Managing the Wallet

1. Backing Up and Restoring The Wallet

1.1 Creating the Wallet

Since version 0.21, Bitcoin Core no longer has a default wallet. Wallets can be created with the `createwallet` RPC or with the `Create wallet` GUI menu item.

In the GUI, the `Create a new wallet` button is displayed on the main screen when there is no wallet loaded. Alternatively, there is the option `File` -> `Create wallet`.

The following command, for example, creates a descriptor wallet. More information about this command may be found by running `bitcoin-cli help createwallet`.

```
$ bitcoin-cli createwallet "wallet-01"
```

By default, wallets are created in the `wallets` folder of the data directory, which varies by operating system, as shown below. The user can change the default by using the `-datadir` or `-walletdir` initialization parameters.

Operating System	Default wallet directory
Linux	`/home/<user>/.bitcoin/wallets`
Windows	`C:\Users\<user>\AppData\Roaming\Bitcoin\wallets`
macOS	`/Users/<user>/Library/Application Support/Bitcoin/wallets`

1.2 Encrypting the Wallet

The `wallet.dat` file is not encrypted by default and is, therefore, vulnerable if an attacker gains access to the device where the wallet or the backups are stored.

Wallet encryption may prevent unauthorized access. However, this significantly increases the risk of losing coins due to forgotten passphrases. There is no way to recover a passphrase. This tradeoff should be well thought out by the user.

Wallet encryption may also not protect against more sophisticated attacks. An attacker can, for example, obtain the password by installing a keylogger on the user's machine.

After encrypting the wallet or changing the passphrase, a new backup needs to be created immediately. The reason is that the keypool is flushed and a new HD seed is generated after encryption. Any bitcoins received by the new seed cannot be recovered from the previous backups.

The wallet's private key may be encrypted with the following command:

```
$ bitcoin-cli -rpcwallet="wallet-01" encryptwallet "passphrase"
```

Once encrypted, the passphrase can be changed with the `walletpassphrasechange` command.

```
$ bitcoin-cli -rpcwallet="wallet-01" walletpassphrasechange "oldpassphrase"
"newpassphrase"
```

The argument passed to `-rpcwallet` is the name of the wallet to be encrypted.

Only the wallet's private key is encrypted. All other wallet information, such as transactions, is still visible.

The wallet's private key can also be encrypted in the `createwallet` command via the `passphrase` argument:

```
$ bitcoin-cli -named createwallet wallet_name="wallet-01" passphrase="passphrase"
```

Note that if the passphrase is lost, all the coins in the wallet will also be lost forever.

1.3 Unlocking the Wallet

If the wallet is encrypted and the user tries any operation related to private keys, such as sending bitcoins, an error message will be displayed.

```
$ bitcoin-cli -rpcwallet="wallet-01" sendtoaddress
"tb1qw508d6qejxtdg4y5r3zarvary0c5xw7kxpjzsx" 0.01
error code: -13
error message:
Error: Please enter the wallet passphrase with walletpassphrase first.
```

To unlock the wallet and allow it to run these operations, the `walletpassphrase` RPC is required.

This command takes the passphrase and an argument called `timeout`, which specifies the time in seconds that the wallet decryption key is stored in memory. After this period expires, the user needs to execute this RPC again.

```
$ bitcoin-cli -rpcwallet="wallet-01" walletpassphrase "passphrase" 120
```

In the GUI, there is no specific menu item to unlock the wallet. When the user sends bitcoins, the passphrase will be prompted automatically.

1.4 Backing Up the Wallet

To backup the wallet, the `backupwallet` RPC or the `Backup Wallet` GUI menu item must be used to ensure the file is in a safe state when the copy is made.

In the RPC, the destination parameter must include the name of the file. Otherwise, the command will return an error message like "Error: Wallet backup failed!" for descriptor wallets. If it is a legacy wallet, it will be copied and a file will be created with the default file name `wallet.dat`.

```
$ bitcoin-cli -rpcwallet="wallet-01" backupwallet /home/node01/Backups/backup-01.dat
```

In the GUI, the wallet is selected in the `Wallet` drop-down list in the upper right corner. If this list is not present, the wallet can be loaded in `File` -> `Open wallet` if necessary. Then, the backup can be done in `File` -> `Backup Wallet...`.

This backup file can be stored on one or multiple offline devices, which must be reliable enough to work in an emergency and be malware free. Backup files can be regularly tested to avoid problems in the future.

If the computer has malware, it can compromise the wallet when recovering the backup file. One way to minimize this is to not connect the backup to an online device.

If both the wallet and all backups are lost for any reason, the bitcoins related to this wallet will become permanently inaccessible.

1.5 Backup Frequency

The original Bitcoin Core wallet was a collection of unrelated private keys. If a non-HD wallet had received funds to an address and then was restored from a backup made before the address was generated, then any funds sent to that address would have been lost because there was no deterministic mechanism to derive the address again.

Bitcoin Core version 0.13 introduced HD wallets with deterministic key derivation. With HD wallets, users no longer lose funds when restoring old backups because all addresses are derived from the HD wallet seed.

This means that a single backup is enough to recover the coins at any time. It is still recommended to make regular backups (once a week) or after a significant number of new transactions to maintain the metadata, such as labels. Metadata cannot be retrieved from a blockchain rescan, so if the backup is too old, the metadata will be lost forever.

Wallets created before version 0.13 are not HD and must be backed up every 100 keys used since the previous backup, or even more often to maintain the metadata.

1.6 Restoring the Wallet From a Backup

To restore a wallet, the `restorewallet` RPC must be used.

```
$ bitcoin-cli restorewallet "restored-wallet" /home/node01/Backups/backup-01.dat
```

After that, `getwalletinfo` can be used to check if the wallet has been fully restored.

```
$ bitcoin-cli -rpcwallet="restored-wallet" getwalletinfo
```

The restored wallet can also be loaded in the GUI via `File` -> `Open wallet`.