Commandes de l'explorateur Bitcoin (bx)

2022-03-17

# Commandes de l'explorateur Bitcoin (bx)

Bitcoin Explorer (bx) est un outil en ligne de commande qui offre une variété de commandes pour la gestion des clés et la construction de transactions. Il fait partie de la bibliothèque Bitcoin libbitcoin.

Usage: bx COMMAND [--help]  
  
Info: The bx commands are:  
  
address-decode  
address-embed  
address-encode  
address-validate  
base16-decode  
base16-encode  
base58-decode  
base58-encode  
base58check-decode  
base58check-encode  
base64-decode  
base64-encode  
bitcoin160  
bitcoin256  
btc-to-satoshi  
ec-add  
ec-add-secrets  
ec-multiply  
ec-multiply-secrets  
ec-new  
ec-to-address  
ec-to-public  
ec-to-wif  
fetch-balance  
fetch-header  
fetch-height  
fetch-history  
fetch-stealth  
fetch-tx  
fetch-tx-index  
hd-new  
hd-private  
hd-public  
hd-to-address  
hd-to-ec  
hd-to-public  
hd-to-wif  
help  
input-set  
input-sign  
input-validate  
message-sign  
message-validate  
mnemonic-decode  
mnemonic-encode  
ripemd160  
satoshi-to-btc  
script-decode  
script-encode  
script-to-address  
seed  
send-tx  
send-tx-node  
send-tx-p2p  
settings  
sha160  
sha256  
sha512  
stealth-decode  
stealth-encode  
stealth-public  
stealth-secret  
stealth-shared  
tx-decode  
tx-encode  
uri-decode  
uri-encode  
validate-tx  
watch-address  
wif-to-ec  
wif-to-public  
wrap-decode  
wrap-encode

Pour plus d'informations, consultez la [page d’accueil Bitcoin Explorer](https://github.com/libbitcoin/libbitcoin-explorer) et [guide d’usage Bitcoin Explorer](https://github.com/libbitcoin/libbitcoin-explorer/wiki).

# Exemples d'utilisation de la commande bx

Regardons quelques exemples d'utilisation des commandes Bitcoin Explorer pour expérimenter avec des clés et des adresses.

Générez une "valeur d’amorçage" aléatoire à l'aide de la commande seed, qui utilise le générateur de nombres aléatoires du système d'exploitation. Transmettez la valeur à la commande ec-new pour générer une nouvelle clé privée. Nous sauvegardons la sortie standard dans le fichier *private\_key* :

$ bx seed | bx ec-new > private\_key  
$ cat private\_key  
73096ed11ab9f1db6135857958ece7d73ea7c30862145bcc4bbc7649075de474

Maintenant, générez la clé publique à partir de cette clé privée à l'aide de la commande ec-to-public. Nous passons le fichier *private\_key* dans l'entrée standard et enregistrons la sortie standard de la commande dans un nouveau fichier *public\_key* :

$ bx ec-to-public < private\_key > public\_key  
$ cat public\_key  
02fca46a6006a62dfdd2dbb2149359d0d97a04f430f12a7626dd409256c12be500

Nous pouvons reformater la public\_key en tant qu'adresse à l'aide de la commande ec-to-address. Nous passons le fichier *public\_key* dans l'entrée standard :

$ bx ec-to-address < public\_key  
17re1S4Q8ZHyCP8Kw7xQad1Lr6XUzWUnkG

Les clés générées de cette manière produisent un portefeuille non déterministe de type 0. Cela signifie que chaque clé est générée à partir d'une valeur d’amorçage indépendante. Les commandes de Bitcoin Explorer peuvent également générer des clés de manière déterministe, conformément au BIP-32. Dans ce cas, une clé "maître" est créée à partir d'une valeur d’amorçage, puis étendue de manière déterministe pour produire un arbre de sous-clés, résultant en un portefeuille déterministe de type 2.

Tout d'abord, nous utilisons les commandes seed et hd-new pour générer une clé principale qui servira de base pour dériver une hiérarchie de clés :

$ bx seed > seed  
$ cat seed  
eb68ee9f3df6bd4441a9feadec179ff1  
  
$ bx hd-new < seed > master  
$ cat master  
xprv9s21ZrQH143K2BEhMYpNQoUvAgiEjArAVaZaCTgsaGe6LsAnwubeiTcDzd23mAoyizm9cApe51gNfLMkBqkYoWWMCRwzfuJk8RwF1SVEpAQ

Nous utilisons maintenant la commande hd-private pour générer une clé de "compte" renforcée et une séquence de deux clés privées au sein du compte :

$ bx hd-private --hard < master > account  
$ cat account  
xprv9vkDLt81dTKjwHB8fsVB5QK8cGnzveChzSrtCfvu3aMWvQaThp59ueufuyQ8Qi3qpjk4aKsbmbfxwcgS8PYbgoR2NWHeLyvg4DhoEE68A1n  
  
$ bx hd-private --index 0 < account  
xprv9xHfb6w1vX9xgZyPNXVgAhPxSsEkeRcPHEUV5iJcVEsuUEACvR3NRY3fpGhcnBiDbvG4LgndirDsia1e9F3DWPkX7Tp1V1u97HKG1FJwUpU  
  
$ bx hd-private --index 1 < account  
xprv9xHfb6w1vX9xjc8XbN4GN86jzNAZ6xHEqYxzbLB4fzHFd6VqCLPGRZFsdjsuMVERadbgDbziCRJru9n6tzEWrASVpEdrZrFidt1RDfn4yA3

Ensuite, nous utilisons la commande hd-public pour générer la séquence correspondante de deux clés publiques :

$ bx hd-public --index 0 < account  
xpub6BH1zcTuktiFu43rUZ2gXqLgzu5F3tLEeTQ5t6iE3aQtM2VMTxMcyLN9fYHiGhGpQe9QQYmqL2eYPFJ3vezHz5wzaSW4FiGrseNDR4LKqTy  
  
$ bx hd-public --index 1 < account  
xpub6BH1zcTuktiFx6CzhPbGjG3UYQ13WR16CmtbPiagEKpEVtpyjshWyMaMV1cn7nUPUkgQHPVXJVqsrA8xWbGQDhohEcDFTEYMvYzwRD7Juf8

Les clés publiques peuvent également être dérivées de leurs clés privées correspondantes à l'aide de la commande hd-to-public :

$ bx hd-private --index 0 < account | bx hd-to-public  
xpub6BH1zcTuktiFu43rUZ2gXqLgzu5F3tLEeTQ5t6iE3aQtM2VMTxMcyLN9fYHiGhGpQe9QQYmqL2eYPFJ3vezHz5wzaSW4FiGrseNDR4LKqTy  
  
$ bx hd-private --index 1 < account | bx hd-to-public  
xpub6BH1zcTuktiFx6CzhPbGjG3UYQ13WR16CmtbPiagEKpEVtpyjshWyMaMV1cn7nUPUkgQHPVXJVqsrA8xWbGQDhohEcDFTEYMvYzwRD7Juf8

Nous pouvons générer un nombre pratiquement illimité de clés dans une chaîne déterministe, toutes dérivées d'une seule valeur d’amorçage. Cette technique est utilisée dans de nombreuses applications de portefeuille pour générer des clés qui peuvent être sauvegardées et restaurées avec une seule valeur de départ. C'est plus facile que d'avoir à sauvegarder le portefeuille avec toutes ses clés générées de manière aléatoire à chaque fois qu'une nouvelle clé est créée.

La valeur d’amorçage peut être encodée à l'aide de la commande mnemonic-encode :

$ bx hd-mnemonic < seed > words  
adore repeat vision worst especially veil inch woman cast recall dwell appreciate

La valeur d’amorçage peut ensuite être décodée à l'aide de la commande mnemonic-decode :

$ bx mnemonic-decode < words  
eb68ee9f3df6bd4441a9feadec179ff1

L'encodage mnémonique peut faciliter l'enregistrement et même la mémorisation de la valeur d’amorçage.