计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.200800021

区块链技术原理与应用综述

郭上铜　王瑞锦　张凤荔
电子科技大学信息与软件工程学院　成都 610054
(229119392@qq.com)

摘　要　近年来,随着数字加密货币逐步走进人们的视野,其底层的区块链技术也引起了研究者的高度重视。区块链作为一种分布式账本技术,具有多方维护、不可篡改、公开透明等特点。首先,将区块链结构按层级进行划分,从低到高介绍了每层的作用和原理,根据开放程度将区块链分为公有链、联盟链、私有链,以比特币、Hyperledger Fabric为例分析了公有链和联盟链的工作机理。其次,对区块链的底层核心技术共识算法、智能合约、隐私安全做了详细阐述。最后,分析了区块链的研究进展并进行了展望。

关键词:数字加密货币;区块链;共识算法;智能合约;隐私保护
中图法分类号　TP311.13

Summary of Principle and Application of Blockchain

GUO Shang-tong, WANG Rui-jin and ZHANG Feng-li
School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

Abstract　In recent years, as digital cryptocurrency has gradually come into people's sight, its underlying technology blockchain has also attracted people's attention. As a distributed ledger technology, blockchain is characterized by multi-party maintenance, non-tampering, openness and transparency. In this paper, the structure of block chain is divided according to the hierarchy, and the functions and principles of each layer are introduced from low to high. Block chain is divided into public chain, alliance chain and private chain according to the degree of openness. The working principle of public chain and alliance chain is illustrated by taking Bitcoin and Hyperledger Fabric as examples. And this paper gives a detailed introduction to the underlying core technology consensus algorithm, smart contract and privacy security of blockchain, and analyzes the research progress and research prospect of blockchain in the end.

Keywords　Digital cryptocurrency, Blockchain, Consensus algorithms, Smart contract, Privacy protect

近年来,随着以比特币为代表的新型数字货币的迅速发展,作为比特币底层支撑技术的区块链技术也越来越受到人们的关注。与传统的中心化数据库相比,区块链通过对分布式数据存储、P2P传输、共识机制、加密算法和智能合约等传统技术的应用,使区块链具有去中心化、不可篡改、可溯源、多方维护、公开透明等特点。

在区块链的相关研究方面,Yao等[1]对区块链原理进行了简要概述,介绍了以太坊、Adept系统、超级账本等典型开源项目,但该工作对共识算法、智能合约等的介绍较为简单。文献[2]介绍了区块链的基础技术,归纳了区块链的类型,指出了区块链的结构和工作原理,但对共识算法、隐私保护、智能合约等关键技术的研究过于简单。文献[3]介绍了一些常见的共识算法,并对算法进行了对比,但其只是从比特币的交易脚本出发,简单介绍了智能合约的工作原理。本文梳理了PBFT,PoW,PoS,DPoS等共识算法的原理和流程。从智能合约的生命周期、运行原理、运行环境着手详细介绍了智能合约在区块链中的应用,列举了区块链中的常见安全问题,并对其攻击原理进行了详细介绍。

1　概述

1.1　发展历程

2008年,"Bitcoin: A Peer-to-Peer Electronic Cash Sys-

到稿日期:2020-08-03　返修日期:2020-12-01　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61802033,61472064,61602096);四川省区域创新合作项目(2020YFQ0018);四川省科技计划重点研发项目(2020YFG0475,2018GZ0087,2019YJ0543);博士后基金项目(2018M643453);广东省国家重点实验室项目(2017B030314131);网络与数据安全四川省重点实验室开放课题(NDSMS201606)
This work was supported by the National Natural Science Foundation of China(61802033,61472064,61602096), Sichuan Regional Innovation Cooperation Project(2020YFQ0018), Sichuan Science and Technology Program (2020YFG0475,2018GZ0087,2019YJ0543), Chinese Postdoctoral Science Foundation(2018M643453), Guangdong Provincial Key Laboratory Project(2017B030314131) and Network and Data Security Key Laboratory of Sichuan Province Open Issue(NDSMS201606).
通信作者:王瑞锦(ruijinwang@uestc.edu.cn)

tem"[4]中提出了被称为"比特币"的数字货币，比特币的设计初衷是在不信任环境下进行数字货币的支付，通过哈希函数、非对称加密、签名等密码学方法来实现用户的匿名以及交易的确认，通过共识机制对共同维护的数据达成一致，对信任危机提出了一种新的解决思路。

自比特币问世以来，比特币的底层技术——区块链技术也在不断的发展，目前区块链的发展可分为3个阶段。

(1)区块链1.0

区块链1.0[5]阶段也可以被称为可编程货币阶段，区块链使互不信任的人在没有权威机构介入[6]的情况下，可以直接使用比特币进行支付。比特币以及随后出现的莱特币、狗狗币、以太币等电子货币的出现，使得价值得以在互联网上流通，而去中心化、跨国支付、随时交易等特点使数字货币对传统金融造成了强烈的冲击。

(2)区块链2.0

区块链2.0阶段可以被称为可编程金融阶段。受比特币交易的启发，人们开始尝试将区块链应用到包括股票、清算、私募股权等其他的金融领域。2016年4月，花旗银行、德意志银行、汇丰银行等80多家金融机构和监管成员依托R3公司发布的区块链平台Corda[7]组成了R3联盟。2015年10月，纳斯达克在Money20/20大会上宣布上线用于私有股权交易的区块链平台——Linq[8]，避免了人工清算可能带来的错误，同时大大减小了人力成本。2015年10月，Ripple公司提出跨链协议——Interledger，该协议旨在打造全球统一的支付标准，简化跨境支付流程。区块链技术的应用使金融行业有希望摆脱人工清算、复杂流程、标准不统一等带来的低效和高成本，使传统金融行业发生颠覆性改变。

(3)区块链3.0

区块链3.0阶段可以被称为可编程社会阶段。随着区块链的发展，人们根据其特点将区块链应用到各种有需求的领域。例如应用区块链匿名性特点的匿名投票领域，利用区块链溯源特点的供应链、物流等领域，以及物联网、智慧医疗、智慧城市、5G、AI等领域。区块链将不可避免地对未来的互联网以及社会产生巨大的影响。

1.2 工作原理

根据目前已有的区块链平台，按准入机制可以将区块链分为3类：公有链、联盟链、私有链。私有链多用于搭建本地区块链以及对智能合约进行发布前的调试，因此本文主要介绍公有链和联盟链。

1.2.1 公有链

在公有链中，任何节点无需许可便可自由地加入或退出区块链网络，加入区块链网络的节点可以得到从创世区块到当前区块上的所有数据，全部节点通过共识机制对新区块的产生以及对区块上记录的交易达成一致，共同维护区块链的稳定。

公有链以比特币(Bitcoin)与以太坊(Ethereum)[9]为代表。图1给出了比特币的工作流程[10]。节点A与节点B之间发生转账交易，节点A首先将自己的交易广播到网络中的所有节点，节点在收到交易请求后验证节点A的签名，验证通过后将一段时间内接收到的交易组成新的区块，各节点(矿工)通过工作量证明(Proof of Work，PoW)竞争算力来获得新区块的记账权，在节点取得记账权后将该区块发布到网络中，其余节点在监听到新区块后检查区块及交易的正确性，若新区块符合要求则将新区块保存到本地并与之前的区块链接形成区块链，同时作为对矿工消耗的计算、电力等资源的补偿，获得记账权的矿工将得到一定的比特币(2020－2024年为6.25个比特币)以及其中的交易费作为奖励。

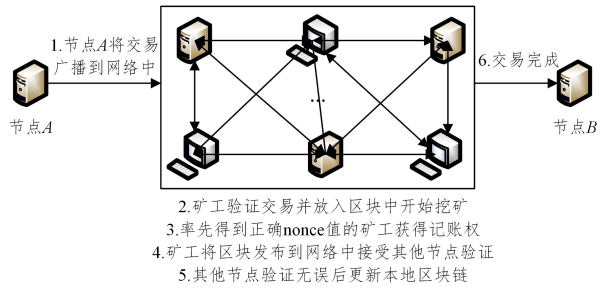


图1 比特币的工作流程

Fig. 1 Workflow of Bitcon

比特币的区块结构如图2所示。一个区块由区块头以及区块体组成，区块头由版本号、前一区块的哈希值、merkle根[11-13]、时间戳、目标难度、随机值组成。前块哈希值保证了之前的区块不可被篡改，同时在逻辑上使区块链接起来。时间戳表明了区块形成的大致时间，使区块能够按照时间顺序排列。矿工将区块头作为输入，不断使随机值加1，再运用双重SHA256算法进行计算，最终得到一个满足目标难度的随机值，此过程即为PoW共识过程。

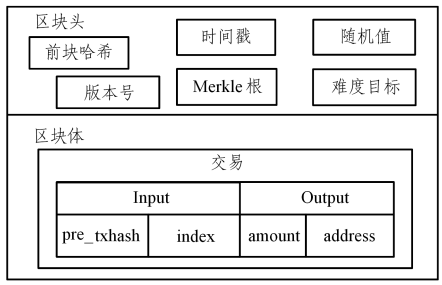


图2 比特币的区块结构

Fig. 2 Block structure of Bitcoin

以太坊的发展分为4个阶段，现阶段(Metropolis，大都会阶段)主要通过PoW共识算法来达成共识，但是因为以太坊的出块速度(9～12 s左右)远远快于比特币(10 min左右)，因此难以避免会出现多名矿工同时挖出新区块的情况，而以太坊为了补偿没有成为最长链的矿工，引入了叔区块的概念。以太坊规定，后来的区块可以引用包括它自己在内的7代以内的叔块，每引用一个叔块，该区块不仅可以得到原本的出块奖励和交易费，还可以再得到1/32个出块奖励，每一个区块最多可以引用2个叔块，而每个被引用的叔块根据引用区块与自己相隔的代数，其能得到的奖励从最开始的7/8个出块奖励降到1/8个出块奖励，以此来解决分叉问题，如图3所示。叔块1和叔块2作为叔区块被与它相隔最近的一代——区块$N+2$所引用，那么叔块1和叔块2分别能得到7/8个出块奖励，同时区块$N+2$能得到额外的1/32＋1/32个出块奖励，最远能被区块$N+7$所引用，此时叔块1和叔块2就只能得到1/8个出块奖励。

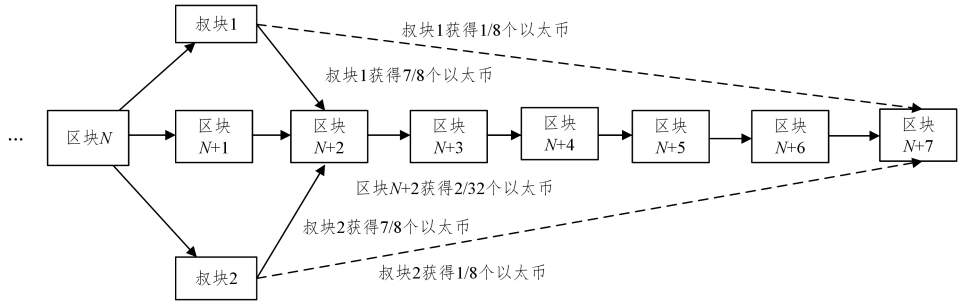


图 3 以太坊叔块示意图

Fig. 3 Uncle block diagram of Ethereum

1.2.2 联盟链

与公有链对所有用户完全开放不同，联盟链只允许授权节点接入网络的半开放式区块链。联盟链针对某些特定群体或机构，通过对节点授权来设置准入门槛，使数据的产生和接触可控，能在一定程度上兼顾数据的多方维护和避免数据泄露。联盟链内部设置记账节点，负责打包交易以及产生新区块，普通节点只负责产生交易和查询交易，没有记账权，避免了 PoW 共识所带来的计算资源、电力资源、存储资源的浪费。因此，联盟链适合彼此已经具有一定信任度的群体或机构使用。目前，全球主要的联盟链平台有超级账本（Hyperledger Fabric）、企业以太坊联盟（EEA）、R3 区块链联盟（Corda）、蚂蚁开放联盟链，其中影响力较大的是 Hyperledger Fabric。

Hyperledger Fabric 是由 Linux 基金会于 2015 年 12 月[14]发起的针对企业级应用的开源区块链项目。除了 Fabric 框架外，Hyperledger 项目还包括 Burrow，Sawtooth，Indy 等技术框架，其应用可覆盖金融、银行、物联网、供应链、制造和科技等多个行业领域。Fabric 中设置负责执行链码（智能合约）的背书节点（Endorser）、负责对交易进行共识并将交易打包的服务排序节点（Ordering-Service-Node，OSD）以及负责验证交易和更新区块链的提交节点（Committer），其工作流程如下：1）客户端产生交易并通过 P2P[15]网络将交易上传至背书节点；2）背书节点执行链码并对执行结果进行签名背书，最后将结果及背书发送给客户端；3）客户端收到足够数量的响应，并在验证合法性之后将链码执行结果发送至排序节点，排序节点内部运行共识算法对交易进行共识及排序，最后将交易按序打包进区块并发送给所有提交节点；4）提交节点验证交易的正确性，验证通过后将区块更新到本地区块链中。

2 区块链架构

随着区块链的发展，不同实现目的的区块链平台相继出现，虽然它们的体系结构并不完全相同，但依然存在着诸多共性。当前通常把区块链平台分为 5 层，分别是数据层、网络层、共识层、合约层和应用层。

2.1 数据层

数据层是所有区块链平台中的最底层，通过封装的链式结构、非对称加密、共识算法等技术手段来完成数据的存储和交易的安全实现，通常选择 LevelDB 数据库来存储索引数据。区块链在 Haber 等的研究基础上[16-18]，使用更简单、运算更快的哈希指针来完成区块之间的链接——通过每个区块头中包含的前块哈希（除创世区块外）使当前区块指向前一区块，从而将一个个孤立的区块在逻辑上连接起来，形成一条链状结构。其在块内通过使用 Merkle 树来组织块内交易，如图 4 所示。每个叶子节点为块内交易数据的哈希值，交易数据两两哈希形成它们的父节点，父节点再两两哈希形成它们的上一层节点，如此重复执行直到生成最终的 Merkle 根，这样保证了任何交易数据的更改都可以通过对比 Merkle 根而被察觉，从而为交易查询提供了快捷可靠的保障。节点之间通过共识算法来保证数据的一致性，使区块链在全网公开的情况下保证数据的不可篡改和可追溯。

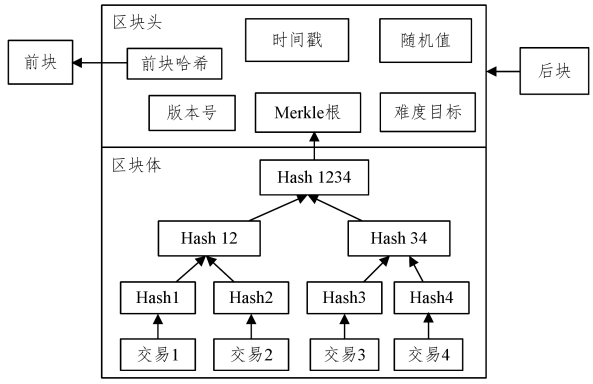


图 4 Merkle 树示意图

Fig. 4 Diagram of Merkle tree

每个区块都是由区块头和区块体两部分组成。区块头中通常存放着前块哈希、时间戳、Merkle 根、随机值、难度目标等数据，区块体中存放着交易数据。目前，数据存储模型主要分为基于交易的模型和基于账户的模型。比特币采用基于交易的模型，在每笔交易中都可以有多项输入和多项输出，通过输入可以一直向前追溯该笔金额到最初的挖矿奖励，通过输出可以向后追溯该笔金额是否被花费，如果一笔交易的输出没有与之对应的输入，则说明该笔金额未被花费；通过获取所有关联比特币地址的未花费输出（Unspent Transaction Outputs，UTXO）形成一个集合，可以快速地验证交易中的比特币是否被花费，以防止针对数字货币的双花攻击。以太坊、Hyperledger Fabric 等采用基于账户的模型。在以太坊中，账户分为外部账户（Externally Owned Account）和合约账户（Contract Account），外部账户的地址是由用户的公钥通过加密[19]产生的，用户通过自己的私钥来控制外部账户完成数字货币的转移和智能合约的部署，以及货币余额状态的查询。合约地址是智能合约的调用地址，根据合约创建者地址和该

地址发送过的交易数进行 RLP 编码，再通过 Keccak-256 进行哈希计算得到，可保存货币余额状态及合约状态，合约账户有对应的代码关联并由代码控制。

2.2 网络层

区块链通过对等节点(Peer-to-Peer)的方式完成组网，消息和数据的传输直接在节点之间完成，节点可以选择在任意时刻加入或退出网络而无需中间环节或中心服务器的参与，因此网络层采用 P2P 协议作为传输协议。若某一节点发布了一个新交易到区块链网络中，时刻监听网络的其余节点，在监听到新的交易后验证交易的签名，验证通过后将交易放入新区块中，获得记账权的节点将新区块发布到网络中，其余节点在监听到新区块后若验证通过，则将新区块存入本地区块链中，并且以新区块的哈希值作为前块哈希继续运行 PoW 算法来争取下一区块的记账权。

2.3 共识层

在一个区块链的分布式系统中，互不信任的节点通过某一机制在短时间内排除恶意节点的干扰，对正确结果达成一致，即称各节点之间达成共识。相比传统分布式系统提出的 CAP[20] 评价标准，区块链提出“不可能三角”评价标准，即去中心化、可扩展性、安全性不能同时满足。从解决传统分布式共识问题的 Paxos，PBFT 等经典共识算法到解决区块链共识的 PoW，PoS 算法，共识算法经历了长足的发展与改进，本文将在第 3 节详细阐述各种类型的区块链共识算法及其应用场景。

2.4 合约层

区块链 2.0 在区块链 1.0 的基础上引入了智能合约，智能合约从本质上来说是通过算法、程序编码等技术手段将传统合约内容编码成为一段可以在区块链上自动执行的程序，是传统合约的数字化形式。智能合约使区块链在保留去中心化、不可篡改等特性的基础上增加了可编程的特点，区块链通过智能合约的调用和事件的触发来完成数字资产的自动处理，适用于包括众筹在内的金融领域，而其因为自动按照合约规则执行的特点也逐渐适用于互联网、管理等领域。本文将在第 4 节详细叙述区块链中的智能合约。

2.5 应用层

区块链目前的应用场景主要集中在数字货币、金融交易、数据鉴证、选举投票、物流等方面，如 Corda，Quorum，Bitcoin，Ethereum 等，另外区块链与一些前沿研究领域如物联网、AI 等也有了不错的交互。应用层除了根据具体的应用业务独立开发一些专用的应用之外，还可以通过对下层数据和业务的集成来提供服务，构建适应性较强的区块链通用服务平台，如微软公司的 Azure BaaS 以及 IBM 的 Hyperledger。

3 共识机制

共识算法的研究由来已久，可分为证明类、随机类、选举类、联盟类、混合类[21]。解决传统分布式数据库一致性的算法有 Paxos[22]、基于 Paxos 且更容易理解与实现的 Raft[23] 算法，但这些共识算法均是默认节点诚实可靠的非拜占庭容错(Crash Fault Tolerance，CFT)算法，不能直接运用在无法保证节点诚实性的区块链网络中。1982 年，Lamport 等正式提出了“拜占庭将军问题”[24]：拜占庭的将军们需要在有叛徒干扰的情况下对进攻和撤退等作战计划达成一致。对于解决“拜占庭将军问题”，Lamport 于同年提出了拜占庭容错算法(Byzantine Fault Tolerance，BFT)，随后 Castro 等于 1999 年提出了实用拜占庭容错算法[25](Practical Byzantine Fault Tolerance，PBFT)，PBFT 算法将 BFT 算法的复杂度从指数级降到了多项式级，使 PBFT 算法能够真正地在实际中应用。拜占庭容错算法的研究也让共识算法从解决传统的分布式数据一致问题进入到解决区块链共识的全新阶段。

3.1 PBFT 共识算法

在一个分布式网络中，假设全部节点的数量为 N，恶意节点的数量为 f，PBFT 算法可以确保当恶意节点数量少于全网节点的 1/3 即满足 $N \geqslant 3f+1$ 时全网对消息达成共识。PBFT 算法包含一个主节点和其余的从节点，当主节点正常工作时，消息需要经过请求(request)、预准备(pre-prepare)、准备(prepare)、承诺(commit)、答复(reply)5 个阶段，如果主节点出错或不能及时处理数据，则启动视图转换协议从备份节点中选择新的主节点继续完成工作。PBFT 算法的共识过程如下：1)客户端向主节点发送请求；2)主节点在收到请求后生成预准备消息发送给全网备份节点；3)备份节点在收到预准备消息后首先进行验证，验证通过后生成准备消息发送给全网节点，同时监听网络中来自其他节点的准备消息；4)在节点收到大于或等于 $2f+1$ 个节点的准备消息后生成承诺消息，同时监听网络中来自其他节点的承诺消息；5)当节点收到大于或等于 $2f+1$ 个节点的承诺消息后完成对消息的承诺，并更新自己的日志，同时将承诺信息反馈给客户端。当客户端收到超过 f 个节点的承诺信息时，表明该请求被大多数节点确认。共识流程如图 5 所示。

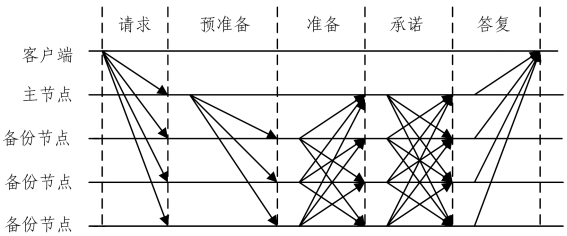


图 5 PBFT 共识流程

Fig. 5 Consensus process of PBFT

基于 PBFT 算法，研究者又提出了许多改进算法。文献[26]在 PBFT 算法的基础上引入门限签名技术来降低通信的复杂度。文献[27]在预准备阶段增加 propagate 过程来提高系统的鲁棒性。PBFT 及其改进算法的应用场景主要在以 Hyperledger Fabric 为代表的联盟链中，联盟链中取消了激励机制，采用 PBFT 算法可以避免大量算力及电力资源等的浪费。

3.2 PoW 共识算法

1993 年，Cynthia 等[28] 首先提出了 PoW 的概念，其最早被用于解决垃圾邮件问题——计算机在发送邮件之前需要进行一定量的计算，这对于普通用户发送邮件是没有影响的，但是对于需要大量发送垃圾邮件的计算机来说，这些计算完全超出了其能力范围。1997 年，文献[29]首次引入 PoW 共识

机制，随后中本聪在比特币白皮书中宣布在比特币中使用PoW机制来决定节点的记账权。在比特币中，每产生2016个块比特币网络就会调整难度目标来控制挖矿难度，使出块时间维持在10 min左右，而在比特币中挖矿的难度主要在于通过双重SHA256计算来找到一个小于目标难度值的随机数 *nonce* 值：节点先将区块头中的 *nonce* 值置为0，再将 *nonce* 值和区块头中的其他数据作为输入进行双重SHA256计算，若计算结果比目标难度值小则合格，否则将 *nonce* 值递增1继续计算，直到找到合适的 *nonce* 值或在发现其他节点已经找到后放弃竞争该块转而进行下一块的争夺。目标难度值通常是前面为连续若干个0的十六进制整数，连续的0的位数越多，挖矿的难度就越大。为了保证区块链的出块速度能维持在10 min左右，每出现2016个区块（大约14天）就会对挖矿的难度目标值进行调整，调整公式为：

$$target = target_{pre} * (time(act)/time(exp)) \tag{1}$$

其中，target表示计算得到的目标难度值；$\text{target}_{\text{pre}}$ 的 *target* 表示当前的目标难度值，$time(act)$ 表示产生前2016个区块总共花费的时间，$time(exp)$ 表示产生2016个区块所期望的时间（2016 * 10 min）。SHA256算法的防强碰撞特性使得矿工几乎只能通过大量的运算来争夺记账权。

PoW机制的引入将记账权分配给全网所有节点，节点通过竞争算力来获得记账权，获得记账权的节点会被给予一定的数字货币作为贡献算力等资源的奖励，有助于实现区块链的去中心化，若有人想要篡改区块链数据则需要拥有超过全网51%的算力，这是很难实现的，因此保证了交易的安全性。但PoW算法也浪费了大量的算力与电力资源，且10 min的出块时间也限制了其商业价值，并且现在算力几乎集中在各大矿池，这不仅与去中心化的初衷相悖，也增加了51%算力的威胁。但PoW共识机制依然被应用在除了比特币之外的各平台中，如现阶段的以太坊（Ethereum）、Dogecoin（狗狗币）、Litecoin（莱特币）。

3.3 PoS共识算法

2012年，点点币（Peercoin）[30]被推出，该数字加密货币首次采用权益证明（Proof of Stake，PoS）机制作为全网共识机制。PoS[31]中引入了“币龄”的概念，币龄＝持有货币数量＊持有时间，在PoS网络中前期通常会通过PoW机制发行一定数量的代币作为起始货币，在之后的PoS机制中矿工在挖矿时需要投入自己的币龄，投入的币龄越多挖矿的难度就越低，在成功出块后投入的币龄会被清空以保障公平性。若想在PoS网络中发起对主链的攻击行为，则需要攻击者持有大量代币，而事实证明有这样能力的用户做出恶意行为所得到的收益远远小于他作为一个诚实节点所得到的收益，因此PoS机制通过捆绑用户切身利益来保证交易的安全。

PoS共识的出现对解决PoW共识所消耗的大量算力与电力起到了一定的缓解作用，且缩短出块时间也能提高交易的处理速度和吞吐量，但PoS本质上还是需要通过哈希运算来竞争记账权且“币龄”的存在也降低了数字货币的流通性。在现有区块链中，以太坊基于PoS提出了Casper共识[32]，以太坊的4个发展阶段为：前沿（Frontier）、家园（Homestead）、大都会（Metropolis）、宁静（Serenity）。2019年1月中旬发布的君士坦丁堡版本（大都会阶段）中使用了PoW和PoS混合共识，为最后的宁静（Serenity）阶段使用纯PoS共识的Casper TFG版本过渡。

3.4 DPoS共识算法

2014年4月，Dan[33]首先提出了权益委托证明共识（Delegated Proof of Steak，DPoS），在DPoS中引入了民主选举的方式，节点通过投票选出 N 个代表组成“委员会”，节点拥有代币的数量越多则投票的权重越大，“委员会”中的节点负责收集、验证交易，以及将交易打包同时验证其他节点产生的新区块。“委员会”中的每个节点都会被轮流分配时间片，在该时间片内节点可以生成新区块，若“委员会”中的节点出现恶意行为，则会被取消出块的权利同时被没收“押金”，然后通过选举产生新的出块者。“委员会”通常会在一段时间后更新，通过新一轮的投票产生新的“委员会”。DPoS共识的出现避免了算力、电力等资源的浪费，采用民主投票的方式保障了节点的利益，出块速度的加快提高了交易速度和吞吐量，但“委员会”的形成会不可避免地带来一定程度的中心化且首富会一定程度地对区块链的安全产生威胁。表1列出了几种主流共识算法的性能的对比。

表1 共识算法性能的对比

Table 1 Consensus algorithm performance comparison

共识算法	PBFT	PoW	PoS	DPoS
去中心化程度	低	高	高	低
敌手模型	$N \geqslant 3f+1$	$N \geqslant 2f+1$	$N \geqslant 2f+1$	$N \geqslant 2f+1$
吞吐量/(tx/s)	小于等于3000	小于等于10	小于1000	大于1000
时延/s	小于10	600	60	—

4 智能合约

智能合约的概念是由Nick于1994年提出的[34]，智能合约最初的定义是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。但是，由于早期的技术和使用场景的限制，智能合约在很长一段时间进展缓慢，直到比特币的底层技术——区块链的出现，才使人们发现区块链的去中心化、可信执行环境完美契合智能合约，智能合约同样也为区块链提供了可编程性，拓展了区块链的应用前景。

4.1 生命周期

智能合约的生命周期可大致概括为协商、开发、部署、运行、销毁这5个阶段。智能合约的主要工作是在开发、部署、运行这几个阶段完成的。智能合约的本质是将传统合约变成一段可以自动执行的程序，在合约形成之初合约的创造者们应就合约内容进行协商，此时的合约与传统合约一样从法律、商业等角度形成了一套行为规则，通过规则的触发产生不同的结果。在规则确定之后，就由专业的技术人员将规则程序化，在经过验证测试后得到逻辑与原合约规则相一致的代码，最后将合约发布到区块链上。在合约发布之后，用户可以通过触发合约的事件来完成合约的调用，而当合约不再被需要时则由合约的部署者通过调用合约函来数完成合约的自毁。

4.2 运行原理

比特币通过执行UTXO（未花费交易）上的锁定脚本

(locking script)和解锁脚本(unlocking script)的结果来判断交易是否可被执行,这些脚本算是智能合约的雏形。但比特币脚本只能执行简单的逻辑和有限的循环,因此比特币脚本是非图灵完备的。智能合约的运行机制如图 6 所示。

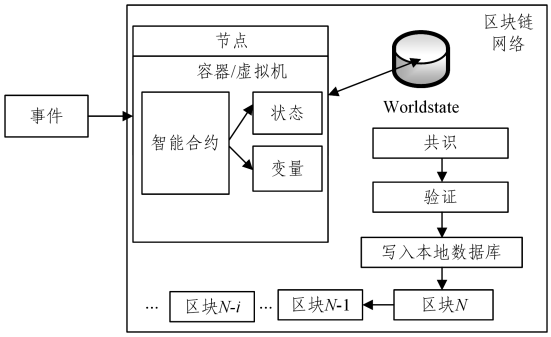


图 6 智能合约的运行原理

Fig. 6 Operation principle of Smart Contract

受比特币的启发,以太坊开发了 2 种图灵完备的语言 Serpent[35] 和 Solidity[36],使以太坊智能合约能够完成除交易之外的其他功能。以太坊智能合约包含若干状态、变量、规则和对应的操作,以太坊中的账户分为外部账户和合约账户。外部账户可以完成合约的部署以及通过调用合约地址来实现对合约的调用,合约创建者将合约编写完成后部署到区块链上,区块链会定期遍历所有智能合约的状态机和触发条件,外部账户通过发送交易的形式来部署和调用智能合约,而区块链在监听到某个合约的触发条件后就将该合约放到一个队列中,在分发到各节点后,节点在验证合约的正确性之后激活该合约的代码并在自己的 EVM[37](以太坊虚拟机)中运行,并将最终的运行结果打包到新区块中。考虑到合约在执行过程中会消耗带宽、计算、存储等资源,同时为了防止垃圾交易和死循环等恶意程序使区块链失控,合约的调用会消耗一定的燃料(gas),gas 是通过以太币兑换的,如果在合约的执行过程中因为燃料不足或指令异常导致合约执行中断,则已消耗的 gas 作为矿工所消耗资源的补偿将不会被退回。区块链的不可篡改性也意味着合约一旦被部署到区块链上就不允许再被修改,而有缺陷的合约往往会造成不可估量的损失,2016 年的“The DAO”事件就因为智能合约本身的漏洞被黑客攻击,损失大约 1200 万个以太币,虽然以太坊官方团队最终没能使攻击者如愿转走这些以太币,但以太坊也因此产生了硬分叉,被人们看好的众筹项目“The DAO”也宣布解散。

4.3 运行环境

智能合约是不能直接运行在区块链节点的外部环境上的,因为合约如果能够直接读写区块链,那么会给恶意代码创造可乘之机,因此智能合约必须运行在一个与外界隔离的沙箱环境中。目前主流的区块链智能合约的运行环境有两种:容器(container)和虚拟机(virtual machine)。

容器是一种轻量级的、可移植的、操作系统层面的虚拟机,它为应用软件及其依赖组件提供了一个资源独立的运行环境。容器是直接建立在宿主机操作系统之上的,容器中的应用软件所依赖的组件会被打包成一个可重用的镜像,镜像的运行环境不会与主操作系统共享内存、CPU、硬盘等资源,因此保证了容器内部的进程与容器外部进程的独立关系。Hyperledger Fabric 就使用轻量级的 Docker 作为智能合约的沙箱,容器的特性使智能合约的运行环境隔离了外部环境,防止了宿主机环境对智能合约的影响,也使各合约之间不会彼此干扰。

虚拟机作为一种成熟的虚拟技术,在许多领域得到了应用。与容器不同的是,虚拟机在宿主操作系统之上通过 Hypervisor 软件将宿主机的资源虚拟为 CPU、内存、I/O 等硬件资源,再在这些虚拟硬件上安装操作系统。以太坊的智能合约就运行在以太坊自定义的虚拟机 EVM 上,合约创建者在合约编译器中将合约编译成 EVM 能够执行的字节码,EVM 执行后将输出作为合约的代码永久存储在区块链上,当合约被调用时,节点读取链上的数据并在 EVM 中执行该合约内容,然后将结果打包进新块中。

5 隐私与安全

随着区块链的不断发展,不断增加的使用人数和不断扩大的应用领域使区块链承担了越来越多的价值,随之而来的隐私与安全问题也越来越受到人们的关注,甚至影响到了区块链的后续发展。

5.1 隐私性

中本聪在设计比特币时,通过每一次交易都生成一个新地址的方法来避免第三方对用户的交易行为进行归纳分析,进而保护用户的身份信息。但比特币并没有做到完全的匿名,同时所有节点都可以任意读取区块链上的交易记录,这也会造成用户的隐私泄露。

在比特币中用户是不需要实名的,客户端每次会为客户生成一套公私钥对,公钥用作交易时的交易地址,用户只需要掌握私钥,用于在用户作为发送方转移货币时对交易进行签名确认,比特币希望以此来实现用户的匿名性。但是,比特币中的每一笔交易都会记录输入地址和输出地址,而且交易金额等信息也都是可见的,而第三方往往能够通过对这些数据进行分析来得出更多信息,如通过分析交易特征和交易规律——用户的消费时间、消费金额、消费地点、消费商品等信息对用户画像[38-40],通过分析交易地址之间的关联关系确定地址所属账户,再通过社会学工程等方式确定用户的真实身份与比特币地址之间的关联[41-44]。区块链的隐私保护技术通常有以下几种(见表 2)。

表 2 隐私保护方法总结

Table 2 Summary of privacy protection methods

	“混币”技术	环签名技术	零知识证明	同态加密
是否依赖第三方	√	×	×	×
是否隐藏交易内容	√	×	√	√
是否隐藏交易地址	√	√	√	×
隐私保护性能	中	高	高	高
代表方案	MixCoin/CoinJoin	Monero	ZeroCash	—

(1)“混币”机制

“混币”机制最早由 Chaum[45] 于 1981 年提出，随后 Grey[46] 提出了混币方案 CoinJoin。CoinJoin 利用比特币交易多输入和多输出的特点，使每一个输入的金额相等且每一个输入都对应一个输出地址，混币参与者在看到接收地址中包含此次交易的接收方地址时就对交易进行了签名确认，混币通过模糊输入地址与输出地址之间的对应关系来隐藏输入输出的关联性。但该方案有一个弊端，即混合方是知道交易的具体信息的，针对该点研究者又提出了许多改进方案。例如 Bonneau 等[47] 提出了 Mixcoin 方案，该方案引入了多个混合方，每一个混合方的输入为下一个混合方的输出，通过这种链式结构可以让混合方无法得知完整的交易路径，从而在一定程度上保护了隐私。文献[48]在 Mixcoin 和 CoinJoin 的基础上，通过让中心节点缴纳保证金的方式来进一步防止中心节点的恶意行为。

(2)环签名技术

环签名(Ring Signature)[49] 的思想是签名方将自己的公钥隐藏在多个公钥中，而验证方只能验证消息是否为环中成员所签署而不知道具体是谁签署的。将环签名应用到区块链中可以实现发送方匿名，应用了环签名的区块链方案有基于 CryptoNote[50] 协议的门罗币(Monero)[51]、布尔币(Boolberry)[52]、StealthCoin、ByteCoin[53] 等。

(3)零知识证明

零知识证明(Zero-Knowledge Proof)[54] 由 Goldwasser 等于 1989 年提出。零知识证明指证明者在不提供除了证明本身之外的其他任何有用信息的情况下，向验证者证明某个结论是正确的。例如，假设某人宣称自己拥有某房间的钥匙，他只需要取出属于那个房间的，而其他地方没有的物品即可证明，该过程并未泄露任何关于钥匙本身的信息。区块链通过采用零知识证明来隐藏交易的详细信息，如输入、输出地址、交易金额等。文献[55]提出了一种利用零知识证明的系统——零币(ZeroCoin)，在零币中可以通过铸币将比特币转化为零币。文献[56]在零币的基础上提出了零钞(Zerocash)，该方案采用非交互式零知识证明技术[57](zk-SNARK)使零知识证明过程更加简洁高效。方案[58]在链下存储交易，通过 zk-SNARK 来验证交易从而保护隐私。Zerocash 是目前隐私保护性能最好的数字加密货币，能够将发送方、接收方、金额等信息全部隐藏，仅需证明交易的存在，zk-SNARK 技术也减少了证明和验证所需的计算量，但是因为其过程缓慢导致该方案性能受限。

(4)同态加密

同态加密理论(Homomorphic Encryption)于 1978 年被首次提出，Craig 于 2009 年首次提出全同态加密的可行方案[59]，使同态加密技术有了突破性的进展。同态加密指对密文进行代数运算后的结果经过解密处理后与用明文进行相应的代数运算得到的结果相同。例如，在加法同态中有明文 A 和 B，加密后的密文 $Enc(A)$ 和 $Enc(B)$，对密文进行加法操作 $C=Enc(A)+Enc(B)$，将 C 解密得到 C'，$C'=A+B$。同态加密在区块链中通常与零知识证明、承诺[60]、范围证明等密码学技术一起使用，来达到隐藏交易的具体信息并且验证交易合法的目的。

5.2 安全性

随着区块链的快速发展，随之而来的各种安全问题也是区块链不得不解决的重中之重。在区块链中常见的攻击有 51%攻击、日蚀攻击、自私挖矿、双花攻击、区块扣留攻击、无利害关系攻击、打磨攻击、权益窃取攻击[61-73] 等，下面主要介绍 51%攻击、日蚀攻击、自私挖矿、双花攻击、区块扣留攻击这 5 种常见攻击方式。

5.2.1 51%攻击

在使用 PoW 算法的区块链网络中，51%攻击是全网不得不重视的一个重要的安全问题。以比特币为例，比特币中采取最长链原则，全网节点只承认最长链上的数据为正确数据，而 PoW 算法通过竞争算力来获得记账权的特点不可避免地使算力强的节点获得优势，而一旦某个节点拥有超过全网 51%的算力，它就有能力对区块链造成破坏，如修改链上的数据进而发起双重花费攻击，延期或阻止某些交易上链从而使交易长时间或一直得不到确认，使其他矿工更难挖掘到新区块，让矿工的积极性受到严重打击，从而进一步造成垄断。但如今人们为了能更快地挖掘到新区块，降低挖矿成本和风险，将各自分散的算力集中在一起形成矿池。现今比特币中的算力几乎集中在各大矿池中，如 AntPool，BTC. COM，Poolin 等，前三大矿池的算力几乎占据了全网 51%的算力，算力的集中不仅与去中心化的初衷相悖，也对区块链的安全造成了威胁。

5.2.2 日蚀攻击

日蚀攻击(Eclipse Attack)是针对区块链网络层的攻击手段，攻击节点通过技术手段使被攻击节点连接的都是被自己控制的节点，从而使被攻击节点获得的区块链数据都是攻击者希望它所看到的，使被攻击者无法获得真实区块数据。

5.2.3 自私挖矿

自私挖矿(Selfish Mining)指矿工在挖到新块后并不立即发布，而是在该块的基础上继续挖掘下一区块，当自己挖掘出来的区块长度大于主链上新区块长度时再将全部区块发布到网络中，使自己成为最长主链。这种攻击不仅会损害诚实矿工的利益，打击矿工的积极性，还会造成区块链上的数据缺失。

5.2.4 双花攻击

双花攻击(Double Spending Attack)是数字货币中必须解决的攻击方式，也叫双重花费攻击，顾名思义即代币被花费了两次。在双花攻击中，攻击者在区块链上造成分叉，然后在另一不包含此次交易的区块上挖掘新块使之所在链成为最长链，攻击者重新获得自己已花费的代币。在比特币中，一个区块在发布后要等待其后面连续 6 个区块的确认后，该块中的交易才被认为是安全的、不可篡改的。

5.2.5 区块扣留攻击

区块扣留攻击(Block Withholding Attack)常发生在矿池之间的恶意竞争。区块扣留攻击指矿工在挖掘出新块后，并不上交正确的 *nonce* 值而是选择不发布该区块，从而造成对该矿池其余矿工的利益损害。

6 区块链的进展与未来

6.1 可扩展性

(1)多链技术

多链指在区块链中有多条并行存在的链。分片是属于多链技术的一种应用。现在主流区块链几乎都是采用 PoW 共识、PoS 共识、PBFT 共识或是它们的改进算法,但是吞吐量一直是制约区块链发展的重要瓶颈。分片技术[74-75]是当前解决区块链交易处理速度慢、系统吞吐量低的较好思路,具有很好的研究前景,以太坊就计划在其新版本中使用分片技术来提高系统的吞吐量。区块链中的分片技术的核心思想是将区块分配到不同的片区,该片区内的节点只负责处理以及验证该分片内的交易,这样在整个区块链网络中通过各个片区并行地运行使区块链网络的处理速度成倍增长。但分片技术若要很好地在区块链中运用,则必须要解决跨片通信和状态交换等问题。除此之外,多链技术还包括 Hyperledger Fabric 的通道技术、Cosmos 中的 zone[76]。

(2)侧链技术

侧链技术指在主链之外还存在一条独立的区块链,这条区块链上可以有自己的账本、交易类型、共识机制、智能合约,通过双向锚定的方式可以实现数字资产在主链和侧链上的互转,是一种可以在不改变主链的情况下扩展主链性能的一种方式。闪电网络[77]是比特币的一种侧链,是一种实现微支付的手段,能够满足微支付的高频、小额、立即确认的需求。在闪电网络中支付是在主链之外完成的,主链只记录交易的最终执行结果,这不仅变相扩展了主链的存储空间,也保护了交易的隐私性。Mimble Wimble 也是一种比特币的侧链方案,它通过取消比特币的交易地址、隐藏交易金额、删除交易的中间状态使其具有较强的隐私保护性能,同时能节省主链的存储空间。

(3)共识算法

区块链共识算法的改进是提高区块链性能的重要研究方向,目前有针对 PoW, PoS, PBFT 等算法本身进行改进的,有不同共识算法混合使用的,也有对传统分布式共识算法做出改进以适应区块链的。文献[78]中的系统通过 PoW 算法选出关键块的出块者,然后由出块者产生微块来记录交易,提高了系统的交易处理速度。文献[79]针对自私挖矿攻击提出了解决方案。文献[80]基于有向无环图(Derected Acyclic Graph, DAG)的 Spectre 共识机制,使所有的区块形成一个无环图状结构,提高了系统的交易处理速度和吞吐量。以太坊的 Casper FFG 共识机制采用基于 Ethash(基于存储困难)的工作量证明机制与 PoS 共识机制结合的方式,为以太坊下一阶段的纯 PoS 共识做铺垫。同样结合 PoW 共识和 PoS 共识的还有 2-hop[81]、燃烧证明(proof of burn, PoB)、活动证明[82](Proof of Activity, PoA)。文献[83]使用了改进的 PBFT 算法。文献[84]中的系统结合了 PoS 算法与经典分布式一致算法。文献[85]中的系统结合了 PBFT 算法与 PoW 算法。

6.2 未来发展

5G 意味着一个万物互联的时代即将来临,随着 5G 的逐步落地,人工智能、大数据、云计算、边缘计算、区块链、物联网[86-99]也迎来了一波高潮。5G 的高传输速率和高带宽解决了区块链的传输时延问题,而区块链去中心化、不可篡改等优势也与 5G 应用形成互补。区块链与物联网的结合是目前区块链发展的重要方向。

物联网(Internet of Things, IoT)是一个由众多物理设备组成的分布式网络,通常这些物理设备具有用于采集数据的传感器和一定的计算和存储能力,可以先对数据进行简单的处理,但最终要将数据传输到中心服务器进行处理,数据在终端节点和中心服务器之间的来回传输不仅会消耗大量带宽,还会对数据的安全产生威胁,并且对于一些对实时性要求较高的场景如自动驾驶来说,较高的时延意味着巨大的安全隐患。而物联网与区块链的结合可以使设备之间通过直接通信来缩短数据的传输时延,再结合边缘计算等技术,不仅可以解决闲置资源浪费等问题,也缩短了终端设备与服务器之间的传输距离。但是,区块链在物联网等领域的应用还要解决共识速度慢的问题,物联网频繁的数据传递要求区块链有更快的交易处理速度,同时海量的数据也对区块链的存储性能形成了巨大的考验,而存储在链上的未加密数据也会造成隐私数据的泄露问题。区块链与物联网、人工智能等技术作为构成未来社会的关键技术,本身就有巨大的研究价值与空间,而区块链与这些技术的结合更是一个重要的研究方向,仍然需要更多的研究者投入更多的精力进行深入研究。

结束语 本文介绍了区块链的底层技术和架构,重点介绍了区块链的隐私保护、共识机制、安全问题、智能合约等方面。区块链在传统互联网的基础上还拥有去中心化、相互信任等传统互联网所不具备的特点,可以大胆畅想未来的互联网将呈现一个以区块链为核心的价值互联网,出现区块链位于互联网之上,而软件应用位于区块链之上的新型互联网结构。随着 5G 时代的来临,区块链将不可避免地与物联网、云计算、大数据、AI 等技术产生接触,而如何使它们更好地融合从而让区块链更好地服务于人类社会将是未来研究者们的一个重要方向。

参 考 文 献

[1] YAO Z J, GE J G. A Summary o the Theory and Application of BlockChain [J]. E-Science Technology & Aplication, 2017, 8(2): 3-17.

[2] HE P, YU G, ZHANG Y F, et al. Survey on Blockchain Technology and Its Application Prospect [J]. Computer Science, 2017, 44(4): 1-7, 15.

[3] SHAO Q F, ZHANG Z, ZHU Y C, et al. Survey of enterprise blockchains [J]. Ruan Jian Xue Bao, 2019, 30(9): 25712592.

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2020-06-13]. https://bitcoin.org/bitcoin.pdf.

[5] CAO B, LIN L, LI Y, et al. Review of blockchain research [J]. Journal of Chongqing University of Post and Telecommunication (Natural Science Edition), 2020, 32(1): 1-14.

[6] Pete Rizzo. Linq [EB/OL]. [2020-10-28]. http://www.coindesk.com/hands-on-with-linq-nasdaqs-private-markets-blockchain-project/.

[7] EYAL I. Blockchain Technology: Transforming Libertarian

Cryptocurrency Dreams to Finance and Banking Realities [J]. Computer,2017,50(9):38-49.

[8] BROWN R G,CARLYLE J,GRIGG I,et al. Corda:An introduction. [EB/OL]. [2020-05-10]. https://cncorda. readthedocs. io/zh_CN/latest/.

[9] BUTERIN V. A next-generation smart contract and decentralized application platform White Paper [EB/OL]. [2020-06-18]. https://github. com/ethereum/wiki /wiki / White-Paper.

[10] YUAN Y,WANG F Y. Blockchain:The State of The Art and Future Trends[J]. Acta Automatica Sinica,2016,42(4):481-494.

[11] ERKLE R C. Protocols for public key cryptosys-tems[C]// Proceedings of the 1980 IEEE Symposium on Security and Privacy (S&P). Oakland,USA,1980:122-134.

[12] ERKLE R C. A digital signature based on a conventional encryption function[C]// Proceedings of the Advances in Cryptology— CRYPTO'87 (CRYPT-O). Santa Barbara,USA,1987:369-378.

[13] SZYDLO M. Merkle tree traversal in log space and time[C]// Proceedings of the Advances in Cryptology — EUROCRYPT. 2004(EUROCRYPT). Interlaken,Switzerland,2004:541-554.

[14] Hyperledger Fabric [EB/OL]. [2020-10-28]. https://wiki. hyperledger. org/display/Fabric.

[15] WANG X L,ZHANG J. Survey on peer-to-peer key technologies [J]. Application Research of Computers,2010,27(3):801-805.

[16] BAYER D,HABER S,STORNETTAW S. Improving the efficiency and reliability of digital time-stamping[C]// Sequences II:Methods in Communication,Security and Computer Science. NewYork,USA:Springer-Verlag,1993:329-334.

[17] HABER S,STORNETTA W S. How to time-stamp a digital document[C]// Proceedings of the Advances in Cryptology-CRYPTO'90(CRYPTO). Santa Barbara,USA,1990:437-455.

[18] HABER S,STORNETTA W S. Secure names for bit-strings [C]// Proceedings of the 4th ACM Conferenceon Computer and Communications Security(CCS). Zurich,Switzerland,1997:28-35.

[19] YANG Y G,ZHANG S X. Review and Research for Consensus Mechanism of Block Chain[J]. Journal of Information Security Research,2018,4(4):369-379.

[20] GILBERT S,LYNCH N. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant Web services [J]. ACM SIGACT News,2002,33(2):51-59.

[21] YUAN Y,NI X C,ZENG S,et al. Blockchain Consensus Algorithms:The State of The Art and Future Trends[J]. Acta Automatica Sinica,2018,44(11):2011-2022.

[22] LAMPORT L. The Part-Time Parliament [J]. ACM Transactions on Computer Systems,1998,16(2):133-169.

[23] ONGARO D,OUSTERHOUT J. In search of an understandable consensus algorithm[C]// The 2014 USENIX Conference on USENIX Annual Technical Conference. USENIX Association,2015:305-320.

[24] LAMPORT L,SHOSTAK R,PEASE M. The Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems,1982,4(3):382-401.

[25] CASTRO M,LISKOV B. Practical Byzantine fault tolerance [C]// Proceedings of the Third USENIX Symposium on Operating Systems Design and Implementation (OSDI). New Orleans,LA,USA,1999:173-186.

[26] GOLAN-GUETA G,ABRAHAM I,GROSSMAN S,et al. SBFT:A scalable decentralized trust infrastructure for Blockchains[EB/OL]. [2020-05-18]. https://arxiv. org/pdf/1804.01626. pdf.

[27] AUBLIN P L,MOKHTAR S B,QUÉMA V. Rbft:Redundant byzantine fault tolerance[C]// IEEE. 2013 IEEE 33rd International Conference on Distributed Computing Systems. New York:IEEE,2013:297-306.

[28] DWORK C,NAOR M. Pricing via Processing or Combatting Junk Mail[C]// Springer-Verlag. 1993.

[29] BACK A. Hashcash-a Denial of Service Counter-Measure[EB/OL]. [2020-06-11]. http://www. hashcash. org/papers/hashcash. pdf,2002-8-1.

[30] SUNNY K,SCOTT N. PPcoin:Peer-to-Peer Crypto-Currency with Proof-of-Stake[EB/OL]. [2020-06-10]. https://decred. org/research/king2012. pdf,2012-8-19.

[31] LARIMER D. Transactions as proof-of-Stake[EB/OL]. [2020-06-10]. https://bravenewcoin. com/assets/Uploads/TransactionsAsProofOfStake10. pdf.

[32] BUTERIN V,GRIFFITH V. Casper the Friendly Finality Gadget[OL]. http://www. aas. net. cn/article/doi/10. 16383/j. aas. 2018. c180268.

[33] LARIMER D. Delegated Proof-of-stake (DP-oS) [EB /OL]. [2020-05-08]. http: // bitsharestalk. org/index. php? topic = 4009. 60.

[34] SZABO N. Formalizing and Securing Relationships on Public Networks[EB/OL]. [2020-06-18]. http://www. firstmonday. org/ojs/index. php/fm/article/view/548/469.

[35] JEREMYVINFOLIO. Serpent[EB/OL]. [2020-06-20]. https://github. com/ethereum/wiki/wiki/Serpent.

[36] ETHEREUM. Solidity[EB/OL]. [2020-06-20]. http://solidity. readthedocs. io/en/latest.

[37] DANNEN C. Introducing Ethereum and Solidity:Foundations of Cryptocurrency and Blockchain Programming for Beginners [EB/OL]. [2020-06-20]. https://lip. hpu. edu. vn/handle/123456789/28117.

[38] RON D,SHAMIR A. Quantitative Analysis of the Full Bitcoin Transaction Graph[C/OL]// Financial Cryptography and Data Security. Lecture Notes in Computer Science. https://doi. org/10. 1007/978-3-642-39884-1_2.

[39] LIAO K,ZHAO Z,DOUPE A,et al. Behind closed doors:Measurement and analysis of CryptoLocker ransoms in Bitcoin [C]// Symposium on Electronic Crime Research. Toronto,ON,2016:1-13.

[40] EYAL I,SIRER E G. Majority is not Enough:Bitcoin Mining is Vulnerable[J]. Communications of the ACM,2018,61(7):95-102.

[41] REID F,HARRIGAN M. An Analysis of Anonymity in the Bitcoin System[C]// IEEE Third International Conference on IEEE Third International Conference on Privacy. IEEE,2012.

[42] ZYSKIND G, NATHAN O, PENTLAND A. Decentralization Privacy: Using Blockchain to Protect Personal Data[J]. IEEE Security and Privacy Workshops, 2015: 180-184.

[43] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: characterizing payments among men with no names [J]. Communications of the ACM, 2016, 59(4): 86-93.

[44] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating User Privacy in Bitcoin[C]// International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013.

[45] CHAU M, DAVID L. Untraceable electronic mail , return addresses, and digital pseudonyms [J]. Communications of the Acm, 1981, 24(2): 84-90.

[46] MAXWELL G. Confidential Transactions [EB/OL]. [2020-06-13]. https://people. xiph. org/~greg/confidential_values. txt, 2017-4-28.

[47] BONNEAU J , NARAYANAN A , MILLER A, et al. Mixcoin: Anonymity for Bitcoin with Accountable Mixes[C]// International Conference on Financial Cryptography & Data Security. Springer, Berlin, Heidelberg, 2014.

[48] Dash. Dashis digital cash[EB/OL]. [2020-06-15]. https://www. dash. org/.

[49] RIVEST R L, SHAMIR A, TAUMAN Y. How to Leak a Secret [C]// International Conference on the Theory & Application of Cryptology & Information Security. Springer, Berlin, Heidelberg, 2001.

[50] BERGAN T, ANDERSON O, DEVIETTI J, et al. CryptoNote v 2. 0[EB/OL]. [2020-06-17]. https: // www. mendeley. com/research-papers/ cryptonote-v-20/, 2017-4-28.

[51] Monero. AboutMonero[EB/OL]. [2020-06-17]. https: // getmonero. org/knowledge-base/about.

[52] Boolberry. What is Boolberry[EB/OL]. [2020-06-17]. https: // www. boolberry. com.

[53] Bytecoin. A clear way to your private future[EB/OL]. [2020-06-19]. https: // cn. bytecoin. org.

[54] GOLDWASSER S, MICALI S, RACKOFF C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing, 1989, 18(1): 186-208.

[55] MIERS I, GARMAN C, GREEN M, et al. Zerocoins: anonymous distributed E-cash from bitcoin[C]// Proceedings of IEEE Symposium on Security and Privacy. USA: IEEE Press, 2013: 394-411.

[56] ASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// Proceedings of the 2014 IEEE Symposium on Security and Privacy. NJ: IEEE, 2014: 459-474.

[57] SBEN-SASSON E, CHIESA A, GENKIN D, et al. SNARKs for C: Verifying program executions succinctly and in zero knowledge[C]// Proceedings of the Advances in Cryptology-CRYPTO 2013(CRYPTO). Santa Barbara, USA, 2013: 90-108.

[58] KOSBA A, MILLER A, SHI E, et al. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts [C]// 2016 IEEE Symposium on Security and Privacy (SP). 2016: 839-858.

[59] GENTRY C. Fully homomorphic encryption using ideal lattices [C]// Proceedings of the 41st Annual ACM Symposium on Theory of Computering(STOC). Bethesda, USA, 2009: 169-178.

[60] PEDERSEN T P. Non-Interactive and Information-Theoretic Secure Verifiable SecretSharing[C]// International Cryptology Conference on Advances in Cryptology. Springer-Verlag, 1991: 129-140.

[61] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse Attacks on Bitcoin's Peer-to-Peer Network[C]// Usenix Conference on Security Symposium. USENIX Association, 2015.

[62] MARCUS Y, HEILMAN E, GOLDBERG S. Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network[J]. IACR Cryptology ePrint Archive, 2018, 2018: 236.

[63] BONNEAU J. Why Buy When You Can Rent? [C]// International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2016.

[64] LIAO K , KATZ J. Incentivizing Blockchain Forks via Whale Transactions[C/OL]// Financial Cryptography and Data Security. https: // doi. org/10. 1007/978-3-319-70278-0_17.

[65] EYAL I. The miner's dilemma[C]// Proceedings of 2015 IEEE Symposium on Security and Privacy (SP 2015). IEEE, 2015: 89-103.

[66] BONNEAU J, MILLER A, CLARK J, et al. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies[C]// 2015 IEEE Symposium on Security and Privacy. IEEE, 2015.

[67] NAYAK K, KUMAR S, MILLER A, et al. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack[C]// IEEE European Symposium on Security & Privacy. IEEE, 2016.

[68] SAPIRSHTEIN A, SOMPOLINSKY Y, ZOHAR A. Optimal selfish mining strategies in Bitcoin[C]// Financial Cryptography and Data Security—FC 2016. Revised Selected Papers. Springer Berlin Heidelberg, 2016: 515-532.

[69] BAG S, RUJ S, SAKURAI K. Bitcoin block withholding attack: Analysis and mitigation[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(8): 1967-1978.

[70] KWON Y, KIM D, SON Y, et al. Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on Bitcoin[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS 2017). ACM, 2017: 195-209.

[71] BISSIAS G, LEVINE B N, OZISIK A P, et al. An analysis of attacks on Blockchain consensus[EB/OL]. [2020-06-22]. http: // arxiv. org/abs/1610. 07985.

[72] CONTI M, KUMAR E S, LAL C, et al. A survey on security and privacy issues of Bitcoin[J]. IEEE Communications Surveys and Tutorials, 2018, 20(4): 3416-3452.

[73] SAAD M, NJILLA L, KAMHOUA C, et al. Countering Selfish Mining in Blockchains[C]// 2019 International Conference on Computing, Networking and Communications (ICNC). Honolulu, Hawaii: IEEE, 2019: 360-364.

[74] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding[C]// 2018 IEEE Symposium on Security and Privacy (SP). San Francisco, CA: IEEE, 2018: 583-598.

[75] LUU L, NARAYANAN V, ZHENG C D, et al. A Secure Shar-

ding Protocol For Open Blockchains[C]// The 2016 ACM SIGSAC Conference. Vienna, Austria: ACM, 2016: 17-30.

[76] KWON J, BUCHAMN E. Cosmos: A network of distributed ledgers[OL]. https://github.com/cosmos/cosmos-sdk/.

[77] POON J, DRYJA T. The Bitcoin lightening network: Scalable off-chain instant payments[OL]. https://lightning.network/docs.

[78] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: A scalable Blockchain protocol[C]// Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2016). Santa Clara, CA, USA, 2016: 45-59.

[79] PASS R, SHI E. FruitChains: A fair Blockchain[C]// Proceedings of the ACM Symposium on Principles of Distributed Computing (PODC 2017). ACM, 2017: 315-324.

[80] SOMPOLINSKY Y, LEWENBERG Y, ZOHAR A. SPECTRE: A fast and scalable crypto currency protocol[J]. IACR Cryptology ePrint Archive, 2016(2): 1159.

[81] DUONG T, FAN L, ZHOU H S. 2-hop Blockchain: Combining proof-of-work and proof-of-stake securely[J]. IACR Cryptology ePrint Archive, 2016(4): 716.

[82] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: Extending Bitcoin's proof of work via proof of stake[J]. SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37.

[83] ABRAHAM I, MALKHI D, NAYAK K, et al. Solida: A Blockchain protocol based on reconfigurable Byzantine consensus [C]// Proceedings of 21st International Conference on Principles of Distributed Systems (OPODIS 2017). 2017(25): 1-19.

[84] GILAD Y, HEMO R, MICALI S, et al. Algorand: Scaling Byzantine agreements for cryptocurrencies[C]// Proceedings of the 26th Symposium on Operating Systems Principles. Shanghai, 2017: 51-68.

[85] KOKORIS-KOGIAS E, JOVANOVIC P, GAILLY N, et al. Enhancing Bitcoin security and performance with strong consistency via collective signing[C]// Proceedings of 25th USENIX Security Symposium. USENIX, 2016: 279-296.

[86] ZOU J, DONG Z, SHAO A, et al. 3D-DAG: A High Performance DAG Network with Eventual Consistency and Finality[C]// 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). Shenzhen: IEEE, 2018: 262-263.

[87] THAM C, CAO B. Stochastic Programming Methods for Workload Assignment in an Ad Hoc Mobile Cloud[J]. IEEE Transactions on Mobile Computing, 2018, 17(7): 1709-1722.

[88] THAM C, CAO B. Stochastic Programming Methods for Workload Assignment in an Ad Hoc Mobile Cloud[J]. IEEE Transactions on Mobile Computing, 2018, 17(7): 1709-1722.

[89] LEI A, CRUICKSHANK H, CAO Y, et al. Blockchain- based dynamic key management for heterogeneous intelligent transporttation systems[J]. IEEE Internet Things, 2017, 4(6): 1832-1843.

[90] TIAGO M. FERNNDEZ C. An Intelligent Power Outlet System for the Smart Home of the Internet of Things[J]. International Journal of Distributed Sensor Networks, 2015, 2015(1): 1-11.

[91] SIDDIQI M, ALL S V, SIVARAMAN V. Secure light- weight context-driven data logging for bodyworn sensing devices[C]// 2017 5th International Symposium on Digital Forensic and Security (ISDFS). New York: IEEE, 2017: 1-6.

[92] KSHETRI N. Can blockchain strengthen the Internet of Things? [J]. IT Professional, 2017, 19(4): 68-72.

[93] TIAN F. An agrifood supply chain traceability system for China based on RFID &-blockchain technology[C]// Proc 13th Int Conf Service Syst Service Manage (ICSSSM). Kunming: IEEE, 2016: 1-6.

[94] SUANKAEWMANEE K, HOANG D T, NIYATO D, et al. Performance Analysis and Application of Mobile Blockchain[C]// 2018 International Conference on Computing, Networking and Communications (ICNC). Maui, HI: IEEE, 2018: 642-646.

[95] XU F, YANG F, ZHAO C, et al. Edge Computing and Caching based Blockchain IoT Network[C]// 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). Shenzhen: IEEE, 2018: 238-239.

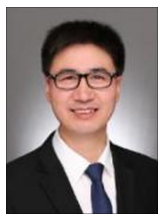
[96] XIA C, CHEN H, LIU X, et al. ETRA: Efficient Three-Stage Resource Allocation Auction for MobileBlockchain in Edge Computing[C]// 2018 IEEE 24th International Conference on Parallel and Distributed Systems (IC-PADS). Singapore: IEEE, 2018: 701-705.

[97] ZHANG H, ZHANG Y, GU Y. A Hierarchical Game Framework for Resource Management in Fog Computing[J]. IEEE Communications Magazine, 2017, 55(8): 52-57.

[98] XIONG Z, ZHANG Y, NIYATO D, et al. When Mobile Blockchain Meets Edge Computing[J]. IEEE Communications Magazine, 2018, 56(8): 33-39.

[99] RAHMAN M A. Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications[J]. IEEE Access, 2018(6): 72469-72478.

GUO Shang-tong, born in 1995, postgraduate, is a member of China Computer Federation. His main research interests include blockchain and privacy protection.



WANG Rui-jin, born in 1980, associate professor, is a member of China Computer Federation. His main research interests include information security, privacy protection and blockchain.