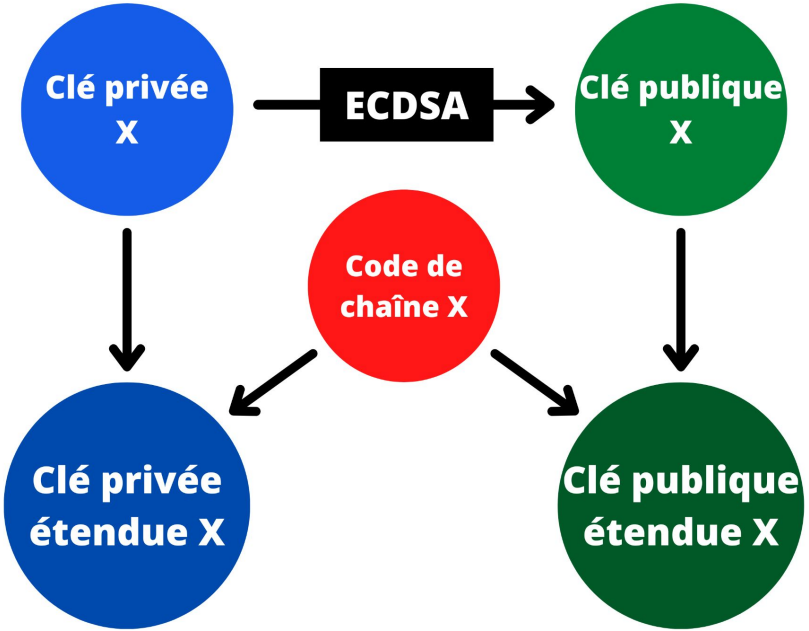
5.2 - Les clés étendues.

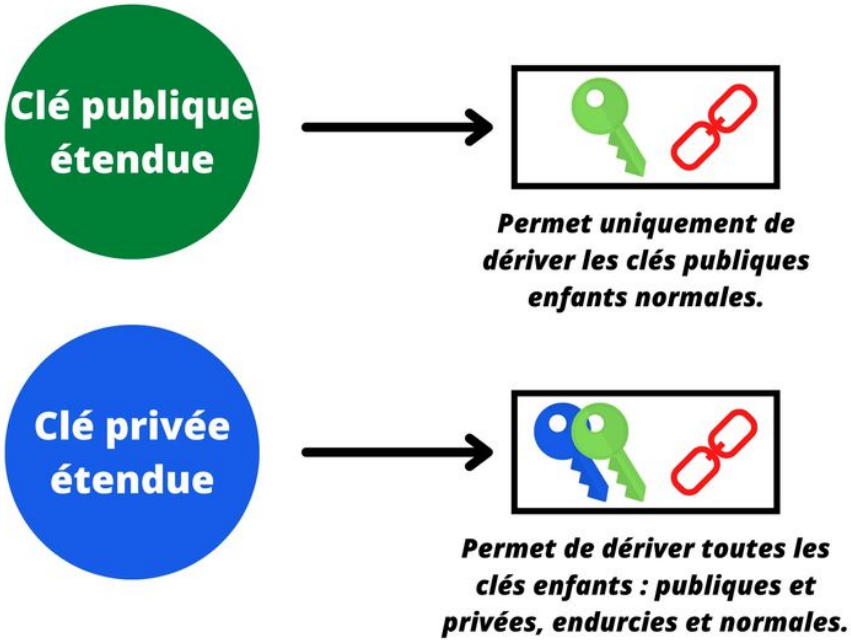
Rappel.

- La base du portefeuille HD : entropie > nombre aléatoire > Phrase mnémonique (et passphrase) > Graine > Clé maîtresse.
- On souhaite dériver plusieurs clés enfants.
- Chaque paire de clé est composée de trois parties : la clé privée, la clé publique et le code de chaîne.

La clé étendue.



Principes de dérivation.



Construction de la clé étendue.

Version	4 octets
Profondeur	1 octet
Empreinte parent	4 octets
Index	4 octets
Code de chaîne	32 octets
Clé (publique ou privée)	33 octets (pour la clé privée qui ne fait que 32 octets, on concatène à la base l'octet 0x00).
Checksum	4 octets

En Base 58:
xpub6CTNzMUkzpurBWaT4HQoYzLP4uBbGJuWY358Rj7rauiw4rMHCyq3Rfy9w4kyJXJzeFfyrK
LUar2rUCukSiDQFa7roTwzjiAhyQAdPLEjqHT

En HEX(base 16):
0488B21E036D5601AD80000000C605DF9FBD77FD6965BD02B77831EC5C78646AD3ACA14DC3
984186F72633A89303772CCB99F4EF346078D167065404EED8A58787DED31BFA479244824D
F50658051F067C3A

Les préfixes.

Préfixe base 58	Préfixe base 16	Réseau	Objectif	Scripts associés	Dérivation	Type de clé
xpub	0488b21e	Mainnet	Legacy et SegWit V1	P2PK / P2PKH / P2TR	m/44'/0' m/86'/0'	publique
xprv	0488ade4	Mainnet	Legacy et SegWit V1	P2PK / P2PKH / P2TR	m/44'/0' m/86'/0'	privée
tpub	043587cf	Testnet	Legacy et SegWit V1	P2PK / P2PKH / P2TR	m/44'/1' m/86'/1'	publique
tprv	04358394	Testnet	Legacy et SegWit V1	P2PK / P2PKH / P2TR	m/44'/1' m/86'/1'	privée
ypub	049d7cb2	Mainnet	Nested SegWit	P2WPKH in P2SH	m/49'/0'	publique
yprv	049d7878	Mainnet	Nested SegWit	P2WPKH in P2SH	m/49'/0'	privée
upub	049d7cb2	Testnet	Nested SegWit	P2WPKH in P2SH	m/49'/1'	publique
uprv	044a4e28	Testnet	Nested SegWit	P2WPKH in P2SH	m/49'/1'	privée
zpub	04b24746	Mainnet	SegWit V0	P2WPKH	m/84'/0'	publique
zprv	04b2430c	Mainnet	SegWit V0	P2WPKH	m/84'/0'	privée
vpub	045f1cf6	Testnet	SegWit V0	P2WPKH	m/84'/1'	publique
vprv	045f18bc	Testnet	SegWit V0	P2WPKH	m/84'/1'	privée

Conclusion.

- Une clé étendue et la clé maîtresse sont deux éléments différents.
- Une clé étendue est une concaténation d'une clé avec son code de chaîne associé.
- Une clé publique étendue permet uniquement de dériver des clés publiques enfants normales. Une clé privée étendue permet de dériver n'importe quelle clé enfant.
- En pratique, on ajoute à une clé étendue des métadonnées, et notamment un préfixe.