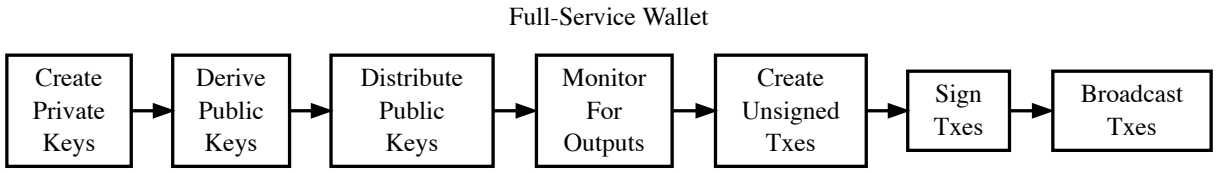
钱包

钱包程序

全服务钱包

bitcoin.core 是一个的标准话的全服务钱包。
一个完整的全服务钱包，包含产生私钥，产生公钥，分发公钥，监视公钥上的交易，创建交易，签名交易，发送交易。
关于全服务钱包的功能流程。如下图:

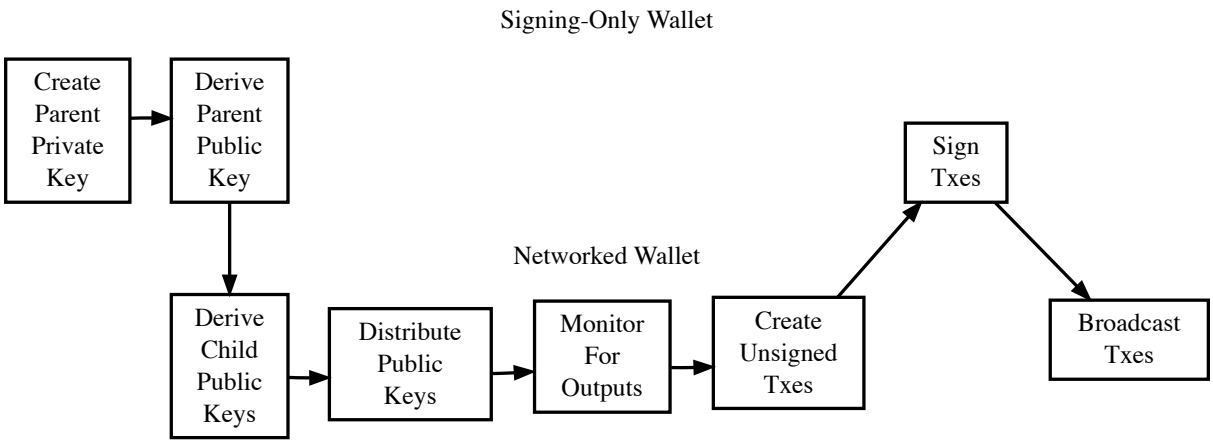


优点:操作简单，一个程序完全实现用户的需求</br>
缺点:由于私钥存储在联网设备中，因此对于用户来说这个是集齐不安全的做法。</br>

ps:为了解决全服务钱包的缺点，因此就出现了一种新的模式，将需要全服务钱包的功能一分为二，
一个是联网钱包，另一个是仅签名钱包。

仅签名钱包

仅签名钱包的功能:1.产生私钥, 2.产生公钥, 3, 签名交易
联网钱包的的功能:1.分发公钥，2.监视公钥上的交易, 3.创建交易, 4.发送交易
仅签名钱包和联网钱包相互配合组成一个全服务钱包,但是相比于普通的全服务钱包，这种模式未将私钥存储在联网设备上,因此十分安全。
仅签名钱包和联网钱包相互配合的流程如下图:



1.联网钱包仅仅只是对于公钥的操作</br>
2.仅签名钱包产生了公钥之后须将公钥通过某种方式(如移动介质)传递给联网程序</br>
3.当联网钱包创建了一笔交易之后需要将交易hex(或者其他的交易形式数据)通过某种方式(如移动介质)传递给仅签名钱包,由仅签名钱包将该交易进行签名,再将签名之后的交易hex(或者其他的交易形式数据)通过某种方式(如移动介质)传递给联网钱包,进行广播交易</br>

钱包文件

定义:钱包就是私钥的集合

私钥的格式

在bitcoin中私钥的形式是以简单的256-bit的随机数字。

钱包导入格式(WIF)

为了使私钥的拷贝复制尽量少的出错,因此引入WIF格式来减少这种错误.WIF采用的是base58check编码。

HD钱包

hd钱包有一个root seed 产生一个根私钥，根私钥生成一个树,每一叶子节点就为 子私钥。 助记词:是将根私钥与一个2048项的字典对应得出的，便于记忆的12～18个单词

Bitcoin.Core钱包

导入方式

1.导入私钥

bitcoin-cli importprivkey [privkey] [accountname]

```
[privatekey]私钥</br>
[accountname]账户名(默认"",可选)</br>
[true|false] 是否rescan(默认true,可选)</br>
```

```
ps:rescan需要花费大约1个小时,在此期间rpc会阻塞
无法进行rpc操作，因此需要等待rescan完成。
```

2.导入助记词

导入助记词有两个步骤:1.通过助记词生成钱包文件。2.通过rpc命令导入钱包文件(需要等待)

- 1.通过助记词生成钱包文件
  进入key-migrate当前目录
  生成钱包文件 *./key-migrate -m "填写助记词"*
  得到钱包文件全路径
- 2.导入钱包文件: bitcoin-cli importwallet [filename]

```
filename:为钱包全路径（通过./key-migrate返回得到）
ps:rescan需要花费大约1个小时,在此期间rpc会阻塞
无法进行rpc操作，因此需要等待rescan完成。
```

实例:

- cd /home/lc (key-migrate文件路径为/home/lc)
- sudo chmod +x key-migrate
- ./key-migrate -m "weapon quick crush salad cricket radio master steak assume build ice ice"
- 返回 succeed and writen to file:/tmp/wallet-keys969403900
- 导入钱包文件 bitcoin-cli importwallet /tmp/wallet-keys969403900
- 等待rescan(约一个小时)

3.导入wallet.dat

导入wallet.dat方式为快速备份导入的方式,可实现快速导入用户钱包资产的需求。但是导入之前需要关闭客户端,将wallet.dat拷贝到数据目录中（拷贝之前如果现有的钱包没有备份,请将现有钱包备份）， 然后启动客户端。

```
客户端启动是会读取wallet.dat(它是钱包相关所有数据的数据库),程序会读取wallet.dat记录到的blockhash然后和主链hash,然后更新wallet.dat的数据。
```

备份方式

1.备份私钥

bitcoin-cli dumpprivkey [address]
[address]地址

> 返回私钥字符串

2.备份钱包文件(私钥的集合)

bitcoin-cli dumpwallet [filename]

> 返回文件全路径

3.备份wallet.dat

备份wallet.dat方式为快速备份导入的方式,可实现快速导入用户钱包资产的需求。备份wallet.dat必须手动关闭客户端,然后手工拷贝wallet.dat(可用linux的cp命令)