链滴

# bitcoin: 压缩公钥与非压缩公钥

作者：shooter

原文链接：https://ld246.com/article/1550844562914

来源网站：链滴

来自简书

btc address: 1FmWXNJT3jVKaHBQs2gAs6PLGVWx1zPPHf

## 前文介绍

生成bitcoin地址 文章中得到了公钥 04d061e9c5891f579fd548cfd22ff29f5c642714cc7e7a9215f071ef5a5723f691757b28e31be71f09f24673eed52348e58d53bcfd26f4d96ec6bf1489eab429d,

**公钥其实是secp256k1椭圆曲线的一个坐标点**，即(x,y)形式，用16进制表示是

(0xd061e9c5891f579fd548cfd22ff29f5c642714cc7e7a9215f0071ef5a5723f69,

0x1757b28e31be71f09f24673eed52348e58d53bcfd26f4d96ec6bf1489eab429d)

而且(x,y) 必然符合：

```
# python code
Pcurve = 2**256 - 2**32 - 2**9 - 2**8 - 2**7 - 2**6 - 2**4 -1 #有限域
x = 0xd061e9c5891f579fd548cfd22ff29f5c642714cc7e7a9215f0071ef5a5723f69
y = 0x1757b28e31be71f09f24673eed52348e58d53bcfd26f4d96ec6bf1489eab429d

x_res = x**3+7
y_res = y**2

(x_res%Pcurve) == (y_res%Pcurve)
```

####为啥符合呢

比特币secp256k1椭圆曲线公式是 $y^2=x^3+7$

**椭圆曲线加密算法** 定义在有限域 $\mathbb{F}_p$上

假设 $y^2=x^3+7$ 在 $\mathbb{F}_{23}$，

$x^3+7 \ mod \ 23$ 就是 ((x**3)+7) % 23

$y^2 \ mod \ 23$ 就是 (y**2)%23

((x**3)+7) % 23 == (y**2)%23必然成立，不成立就不符合椭圆曲线加密的定义了。

secp256k1的有限域是Pcurve，Pcurve是个质数。

####未压缩公钥

前缀04+x坐标+y坐标

04d061e9c5891f579fd548cfd22ff29f5c642714cc7e7a9215f0071ef5a5723f691757b28e31be71f9f24673eed52348e58d53bcfd26f4d96ec6bf1489eab429d

## 压缩公钥

前缀03+x(如果y是奇数)，前缀02+x(如果y是偶数)

0x1757.....429d从最后一位 0xd来看，这个数是奇数，所以压缩公钥是03d061e9c5891f579fd548cf22ff29f5c642714cc7e7a9215f0071ef5a5723f69

现在一般都使用压缩公钥, 压缩/未压缩公钥生成的地址确实会不一样,
非压缩公钥早已成了非主流。

## 比特币地址

以下是同一个私钥，不同类型的公钥生成的地址。
代码见 gen_addr

14xfJr1DArtYR156XBs28FoYk6sQqirT2s
35egEPVeimCvWAmXeHXcYtAUtdA8RtsNUY
mjUcbu6BytKoC7YiEkqPxB1sc6U7nnjFse
##############压缩公钥##############
1ASfqPzBTfPSBA9DWdHYYNk4qM5NoGNtzL
3B8gkwUd1ZhpGKqedix8y16zysN6QWqQxS
mpxd8T5AGgpgxGcqECFvNHxPhLg5of8Sh3