametro per aumentare la sicurezza.
- L'output di PBKDF2 è una combinazione di:
  - Una chiave privata master $m$, che serve come punto di partenza per la derivazione delle chiavi successive.
  - Un chain code, un valore aggiuntivo necessario per la derivazione deterministica.

## 4.3 Derivazione delle chiavi figlie

Ogni chiave figlia $k_i$ viene derivata dalla chiave padre $k_p$ e dal relativo chain code, seguendo l'algoritmo definito nel BIP 32. I passaggi sono i seguenti:

- Si calcola l'HMAC-SHA512 del concatenato $k_p + index$, utilizzando il chain code come chiave HMAC:
$$I = HMAC - SHA512(chain\ code_p, k_p \parallel index)$$
- Il risultato $I$ è suddiviso in due parti:
  - $I_L$: La prima metà (32 byte), utilizzata come nuova chiave privata figlia.
  - $I_R$: La seconda metà (32 byte), utilizzata come nuovo chain code per la chiave figlia.
- La chiave figlia $k_i$ è definita come:
$$k_i = (I_L + k_p) \mod n$$
Dove $n$ è l'ordine della curva ellittica utilizzata (secp256k1).

## 4.4 Struttura gerarchica

Le chiavi generate sono organizzate secondo una struttura gerarchica, che segue un percorso deterministico rappresentato come:

```
m / purpose' / coin_type' / account' / change / address_index
```

Dove:

- $m$: La chiave master.
- **Purpose:** Indica lo standard utilizzato (ad esempio, 44' per il BIP 44).
- **Coin type:** Specifica la criptovaluta (ad esempio, 0' per Bitcoin).
- **Account:** Permette la gestione di account separati all'interno dello stesso wallet.
- **Change:** Indica se la chiave è utilizzata per ricevere fondi (0) o per il cambio (1).
- **Address index:** L'indice specifico della chiave figlia.

## 4.5 Algoritmo di derivazione

L'algoritmo di derivazione utilizza l'HMAC-SHA512 per garantire che ogni chiave figlia sia univoca e sicura. I dettagli dell'algoritmo sono:

1. **Input:**
   - La chiave padre $k_p$.
   - Il chain code $c_p$ associato.
   - L'indice della chiave figlia $i$.
2. **Calcolo:**
$$I = HMAC - SHA512(c_p, k_p \parallel i)$$
3. **Output:**
   - $k_i = I_L + k_p \mod n$: La chiave figlia.
   - $c_i = I_R$: Il nuovo chain code figlio.

Questo processo può essere ripetuto per generare chiavi figlie a qualsiasi livello della gerarchia, mantenendo sempre la possibilità di rigenerare le chiavi in modo deterministico a partire dalla chiave master.

## 4.6 Esempio di percorso deterministico

Un esempio pratico di percorso deterministico utilizzando lo standard BIP 44 è:

```
m / 44' / 0' / 0' / 0 / 0
```

Che può essere interpretato come:

- $m$: La chiave master.
- $44'$: Segue lo standard BIP 44 per HD Wallets multi-asset.
- $0'$: Specifica Bitcoin come asset.
- $0'$: Rappresenta il primo account.
- 0: Chiave per ricezione di fondi.
- 0: Primo indirizzo generato.

Questa struttura flessibile consente di gestire più account, asset e categorie di chiavi, mantenendo al contempo un sistema di backup centralizzato e sicuro.

## 4.7 Come funziona Electrum?

Electrum è uno dei wallet Bitcoin più popolari e avanzati, progettato per offrire una gestione sicura e semplice delle chiavi private. Sebbene segua i principi generali degli **HD Wallets** definiti nel **BIP 32**, Electrum introduce alcune particolarità nel suo funzionamento.

### 4.7.1 Struttura delle chiavi in Electrum

Electrum utilizza una struttura deterministica per generare le chiavi private e pubbliche, ma con alcune differenze rispetto allo standard BIP 44:

- Electrum segue una propria gerarchia deterministica per la derivazione delle chiavi, utilizzando un **seed proprietario**.
- Le chiavi vengono derivate da un **seed phrase** che può essere rappresentato da 12 o più parole leggibili dall'utente.
- Non utilizza il BIP 39 per la generazione della seed phrase, bensì un formato personalizzato che garantisce la compatibilità solo con altri wallet Electrum.

### 4.7.2 Percorso deterministico in Electrum

Il percorso utilizzato da Electrum è semplificato rispetto al BIP 44. Ad esempio:

```
m / 0 / index
```

Dove:

- $m$: La chiave master derivata dal seed.
- 0: Indica il primo livello per gli indirizzi utilizzati per ricevere fondi.
- *index*: Specifica l'indice dell'indirizzo, incrementato per ogni nuovo indirizzo generato.

Electrum non utilizza la struttura multi-asset del BIP 44, in quanto è specifico per Bitcoin.

### 4.7.3 Seed phrase in Electrum

Electrum genera una **seed phrase proprietaria**, che:

- È compatibile solo con Electrum, rendendo il backup portabile solo tra istanze dello stesso software.
- Utilizza un'entropia di 128 bit, combinata con un checksum interno, per garantire l'integrità e la sicurezza della frase.
- Può essere rappresentata con o senza una passphrase aggiuntiva, a seconda di come preferisce l'utente.

### 4.7.4 Gestione delle chiavi pubbliche e private

Electrum consente di visualizzare e utilizzare sia le chiavi pubbliche sia le chiavi private per ogni indirizzo generato. Offre inoltre la possibilità di:

- Importare chiavi private da altri wallet.
- Esportare chiavi pubbliche per integrarle con sistemi esterni o software di terze parti.
- Supportare indirizzi compatibili con SegWit, offrendo una gestione efficiente delle transazioni.

### 4.7.5 Sincronizzazione e archiviazione leggera

Una delle caratteristiche distintive di Electrum è la sua architettura leggera. Non richiede il download completo della blockchain, ma utilizza server remoti per verificare le transazioni e sincronizzare il portafoglio. Questo lo rende ideale per dispositivi con risorse limitate.

### 4.7.6 Vantaggi di Electrum

- **Velocità:** Grazie all'uso di server remoti, il tempo di sincronizzazione è minimo rispetto ai wallet full node.
- **Flessibilità:** Supporta funzioni avanzate come SegWit, multi-firma e hardware wallet.
- **Sicurezza:** Le chiavi private non lasciano mai il dispositivo dell'utente, e il seed phrase è necessario per ogni ripristino.
- **Compatibilità:** Electrum è compatibile con la maggior parte degli hardware wallet, inclusi Trezor e Ledger.

Electrum è quindi una scelta eccellente per utenti esperti che necessitano di un wallet Bitcoin leggero, sicuro e versatile, pur mantenendo la compatibilità con standard moderni e avanzati come SegWit.

# 5 Conclusioni

Gli **HD Wallets (Hierarchical Deterministic Wallets)** rappresentano un pilastro essenziale nell'ecosistema delle criptovalute, rivoluzionando il modo in cui vengono gestite e protette le chiavi crittografiche. Introdotti con il **BIP 32**, questi wallet hanno reso possibile una gestione delle chiavi avanzata, sicura e intuitiva, superando le limitazioni dei metodi tradizionali.

Grazie alla loro **struttura gerarchica**, gli HD Wallets consentono di generare un numero virtualmente illimitato di chiavi private e pubbliche a partire da una sola chiave master. Questo approccio semplifica la gestione degli indirizzi, offre una migliore organizzazione delle chiavi e consente l'isolamento delle operazioni critiche. Inoltre, l'introduzione delle **seed phrase** (BIP 39) ha reso il processo di backup e ripristino estremamente semplice, riducendo significativamente i rischi legati alla perdita di fondi.

Gli standard successivi, come il **BIP 44**, hanno ulteriormente ampliato le possibilità degli HD Wallets, permettendo la gestione di più asset e account dallo stesso wallet. Questa compatibilità multi-asset ha consolidato gli HD Wallets come la soluzione di riferimento per utenti che operano su diverse blockchain.

Dal punto di vista della sicurezza, gli HD Wallets offrono una protezione avanzata contro attacchi crittografici, grazie alla derivazione delle chiavi pubbliche direttamente dalla chiave master e all'utilizzo di chiavi hardened per applicazioni sensibili. La robustezza dell'algoritmo di derivazione HMAC-SHA512 e l'isolamento delle chiavi figlie garantiscono un elevato livello di protezione per i fondi digitali.

In conclusione, gli HD Wallets rappresentano un equilibrio perfetto tra semplicità d'uso e sicurezza crittografica. La loro adozione ha reso le criptovalute più accessibili a un pubblico più ampio, mantenendo al contempo un alto standard di sicurezza. Grazie alla loro flessibilità e alla capacità di adattarsi a esigenze diverse, gli HD Wallets continueranno a essere uno strumento fondamentale nell'evoluzione dell'ecosistema blockchain.