2.2钱包、私钥、签名与交易

01 地址与私钥

1.地址与私钥

- 比特币的**所有权是通过私钥和地址来确立的**。地址类似于一个银行账户的账号，要想给一个人转比特币，只要知道他的比特币地址就可以了。私钥的作用主要是给交易来签名，用来证明这笔交易是由你发起的，别人收到这笔交易，通过验证签名就可以确认交易中涉及的资金是合法的。

02 地址与私钥

2.与比特币相关的密码学知识

根据加、解密密钥使用策略不同，可将密码体制分为对称密码体制和非对称密码体制。

- 对称密码体制（Symmetric Cryptosystem）：如果一个密码体制中的加密密钥ke和解密密钥kd相同，或者由其中一个密钥很容易推算出另一个密钥，则称为对称密码体制。

- 非对称密码体制(Asymmetric Cryptosystem)如果在计算上由加密密钥ke不能推出解密密钥kd，因此可以将ke公开，这种密码体制也被称为公钥密码(Public Key Cryptosystem)。**比特币使用的就是这种非对称密码体制。**

03 地址与私钥

2.与比特币相关的密码学知识

- 公钥加密发明于20世纪70年代，它是计算机和信息安全的数学基础。自从公钥加密被发明之后，一些合适的数学函数被提出，这些数学函数都是不可逆的，就是说只能向一个方向计算，但不可以向相反方向倒推。
- 在比特币中，公钥用于接收比特币，私钥用于生成其对应地址上支付比特币所必需的签名，以唯一确定这些比特币的所有权。私钥的产生依赖密码学安全的伪随机数生成器
- 私钥空间的大小是2^{256}

04 地址与私钥

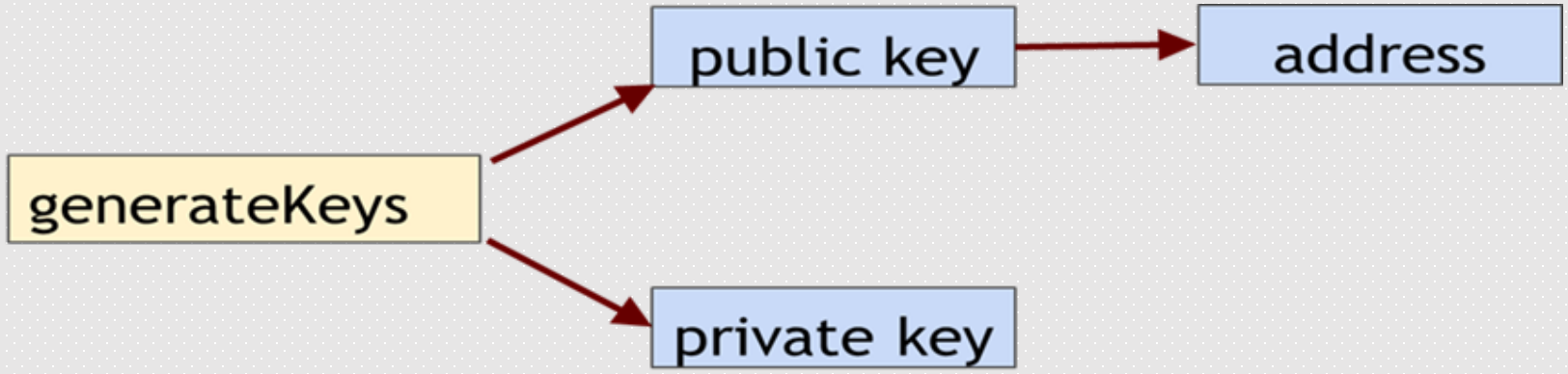
3.比特币地址的生成

- 具体到比特币地址的生成，其实是**先产生私钥**，私钥通过椭圆曲线算法这种不可逆的函数来产生公钥，**公钥经过一系列不可逆的运算再来产生地址。私钥的本质其实是一个随机选出的数字。**

- 你可以用硬币、铅笔和纸来随机生成你的私钥：掷硬币256次，用纸和笔记录正反面并转换为0和1，随机得到的256位二进制数字可作为比特币钱包的私钥。

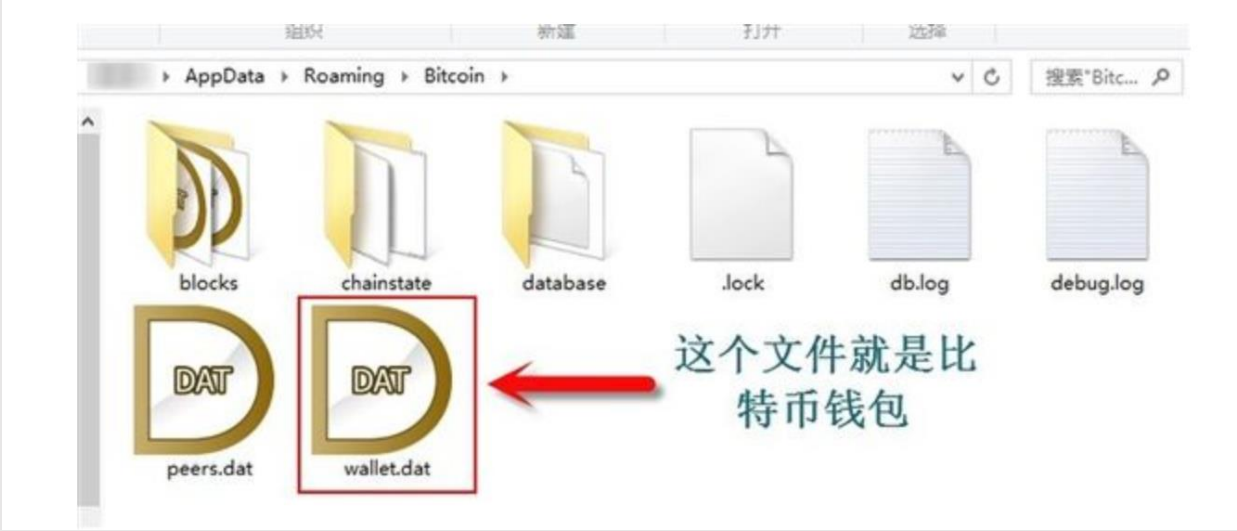
05 钱包

- **私钥持有者才是比特币的拥有者**
- 那么私钥放在哪呢？钱包是私钥的容器。
- 钱包是密钥的管理工具，它只包含密钥而不是确切的某一个代币。一个比特币钱包中包含一系列的密钥对，每个密钥对包括一个私钥和一个公钥。



06 钱包

- 比特币钱包有很多种，有PC端的、手机端的，也有专门的硬件钱包，甚至还有用纸写上私钥的纸钱包。我们一般使用的都是软件钱包，私钥存在一个叫**wallet.dat**的文件中。
- wallet.dat文件其实是用我们自己设置的密码加密过的，登录钱包软件时，需要用户输入密码来对文件进行解密得到真正的私钥，这时私钥存在钱包程序的内存中，当我们需要发起一笔交易时，钱包软件去内存中获取这一私钥来对交易进行签名操作。



07 钱包

冷钱包与热钱包

冷钱包：又被称作离线钱包，从它的生成到使用都是**在非联网状态**下，这类钱包往往依靠不联网的电脑、手机以及其他的硬件设备运行。它的优点是可以完美的避开黑客攻击和木马病毒(因为不联网）但缺点是使用起来比较麻烦，如果要发送交易，需要用中介在离线电脑和在线电脑之间交换交易信息、签名数据，成本较高。

热钱包：是在**联网的状态**下使用的，这类钱包通常以在线钱包和交易平台钱包等形式出现。它的优点是你用起来会很方便，成本低，但缺点是外界可以通过互联网访问到你存储私钥的位置，存在被黑客攻击的可能性。

08 交易

比特币交易就是从**一个比特币钱包向另一个中转账**，每笔交易都有数字签名来保证安全。一个交易一旦发生那么就是对所有人都**公开的**，每个交易的历史**可以最终追溯**到相应的比特币最初被挖出来的那个点。

用户用钱包中的私钥来签名交易，从而证明他们拥有交易的输出，比特币是以交易输出的形式储存在区块链中的。比特币并不存在于任何地方，世界上没有一个可以摸得着的实物，或者是一个数据文件，可以被叫做“比特币”的。有的只是各个地址之间的转账记录，余额时增时减。所有的交易都存放在一个非常大的账本文件中，这个文件叫做“区块链”。

09 交易

2.交易包含的内容

如果 Alice 给 Bob 发送一些比特币，那么这个交易就有三项信息：

1、**输入。**这里面记录了最初 Alice 拥有的这些币是从哪个地址转给她的，我们假设她是从她的朋友 Eve 那里得到的币。

2、**数目。**这个就是 Alice 到底给 Bob 转了多少个比特币。

3、**输出。**Bob 的比特币地址。

除了第一笔交易是矿工的挖矿所得外，**每一笔交易都拥有一个或多个输入，以及一个或多个输出。**

10 交易

2.交易包的内容

第一笔矿工挖矿的收入交易通常被称为Coinbase，它没有输入，所以交易输入的哈希总是被标记为00000000...0000，其他的交易，任何一个交易输入都会唯一追溯到区块链上在本区块之前的某个交易哈希，以及索引。通过交易哈希和索引（从0开始），即可唯一确定一个未花费的交易输出——UTXO（Unspent Transaction Output）。这样，每一个交易输入都和之前的某个交易输出关联了起来。

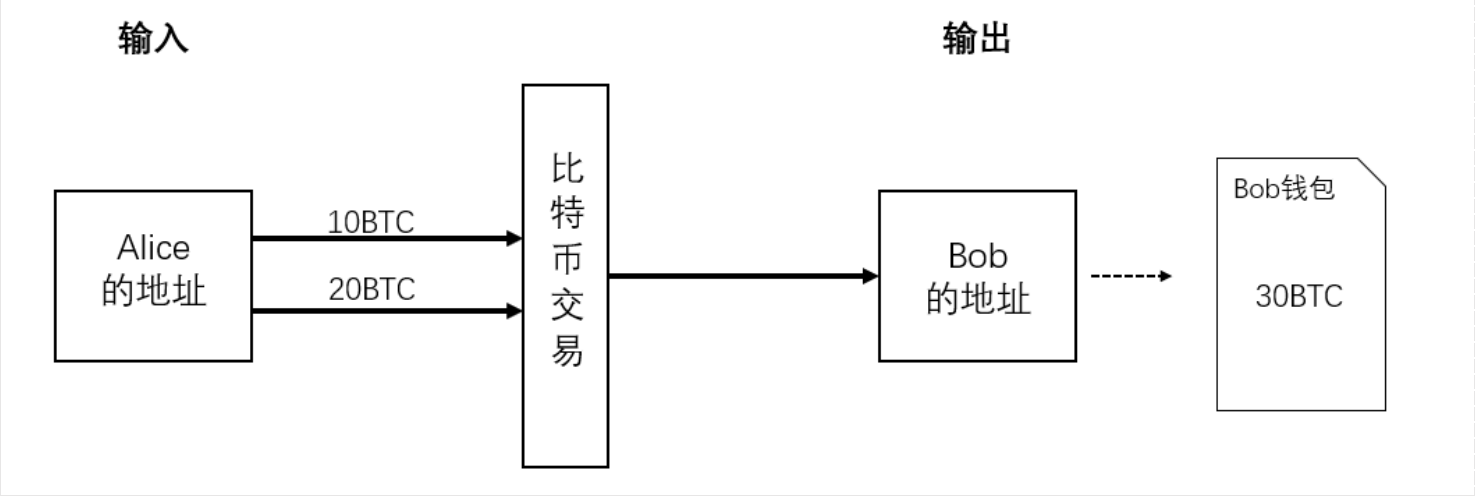
比如，Alice给Bob打过两笔比特币，一笔是10个比特币，一笔是20个比特币，而Bob未向别人支付过比特币，那么，钱包软件显示Bob的比特币余额的时候，其实是把这两笔交易的输出加起来，得到30个比特币这个值。

11 交易

2.交易包含的内容

比特币的交易其实是一个包含输入值与输出值的数据结构。输入与输出都可以有多个。

Alice给Bob打过两笔比特币（一笔是10，一笔是20），现在Bob要给Tom跟Jimmy分别支付5个比特币与20个比特币，因为这时候Alice打给Bob的任何一笔输入都不足以支付这两个输出之和，所以输入也需要两个，Alice向Bob转账的**两笔交易都要作为输入。**

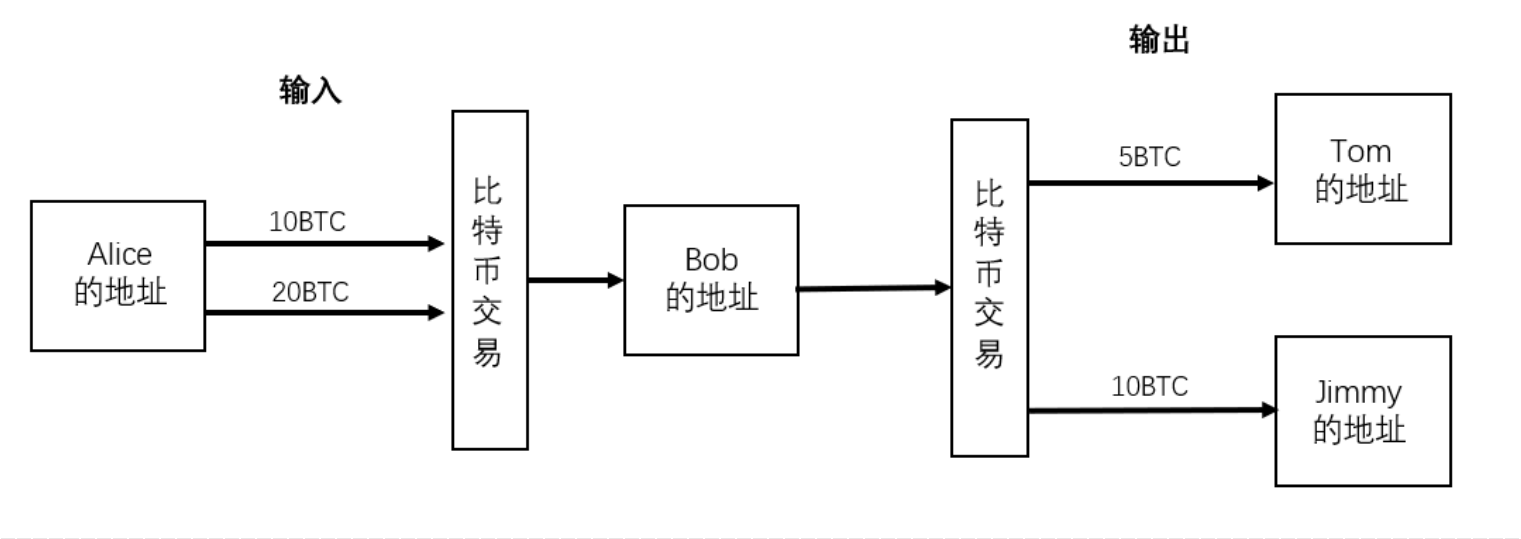


12 签名与验签

为什么其它人不可以引用Alice打给Bob的这两笔交易输出作为输入呢?

这是因为Alice在给Bob转账的时候，加了一个条件，这个条件在比特币交易中叫做**公钥脚本**。在这个例子中，公钥脚本的内容就是使用交易输出的账户地址必须是Bob本人。

那么还有一个问题，其它人可不可以冒充Bob来花费这笔输出呢?



12 签名与验签

签名必须使用私钥，而只有私钥对应的公钥才能验证签名通过。

比特币中还支持多方签名，就是说，如果Bob要使用Alice转给他的这两笔交易输出，不光要Bob签名，Alice也要签名，这样的话，即使其中一人的私钥被盗，也不会丢失比特币了