基于属性密码体制的区块链安全技术研究进展

陈 露[1,2,3],相 峰[4],孙知信[1,2,3]

(1. 南京邮电大学江苏省邮政大数据技术与应用工程研究中心,江苏南京 210003;
2. 南京邮电大学国家邮政局邮政行业技术研发中心(物联网技术),江苏南京 210003;
3. 南京邮电大学宽带无线通信技术教育部工程研究中心,江苏南京 210003;
4. 物流信息互通共享技术及应用国家工程实验室,上海 200000)

摘 要: 区块链是一种集合了分布式存储、点对点传输、共识机制、密码学算法和智能合约等关键技术的分布式账本,具有去中心化、不可篡改、透明化等特性.近年来区块链技术的安全性问题逐渐显露,阻碍了区块链应用的发展.本文介绍了区块链的基本概念与安全模型,分析了区块链的安全性问题;然后,基于属性密码体制,从访问控制、密钥管理、数据隐私保护这三个方面分析了区块链安全技术的各类研究,论述了主要的解决方案的特点;最后,总结了基于属性密码体制的区块链安全技术研究进展,并对未来的研究工作进行了讨论.

关键词: 区块链安全; 密码学; 属性加密; 属性签名

中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2021)01-0192-09

电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20191375

A Survey of Blockchain Security Technologies Based on Attribute-based Cryptography

CHEN Lu[1,2,3], XIANG Feng[4], SUN Zhi-xin[1,2,3]

(1. *Engineering Research Center of Post Big Data Technology and Application of Jiangsu Province, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*;
2. *Research and Development Center of Post Industry Technology of the State Posts Bureau (Internet of Things Technology), Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*;
3. *Engineering Research Center of Broadband Wireless Communication Technology of the Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*;
4. *National Engineering Laboratory for Logistics Information Technology, Shanghai* 200000, *China*)

Abstract: Blockchain is a distributed ledger that integrates key technologies such as distributed storage, peer-to-peer transmission, consensus mechanism, cryptographic algorithm and smart contract. It has the characteristics of decentralization, non-tampering, transparency and so on. In recent years, security problems of blockchain have gradually emerged, hindering the development of blockchain applications. This paper introduces the basic concept and security model of the blockchain, and analyzes the security problems of the blockchain. Then, based on the attribute-based cryptography, the various researches of the blockchain security technology are analyzed from the three aspects of access control, key management, and data privacy protection, and the characteristics of the main solutions are discussed. Finally, we summarize the research progress of the blockchain security technology based on the attribute-based cryptography, and discuss the future research work.

Key words: blockchain security; cryptography; attribute-based encryption; attribute-based signature

1 引言

区块链的概念最早于 2008 年由区块链之父中本聪在比特币白皮书[1]中阐述,是利用密码学技术保证数据的不可篡改性和不可伪造性,利用分布式节点共识算法生成和更新数据,利用自动化脚本代码编程和操作数据的一种全新的去中心化基础架构与分布式计算范式[2].区块链的本质是一种去中心化、不可篡改、可

收稿日期:2019-12-13;修回日期:2020-07-01;责任编辑:李勇锋
基金项目:国家自然科学基金(No. 61672299, No. 61972208);江苏省研究生科研创新计划(No. SJKY19-0770)

追溯、多方共同维护的分布式数据库[3],它的共识机制有效地解决了拜占庭将军问题[4,5]以及双重花费问题[6].

区块链技术在金融领域最早且最广泛的应用是比特币.自比特币以来,不同的区块链技术催生了不同的加密货币,目前正在全球范围内进行交易[7].区块链的应用还包括医疗、农业、物联网等[8]领域.然而,随着区块链应用的蓬勃发展,其安全性问题逐渐显露.2014年,著名比特币交易平台 Mt. Gox 遭到交易延展性攻击[9],85 万枚比特币被盗.2017 年,麻省理工学院的学术研究专家组通过邮件的方式提醒 IOTA 的哈希算法 Curl-P 存在漏洞,引起了学术界在区块链密码学安全技术方面的关注.区块链中现有的密码学技术难以适应区块链的分布式环境与细粒度的访问控制等需求,阻碍了区块链应用的扩展.属性密码体制[10]属于公钥加密体制,它将属性作为公钥,并将它们与密文或用户的密钥相关联,这种模式适合分布式计算环境,具有广阔的应用领域[11].基于属性密码体制所具有的优势,学术界已有学者提出采用属性密码体制来解决区块链应用在功能以及安全方面存在的问题[12~15].

2　区块链与属性密码体制概述

2.1　区块链基本概念及安全模型

根据访问权限的不同,区块链可分为公有链、联盟链和私有链.以比特币为例,区块链的结构如图 1 所示,区块按照时间顺序排列形成链式结构,其他不同开放程度的区块链结构与其大致相同.区块由区块头和区块体组成.区块体中存储交易数据,交易数据的哈希值存储于 Merkle 树的叶子节点中,再进行两两哈希,最终形成 Merkle 根.区块头包含了版本号、时间戳、难度值、随机数、Merkle 根,以及前一区块的哈希值.区块之间通过前一区块的哈希值连接,形成链式结构.

区块链通过链式结构与 P2P 网络实现数据的分布式存储与去中心化特性;利用共识机制使网络中的节点达成一致,确保数据的一致性;采用密码学技术保障区块中信息的完整性、可追溯性、不可篡改性;并支持用户创建灵活的智能合约,极大地扩展了区块链的应用.

近年来国内外针对区块链安全的学术研究显著上升[16~20].交易、用户信息、智能合约等大量数据的存储使得区块链面临隐私泄露的风险;区块链中的大量密钥缺乏安全有效的管理,存在泄露的风险;一对一加密机制不满足目前区块链应用中复杂的访问控制需求,也不利于数据的安全共享.如图 2 所示,区块链安全模型从下至上可抽象为三个层次.

数据层:主要包含区块结构,链式结构与交易信息.数据层利用多种密码学技术如哈希函数、非对称加密

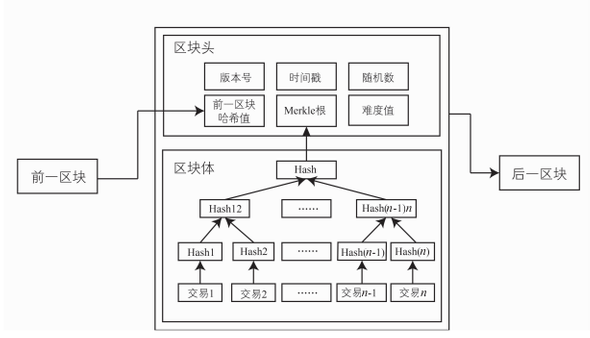

图1　区块链结构

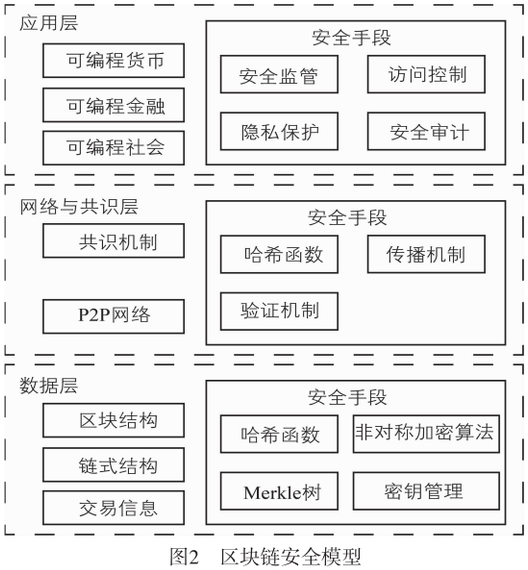

图2　区块链安全模型

算法、Merkle 树、密钥管理等来保证安全性.

网络与共识层:主要包含区块链的组网方式和共识机制;区块链采用 P2P 网络进行点对点传输,节点验证交易并将其存储于区块,节点通过共识机制保证区块链的一致性.网络与共识层利用哈希函数、数据的传输机制与验证机制来保证安全性.

应用层:主要包含各种基于区块链的上层应用和平台;应用层利用安全监管、访问控制、隐私保护和安全审计等手段来保证安全性.

从区块链安全模型的构成来看,密码学技术存在于区块链安全模型每一层,它是区块链技术的重要支撑.

2.2　属性密码体制及其应用

属性密码体制的研究主要可分为属性加密(Attribute-Based Encryption,ABE)和属性签名(Attribute-Based Signature,ABS)两大类.

ABE 可分为密钥策略属性加密(Key-Policy Attribute-Based Encryption,KP-ABE)[21]和密文策略属性加密(Ciphertext-Policy Attribute-Based Encryption, CP-ABE)[22].

CP-ABE 将密文对应于访问结构,密钥对应于属性集合,这种机制常用于云存储与细粒度共享. KP-ABE 中,用户私钥基于访问结构,密文对应于属性集合,适用于静态场景,例如付费视频、日志加密管理等.

ABS 是模糊身份签名体制[23]的扩展,它通过属性对签名者进行定义,向验证者确保消息由签名者签名,有助于在匿名身份验证系统中提供细粒度的访问控制.

3 基于属性密码体制的区块链安全

本节将从访问控制、密钥管理、数据隐私保护三个方面分析属性密码体制在区块链安全中的研究进展.

3.1 区块链访问控制

3.1.1 未使用属性密码体制的区块链访问控制

传统的访问控制模型有自主访问控制(Discretionary Access Control,DAC)[24],强制访问控制(Mandatory Access Control,MAC)[25],基于角色的访问控制(Role-Based Access Control,RBAC)[26]和基于属性的访问控制(Attribute-Based Access Control,ABAC)模型[27].

DAC 由文件所有者决定其他用户对该文件的全部或部分访问权,系统无法控制,不适合大型的复杂系统,开销大且效率低,安全性不够高;MAC 根据系统指定的访问策略进行多级别访问控制,用户不能直接对数据进行控制,访问规则制定严格,不够灵活;RBAC 用一个中央服务器处理所有用户的访问请求,通常给一类角色分配相同的权限,降低了权限授予的复杂性与管理的开销,但其缺乏动态性;ABAC 与 RBAC 相比更适合于复杂的场景,能够提供更加细粒度的访问控制,灵活性比较高.

上述传统访问控制模型已应用于区块链中[28~30],但多数依赖于中心实体进行访问决策,很难适应区块链复杂的新需求与分布式模型.

3.1.2 使用属性密码体制的区块链访问控制

研究人员采用属性密码体制改进区块链的访问控制模型,用以提高访问控制的安全性与灵活性.

(1)提高访问控制的细粒度与灵活性

为了解决访问控制粒度较粗和权限滥用的问题,Yu 等学者[31]结合 CP-ABE 设计了 ATRBAC 模型(Attribute and Trust-Based RBAC Model). 在 RBAC 的基础上添加了属性/信任管理模块,为用户授予了一组属性集合,为角色嵌入了访问结构. 该方案在权限授予的动态性和访问控制的细粒度上有一定的进步,可与区块链技术相结合,为后续研究提供了思路. 同样采用了 CP-ABE,Jemel[32]等学者设计了具有时间维度的区块链安全访问控制模型,在该模型中通过两种交易进行访问控制,分别用于访问策略设置和访问请求. 数据所有者生成密钥 K_1,K_2 用于共同加密数据,K_2 通过时间优化的 CP-ABE 算法再次加密. 区块链中的节点通过访问者的属性,当前时间和 CP-ABE 来解密 K_2,用以验证用户的合法性,再将验证的交易存储于区块中. 区块链网络节点即使全部拥有 K_2,也缺少 K_1,而即使用户拥有 K_1,没有相应的属性或正确的访问时间间隔,也不具有对数据的访问权. 因此,该模型支持细粒度的访问控制管理,并支持访问策略的更改,实时性更优.

上述方案适合私有链的场景,与之不同,王秀利等人[33]利用 ABE 改进了企业级联盟链的加密方式与存储方式. 该联盟链分为企业链和行业链. 对于企业内部访问,数据上传者制定访问策略,对数据进行对称加密存储,企业节点对数据索引 *add* 和对称加密密钥 *rs* 进行加密后广播至区块链,同时将索引与数据的映射存入底层数据库,满足了企业复杂的等级和权限需求. 对于行业内部访问,行业链增加了企业属性,企业通过访问控制树对数据加密,以进行与其他企业的交互. 联盟链中存在企业节点、行业节点和边缘节点,边缘节点可以同时加入两种链中,通过智能合约验证企业的访问权. 该模型既满足了企业内部访问控制的需要,企业之间又可通过边缘节点进行数据的交互.

一般的 CP-ABE 依赖于中心机构,对区块链的访问控制安全有一定的威胁,多属性机构 CP-ABE(Multi-Authority CP-ABE,MACP-ABE)[34]可以解决这种问题,任何人都可以创建属性并授权不同的用户. Li 等学者[35]提出了基于 MACP-ABE 的区块链访问控制方案,数据访问者可以组合不同来源的私钥来匹配密文策略. 在该方案中,区块链上存在三种类型的交易信息 $TX_{\text{ATTRIBUTE}}$,TX_{DATA} 和 TX_{ACCESS},分别用于属性分发,数据存储和访问策略分配、检索与验证. 数据访问者发送 TX_{ACCESS} 到区块链来提供 TX_{DATA} 的哈希值和具有签名的地址指针,区块链通过所设置的访问策略来验证交易 TX_{ACCESS} 的有效性.

(2)提供身份验证并增加访问控制的安全性

Li G 等人[35]在访问控制模型中通过多属性机构签名机制(MA-ABS)对地址指针签名. MA-ABS 不依赖于中心机构,区块链利用签名 σ,信息 M,访问策略 (A,ρ),公钥 $\{PK_i\}$ 和公共参数 GP,通过相关属性的公钥进行验证. 不同于对地址指针进行签名,Khan Sarmad 等人[36]采用 RSA 加密算法将数据加密存储于区块链,然后利用 ABS 对 RSA 私钥进行签名再发送给用户,作为用户的对称密钥,该对称密钥再对私钥进行加密. 用户必须上传加密私钥以进行身份验证,通过后使用该用户的对称密钥解密上传的密钥.

图 3 总结了基于属性密码体制的区块链访问控制模型,数据所有者根据属性设置访问策略,对数据加密存储(属性授权中心 AA 个数不定),并发布带有访问策略的交易到区块链,节点验证后存储在区块链中. 数据

访问者想要访问数据时,发布带有访问请求的交易,访问者属性满足访问策略时,区块链授予相应访问权,访问者获得加密数据.

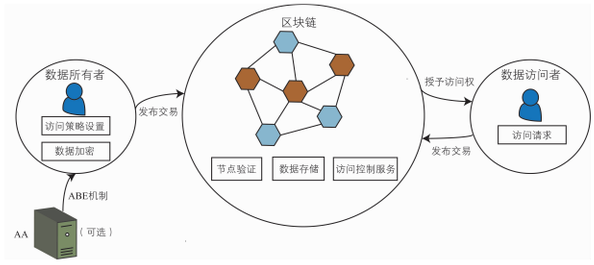

图3　基于属性密码体制的区块链访问控制模型

3.2　区块链密钥管理

许多基于区块链的应用使用私钥来识别用户的身份[37],密钥存储的环境安全性较低. 密钥的生成、存储与传输等过程中同样也存在安全风险.

3.2.1　未使用属性密码体制的区块链密钥管理

大多数区块链的密钥管理依赖于非对称密码体制,但存在许多可用性问题[38]. 区块链现有的密钥管理方案难以实现密钥的追溯,并缺乏撤销与更新机制,安全性与灵活性有待提高.

现有的区块链密钥管理方案大多为公钥方案,公钥操作涉及了大量计算,且需要大量分发公钥证书并频繁验证,造成管理的不方便以及巨大的开销. Lin Q 等人[39]采用线性同态加密方案与身份密码体制,同基于证书的公钥基础结构相比,它减小了基于证书的密码系统造成的系统开销,可应用于区块链中,但其计算过程较为复杂. Albakri 等人[40]率先提出了区块链中基于轻量级二元多项式的密钥管理方案,将令牌预加载到实体中,加快了密钥建立的过程,能够减小处理交易的开销,但缺乏密钥撤销与追溯机制.

3.2.2　使用属性密码体制的区块链密钥管理

尽管上述研究试图在区块链中实现安全的密钥管理,但过程较为复杂,未能实现密钥的追溯、撤销、更新机制. 为了解决这些问题,研究人员将属性密码体制引入区块链.

(1)实现密钥可追溯性

基本 ABE 方案中的密钥不包含用户特定信息,恶意用户可以共享密钥而不被发现. 此外,属性授权机构可从任何属性集中生成密钥,一旦发生密钥滥用,无法判断该行为来自恶意用户还是属性授权机构. Wu A 等人[41]针对区块链中的密钥滥用问题提出了一种在区块链中的高效可追踪密钥方案,使得区块链对密钥具有可公开验证的追溯性. 该方案通过 CP-ABE 将用户的签名和属性授权中心的主密钥嵌入到用户的密钥中,添加了验证阶段和审核阶段,每个阶段都分为用户滥用密钥和属性授权机构滥用密钥两种情况进行判断与审核,即允许任何第三方组织在发生密钥滥用时审核滥用密钥的来源,判断其来自于用户还是属性机构授权.

(2)实现密钥撤销机制与更新机制

为了实现密钥撤销和解决用户密钥协调问题,Bramm[42]提出了一种区块链中的分布式属性加密协议. 在该协议中,由属性机构 AA 决定将其域中的哪些属性分配给用户,数据所有者和使用者可以组合来自多个 AA 的不同属性. 区块链以交易的形式存储所有用于密钥生成的属性,该协议以 CP-ABE 为基础,允许通过交易随时动态地创建和删除新的属性.

不同于基于交易的密钥撤销,He[43]等人采用哈希算法计算不同时间片中的时间值,并使用加密算法对当前时间片的密钥进行合并和计算,在区块链上实现了用户属性和私钥的自动撤销.

Guo 等人[44]提出了区块链中的基于 ABE 的独立更新密钥的方案. 区块链系统由多个授权中心共同管理,每个区块都存储相关数据的索引,每两个授权中心共享一个伪随机函数种子 S_{ql},每个用户的私钥都包含每个授权中心的私钥. ABE 算法通过授权机构的授权为私钥组件添加版本号 Ver,用以分别更新区块链中用户的密钥,且不会影响其他的用户,拥有较强的动态性与灵活性,享有前向安全性.

区块链密钥管理方案的对比如图 4 所示. 未使用属性加密体制的密钥管理缺乏密钥追溯、撤销、更新机制,未能在安全性上有较多优化.

3.3　区块链数据隐私保护

区块链的数据隐私保护主要分为对交易数据隐私的保护和对用户身份信息隐私的保护.

3.3.1　未使用属性密码体制的区块链数据隐私保护

在区块链模型中,通常使用哈希算法与非对称加密算法来保护区块所有者或交易者的隐私.

哈希算法是一种数学函数,它在合理的时间内将任意长度的输入转变为固定长度的输出,具备单向性,抗碰撞性. 哈希算法可以对信息进行简化,验证和标识,被广泛用于区块的构建以及交易的确认中;非对称密码算法是区块链广泛采用的密码算法,其生成一个公私钥对,加密和解密使用不同的密钥. RSA 算法是一种常见的非对称密码算法,其破解的关键在于密钥长度,密钥越长越安全,但会损失性能;比特币使用椭圆曲线算法生成公私钥,相比于 RSA,其密钥长度更短.

3.3.2　使用属性密码体制的区块链数据隐私保护

近年来区块链数据隐私的相关研究显著上升[45~50],虽然在区块链的数据隐私保护安全性上有一定进步,仍难以满足区块链应用复杂的新需求. 属性密码体制在数据管理与隐私保护上极具前景.

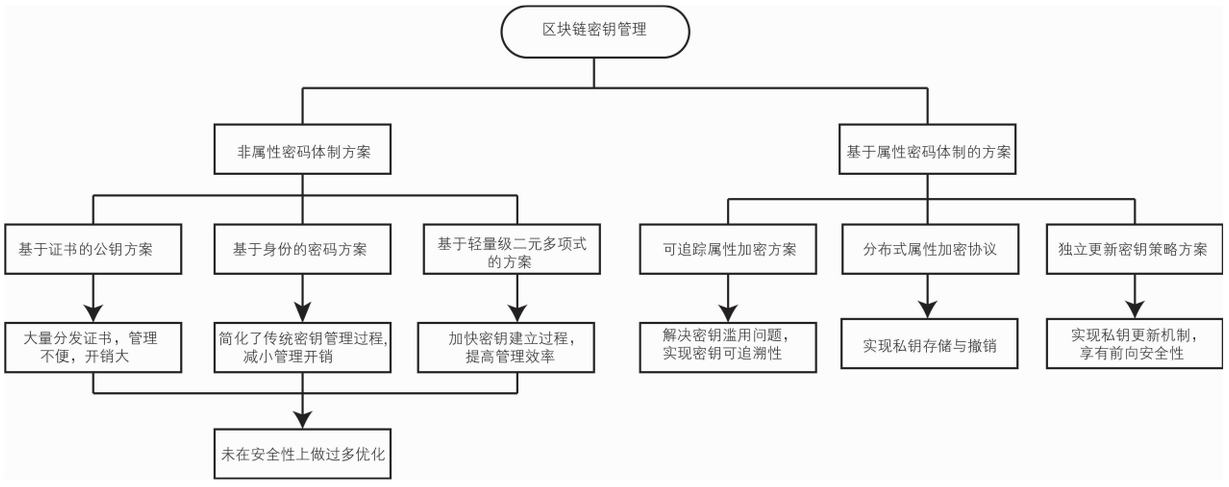

图4 区块链密钥管理安全方案对比

(1)交易数据隐私保护

数据加密技术可以保护交易数据隐私. Lewko 等人[51]指出区块链虽然在某种程度上支持完整性和不可否认性,但是其仍存在安全问题的主要原因是这些区块链技术都依赖于对称密钥加密来进行数据加密. 如果数据是通过对称密钥方案加密的,则密钥必须与数据一起共享,使得区块链的数据隐私受到威胁.

在基于私有链的应用中,Yuan 等人[52]利用 CP-ABE 在区块链上实现了一种保护数据隐私的监管机制,对数据的加解密进行控制,数据的每次更改操作都被记录在区块链上,保证了数据的机密性. 数据先经过加密生成元数据,再生成哈希值 H_R. 此外,该机制规定高级用户可以查询高级和低级数据,但是低级用户只能查询低级数据. 该机制可以检测到任何恶意用户共享密钥和非授权用户生成解密密钥的行为,且允许第三方验证解密密钥用户的身份,实现了公开验证的可追溯性,可以追踪公开解密密钥的恶意用户.

Rahulamathavan 等人[53]提出了物联网中的区块链安全隐私保护架构. 整个架构无中央机构和存储服务器,传感器节点执行不同的功能,低级节点采集数据,高级节点收集到一组数据后向矿工广播交易. 传感器生成的数据首先采用 MA-ABE 加密,每个矿工将检查自己是否具有正确的属性,具有正确属性的矿工严格验证交易合法性,这将减轻数据操纵等安全攻击,数据被接受并附加到区块链就无法篡改.

一般来说,公有链的功能比私有链强大,但许多业务为了保护交易数据隐私而被迫选择了私有链,无法充分利用公有链系统的优势. 与上述方案不同,Huang 等人[54]采用跨区块链(Private Blockchains over Public Blockchains,PoP)方案,使用户在维护隐私的同时仍利用公有链的分布式信任机制. 该方案将私有链看作是使用 ABE 保护的状态通道,在公有链上附加了多个私有链,在链下采用 ABE 方式生成智能合约与公有链进行交互,降低私有链交易的计算强度,私有链不必经过所有节点的验证.

(2)用户身份信息隐私保护

Sun 等学者[55]在分布式 ABE 的基础上,设计了联盟链中的身份信息隐私保护机制,防止恶意用户通过交易进行推理攻击而获得交易方的身份信息,同时又能验证数据的真实性与来源的可靠性. 在该机制中,签名者的签名密钥与属性相关联,验证者可有效地验证签名者的属性而不暴露其身份,且多个属性机构可以向用户颁发属性证书和相应的签名密钥,无需依靠中央机构. 该方法在区块头中存放了签名信息,区块头的结构如式(1)所示,其中 H 为哈希函数,Sig_{SIK} 为区块发布者的签名,SIK 为基于属性的签名私钥.

$$BlockHeader_n=(H_{Block_n},H_{Block_{n-1}},timesamp,Sig_{SIK}) \quad (1)$$

(3)交易信息和身份信息隐私保护

Zhang[56]提出了超级账本下的支持隐私保护的数据共享架构,用户独立决定谁可以共享其数据,而不会损害数据和身份隐私. 该方案将 ABE 嵌入智能合约,数据所有者上传加密数据,然后生成访问控制列表放入智能合约中,当其他用户想要访问数据时,先运行智能合约中的算法获得访问策略,若该用户的属性满足访问策略,则将经过属性签名的交易发送至智能合约,签名验证成功则用户即可获得经过 ABE 加密的私钥. 若失败,数据访问者可与所有者直接交互,更新访问控制列表. 数据管理者或授权机构设置访问策略,并有权修改用户的访问权限;该架构可保证用户的匿名性,并提供身份验证.

表 1 比较了区块链中几种数据隐私保护方案的数据类型、区块链类型和采用的隐私保护方法.

表1　区块链中几种数据隐私保护方案对比

隐私保护方案	交易数据隐私保护	身份信息隐私保护	区块链类型	采用的隐私保护方法
[46]	Y	N	公有链	零知识证明
[49]	Y	N	联盟链	概率陷阱门
[52]	Y	N	私有链	CP-ABE
[54]	Y	N	PoP 链	ABE
[55]	N	Y	联盟链	ABS
[56]	Y	Y	联盟链	ABS,CP-ABE

如图5所示,基于属性密码体制的区块链隐私保护能够通过 ABE、ABS 机制对数据的进行加密传输,通过区块链保证数据的不可篡改性,并实现匿名验证、权限分级、行为记录等隐私保护机制,属性加密与签名技术能够嵌入到智能合约,自动执行身份验证、权限授予等操作以支撑上层应用.

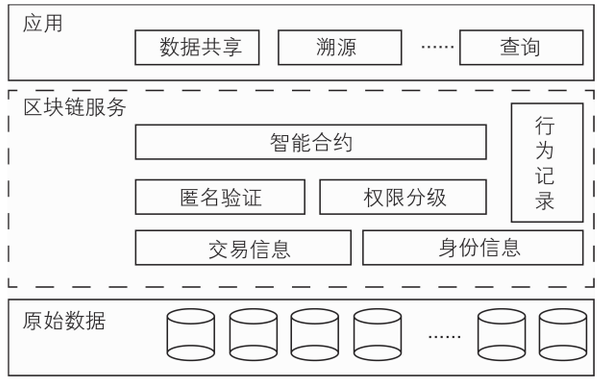

图5　基于属性密码体制的区块链隐私保护模型

4　总结与展望

本文基于属性密码体制,从访问控制、密钥管理、数据隐私保护三个方面综述了区块链安全技术的研究进展,指出了目前面临的挑战,为区块链安全技术提供了研究方向.

4.1　区块链安全问题

4.1.1　效率问题

在实际应用中,数据的大量存储,区块的生成与共识给区块链带来的负担使得区块链应用受到限制. 同时,现有的密码体制在保证区块链安全的同时,通信量较大,耗费了大量的计算资源,效率较低.

4.1.2　密钥管理问题

区块链中密钥的生成、存储与分发等过程存在安全风险,管理、控制和使用密钥是一个复杂的任务. 如何通过现有的密码体制实现密钥的撤销,追溯,更新机制是一个值得研究的问题.

4.1.3　隐私泄露问题

区块链中交易数据的机密性、完整性、可用性都面临着威胁. 现有方案可以对区块链的身份验证和数据机密性以及区块设计、链式结构进行优化,但仍无法完全避免各种数据隐私的泄露. 此外,当存在多条区块链时,如何进行安全的互联互通以保护数据隐私也是一个问题.

4.2　未来工作与研究方向

基于4.1节区块链安全技术所面临的问题,本文给出了几个未来的研究方向,以供探讨.

4.2.1　共识机制优化

区块的生成与共识需要耗费大量时间与计算资源,不利于访问策略的实施与更新. DPOS 共识机制[57]一定程度上能够减小节点的计算开销,提高数据共享的效率,但受到存储空间的限制. 因此,通过优化的共识机制降低区块链访问控制中的节点计算开销是一个值得研究的问题.

4.2.2　跨链访问

多条区块链场景不仅涉及某条链内部的访问控制,还要实现跨链访问. 引入哈希锁定、侧链技术等跨链机制[58],研究同构、异构区块链之间的跨链访问,实现区块链间的可信交互是一个挑战性的工作.

4.2.3　存储模型优化

区块链上存储的数据过大会影响工作性能,很多情况下采取了不同的存储方式,例如链上存储、链下存储[59]等方式,不同的应用场景对数据存储的安全性要求也不同. 未来可根据实际场景选择合适的区块链结构进行存储,根据不同的安全性要求设置安全级别,研究不同的安全存储手段.

4.2.4　加密算法优化

现有的加密算法计算量大,多轮通信也会使区块链工作效率低下. 改进现有的属性加密、安全多方计算[60]、同态加密等技术,提高加密算法的效率,降低通信轮数,使现有密码体制更好地应用到区块链中具有重要的研究意义.

4.2.5　密钥管理方法

未来可设计密钥管理智能合约,实现密钥的存储、验证与分发;通过区块链的不可篡改性实现密钥可追溯性,利用优化的签名机制、限时机制、秘密共享技术等实现密钥的恢复、更新与撤销,研究高安全性的密钥管理方案.

参考文献

[1] Nakamoto S. Bitcoin:a peer-to-peer electronic cash system [EB/OL]. http://bitcoin. org/bitcoin. pdf,2009.

[2] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(04):481 -494.
Yuan Yong, Wang Feiyue. Blockchain:the state of the art

and future trends[J]. IEEE/CAA Journal of Automatica Sinica,2016,42(04):481 – 494. (in Chinese)

[3] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J]. 计算机学报,2018,41(05):969 – 988.
Shao Qifeng, Jin Cheqing, Zhang Zhao, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers,2018,41(05):969 – 988. (in Chinese)

[4] Lamport L,et al. The Byzantine generals problem[J]. ACM Trans on Programming Languages and Systems,1982,4(3): 382 – 401.

[5] Zheng ZB,et al. An overview of blockchain technology:architecture,consensus,and future trends[A]. IEEE Int'l Congress on Big Data[C]. Piscataway:IEEE,2017. 557 – 564.

[6] Hinz J,Taylor P. A Note on Optimal Double Spending Attacks[M]. Switzerland:Springer Cham,2019. 2:545 – 551.

[7] Tasatanattakool P,Techapanupreeda C. Blockchain:challenges and applications[A]. 2018 International Conference on Information Networking (ICOIN)[C]. Piscataway:IEEE, 2018. 473 – 475.

[8] Joshi AP,Han M,Wang Y. A survey on security and privacy issues of blockchain technology[J]. Mathematical Foundations of Computing,2018,1(2):121 – 147.

[9] Takemoto Y, Knight S. Mt. Gox files for bankruptcy, hit with lawsuit [EB/OL]. https://www. reuters. com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228, 2018.

[10] Pang L J,Yang J,Jiang Z T. A survey of research progress and development tendency of attribute-based encryption [J]. The Scientific World Journal,2014,2014:193426.

[11] Yan XX, Meng H. Ciphertext policy attribute-based encryption scheme supporting direct revocation[J]. Journal on Communications,2016,37(5):44 – 50.

[12] Zhang M Q,Du WD,et al. A full secure KP-ABE scheme in the standard model[J]. Journal of Computer Research and Development,2015,52(8):1893 – 1901.

[13] Zhu Y, Qin Y, Gan G H, Yang S. TBAC: Transaction-based access control on blockchain for resource sharing-with cryptographically decentralized authorization[A]. IEEE International Conference on Computer Software and Applications[C]. Piscataway:IEEE,2018. 535 – 544.

[14] Sun Y,Zhang R,Wang X,et al. A decentralizing attribute-based signature for healthcareblockchain[A]. Int'l Conf on Computer Communication and Networks[C]. Piscataway:IEEE,2018. 1 – 9.

[15] Wang H,Song Y J. Secure cloud-based EHR system using attribute-based cryptography and blockchain[J]. Journal of Medical Systems,2018,42(8):152 – 161.

[16] Şahan S,Ekici AF,Bahtiyar S. A multi-factor authentication framework for secure access to blockchain[A]. Int'l Conf on Computer and Technology Applications[C]. New York:ACM,2019. 160 – 164.

[17] Ye CC,Li GQ,et al. Security detection model of blockchain[J]. Journal of Software,2018,29(5):1348 – 1359.

[18] Gervais A,Karame G,et al. On the security and performance of proof of work blockchains[A]. ACM SIGSAC Conference[C]. New York:ACM,2016. 3 – 16.

[19] Kokoris-Kogias E, Jovanovic P, et al. Enhancing bitcoin security and performance with strong consistency via collective signing[J]. Applied Mathematical Modelling, 2016,37(8):5723 – 5742.

[20] Kiayias A,Russell A,et al. Ouroboros:A provably secure proof-of-stake blockchain protocol[A]. Proc of Annual International Cryptology Conference[C]. Switzerland: Springer,Cham,2017. 357 – 388.

[21] LiN,Yan Z,et al. Securing communication data in pervasive social networking based on trust with KP-ABE[J]. ACM Transactions on Cyber-Physical Systems, 2018, 3 (1):1 – 23.

[22] Reshma V,Gladwin SJ,et al. Pairing-free CP-ABE based cryptography combined with steganography for multimedia applications[A]. Int'l Conf on Communication and Signal Processing[C]. Piscataway:IEEE,2019. 0501 – 0505.

[23] Yang P,Cao Z,Dong X. Fuzzy identity based signature with applications to biometric authentication[J]. Computers & Electrical Engineering,2011,37(4):532 – 540.

[24] Sánchez YKR,Demurjian SA,et al. Attaining role-based, mandatory,and discretionary access control for services by intercepting api calls in mobile systems[A]. Web Information Systems and Technologies[C]. Berlin: Springer, 2018. 322:221 – 248.

[25] Taubmann B, Rakotondravony N, et al. Cloud Phylactor: harnessing mandatory access control for virtual machine introspection in cloud data centers[A]. IEEE Trustcom/BigDataSE/ISPA[C]. Piscataway:IEEE,2016. 957 – 964.

[26] Power DJ, Slaymaker M, et al. On formalizing and normalizing role-based access control systems[J]. Computer Journal,2018,52(3):305 – 325.

[27] Jha S,Sural S,Atluri V,et al. Security analysis of ABAC under an administrative model[J]. IET Information Security,2019,13(2):96 – 103.

[28] Ouaddah A, Abou Elkalam A, et al. FairAccess: a new blockchain-based access control framework for the internet of things[J]. Security & Communication Networks, 2016,9(18):5943 – 5964.

[29] Cruz JP, Kaji Y, Yanai N. RBAC-SC: role-based access control using smart contract[J]. IEEE Access, 2018, 6: 12240 – 12251.

[30] Zhu Y,Qin Y,Zhou ZY,et al. Digital asset management

with distributed permission over blockchain and attribute-based access control[A]. IEEE Int'l Conf on Services Computing[C]. Piscataway:IEEE,2018. 193 – 200.

[31] 余波,台宪青,马治杰. 云计算环境下基于属性和信任的 RBAC 模型研究[J]. 计算机工程与应用,2020,(9):84 – 92.
Yu Bo, Tai Xianqing, Ma Zhijie. The study on attribute and trust-based RBAC model in cloud computing[J]. Computer Engineering and Applications,2020,(9):84 – 92. (in Chinese)

[32] Jemel M, Serhrouchni A. Decentralized access control mechanism with temporal dimension based on blockchain[A]. IEEE 14th Int'l Conf on E-business Engineering (ICEBE)[C]. Piscataway:IEEE,2017. 177 – 182.

[33] 王秀利,江晓舟,李洋. 应用区块链的数据访问控制与共享模型[J]. 软件学报,2019,30(6):1661 – 1669.
Wang Xiuli,Jiang Xiaozhou,Li Yang. Model for data access control and sharing based on blockchain[J]. Journal of Software,2019,30(6):1661 – 1669. (in Chinese)

[34] Xiao M,Hu X. Multi-authority attribute-based encryption access control scheme in wireless body area network[A]. International Conference on Information Systems Engineering[C]. Piscataway:IEEE,2019. 39 – 45.

[35] Li G,Hiroyuki S. A privacy-preserving and fully decentralized storage and sharing system onblockchain[A]. IEEE 43rd Annual Computer Software and Applications Conf[C]. Piscataway:IEEE,2019. 694 – 699.

[36] Sarmadullah K,Rafiullah K. Multiple authorities attribute-based verification mechanism for blockchain mircogrid transactions[J]. Energies,2018,11(5):1154.

[37] Dai FF,Shi Y,Meng N,et al. From bitcoin to cyber-security:a comparative study of blockchain application and security issues[A]. 4th Int'l Conf on Systems and Informatics[C]. Piscataway:IEEE,2017. 975 – 979.

[38] Eskandari S,Barrera D,et al. A first look at the usability of bitcoin key management[A]. NDSS Symposium[C]. Internet Society,2015. 1 – 10.

[39] Lin Q,Yan HY,Huang ZA,et al. An ID-based linearly homomorphic signature scheme and its application in blockchain[J]. IEEE Access,2018,6:20632 – 20640.

[40] Albakri A, Harn L, Maddumala M. Polynomial-based lightweight key management in a permissioned blockchain[A]. IEEE Conference on Communications and Network Security[C]. Piscataway:IEEE,2019. 1 – 9.

[41] Wu A X,Zhang Y H,et al. Efficient and privacy-preserving traceable attribute-based encryption in blockchain[J]. Annals of Telecommunications,2019,74(7 – 8):404 – 411.

[42] Bramm G, Gall M, et al. BDABE-blockchain-based distributed attribute based encryption[A]. International Conference on Security and Cryptography[C]. Piscataway:IEEE,2018. 265 – 276.

[43] He Q S, Xu Y, et al. A privacy-preserving internet of things device management scheme based on blockchain[J]. International Journal of Distributed Sensor Networks,2018,14(11):1 – 12.

[44] Guo R, Shi H X, Zheng D, et al. Flexible and efficient blockchain-based abe scheme with multi-authority for medical on demand in telemedicine system[J]. IEEE Access,2019,7:88012 – 88025.

[45] Sharath Y J,Bangera K,et al. Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications[A]. IEEE 25th International Conference on High Performance Computing Workshops[C]. Piscataway:IEEE,2018. 81 – 85.

[46] 田道坤,彭亚雄. 在区块链中基于混合算法的数字签名技术[J]. 电子科技,2018,31(7):23 – 27.
Tian Daokun, Peng Yaxiong. Digital signature technology based on hybrid algorithm in blockchain[J]. Electronic Sci&Tech,2018,31(7):23 – 27. (in Chinese)

[47] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[A]. IEEE Symposium on Security and Privacy[C]. Piscataway:IEEE,2016. 839 – 858.

[48] Li L, Liu J Q, Cheng L C, et al. CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE Trans on Intelligent Transportation Systems,2018,19(7):2204 – 2220.

[49] Noether Shen, Mackenzie Adam, et al. Ring Confidential Transactions[OL]. DOI:10.5195/LEDGER.2016.34,2019.

[50] Tahir S, Rajarajan M. Privacy-preserving searchable encryption framework for permissioned blockchain networks[A]. IEEE International Conference on iThings and IEEEGreenCom and IEEE CPSCom and IEEE SmartData[C]. Piscataway:IEEE,2018. 1628 – 1633.

[51] Lewko A B, Waters B. Decentralizing attribute-based encryption[A]. The 30th Annual International Conference Theory and Applications of Cryptographic Techniques:advances in cryptology[C]. New York: ACM, 2011. 568 – 588.

[52] Yuan C,Xu M X,et al. Blockchain with accountable CP-ABE:How to effectively protect the electronic documents[A]. IEEE International Conference on Parallel and Distributed Systems[C]. Piscataway:IEEE,2017. 800 – 803.

[53] Rahulamathavn Y, W Phan RC, et al. Privacy-preserving blockchain based IOT ecosystem using attribute-based encryption[A]. IEEE International Conference on Advanced

Networks and Telecommunications Systems(ANTS)[C]. Piscataway:IEEE,2017. 1 - 6.
[54] Huang D J,Chung C J,et al. Building private blockchains over public blockchains (PoP):an attribute-based access control approach[A]. 34th ACM/SIGAPP Symposium[C]. New York:ACM,2019. 355 - 363.
[55] Sun Y,Zhang R,et al. A decentralizing attribute-based signature for healthcare blockchain[A]. International Conference on Computer Communication and Networks[C]. Piscataway:IEEE,2018. 1 - 9.
[56] Zhang YR,He D,Choo KKR. BaDS:blockchain-based architecture for data sharing with ABS and CP-ABE in IOT[J]. Wireless Communications and Mobile Computing,2018,(2018):1 - 9.
[57] Zhou T,Li X,Zhao H. DLattice:A permission-less blockchain based on dpos-ba-dag consensus for data tokenization[J]. IEEE Access,2019,(99):1 - 1.
[58] 李芳,李卓然,等. 区块链跨链技术进展研究[J]. 软件学报,2019,30(6):1649 - 1660.
Li Fang,Li Zhuoran,et al. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software,2019,30(6):1649 - 1660. (in Chinese)
[59] Zheng QH,Li Y,Chen P,Dong XH. An innovative IPFS-based storage model for blockchain[A]. IEEE/WIC/ACM International Conference on Web Intelligence[C]. Piscataway:IEEE,2018. 704 - 708.
[60] 窦家维,王文丽,刘旭红,等. 有理区间的安全多方计算与应用[J]. 电子学报,2018,46(9):2057 - 2062.
Dou Jiawei,Wang Wenli,Liu Xuhong,et al. Secure multi-party computation of rational interval and its applications[J]. Acta Electronica Sinica,2018,46(9):2057 - 2062. (in Chinese)

作者简介

陈 露 女,1995 年 3 月出生于江苏南京. 博士研究生,主要研究方向为网络安全技术,区块链技术.

相 峰 男,1967 年 4 月出生于山东龙口. 硕士,物流信息互通共享技术及应用国家工程实验室主任,主要研究方向为物流工程与企业管理,区块链技术.

孙知信(通信作者) 男,1964 年 9 月出生于安徽宣城. 博士,教授,博士生导师,主要研究方向为网络通信的理论与技术,计算机网络及安全,区块链技术.
E-mail:sunzx@ njupt. edu. cn