国产密码体系在区块链中的应用与挑战

文｜北京大学信息科学技术学院教授、区块链研究中心主任 **陈钟** 北京大学软件工程国家工程中心 副研究员 **关志**

区块链技术在国内应用越来越广泛，区块链中涉及大量的密码学技术，在某些关键领域，这些密码学技术必须符合国家密码标准，因此了解国产密码体系及其在区块链上的应用就显得十分重要。

一、国产密码体系

随着《网络安全法》和《密码法》的发布，信息安全受到空前重视从而上升至国家战略层面，密码作为网络安全的核心技术，在保障信息安全方面起着极大的作用，构建以国产密码为基础的网络空间安全体系已经刻不容缓。实际上自 2012 年以来，国家密码管理局就以《中华人民共和国密码行业标准》（以下简称《国密行标》）的方式，发布了一系列的国产密码算法，并以此为核心，对涉及的国产密码硬件，安全通信协议、认证协议、密码编程接口和密码应用进行了规范，此外，对基于国产密码的设备管理、设备检测、密钥管理和可信计算也制定了相关标准。目前，我国已经建立起一整套比较完备的国产密码标准体系，在国民经济和社会信息化发展发挥了重要作用。国密标准体系如图 1 所示。

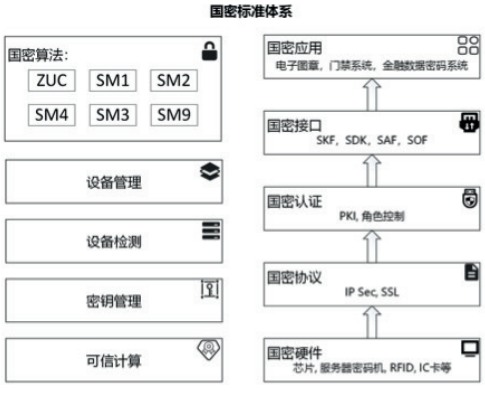

图 1 国密标准体系

1. 国密算法简介

国密算法是中国国家商用密码算法的简称，也是国密体系的核心所在，主要包括 SM2/SM3/SM4 等密码算法标准及其应用规范，其中“SM”代表“商密”，即用于商用的、不涉及国家秘密的密码技术。其中 SM2 为基于椭圆曲线密码的公钥密码算法标准，包含数字签名、密钥交换和公钥加密，用于替换 ECDSA、ECDH、RSA 等国际算法；SM3 为密码杂凑算法，用于替代 MD5/SHA–1/SHA–256 等国际算法；SM4 为分组密码算法，用于替代 AES、3DES 算法；SM9 为基于身份的密码算法，可以替代基于数字证书的 PKI/CA 体系。通过部署国密算法，可以降低由弱密码和错误实现带来的安全风险和部署 PKI/CA 带来的开销。

2. 国密算法分类

我们可以将国密算法分为对称密码算法、非对称密码算法、哈希密码算法三类，对称密码算法包括分组密码算法 SM4 和流密码算法 ZUC；非对称密码包括 SM2 和 SM9 算法；哈希密码算法包括 SM3。下面我们对主要的密码算法进行简单的介绍。

SM4 是我国无线局域网标准 WAPI 中所采用的分组密码标准，随后被我国商用密码标准采用。作为我国商用密码的分组密码标准，预计 SM4 在国内的敏感但非机密的应用领域会逐渐取代 3DES、AES 等国外分组密码标准，用于通信加密、数据加密等应用场合。

祖冲之 (ZUC) 序列密码算法是国家密码管理局公布的《国密行标》中的对称密码算法之一，这个算法也是 3GPP LTE 中的三个算法标准之一。在 3GPP LTE 标准中使用了基于祖冲之的 128–EEA3 加密算法和 128–EIA3 完整性算法。目前国密标准中的对称加密算法包括 SM4、SM1、SSF33 三个分组密码和 ZUC 序列密码，SM1 和 SSF33 仅有硬件实现，而 SM4 在通用处理器上的软件实现性能较慢，ZUC 是用于高速加密软件实现的一个较优选择。

SM2 椭圆曲线公钥密码算法是由国家密码管理局在 2012 年发布的一系列基于椭圆曲线密码的密码标准（GM/T 0003.2–2012 SM2 椭圆曲线公钥密码标准），这

些标准以《国密行标》发布，其中包含 SM2 数字签名算法（参见 GM/T 0003.2–2012 中的第 2 部分）、密钥交换协议、公钥加密算法以及推荐的 256 比特素数域椭圆曲线参数（参见 GM/T 0003.2–2012 中的第 5 部分：参数定义）。

SM9 数字签名方案是国密标准中两个数字签名算法标准之一，也是国密 SSL 协议中几个密码套件采用的签名算法，因此可以预计会成为一个应用较为广泛的重要数字签名算法。

SM3 密码杂凑函数是由中国国家密码管理局公布的中国密码行业标准，用于在商用领域中取代 SHA–1、SHA–2 等国外算法。SM3 也是目前中国商用密码标准体系中唯一的密码杂凑函数，是 SM2 公钥密码算法、SSL VPN 协议等商用密码标准中的关键组成部分。由于目前使用最广泛的 Intel/AMD X86 处理器和 ARM 处理器并不提供 SM3 算法的硬件实现，因此如何在这些通用处理器上提供 SM3 算法的高性能软件实现对 SM3 算法的实际应用具有重要的意义。

二、关于区块链

1. 区块链简介

区块链技术最早来源于比特币，区块链是一类综合利用对等网络、密码学算法、分布式共识协议、脚本语言等技术的分布式数据存储与计算系统，有时也将区块链称为分布式账本（Distributed Ledger）。比特币采用分布式对等网络架构，利用数字签名技术验证交易合法性，以基于工作量证明（Proof–of–Work，PoW）的共识算法同步节点历史数据，结合内在的经济激励机制，最终构成一个可持续的、不依赖可信第三方的电子现金系统。在比特币中，历史交易以区块（Block）的方式组织为单向增长的线性数据结构，并通过密码学算法和分布式共识机制保证数据完整性和不可篡改性。去中心化、不可篡改、可编程是区块链的三大关键特性。

2. 区块链中的密码算法

区块链基础架构中的密码算法整体上分为哈希算法和非对称加密算法。区块链以区块形式封装交易并通过加密哈希将块链接在一起。图 2 显示了区块链的基本结构。区块链中的每个区块都包含一个区块头以及交易集，每个块都包含了前一块的哈希时间戳和其他一些块字段（例如，版本，随机数）。比特币主要使用的哈希算法是 SHA–256 算法，在比特币中，使用哈希算法把交易生成数据摘要，当前区块里面包含上一个区块的哈希值，后面一个区块又包含当前区块的哈希值，就这样一个接一个的连接起来，形成一个哈希指针链表。其中，默克尔根哈希 (Merkle Root Hash) 是交易集默克尔树的一个承诺 (Commit)。它其实是一个用哈希指针建立的二叉树或多叉树。比特币中对每一笔交易做一个哈希计算，然后把每 2 个交易的哈希结果再进行合并做哈希计算，如图中 2 中的第 n+2 个区块中，交易 A 的哈希值是 hA=H(A)，交易 B 的哈希值是 hB=H(B)，再对这 2 个交易合并哈希计算后就是 hAB=H(hA|hB)，就这样一直往上合并计算，算到最后的根部就是默克尔根哈希了。在区块链中，每个用户都有一对密钥（公钥和私钥），比特币系统中使用用户的公钥的哈希值作为交易账户地址。

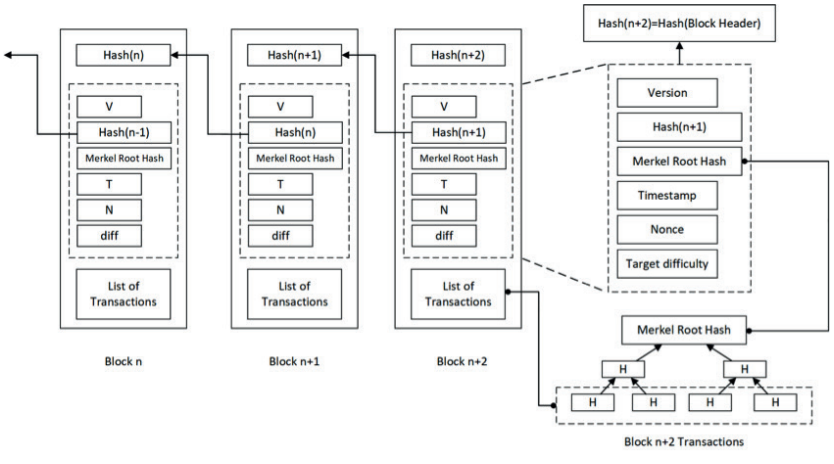

图 2 区块链结构示意

3. 区块链的分类

整体上说，区块链主要分为三大类：公有链、私有链和联盟链。比特币、以太坊等均属于公有链，公有链不对参与用户的身份进行验证，任何人都可以加入到区块链的网络中，有着更好地去中心化性，但这对

于某些企业应用来说可能并不适合。企业可以针对自己的业务需求搭建私有链，但是私有链存在信息孤岛的问题。联盟链介于私有链和公有链之间，其由参与成员机构共同维护，并提供了对参与成员的管理、认证、授权、监控、审计等全套安全管理功能。

4. 区块链中的隐私问题

对于公有链而言，区块链上的数据可以由所有的节点访问，所以其隐私和安全就变得尤为重要。公有链的隐私主要分为身份隐私和交易隐私，身份隐私主要指的是区块链地址信息与现实生活中的身份的相对应的关系。交易隐私指的是区块链上公开的信息如输入地址、输出地址、交易金额以及地址之间的关系等。身份和交易信息是用户的关键数据，一旦泄露可能会对用户造成危害。

区块链特殊的架构，使得其隐私的保护不同于传统的隐私保护方式。针对区块链的隐私保护，出现了很多密码学方案：门罗币 (Monero) 使用同态加密的方式在隐藏交易实际数额的同时也支持交易的审核，同时使用环签名构建了匿名的数字加密货币，为用户提供更强的隐私性，通过使用隐蔽地址来隐藏交易数据。大零币 (Zcash) 利用零知识证明的方式进行交易，在满足验证和共识机制下隐藏交易的发送方，收款方和交易金额等。达世币 (Dash) 增加了基于主节点的混币政策，隐藏资金的流向。

三、国密算法在区块链中的应用和挑战

1. 应用与挑战

目前各主流区块链公司都有尝试将国密应用在区块链上，这些工作主要集中在：(1) 用 SM3 代替 SHA–256 等作为默认的密码杂凑算法；(2) 用 SM2 替代 ECDSA 签名算法；(3) 用 SM2 证书代替 RSA、ECDSA 证书。对于上层的协议如 SSL 则涉及较少，与区块链相关的硬件设施（如硬件钱包）也很少采用国密标准（如 SKF）进行设计。此外区块链中比较热门的密码学协议如：零知识证明、多方安全计算等，因为国密中并没有针对性的标准，很难将其国密化。

因为国密算法的开发及优化涉及大量的专业知识且工作量巨大，多数公司还是选择开源的国密实现（如 GmSSL）在区块链系统上进行集成，由于这些区块链系统在设计之初并没有考虑国密的兼容性问题，集成的工作量仍然很大，为了解决这个问题，HyperLedger 成立了 URSA 项目，旨在为 fabric 等底层区块链系统打造一个支持多数密码算法（包含国密）的密码库。

随着区块链领域对共识算法、签名方案、隐私保护、数据安全共享等需求的不断发展变化，国产密码体系涵盖的基础密码已经无法满足区块链的应用需求，亟需能够和现有国产密码安全参数保持兼容的一系列新型密码方案，区块链领域的特殊性使得和密钥、密码消息有关的数据格式和传统 PKI 体系有一定差异，因此也需要制定有针对性的规范。区块链，特别是公有链，通常需要在全球范围内部署，因此国产密码体系需要国际化，不仅是算法和标准的公开，还需要设计原理和安全参数选择的公开透明。

一个成功的区块链系统的部署运行生命周期完全可能超过某个密码算法标准的生命周期，目前国产密码标准中的算法的安全性均为 128 比特，不包含支持抗量子计算机的算法，也不支持适用于物联网的轻量级密码算法。区块链应用国产密码算法的同时也应注意密码算法的灵活性，区块链系统在设计上满足可以在无需硬分叉的条件下替换或更新密码算法，以满足应用场景、合规性、性能或者安全性的要求。

2. 对策与建议

随着区块链底层技术研发及应用加速推进，其中的国密算法应用与创新也真正提到议事日程，加强我国联盟链方面的自主创新研究与开发迫在眉睫。结合北京大学多年在 GmSSL 开源项目及作为 Hyperledger 大学会员的研究与实践，我们认为国密算法体系应对挑战可以从以下几方面着手：（1）加快推进现行国密算法在区块链底层技术的应用研究、实验、验证和标准化工作，制定相关应用指南；（2）进一步拓展国密算法体系，包括更为丰富的加密、签名、共识、安全多方计算等方案，并逐步实现标准化；（3）进一步研究硬件密码处理模块对区块链系统的支撑与集成应用，在物联网、工业互联网等领域加速推进协同创新；（4）加大力度推进国际合作，在合作中提升和发挥我们原始创新和引领能力，扩大技术及应用的影响力。