比特币的私钥格式

发表于 2024-10-26 | 阅读次数： 37

比特币的私钥是一个**小于 n 的正整数**。n 的值等于

```
0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141
```

换算成十进制为

```
115792089237316195423570985008687907852837564279074904382605163141518161494337
```

这是一个非常大的数，它介于 2^{255} 和 2^{256} 之间。

```
>>> n = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141
>>> print(n)
115792089237316195423570985008687907852837564279074904382605163141518161494337
>>> 2 ** 255 < n < 2 ** 256
True
```

在发送比特币等链上资产时，需要用私钥创建数字签名以证明用户对这些资产的控制权。丢失或泄露私钥都意味着资金损失，所以对私钥的保护十分重要，具体可以分为三个方面：

- 生成私钥，使用安全的随机源保证他人无法用可重复的过程碰撞出你的私钥
- 存储和使用私钥，保证你的私钥不会泄漏给他人或被他人窃取
- 备份私钥，让你在意外丢失私钥时还能从备份恢复它

WIF

可以直接使用十进制或十六进制来表示私钥，但为了转录方便避免抄写错误，私钥一般会被编码成 WIF（Wallet Import Format）格式。

WIF 是对私钥 Base58Check 编码的结果，因为一些历史原因，WIF 分为压缩（compressed）和不压缩（uncompressed）两种格式。对于要编码的私钥：

```
0xF97C89AAACF0CD2E47DDBACC97DAE1F88BEC49106AC37716C451DCDD008A4B62
```

1. 根据网络类型在私钥前添加前缀，例如比特币主网（Mainnet）要添加 0x80 前缀。

```
0x80F97C89AAACF0CD2E47DDBACC97DAE1F88BEC49106AC37716C451DCDD008A4B62
```

2. 根据压缩格式在私钥后添加后缀，WIF compressed 要添加 0x01 后缀，WIF uncompressed 不添加任何后缀。

```
# WIF compressed
0x80F97C89AAACF0CD2E47DDBACC97DAE1F88BEC49106AC37716C451DCDD008A4B6201
# WIF uncompressed
0x80F97C89AAACF0CD2E47DDBACC97DAE1F88BEC49106AC37716C451DCDD008A4B62
```

3. 对上一步的结果做 Base58Check 编码。

```
# WIF compressed
L5agPjZKceSTkhqZF2dmFptT5LFrbr6ZGPvP7u4A6dvhTrr71WZ9
# WIF uncompressed
5KiANv9EHEU4o9oLzZ6A7z4xJJ3uvfK2RLEubBtTz1fSwAbpJ2U
```

对同一个私钥，不同的网络类型和不同的 WIF 格式会得到不同的编码结果。

网络	WIF 压缩格式	前缀	后缀	WIF
Mainnet	compressed	0x80	0x01	L5agPjZKceSTkhqZF2dmFptT5LFrbr6ZGPvP7u4A6dvhTrr71WZ9
Mainnet	uncompressed	0x80	无	5KiANv9EHEU4o9oLzZ6A7z4xJJ3uvfK2RLEubBtTz1fSwAbpJ2U
Testnet	compressed	0xEF	0x01	cVwfreZB3i8iv9JpdSStd9PWhZZGGJCFLS4rEKWfbkahibwhticA
Testnet	uncompressed	0xEF	无	93UnxexmsTYCmDJdctz4zacuwxQd5prDmH6rfpEyKkQViAVA3me

在 WIF 中编码额外的前缀和后缀信息，是为了方便钱包软件在用户导入私钥时能正确的初始化。私钥只是一个大整数，压缩和不压缩是 WIF 的两种格式，私钥本身不能被“压缩”。