doi: 10.13682/j.issn.2095-6533.2018.01.001

区块链技术:应用及问题

翟社平，段宏宇，李兆兆，高 山，李 婧

（西安邮电大学 计算机学院，陕西 西安 710121）

摘 要：区块链技术使用分布式存储、P2P网络、共识机制、非对称加密和智能合约等关键核心技术，在不可信环境中，建立起一种信息与价值传递交换机制，以保障数据的一致性和完整性，是构建未来价值互联网的基石。区块链技术具有去中心化、安全可靠和公开透明的特点，这使其在点对点交易、文件存储、健康医疗等场景中得到广泛应用。但是，区块链技术依旧存在交易吞吐量低、用户信息和交易数据隐私易泄露以及加密算法安全局限等问题，在其发展和应用过程中亟待解决。作为一项新兴技术，区块链有广阔的发展前景，有望改变互联网治理模式，推动互联网成为新型信用基础设施。

关键词：区块链；去中心化；分布式存储；共识机制；价值互联网

中图分类号：TP391 **文献标识码**：A **文章编号**：2095-6533(2018)01-0001-13

Blockchain: applications and problems

ZHAI Sheping, DUAN Hongyu, LI Zhaozhao, GAO Shan, LI Jing

(School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract: Blockchain technology uses key core technologies such as distributed storage, P2P network, consensus mechanism, asymmetric encryption and smart contract, to establish a reliable transfer exchange mechanism for information and value in an untrusted environment, which ensures the consistency and integrity of the data and lays a foundation for the construction of the future value Internet. The blockchain technology is characterized by decentralization, security, reliability and transparency, which makes it widely used in point-to-point transactions, file storage, health care and other scenarios. However, there are still some problems in blockchain technology, such as low transaction throughput, easy disclosure of user information and transaction data privacy, and security limitations of encryption algorithms, which are urgently needed to be solved in the process of its development and application. As a new technology, blockchain has a broad development prospect, which is expected to change the Internet governance model and promote the Internet to become a new type of credit infrastructure.

Keywords: blockchain, decentralization, distributed storage, consensus mechanism, value Internet

区块链是使用分布式数据库进行识别、传播和记载信息的智能化对等网络，也称价值互联网[1]。区块链技术最初是为了解决传统中心化交易存在的不可信第三方问题所提出的方案，它基于去中心化的对等网络，将密码学原理、时序数据和共识机制相结合，来保障分布式数据库中各节点的连贯和持续，使信息能即时验证、可追溯、难以篡改和无法屏蔽，进而创造了一套隐私、高效、安全的共享价值

收稿日期：2017-11-23

基金项目：陕西省自然科学基金资助项目(2012JM8044)；工业和信息化部通信软科学项目(2017-R-22，2018-R-26)；陕西省社会科学基金资助项目(2016N008)；陕西省教育厅科学研究计划资助项目(17JK0710)；西安市社会科学规划基金资助项目(17X63)；西安邮电大学研究生创新基金资助项目(CXL2016-13，CXJJ2017006)

作者简介：翟社平(1971－)，男，博士，副教授，从事语义计算研究。E-mail：zhaisheping@xupt.edu.cn

段宏宇(1993－)，男，硕士研究生，研究方向为智能信息检索。E-mail：duanhy07@163.com

体系[2]。发展至今，区块链不单局限于数字货币应用，其与大数据、云计算、人工智能等新一代信息技术相结合，在多领域展现出独特的应用价值和市场前景。区块链技术有望改变互联网治理模式，推动互联网成为新型信用基础设施，其在各行业中的应用将深刻颠覆人们的传统生活方式，因此，它将成为世界各国在新一代信息技术领域战略竞争的热点。

详细阐述区块链涉及到的区块数据存储、区块数据传输与同步、节点共识、非对称加密、智能合约等关键技术，对区块链技术的应用场景进行总结，同时从扩展性、安全性、隐私保护三个方面说明区块链技术的现存问题。

1 区块链关键技术

1.1 国内外研究现状

区块链技术的发展大致经历了 3 个阶段：多技术组合创新的起源阶段、以比特币关键技术为代表的区块链技术 1.0 阶段、以智能合约为代表的区块链技术 2.0 阶段。国内外学者针对区块链的底层技术、应用场景及市场监管展开深入研究，探索区块链技术在实际生活中的应用。

国外针对区块链技术的研究开展较早，2014 年，美国以太坊平台 Ethereum 基于区块链为用户提供可编程智能合约开发服务[3]。2015 年，IBM 宣布加入区块链开放式账本。同年，微软公司在 Azure云计算平台的基础上推出了区块链即服务(blockchain as a service，BAAS)[4]。虽然国内区块链起步比国外晚 2 至 3 年，但热度爆发的速度更快。2016 年 2 月，全球首家专注网络空间设施创新的中关村区块链产业联盟在北京成立。2016 年 10 月，工业和信息化部发布《中国区块链白皮书》[5]，这是国内首个落地的区块链官方指导文件。2017 年 3 月，国内首个完全自主知识产权的智能合约平台“信和云”由阿里巴巴与普华永道合作推出。2017 年 4 月，腾讯发布区块链平台 Trust SQL，为上层应用场景提供区块链基础服务。2017 年 9 月，上海保交所发布区块链底层技术平台，为保险行业交易提供区块链基础设施。

从技术发展角度来看，区块链技术正处于发展的期望膨胀期。在行业应用需求的推动下，国内外研究机构也投入大量的人力和财力对区块链技术展开研究。从计算机软件及计算机应用学科角度出发，对国内外高影响因子文献进行分析，在区块链技术综述、区块链技术研究和区块链技术应用三个方面给出分类总结。从表 1 中可以看出，目前区块链的相关文献主要集中于底层技术和应用场景研究，技术综述型文献较少。通过对区块链技术研究型的已有文献来看，研究者们的主要关注点集中在系统框架开发、数据安全和智能化平行区块链三个方面，并有学者指出未来区块链的发展是基于人工智能的平行区块链，这也将是区块链技术驱动的智能产业必然发展趋势。

表 1 区块链文献分析

名称	类别	文献编号	结论分析
技术综述型	技术发展综述	[6-8]	介绍区块链的研究现状和发展前景，对相关重要技术的发展进行概述。
	技术研究综述	[9-11]	
技术研究型	系统框架开发研究	[12-16]	从底层技术出发，主要研究内容包括系统开发方法、系统结构、数据安全和共识、存储容量、可扩展性和智能化平行区块链等。
	数据安全性研究	[17-21]	
	智能化平行区块链研究	[22-27]	
技术应用型	技术应用场景研究	[28-38]	针对区块链在金融、新能源、可信数据管理、供应链管控与溯源、电子取证和个人隐私保护等方面的应用进行分析。

1.2 分布式数据存储技术

相比于传统分布式系统数据分散存储、极易遭受网络攻击的特性[39]，区块链采用分布式数据存储技术，以特殊的链式结构存放数据，只提供写、读权限，不允许修改和删除，并且全网中每个节点都保存完整数据的副本，单节点故障并不影响系统运行，同时区块链的链式结构使得所有数据都可追踪，数据安全性得到较大提高[40]。区块链可描述为一个由多个节点组成的分布式数据存储系统，它将一段时间内的交易以 Merkle 树形式组织，将数据和代码封装形成区块，按照时间顺序依次组织区块，同时利用密码学原理保证了数据不可篡改和伪造。区块链的分布式存储涉及区块结构、Merkle 树、时间戳和 SHA256 算法等关键技术。

区块是包含区块链全网数据信息的一种数据结构，由包含元数据的数据头和包含所有交易数据

的区块体共同组成[41]。

区块的字段结构如表 2 所示,前一区块哈希是区块成链的关键字段,该字段是对上一个区块的数据信息进行哈希运算所得的结果,各个区块利用该哈希值依次连接,形成从创世区块到当前区块的一条最长主链,记录了完整的区块链数据信息,提供区块链数据的溯源和定位功能,区块链的链式结构如图 1 所示。

表 2　区块数据结构表

结构	字段	说明
区块头	前一区块哈希	父区块的哈希值,通过这个值每个区块首尾相连组成区块链
	随机数	记录解密该区块相关数学题的答案的值
	时间戳	记录区块产生时间,精确到秒
	难度目标	区块相关数学题的难度目标
	Merkle 根	该区块中所有交易的 Merkle 树根的哈希值
区块体	交易列表	所有交易数据的具体信息,以 Merkle 树组织

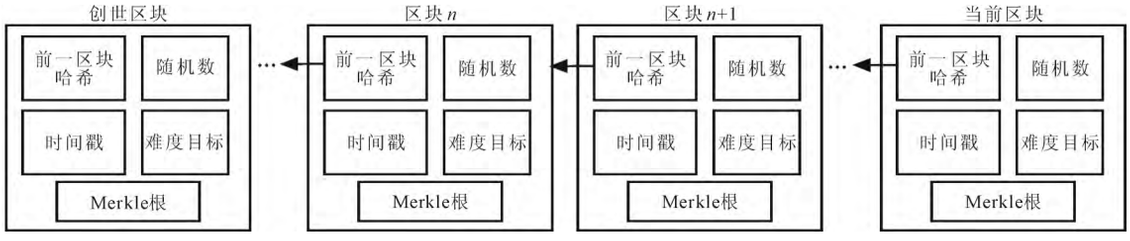

图 1　区块链链式结构

SHA256 是一种求哈希值的加密算法,任何一串数据经过 SHA256 运算得到 256 位的 Hash 值[42]。相同的数据输入将得到相同的结果,输入数据只要稍有变化则得到完全不同的结果,正向计算(由数据计算相应的 Hash 值)十分容易,逆向计算(由 Hash 计算出相应的数据)非常难。区块链不直接保存原有数据和交易记录,而是将原始交易记录经过散列运算,得到一定长度的散列值,将这串字母与数字组成的定长字符串记录到区块。区块链使用双 SHA256 散列函数,将任意长度原始交易记录经过 2 次 SHA256 散列运算,得到一串 256 位的散列值,便于存储和查找[43]。同时,SHA256 函数也用于区块链的工作量证明,系统中所有节点寻找一个随机数,使新区块头的双 SHA256 散列值小于或等于目标散列值,并加入难度值,使区块相关数学问题的解决时间平均为 10 分钟,进而使得区块链系统的出块时间维持在 10 分钟,保证区块链系统的稳定性。

时间戳以 Unix 纪元为时间编码,采用精确的时间源、高强度高标准的安全机制,以确认区块链系统处理数据在某一时间的存在性和相关操作的相对时间顺序,为区块链系统中的时间防抵赖提供基础服务[44-45]。时间戳表示区块链中的数据在某个特定时间之前就已经存在,且数据完整、可验证、可追溯,区块链系统中每一个区块生成时都必须加盖时间戳才可以向全网广播。时间戳作为区块数据的存在性证明有助于形成不可篡改、不可伪造的分布式账本,还为未来基于区块链技术的互联网和大数据增加了时间维度,使通过区块链数据和时间戳来重现历史成为可能。

Merkle 树是一种哈希二叉树,最初是由著名的密码学家 Merkle 提出的,用于快速校验大规模数据的完整性[46]。Merkle 树极大地提高了区块链的运行效率和可扩展性,使得区块头只需包含哈希值而不必封装底层数据。另外,Merkle 树的查找算法简单,即在不需要运行完整区块链网络节点的情况下,也能对数据进行检验,极大地降低了运行时的资源占用。在区块链系统中,使用 Merkle 树组织交易数据,提供交易数据的快速追踪,其构建过程自底向上。

如图 2 所示,首先对某时间段内的交易数据分别进行哈希运算得到对应哈希序列,将哈希序列存储至相应叶子节点中,对相邻叶子节点的哈希值进行哈希运算,如此递归操作直至只剩顶部的一个节点,即 Merkle 根,并将该节点记入区块头中[47-48]。

Merkle 构建算法可描述如下。

输入　交易数据

输出　Merkle 根哈希值

步骤 1 对交易数据做双重 SHA256 运算，即

$$Node_{0i} = SHA256(SHA256(Data_{0i}))$$

$(i=1,2,3,4)$。

步骤 2 相邻两个 Hash 块串联，进行双重 SHA256 运算。

步骤 3 递归操作步骤 2，直至只剩顶部一个结点。

步骤 4 返回 Merkle 根哈希。

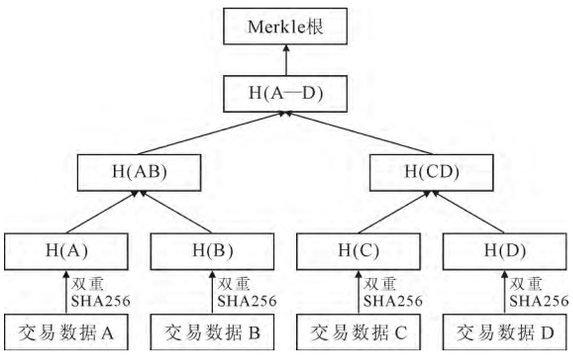

图 2 Merkle 树

哈希算法、时间戳、Merkle 树是区块头的重要组成部分，交易数据则是区块体存储的重要信息。区块链综合应用多种技术就是为了确保新交易数据的快速生成、安全传播和有效验证，并且最终添加至整个分布式总账即区块链中，全网每个节点都拥有总账的副本以确保交易数据一致可靠且不可篡改。在区块链交易系统中，交易的基本单位被定义成未花费交易输出(unspent transaction output，UTXO)，指记录于区块链系统中的无法再细分、被所有者“锁住”并被整个网络识别成货币单位的一定量的货币。每一个交易可以分为交易输入和交易输出两部分，交易输入和交易输出包含用来验证交易合法性的脚本。输出脚本明确了下一笔交易取得当前 UTXO 使用权的条件，又称锁定脚本，通常包含公钥的哈希。输入脚本说明了锁定脚本在其交易输出上所设定的花费 UTXO 的条件，又称解锁脚本，通常含有一个由用户私钥生成的数字签名。在交易验证阶段，需要将两个脚本组合在一起，以堆栈执行引擎形式进行验证，只有组合脚本验证通过，包含在交易中的 UTXO 才可以被使用，才可以证明交易有效，从而保证了全网中所有数据一致可信。

1.3 对等网络可靠性传输技术

区块链网络采用对等网络(peer to peer，P2P)[49]技术实现了分布式节点间通信与数据传输。不同于传统中心化网络模式，区块链系统中每个节点拥有相同的数据操作权限，以扁平式拓扑方式相互连通和交互，不存在任何中心化的特殊节点和层级结构。所有节点之间均通过特定的软件协议共享部分计算资源、软件或者信息内容，每个节点均会承担网络路由、验证交易信息、传播交易信息、发现新节点等工作[50]。P2P 网络技术是构成区块链技术基础架构的核心技术之一，区块链节点间连接的建立以及节点间数据通信都基于 P2P 技术。

区块链网络中的通信是靠对等节点响应确认并建立连接实现的，网络中的对等节点利用 verack 消息对 version 消息确认并建立连接，如果接收节点需要互换连接并连回起始节点，也会传回该对等节点的 version 消息，如图 3 所示。区块链网络中没有特殊节点，但客户端会维持一个列表，列出了长期稳定运行的节点，这样的节点被称为“种子节点”。新节点并不一定需要与种子节点建立连接，但可以通过连接到种子节点来快速发现区块链网络中的其他节点。在区块链客户端中，起始时将至少一个区块链节点的 IP 地址提供给正在启动的节点(该节点不包含任何区块链网络的组成信息)[51]。在这之后，启动节点可以通过后续指令建立新的连接，用户可以使用命令行参数把启动节点“引荐”并连接到一个节点，并将该节点用作 DNS 种子。在种子节点被用于形成“引荐”信息之后，客户端会断开与它的连接、并与新发现的对等节点进行通信。

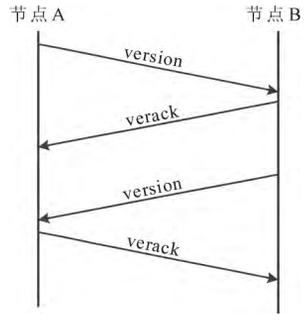

图 3 对等节点“握手”通信

区块链网络使用广播的方式传播交易信息，当建立一个或多个连接后，新节点将一条包含自身 IP 地址的 addr 消息发送给其相邻节点。相邻节点再将此条 addr 消息依次转发给其各自的相邻节点，从而保证新节点信息被多个节点所接收，保证连接更稳定。另外，新接入的节点可以向它的相邻节点发送 getaddr 消息，要求它们返回其已知对等节点的 IP 地址列表。通过这种方式，节点可以找到需要连接到的对等节点，并向网络发布它的消息以便其他节点查找，图 4 描述了这种地址发现过程。

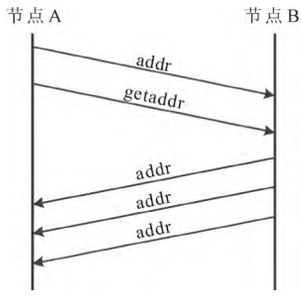

图 4　地址广播发现

1.4　共识机制

共识机制在去中心化的思想上解决了节点间互相信任的问题,使得区块链系统的节点达成一致,有效避免了分布式系统的网络延迟、传输错误、黑客入侵等问题[52]。目前常用的共识机制有工作量证明(proof of work,POW)、权益证明(proof of stake,POS)、股份授权证明(delegated proof of stake,DPOS)、实用拜占庭容错(practical byzantine fault tolerance,PBFT)等。

POW 是区块链系统最早使用的共识机制之一,它通过引入分布式系统的强大算力来达成共识。区块链的共识的达成实质上是新区块的生成过程,所有参与"挖矿"的节点都在遍历寻找一个随机数,这个随机数使得当前区块的区块头的双 SHA256 运算结果小于或等于某个值,找到符合要求随机数的节点获得当前区块的记账权,负责将一定时间内的交易数据打包形成新区块,并广播至全网,从而获得一定数额的 Coinbase 奖励[53],工作量证明过程如下。

(1) 将当前阶段全网交易打包进区块,组成交易列表,通过 Merkle 树构建算法生成 Merkle 根哈希。

(2) 把 Merkle 根哈希及其他相关字段组装成区块头,将区块头的 80 字节数据作为工作量证明的输入记为 Block_Header,随机数初始值置 0。

(3) 不断变更随机数的数值,并对每次变更后的的区块头做双重 SHA256 运算(即 SHA256(SHA256(Block_Header))),将结果值与当前网络的目标值做对比,如果小于目标值,则解题成功,工作量证明完成[54]。区块链系统规定每经过 2016 个区块对难度目标进行调整,使得每个区块的生成时间保持在 10 分钟,新难度目标的计算公式为

$$T_{new}=T_{old}\times\frac{T_{total}}{2016\times10}。$$

其中,T_{new} 是新难度目标,T_{old} 是旧难度目标,T_{total} 指过去 2016 个区块的生成总时间。目标难度的调整由区块链系统自行完成,保证了系统的稳定性。

POS 是为解决 POW 共识的资源浪费和安全性缺陷而提出的替代方案,它采用权益证明来代替 POW 中工作量证明,由系统中具有最高权益而非最高算力的节点获得区块记账权[55]。POS 是根据钱包里面货币的多少以及货币在钱包里存在的天数来合成一个单位,称为"币天",钱包里的币天数越大的节点拥有记账权的概率就越大[56]。POS 机制仅依靠内部币龄和权益而不需要消耗外部算力和资源,从根本上解决了 POW 共识算力资源浪费的问题,但同时丢弃了 POW 的一些优势,因此更容易造成分叉[57],一笔交易需要等待更多确认才能确保安全,链中数据有极大可能被篡改,存在一定的安全隐患。

DPOS 是基于 POS 衍生出的更专业的解决方案,是类似于董事会的投票机制,由全网所有持有数字货币的人投票选举出 n 个记账节点,在节点中提案者提交的提案被这些记账节点投票决定谁是正确的[55]。被选出的特权节点不具备永久性,一旦在生成区块的时候由于网络故障、节点宕机、恶意行为等原因未能生成,节点被除名,再次选举新节点来替代,除名选举在系统中时刻进行。DPOS 共识机制中,每个节点都能自主决定其信任的授权节点并由这些节点轮流记账生成新区块,因而大幅减少了参与验证和记账的节点数量,可以实现快速验证,但是一定程度上失去了去中心化的概念。

PBFT 是一种采用许可投票、少数服从多数来选举领导者进行记账的共识机制,但此共识机制允许容错。该共识机制允许强监管节点参与,具备权限分级能力,性能更高且耗能更低,每轮记账都会由全网节点共同选举领导者,允许 33% 的节点作恶,容错性为 33%。PBFT 机制共识效率高,可实现高频交易,但当系统只剩下 33% 的节点运行时,系统会停止运行。

以上四个共识机制各有优缺点,其中 POW 机制是去中心化程度最高的共识机制,DPOS 机制可以理解为多中心化的机制。区块链系统开发者往往结合实际应用场景选择合适的共识机制,其特点对比如表 3 所示。

表 3　共识机制特点对比表

共识机制	POW	POS	DPOS	PBFT
完全去中心化	√	×	×	×
承载更多交易量	×	×	√	√
更快的确认速度	×	×	√	√
高效节能	×	√	√	√

1.5 非对称加密机制

非对称加密是为满足安全性需求和所有权验证需求而集成到区块链中的加密技术，在加密和解密过程中使用两个非对称密码，称为公钥和私钥。公钥可公开发布，用于发送方加密要发送的信息，私钥用于接收方解密接收到的加密内容。常见的非对称加密算法有 RSA 算法、Elgamal 算法、椭圆曲线密码(elliptic curves cipher，ECC)等[58]。在区块链系统中，使用 RSA 进行数字签名、数字加密，使用椭圆曲线加密算法生成区块链系统交易地址。

区块链使用数字签名确认消息是由发送方签名并发出的，信息发送者用自己的私钥对待发送信息进行加密发送给接收者，接收者采用发送者对应的公钥对加密信息进行解密获得原始信息[59]。以图 5“交易 2”为例，“交易 2”的签名过程是付款人(用户 1)来完成的，用已经公开的收款人(用户 2)的公钥加密上一笔交易单数据，算出哈希值 x，付款人(用户 1)用付款人私钥对 x 进行加密，得到付款人(用户 1)签名，将付款人签名附加在交易单中，发给收款人(用户 2)。

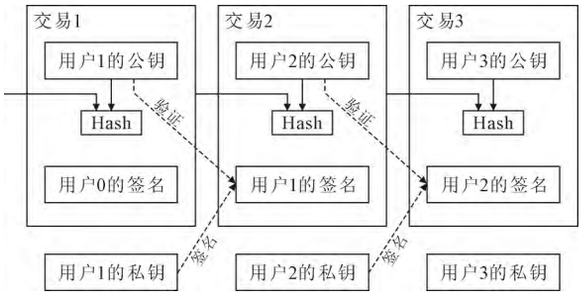

图 5 交易签名和验证过程

区块链通过交易验证确认交易单是否有效。交易的接收方会首先验证交易的有效性。以图 5“交易 2”为例，验证过程是收款人(用户 2)来完成的，用公开的付款人(用户 1)的公钥来解密用户 1 的私钥，进一步解密付款人(用户 1)的签名，得到哈希值 x。收款人(用户 2)利用自己的公钥和上一交易单的数据进行哈希计算，也得到另一个散列值 y。如果这个 y 和之前交易签名的 x 一样，交易单有效。

区块链系统的交易地址标识的生成过程如图 6 所示，系统首先使用随机数生成器生成一个 256 位二进制随机数作为私钥，该私钥不直接提供给用户，对其进行 SHA256 哈希运算生成 256 位的哈希序列，之后经区块链自定义方案即 Base58Check 编码方案将哈希值和校验数据转换为一种字母-数字表示，形成 50 字符长度的易识别字符提供给用户。二进制公钥通过 Secp256k1 椭圆曲线加密算法生成 65 字节的非压缩公钥，该非压缩公钥被定义成一个点，即 $K=(x,y)$，生成过程是

$$K=k*G,$$

其中 k 是二进制私钥，G 是椭圆曲线的中被称为生成点的一个常数点，定义为

$$G=0279\text{BE}667\text{EF}9\text{DCBBAC}55\text{A}0$$
$$6295\text{CE}870\text{B}07029\text{BFCDB}2\text{D}$$
$$\text{CE}28\text{D}959\text{F}2815\text{B}16\text{F}81798,$$

K 是所得公钥，“$*$”则是椭圆曲线乘运算[60]。该公钥用来生成区块链系统的交易账户地址标识[61]，首先对公钥进行两次 SHA256 哈希运算，得到一个 32 字节的字符串，取运算结果的前 4 字节作为公钥哈希的校验码，将其链接在 20 字节公钥的尾部，最后对得到的 24 字节字符串进行 Base58 编码转化，形成 33 字符的交易地址标识。

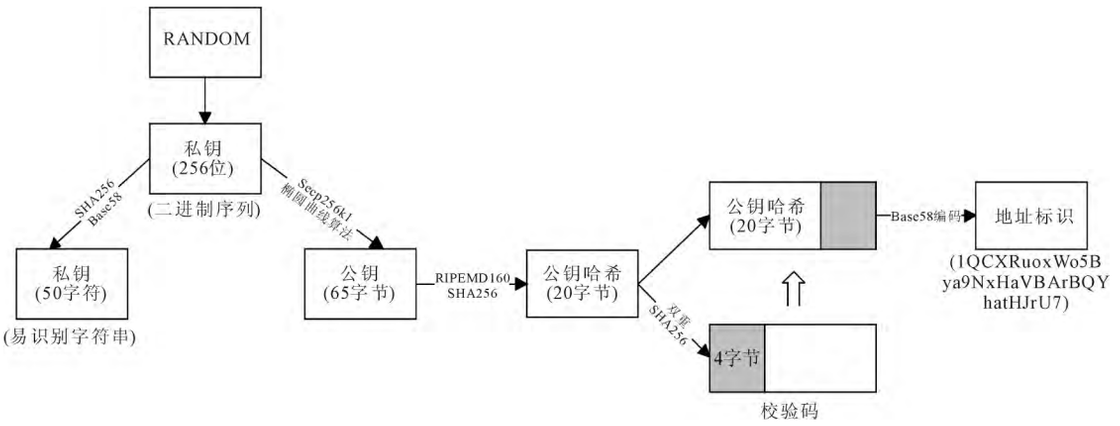

图 6 交易地址生成过程

1.6 智能合约

智能合约是 1994 年由计算机科学家加密大师尼克·萨博首次提出的概念，当时计算程序很难控制现实世界资金的转移导致智能合约没有得到很好的应用。区块链技术的出现不仅可以支持可编程合约，而且具有去中心化、不可篡改、过程透明、

可追踪等优势特征,完全适用于智能合约。区块链系统中的智能合约技术是一个能够自动执行合约条款的计算机化程序[62],智能合约以代码和数据集合的形式存储在区块链上,通过区块链节点在时间或事件的驱动下以分布式的方式执行,所有相关条款都由代码编成,能够进行自动结算,通过签名或其他外部数据信息触发事件来执行。

智能合约是能够使区块链技术应用到现实的关键技术,区块链技术中的智能合约包括事务处理和保存的机制以及一个完备的状态机,事务的保存和状态处理都在区块链上完成,状态机用于接受和处理各种智能合约。事务主要包含需要发送的数据及对这些数据的描述信息,事务信息传入智能合约后,合约资源集合中的资源状态会被更新,进而触发智能合约进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足,则由状态机根据预设信息选择合约动作自动执行。基于区块链的智能合约构建及执行分为如下几步,如图 7 所示。

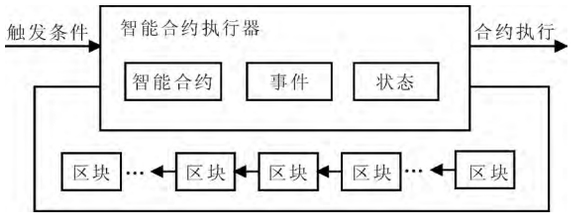

图 7　智能合约运作机制

(1) 多方用户共同参与制定一份智能合约,包含了双方的权利和义务,以电子化的编程机器语言方式发布,参与者分别用各自私钥进行签名以确保合约的有效性。

(2) 合约通过 P2P 的方式在区块链全网中扩散,区块链中的验证节点会将收到的合约先保存到内存中,等待新一轮的共识时间,触发对该份合约的共识和处理,最终达成一致的合约集合会以区块的形式扩散到全网。

(3) 智能合约会定期检查自动机状态,逐条遍历每个合约内包含的状态机、事务以及触发条件,满足触发条件的合约将自动执行。

基于区块链技术的智能合约不仅可以发挥成本效率方面的优势,而且可以避免恶意行为对合约正常执行的干扰。将智能合约以数字化的形式写入区块链中,由区块链技术的特性保障合约的存储、读取、执行的整个过程透明可跟踪且不可篡改,同时,由区块链自带的共识机制所构建的状态机系统可以保证智能合约高效运行。

2　区块链技术应用场景

区块链在应用层面具有安全可靠、公开透明和自动化的特点,这些特点推动其应用场景从最初单纯的数字货币过渡到更广泛的金融行业,并且已经延伸至社会系统中的多个领域。列举出点对点交易、文件存储、健康医疗、电子存证、版权管理和农产品溯源六个应用场景,对区块链技术在这些场景中的实现进行阐述。

(1) 点对点交易

基于区块链系统的点对点交易无需第三方中介机构参与,消费者能够自由地进行生产和交易,大幅减少信息传递过程中出现的错误,提升信息传输效率[63]。这种交易模式通过计算机程序自动确认执行双方交易结果,即交易确认和清算结算在同一时间完成,极大提高了金融交易和结算效率。在区块链点对点交易机制中,非对称加密算法和数字签名机制保障了交易账户的有效性,工作量证明机制实现了记账权的公正性,交易参与者可在区块链上凭借数字签名启用唯一对应的账户进行交易,其交易信息将被随机的第三方角色记录进区块链永久储存起来,而所有交易顺次相关联的链条式记录保障了交易的可追溯性和防篡改。区块链技术应用于点对点交易系统绕过了代理行、中央托管等机构,完善了交易双方的通讯方式,消除交易对第三方的依赖,提高了交易效率,增加了数据安全性,使得交易市场信息更加透明化。

(2) 文件存储

当前文件存储模式极易消耗资源、效率低下且容易窃取,将区块链技术和云计算相结合,可以实现基于区块链的分布式数据存储,以一种安全、高效、廉价的方式来存储数据,将数据散布在许多节点上,以密码学原理保障数据安全。所有用户数据进行碎片化处理,分割成单位区块保存,将用户关键元数据信息保存至区块链中,使用加密算法对用户敏感信息进行加密以保障隐私。北京邮电大学区块链研究实验室提出一种基于区块链的云计算电子取证模型,设计适用于取证的区块数据结构,设计改进的 PBFT 共识算法,有效地对电子证据信息进行保全和验证,保障取证数据的完整性和实效性[32]。另外,分布式文件云存储服务运营商 Sia 发布了一款基于区块链的数据存储协作云服务[64],该平台具有自动化点对点的特性,允许用户在可靠的

安全协议下定制存储计划。平台将用户数据分散存储在众多节点上，数据可以被自动化智能合约追踪，同时由多阶段进程提供保护，并用加密算法 Twofish 加密，实现了一个非信任的、具有容错能力的文件存储服务。

(3) 健康医疗

区块链技术应用于医疗领域可以解决病历隐私泄露、数据共享不安全、保险索赔的低效等问题，其可追溯的特点及其分布式存储技术可以把医疗机构之间孤立的数据连接起来。利用区块链技术存储医疗数据，对数据添加时间戳字段保障来源，实现病历泄露源精准定位、电子病历的多方查看权限，确保数据不被篡改，有助于精准医疗，易于医疗数据扩展，最终实现医疗数据的安全有序共享。研究者针对各医疗机构间共享数据困难的问题，利用区块链技术构建了一个基于区块链的医疗数据共享模型，在将病人隐私信息加密存储的前提下提出分层存储的思想，在对现有医疗机构进行分类的基础上配合使用改进的共识机制实现了方便、安全、快捷的医疗数据共享。在实际应用中，雷盈科技公司团队开发出“超级医疗账本”项目[65]，将病历信息加密保存在区块链中，设置一定的访问控制策略，跨院医生需经病人同意才可调取电子病历，旨在将病历数据转化加密数字资产，建造健康档案共享与数据流通系统。

(4) 电子存证

区块链电子存证系统以区块链作为底层技术，解决互联网世界中电子数据的易变性、无痕性和不易归档性等固有问题，让电子数据可证明、可追溯、可信赖。区块链存证是将需要存证的信息加上随机数生成哈希值[66]，再由利益相关人或见证人签名并生成哈希，最后记录在区块链上。用户可以将电子文件的签署时间、签署主体、文件哈希值等的数字指纹信息同步保存至区块链，司法鉴定中心与公证处等机构作为认证节点接入区块链，广播某个电子凭证的哈希，实现链上存证，提供法律效力，防范电子文件毁损或丢失造成的法律风险，保障参与方的权益。除司法机构之外的节点完成实名认证、模板处理、文件合并等各种业务功能，可以实现链上直接验证凭证真伪；一旦产生纠纷，用户下载电子文件全文，将文件数据与之前存证的数据进行比对后，即可生成相应的鉴定报告，维护自身合法权益。区块链中存储的电子文件都会进行加密处理，即使数据被黑客窃取，黑客也无法解密获取原始数据，这样提高了数据存证的安全性。

(5) 版权管理

现有的版权管理大多是基于中心化的网站，存在内容不精确、容易遭受攻击、没有严格可信的可追溯性等缺点，而区块链技术与逐渐增强的版权保护意识不谋而合。区块链技术的时间戳和非对称密码学加密的特性保证了区块数据不能被伪造和篡改，上传至区块链的每一个信息区块都拥有自己独有的时间戳和哈希值，版权所有人对于版权的每次交易活动如授权、分发、跟踪、使用、销毁等都会根据时间形成一条独一无二的副链，这为版权纠纷的举证提供了有力帮助。同时分布式存储让区块链具有了透明性和公开性，只要进行过区块链注册的人，均可知道作品的归属权等相关信息。区块链技术还为版权所有者提供了可编程的脚本系统，版权所有者可以灵活设置条件来对版权进行授权，例如通过智能合约，版权所有者可以设置通过支付一定数量的货币后，支付人可以获得一个拥有查看作品权限的私钥。国外已经有公司利用区块链技术实现音乐版权的管理，可以追踪用户购买音乐的全记录。基于区块链技术的 Colu 公司在区块链的基础上建立了一个平台[67]，为数字资产的发行和分配提供安全渠道，包括音乐作品的上市和注册，能够为所有市场参与者提供更高的透明度和效率。

(6) 农产品溯源

基于区块链的农产品溯源综合利用区块链技术以及物联网智能设备和防伪技术，打通底层区块链技术和物联网智能硬件数据，实现实时记录农产品生长信息，把采集的数据实时同步上链，并接入生态联盟链，追溯整个农产品的成长过程。区块链能够围绕核心企业搭建一条包括制造商、供应商、零售商、物流公司、消费者在内的信息联盟，并将资金流、信息流、货物流等信息都记录在这链条上。在整个生产链上，从农产品的供应源、培养基地，到加工厂、检疫部门、物流企业等环节不再存在信息壁垒，所有信息都通过区块链进行流转，并通过共识算法保证信息的不可篡改，完全真实可靠。将区块链技术运用于物联网农产品，为物联网农产品追溯提供新的解决思路，为推进农产品溯源真实可靠、方便查询、不可复制等方面产生巨大作用。

基于区块链技术的应用不局限于以上六个场景，区块链技术将重新定义整个世界，新业态、新模式将不断衍生。可以说，区块链技术是建立价值互联网的基础，将实现价值在互联网上的自由流通。

3　区块链技术面临的问题

随着区块链技术的广泛应用与研究的不断深入,区块链技术所存在的一些问题逐渐显现,如区块链大小与系统交易吞吐量的不平衡、数据安全存在隐患、数据隐私较难保障等。从区块链的设计和需求出发,探讨区块链技术的特征,揭示它在系统可扩展性、系统安全性和隐私保护等方面的问题。

3.1　扩展性问题

如今加密货币领域面临的最大问题就是扩展性问题[68],对于区块链的实现框架,扩展性主要包括两个方面,一是区块存储的扩展,另一个是提升交易吞吐量的扩展程度。区块链的数据通常是只能追加记录,而不能修改和删除记录。针对之前数据有误的情况,需要在现有数据链中增加一条新数据,并且再增加一条声明,表明前述记录添加有误,才能保存完整数据。只有数据完整,新加入的节点才有能力对全网的完整交易历史进行验证,而无须信任其他节点。这种机制为区块链的去中心化机制提供了便利,但是也影响了系统的可扩展性。另外,目前主流的支付处理商例如 Visa 信用卡可以处理 2000 笔交易/秒,最高可达 56000 笔交易/秒,当前区块链网络每秒只能处理 7 笔。如果单纯调整区块链中区块的大小,使得每个区块可以存放更多交易数据,显然可以提高交易吞吐量。然而区块数据量增大将导致单个用户节点不能运行完整的区块链节点,只有可以负担起全节点资源消耗的商业机构才可以运行完整节点。全网的算力将集中在部分实体机构中,这些实体可以共谋对区块链进行恶意攻击或篡改以谋求自身利益最大化。在网络节点数目足够多的情况下,全网可以保证抵御 51%攻击,然而节点数目增多,网络中节点间交互和通信会占用更多网络资源,这导致区块链网络处理速度的降低。悉尼大学构建出一个在公有和私有环境中工作的区块链,称作“红腹区块链”,使交易能够以点对点的方式进行,也能够在仅限于特定用户的行业环境中进行,进而使得该区块链可以在 100 台机器上每秒处理超过 44 万次的交易[69],但该区块链仍处于实验阶段,尚未投入使用。因此区块链的开发者应考虑如何设计一个高性能的区块链,在保证安全性和网络正常运行的前提下提高交易效率。

3.2　安全性问题

区块链技术虽然基于密码学原理,但并非绝对安全,主要可以从区块链加密算法、区块链节点间的共识协议与区块链公私钥使用安全性几个方面考虑。在算法层面,以目前我国天河二号的算力来说,产生区块链 SHA256 哈希算法的一个哈希碰撞大约需要 248 年,但随着量子计算机等新计算技术的发展,NP 完全问题的破解将成为可能[70]。协议方面,基于 POW 共识过程的区块链主要面临的是 51%攻击问题,即节点通过掌握全网超过 51%的算力就有能力成功篡改和伪造区块链数据。51%算力是考虑到区块链中攻击者用更大代价的货币来换取较小价值的收益是不划算的,但区块链应用前景广阔,不排除攻击者为了某种目的不惜成本地攻击,且理论上技术手段可实现。使用安全性方面,区块链技术一大特点就是不可逆、不可伪造,但前提是私钥是安全的。私钥是用户生成并保管的,没有第三方参与,私钥一旦丢失,便无法对账户的资产做任何操作,同时也无法排除私钥被他人窃取从而造成数据隐私泄露的情况。区块链大量应用了各种密码学技术,属于算法高度密集工程,在实现上比较容易出现问题,The DAO 项目被攻击就是一个典型的例子,2016 年由于其智能合约中存在漏洞而被黑客攻击,损失达到 6000 万美元,本次攻击是通过代码的递归调用攻击合约漏洞实现的,是对于区块链去中心化信任机制的一次严峻问题。针对区块链系统的各种安全问题,应考虑综合应用密码学技术、网络安全技术从算法、协议、使用和实现方面提高区块链安全性,应对现存的安全问题。

3.3　隐私保护问题

区块链系统中的隐私一般分为身份隐私和交易隐私两类,身份隐私是指用户身份信息和区块链地址之间的关联关系,交易隐私是指区块链存储的交易记录和交易记录背后的知识。相对于传统的中心化架构,区块链机制不依赖特定中心节点处理和存储数据,因此能够避免集中式服务器单点崩溃和数据泄露的风险,然而随着区块链技术不断发展和广泛应用,其面临的隐私泄露问题越来越突出。用户在使用区块链地址参与区块链业务时,有可能泄露一些敏感信息,区块链系统中通过账户地址标识实现数据或交易的传输,而一个地址的统一性无法掩盖,不同地址之间稳定的关联交易也有迹可

循，例如区块链交易在网络中的传播轨迹，这些信息有可能被用户推测区块链地址对应的真实身份。此外，交易记录通常能反映一些敏感数据，有可能泄露用户的隐私，例如在数字货币应用中，分析人员通过分析交易记录可以获得用户的交易规律，甚至能推测出用户的身份信息、消费水平、位置信息及生活状态等。身份隐私和交易隐私是用户在使用区块链技术时需要重点保护的内容，这些信息一旦泄露有可能对用户造成巨大威胁。为了实现对这些数据的隐私保护，可以采用基于属性的密码访问控制技术，将一般访问控制技术同密码学工具相结合，实现对访问对象的安全访问。

4 结语

作为一种全新的去中心化基础架构与分布式计算范式，区块链在全球范围内受到广泛关注。首先，从技术角度来讲，区块链通过共识机制保证全网就区块信息达成一致共识，网络中对等节点结合非对称加密机制共同维护区块链系统的安全可靠。其次，区块链去中心化、公开透明和自动化的特点消除了对第三方中介机构的需求，这将促使区块链技术应用到更多的实际业务场景之中。最后，问题与机遇并存，区块链有望成为智能技术时代的新动力和新引擎，实现从信息互联网向价值互联网、秩序互联网的转化，并在多领域产生颠覆性变革。

参 考 文 献

[1] 赵刚. 区块链：价值互联网的基石[M/OL]. 北京：电子工业出版社，2016：1-245[2017-10-07]. http://www.phei.com.cn/module/goods/wssd_content.jsp?bookid=46766.

[2] AHRAM T, SARGOLZAEI A, SARGOLZAEI S, et al. Blockchain technology innovations[C/OL]//2017 IEEE Technology & Engineering Management Conference (TEMSCON). Santa Clara: IEEE, 2017: 137-141[2017-10-08]. https://doi.org/10.1109/TEMSCON.2017.7998367.

[3] JAN. 以太坊(Ethereum)：下一代智能合约和去中心化应用平台[EB/OL]. (2015-11-03)[2017-10-08]. http://ethfans.org/posts/ethereum-whitepaper.

[4] 恒亮. 微软区块链服务(BaaS)正式开放基于 Azure 云平台[EB/OL]. (2016-08-04)[2017-10-08]. https://www.leiphone.com/news/201608/kLuLemLh6QNLmnBU.html.

[5] 中国大数据产业观察. 首份《中国区块链技术和应用发展白皮书(2016)》发布[EB/OL]. (2016-10-21)[2017-10-08]. http://www.cbdio.com/BigData/2016-10/21/content_5351215.htm.

[6] 袁勇，王飞跃. 区块链技术发展现状与展望[J/OL]. 自动化学报，2016，42(4)：481-494[2017-10-08]. http://mall.cnki.net/magazine/article/MOTO201604001.htm. DOI：10.16383/j.aas.2016.c160158.

[7] 何蒲，于戈，张岩峰，等. 区块链技术与应用前瞻综述[J/OL]. 计算机科学，2017，44(04)：1-7[2017-10-14]. http://dx.chinadoi.cn/10.11896/j.issn.1002-137X.2017.04.001.

[8] 沈鑫，裴庆祺，刘雪峰. 区块链技术综述[J/OL]. 网络与信息安全学报，2016，2(11)：11-20[2017-10-08]. http://dx.chinadoi.cn/10.11959/j.issn.2096-109x.2016.00107.

[9] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C/OL]//2017 IEEE International Congress on Big Data (BigData Congress). Honolulu: IEEE, 2017: 557-564[2017-10-08]. https://doi.org/10.1109/BigDataCongress.2017.85.

[10] 祝烈煌，高峰，沈蒙. 区块链隐私保护研究综述[J/OL]. 计算机研究与发展，2017，54(10)：2170-2186[2017-10-08]. http://dx.chinadoi.cn/10.7544/issn1000-1239.2017.20170471.

[11] DU M X, MA X F, ZHANG Z, et al. A review on consensus algorithm of blockchain[C/OL]//2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Banff: IEEE, 2017: 2567-2572[2017-10-08]. https://doi.org/10.1109/SMC.2017.8123011.

[12] 蔡维德，郁莲，王荣，等. 基于区块链的应用系统开发方法研究[J/OL]. 软件学报，2017，28(6)：1474-1487[2017-10-11]. http://dx.chinadoi.cn/10.13328/j.cnki.jos.005232.

[13] 贾大宇，信俊昌，王之琼，等. 区块链的存储容量可扩展模型[J/OL]. 计算机科学与探索. (2017-09-30)[2017-10-30]. http://kns.cnki.net/kcms/detail/11.5602.tp.20170928.1555.008.html. DOI：10.3778/j.issn.1673-9418.1709032.

[14] 喻辉，张宗洋，刘建伟. 比特币区块链扩容技术研究[J/OL]. 计算机研究与发展，2017，54(10)：2390-2403[2017-10-08]. http://dx.chinadoi.cn/10.7544/issn1000-1239.2017.20170416.

[15] BARTOLETTI M, BRACCIALI A, LANDE S, et al. A general framework for blockchain analytics [C/OL]//1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. New York: ACM, 2017: 1-6 [2017-10-10]. https://doi.org/10.13140/RG.2.2.10817.25444.

[16] HARI A, LAKSHMAN T V. The Internet blockchain: a distributed, tamper-resistant transaction framework for the Internet [C/OL]//HotNets'16 Proceedings of the 15th ACM Workshop on Hot Topics in Networks. New York: ACM, 2016: 204-210[2017-10-12]. https://doi.org/10.1145/3005745.3005771.

[17] 王继业,高灵超,董爱强,等. 基于区块链的数据安全共享网络体系研究[J/OL]. 计算机研究与发展, 2017, 54(4):742-749[2017-10-08]. https://doi.org/10.7544/issn1000-1239.2017.20160991.

[18] 朱岩,甘国华,邓迪,等. 区块链关键技术中的安全性研究[J/OL]. 信息安全研究, 2016, 2(12):1090-1097 [2017-10-17]. https://doi.org/10.3969/j.issn.2096-1057.2016.12.004.

[19] HALPIN H, PIEKARSK M. Introduction to security and privacy on the blockchain[C/OL]//2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Paris: IEEE, 2017: 1-3 [2017-10-10]. https://doi.org/10.1109/EuroSPW.2017.43.

[20] GERVAIS A, KARAME G O. On the security and performance of proof of work blockchains[C/OL]ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016:3-16[2017-10-08]. https://doi.org/10.1145/2976749.2978341.

[21] RODRIGUES B, BOCEK T, LAREIDA A, et al. A blockchain-based architecture for collaborative DDoS mitigation with smart contracts [C/OL]//TUNCER D, KOCH R, BADONNEL R, et al. Security of Networks and Services in an All-Connected World. AIMS 2017. Lecture Notes in Computer Science, vol 10356. Cham: Springer, 2017:16-29[2017-10-08]. https://doi.org/10.1007/978-3-319-60774-0_2.

[22] 袁勇,王飞跃. 平行区块链: 概念、方法与内涵解析[J/OL]. 自动化学报, 2017,43(10):1703-1712[2017-10-08]. http://dx.chinadoi.cn/10.16383/j.aas.2017.c170543.

[23] 李牧南. 区块链和比特币相关主题的知识结构分析: 共被引和耦合聚类分析视角[J/OL]. 自动化学报, 2017, 43(9):1509-1519[2017-10-08]. http://dx.chinadoi.cn/10.16383/j.aas.2017.c160648.

[24] 袁勇,周涛,周傲英,等. 区块链技术:从数据智能到知识自动化[J/OL]. 自动化学报, 2017, 43(9):1485-1490 [2017-09-23]. http://www.aas.net.cn/CN/Y2017/V43/I9/1485.

[25] 唐长兵,杨珍,郑忠龙,等. POW 共识算法中的博弈困境分析与优化[J/OL]. 自动化学报, 2017, 43(9): 1520-1531[2017-09-23]. http://dx.chinadoi.cn/10.16383/j.aas.2017.c160672.

[26] SANKAR L S, SINDHU M, SETHUMADHAVAN M. Survey of consensus protocols on blockchain applications [C/OL]//2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS). Coimbatore: IEEE, 2017: 1-5[2017-10-08]. https://doi.org/10.1109/ICACCS.2017.8014672.

[27] FUKEMITSU M, HASEGAWA S, IWAZAKI J, et al. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain[C/OL]//2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA). Taipei: IEEE, 2017: 803-810[2017-10-08]. https://doi.org/10.1109/AINA.2017.11.

[28] 张俊,高文忠,张应晨,等. 运行于区块链上的智能分布式电力能源系统:需求、概念、方法以及展望[J/OL]. 自动化学报, 2017, 43(9): 1544-1554 [2017-10-08]. http://dx.chinadoi/10.16383/j.aas.2017.c160744.

[29] 钱卫宁,邵奇峰,朱燕超,等. 区块链与可信数据管理: 问题与方法[J/OL]. 软件学报, 2018,29(1):150-159 [2017-10-30]. http://dx.chinadoi.cn/10.13328/j.cnki.jos.005434.

[30] 陆尧,文捷. 基于比特币技术的供应链管控与溯源方案[J/OL]. 计算机工程. (2017-11-10)[2017-11-12]. http://kns.cnki.net/kcms/detail/31.1289.TP.20171110.1508.004.html.

[31] 黄洁华,高灵超,许玉壮,等. 众筹区块链上的智能合约设计[J/OL]. 信息安全研究, 2017, 3(3): 211-219 [2017-09-08]. http://ris.sic.gov.cn/CN/Y2017/V3/I3/211. DOI: 10.3969/j.issn.2096-1057.2017.03.003.

[32] 黄晓芳,徐蕾,杨茜. 一种区块链的云计算电子取证模型[J/OL]. 北京邮电大学学报, 2017(5): 1-4[2017-10-22]. http://kns.cnki.net/kcms/detail/11.3570.TN.20171002.1705.008.html.

[33] 赵赫,李晓风,占礼葵,等. 基于区块链技术的采样机器人数据保护方法[J/OL]. 华中科技大学学报(自然科学版), 2015, 43(s1): 216-219[2017-09-08]. http://dx.chinadoi.cn/10.13245/j.hust.15S1052.

[34] **章宁，钟珊. 基于区块链的个人隐私保护机制**[J/OL]. **计算机应用**，2017，37(10)：2787-2793[2017-10-08]. http://dx.chinadoi.cn/10.11772/j.issn.1001-9081.2017.10.2787.

[35] **李悦，黄俊钦，王瑞锦. 基于区块链的数字作品** DCI **管控模型研究**[J/OL]. **计算机应用**，2017，37(11)：3281-3287[2017-09-07]. http://www.joca.cn/CN/Y/V/I/0. DOI：10.11772/j.issn.1001-9081.2017.11.3281.

[36] **薛腾飞，傅群超，王枞，等. 基于区块链的医疗数据共享模型研究**[J/OL]. **自动化学报**，2017，43(9)：1555-1562[2017-10-22]. http://dx.chinadoi.cn/10.16383/j.aas.2017.c160661.

[37] **吴振铨，梁宇辉，康嘉文. 基于联盟区块链的智能电网数据安全存储与共享系统**[J/OL]. **计算机应用**，2017，37(10)：2742-2747[2017-10-08]. http://dx.chinadoi.cn/10.11772/j.issn.1001-9081.2017.10.2742.

[38] LIU P T S. Medical record system using blockchain, big data and tokenization[C/OL]//LAM K Y, CHI C H, QING S. Information and Communications Security. ICICS 2016. Lecture Notes in Computer Science, vol 9977. Cham: Springer, 2016: 254-261 [2017-09-07]. https://doi.org/10.1007/978-3-319-50011-9_20.

[39] **吴明礼，张宏安. 存储技术综述**[J/OL]. **北方工业大学学报**，2015，27(1)：30-35[2017-10-15]. http://dx.chinadoi.cn/10.3969/j.issn.1001-5477.2015.01.005.

[40] SWAN M. Blockchain: blueprint for a new economy[M/OL]. [S.l]: O'Reilly Media. 2015: 13-146[2017-10-15]. http://shop.oreilly.com/product/0636920037040.do.

[41] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2008-10-31)[2017-10-08]. http://nakamotoinstitute.org/bitcoin.

[42] Secure Hash Algorithm[Z/OL]//VAN TILBORG H C A, JAJODIA S. Encyclopedia of Cryptography and Security. Boston: Springer, 2011: 46-59[2017-10-23]. https://doi.org/10.1007/978-1-4419-5906-5_1209.

[43] COURTOIS N T, GRAJEK M, NAIK R. Optimizing SHA256 in bitcoin mining[C/OL]//KOTULSKI Z, KSIEZOPOLSKI B, MAZUR K. Cryptography and Security Systems. CSS 2014. Communications in Computer and Information Science, vol 448. Berlin: Springer, 2014: 131-144 [2017-10-22]. https://doi.org/10.1007/978-3-662-44893-9_12.

[44] STAVROU A, VOAS J. Verified Time[J/OL]. Computer, 2017, 50(3): 78-82[2017-10-22]. https://doi.org/10.1109/MC.2017.63.

[45] GIPP B, MEUSCHKE N, BEEL J, et al. Using the blockchain of cryptocurrencies for timestamping digital cultural heritage[J/OL]. Bulletin of IEEE Technical Committee on Digital Libraries(TCDL), 2017, 1(13): 1-3[2017-10-22]. http://www.ieee-tcdl.org/Bulletin/v13n1/papers/gipp.pdf.

[46] MERKLE R C. Protocols for public key cryptosystems [C/OL]//1980 IEEE Symposium on Security and Privacy. Oakland: IEEE, 1980: 122-122[2017-10-22]. https://doi.org/10.1109/SP.1980.10006.

[47] LIN I C, LIAO T C. A survey of blockchain security issues and challenges[J/OL]. International Journal of Network Security, 2017, 19(5): 653-659[2017-10-25]. https://doi.org/10.6633/IJNS.201709.19(5).01.

[48] ZHAO J L, FAN S K, YAN J Q. Erratum to: overview of business innovations and research opportunities in blockchain and introduction to the special issue[J/OL]. Financial Innovation, 2017, 3(1): 28[2017-10-26]. https://doi.org/10.1186/s40854-017-0059-8.

[49] BALLETTE M, GASPARRONI M, BRICK P. Peer to peer network: US8214489[P/OL]. 2012-07-03[2017-10-21]. http://www.google.com/patents/US8214489.

[50] KRAFT D. Difficulty control for blockchain-based consensus systems[J/OL]. Peer-to-Peer Networking and Applications, 2016, 9(2): 397-413[2017-10-23]. https://doi.org/10.1007/s12083-015-0347-x.

[51] RITZDORF C. Secure peer-to-peer trading in small and large-scale multiplayer games[J/OL]. Multimedia Systems, 2014, 20(5): 595-607 [2017-10-08]. https://doi.org/10.1007/s00530-014-0372-2.

[52] **田怡萌，李小勇，刘海涛. 分布式文件系统副本一致性检测研究**[J/OL]. **计算机研究与发展**，2012(S1)：276-280[2017-10-08]. http://mall.cnki.net/magazine/article/JFYZ2012S1053.htm.

[53] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: extending bitcoin's proof of work via proof of stake[J/OL]. Acm Sigmetrics Performance Evaluation Review, 2014, 42(3): 34-37[2017-10-15]. https://dl.acm.org/citation.cfm?doid=2695533.2695545. DOI: 10.1145/2695533.269554.

[54] VUKOLIC M. The quest for scalable Blockchain fabric: Proof-of-work vs. BFT replication[C/OL]//CAMENISCH J, KESDOGAN D. Open Problems in Network Security. iNetSec 2015. Lecture Notes in Computer Science, vol 9591. Cham: Springer, 2016: 112-125[2017-10-16]. https://doi.org/10.1007/978-3-

319-39028-4_9.

[55] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol[C/OL]//KATZ J, SHACHAM H. Advances in Cryptology: CRYPTO 2017. Lecture Notes in Computer Science, vol 10401. Cham: Springer, 2017: 357-388 [2017-10-22]. https://doi.org/10.1007/978-3-319-63688-7_12.

[56] BARTOLETTI M, LANDE S, PODDA A S. A proof-of-stake protocol for consensus on bitcoin sub-chains [C/OL]//BRENNER M. Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science, vol 10323. Cham: Springer, 2017: 568-584 [2017-10-17]. https://doi.org/10.1007/978-3-319-70278-0_36.

[57] LI W T, ANDREINA S, BOHLI J-M, et al. Securing proof-of-stake blockchain protocols [C/OL]//GARCIA-ALFARO J, NAVARRO-ARRIIBAS G, HARTENSTEIN H, et al. Data Privacy Management, Cryptocurrencies and Blockchain Technology. ESORICS 2017, DPM 2017, CBT 2017. Lecture Notes in Computer Science, vol 10436. Cham: Springer, 2017: 297-315[2017-10-19]. https://doi.org/10.1007/978-3-319-67816-0_17.

[58] **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**[J/OL]. **密码学报**, 2017, 4(2): 187-198 [2017-10-22]. http://dx.chinadoi.cn/10.13868/j.cnki.jcr.000173.

[59] JAMTHAGEN C, HELL M. Blockchain-based publishing layer for the keyless signing infrastructure[C/OL]//Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences. Toulouse: IEEE, 2017: 374-381 [2017-10-22]. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0072.

[60] BOS J W, HALDERMAN J A, HENINGER N, et al. Elliptic curve cryptography in practice [C/OL]//CHRISTIN n, SAFAVI-NAINI R. Financial Cryptography and Data Security. FC 2014. Lecture Notes in Computer Science, vol 8437. Berlin: Springer, 2014: 157-175[2017-10-22]. https://doi.org/10.1007/978-3-662-45472-5_11.

[61] FILTZ E, POLLERES A, KARL R, et al. Evolution of the bitcoin address graph[M/OL]//HABER P, LAMPOLTSHAMMER T, MAYR M. Data Science: Analytics and Applications. Wiesbaden: Springer Vieweg, 2017: 77-82[2017-10-22]. https://doi.org/10.1007/978-3-658-19287-7_11.

[62] WATANABE H, FUJIMURA S, NAKADAIRA A, et al. Blockchain contract: securing a blockchain applied to smart contracts[C/OL]//2016 IEEE International Conference on Consumer Electronics (ICCE). Las Vegas: IEEE, 2016: 467-468 [2017-10-21]. https://doi.org/10.1109/ICCE.2016.7430693.

[63] **邓迪,孟繁轲,丁江. 一种点对点的数字资产交易方法及系统**: CN106780028A[P/OL]. 2017-05-03[2017-10-21]. https://www.google.com/patents/CN106780028A?cl=zh.

[64] GSJ. **基于区块链技术的文件存储服务** Sia[EB/OL]. (2015-12-09)[2017-10-23]. http://www.8btc.com/sia-blockchain.

[65] **零传媒. 一枚连续创业者要用区块链技术筑起"红利之墙"**[EB/OL]. (2017-06-13)[2017-10-08]. http://www.sohu.com/a/148406483_388414.

[66] **王志文,吴思进. 区块链信息存证及隐私保护方法**: CN105610578A [P/OL]. 2016-05-25 [2017-11-02]. http://www.xjishu.com/zhuanli/CN105610578.html.

[67] Printemps. **区块链公司** Colu **上线,携手** Revelator **简化音乐版权管理**[EB/OL]. (2015-08-13)[2017-10-08]. http://www.btc38.com/btc/altgeneral/7963.html.

[68] **高航,俞学劢,王毛路. 区块链与新经济: 数字货币** 2.0 **时代**[M/OL]. **北京:电子工业出版社**, 2016: 330-333[2017-10-08]. http://cbjj.phei.com.cn/module/goods/wssd_content.jsp?bookid=46518.

[69] The University of Sydney. Red Belly Blockchain[EB/OL]. (2017-07-03)[2017-11-08]. http://poseidon.it.usyd.edu.au/~concurrentsystems/rbbc/.

[70] **张亮亮,张翌维,梁洁,等. 新量子技术时代下的信息安全**[J/OL]. **计算机科学**, 2017, 44(7): 1-7[2017-11-12]. https://doi.org/10.11896/j.issn.1002-137X.2017.07.001.

[责任编辑:瑞金]