# IOTA 调研

## 一、账户模型

1. 地址

传统的以区块链为基础的系统，例如比特币，你的钱包地址是可以被多次重复使用的。

**IOTA的地址(在进行对外转账时)只能被使用一次**。一个IOTA地址如果只用来收账，可以使用无限次。但一旦当你使用这个地址向外转账完成后，就不应该再使用改地址了。

**这是出于安全性的考虑。**当你对外进行转账的时候（如果你发送的是IOTA），这个特定地址中的部分私有密钥被暴露，进而给了其他人（例如黑客）暴力破解全部密钥，进而最终获得存储在这个地址中的所有IOTA 的可能性。你通过同一个IOTA地址向外转账的次数越多，黑客就越容易暴力破解你的密钥。需要注意的是，获得一个地址的密钥不会暴露你的IOTA种子或是在你的种子（账户）中的其他地址的密钥。

1. 种子

**种子是81位长的字符串**，而且你必须使用A、B、C...Z和数字9随机产生一个长度为81位字符的串。当你访问IOTA钱包时，你只需要输入IOTA种子即可。所以，请务必妥善保管好你的种子。

IOTA种子的可能性组合有：27^81 = 8.7x10^115。假设有一台超级计算机，在一秒钟内生成并读取1万亿个不同种子。8.7x10^115 种子组合 / 1x10^12 每秒钟生成 = 8.7x10^103 秒钟 = **2.8x10^96 年**

1. 种子生成的方法

3.1 离线

Linux

cat /dev/urandom |tr -dc A-Z9|head -c${1:-81}

Mac

cat /dev/urandom |LC\_ALL=C tr -dc 'A-Z9' | fold -w 81 | head -n 1

* 1. 在线

[1.https://ipfs.io/ipfs/QmdqTgEdyKVQAVnfT5iV4ULzTbkV4hhkDkMqGBuot8egfA](https://www.iotachina.com/go?url=https://ipfs.io/ipfs/QmdqTgEdyKVQAVnfT5iV4ULzTbkV4hhkDkMqGBuot8egfA)

[2. https://github.com/eukaryote31/iota-seed-gen](https://www.iotachina.com/go?url=https://github.com/eukaryote31/iota-seed-gen)

[3. https://github.com/erdii/iota-seedgen](https://www.iotachina.com/go?url=https://github.com/erdii/iota-seedgen)

1. 地址的工作原理

4.1 种子、索引与地址的生成

**当一个新地址被生成时，它是由一个种子和地址索引组合而成的，地址索引可以是任何一个正整数（包括“0”）。**IOTA钱包通常从地址索引0开始生成地址（通过IOTA种子和地址索引0）。如果钱包发现这个地址没有被附加到缠结（Tangle）中，钱包会用这个地址作为一个新的地址。但是当它发现某个地址如果已经被连接到缠结(Tangle)中，它会跳过这个地址索引，继续生成并直到找到新的未被使用的地址为止。

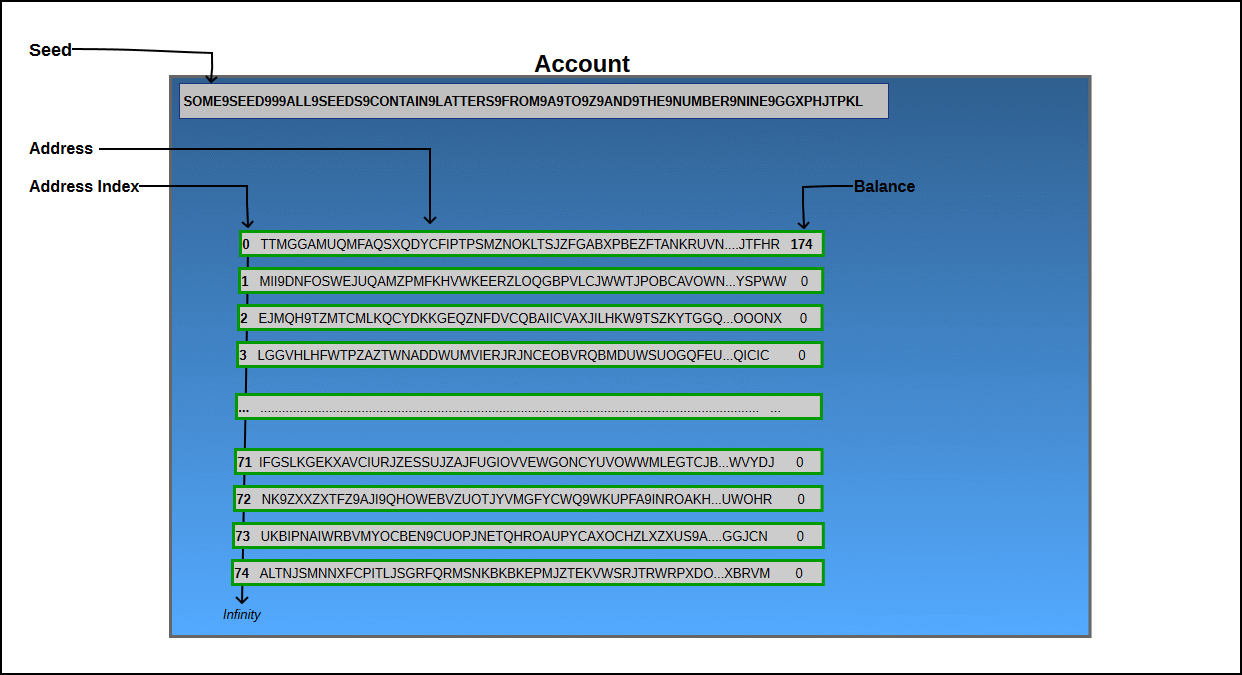
* 1. 转账操作的过程

转账交易的过程可以分为两个主要步骤：

1）对转账交易进行本地签名，这一步需要使用您的IOTA种子进行签名操作。

2）把准备好的转账交易数据，从缠结中选择两个尚未进行的交易，然后做POW， 这一步被称为“附加”。

* 1. 地址是依次生效的



## 二、经济模型

**IOTA没有经济激励机制**。

IOTA 的代币为 MIOTA， **在创世块中已经将所有的代币分配出去**，运行过程中没有新的代币的产生，也就是**没有挖坑**的概念， 所有的代币都从创世块中流动出来。

详细信息如下：

