区块链技术中的密码应用

李 晶

随着比特币的出现，其底层区块链技术的去中心化、去中介化、不可篡改等优势逐步引起了政府的关注和企业的推崇。从本质上讲，区块链综合运用了 P2P 网络、共识机制和诸多密码学方法，生成信息强相关的数据库并分布存储，增强了系统运行的平稳性和健壮性。

本文将介绍几种出现在区块链技术中的密码算法和方案，包括杂凑算法、数字签名算法、零知识证明和同态加密等。

1. 区块链简介

区块链使用多种密码学工具将数据区块以时间顺序相连，形成一种不可篡改、不可伪造的链式数据结构。

常见的区块链（比如说比特币）的工作流程主要包括如下步骤：

1) 交易节点将交易信息签名，并向全网广播；

2) 接收节点对收到的数据进行完整性、认证性检验，通过检验后，数据记录将被纳入到一个区块中；

3) 全网所有接收节点对区块执行共识算法（工作量证明、权益证明等）；

4) 区块通过共识算法过程后被正式纳入区块链中存储，全网节点执行共识规则接受该区块，而接受的方法，就是将该区块的哈希值视为最新的区块哈希值，此后新区块的制造将以该区块链为基础进行延长。

密码学工具的应用，主要体现在：第 1）步中，杂凑算法生成交易双方地址并确保地址的唯一性和随机性，数字签名算法确保交易信息的不可伪造性，多重签名算法可进一步增强；第 2）步中，杂凑算法确保数据的完整性，并通过 Merkle-Tree 机制有效打包大量交易信息；第 3）步中，杂凑算法的输出随机性保证了工作量证明机制的有效性以及新数据块 ID 的唯一性。此外，环签名、零知识证明、同态加密等算法可以增强 1）和 2）的隐私保护。

2. 区块链技术中的密码算法

2.1 杂凑算法

杂凑（Hash）算法，也被称为杂凑函数，能够将任意长度的信息压缩为固定长度的输出值，这个固定长度的输出值通常是一个随机数，也被形象地称作输入消息的“摘要”或“指纹”，具有定长性、单向性和抗碰撞性。源于这三个特性，以及输出的随机性，杂凑算法被反复应用到区块链技术中，比如工作量证明（区块的产生过程）、Merkle Tree 以及地址的生成等。

2.1.1 工作量证明

比特币中设计了工作量证明机制控制比特币发放的数量和速度，技术上依靠杂凑算法输出值的随机性实现。矿工通过不断修改随机数 Nonce 的值，重复计算区块头的 Hash，使得 Hash(Nonce) < Target，其中 Target 是合格区块的量化指标，最终满足条件的 Hash(Nonce) 即为新产生区块的 ID。

在区块链技术应用中，比特币、域名币等使用了 SHA256 算法；后续随着显卡挖矿及矿池的出现，为了更强地抵御矿机优化，莱特币、狗狗币等采用了一位著名黑客开发的 SCRYPT 算法；以太坊使用了 Ethash 算法；Zcash 使用了由 Alex Biryukov 等发明的 Equihash 算法。这些算法通过增加计算量、内存规模等方式降低了矿机的运行速度。

对于具体杂凑算法的应用，主要包括串联杂凑算法和并联杂凑算法两种。

串联杂凑算法就是对输入数据进行多次 hash。2013 年 7 月，夸克币（Quark）首创使用 9 轮 Hash 算法，即对输入数据运算了 9 次 hash 函数，前一轮运算结果作为后一轮运算的输入。Quark 共使用 6 种杂凑算法，分别为 BLAKE、BMW、 GROESTL、JH、KECCAK 和 SKEIN。受此启发，达世币进一步使用 11 种杂凑算法（X11），接着 X13，X15 这一系列被开发出来。但这种串联算法事实上降低了应用安全性，因为其中任何一个算法的碰撞，都将导致最终的碰撞。

为了提高交易效率，HeavyCoin 率先尝试了并联杂凑算法，其运行机制如下：

1）对输入数据 x 首先运行一次 HEFTY1 运算，得到结果 d1；

2）以 d1+x 为输入，依次进行 SHA256、KECCAK512、GROESTL512、BLAKE512 运算，分别获得输出 d2、d3、d4 和 d5；

3）分别提取 d2-d5 前 64 位，混淆后形成最终的 256 位 Hash 结果，作为区块 ID（如图 1）。

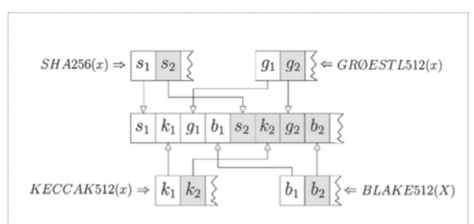

图 1

HeavyCoin 将四种算法并联在一起，其中一种算法被破解只会危及其中 64 位，四种算法同时被破解才会危及货币系统的安全性。

2.1.2Merkle Tree

在区块的构建过程中，Merkle Tree 被用来通过杂凑函数归纳一个区块中的所有交易信息，同时生成整个交易集合的数字指纹，且提供了一种校验区块是否存在某笔交易的高效途径。生成一棵完整的 Merkle Tree 需要递归地对杂凑节点对进行杂凑，并将新生成的杂凑节点插入到 Merkle Tree 中，直到只剩一个杂凑节点，该节点就是 Merkle Tree 的根（如图 2 所示）。比特币的 Merkle Tree 中使用了两次 SHA-256 算法，也被称为 double-SHA-256。

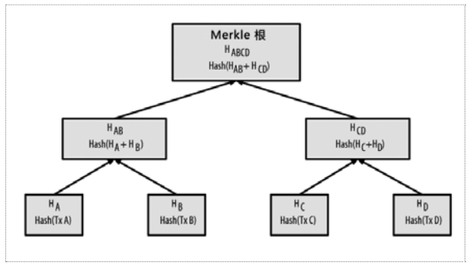

图 2 在 Merkle Tree 中计算节点

2.1.3 地址生成

在一些加密货币交易的支付环节，收件人的公钥是通过其数字指纹表示的，称为地址，就像支票上的支付对象的名字（即“收款方”）。借助于杂凑算法的输出随机性和不可逆特性，地址在一定程度上能够起到匿名效果。比特币地址是由公钥经过 SHA-256 算法和 RIPEMD-160 算法通过杂凑得到的。

2.2 数字签名

数字签名是电子签名的一种重要技术，能够解决电子数据交换过程中的伪造、抵赖、冒充和篡改等问题，利用杂凑函数压缩技术和公钥加密技术，使收发数据双方确保：接收方能够鉴别发送方所宣称的身份，发送方以后不能否认其发送过该数据这一事实。

在区块链技术的应用中主要使用椭圆曲线算法进行签名 / 验签，如比特币使用 Secp256k1 标准所定义的椭圆曲线（，该曲线在素数阶 p 的有限域内，）。签名算法使用私钥和公钥，私钥用于对交易进行签名，将签名与原始数据发送给整个比特币网络，公钥则用于整个网络中的节点对交易有效性进行验证。

在个别应用中，为了提升交易的安全性采用了多重签名，为了增强区块链的隐私保护应用了环签名。

2.2.1 多重签名

为进一步提高交易的安全性，比特币引入了多重签名，即比特币地址需要多个签名才能支付，从而保证资金的安全。多重签名的实现采用比特币脚本的方式，它设置了这样一个条件，假如记录在脚本中的公钥个数为 N，则至少需提供其中的 M 个公钥才可以解锁，也被称为 M-N 组合。

在后续的区块链技术中，以太坊、币须网等都引入了多重签名。

2.2.2 环签名

为了增强区块链的隐私保护，隐藏签名者的身份，环签名是一种可行的解决办法。在环签名方案中，环中一个成员可以利用他的私钥和其他成员的公钥进行签名，但却不需要征得其他成员的允许，而验证者只知道签名来自这个环，但不知道谁是真正的签名者。环签名解决了对签名者完全匿名问题，环签名允许一个成员代表一组人进行签名而不泄漏签名者的信息。

环签名在 Bytecoin、暗币网、门罗币、ShadowCash、以太坊等中均有使用。

2.3 零知识证明

零知识证明是一种在无需泄露数据自身信息的前提下证明某些数据运算的一种密码技术，允许两方（证明者和验证者）来（被）证明某个提议是真实的，且无需泄露除了它是真实的之外的任何信息。零知识证明具有完备性、合理性、零知识性，在区块链技术中实现了信息匿名化，从而保护用户的隐私。

目前，在区块链技术中，零知识证明主要应用在 Zcoin 和 Zcash 加密货币里，达到了零知识级匿名。Zcoin 通过零币协议能够隐藏交易发送者和交易接收者，但不能隐藏交易信息。Zcash 使用了简洁的非交互式参数的知识 (zk-SNARKs)，通过 Zerocash 协议保护账务隐私。Zcash 的匿名性，归功于 zk-SNARKs 的真实性，它利用一个公有链来展示交易，但会隐藏掉交易的金额。

2.4 同态加密

同态加密是一种无需对加密数据进行解密就可以实现某些计算的方法。它允许人们对密文进行特定的代数运算得到新的密文，将其解密所得到的结果与对相应明文进行同样的运算结果保持一致。

在区块链技术应用中，同态加密技术可以加密公有链上的数据以保护隐私，且并不改变其为公有链的属性；同时，可以随时对公有链上的加密数据进行审计。

同态加密技术可以在以太坊的智能合约中实现，如管理员工开支。在这个使用案例中，员工可以加密他们的开支详细信息来保护他们的隐私，在智能合约上经过加密的开支信息会被算入总开支。当公司会计想要分析开支时，可以在本地对最终的智能合约进行解密，将总开支详细分解开。这样只有最终机构能够看到开支详细信息，其他的用户则只能看到一些加密的条目。

3. 总结

安全评估与防御一直是区块链技术发展过程中的重要研究对象。在这其中，密码算法起到了关键支撑作用。杂凑算法、数字签名算法保障了区块链技术的不可篡改性和不可伪造性，多重签名进一步强化了不可伪造性，环签名、同态加密、零知识证明等在不同程度上保障了用户的隐私性。但这些算法 / 方案中，只有杂凑算法能够较好地抵御量子攻击，所以研究如何保护区块链技术不受量子攻击破坏仍是一个未解难题。

此外，研究如何管理密钥、确保数据安全也是区块链技术研究中的重要内容。