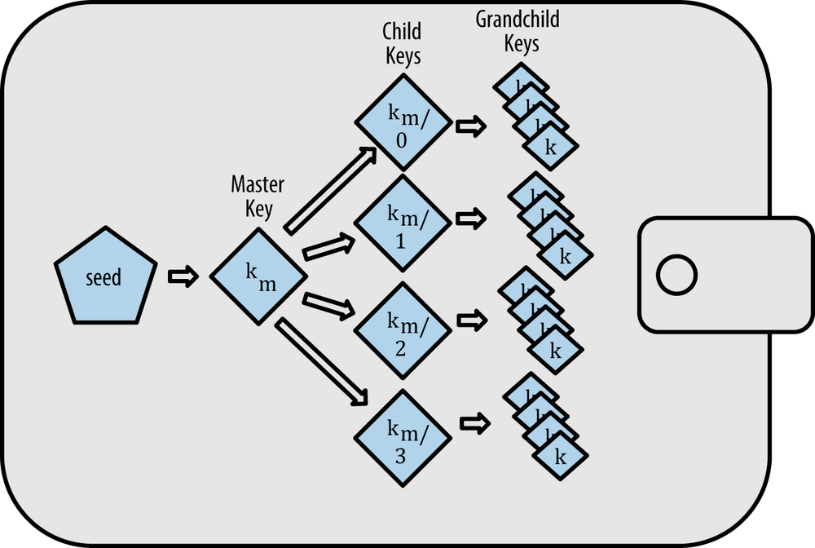
What is HD Wallet, BIP32, BIP39 and BIP44?

HD Wallet ： HD是Hierarchical Deterministic的縮寫。分層的意思就是，假設有一間大公司，他可以為各個子部門分別生成不同的私鑰，子部門還可以再管理子子部門的私鑰，每個母部門可以看到所有子部門的幣，也可以花這裡面的幣；也可以只給會計人員某個層級的公鑰，讓他可以看見這個母部門及子部門的收支紀錄，但不能花這裡面的幣，使得財務管理更為方便。而最早的HD概念源於BIP32，以下簡述。

BIP (Bitcoin Improvement Proposals)，是提出比特幣新功能或改進措施的文件，通常可由任何人提出，經過審核後公佈在 bitcoin/bips 上。而其中的 BIP32, BIP39, BIP44 共同定義了目前被廣泛使用的 HD Wallet，包含其設計動機和理念、實作方式、實例等。

BIP 32 ： 定義HD Wallet，是一個系統可以從單一種子產生一樹狀結構儲存多組 keypairs（私鑰和公鑰）。好處是可以方便的備份、轉移到其他相容裝置（因為都只需要 seed），以及分層的權限控制等。



BIP 39 ： 因為種子為一串很長的亂數，不便記憶，因此將種子用方便記憶和書寫的單字表示，拓展了HD Wallet錢包種子的生成演算法。一般由 12 個單字組成，稱為 mnemonic code(助記詞或助記碼)。例如：[rose rocket invest real refuse margin festival danger anger border idle brown]

BIP 44 ： 基於 BIP 32 的系統，可增加多幣種，透過HD Wallet派生多個位址，可以同時管理主網與測試網的比特幣；也就是賦予樹狀結構中的各層特殊的意義，讓同一個種子可以支援**多幣種、多帳戶**等。各層定義如下：m / purpose' / coin\_type' / account' / change / address\_index，其中的 purporse' 固定是 44'，代表使用 BIP 44。而 coin\_type' 用來表示不同幣種，例如 Bitcoin 就是 0'，Ethereum 是 60'。