区块链在数据安全领域的研究进展

刘明达[1)] 陈左宁[2)] 拾以娟[1)] 汤凌韬[1)] 曹 丹[1)]

[1)](江南计算技术研究所 江苏 无锡 214083)

[2)](中国工程院 北京 100088)

摘 要 大数据时代,数据已成为驱动社会发展的重要的资产.但是数据在其全生命周期均面临不同种类、不同层次的安全威胁,极大降低了用户进行数据共享的意愿.区块链具有去中心化、去信任化和防篡改的安全特性,为降低信息系统单点化的风险提供了重要的解决思路,能够应用于数据安全领域.该文从数据安全的核心特性入手,介绍区块链在增强数据机密性、数据完整性和数据可用性三个方向的最新研究成果,对各研究方向存在的缺陷进行分析,进而对未来发展方向进行了展望.该文认为,区块链技术的合理应用能够增强分布式环境下的数据安全,有着广阔的前景.

关键词 区块链;数据安全;数据共享;机密性;完整性;可用性

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2021.00001

Research Progress of Blockchain in Data Security

LIU Ming-Da[1)] CHEN Zuo-Ning[2)] SHI Yi-Juan[1)] TANG Ling-Tao[1)] CAO Dan[1)]

[1)](*Jiangnan Institute of Computing Technology*, *Wuxi*, *Jiangsu* 214083)

[2)](*Chinese Academy of Engineering*, *Beijing* 100088)

Abstract In the era of big data, data has become an important asset driving social development. However, data faces different types and different levels of security threats throughout its life cycle, which greatly reduces users' willingness to share data. Blockchain has several security features such as decentralization, immutable, and tamper resistance. It provides an important solution for reducing the risk of a single point of information systems and can be applied to the field of data security. This article starts with the core characteristics of data security, and introduces the latest research results of blockchain in three directions: confidentiality, integrity, and availability. At first, this paper analyzes the shortcomings of each research direction. In terms of data confidentiality, the blockchain can effectively supplement data confidentiality protection in 5 areas. (1) Blockchain can be applied to enhance the security of data encryption, establish a decentralized trusted third party for cryptographic protocols, and provide a reliable incentive mechanism. For example, it can be applied to searchable encryption, proxy re-encryption, and secure multiparty computing. (2) Blockchain is applied to identity authentication, which can realize decentralized PKI technology and identity management, solve the single point problem in identity authentication, the problem of certificate transparency, and the problem of malfeasance by certification centers. And it can establish a safe and trusted digital identity authentication system. (3) Blockchain can apply access control. On the one hand, it can solve the problem of single point of access control, providing a more robust access control system for common scenarios

收稿日期:2019-09-04;在线发布日期:2020-02-06.本课题得到国家科技重点专项"核高基"(2017ZX01028101)、国家自然科学基金(91430214,6732018)资助.**刘明达**,博士研究生,主要研究方向为信息安全、区块链.E-mail:happyliumd@163.com.**陈左宁**,博士,教授,中国工程院院士,中国计算机学会(CCF)会士,主要研究领域为软件理论、操作系统、信息安全.**拾以娟**,博士,副研究员,主要研究方向为信息安全、区块链.**汤凌韬**,博士研究生,主要研究方向为网络安全.**曹 丹**,博士,工程师,主要研究方向为网络安全、密码学.

and IoT scenarios, and achieving the management of access policies and transactions of access rights. On the other hand, it can improve the credibility of attribute-based encryption authorization institutions, which improves the security of ABE. (4) The combination of blockchain and trusted execution technology can establish trusted remote state management which enhances the availability of TEE. (5) The application of blockchain to the construction of covert channels can solve problems such as communication tampering, single channels and poor privacy. In terms of data integrity, blockchain has three applications. (1) Blockchain can achieve data confirmation and traceability, establishing a credible flow trajectory for data. (2) Blockchain can be used to build a more credible log audit system and improve the security of information systems. (3) Blockchain can be combined with various industry applications to achieve more reliable data integrity protection. In terms of data availability, blockchain has two kinds of applications. (1) The blockchain itself is a solution to consistency in the byzantine environment, which can achieve byzantine consensus in a large-scale network environment. (2) A more secure and reliable distributed database system based on the blockchain. On the one hand, the blockchain itself can be used to implement a byzantine fault-tolerant distributed storage system. On the other hand, blockchain can supplement the shortcomings of existing distributed storage. Finally, this article analyzes the research of blockchain in the field of data security, summarizes the current research challenges. At last, focusing on blockchain efficiency, data security, privacy protection, infrastructure security, blockchain isomorphization, and practicality, this paper looks forward to future research. We believes that the correct application of blockchain technology can enhance data security in a distributed environment with broad prospects.

Keywords blockchain; data security; data sharing; confidentiality; integrity; availability

1 引 言

我们身处数字化时代,这意味着数据正在与我们的世界紧密融合,数据正在改变人类的认知水平和生活方式,人类文明进入大数据的新时代.数据已成为一种与矿产石油同样的经济资产[1],并且其总量正在飞速增长.数据主权也将成为大国博弈的重要争夺对象.

但是,信息孤岛问题也是客观存在的,各行各业普遍面临"人人有数据,人人缺数据"的局面.数据共享是数据增值的必要手段.数据在改变人类生活方式的同时,其安全问题同样给人带来了严重的困扰.仅 2018 年就发生了多起严重的数据泄露事件①.其中,Aadhaar 印度国家身份认证系统泄露了 11 亿印度公民的敏感信息,喜达屋酒店泄露了 5 亿消费者信息,Facebook 泄露了 8700 万用户信息.我国境内同样有大规模的数据泄露事件②,如华住旗下酒店泄露 2.4 亿条记录,AcFun 泄露 900 万用户密码数据,前程无忧泄露 195 万条个人求职简历.上述事件泄露的属于个人隐私数据,而涉及国家政府的数据泄露则会带来更大的危害.如 2017 年 12 月,美国陆军及 NSA 情报平台约 100G 文件暴露在 AWS S3 存储服务器上,包括高度敏感、机密性的国家安全数据③.因此,数据安全问题必须受到足够的重视.

数据安全的研究主要集中在三个方面,机密性、完整性和可用性.主要研究内容和研究进展在本文第 2 节简单介绍.但是当前的数据安全解决方案在安全假设、协议设计和方案实施等层面存在不同程度的中心化局限.如密码协议的可信第三方假设、访问控制的中心化判决机构、数据的集中式存储等.中心化一方面会造成单点故障,导致安全服务不可用;另一方面安全中心如果被控制,将会从根本上破坏信息系统的安全性.

区块链脱胎于比特币技术④,本质上是一个拜占庭环境下的副本状态机协议[2-3].区块链突破了传统中心式系统架构的缺陷,具有去中心化、去信任、

① https://www.freebuf.com/news/193172.html
② https://bbs.360.cn/thread-15659132-1-1.html
③ https://www.aqniu.com/industry/30413.html
④ https://bitcoin.org/en/

匿名、防篡改的安全特性，能够在大规模网络环境下实现分布式的高效共识，建立安全可信的数据存储系统，并通过智能合约机制实现大规模可信的分布式计算能力. 区块链与数据安全的结合能够降低中心化风险，具有广阔的学术和应用价值. 区块链和数据安全的结合分为两个层面：(1) 区块链本身的数据安全问题[4]；(2) 区块链技术应用于数据安全领域. 本文仅针对第二个问题展开研究和评述.

刘敖迪等人[5]分析了区块链在信息安全领域的研究进展，包括认证技术、访问控制技术和数据保护技术. 但是区块链技术的研究与发展日新月异，区块链在数据安全领域的应用早已超越这三个方面，并且这三个方向也产生了很多新的研究成果. 从数据安全的基本要求出发，区块链在数据安全领域的研究同样可以总结为机密性、完整性和可用性三个核心方向. 区块链与数据安全技术的结合能够实现更强的数据安全保护. 此外，在数据安全共享方面，区块链凭借其去中心化、去信任化和不可篡改的安全特性，能够实现更加安全有效的数据共享平台，保护分布式环境下的数据共享安全.

本文将研究区块链在数据安全领域的研究进展，梳理区块链和现有数据安全保护技术结合产生的新理论、新技术和新方法. 本文第 2 节介绍数据安全的研究现状和区块链技术；第 3 节介绍区块链在增强数据机密性方向的研究成果；第 4 节介绍区块链在增强数据完整性方向的研究成果；第 5 节介绍区块链在增强数据可用性方向的研究成果；第 6 节进行总结与研究展望.

2　研究背景

(1) 数据安全研究现状

数据安全是云计算大数据应用背景下的关键问题，也是难点所在. 数据安全和数据全生命周期紧密关联，在采集生产、存储流转以及使用过程均面临一系列的安全问题. 数据安全通常认为是数据生命周期中的机密性、完整性和可用性①. 针对数据安全问题，相关研究者已经展开了大量的研究工作.

数据机密性缺失会直接导致数据泄露，而在分布式环境下，数据共享会带来更深层次的隐私挖掘. 数据机密性保护的研究主要围绕五个方面展开：数据加密技术、访问控制、身份认证、可信计算和隐蔽通信. 其中，数据加密技术的研究主要集中在可搜索加密、属性密码、安全多方计算、代理重加密、同态密码等.

数据完整性的需求存在于数据采集传输、数据存储和数据使用的多个阶段，其目的在于识别损坏数据的行为. 在数据采集和传输阶段通常采用数据封装和签名技术保证数据完整性；在数据传输阶段采用丢包恢复技术；在数据使用时采用可验证计算的手段，保证数据输入和输出的完整性. 此外，可信计算技术也可以为数据完整性提供不同程度保护.

数据可用性是一个系统性的问题，确保数据可用性是一项困难的工作. 尤其是在大数据环境下，数据作为重要的信息资产，其可用性对于数据挖掘、机器学习等计算模型的结果都有着重要的影响. 李建中等人[6]将数据可用性定义为一致性、精确性、完整性、时效性和实体同一性. 分布式的数据存储也是解决数据可用性的重要手段. 在实际环境中，数据可用性主要面临的威胁来自于 DDoS(Distributed Denial of Service attack)攻击，它能使应用系统无法提供正常的数据服务.

大数据时代，数据只有共享才能够产生更大的价值，安全问题又成为了数据共享的壁垒. 我们认为，不能因为数据安全存在风险就“因噎废食”而不进行数据共享. 共享场景下的数据安全解决方案和具体的应用场景紧密关联，通常是上述数据安全方案的融合.

(2) 区块链简介

区块链应用于数据安全领域时，可以将区块链抽象为一个理论模型 $F_{\text{blockchain}}$. $F_{\text{blockchain}}$ 是一个基于区块链技术实现的去中心或弱中心的可信数据库系统，能够实现不可篡改、不可删除的数据存储，并且能够通过智能合约实现复杂的应用逻辑，实现大规模可信的分布式计算能力. Goyal 等人[7]指出，区块链可以作为密码学中可信假设的替代方案，比如公共字符串或者公共随机数，以取代中心化的可信机构.

区块链产生的过程可以简单概括为：发起交易、传播交易、验证交易和添加区块. 用户首先发起一笔交易，交易根据业务实际逻辑可以是转账、数据记录或者其他信息；然后区块链节点将交易广播到 P2P 网络中；各共识节点验证交易的合法性并检查用户状态，得到验证结论；最后新的区块会添加到区块链

① http://www.raincent.com/content-10-11877-1.html

上,不可篡改或删除.无论是以 Bitcoin、Hyperledger Fabric[①]为代表的传统链式结构,还是以 IOTA[②] 为代表的基于有向无环图的链,都可以套用这个模型.在实际的区块链实践中,这些过程又是可以拆分和优化的,如 Hyperledger Fabric 通过将排序和验证分离,提高了系统的灵活性,能够满足多种应用场景的需求.

针对区块链技术本身的原理,相关研究者已经进行了大量的工作,取得了丰硕的研究成果,主要包括区块链共识机制、匿名性和可扩展性等.共识机制是区块链技术的核心,决定了安全性、可扩展性和去中心化程度,是区块链技术研究的核心,已取得了丰富的研究成果.宋焘谊[8]、刘懿中[9]、郑敏[10]等人均已进行了深入研究分析,本文不再展开.匿名性是研究如何解决区块链隐私泄露问题,对区块链交易涉及的隐私进行保护,祝烈煌[4]、付烁[11]等人已经进行了深入的研究探索.可扩展性是区块链实用化的关键技术,其主要的瓶颈有:交易吞吐量不足、共识延迟高、链间难以互通等.研究者为了解决扩展性问题,对链下支付网络、分片技术、扩容技术和跨链技术等展开了深入的研究,潘晨[12]、李芳[13]、喻辉[14]等人已进行了详细的分析.总之,区块链技术的研究和区块链应用的研究是互相促进的,安全、可靠、高效、可扩展的区块链系统是区块链应用于数据安全领域的基础.

3 区块链增强数据机密性

区块链增强数据机密性的研究偏重于学术层面,能够对数据机密性保护方法存在的缺陷进行有效的补充.本节从数据加密、身份认证、访问控制、可信执行环境和隐蔽信道 5 个方面进行介绍,如表 1 所示.

表 1 区块链在数据机密性研究中的应用

应用方向	研究内容	解决的问题
数据加密	区块链应用于可搜索加密、代理重加密、安全多方计算	为密码协议建立可信第三方,为密码协议提供可靠的激励机制
身份认证	去中心化的 PKI 技术和身份管理	解决认证单点化,证书透明度和认证中心渎职的问题
访问控制	去中心化的访问控制模型	解决访问控制单点化问题,实现动态灵活的访问控制
	区块链增强属性加密机制	提高属性密码授权机构的可信度
可信执行	区块链增强可信执行 TEE 的安全性	实现可信的远程状态管理,提高 TEE 的可用性
隐蔽信道	区块链作为隐蔽信道的信息载体	解决隐蔽通信易被干扰篡改,信道单一,隐私性差等问题

3.1 数据加密

目前,区块链和密码技术的结合已成为重要的研究方向[15],其中大量的研究聚焦在如何将新型密码技术应用于区块链平台,以满足区块链的各种特殊安全需求.而本文关注如何使用区块链技术弥补现有密码技术的不足,研究方向主要包括可搜索加密、代理重加密、安全多方计算,如表 2 所示.区块链应用于数据加密主要有两种方式:一是用区块链实现去中心化的服务,以建立分布式的可信第三方,以对抗单点化风险.密码协议中往往有可信第三方或半可信第三方的假设,区块链实现分布式的可信第三方能够为密码协议的安全假设提供可行的解决方案.二是提供可靠的激励机制,从而降低攻击者作恶的动机,提高作恶的难度.敌手的恶意行为通常需要付出一定的代价,区块链为惩罚恶意行为提供了一种经济学上的机制.

表 2 区块链在数据加密中的应用

区块链功能	应用方向	核心思想
分布式可信第三方	可搜索加密	代替中心服务器执行搜索[18]
	代理重加密	代替中心服务器执行重加密[19]
	安全多方计算	提供可信证据公告板,见证加密协议的公平性[34]
可靠的激励机制	可搜索加密	激励各参与方正确执行,惩罚作恶行为[18]
	代理重加密	激励重加密节点正确执行,惩罚作恶行为③
	安全多方计算	保证计算参与者的计算参与度,激励各方完成计算任务,惩罚作恶行为[24-32]

(1)可搜索加密

现有的可搜索加密模型通常会假设一个诚实但好奇的远程服务器,能够按照既定的规则运行密码协议[17].为了解决这一问题,需要针对恶意服务器进行特殊的安全设计.但是,目前的方案主要集中在作弊行为的检测上,并没有提出有效的应对措施,这也限制了这些方案的实际应用.

Hu 等人指出该问题的主要原因是中心化的服务器能力过强且缺乏有效的监督机制,进而探索通过引入区块链技术解决该问题[18].该研究提出使用智能合约替换中央服务器,构建了一个分布式的隐私保护的搜索方案 scheme Ⅱ,如图 1 所示.该方案在以太坊上实现,用户需持有 Token 才能完成各项数据操作,包括搜索、增加和删除.数据所有者可以

① https://www.hyperledger.org/projects/fabric
② https://www.iotachina.com/what-is-iota
③ https://www.nucypher.com

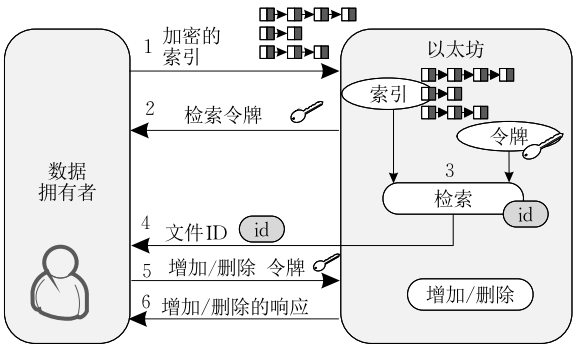

图 1　scheme II[18] 系统架构

获得正确的搜索结果，而不需要担心服务器的恶意行为. 另外，该方案从实际应用的角度出发，采用了数字货币奖励的机制，保证各参与方的经济权益.

(2) 代理重加密

区块链和代理重加密的结合目前研究相对较少，核心思想是使用区块链的分布式特性管理代理重加密的密钥，以规避可信第三方的单点风险. NuCypher KMS① 项使用区块链技术，实现分布式的重加密密钥分片存储. 并且区块链的抵押机制和激励机制能够保证重加密节点按照正确的方式运行. 另外，Agyekum 等人[19] 提出一种基于区块链和代理重加密的数据共享方案，利用区块链网络作为代理服务器并对数据执行加密操作，能够在确保数据机密性的同时防止合谋攻击.

(3) 安全多方计算

安全多方计算(Secure Multi-party Computation，SMC)能够实现互不信任的多方进行协同计算，并保证隐私不会泄露. 区块链和 SMC 的结合主要集中在理性安全多方计算[20](Rational Secure Multi-Party Computation，RSMPC)这一研究领域，RSMPC 利用博弈论的方法解决安全多方计算的问题. 在 RSMPC 中，参与者属于理性参与者，参与计算的目标是追求利益的最大化. 参与者参与多方安全计算的目的是获得计算结果，或得到经济补偿. 在理想的情况下，如果敌手违反了协议，需要有公平的机制对诚实用户给予补偿. 但是前期工作[21-23] 的主要问题在于，他们依托电子货币系统或者完全可信的中央银行系统实现公平机制，而这在早期的研究实践中是很难实现的.

区块链作为一种可信电子货币的实现方式，能够为 RSMPC 提供经济激励，解决参与者的动机问题. Andrychowicz 等人提出将比特币系统用于两方安全计算，保证一方随意终止协议，另一方能够获得补偿[24]. 随后他们进一步构造了安全多方彩票协议[25]，用区块链技术解决了无法强制补偿的缺陷，实现了诚信客户的公平性. 另外，Kiayias 等人[26] 提出使用全局交易账本(Global Transaction Ledger)实现公平且健壮的多方安全计算协议，全局账本的具体实现方法是区块链技术. Kiayias 等人的贡献有三个方面：(1) 提出了一种新型的带有补偿的安全多方计算形式化模型；(2) 对协议进行了安全性的证明；(3) 首次提出了一种常数轮健壮的多方计算协议.

Kumaresan、Bentov 等人在该方向进行了一系列的研究工作[27-32]. 文献[27]指出，在多方安全计算中，敌手可能在得到计算结果后就终止安全协议，这将损害合法用户的利益. 这个问题的解决方案包括逐步释放机制(gradual release mechanism)、乐观模型(optimistic models)和部分公平的安全计算(partially fair secure computation). 但是这三种方案存在两个核心缺陷，一是诚实方为了运行安全协议需要花费昂贵的代价，二是必须保证可信第三方不会与敌手串谋. 为了解决这一问题，他们设计了基于 Bitcoin 的公平安全计算协议，而不依赖于可信中央银行. 另外，该研究设计了用于公平抽奖的安全计算协议，而不需依赖于可信的博彩网站. 在形式化方面，该研究定义了三种密码学原语，包括索赔和退款函数 F_{CR}^{*}(Claim-or-refund functionality)、带惩罚的安全计算 F_{f}^{*}(Secure computation with penalties)和带惩罚的安全彩票 F_{lot}^{*}(Secure lottery with penalties)，只需要运行常数次 F_{CR}^{*} 即可完成计算任务. 文献[28]研究了如何使用 Bitcoin 刺激参与者完成正确的计算，包括可验证云计算，带有限制泄露的安全计算，公平安全计算和非交互式悬赏. 文献[29]研究如何基于 Bitcoin 实现去中心化的扑克游戏，其本质是具有奖惩功能的安全多方计算和无可信中心的安全智能合约. 文献[30]是在文献[27]和文献[29]的基础上进行的改进，提出两种针对带惩罚安全计算模型的优化方案，一方面通过调整优化算法中的交易数量，将算法复杂度由平方阶降为线性阶；另一方面通过对多阶段的计算过程进行改进，实现了交易数量的线性增长. 文献[31]通过惩罚来分摊安全计算的成本，对文献[27]的 F_{CR}^{*} 函数进行性能优化，降低了链上的交互开销. 文献[32]在智能合约之上实现了新的多方计算协议，和基于 Bitcoin 的方案相比，通信的复杂度由平方阶降低到常数阶.

① https://www.nucypher.com

另外，Choudhuri 等人[33]指出，公平的真正含义是各方都得到输出或者各方都得不到输出，因此从激励机制的角度出发结合区块链和多方安全计算并不能实现真正意义的公平. 他们指出，公共公告板(Public Bulletin Boards)能够产生不可伪造的证据，并证明证据已经发布. 这种特性可以用于见证加密协议的公平性，进而构造了一种安全多方计算协议. 区块链是公共公告板的一种实现方法.

综上所述，区块链技术以其分布式的特性，可以作为密码学中可信第三方的实现方案. 区块链技术的防篡改特性能够为密码协议提供可信赖的激励机制，提高敌手在博弈中的作恶难度，降低作恶动机. 因此，区块链能够为数据加密提供了更强大的安全保障.

3.2 身份认证

区块链和身份认证的结合主要包括两个方面：(1)基于区块链构建去中心化的公钥基础设施(Public Key Infrastructure，PKI)，并基于分布式 PKI 为各类应用系统提供身份认证支撑；(2)基于区块链实现去中心化的身份管理，实现类电子身份证系统. 如表 3 所示.

表 3 区块链在身份认证中的应用

应用方向	研究内容	核心思想
去中心化的 PKI 系统	基于区块链实现的 PKI 体系	基于区块链交易实现证书全生命周期管理[36-44]
	改造现有的 PKI 系统	公开的证书审计和透明的证书撤销[45-47]
去中心化的身份管理	实现类电子身份证的管理	区块进行身份管理，实现多方跨域的身份认证[49-53]

3.2.1 去中心化的 PKI 技术

数字证书是重要的身份认证技术，而目前集中式的 PKI 系统存在三大安全问题：单点失效问题，证书颁发机构(Certificate Authority，CA)易受攻击问题，以及中心渎职问题[34]. 中心化的 PKI 应用于分布式环境中时，不可信的 CA 会带来严重的安全风险[35]：CA 故障会导致所有用户的证书不可用；中心化的 CA 攻击目标明显，黑客可以使用 CA 签发虚假证书实现中间人攻击；用户无法验证证书的合法性，只能单方面信任 CA 机构，证书透明化问题严重；用户无法察觉 CA 渎职的现象. 区块链技术能够基于共识机制建立分布式的信任验证，能够规避对集中式 CA 的过度依赖，为去中心化的 PKI 系统构建提供了可行的思路.

区块链应用于 PKI 系统目前有两种研究思路. 一是基于区块链实现去中心化的 PKI 体系，使用区块链交易承载证书签发、证书验证、证书更新、证书撤销等功能，具有不可篡改的特性. 二是使用区块链技术对现有基于 CA 的 PKI 体系进行改造，实现公开的证书审计和透明的证书撤销.

(1)基于区块链实现 PKI 体系

基于区块链的 PKI 目前已成为重要的研究方向. MIT 的 Conner 等人首次提出基于区块链技术实现分布式的 PKI 系统 Certcoin[36-37]，其核心是利用区块链技术实现分布式的公共账本，将用户身份和证书公钥关联，构建去中心化的 PKI 系统. 由于任何用户都可以查看证书的签发过程，因此 Certcoin 解决了传统 PKI 体系面临的 CA 单点化问题和证书不透明的问题. 对基于区块链实现 PKI 体系的一般化方法进行总结，主要流程包括：

① 身份注册. 用户生成身份信息，并向全网发布. 其他节点收到后对信息进行验证. 如果验证节点获得记账权，则将注册信息打包到新区块的提议中，进而被全网验证通过，完成注册.

② 公钥更新. 用户发布公钥更新信息，声明新公钥和对旧公钥的所有权. 更新请求经过全网验证共识后写入区块链系统，新公钥生效.

③ 公钥查询. 用户通过遍历区块链账本获取所查询的公钥状态.

④ 公钥废除. 用户发布公钥废除信息，声明对该公钥的所有权. 废除请求经过全网验证共识后写入区块链系统.

⑤ 身份认证过程. 所有对身份证据的确认都通过查询区块链系统完成，如果身份处于合法可用状态，则身份认证顺利完成.

相关研究者围绕基于区块链 PKI 系统的基础模型，展开了一系列的优化研究工作. Ali 等人[39]在去中心化的域名系统 Namecoin[40]之上，提出了构建分布式 PKI 系统的方法 Blockstack，实现了公钥和用户可读身份的绑定，并实现了交叉链之间的迁移. Leiding 等人[38]分析了基于 CA 或 PGP 信任网络(Web of Trust，WoT)[41]的 PKI 体系存在的问题，提出了 Authcoin 协议，实现了公钥验证时更加灵活的质询和回复. 相比于基于 CA 的 PKI，该协议具有更好的透明度和容错性；相比于 PGP 信任网络，Authcoin 更容易抵御女巫攻击(Sybil Attack). Bui 等人[42]针对证书撤销问题，提出将撤销证书的哈希值存入区块链以供查询，然而证书撤销对实时性要求较高，该方法无法处理大量的证书. 同样针对当前 PKI 体系存在的中心化和证书不透明的问题，

Al-Bassam 等人[43]基于信任网络和智能合约提出了 SCPKI，更方便地进行证书合法性检测和细粒度属性验证，实现用户身份和属性之间的信任传递. Hari 等人[44]提出一种在区块链分布式 PKI 基础上，实现 BGP 路由传播和 DNS 中可信节点的认证方法.

(2) 改造现有的 PKI 系统

与上述去中心化的 PKI 系统不同，一些学者对现有的以 CA 为中心的 PKI 系统进行改造，利用区块链实现公开的证书审计和透明的证书撤销. 该研究方向从现实安全需求出发，对现有 PKI 体系中的 CA 系统进行分布式改造，用区块链系统记录 CA 发证、验证和撤销的过程，从而消除 CA 系统的作恶行为.

Matsumoto 等人[45]从提升 TLS 协议安全性的角度出发，针对未授权证书被签发用以实现中间人攻击的问题，提出了一个审理未授权证书的自动化平台 IKP，利用智能合约和共识机制，在保证原有功能的同时实现去中心化，同时采用数字货币激励用户对非法证书的举报. Chen 等人[46]针对现实生活中 CA 故障的问题，提出一种无需 CA 中心的基于区块链的公开可审计认证体系 Certchain，利用一种可靠性排名共识和数据结构 CertOper 实现证书的正确性和可追溯性；利用 DCBF (Dual Counting Bloom Filter) 实现撤销证书的高效确认，并通过设计的三层检验机制将假正率降为 0. Certchain 的证书可追溯性由区块链的链式结构保证，如图 2 所示. Wang 等人[47]针对 CA 易被入侵从而签发虚假证书的现状，利用区块链提高证书及其撤销的透明度，提出的架构与采用 X.509 标准的 PKI 体系兼容，将基于 SSL/TLS 协议的网页服务器的证书及其撤销情况记录为一笔交易，公布于区块链.

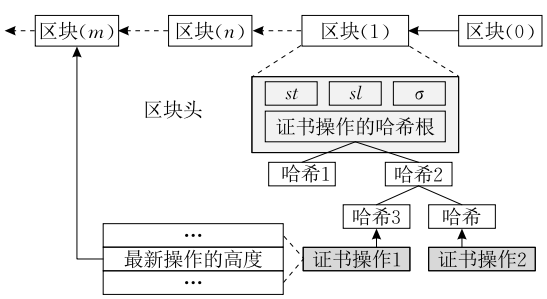

图 2　Certchain[46]证书追溯

此外，由于区块链是一个公开的账本，存在隐私泄露的风险. 相关研究者在基于区块链的 PKI 系统研究基础上，对去中心化的匿名证书系统展开了研究[42,48].

3.2.2　去中心化的身份管理

身份管理(Identity Management，IdM)是信息安全的关键技术，涉及身份创建、身份描述、身份管理等诸多方面. 由于数据泄露事件层出不穷，身份欺骗事件日益增加，集中式的 IdM 面临严重的安全挑战，用户容易丧失其数字身份的控制权和所有权. 该研究方向和去中心化 PKI 技术的区别在于，身份管理中数字身份的发布者必须是权威部门. 因此，在实现基于数字身份的信任服务时，实体包括身份发布方、用户和身份验证方，在区块链网络中具有不同的身份和任务. 其中，用户需要向发布方提供身份证明材料，如身份证、驾驶证等，并得到电子身份凭据；身份发布方需要验证用户提供的证明材料，一方面向用户颁发电子身份，另一方面要写入区块链系统，使之生效；身份验证方从用户得到身份证明，并向区块链网络查询确认.

从基础框架入手，研究者对基于区块链的去中心化身份管理系统展开了研究工作. Dunphy 等人[49]指出，区块链技术具有去中心化、防篡改、用户可控的安全特性，并从身份管理系统的特点出发，对三个典型的基于区块链的身份管理系统(uPort①、Sovrin②、ShoCard③)进行深入研究. 分析结果表明，基于区块链的身份管理是有意义的，但是这三种方案均不能完美解决身份管理问题，主要原因有两个：(1) 未能解决可用性的问题，用户无法妥善管理私钥；(2) 通用数据保护条例(General Data Protection Regulation，GDPR)对个人数据的监管十分严格，区块链的公开特性和隐私保护相悖，这为区块链应用的设计带来了挑战. Stokkink 等人[50]探索了基于区块链的数字身份部署方法，通过设计对身份的全套声明链条(claim chain)实现数字身份自主化管理. Lee 等人[51]针对移动场景提出了 ID 即服务的概念(IDaas)，为电信公司、移动用户和应用商建立互相认证机制，提供身份和管理服务，而这个过程无需共享任何安全凭证. 董贵山等人[52]提炼了基于区块链的身份管理模型，描述了基于区块链的信任服务关系. 作者认为区块链技术能够建立全网统一的信任模型、规避信用中介的单点风险以及降低系统维护的成本，下一步要研究区块链如何满足细粒度身份权限管理的需求. Takemiya 等人[53]提出了一个面

① https://www.uport.me/
② https://sovrin.org/
③ https://shocard.com/

向移动应用场景的身份系统 Sora Identity，用于存储加密数据并提供个人信息的验证服务.

综上所述，基于区块链的身份认证技术能够有效解决认证中心单点化以及认证透明度的问题，为分布式环境下信任关系的构建提供一条行之有效的思路.

3.3 访问控制

区块链与访问控制的结合有两个研究方向，一是实现去中心化的访问控制模型，解决信息系统尤其是物联网场景下中心化访问控制的安全和效率问题；二是对基于密码学的访问控制属性密码进行安全性的增强，实现去中心化的授权中心. 如表 4 所示.

表 4 区块链在访问控制中的应用

应用方向	研究内容	核心思想
去中心化的访问控制	面向通用场景的访问控制模型	区块链与访问控制模型结合，充当可信实体，实现权限策略不可篡改[54-56]和跨域访问控制[57]
		区块链充当访问控制实体，用交易或合约进行访问控制[58-63]
	面向物联网场景的访问控制	将访问控制权限作为资产，由区块链提供可信的存储，并且进行分布式权限交易管理[62-68]
区块链增强属性密码	密钥审计	记录所有操作增强密钥审计[73]
	提高授权机构的可信度	建立分布式属性判决和密钥管理中心，解决分布式环境下的多授权机构的互信和串谋问题[74-76]

3.3.1 去中心化的访问控制

针对传统访问控制存在的不足，刘敖迪等人[5]对区块链技术应用于访问控制领域的研究总结为两个方向：(1) 基于交易进行策略/权限管理；(2) 基于智能合约进行访问控制. 并将区块链应用于访问控制的优点总结为五个方面：(1) 策略发布在区块链上，对所有主体透明可见，不存在第三方越权行为；(2) 访问权限能够基于区块链进行交易从而实现受控资源的转移，且资源拥有者无需介入，权限管理机制更加灵活；(3) 权限定义和权限交易过程在区块链上公开，便于审计；(4) 能够实现资源的管理权和使用权真正被用户掌握；(5) 基于智能合约实现自动化的访问控制保护.

本文从应用场景的角度对区块链访问控制模型进行分类，一种是面向通用场景的访问控制模型，另一种是面向物联网场景的访问控制模型. 需要说明的是，面向通用场景的访问控制具有普适性，主要面向传统的网络系统，参与访问控制的节点数量较少，参与节点的计算能力较强，也可称之为非物联网的场景. 物联网场景下的访问控制具有特殊的特点和需求(详见 3.3.1 节第二部分)，因此需要单独进行介绍.

(1) 面向通用场景的访问控制模型

从通用场景的访问控制基本模型的角度，相关研究者针对现有访问控制模型的缺点，提出了扩展改进的方案.

史锦山等人[64]分析总结了区块链应用于访问控制的两种解决方法. 一是区块链与访问控制模型结合，模型中存在中心授权服务器，但是由区块链充当模型中的可信实体，实现权限策略不可篡改. 区块链的作用是记录权限拥有者以及提供权限转移功能. 授权服务器发布授权访问权限的交易，区块链记录该访问权限并通知资源的拥有者. 资源申请者访问资源时，首先需要告诉区块链自己的访问行为. 二是区块链充当访问控制实体，模型中取消中心化授权机构的设计，用交易或合约进行访问控制，访问控制权限能够通过智能合约灵活转移. 其思想是，资源拥有者将访问控制策略发布到区块链中，由区块链决策是否授予其对资源的访问权限. 区块链不仅存储访问策略和提供权限转移，并且提供自动执行访问控制策略进行授权的功能.

Maesa 等人[54]对基于属性的访问控制模型(Attribute Based Access Control，ABAC)进行了扩展，用区块链交易实现访问控制的策略管理. 核心机制是将集中式的策略管理点(Policy management Point，PAP)用区块链进行分布式改造，实现对策略的全生命周期的管理，并提供不可篡改的日志功能. 刘敖迪等人[55]同样以 ABAC 为基础模型，用智能合约管理资源访问策略，通过基于事务的访问控制策略管理，实现动态环境下的数据资源访问控制. 王秀利等人[56]用属性基加密机制作为访问控制模型，提出一种企业级的数据共享与访问控制的框架，实现了企业内部细粒度的访问控制和数据共享. Cruz 等人[57]针对基于角色的访问控制模型(Role-Based Access Control，RABC)难以跨域跨组织部署的问题，提出一种使用智能合约的角色访问控制模型 RBAC-SC，通过智能合约发布用户角色，分配角色信息，并采用质询-响应认证协议来验证用户对角色的所有权.

Zyskind 等人[58]针对移动应用场景，实现了移动应用程序的细粒度权限管理框架，将交易 T_{access} 用于访问控制策略管理，将交易 T_{data} 用于存储和数据索引，用户和服务方可以作为联合身份对权限进行

管理，如图 3 所示. 刘明达等人[59]针对可信网络连接(Trusted Network Connect，TNC)结构面临的访问控制单点化和策略决策中心化的问题，从理论上提出一种基于区块链的分布可信网络连接架构，研究如何在分布式网络环境中构建分散式信任根，并提出了一种分布式的远程证明协议[60]. 对 MedRec 框架[61]、Sifah[62]、Alansari[63]也进行了相关的研究.

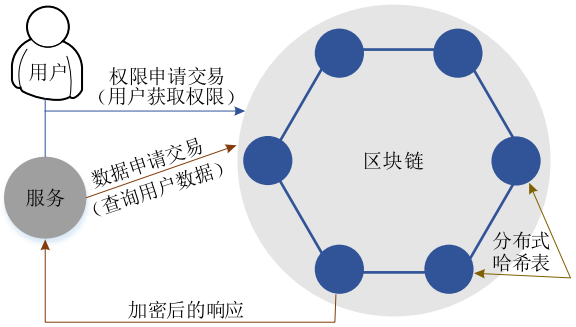

图 3　Zyskind[58]框架结构

(2) 面向物联网场景的分布式访问控制

物联网场景是基于区块链的访问控制未来重要的研究和应用方向，相关研究者深入研究了物联网的分布式访问控制，得到了一系列的研究成果. 区块链应用于物联网访问控制的核心思想是，将访问控制权限作为资产，由区块链提供可信的存储，并且进行分布式权限交易管理. 需要说明的是，本文重点是介绍区块链应用于物联网访问控制的基本思想和典型研究，没有针对研究细节更多展开. 史锦山等人[64]针对物联网区块链的访问控制进行了更加详细的综述，指出区块链能够满足物联网中设备轻量、节点海量和动态性带来的特殊需求，并分析了区块链针对这三个特性的解决方案.

区块链访问控制应用与物联网环境时，同样采用了“(1) 面向通用场景的访问控制模型”中描述的两种方法，但是又和物联网环境的特点紧密关联. Ouaddah 等人[65]指出，物联网访问控制面临集中式和分布式方案的博弈. 集中式方案的缺点包括：单点故障问题，用户无法参与对自己数据的访问控制，物联网设备管理代价昂贵，难以构建外部信任实体和设备用户之间的强信任关系. 而分布式方案的缺点包括：需要构建复杂的分布式安全机制，受约束的设备缺乏密集计算能力无法实施访问控制逻辑，难以实现远程动态的访问策略管理与更新. 在此研究基础上，他们提出了 FairAccess[66-67]机制，通过引入授权、获取、委托和撤销访问这 4 种交易类型，将访问控制策略存储到区块链中，并向被授权的访问者账户发放授权令牌，拥有令牌就代表能够访问对应资源. 区块链的令牌机制能够有效降低物联网设备处理访问控制信息的开销，实现了用户驱动的透明化细粒度访问控制. 但是 FairAccess 仍旧存在一些缺陷，如新访问建立、令牌到期或撤销必须由主体参与，令牌需要两个区块落账才能够生效导致高昂的时间成本，仅支持基于令牌的授权，而令牌需要集中式的发行者.

CapChain[68]提出将区块链作为可信的访问控制列表，将访问权限看作一种数字资产，通过区块链事务在用户之间进行传递. 每一个 IoT 设备都有一个或多个所有者，他们可以根据访问控制策略设置访问控制规则，并在区块链上委派给其他用户. 设备需要验证区块链上是否有授权凭证，进而决定是否向用户开放其权限.

ControlChain[69]克服了 FairAccess 的缺陷，设计了一种由四个不同功能区块链组成的访问控制架构. 其中 Context Blockchain 存储数据的上下文信息，用于授权决策；Relationships Blockchain 用于存储身份标识和实体之间的关系；Rules Blockchain 用于记录访问控制的授权规则，定义采用的访问控制模型，如 RBAC、ABAC；Accountability Blockchain 上记录允许或禁止访问的信息，用于问责和审计. 按照功能划分为 4 链结构的好处在于，可以根据实际物联网场景和访问控制模型的需求，灵活进行系统构建. ControlChain 如图 4 所示，所有访问控制行为在各链上进行记录.

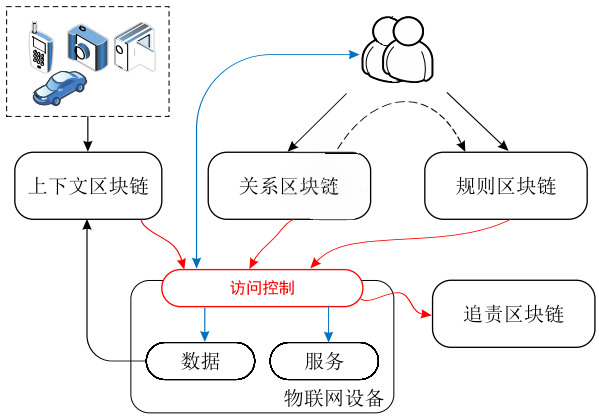

图 4　ControlChain[69]架构

IoT Passport[70]旨在实现分布式的跨平台协作，利用智能合约强制性的规则，为每个 IoT 设备颁发物联网护照. IoT Passport 进行了更加细致的设计，提出了基于区块链的信任框架(Blockchain-Based Trust Framework，BBTF). BBTF 分为感知

层、网络层和应用层，这与物联网的典型架构一致，使得区块链能够为物联网各层次信任关系的构建发挥作用. BBTF 在访问控制方面实现了跨平台的设计，使用了 ABAC 作为基本的访问控制模型，访问控制策略由智能合约编写并部署在区块链中. 在执行的时候，首先主体请求对对象的访问权限，然后对象执行智能合约对主体的身份进行验证. 此外，Outchakoucht[71]、Ourad[72] 等人也进行了相似的研究.

综上所述，区块链与访问控制的结合能够有效解决访问控制单点化问题，实现更加动态灵活细粒度的访问控制策略，且支持可信透明的审计.

3.3.2 区块链增强属性加密

属性基密码机制(Attribute-Based Encryption，ABE)以属性为公钥，将密文和用户私钥的属性关联，能够灵活地表示访问控制策略，实现低开销的细粒度访问控制. 在目前的 ABE 方案中，授权机构能够解密存储在云服务器中的所有数据，导致密钥滥用和隐私数据泄露的问题. 另外，责任认定问题也是 ABE 的难点. 基本的 ABE 模型属于单机构情形，不能满足分布式环境的需求，并且授权机构要求绝对可信，这在分布式环境下也难以保证，所以多机构 ABE 模型也是属性密码研究的重点问题. 研究者对如何将区块链和属性密码结合进行了一些探索性的工作. 通过记录信息系统的所有操作记录，实现立分布式属性判决和密钥管理中心，解决分布式环境下的多授权机构的互信和串谋问题.

Yuan 等人[73]提出将区块链和可追责 CP-ABE (Ciphertext Policy Attribute Based Encryption)算法结合，实现了一种电子文件保护系统，数据的每一项操作记录都写入区块链系统，提高对密钥滥用行为的审计能力. Jemel 等人[74]在 Bitcoin 的基础上实现了分布式的属性验证. 当用户存储数据到云端时，首先使用密钥 K 对数据进行加密，然后将加密密钥 K 用 CP-ABE 进行加密保护，并将加密后的密钥密文存储于区块链网络中，其中加密属性由用户设置. 申请数据时，申请者的属性由区块链进行判决，如果通过，就可以获得数据加密密钥. Wang 等人[75]采用了相同的思路保护数据加密密钥. 不同的是，他们使用智能合约进行属性的合法性判决，而智能合约可以承载更加复杂的逻辑. Zhang 等人[76]提出了 BaDS 框架，实现了基于区块链的属性验证机制，如图 5 所示.

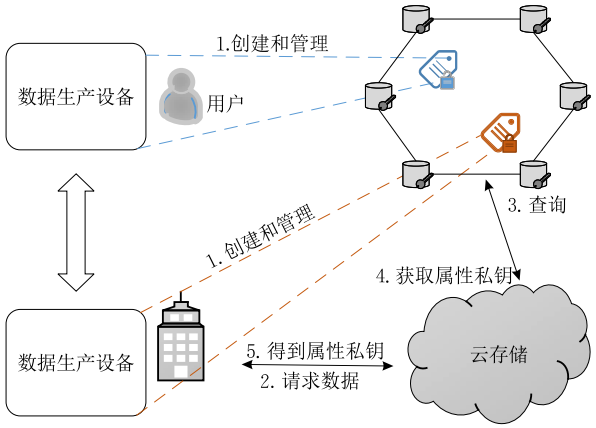

图 5 BaDS[76]框架

数据交易请求

(1) Owner A 使用 KEY 对数据 DATA 进行加密，并对 KEY 使用 KEY_ABE 进行加密. $E(Data)_{KEY}$ 存入云存储，$E(KEY)_{KEY\_ABE}$ 调用智能合约存入区块链.

(2) User B 首先调用智能合约的 getPACT 接口判断属性是否符合访问控制策略. 如果有，执行(3)；如果没有，需要向 Owner A 申请权限，进入权限更新请求阶段.

(3) User B 构造属性证据，打包成区块链交易，用属性私钥进行签名，广播到区块链网络.

(4) 各区块链节点调用 ABS. Veri 算法对签名属性进行验证，验证结果基于 PBFT 算法达成一致.

(5) 智能合约将 $E(KEY)_{KEY\_ABE}$ 发送到 User B，进而解密得到 KEY.

进入权限更新请求

(1) Owner A 调用合约里的 UpdatePACT 算法，根据需求对访问控制策略进行增加、删除或修改.

综上所述，使用区块链技术增强属性加密的基本思路相似，能够一定程度上解决控制中心单点化问题、多授权机构互信问题以及对抗多用户之间的串谋攻击.

3.4 可信执行环境

区块链和可信执行环境(Trusted Execution Environment，TEE)结合有两个研究方向. 一是用 TEE 解决区块链系统面临的问题：(1) 面向拜占庭容错场景，基于 TEE 技术实现更加安全高效健壮的共识算法[77-82]；(2) 基于 TEE 构建智能合约的安全执行环境[83-86]. 而我们关注第二类研究方向，用区块链技术弥补 TEE 无法解决的安全问题，主要研究包括 Cheng 等人[87]提出的 Ekiden 模型和 Kaptchuk

等人[88]提出的 ELI 协议.

TEE 技术是解决安全计算的重要手段，能够为数据安全保护提供强大的安全模型. 但是恶意主机能够对 TEE 产生很多影响：(1) 阻断或篡改网络通信，限制 TEE 和外部世界的通信联系；(2) 篡改非易失性数据，将旧的计算状态重新载入 TEE 的 Enclave 环境，实施重放攻击. 即便 TEE 设计生产过程完全可靠，也会受到这两个问题的影响.

针对 TEE 的可用性问题，目前有两种解决方案：(1) 在 TEE 的设计中，增加防篡改的非易失性存储器设计[89]，但这类方案不仅会增加成本，而且不适用于分布式的计算环境；(2) 将 Enclave 的状态管理任务委托给远程的可信第三方[90]，但是这种方法只是将信任根转移到了不同的物理位置，而远程服务器面临着同样的问题.

Ekiden 和 ELI 都针对这一问题提出了解决方案，基本原理相似，本文以 Ekiden 为例进行介绍. 在 Ekiden 中有三种实体，客户端是智能合约的用户；计算节点提供 TEE 服务，包括合约 TEE 和密钥管理 TEE，并且所有支持 TEE 的平台都可以加入成为计算节点；共识节点维护不可篡改的区块链账本. Ekiden 的流程是合约创建和合约执行.

合约创建

(1) 客户端发送合约代码到计算节点，计算节点将合约加载到 TEE 中，并实例化代码.

(2) TEE 分配合约 id，称之为 cid，从 Key manager(在 TEE 中进行维护)得到新的公私密钥对 $(pk_{\text{cid}}^{\text{in}}, sk_{\text{cid}}^{\text{in}})$ 和 $key_{\text{cid}}^{\text{state}}$，并得到加密后的初始状态 $\text{Enc}(key_{\text{cid}}^{\text{state}}, \mathbf{0})$，$pk_{\text{cid}}^{\text{in}}$ 就是智能合约的公钥. 需要说明的是，所有 TEE 中的计算都会产生一个证据 σ_{TEE} 证明计算是在 TEE 中完成的，而证据的验证由 SGX 的远程证明服务[91]提供，后文不再赘述.

(3) 计算节点将(合约代码，$pk_{\text{cid}}^{\text{in}}$，$\text{Enc}(key_{\text{cid}}^{\text{state}}, \mathbf{0})$，$\sigma_{\text{TEE}} \parallel$ 其他证据)发送到共识节点，验证后将初始状态和公钥记录到区块链上. 合约代码根据机密性要求，也可以由 $key_{\text{cid}}^{\text{state}}$ 加密后上链.

合约执行

合约执行过程如图 6 所示，描述如下：

(1) 客户端调用智能合约，输入 inp. 客户端首先在链上得到 $pk_{\text{cid}}^{\text{in}}$，并计算 $inp_{\text{ct}} = \text{Enc}(pk_{\text{cid}}^{\text{in}}, \text{inp})$，并将 $(\text{cid}, inp_{\text{ct}})$ 发送到计算节点.

(2) 计算节点根据 cid，从区块链上得到智能合约代码和前序运行状态 $st_{\text{ct}} := \text{Enc}(key_{\text{cid}}^{\text{state}}, st_{\text{prev}})$，然后将 inp_{ct} 和 st_{ct} 载入 Contract TEE 进行计算.

(3) Contract TEE 从 Key Manager 得到 $sk_{\text{cid}}^{\text{in}}$ 和 $key_{\text{cid}}^{\text{state}}$，就能够对(2)中的两个密文解密，得到本次的输入和前序的计算状态. 然后执行计算 $(\text{outp}, st_{\text{new}}) = \text{Contract}(\text{inp}, st_{\text{prev}})$.

(4) 计算 $st'_{\text{ct}} = \text{Enc}(key_{\text{cid}}^{\text{state}}, st_{\text{new}})$，并伴有 TEE 的计算证据.

(5) 计算节点和客户端之间运行原子协议，把 outp 传递到客户端，把 st'_{ct} 和证据传递到共识节点. 原子协议保证，只有在 st'_{ct} 和证据被共识节点验证接受的情况下，outp 才会发送给客户端.

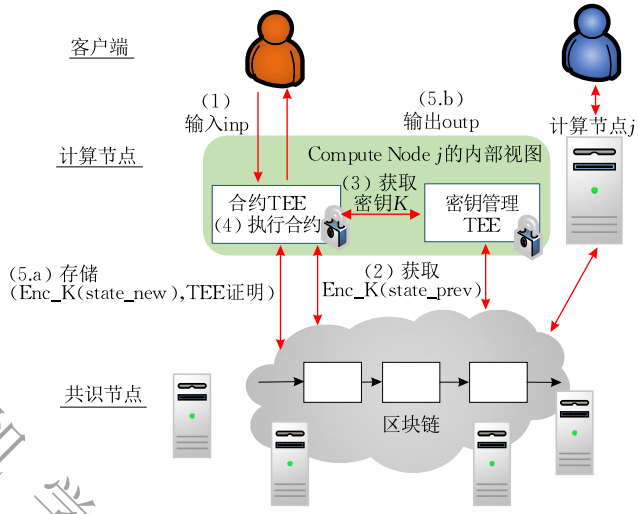

图 6　Ekiden[88]合约执行流程

对上述过程进行分析可以看出，TEE 的运行状态会加密存储到区块链网络中，即便 TEE 的可用性遭到破坏，其计算状态已经被安全保存在区块链网络之上. 即便只有一个计算节点能够运行 TEE，仍然可以把运行状态从区块链下载到 TEE 中，系统可以对外正常提供合约服务. 因此，引入区块链技术为 TEE 提供安全可信的状态存储服务，能够有效的增强 TEE 的可用性，进而能够为计算系统提供更加可靠的数据机密性服务.

3.5　隐蔽信道

隐蔽信道是一种违反通信限制规则，无法被监测的隐蔽通信手段，常应用于军事等特殊领域. 隐蔽通信需要可靠的信息载体，如网络数据包、网络协议字段和时间特征等. 传统的隐蔽传输通常采用单一信道的定向发送的模式，不仅容易被检测，并且传输受到网络环境的影响，可靠性很差. 另外，身份隐私性也是隐蔽信道需要解决的难题. 相关研究者提出用区块链技术实现隐蔽信道，并展开了部分探索性工作.

Partala[95]指出，区块链具有匿名、防篡改和防删除的安全特性，可以作为隐蔽通信的信息媒介，进而提出了一种将信息隐藏到区块链交易中的方法BLOCCE，如图7所示，基本过程描述如下：

(1) Alice生成多个公私密钥对，并根据公钥得到对应的付款地址；

(2) Alice生成到这些地址的转账交易，并根据需要隐藏的文本消息 m，对它们进行排序，使支付地址的最低有效位(LSB)形成 m；

(3) Alice以排好的顺序将付款提交给区块；

(4) Bob从区块链上读取Alice发出的交易，并从支付地址的LSB恢复出隐藏的文本消息 m.

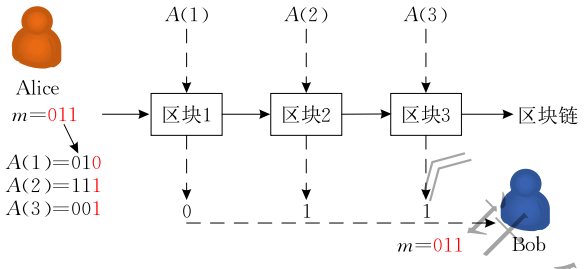

图7 BLOCCE[96]执行流程

可以看出BLOCCE的探索比较简单，该方案在匿名性等方面还存在缺陷，并且一个交易只能够传递1位数据，信道容量低，通信花销大.

李彦峰等人[96]进行了丰富的研究工作. 他们提出了区块链环境下网络隐蔽信道的形式化模型. 该模型由信息发送方，信息接收方，原始信息和信息传输部分组成，核心的流程是信息编码和调制，对等网络传输，链式存储，信息解调和解码. 他们经过证明指出，基于区块链的隐蔽信道具有很强的抗干扰性、抗篡改性、多线路通信性、接收方匿名性和线路无关性. 可以采用具有不同安全特性(如匿名性)的区块链系统满足上述特性. 在此基础之上，他们提出了对区块链隐蔽信道的评估方法，即抗检测性评估，顽健性评估和传输效率评估. 另外，他们提出了一种基于交易时间间隔的区块链隐蔽信道的实现方式.

祝烈煌①教授指出，区块链应用于隐蔽信道仍存在诸多技术上的挑战：(1)数据多副本，需要研究如何在公开和透明场景下隐藏传输行为；(2)交易可溯源，需要增强区块链账号的匿名机制；(3)交易难筛选，需要研究如何提高特殊交易识别的效率；(4)需要研究群组隐蔽传输时内部泄露的对抗机制. 问题(1)和(2)的科学问题是无中心开放网络数据隐蔽传输理论模型，问题(3)的科学问题是非定向数据隐蔽传输的高效定向筛选方法，问题(4)的科学问题是容忍内部泄密的群组隐蔽传输安全机制.

综上所述，先期的探索已经说明区块链适用于构建隐蔽信道，但是这个研究领域尚处于初期阶段. 仍需要研究者进行大量的研究工作，实现实用化的隐蔽通信.

4 区块链增强数据完整性

区块链本身是一种不可篡改的账本，而数据完整性保护的核心是数据不被篡改，因此使用区块链增强数据完整性是一个有意义的研究和应用方向. 本文从数据完整性保护和云环境下数据可信两个方向进行介绍.

4.1 数据完整性保护

区块链与数据完整性保护的结合主要有三个方面：数据确权与溯源，实现数据流转过程的可追溯记录；可信日志审计，为信息系统实现更加可信的日志审计系统；区块链与各行业应用的结合，为行业应用提供数据完整性保护功能. 如表5所示.

表5 区块链在数据完整性保护中的应用

应用方向	研究内容	核心思想
数据确权与溯源	实现数据流转和溯源的管理	将数据流转记录和数据完整性证据写入区块链系统，保证数据在流转过程中不被篡改[98-106]
可信日志审计	建立基于区块链的日志审计系统	将日志和日志完整性证据写入区块链系统，实现日志数据无法被删除篡改，且能够恢复[107-113]
区块链＋	区块链应用于各行业	将数据确权和追溯需要的数据写入区块链系统[114-121]

4.1.1 数据确权与溯源

数据确权与溯源是分布式环境下数据共享的重要需求，其核心思想是将数据流转记录和数据完整性证据写入区块链系统，保证数据在流转过程中不被篡改，从而维护各数据方的权益. 如果需要共享的数据经由区块链存储进行传递，数据确权和溯源将更为直接有效. 如果有机密性要求，则可以将数据加密后上链.

Neisse等人[97]针对欧盟通用数据保护条例对数据处理全流程可追踪可审计的要求，提出了基于区块链的数据管理方案，使用智能合约记录数据来源，将数据使用流转过程记录到区块链中，实现数据确权和数据溯源. Chowdhury等人[98]指出，在数据

① https://mp.weixin.qq.com/s/mlQR_ObfJqBenQfizFZ8GA

共享的场景中，数据通常由第三方服务进行托管，导致数据真实性验证机制复杂且低效. 他们提出了一种个人数据存储系统，数据所有者将数据完整性证据(哈希值)上传到区块链系统，保证数据申请方能够快速验证数据是否被篡改. Liu 等人[99]采用了相同的思路，实现了监控视频的完整性检查. DECS[100]框架针对中心化的数据交易市场无法保证双方数据权益的问题，基于智能合约实现了去中心化的数据交易模型，一方面能够保证数据拥有者对数据的控制权，确保数据权益；另一方面保证数据受让方能够得到真实可靠的数据，防止数据拥有者随意改动价格或者拒绝提供数据. DESC 框架如图 8 所示.

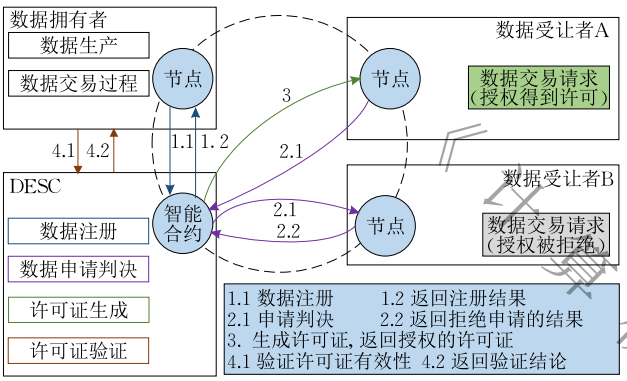

图 8　DESC[101]工作流

Zheng[101]、Shafagh[102]和董祥千[103]等人同样提出了用区块链进行可信数据管理，其核心方法是将数据证据上链，防止共享的数据被篡改. Renner 等人[104]提出 Endolith 框架，实现对文件数据的完整性保护与追踪. Liang 等人[105]针对云环境下数据来源可信审计的问题提出 ProvChain，用于记录云存储中用户收集数据的操作，从数据进入云环境开始建立可信的审计溯源记录.

综上所述，区块链技术能够提供可信的数据和流转记录存证，能在一定程度上实现数据共享过程中的确权与溯源.

4.1.2　可信的日志审计

从安全的角度看，日志是用于安全威胁检测的关键数据，攻击者在实施入侵攻击行为窃取数据后，通常选择删除或篡改日志系统，以消除作恶证据. 因此，日志审计有两个目的，一是判断日志是否被篡改或删除，二是恢复被破坏的日志记录. 目前解决这一问题通常有三类解决方案：(1) 日志系统“只读”设计，但这无法对抗日志被删除的场景，需要设计复杂的日志副本集群；(2) 使用可信第三方存储日志，但是实现完全可信的第三方是困难的；(3) 使用聚合签名，但是无法有效恢复被删除的日志.

区块链去中心化、不可篡改的安全特性和日志系统的结合可以实现更加健壮可信的日志审计系统，其基本思想比较简单，将日志数据和日志完整性证据写入区块链系统，实现日志数据无法被删除篡改，并且能够恢复. 研究者已经展开了一系列的研究工作，如 Cucurull[106]、Sutton[107]、Suzuki[108]、Logchain 框架[109]、Aniello[110]. 这些研究虽然面向不同的应用场景，并且在隐私保护、区块链平台、共识机制等问题的设计有所不同，但基本原理与核心思路相同，不再展开描述.

但是，用区块链技术实现日志系统尚存在一些需要解决的问题. 一是如何保证上链数据的可信性，区块链只能够保证已产生日志的可信，而这些日志本身是否是合法的，区块链无法解决. 二是面向日志量大的应用场景，需要解决高效日志检索审计和高吞吐量的问题，可以采用有向无环图(Directed Acyclic Graph，DAG)的方式构建大吞吐量的区块链系统. 三是解决日志数据量庞大的问题，需要研究可删除的区块链技术，按照合理的时间粒度对过期区块进行有效删除.

4.1.3　“区块链＋”

“区块链＋”是区块链和行业应用进行结合的概念，指的是用区块链技术为各种应用场景提供可信数据存证和溯源. 典型的应用领域包括医疗数据管理[111-112]、学历认证[113]、司法证据[114]、征信管理[115]、档案管理[116]、防伪溯源[117]和电子合同[118]等. 区块链技术能够为这些行业中关键数据的完整性保护提供可行的方案，但是目前尚未有成规模的应用场景落地.

4.2　云环境下数据可信管理

区块链技术在云数据可信管理中主要有三个研究方向，云数据审计，云数据可信删除和云虚拟机可信管理. 其核心思想都是用区块链作为不可篡改的存证，确保云数据管理服务的可信. 如表 6 所示.

表 6　区块链在云数据可信管理中的应用

应用方向	研究内容	核心思想
云数据审计	增强云存储和审计服务的可信度	审计结果记录到区块链网络，确保审计服务的可追溯性[120]
云数据可信删除	可公开验证的云数据删除	将数据删除命令和删除完成的证据存入区块链[121-122]
云虚拟机可信管理	云虚拟机和安全组件度量值的可信管理	用区块链管理虚拟机[123]或 TCB[124]的度量值，确保可信度量值完整可信

(1) 云数据审计

Xue 等人[119]指出,由于下载所有数据进行完整性审计代价昂贵,目前通常采用的是授权第三方审核员(Third-Party Auditor,TPA)对外包数据进行公开审核的方案. 而这种方法目前面临两个问题:① 大多数方案都是基于 PKI 体系,面临证书管理相关的诸多问题,如证书撤掉存储和分发,且效率低下;② TPA 的可信度问题,审计员存在被腐蚀的风险. 因此,他们提出了一种基于身份的公共审计方案 IBPA,将 TPA 的审计结果记录到区块链网络,确保审计服务的可追溯性,降低 TPA 作恶的风险. 另外,IBPA 方案在产生挑战消息时,借鉴了比特币的随机数机制,实现了挑战信息的不可预测性,从而保证了审计对象的随机性. IBPA 方案是使用区块链实现云数据审计的探索性工作,能够提高云存储服务和第三方审计服务的可信度. 但是,该方案增加了用户的计算、存储和网络方面的开销,需要进一步研究更加轻量简洁的审计机制.

(2) 云数据可信删除

云数据的可信删除是云数据安全的重要问题,要求云平台能够正确执行用户的数据删除命令. 在当前的解决方案中,用户无法验证数据删除命令的执行结果. 为了保证删除结果的正确性,并且对服务器的恶意行为进行追踪,需要研究如何构建可公开验证的数据删除协议.

Yang 等人[120]和刘忆宁等人[121]都针对这个问题提出了基于区块链的可公开验证的云存储数据删除方案,核心思路相似,如图 9 所示.

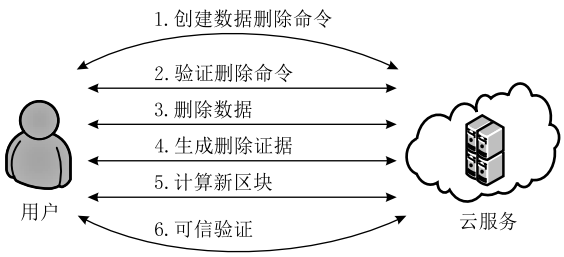

图 9 基于区块链的云数据删除协议框架[121]

Yang 的方法是,用户将签名后的数据删除命令发送到云服务器,云服务器执行删除操作后,执行方法 GenProof()得到删除证据 $proof_i$=(“delete file”, Sig_{Del}, Sig_s, t_d),其中 $Sig_s = Sig_{\mathrm{SKs}}$(“delete file”, Tag_F, t_d). 然后,$proof_i$ 会记录到区块链上,从而可以被各方进行验证. 刘忆宁的方法不同点在于,用户的数据删除命令是发送到区块链上的,云服务器需要在交易确认后执行数据删除的动作,进一步提高了证据的可信度.

若用户是不诚实的,用户可以指责服务端进行了非授权的删除,那么服务端可以从区块链上拿到证据,证明删除命令是用户签名后发出的. 若服务端不诚实,需要讨论两种情况:如果未经授权删除了用户的数据,此时区块链上没有用户发出删除命令的记录,服务端被追责;如果服务端提供伪造的证据并未真正执行删除操作,一旦检测到本应删除的数据仍在云存储中,服务端同样会被追责.

上述方案为云数据可信删除提供了公开验证的解决方案,但是仍然没有形成安全闭环. 在上述研究的安全方案中,若云服务未删除数据却伪造删除证据,此时的安全性依赖于用户能够检测到自己的数据未被删除,这从概率上存在审计遗漏的问题. 另外,云服务是数据管理者,云服务商如果在删除时恶意备份或转移数据,同样会导致数据删除无法验证. 我们认为,可以使用可信执行技术对上述方案进行增强,将云服务器执行数据删除的代码由 TEE 执行,并提供执行证据,这能够提高数据删除的证据的可信度.

(3) 云虚拟机的可信管理

虚拟机(Virtual Machines,VM)是 IaaS(Infrastructure as a Service)云的基本工作单元,其可信度直接影响云环境的安全,而 VM 的度量值就是可信度的核心证据,主要包括哈希值、属性、日志和测试报告. 目前 VM 度量值安全存储主要有两种路线:① 使用可信硬件(TPM,vTPM,Intel SGX 和 ARM Trustzone),但是这类方法需要额外的硬件,并且可信硬件的内部存储空间是有限的,这导致无法完全适用于 IaaS 云;② 基于大型数据中心的安全组件集群进行保护,但是中心化的管理方式为 VM 度量值的保管带来了挑战. 用区块链进行云虚拟机的可信管理能够有效解决上述问题.

Zhao 等人[122]提出了 Mchain 框架,将 VM 的度量值存储到区块链网络中,并制定了访问策略限制数据的暴露范围,从而实现了 VM 度量值的完整性保护. 为了提高云环境下服务的并发性,Mchain 设计了双层链网络. Park 等人[123]提出了 TM-Coin 方案,用区块链管理可信计算基 TCB 的度量值,能够实现物联网环境下高效的可信远程证明.

5　区块链增强数据可用性

区块链是一种分布式的解决方案，能够有效对抗单点失效问题，从而实现更加健壮的信息系统. 区块链共识协议是拜占庭环境下的一致性算法，能够为分布式一致性提供可行的解决方案. 另外，基于区块链实现分布式存储系统，同样能够提高数据的可用性.

5.1　拜占庭环境下的一致性算法

分布式技术的大规模应用要求数据服务具有高可用性，副本复制技术是提高可用性的关键技术，其核心问题是通过分布式共识算法实现副本之间的一致性[124]. 共识算法分为两大类[125]，一种是非拜占庭容错的一致性算法，也叫崩溃容错(Crash Fault-Tolerant，CFT)，另一种是拜占庭容错(Byzantine-Fault-Tolerance，BFT)[126]. 核心区别在于，CFT 假设不存在恶意篡改和伪造数据的拜占庭节点，而 BFT 假设存在恶意节点. 因此，BFT 算法在实现中需要更高的复杂度，例如 CFT 类算法 RAFT[127]的复杂度为 $O(n)$，而 BFT 类算法 PBFT[128]复杂度为 $O(n^2)$. 多项式级的通信复杂度导致 BFT 算法无法应用到复杂网络环境，业内普遍认为 100 个节点是 BFT 算法的上限①. 在实际构建分布式系统，尤其是大规模系统时，通常采用 CFT 类算法. 随着网络安全威胁的日益增加，BFT 的安全假设和实际应用场景更加吻合，但是在区块链技术出现之前，没有一个共识算法能够支撑大规模分布式环境下的拜占庭容错.

袁勇等人[129]指出，从分布式共识算法的角度看，比特币的根本贡献在于首次实现并验证了一类可用的、互联网规模的拜占庭环境下的一致性算法. 区块链系统通过引入激励机制，保证分布式系统中的所有节点正确执行一致性协议. 研究者已经针对区块链共识协议展开了大量的研究工作[130]，具体算法不是本文研究内容，不再赘述. 总之，区块链实现了拜占庭环境下的一致性算法，增强了分布式环境下数据和系统服务的可用性，可以看做区块链在数据安全领域的应用.

5.2　基于区块链的分布式存储系统

基于区块链技术实现分布式存储系统是区块链解决数据可用性的主要研究方向，包含两类研究内容：(1)把区块链作为分布式存储的一种实现形式，讨论其实现、优化和应用场景；(2)用区块链技术解决现有分布式存储系统面临的问题，实现更加健壮的分布式存储系统. 如表 7 所示.

表 7　区块链在分布式存储系统中的应用

应用方向	研究方向	研究内容
区块链分布式存储	区块链本身作为分布式存储	用区块链存储数据，增强数据可用性，对抗 DDoS 攻击[134-137]
		区块链替换传统数据库的优化研究[138-142]
区块链应用于分布式存储	单信任主体的分布式存储	通过存储数据标签[134]或数据库操作日志[135]的方式，提高云存储的监管和审计能力
	去中心化的分布式存储	将区块链作为去中心化分布式存储的激励层，确保存储空间和检索服务充足稳定(Filecoin，Sia，Storj)[136，139-141]
		安全[138]和性能[137]的优化研究

5.2.1　区块链分布式存储

将区块链看做分布式存储的一种实现方式，首先要研究区块链分布式存储和传统分布式存储的区别. Dinh 等人[131]对三种典型的区块链进行实验与分析. 分析结果表明，与传统分布式数据库 H-Store[132]相比，吞吐量降低了 6 个数量级而延迟增加了 4 倍，这导致区块链分布式存储尚无法替代现有的数据库系统. 他们指出，根本问题在于分布式数据库采用的共识协议是 CFT 类的算法，如两段提交(two-phase commit)或类 Paxos 算法，而区块链数据库使用的是类 BFT 算法，性能无法与 CFT 类算法相比. 区块链用作分布式存储有两个主要研究内容：一是探索如何基于区块链实现分布式的存储，以有效对抗 DDoS 等攻击行为，该方向侧重于数据库基础结构设计；二是探索如何对区块链数据库进行优化，使区块链数据库具备传统数据库的基本功能，并且在性能和安全性方面提出优化方案.

研究者针对如何基于区块链技术构建分布式存储系统展开了一系列的研究工作. 首先是探索用区块链实现分布式数据库的应用价值与可行性. Jeon 等人[133]针对物联网环境下使用 MYSQL 数据库带来的安全问题，提出用区块链存储传感器数据，从而有效对抗 DDoS 攻击，降低存储成本. 乔蕊等人[134]提出使用区块链技术对动态数据进行存储和管理，将动态数据及其操作记入区块链系统供用户访问. Nathan 等人[135]提出了基于区块链的关系型数据库的设计方法，根据事务执行和排序完成的前后关系提出了两种副本执行方案，并基于 PostgreSQL 实现了原型系统. Helmer 等人[136]提出了 EthernityDB，

① https://www.jianshu.com/p/5d10cf62d942

将数据库功能集成到以太坊上，所有数据能够在链上保存. 基于区块链实现分布式数据库能够在更高的安全假设之下满足应用对数据库的使用需求.

区块链替换传统数据库在功能和性能上都需要进行优化，如高效的查询检索、区块链吞吐量和延迟等. Muzammal 等人[137]指出，由于区块链缺乏用于索引的数据结构，导致区块链数据库无法提供数据库应有的搜索查询功能. 而传统数据库系统虽然在快速查询检索方面有很多优化，但是难以抵抗恶意篡改，并且存在副本一致性问题. 他们针对上述问题设计了 ChainSQL 系统，实现了应用程序和数据库之间的区块链中间件，把所有数据库操作以日志的形式全部记录到区块链上，新加入节点可以通过区块链记录解析出完整的数据库存储. ChainSQL 是一种透明化的实现方式，用户不会感知到区块链的存在，这提高了系统的实用性. 焦通等人[138]针对区块链数据库的查询缺陷，设计了一种可查询且防篡改的数据库系统，提出了一种基于哈希指针的不可篡改索引，能够实现区块链数据的快速检索，赋予了区块链数据库查询功能. El-Hindi[139]提出了 BlockchainDB，利用区块链作为本地存储层，增加了数据库层，以支持对共享库表的检索与访问. BlockchainDB 采用了灵活的分片技术，允许应用自定义副本在节点中的存储形式，实现安全和效率的平衡. BlockchainDB 的数据库网络如图 10 所示. 另外，Wang 等人[140]在 2018 年提出了面向区块链的存储系统 ForkBase，通过实现新型索引类 SIRI，支持高效的检索查询和重复内容删除. 在此基础之上，该团队 Ruan 等人[141]针对区块链系统缺乏高效数据追溯的方法的问题，克服了只能依靠事务回放的缺陷，提出了 LineageChain 系统，实现了细粒度的安全高效的区块链数据回溯. LineageChain 能够实现在线交易时精细安全地保留数据的变迁轨迹，并提供访问接口. 该研究获得了 VLDB2019 的最佳论文奖①.

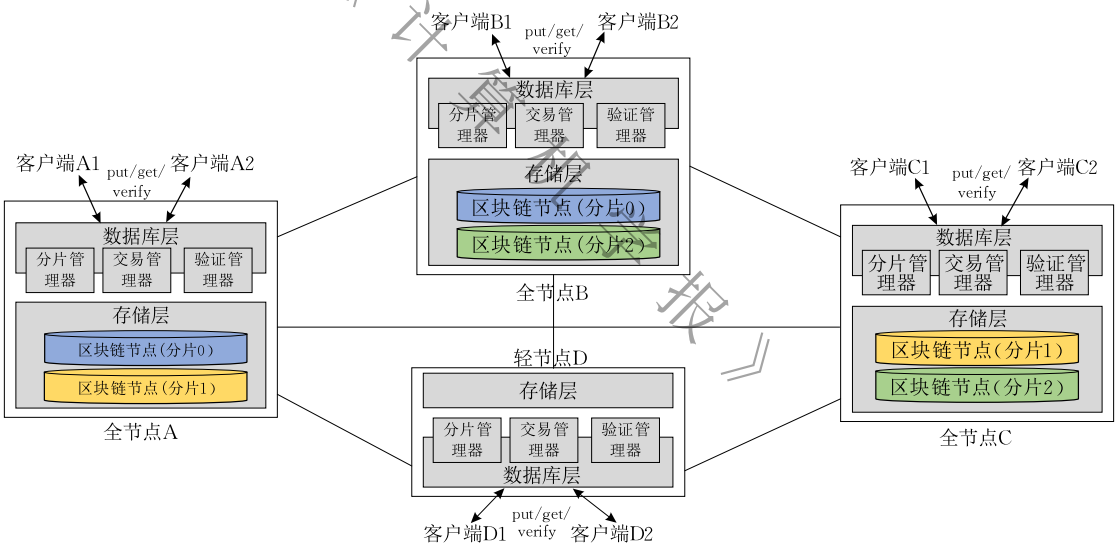

图 10 BlockchainDB[142]数据库典型架构

综上所述，基于区块链实现可用的分布式存储系统是一个有价值的研究方向，能够提高数据可用性，但是其性能问题亟待解决.

5.2.2 区块链技术应用于分布式存储

研究区块链技术如何与分布式存储结合，首先要明确研究的对象. 分布式存储是一个复杂的研究领域，其内含早已超出“数据分散存储在不同设备上②”这一原始的定义. 本文从信任关系的角度出发，将分布式存储划分为两种. 一类是单信任主体的分布式存储，如 Amazon EC2③、阿里云④等云平台. 这些平台使用了分布式存储技术，采用了去中心化的数据管理方式，但是用户对云存储的信任本质上是对某个云服务商或企业的信任，并非完全去中心化. 另一类是多信任主体的分布式存储，也可以称为去中心化的分布式存储. 多信任主体的分布式存储把数据存储于网络中的多个节点，并且节点的信任主体是不同的，典型的系统有 IPFS⑤、Storj⑥、Sia⑦和 Swarm⑧. 目前区块链技术和两种分布式存储都

① http://www.vldb.org/2019/?papers-research#Research_Session_24
② https://baike.baidu.com/item/分布式存储/5557030
③ https://aws.amazon.com/cn/ec2/
④ https://cn.aliyun.com/
⑤ http://www.ipfs.cn/
⑥ https://storj.io/
⑦ https://sia.tech
⑧ https://swarm-guide.readthedocs.io/en/latest/

有结合性的研究，但主要集中在后者.

(1) 单信任主体的分布式存储

在单信任主体的分布式存储中，区块链用于存储大规模分布式云存储的中间数据，如数据标签、操作日志等，建立可信的安全存证服务.

Do 等人[142]提出 BlockDB 框架，将用户上传到云存储数据的关键字标签存储到区块链，由区块链管理云存储数据的搜索权限，增强了用户对云存储数据的监管能力. Zou 等人[143]针对分布式存储系统存储副本面临分叉(Fork)的问题，提出了面向云存储的区块链中间件 ChainFS，将分布式存储的所有操作日志记录到区块链中，客户端可以通过下载日志链对所有的操作和事务按序进行检查.

(2) 去中心化分布式存储

IPFS、Storj 和 Sia 等项目的核心是去中心化的分布式存储协议，并不是区块链系统，这一点经常被混淆. 区块链只是应用在这些项目中用于解决某些问题. IPFS 等协议旨在利用网络中的闲置存储资源，建立一个分布式的数据存储系统，将数据分块分散存储到不同的网络存储位置，并提供快速恢复数据的能力. 即便有节点数据丢失或损坏，高冗余能力也可以保证数据是可恢复的.

为了实现大规模的分布式存储需要解决 3 个问题：(1) 如何提高存储容量，也就是吸引更多用户提供存储资源；(2) 如何提高检索效率，实现服务的快速响应；(3) 保证数据存储和流通安全. 研究者针对这一问题引入区块链技术作为分布式存储的激励层，并得到了一系列的研究成果. 最具有代表性的方案是 Filecoin 项目①，这是一种基于 IPFS 的分布式存储系统，如图 11 所示. 在 Filecoin 中，引入了叫作 filecoin 的代币，激励各方参与到 Filecoin 网络中. 存储方可以通过存储证明机制(Proof of Storage)证明自己的有效存储容量从而获得代币，解决了第一个问题；检索服务方可以提供数据检索服务，高效的检索能够获得更多的代币，解决了第二个问题. 而数据安全方面可以通过加密技术解决，并且区块链能够提供数据访问的存证. 但是，Filecoin 项目尚处于研发阶段，并未真正落地. 在 Storj 和 Sia 项目中，区块链同样发挥了类似的作用.

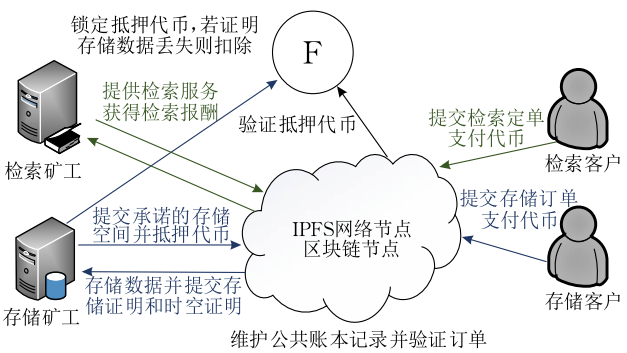

图 11　Filecoin 网络架构

此外，学术界在这一研究方向同样进行了一系列的研究与探索，主要针对已经实际落地的 Storj 和 Sia 项目进行改进. Storj 和 Sia 使用加密货币的激励机制保证各参与方行为合规，但缺乏针对错误行为的主动快速的检查机制，只有在下载数据时才能发现数据损坏的行为. 针对这一问题，Ruj 等人[144]提出了 BlockStore 框架，其中区块链用于记录存储资源的供需关系，并提供支付和罚款功能. BlockStore 设计了特殊的数据结构 Space Wallet，用于存储可用的存储空间列表，实现存储的高效分配. 此外，BlockStore 提供了数据存储的定期审核机制，保证对错误行为的及时发现与追踪. Chen 等人[145]从性能优化角度出发，提出采用更高效的 Zigzag code 代替 Storj 和 Sia 使用的 Reed Solomon (RS) code，以获得更高的性能. Fukumitsu 等人[146]从安全性角度出发指出，Storj 将用户完整的元数据加密存储到区块链上，容易遭到离线暴力破解. 另外 Storj 的口令认证服务是中心化的，同样容易遭到攻击. 因此，他们提出将加密后的元数据分成多份随机存储到 P2P 网络中的节点中，存储节点使用可记忆的信息(ID，password)确定，从而提高了存储安全性. 另外，Ali[147]、Li[148]和 Li[149]等人同样提出了和 Filecoin 相似的解决方案.

综上所述，区块链为去中心化的分布式存储提供了激励机制和审计机制，有助于激励各方积极参与，从而实现更大规模的分布式存储系统.

6　研究挑战与展望

6.1　研究挑战

本文深入研究了区块链在数据安全领域的研究进展，按照区块链增强数据机密性、数据完整性和数据可用性三个方向进行了详细的介绍. 但是当前的研究仍然存在一些不足和挑战.

6.1.1　机密性

(1) 数据加密

区块链作为密码学中可信第三方的实现方案

① https://filecoin.io/

时,能够有效解决中心化带来的安全风险.区块链技术的防篡改特性能够为密码协议提供可信赖的激励机制,具有良好的安全效果.

但是区块链是一个公开的账本,恶意节点虽然无法作恶,但是能够获得所有的账本数据,进而能够进行更加深入的数据分析.因此,需要进一步研究如何解决区块链的隐私保护问题.另外,区块链需要运行多方参与的拜占庭容错协议,其中交互式的 BFT 类算法需要进行多轮的消息通信,而非交互式的区块链共识需要等待多个区块落账后才能确认交易.因此,区块链的引入必然会带来额外的响应延迟,这可能会成为密码协议的性能瓶颈,对区块链与数据加密结合的方案实用性带来较大的影响.

(2)身份认证

基于区块链的身份认证技术能够有效解决认证中心单点化以及认证透明度的问题,但仍处于初级阶段,应用落地尚需时日.在去中心的网络尤其是大规模网络中,密钥恢复问题、证书撤销问题、用户隐私保护问题、跨域身份认证以及认证效率问题都是亟待解决的难点.另外,基于区块链的身份认证机制需要与现有的认证系统进行融合,才能够更容易得到推广.例如,引入无需可信管理者的动态密码累加器实现更加高效安全的认证;基于秘密共享技术实现分布式环境下的密钥恢复;使用零知识证明对身份认证过程进行隐私保护.

(3)访问控制

① 去中心化的访问控制

在面向通用场景的基于区块链的分布式访问控制方面,访问控制策略如何进行更新或撤销,如何承载复杂的大数据量的交易,链上的策略和权限进行隐私性设计,如何提高区块链访问控制的响应速度,如何实现跨域的访问控制机制都是需要研究的内容.例如,采用多链技术实现大数据环境下的访问控制,通过降低单链的数据规模的方式,提高特定应用场景下策略的更新效率;采用可信计算技术提高策略和权限管理认证的安全性.

在面向物联网环境的基于区块链的分布式访问控制方面,针对智能生活的应用场景,需要设计上下文感知的细粒度访问控制模型,对不同用户采用不同的授权策略;实际应用中跨平台跨信任模型需要根据参与者的动态业务需求覆盖任意场景,需要研究在协作物联网中如何建立跨平台信任模型;区块链上的策略是动态变化的,尤其物联网环境中的设备和用户数量巨大,需要研究如何进行高效快速的策略管理;区块链部署需要较多的资源,需要研究轻量级区块链系统,其加密算法,密码协议和存储结构都需要特殊的轻量化设计.

② 区块链增强属性加密

目前,使用区块链技术增强属性加密的基本思路相似,能够一定程度上解决控制中心单点化问题、多提高授权机构互信以及对抗多用户之间的串谋攻击.但是目前方案存在的问题是,多授权机构各自拥有属性私钥,容易产生密钥泄露风险.可以采用秘密共享等技术,实现分布式的密钥管理,进一步降低中心化的风险.另外,属性密码滥用和责任认定是该研究方向的痛点,而区块链有防抵赖的特性,两者的结合是一个有价值的研究方向.

(4)可信执行环境

区块链为 TEE 可用性提供了行之有效的解决思路,进而增强了计算系统的数据机密性保护.Ekiden 是当前的典型架构,但是仍旧存在诸多问题.在密钥管理方面,Ekiden 采用了全部 TEE 共享一个主密钥的方案,并假设 TEE 本身是可信的.但是在实际情况中,TEE 会由于侧信道攻击导致密钥泄露,包括(主密钥,key_{cid}^{state},sk_{cid}^{in}).因此,需要在更强的安全模型下采用秘密共享、安全多方计算等技术实现密钥管理.GXChain 项目做了部分探索工作①.在性能方面,Ekiden 探索如何用智能合约承载深度学习框架.但是这个计算过程是基于 CPU 的,难以承载更加复杂的智能合约,也就无法承载更复杂的深度学习应用.Graviton[94] 实现了 GPU 上的 TEE 扩展,建立了 CPU 直接到 GPU 的信任链,保护了 GPU 上的模型和数据安全.因此我们认为可以进一步研究如何将 GPU-TEE 扩展到 Ekiden 模型之上,以承载更加复杂的智能合约逻辑.

(5)隐蔽信道

区块链应用于隐蔽信道构建是一个比较新的研究方向,当前的研究仅证明了该研究思路的可行性,但仍有较多问题需要解决.比如,如何在完全公开透明的场景下隐藏数据传输、如何建立账号匿名机制以对抗针对账本数据的关联分析、如何提高信息恢复效率、如何建立群组之间的隐蔽信道等.另外,从正反博弈的角度考虑,针对区块链隐蔽信道的检测技术同样需要进行研究,实现对恶意行为和非法通信的追踪与溯源.

6.1.2 完整性

区块链应用于数据完整性保护时,无论是数据

① https://static.gxchain.org/files/GXChain_TCP_V1.0_CN.pdf

确权与溯源、基于区块链的日志审计还是其他数据可信管理服务，其根本思想都是将数据的流转记录和完整性证据存储到区块链平台上，从而获得不可篡改的安全特性.但是，目前的方案存在两个明显的不足：

(1)未能实现完整的数据安全闭环

根本原因在于目前的区块链本身是一个被动的账本，只能够相信起始数据的真实性，无法从语义和内涵上判断链上的记录是否可靠.例如，数据拥有者声称自己拥有数据，并将元数据和证据上链，此时区块链只能相信而无法主动验证.无论是数据确权与溯源，日志审计还是应用于云环境下实施数据可信删除，均面临这个问题.因此，需要进一步研究如何基于区块链技术实现一个完整的数据确权溯源的闭环，实现数据全生命周期的管控.

(2)用于大数据环境时的效率问题

为了实现数据完整性的保护，区块链平台承载的数据量和应用场景是紧密相关的.大数据应用场景具有数据量大、数据动态变化、数据交易频繁的特点，这就要求区块链具有良好的吞吐量和延迟.

6.1.3　可用性

(1)区块链实现分布式存储

基于区块链实现分布式存储时，需要对标传统分布式数据库的技术和功能.由于区块链数据库采用的是拜占庭容错的算法，本身存在性能上的差距，并且不具备完善的数据库功能.因此需要针对应用需求进行大规模的优化.可以从5个方向对区块链分布式存储进行优化：①将区块链计算和共识解耦，降低单节点的计算负担，并且设计更加适合查询与分析的区块链数据结构；②引入可信硬件(TPM，SGX)，降低拜占庭容错协议的网络复杂度，提高共识性能；③改变共识协议的流程结构，针对具体的应用场景和安全假设，简化共识协议的设计，如Hotstuff算法[150]；④采用分片技术(Sharding)提高事务处理速度，降低成本；⑤支持声明式语言(如SQL)的智能合约，以实现更复杂的逻辑满足分布式数据库系统的要求.我们认为，针对区块链性能优化的研究有助实现更加实用的区块链数据库.

(2)区块链应用于分布式存储

区块链为去中心化的分布式存储提供了激励机制和审计机制，有助于激励各方积极参与，从而实现更大规模的分布式存储系统.但是，仍有一些问题亟待解决：①目前的应用模式本质上是去中心化的“网盘”，不支持复杂的查询检索；②安全设计不足，以IPFS为例，只要得到数据内容地址，就能够拿到完整的数据.类Filecoin方案从经济角度出发解决问题，然而不是所有的场景都可以运行代币.我们认为可以结合去中心化访问控制模型的实现方法，使用区块链为分布式数据存储建立基于属性和权限访问控制体系，以满足更多应用场景的需求；③现有的方案通常将数据加密后分片存储，但是密钥仍旧是集中式的管理，需要研究去中心的密钥托管方案，可以采用门限签名、多方安全计算等手段实现，KeyShard项目①进行了相关探索.

6.2　展　望

本文已在6.1节对各研究方向的缺陷进行了分析，其中包含部分共性问题.为了实现基于区块链技术解决分布式数据共享安全的目标，从实际方案应用落地的角度出发，需要重点解决以下几个问题：

(1)区块链的效率问题.

区块链的效率是基于区块链的数据安全解决方案能否真正落地的关键因素.区块链的效率优化是一个综合性的问题，下面从理论和实践两个方面进行阐述.

在基础理论方面，根据CAP理论[151]，需要在支持分区容错的前提下，对一致性和可用性进行平衡.而在PACEL权衡的理论中[152]，当不发生网络分区时，需要在一致性和延迟之间找到平衡.因此，区块链的性能优化必须针对特定的应用场景采取特殊的优化方案.例如，在某个权威机构组成的联盟链中，发生网络分区的概率较低，此时可以在PACEL的指导下，根据实际需求在强一致性和低延迟之间进行取舍.

在实践方面，区块链的优化涉及到诸多方面的内容：①共识协议.共识协议与吞吐量、可扩展性、延迟等核心指标具有直接的关系，是区块链优化的重要的内容.需要研究共识协议本身的优化方案，可以采取分片、流水线设计、引入可信硬件、降低去中心化程度(如线性的BFT类算法Hotstuff)等方式；②网络优化.针对区块链网络中实际数据包的大小，设计合理的区块大小和出块间隔；③算法加速，对区块链中涉及到的算法进行性能提升，如采用硬件加密算法提升签名验签性能，采用聚合签名降低签名验签的数量，采用门限密码降低区块链的通信复杂度，针对特定场景设计实现轻量级的区块链系统.在不同的应用场景中，需要针对特殊需求对区块链系统的吞吐量，延迟，可扩展性等进行优化.

(2)数据管控的安全闭环问题.

目前，基于区块链实现数据存证和管控是区块

① https://keyshard.platon.network

链在数据安全中重要的应用方向，但是存在两个难点问题.

一是数据源头的可信性问题. 如 6.1.2 节中的阐述，区块链本身是一个被动式的账本，无法证明数据本身是否可信. 例如，区块链无法判断上传的日志数据是否是真实，只能够保证这些数据不会篡改；区块链能够刻画农产品的流转轨迹，但是无法保证上链“阳澄湖大闸蟹”的真伪，仍旧需要相关协会和政府部门的背书. 因此，需要引入更多的技术和管理机制与区块链结合，解决数据源头的可信性问题. 比如，结合可信执行和数据标签技术，保证数据生产过程的安全可信，确保数据标签的真实有效；加强对区块链账本的审计与追溯，快速发现虚假数据，追溯数据产生的源头，进而剔除不可信的数据源.

二是数据交易场景中的“最后一公里”问题. 基于区块链的数据交易市场能够实现分布式的数据检索、申请和授权. 申请者可以持有数据授权的令牌向数据拥有者申请数据. 如果数据经由链下通道发送，这个过程脱离了区块链的控制，仍然存在抵赖的问题. 如果数据通过链上发送，就会面临数据的隐私保护问题. 尤其是敏感的数据，即便以密文形态在链上传播，仍然存在被分析破解的风险. 这个问题是安全与可用性之间的权衡，需要针对具体的应用和信任场景进行抉择.

(3) 隐私保护问题.

区块链是一个公开的账本，这个特性对于实现不可抵赖的机制是至关重要的，但是会带来隐私保护问题. 在区块链与数据安全结合的应用领域中，区块链通常作为分布式的可信第三方或者激励层，参与者有可能通过分析数据账本挖掘其中的隐秘关联. 因此，需要进一步研究如何在上述研究中引入隐私保护机制，采用零知识证明和同态加密技术，提高密码安全系统的隐私保护能力，尤其是需要突破零知识证明和同态加密的性能壁垒. 另外，可以采用通道技术，根据业务领域进行账本隔离，从而增强账本的隐私保护.

(4) 区块链基础设施安全

本文研究的是区块链如何应用于数据安全，因此区块链基础设施本身的安全至关重要. 如果区块链平台自身带来更大的安全隐患和威胁，该方向的研究便失去意义. 区块链基础设施安全主要考虑 5 个方面①. (a) 密码学. 主要包括哈希、数字签名、密码协议等，如果基础密码学技术存在漏洞，区块链的基础设施从根本上就是不安全的. 目前，区块链采用了比较多的新型的算法和协议，这个问题会比较明显；(b) 私钥安全. 私钥是用户参与区块链系统的核心凭证，私钥的生产、使用和管理十分重要. 因此，高安全的钱包设计，基于硬件的私钥保护，分布式的密钥管理都是值得研究的方向；(c) 节点系统安全. 这属于传统的安全范畴. 在联盟链中，区块链节点较少，需要采用更加可靠的安全机制增强区块链节点的系统安全；(d) 共识协议. 拜占庭容错是区块链共识协议的核心，共识协议能否真正实现对少部分拜占庭节点的容错能力是至关重要的. 共识协议的设计不仅要从理论上进行安全性证明，在实际编码实现时，更需要充分考虑安全性的因素；(e) 智能合约漏洞. 目前，智能合约是区块链特有且危害最大的安全隐患，主要包括合约逻辑缺陷和编码漏洞风险. 因此，必须进行智能合约代码的形式化验证，实现对合约的安全审计. 杨霞教授在该方向进行了大量的研究和实践②.

(5) 区块链系统的同构化问题.

拜占庭场景下通常有失效隔离的假设，各节点之间的崩溃或安全问题不会互相影响. 但是在实际场景尤其是云环境中，承载区块链节点的操作系统可能相同，这就导致相同的漏洞可以威胁到所有节点，攻击难度并未随着节点数量成倍增加. 一方面可以借鉴拟态计算的思想，实现动态异构冗余的区块链系统[153]，另一方面可以引入可信执行技术，把简单的签名背书扩展为基于 TEE 的执行背书，以提高单节点的安全性.

(6) 区块链工程落地问题.

区块链的安全假设本质上是概率性的，只有当节点数量达到一定规模时才更有意义. 但是，在联盟链或私有链的实际应用中，不可能占用过多的计算节点组成区块链网络. 需要研究如何在小规模节点场景下提高单节点的安全性，可以采用拟态计算、可信计算等方式. 另外，运行区块链系统需要占用较大的计算、存储和网络带宽. 本文研究的是区块链如何应用于数据安全领域，需要进行区块链效益的量化评估工作，对区块链系统占用资源和达到的安全收益进行分析，为工程落地提供参考依据.

7 结束语

本文对区块链在数据安全领域的研究进展进行了较为全面的综述，并对各类研究进行了缺陷分析

① https://www.jianshu.com/p/ffdbd0bb7c5c
② https://blog.csdn.net/Blockchain_lemon/article/details/80656406

和研究展望.研究结果表明,区块链具有中心化、防篡改、可追溯的重要安全特性,能够在机密性,完整性和可用性三个层面为数据安全保护提供切实有效的解决思路,有着广阔的应用前景.

致　谢　在此,我们向对本文研究工作给予支持和建议的同行表示衷心的感谢!

参　考　文　献

[1] Walker S J. Big data: A revolution that will transform how we live, work, and think. Mathematics & Computer Education, 2014, 47(17): 181-183

[2] Eyal I, Gencer A E, Sirer E G, Renesse R V. Bitcoin-NG: A scalable blockchain protocol//Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation. USENIX Association Berkeley, USA, 2015: 45-59

[3] Vukolić M. The quest for scalable blockchain fabric: Proof-of-Work vs. BFT replication//Camenisch J, eds. International Workshop on Open Problems in Network Security. New York, USA: Springer, 2015: 112-125

[4] Zhu Lie-Huang, Gao Feng, Shen Meng, et al. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017, 54(10): 2170-2186(in Chinese)
(祝烈煌,高峰,沈蒙等.区块链隐私保护研究综述.计算机研究与发展,2017,54(10):2170-2186)

[5] Liu Ao-Di, Du Xue-Hui, Wang Na, et al. Research progress of blockchain technology and its application in information security. Journal of Software, 2018, 29(7): 2092-2115(in Chinese)
(刘敖迪,杜学绘,王娜等.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)

[6] Li Jian-Zhong, Liu Xian-Min. An important aspect of big data: Data usability. Journal of Computer Research and Development, 2013, 50(6): 1147-1162(in Chinese)
(李建中,刘显敏.大数据的一个重要方面:数据可用性.计算机研究与发展,2013,50(6):1147-1162)

[7] Goyal R, Goyal V. Overcoming cryptographic impossibility results using blockchains//Kalai Y, Reyzin L, eds. Theory of Cryptography(TCC). Lecture Notes in Computer Science, vol. 10677. Cham: Springer, 2017: 529-561

[8] Song Tao-Yi, Zhao Yun-Lei. Comparison of Blockchain Consensus Algorithm. Computer Applications and Software, 2018, 35(8): 1-8(in Chinese)
(宋焘谊,赵运磊.区块链共识算法的比较研究.计算机应用与软件,2018,35(8):1-8)

[9] Liu Yi-Zhong, Liu Jian-Wei, Zhang Zong-Yang, et al. Overview on blockchain consensus mechanisms. Journal of Cryptologic Research, 2019, 6(4): 395-432(in Chinese)
(刘懿中,刘建伟,张宗洋等.区块链共识机制研究综述.密码学报,2019,6(4):395-432)

[10] Zheng Min, Wang Hong, Liu Hong, et al. Survey on consensus algorithms of blockchain. Netinfo Security, 2019, 19(7): 8-24(in Chinese)
(郑敏,王虹,刘洪等.区块链共识算法研究综述.信息网络安全,2019,19(7):8-24)

[11] Fu Shuo, Xu Hai-Xia, Li Pei-Li, et al. A survey on anonymity of digital currency. Chinese Journal of Computers, 2019, 42(5): 1045-1062(in Chinese)
(付烁,徐海霞,李佩丽等.数字货币的匿名性研究.计算机学报,2019,42(5):1045-1062)

[12] Pan Chen, Liu Zhi-Qiang, Liu Zhen, Long Yu. Research on scalability of blockchain technology: Problems and methods. Journal of Computer Research and Development, 2018, 55(10): 2099-2110(in Chinese)
(潘晨,刘志强,刘振,龙宇.区块链可扩展性研究:问题与方法.计算机研究与发展,2018,55(10):2099-2110)

[13] Li Fang, Li Zhuo-Ran, Zhao He. Research on the progress in cross-chain technology of blockchains. Journal of Software, 2018, 29(6): 1649-1660(in Chinese)
(李芳,李卓然,赵赫.区块链跨链技术进展研究.软件学报,2018,29(6):1649-1660)

[14] Yu Hui, Zhang Zong-Yang, Liu Jian-Wei. Research on scaling technology of Bitcoin blockchain. Journal of Computer Research and Development, 2017, 54(10): 2390-2403(in Chinese)
(于喻辉,张宗洋,刘建伟.比特币区块链扩容技术研究.计算机研究与发展,2017,54(10):2390-2403)

[15] Wang Hua-Qun. Cryptography on the blockchain. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2017, 37(6): 61-67(in Chinese)
(王化群.区块链中的密码学技术.南京邮电大学学报:自然科学版,2017,37(6):61-67)

[16] Jarecki S, Jutla C, Krawczyk H, et al. Outsourced symmetric private information retrieval//Proceedings of the ACM Conference on Computer and Communications Security. Berlin, Germany, 2013: 875-888

[17] Wang Q, Ren K, Du M, et al. SecGDB: Graph encryption for exact shortest distance queries with efficient updates//Proceedings of the 21st International Conference on Financial Cryptography and Data Security. Sliema, Malta, 2017: 79-97

[18] Hu S, Cai C, Wang Q, et al. Searching an encrypted cloud meets blockchain: A decentralized, reliable and fair realization//Proceedings of the IEEE Conference on Computer Communications. Honolulu, USA, 2018: 792-800

[19] Agyekum O, Opuni-Boachie K, Xia Q, et al. A secured proxy-based data sharing module in IoT environments using blockchain. Sensors, 2019, 19(5): 1235

[20] Halpern J, Teague V. Rational secret sharing and multiparty computation//Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC 2004). Chicago, USA, 2004: 623-632

[21] Belenkiy M, Chase M, Erway C C, et al. Making P2P accountable without losing privacy//Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society (WPES 2007). Alexandria, USA, 2007: 31-40

[22] Alptekin K, Anna L. Usable optimistic fair exchange. Computer Networks, 2012, 56(1): 50-63

[23] Lindell A Y. Legally-enforceable fairness in secure two-party computation//Malkin T, ed. Cryptographers' Track—RSA 2008, volume 4964 of LNCS. Berlin, Germany: Springer, 2008: 121-137

[24] Andrychowicz M, Dziembowski S, Malinowski D, et al. Fair two-party computations via Bitcoin deposits//Proceedings of the Financial Cryptography and Data Security. Berlin, Germany, 2014: 105-121

[25] Andrychowicz M, Dziembowski S, Malinowski D, et al. Secure multiparty computations on Bitcoin//Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, USA, 2014: 443-458

[26] Kiayias A, Zhou H S, Zikas V. Fair and robust multi-party computation using a global transaction ledger//Proceedings of the Advances in Cryptology—EUROCRYPT 2016. Berlin, Germany, 2016: 705-734

[27] Bentov I, Kumaresan R. How to use Bitcoin to design fair protocols//Proceedings of the Advances in Cryptology (CRYPTO 2014). Heidelberg, Germany, 2014: 421-439

[28] Kumaresan R, Bentov I. How to use Bitcoin to incentivize correct computations//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Scottsdale, USA, 2014: 30-41

[29] Kumaresan R, Moran T, Bentov I. How to use Bitcoin to play decentralized poker//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Denver, USA, 2015: 195-206

[30] Kumaresan R, Vaikuntanathan V, Vasudevan P N. Improvements to secure computation with penalties//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 406-417

[31] Kumaresan R, Bentov I. Amortizing secure computation with penalties//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria, 2016: 418-430

[32] Bentov I, Kumaresan R, Miller A. Instantaneous decentralized poker//Takagi T, Peyrin T, eds. Advances in Cryptology—ASIACRYPT 2017. Lecture Notes in Computer Science, vol. 10625. Cham: Springer, 2017: 410-440

[33] Choudhuri A R, Green M, Jain A, et al. Fairness in an unfair world: Fair multiparty computation from public bulletin boards//Proceedings of the ACM Conference on Computer and Communications Security. Dallas, USA, 2017: 719-736

[34] Ellison C, Schneier B. Ten risks of PKI: What you're not being told about public key infrastructure. Computer Security Journal, 2000, 16(1): 1-7

[35] Lin J Q, Jing J W, Zhang Q L, Wang Z. Recent advances in PKI technologies. Journal of Cryptologic Research, 2015, 2(6): 487-496

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

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

[38] Leiding B, Cap C H, Mundt T, et al. Authcoin: Validation and authentication in decentralized networks//Proceedings of the Mediterranean Conference on Information Systems (MCIS 2016). Paphos, Cyprus, 2016: 5

[39] Ali M, Nelson J, Shea R, Freedman M J. Blockstack: A global naming and storage system secured by blockchains//Proceedings of the USENIX Annual Technical Conference. Denver, USA, 2016: 181-194

[40] Kalodner H, Carlsten M, Ellenbogen P, et al. An empirical study of Namecoin and lessons for decentralized namespace design//Proceedings of the 14th Workshop on the Economics of Information Security. Delft, Netherlands, 2015: 1-23

[41] Caronni G. Walking the Web of trust//Proceedings of the IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises. Gaithersburg, USA, 2000: 153-158

[42] Bui T, Aura T. Application of public ledgers to revocation in distributed access control//Proceedings of the 20th International Conference on Information and Communications Security. Lille, France, 2018: 781-792

[43] Al-Bassam M. SCPKI: A smart contract-based PKI and identity system//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. New York, USA, 2017: 35-40

[44] Hari A, Lakshman T V. The Internet Blockchain: A distributed, tamper-resistant transaction framework for the Internet//Proceedings of the 15th ACM Workshop on Hot Topics in Networks. Atlanta, USA, 2016: 204-210

[45] Matsumoto S, Reischuk R M. IKP: Turning a PKI around with decentralized automated incentives//Proceedings of the IEEE Symposium on Security and Privacy. San Jose, USA, 2017: 410-426

[46] Chen J, Yao S X, Yuan Q, et al. CertChain: Public and efficient certificate audit based on blockchain for TLS connections//Proceedings of the IEEE Conference on Computer Communications. Honolulu, USA, 2018: 2060-2068

[47] Wang Z, Lin J, Cai Q, et al. Blockchain-based certificate transparency and revocation transparency//Proceedings of the Financial Cryptography and Data Security Workshops. Nieuwpoort, Curaçao, 2019: 144-162

[48] Axon L, Goldsmith M. PB-PKI: A privacy-aware blockchain-based PKI//Proceedings of the International Joint Conference on e-Business and Telecommunications International Conference on Security and Cryptography. Madrid, Spain, 2017: 311-318

[49] Dunphy P, Petitcolas F A P. A first look at identity management schemes on the blockchain. IEEE Security & Privacy, 2018, 16(4): 20-29

[50] Stokkink Q, Pouwelse J. Deployment of a blockchain-based self-sovereign identity//Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax, Canada, 2018: 1336-1342

[51] Lee J H. BIDaaS: Blockchain based ID as a service. IEEE Access, 2018, (6): 2274-2278

[52] Dong Gui-Shan, Chen Yu-Xiang, Zhang Zhao-Lei, et al. Research on identity management authentication based on blockchain. Computer Science, 2018, 45(11): 59-66(in Chinese)
(董贵山，陈宇翔，张兆雷等. 基于区块链的身份管理认证研究. 计算机科学，2018，45(11)：59-66)

[53] Takemiya M, Vanieiev B. Sora identity: Secure, digital identity on the blockchain//Proceedings of the IEEE Computer Software & Applications Conference. Tokyo, Japan, 2018: 582-587

[54] Maesa D D F, Mori P, Ricci L. Blockchain based access control//Chen L, Reiser H, eds. Distributed Applications and Interoperable Systems (DAIS 2017). Lecture Notes in Computer Science, vol. 10320. Cham: Springer, 2017: 206-220

[55] Liu Ao-Di, Du Xue-Hui, Wang Na, et al. A blockchain-based access control mechanism for big data. Journal of Software, 2019, 30(9): 2636-2654(in Chinese)
(刘敖迪，杜学绘，王娜等. 基于区块链的大数据访问控制机制. 软件学报，2019，30(9)：2636-2654)

[56] Wang Xiu-Li, Jiang Xiao-Zhou, Li Yang. Model for data access control and sharing based on blockchain. Journal of Software, 2019, 30(6): 1661-1669(in Chinese)
(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. 软件学报，2019，30(6)：1661-1669)

[57] Cruz J P, Kaji Y, Yanai N. RBAC-SC: Role-based access control using smart contract. IEEE Access, 2018, (6): 12240-12251

[58] Zyskind G, Nathan O, Pentland A S. Decentralizing privacy: Using blockchain to protect personal data//Proceedings of the IEEE Symposium on Security and Privacy Workshops. San Jose, USA, 2015: 180-184

[59] Liu Ming-Da, Shi Yi-Juan, Chen Zuo-Ning. Distributed trusted network connection architecture based on blockchain. Journal of Software, 2019, 30(8): 2314-2336(in Chinese)
(刘明达，拾以娟，陈左宁. 基于区块链的分布式可信网络连接架构. 软件学报，2019，30(8)：2314-2336)

[60] Liu Ming-Da, Shi Yi-Juan. Remote attestation model based on blockchain. Computer Science, 2018, 45(2): 48-52, 68 (in Chinese)
(刘明达，拾以娟. 基于区块链的远程证明模型. 计算机科学，2018，45(2)：48-52，68)

[61] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management//Proceedings of the International Conference on Open and Big Data. Vienna, Austria, 2016: 25-30

[62] Sifah E B, Xia Q, Agyekum K O B O, et al. Chain-based big data access control infrastructure. The Journal of Supercomputing, 2018, 74(3): 4945-4964

[63] Alansari S, Paci F, Sassone V. A distributed access control system for cloud federations//Proceedings of the IEEE International Conference on Distributed Computing Systems. Atlanta, USA, 2017: 2131-2136

[64] Shi Jin-Shan, Li Ru. Survey of blockchain access control in Internet of Things. Journal of Software, 2019, 30(6): 1632-1648(in Chinese)
(史锦山，李茹. 物联网下的区块链访问控制综述. 软件学报，2019，30(6)：1632-1648)

[65] Ouaddah A, Mousannif H, Elkalam A A, et al. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 2016, 112(1): 237-262

[66] Ouaddah A, Abou Elkalam A, Ait Ouahman A. FairAccess: A new blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 2016, 9(18): 5943-5964

[67] Ouaddah A, Elkalam A A, Ouahman A A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT//Rocha Á, Serrhini M, Felgueiras C, eds. Europe and MENA Cooperation Advances in Information and Communication Technologies. Advances in Intelligent Systems and Computing, vol. 520. Cham: Springer, 2017: 523-533

[68] Le T, Mutka M W. CapChain: A privacy preserving access control framework based on blockchain for pervasive environments//Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP). Taormina, Italy, 2018: 57-64

[69] Pinno O J A, Grégio A, De Bona L C E. ControlChain: Blockchain as a central enabler for access control authorizations in the IoT//Proceedings of the IEEE Global Communications Conference. Abu Dhabi, The United Arab Emirates, 2017: 1-6

[70] Tang B, Kang H J, Fan J W, et al. IoT Passport: A blockchain-based trust framework for collaborative Internet-of-Things//Proceedings of the ACM Symposium on Access Control Models and Technologies. Toronto, Canda, 2019: 83-92

[71] Outchakoucht A, Hamza E, Leory J. Dynamic access control policy based on blockchain and machine learning for the Internet of Things. International Journal of Advanced Computer Science and Applications, 2017, 8(7): 417-424

[72] Ourad A Z, Belgacem B, Salah K. Using blockchain for IOT access control and authentication management//Proceedings of the International Conference on Internet of Things. Berlin, Germany, 2018: 150-164

[73] Yuan C, Xu M, Si X, et al. Blockchain with accountable CP-ABE: How to effectively protect the electronic documents//

Proceedings of the IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS). Shenzhen, China, 2017: 800-803

[74] Jemel M, Serhrouchni A. Decentralized access control mechanism with temporal dimension based on blockchain//Proceedings of the 2017 IEEE International Conference on e-Business Engineering. Shanghai, China, 2017: 177-182

[75] Wang Shangping, Zhang Yinglong, Zhang Yaling. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 2018, 20(6): 38437-38450

[76] Zhang Y, He D, Choo K K R. BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT. Wireless Communications and Mobile Computing, 2018, 2018: 1-9

[77] Behl J, Distler T, Kapitza R. Hybrids on steroids//Proceedings of the 12th European Conference on Computer Systems EuroSys. Belgrade, Serbia, 2017: 222-237

[78] Andreina S, Bohli J M, Karame G O, et al. PoTS—A secure proof of TEE-stake for permissionless blockchains. IACR Cryptology ePrint Archive, 2018: 1135(2018)

[79] Milutinovic M, He W, Wu H, et al. Proof of luck: An efficient blockchain consensus protocol//Proceedings of the ACM 1st Workshop on System Software for Trusted Execution. Trento, Italy, 2016: 2:1-2:6

[80] Zhang F, Eyal I, Escriva R, et al. REM: Resource-efficient mining for blockchains//Proceedings of the 26th USENIX Security Symposium. Vancouver BC, Canada, 2017: 1427-1444

[81] Li W, Andreina S, Bohli J M, Karame G. Securing proof-of-stake blockchain protocols//Garcia-Alfaro J, Navarro-Arribas G, Hartenstein H, Herrera-Joancomartí J, eds. Data Privacy Management, Cryptocurrencies and Blockchain Technology. Lecture Notes in Computer Science, vol. 10436. Berlin, Germany: Springer, 2017: 297-315

[82] Chen L, Xu L, Shah N, et al. On security analysis of proof-of-elapsed-time (PoET)//Spirakis P, Tsigas P, eds. Stabilization, Safety, and Security of Distributed Systems. Lecture Notes in Computer Science, vol. 10616. Berlin, Germany: Springer, 2017: 282-297

[83] Yuan R, Xia Y B, Chen H B, et al. ShadowEth: Private smart contract on public blockchain. Journal of Computer Science and Technology, 2018, 33(3): 542-556

[84] Kosba A, Miller A, Shi E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts //Proceedings of the IEEE Symposium on Security and Privacy (SP). San Jose, USA, 2016: 839-858

[85] Zhang F, Cecchetti E, Croman K, et al. Town crier: An authenticated data feed for smart contract//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security(CCS'16). New York, USA, 2016: 270-282

[86] Juels A, Kosba A, Shi E. The Ring of Gyges: Investigating the future of criminal smart contracts//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security(CCS'16). New York, USA, 2016: 283-295

[87] Cheng R, Zhang F, Kos J, et al. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contract execution//Proceedings of the IEEE European Symposium on Security and Privacy. Stockholm, Sweden, 2019: 185-200

[88] Kaptchuk G, Green M, Miers I. Giving state to the stateless: Augmenting trustworthy computation with ledgers //Proceedings of the Annual Network and Distributed System Security Symposium. San Diego, USA, 2019: 189-190

[89] Parno B, Lorch J R, Douceur J R, et al. Memoir: Practical state continuity for protected modules//Proceedings of the IEEE Symposium on Security and Privacy. Washington, USA, 2011: 379-394

[90] Matetic S, Ahmed M, Kostiainen K, et al. ROTE: Rollback protection for trusted execution//Proceedings of the 26th USENIX Conference on Security Symposium. USENIX Association, Vancouver, Canada, 2017: 1298-1306

[91] Subramanyan P, Seshia S. A formal foundation for secure remote execution of enclaves//Proceedings of the ACM SIGSAC Conference on Computer & Communications Security. Dallas, USA, 2017: 2435-2450

[92] Hähnel M, Cui W, Peinado M. High-resolution side channels for untrusted operating systems//Proceedings of the USENIX Annual Technical Conference (USENIX ATC 17). Santa Clara, USA, 2017: 299-312

[93] Lee J, Jang J, Jang Y, et al. Hacking in darkness: Return-oriented programming against secure enclaves//Proceedings of the USENIX Security. Vancouver, Canada, 2017: 523-539

[94] Volos S, Vaswani K, Bruno R. Graviton: Trusted execution environments on GPUs//Proceedings of the USENIX Symposium on Operating Systems Design and Implementation (OSDI'18). Carlsbad, USA, 2018: 681-696

[95] Partala J. Provably secure covert communication on blockchain. Cryptography, 2018, 2(3): 18

[96] Li Yan-Feng, Ding Li-Ping, Wu Jing-Zheng, et al. Research on a new network covert channel model in blockchain environment. Journal on Communications, 2019, 40(5): 67-78(in Chinese)
(李彦峰, 丁丽萍, 吴敬征等. 区块链环境下的新型网络隐蔽信道模型研究. 通信学报, 2019, 40(5): 67-78)

[97] Neisse R, Steri G, Nai-Fovino I. A blockchain-based approach for data accountability and provenance tracking//Proceedings of the 12th International Conference on Availability, Reliability and Security. Reggio Calabria, Italy, 2017: 14:1-14:10

[98] Chowdhury M J M, Colman A, Kabir M A, et al. Blockchain as a notarization service for data sharing with personal data store //Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. New York, USA, 2018: 1330-1335

[99] Liu Ming-Da, Shang Jing, Liu Peng, et al. VideoChain: Trusted video surveillance based on blockchain for campus//Proceedings of the 4th International Conference on Cloud Computing and Security. Haikou, China, 2018: 48-58

[100] Liang J, Han W, Guo Z, et al. DESC: Enabling secure data exchange based on smart contracts. Science China Information Sciences, 2018, 61(4): 049102:1-049102:3

[101] Zheng B K, Zhu L H, Shen M, et al. Scalable and privacy-preserving data sharing based on blockchain. Journal of Computer Science and Technology, 2018, 33(3): 557-567

[102] Shafagh H, Burkhalter L, Hithnawi A, et al. Towards blockchain-based auditable storage and sharing of IoT data//Proceedings of the 2017 ACM on Cloud Computing Security Workshop. Dallas, USA, 2017: 45-50

[103] Dong Xiang-Qian, Guo Bing, Shen Yan, et al. An efficient and secure decentralizing data sharing model. Chinese Journal of Computers, 2018, 41(5): 1021-1036(in Chinese)
(董祥千，郭兵，沈艳等. 一种高效安全的去中心化数据共享模型. 计算机学报，2018, 41(5): 1021-1036)

[104] Renner T, Müller J, Kao O. Endolith: A blockchain-based framework to enhance data retention in cloud storages// Proceedings of the 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing. Cambridge, UK, 2018: 627-634

[105] Liang X, Shetty S, Tosh D, et al. ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability//Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. Madrid, Spain, 2017: 468-477

[106] Cucurull J, Puiggali J. Distributed immutabilization of secure logs//Barthe G, Markatos E, Samarati P, eds. Security and Trust Management. Lecture Notes in Computer Science, vol. 9871. Berlin, Germany: Springer, 2016: 122-137

[107] Sutton A, Samavi R. Blockchain enabled privacy audit logs//d'Amato C, et al, eds. The Semantic Web — ISWC 2017. Lecture Notes in Computer Science, vol. 10587. Berlin, Germany: Springer, 2017: 645-660

[108] Suzuki S, Murai J. Blockchain as an audit-able communication channel//Proceedings of the 41st IEEE Annual Computer Software and Applications Conference. Turin, Italy, 2017: 516-522

[109] Pourmajidi W, Miranskyy A V. Logchain: Blockchain-assisted log storage//Proceedings of the 11th IEEE International Conference on Cloud Computing. San Francisco, USA, 2018: 978-982

[110] Aniello L, Baldoni R, Gaetani E, et al. A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database//Proceedings of the IEEE 13th European Dependable Computing Conference (EDCC). Geneva, Switzerland, 2017: 151-154

[111] Dagher G G, Mohler J, Milojkovic M, et al. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 2018, 39(2): 283-297

[112] Kai F, Shangyang W, Yanhui R, et al. MedBlock: Efficient and secure medical data sharing via blockchain. Journal of Medical Systems, 2018, 42(8): 136-147

[113] Turkanovic M, Hölbl M, Kosic K, et al. EduCTX: A blockchain-based higher education credit platform. IEEE Access, 2018, 6(1): 5112-5127

[114] Lin Shao-Wei. Regulation by blockchain: The emerging battle for supremacy between the code of law and code as law. Oriental Law, 2019, (3): 121-136(in Chinese)
(林少伟. 区块链监管："法律"与"自律"之争. 东方法学，2019, (3): 121-136)

[115] Chen Chun-Ling, Shen Yang, Yu Han, Decentralized model for credit information system. Computer Technology and Development, 2019, 29(3): 128-132(in Chinese)
(陈春玲，沈阳，余瀚. 去中心化的征信系统模型研究. 计算机技术与发展，2019, 29(3): 128-132)

[116] Tan Hai-Bo, Zhou Tong, Zhao He, et al. Archives data protection and sharing method based on blockchain. Journal of Software, 2019, 30(9): 2620-2635(in Chinese)
(谭海波，周桐，赵赫等. 基于区块链的档案数据保护与共享方法. 软件学报，2019, 30(9): 2620-2635)

[117] An Rui, He De-Biao, Zhang Yun-Ru, et al. The design of an anti-counterfeiting system based on blockchain. Journal of Cryptologic Research, 2017, 4(2): 199-208(in Chinese)
(安瑞，何德彪，张韵茹等. 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)

[118] Tian Hai-Bo, He Jie-Jie, Fu Li-Qing. A privacy preserving fair constract signing protocol based on block chains. Journal of Cryptologic Research, 2017, 4(2): 187-198(in Chinese)
(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)

[119] Xue J, Xu C, Zhao J, et al. Identity-based public auditing for cloud storage systems against malicious auditors via blockchain. SCIENCE CHINA Information Sciences, 2019, 62(3): 32104:1-32104:16

[120] Yang C, Chen X, Xiang Y. Blcokchain-based publicly verifiable data deletion scheme for cloud storage. Journal of Network and Computer Applications, 2018, 103(2): 185-193

[121] Liu Yi-Ning, Zhou Yuan-Jian, Lan Ru-Shi, Tang Chun-Ming. Blockchain-based verification scheme for deletion operation in cloud. Journal of Computer Research and Development, 2018, 55(10): 2199-2207(in Chinese)
(刘忆宁，周元健，蓝如师，唐春明. 基于区块链的云数据删除验证协议. 计算机研究与发展，2018, 55(10): 2199-2207)

[122] Zhao B, Fan P, Ni M. Mchain: A blockchain-based VM measurements secure storage approach in IaaS cloud with enhanced integrity and controllability. IEEE Access, 2018, 6(8): 43758-43769

[123] Park J, Kim K. TM-Coin: Trustworthy management of TCB measurements in IoT//Proceedings of the PerCom Workshops. Kona, USA 2017: 654-659

[124] Wang Jiang, Zhang Ming-Xing, Wu Yong-Wei, et al. Paxos-like consensus algorithms: A review. Journal of Computer Research and Development, 2019, 56(4): 692-707 (in Chinese)

(王江，章明星，武永卫等. 类 Paxos 共识算法研究进展. 计算机研究与发展，2019，56(4)：692-707)

[125] Liu S，Viotti P，Cachin C，et al. XFT：Practical fault tolerance beyond crashes//Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation. Savannah，USA，2016：485-500

[126] Fan Jie，Yi Le-Tian，Shu Ji-Wu. Research on the technologies of Byzantine system. Journal of Software，2013，24(6)：1346-1360(in Chinese)
(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)

[127] Ongaro D，Ousterhout J K. In search of an understandable consensus algorithm//Proceedings of the USENIX Annual Technical Conference. Philadelphia，USA，2014：305-319

[128] Castro M，Liskov B. Practical Byzantine fault tolerance//Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans，USA，1999：173-186

[129] Yuan Yong，Ni Xiao-Chun，Zeng Shuai，et al. Blockchain consensus algorithms：The state of the art and future trends. Acta Automatica Sinica，2018，44(11)：93-104(in Chinese)
(袁勇，倪晓春，曾帅等. 区块链共识算法的发展现状与展望. 自动化学报，2018，44(11)：93-104)

[130] Du Mingxiao，Ma Xiaofeng，Zhang Zhe，et al. A review on consensus algorithm of blockchain//Proceedings of the IEEE International Conference on Systems，Man，and Cybernetics. Banff，Canada，2017：2567-2572

[131] Dinh T T A，Liu R，Zhang M，et al. Untangling blockchain：A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering，2018，30(7)：1366-1385

[132] Kallman R，Kimura H，Natkins J，et al. H-Store：A high-performance，distributed main memory transaction processing system. Proceedings of the VLDB Endowment，2008，1(2)：1496-1499

[133] Jeon J H，Kim K H，Kim J H. Block chain based data security enhanced IoT server platform//Proceedings of the International Conference on Information Networking. Chiang Mai，Thailand，2018：941-944

[134] Qiao Rui，Dong Shi，Wei Qiang，et al. Blockchain based secure storage scheme of dynamic data. Computer Science，2018，45(2)：57-62(in Chinese)
(乔蕊，董仕，魏强等. 基于区块链技术的动态数据存储安全机制研究. 计算机科学，2018，45(2)：57-62)

[135] Nathan S，Govindarajan C，Saraf A，et al. Blockchain meets database：Design and implementation of a blockchain relational database//Proceedings of the 45th International Conference on Very Large Data Bases. Los Angeles，USA，2019：1539-1552

[136] Helmer S，Roggia M，Ioini N. E，Pahl C. EthernityDB—Integrating database functionality into a blockchain//Benczúr A，et al，eds. New Trends in Databases and Information Systems. Communications in Computer and Information Science，vol. 909. Berlin，Germany：Springer，2018：37-44

[137] Muzammal M，Qu Q，Nasrulin B. Renovating blockchain with distributed databases：An open source system. Future Generation Computing System，2019，90(1)：105-117

[138] Jiao Tong，Shen De-Rong，Nie Tie-Zheng，et al. BlockchainDB：A querable and immutable database. Journal of Software，2019，30(9)：2671-2685(in Chinese)
(焦通，申德荣，聂铁铮等. 区块链数据库：一种可查询且防篡改的数据库. 软件学报，2019，30(9)：2671-2685)

[139] El-Hindi M，Binnig C，Arasu A，et al. BlockchainDB：A shared database on blockchains//Proceedings of the 45th International Conference on Very Large Data Bases. Los Angeles，USA，2019：1597-1609

[140] Wang S，Dinh T T A，Lin Q，et al. ForkBase：An efficient storage engine for blockchain and forkable applications//Proceedings of the 44th International Conference on Very Large Data Bases. Rio de Janeiro，Brazil，2018：1137-1150

[141] Ruan P，Dinh A，Lin，et al. Fine-grained，secure and efficient data provenance on blockchain systems//Proceedings of the 45th International Conference on Very Large Data Bases. Los Angeles，USA，2019：975-988

[142] Do H G，Ng W K. Blockchain-based system for secure data storage with private keyword search//Proceedings of the IEEE World Congress on Services. Honolulu，USA，2017：90-93

[143] Zou Qiwu，Tang Yuzhe，Chen Ju，et al. ChainFS：Blockchain-secured cloud storage//Proceedings of the 11th IEEE International Conference on Cloud Computing. San Francisco，USA，2018：987-990

[144] Ruj S，Rahman M S，et al. BlockStore：A secure decentralized storage framework on blockchain//Proceedings of the 32nd IEEE International Conference on Advanced Information Networking and Applications. Krakow，Poland，2018：1096-1103

[145] Chen Yongle，Li Hui，Li Kejiao，Zhang Jiyang. An improved P2P file system scheme based on IPFS and blockchain//Proceedings of the BigData Conference. Boston，USA，2017：2652-2657

[146] Fukumitsu M，Hasegawa S，Iwazaki J，et al. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain//Proceedings of the 31st IEEE International Conference on Advanced Information Networking and Applications. Taipei，China，2017：803-810

[147] Ali S，Wang G，White B，Cottrell R L. A blockchain-based decentralized data storage and access framework for PingER//Proceedings of the 17th IEEE International Conference on Trust，Security and Privacy in Computing and Communications. New York，USA，2018：1303-1308

[148] Li Jiaxing，Wu Jigang，Chen Long. Block-secure：Blockchain based scheme for secure P2P cloud storage. Information Sciences，2018，465(6)：219-231

[149] Li Jiaxing, Liu Zhusong, Chen Long, et al. Blockchain-based security architecture for distributed cloud storage// Proceedings of the IEEE International Symposium on Parallel and Distributed Processing with Applications and IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC). Guangzhou, China, 2017: 408-411

[150] Yin M, Malkhi D, Reiter M K, et al. HotStuff: BFT consensus with linearity and responsiveness//Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC). Toronto, Canada, 2019: 347-356

[151] Gilbert S, Lynch N A. Perspectives on the cap theorem. IEEE Computer, 2012, 45(2): 30-36

[152] Abadi D. Consistency tradeoffs in modern distributed database system design. IEEE Computer, 2012, 45(2): 37-42

[153] Xu Mi-Xue, Yuan Chao, Wang Yong-Juan, et al. Mimic blockchain—Solution to the security of blockchain. Journal of Software, 2019, 30(6): 1681-1691(in Chinese)
(徐蜜雪, 苑超, 王永娟等. 拟态区块链——区块链安全解决方案. 软件学报, 2019, 30(6): 1681-1691)

LIU Ming-Da, Ph. D. candidate. His research interests include information security and blockchain.

CHEN Zuo-Ning, Ph. D., professor, Chinese Academy of Engineering Academician. Her research interests include software theory, operating system and information security.

SHI Yi-Juan, Ph. D., associate professor. Her research interests include information security and blockchain.

TANG Ling-Tao, Ph. D. candidate. His research interest is network security.

CAO Dan, Ph. D., engineer. Her research interests include network security and cryptography.

Background

This research belongs to Information Security and Blockchain area, focusing on the research progress of blockchain in the field of data security. Current data security solutions have varying degrees of centralization limitations in terms of security assumptions, protocol design, and implementation. The blockchain breaks through the shortcomings of the traditional central system architecture, with decentralized, trusted, anonymous, tamper-proof security features, enabling distributed and efficient consensus in large-scale network environments, and establishing a secure and trusted database system. The combination of blockchain and data security can reduce the risk of centralization and has broad academic and application value.

This paper selects a unique research perspectivethat is how to use blockchain in the field of data security. We sort out the new theories, new technologies and new methods generated by the combination of blockchain and existing data security protection technologies, such as searchable encryption, MPC, identity authentication, access control, TEE, covert channel, data manager, distributed storage and so on. We also analysis the problems with these methods and give us the research directions which we think are valuable. Our team has in-depth research in data security, distributed systems cryptography, trusted computing, and blockchain.

This work is supported by the CHB National Science and Technology Major Project of China No. 2017ZX01028101, the National Natural Science Foundation of China under Grant Nos. 91430214, 6732018.