计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.201200163

# 区块链技术研究综述

代闯闯[1,2] 栾海晶[1,2] 杨雪莹[1,2] 过晓冰[3] 陆忠华[1,2] 牛北方[1,2]
1 中国科学院计算机网络信息中心 北京 100190
2 中国科学院大学 北京 100049
3 联想研究院 北京 100085
(dcc@cnic.cn)

**摘 要** 随着比特币等虚拟数字货币的日益普及与发展,区块链技术受到了研究人员的广泛关注。区块链技术是一种按照时间顺序将区块以链式结构组合而成的分布式数据账本,具有去中心化、可编程、可溯源、不可篡改等特性,在金融领域中的研究尤为广泛。文章面向区块链技术的发展,介绍区块链技术的起源和概述,详细地讨论环签名、零知识证明、数字签名和同态加密等区块链关键技术,综述区块链技术的特点和种类。对区块链技术的应用领域进行概括,重点关注其应用原则和应用领域相关的案例,分析区块链应用当前的发展现状,并对未来区块链技术的发展方向进行分析与预测。

**关键词**:区块链;比特币;共识机制;环签名;零知识证明;数字签名;智能合约;去中心化
**中图法分类号** TP399

## Overview of Blockchain Technology

DAI Chuang-chuang[1,2],LUAN Hai-jing[1,2],YANG Xue-ying[1,2],GUO Xiao-bing[3],LU Zhong-hua[1,2] and NIU Bei-fang[1,2]
1 Computer Network Information Center,Chinese Academy of Sciences,Beijing 100190,China
2 University of Chinese Academy of Sciences,Beijing 100049,China
3 The Lenovo Research,Beijing 100085,China

**Abstract** With the increasing popularity and development of virtual digital currencies such as bitcoin,blockchain technology has been widely concerned by researchers. Blockchain technology is a distributed data ledger which combines blocks in a chain structure according to the time sequence. It has the characteristics of decentralization,programmability,and traceability. It has been widely studied in the financial field. Facing the development of blockchain technology,this paper introduces the origin and overview of blockchain technology,discusses in detail the crucial technologies of blockchain,consisting of ring signature,zero knowledge proof,digital signature and homomorphic encryption,and summarizes the characteristics and types of blockchain technology. This paper summarizes the application field of blockchain technology,focuses on its application principles and relevant cases in the application field,analyzes the current development status of blockchain application,and analyzes and forecasts the development direction of blockchain technology in the future.

**Keywords** Blockchain,Bitcoin,Consensus mechanism,Ring signature,Zero knowledge proof,Digital signature,Smart contract,Decentralization

## 1 引言

区块链技术并非偶然产生的,而是互联网技术发展到一定时期的必然结果[1]。区块链技术最初源于比特币[2],是比特币等虚拟数字货币的核心支撑技术[3],目的是解决在没有可信的中心机构以及信息不对称、不确定的情况下,如何构建一个“信任”生态体系来满足活动发生、发展的需求。作为计算机科学领域的前沿技术,区块链技术有望成为继蒸汽技术革命、电力技术革命、信息技术革命之后的又一颠覆式创新技术革命。区块链是将数据区块按照时间先后顺序以链表的方式组成的数据结构,并结合共识机制、密码学等方式实现不可撤销、不可伪造的分布式交易验证的去中心化账本,能够对具有时间先后关系且能在系统内进行验证的数据信息实现可靠存储[4]。

## 2 区块链技术起源

### 2.1 比特币系统结构

2008 年 11 月,化名为中本聪(Satoshi Nakamoto)的学者在其发表的论文《比特币:一种点对点式的电子现金系统》(Bitcoin:A peer-to-peer Electronic Cash System)中首次提出了比特币这一虚拟数字货币的概念[2],该货币于 2009 年 1 月上线,总量为 2100 万。比特币系统作为首个去中心化的加密货币系统,自 2009 年面世发展至今,显现出高度的可靠性和安全性。比特币系统的核心思想是以去信任和去中心化为基

基金项目:中国科学院战略先导科技专项(XDC01040100);广西科技重大专项(桂科 AA18118054)
This work was supported by the Strategic Priority Research Program of the Chinese Academy of Sciences(XDC01040100) and Science and Technology Major Project of Guangxi(Guike AA18118054).
通信作者:牛北方(bniu@sccas.cn)

本目标，简化系统中的价值交换过程，去除无关第三方在中心架构中的参与[5]。

比特币是由交易、共识协议和通信网络等技术组件所构成的一种去中心化的电子交易系统，其涵盖的技术组件形成了整个比特币系统的3个渐进的层次：交易、区块和区块链[6]。比特币系统中的每个区块可划分为区块头和区块体两部分，区块体中存储当前区块所包含的全部交易记录。比特币系统中的交易记录类似于物理系统中的交易记录，每一条交易记录中均包括交易信息的输入、输出地址以及转让的数目等信息。根据这些交易信息可自底向上生成对应的默克尔树(Merkel Tree)[2]结构的形式。默克尔树根节点的哈希值会存储在区块的头部，在每个区块生成时，区块的记账者会为该区块加盖时间戳，用于标明该区块的生成时间。随着时间戳的增强，区块会不断延展形成一个具有时间维度的区块链条，使得数据信息能够按照时间进行追溯[7]。除此之外，区块头中还有版本号、前一区块头部的哈希值、随机数和目标哈希值等信息。最后，对本区块头部的信息进行哈希，产生的哈希值存在下一个区块的头部[8]，在逻辑结构上，使得每一个区块以链的形式串联起来。比特币系统的相应数据结构如图1所示。

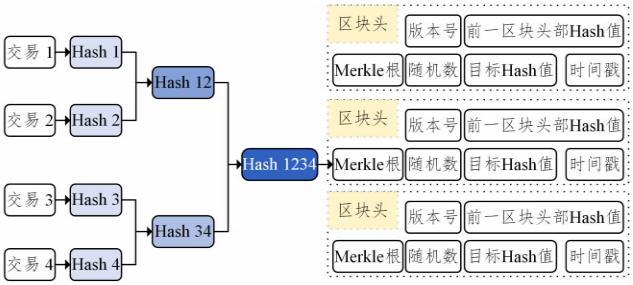


图1 比特币系统的数据结构

Fig. 1 The data structure of the Bitcoin system

### 2.2 比特币系统运行机制

比特币系统的运作机制就是实现账本的记账过程，该记账过程对于用户而言是透明的[5]。在具有中心架构的系统中，账本的记账权由账本的所有者管理，例如商场的记账权由商场来控制，银行的记账权由银行来控制。然而，在比特币系统中，为达到去中心化和去信任的目的，账本的记账权不能集中在单一机构或者某个中心内部，而应将账本的记账权下放到分布式系统的各个节点当中。比特币系统采用分布式系统达到去中心化的目的，而具体该分布式系统中的哪个节点获得某交易记录的记账权，需系统中的每个节点通过竞争来获取。各个节点在竞争的过程中需要付出一定的代价来防止作恶，只有遵守相应的规则才能够获得系统的奖励，整个系统由奖惩机制驱动，可进行良性循环。在比特币系统中，该过程被称为挖矿，其中的各个节点被称为矿工。在解决了账本记账权的归属问题后，下一步应当考虑的是比特币系统中的节点如何成功实现交易数据的同步更新，即在分布式系统中如何确保各个节点中所交易数据信息的一致性。该问题可以通过共识机制来解决，系统中的各个节点在接收到区块链中新区块的数据时，需停止当前的挖矿工作，对新区块进行数据一致性验证。

比特币系统的运行机制可简述为如下流程[5]：首先由用户发起一笔交易，该交易以广播的形式发送到区块链系统中的各个节点。网络中的各个节点在接收到交易后会验证该交易消息的有效性和正确性，如果交易信息未验证通过，节点将拒绝接收该交易，并将交易被拒绝的信息返回给交易的发起者。如果交易信息验证通过，节点会将该交易信息放到自己的交易池中，并继续向网络中传播。各节点对各自交易池中的交易进行打包，并加入随机数进行相应的计算。最先计算出符合要求哈希值的节点将获得所打包区块中交易的记账权，即创建新区块。随后，该节点会将计算得到的新区块广播到比特币系统中的其他节点，其他节点在收到该区块后，会立即验证该区块的有效性和正确性。验证成功后会将收到的新区块链接到自己的本地链中，同时会删除原本自己的交易池中所打包的区块，按照上述步骤再进行新一轮的区块生成过程。比特币系统的运行机制如图2所示。

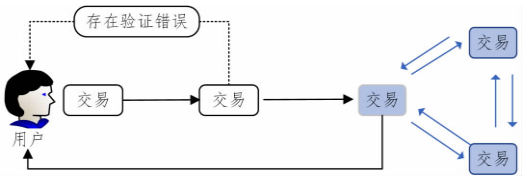


图2 比特币系统的运行机制

Fig. 2 The operating mechanism of the Bitcoin system

## 3 区块链的分类

区块链的共识机制致力于解决在分布式存储过程中区块链发展所面临的一致性问题，即“拜占庭将军”问题。基于不同场景下的信任创建方式，区块链可归纳为如下两类：许可链和非许可链。基于数据的读写权限和管理权限的差异，区块链可划分为公有链、私有链和联盟链[9]。下文会对公有链、私有链和联盟链3种不同区块链的权限和共识机制进行介绍。

### 3.1 公有链

公有链，也称非许可链，没有集中式的管理机构。网络中的参与节点可任意接入，可随意查看区块链上的任意信息，且对相关的数据信息未设置读写访问权限。典型的共识算法可分为工作量证明(proof of work，PoW)[10]、权威证明(proof of authority，PoA)[11]和股权证明(proof of stake，PoS)[12]三类。PoW是比特币系统所采用的常见共识机制，要求区块链上的各节点基于其自身的算力求解一个难度适中且易于验证的数学问题(挖矿)，最快求解出该问题的节点拥有区块的记账权，且获得一定数目的比特币作为挖矿的工作奖励。PoW共识算法在比特币系统中发挥了至关重要的作用，能够对比特币系统中的货币发行、流通、回笼和市场交换等流程进行有机整合，从而构建一个安全可靠的系统。然而，PoW共识算法仍存在很多不足，例如，算力竞争所带来的高昂电力和设备成本等问题。为改善PoW共识算法所带来的算力资源浪费，PoS共识算法中规定具备最高权益的区块链节点将拥有区块的记账权，而不是具备最大算力的区块链节点拥有区块的记账权。PoS共识算法中的权益一般指的是用户在区块链上所持有的Token数量或Token时间等虚拟资源。根据矿工所持有权益的大小来设置其挖矿的难度，权益越大时挖矿的难度就越小，通过所持权益的大小来决定区块链系统中的记账权，从而可有效地避免资源的浪费。因此随着挖矿难度的日益增加，比特币系统由初期的PoW共识算法来维护转变为由PoS共识算法来维护，PoS能够从一定程度上减少算力资源的浪费以及缩短区块链中各节点达成共识所需要的时间。对现有权益证明进行改进，提出了权威证明。PoA共识算法指的是链上

各节点通过投票方式选举出的权威节点最终将获得该区块的记账权[13]。与其他共识算法有所不同，PoA 共识算法能够有效地避免算力资源浪费和 51%算力攻击的问题。

### 3.2 私有链

私有链由私有组织或单位创建，写入权限仅局限在组织内部，读取权限有限对外开放。私有链通常采用具有可信中心的部分去中心化结构和容错性低、性能效率低的 Paxos 和 Raft 等共识机制[14]，因此记账效率要远高于联盟链和公有链。其中，Paxos 机制是基于消息传递的一致性算法，主要用于解决如何调整分布式系统中的某个值使其达成一致的问题。Raft 机制能够实现秒级共识的效果，确保了结果的可靠性和准确性。

### 3.3 联盟链

联盟链，也称为许可链[15]，介于公有链和私有链之间，在结构上采用“部分去中心化”的方式，由若干机构联合构建，只限联盟成员参与，某个节点的加入需要获得联盟其他成员的许可，数据读取权限和记账规则等均需根据联盟中的相关规则进行定制。与公有链相比，联盟链所拥有的节点数量较少[29]。典型的共识机制有拜占庭容错机制（byzantine fault tolerance，BFT）[16]和实用拜占庭容错机制（practical byzantine fault tolerance，PBFT）[17]。在 BFT 算法中，拜占庭问题能够解决的前提条件是拜占庭节点数目不超过节点总数目的 1/3。原始的拜占庭容错机制可划分为两种协议：口头协议和书面协议。口头协议的核心思想是将所接收到的“命令”在各个节点之间进行传输，最终根据各个节点所获取的综合信息来确定出最终的结果。书面协议的核心思想是对所传输的信息进行数据签名，该协议能够防止拜占庭节点随意修改接收到的信息[8]。其中，PBFT 是对 BFT 的升级改进，实用拜占庭容错算法解决了原始拜占庭容错算法中数据信息的传输复杂度较高的难题，但是对于大规模的公有链却不适用，因为该链节点很多，节点数目越多，节点之间的通信时间就越长。除此之外，PBFT 对 BFT 中所存在的算法效率较低的情况进行了改善，共识算法的复杂度由指数级降至多项式级，使得在实际应用场景中 PBFT 算法得到了普及发展[18]。

### 3.4 链的对比

在分布式结构上，不同类型的区块链系统具有一定的差异。由于具备不同的区块链共识机制，因此应用场景也有较大的差别。公有链是完全的去中心化架构，各参与节点具有平等的数据读写等权利，通常用于搭建开放式的共享记账系统。联盟链是部分去中心化的分布式结构，由参与联盟的多个组织或机构形成多中心的分布式系统，通常用于在各行业机构创建权利相对对等的组织团体以共享数据。私有链在公司或机构内部形成小范围的可信中心化结构，省略激励层以提高性能效率，用于企业和机构内容的数据共享管理[19]。目前，在区块链领域中派生出两种发展方向：一种是以比特币、以太坊为代表的公有链的发展方向，一种是以超级账本为代表的私有链/联盟链的发展方向。比特币、以太坊等具有全球化、不受特定机构或组织约束的特点，而超级账本则致力于构建一个既能满足不同领域需求又能满足各监管架构要求的开放平台。

## 4 区块链的三大发展阶段

自比特币提出以来，加密货币（尤其比特币）一直受到投资者、监督机构和媒体的高度关注[6]。目前，虽然区块链的发展标准尚未统一，但却可通过其发展演化过程来更深入地认识了解区块链[9]。根据区块链的发展演化阶段，区块链经历了以比特币为代表所实现可编程货币的区块链 1.0 模式、以太坊为代表实现可编程金融的区块链 2.0 模式、以 EOS 为代表实现可编程社会的区块链 3.0 模式 3 个发展时期[20]，本节会对其展开详细的介绍。

### 4.1 区块链 1.0

区块链 1.0 是区块链技术的基础版本，能实现可编程货币，是与货币支付、汇款、兑换、交易和转移等功能相关的数字货币应用。常见的数字货币有比特币、莱特币（Litecoin，LTC）和瑞波币（Ripple，XRP）等。

在区块链 1.0 阶段，比特币是当之无愧的主角，戴尔、微软等电子商务网站相继接受比特币作为支付方式[21]。比特币作为最早实现去中心化的数字货币，运用分布式记账技术，使得整个交易过程实现了去中心化的效果[5]。交易无需通过任何第三方的机构或者组织进行监督或验证，而是由区块链系统中的各个节点来验证交易的合理性。比特币平台不仅可用于创建比特币，还可用于创建其他货币。代币原本指的是具有与货币相似的尺寸及形状、具有支付功能和固定流通范围的货币替代品[22]。早期的代币主要以购物券、电子消费卡等形式存在。随着消费方式的多样化，传统代币逐渐消失，取而代之的为以点币为主的虚拟货币。随着互联网技术的快速发展，网络虚拟货币逐渐成为一种在网络空间中流通的、具有货币职能的代币[23]。

莱特币 2011 年面世，是一种比特币替代币。在技术原理上，莱特币与比特币基本类似，但却是一种更为轻量的数字资产。莱特币能够降低硬件成本，使得普通人挖矿也成为了可能。

然而，瑞波币与比特币之间差异很大。瑞波系统是由美国旧金山的瑞波实验室所研发的一种基于移动互联网的金融交易协议。该协议能够实现在全球货币或者价值体间的实时、自由、免费的汇兑与转换，例如人民币、美元、欧元、英镑、比特币和飞行里程等，交易确认仅需几秒钟，交易费用几乎为 0，减免了原本异地跨行、跨境操作的支付费用[24]。瑞波币是瑞波系统中与货币流通有关的工具，是不同类别货币间进行兑换的桥梁货币。由于瑞波币具有在不同网关间自由流通的特性，因此在该系统内，其他类别的货币在不兑换成瑞波币的情况下，则很难实现跨行跨境转账。

### 4.2 区块链 2.0

区块链 2.0 是区块链技术的进阶版本，能实现可编程金融，是与股票、债券、期货和智能合约等相关的金融领域应用。在区块链 2.0 中，以以太坊为代表实现了更复杂的分布式合约记录-智能合约[25]。受比特币的启发，Buterin 于 2013 年提出了以太坊的概念，以太坊的最大特点就是增加了对智能合约的支持[26]。理想状态下，智能合约可看成一台图灵机，是能按预先设定的规则自动执行的一段程序代码，但由于缺乏可信的运行环境，智能合约并未广泛地投入应用。区块链的运行环境高度可信，使得智能合约的概念得以运行实施。将该合约记录在区块链中，一旦满足合约的触发条件，就可独立执行预定义的代码逻辑，并且执行后的结果无法在链中更改。

目前，以太坊平台是一个较为成熟、具有高度去中心化的智能合约平台，通过时间戳、分布式共识等区块链技术，实现

信息的交易共享[27]。以太坊为智能合约平台提供了一定的图灵完备性，为区块链技术提供了广泛的使用场景[28]。然而，在以太坊平台中所存在的安全威胁以及交易需较长检验时间的问题，使该平台无法满足商业化应用的需求，在此情况下，Linux 基金会于 2015 年主导研发了 Hyperledger 平台，旨在创建跨行业的基于区块链技术的开源规范和标准，为联盟链中相互合作的企业构建一个去中心化、公开透明的开发平台[29]，其中最为典型的平台是 Hyperledger Fabric 联盟链[30]。

### 4.3 区块链 3.0

区块链 3.0 是区块链技术的高级版本，能够实现可编程社会，可应用到任何有需求的领域，包括金融、物流、医疗健康、电子政务以及社交媒体等领域，进而涵盖整个人类社会。目前，区块链行业进入了由 2.0 向 3.0 过渡的阶段，若区块链 1.0 版本和区块链 2.0 版本的典型特点分别是数字货币和智能合约，区块链 3.0 版本的特点则是基于规则的可信智能社会治理体系[31]。区块链 3.0 的核心是区块链应用落地[32]。迅雷链克是区块链 3.0 背景下的典型应用，也是区块链技术与云计算的成功结合。共享计算是迅雷自主研发的技术，已成为迅雷的主营业务，其基本原理是运用智能硬件“玩客云”对网络中用户的空闲带宽、流量等计算资源进行集中搜集后，借助迅雷公司独特的技术手段，将物理位置相对分散的计算资源打包转换为云计算服务后，销售给其他用户，最后可通过“链克”对分享空闲计算资源的用户给予相应的奖励[33]。基于云计算的空闲资源利用的方式，颠覆了目前在云计算行业中普遍依赖数据中心来生产计算力的模式，该方式能精准反映出用户所分享资源的数目和质量，使得共享资源的分配使用更具公开性和透明性，因此，有望从根本上解决计算成本常年居高不下的难题。

去中心化是区块链技术的核心思想，采用了 P2P 的网络结构。参与到区块链网络中的各节点既是客户端又是服务器，当链上的某个节点发起交易时，网络中的其他节点会对其准确性和有效性进行一致性验证，达成共识后的交易会被加入到区块链中。为达成共识，交易的发起者需对其所做的工作进行证明。最常使用的共识机制可分为工作量证明、股权证明、权益证明、拜占庭容错机制和实用拜占庭容错机制等。在区块链 3.0 中，常见的共识机制不再被封装在区块链的底层结构中不可更改，用户可根据实际需要将不同的共识机制进行相应的组合[34]。除此之外，区块链 3.0 能够实现智能合约的定制开发，编写好的智能合约能够方便地部署在区块链中。

## 5 区块链技术概述

区块链技术最早是由 ScottStornetta 于 1991 年提出，是一种被称为“区块链”的数字架构系统[35]。近年来，区块链技术引起了各领域研究人员的普遍关注。区块链是由众多具有对等关系的网络节点构成的，以扁平式的结构交互连通，无中心化节点，节点之间无需互相信任。各网络节点在激励机制的作用下共同维护一个由区块所构成的链式结构[36]。区块链作为比特币等数字加密货币的核心支持技术，能够有效地解决数字货币长期所面临的拜占庭将军问题和双重支付问题[37]。传统的社会信任是建立在基于信用“背书”机制和可信第三方的基础上，由银行等可信的第三方机构或组织来提供信任支持。然而，在没有可信的第三方机构或组织的情况下，两个实体间直接建立信任关系却很困难，区块链技术能够通过共识机制和分布式节点的交易验证等技术来解决去中心化系统中节点间的信任构建问题，使节点间信任机制达到去中心化的目的[38]。虽然区块链已出现十余年，然而早期的研究重点主要集中在比特币系统是否安全可靠上，区块链技术方面的研究较少。近年来，随着比特币等虚拟数字货币的日益普及与发展，区块链技术在不同领域的应用与发展也呈现出爆炸式的增长趋势[39]。区块链技术并不单局限于其链式数据结构，而是将环签名、零知识证明、数字签名和同态加密等技术进行组合，使链上节点不依赖于单个中心，是一种新颖的分布式交易验证和数据共享技术。

### 5.1 区块链关键技术

#### 5.1.1 数字签名

数字签名(Digital Signature)方案最早是由 Whitfield Diffie 和 Martin Hellman 于 1976 年所提出，是由签名者对电子文件进行电子签名，使得签名者无法对其所签署的签名进行否认或抵赖，实现的功能与手写签名相同[40]。公钥加密技术是数据签名方案的核心技术，在该技术中，每个用户均持有一对密钥，即公钥和私钥，其中公钥用于数字签名的验证，私钥则用于数字签名的生成。数字签名方案至少应具备如下 3 个条件：事后签名者不能抵赖其对报文的签名；接收者可对签名的真伪性进行验证，且无法对该签名进行伪造；当接收者和签名者对数字签名的合法性和真伪性存在争执时，可信的第三方能够有效地处理双方之间所产生的争执[41]。

目前，对数字签名的研究主要集中在基于公钥密码体制的数字签名研究上，1978 年 Rivest 等提出了基于 RSA 公钥算法的数字签名方案[42]，1985 年 ELGamal 提出了基于离散对数的数字签名方案[43]。由于现有的公钥加密体系是基于单向哈希函数的数学运算，其运算速度非常缓慢，因此对整个消息文本直接进行公钥密码算法加密在实际的应用场景中并不可行。为了改善该问题，通过对待签名的消息文本进行预处理，从消息文本中提取一个固定大小的特征值，该值可唯一表示这段消息，即信息摘要。消息摘要具有以下特性：1)在消息文本中任意细微的变化，将导致信息摘要的巨大改变；2)尝试从消息摘要中恢复和获取原始的消息文本是不太现实的；3)在计算中找到具有相同摘要值的两条消息文本是不可行的[40]。

#### 5.1.2 同态加密技术

在当今的大数据时代，用户的数据信息时常面临隐私泄露的风险，因此如何有效地避免数据信息的泄露已经成为全社会共同面临的难题。在互联网时代，特别是在云计算的环境中，云服务提供商和用户耗费了过多的计算资源来进行隐私保护，为了解决这个问题，同态加密(Homomorphic Encryption)技术应运而生[44]。同态加密的概念是 1978 年 Rivest 等所提出的[45]，这是一种可对密文进行直接操作的加密方案[46]。同态加密的核心思想是在私钥未知的情况下，对待加密数据执行特定的计算，使计算后得到的加密数据解密后的结果与对明文执行相同的计算获得的结果相同[47]，也就是说同态加密技术能够达到这样的一种效果[48]：对明文进行的一种特定的代数算法与对密文进行相同的代数算法是等价的。根据该性质，可以对明文直接进行相关的操作而无需先解密得到明文之后再进行相关的操作。

#### 5.1.3 零知识证明

零知识证明(Zero-Knowledge Proof)是由 Goldwasser 等[49]于 1985 年所提出的,指的是某一方(验证者)在另一方(证明者)不提供任何可靠信息时,能够相信证明者所提出的论断是有效且正确的,从而很好地保护了证明者数据信息的隐私安全。零知识证明具有如下的性质:第一是完备性,如果论断是正确的,诚实的证明者能以极高的概率使诚实的验证者相信该事实;其次是正确性,如果论断是错误的,欺骗性的证明者只能以极低的概率使诚实的验证者相信其是真实可靠的;最后是零知识性,零知识证明过程运行结束后,验证者只能获取"证明者拥有这条知识"的信息,却无法获得关于这条知识本身的任何信息[50]。

### 5.2 区块链技术特征

区块链具有多中心化、多方维护、时序数据、智能合约(Smart contract)[51-52]、不可篡改、开放共识、安全可信等特性。第一是多中心化验证,链上数据的验证、核算、存储、维护和传输等过程均依赖分布式系统结构,运用纯数学方法代替中心化组织机构在多个分布式节点之间构建信任关系,从而建立去中心化的可信的分布式系统[39];第二是多方维护,激励机制可确保分布式系统中的所有节点均可参与数据区块的验证过程,并通过共识机制选择特定节点将新产生的区块加入到区块链中;第三是时序数据,区块链运用带有时间戳信息的链式结构来存储数据信息,为数据信息添加时间维度的属性,从而可实现数据信息的可追溯性;第四是智能合约,区块链技术能够为用户提供灵活可变的脚本代码,以支持其创建新型的智能合约[53],例如以太坊(Ethereum)等开源社区平台利用完善的脚本语言为用户提供了任意精准定义的智能合约,实现了数据信息在多个互不信任对象之间的可信共享智能合约等[54];第五是不可篡改,在区块链系统中,因为相邻区块间后序区块可对前序区块进行验证,篡改某一区块的数据信息,则需递归修改该区块及其所有后序区块的数据信息,且需在有限的时间内完成,然而每一次哈希的重新计算代价是巨大的,因此可保障链上数据的不可篡改性;第六是开放共识,在区块链网络中,每台物理设备均可作为该网络中的一个节点,任意节点可自由加入且拥有一份完整的数据库拷贝;第七是安全可信,数据安全可通过基于非对称加密技术对链上数据进行加密来实现,分布式系统中各节点通过区块链共识算法所形成的算力来抵御外部攻击、保证链上数据不被篡改和伪造,从而具有较高的保密性、可信性和安全性。

## 6 区块链应用

区块链技术自面世以来,就与金融领域息息相关。最先兴起并引发全球关注的区块链应用是以比特币为代表的虚拟货币发行,以及依托虚拟货币的各类首次发行货币项目(Initial Coin Offering,ICO)[55]。ICO 指的是企业在研发新的区块链项目时,通过发行代币等货币替代品,来筹集比特币等数字货币的行为,其本质是初创企业通过发行代币以实现融资的目标。与传统的融资方式相比,ICO 具备融资快、成本低等巨大的优势,位于法律监督领域的空白地带,吸引了很多的非理性投资者和不法分子,严重干扰金融领域的市场秩序。为防范系统性金融风险,全球多个国家先后制定了 ICO 监管政策,其中我国采取的政策最为严格。2017 年 9 月,中国人民银行、工商总局等七部委发布了《关于防范代币发行融资风险的公告》,将代币发行视为未经法律许可的非法公开融资行为。在以上严厉政策监管之下,比特币等虚拟货币价格纷纷下跌,ICO 也逐渐趋于理性。在各国对虚拟货币以及 ICO 进行严格监督的同时,区块链技术正在蓬勃发展,其应用也日益广泛[56]。下文会详细介绍区块链技术的应用原则及其在物联网应用领域、金融应用领域、产业供应链领域、物流供应链以及其他领域目前的发展现状以及详细的应用案例。

### 6.1 应用原则

区块链作为近年来的新兴技术在很多领域均具备开展应用的能力。然而,区块链技术并非万能的,技术上的公开透明、不可伪造、可追溯性和去中心化等特点,使其在特定的场景下具有很高的使用价值。在应用区块链时,应遵循如下原则:第一是多信任主体。区块链是典型的信任机器,企业主体间不存在天然的信任关系,需依赖区块链来建立信任关系;反之,若各实体间是强信任关系或已具备完善的保障制度,则不存在应用区块链的必要。第二是多方协作。若应用场景存在大量的协作方和高昂的对账成本,基于区块链的底层账本所搭建的智能合约系统能够有效地降低对账成本、提升效率,该系统能够保障数据的可靠性、权威性和高效性,极具现实使用意义[57]。第三是商业逻辑完备。由于区块链各节点间存在完备的商业逻辑,可形成多赢局面,因此参与者才会使用整条区块链。第四是依据系统控制权和交易信息的公开性来进行归类。公有链允许节点的任意加入,对信息的传播不加以制约,信息对整个系统公开透明;联盟链只允许通过认证的机构参与共识,根据共识机制对交易信息进行局部公开;私有链的适用范围最受限制,仅适用于特定的机构内部。

### 6.2 区块链技术的发展现状及应用案例

#### 6.2.1 物联网应用领域

区块链与物联网的融合应用可分为横向和纵向两种模式。从横向模式来看,区块链可对整个物联网产业链进行升级改进,解决在物联网应用领域中所出现的生态链冗长、信息高度不对称的问题。区块链将物联网设备采集到的数据视为数字化资产,利用自身的技术特点,使得网络上的参与方在达成共识的前提下挖掘和利用所采集到的数据,保障数据信息的安全性和一致性,消除物联网产业链的信息壁垒,为物联网中的相关用户提供高质量的多维数据,提高数据的应用价值。从纵向模式来看,运用区块链技术在互联网技术设备和物联网设备间创建连接,可以确保数据信息的安全性、可靠性和不可篡改性。物联网采集的数据是物理世界中的目标对象通过感知控制域中的设备连接所映射成的虚拟空间中的数字化资产对象。通过区块链技术在目标对象、设备、平台间实现数据信息采集的客观性和有效性,从而有效确保在物理世界的实体资产与虚拟世界的数字资产间的可靠性和一致性。

由于目前的充电行业普遍存在着支付协议复杂、支付方式不统一、充电桩相对短缺和电力费用计算不精准等问题,德国莱茵公司和 Slock.it 联合研发出一种基于区块链的点对点式电动汽车充电项目[58]。该项目的核心思想是在每个充电桩上部署树莓派等简易型 Linux 系统设备,基于区块链技术将附属同一公司的多家充电桩和拥有充电桩的个人用户进行串联,并运用适配个人接口的智能插头来对电动汽车进行充电。除此之外,在该项目中引入了区块链电子钱包技术,能实现车主身份的自主验证,以及在无第三方机构人工确认的情况下,自动支付行车过程中所涉及的电力收费、停车收费和高

速公路收费等。目前，该项目已被美国加州初创公司引入，并致力于在该州进行推广。

6.2.2 金融应用领域

区块链技术最早起源于加密数字货币，因此与金融领域密切相关，其目的是实现数字货币的支付。区块链去中心化的技术特性给依赖第三方机构的电子支付和资金托管等领域带来了颠覆性的变革。传统的金融交易需要通过银行证券以及交易所等中心化机构或组织的协调来开展工作，而区块链技术无需依附任何中间环节，即可构建了一种点对点式的数据传输方式，极大改善了交易速率和成本等，简化了相应的业务流程[28]。与传统的 VISA 系统 10%的费率和一周的到账时间相比，基于区块链技术的蚂蚁金服已能够实现 1 min 到账，平均效率可提升一万倍，同时也具有更加低廉的支付成本。然而，在交易验证的实时性和吞吐量上仍需进一步提升，现有的 VISA 系统每秒可支持数百笔交易，支付宝每秒成交的交易数目也达到了 8.59 万[19]，而基于 DPoS 共识机制的 EOS 系统目前的 TPS 是 3000 笔。可见区块链系统的处理能力还不足以替代现有的集中式交易系统。除此之外，区块链技术能直接创建支付流，可以跨国跨境实现超低费率的瞬时支付。目前，研究人员迫不及待进行了很多的尝试，以区块链技术作为基础，Frey 等构建了购物系统架构[59]、English 等利用电子货币进行薪酬支付[60]，Bogner 等开发了租用物品平台[61]，这些尝试可为未来区块链技术的进步发展提供更加广阔的思路。

在供应链金融的应用场景中，区块链从效率、成本和信任 3 个维度解决了企业融资过程中所遇到的难题。区块链可为供应链中不同参与方提供平等协作的平台，达到了数据实时对账的效果，能够有效地防止数据的伪造和篡改。2015 年，纳斯达克在基于区块链的平台上实现了首个证券交易。在基于区块链技术的 Linq 平台上，实现了首个证券交易记录。Linq 平台将股票发行至私人投资者，在无第三方中介或清算机构的参与下，即可运用去中心化的账本来验证股票交易的可行性。该平台使得传统繁琐的管理功能更现代化和安全有序。与传统人工记录台账相比，区块链技术能缩短交易结算时间以及大幅度加快交易的资金传输速度。

6.2.3 产业供应链领域

通常情况下，产业供应链指的是在产品的生产流通过程中，由供应商、制造商、经销商、零售商以及消费者等所构成的动态连接网络[62]，供应链管控已成为衡量现代企业竞争力的显著指标[63]。产业供应链系统中往往存在着数百加工环节，如此庞大的节点数量为产业供应链的追踪管理带来了极大的挑战。由于在产业供应链的流动过程中，存在着大量产品生产、运输和销售等数据信息的交互与处理，因此将区块链技术引入到产业供应链系统中，实现供应链的自动化和信息化已发展为该行业主流的发展趋势。基于相关领域已取得的研究成果，运用区块链系统存储并管理供应链数据，能够实现供应链产业中的产品溯源、查询和验证等功能，从而提升整个行业的透明性和可靠性。

本节将以京东的跑山鸡为例对产业供应链的溯源、查询和验证功能进行详细介绍。在产业供应链的溯源和查询阶段，原有的机制使得代理商在取走货物后生产商就无法获得后续的销售信息。然而，通过区块链系统可将生产数据和销售数据进行有机结合，一方面可有助于最终消费者对产品进行溯源，通过对产品二维码进行扫描，即可查询该产品的生长环境、生长周期和产地等信息，构建可溯源的农产品体系；另一方面，产业供应链为厂商提供透明的数据管理，以便于对后续的生产销售进行规划。在产业供应链的验证阶段，目前的防伪验证方案通常使用验证码和验证平台相结合的方式，用户将产品标签上的验证码输入到厂商维护的平台上，从而获取产品的验证信息。然而，该方案却存在如下缺点：产品的验证码极易伪造，生产厂商在获得一个合法的验证码后可生产大量同款产品的验证码；验证平台的维护成本较高，部分的生产厂商无力承担。基于上述缺点，运用区块链技术对该方案进行改进，将产业供应链上通过质检的单品以“单品＋代工厂”多标签的交易形式加入到区块链中，从而在供应链的起始位置形成“厂商->代工厂->产品->单品”的树形结构，这种单向性能够保证该结构的安全性和易于验证性，使得非法厂商无法伪造商品的各项生产信息。由于用户可查询到产品在整条供应链上的传输记录，因此不会出现类似验证码的伪造问题。在实际应用中，区块链还需要进一步提升信息安全性、构建溯源机制来支持产业供应链的相关应用。通过区块链技术可降低物流运输费用，可随时追踪产品的生产和运输等过程，能够快速检索产品的相关信息，同时能够有效地提高产品供应链的效率[64]。

6.2.4 物流供应链领域

通常情况下，物流供应链指的是供应商、制造商、分销商、零售商和用户等所组成的物流网络。在该供应链的节点间所流动的原材料、中间产品和最终产品等组合成了供应链上的物资流[65]。由于该供应链上节点数量众多，因此在物资流通过程中，不同节点间存在着大量的信息交互。由于在供应链的运行过程中所生成的数据以物理上相对分散的方式存储在各节点的私有系统内部，无法确保数据信息的公开透明性，会带来很多问题：1）数据信息在节点间无法实时共享，导致上游节点需保留大量的库存来满足下游的需求；2）中小型物流企业普遍面临着融资难的问题；3）供应链网络中信息传输不畅导致其上各节点无法在第一时间掌握相关情况，会极大地影响物流供应链的运行效率。

在政府的大力推动下，国内外的著名企业开展了很多与物流供应链领域相关的区块链项目。例如基于区块链的 Yojee 物流软件。该软件可在区块链上记录货物的整个传输流程，装载、运输、派送、取件等流程清晰可见，从而可实现对运输车队的实时管控。在物流供应链中，基于机器学习方式将货物的交付工作自动分配给物流司机，可大幅减少人工调度员的参与。除此之外，可运用现有的交付基础设施来协助物流企业随时调整车队，不仅缩减了物流供应商的运输成本，而且可为最终用户创建更便捷的支付方式。基于区块链技术，Yojee 软件能够实时记录卖方、买方等相关交易信息，通过双方的数字签名在全网进行验证，若在全网的加密记录信息是一致的，则可证明其是有效的，从而将该信息上传至整个区块链网络，实现数据信息的可靠共享。基于区块链可追溯的特性，该软件可通过区块链记录货物从出发到接收的整个流程信息，从而规避丢包、错误认领包裹等现象的发生。针对快递签收情况，仅需对区块链进行查询即可，从而可避免出现快递员通过伪造数据签名来冒领快递包裹的情况。企业可运用区块链技术对包裹的流向进行实时追踪，可确保其线下各营销商的利益。

6.2.5 其他领域

可追溯性是区块链技术的重要特性，在共识机制下将存储交易的区块按照时间维度添加到链的尾部，从而保障链上数据的可靠性。在社交媒体领域，该特性可用于追踪互联网上用户的发言，迅速追责，从而构建一个安全有序的网络环境[66]；在商业领域，区块链技术可以用于搭建商家信誉度反馈系统[67]，从而维护消费者的合法权益；在保险领域，可有效避免欺诈骗险等不诚实行为，维护保险公司的利益。除此之外，区块链和电子政务也息息相关。政府的各项工作受到群众的监督，其文献信息[68]、政务信息需要做到公开透明，项目的招标进度需公平公开公正。区块链技术可在互不信任的企业竞标者之间达成信任共识，通过合约来确保项目的进度，从而可保障交易信息的不可篡改性、不可伪造性和公开透明性。

## 7 区块链技术未来发展

在实际的应用场景中，当前的区块链平台在诸多方面尚存在很多问题[69]，仍需要区块链技术的发展进步来进行相应的改善。区块链技术具有去中心化、公开透明、不可篡改和信息可追踪性等特性，因此该技术在不同的产业领域均有一定的发展前景。区块链技术给未来技术的发展带来了很多积极的影响：1)无需繁琐的个人证明。目前，在跨国旅游时，出生证、房产证和结婚证由于地域等原因会变得没有效力。区块链所具有的不可篡改的特性可从根本上解决这一问题，通过在区块链上对这些证件进行公证[70]，并结合智能合约机制则能较为圆满地解决复杂规则所构成的难题[71]。区块链不可逆的特点能够验证这些证件的真实性，通过智能合约则可检验其合法性，区块链技术可根据安全部门的要求随时更新这些证件，极大地便利了人们的海外出行。2)将区块链技术与数字版权保护进行有机结合。创作者可在区块链平台上传原始作品，经区块链发布后，用户即可看到创作者的作品信息，通过支付版权税的方式获得该作品的使用权，该版税无需经过版权方，会直接经过区块链系统到达创作者的账户中。随着区块链技术的发展进步，如能够解决上述问题，它将不仅可保护数字版权信息，还可改变数字版权的交易方式、收益的分配方式以及用户的付费机制，未来还可搭建融合用户、版权方、制作方和发行方的产业链共享平台[72]。3)将联盟区块链应用于医疗健康数据的安全存储和共享。在医疗健康数据系统中，每条数据均详细记录了每位患者的用药情况、就诊记录、过敏史、化验结果等信息。基于目前医疗资源的分布可将医疗机构划分为不同的级别，使用 PBFT 等多种不同的共识机制确保在没有中心系统干预的情况下使联盟链中的医疗机构能够共享该联盟中不同医院间的患者健康数据，减少传统的集中化存储方法所带来的安全威胁[73]。4)将侧链技术应用于供应链溯源系统[74]。在供应链系统中，供应商、加工商、经销商分别将原材料信息、产品的加工信息、产品的销售信息加入到区块链中，但由于数据信息过多会给整个系统带来巨大的压力以及高昂的手续费，可以采用侧链技术加以改善。侧链技术[75]是一种将比特币在比特币主链和其他区块链之间进行安全转移的协议。该协议可将一些小额频繁的交易转移到侧链上，不仅可提高区块链主链的运行效率，而且可大幅降低交易的手续费[76]。5)将区块链技术应用到教育领域中。利用区块链不可篡改和不可伪造的特性，由证书颁发机构将每个人不同时期的学历证书发布到区块链网络中，保证了链上证书的真实性，使得证书真伪性的检验变得更加简单、便捷，也可大大降低搭建和维护证书存储网站的费用，这可能会成为未来解决学历证书伪造的完美方案[77]。

**结束语** 本文系统性介绍了比特币系统的结构和运行机制、区块链技术的原理，以及区块链的技术特征和种类，最后介绍了区块链应用的发展现状和区块链技术未来的发展。目前，基于区块链技术的相关应用还处于起步状态，虽然出现了很多的商业化应用，但是并未在大范围内普及，将对区块链技术的长远发展带来很多不利的影响。因此，本文对区块链技术的相关综述，希望对相关的研究人员探索新的研究成果提供一定的参考借鉴。

## 参 考 文 献


[1] HUANG H Y, YANG X H, WANG X L, et al. Overview of domestic blockchain research based on CNKI [J]. Software Guide, 2020, 19 (1): 234-237.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf: bitcoin, 2018.

[3] HAN X, YUAN Y, WANG F Y. Blockchain security: research status and prospects [J]. Journal of Automation, 2019, 45 (1): 206-225.

[4] SHEN X, PEI Q Q, LIU X F. Overview of blockchain technology [J]. Journal of Network and Information Security, 2016, 2 (11): 11-20.

[5] CAI X Q, DENG Y, ZHANG L, et al. Principle and core technology of blockchain [J]. Journal of Computer Science, 2019, 42 (115): 1-51.

[6] WANG Q, QIN B, HU J K, et al. Preserving transaction privacy in bitcoin[J]. Future Generation Computer Systems, 2020, 107: 793-804.

[7] LIU A D, DU X H, WANG N, et al. Blockchain technology and its research progress in the field of information security [J]. Journal of Software, 2018, 29 (7): 2092-2115.

[8] ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology [J]. Computer Engineering, 2019, 45 (5): 1-12.

[9] SHI J S, LI R. Overview of blockchain access control under the Internet of things [J]. Journal of Software, 2019, 30 (6): 1632-1648.

[10] GARAY J A, KIAYIAS A, LENOARDOS N. The bitcoin backbone protocol: Analysis and applications[C]// Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria, 2015: 281-310.

[11] CAO Z. A consensus mechanism for alliance chain [J]. Cyberspace Security, 2019, 10(1): 96-101.

[12] KING S, NADAL S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake[EB/OL]. https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf: Google, 2012.

[13] LI G, ZHANG J H, ZANG J M. Research on improved POA consensus mechanism blockchain system for solving civil aviation virtual seat occupation [J]. Computer Application Research, 2020: 1-7.

[14] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]// Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference. Philadel-

phia,USA,2014:305-320.
[15] TAN H B,ZHOU T,ZHAO H,et al. Archive data protection and sharing method based on blockchain [J]. Journal of Software,2019,30 (9):2620-2635.
[16] LAMPORT L,SHOSTAK R,PEASE M. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems,1982,4(3):382-401.
[17] CASTRO M,LISKOV B. Proactive recovery in a Byzantine-fault-tolerant system[C]// Proceedings of the 4th Conference on Symposium on Operating System Design and Implementation. Berkeley,United States,2000:273-288.
[18] YUAN Y,NI X C,ZENG S,et al. Development status and Prospect of blockchain consensus algorithm [J]. Journal of Automation,2018,44 (11):2011-2022.
[19] YU G,NIE T Z,LI X H,et al. Distributed data management technology in blockchain system - challenges and prospects [J]. Journal of Computer Science,2019,42 (116):1-27.
[20] PORTMANN E. Rezension "Blockchain:Blueprint for a New Economy"[J]. Praxis Der Wirtschaftsinformatik,2018,55(6):1362-1364.
[21] ZHANG J,GAO W Z,ZHANG Y C,et al. Intelligent distributed power energy system running on blockchain:demand,concept,method and prospect [J]. Journal of Automation,2017,43(9):1544-1554.
[22] FU X Q,YANG Y. An improved mobile payment system model [J]. Journal of Huazhong University of science and technology (Natural Science Edition),2004,32(12):49-50,74.
[23] FANG Y B,ZHOU C G. Token system based on blockchain smart contract [J]. Computer Application Research,2020,37(12):1-7.
[24] HE H L. Ruibo coin and operation mechanism of Ruibo system [J]. Times finance,2016(20):267-278.
[25] SZABO N. Smart contracts:building blocks for digital markets [EB/OL]. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html:Google,1996.
[26] BUTERIN V. Ethereum:a next generation smart contract and decentralized application platform [EB/OL]. https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalikbuterin.pdf:Google,2016.
[27] XU X B,SUN B S,QI X H,et al. Scalable information sharing mechanism of Internet of things based on Ethereum [J]. Computer Applications and Software,2019,36 (12):111-116,142.
[28] ZHU J M,ZHANG Q N,GAO S. Research progress on key technologies and applications of blockchain [J]. Journal of Taiyuan University of technology,2020:1-14.
[29] MENG W T,ZHANG D W. Optimization scheme of hyperledger fabric consensus mechanism [J]. Journal of Automation,2020:1-14.
[30] ANDROULAKI E,BARGERA,BORTNIKOV V,et al. Hyperledger fa-bric:a distributed operating system for permissioned blockchains [EB/OL]. https://www.colabug.com/3052594.html:Google,2018.
[31] MEI Y X,DIAO X L. The era of blockchain from 2.0 to 3.0 requires the deep integration of eliminating the false and preserving the true and the real economy [J]. Communication World,2018 (27):48-49.
[32] XU M X,YUAN C,WANG Y J,et al. Pseudo blockchain-blockchain security solution [J]. Journal of Software,2019,30(6):1681-1691.
[33] SONG Q. On the development of blockchain-Xunlei chain shows the technological advantages of the 3.0 era [J]. Computer and Network,2018,44(5):33.
[34] LI Y. Identity authentication system based on blockchain 3.0 Architecture [J]. Journal of Suzhou University,2019,34 (11):70-76.
[35] WANG J W,ZHENG Z Z,WU F,et al. Data market based on blockchain based data market [EB / OL]. http://kns.cnki.net/kcms/detail/10.1321.g2.20200311.1050.004.html:Big data,2020.
[36] YUAN B A,LIU J,LI G. Fair multi-party undeniable protocol based on blockchain [J]. Journal of Cryptologic Research,2018,5(5):546-555.
[37] KARAME G O,ANDROULAKI E,ROESCHLIN M,et al. Misbehavior in bitcoin:A study of double-spending and accountability[J]. ACM Transactions on Information and System Security,2015,18(1):1-32.
[38] YE C C,LI G Q,CAI H M,et al. Security detection model of blockchain [J]. Journal of Software,2018,29(5):1348-1359.
[39] YUAN Y,WANG F Y. Development status and Prospect of blockchain technology [J]. Journal of Automation,2016,42(4):481-494.
[40] ZHANG L. Overview of digital signatures[C]// Society for the Application of Intelligent Information Technology. China:Henan,2011:541-544.
[41] ZHAO X. Overview of digital signatures [J]. Computer Engineering and Design,2006,27(2):195-197.
[42] JAIN J,SINGH A. Quantum-based Rivest-Shamir-Adleman (RSA) approach for digital forensic reports[J]. Modern Physics Letters B,2020,34(6):2050085.
[43] KARIMA D,LAMINEM. Two dimensional ElGamal public key cryptosystem[J]. Information Security Journal:A Global Perspective,2019,28(4/5):120-126.
[44] FU Y,YU Y H,WU X P. Differential privacy protection technology and application in big data environment [J]. Journal of Communications,2019,40(10):157-168.
[45] RIVEST R L,SHAMIR A,ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM,1978,21(2):120-126.
[46] HU Z,YANG G,YANG B S,et al. Parallel homomorphic encryption algorithm based on MapReduce [J]. Computer Applications,2015,35(12):3408-3412,3418.
[47] WANG R J,TANG Y C,ZHANG W Q,et al. Privacy protection scheme of Internet of vehicles based on homomorphic encryption and blockchain technology [J]. Journal of Network and Information Security,2020,6(1):46-53.
[48] GUO J L,HOU H X. Laboratory open management system based on homomorphic encryption technology [J]. Information Security Research,2020,6(2):188-192.
[49] GOLDWASSER S,MICALI S,RACKOFF C. The knowledge complexity of interactive proof-systems[J]. SIAM Journal on Computing,1989.18(1):186-208.
[50] LI X D,NIU Y K,WEI L B,et al. Overview of bitcoin privacy protection [J]. Journal of Cryptography,2019,6(2):133-149.
[51] RIVEST R,SHAMIR A,TAUMANY. How to leak a secret

[C]// Proceedings of 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia, 2001: 552-565.
[52] SZABO N. Formalizing and securing relationships on public networks[J]. First Monday, 1997, 2(9).
[53] SHAO Q F, ZHANG Z, ZHU Y C, et al. Overview of enterprise blockchain technology [J]. Journal of Software, 2019, 30(9): 2571-2592.
[54] ZENG S Q, HUO R, HUANG T, et al. Research review of blockchain Technology: principle, progress and application [J]. Journal of Communications, 2020, 41(1): 134-151.
[55] HAN F. On the civil protection of China's investors' rights and interests under the new ICO Regulations [J]. Journal of Taiyuan University (Social Science Edition), 2019, 20(6): 73-82.
[56] OUYANG L W, WANG S, YUAN Y, et al. Smart contract: Architecture and progress [J]. Journal of Automation, 2019, 45(3): 445-457.
[57] SANG A Q, SHEN M, ZHU L H, et al. Research on multi-party collaborative security identity authentication mechanism based on blockchain [J]. Journal of Nanjing University of Information Engineering (Natural Science Edition), 2019, 11(5): 581-589.
[58] WANG Y, HE M J. Application case analysis of blockchain and Internet of things [J]. Integrated Circuit Application, 2018, 35(3): 70-74.
[59] FREY R M, VUCKOVAC D, ILIC A. A Secure Shopping Experience Based on Blockchain and Beacon Technology[C]// Proceedings of the 10th ACM Conference on Recconmmender Systems. Boston, MA, USA, 2016: 3-4.
[60] ENGLISH S M, NEZHADIAN E. Conditions of full disclosure: The blockchain remuneration model[C]// Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops. Paris, France, 2017: 64-67.
[61] BOGNER A, CHANSON M, MEEUW A. A decentralised sharing app running a smart contract on the ethereum blockchain [C]// Proceedings of the 6th International Conference on the Internet of Things. Stuttgart, Germany, 2016: 177-178.
[62] LAMBERT D M, COOPER M C, PAGH J D. Supply chain management: implementation issues and research opportunities[J]. International Journal of Logistics Management, 1998, 9(2): 1-20.
[63] LU Y, WEN J. Supply chain control and traceability scheme based on bitcoin technology [J]. Computer Engineering, 2018, 44(12): 85-93, 101.
[64] HOU Z G, LIANG H. Research on development status and characteristic application of blockchain technology [J]. Scientific and Technological Innovation and Application, 2019 (30): 18-20, 23.
[65] RAO D N, WANG J X, JIANG Z H, et al. Overview of the application of blockchain technology in logistics supply chain [J]. Software Guide, 2018, 17(9): 1-3, 8.
[66] CHAKRAVORTY A, RONG C. Ushare: user controlled social media based on blockchain[C]// Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication. Beppu, Japan, 2017: 99.
[67] DENNIS R, OWEN G. Rep on the block: A next generation reputation system based on the blockchain[C]// Proceedings of the 10th International Conference for Internet Technology and Secured Transactions. London, UK, 2015: 131-138.
[68] GERSTL D S. Leveraging bitcoin blockchain technology to modernize security perfection under the uniform commercial code [C]// Proceedings of the International Conference of Software Business. Ljubljana, Slovenia, 2016: 109-123.
[69] SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain Technology: Architecture and progress [J]. Journal of Computer Science, 2018, 41(05): 969-988.
[70] HUANG Y X, LIANG Z H, HUANG P, et al. Supply chain trusted data management based on blockchain [J]. Computer System Application, 2018, 27(12): 9-17.
[71] LUO W H. Rules and consensus: from electronic signature to blockchain [J]. Journal of China University of Political Science and Law, 2019(2): 48-59, 206.
[72] ZHANG S, DONG Y. Research on digital copyright protection based on blockchain technology [J]. Research on Science and Technology Management, 2020, 40(1): 132-136.
[73] FENG T, JIAO Y, FANG J L, et al. Health data security model based on alliance blockchain [J]. Computer Science, 2020, 47(4): 305-311.
[74] ZHANG C D, WANG B S, DENG W P. Design of supply chain traceability system based on side chain technology [J]. Computer Engineering, 2019, 45(11): 1-8.
[75] WORLEY C, SKJELLUM A. Blockchain tradeoffs and challenges for current and emerging applications: generalization, fragmentation, sid-echains, and scalability[C]// Proceedings of the 2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. Washington D. C., USA, 2018: 1582-1587.
[76] TIAN Y L, YANG K D, WANG Z, et al. Blockchain data traceability algorithm based on attribute encryption [J]. Journal of Communications, 2019, 40(11): 101-111.
[77] YANG X M, LI X, WU H Q, et al. Application mode and practical challenges of blockchain technology in Education [J]. Modern Distance Education Research, 2017(2): 34-45.

**DAI Chuang-chuang**, born in 1993, Ph.D. His main research interests include algorithms and software in high-performance and blockchain.

**NIU Bei-fang**, born in 1978, Ph.D, professor. His main research interests include the research of high-performance computing technology for biological and medical bigdata, specifically involving cancer genomics and macrogenomics, especially the "precision medicine" data processing technology based on the next generation.