base58 与 base64 的区别

wstart / 2018-04-09 09:46:16 / 浏览数 8801

最近在代码审计一个区块链的源代码的时候发现的。

审查发现用的是base58的编码。

没看清楚，直接用base64去解，后来才发现不是base64，大写的一个囧

后来查了查资料

Base58是用于Bitcoin中使用的一种独特的编码方式，主要用于产生Bitcoin的钱包地址。

相比Base64，Base58不使用数字"0"，字母大写"O"，字母大写"I"，和字母小写"l"，以及"+"和"/"符号。

设计Base58主要的目的是：

- 避免混淆。在某些字体下，数字0和字母大写O，以及字母大写I和字母小写l会非常相似。
- 不使用"+"和"/"的原因是非字母或数字的字符串作为帐号较难被接受。
- 没有标点符号，通常不会被从中间分行。
- 大部分的软件支持双击选择整个字符串。

但是这个base58的计算量比base64的计算量多了很多。因为58不是2的整数倍，需要不断用除法去计算。

而且长度也比base64稍微多了一点。

附一段 base58 的python 加解密的实现

```
__b58chars = '123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz'
__b58base = len(__b58chars)


def b58encode(v):
   """ encode v, which is a string of bytes, to base58.
   """

   long_value = int(v.encode("hex_codec"), 16)

   result = ''
   while long_value >= __b58base:
       div, mod = divmod(long_value, __b58base)
       result = __b58chars[mod] + result
       long_value = div
   result = __b58chars[long_value] + result

   # Bitcoin does a little leading-zero-compression:
   # leading 0-bytes in the input become leading-1s
   nPad = 0
   for c in v:
       if c == '\0':
           nPad += 1
       else:
           break

   return (__b58chars[0] * nPad) + result


def b58decode(v):
   """ decode v into a string of len bytes
   """

   long_value = 0L
   for (i, c) in enumerate(v[::-1]):
       long_value += __b58chars.find(c) * (__b58base ** i)

   result = ''
   while long_value >= 256:
```

```
        div, mod = divmod(long_value, 256)
        result = chr(mod) + result
        long_value = div
    result = chr(long_value) + result

    nPad = 0
    for c in v:
        if c == __b58chars[0]:
            nPad += 1
        else:
            break

    result = chr(0) * nPad + result
    return result

if __name__ == "__main__":
    print  b58encode("hello world")
    print  b58decode("StV1DL6CwTryKyV")
```

点击收藏 | 0 关注 | 1

上一篇：ELF病毒分析 下一篇：ThinkPHP框架 5.0.x...

1. 3 条回复

ADog 2018-04-09 10:08:43

我比较关注的是区块链代码审计，审计关注点是啥啊？

0 回复Ta

wstart 2018-04-09 10:11:42

@ADog
我主要看2块

1. 实现的算法是否严谨。 比如共识算法是否可以伪造，重放等
2. =。= 普通常见的越权...

由于地址钱包是base58生成的。所以我弄了生成器去看他认不认=。=

0 回复Ta

ADog 2018-04-09 11:50:16

@wstart 感谢师傅解答~

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板