第06课：区块链...

大家好，我是丹华。今天我们介绍区块链技术的第二个支柱，密码学。这块内容可能比较有技术性，大家有兴趣可以参考一些教材，比如 Christof Parr 的《深入浅出密码学》一书。

密码学技术是整个信息技术的基石。区块链中大量使用了信息安全和密码学技术，包括：哈希算法、非对称加密、数字签名、零知识证明等。

6.1 哈希算法

哈希即 Hash，也称为散列算法。区块链采用密码学哈希算法，保证区块链账本的完整性（不被破坏）。常见的哈希函数包括庞杂的SHA家族等，比特币使用的是 SHA256。

哈希函数是一个数学函数，它具有以下特性：

1. 输入可以是任意大小的字符串；
2. 产生固定大小的输出
3. 能进行有效的计算

哈希算法能将任意大小的二进制数据转换为一串较短的字符串。你可以将哈希输出理解为输入的一个指纹或唯一标记。这个指纹或标记严格依赖于输入的数据，且不泄露输入数据的任何信息。还有防撞击特性：输入数据不同，得到的哈希结果一定不同。

哈希函数具有输入敏感特性。也就是说，如果输入数据发生微小改变——比如改一个字符，那么输出将发生很大的变化。这带来两点好处：第一，你无法通过输出的变化，来推测输入发生了什么变化。第二，保存哈希值可以验证数据是否被篡改。

如果输入数据 A 被篡改为 B，而我们又存储了 A 的哈希值 X，只需对 B 进行哈希运算，看结果 Y 是不是与 X 相同，而且这个验算过程非常简单快捷。如果 Y=X，则 B=A，数据没有被改动。如果 Y≠X，则可断定 B≠A，证明原始数据 A 被篡改了。

以上就是区块链"无法篡改"的机制。在每个区块内，生成包含上一个区块的哈希值，并在区块内生成验证过的交易的 Merkle 根哈希值。一旦整个区块链某些区块被篡改，都无法得到与篡改前相同的哈希值，从而保证，当区块链被篡改时能够被网络节点迅速识别，最终保证区块链的完整性。

6.2 非对称加密

对称加密是指，同一个密钥可以同时用作信息的加密和解密。

非对称加密则需要两个密钥：一个公开密钥（public key）和一个私有密钥（private key）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。并且将公钥公开后，根据公钥无法测算出对应的私钥。

非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。

常见的非对称加密算法包括 RSA 体系。

非对称加密强大的地方在于，它成功实现了在不安全环境中（如公开网络）传递敏感信息，多方通信需要的密钥数量较少，简化了密钥维护工作，而且可用于更强大的数字签名技术。

总结一下，使用公钥加密、私钥解密，完成了乙方到甲方的一次数据传递，通过私钥加密、公钥解密，同时通过私钥签名、公钥验证签名，完成了一次甲方到乙方的数据传递与验证，两次数据传递完成一整套的数据交互。

6.3 Merkle Tree

梅克尔树（Merkle trees）是区块链的基本组成部分，1979年由拉尔夫·梅克尔（Ralph Merkle）申请专利。理论上来讲，没有梅克尔树，区块链也可以实现。但这样每一笔交易的区块头会非常大，这会带来可扩展性方面的潜在困难。

简单的梅克尔树结构类似一个二叉树，所有区块都被两两分组，指向这些区块的指针被存储在上一层的父节点中，而这些父节点再次被两两分组，指向父节点的指针被存储在上一层的父节点中，一直持续这个过程，直到最后达到树的根节点。

利用梅克尔树，可以高效实现区块的隶属证明。假设现在某人需要证明某个数据区块隶属于梅克尔树，我们只需要记住根节点，然后他展示给我们数据区块的信息以及该数据区块通向梅克尔根的哪些数据区块，我们可以忽略梅克尔树的其余部分，而通过只该分支的数据到达这个目的。这点可以支持钱包的轻客户端开发。

比特币钱包服务用 Merkle Tree 的机制来作“百分百准备金证明”。过程是构建 Merkle Tree，当构建完该树，且根节点的余额与公布的储蓄地址余额相同，即证明了100%储备。

以太坊使用了更复杂的 Merkle Patricia Tree 技术。

6.4 数字签名

数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送者的公钥才能解密被加密的摘要信息，然后用 Hash 函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

数字签名是个加密的过程，数字签名验证是个解密的过程。

数字签名技术可以保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。实际上，数字签名是对纸质文档中广泛存在的公章、骑缝章、骑缝签名的数字对应物和颠覆。

有效的数字签名给了参与方一个坚强的理由去相信：

1. 该消息是由已知的发送者（身份认证）创建的；

2. 发送方不能否认已发送消息（不可否认性）；
3. 消息在传输中未被更改（完整性）。

比特币中使用的数字签名算法是椭圆曲线数字签名算法 ECDSA（Elliptic Curve Digital Signature Algorithm）。ECDSA 是用于基于椭圆曲线私钥/公钥对的数字签名的算法。

6.5 零知识证明

战争中你被俘了，敌人拷问你情报。你是这么想的：如果我把情报都告诉他们，他们就会认为我没有价值，就会杀了我；但如果我死活不说，他们也会认为我没有价值而杀了我。怎样才能做到既让他们确信我知道情报，但又一丁点情报也不泄露呢？这就是零知识证明的问题情境。

零知识证明（Zero—Knowledge Proof），是由三位数学家 S.Goldwasser、S.Micali 及 C.Rackoff 在20世纪80年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

零知识证明就是既能充分证明自己是某种权益的合法拥有者，又不把有关的信息泄露出去——即给外界的“知识”为“零”。

早在16世纪文艺复兴时期，意大利有两位数学家抢夺一元三次方程求根公式发现者的桂冠，就采用了零知识证明。当时，数学家塔尔塔里雅和菲奥都宣称自己掌握了这个求根公式。为了证明自己没有说谎，又不泄露公式的具体内容，他们摆开了擂台：双方各出30个一元三次方程给对方解，谁能全部解出，就说明谁掌握了这个公式。比赛结果显示，塔尔塔里雅解出了菲奥出的全部30个方程，而菲奥一个也解不出。于是人们相信塔尔塔里雅是一元三次方程求根公式的真正发现者，虽然当时除了塔尔塔里雅外，谁也不知道这个公式到底是个什么样子。

零知识证明的优点包括，不降低安全性，工作高效，计算过程量小，双方交换信息少。数字货币 ZCash 就使用了零知识证明，在整个交易过程中实现完全匿名。

不是小结

最后，下图5.1 给出一个比特币系统中从公钥到比特币地址的一个密码学过程，方便读者能够对密码学在比特币中的具体应用有一个最小的、直观的理解。

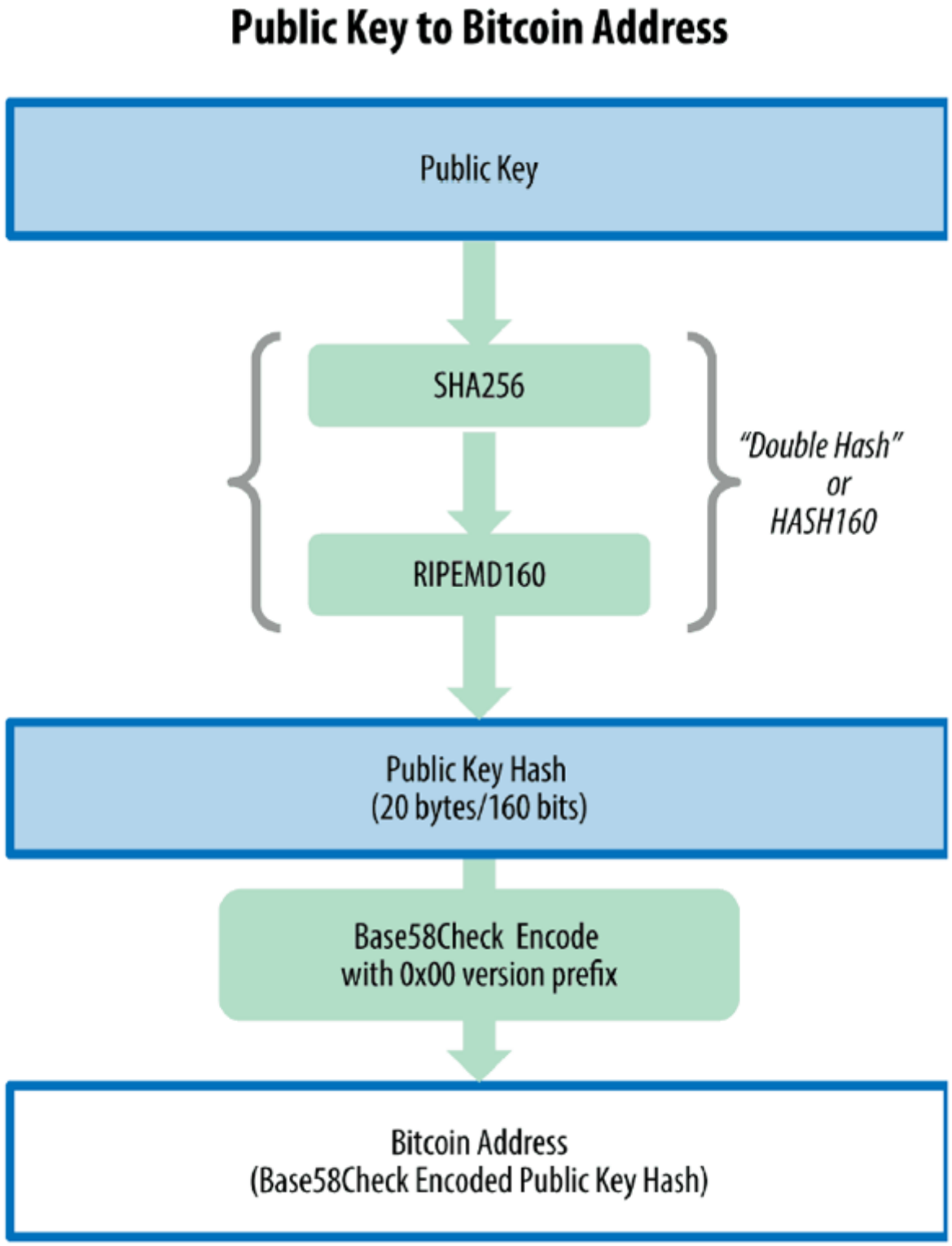

图5.1 比特币中从公钥到地址的密码学过程（摘自 *Mastering Bitcoin* 一书）