پیوست ب

فرمان‌های کاوشگر بیت‌کوین (bx)

کاوشگر بیت‌کوین (Bitcoin Explorer)، یا به اختصار bx، یک ابزار خط-فرمان برای مدیریت کلیدها و ساخت تراکنش است. کاوشگر بیت‌کوین جزئی از کتابخانه‌ی libbitcoin است. طرز استفاده از این ابزار چنین است:

```
bx COMMAND [-help]
```

که در آن COMMAND می‌تواند هر یک از فرمان‌های زیر باشد:

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
```

[برای اطلاعات بیشتر درباره‌ی bx به https://github.com/libbitcoin/libbitcoin-explorer مراجعه کنید. مستندات این ابزار را هم می‌توانید در صفحه‌ی https://github.com/libbitcoin/libbitcoin-explorer/wiki ببینید.]

چند نمونه از کاربرد فرمان‌های bx

اجازه دهید طرز استفاده از فرمان‌های bx را با چند مثال نشان دهیم.

دستور ترکیبی زیر با فرمان seed یک عدد تصادفی تولید کرده و پس از ایجاد یک کلید خصوصی از این عدد تصادفی، آن را در یک فایل ذخیره می‌کند:

```
$ bx seed | bx ec-new > private_key
$ cat private_key
73096ed11ab9f1db6135857958ece7d73ea7c30862145bcc4bbc7649075de474
```

اکنون می‌توان با این کلید خصوصی یک کلید عمومی ایجاد کرده و در یک فایل ذخیره کرد:

```
$ bx ec-to-public < private_key > public_key
$ cat public_key
02fca46a6006a62dfdd2dbb2149359d0d97a04f430f12a7626dd409256c12be500
```

قدم بعدی می‌تواند تبدیل این کلید عمومی به یک آدرس بیت‌کوین (غیرقطعی نوع- ۰) باشد:

```
$ bx ec-to-address < public_key
17re1S4Q8ZHyCP8Kw7xQad1Lr6XUzWUnkG
```

برای تولید کلیدهای قطعی نوع- ۲ ابتدا باید یک «کلید اصلی» بسازیم:

```
$ bx seed > seed
$ cat seed
eb68ee9f3df6bd4441a9feadec179ff1

$ bx hd-new < seed > master
$ cat master
xprv9s21ZrQH143K2BEhMYpNQoUvAgiEjArAVaZaCTgsaGe6LsAnwubeiTcDzd23mAoyizm9cApe51gNf
LMkBqkYoWWMCRwzfuJk8RwF1SVEpAQ
```

اکنون می‌توان با فرمان hd-private یک کلید تقویت‌شده از این کلید اصلی استخراج کرده:

```
$ bx hd-private -hard < master > account
$ cat account
xprv9vkDLt81dTKjwHB8fsVB5QK8cGnzveChzSrtCfvu3aMWvQaThp59ueufuyQ8Qi3qpjk4aKsbmbfxw
cgS8PYbgoR2NWHeLyvg4DhoEE68A1n
```

و سپس کلیدهای خصوصی فرعی (اندیس‌دار) را ساخت:

```
$ bx hd-private -index 0 < account
xprv9xHfb6w1vX9xgZyPNXVgAhPxSsEkeRcPHEUV5iJcVEsuUEACvR3NRY3fpGhcnBiDbvG4LgndirDsi
ale9F3DWPkX7Tp1V1u97HKG1FJwUpU

$ bx hd-private -index 1 < account
xprv9xHfb6w1vX9xjc8XbN4GN86jzNAZ6xHEqYxzbLB4fzHFd6VqCLPGRZFsdjsuMVERadbgDbziCRJru
9n6tzEWrASVpEdrZrFidt1RDfn4yA3
```

کلیدهای عمومی فرعی (اندیس‌دار) نیز با فرمان hd-public از این کلیدهای خصوصی ساخته می‌شوند:

```
$ bx hd-public -index 0 < account
xpub6BH1zcTuktiFu43rUZ2gXqLgzu5F3tLEeTQ5t6iE3aQtM2VMTxMcyLN9fYHiGhGpQe9QQYmqL2eYP
FJ3vezHz5wzaSW4FiGrseNDR4LKqTy

$ bx hd-public -index 1 < account
xpub6BH1zcTuktiFx6CzhPbGjG3UYQ13WR16CmtbPiagEKpEVtpyjshWyMaMV1cn7nUPUkgQHPVXJVqsr
A8xWbGQDhohEcDFTEYMvYzwRD7Juf8
```

برای تولید کلیدهای عمومی (از کلیدهای خصوصی متناظر) از فرمان hd-to-public نیز می‌توان استفاده کرد:

```
$ bx hd-private -index 0 < account | bx hd-to-public
xpub6BH1zcTuktiFu43rUZ2gXqLgzu5F3tLEeTQ5t6iE3aQtM2VMTxMcyLN9fYHiGhGpQe9QQYmqL2eYP
FJ3vezHz5wzaSW4FiGrseNDR4LKqTy

$ bx hd-private -index 1 < account | bx hd-to-public
xpub6BH1zcTuktiFx6CzhPbGjG3UYQ13WR16CmtbPiagEKpEVtpyjshWyMaMV1cn7nUPUkgQHPVXJVqsr
A8xWbGQDhohEcDFTEYMvYzwRD7Juf8
```

برای تولید کُد یادافزا برای این کلیدهای قطعی به یک بذر نیاز داریم؛ فرمان‌های seed و hd-mnemonic می‌توانند برای تولید واژه‌های تصادفی کُد یادافزا به کار گرفته شوند:

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

این بذر سپس باید با فرمان mnemonic-decode کُدگذاری شود:

```
$ bx mnemonic-decode < words
eb68ee9f3df6bd4441a9feadec179ff1
```

همان طور که می‌دانید، کُدگذاری واژه‌های یادافزا ثبت و همچنین به خاطر سپردن بذرها را ساده‌تر می‌کند.