# 精通比特币一基础

**说明：有些技术内容是从网上搜索得到。**

# 什么是比特币

**术语：深度和高度**

在比特币的区块链上，有两个简单的术语需要说明一下，高度好理解，就是区块的数量，书上也解释了，一个区块一定只有一个高度，但是一个高度并不一定只有一个区块。

深度，从某种意义上来讲，深度和高度有一定的关系，但是并不完全相同，深度是指交易的长度。简易支付验证是通过参考交易在区块链中的深度，而不是高度，来验证它们。

比特币：比特币是构成数字货币生态系统基础的概念和技术的集合。称为比特币的货币单位用于存储和传输比特币网络中的参与者之间的价值。

**它有以下几个特点**：

分布式、弱控制、公开的、集体维护、自治机制、加密的、不可篡改、耦合连接

**它有以下几个主要的技术基础：**

**1、区块** ：构成比特币的基础的数据结构，细节参考精通比特币的相关章节。

**2、点对点技术（peer-to-peer）：**也就是P2P网络，这个是一个比较长远的技术。

**3、哈希算法：**主要算法是Secure Hash Algorithm (SHA)和the RACE Integ rity Primitives Evaluation Message Digest (RIPEMD)，具体地说是SHA256和RIPEMD160

**4、共识机制—工作量证明机制：**POW

工作量证明机制POW（Proof of Work )。POW的基本步骤：

（1）节点监听全网数据记录，通过基本合法性验证的数据记录将其暂存。

（2）节点消耗自身算力尝试不同的随机数，进行制定的哈希计算，并不断重复该过程直至找到合理的随机数。

（3）找到合理的随机数后，生成区块信息，首先输入区块头信息，然后是数据记录信息。

（4）对外部广播出新产生的区块，其他节点验证通过后，链接至区块链中，主链高度加一，然后所有节点切换至新区块后面继续进行工作量证明和区块产生。

每一个验证节点通过随机的散列运算，争夺区块链的记账权，避免双重支付，这一过程需要消耗电力、算力来完成，因此验证节点也称为“矿工”，计算过程称为“挖矿”。

POW中，平均每10分钟有一个节点找到一个区块，一般情况下，需要6个区块的生成时间进行确认，因此一般交易在6个区块（1个小时）后被认为是安全确认且不可逆的。

不过这种说法还是不严谨的。因为在某些特殊情况下，还是会有可能改变的。

**5、时间戳：**这个在书中写得很详细，有各种应用场景，比如延时交易，延时输出，相对时间交易等。

**6、节点信任机制：**在信息不对称的情况下，无需相互担保信任或第三方（所谓的中心）核发信用证书，采用基于互联网大数据的加密算法创设的节点普遍通过即为成立的节点信任机制：节点越多，需要的算力越强，超过51%的节点都通过，才能确立新区块

**7、非对称加密算法：**主要就是椭圆曲线，不过出现了很多其它的算法。

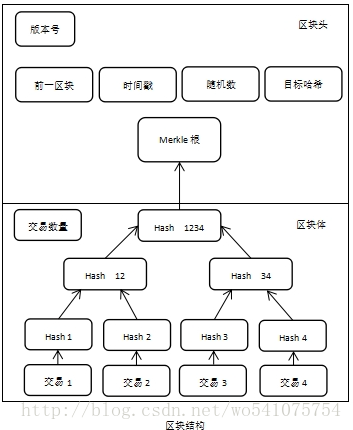
**8、分布式网络：**这里需要说明的一点是，分布式网络不是完全没有中心，而是尽量弱化中心。

**9、Merkle tree 梅克尔树结构**：

https://iwilcox.me.uk/2014/proving-bitcoin-reserves

准备在后期详细展开一下。这里只是简单的讲解一下。默克尔树是很多区块链和P2P网络应用验证的一个方式。只不过有二叉的和N叉的（瑞波最多是18叉）。有一个也有多个。（以太坊是三个）

构造一个默克尔树书上讲的很明白，这里就不再细讲，基本就是拉成一个队列，不是偶数的复制最后一个加到队列尾部，然后两两哈希迭代（注意每次是双哈希，书上有源码，这个源码是基于libbitcoin，大家跳到 bc::bitcoin\_hash,可以看到他是一个SHA(SHA())），直到余下一个，返回即可。



这里想简单说一下验证的过程，验证过程是这样，一个SPV(简单验证)的钱包拿到一笔交易后，得到一个交易的哈希值，那么他就发起一个请求（merkle block message），要求一个全节点提供这个交易的验证的默克尔树的验证路径，（书上讲了，只需要log~2~(N)）,拿到这个验证路径后，SPV再验证一次，如果证明即可。最后，等待六个区块生成，完整交易成功。（不过实际上小额交易大家都不会等待）具体如下：

**在客户端收到merkle block message之后，要执行下面的步骤**：

**前提：已经有很多的包和提供了查找路径的方法**

1、通过上述方法找到包含该交易的区块

2、检查该区块是否是整个网络中最长链条里面的

3、取出所有交易生成merkle tree，利用getProof方法得到该交易的验证路径

4、将该验证路径发送回请求源

**SPV得到响应之后，要做如下验证**：

1、同步区块链，确保是整个网络中最长的一条

2、先拿到merkle root去区块链中查找，确保该merkle root hash是在链条中

3、利用拿到的验证路径，再进行一次merkle校验，确保验证路径全部合法。

为什么SPV还要再做一次merkle校验呢？主要是为了确保响应方发送的验证路径的有效性。

# 比特币的钱包有几种

比特币钱包按书上分类有以下几种：

非确定性（随机）钱包

确定性（种子）钱包

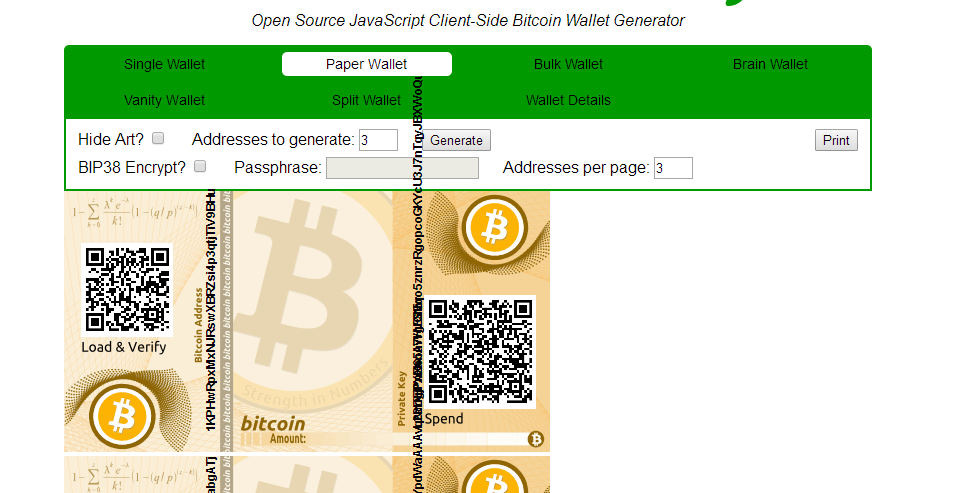
分层确定性钱包（HD Wallets (BIP-32/BIP-44)）

种子和助记词（BIP-39）

按习惯有冷热钱包之分；按在线与否分为在线离线钱包，但其常见的形式主要有：

单钱包，纸钱包，虚荣钱包，批量钱包，分裂钱包





虚荣钱包可能大家听起来有点别扭，其实就是大家认为的靓号，比如连续几个8，几个6，顺子之类的。这个需要专门的机器来不断的哈希碰撞出来，所以会昂贵一些。不过需要注意的是，虚荣钱包可能会出现两种极端情况，一种是很容易被误用，比如ABJ88888XXX,有人换成自己的ABI88888XXX，付款的客户一不小心就付错了。

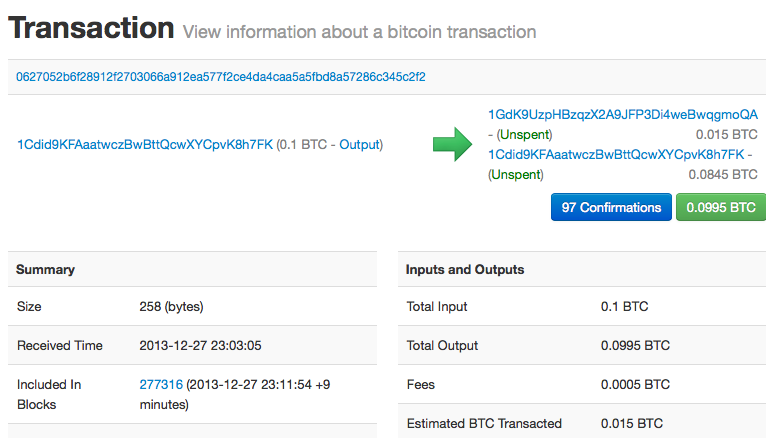
另外一种就是反而更不容易被误用，就是你的靓号更长，这样获得一个类似的号，基本是不可能的。比如连续几十个8.

分裂钱包也比较容易理解，其实就是可以把自己私钥分解成N个私钥，只要持有设定的N个中的M个（M <=N）,就可以还原出正确的私钥。

# 交易的简单过程

P2PKH，P2PK这两个基本类似，前者只是为了省点空间地址。

P2SH（Pay-to-Script-Hash）：其实用脚本的原因，一个目的同上面一样，另外一个就是为了实现更强大的功能，比如多重签名，延迟交易等。



详细的交易过程，书有，这里不再赘述。这里只说明一下，交易必须是基于UTXO的。即未花费的交易。

这里需要注意的是，一个上一个交易的输出是下一个交易的输入；二是交易脚本故意设置成了非图灵完备。

不过，在以太坊的虚拟机EVM，实现了一个准图灵机。

# 找零需要注意的地方

找零的过程没有什么问题，问题是找零的设置，首先，BITCOIN网络在直接交易时，是允许你不设找零地址的，那么余下的币就直接做为了手续费，这在小额交易时还可以忍受，如果你是大额交易，男人哭吧哭吧不是罪。

另外一个是如果使用钱包，虽然没有设置找零的地址，但是钱包会默认给你找一个。一般来说，钱包在生成时会自动生成N个密钥对，目前以100个居多。比特币网络为了保护隐私，一般不建议找零时设置发送的地址，当然，这样不是不可以，只是说会泄露你的秘密。

这样又会带来一个问题，前面说过，钱包有好多种，特别是现在好多的钱包就是基于原来的非确定性钱包的。那么交易一百次后，钱包会再次生成一批密钥对，而这时如果你没有备份，意味着一旦出事情，你的钱包是无法恢复出来全部的币的，结果你应该知道。

不过，最新的记忆型钱或者说分层的确定钱包，应该没有这个问题。

还有一个需要注意的，如果钱包有好多钱，最好每次交易都要在完成后做备份，网上有不少类似的事故，损失有大有小。

# 与第一版的比较

前两章中与第一版基本没有什么区别，不过从后面交易的章节开始就增加了BIP的环节。

**Merkle tree 梅克尔树结构**

**https://blog.csdn.net/pony\_maggie/article/details/74538902**