软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(7):2092−2115 [doi: 10.13328/j.cnki.jos.005589]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链技术及其在信息安全领域的研究进展*

刘敖迪[1,2], 杜学绘[1,2], 王 娜[1,2], 李少卓[1,2]

[1](信息工程大学,河南 郑州 450001)

[2](河南省信息安全重点实验室,河南 郑州 450001)

通讯作者: 杜学绘, E-mail: dxh37139@sina.com

摘 要: 区块链是一种源于数字加密货币比特币的分布式总账技术,其发展引起了产业界与学术界的广泛关注.区块链具有去中心化、去信任、匿名、数据不可篡改等优势,突破了传统基于中心式技术的局限,具有广阔的发展前景.介绍了区块链技术在信息安全领域的研究现状和进展.首先,从区块链的基础框架、关键技术、技术特点、应用模式、应用领域这 5 个方面介绍了区块链的基本理论与模型;然后,从区块链在当前信息安全领域研究现状的角度出发,综述了区块链应用于认证技术、访问控制技术、数据保护技术的研究进展,并对比了各类研究的特点;最后,分析了区块链技术的应用挑战,对区块链在信息安全领域的发展进行了总结与展望,希望对未来进一步的研究工作有一定的参考价值.

关键词: 区块链;信息安全;认证技术;访问控制;数据保护

中图法分类号: TP309

中文引用格式: 刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展.软件学报,2018,29(7):2092−2115. http://www.jos.org.cn/1000-9825/5589.htm

英文引用格式: Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):2092−2115 (in Chinese). http://www.jos.org.cn/1000-9825/5589.htm

Research Progress of Blockchain Technology and Its Application in Information Security

LIU Ao-Di[1,2], DU Xue-Hui[1,2], WANG Na[1,2], LI Shao-Zhuo[1,2]

[1](Information Engineering University, Zhengzhou 450001, China)

[2](He'nan Province Key Laboratory of Information Security, Zhengzhou 450001, China)

Abstract: Blockchain is a distributed public ledger technology that originates from the digital cryptocurrency, bitcoin. Its development has attracted wide attention in industry and academia fields. Blockchain has the advantages of de-centralization, trustworthiness, anonymity and immutability. It breaks through the limitation of traditional center-based technology and has broad development prospect. This paper introduces the research progress of blockchain technology and its application in the field of information security. Firstly, the basic theory and model of blockchain are introduced from five aspects: Basic framework, key technology, technical feature, and application mode and area. Secondly, from the perspective of current research situation of blockchain in the field of information security, this paper summarizes the research progress of blockchain in authentication technology, access control technology and data protection technology, and compares the characteristics of various researches. Finally, the application challenges of blockchain technology are

* 基金项目: 国家重点研发计划(2016YFB0501901); 国家高技术研究发展计划(863)(2015AA016006); 国家自然科学基金(61502531); 河南省自然科学基金(162300410334)

Foundation item: National Key Research and Development Program of China (2016YFB0501901); National High Technology Research and Development Program of China (863) (2015AA016006); National Natural Science Foundation of China (61502531); Natural Science Foundation of He'nan Province, China (162300410334)

收稿时间: 2017-11-20; 修改时间: 2018-03-17; 采用时间: 2018-04-21; jos 在线出版时间: 2018-04-27

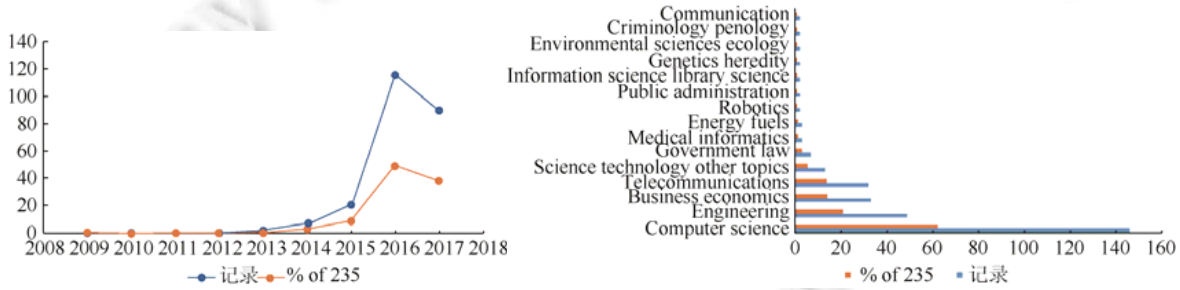
CNKI 网络优先出版: 2018-04-27 14:58:41, http://kns.cnki.net/kcms/detail/11.2560.TP.20180427.1458.012.html

analyzed, and the development outlook of blockchain in the field of information security is highlighted. This study intends to provide certain reference value for future research work.

Key words: blockchain; information security; authentication technology; access control; data protection

区块链技术[1]作为比特币、以太坊等数字加密货币[2]的核心技术,能够有效解决数字货币长期所面临的拜占庭将军问题[3,4]和双重支付问题[5,6].近年来,得到了各领域研究人员的广泛关注.传统社会的信任是建立在可信第三方、基于信用“背书”的信任机制下,由权威的第三方机构(如银行)来提供社会的信任支撑.因此,在没有第三方中心的条件下,直接在两个陌生实体间建立信任是很困难的事情,而区块链能够通过分布式节点的验证和共识机制解决去中心化系统节点间信任建立的问题,实现了去中心化、分布式的信任建立机制.从而在信息传输的同时完成价值的转移,能够实现当前网络架构由“信息互联网”向“价值互联网“的重大转变.基于区块链技术,比特币是人类第一次实现在没有任何中介机构参与下,完成了双方可以互信的转账行为,这是对传统信任领域的一次重大突破.

区块链技术最早于 2008 年中本聪发表的论文《Bitcoin: A peer-to-peer electronic cash system》[7]中有所阐述.在比特币被提出的早期并没有引起人们足够的重视,但是随着比特币网络多年来的稳定运行与发展,使得比特币在全球流行起来.并且,使得比特币的底层技术区块链逐渐引起了产业界的广泛关注.国际权威杂志《经济学人》、《哈佛商业周刊》、《福克斯杂志》等相继报道区块链技术将改变世界.麦肯锡研究报告指出,区块链技术是继蒸汽机、电力、信息和互联网科技之后,目前最有潜力触发第 5 轮颠覆性革命浪潮的核心技术.创业公司 R3 联合全球 42 家顶级银行成立区块链联盟从事相关领域技术研究.2016 年 7 月,区块链技术到达 Gartner 技术成熟度曲线的顶端,即过高期望峰值期.2017 年 9 月,澳大利亚、英国等多国将区块链纳入国家数字经济战略.剑桥大学同期研究表明:67%的国家中央银行及 86%的其他公共部门机构正在对区块链相关技术进行直接试验.2017 年 9 月,国务院印发《国家技术转移体系建设方案》中指出要加快区块链科技成果的转移转化.2017 年 10 月,Gartner 公司将区块链技术列为 2018 年十大重大战略科技之一,并预测到 2020 年,银行产业将因使用基于区块链的数字加密货币获得超过 10 亿美元的价值.



(a) 相关年份论文发表数量及比例 (b) 不同研究方向论文数据

Fig.1 Paper retrieve results in Web of Science

图 1 Web of Science 检索结果

早期,人们更关注于比特币等数字加密货币自身的金融功能,将更多的研究精力放到应用区块链技术在金融领域产生突破性变革上.但是,随着人们对区块链技术本质和特点的深入认识,发现区块链技术不单适用于比特币等数字加密货币领域,作为一种创新的技术框架,更能在任何需要建立分布式、点对点信任关系的领域有所作为,实现颠覆性的技术效果,应用于社会、生活的多个方面,改变人们传统的工作、生活习惯.区块链作为一项技术手段最早由产业界推动其研究与发展,近几年才真正引起学术界的广泛关注.如图 1 所示,在 Web of Science 数据库中,以 blockchain 为主题进行检索,截止到 2017 年 10 月共有 235 项检索结果,可以看出近 5 年来关于区块链技术的研究论文数量增长迅速,相关领域涵盖计算机科学、电子商务、数字医疗、环境科学等多个

学科.可以预见,区块链作为一项解决信任问题的普适性技术框架,随着网络信息技术的发展,将被扩展到更多新的应用领域,将来必定会产生更加丰硕的研究成果.

信息安全技术要解决的关键科学问题之一就是实体间信任建立问题.目前常采用基于可信第三方的信任机制.例如,基于第三方证书认证机构(certification authority,简称 CA)建立起交互实体间的信任关系,基于第三方属性权威(attribute authority,简称 AA)实现对用户的权限管理,用户信赖第三方机构将数据集中存储等.但是,鉴于互联网的分布式本质,这种基于第三方的信任机制难以满足分布式条件下大规模 PKI 系统的构建、跨域访问的身份交叉认证、安全可信透明的访问控制、用户高敏感隐私数据保护等更高需求,而且还面临着严重的安全挑战,导致安全事故频发.如 2013 年 12 月,TurkTrust CA 公司曝出发布虚假证书事件;2016 年 5 月,Aesthetic Dentistry 等诊所 18 万份患者病历被恶意攻击者盗取;2017 年 9 月,美国老牌征信公司 Equifax 遭到黑客攻击,1.4 亿用户个人信息遭到泄露等.同时,随着云计算、物联网等分布式计算模式的出现和日益广泛的应用,如何建立用户与云计算平台、分布式计算节点间的信任关系也成为信息安全技术面临的一大挑战.如在云计算环境下,用户的数据存储在云平台、用户的服务外包给云平台,而云平台可能存在用户不可知的越权行为,导致信任透明度的问题;在云计算、物联网环境下,用户、资源、服务、终端存在不限时间、不限地点、不限方式的泛在接入特点,实体自由进出网络,带来实体间直接信任关系的建立难题等.区块链技术的出现为分布式环境下实体间信任建立问题的解决提供了新的思路和方法.本文将对区块链技术的相关概念、原理及研究现状进行详细的介绍与分析,着重对区块链技术在信息安全领域的研究进展进行总结并对其发展加以展望,希望能给当前及未来的相关研究提供一定的参考与帮助.

本文第 1 节从基础框架、关键技术、技术特点、应用模式、应用领域这 5 个角度对区块链技术进行总结.第 2 节对区块链在信息安全领域的研究现状进行综述,主要包括认证技术、访问控制技术和数据保护技术这 3 个方面.第 3 节分析区块链技术应用于信息安全领域未来研究的挑战并提出展望.

1 区块链概述

1.1 基础框架

学术界对区块链技术并没有统一的定义,但一般认为,区块链是一种按照时间顺序将数据区块以链条的方式组合形成的特定数据结构,并以密码学方式保证其不可篡改和不可伪造的去中心化、去信任的分布式共享总账系统.从数据的角度来看,区块链是一种实际不可能被更改的分布式数据库.传统的分布式数据库仅由一个中心服务器节点对数据进行维护,其他节点存储的只是数据的备份.而区块链的“分布式”不仅体现为数据备份存储的分布式,也体现在数据记录的分布式,即由所有节点共同参与数据维护.单一节点的数据被篡改或被破坏不会对区块链所存储的数据产生影响,以此实现对数据的安全存储.从技术的角度来看,区块链并不是一项单一的技术创新,而是 P2P 网络技术[8]、非对称加密技术[9]、共识机制[10]、链上脚本[11−13]等多种技术深度整合后实现的分布式账本技术[14].区块链技术利用加密的链式区块结构来验证和存储数据,利用 P2P 网络技术、共识机制实现分布式节点的验证、通信以及信任关系的建立,利用链上脚本能够实现复杂的业务逻辑功能以对数据进行自动化的操作,从而形成的一种新的数据记录、存储和表达的方法.区块链的基础框架如图 2 所示,主要由数据层、网络层、共识层以及应用层组成.

其中,数据层包括底层数据区块及其链式结构,由哈希算法、时间戳、Merkle 树、非对称加密等相关技术进行支撑,从而保护区块数据的完整性和可溯源性;网络层包括数据传播机制及交易验证机制,由 P2P 网络技术进行支撑,完成分布式节点间数据的传递和验证;共识层主要包括共识机制,通过各类共识算法来实现分布式节点间数据的一致性和真实性,一些区块链系统,如比特币中共识层还包括发行机制和激励机制,将经济因素集成到区块链技术,从而在节点间达成稳定的共识;应用层能够实现区块链的各种顶层的应用场景及相关系统的实现与落地,通过区块链支持的各类链上脚本算法及智能合约来进行支撑,提供了区块链可编程特性的基础.在该框架中,基于时间戳的链式区块结构、基于 P2P 网络的数据传输机制、分布式节点的共识机制和灵活可编程的链上脚本是区块链技术最有代表性的创新点.

Fig.2 Basic framework of blockchain technology

图 2 区块链基础框架

1.2 关键技术

1.2.1 基于时间戳的区块链式结构

区块链通过数据区块和链式结构来存储数据.每个数据区块包括区块头和区块体两部分,都有唯一的哈希值作为区块地址与之对应,当前区块通过存储前一区块哈希值与前一区块相连,从而形成链式结构,如图 3 所示.区块头中封装了前一区块链的哈希值、时间戳、Merkle 树根值等信息;区块体存储交易信息,即由区块链记录的数据信息,每笔交易都由交易方对其进行数字签名,从而确保数据未被伪造且不可篡改,每一笔已完成的交易都将被永久性地记录在区块体中,供全体用户查询.全部交易数据基于 Merkle 树的哈希过程生成唯一的 Merkle 树根值存储在该区块的区块头,Merkle 树这种存储结构极大地提高了查询和校验交易信息的运行效率和扩展性.同时,每个区块生成时,都由区块的记账者为区块加盖时间戳,标明区块产生的时间.随着时间戳的增强,区块不断延长从而形成了一个拥有时间维度的链条,使得数据能够按时间进行追溯,从而保证数据的可追溯性.在比特币系统中,区块头还包括随机数、目标哈希值等信息,以为比特币系统中 PoW 共识机制的运行提供数据支撑.

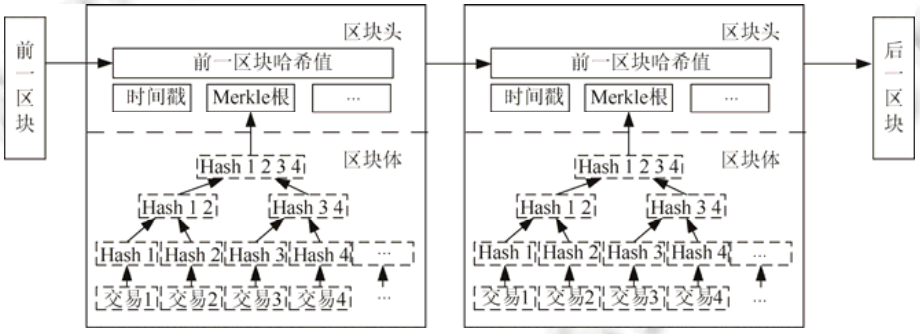


Fig.3 Data structure of blockchain

图 3 区块链数据结构

1.2.2 基于 P2P 的数据传输机制

P2P 网络(peer-to-peer network)是一种在对等实体之间分配工作负载和任务的分布式网络架构,是对等计算模型形成的一种组网或网络通信形式.区块链系统建立在 IP 协议和分布式网络基础上,它不依靠传统的电路交换,而是完全通过互联网去交换信息.网络中所有的节点具有相同的地位,不存在占有核心地位的中心节点和层级结构,实现了完全的去中心化.如图 4 所示,每个节点均会承担网络路由任务,把其他节点传递来的交易信息转发给更多的相邻节点,并且节点具有验证区块数据的能力,但不必所有节点都存储完整的区块链数据,节点间可以通过基于 Merkle 树的简易支付验证方式(simplified payment verification,简称 SPV)向相邻节点请求所需数据以验证交易的合法性,并对交易数据进行更新.在比特币系统中,网络中有些节点还具有钱包和挖矿功能.

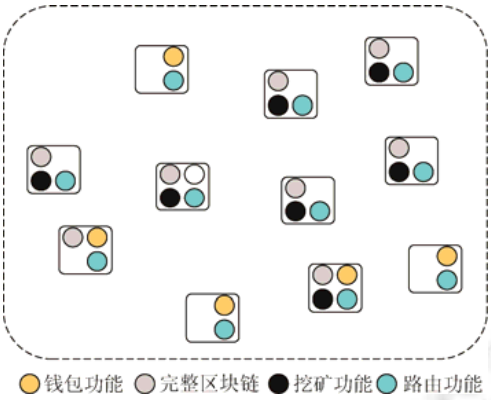


Fig.4 Node network structure

图 4 节点网络

1.2.3 分布式节点的共识机制

共识机制是分布式节点间根据某一事先协商好的规则来确定分布式账本(即区块)的记账权归属的方法,以此使不同节点对交易数据达成共识,保障分布式账本数据的一致性和真实性.共识机制主要用来解决拜占庭将军问题,文献[15,16]的研究表明,在可靠且可认证的同步通信条件下,拜占庭将军问题能够得到较好的解决,但在分布式异步通信条件下,很难找到一种有效的解决方案.在实际应用背景下,根据不同的限制条件,主要有强一致性共识和最终一致性共识两大类共识算法被提出,如图 5 所示.

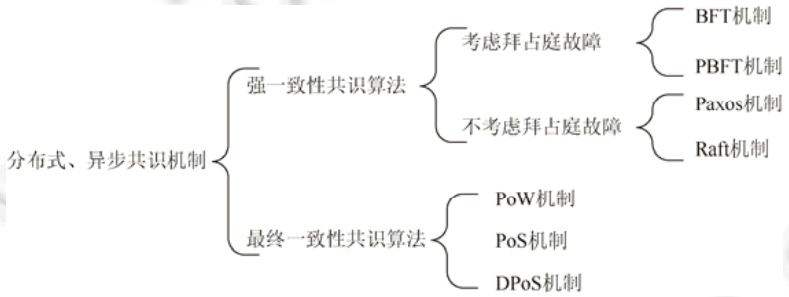


Fig.5 Classification of consensus mechanism

图 5 共识机制分类

基于强一致性共识算法的共识机制多用于节点数量相对较少且对一致性和正确性有更强要求的私有链/联盟链中,典型机制包括考虑拜占庭故障的传统分布式一致性算法 BFT(Byzantine fault tolerance)机制[15]、PBFT(practical Byzantine fault tolerance)机制[17]和不考虑拜占庭故障的 Paxos 机制及 Raft 机制.最终一致性共识算法多用于节点数量巨大且很难使所有节点达到 100%一致性和正确性的公有链,典型机制包括工作量证明 PoW(proof of work)、权益证明 PoS(proof of stake)和授权股份证明 DPoS(delegated proof of stake).表 1 给出代表性共识机制的对比情况,通过对比可知,强一致共识算法安全性更强,但算法复杂度高,是一种多中心机制.而最终一致性共识算法去中心化程度更高且算法复杂度低,但安全性没有强一致共识算法高.比特币系统采用的是 PoW 共识机制.

Table 1 Comparison of consensus mechanism

表 1 共识机制对比

共识机制	核心思想	优点	缺点
PBFT	主节点排序请求,从节点响应请求,多数节点响应结果为最终结果	能够解决拜占庭故障问题,共识结果的一致性和正确性程度高,共识达成时间快	去中心化程度不足,是一种多中心化机制,算法复杂度高,当节点数量过多时,运行效率较低

Table 1 Comparison of consensus mechanism (Continued)
表 **1** 共识机制对比(续)

共识机制	核心思想	优点	缺点
Raft	通过分布式节点选举出的领导人节点得到区块记账权	共识结果的一致性和正确性程度高,大幅缩短共识达成时间,可达到秒级验证	去中心化程度不足,是一种多中心化机制,算法复杂度较高
PoW	引入分布式节点算力竞争来保证数据的一致性和共识安全性	完全去中心化,节点自由进出,避免了建立和维护中心化信用机构的成本	资源大量浪费,挖矿激励机制造成矿池算力高度集中,背离了去中心化设计初衷,共识达成周期较长,存在 51%攻击
PoS	系统中具有最高权益的节点(如币龄最长)获得区块记账权	缩短了共识达成的时间,减少了 PoW 机制的资源浪费	降低了网络攻击成本,节点共识受少数富裕账户支配,存在失去公平性的可能
DPoS	通过股东投票方式选出代表得到记账权	大幅缩短共识达成时间,可达到秒级验证	无法实现完全去中心化,若节点数量过少,投票选出的代表节点代表性不强

1.2.4 灵活可编程的链上脚本

链上脚本是区块链上实现自动验证、可编程、脚本合约自动执行的重要技术.早期比特币的脚本机制相对简单,是一个基于堆栈式、解释相关的 OP 指令引擎,能够解析少量脚本规则,无法实现复杂的业务逻辑.但比特币脚本为区块链可编程能力提供了一个原型设计,在随后的发展过程中,很多区块链项目都深入强化了脚本机制.如第二大区块链平台以太坊[18]设计了一种基于“EVM 虚拟机”的图灵完备脚本语言,能够实现复杂的业务逻辑功能,极大地扩宽了区块链的应用领域,首次实现了区块链技术与智能合约的完美融合.链上脚本技术为区块链提供了应用层的扩展接口,任何开发人员都可基于底层区块链技术通过脚本实现其所要实现的工作,为区块链的应用落地奠定了基础.

1.3 技术特点

区块链技术具有如下技术特点.

(1) 开放共识:任何人都可以参与到区块链网络,每一台设备都能作为一个节点,每个节点都允许获得一份完整的数据库拷贝.

(2) 去中心化:由众多节点共同组成一个端到端的网络,不存在中心化的设备和管理机构.网络的维护依赖网络中所有具有维护功能的节点共同完成,各节点地位平等,一个节点甚至几个节点的损坏不会影响整个系统的运作,网络具备很强的健壮性.

(3) 去信任:节点之间无需依赖可信第三方事先建立信任关系,只要按照系统既定的规则运行即可在分布式节点间完成可信的协作与交互.同时,区块链的运行规则和节点间数据是公开透明的,没有办法欺骗其他节点.

(4) 匿名性:区块链中的用户只与公钥地址相对应,而不与用户的真实身份相关联.用户无需暴露自己的真实身份即可完成交易、参与区块链的使用.

(5) 不可篡改:区块链系统中,由于相连区块间后序区块对前序区块存在验证关系,若要篡改某个区块的数据,就要改变该区块及其所有后序区块数据,并且还须在共识机制的特定时间内改完.因此,参与系统的节点越多,区块链的安全性就越有保证.在比特币系统中,除非能够控制整个系统中超过 51%的节点同时修改,否则很难实现攻击.

(6) 可追溯性:区块链采用带时间戳的链式区块结构存储数据,为数据增加了时间维度,并且区块上每笔交易都通过密码学方法与相邻两个区块相联,因此任何一笔交易都是可追溯的.

(7) 可编程性:区块链支持链上脚本进行应用层服务的开发,并且用户能够通过构建智能合约实现功能复杂的去中心化应用.

1.4 应用模式

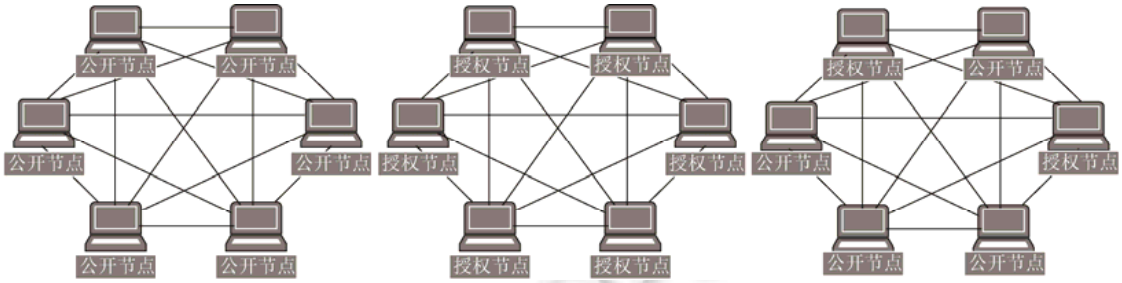
如图 6 所示,区块链技术的应用模式主要包括公有链、私有链、联盟链这 3 种类型.

(1) 公有链中无中心化的官方组织及管理机构,参与的节点可自由进出网络,不受系统限制,任何节点间都

能够基于共识机制建立信任从而开展工作,网络中数据读写权限不受限制.

(2) 私有链建立在企业、政府等相关机构内部,网络中的所有节点被一个组织控制,系统的运行规则及共识机制由该组织自行决定,不同节点被赋予了不同的操作能力,写入权限仅限在该组织内部节点,读取权限有限对外开放.由少数高能力节点对全局节点进行管理,不同节点间的地位可能不平等,但同时也保留区块链的不可篡改、安全和部分去中心的特征.

(3) 联盟链由若干机构联合发起组成,部分节点可以任意接入,另一部分则必须通过授权才可以接入,介于公有链和私有链之间,具有多中心或部分去中心的特征,兼顾了公有链和私有链的特点.



(a) 公有链 (b) 私有链 (c) 联盟链

Fig.6 Type of blockchain

图 6 区块链的种类

相对于公有链,联盟链/私有链具有一些优势.例如,成员只要得到管理方的许可,即可改变区块链运行规则,无需征求网络中其他节点的意见,效率较高.同时,交易的确认只在联盟或机构内部人员间进行,不涉及到大量低信任度的外部用户,因此共识成本会显著降低.由于联盟链/私有链使用过程不会匿名化,更容易被监管,所以监管机构也更支持其发展.但是,规则越容易修改,也就越容易给攻击者留下安全漏洞,系统的应用将受到限制.目前在区块链领域派生出两条发展方向:一是以比特币、以太坊为代表的公有链方向;一是以超级账本为代表的联盟链/私有链方向.比特币、以太坊等具有全球化、不受特定组织约束的特点;而超级账本希望打造一个能够满足不同领域商业诉求,同时又能满足各国监管要求的开放区块链平台,推动其成为事实上的区块链国际标准.

Table 2 Comparison of blockchain application patterm

表 2 区块链应用模式对比

	公有链	联盟链	私有链
中心化程度	去中心化	多中心化	相对中心化
参与方	任何人	具有特殊特征的成员	中心指定的可参与成员
记账者	所有参与者	参与者协商决定	自定
优势	完全解决信任问题;可全球用户访问,应用程序容易部署,进入壁垒最低	容易进行权限控制;具有很高的可扩展性,易于推广	能耗低;交易量大、交易速度快;节点通过授权进入,不存在 51%攻击风险
缺点	交易量受限,对共识机制的安全性要求高	无法完全解决信任问题	接入节点受限,不能完全解决信任问题
使用场景	网络节点间没有信任的场景(如比特币、以太坊)	连接多个公司或中心化组织(如 Hyperledger)	节点之间高度信任场景(如中心化交易所)

1.5 应用领域

比特币可以看作是与区块链同时产生的第 1 个区块链实际应用,所以在发展初期,区块链技术主要应用于数字货币及金融领域.随着区块链技术的发展以及人们对区块链特点的深入研究,区块链越来越多的被应用于非金融领域.如图 7 所示,当前区块链技术在非金融领域研究主要集中在以下 3 个方面:(1) 信息记录及管理领域,如信用记录[19−21]、公民及企业信息管理[22]、资产管理[23]、防伪[24]、教育医疗信息管理[25−28]、打分评价[29]、

合同签署[30]等方向;(2) 信息安全领域,如认证技术、访问控制、数据保护等方向;(3) 其他领域,如共享经济[29,31]、能源互联网[32−34]、智能交通[35]等方向.其中,信息安全领域是研究的一个重点,在云计算[36,37]、物联网[38]、移动网络、大数据[39]等新技术条件下对认证技术、访问控制、数据保护等信息安全技术提出去中心、分布式、匿名化、轻量级、高效率、可审计追踪等更高要求,而区块链具有的开放共识、去中心、去信任、匿名性、不可篡改、可追溯性等特点正好与之相吻合,因此,区块链技术能够解决很多传统信息安全技术无法很好解决的问题.

Fig.7 Applications field of blockchain

图 7 区块链应用领域

2 区块链技术在信息安全领域的应用

本节内容将对区块链技术应用于信息安全领域的身份认证、访问控制、数据保护这 3 个方向的研究现状进行详细的分析与总结.

2.1 身份认证方向

2.1.1 基于区块链的身份认证技术

作为信息安全的核心技术之一,身份认证是一项在计算机及网络环境中对用户真实身份进行鉴别的技术.当前主流的认证方法是基于可信第三方认证服务器来对用户身份进行管理,通过用户所知(如用户的口令)、所有(如数据证书、身份令牌)和生物特征(如指纹和虹膜)来确认用户身份.目前,基于区块链的身份认证技术研究主要包括以下 3 个方面.

(1) 基于区块链的 PKI

目前,基于数字证书的认证是一项重要的身份认证技术.但是,目前实现数字证书管理的集中式 PKI 在分布式环境中面临的最大问题是 CA 不可信的问题,从而导致实体身份的不可信.CA 被攻击或恶意的 CA 签发证书将为信息系统带来重大的安全隐患[40],黑客可以通过攻击用户所信任的 CA 来执行恶意操作签发包含虚假信息的用户证书,从而实现中间人攻击.用户无法对 CA 签发证书的过程进行验证,从而存在证书透明度问题.另外,由于中心式的 CA 管理架构,如果 CA 发生故障,将影响所有用户证书的使用,存在单点故障问题.区块链在身份认证方向的一项重要应用是基于区块链构建分布式公钥管理基础设施(public key infrastructure,简称 PKI)[41−43],基于公共总账来建立 PKI,能够消除 PKI 的信任根,实现真正的分布式 PKI 建设.

基于此,2014 年,首个基于区块链技术的分布式 PKI 系统 Certcoin[41,42]由麻省理工大学学者 Conner 提出,其核心思想是通过公共总账来记录用户证书,以公开的方式将用户身份与证书公钥相关联,从而实现去中心化的 PKI 建设,任何用户都可以查询证书签发过程,解决传统 PKI 系统所面临的证书透明度及 CA 单点故障的问题.

Certcoin 架构如图 8 所示,通过以区块链交易的形式发布用户及其公钥来实现证书的注册、更新和撤销,通过区块链不可篡改的属性来保障 PKI 的正常运行,Merkle 根只记录交易的哈希值,用户无需下载全部区块链交易数据即可完成对证书的验证.

但是,由于区块链中交易信息对所有人都是公开可见的,Certcoin 这种直接将公钥链接用户真实身份的方式并不适用于车载网、物联网等需要保护用户身份隐私的场景.基于此,Axon[44,45]对 Certcoin 模型进行改进,提出了一个隐私感知 PKI 模型 PB-PKI(privacy-awareness in blockchain-based PKI).如图 9 所示,该模型不同于传统 PKI 直接通过公钥链接用户真实身份,而是通过线下密钥对线上密钥进行保护,从而实现对用户真实身份的保护.同时,Axon 将用户隐私层次划分为全局隐私和邻近隐私,针对不同的应用场景来进行不同程度的隐私披露.对于可信的邻近节点,用户真实身份与公钥直接关联;对于不可信的全局节点不关联实现匿名化的身份认证,减少了用户隐私信息泄露的风险.

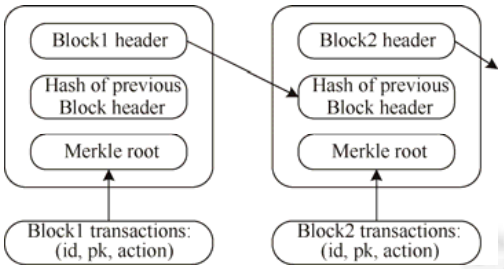


Fig.8 PKI architecture of Certcoin

图 8 Certcoin 的 PKI 架构

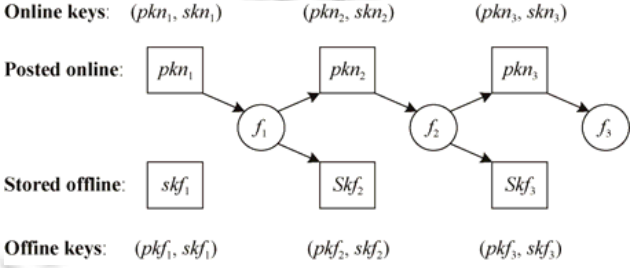


Fig.9 Online key is protected by offline key in PB-PKI

图 9 PB-PKI 使用线下密钥对线上密钥进行保护

不同于上述基于区块链来建立分布式 PKI 系统,Matsumoto[46]针对现有 PKI 系统中 CA 抵抗攻击投入不足的问题展开研究.基于区块链平台的金融特点,提出了一种及时响应的 PKI 框架 IKP(instant karma PKI).IKP 基于以太坊平台以经济手段激励 CA 正确颁发证书,引入探测器检测、报告非法证书,并对颁发非法证书的 CA 进行经济处罚.参与的 HTTPS 域通过发布域证书策略 DCP(domain certificate policy)来规定该域 TLS 证书必须遵循的标准,违背 DCP 规定的证书即是非法证书.同时,成员 CA 可以向域出售响应策略 RP(reaction policy),即如果一个非法证书被上报,发布该非法证书的 CA 将基于智能合约进行赔付交易,类似于金融保险来对用户进行理赔.另外,探测器上报非法证书也是需要费用的,如果上报的证书确实是非法证书,探测器将获得对非法证书数量相关联的奖励,这样能够有效避免探测器上报所有 CA 证书来骗取奖励.图 10 给出了 IKP 的组成架构.

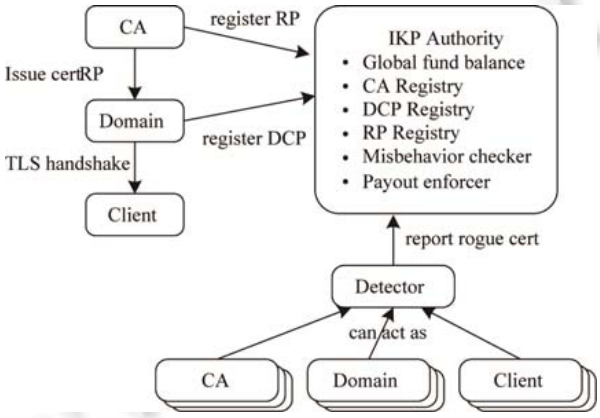


Fig.10 Structure and composition of IKP

图 10 IKP 架构示意图

(2) 基于区块链分布式 PKI 的认证

基于区块链的分布式 PKI 架构,文献[27]实现了 BGP 路由传播和 DNS 映射中可信节点的认证,以防止恶意节点攻击.文献[47]解决了个人云环境的身份管理和证书管理问题,提高了不同云间互操作前认证的效率及安全性,将认证的安全性及可靠性与区块链技术的安全性及可靠性保持一致.文献[48]针对 B2B/B2C 在现实生活中面临的严重交易信用问题,提出了基于区块链的B2B+B2C供应链动态多中心协同认证模型,使模型中企业内部交易主体、供应商、销售商之间任何一个交易主体都有交易行为证明的能力,能够有效防止不同供应商的共谋攻击.文献[49]将区块链 PKI 用于无线传感器网络信任的建立.文献[50]针对智能合约中数据来源的安全认证问题,通过前端的区块链和后端的可信硬件 SGX 实现对数据来源的认证.AI-Bassam[51]针对当前 X.509 证书标准只能对于用户身份签发证书,而无法签署细粒度的身份属性信息证书的问题,基于智能合约对其进行了改进,增加了对属性信息的认证.若用户身份信息得到认证后,该身份对应的属性也是值得信任的,实现了用户身份与用户属性之间信任的传递.

(3) 基于区块链的金融功能实现认证

一些学者利用区块链的金融功能,将数字加密货币(如比特币)作为身份认证中“所有”要素,基于用户所持有的数字货币实现对用户的身份认证.如 Tomoyuki[52]提出了一种基于区块链 2.0 技术的方法来解决 WiFi 的用户身份认证问题,该方法将数字货币作为用户身份凭证,基于区块链平台,通过 Auth-Wallet 来为合法用户分配用于登录认证的 Auth-Coin,用户在登录时,只要用户拥有 Auth-Coin 即可通过身份认证过程,从而访问 WiFi 网络.这样做的好处是无需在每次认证过程中披露用户的用户名、密码等隐私信息,并且只需用户在注册过程中与认证服务器进行一次注册交互过程即可,在之后的访问过程中无需再次与认证服务器进行交互,实现了对隐私身份信息的保护,减少了账号泄露的风险,并且较之需要输入用户名-密码才可登录的 WiFi 网络,更加便利,易于用户使用.此外,Raju[53]使用以太坊的匿名账户钱包通过公钥地址实现对认知蜂窝网络的用户身份管理,并通过智能合约实现了网络的接入认证和支付功能.

2.1.2 区块链中的认证问题

以上研究是运用区块链技术作为基础来提供认证服务,同时,一些学者也对基于区块链的数字加密货币自身的认证问题进行了研究.由于区块链有较好的匿名性,因此在公有链中,可以帮助用户隐藏真实身份,有效地保护用户隐私信息.但在数字货币领域以及私有链/联盟链中,需要保证区块中节点身份的真实性,过强的匿名性将会对洗钱、贩毒、组织内恶意攻击等违法活动带来庇护.基于此,Thomas[54,55]针对私有区块链和联盟区块链交易前的身份认证问题,提出了 ChainAchor 框架.ChainAchor 基于零知识证明理论为区块链中的实体提供匿名但可验证的身份认证服务,真实用户可以保留多个有效身份并且在交易过程中可有选择性地进行身份暴露.同时,ChainAchor 为实体在被授权的区块链中发起交易、读交易和验证交易提供保护服务.共识节点通过对匿名成员公开密钥的(只读)列表进行查找来对共享许可的区块链进行管理,如图 11 所示为 ChainAchor 的工作流程.文献[56]从数字货币更好的应用推广角度出发,在比特币中引入集中式的证书管理,有利于国家及相关组织对数字货币持有人的身份实施监管.

综上所述,基于区块链对用户身份及证书信息进行管理,能够有效地解决证书透明度及单点故障的问题,并且能够有效降低中心 PKI 建设的成本,实现用户身份的轻量级认证.另外,将区块链的金融功能引入认证技术,将数字加密货币充当“身份令牌”,能够极大地减轻用户负担并降低隐私信息泄露的风险;基于区块链技术,能够在保证用户身份不被公开的前提下,实现对用户身份的匿名认证,这对于保护用户身份信息具有重要意义.但是,由于区块链中数据只增不删,对于用户身份及证书的更新及撤销就成为了一个问题,Bui[57]提出将需要撤销证书的 Hash 值作为撤销信息单独存储在区块链中供用户查询.但是,由于区块链发布的证书更新及撤销操作需要多个新区块的确认,从而存在响应时延.当证书操作量大且实时性要求较高时,存在效率低下、更新及撤销操作不及时、操作流程复杂的缺陷,还没有从根本上解决问题.另外,当前成果大多基于理论研究和模拟实验,真实环境效果未知,该领域还有待尽一步的深入研究.

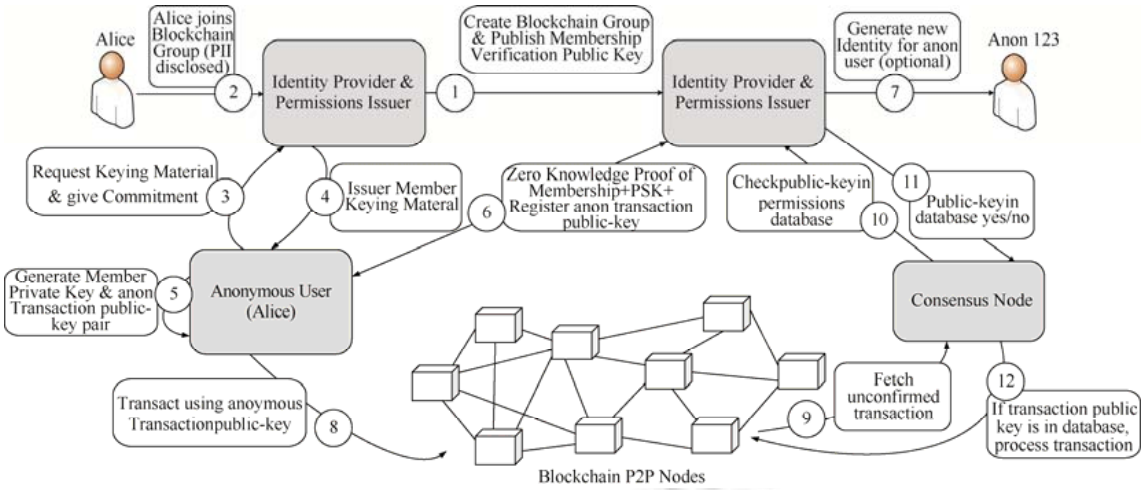


Fig.11 Work process of ChainAnchor

图 11 ChainAnchor 工作流程

2.2 访问控制方向

访问控制技术用于对用户权限进行管理,允许合法用户依照其所拥有的权限访问系统内相应资源,禁止非法用户对系统的访问,从而保证信息的安全和业务的正常运转.目前,基于区块链的访问控制技术研究主要包括基于交易进行策略/权限管理和基于智能合约进行访问控制这两个方面.

2.2.1 基于交易进行策略/权限管理

区块链上记录的数据对所有用户可见且不可篡改,因此可以使用区块链来对访问控制的策略/权限进行管理,从而实现公开透明的访问控制.这就需要将传统访问控制中用户、角色、属性、资源、动作、权限、环境等概念与区块链中交易、帐户、验证、合约等相关概念进行结合.Damiano 机制[58]、Zyskind 机制[59]、FairAccess[60−62]和 Dorri[63,64]分别从不同的角度将区块链交易与访问控制技术相结合.

Damiano[58]探索了使用基于区块链交易的形式来创建、管理、执行访问控制策略的可行性,并通过比特币平台进行了实现.该方法对 ABAC 模型[65−67]的标准工作流进行了扩展,用区块链来代替传统的关系型数据库存储访问控制策略,通过交易的形式进行访问控制策略管理.交易类型包括策略创建交易(policy creation transaction,简称 PCT)和权限转移交易(right transfer transaction,简称 RTT),PCT 用于实现策略的创建、更新、撤销,RTT 用于实现用户间权限的转移.由于区块链是一个数据只增不减的总帐系统,Damiano 巧妙地通过对需要更新或撤销策略的 PCT 输出进行花费形成新的 PCT 实现策略的更新和撤销,从而对相应策略形成了一个交易链,实现对策略的全周期管理.策略和权限的转移保存在公开可见的区块链中,还实现了分布式、不可篡改的日志审计功能,防止参与方以欺诈方式拒绝承认已被策略授予的权限.如图 12 所示,Damiano 机制的工作流程如下.

(1) 用户向资源 resource 发送访问请求,由策略执行点 PEP(policy enforcement point)将请求转发给上下文处理器 CH.

(2) CH 向策略管理点 PAP 发送策略查询请求,由 PAP 基于请求中的资源权限链接 RTT 从区块链中检索并恢复资源 resource 拥有者签发的所有策略.

(3) PAP 整合所检索的策略生成一个标准的 XACML 策略[68],并将该策略返回给 CH.

(4) CH 向策略信息点 PIP 检索相关属性,转发新请求给策略判决点 PDP.

(5) 由 PDP 对其进行访问控制判决并将判决结果(允许或拒绝)返回给 CH.

(6) CH 将判决结果发送至 PEP,由 PEP 对用户进行访问控制.

Zyskind 机制[59]实现了移动应用程序的细粒度权限管理,其框架如图 13 所示,服务表示应用程序,T_{access} 用

于管理策略,T_{data} 用于存储和索引数据.区块链中每个用户和服务都对应一个公钥地址作为身份的凭证,由用户公钥(资源拥有方)与服务公钥(资源请求方)共同以联合身份的形式对权限进行管理.

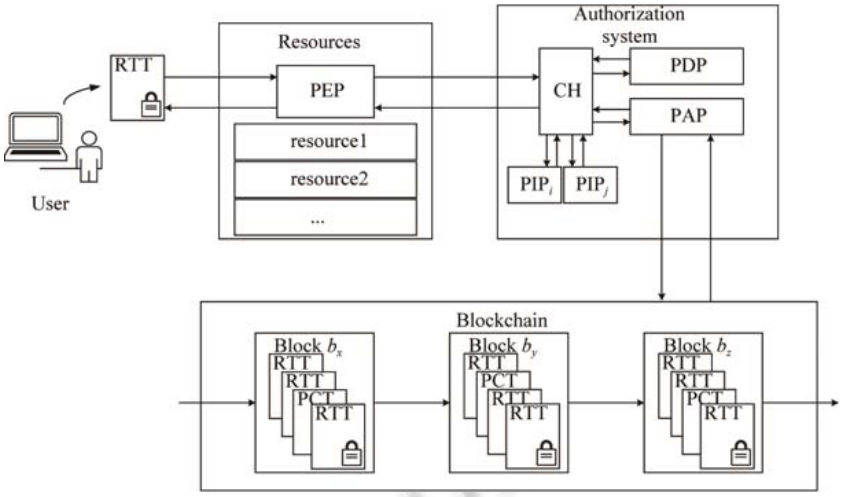


Fig.12 System structure and composition of Damiano

图 12 Damiano 系统结构与组成

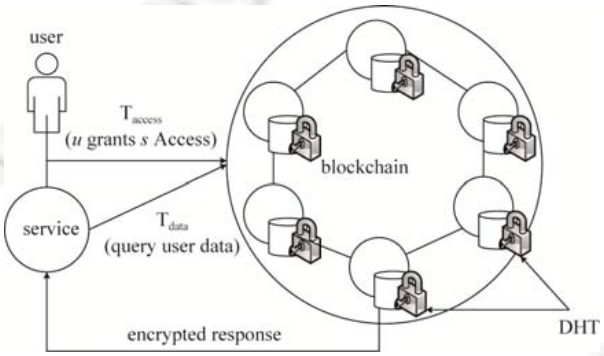


Fig.13 Framework structure of Zyskind

图 13 Zyskind 框架结构

$Compound_{u,s}^{(public)} = (pk_{sig}^{u,s}, pk_{sig}^{s,u})$($Compound_{u,s}^{(public)}$ 表示联合身份, $pk_{sig}^{u,s}$ 代表用户 *u* 的公钥, $pk_{sig}^{s,u}$ 代表服务 *s* 的公钥)策略用 POLICY 进行表示,例如 $POLICY_{u,s}$={*location*,*contacts*},表示当用户安装一个手机 APP 时,允许该 APP 请求访问的用户地址和联系人.以用户和服务联合身份发布 T_{access} 交易,将策略 $POLICY_{u,s}$ 存储在区块链中.若要更新策略,则重新进行新的 T_{access} 交易;若要撤销策略,则改为空的 T_{access} 交易即可.当服务发送访问请求时,用请求的发送方、接收方公钥来验证策略交易签名,进行访问控制判决.该方法扩展了区块链中“交易”的内涵,通过“交易”实现了访问控制.

FairAccess[60−62,69]机制将策略以(resource,requester)的形式存储在区块链交易中,引入比特币中 Wallet 概念,为不同的 IoT 设备安装自己的 Wallet,Wallet 具有访问控制代理的功能,其结构如图 14 所示.通过向被授权的访问请求方账户发送授权令牌的形式进行权限管理,授权令牌代表了能够访问对应资源的权利,令牌由资源拥有者使用请求方公钥进行签名来保证其不可伪造.通过授权令牌能够有效减轻计算资源受限的 IoT 设备处理访问控制信息的开销,且仅通过验证交易签名即可实现对权限的验证.在比特币系统中,不同用户间比特币交易通过未花费的交易输出(unspent transaction output,简称 UTXO)实现,交易的输入是请求方被锁定的 UTXO,输出是被

交易新创建的 UTXO.与比特币这种基于 UTXO 的交易机制类似,FairAccess 使用授权令牌来代表 UTXO,通过 GrantAccess Transaction、GetAccess Transaction、DelegateAccess Transaction 这 3 种交易类型实现授权、获取权限、委派权限.权限的撤销由令牌的时间戳和失效时间进行控制,当令牌超过有效期时,令牌所记录的权限被撤销.从而实现了由用户驱动的、透明化的访问控制.

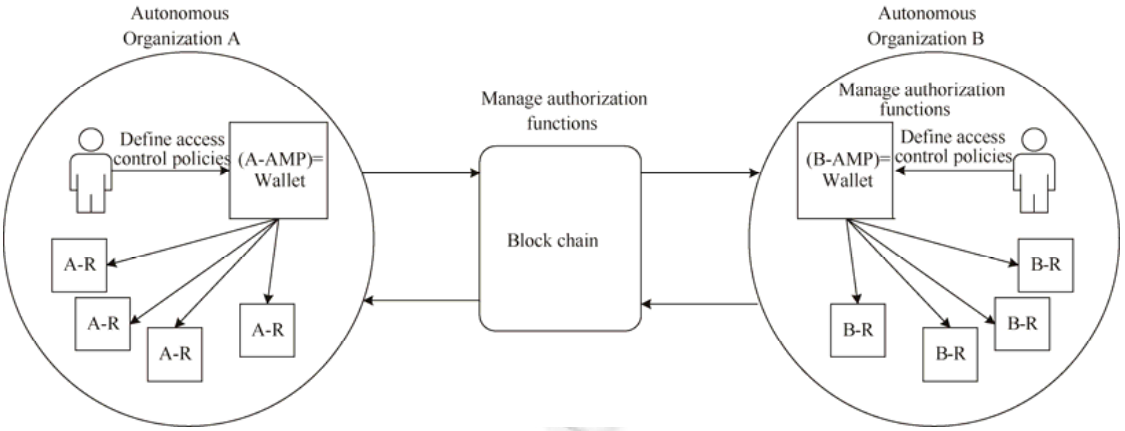


Fig.14 Framework structure of FairAccess

图 14 FairAccess 框架结构

以上机制更适用于公有链的应用场景中.而在私有链的应用场景中,存在区块链维护成本高、签名开销较大、响应时延较长的问题,特别是在计算能力有限的设备中存在性能瓶颈.Dorri[63,64]以智能家居的应用背景为例,建立本地私有区块链,提出了轻量级的解决方案,通过中心矿机消解工作量证明[64]来减小区块链的维护成本,引入了存储、访问、监控、生成设备、删除设备等交易类型.同时,Dorri 对传统区块链协议进行了扩展,增加了策略头存储策略列表,策略头用于授权设备且执行 HOME 主人的访问控制策略.

基于区块链构建访问控制机制,通过交易来对访问控制策略/权限进行管理能够有效地保护用户资源,实现对资源由用户驱动、公开、透明的访问控制.并且,通过将区块链与当前主流的访问控制模型相结合,兼容性高,易于实现.但是,由于当前主流的区块链共识机制是基于算力的,单独运行区块链来提供访问控制服务存在较大的计算开销.并且,区块生成需要一定时间,难以实现策略的实时更新.基于交易进行策略/权限管理研究对比情况见表 3.

Table 3 Research comparison of policy/right based on the transaction

表 3 基于交易进行策略/权限管理研究对比

	Damiano	Zyskind	FairAccess	Dorri
应用背景	泛化	移动应用	物联网	物联网
访问控制机制	ABAC	DAC	OrBAC[70]	ACL
安全性分析	未分析	已分析	未分析	已分析
计算开销	高	中	中	低
私有链	否	否	否	是

2.2.2 基于智能合约进行访问控制

智能合约[71]是存储在区块链上能够自动运行的脚本.1994 年,Szabo 首次提出了智能合约的概念,定义其是一种“通过计算机执行合同条款的交易协议”,即通过代码程序来自动执行合同[72].只要满足合同条款,交易将无需第三方监督自动进行.虽然智能合约的概念很早就被提出,但直到以太坊平台的发布,才为智能合约的飞速发展提供了基础.由于智能合约具有强制自动执行的特点,一些研究通过使用智能合约来实现对资源的访问控制.

文献[73–77]针对当前医疗数据碎片化严重、共享效率低、传输过程不安全、缺乏数据完整性校验及隐私信息保护不足的问题,基于以太坊平台使用智能合约实现对医疗数据的访问控制.其中,最有代表性的是

MedRec 框架[75,76],该框架将智能合约与访问控制相结合进行自动化的权限管理,实现了对不同组织的分布式医疗数据的整合和权限管理.如图 15 所示,MedRec 框架包括 3 个层次的合约,Registrar Contract 用来管理病人身份信息,Patient Provider Relationship 用来进行数据的权限管理,Summary Contract 将病人的身份信息与权限信息相关联.

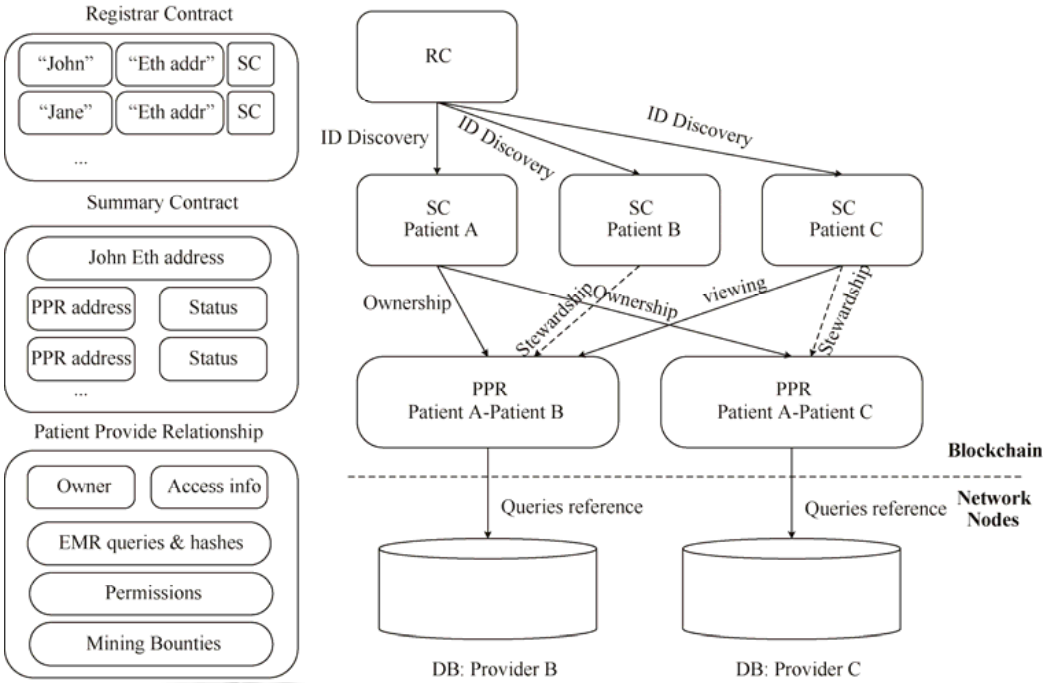


Fig.15 Smart contract framework of MedRec

图 15 MedRec 的智能合约框架

MedRec 框架的优点是基于区块链技术实现了跨医疗组织的医疗数据的去中心化整合,使得医疗数据真正受到病人自己的控制,依据合约医疗组织无法在未征得病人同意的情况下私自使用病人医疗数据,有效地实现了对病人隐私数据的保护.MedRec 框架使用 PoW 共识机制,维持区块链一致性所需计算开销过大.基于此,MDSN 框架[78]对共识机制进行创新,使用 DPoS 共识机制来减轻节点计算压力,并为不同节点引入信誉体系,采用代理重加密的方法对医疗数据进行访问控制,在保护隐私的同时,有效地提高了数据共享效率,但也存在数据存储能力有限的不足.文献[79]基于智能合约对 FairAccess 机制进行了改进,并将访问控制与增强学习相结合,以此来对策略进行动态自适应的优化.文献[80,81]引入可信硬件来为智能合约提供密码学保护.基于智能合约的访问控制研究对比情况见表 4.

Table 4 Research and comparison of access control based on smart contract

表 4 基于智能合约的访问控制研究对比

	MedRec	MDSM	文献[83]	文献[84,85]
应用背景	医疗	医疗	物联网	联盟云
访问控制机制	ACL	代理重加密	OrBAC	ABAC
共识机制	PoW	DPoS	PoW	PoW
计算开销	中	低	中	高
私有链	是	否	否	否

综上所述,将区块链技术应用于访问控制领域主要有如下 5 个优点.

(1) 策略被发布在区块链上,能够被所有的主体可见,不存在第三方的越权行为;

(2) 访问权限能够基于区块链通过与权限拥有者进行交易,实现被访问资源权限更容易地从一个用户转移

给另一个用户,资源拥有者无需介入到用户之间,权限管理更加灵活;

(3) 权限最初由资源拥有者通过交易对其进行定义,整个权限的交易过程在区块链上公开,便于审计;

(4) 资源的管理使用权真正掌握在用户手中;

(5) 基于智能合约能够实现对资源自动化的访问控制保护.

但是,也存在一些亟待解决的问题.

(1) 由于被区块链记录的交易不可撤销,访问控制策略及权限不易更新;

(2) 区块容量有限,单个交易无法存储较大规模数据,使其应用受限;

(3) 所有策略及权限交易信息都公开存放在区块链上,容易被攻击者利用,产生安全风险,需要有效的方法对交易信息进行保护;

(4) 区块链技术交易确认需要时间(如比特币 10 分钟左右才产生新的区块),无法对实时请求进行响应.

2.3 数据保护方向

数据保护技术的核心是实现对数据机密性和完整性保护.机密性是指数据不被未授权者访问的属性;完整性是指保证数据真实、有效、未被篡改的属性.当前一些学者围绕区块链对数据保护问题展开研究.区块链是一种分布式的共享总账系统,但是,由于区块容量有限,难以存储大规模的数据,针对数据规模的不同分别采取链上数据保护和链上链下相结合两种数据保护方案.

2.3.1 链上数据保护

(1) 采用区块链保障数据的完整性

区块链上记录的数据只增不减且不可篡改,该特性可用于对数据使用全流程的监控,实现不可篡改的数据记录,用于日志审计、数据真实性保障、合同管理、数字取证等领域.

2016 年,欧洲议会批准了商讨 4 年之久的通用数据保护条例(general data protection regulation,简称 GDPR)[82],该条例要求针对欧盟公民数据的控制、处理过程实现全流程可追踪、可审计.基于此,Ricardo[83]提出了一个基于区块链数据的管控方法,该方法支持数据问责和来源追踪,如图 16 所示.该方法依赖于部署在区块链上的公开审计合约 Pubilcly Auditable Contracts 的使用,将数据的控制策略写入到智能合约,由合约自动完成对数据来源进行追踪并对数据使用流程记录日志,从而增加了数据使用和访问的透明度.

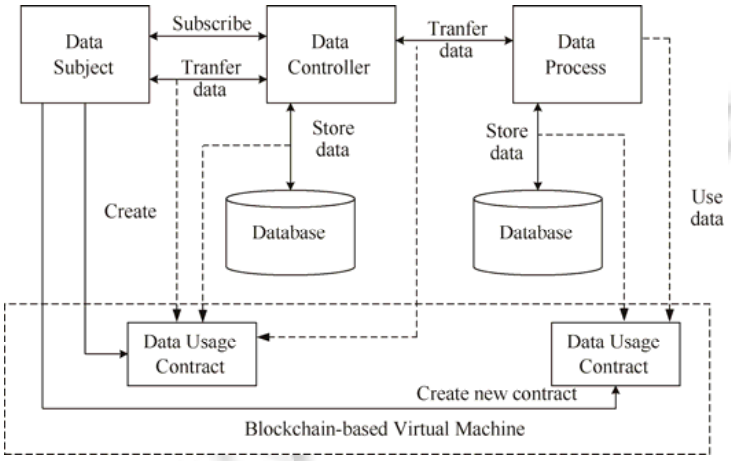


Fig.16 System framework of Ricardo

图 16 Ricardo 系统框架

数据安全创业公司 GurdTime 开发了一款基于区块链技术无秘钥签名架构的数据保护产品 KSI 来保证原始数据的真实、可靠,KSI 在区块链上存储原始数据及其哈希表,利用哈希算法来验证复制数据的真实性.文献[84]提出了一种基于区块链的传感数据真实性保障方法,并在微生物采样机器人系统中展开了应用.该方法可

以保证机器人在完成工作任务时记录数据的真实性,避免受到外部人为干预的影响.文献[85]使用区块链来实现不可篡改的安全审计日志.文献[25]将区块链技术用于医疗数据的真实性保护,防止数据被恶意攻击者篡改.文献[86]将区块链应用于云环境的数字取证,保障证据信息的完整性和时效性.文献[87]针对可穿戴设备计算能力有限的问题,利用 Bloom Filter 这种空间效率很高的数据结构优化了区块数据管理,提高了算法的空间和时间效率.

(2) 区块链中数据的隐私保护

由于区块链中存储的交易信息与智能合约直接暴露在区块链中,所有用户都可对其进行查看,这就带来了交易数据隐私暴露的问题.Hawk[88]是一个基于密码学的区块链合约开发平台,用来解决区块链上隐私和智能合约安全保护的问题,不把隐私交易信息直接存储于区块链.与传统智能合约开发相似,Hawk 允许程序员以直观的方式编写具有隐私保护需求的智能合约,而不必考虑加密的实现,由 Hawk 编译器自动生成高效的基于零知识证明的加密协议来与区块链进行交互.如图 17 所示,Public 用来处理不涉及隐私数据的代码,Private 用来处理隐私数据的代码,对 Private 处理的数据进行加密保护.

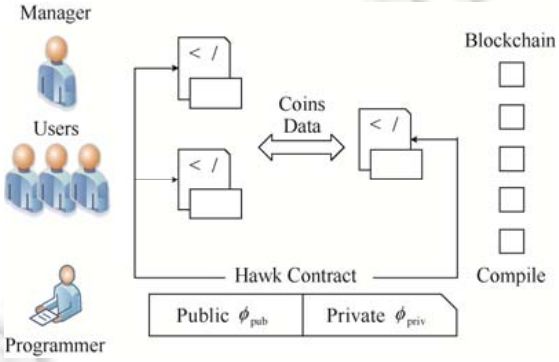


Fig.17 System framework of Hawk

图 17 Hawk 系统架构

综上所述,由于区块链的高度安全性及时间维度,因此,链上数据拥有极高的数据抗篡改特性,能够有效保障数据的完整性,且成本低廉、易于实施,可广泛应用于物联网设备数据保护、大数据隐私保护、数字取证、审计日志记录等多个技术领域.

2.3.2 链上链下结合的数据保护

针对区块链未对交易数据进行加密保护,并且区块链的存储容量和计算资源受限的问题,文献[89]基于区块链技术实现在保护数据隐私安全的前提下数据的共享,数据共享过程由 User、Service、Blind Escrow 和区块链共同实现.Service 对 User 元数据进行签名,并将签名的哈希值存储在链上.另外,Service 将元数据加密存储在链下被 User 信任的第三方数据库 Blind Escrow 中,以保证数据的安全.User 和 Service 通过共享秘钥实现对用户加密数据的访问,如图 19 所示为写数据流程.

文献[90]提出了一种能够实现安全数据保护的分布式计算框架 Enigma,将数据的管理与存储分离,依靠区块链通过 DHT[91]存储数据索引来管理数据,依靠计算和存储能力更强的链下计算节点来存储数据.每个节点可以存储非加密的共享数据和已加密的隐私数据.Enigma 将数据访问分为 Public ledger、DHT(distributed hash-table)、MPC(multi-party compution)3 种类型.Public ledger 将数据存储在区块链中面向所有用户公开,DHT 和 MPC 只在区块链中存储数据的索引,在索引指向的地址中存储加密数据.区块链技术用来确保数据的完整性,DHT 链下存储用来确保数据的机密性,在数据共享的过程中,仅共享数据的地址,而不是共享数据的内容,从而实现了对数据的保护.Enigma 框架也能用于完成复杂的分布式计算任务.

综上所述,由于区块链容量有限,区块链技术应用于数据保护,通常使用数据存储与数据管理分离的方式,数据索引及操作权限由区块链进行管理,真实数据并不存储在区块链中,而是集中存储于专用的数据服务器.通

过区块链分布式总帐来保证数据的完整性,数据服务器保证数据的机密性.但是,这种方法也存在一些共性问题.

(1) 数据的管理寄托于区块链自身的安全机制,若区块链遭遇共识攻击(如 51%攻击),数据的安全性将无从谈起;

(2) 用户身份与区块链中的公钥地址唯一对应,若用户私钥丢失,将无法找回,与用户相关的数据资源也将全部丢失.因此,如何保证区块链的共识安全、账户安全还有待于尽一步的研究.

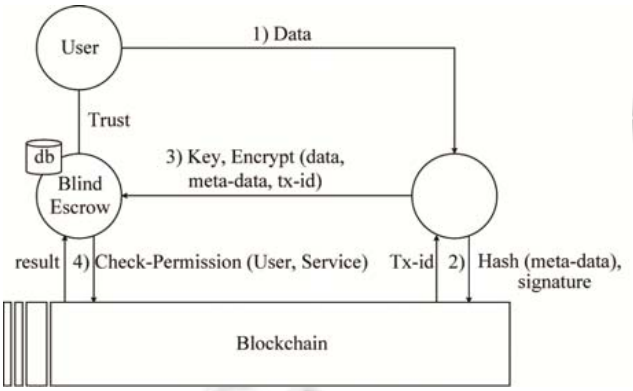


Fig.18 Writing data process of Lazarovich method

图 18 Lazarovich 方法的写数据流程

3 研究挑战与展望

3.1 区块链技术自身存在的问题

虽然区块链技术具有很多优势并且取得了丰硕的研究成果,但是目前区块链技术在平台安全性、匿名性与隐私性、技术壁垒等方面都存在着很多亟待解决的问题.这些问题也是区块链技术应用于信息安全领域时必须要解决的关键问题.

1) 区块链平台安全性问题

若将区块链应用于信息安全领域,区块链系统的安全性就成为了保障整个信息系统安全的基石和前提.区块链系统安全性主要包括两个方面.

(1) 区块链自身安全问题

区块链安全性靠共识机制进行支撑,当前最流行且应用最广泛的是基于算力的 PoW 共识机制,主流公有链平台比特币、以太坊等都依赖于分布在世界各地的“矿工”持续不断地“挖矿”来维持系统正常运转,但由于挖矿激励机制,造成全球算力的大量集中.从概率上讲,算力超强就代表能够获得越多的货币奖励,算力低的矿工将因为得不到激励而逐渐被淘汰出局,最后将导致整个区块链平台的维护只由少数具有超强算力的矿池节点来提供支撑,这违背了区块链技术分布式、去中心化的设计初衷.以比特币为例,截止到 2017 年 10 月,全球前四大矿池 AntPool(占 20.78%)、BTC.TOP(占 13.48%)、BTC.com(占 11.8%)、ViaBTC(占 9.55%)的算力总和占到全球算力的 55.62%.从理论上讲,如果能够控制整个网络的算力 51%以上,就能够通过算力优势来对区块链上数据进行篡改,从而对区块链所建立的信任体系进行颠覆[92].而不基于算力的 PoS、DPoS 等共识机制的安全性还未得到理论上的有效证明,PBFT 等强一致性算法又存在算法复杂度高、去中心化程度低等不足.因此,要将区块链应用于信息安全领域,安全的共识机制的研究是面临的重大挑战之一.

(2) 用户账户的安全性问题

传统的身份账户由第三方进行保护,当用户账号发生丢失等意外时,用户可以凭借有效的身份证明对密码进行重置.而区块链账号仅由持有人地址对应的私钥对其保护,涉及账号的所有交易都要使用该私钥,一旦私钥

丢失,则无法重置或找回,用户将永久性失去其账户内的数字资产,这是区块链去中心化机制所带来的弊端.既然该私钥如此重要,管理区块链账户即是对私钥进行保管和使用.如何在方便账户使用的同时又保障数字资产的安全性还需要进行深入的研究,从而实现保障账户安全性与可用性的统一.

2) 匿名性和隐私性

区块链技术经常被宣传的优点之一就是匿名性[93],但是以数字加密货币为例,从实际情况上来看,其并不具备真正的匿名性,且隐私性无法得到真正的保障[94,95].区块链是完全透明的系统,交易信息以公共总账方式公开存储,这使得任何人都可以查询所有交易信息.通过数据挖掘技术,可以发现很多地址间的关联关系.从积极的方面说,监管机构能够从中得到非法交易人员及攻击者犯罪的蛛丝马迹;而从消极的方面来说,用户的隐私无法得到有效的保障,每个用户能够拥有多个地址,就好比将每笔交易都用假名向公众进行公开发布,一旦其中一个地址假名的真实身份被泄漏,所有交易及相关隐私数据都将暴露在公众的视野中.

3) 技术壁垒问题

区块链作为一项新兴信息,自身还存在很多不足和需要改进的地方.

(1) 区块链的技术操作较为麻烦,并且区块链交易处理速度较慢.以比特币为例,每一交易区块处理大约需要 10 分钟,无法对实时请求进行相应.区块链安全性也与处理时间成正比,处理时间越短,系统抵抗篡改攻击、非法交易的效果就越差.

(2) 区块链是一种数据只增不删的分布式总账系统,区块链数据所占容量也不断增大,从 2014 年~2016 年,比特币中完整区块链容量从 14GB 增长到 132GB,截止到 2017 年 10 月,以太坊的区块链容量已经达到 180GB,这样大的容量需要交易用户具有很高的网络带宽,技术及应用整合存在难度,如何实现区块链的轻量化也是一个急需解决的问题.

(3) 由于区块容量所限,无法存放大规模数据,这也限制了区块链技术的应用.以比特币为例,比特币单个区块容量有 1MB 的最大值限制,当所要存储在区块链上的数据超过 1MB 时,就要对数据进行分割,将分割后的数据存储在不同的区块上.然而,新区块在共识机制下成功接入区块链需要等待一定时间来保证通过绝大多数节点的验证,这在存取效率上是难以接受的,从而导致区块难以直接存放大规模数据.

(4) 由于区块链技术目前还在不断发展完善,还没有相关技术标准的出台.从而导致现阶段各行业在应用区块链技术时,缺乏核心的技术理念和基本的应用共识,不同区块链平台及应用都采用了各自不同的技术标准,自成体系,难以实现不同区块链间数据的互通互连,并导致整个行业发展分散化、碎片化,无法形成发展合力.同时,由于缺少权威机构对区块链相关产品可靠性、安全性的评估机制,使得区块链产品质量良莠不齐.

3.2 区块链技术应用于信息安全领域的研究展望

下面对信息安全与区块链技术能够相结合的研究方向进行展望,以供研究探讨.

(1) 身份管理方向

区块链技术能够实现用户身份产生、认证、使用以及注销的全生命周期管理.特别是基于区块链技术在无中心环境下,通过公共总账建立的分布式 PKI 系统,能够实现对用户证书可信、透明的管理.已有的研究工作往往只面向单一安全域内用户身份的管理,但在实际应用中,不同机构和服务间需要进行交互,存在跨越多个安全域进行访问的需求,每个安全域内可能都存在一套本域身份管理机制,在这种情况下,需要进行交叉认证,实现跨域互联,难以采取统一方式实现身份联合和单点登录,存在跨域访问时用户身份隐私泄露的风险,并且带来了重复认证的额外运行开销.同时,证书撤销一直都是 PKI 关注的重点,由于证书撤销受计算、通信、存储、时延等因素的影响,难以实现实时的证书撤销操作,存在重放攻击的危险.另外,基于区块链的 PKI 研究也要考虑与现有证书系统的兼容性,从而实现其更好的推广与应用.因此,未来的研究可以尝试对应用区块链技术解决大规模跨域 PKI 应用、证书及时撤销、不同 PKI 系统兼容性等难题进行深入研究.

(2) 访问控制方向

将区块链技术结合当前主流的访问控制模型(如 DAC 模型、MAC 模型、RBAC 模型及 ABAC 模型等)和标准访问控制策略语言(如 XACML、SAML 等),能够实现对资源由用户驱动的、透明的访问控制.但当前研究

应用场景较为单一,主要是用来实现对单一服务或机构内部用户权限的管理,无法解决组合服务或域间互操作所面临的策略合成问题.在陌生服务及组织间建立信任关系,需要提高策略合成的透明度和策略的动态适应能力、检测冲突策略并及时消解策略冲突、提高互操作的灵活性,从而实现对动态资源权限的细粒度控制.同时,可将信任模型研究引入访问控制机制,通过区块链所具有的金融功能采取相应的奖励和惩罚机制对实体间的信任度进行维护,根据实体信任度的不同为其设定相应的角色或属性,以此来判断实体所能获得的相应权限,从而保护实体间交互的安全性,防止恶意攻击事件的发生.另外,当前策略信息都以公开的方式存储在区块链中,如何采取有效的方法来对策略信息进行保护还需深入研究.

(3) 数据保护方向

区块链所具有的不可篡改特性能够有效地对数据的完整性进行保护,而数据的机密性需要依赖密码学技术进行保护.已有的研究基于性能和可用性的考量,使用的都是传统的密码学技术,如单向 Hash 函数、对称加密算法和非对称加密算法等,而不是更强大的密码学工具,如同态加密等.这限制了当前区块链数据保护方案在功能性和安全性上所能够达到的上限,随着计算机存储能力和计算能力的增长,可以对通用的强大密码学工具进行适当的特殊化,从而适用于云计算、大数据等计算环境,达到实用效果.同时,在数据保护过程中,可以将区块链技术与可信硬件相结合,确保数据在存储、传输、使用过程中的安全性.另外,由于用户使用数据服务时,大规模的数据需要存储在链下第三方数据服务器中,用户难以确认服务器是否真正执行了数据删除操作.因此,确保数据的可信删除也需要进一步的研究.

(4) 其他方向

区块链能够对数据处理全流程进行追踪与管控,基于区块链存储审计日志数据可保证审计日志数据的真实性.为了能够及时预警攻击行为,对审计信息进行及时分析并发现攻击者对系统的攻击行为显得尤为重要,区块链具有时间维度,其可追溯且无法被篡改的特性能够为入侵检测技术提供真实的审计日志信息和高可信度的操作证明.同时,数字取证技术也可以依赖于可信的区块链数据,发现犯罪痕迹、提取犯罪证据.

4 结束语

信息技术的飞速发展在方便人们生产与生活的同时也带来了很多新的安全问题.区块链具有的开放共识、去中心、去信任、匿名性、安全不可篡改、可追溯性等特点能够为如何有效地保障数据安全提供一条解决问题的思路.本文系统地梳理了区块链的基础框架、关键技术、技术特点、应用模式和应用领域,并对区块链技术在信息安全领域的研究进行了综述,以期对未来研究提供有益的启发与借鉴.

References:

[1] Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.

[2] Mukhopadhyay U, Skjellum A, Hambolu O, Oakley J, Yu L, Brooks R. A brief survey of Cryptocurrency systems. In: Privacy, Security and Trust. 2017. 745–752. [doi: 10.1109/PST.2016.7906988]

[3] Antonopoulos AM. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. O'Reilly Media, Inc., 2014.

[4] Fan J, Yi LT, Shu JW. Research on the technologies of Byzantine system. Ruan Jian Xue Bao/Journal of Software, 2013,24(6): 1346–1360 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4395.htm [doi: 10.3724/SP.J.1001.2013.04395]

[5] Dwyer GP. The economics of bitcoin and similar private digital currencies. Social Science Electronic Publishing, 2015,17:81–91. [doi: 10.1016/j.jfs.2014.11.006]

[6] Karame GO, Androulaki E, Roeschlin M, Gervais A. Misbehavior in bitcoin: A study of double-spending and accountability. ACM Trans. on Information & System Security, 2015,18(1):2. [doi: 10.1145/2732196]

[7] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. In: Consulted. 2008.

[8] Donet J a D, Pérez-Sola C, Herrera-Joancomartí J. The bitcoin P2P network. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. 2014. 87–102. [doi: 10.1007/978-3-662-44774-1_7]

[9] Stallings W. Cryptography and network security: Principles and practice. Int'l Annals of Criminology, 1999,46(4):121–136.

[10] Mattila J. The blockchain phenomenon—The disruptive potential of distributed consensus architectures. ETLA Working Papers, 2016.

[11] Peters GW, Panayi E. Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. Springer Int'l Publishing, 2016.

[12] Bhargavan K, Swamy N, Zanella-Béguelin S, Delignat-Lavaud A, Fournet C, Gollamudi A, Gonthier G, Kobeissi N, Kulatova N, Rastogi A. Formal verification of smart contracts: Short paper. In: Proc. of the ACM Workshop. 2016. 91–96. [doi: 10.1145/2993600.2993611]

[13] Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami J. Blockchain contract: Securing a blockchain applied to smart contracts. In: Proc. of the IEEE Int'l Conf. on Consumer Electronics. 2016. 467–468. [doi: 10.1109/ICCE.2016.7430693]

[14] Evans DS. Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. Social Science Electronic Publishing, 2014. 203–231. [doi: 10.2139/ssrn.2424516]

[15] Lamport L, Shostak RE, Pease MC. The Byzantine generals problem. ACM Trans. on Programming Languages and Systems, 1982, 4(3):382–401. [doi: 10.1145/357172.357176]

[16] Fischer MJ, Lynch NA, Paterson M. Impossibility of distributed consensus with one faulty process. Journal of the ACM, 1985, 32(2):374–382. [doi: 10.1145/3149.214121]

[17] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. on Computer Systems, 2002,20(4): 398–461. [doi: 10.1145/571637.571640]

[18] Buterin V. Ethereum White Paper. 2013.

[19] Schaub A, Bazin R, Hasan O, Brunie L. A trustless privacy-preserving reputation system. In: Proc. of the IFIP Int'l Information Security and Privacy Conf. Springer Int'l Publishing, 2016. 398–411. [doi: 10.1007/978-3-319-33630-5_27]

[20] Yang Z, Zheng K, Yang K, Leung VC. A blockchain-based reputation system for data credibility assessment in vehicular networks. In: Proc. of the IEEE Int'l Symp. on Personal, Indoor, and Mobile Radio Communications. 2017. 1–5. [doi: 10.1109/PIMRC.2017.8292724]

[21] Dennis R, Owen G. Rep on the block: A next generation reputation system based on the blockchain. In: Internet Technology and Secured Transactions. 2016. 131–138. [doi: 10.1109/ICITST.2015.7412073]

[22] Yasin A, Liu L. An online identity and smart contract management system. In: Proc. of the Computer Software and Applications Conf. 2016. 192–198. [doi: 10.1109/COMPSAC.2016.2]

[23] Wijaya DA. Extending asset management system functionality in bitcoin platform. In: Proc. of the Int'l Conf. on Computer, Control, Informatics and ITS Applications. 2017. 97–101. [doi: 10.1109/IC3INA.2016.7863031]

[24] An R, He DB, Zhang YR, Li L. The design of an anti-counterfeiting system based on blockchain. Journal of Cryptologic Research, 2017,4(2):199–208 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000174]

[25] Zhang J, Xue N, Huang X. A secure system for pervasive social network-based healthcare. IEEE Access, 2016,4(99):9239–9250. [doi: 10.1109/ACCESS.2016.2645904]

[26] Mettler M. Blockchain technology in healthcare: The revolution starts here. In: Proc. of the IEEE Int'l Conf. on E-Health Networking Applications and Services. IEEE, 2016. 1–3. [doi: 10.1109/HealthCom.2016.7749510]

[27] Hari A, Lakshman TV. The Internet blockchain: A distributed, tamper-resistant transaction framework for the Internet. In: Proc. of the ACM Workshop on Hot Topics in Networks. 2016. 204–210. [doi: 10.1145/3005745.3005771]

[28] Sharples M, Domingue J. The blockchain and Kudos: A distributed system for educational record, reputation and reward. In: Proc. of the European Conf. on Technology Enhanced Learning. 2016. 490–496. [doi: 10.1007/978-3-319-45153-4_48]

[29] Huckle S, Bhattacharya R, White M, Beloff N. Internet of Things, blockchain and shared economy applications. Procedia Computer Science, 2016,98(C):461–466. [doi: 10.1016/j.procs.2016.09.074]

[30] Tian HB, He JJ, Fu LQ. A privacy preserving fair constract signing protocol based on block chains. Journal of Cryptologic Research, 2017,4(2):187–198 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000173]

[31] Pazaitis A, De Filippi P, Kostakis V. Blockchain and value systems in the sharing economy: The illustrative case of backfeed. Social Science Electronic Publishing, 2018,1:125–162. [doi: 10.1016/j.techfore.2017.05.025]

[32] Mihaylov M, Razo-Zapata I, Radulescu R, Nowe A. Boosting the renewable energy economy with NRGcoin. ICT for Sustainability, 2016. [doi: 10.2991/ict4s-16.2016.27]

[33] Murkin J, Chitchyan R, Byrne A. Enabling peer-to-peer electricity trading. ICT for Sustainability, 2016. [doi: 10.2991/ict4s-16.2016.30]

[34] Zhang N, Wang Y, Kang CQ, Cheng JN, He DW. Blockchain technique in the energy Internet: Preliminary research framework and typical applications. CSEE, 2016,36(15):4011–4022 (in Chinese with English abstract). [doi: 10.13334/j.0258-8013.pcsee.161311]

[35] Yuan Y, Wang FY. Towards blockchain-based intelligent transportation systems. In: Proc. of the IEEE Int'l Conf. on Intelligent Transportation Systems. 2016. 2663–2668. [doi: 10.1109/ITSC.2016.7795984]

[36] Wang YD, Yang JH, Xu C, Ling X, Yang Y. Survey on access control technologies for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2015,26(5):1129–1150 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4820.htm [doi: 10.13328/j.cnki.jos.004820]

[37] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. Ruan Jian Xue Bao/Journal of Software, 2011,22(1):71–83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[38] Zhang YQ, Zhou W, Peng AN. Survey of Internet of Things security. Journal of Computer Research and Development, 2017,(10):2130–2143 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2017.20170470]

[39] Feng DG, Zhang M, Li H. Big data security and privacy protection. Chinese Journal of Computers, 2014,37(1):246–258 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2014.00246]

[40] Lin JQ, Jing JW, Zhang QL, Wang Z. Recent advances in PKI technologies. Journal of Cryptologic Research, 2015,2(6):487–496 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000095]

[41] Fromknecht C, Velicanu D. CertCoin: A NameCoin based decentralized authentication system. Technical Report, 6.857 Class Project, Massachusetts Institute of Technology, 2014.

[42] Fromknecht C, Velicanu D. A decentralized public key infrastructure with identity retention. Technical Report, 803, Massachusetts Institute of Technology, 2014.

[43] Lewison K, Corella F. Backing rich credentials with a blockchain PKI. Technical Report, Pomian & Corella, LLC, 2016.

[44] Axon L. Privacy-Awareness in blockchain-based PKI. Technical Report, 21-15, University of Oxford, 2015.

[45] Axon L, Goldsmith M. PB-PKI: A privacy-aware blockchain-based PKI. In: Proc. of the Int'l Conf. on Security and Cryptography. 2017. 311–318. [doi: 10.5220/0006419203110318]

[46] Matsumoto S, Reischuk RM. IKP: Turning a PKI around with decentralized automated incentives. In: Security and Privacy. 2017. 410–426. [doi: 10.1109/SP.2017.57]

[47] Faisca JG, Rogado JQ. Personal cloud interoperability. In: World of Wireless, Mobile and Multimedia Networks. 2016. 1–3. [doi: 10.1109/WoWMoM.2016.7523546]

[48] Zhu JM, Fu YG. Supply chain dynamic multi-center coordination authentication model based on block chain. Chinese Journal of Network and Information Security, 2016,2(1):27–33 (in Chinese with English abstract). [doi: 10.11959/j.issn.2096-109x.2016.00019]

[49] Kuo TT, Hsu CN, Ohno-Machado L. ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. Technical Report, University of California San Diego, 2018.

[50] Zhang F, Cecchetti E, Croman K, Juels A, Shi E. Town Crier: An authenticated data feed for smart contracts. In: Proc. of the ACM Conf. on Computer and Communications Security. 2016. [doi: 10.1145/2976749.2978326]

[51] Al-Bassam M. SCPKI: A smart contract-based PKI and identity system. In: Proc. of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017. 35–40. [doi: 10.1145/3055518.3055530]

[52] Sanda T, Inaba H. Proposal of new authentication method in Wi-Fi access using Bitcoin 2.0. In: Proc. of the 2016 IEEE Global Conf. on Consumer Electronics. 2016. 1–5. [doi: 10.1109/GCCE.2016.7800479]

[53] Raju S, Boddepalli S, Gampa S, Yan Q, Deogun JS. Identity management using blockchain for cognitive cellular networks. In: Proc. of the IEEE Int'l Conf. on Communications. IEEE, 2017. 1–6. [doi: 10.1109/ICC.2017.7996830]

[54] Hardjono T, Alex. Verifiable anonymous identities and access control in permissioned blockchains. Technical Report, Massachusetts Institute of Technology, 2016.

[55] Hardjono T, Smith N. Cloud-Based commissioning of constrained devices using permissioned blockchains. In: Proc. of the ACM Int'l Workshop on Iot Privacy, Trust, and Security. 2016. 29–36. [doi: 10.1145/2899007.2899012]

[56] Ateniese G, Faonio A, Magri B, Medeiros BD. Certified bitcoins. In: Proc. of the Int'l Conf. on Applied Cryptography and Network Security. 2014. 80–96. [doi: 10.1007/978-3-319-07536-5_6]

[57] Bui T, Aura T. Application of public ledgers to revocation in distributed access control. Technical Report, Aalto University, 2016.

[58] Maesa DDF, Mori P, Ricci L. Blockchain based access control. In: Proc. of the IFIP Int'l Conf. on Distributed Applications and Interoperable Systems. Springer-Verlag, 2017. 206–220. [doi: 10.1007/978-3-319-59665-5_15]

[59] Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the IEEE Security and Privacy Workshops. 2015. 180–184. [doi: 10.1109/SPW.2015.27]

[60] Ouaddah A, Elkalam AA, Ouahman AA. FairAccess: A new Blockchain—Based access control framework for the Internet of Things. Security & Communication Networks, 2016, 9. [doi: 10.1002/sec.1748]

[61] Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 2017,112:237–262. [doi: 10.1016/j.comnet.2016.11.007]

[62] Ouaddah A, Elkalam AA, Ouahman AA. Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT. Springer Int'l Publishing, 2017. [doi: 10.1007/978-3-319-46568-5_53]

[63] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: Proc. of the IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing. 2017. [doi: 10.1109/PERCOMW.2017.7917634]

[64] Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of Things: Challenges and solutions. Technical Report, University of New South Wales (UNSW), 2016.

[65] Hu V, Ferraiolo D, Kuhn R, Schnitzer A, Sandlin K, Miller R, Scarfone K. Guide to attribute based access control (ABAC) definition and considerations. Technical Report, ITLB, 2013. [doi: 10.6028/NIST.SP.800–162]

[66] Li XF, Feng DG, Cheng CW, Fang ZH. Model for attribute based access control. Journal on Communications, 2008,29(4):90–98 (in Chinese with English abstract).

[67] Wang XM, Fu H, Zhang LC. Research progess on attribute-based access control. ACTA ELECTRONICA SINICA, 2010,38(7):1660–1667 (in Chinese with English abstract).

[68] Sinnema R, Wilde E. eXtensible access control markup language (XACML). Technical Report, RFC7061, EMC Corporation, 2013.

[69] Ouaddah A, Bouij-Pasquier I, Elkalam AA, Ouahman AA. Security analysis and proposal of new access control model in the Internet of Thing. In: Proc. of the Int'l Conf. on Electrical and Information Technologies. 2015. 30–35. [doi: 10.1109/EITech.2015.7162936]

[70] Kalam A a E, Benferhat S, Miège A, Baida RE, Cuppens F, Saurel C, Balbiani P, Deswarte Y, Trouessin G. Organization based access control. In: Proc. of the IEEE Int'l Workshop on Policies for Distributed Systems and Networks. 2003. 120–131. [doi: 10.1109/POLICY.2003.1206966]

[71] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access, 2016,4:2292–2303. [doi: 10.1109/ACCESS.2016.2566339]

[72] Kõlvart M, Poola M, Rull A. Smart Contracts. Springer Int'l Publishing, 2016. [doi 10.1007/978-3-319-26896-5_7]

[73] Mcfarlane C, Beer M, Brown J, Prendergast N. Patientory: A healthcare peer-to-peer EMR storage network v1.1. Technical Report, ICObazaar, 2017.

[74] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-Preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities & Society, 2018, 39. [doi: 10.1016/j.scs.2018.02.014]

[75] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. In: Proc. of the Int'l Conf. on Open and Big Data. 2016. 25–30. [doi: 10.1109/OBD.2016.11]

[76] Ekblaw A, Azaria A, Halamka JD, Md†, Lippman A. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. Technical Report, 5-56-ONC, Massachusetts Institute of Technology, 2016.

[77] Kim KJ, Hong SP. Study on rule-based data protection system using blockchain in P2P distributed networks. Int'l Journal of Security and its Applications, 2016,10(11):201–210. [doi: 10.14257/ijsia.2016.10.11.18]

[78] Xue PF, Fu QC, Wang C, Wang XY. Study on medical data sharing model based on blockchain. ACTA AUTOMATICA SINICA, 2017,43(9) (in Cinese with English abstract). [doi: 10.16383/j.aas.2017.c160661]

[79] Outchakoucht A, Es-Samaali H, Philippe J. Dynamic access control policy based on blockchain and machine learning for the Internet of Things. Int'l Journal of Advanced Computer Science & Applications, 2017,8(7). [doi: 10.14569/IJACSA.2017.080757]

[80] Alansari S, Paci F, Sassone V. A distributed access control system for cloud federations. In: Proc. of the IEEE Int'l Conf. on Distributed Computing. 2017. [doi: 10.1109/ICDCS.2017.241]

[81] Alansari S, Paci F, Margheri A, Sassone V. Privacy-Preserving access control in cloud federations. In: Proc. of the IEEE Int'l Conf. on Cloud Computing. IEEE Computer Society, 2017. 757–760. [doi: 10.1109/CLOUD.2017.108]

[82] European Parliament and of the Council. General data protection regulation. Official Journal of the European Union (OJ), 2016,59: 1–88.

[83] Neisse R, Steri G, Naifovino I. A blockchain-based approach for data accountability and provenance tracking. In: Proc. of the Int'l Conf. on Availability, Reliability and Security. ACM, 2017. 14.

[84] Zhao H, Li XF, Zhang LK, Wu ZC. Data integrity protection method for microorganism sampling robots based on blockchain technology. Journal of Huazhong University of Science & Technology (Natural Science Edition), 2015,43(s1):216–219 (in Chinese with English abstract). [doi: 10.13245/j.hust.15S1052]

[85] Cucurull J, Puiggalí J. Distributed immutabilization of secure logs. In: Proc. of the Int'l Workshop on Security and Trust Management. 2016. 122–137. [doi: 10.1007/978-3-319-46598-2_9]

[86] Huang XF, Xu L, Yang L. A blockchain model of cloud forensics. Journal of Beijing University of Posts and Telecommunications, 2017,(5):1–4 (in Chinese with English abstract).

[87] Siddiqi M, All ST, Sivaraman V. Secure lightweight context-driven data logging for bodyworn sensing devices. In: Proc. of the Int'l Symp. on Digital Forensic and Security. 2017. 1–6. [doi: 10.1109/ISDFS.2017.7916500]

[88] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Security and Privacy. 2016. 839–858. [doi: 10.1109/SP.2016.55]

[89] Lazarovich A. Invisible ink: Blockchain for data privacy [Ph.D. Thesis]. Boston: Massachusetts Institute of Technology, 2015.

[90] Zyskind G, Nathan O, Pentland A. Enigma: Decentralized computation platform with guaranteed privacy. Computer Science, 2015.

[91] Maymounkov P, Mazières D. Kademlia: A peer-to-peer information system based on the XOR metric. In: Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems. 2002. 53–65.

[92] Bissias G, Levine BN, Ozisik AP, Andresen G. An analysis of attacks on blockchain consensus. arXiv:1610.07985, University of Massachusetts Amherst, 2016.

[93] Dhar A, Saxena A, Misra J. Increasing anonymity in bitcoin. Lecture Notes in Computer Science, 2014,8438:122–139. [doi: 10.1007/978-3-662-44774-1_9]

[94] Monaco JV. Identifying bitcoin users by transaction behavior. In: Proc. of the SPIE DSS. 2015. [doi: 10.1117/12.2177039]

[95] Spagnuolo M, Maggi F, Zanero S. BitIodine: Extracting Intelligence from the bitcoin network. Lecture Notes in Computer Science, 2014,8437:457–468. [doi: 10.1007/978-3-662-45472-5_29]

附中文参考文献:

[4] 范捷,易乐天,舒继武.拜占庭系统技术研究综述.软件学报,2013,24(6):1346–1360. http://www.jos.org.cn/1000-9825/4395.htm [doi: 10.3724/SP.J.1001.2013.04395]

[24] 安瑞,何德彪,张韵茹,李莉.基于区块链技术的防伪系统的设计与实现.密码学报,2017,4(2):199–208. [doi: 10.13868/j.cnki.jcr.000174]

[30] 田海博,何杰杰,付利青.基于公开区块链的隐私保护公平合同签署协议.密码学报,2017,4(2):187–198. [doi: 10.13868/j.cnki.jcr.000173]

[34] 张宁,王毅,康重庆,程将南,贺大玮.能源互联网中的区块链技术:研究框架与典型应用初探.中国电机工程学报,2016,36(15): 4011–4022. [doi: 10.13334/j.0258-8013.pcsee.161311]

[36] 王于丁,杨家海,徐聪,凌晓,杨洋.云计算访问控制技术研究综述.软件学报,2015,26(5):1129–1150. http://www.jos.org.cn/1000-9825/4820.htm [doi: 10.13328/j.cnki.jos.004820]

[37] 冯登国,张敏,张妍,徐震.云计算安全研究.软件学报,2011,22(1):71–83. http://www.jos.org.cn/1000-9825/3958.htm [doi: 10.3724/SP.J.1001.2011.03958]

[38] 张玉清,周威,彭安妮.物联网安全综述.计算机研究与发展,2017,(10):2130–2143. [doi: 10.7544/issn1000-1239.2017.20170470]

[39] 冯登国,张敏,李昊.大数据安全与隐私保护.计算机学报,2014,37(1):246–258. [doi: 10.3724/SP.J.1016.2014.00246]

[40] 林璟锵,荆继武,张琼露,王展.PKI 技术的近年研究综述.密码学报,2015,2(6):487–496. [doi: 10.13868/j.cnki.jcr.000095]

[48] 朱建明,付永贵.基于区块链的供应链动态多中心协同认证模型.网络与信息安全学报,2016,2(1):27–33. [doi: 10.11959/j.issn.2096-109x.2016.00019]

[66] 李晓峰,冯登国,陈朝武,房子河.基于属性的访问控制模型.通信学报,2008,29(4):90–98.

[67] 王小明,付红,张立臣.基于属性的访问控制研究进展.电子学报,2010,38(7):1660–1667.

[78] 薛腾飞,傅群超,王枞,王新宴.基于区块链的医疗数据共享模型研究.自动化学报,2017,43(9). [doi:10.16383/j.aas.2017.c160661]

[84] 赵赫,李晓风,占礼葵,吴仲城.基于区块链技术的采样机器人数据保护方法.华中科技大学学报(自然科学版),2015,43(s1):216–219. [doi: 10.13245/j.hust.15S1052]

[86] 黄晓芳,徐蕾,杨茜.一种区块链的云计算电子取证模型.北京邮电大学学报,2017,(5):1–4.

刘敖迪(1992－),男,吉林舒兰人,博士生,主要研究领域为区块链安全,云计算安全,网络信息安全.

王娜(1980－),女,博士,副教授,主要研究领域为云计算安全,网络与信息安全.

杜学绘(1968－),女,博士,教授,博士生导师,主要研究领域为大数据安全,云计算安全,信息系统多级安全.

李少卓(1995－),男,硕士生,主要研究领域为网络与信息安全.