



信息通信领域产学研合作特色期刊 | 十佳皖刊
第三届全国期刊奖百种重点期刊 | 中国科技核心期刊

ISSN 1009-6868
CN 34-1228/TN
CODEN ZTJHAY

中兴通讯技术

ZTE TECHNOLOGY JOURNAL

<http://tech.zte.com.cn>

2018年12月 • 第6期

专题：区块链技术及其物联网应用

BLOCKCHAIN



《中兴通讯技术》第8届编辑委员会成员名单

- 顾问

侯为贵（中兴通讯股份有限公司创始人） | 钟义信（北京邮电大学教授） | 陈锡生（南京邮电大学教授）
- 主任

陆建华（中国科学院院士）
- 副主任

徐子阳（中兴通讯股份有限公司总裁） | 糜正琨（南京邮电大学教授）

编委（按姓名拼音排序）

- 陈建平

上海交通大学教授
- 陈前斌

重庆邮电大学副校长
- 葛建华

西安电子科技大学教授
- 管海兵

上海交通大学教授
- 郭庆

哈尔滨工业大学教授
- 洪波

中兴发展股份有限公司总裁
- 洪伟

东南大学教授
- 纪越峰

北京邮电大学教授
- 蒋林涛

中国信息通信研究院科技委主任
- 李尔平

浙江大学教授
- 李红滨

北京大学教授
- 李建东

西安电子科技大学副校长
- 李军

清华大学教授
- 李乐民

中国工程院院士
- 李融林

华南理工大学教授
- 李少谦

电子科技大学教授
- 刘建伟

北京航空航天大学教授
- 陆建华

中国科学院院士
- 马建国

广东工业大学教授
- 孟洛明

北京邮电大学教授
- 糜正琨

南京邮电大学教授
- 任品毅

西安交通大学教授
- 孙知信

南京邮电大学教授
- 谈振辉

北京交通大学教授
- 唐雄燕

中国联通网络技术研究院首席科学家
- 王文博

北京邮电大学副校长
- 王文东

北京邮电大学教授
- 王喜瑜

中兴通讯股份有限公司执行副总裁
- 王翔

中兴通讯股份有限公司高级副总裁
- 卫国

中国科学技术大学教授
- 吴春明

浙江大学教授
- 邬贺铨

中国工程院院士
- 徐安士

北京大学教授
- 徐子阳

中兴通讯股份有限公司总裁
- 续合元

中国信息通信研究院副总工
- 薛一波

清华大学教授
- 杨义先

北京邮电大学教授
- 杨震

南京邮电大学校长
- 易芝玲

中国移动研究院首席科学家
- 张宏科

北京交通大学教授
- 张平

北京邮电大学教授
- 张云勇

中国联通研究院院长
- 赵慧玲

工业和信息化部科技委信息网络专家组组长
- 郑纬民

清华大学教授
- 钟章队

北京交通大学教授
- 周亮

南京邮电大学教授
- 朱近康

中国科学技术大学教授
- 祝宁华

中国科学院半导体研究所副所长



信息通信领域产学研合作特色期刊
第三届国家期刊奖百种重点期刊
中国科技核心期刊
工信部优秀科技期刊
十佳皖刊
中国五大文献数据库收录期刊
1995年创刊

办刊宗旨

以人为本,荟萃通信技术领域精英
迎接挑战,把握世界通信技术动态
立即行动,求解通信发展疑难课题
励精图治,促进民族信息产业崛起

Contents 目次

中兴通讯技术 (ZHONGXING TONGXUN JISHU) 总第143期 第24卷 第6期 (卷终) 2018年12月

专题：区块链技术及其物联网应用

- 02 区块链共识机制研究: 典型方案对比 刘懿中, 刘建伟, 喻辉
08 区块链共识机制发展与安全性 王李笑阳, 秦波, 乔鑫
13 比特币生成原理及其特点 林成骏, 伍玮
19 区块链概念剖析及其在物联网中的部分应用 田海博
23 基于区块链的物联网密钥协商协议 张佳妮, 何德彪, 李莉
28 基于区块链的电子数据存证的设计与实现 冒小乐, 陈鼎洁, 孙国梓
35 区块链技术在物联网中的身份认证研究 杨惠杰, 周天祺, 桂梓原
41 一种基于区块链的身份识别技术 苏宣瑞, 邹秀清, 丁勇

专家论坛

- 49 区块链的理想与现实 何宝宏
52 区块链: 描绘物联网安全新愿景 徐恪, 吴波, 沈蒙

企业视界

- 56 NG-PON 技术背景、应用和展望 陈爱民

技术广角

- 60 基于 BGP 的域间二维路由方案 耿男, 金飞蔡, 徐明伟

综合信息

《中兴通讯技术》2019年专题计划(59) 《中兴通讯技术》第24卷总目次(I)

期刊基本参数: CN 34-1228/TN*1995*b*16*64*zh*P* ¥ 20.00*15000*12*2018-12

Contents 目次

ZTE TECHNOLOGY JOURNAL Vol. 24 No. 6 Dec. 2018

Special Topic: Blockchain Technology and Its Application in Internet of Things

- 02 Research on Blockchain Consensus: Comparison of Typical Schemes LIU Yizhong, LIU Jianwei, YU Hui
- 08 Development and Security of Blockchain Consensus Mechanism WANG Lixiaoyang, QIN Bo, QIAO Xin
- 13 The Generation Principles and Characteristics of Bitcoin LIN Chengjun, WU Wei
- 19 Concept and Partial Applications of Blockchain in Internet of Things TIAN Haibo
- 23 Blockchain-Based Key Agreement Protocol for Internet of Things ZHANG Jiani, HE Debiao, LI Li
- 28 Design and Implementation of Electronic Data Storage and Certificate System Based on Blockchain MAO Xiaole, CHEN Dingjie, SUN Guozi
- 35 Blockchain Technology for Identity Authentication in Internet of Things YANG Huijie, ZHOU Tianqi, GUI Ziyuan
- 41 An Authentication Technology Based on Blockchain SU Xuanrui, ZOU Xiuqing, DING Yong

Expert Forum

- 49 Vision and Reality of Blockchain HE Baohong
- 52 Blockchain: New Vision for Security of Internet of Things XU Ke, WU Bo, SHEN Meng

Enterprise View

- 56 The Technical Background, Application and Prospect of NG-PON CHEN Aimin

Technology Perspective

- 60 A Design of Inter-Domain Destination and Source Routing Based on BGP GENG Nan, JIN Feicai, XU Mingwei

敬告读者

本刊享有所发表文章的版权,包括英文版、电子版、网络版和优先数字出版版权,所支付的稿酬已经包含上述各版本的费用。

未经本刊许可,不得以任何形式全文转载本刊内容;如部分引用本刊内容,须注明该内容出自本刊。

2018年第1—6期专题

1 5G 承载网技术和优化组网

张云勇 中国联通研究院院长
徐雷 中国联通研究院高级工程师

2 大数据智能化无线网络技术

陈前斌 重庆邮电大学副校长

3 毫米波与太赫兹通信技术的应用

洪伟 东南大学教授
王海明 东南大学教授

4 5G 回传网络光电子器件技术

孙笑晨 苏州洛合镭信光电科技有限公司技术总监
王会涛 中兴光电子技术有限公司规划总监

5 可再生能源供电的无线通信与网络

牛志升 清华大学教授
易芝玲 中国移动研究院首席科学家

6 区块链技术及其物联网应用

刘建伟 北京航空航天大学教授

专题：区块链技术及其物联网应用

策划人简介



刘建伟

北京航空航天大学教授、博士生导师，网络空间安全学院院长、党委书记，中国密码学会理事，教育部高等学校信息安全专业教学指导委员会委员；长期从事网络安全、密码学的教学和科研工作；享受中华人民共和国国务院政府特殊津贴，科研成果分别获得国家技术发明一等奖、国防技术发明一等奖、山东省计算机应用新成果二等奖、山东省科技进步三等奖，2015年分别荣获北京教学名师奖、北航教学名师奖，2016年荣获中国互联网发展基金会网络安全优秀教师奖，2017年荣获北京市优秀教师奖、北京市教学成果二等奖等；发表SCI/EI收录论文200余篇，出版教材5部、译著1部，获授权发明专利46项，软件著作权登记3项。

内容导读

作为现代密码学、分布式计算、共识机制等技术的综合应用，区块链技术逐渐受到了社会各界的广泛关注。区块链技术具有去中心化、开放透明、信息不可篡改、隐私保护等特点，在数字经济、电子商务、身份认证、社交通信、物联网(IoT)、数据存证、食品安全等诸多领域有着良好的应用前景。区块链技术由此逐渐成为计算机科学领域的一项新兴热点技术。

快速发展的区块链技术也面临着巨大的挑战。首先，区块链作为分布式系统，需要花费一定的计算和通信资源来达成共识，严重制约了区块链的运行效率。虽然通过改进共识算法，区块链的处理能力从比特币每秒处理7次交易，提升到以太坊每秒处理20次交易，乃至到Omniledger每秒处理上千次交易；然而与当前主流支付系统如VISA、支付宝和银联等的交易吞吐率相比，现有的区块链方案还远远达不到日常的使用需求。其次，区块链在提供安全特性的同时，自身也存在着安全问题。据Carbon Black的调查数据，仅2018年上半年，有价值约11亿美元的数字加密货币被盗。如何更好地利用区块链技术服务实体经济，将区块链技术与国家信息科技发展结合起来依然是一个亟需解决的重要课题。

本期专题就区块链的技术原理、发展现状和趋势、关键技术和IoT应用展开讨论。在区块链的基础原理方面，《比特币生成原理及其特点》介绍了区块链最初的应用——比特币的生成原理和特色，简要讨论目前区块链技术存在的缺陷；《区块链共识机制研究：典型方案对比》主要介绍了区块链的核心共识算法的主要技术路线和当前的研究现状，分析了每一类共识机制的优缺点。在区块链中的安全风险方面，《区块链共识机制发展与安全性》着重对共识机制中存在的攻击威胁和防范策略进行解析；《区块链概念剖析及其在物联网中的部分应用》分析了IoT场景下几个典型的区块链项目，并对其中的主要问题和主要方法进行了分析，并指出IoT的数据体量和数据安全问题依旧需要重点考虑。在区块链的应用研究方面，《基于区块链的物联网密钥协商协议》提出使用基于身份的Schnorr签名替换原有的椭圆曲线数字签名算法(ECDSA)签名，实现IoT设备间轻量级的身份认证；《区块链技术在物联网中的身份认证研究》提出了应用于体域网身份认证的区块链系统框架，探讨了在IoT平台中区块链技术可能存在的问题和未来发展方向；《基于区块链的电子数据存证的设计与实现》介绍一种基于区块链的电子数据存证系统，致力于解决电子数据存证存在的安全问题；《一种基于区块链的身份识别技术》基于以太坊的智能合约技术提出一种新型身份识别系统，具有高拓展性、高可靠性、高安全性的特点，支持不同平台进行统一的身份认证。本期专题论文来自北京航空航天大学、人民大学、复旦大学、武汉大学、中山大学、南京信息工程大学、南京邮电大学、桂林电子科技大学等中国知名高校的区块链研究专家学者，凝聚了他们的研究成果和工作经验，希望能给读者提供有益的启示和参考。在此，对各位作者的大力支持表示衷心感谢。

刘建伟

2018年11月20日

区块链共识机制研究: 典型方案对比

Research on Blockchain Consensus: Comparison of Typical Schemes

刘懿中/LIU Yizhong
刘建伟/LIU Jianwei
喻辉/YU Hui

(北京航空航天大学, 北京 100191)
(Beihang University, Beijing 100191, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0002-006

摘要: 共识机制是区块链技术的核心, 研究了区块链现有的共识机制, 并分类如下: 基于工作量证明(PoW)的共识机制、基于权益证明(PoS)的共识机制、采用单一委员会的混合共识机制和采用多委员会的混合共识机制。给出了每一类共识机制的基本流程, 并列举相应的典型方案, 分析了每一类共识机制的优缺点, 指出了区块链共识机制未来的研究方向。

关键词: 区块链; 共识机制; PoW; PoS; 拜占庭容错

Abstract: The core problem of blockchain is consensus. In this paper, the current consensus mechanisms of blockchain are classified as follows: the proof-of-work (PoW) consensus, the proof-of-stake (PoS) consensus, the hybrid consensus based on single-committee and hybrid consensus based on multiple-committees. The basic procedure of every kind of consensus is listed and enumerate corresponding typical schemes are given. Then the advantages and disadvantages of different kinds of consensus are analyzed. Finally, the future research direction of consensus is given.

Keywords: blockchain; consensus mechanism; PoW; PoS; byzantine fault tolerance

1 背景和相关工作

2008年, 化名为“中本聪”的研究人员首次提出了比特币^[1]。在随后几年中, 数字货币发展迅速, 出现了像以太坊、莱特币等具有代表性的一些数字货币。而支撑这类数字货币的区块链技术也逐渐得到研究人员的重视。

区块链技术保证在不可信、分布式环境下, 所有节点通过一定的共识算法对公共账本达成一致。在区块链中, 账本以区块的形式构成, 每个合法的区块都以特定的密码学方式链接到前一个块, 这也就是区块“链”的内涵。随着区块的不断生成和添加, 历史区块内容不能被修改, 区块中记录的所有内容能够被网络中所有节点获取。

区块链具有去中心化、公开透明、历史数据防篡改等特点。区块链的共识不需要任何可信的第三方, 所有分布式节点参与共识。在公有链

中, 任何节点能够自由加入、退出网络, 节点数量随时变化并且不可预知。一旦区块链中区块数据达到一定的“深度”(例如: 在比特币中, 超过6个区块), 则可认定区块内容很大概率不会被篡改。

目前区块链的体系架构一般分为以下几个层面: 从下到上依次是数据层、网络层、共识与激励层、合约层和应用层。数据层包括最基本的交易数据、区块数据和时间戳等, 数据层采用哈希函数、数字签名等密码学技术, 为区块链提供最基本的安全保证; 网络层采用基于点对点的网络结构, 负责区块数据、节点间消息的传播, 区块链网络中节点一般采用八卦协议进行通信; 共识与激励层是区块链技术的核心, 决定了区块以什么方式在节点间达成一致, 比特币采取的

共识机制是工作量证明(PoW), 而激励制度是对区块记录者进行一定的奖励分配, 从经济学的角度使区块链系统维持正常运行; 合约层主要是在以太坊等新型区块链系统中的智能合约, 以脚本代码的形式完成用户设定的交易过程; 应用层主要指的是区块链系统的综合应用, 如电子投票平台、食品溯源等。

共识机制作为区块链的核心技术显得十分重要。共识机制的目的是实现公共账本的2个关键特性: 一是一致性, 即去掉区块链末端 k 个区块(k 为区块链的安全参数, 比特币中 $k=6$)之后, 诚实节点的区块链能够互相成为前缀, 也就是说, 诚实节点的区块最终会达成一致; 二是活性, 即诚实用户上传的交易, 在一定的时间之后, 一定会出现在其他所有诚实

收稿日期: 2018-10-22

网络出版日期: 2018-12-03

基金项目: 国家重点研发计划(2017YFB1400700)、国家密码发展基金(MMJJ20180215)

节点的账本中。为了更好地保证以上2个特性的实现,许多共识机制应运而生。

1.1 相关工作

BONNEAU J等人^[2]对比特币和其他数字货币完成了分类和调研。BANO S等人^[3]对区块链时代的共识机制进行了分类和详细的研究。ZOHAR A^[4]分析了以比特币为代表的加密货币的可扩展性和安全性,强调了基于PoW的共识协议中激励机制的重要性,与整个系统的安全密切相关;CACHIN C和VUKOLIC M^[5]讨论了经典共识中的重要概念,重点对需要身份准入的区块链系统进行研究;BANO S、Al-BASSAM M和DANEZIS G^[6]对可扩展区块链的设计给出了具体的发展路线图;PASS R和SHI E^[7]分析了大规模共识的形式化模型,并定义其安全性质。

1.2 研究方法论

共识机制分为经典分布式共识和区块链共识两大类,文中我们主要研究区块链共识,将区块链共识分为基于PoW的共识机制、基于权益证明(PoS)的共识机制、采用单一委员会的混合共识机制、采用多委员会的混合共识机制几大类,并给出了每一类共识机制的基本流程、典型共识方案和优缺点分析。

PoW共识机制主要利用节点算力来选择区块的生产者,节点通过找到满足要求的哈希函数原像完成PoW的过程。PoS共识机制主要根据节点拥有财产的数量随机决定区块生产者,拥有财产越多的节点,成为区块生产者的概率越大。采用单一委员会的混合共识机制首先利用PoW或PoS的形式选出一定数量的节点组成“委员会”,然后在委员会内部采用经典分布式共识完成区块的生产和确认。采用多委员会的混合共识也被称为分片共识,利用多个并行的委员会同时处理交易,实现网络的

可扩展性。

本文对区块链共识的分类和典型方案研究如表1所示。

1.3 共识概述

从总体层面上来讲,共识主要分为2类,一类是以实用拜占庭容错共识(PBFT)为代表的经典分布式共识,通常在授权网络中,参与节点通过多轮投票的方式达成对某个提议值的一致。另一类是以比特币为代表的区块链共识,通常在非授权网络中,节点能够随时加入或退出,通过特定算法完成出块者选举、区块生成、节点区块链更新等过程,保证最终诚实用户手中账本一致。本文中,我们主要研究区块链中的共识机制。

区块链作为一个分布式的公开账本,每个区块相当于一轮产生的账本,用于记录本轮内发生的交易;而共识机制首先需要确定的问题便是每一轮的账本由谁来负责撰写,我们将其称之为“出块者”。出块者一般有2种:第1种是单一的节点作为出块者,如比特币、Bitcoin-NG;第2种是多个节点组成委员会,整个委员会相当于出块者的角色,完成区块的生成。出块者选举的过程需要防止女巫攻击,简单来说就是敌手通过制造多个假身份来增加其成为出块者的概率,因此需要采用PoW、PoS等机制。通常单一节点作为出块者为概率性共识,又被称为弱共识,即区块链可能出现分叉的情况;而委员会作为出块者的共识为确定性共识,又被称为强共识,每一轮的区块是确定的,一般不会出现分叉。

在完成出块者选举之后,出块者

负责完成区块生成的工作。区块一般要包括本轮产生的交易、上个区块的哈希值、时间戳等内容。在这里,区块生成又可以分为2类:第1类是一个出块者只负责生成一个区块,下一个区块由新的出块者生成,如比特币;第2类是一个出块者对应多个区块,一个出块者工作的整个时间周期被称为一个时期,一个时期包括多个轮,每一轮对应一个区块,如Bitcoin-NG等。出块者在生成区块之后,将区块在全网进行广播。

网络中的其他节点在收到新区块之后,首先验证区块的合法性,是否包含上个区块的哈希值。对于概率性共识,如比特币中,还需要对区块中交易的合法性、PoW的正确性进行验证,验证通过后节点将本地链进行更新,并开始新一轮的“挖矿”;对于确定性共识,节点直接更新本地区块链。

2 基于PoW的共识机制

2.1 基本概念

PoW的概念最早是在1993年被DWORK C和NAOR M^[8]提出,最初被用来防止垃圾邮件。邮件发送者必须要计算出某个特定数学难题的解才能够完成邮件的发送。后来在1997年的Hashcash中,BACK A^[9]将其拓展,利用哈希算法作为PoW的核心。因为哈希函数为单向函数,能够抵抗原像攻击,因此设定哈希函数的特定输出值作为难度,输入值中嵌入随机数,当输出值小于或大于难度值时,输入的随机数便是哈希函数的解,即完成了PoW的过程。工作量证

▼表1 区块链共识分类和典型方案

	核心算法	典型方案	交易速度/(tx/s)	交易确认时延/s
基于PoW的共识	PoW	Bitcoin	7	600
基于PoS的共识	PoS	Ouroboros	257	30
单一委员会的混合共识	PoW/PoS+PBFT	ByzCoin	1 000	25
多委员会的混合共识	PoW/PoS+PBFT	Omniledger	5 000	25

PBFT: 实用拜占庭容错共识 PoS: 基于权益证明 PoW: 基于工作量证明

明的本质是: 只有完成了一定数量运算的节点才能够被授权参与某项活动, 即防止敌手制造多个假身份发起的女巫攻击。PoW 与节点算力密切相关^[9]。

2.2 典型方案

(1) 比特币

在比特币中, 平均约每 10 min 会产生一个最大 1 MB 的区块, 区块由区块体和区块头组成, 如图 1 所示。区块体主要是本时间段产生的交易, 区块头包括上个区块的哈希值 A_{r-1} 、当前交易构成的默克尔树根哈希 $Merkle_r$ 、时间戳 T 和随机数 $Nonce$ 等。由于区块头包含指向上个区块的哈希值, 因此区块构成了“链”状的结构, 所以被称为区块链。而随机数 $Nonce$ 便是工作量证明的解。比特币中工作量证明的目的是决定区块的出块者, 并且一轮中只有 1 个出块者, 对应 1 个区块。比特币中的工作量证明用公式可以简化表示为 $H(A_{r-1}, Merkle_r, Nonce) < D$, 其中 $H()$ 是单向哈希函数, 比特币中使用 SHA256 (SHA256()) 实现, 输出字符长度为 256 bit。 D 是当前挖矿难度, 比特币中通过对挖矿难度的动态调整来保持大约每 10 min 1 个区块的速度。区块的时间间隔和区块大小与比特

币系统的安全性有着密切联系, 不能够对其进行随意更改, 这也是目前比特币交易速度只有 7 交易/秒的原因, 因此比特币的交易处理能力有限, 许多诸如链下支付通道的研究意在提升比特币的交易规模。

(2) Bitcoin-NG

由于比特币交易规模有限, 为了提高区块链处理交易的能力, 当前研究主要分为线下和线上 2 个方向。线下解决方案主要指的是利用链下微支付通道处理小额交易, 线上解决方案主要是对基于 PoW 的共识机制的改进。线下方案不属于本文讨论范围, 不在此赘述。线上方案代表主要是 Bitcoin-NG, 由 EYAL I 等人^[10]于 2016 年提出。Bitcoin-NG 的 PoW 机制与比特币基本一致, 只不过出块者和区块是“一对多”的关系, 即一个出块者负责多个区块的生成。在 Bitcoin-NG 中, 区块分为 2 种: 关键块和微块, 关键块包含上个区块哈希值、时间戳、挖矿难度、随机数和出块者公钥, 关键块不记录交易, 只是负责选择出块者。与比特币类似, Bitcoin-NG 平均每 10 min 生成一个关键块, 对应一个时期, 在每个时期内, 出块者以小于等于 10 秒/个的速率产生微块, 记录每一轮的交易。微块包含上个区块的哈希值、当前轮的交易、

时间戳等信息。Bitcoin-NG 在一定程度上增加了交易规模。

基于 PoW 的共识机制还有 GHOST^[11]、Spectre^[12]等。

2.3 优缺点分析

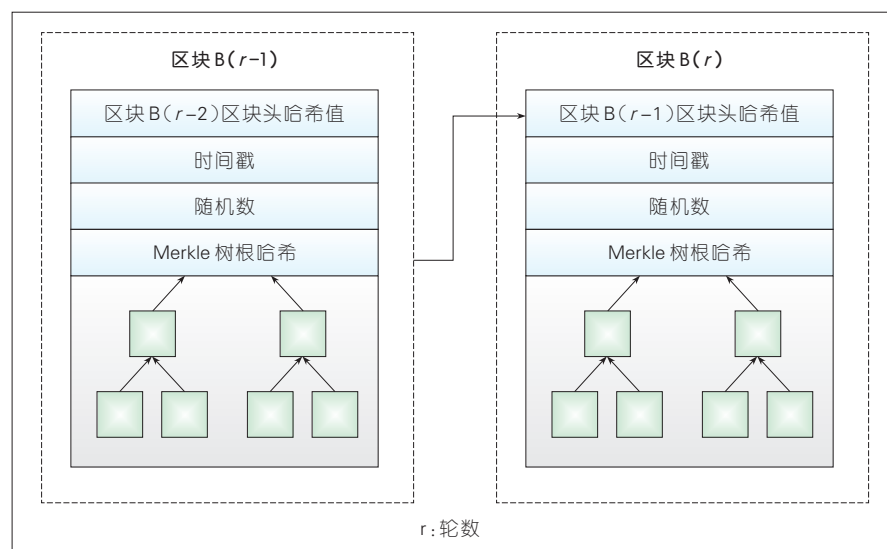
采用 PoW 的共识机制最大的问题是能源的巨大浪费。以比特币为例, 由于比特币每 10 min 产生一个区块, 并且给予区块生产者一定奖励 (目前是 12.5 比特币) 和交易费作为激励, 而目前比特币价格在每比特币一万美元左右浮动, 因此想要获得高额回报的“矿工”们利用所有算力资源, 进行不间断的哈希运算, 这就造成了巨大的能源浪费。从最初的中央处理器 (CPU) 挖矿、图形处理器 (GPU) 挖矿, 到现在的现场可编程门阵列 (FPGA) 和专用集成电路 (ASIC) 挖矿, 比特币所消耗的电量成倍增长, 据估计目前由于挖矿造成的每年消耗的能源已经超过了 31 TWh, 已经超过了全球 159 个国家消耗的能源, 而 77.7% 的算力集中在中国境内, 挖矿造成的巨大能源消耗已经使中国电力网络不堪重负。

此外, 基于 PoW 的共识机制还面临多种攻击, 包括: 自私挖矿^[13]、扣块攻击 (BWH)^[14]、扣块后分叉攻击 (FAW)^[15], 利用区块链产生分叉的特点, 制定利己的区块发布策略, 获得高于自身实际算力的高额回报; 日蚀攻击^[16]、延时攻击^[17], 以及网络隔离攻击^[18], 通过劫持网络流量或其他方法, 将区块链中网络节点的 117 个信息输入通道控制或是将其与其他网络节点隔离, 使其只能接收到敌手发送的信息, 在此基础上发动女巫攻击、双花攻击^[19]、分布式拒绝服务攻击 (DDoS) 等。

3 基于 PoS 的共识机制

3.1 基本概念

为了解决 PoW 带来的巨大能源消耗, PoS 的概念被提出。PoS 的总



▲ 图 1 比特币区块结构图

体思路是:从所有的持币者中随机选取持币者作为出块者,持币者被选中的概率与其持币数目成正比,即持有越多的币,被选中的概率越大。PoS中出块者的选举方式一般分为2类:一类是公开选举,选举结果能够被所有参与者获知,如Ouroboros等;一类是私下选举,参与者利用私有信息确认是否被选中作为出块者,在出块者发布区块之后,其他参与者能够验证其合法性,如Ouroboros Praos等。私下选举能够抵抗DoS攻击,因为在出块者公布区块之前,选举的结果对于其他参与者而言都是未知的;而一旦出块者公布区块,区块被加入到区块链中,此时已经失去了DoS攻击的意义。

3.2 典型方案——Ouroboros

Ouroboros是首个被证明安全的基于PoS的共识机制,由KIAYIAS A等人^[20]在2017年提出。在Ouroboros中,参与者首先运行一轮多方计算产生一个随机种子,然后将随机种子作为输入放到伪随机函数中,该伪随机函数随机选取一个参与者作为出块者,参与者被选中的概率与其持币数量成正比。出块者生成本轮区块并将其广播,Ouroboros的出块者和区块是一一对应的关系。Ouroboros最主要的贡献是将PoS共识机制进行形式化定义,并对其安全性给出了严格的数学证明。Ouroboros在40个节点参与、出块间隔为5 s的情况下,能够达到的交易规模为257交易/秒,交易确认时间大概为30 s。

基于PoS的共识机制还包括PPCoin^[21]、Casper^[22]、Snow-White^[23]等。

3.3 优缺点分析

PoS在解放工作量证明的同时,引入了一些新的安全问题,其中CHEPURNOY A^[24]提出现有PoS机制存在的“无利害关系”问题,即拥有较少财产的用户,其作为区块生产者和验证者进行恶意操作的成本很低,基

于理性节点的自利假设,参与者恶意操作可能性较大,可以同时链的不同分叉上挖矿,无需花费额外的成本,导致链倾向于分叉,使得这些基于PoS的协议安全性降低。另外,区块生产者能够发动粉碎攻击^[25],不断重新生成新的区块,直到生成的区块有利于其成为下面区块的生产者。与此同时,PoS共识机制可能遭受长程攻击^[26],攻击者通过贿赂其他人,来获得他人的私钥。GAZI P、KIAYIAS A等人^[27]提出了针对PoS机制的权益击穿攻击,如果PoS共识机制未采用检查点机制来进行全网状态统一,攻击者能够利用交易费作为激励的形式,通过长时间的累积制造区块分叉,进而发动双花攻击。

4 混合共识机制——单一委员会

4.1 基本概念

混合共识指的是利用PoW、PoS等防女巫攻击手段,选举一定数量的节点作为委员会,即出块者,委员会内部通过经典分布式共识算法就区块达成一致。混合共识中利用共识委员会的形式来代替单一的节点,有着更高的容错能力。

混合共识的2个重要部分是时期内共识和重配置。时期内共识是指在协议正常运行过程中,协议以时期为单位推进,每个时期包括多个轮。在每个时期,委员会的配置是固定的,即委员会成员身份确定且委员会领导者确定。委员会领导者一般通过每一时期的随机数决定,负责每一轮区块的提议。通常来说,每一轮委员会内部运行类似于PBFT的分布式经典共识协议,生成一个新的区块,一个时期对应多个区块的生成。

重配置指的是时期与时期之间进行的委员会成员的更新迭代。由于敌手的存在,敌手可能会对诚实用户实施腐化,腐化后的用户被敌手完全控制。为了防止敌手控制的用户

比例超过一定限制,就必须对委员会成员进行更新。混合共识中,重配置通过PoW或PoS的方法,选取新的节点对旧的委员会成员进行替换。由于委员会需要持续运作,一般只替换掉委员会中的部分成员,而不是每次重配置都全部更新。

4.2 典型方案——ByzCoin

2016年KOGIAS E K等人^[28]对Bitcoin-NG进行了改进,提出了ByzCoin。ByzCoin将PoW与PBFT相结合,委员会选举方式采用PoW机制,最新找到PoW的144个节点(或1 008个)进入委员会,并且委员会采用窗口滑动的方式进行更新,即新找到PoW的节点并将最久远的节点替换,每次只替换一个节点,新找到PoW的节点成为本时期的领导者。在委员会中,委员会成员的权限与其产生区块的数量成正比,即如果某个用户在144个区块中产生了3个区块,他便有3票的投票权。委员会内部采用改进的PBFT完成共识,利用群体签名(CoSi)代替传统PBFT中的消息认证码(MAC),使得通信复杂度降低为 $O(\log(n))$,验证复杂度为 $O(1)$ 。ByzCoin中的区块借鉴了Bitcoin-NG的思想,分为关键块和微块,关键块主要用来完成委员会成员的选举和领导者的选举。微块由委员会内部共识产生,记录一轮中产生的交易以及对交易的CoSi签名认证。在委员会成员1 008个、区块大小为32 MB的情况下,ByzCoin的交易速度则会超过1 000交易/秒。

其他采用单一委员会的混合共识还有Solida^[29]、Thunderella^[30]、Algorand^[31]等,其中Algorand采用的是PoS选取委员会的方式。

4.3 优缺点分析

混合共识机制利用PoW或PoS选举委员会,然后利用委员会内部共识完成交易区块的添加,突破了比特币中区块大小和出块速度的限制,所以

交易规模有了明显提升,一般能够达到每秒钟上千个交易的量级。与此同时,由于采取的共识是确定性共识,也就是强共识,所以交易确认时间大大缩短。

混合共识机制带来了新的安全问题。如 PBFT 之类的委员会内共识算法需要确保委员会中诚实节点占据 2/3 以上,而通过 PoW 选举这样的委员会会对诚实用户算力比例产生新的要求。如果不采取相应的措施,由于自私挖矿的存在,诚实节点算力需要占据 3/4 以上才能确保诚实用户产生的区块数量占比在 2/3 以上,满足委员会内诚实用户的占比要求。另外,混合共识中的重配置也是十分重要的问题,在重配置过程中,应当确保以下条件满足:第一,交易处理的不间断性,即重配置过程不会影响委员会处理交易;第二,重配置之后的委员会诚实成员占据 2/3 以上,才能确保委员会不会被敌手控制;第三,重配置的频率应当被合理设置,充分考虑敌手腐化节点的能力和节点的激励等问题。

5 混合共识机制——多委员会

5.1 基本概念

多委员会的混合共识机制在单一委员会基础上进行设计,主要为了解决全网节点处理交易的可扩展性问题。可扩展性指的是网络处理交易能力随着全网节点的增加而增加。单一委员会的混合共识机制虽然在很大程度上增大了交易处理规模,但是当全网节点增多,导致交易数量增多,此时如果委员会成员数目不变,那么其交易处理能力并不会改变。多委员会的混合共识机制又被称为分片共识机制,其原理是将网络节点分为多个并行的片区,每个片区由各自的委员会负责并行处理对应的交易。当网络节点增多时,片区增加,交易处理能力随之增加。分片共

识中不同交易分属于不同的片区,分别完成交易的处理和存储过程。分片共识中最关键的问题是跨区交易的处理,所谓跨区交易指的是一个交易有多个输入,而输入由多个片区掌管,因此跨区交易的处理牵涉到多个委员会的共同处理,需要设计合理高效的跨区交易处理方式避免交易锁死等可能出现的情况。

5.2 典型方案——Omniledger

分片共识比较典型的方案是 Omniledger,由 KOGIAS E K 等人^[32]在 2018 年提出。Omniledger 主要贡献如下:第一,实现了交易的原子性,跨区交易只能处于失败或成功 2 种状态,避免了交易锁死的状态;第二,实现了交易的可扩展性,网络的交易处理能力随节点数的增加而线性增长;第三,实现了交易确认的低延时,网络能够持续处理交易。在 Omniledger 中,有 2 种区块:第 1 种是身份区块,用于记录每一时期参与共识的委员会节点的身份;第 2 种是交易区块,每个片区单独处理本片区内交易,并形成各自的区块链。为了处理跨区交易,Omniledger 设计了锁定-解锁的原子性跨区交易处理方法。客户端将交易上传至交易输入对应的分片,如分片 1 和分片 2,每个分片各自判断交易输入是否可用,即是否属于未花费交易池(UTXO)。如果交易输入可用,则生成对应的接受证明(PoA),即交易输入在 UTXO 中的默克尔树路径;如果不可用,则生成对应的拒绝证明(PoR)。当分片 1 和分片 2 都提供 PoA 时,交易锁定,经过交易输出分片 3 的共识,完成交易的解锁和确认。当分片 1 或分片 2 中任意一个提供 PoR 时,交易解锁并放弃。在 Omniledger 中,每个时期都会利用 RandHound^[33]分布式随机数生成算法生成随机数,用于委员会领导者的选举和委员会成员重配置时替换节点的选择。

采用多委员会的共识机制还包

括 ELASTICO^[34]、ChainSpace^[35]、RapidChain^[36]等。

5.3 优缺点分析

多委员会的混合共识能够实现交易的可扩展性,交易处理性能随节点数目增多、分区数增多而线性增长,交易规模进一步增大。Omneledger 在每个分区人数为 70,分区数为 16 时交易处理速度能够达到 5 000 交易/秒。多委员会的混合共识主要需要解决的问题是跨区交易处理问题、委员会重配置问题、抗偏置随机数生成问题等。

6 结束语

区块链共识算法是区块链技术研究的重点,未来主要的发展趋势是:将拜占庭容错算法与区块链技术相结合,在开放的区块链网络中建立动态、封闭的共识委员会,实现安全、高效的混合共识;将区块链技术和可信硬件或其他最新密码技术结合;对区块链共识委员会中成员身份进行高效管理;实现对恶意委员会的检测和恢复;防止拥有大算力或高权益矿工对委员会的控制;共识算法中充分考虑网络的一致性和活性等。

参考文献

- [1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. [2018-10-22]. <https://bitcoin.org/bitcoin.pdf>
- [2] BONNEAU, MILLER A, CLARK J, et al. Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies[C]// 2015 IEEE Symposium on Security and Privacy (SP). USA: IEEE, 2015: 104-121. DOI:10.1109/SP.2015.14
- [3] BANO S, SONNINO A, AL-BASSAM M, et al. Consensus in the Age of Blockchains [EB/OL]. [2018-10-22]. <https://arxiv.org/pdf/1711.03936.pdf>
- [4] ZOHAR A. Securing and Scaling Cryptocurrencies[C]//Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence. Australia: IJCAI, 2017, 17: 5161-5165. DOI: 10.24963/ijcai.2017/742
- [5] CACHIN C, VUKOLIC M. Blockchains Consensus Protocols in the Wild [EB/OL]. [2018-10-22]. <https://arxiv.org/pdf/1707.01873.pdf>

- [6] BANO S, AI-BASSAM M, DANEZIS G. The Road to Scalable Blockchain Designs [J]. USENIX; login: magazine, 2017, 42(4): 6
- [7] PASS R, SHI E. Rethinking Large-Scale Consensus[C]//2017 IEEE 30th Computer Security Foundations Symposium (CSF). USA: IEEE, 2017: 115–129. DOI:10.1109/CSF.2017.37
- [8] DWORK C, NAOR M. Pricing via Processing or Combatting Junk Mail[C]// Proceeding of the 12th Annual International Cryptology Conference on Advances in Cryptology. Germany: Springer, 1992: 139–147. DOI: 10.1007/3-540-48071-4_10
- [9] BACK A. Hash Cash: A Partial Hash Collision Based Postage Scheme[EB/OL]. (2001–05–02)[2018–10–22]. <http://www.hashcash.org>
- [10] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: A Scalable Blockchain Protocol [EB/OL]. (2015–10–07)[2018–10–22]. <http://arxiv.org/abs/1510.02037>
- [11] YONATAN S, AVIV Z. Secure High-Rate Transaction Processing in Bitcoin [C] // International Conference on Financial Cryptography and Data Security. Germany: Springer, 2015: 507–527. DOI:10.1007/978-3-662-47854-7_32
- [12] SOMPOLINSKY Y, LEWENBERG Y, ZOHAR A. SPECTRE: A Fast and Scalable Cryptocurrency Protocol [J]. IACR Cryptology ePrint Archive, 2016(2): 1159
- [13] EYAL I, SIRER E G. Majority is not Enough: Bitcoin Mining is Vulnerable[C]//International Conference on Financial Cryptography and Data Security. Germany: Springer, 2014: 436–454. DOI: 10.1007/978-3-662-45472-5_28
- [14] 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. DOI:10.1109/tifs.2016.2623588
- [15] KWON Y, KIM D, SON Y, et al. Be Selfish and Avoid Dilemmas [C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security – CCS '17. USA: ACM, 2017. DOI:10.1145/3133956.3134019
- [16] HEILMAN E, KENDLER A, ZOHAR A, et al. Eclipse Attacks on Bitcoin's Peer-to-Peer Network[C]// Usenix Conference on Security Symposium. USA: USENIX, 2015:129–144
- [17] APOSTOLAKI M, ZOHAR A, VANBEVER L. Hijacking Bitcoin: Routing Attacks on Cryptocurrencies[C]//2017 IEEE Symposium on Security and Privacy (SP). USA: IEEE, 2017: 375–392. DOI:10.1109/SP.2017.29
- [18] KIFFER L, LEVIN D, MISLOVE A. Stick a Fork in It: Analyzing the Ethereum Network Partition[C]// the 16th ACM Workshop. USA: ACM, 2017:94–100. DOI: 10.1145/3152434.3152449
- [19] KARAME G O, ANDROULAKI E, CAPKUN S. Double-Spending Fast Payments in Bitcoin [C]//Proceedings of the 2012 ACM conference on Computer and communications security – CCS '12. USA: ACM, 2012. DOI:10.1145/2382196.2382292
- [20] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol[C]// Annual International Cryptology Conference. Switzerland: Springer, 2017: 357–388. DOI: 10.1007/978-3-319-63688-7_12
- [21] KING S, NADAL S. Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[EB/OL]. (2012–08–19)[2018–10–22]. https://www.researchgate.net/publication/265116876_PPcoin_Peer-to-Peer_Crypto-Currency_with_Proof-of-Stake
- [22] BUTERIN V, GRUFFUTH V. Casper the Friendly Finality Gadget [EB/OL]. (2017–10–02)[2018–10–22]. <https://arxiv.org/pdf/1710.09437>
- [23] BEBTOV I, PASS R, SHI E. Snow White: Provably Secure Proofs of Stake [EB/OL]. (2016–09–21)[2018–10–22]. <https://eprint.iacr.org/2016/919>
- [24] CHEPURNOY A. Interactive Proof-of-Stake [EB/OL]. (2016–01–03)[2018–10–22]. <https://arxiv.org/pdf/1503.07768.pdf>
- [25] DAVARONAH K, KAUFMAN D, PUBELLIER O. NeuCoin: the First Secure, Cost-efficient and Decentralized Cryptocurrency [EB/OL]. (2015–03–28)[2018–10–22]. <https://arxiv.org/pdf/1503.07768>
- [26] BARBER S, BOYEN X, SHI E, et al. Bitter to Better—How to Make Bitcoin a Better Currency[C]//International Conference on Financial Cryptography and Data Security. Germany: Springer, 2012: 399–414. DOI: 10.1007/978-3-642-32946-3_29
- [27] GAZI P, KIAYIAS A, Russell A. Stake-Bleeding Attacks on Proof-of-Stake Blockchains[EB/OL]. (2017–10–03)[2018–10–22]. <https://eprint.iacr.org/2018/248.pdf>
- [28] KOGIAS E K, JOVANOVIĆ P, GAILLY N, et al. Enhancing Bitcoin Security and Performance with Strong Consistency Via Collective Signing[C]//25th USENIX Security Symposium (USENIX Security 16). USA: USENIX, 2016: 279–296
- [29] ABRAHAM I, MALKHI D, NAYAK K, et al. Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus [EB/OL]. (2016–07–28)[2018–10–22]. <https://arxiv.org/pdf/1612.02916>
- [30] PASS R, SHI E. Thunderella: Blockchains with Optimistic Instant Confirmation[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Switzerland: Springer, 2018: 3–33
- [31] GILAD Y, HEMO R, MICALI S, et al. Algorand: Scaling Byzantine Agreements for Cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. USA: ACM, 2017: 51–68. DOI: 10.1145/3132747.3132757
- [32] KOGIAS E K, JOVANOVIĆ P, GASSER L, et al. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding [C]//2018 IEEE Symposium on Security and Privacy (SP). USA: IEEE, 2018: 583–598. DOI: 10.1109/SP.2018.000–5
- [33] SYTA E, JOVANOVIĆ P, KOGIAS E K, et al. Scalable Bias-Resistant Distributed Randomness[C]//2017 IEEE Symposium on Security and Privacy (SP). USA: IEEE, 2017: 444–460. DOI:10.1109/SP.2017.45
- [34] LUU L, NARAYANAN V, ZHENG C D, et al. A Secure Sharding Protocol for Open Blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security – CCS'16. USA: ACM, 2016:17–30. DOI:10.1145/2976749.2978389
- [35] AL-BASSAM M, SONNINO A, BANO S, et al. Chainspace: A Sharded Smart Contracts Platform [EB/OL]. (2017–09–28)[2018–10–22]. <https://arxiv.org/pdf/1708.03778>
- [36] ZAMANI M, MOVAHEDI M, RAYKOVA M. RapidChain: Scaling Blockchain via Full Sharding[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. USA: ACM, 2018: 931–948

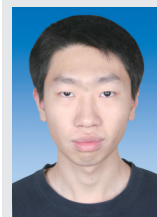
作者简介



刘懿中, 北京航空航天大学在读博士; 主要研究领域为公钥密码学、区块链。



刘建伟, 北京航空航天大学教授; 主要研究领域为网络安全和密码学; 先后主持国家级/省部级课题10余项, 获得国家技术发明奖一等奖1项、国防技术发明一等奖1项、山东省计算机应用优秀成果二等奖1项、山东省科技进步三等奖1项; 发表SCI/EI收录论文200余篇, 出版教材5部、译著1部, 获授权发明专利46项, 软件著作权登记3项。



喻辉, 北京航空航天大学在读硕士; 主要研究领域为密码学、区块链和数字货币。

区块链共识机制发展与安全性

Development and Security of Blockchain Consensus Mechanism

王李笑阳/WANG Lixiaoyang
秦波/QIN Bo
乔鑫/QIAO Xin

(中国人民大学, 北京 100872)
(Renmin University of China, Beijing 100872, China)

区块链本质上是一种去中心化的、节点与节点之间地位平等的数据库,其概念首次出现在中本聪的《比特币:一种点对点式的电子现金系统》一文中^[1]。区块链通过运用加密算法、时间戳、共识机制和奖励机制,帮助陌生的节点建立了信任,目前广泛应用于代币以及分布式系统之中。区块链有着匿名性与安全性的特点,避免了中心化带来的数据丢失风险和管理问题。在区块链基础上,又延伸出超级账本、智能合约等概念。作为区块链中构建信任的核心,共识机制也愈发受到学界的持续关注。

由于区块链中节点众多,节点地理分布较广,且不同节点之间的通信存在延迟,因此需要一种算法决定新

块的记账权以保证节点数据的一致性,这种算法被称为共识机制^[2]。共识机制以所有诚实节点数据保持一致为目标,同时要求在节点互相平等的情况下明确记账权的归属。由于共识机制的存在,用户无需信任交易,另一方同时也无需信任第三方机构即可完成交易。区块链支持多种共识机制,这些共识机制在效率、安全性、资源消耗等方面各不相同,因此文章中我们着重探讨了常见共识机制的发展历史、效率以及安全性。

1 共识机制发展

1.1 共识机制的概念

共识机制,即多个个体达成一致的机制。共识机制可以根据达成共识的个体,分为算法共识和决策共识

2类^[3]。算法共识致力于研究复杂的网络环境下,去中心化的网络如何达成一致的问题,本质是多个机器达成共识。决策共识目的是帮助人达成一致,在分布式人工智能领域较为常见。区块链中共识算法属于前者,目的在于在多个节点中记录同样的账本。区块链中共识机制要求满足2个性质:一致性,即不同的节点记录的数据必须相同;有效性,节点记录的数据格式和内容必须满足区块链规则。

1.2 非拜占庭容错共识机制

共识问题,首先在数学界受到关注。早在1959年,EISENBERG E和GALE D研究了特定条件下如何在—组个体中形成共识概率分布问题。随后共识问题受到了不同学界的广

中图分类号:TN929.5 文献标志码:A 文章编号:1009-6868(2018)06-0008-005

摘要: 在总结了共识机制发展的基础上,着重对共识机制当前存在的攻击威胁以及防范策略进行解析,并据此提出了区块链共识机制的4种信任基础即对数学、密码学的信任,对节点注重自身利益的信任,多人信任以及人为信任。指出目前共识机制发展方向之一是同一信任之下的信任对象替换。

关键词: 共识算法;安全性;区块链;分布式系统;拜占庭容错

Abstract: The attack threats and preventive strategies existing in consensus mechanism are analyzed in this paper, and four trust bases of blockchain consensus mechanism are put forward, including trust in mathematics and cryptography, trust in nodes focusing on their own interests, multi-person trust and artificial trust. Finally, it points out that one of the development directions of the current consensus mechanism is the replacement of trust objects under the same trust.

Keywords: consensus algorithm; security; blockchain; distributed system; Byzantine fault tolerance

收稿日期:2018-10-17

网络出版日期:2018-11-19

基金项目:国家重点研发计划(2017YFB1400700)、国家自然科学基金面上项目(61772538,61532021)、国家自然科学基金重点项目(91646203,61672083)、信息保障技术重点实验室装备预研基金项目(61421120305162112)、“十三五”国家密码发展基金密码理论课题(MMJJ20170106)

泛关注。

在计算机界,尤其是分布式系统部分,共识问题引起了广泛关注。在共识问题的发展过程中,首先仅考虑了节点的可靠性,之后加入了容错问题,但节点依然要求相对可信。在当前常用的共识算法中,许多算法允许节点随意加入网络而不要求较高的可信性。

1989年,LAMPORT L已经提出了Paxos算法^[4],但由于Paxos算法过程较为复杂,且文章内容过于晦涩难懂,直到1998年才通过评审。此种算法基于消息传递模型,适用于多个过程需要达成共识的场合。

2013年,ONGARO D和OUSTERHOUT J在《In Search of An Understandable Consensus Algorithm》一文中提出了Raft共识算法^[5]。作者基于Paxos进行了改进,使之更容易理解。它与Paxos相当,对构建实际系统起了促进作用。目前百度公开了Raft开源实现代码。

验证池共识机制在基于传统的共识算法上进行了改进,适用于几大商业中心的联合建链。该方案是基于传统的拜占庭容错(BFT)及其变种的共识方案,需要参与者能够相互辨识,不需要发币即可实现。验证池算法十分高效,可以实现秒级共识。

1.3 BFT上的突破

拜占庭将军问题,指的是地理上有一定间隔且可能不诚实的节点如何达成一致的问题。BFT指的是在整个系统中节点共有 n 个,最终要求诚实节点达成一致的情况下最多允许多少非诚实节点。经典算法下,要求非诚实节点数量 t 与整个系统节点数量 n 满足 $n \geq 3t+1$ 。最早在1999年的《Practical Byzantine Fault Tolerant》^[6]一文中作者就给出了容错量为 $1/3$ 的算法。在分布式数据库中,为了避免部分服务器被黑客侵入造成整个网络崩溃的问题,采用了带有容错的公式算法。更进一步地,中

本聪在设计区块链网络时提出了创新算法思路,增加了提出议案的经济成本,采用经济惩罚来制约破坏者。

2008年,中本聪提出了工作量证明(PoW)共识机制。该共识机制沿用了PoW的概念^[7]。这一算法要求节点在提出议案之前必须进行大量工作(运算),并且提出议案时必须同时提交做出了大量工作的证明,这一方案将节点容错量转换为算力容错量,对女巫攻击进行了有效防范,可以允许节点自主添加到网络。在此之后提出的Proof of X的共识方案也是基于此种思想。传统分布式网络要求节点需要相对可信且进入网络需要认证,而这一共识机制使其变为了任意节点均可加入网络,使比特币可以应用于现实环境。

1.4 BFT共识算法与应用

早在中本聪提出比特币之前,BFT算法已经存在,1999年LISKOU B等提出了实用拜占庭容错算法。该算法达成共识需要“请求、预准备、准备、确认、回应”5个步骤。其中“预准备、准备、确认”3个步骤用于保障一致性。该算法虽然拥有 $1/3$ 的容错性,但并不能防范女巫攻击,因此不能用于公有链类型货币中。实用拜占庭容错算法(PBFT)是传统一致性算法的改进,算法十分高效,在不需要货币体系的许可链或者私有链中较为常用。目前,IBM创建的超级账本就是使用了该算法作为共识机制。

秉持分布式系统无法同时兼顾一致性、可用性与分区容忍性(CAP)原理^[8],中本聪设计了PoW共识机制。现阶段常见共识算法其中一类为证明类共识,即Proof of X共识方案,是在PoW共识方案之上的变种,将PoW更换为其余证明。PoW算法现阶段依然盛行,使用PoW共识的代表货币比特币依然占据最大市值。

2011年7月,一位名为MECHANIC Q的数字货币爱好者首次提出权益证明(PoS)共识算法^[9]。

该算法以节点持有币数乘持有时间作为一个节点的权益,当前权益最高的节点最可能获得生成新块的权力。点点币、黑币采用了PoW与PoS混合的共识算法,同时以太坊共识机制拟采用PoW与PoS混合的方案。

SCHWARTZ D提出了瑞波协议共识算法,该算法在产生新块之前要求多轮投票,不需要挖矿。此算法较为高效,但BFT能力为仅 $(n-1)/5$ 且节点必须提前确定。代表性应用为瑞波币。

2013年8月,股份授权证明(DPoS)算法由比特股项目提出。该算法根据权益投票选举,选举中得到票数最多的前 N 个节点成为“代表”,轮流产生新块。DPoS目前应用于EOS中,支持了EOS的高效率交易。

2015年,小蚁链(NEO)白皮书提出授权拜占庭容错(DBFT)共识算法。DBFT允许大规模节点参与投票,拜占庭容错量为 $1/3$ 。DBFT在生成新的区块前需要先经过投票。为了减少资源消耗,NEO需要通过投票确定多个记账人组成记账人团体,记账人团体间按BFT算法达成一致。

当前阶段,共识算法呈现出百花齐放的态势,例如2-hop^[10],限制51%攻击者在拥有51%以上算力的同时还需要拥有51%以上的权益。目前燃烧证明(PoB)、活跃证明(PoA)等共识机制成为了新研究方向。另外,存在共识算法在PoW基础上添加了Ghost协议,将无用的挖矿算力转换为解决有效问题。这些算法大多是PoW、PoS或者传统一致性算法的改进或混合,《区块链共识算法发展现状与展望》^[11]一文将当前的共识协议进行总结并对其脉络进行梳理,指出了共识协议的发展方向。

2 共识机制分析

2.1 共识机制本质

区块链的创新在于在去中心化系统中如何取得信任,并以此获得可

容错性、抗攻击性、抗共谋性。而作为取得信任的核心,共识机制是区块链的神韵。目前,共识机制面对场景多种多样,共识机制的设计也多种多样,然而共识机制的本质始终相同,即消耗资源以换取信任。因此,共识机制的评判标准可以总结为“消耗多少资源,换取多少节点的信任,换取信任的程度,换取信任的速度,换取是否需要前提条件”,即资源消耗问题、节点扩展性问题、安全性问题、效率问题以及开放性问题。不同的场景中对以上问题的注重程度不同,因此所适用的共识机制不同,例如:大额资金交易过程中安全性的重要程度远远高于资源消耗的重要程度,因此大多选择 PoW 共识机制。而小额资金交易过程中,对效率要求较高,因此 DPoS 是一个较好的选择。

共识机制使用资源换取效率的过程并不是凭空产生的,而是有着一定的前提。当前共识机制信任来源总结如下,其中一种共识机制不一定基于全部信任来源:

(1)对数学、密码学的信任。任何共识机制都不能离开数学基础,例如:PoW 建立在哈希函数的单向性之上,任何挖矿手段也都需要数学的参与,甚至随机选择过程中同样需要数学知识。对数学的信任是最有力的信任,人为条件不能改变这种信任。

(2)相信节点注重自身利益。此种信任是强有力的信任,中本聪曾经提到:占据整个系统 51%算力的节点为了自身利益,会自动维护整个系统,而不至于发动攻击。这种思想即建立于节点足够理性、足够注重利益的基础之上。同时一些保证金制度、投票制度同样基于此种信任。

(3)多人信任。多人信任是指大部分认定的即为正确。这种信任借用了在生活中的信任,例如:只需要一定数目的商家支持比特币支付,那么比特币就可以流通。在 PoW 共识中,多算力认定的数据即为正确。多人信任不仅局限于人,同时也可能为

算力、权益等。目前存在的“一中央处理器(CPU)一票”思想也是基于此种信任,选举类共识机制是基于此种信任的典型代表。

(4)人为信任。人为信任包括身份认证和证书等其他事先约定的信任。无论是在传统的一致性算法还是在区块链共识算法中都十分常见。分布式系统中的管理员是身份认证的典型代表。在区块链中一些联盟链需要证书认证都基于此种信任。基于人为信任会极大影响区块链的去中心化程度,但由于事先约定的缘故,不需要大量资源换取信任,是代价最小的一种方式,同时可能换取效率的提升。

同时,在区块链中共识机制与激励机制息息相关,许多共识机制的改进是为了更好地设计激励机制,文章中我们对此不做讨论。

2.2 PoW、PoS、Dpos 详情

目前存在的主流共识机制大多为 PoW 的改进(PoX 系列)、PoS 的改进、传统共识算法的改进或者 PoW 与 PoS 的结合。虽然共识机制经过多年改进,仍然有着部分缺陷,面临着严重威胁。本文针对 PoW、PoS、DPoS 三大共识机制对其基本方案、效率以及面临攻击和问题进行探究。

(1)PoW:是目前数字货币最为普遍的算法之一,代表案例为比特币。比特币效率较低,生成一个区块时间为 10 min,不能适用于小额快速交易。参照《Mastering Bitcoin》^[11]中的详细描述,挖矿公式简记为 $H(\text{block header}) < \text{difficulty}$,其中 block header 为区块头,H 为某一哈希函数,difficulty 为挖矿难度。挖矿难度根据生成块的时间进行调整,保证生成块的时间为 10 min 左右。矿工只能通过遍历的方式使区块头满足上述公式,遍历的过程即为工作量。PoW 共识较为安全但效率不高且存在大量算力浪费。该共识机制下节点加入不需要验证,因此去中心化程度较高,但目

前存在矿池集中的现象。

(2)PoS:是当前数字货币的典型共识算法之一,在最早的点点币版本中,挖矿难度同代币数量与持有时间的乘积成反比。挖矿公式为: $H(H(B_{\text{prev}}), A, t) \leq \text{balance}(A) \times m \times \text{Age}$,其中 H 为某一哈希函数, $H(B_{\text{prev}})$ 为对上一块进行哈希运算,t 为时间戳,balance(A)为余额,m 为事先定义值,Age 为持币时间。目前改进方案中,权益与 Age 不再线性相关。由于不再花费大量时间进行运算,PoS 速度较快,效率较 PoW 高。

(3)DPoS:意为股份授权证明,同样秉持着权益越高越容易计算新块的思想。该方案类似于股份制公司。用户根据持有代币的多少拥有不同数量的选票,同时可以投票选举相对可信的代表,并且由代表轮流产生新块。在比特股中,代表的数量被限定为 101 个。该算法效率极高,使用该共识算法的 EOS 号称每秒百万级处理速度,然而要求代表相对可信,去中心化程度不如前二者。

2.3 共识算法攻击方式

文章中我们仅讨论针对共识机制的攻击方式,并不考虑例如双花攻击、日蚀攻击、整数溢出攻击、分布式拒绝服务(DDoS)等针对区块链其余部分的攻击方式。白帽汇安全学院列举了 5 种针对共识机制的攻击方式^[12],部分攻击方式仅针对部分共识算法。

(1)短距离攻击。短距离攻击步骤为:首先向全网提交一个交易,然后攻击者试图回滚该交易,攻击者在该交易之前的区块上继续进行挖矿,在该交易得到 n 次确认后,若不含该交易的分叉区块数足够长,则该分叉成为主链,成功回滚交易。

短距离攻击的典型代表是贿赂攻击。贿赂攻击的核心思想在于使用贿赂促使节点选择在对攻击者有利的链。典型攻击步骤如下:

1)攻击者购买商品,并使用数字

货币支付;

2) 商户开始等待交易入链;

3) 攻击者宣称奖励不包含此次交易的最长链, 如果这条主链被广泛接受, 攻击者被认为没有交易;

4) 当步骤3中产生的链足够长时, 攻击者使用更大的奖励贿赂一部分矿工生成包含此次交易的链条。虽然存在更长主链, 但矿工为了自身利益, 会选择从之前开始重新挖矿;

5) 在此次交易得到6次确认之后, 攻击者顺利地造成了交易得到确认而主链上并没有此笔交易的情况, 此时攻击者停止奖励;

6) 货物到手, 由于包含交易的链较不包含交易的链短, 不包含交易的链成为主链。

对于矿工而言, 如果不存在奖励(贿赂)的情况下, 是否添加攻击者进行的交易获得的奖励是相同的, 因此攻击者在步骤3只需要较少奖励即可诱使矿工在主链中不加入这笔交易。攻击者在整个攻击过程中, 只需要贿赂金额小于商品金额即可攻击成功。

对于不等待确认的商户来说, 只需要很小甚至不需要贿赂即可简单的促使这笔交易失效。

(2) 长距离攻击。长距离攻击与短距离攻击不同, 指攻击者在拥有一部分资源的情况下, 直接对已经存在的区块进行分叉, 可能获得更多的挖矿奖励或者否认某笔交易。

长距离攻击的代表为51%攻击, 恶意节点占据了整个节点的主要部分。这一攻击和共识机制的去中心化程度有着密切联系, 常用于采用PoS共识的区块链和小型采用PoW共识的系统中。中本聪在提出比特币构想中秉持了大多数原则, 即大多数算力所在的链即为正确的链。为了获得挖矿奖励, 对于诚实的节点而言, 在最长的链上生成区块是有利的。由于生成新的区块的权力只与算力相关, 在大部分节点诚实的情况下, 对攻击者有利的链长度赶超过

6次确认的合法区块链概率极低。然而, 假设攻击者拥有系统一半以上的算力, 那么经过足够长时间之后必然可以使整个系统按照攻击者想法运行。中本聪认为: 拥有51%算力的攻击者是系统的实际受益者, 在足够理性的情况下并不会攻击系统。然而, 现实中已经存在51%算力攻击的实际案例: 一些老牌大型PoW共识区块链矿工入侵新型PoW区块链。在PoS中不要求算力, 生成块的速度相对较快。因此, 攻击者可能期望重写整个区块链。

目前已有学者在在51%攻击基础上进行改进, 大约只需要1/3的算力即可达到与51%攻击相同的效果。

(3) 币龄累积。币龄累积是针对初期PoS共识机制的常见攻击方式, 不存在于PoW。因为持币时间越长, 获得记账权的概率越大。在攻击者拥有足够代币之后, 可以通过累积时间来达到控制网络新生成块的目的。在代币足够的情况下, 攻击者甚至可以将自身代币分散于多个节点, 这一攻击方式可以帮助攻击者多次生成有利块, 比如回滚以进行双花攻击。占有代币1%的攻击者可以通过2个月不进行交易来进行攻击。基于同样的理由, PoS可能出现冷启动的问题。

(4) 预计算。在新一代的PoS共识机制中, 挖矿公式可简写为 $H(H(B_{prev}), A, t) \leq \text{balance}(A)m$ 。由于新块的挖矿只与时间、余额以及上一块的哈希值有关, 因此控制当前块的生成可以帮助攻击者得到新块的挖矿权。在某一节点拥有一定数量代币以及算力足够的情况下, 该节点可以通过随机试错方式控制第N块的哈希值使得攻击者有能力对N+1块进行挖矿。

(5) 女巫攻击。在《The Sybil Attack》^[13]一文中, DOUCEUR J R详细地描述了女巫攻击的全过程。女巫攻击的核心思想在于: 通过控制多数节点或者伪造多个节点进行攻击。女巫攻击的条件在于对等网络中实

体为一个运行程序, 且同一实体可以拥有多个网络身份。例如: 在一投票的对等网络中, 攻击者可以通过伪造多个IP达到多次投票的目的。不仅仅在区块链网络中, 现今许多投票项目同样可以通过女巫攻击攻破。

2.4 可能存在的问题

(1) 挖矿耗能问题。在PoW共识机制中, 挖矿仅为简单的遍历, 浪费了大量的算力。根据加密货币信息网站Digiconomist的数据称: 目前投入到比特币和以太坊挖矿当中的电力可以在所有国家和地区消耗电力中排名第71位, 其中比特币矿机消耗功率为14.54万兆瓦^[14]。这些耗能仅用于交易的确认, 造成了巨大的浪费。同时, 挖矿造成了显卡等产品的大量损耗, 造成产品单价激增。

(2) 去中心化程度不足问题。在PoS以及PoW共识机制中, 节点与节点之间地位完全平等, 因此去中心化程度较高。然而由于比特币等货币算力不断上涨, 单个设备挖矿已经很难获得挖矿的奖励。促使一些“bitcointalk”上的极客开发出一种可以将少量算力合并联合运作的方法, 使用这种方式建立的网站便被称作“矿池”。对于比特币而言, 目前全球约70%的算力在中国矿池手中, 这可能会造成去中心化程度不足与51%攻击。由于PoS对硬件要求较小, 普通计算机可以挖矿, 因此去中心化程度更高。对于DPoS而言, 节点之间并不完全平等, 因此去中心化程度不如PoW与PoS。

(3) 冷启动问题。对于PoS共识机制而言, 持币量和持币时间的增长会降低挖矿难度。因此在PoS共识下, 初期持有代币的节点更加倾向于不进行交易, 以获得挖矿利润。这就会造成代币不流通的问题, 系统的启动较为困难。

(4) 账本分叉问题。在区块链中, 通常以最长的链作为主链, 矿工在最长的链上进行挖矿。在PoW共

识算法下,由于矿工算力有限,面临多条链时,矿工通常会在最长链上进行挖矿。然而在 PoS 共识机制下,矿工为了自身利益,通常会选择多个链进行挖矿,这可能导致区块链的分叉。同时,攻击者如果使用了预计算与币龄累积攻击同样可能造成账本分叉。

2.5 共识算法的防范与改进

(1) PoW。由于 PoW 要求大量运算力,因此贿赂攻击很难实现,攻击者需要贿赂大部分节点才可以实现贿赂攻击,这往往得不偿失。同样由于挖矿需要大量算力,女巫攻击失去了效果。同时 51% 攻击要求攻击者拥有 51% 算力,攻击条件十分苛刻。在新生 PoW 链中,为了防止原有的大型 PoW 链矿工发动 51% 攻击,往往改动地址生成过程中的哈希函数。针对 PoW 耗能过高问题,目前部分节点采用 Ghost 协议,此协议将无用的挖矿改为了计算大素数等数学问题,部分解决了耗能问题。

(2) PoS。对于短距离攻击,最常见的解决方式为在 PoS 共识机制中引入保证金和惩罚措施,这基于“节点注重自身利益”这一条件下,目前以太坊拟采用 casper 协议抵御攻击。在引入保证金机制后,节点会为保证金反对做出对区块链不利的决策。惩罚措施可以使节点得不到攻击者事先声明的报酬,促使节点做出对区块链有利的决策。针对币龄累积攻击,通常限制持币时间对挖矿难度的降低作用。蜗牛币提出了股份速率证明 (PoSV) 机制,将难度函数改进为指数衰减函数。在 PoSV 共识下,节点累计足够长的时间之后,继续累积很难提高收益,解决了币龄累积攻击。针对冷启动问题,目前大多数区块链采取了在链初期首先使用 PoW 机制,中期使用 PoW+PoS 结合方式,最后采用纯 PoS 共识机制。

(3) DPoS。DPoS 机制本身对短距离攻击与预计算攻击有较强防范,

其余防范方式与 PoS 基本相似。

2.6 共识机制效率与安全性对比

共识机制经过了数年的发展,在经过探索和开放式创新之后,势必进入到性能安全性等的比拼之中。表 1 分别为 PoW、PoS、DPoS 面临的攻击威胁表。

为了保证较高的安全性,一部分共识算法在效率方面做出了退步,表 2 为当前主流共识机制性能、特点的对比。

总结来看:当前 PoW 共识机制的安全性较高、面临攻击威胁小,但效率较低;PoS 和授权股权证明效率较高,但牺牲了部分安全性。传统共识机制对各种攻击防范较为到位并且效率比较高,但是大多不能进行拜占庭容错。

3 结束语

目前共识机制应用的场景越来越广泛,且不同场景下对共识机制安全性与效率要求不同,能否找到一种适用于大多数场景的共识成为关键。

共识机制的发展目标在于资源消耗问题、节点扩展性问题、安全性问题、效率问题以及开放性问题 5 个方面的提升,例如:Ghost 协议是在 PoW 基础之上缓解了部分资源消耗的问题。在 5 个维度不能同时提升的情况下根据特定情况选择牺牲一

▼表 1 工作量证明、权益证明、授权股权证明面临威胁

面临威胁	PoW	PoS	DPoS
短距离攻击	低	高	低
长距离攻击	低	高	高
币龄累积	低	高	高
预计算	低	高	低
女巫攻击	高	高	高
冷启动	无	高	中
挖矿耗能	高	低	低
账本分叉问题	低	高	高

DPoS: 股份授权证明 PoW: 工作量证明
PoS: 权益证明

部分换取另一部分的提升同样是当前研究的热点。当前为了适应实际生活的交易,牺牲部分安全性以换取效率的共识机制十分常见,例如: DPoS 机制。

根据基于方案的不同,当前共识机制可以归结为传统一致性算法的改进、PoW 算法的改进、PoS 算法的改进,以及 PoW 与 PoS 的结合。PoW 与 PoS 的结合是当前共识机制的发展趋势之一,通常属于时间效率与安全性的妥协。

根据基于信任来源的不同,当前共识机制许多是在同一信任类型下的替换,例如: Proof of X 类型的共识协议,通常是在多人信任之下修改信任的对象。是否可以找到一种可信

►下转第 40 页

▼表 2 共识机制性能

共识机制	时间效率	拜占庭容错	资源消耗	代表应用
PoW	高延迟	是 (<1/2)	高	比特币
PoS	低延迟	是 (<1/2)	低	点点币
DPoS	低延迟	是 (<1/2)	低	EOS
委托拜占庭共识	低延迟	是 (<1/3)	低	小蚁币
PBFT	低延迟	是 (<1/3)	低	超级账本
瑞波共识	低延迟	是 (<1/5)	低	瑞波币
Paxos (族)	低延迟	否	低	Chubby
Raft	低延迟	否	低	Etcd

Chubby: Google 设计的提供粗粒度锁服务的一个文件系统
DPoS: 股份授权证明
EOS: 一种为商用分布式应用设计的区块链操作系统

Etcd: 一个开源的、分布式的键值对数据存储系统
PBFT: 实用拜占庭容错算法
PoS: 权益证明
PoW: 工作量证明

比特币生成原理及其特点

The Generation Principles and Characteristics of Bitcoin

林成骏/LIN Chengjun

伍玮/WU Wei

(福建师范大学, 福建 福州 350007)
(Fujian Normal University, Fuzhou 350007, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0013-006

摘要: 从密码技术出发, 着重分析比特币的生成和运行原理。其中, 通过哈希函数的压缩性和单向性, 分别描述了比特币的核心技术区块链以及工作量证明(PoW)的难度; 利用数字签名的完整性和认证性分析比特币交易的验证过程。基于对比特币优缺点的分析, 认为目前比特币的隐私保护和监管问题仍然突出。

关键词: 比特币; 区块链; 哈希函数; 数字签名

Abstract: Based on the cryptographic techniques, the generation and operation principles of Bitcoin are emphatically analyzed in this paper. The blockchain (the core technology of Bitcoin) and the difficulty of power-of-work (PoW) are described respectively by using the compressibility and one-wayness of hash functions; the authentication process of Bitcoin transactions is analyzed by using the integrity and authenticity of digital signature. Finally, the advantages and disadvantages of Bitcoin are summarized. It is considered that the privacy protection and regulation are still the main problems of Bitcoin.

Keywords: Bitcoin; blockchain; hash functions; digital signature

1 比特币生成背景及其意义

数字货币是一种以电子形式存在的货币, 不再像虚拟货币一样局限于网络游戏, 而是能够像法币一样购买真实的物品。密码货币是数字货币的重要组成部分之一, 利用严谨的密码学原理进行货币的产生、记账和交易。自从第一个密码货币即比特币诞生后, 诸如以太坊、门罗币和零币等一系列密码货币相继面世, 密码货币市场呈现井喷式发展; 但是密码货币在具有价值的同时, 也伴随着一定的风险。分析密码货币的生成和运行原理能够让人们对数字货币有更深理解, 从而做到理性投资。

比特币是最具有代表性的密码货币之一, 后续的密码货币在一定的程度上是延续比特币的技术原理。当然后续的密码货币在共识机制、交易匿名性以及数据隐私保护方面都取得了较大突破。例如: 以太坊^[1]利用权益证明(PoS)机制, 大幅度缩减挖矿开销的计算资源; 门罗币利用可

链接环签名技术^[2], 为发送者提供匿名保护, 同时可以检测双重支付; 零币^[3]采用非交互零知识证明机制^[4]进一步提高了匿名性, 实现了发送者和接收者匿名以及数据隐私, 但是计算和存储开销增大。本节主要介绍比特币的生成背景和研究意义。

1.1 比特币的生成背景

比特币的诞生充满了神奇色彩, 其中包含了密码学、经济学的许多前沿理论。它基于前人提出的理论基础, 并充分结合了当时特殊的社会环境背景。

(1) 密码学、经济学的理论基础是比特币诞生的内在条件。1976年, HAYEK^[5]在《Denationalization of Money》一书中提出只有货币非国家化才能控制货币发行量, 避免因不断发行而导致货币贬值的命运。1981

年, LAMPORT L^[6]提出了哈希链的概念, 即每轮哈希函数的输入均为上一轮输出的哈希值, 从而为数据提供完整性服务, 哈希链可以视为比特币的核心技术区块链雏形。1982年, CHAUM D^[7]提出盲签名的思想, 目的是为了构建不可追踪的密码学网络支付系统, 该想法被认为是比特币设计思想的雏形。1991年, CHAUM D和HEYST van E^[8]提出群签名。一位群管理员为每一位群成员发放私钥, 每位群成员均可代表整个群对消息进行签名, 除了群管理员外, 其他实体无法得知签名人的身份, 只知道签名人来自于该群。依据群签名技术, CHAUM D和HEYST van E设计出第一个密码学匿名现金系统Ecash, 但是Ecash依赖于一个中心且货币不具备可分性。1987年, MERKLE R C^[9]提出了一种哈希函数二叉树(即

收稿日期: 2018-10-23

网络出版日期: 2018-11-24

基金项目: 中国自然科学基金
(61822202, 61872089)

Merkle 树), 可以单独对部分数据进行验证, 而无需检验所有数据, 同时可以快速查询数据。1992 年, DWORK C 和 NAOR M^[10] 提出工作量证明 (PoW) 机制, 用于防止垃圾邮件, 邮件发送者通过一系列复杂的计算, 向接收者证明邮件是值得阅读的。1998 年, SZABO N^[11] 将 PoW 思想应用于分布式数字货币, 用户致力于解决密码学难题, 正确答案需在网络中发布, 且作为下一个困难问题的输入之一, 从而得到一个不断增长的链条。该机制被称为“Bit Gold”, 可以视为比特币体系的前驱。2001 年, NIST^[12] 发布了 SHA-256 算法, 可以将任意长度的消息映射到 256 bit 长度的消息摘要。

(2) 比特币诞生^[13] 的特殊社会背景。2008 年末, 受美国金融危机影响, 许多国家的人民陷入恐慌, 一些政府为应对金融危机甚至做出过激反应, 政府和银行的信誉也因此受到重创。与此同时, NAKAMOTO S^[14] 在 metzdowd.com 中发表了一篇名为《Bitcoin: A Peer-to-Peer Electronic Cash System》的论文, 并且实际运行了其提出的比特币理论系统, 即比特币“挖掘”过程。2009 年 1 月 3 日, 比特币的第一个区块问世, 其中含有系统奖励的 50 枚比特币。

当代货币体系是各国法币的集合, 而 2008 年金融危机暴露出法币的缺陷, 让人们当代各国货币体系产生质疑。法币具有 2 条先天缺陷: 一是由政府垄断, 发行的主体是国家; 二是发行数量也由国家控制, 自从美元与黄金脱轨, 阻碍法币数量增长的机制不复存在, 法币贬值的趋势很难逆转。比特币的诞生与金融危机是否有着某种关联, 又是否能够克服法币的缺陷提供新思路, 这些我们不得而知。但比特币理论为我们提供了一种新的技术思想, 即如何在无第三方机构的情形下构建可信机制, 该思想有助于推动金融服务、公共服务、物联网 (IoT) 等领域的技术

革新。

1.2 比特币的研究意义

从比特币出现至今, 密码货币的热潮仍然存在, 且对世界各国的经济活动和社会生活影响日益扩大。但是很多人只了解到比特币是一个迅速增值的密码货币, 却不了解它是如何产生、如何交易; 作为一个新生物, 它的价值何在, 存在价值的同时又是伴随着怎样的风险呢? 基于此, 一方面, 我们要了解它的运行原理, 分析它的价值和风险; 另一方面, 区块链作为比特币的核心技术之一, 已经从单一的密码货币领域, 发展到社会的各行各业, 例如: 在医疗健康领域, 可以为病人提供隐私保护服务; 在 IoT 领域, 可以为用户提供产品溯源、防伪以及认证服务; 在教育领域, 可以为学生提供学历证明、成绩证明以及档案管理服务。然而, 除了密码货币领域的应用外, 区块链技术在其他领域的应用尚处于摸索阶段, 相应技术理论尚未成熟。因此, 了解比特币的技术原理, 有助于我们今后更好地探索其应用在其他领域的应用。

2 比特币的密码学基础

比特币作为重要的密码货币之一, 它的产生、交易和记账都依赖于严谨的密码学原理, 首先介绍几个密码学的基础概念。

2.1 哈希函数

区块链是比特币的核心技术, 而区块链事实上是一条哈希链, 通过哈希函数串联一块块历史数据。本节主要介绍哈希函数及其相关概念。

2.1.1 哈希函数的定义

哈希又译为“散列”, 哈希函数以任意长度的消息为输入, 输出固定长度的消息摘要。例如: 哈希函数 SHA-256 输出的哈希值为 256 bit。通常情形下, 哈希函数是一类压缩函数, 它的值域远小于定义域, 即一个

消息摘要存在多个原像与之对应。比特币系统中所应用的哈希函数还需要满足以下 3 个安全要求:

(1) 对任意消息 m , 很容易计算出它的哈希值 $y=h(m)$;

(2) 由 y 得出 m 在计算上不可行 (单向性或原像稳固性);

(3) 已知消息 m , 很难找出另一个消息 n 使得 $h(n)=h(m)$ (抗碰撞性)。

2.1.2 哈希校验

由于哈希函数具有单向性和抗碰撞性, 因此可用于检验消息的完整性, 即检验消息在传送过程中是否被篡改。该过程被称为哈希校验。

效验步骤: 假设 B 要发送一条消息 m 给 A, 首先计算 m 的消息摘要 $y=h(m)$, 并附在消息后面一起发出。A 收到消息 m' 后, 检验 $h(m')\stackrel{?}{=}y$ 。如果相等, 由于哈希函数具有强抗碰撞性, A 可在很大程度上相信消息在传送过程中没有被篡改。

2.1.3 哈希现金

哈希现金 (Hashcash) 最早是由 ADAM B 提出的^[15], 其本质是一种 PoW 系统^[10]。用户 A 要求发给他的邮件的哈希值必须包含某段特定字符串, 例如: 用户 A 要求邮件的哈希值的前 8 位必须是 0, 否则拒绝接收该邮件。那么发给 A 的邮件正文必须添加某些随机字符使得哈希值满足该要求, 这个工作是没有捷径的, 计算机必须不断循环进行如下步骤: 随机选取某些字符, 并将其串联到邮件末尾, 计算串联后的邮件的哈希值, 直到哈希值的前 8 位是 0 为止。当然, 计算开销取决于计算机的算力, 当要求的难度提升巨大时, 想要通过随意转发垃圾邮件的方式完成 A 的要求的可能性几乎为零, 从而达到了防止垃圾邮件的目的。

2.2 数字签名

2.1.2 节介绍了哈希函数可以用

于检验消息是否被篡改,但是消息的接收方却无法确认消息的发送方是谁。数字签名能很好地克服该缺点,用户首先产生2把不同密钥,其中一把为私钥,需要秘密保管;另一把为公钥,需要公开发布,且他人很难从用户的公钥推算出相应的私钥。一个数字签名方案^[16-17]包含3个多项式时间算法:

(1)密钥生成。输入系统安全参数(可以理解为用户所需密钥的长度),输出 Alice 的公钥 pk 和私钥 sk 。其中,公钥是公开的,任意实体都能获得 Alice 的公钥,而私钥则由 Alice 保密。

(2)签名。Alice 想以认证的形式将信息 m 发送给 Bob,即 Alice 希望 Bob 能够检验消息在传送过程中是否被篡改(消息完整性)以及消息的来源(消息认证性)。算法输入 Alice 的私钥 sk 和消息 m ,输出签名 σ 。

(3)验证。Bob 用 Alice 的公钥 pk 验证 σ 是否为消息 m 的签名。如果验证通过,算法输出 1;否则输出 0。

除了消息认证性和完整性外,签名还能提供不可否认性服务,即当签名人抵赖所签署过的消息时,签名 σ 可以提交给第三方仲裁机构来判定。除了上述 3 个多项式时间算法外,数字签名方案还需要满足一定的正确性要求:签名人所签署过的消息签名对必须以压倒性概率通过验证算法。

哈希-签名(Hash-Sign)思想是一类构造安全数字签名的重要措施,即先计算消息的哈希值,然后对哈希值进行签名。该思想有 3 个优点:可以抵抗无消息攻击;哈希函数可以将任意长度的消息映射成固定长度的消息摘要,于是签名算法的输入长度变成一个固定值;在证明签名方案的安全性时,可以将哈希函数模拟成随机预言器。

比特币系统所使用的签名算法为椭圆曲线数字签名算法(ECDSA)。

(1)定义 $1^{[16,18]}$ 。设定义在域 F_p

($p > 3$ 且 p 是素数)上的椭圆曲线方程为:

$$y^2 = x^3 + ax + b \quad a, b \in F_p, \quad (1)$$

$$\text{且 } (4a^3 + 27b^2) \bmod p \neq 0. \quad (2)$$

$$\text{令 } E_p(a, b) = \{(x, y) | x, y \in F_p\} \cup \{O\}, \quad (3)$$

其中, O 为无穷远点。我们称 $E_p(a, b)$ 为素数域 F_p 上的椭圆曲线。椭圆曲线 $E_p(a, b)$ 上的点数用 $\#E_p(a, b)$ 表示,称为椭圆曲线的阶。

(2)构建素数域上椭圆曲线的运算法则^[16,18]。 $E_p(a, b)$ 上的点按如下加法法则构成一个 Abelian 群:

$$1) O + O = O, O \text{ 可以视为零元};$$

$$2) \forall P = (x, y) \in E_p(a, b) \setminus \{O\},$$

$$P + O = O + P = P;$$

$$3) \forall P = (x, y) \in E_p(a, b) \setminus \{O\}, P \text{ 的逆元为 } -P = (x, -y), \text{ 满足 } P + (-P) = O;$$

$$4) 2 \text{ 个非零元的不同点相加, 设 } O, P_2 = (x_2, y_2) \in E_p(a, b) \setminus \{O\}, \text{ 且 } x_1 \neq x_2, \text{ 若 } P_3 = (x_3, y_3) = P_1 + P_2, \text{ 则 } (x_3, y_3) = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1), \text{ 其中}$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1};$$

$$5) \text{ 倍点原则, 设 } P_1 = (x_1, y_1) \in E_p(a, b) \setminus \{O\}, \text{ 且 } y_1 \neq 0, \text{ 若 } P_3 = (x_3, y_3) = P_1 + P_1, \text{ 则 } (x_3, y_3) = (\lambda^2 - 2x_1, \lambda(x_1 - x_3) - y_1), \text{ 其中 } \lambda = \frac{3x_1^2 + a}{2y_1}.$$

(3) ECDSA^[18]。首先考虑等式: $K = kG$, 若已知 k 和 G , 则由加法法则易得 K ; 但若只给定 G 和 K , 求 k (K 关于基底 G 的对数)在一些椭圆曲线上是困难的, 该问题即为椭圆曲线上的离散对数问题。为了使该问题足够困难, 椭圆曲线需要满足以下条件: $\#E_p(a, b)$ 有一个大的素因子 n , 满足 $n \geq 2^{160}$ 且 $n \geq 4\sqrt{q}$ 。接下来我们介绍具体的签名算法。

1) 密钥生成。算法输入安全参数 1^{160} , 随机选取整数 $k \in [1, n-1]$, 基点 $G \in E_p(a, b)$, 计算 $K = kG$ 。算法输出公钥 K , 私钥 k 。

2) 签名。算法输入签名人私钥 k 和消息 m , 然后进行如下步骤:

$$(a) \text{ 随机选取整数 } d \in [1, n-1];$$

$$(b) \text{ 计算 } dG = (x_1, y_1) \text{ 和 } r = x_1 \bmod n. \text{ 如果 } r = 0, \text{ 返回步骤 } a;$$

$$(c) \text{ 计算 } s = d^{-1}(H(m) + kr) \bmod n.$$

如果 $s = 0$, 返回步骤 a ;

$$(d) \text{ 输出 } m \text{ 的签名 } \sigma = (r, s).$$

3) 验证。算法输入签名人公钥 K , 签名 σ 和消息 m , 然后进行如下步骤:

$$(e) \text{ 验证 } r, s \in [1, n-1];$$

$$(f) \text{ 计算 } u_1 = H(m)s^{-1} \bmod n \text{ 和 } u_2 = rs^{-1} \bmod n;$$

$$(g) \text{ 计算 } X = u_1G + u_2K = (x_1, y_1), \text{ 如果 } X = O, \text{ 算法输出 } 0; \text{ 否则, 继续计算 } v = x_1 \bmod n;$$

$$(h) \text{ 若 } v = r, \text{ 算法输出 } 1; \text{ 否则, 算法输出 } 0.$$

3 比特币原理

本节主要介绍比特币的生成以及交易原理^[14,19]。

(1) 比特币地址。现实中, 人们想进行存钱、转账等一系列操作, 先得前往银行开个账户, 然后领取银行分配的一串数字帐号(银行卡号), 帐号的密码由用户设定。而在比特币体系中, 账户不需要由中心机构来开设, 用户首次使用比特币时只需下载客户端。用户的公私钥对由签名方案的密钥生成算法产生, 公钥即为比特币地址, 私钥由用户储藏在钱包文件中。事实上, 比特币系统具有去中心化和弱匿名性的特点, 去中心化是由于比特币的生成和交易过程没有中心机构参与; 弱匿名性是指比特币系统采用的是假名技术, 用户的公钥无法与其现实生活中的身份相联系。但是该技术无法为用户提供地址不可关联性服务和交易金额的机密性服务。地址不可关联性指的是: 任意给定 2 个公钥地址, 敌手无法在多项式时间内判断 2 个地址是否属于同一个用户。这些更强的匿名性可以由零知识证明或环签名技术实

现,本文不进行展开。

(2) 点对点(P2P)网络。NAKAMOTO S^[14]曾说过:“比特币是一种P2P的现金支付系统。”这种P2P结构的特点是:中心平台不是必要条件,每一台电脑都是一个独立体,独立体间通过互联网相互连接,最终形成密密麻麻的网络节点图。因此P2P网络一旦启动就无法停止下来,除非所有实体都退出该网络。

3.1 比特币的交易流程

3.1.1 比特币交易链条

比特币不是基于账户的密码货币,而是基于交易的密码货币。在基于账户的货币中,我们可以通过账户直接查询余额;但在比特币系统中,我们需要通过未花费交易输出(UTXO)来统计该地址余额。

每一笔交易都是由交易输入和交易输出构成。交易输入里面的字段主要是脚本签名(包含本次交易的签名和付款人公钥)、UTXO的索引,该字段表明了付款人信息和付款人的金额来源。其中,数字签名使用ECDSA,付款人先将本次交易关键数据(例如:UTXO索引、交易金额和收款人公钥)作为哈希函数的输入,计算相应的哈希值,再使用私钥对哈希值签名;交易输出里面的字段主要是脚本公钥(包含若干个脚本指令和收款人公钥地址的哈希值)、地址和金额。该字段主要表明收款人的地址和收款金额。

3.1.2 比特币交易步骤

(1) 验证本次交易是否是可支付的。比特币的所有交易记录提供了比特币UTXO查询,只有当本次交易的UTXO对应的金额大于或等于收款金额时,该笔交易才是可支付的。

(2) 用私钥签署这笔交易,并将签名放置在交易的脚本签名中。

(3) 将该交易单广播出去,寻求其他实体的认可。所有合法的比

特币交易最终都会被封装在历史区块之中。

但是上述转账过程存在一个问题:收款人很难确认比特币所有者是否对该比特币进行双重支付。

3.1.3 双重支付

(1) 无双重支付的情形。假设A有1枚比特币,要将其转给B。A首先构造一笔交易Tx1:使用私钥签署该笔交易,并将交易单Tx1广播出去。其他实体收到信息后,通过UTXO索引计算A是否有能力支付1枚比特币,如果有能力支付,则认为此次交易是合法。最后,A的钱包地址减少1枚比特币,B的钱包地址增加1枚比特币。

(2) 有双重支付的情形。如果A利用同一个UTXO构造2笔交易(Tx1:从A地址转1枚比特币给B地址;Tx2:从A地址转1枚比特币给C地址),并用私钥分别签署这2笔交易。由于消息传送具有随机性与先后性,有些实体先收到第1条交易,而有些实体会先收到第2条交易,那么比特币系统会以哪条交易为准?

3.2 挖矿

挖矿是比特币系统的工作机制,能很好地解决双重支付的问题,本节主要介绍挖矿的流程。

3.2.1 区块及其作用

区块的主要成分包括:前一个区块的哈希值、难度值、当前区块所有交易的Merkle根节点的哈希值、时间戳(区块的创建时间)和随机数。值得注意的是:上述成分中出现2个哈希值,它们使用相同的哈希函数SHA256(SHA256())(使用2次SHA256算法),区别在于函数输入不同。第1个哈希值是前一个区块创建者挑战PoW成功后的结果,区块中的随机数为创建区块的实体随机选取,目的是为了找到满足PoW要求的随机数,具体将在3.2.2节介绍;第2个是Merkle

根节点的哈希值,实体将收集到的交易放置在树状结构的最底层,每笔交易都视为一个叶子节点,开始构建Merkle树:首先计算每笔交易的哈希值,然后从下往上依次将每2个哈希值作为哈希函数的输入(每个树节点依然使用SHA256(SHA256())算法),计算出上一层哈希值,直到计算出最顶层的哈希值,即Merkle根节点的哈希值。Merkle树有2个优点:可以单独取出一个分支,对数据进行验证;可以依据树状结构快速查询到一笔交易。

区块分为区块头和区块体2部分:区块头包含前一个区块的哈希值、难度值、Merkle根节点的哈希值、时间戳和随机数;区块体包含当前区块的所有交易。

区块链就是按创建的时间顺序进行排列的区块链条,它完美地实现了一个牢不可摧且永不停息的比特币交易数据库。

比特币系统大约每10 min产生一个区块,该区块包含这10 min内未确认的交易以及前一个区块(银行的系统如果崩溃将导致其所有数据都失去了,但是比特币系统则不同,每个节点在工作时都得下载一个最新区块,该区块就包含历史全部记录,故在比特币世界中只要还有一个节点在运作,那么它的历史数据就不会丢失,因此可以视比特币系统亦或者区块链为分布式记账),因此从第一个区块问世至今就形成了一条完整的区块链。区块有2点作用:收集交易记录;做存在证明和防篡改,因为区块的哈希值施加了时间戳,一方面能证明区块的存在时间,另一方面由哈希函数的抗碰撞性知区块被篡改的概率可忽略。

3.2.2 PoW

在介绍哈希函数时已经阐述了Hashcash, Hashcash设定特定的哈希值开头作为实体的挑战目标,而实体则不断尝试不同的随机数,以期得到

满足要求的哈希值。在比特币区块的建设过程中引入一个类似 Hashcash 的规则,即 PoW 机制,它的本质是为了防止低算力的实体随意或恶意发布区块。此时,哈希函数的输入为区块头,输出是一个 256 bit 的哈希值。比特币系统会把每个区块完成的时间控制在 10 min 左右。如果难度低于 10 min,系统就自动调高难度值,增加哈希值开头 0 的位数;如果难度高于 10 min,就适当减少哈希值开头 0 的位数,以调低难度值。这是比特币系统默认的一个规则:维持 10 min 产生一个区块。这个 PoW 的过程被称为挖矿。

挖矿的本质是争夺记账权,实体(矿工)收集、检验和确认过去一段时间内发生的交易。当找到一个符合 PoW 机制的哈希值,矿工就能够将自己封装的区块广播出去,让其他矿工验证该区块。如果有矿工接受该区块并以它为基础继续挖下一个区块,那么该区块中的所有交易单就获得一次确认。每延长一个区块就等价于该区块中的交易多了一次确认。若得到 6 次确认,那么该区块就获得全网的认可,封装到历史区块中。矿工挖矿的具体流程如下:

(1) 下载一个最新区块(其中包含所有历史交易记录),计算出它的哈希值;

(2) 收集尚未被确认的交易单并使用签名技术校验交易单的有效性,把有效的交易单纳入新的区块;

(3) 选取一个随机数(这是为了满足 PoW 机制的要求);

(4) 将第(1)~(3)步产生的数值作为 SHA-256(SHA-256())算法的输入,得到一个 256 bit 的二进制数,并检查这个数是否符合 PoW 机制的要求;

(5) 如果满足 PoW 要求,则向全网广播新区块。若其他矿工接受本区块,就会在该区块末尾继续进行挖矿工作以延长区块链。若不符合 PoW 要求,则重复第(2)~(5)步,直

到符合要求或者接收到其他矿工发布的新区块。

在比特币世界中每 10 min 会产生新增比特币奖励给成功建立新区块的矿工,每个区块的奖励在最初的 4 年中是 50 个比特币(4 年大概产生 21 万个区块),之后的 4 年每个区块是 25 个比特币,依次类推下去,最终系统只能产生 2 100 万个比特币^[20]。同时,新区块的建立者会获得每笔交易所产生的交易费用。

基于上述挖矿过程可知:双花意味着需要广播同一笔比特币的 2 次不同交易单。矿工在收集时只会将其中一个封装在自己的区块中,从而能够有效地防止双花。

3.2.3 区块链的延长和交易的最终确认

每笔比特币交易只有获得 6 次确认,才能认定为有效。在挖矿过程中,同一段时间会生成很多有效区块,不同有效区块中的元素除前一个区块的 ID 是相同外,其他元素几乎都不同,例如:交易单集合就是不同的。若 1 个节点收到 2 个有效区块,则将这 2 个区块都放在主区块链的后面,并形成 Y 型分叉,后续收到的区块则基于这 2 个区块产生,使区块链延伸下去。矿工始终选择最长的分支成为主区块链的一部分,并继续工作以延长区块链。一般包含这个交易的区块出现后,还需等待 5~6 个后续的区块生成,才能确定该区块是否进入主区块链,从而最终确认区块中的交易是否有效。可见比特币的交易所需时间比较长。

4 比特币的主要特点

比特币的本质和大多数虚拟货币一样,由一堆代码组成,但同时它 also 具有许多传统虚拟货币不具备的优点^[21-23]。

(1) 去中心化思想,发行数量固定。法币的发行受政府与中央银行约束;但比特币不同,它采用区块链

技术和非对称密码技术,发行不受央行约束,而且比特币的发行具有上限,从而避免一些因为人为决策因素而导致的货币贬值。

(2) 交易成本低廉。比特币的交易不需要中介机构,交易成本低廉(但对小额交易而言,成本较高)。同时,比特币中的用户采用的是假名,国家很难收取比特币的交易税。

(3) 货币不可伪造,无法双重支付,交易不可逆转。系统中的每个区块都有记录可查,想要伪造比特币几乎不可能。区块链会不停地延长,一旦交易被全网接受并装入历史区块后是不可撤销或逆转的。同时,比特币的 PoW 机制能很好地防止双重支付现象。

(4) 全球化转账支付。比特币的交易效率相对与中国境内的同行或跨行转账效率慢,这是因为中国的银行都有一个可信任的第三方(央行),因此交易双方的身份认证很便捷;但比特币具有一个显著的优势:可打破国界进行全球化转账支付,且该效率比目前法币的跨国转账效率高。法币进行跨国转账时,两国的银行中间缺少一个可信赖的第三方,造成双方的身份认证十分漫长。

(5) 开源。比特币的原理和技术都是公开的,还有其软件代码也是基于开源协议发布的,莱特币就是基于比特币协议产生。

与此同时,比特币的缺点也是显而易见。

(1) 在比特币世界中,私钥代表一切,一旦私钥泄漏或遗忘,意味着你的比特币财富也将失去,且他人无法帮你找回丢失的比特币。

(2) 比特币无央行发行,无政府部门为其交易和安全保驾护航,这也是人们对比特币信心不足的主要原因之一。

(3) 比特币的系统虽然很健壮,但它的交易平台(通常是一个网站)是脆弱的,易遭受黑客攻击,例如: Mt.Gox 曾是世界最大的比特币交易

平台,但被恶意攻击,于2014年2月28日宣布破产,比特币的行情大跌。

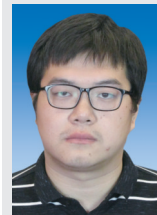
5 结束语

文中,我们主要介绍比特币系统中涉及的相关密码技术,包含签名、哈希函数以及区块链技术。尤其是区块链技术,以链状结构存储数据,以密码技术为数据传输提供机密性和认证性服务,从而形成一条分布式存储、无法篡改、永无止息的数据库。但比特币等诸多数字货币在一定程度上具有匿名性,使得监管问题日益严峻,如何在保护实体隐私的同时实施有效的监管是数字货币领域的一大挑战。另一方面,由于区块链技术能摆脱第三方机构制约,使得它不再局限于数字货币领域。目前,区块链技术在金融服务、公共服务和IoT等领域的应用尚处于探索阶段,有待进一步发掘。

参考文献

- [1] BUTERIN V. Ethereum: A Next Generation Smart Contract and Decentralized Application Platform [EB/OL]. [2018-10-23]. <https://github.com/ethereum/wiki/wiki/White-Paper>
- [2] LIU J K, WEI V K, WONG D S. Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups [C]// Information Security and Privacy: 9th Australasian Conference, (ACISP 2014). Berlin: Springer, 2004: 325-335. DOI: 10.1007/978-3-540-27800-9_28
- [3] BEN-SASSON E, CHIESA A, GARMAN C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin[C]// 2014 IEEE Symposium on Security and Privacy. USA: IEEE, 2014: 459-474. DOI: 10.1109/SP.2014.36
- [4] BEN-SASSON E, CHIESA A, GREEN M, et al. Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs[C]// 2015 IEEE Symposium on Security and Privacy. IEEE: USA, 2015: 287-304. DOI:10.1109/SP.2015.25
- [5] HAYEK F A. Denationalization of Money [EB/OL]. [2018-10-23]. https://mises-media.s3.amazonaws.com/Denationalisation%20of%20Money%20The%20Argument%20Refined_5.pdf?file=1&type=document
- [6] LAMPORT L. Password Authentication with Insecure Communication [J]. Communications of the ACM, 1981, 24(24): 770-772. DOI: 10.1145/358790.358797
- [7] CHAUM D. Blind Signatures for Untraceable Payments [C]// Advances in Cryptology: Proceedings of CRYPTO '82. Berlin: Springer, 1982
- [8] CHAUM D, HEYST van E. Group Signatures [C]// Advances in Cryptology - EUROCRYPT'91, Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1991: 257-265. DOI: 10.1007/3-540-46416-6_22
- [9] MERKLE R C. A Digital Signature Based on a Conventional Encryption Function[C]// Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1988: 369-378
- [10] DWORK C, NAOR M. Pricing via Processing or Combatting Junk Mail[C]// CRYPTO '92 Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer, 1992: 139-147. DOI: 10.1007/3-540-48071-4_10
- [11] SZABO N. Bit Gold[EB/OL]. [2018-10-23]. https://en.wikipedia.org/wiki/Nick_Szabo#Bit_gold
- [12] NIST. Descriptions of SHA-256, SHA-384 and SHA-512[EB/OL]. [2018-10-23]. <http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf>
- [13] 李钧, 长铁. 比特币[M]. 北京: 中信出版社, 2014
- [14] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. (2009-02-08) [2018-10-23]. <https://bitcoin.org/bitcoin.pdf>
- [15] ADAM B. A Partial Hash Collision Based Postage Scheme [EB/OL]. [2018-10-23]. <http://www.hashcash.org/papers/announcetxt>
- [16] KATZ J, LINDELL Y. Introduction to Modern Cryptography [M]. Florida: CRC Press, 2007
- [17] DIFFIE W, HELLMAN M E. New Directions in Cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654. DOI: 10.1109/TIT.1976.1055638
- [18] JOHNSON D, MENEZES A, VANSTONE S. The Elliptic Curve Digital Signature Algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63. DOI: 10.1007/s102070100002
- [19] FRANCO P. Understanding Bitcoin [M]. Britain: John Wiley & Sons, 2014
- [20] 于江. “新型货币比特币”:产生,原理与发展[J]. 吉林金融研究, 2013, (5): 17-19. DOI: 10.3969/j.issn.1009-3109.2013.05.005
- [21] 罗强, 张睿. 比特币[M]. 北京: 机械工业出版社, 2014
- [22] 张超. 新型虚拟货币比特币的发展现状及其对现实经济和金融影响的研究[J]. 时代金融, 2013, (5): 291-293
- [23] 刘宁, 沈大海. 解密比特币[M]. 北京: 机械工业出版社, 2014

作者简介



林成骏, 福建师范大学数学与信息学院在读硕士研究生; 研究方向为格密码与同态签名。



伍玮, 福建师范大学数学与信息学院副教授; 研究方向为密码学; 主持国家自然科学基金项目2项, 参与教育部留学回国人员基金等科研项目; 获得福建省自然科学基金优秀学术论文三等奖; 已发表学术论文60余篇。

区块链概念剖析及其在物联网中的部分应用

Concept and Partial Applications of Blockchain in Internet of Things

田海博/TIAN Haibo

(中山大学, 广东 广州 510275)
(Sun Yat-Sen University, Guangzhou
510275, China)

中本聪提出一种点到点的现金系统^[1],并在2009年公开了源代码。通过社区的推进,人们开始尝试使用比特币进行支付,第一个例子就是使用一万个比特币购买一个披萨。比特币源于社区,并自带粉丝,社区内成员自我铸币、自我消费。继比特币之后,出现了如莱特币^[2]、点点币^[3]、名字币^[4]等以各种名目发行的密码货币,因其总量固定,所以粉丝越多其汇率越高。

GAVIN W^[5]在2014年对比特币做了2个改进:第1个是提供以太坊虚拟机(EVM),用于执行任意用户自定义的代码,实现智能合约;第2个就是把比特币中存放在未花费输出交易(UTXO)中的货币和状态、代码存放在一个账户下面,即所谓的账户模型。以太坊的出现,极大地简化了人们发行新币的过程,于是区块链领域上演了一场初始代币发行(ICO)的大剧,各类项目良莠不齐。

IBM开发的Fabric^[6]看到了另外一

摘要: 把去中心化、不可篡改和激励机制定义为区块链技术的典型特点,而把可追踪、匿名和可编程定义为区块链技术的功能特性,同时分析了每一个特点和特性的底层支撑技术,以更好地判断区块链项目的真伪及可实现性。在该定义的基础上,分析了物联网(IoT)场景下几个典型的区块链项目,并对其中的一些主要问题和主要方法进行了详细阐述,认为IoT的数据体量和数据安全问题依旧是需要重点考虑的问题。

关键词: 区块链;支撑技术;IoT应用

Abstract: The decentralization, non-tampering and incentive mechanism are defined as the typical features of blockchain technology, and the traceability, anonymity and programmability are defined as its functional characteristics. Then the underlying supporting technologies of each feature are analyzed to better judge the authenticity and realization of blockchain projects. Further, several typical blockchain projects in the Internet of things (IoT) scenario are analyzed, and main problems and technical methods are described. It is pointed out that the data volume and data security of the IoT are still the key issues to be considered.

Key words: blockchain; supporting technologies; IoT applications

个生存空间,那就是避开以太坊,构造联盟链,在企业中运行。得益于IBM的代码质量和一贯良好的形象,Fabric很快在联盟链中占据了主导地位。Fabric的特点是不用密码货币,转而用节点背书,其中每个节点的身份可以识别,不诚实的节点需要付出代价。目前在大部分所谓落地的应用中,例如:银行、供应链、积分、税务等场景,无一例外地采用了联盟链的模式。

区块链是内生在比特币中,用于记录比特币交易,所以有时称之为账本。ARUIND N等人^[7]从数据结构上看,认为区块链就是一个用哈希指针取代了内存指针的一个链表。PASS

R等人^[8]从协议上看,认为区块链就是一个协议,协议参与者各自本地维护的一个数据列表称为链,参与者把收到的消息包含在自己的和其他所有参与者的链中。这些定义各有其优缺点,例如:ARUIND N的定义没有考虑共识,PASS R等人的定义专门用于比特币。

本质上,区块链由一组基于点对点(P2P)网络的节点形成,各节点通过执行共识算法,维护其各自数据的一致性。去中心化、不可篡改和激励机制通过该定义可以体现。其中,P2P网络和共识算法是去中心化的具体体现,也是不可篡改的前提和必要条件,激励机制则是各节点维护其数

收稿日期:2018-10-22
网络出版日期:2018-11-14
基金项目:国家重点研发计划
(2017YFB0802500)

据一致性的动力所在。可追踪、匿名、可编程这些特点则是对区块链的一致数据赋予语义之后得到的功能特性。我们下面对区块链技术进行分析,指出其典型特点和功能特性的技术支撑,然后再探讨区块链技术在物联网(IoT)场景的几个应用。

1 区块链典型特点

区块链技术的典型特点包括去中心化、不可篡改和激励机制。

1.1 去中心化

去中心化属于区块链技术的基本属性,是区块链技术和其他技术得以区分的基本特点。去中心化既有物理基础又有组织形式,具体如下:

(1) 物理基础

比特币、众多山寨币和一些无币区块链项目大都会坚持使用P2P网络,这其实是去中心化的物理基础。我们知道纯粹的P2P网络是没有服务器角色的,每个节点既是服务器又是客户端,彼此地位均等。这种地位均等与设备的计算能力、网络带宽等无关。

(2) 组织形式

在P2P网络之上,基于比特币的工作量证明(PoW)算法,比特币中每个节点潜在地具有记账的权力,这是一种表面的去中心化,因为这种权力与节点的算力等资源密切相关。事实上,比特币网络中记账的权力集中在几个大矿池手中,是一种联盟记账的模式。成为这个特定联盟的节点并不需要其他节点的允许,而是单纯地依靠算力比拼,可以称之为无组织算力联盟。我们使用无组织这个词,是因为在这个联盟中,各个成员节点是纯粹的竞争性关系,不存在哪一个矿池服从其他矿池的情况,这与一般的由某个企业或者单位主导形成的联盟有所不同;在基于其他共识算法的区块链中,具有记账权力的节点首先是独立的,然后节点之间依靠某种规则确定记账节点的集合,形成

一个动态的记账联盟,与比特币的最终形态是类似的,不同之处在于不依赖PoW的记账联盟往往则需要某种集体许可的机制,这是一种有组织的联盟。

1.2 不可篡改

数据不可篡改是区块链中数据的基本属性,我们分基于PoW、基于数字签名和基于数据冗余3部分来阐述。

(1) 基于PoW的不可篡改

对于采用PoW的区块链技术,每一个区块的生成背后都有算力的竞争,进而有区块难度的概念。区块难度基本表明了一个区块生成时生成该区块的节点所需要付出的计算代价。因此,给定一个比特币区块链,任何设备想要重新生成一条具有同等难度的区块链都必须付出同等的累积计算力量。鉴于比特币区块链消耗的巨大大计算资源,在计算能力没有本质突破的前提下,任何设备都难以承受重新生成一条区块链的代价。因此,比特币区块链的数据拥有者们只能删除自己存储的数据,而无法对其进行任何修改;而单个节点对数据的删除,并不会改变其他节点拥有的数据副本,因而比特币网络中的数据具有非常强的不可篡改性。

(2) 基于数字签名的不可篡改

权益证明(PoS)是根据节点权益决定区块的生成节点的一种共识算法。当PoS共识指定某个节点充当区块的生成节点时,该节点通过数字签名表明该区块是其生成的。因此基于PoS的区块链是一种由数字签名保护的区块链。给定任意一个PoS区块链,一个节点可以删除数据,也可以自己生成很多的公私钥对,进而形成一个具有不同数字签名的伪区块链。与基于计算难度的区块链不同,这个伪区块链只能通过验证数字签名来区分,进而需要PoS区块链明确哪些公钥是属于这个区块链的,哪些是合法的。只有这些明确了,才能

明确哪一个PoS区块链是真的,哪一个假的。在一个PoS区块链有明确的参与节点边界之后,单个节点的数据删除并不会影响其他节点的数据副本,因而数据具有不可篡改性。如果这个节点边界的范围非常小,并且所有节点的数据都被删除了,数据就真的从这个区块链删除了,这就是明确的边界带来的代价。

(3) 基于数据冗余的不可篡改

采用拜占庭容错类算法的区块链或直接采用修改的分布式数据库技术保持数据一致性的区块链,如果不采用数字签名,其数据的不可篡改性只能来自数据冗余。任意节点可以修改自己的本地数据,但是节点是独立的。一个节点删除或修改自己的数据并不影响其他节点,因而当查询一份数据时,多数节点给出的结果就是该数据的真实情况。此时数据的不可篡改依赖维护一个区块链的诚实节点的数量。我们再次强调节点独立的重要性:对于一些直接采用了分布式数据库技术的区块链项目,经过测试,维护分布式数据库的节点并不是独立的,因而任意有权限的节点删除数据会使得其他节点“同步”地删除数据,这样的区块链项目是没有不可篡改性的。类似地,由单个企业或者单位维护的区块链项目,其不可篡改性是需要质疑的。

1.3 激励机制

激励机制在区块链中有重要的作用,它使得人们对联盟节点的行为可以预期,进而产生信任。以无组织算力联盟为例,联盟成员一般不会特意地阻断某一个交易,联盟成员会努力计算,期望自己获得区块的奖励。这种可预期的行为是信任产生的基础。所以区块链的可信与区块链节点行为的可预期相关,而行为的可预期则与激励机制相关。比特币长期的实践经验告诉我们:激励良好且相互制衡的联盟成员行为可以预期、可以信任。在有组织的联盟中,激励机

制同样是不可或缺的,在其治理下,可以使用奖惩的方法,并且形式也可以多样化,可以不使用货币,形成所谓的无币区块链项目。

在有币的区块链项目中,激励机制是否有效取决于项目的代币是否可支付,例如:比特币的可支付来自社区内的认同。众所周知,有一万个比特币换取披萨的事情,那么为什么是一万个不是五千个呢?我们可以推测持有比特币的一方用电费来衡量自己获取的比特币在当时的价值,披萨的销售者一方面必然是比特币社区的成员,一方面还可以用电费衡量披萨的价值,于是你情我愿之下,才会有这样的一笔交易。我们特别推测了披萨店主应该是比特币社区的成员,或可以说是比特币的粉丝;否则,这笔交易是不会发生的。所以我们认为认同是支付的前提。如果项目的参与者对项目不认同,可支付性降低,激励机制失效,那么这个项目就很难有效地运行。

1.4 功能特性

区块链技术的基本特点是区块链得以成为区块链的关键,而功能特性则是对数据进行不同的语义赋值之后得到的特性,例如:可追踪、匿名和可编程。

(1) 可追踪

当区块链中的数据彼此具有链接关系时,就有了某种可追踪性。以比特币为例,一个新生成的比特币交易中包含输入交易的哈希值,输入交易也是交易,也包含其输入交易,以此类推,可以直接推到多个铸币交易。那么,从铸币交易集合到新生成的这个比特币交易就形成了一棵树,树根是新生成交易,树上的任意一笔交易都与新生成的交易相关。然而,在不使用区块链技术的情况下,一个中心化的服务器也可以使用这种链式关系来形成其存储数据的可追踪性。因此,可追踪性只与具体的数据结构以及应用的语义有关系。

(2) 匿名

区块链中的数据都是有来源的,在大多数项目中,这个来源只能使用一串公钥标识出来。公钥是可以任意生成的,因而与人或物的一些真实身份信息没有直接的对应关系,因而具有了某种匿名性。比特币提供的这种匿名准确一些叫做假名。一个实体可以随便生成公钥,但公钥与资产绑定后,通过交易的可追踪性可以大概率地通过一些简单的聚合算法找出一个实体的不同公钥。这些公钥尽管还不能直接对应到人,但再加上一些交易时间分析、IP地址分析和社会工程学方法,终究还是可以把人找出来,因此比特币的这种假名技术并没有提供太多的保护。有许多的项目致力于提高匿名性,提供真实匿名的系统,例如:零币,可以隐藏交易金额、实体等信息,具有更好的匿名性。匿名性是对数据的语义分析之后得到的某个项目是否保护参与实体身份等信息的安全属性。

(3) 可编程

比特币提供的脚本语言可以让交易方明确比特币转移的条件;而脚本语言本质上是一种编程语言,因而人们一般认为区块链资产具有可编程的特点。以太坊的出现强化了人们的这种观念。以太坊提供了一个准图灵机,让人们可以自定义智能合约,以完成资产的管理。智能合约是一种技术手段,随着合约内容涉及的应用领域不同,出现了保险、供应链、公证等诸多社会生活领域的智能合约,因而出现了所谓可编程社会的观点。事实上,可编程也可以看成对数据的语义赋值之后的功能特性,只不过现在维持一致的数据包括了“代码数据”而已。

以上我们把区块链的技术特点分为去中心化、不可篡改、激励机制3个,并把可追踪、匿名、可编程看成区块链数据的语义赋值。通过这些分析,我们自然地可以把单个企业提供的“区块链”服务、“云区块链”等

项目与真正的区块链项目区分开。

2 区块链技术在IoT中的部分应用

IoT场景有2个典型特点:数据量大,设备无时无刻不在产生数据;数据安全很重要,因为IoT数据可以与工控安全、居家环境等现实社会的生产生活建立直接的关联,因而其数据的机密性、完整性和可用性是必须要考虑的。区块链技术所保障的仅仅是数据的完整性,为数据的可用性提供了便利,但是并没有对数据机密性进行任何的考虑。下面我们选择几个典型的IoT场景区块链项目来分析区块链技术在IoT中的应用。

2.1 IOTA技术

IOTA^[9]是区块链技术在IoT中应用的一个主要代表,主要考虑了IoT数据体量的问题。IOTA技术的白皮书主要披露了一个纠缠(Tangle)账本。纠缠账本是一种基于有向无环图(DAG)的分布式账本底层技术,其基本安全假设为:攻击者生成交易的速度需要小于诚实网络节点生成交易速度的和。在这一假设下,为了鼓励诚实节点生成交易,不收交易费。考虑到IoT设备生成的数据体量较大,不收交易费也就成了该技术适用于IoT的一个主要原因。

纠缠账本的问题集中在账本安全性和激励机制2个方面:在账本安全性上,交易速度的假设还需要实践检验;在激励机制上,在没有交易费的情况下如何激励节点存储大量的IoT交易也是需要经过实践检验的。

2.2 沃尔顿链

沃尔顿链^[10]是一个结合硬件的IoT应用项目,考虑了IoT数据的产生和管理问题。该团队开发出了区块链读写器,可以把标签数据的哈希值通过读写器直接写入区块链中。同时读写器与标签具有双向认证的功能,可以确保数据的来源是经过认证

的。对于数据量较大的问题,该团队构思了跨链架构,希望该架构能承载众多不同形态、不同应用场景的子链。该项目的跨链思路还需要实践检验。

2.3 智能混杂网络(SMT)项目

SMT项目^[14],致力于为移动设备提供一个有激励措施的通信平台,其考虑更多的是IoT的数据通信方式的问题。从愿景上看,该项目希望提供一个平行于互联网的全球移动设备通信平台。从技术组成上看,该项目基于以太坊,准备采用雷电网络的技术支持移动设备之间的“链下”支付。该技术特点与愿景是有矛盾的,因为雷电网络终究是不能离开以太坊的在线支持。该项目的激励措施在于转发数据可以获得奖励,但白皮书中并没有披露具体的奖励算法,毕竟数据的来源往往是一个用户,而参与转发的则涉及多个用户。另外,IoT场景中的通信问题是否是一个关键性的问题还需要实践检验。

2.4 Streamr项目

Streamr项目^[12],意在基于以太坊智能合约建立一个适用于IoT的数据产生和消费平台。IoT设备作为数据产生的源头,把经过接收方公钥加密的数据发送给该网络的中介节点。不同的中介节点群处理不同的IoT数据,形成可扩展的架构。中介节点群之间的管理通过以太坊智能合约实现。数据接收方通过中介节点获得加密的数据,并通过自定义的该项目的合约平台完成数据处理。然而,以太坊作为一个一般性平台,最近一直受到交易速度的困扰。该项目底层完全依赖以太坊,其基本的交易处理速度受限于以太坊,因此在IoT中的

实用性还需要进一步的检验。

2.5 Ruff项目

Ruff项目^[13],把边缘计算的概念和区块链结合在一起,提供了统一的IoT应用接口,并提供IoT主控设备和受控设备的全局管理,它属于IoT数据应用层面的项目。该项目中轻节点代表具体的IoT受控设备,该设备通过存储主控设备的公钥来识别主控设备的命令。通过智能合约,主控设备可以把受控设备的部分功能以租赁或转移的形式提供服务。该项目搭建自己的公链,采用了股份授权证明(DPoS)共识算法,每轮选择105个节点参与区块生成。该公链能否承载其设备租赁的服务模式,还需要在实践中检验。

以上我们对几个典型的以IoT为应用场景的区块链项目进行了分析,可以看到目前人们对于IoT场景下数据量较大、数据较为敏感的问题已经有了初步的建议方案,另外对IoT的通信方式、数据使用方式、数据生成方式进行了积极的探索。

3 结束语

本文中,我们提出去中心化、不可篡改和激励机制属于区块链技术的本质特点,而可追踪、匿名、可编程属于区块链数据之上的功能特性,以此可以区分一些区块链项目和借区块链概念的项目。进一步地,我们分析了区块链技术在IoT场景的几个应用,对其中的主要问题和主要方法进行了阐述,指出IoT的数据体量和数据安全问题依旧是区块链技术在IoT场景应用需要重点考虑的问题。

参考文献

- [1] SATOSHI N. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. [2018-10-

- 22]. <https://bitcoin.org/bitcoin.pdf>
 [2] QIWEI L. Litecoin - Open Source P2P Digital Currency [EB/OL]. [2018-10-22]. <https://litecoin.org>
 [3] KING S, NADAL S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [EB/OL]. [2018-10-22]. <https://peercoin.net>
 [4] Namecoin [EB/OL]. [2018-10-22]. <https://github.com/namecoin>
 [5] GAVIN W. Ethereum: A Secure Decentralised Generalised Transaction Ledger [EB/OL]. [2018-11-08][2018-10-22]. <https://ethereum.github.io/yellowpaper/paper.pdf>
 [6] Hyperledger Fabric [EB/OL]. [2018-10-22]. <http://hyperledger-fabric.readthedocs.io/en/release-1.1>
 [7] ARVIND N, JOSEPH B, EDWARD F, et al. Bitcoin and Cryptocurrency Technologies A Comprehensive Introduction [M]. Princeton: Princeton University Press, 2016
 [8] PASS R, SEEMAN L, SHELAT A. Analysis of the Blockchain Protocol in Asynchronous Networks [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. France: Springer International Publishing, 2017, (10211):643-673
 [9] SERGUER P. The Tangle [EB/OL]. [2017-10-01][2018-10-22]. <http://www.docin.com/p-2088809407.html>
 [10] Waltonchain. Waltonchain White Paper [EB/OL]. [2018-10-22]. https://www.waltonchain.org/templates/default/doc/Waltonchain White Paper 2.0_CN.pdf
 [11] SMARTMESH. The Smartmesh whitepaper [EB/OL]. [2018-10-22]. <https://smartmesh.io>
 [12] STREAMR. Unstoppable Data for Unstoppable Apps: DATAcoin by Streamr [EB/OL]. [2018-10-22]. <https://www.streamr.com>
 [13] ROY L. Ruff IoT Blockchain Whitepaper [EB/OL]. [2017-10-01][2018-10-22]. <https://github.com/RuffNotes/RuffChain/blob/master/WhitePaper.md>

作者简介



田海博,中山大学数据科学与计算机学院副教授、网络空间安全系副主任;主持国家自然科学基金项目、教育部基金项目、广东省自然科学基金项目等,作为骨干人员参与了国家重大研发计划网络空间安全专项2项;目前已发表论文60余篇,公开专利30件,参与起草已发布的行业标准1部。

基于区块链的物联网密钥协商协议

Blockchain-Based Key Agreement Protocol for Internet of Things

张佳妮/ZHANG Jiani
何德彪/HE Debiao
李莉/LI Li

(武汉大学, 湖北 武汉 430070)
(Wuhan University, Wuhan 430070, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0023-005

摘要: 针对传统物联网(IoT)交易场景下, 双方使用椭圆曲线算法签名交易时证书颁发与维护的巨额开销问题, 提出使用基于身份的 Schnorr 签名替换原有的椭圆曲线数字签名, 以实现 IoT 设备间轻量级的身份认证。提出了基于 Diffie-Hellman 和基于 YAK 2 种比特币密钥协商协议, 实现了交易后比特币用户间端到端的安全通信。其中, 基于 YAK 的密钥协商协议通过零知识证明(ZKP)提供了前向安全。

关键词: 区块链; IoT; Schnorr; 密钥协商; ZKP

Abstract: In view of huge cost of certificate issuance and maintenance in traditional Internet of things (IoT) transaction scenario where both parties use elliptic curve algorithm to sign transactions, an identity-based Schnorr signature is proposed to replace the original elliptic curve digital signature to realize the lightweight identity authentication between IoT devices. Two bitcoin key agreement protocols based on Diffie-Hellman and YAK have been proposed which achieve end-to-end secure communication between bitcoin users after transactions. Meanwhile, the YAK-based protocol can provide forward security through Zero-Knowledge Proof (ZKP).

Keywords: blockchain; IoT; Schnorr; key agreement; ZKP

国际电信联盟 (ITU) 将物联网 (IoT) 定义为: 信息社会全球基础设施 (通过物理和虚拟手段) 将基于现有和正在出现的、信息互操作和通信技术的物质相互连接, 以提供先进的服务。它起源于 1999 年美国麻省理工学院 (MIT) 提出的无线射频识别 (RFID) 的思想, 并在 2005 年的信息社会世界峰会 (WSIS) 被正式确定概念^[1]。IoT 本质上是一个传感器智能网, 它通过 RFID、红外感应器、激光扫描仪等传感设备将物与互联网相连, 从而实现智能化识别、定位、监测控制与管理。IoT 被认为是信息产业继计算机、互联网之后的第 3 次浪潮, 是实现智慧城市^[2]的关键技术; 但其自身存在一些技术瓶颈。传感网络的大规模和分布式特性使得 IoT 的安全运维成为一大挑战, 例如: 基于 Mirai 僵尸物联网的分布式拒绝服务 (DDoS) 攻击就曾使得 Dyn 瘫痪, Twitter、Paypal 等人气网站停止服务。随着 IoT 设备的指数级增长, 数

据流的中心化管理负载过重, 容易造成信息堵塞。此外, IoT 还存在数据标准不一致引起的通信兼容问题。

区块链作为一种新兴的信息技术, 具有公开可验证、可编程、可追溯、防篡改等性质。通过区块链技术构建 IoT 系统 (如图 1 所示), 由区块链充当通用的数字账本, 节点设备广播交易, 经区块共识后记录上链, 可实现数据的可证溯源。同时, 加密算

法保障了交易数据的隐私性、完整性, 共识算法实现了节点间数据的一致性。区块链去中心化的运行机制规避了高额的运维成本, 数以亿计闲置设备的算力、存储被充分利用, 实现了 IoT 安全扩容。此外, 其激励机制促进了数据升值, 点对点 (P2P) 网络打破了信息孤岛桎梏, 促进了设备间的多方协作和信息交流。2015 年出现的比特币电脑可实现区块链小

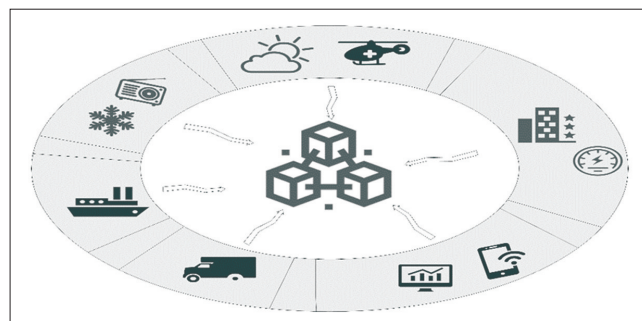


图 1
区块链在物联网的应用

收稿日期: 2018-10-17
网络出版日期: 2018-11-19
基金项目: 国家重点研发计划基金资助项目 (2018YFC1315404)、国家自然科学基金资助项目 (61402339, 61572370)

微支付网络与IoT的连接。通过分布式资源调配,构建起真正的分享经济模式。2017年全球首个IoT区块链(BOT)项目成立,定义了可信IoT服务平台框架。区块链与IoT的结合有效地解决了IoT缺乏隐私、运维高昂、通信不兼容等行业痛点,有力地推动了智慧城市^[3]的发展。

为了实现IoT设备安全可靠的数据通信,亟需一个安全的密钥协商协议以提供身份认证。文献[4]首次提出2个比特币密钥交换协议,以实现交易后比特币用户间端到端的安全通信。然而在该方案中,交易双方使用椭圆曲线数字签名算法(ECDSA)确定交易的所有权。随着IoT设备的指数级增长,数以亿计的设备都需要生成和维护一个公钥证书。为了规避证书颁发与维护的巨额开销,我们提出使用基于身份的Schnorr签名替换原有的ECDSA签名,不再使用公钥证书,从而实现了物联网设备轻量级的身份认证。进一步地,我们提出了2种密钥协商方式:基于Diffie-Hellman的比特币密钥协商协议、基于YAK的比特币密钥协商协议。其中,基于YAK的比特币密钥协商协议通过零知识证明(ZKP)提供了前向安全性。

1 关键技术

1.1 基于身份的Schnorr签名方案

该方案由以下4个算法组成。

(1) *Setup*: 输入安全参数 k , 系统选择一个阶 q 为 $2^k \leq q < 2^{k+1}$ 的群 G , 令 g 为 G 的生成元。系统选择2个安全的密码哈希函数 $H_1, H_2: \{0,1\}^* \rightarrow Z_q$, 并随机选择 $s \in {}_R Z_q$ 作为系统主私钥。最后,系统秘密保存 s 并公开参数 $\{G, g, q, H_1, H_2, g^s\}$ 。

(2) *Extract*: 给定用户身份 $id \in \{0,1\}^*$, 系统随机选择 $r \in {}_R Z_q$, 计算 $d_{id} = r + sH_1(g^r, id) \bmod q$, 并通过安全信道发送 d_{id} 给用户。

(3) *Sign*: 给定消息 $m \in \{0,1\}^*$,

用户随机选择 $t \in {}_R Z_q$, 计算 $e = t + d_{id} \cdot H_2(id, g^t, m) \bmod q$, 用户输出消息 m 的签名 $\sigma = (g^t, e, g^r)$ 。

(4) *Verify*: 给定消息签名对 (m, σ) , 验证者通过式(1)验证签名 σ 的有效性:

$$Ver(id, m, \sigma) = 1 \Leftrightarrow g^e = g^t (g^r g^{s \cdot H_1(g^t, id) \cdot H_2(id, g^t, m)}) \quad (1)$$

若签名 σ 有效, 返回“1”; 否则, 返回“0”。

1.2 比特币

比特币^[5]是区块链技术在数字金融领域的第一个应用, 是一种基于P2P网络的虚拟加密货币。它为每个比特币用户生成公私钥对, 其中私钥用于签名交易, 公钥用于验证数据。比特币网络可以实现用户匿名识别、比特币转移, 以及历史交易的记录上链, 具有去中心化、匿名性、通胀预防等特点。目前, 一些主流交易平台有: btc-e.com、bitstamp; 中国的主流交易平台有比特币中国、OKCoin、火币等。截至日前, 比特币的流通市值已达到7 743.97亿元人民币, 日成交额达到280.328亿元人民币。

1.2.1 比特币交易

比特币交易是相互关联的输入输出交易事务, 使用未经使用的交易的输出(UTXO)作为输入, 并生成新的输出。同一笔交易可以有多个输入和多个输出, 具体交易格式如表1所示。

比特币地址由公钥经一系列哈希、编码而来, 即:

比特币地址 = Base58{Hash160||前4字节(SHA256(SHA256(Hash160||地址版本号)))}

其中, Hash160=RIPEMD160

(SHA256(65字节公钥))。

1.2.2 区块

网络中的所有交易由背书节点收集验证打包上链, 经过6个区块确认后交易不可逆转。平均每10 min生成一个新区块链接到最长的链尾部。整个区块链是一个链式结构^[6], 如图2所示, 其中Tx表示交易。

1.2.3 共识机制

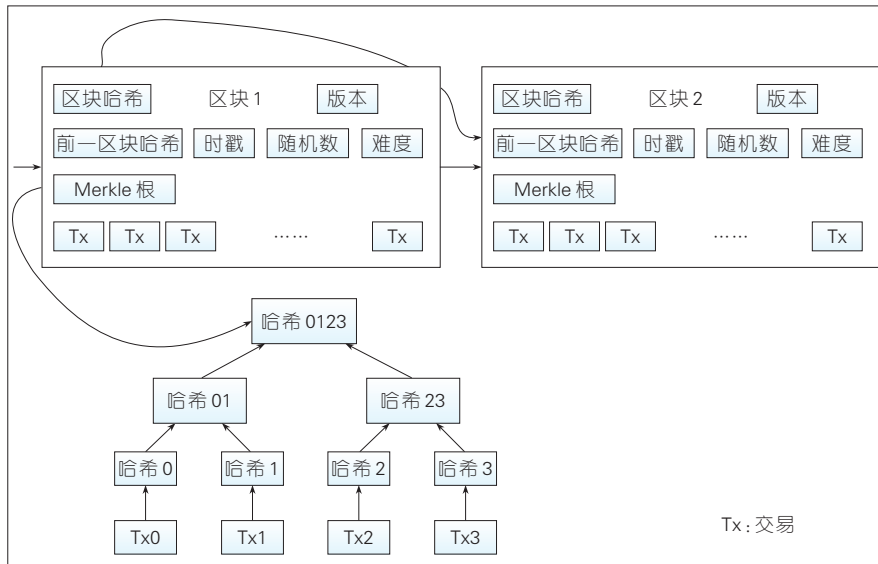
共识机制^[7-8]是分布式网络中互不信任节点间建立共识的规则与方法。现有的共识机制根据通信方式可分为异步通信共识机制和同步通信共识机制。异步通信共识机制的代表为有向无环图(DAG), 与定期检查同步点的日志机制不同, DAG采用异步处理事务操作的方式, 极大地提高了系统吞吐量。区块链主要使用同步通信共识机制。其中, 同步通信共识机制包括强一致性共识算法和最终一致性共识算法。最终一致性共识算法多用于私有链、联盟链的共识, 可进一步细分为具备拜占庭容错特性^[9]的一类, 如授权拜占庭容错(DBFT)、实用拜占庭容错(PBFT)、资产证明(PoA)、Ripple、Pool验证池等; 不具备拜占庭容错特性的一类, 如Paxos、Raft等。强一致性共识算法多用于公有链的共识, 包括工作量证明(PoW)、权益证明(PoS)、股份授权证明(DPoS)、重要性证明(PoI)等, 具体分类参见表2。

比特币区块链的共识主要采用强一致性算法中的PoW、PoS、DPoS。

(1) PoW。寻找随机数 n , 使得: $SHA(SHA(rlh_p || rlh_n || h_m)) < \text{目标哈希}$, 最先找到随机数 n 的矿工获得记账权并获得比特币奖励, 这一过程也称

▼表1 比特币交易格式

交易类型与编号	输入	输出
Coinbase, 001		序号为1, 金额为10, 地址为Alice
002	001	序号为1, 金额为2, 地址为Bob
002	001	序号为2, 金额为8, 地址为Alice



▲图2 区块链的链式结构

▼表2 共识机制的分类

算法类型	同步通信	异步通信
最终一致性共识算法(具备拜占庭容错(私链/联盟链))	DBFT、PBFT、PoA、Ripple、Pool验证池	DAG
最终一致性共识算法(不具备拜占庭容错(公有链))	Paxos、Raft	DAG
强一致性共识算法	PoW、PoS、DPoS、Pol	DAG

DAG: 有向无环图 DPoS: 股份授权证明 PoA: 资产证明 PoS: 权益证明
 DBFT: 授权拜占庭容错 PBFT: 实用拜占庭容错 Pol: 重要性证明 PoW: 工作量证明

“挖矿”。挖矿难度的调整周期为2周,目的是使区块的生成时间稳定在10 min左右。PoW具有完全去中心化、节点可自由进出等优点,但挖矿行为造成大量的资源浪费,且共识周期较长,存在51%攻击,不适合商业应用。

(2) PoS。系统中具有最高权益的节点(如币龄最长)获得记账权。PoS的优点在于减少了PoW的资源消耗,缩短了共识时间,且恶意节点只有掌握超过全网1/3的资源,才能破坏整个共识过程;但共识过程需等待多个确认,容易产生分叉。

(3) DPoS。记账权由101位受托人轮流实现。其中,受托人由股东根据股份权益选出,且需保证99%以上的在线时间。DPoS机制大幅度缩减了验证和记账节点的数量,可以达到秒级验证;但其去中心化的程度不足,依赖于代币的特性限制了其应用

领域。

2 方案设计

考虑IoT中的2台设备Alice和Bob。区块链充当数据管理系统,IoT中所有的交易都记录上链。Alice和Bob通过以下方式实现密钥协商。

2.1 基于Diffie-Hellman的比特币密钥协商协议

如图3所示,协议的具体执行过

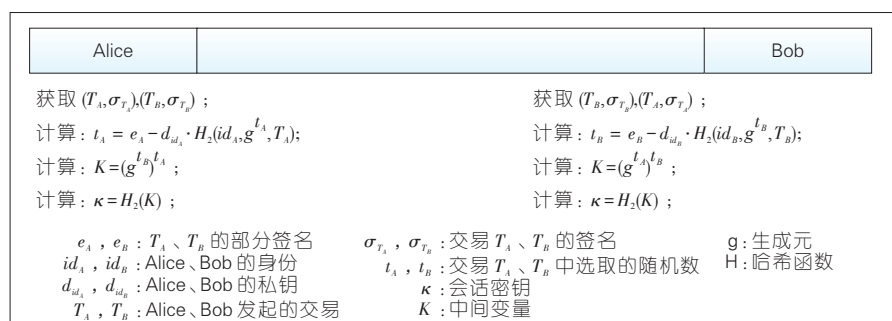
程如下:首先,Alice利用私钥 d_{id_A} 提取出与交易 T_A 相关的一次性随机数 t_A 。然后,Alice在链上获取Bob的交易签名对 (T_B, σ_{T_B}) ,并从 σ_{T_B} 中提取与公钥相关的 g^{t_B} 。Alice根据 t_A , g^{t_B} 计算会话密钥 κ 。同理,Bob计算一次性随机数 t_B ,从 σ_{T_A} 中提取 g^{t_A} ,进一步计算会话密钥 κ 。

本协议实现了IoT设备基于交易的密钥协商,任意2个设备节点只需从链上获取自身及对方的交易签名对,就能线下计算会话密钥 κ 。本协议中,与交易相关的随机数可直接利用私钥计算,避免了随机数存储的开销,克服了IoT设备资源受限的缺陷。

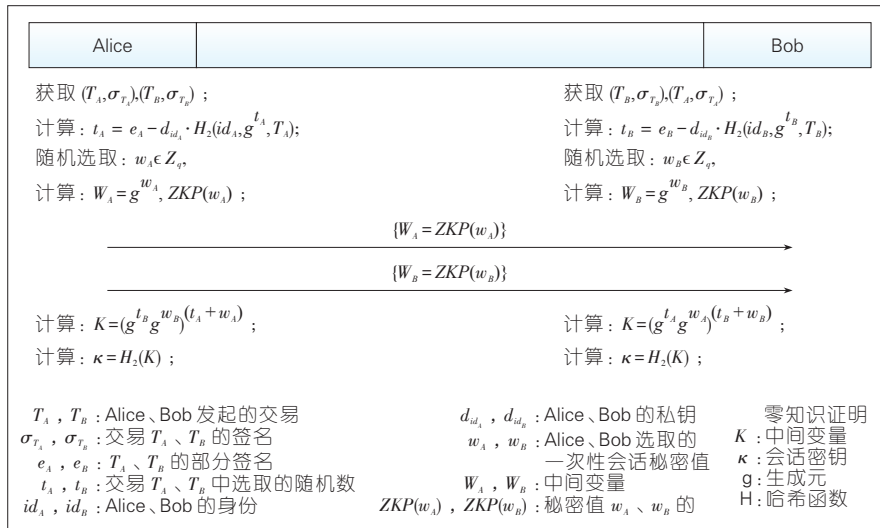
2.2 基于YAK的比特币密钥协商协议

如图4所示,协议的具体执行过程如下:首先,Alice(Bob)利用私钥 d_{id_A} (d_{id_B})提取出与交易 T_A (T_B)相关的一次性随机数 t_A (t_B)。然后,Alice(Bob)在链上获取Bob(Alice)的交易签名对 (T_B, σ_{T_B}) ((T_A, σ_{T_A}))。Alice(Bob)选取随机数 $w_A \in Z_q$ ($w_B \in Z_q$),计算 W_A (W_B)以及 w_A (w_B)的零知识证明 $ZKP(w_A)$ ($ZKP(w_B)$)并发送给对方。Alice(Bob)通过 $ZKP(w_B)$ ($ZKP(w_A)$)验证随机数 w_B (w_A)的真实性并计算会话密钥 κ 。

同2.1类似,本协议中节点可直接利用私钥计算与交易相关的随机数。不同的是:此协议是交互性的,双方进行密钥协商时需选取随机数 w_A 、 w_B 作为与会话相关的秘密值并做ZKP,对方通过ZKP验证随机数的真实性后方可计算 κ 。假设IoT节点



▲图3 基于Diffie-Hellman的比特币密钥交换协议



▲图4 基于 YAK 的比特币密钥交换协议

私钥的安全性被攻陷,敌手截获了交易后的某次会话。由于每次会话都重新选取随机数,则实现了后续会话的不可追踪,提供了前向安全性。

本文中我们采用了 Schnorr ZKP 方案^[10],假设 Alice 对秘密值 w_A 做了零知识证明 $ZKP(w_A)$,可通过如下方式使 Bob 相信自己拥有这一秘密而不向 Bob 泄露秘密 w_A 的任何信息。

(1) ZKP 产生 (ZKP-Gen)

1) Alice 随机选取 $l \in {}_R Z_q$, 计算 $L = g^l, h = H(g, L, w_A, id_A), r = l - w_A h$;

2) Alice \rightarrow Bob: $W_A, \{id_A, L, r\}$ 。

(2) ZKP 验证 (ZKP-Verify)

给定 $W_A, \{id_A, L, r\}$, Bob 相信 Alice 拥有秘密值 w_A 当且仅当式(2)成立:

$$Alice \text{ 拥有秘密值 } w_A \Leftrightarrow L = g^r (W_A)^h \quad (2)$$

同理, Alice 通过此方式验证 Bob 确实拥有秘密值 w_B 。

3 安全分析

对于密钥协商协议的安全,我们考虑以下3种安全特性。

(1) 私钥安全:一次性会话中秘密值的泄露不影响设备节点静态私钥的安全性。

(2) 前向安全:即使用户私钥被攻陷,已建立会话的会话密钥的安全性不受影响。

(3) 会话密钥安全:攻击者冒充用户,但无法访问用户的私钥,则无法计算会话密钥。

3.1 基于 Diffie-Hellman 的比特币密钥协商协议

假设 Alice 和 Bob 分别从链上获取了交易签名对 $(T_A, \sigma_{T_A}), (T_B, \sigma_{T_B})$, 我们证明所提协议可以提供私钥安全和会话密钥安全。

(1) 私钥安全的证明

假设存在一个概率多项式时间的被动敌手 A , 已掌握 Bob 的与交易相关的随机数 t_B 。若 A 获得了 Alice 的秘密值 w_A , A 可通过 $K = (g^{t_A})^{w_A}$ 计算得到会话密钥,然而 A 无法获得 d_{id_A} 的任何信息。

(2) 会话密钥安全证明

假设存在一个概率多项式时间的主动敌手 B , 冒充 Bob 与 Alice 进行通信。现假定 Alice 和 Bob 选取的与交易相关的随机数分别为 $t_A = \varphi, t_B = \phi$ 。给定一个计算型 Diffie-Hellman 问题 $(g^\varphi, g^\phi, g^{\varphi\phi})$, 假定敌手 B 能成功计算 K , 由 $K = (g^{t_A})^{t_B}$, 可得 $g^{\varphi\phi} = K$, 则困难问题计算型 Diffie-Hellman (CDH), 与实际矛盾。

3.2 基于 YAK 的比特币密钥协商协议

假设 Alice 和 Bob 分别从链上获

取了交易签名对 $(T_A, \sigma_{T_A}), (T_B, \sigma_{T_B})$ 。与 3.1 节不同,此协议会话密钥的产生依赖于与交易相关的随机数 (t_A, t_B) , 以及交互过程中选取的秘密值 (w_A, w_B) 。我们证明了此协议可以提供私钥安全、会话密钥安全以及前向安全。

(1) 私钥安全

证明如下:假设存在一个概率多项式时间的主动敌手 A , 已掌握 Bob 的与交易相关的随机数 t_B 以及 Bob 某一次会话选取的秘密值 w_B 。若 A 获得了 Alice 的秘密值 w_A , A 可通过 $K = (g^{t_A} g^{w_A})^{(t_B + w_B)}$ 计算会话密钥,然而 A 无法获得 d_{id_A} 的任何信息。

(2) 前向安全

证明如下:假设存在一个概率多项式时间的被动敌手 A , 已获取 Alice 和 Bob 的与交易相关的随机数 t_A 和 t_B 。现假定 Alice 和 Bob 交互过程中选取的随机数分别为 $w_A = \varphi, w_B = \phi$ 。给定一个计算型 Diffie-Hellman 问题 $(g^\varphi, g^\phi, g^{\varphi\phi})$, 假定敌手 A 能成功计算 K , 由 $K = (g^{t_A} g^{w_A})^{(t_B + w_B)} = g^{t_A t_B} g^{\varphi t_B} g^{t_A \phi} g^{\varphi \phi}$, 可得 $g^{\varphi\phi} = K / g^{t_A t_B} g^{\varphi t_B} g^{t_A \phi}$, 则困难问题 CDH 可解,与实际矛盾。

(3) 会话密钥安全

证明如下:假设存在一个概率多项式的主动敌手 B , 冒充 Bob 与 Alice 进行通信。 B 已获取 Alice 的与交易相关的随机数 t_A , 并从公开信道上截获了 W_B 。现假定 Alice 交互过程中选取的随机数为 $w_A = \varphi$, Bob 选取的与交易相关的随机数为 $t_B = \phi$ 。给定一个计算型 Diffie-Hellman 问题 $(g^\varphi, g^\phi, g^{\varphi\phi})$, 假定敌手 B 能成功计算 K , 由 $K = (g^{t_A} g^{w_A})^{(t_B + w_B)} = g^{t_A t_B} g^{\varphi t_B} g^{t_A \phi} g^{\varphi \phi}$, 可得 $g^{\varphi\phi} = K / g^{t_A t_B} g^{\varphi t_B} g^{t_A \phi} = K / g^{t_A \phi} (W_B)^{(t_A + \varphi)}$, 则困难问题 CDH 可解,与实际矛盾。故会话密钥不能被成功计算,此协议可以提供会话密钥安全。

4 性能分析

文章中,我们在 Ubuntu 平台搭建 regtest 测试链,基于 c++ 版本的比特

基于区块链的电子数据存证的设计与实现

Design and Implementation of Electronic Data Storage and Certificate System Based on Blockchain

冒小乐/MAO Xiaole¹
陈鼎洁/CHEN Dingjie²
孙国梓/SUN Guozi¹

(1. 南京邮电大学, 江苏 南京 210023;
2. 复旦大学, 上海 200433)
(1. Nanjing University of Posts and
Telecommunications, Nanjing 210023, China;
2. Fudan University, Shanghai 200433,
China)

区块链作为一项新兴科技, 运用了分布式存储、共识机制、点对点(P2P)网络、加密算法等技术, 它实质上是提供拜占庭容错以保证一致性的去中心化分布式数据库。与传统的数据库将读写数据库的权限完全交付给某个公司或管理员的 centralized 方式不同, 区块链以去中心化和去信任的方式允许全球范围内任何有能力的节点成为区块链网络的成员之一, 享受与其他所有节点同等的读写操作权利, 集体维护区块链的运行。最终, 区块链系统中的所有节点通过共识机制同步彼此的数据信息, 以保证在区块链网络中所有数据的一致性和可靠性。

电子数据是现代高科技的产物,

收稿日期: 2018-10-23

网络出版日期: 2018-11-24

基金项目: 国家自然科学基金(61502247)、数学工程与先进计算国家重点实验室开放基金课题(2017A10)、信息网络安全公安部重点实验室开放课题(C17611)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0028-007

摘要: 设计了一种基于区块链的电子数据存证系统, 该系统充分利用了区块链的去中心化、不可篡改性等特性, 将数据关键信息锚定在主链上, 同时控制了不同用户对电子数据的访问权限, 有效解决了电子数据存证存在的安全问题。为用户提供了数据上传、下载、查询、比对和授权等服务, 同时引入了分布式存储技术和用户积分机制, 增加系统的可靠性。

关键词: 区块链; 智能合约; 去中心化; 分布式存储; 电子数据

Abstract: An electronic data storage and certificate system is designed in this paper. This system makes full use of the decentralization and non-tampering of the blockchain. The key data information is anchored on the main chain, and the access rights of different users to electronic data are controlled. Thus, the security problems of existing mechanisms are resolved. The system provides users with data upload, download, query, comparison and authorization services. The distributed storage technology and user integration mechanism are introduced to increase the reliability of the system.

Keywords: blockchain; smart contract; decentralization; distributed storage; electronic data

它需要我们对它进行存储并且防篡改。电子数据具有易创建、易存储、易传输和高利用率等特点, 是可靠、有证明力度的电子数据证据。数据存证首先要对数据按类型进行很好的存储保存, 并且还要对数据的可信性、完整性有很好的保障, 并且还要方便对数据进行存储、共享、验证、分享等操作。区块链技术可以保障完善的安全加密性和用户验证。

目前电子存证还有几个问题需要解决: (1) 存证过程中自动化程度不高; (2) 存证过程中电子数据存证风险较大; (3) 第三方机构法律处理

流程繁琐; (4) 电子数据安全缺失; (5) 双方信任缺失。

在文章中, 我们提出了一个安全的、可扩展的电子数据存证系统, 该系统采用数据与用户对应映射关系查找来确保对电子数据池的高效访问控制。我们设计了一个基于区块链的数据存证方案, 允许数据用户/所有者在身份验证后, 从电子存储库访问电子数据。数据存储主要进行分片冗余算法和分布式存储保证数据安全性, 并且系统引入用户积分机制, 保证系统负载均衡。验证和后续服务封闭在系统内部, 写入区块并成

为区块链的一部分。

1 区块链研究的相关工作

1.1 区块链主要应用方向现状

XIA Q 在他们的研究中简要地解决了医疗数据共享系统中的访问控制管理问题,主要设计了一个基于区块链的数据共享方案^[1],允许数据用户/所有者在身份验证和加密密钥验证后,从共享存储库访问电子病历。SIFAH E B 等人也提出了基于区块链的共享医疗数据方案,重点在于提供数据访问控制、出处和审计的同时^[2],在云服务提供商之间共享医疗数据。SHAE Z 提出了一个用于临床试验和精密医学的区块链平台架构,并讨论了各种设计方面问题,并对技术要求和挑战提供了一些见解^[3]。

VO H T 等人研究了一个基于区块链的即付即用的汽车保险应用,系统透明地保存记录并根据运行时间条件执行智能合同,确保所有与用户有关的数据都被透明地记录下来^[4]。XU R 等人提出了一种基于区块链的网络媒体数字版权管理方案,该方案可以利用区块链的这些功能来实现网络媒体的有效生产管理、版权管理、交易管理和用户行为管理^[5]。

针对区块链访问控制的研究也有很多,例如:ZYSKIND G 等人提出当使用第三方移动服务时,需要解决隐私保护问题。与现有应用程序不同,平台只允许用户根据存储在区块链中的访问控制策略^[6]更改使用权限。HARDJONO T 更详细地描述了基于区块链的访问控制管理的系统,该系统为试图执行交易的实体提供匿名操作但可以进行身份验证,与前面系统相比,在用户匿名实体方面做出了更全面的考虑^[7]。

在安全、云存储等方面,业界也有进一步的考虑:LIANG X 等人提出了一种使用区块链技术的分散且可信的云数据起源架构。基于区块链的数据来源可以提供防篡改记录,实

现云中数据的透明度,增强原始数据的隐私性和可用性^[8]。TRAN A B 等人提出了一个基于浏览器的工具,用于用户注册的管理和部署,并调用区块链上的智能合约^[9]。

1.2 区块链存证方向现状

李兆森等人在基于区块链的电子数据存证应用研究中,从电子数据存储应用场景出发,研究如何将业务与区块链技术相结合,提出一种优化当前数据存储的方法,以此高效地为用户服务^[10]。李小良等人在网络犯罪中电子证据的收集及保全分析中探讨网络犯罪中电子证据的收集含义,分析电子证据收集在网络犯罪中的特殊性,提出收集和保存电子证据的方法^[11]。徐蕾等人在基于区块链的云取证系统中,采用区块链的分布式数据库特点——首尾相连的链式结构技术,设计了一中去中心化、可验证、不可篡改的系统^[12]。邓秀珍等人提出网贷平台电子数据保存的欠缺与对策,提出电子数据保存形式不规范、存证平台的中立性问题不明确、电子数据保存的具体数据技术不明确、存证方面的内容审核、存证服务的收费,以及存证服务的失效等一系列的问题^[13]。

电子数据的形式比较混乱,不能有效地统一数据格式,使数据存储的过程更加繁琐。电子数据存储中存在很大的数据安全隐患,中心化的存储方式可能会造成数据被篡改和遗失等风险,使得整个系统不完全可信。其次,电子数据在获得验证结果的等待时间较长,获得结果滞缓,使用户无法及时有效获得结果,不能及时给出相应信息,系统效率低下。我们致力于解决电子数据在目前遇到的各种问题,并研究了基于区块链技术来解决电子数据存证问题的现状。

2 区块链存证的架构设计及技术原理

本系统的设计采用浏览器/服务

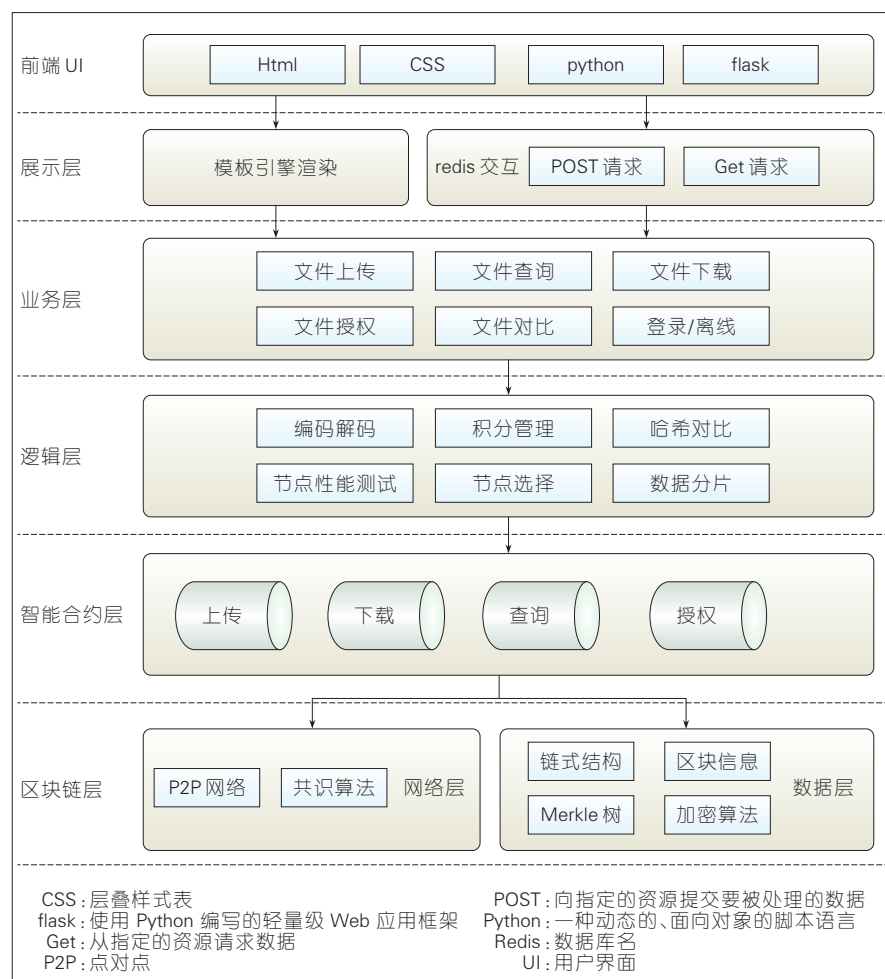
器(B/S)体系结构,分为4层,从上至下依次为:应用层、逻辑层、智能合约层和区块链层,如图1所示。

(1)应用层:主要包含图1中的前端用户界面(UI)、展示层和业务层。前端UI主要负责为用户访问系统提供可视化的Web界面。当获取用户提交的请求后,将用户请求信息发送给逻辑层进行核心计算;等待后台数据处理完毕后,再将用户信息通过Web界面直观地反馈给用户。用户既可以是需要保全数据的客户,也可以是需要下载数据进行公证的第三方机构。

(2)逻辑层:系统核心功能的实现层。根据应用层为用户提供的六大功能界面,逻辑层需要分别给出对应模块的实现方法。其中,基于传输控制协议(TCP)的Socket多线程并发模块是整个逻辑层能够顺利运行的框架基础,系统利用该模块实现多节点之间数据的可靠传输。进一步地,运用里所码的编码解码方式对电子数据进行分片处理,引入用户节点性能测试模块,对节点性能进行排序,用于数据的上传和下载功能模块;引入Hash比对模块检测文件数据是否保存完整;引入用户积分模块,保障系统的负载均衡;引入用户注册、登录功能记录用户信息,方便对用户进行管理。

(3)智能合约层:部署在以太坊上,并与系统进行交互。智能合约层主要负责将逻辑层的数据处理结果(如电子数据及其分片的指纹信息、用户节点的积分信息等)锚定到区块链层的存储区内。系统智能合约主要由若干的结构体组成(如文件、纪录、用户等),并以此结构方式存储电子数据的关键信息。该方法显著地提高了系统查询电子数据的效率,增强了系统的运行速率。

(4)区块链层:系统的去中心化数据库,存储系统交互产生的数据信息。其中,网络层承担信息通信,产生新区块,维护区块链网络稳定运



▲ 图1 系统功能架构图

行;数据层保存着整个系统所有上传下载的关键信息。

借助区块链的新兴技术,把电子数据记录分布式存储在区块链上,并结合 Reed-solomon 码、时间戳、哈希算法、模糊层次分析法、理想优基点、客户关系管理(RFM)积分模型和智能合约等技术,我们设计并搭建了基于区块链的分布式存储系统。系统主要对数据进行冗余分片,根据用户需求,将数据分成 n 个信息片和 m 个冗余片,再将数据分片进行分布式存储。对系统存储主机信息进行采集,结合模糊层次分析法和理想优基点,计算出系统存储主机的网络综合性评分,保证系统数据存储的负载均衡。并根据智能合约去中心化的特点,使用哈希算法进行数据的完整性

验证,使用共识算法保障计算节点间数据的一致性。我们设计了一种去中心化的、可验证的分布式存储系统。基于该系统提供的功能,用户可以是双边或多边,等公检法第三方机构共同参与下,自动实现电子数据存证的事务处理和存证机制等。

2.1 区块链技术

区块链是所有节点共享的交易数据库,这些节点基于交易协议参与到网络中来。区块链包含每一个曾在系统中执行过的交易,根据这些交易信息,人们可以找到任何时候、任一地址的信息。如果把区块链作为一个状态机,则每次交易就是试图改变一次状态,而每次共识生成的区块,就是参与者对于区块中交易导致

状态改变的结果进行确认的结果。

在实现上,首先假设存在一个分布式的数据记录账本,这个账本只允许添加,不允许删除。账本底层的基本结构是一个线性的链表,这也是其名字“区块链”的来源。链表由一个个“区块”串联组成,后继区块记录前导区块的哈希值。新的数据要加入,必须放到一个新的区块中,而这个块(以及块里的交易)是否合法,可以通过计算哈希值的方式快速检验出来。任意维护节点都可以提议一个新的合法区块,然而必须经过一定的共识机制来对最终选择的区块达成一致。

2.2 智能合约

智能合约是以太坊中最为重要的一个概念,即以计算机程序的方式来缔结和运行各种合约。在20世纪90年代,SZABO N等人就提出过类似的概念^[1],但一直因为缺乏可靠执行智能合约的环境,而被当作一种设计理论。区块链技术的出现,恰好补充了缺陷。

文章中,我们在智能合约的编写过程中,定义了文件、纪录、成员和用户4个结构体变量,分别存储电子数据文件的关键信息、电子数据文件分片的关键信息、用户资料和电子数据文件的所有关系。基于上述4个变量,我们依次编写了电子数据信息的上传、电子数据信息的查询、电子数据的授权、用户信息的更新和用户信息的查询。考虑到以太坊数据写入的速度较慢,容易影响用户体验,因此采用异步请求方式(sendAsync)执行事务,以此来加快电子数据的查询传输速率。

2.3 密码学

哈希函数是密码学的一个重要分支,它是一种将任意长度的输入变换为固定长度的输出且不可逆的单向密码体制。哈希函数主要运用于数字签名和消息完整性验证。

本文中我们采用哈希算法,主要的过程为:发送方采用单向哈希函数对消息进行计算,得到摘要并发送消息和摘要。接收方将接收到的消息,按同样方式进行哈希函数计算,并将新得出的结果与发送方的原摘要结果进行比对。如结果一致,说明消息完整。在本系统中,摘要信息的不可变,保证了需要存证信息的完整性和真实性。将需要存证的电子数据放在区块链中,避免数据被恶意篡改。

2.4 Reed-solomon 码

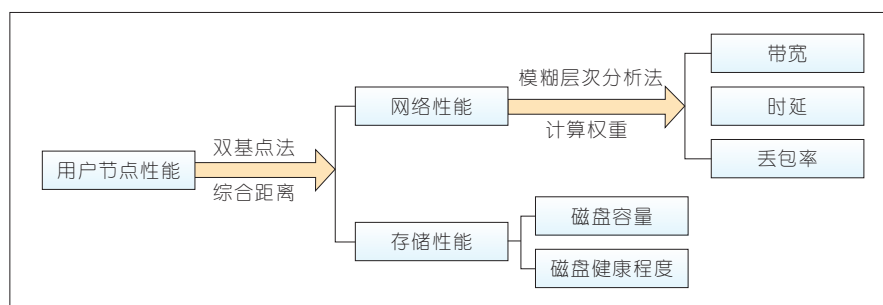
Reed-Solomon 码是一种定义在域上的线性编码方法,该编码方法将 k 个源数据变换生成 l 个编码数据。与前向纠错码(FEC)编码思想一致,我们采用 Reed-Solomon 码来实现数据包层的 FEC 编码变换^[15]。

当用户上传电子数据时,系统首先会对电子数据进行分片处理。分片工作主要依赖里所码的编码实现。用户需要提供2个重要参数:信息分片数目和冗余分片数目。系统根据上述2个参数和待上传文件的大小,调整出恰当的编码缓冲区大小,完成对文件的分片处理。

2.5 多目标节点决策模型

作为一个电子数据存证系统,本系统依赖于多个用户节点共同完成电子数据的存证保管工作,这一过程涉及到对多用户节点的选择。文章中,我们设计了如何挑选出系统当前性能最优的若干节点并协同完成分布式的存储工作。图2展示了用户节点性能评估的主要设计过程。

对比以太坊依靠各节点的计算力使之持续运转,本系统主要依靠各节点的存储算力。因此,决定对用户节点的性能评估从网络性能和存储水平2方面展开。其中,网络性能的高低影响电子数据分片的传输速度,存储水平的高低影响电子数据分片的存储可靠性。网络性能的参数比重通过模糊层次分析法(FAHP)计算



▲ 图2 用户节点性能评估框架

出。然后通过双基点法(TOPSIS)计算各优基点与理想/反理想优基点的欧氏距离,得出综合距离并进行节点顺序排名。

3 区块链存证的系统工作步骤

我们制定了数据共享机制,以确保数据的安全性和出处。存证系统的详细流程如图3所示,主要分为6个步骤。

(1)用户登录本系统后,该用户节点首先向系统各节点广播本节点性能文件,系统合约成员类获取用户信息,并通过用户节点获取到其他用户节点的性能信息,为后面的数据分片存储获取性能主机的值。

(2)用户上传需要存证的文件,将文件的关键信息写入到合约文件类中去,以此建立用户和数据的对应映射关系。

(3)系统利用冗余分片算法对上传的电子数据进行分片,然后根据前面获取的节点性能信息选取若干最优性能的节点,用于存储系统的分片数据。

(4)系统根据性能评分排序选中的节点,对不同的节点进行数据分发,并将分发的信息返回给智能合约,包括数据分片存储的IP地址、分片存储的绝对路径和数据分片的哈希值等。

(5)当用户需要对电子数据进行下载或查询访问操作时,系统根据用户请求、用户授权请求,将用户信息与需要访问的数据建立对应的映射

关系,然后用户便可以进行操作。

(6)系统从合约中读取到电子数据的相关存储信息,通过存储信息获得电子数据存储的位置,并下载电子数据分片,还原数据并比对文件哈希值,以验证电子数据的完整性。

基于区块链智能合约的存证系统的主要任务是对电子证据进行上传、保全、查询、比对和下载。本系统基于去中心化设计,不再需要系统管理人员,转而使用智能合约进行数据交互。系统主要功能有4个特性:安全性、完整性、机密性和可授权性。

(1)系统的安全性。使用基于Reed-Solomon的编码方式进行分布式存储,在节点主机被攻击、磁盘损坏等分片被丢失的情况下仍然可以还原文件,同时分布式还可以降低中心化服务器被内部篡改的风险。

(2)系统的完整性。使用哈希算法SHA-256对文件进行完整性校验,并把校验存储于区块链智能合约中。

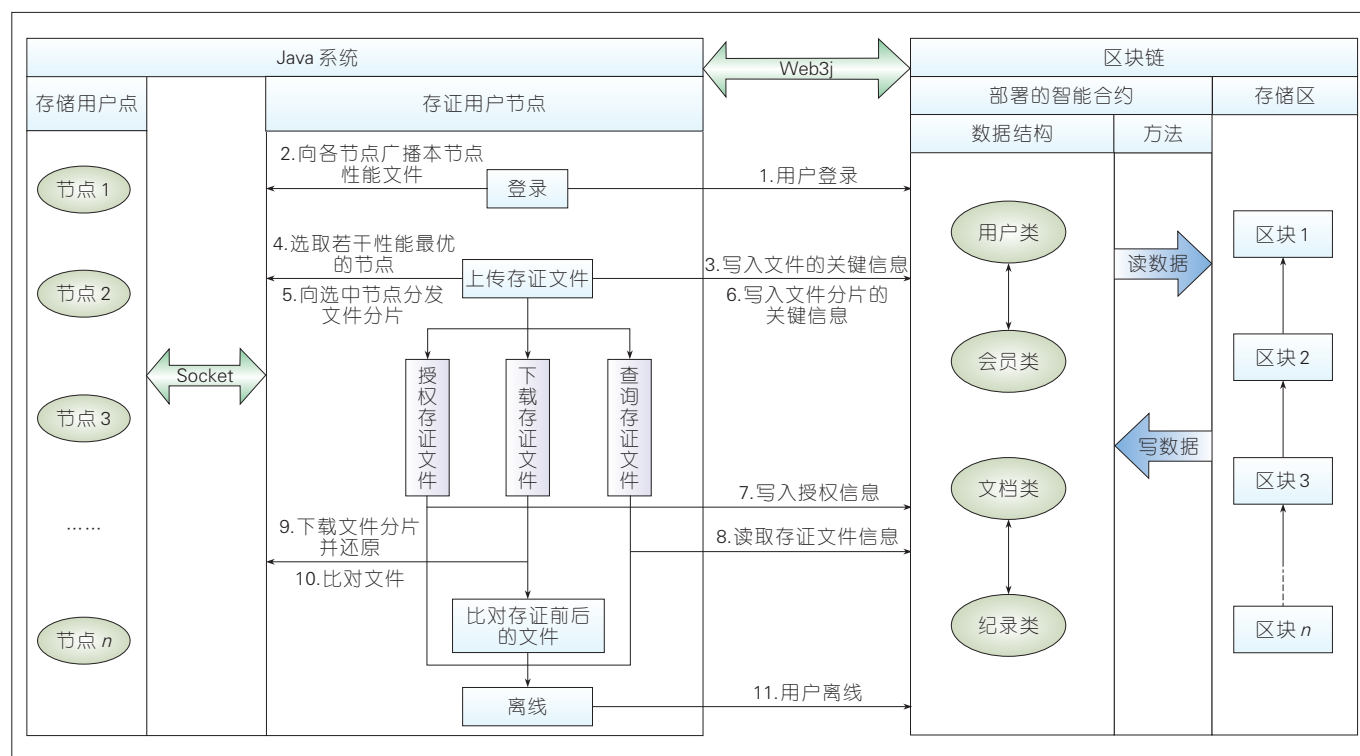
(3)系统的机密性。去中心化分布式存储,可以保证任一单一存储节点无法得到完整文件信息,更不可能还原信息,这可防止存储主机被黑或者内部人员泄露信息。

(4)系统的可授权性。用户上传保存的文件除了由用户自己访问之外,还可以由被用户授权的第三方来访问。

系统主要的六大模块功能,将在以下的小节中详细介绍。

3.1 系统数据保全功能

系统先根据用户分片需求计算



▲ 图3 系统详细流程图

出本次保全用户所需花费的积分,然后获取区块链中用户对对应积分值进行积分数值更新。当用户积分值 c 大于上传操作花费 m 时,系统才提供上传功能。若是积分值 c 小于 m 时,系统会提醒用户积分不足,无法进行上传操作,如图4所示。

3.2 系统上传功能

用户首先在本系统注册,提交完注册信息后就拥有注册用户初试积分,同时用户所在主机会在对系统内的主机发送请求,提出电子数据上传操作,并获取到系统其他主机的性能,计算出系统所有主机性能评分情况。然后系统会根据用户设定的电子数据分片数目,将数据进行分片并将其进行存储分发,同时将文件分片信息写入到区块链中,并更新用户在区块链上对应的积分数值,具体如图5所示。

3.3 系统数据查询功能

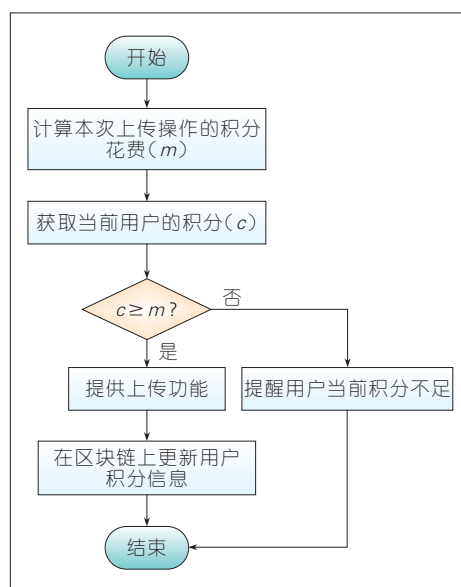
在本系统中,用户可以即时查询

获取文件的电子数据。根据电子数据用户隐私需求,电子数据仅该用户自己可见(在默认情况)。当用户需要查看其他用户的电子数据时,先给出需要查看文件的序号,系统根据文件序号查询区块链上文件序号对应用户的用户名。当文件属于查看用

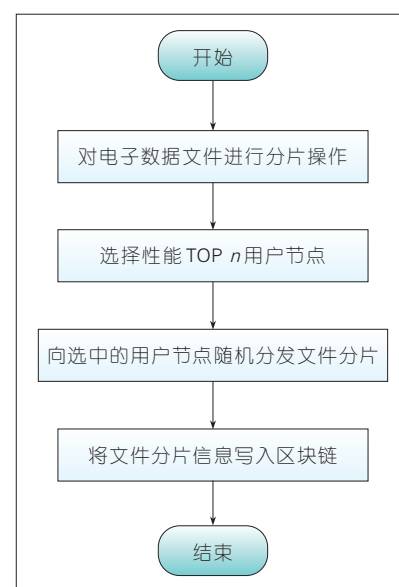
户的用户名时,则可以查看用户数据;如果文件不属于该用户名类,则文件不能被查看,具体如图6所示。

3.4 系统数据下载功能

当用户下载文件时,系统先判断用户是否拥有该文件的访问权限,如



▲ 图4 系统保全流程图



▲ 图5 系统上传流程图

果拥有权限,系统从区块链合约中读取该文件的分片信息,根据分片信息获取分片存储主机地址和路径,然后下载数据分片并重新组合数据。这与上一步的电子数据查询功能类似,用户下载的数据文件必须获得相应的授权,以此保证用户的隐私安全,具体如图7所示。

3.5 系统数据比对功能

系统在获得数据分片后,对分片进行哈希计算,得到每个分片的哈希值后,与之前原数据存储在智能合约中的哈希值进行比对、验证。如果哈希值相同,则系统返回数据未被改动;反之,则提醒用户数据已经被篡改。另外,考虑到分布式存储的容错

性,如果出现部分分片丢失,只要丢失的分片数量小于系统数据冗余分片数量,系统仍然能够还原数据源文件,具体如图8所示。

3.6 系统数据授权功能

考虑到系统的功能需求,我们要对用户的个人隐私进行保护,所以系统默认用户的电子数据是用户个人所拥有,他人在没授权情况下无法查看。用户可以授权给他人,被授权用户可以查看被授权的文件和电子数据。授权主要将授权用户的公钥输入系统与待授权文件建立映射关系,并写入区块链,则完成授权,具体如图9所示。

4 系统功能测试与评估

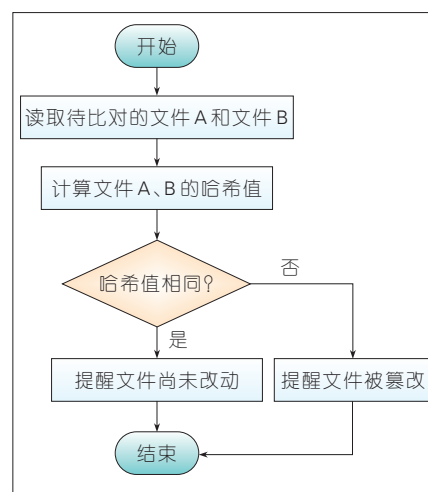
我们提出的区块链存证系统拥有以下功能。

(1)系统为存储应用程序中的所有数据访问提供实时审核。我们使用电子数据文件作为数据单元,对数据对象的所有操作进行审计,并使用区块链进行记录。通过这种方式,可以收集和监测控制所有电子数据访问情况。

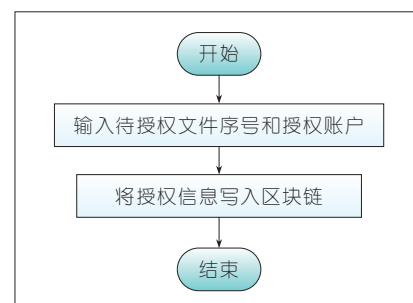
(2)系统为文件安全纪录保存提供防篡改时间戳。对于每条电子数据,我们都会将数据上传到区块链网络,我们创建了不可改变的文件数据指纹,并且通过验证区块链数据对比来检测对系统数据的任何更改。

(3)系统为用户数据提供隐私保护。用户访问记录在区块链网络中是匿名的。数据源是无法查询到用户账户。匿名保存体现在2个方面:一方面,由于用户ID被散列随机,所以用户身份不会和源数据连接到一起;另一方面,也实现了每个用户之间的不可连接性,尤其是对于被授权数据的上传用户保护。

文章中,我们对基于区块链的电子数据存证系统进行功能测试,分析该系统功能的可用性、界面的合理性和数据交互的正确性等。



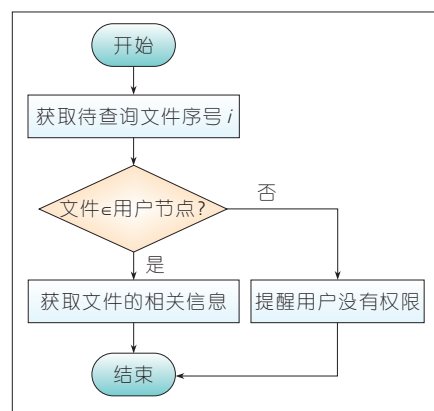
▲ 图8 系统比对流程图



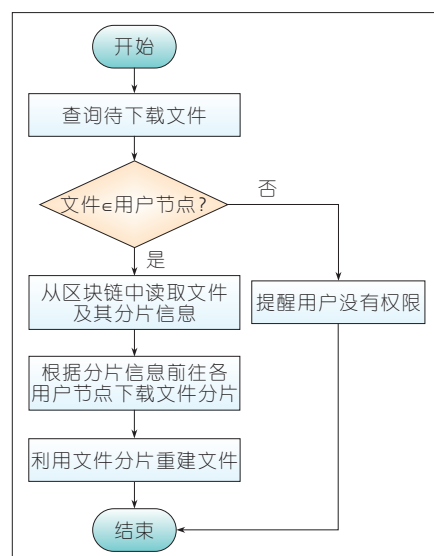
▲ 图9 系统授权流程图

为了验证该系统可使用性和扩展性,实验模拟了系统在局域网下的数据分布式存证。测试环境为:在局域网内,部署了4台linux服务器,同时运行服务端程序,与客户端进行数据同步交互。

针对以上系统实验,我们进行了压力测试。在验证时,我们设置相同的区块生成时间,然后分别选取不同的时段进行数据验证。我们共选取了50组不同大小的电子数据文件(文件大小从23 kB到3 900 kB不等),并依次将文件按照系统提供功能进行验证,然后记录并对比系统完成一次流程的时长,另外操作的数据类型也不同,以此获得更多数据的评估时间。另外,我们专注于为每个起源数据请求区块链存证的效率。通过计算可得出:每次运行操作1条记录,平均每条数据大小为1 054.7 kB,平均耗时间为4~7 s。对于每次



▲ 图6 系统查询流程图



▲ 图7 系统下载流程图

不同数据的操作,都会记录不同文件操作的所花费的平均时间,并最后计算获得结果如表1。

▼表1 实验结果评估表

操作类型	文件平均大小/kB	平均消耗时间/s	数据验证率/%
文件上传	1 054.7	7.3	100
文件查看	1 054.7	5.8	100
文件下载	1 054.7	4.4	100
文件对比	1 054.7	4.7	100

表1显示:系统对数据检索的速率一般,数据验证对比结果正确率达到百分百,也就是说系统可以完整地数据存证。

5 结束语

本文的主要贡献如下:

(1)提出了一种将电子数据存证与区块链技术相结合的系统,电子数据的存证用于对各类数据的存储和验证,区块链技术用于对获取到的电子数据进行固定保存。

(2)应用了电子数据的分布式存储方式,对数据进行冗余分片,保证了数据的存储安全性。并在系统中引入积分制度,按照用户上传存证和提供存储方式进行积分的数据变化,维持系统的负载均衡,保证了系统的安全性和稳定性。

借助区块链这一全新技术,我们将电子数据的“数字指纹”存储在区块链上,并利用智能合约、分布式存储、容错编码、多属性决策等技术,设计并实现了基于区块链的电子数据存证系统。系统基于区块链的去中心化和不可篡改的属性,保证了电子数据的真实性、完整性和唯一性。此外,本系统针对用户还制订了积分制度,以保证系统能吸引更多用户,从而提高本存证系统的可靠性。

我们还开发了一个简易的基于区块链的电子数据存证系统,该系统主要是在局域网内进行主机分布式存储,未来还需要进一步优化,实现可以广域网内进行分布式存储。另

外,我们认为区块链所使用的共识机制是PoW,此机制时间周期较长,资源需求过高,可以进行优化。我们所

提的系统客户端与服务器端通信过程中,采用的是明文通信方式,存在安全隐患,后面可以使用对称加密来完善安全性。

致谢

本文的工作得到了南京邮电大学李华康老师的指导和帮助,雷鹏同学承担了部分试验工作,谨致谢意!

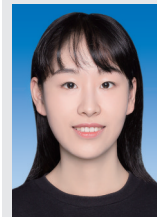
参考文献

- [1] QI X, EMMANUEL B S, ABLA S, et al. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments [J]. Information, 2017, 8(2):44. DOI: 10.3390/info8020044
- [2] XIA Q, SIFH E B, ASAMOAH K O, et al. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain [J]. IEEE Access, 2017, (5): 14757-14767. DOI:10.1109/access.2017.2730843
- [3] ZOYIN S, JEFFREY N. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine[C]//2017 IEEE 37th International Conference on Distributed Computing Systems. USA: IEEE, 2017:1063-6927. DOI: 10.1109/ICDCS.2017.61
- [4] XIA Q, HOANG T V E, LENIN M, et al. Blockchain-Based Data Management and Analytics for Micro-Insurance Applications [C]// CIKM '17 Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. USA: ACM, 2017: 2539-2542. DOI: 10.1145/3132847.3133172
- [5] XU R Z, ZHANG L, ZHAO H, et al. Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology[C]//2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS). USA: IEEE, 2017. DOI: 10.1109/ISADS.2017.21
- [6] ZYSKIND G, NATHAN O, PENTLAND A S. Decentralizing Privacy: Using Blockchain to Protect Personal Data[C]//Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW 2015). USA: IEEE, 2015: 180-184. DOI: 10.1109/SPW.2015.27
- [7] HARDJONO T, SMITH N. Cloud-Based Commissioning of Constrained Devices Using Permissioned Blockchains [C]// Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security - IoTPTS '16, 2016.USA:ASM,2016. DOI:10.1145/2899007.2899012
- [8] LIANG X P, SHETTY S, TOSH D, et al. ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability[C]//2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). USA:IEEE, 2017: 468-477. DOI:10.1109/CCGRID.2017.8
- [9] AN B T, XU X W, WEBER I, et al. Regeator: a Registry Generator for Blockchain[C]// CAiSE 2017 Forum and Doctoral Consortium Papers. Germany: CAiSE, 2017: 81-88
- [10] 李兆森, 李彩虹. 基于区块链的电子数据存证应用研究[J]. 软件, 2017, 38(8): 63-67
- [11] 李小良. 网络犯罪中电子证据的收集及保全分析[J]. 法制与社会, 2016, (32): 258-259. DOI:10.19387/j.cnki.1009-0592.2016.11.270
- [12] 徐蕾. 基于区块链的云取证系统[D]. 四川:西南科技大学,2017
- [13] 邓秀珍, 周恒. 网贷平台电子证据保存的欠缺与对策[J]. 金融电子化, 2016(10): 30-31
- [14] 王春宇, 张守坤. 智能合约与金融合约[J]. 商, 2016(6):198
- [15] 黄宏博, 肖峻岭, 佟刚. 基于 Reed-Solomon 算法的 QR 码纠错编码[J]. 计算机工程, 2003, 29(1): 102-104

作者简介



冒小乐, 南京邮电大学在读硕士研究生; 主要研究方向为区块链相关技术。



陈鼎洁, 复旦大学在读硕士研究生; 主要研究方向为区块链相关技术。



孙国梓, 南京邮电大学教授; 主要研究方向为电子数据取证、区块链技术; 先后主持和参加基金项目10余项, 获得3项科研成果奖; 已发表论文100余篇, 被SCI/EI检索60余篇。

区块链技术在物联网中的身份认证研究

Blockchain Technology for Identity Authentication in Internet of Things

杨惠杰/YANG Huijie
周天祺/ZHOU Tianqi
桂梓原/GUI Ziyuan

(南京信息工程大学, 江苏 南京 210044)
(Nanjing University of Information Science & Technology, Nanjing 210044, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0035-006

摘要: 基于物联网(IoT)平台的特点,将区块链技术与体域网相结合,提出了应用于体域网身份认证的区块链系统框架,实现用户和传感器、路由器、多服务器间的身份认证,并分析了该框架的安全性。最后,基于研究结果,探讨了在IoT平台中区块链技术可能存在的问题和未来发展方向。

关键词: 区块链技术; 体域网; 认证; 非对称加密算法; 共识机制

Abstract: Based on the characteristics of the Internet of things (IoT) platform, a blockchain system framework applied to the identity authentication of the body area network is proposed, which combines blockchain technology with body area network. This framework realizes the identity authentication between users and sensors, routers and multi servers. Then the feasibility and security of the framework are analyzed. Finally, based on the research results, the possible problems and future development directions of blockchain technology in the IoT platform are discussed.

Keywords: blockchain technology; body area network; authentication; asymmetric encryption algorithm; consensus mechanism

近年来,随着新一轮经济科技的不断发展,物联网(IoT)平台已被世界发达国家列为重大发展战略。中国也在《“十三五”规划纲要》里明确指出:将物联网作为战略性新兴产业上升为国家发展重点^[1]。现如今IoT技术被广泛应用在智能城市、智能家居、智能医疗、车联网、环境监测等实际应用环境中,人们的实际生产生活已经与物联网技术紧密相连,不可分割^[2-5]。为实现实时感知环境信息或传输数据给用户,开发人员会将不同种类的传感器嵌入到智能设备或具体物体中,例如:可穿戴设备、传感器和专业工具等智能设备在网络中相互连通,并在网络中完成数据加密、数据传输和数据分析等,协助人们完成IoT平台数据采集和数据分析等工作^[6-8]。在上述过程中,无论哪种实际应用场景都需要智能设备能够及时完成对数据的响应或传输,即

使数据是在公开信道中传输,也要保证数据传输是不可泄漏的。一旦数据传输速度降低或者数据丢失,将会影响用户的使用效果;一旦数据在传输过程中被恶意对手篡改或攻击,整个处理数据的过程都会被视为不安全。因此,提高在IoT平台下的数据传输性能和数据安全性,是当前亟待解决的问题。

经过上述的分析,不难发现:传统的IoT技术和中心化的系统框架已经很难满足未来的发展需求。针对IoT平台的特点,区块链技术能解决大量的智能设备数据在中心化的系统框架中会出现的安全和管理问题。区块链是一种集成分布式数据库、共识机制、点对点(P2P)传输和非对称加密算法等新型应用模式,具有去中心化、开放性、自治性、匿名性和信息不可篡改的特点。本文主要

对IoT平台之一的体域网展开了详细研究,结合新兴的区块链技术,针对传输的安全性能和数据传输性能差的特点,研究分析了适用于体域网的身份认证技术,利用区块链技术在体域网平台下设计一个新兴的系统框架,主要解决以下问题:

(1)数据的安全问题。由于体域网处于一个公共信道中,因此存在恶意对手对数据进行攻击、篡改或重放等,造成数据丢失或被窃取的安全性问题。在体域网中,数据一旦受到篡改,则可能酿成医疗事故。

(2)数据的传输问题。在不同网络中传输数据时,需要使用不同的通信协议,导致不同协议之间需要相互转换格式,产生了大量的通信开销,并降低了通信效率。

(3)设备的成本问题。在体域网中需要使用大量的传感器和路由器,

收稿日期: 2018-10-23

网络出版日期: 2018-11-27

基金项目: 国家自然科学基金(61672295, 61672290, 61772280)、国家信息安全重点实验室(2017-MS-10)、桂林密码学和信息安全重点实验室(GCIS201715)、江苏省研究生科研与实践创新计划项目(KYCX18_1017, KYCX18_1039)

保证数据的采集和传输。在无形中,增加了通信的成本和能源消耗。

1 体域网身份认证现状

无线体域网中收集的都是与人体相关的生理隐私数据,这些数据可被用于医疗、体育、军事和商务社交等方面,并产生各种社会价值。为了保护这些与个人隐私相关的生理数据,首先要进行各个实体间的身份认证,许多研究学者对此展开了研究。这些研究成果大体上可以分为2类:一种是采用人体独特的生物信息进行认证,另一种是利用传统的密码学方式进行认证。

在2003年,CHERUKURI S等人^[9]首次利用人体的生物特征信息进行身份认证研究,并提出了可行的Biosec方案。在该方案中,结合纠错码技术以及生物识别技术解决生物特征测量误差和随机性问题,可用于安全通信无线生物传感网络的身份认证。但是其中的生物特征测量方法并不完善,存在缺陷。随后,文献[10-12]对模糊金库算法进行研究并应用于节点间身份认证。模糊金库算法主要利用人体独特的生物特征数据构造一个数据集合,并在数据集合中加入大量的噪声点,用处理后的数据集合对密钥信息进行加密,然后将此加密后的数据用来进行身份认证。如果其他节点想进行解密操作,其自身得拥有与密文中的生物特征数据集合相似的数据集合。但是在模糊金库算法中,网络中通信开销消耗和金库大小有关联,这会导致节点能耗过大的问题。针对此问题,ZAGHOUANI E K等人^[13]于2015年利用线性预测编码技术解决了上述能耗过大的问题,并提出了心电图结果线性预测密钥(ELPA)方案。在此基础上,ZAGHOUANI E K等人^[14]于2017年将线性预测编码技术与心电图生物识别技术相结合,可在隐藏心电信号隐私数据的同时实现对病人身份的认证。同模糊金库算法相比,该降

低了计算复杂性和通信开销。

LAMPOR L^[15]于1981年提出了首个远程认证协议,采用了用户密码认证方案,这一方案为今后的远程认证方案奠定了基础。该协议允许节点通过不安全公共信道向服务器进行身份认证。此后也有许多远程认证协议被提出,这些协议都利用了传统密码学方式,需要证书授权中心和公钥基础设施的参与,不适合资源受限的传感器设备。LIU J等人^[16,17]对无证书公钥密码进行研究并在无线体域网中首次提出了2个保护隐私的无证书远程匿名认证协议。由于协议中服务器端需要存储认证表来进行身份认证操作,易被篡改和伪造,同时也不满足前向安全性等要求。同时由于使用了双线性对等密码学操作,传感器的计算负担较大,不适合资源受限的客户端。XIONG H^[18]则于2014年提出了一种基于无证书加密的远程匿名认证协议,该协议在客户端使用较多的点乘操作并且没有考虑到密钥的撤销问题,同时用户的个人生理数据易被恶意实体收集,因此存在较大的安全问题和计算负担。为了提高无线体域网中认证的安全性并降低计算的成本,SHEN等人^[19]于2018年针对无线体域网提出了一种综合认证协议,该协议包括了一种高效的多层认证协议和针对无线体域网的安全会话密钥生成方案。该协议借助个人数字助理和无证书认证技术,可以有效地降低传感器能耗和计算负担,具有一定的实践指导意义。

综上所述,在无线体域网中,全球学者对于身份认证的研究已取得一定的成果,可实现匿名、安全和高效的认证,并在实践中得到应用。采用传统密码学方式进行身份认证虽然可以避开生物信息认证的缺陷,但其本身也存在计算开销较大、传输速度慢、易受共谋攻击和中间人攻击等问题,同时数据易受篡改,对资源受限的传感器节点来说仍然是不小的

挑战。

2 区块链概述

区块链技术是使用块式和链式的存储结构来认证和保存数据,使用共识算法实现生成新区块,使用非对称加密算法保证数据在信道中的安全传输,使用智能合约来处理数据的新分布式技术。区块链分为私有链、联盟链和公有链。从本质上讲,区块链就是一个去中心化的分布式数据库,任何用户都可以参与到区块链中。用户周围的路由器设备就是一个节点,每个节点都拥有一整套数据的备份,并且各个节点间使用相同的共识机制,通过竞争计算来生成或更新区块链。基于区块链结果的特点,如果任何一个节点失败,其他节点仍能进行正常的工作,且能分辨出是哪一个节点失败。因此,区块链技术解决了传统平台易受攻击或篡改的缺陷。

2.1 区块链的基础架构

区块链的基础架构主要分为应用层、合约层、激励层、共识层、网络层和数据层,具体的基础架构如图1所示。

数据层主要封装了区块链的物理结构,该结构中包含诸如哈希函数、时间戳等技术,保证信息的不可篡改性;网络层描述了组网方式、验证机制和传播机制,实现区块链网络节点间的信息交流;共识层选择一种共识记住,用以验证区块的正确性;激励层主要借助设计一些激励策略,保证节点在区块链中参与验证工作,确保共识的稳定;合约层中主要包含各种脚本、算法和智能合约,当其满足触发条件的时候,系统自动执行合约中的命令;应用层为封装的有关区块链应用提供了接口,例如基于区块链的跨境支付平台OKLINK。

2.2 区块链的关键技术

在本节中,我们主要从区块结



图1
区块链技术的基础架构

构、非对称加密算法、分布式结构和智能合约4个部分进行阐述。

(1) 区块结构

区块链是由2个部分组成:区块和链式,该结构能有效防止恶意用户对数据进行篡改,并能验证新生成区块的合法性。区块链中的网络节点就是区块,每个区块均由2个部分组成:区块头和区块体。

(2) 分布式结构

区块链的分布式结构不再让数据集中在服务器上,而是使数据能够分散地存储在不同的节点上。当节点想要写入数据时,需半数以上其余节点通过共识机制确认该节点的身份,才能够将数据写入到节点中。分布式结构能够有效地增强系统的健壮性,即单一节点的失效不会影响整个系统。

(3) 智能合约

在智能合约中封装了预先设定的响应条件、触发条件等内容。各个节点就所签署的合约达成一致后将合约内容以代码的形式嵌入区块链中。一旦有满足合约中相应条件或者触发条件时,自动激活并且执行智

能合约。

3 适用于体域网平台的区块链身份认证应用设计

由于区块链技术具有去中心化、透明性、高效率和不具名性的特点,因此该技术可以广泛应用到数字货币、征信管理、金融市场、资产管理等相关场景。同时,区块链和IoT均有着去中心化和分布式的特点,有学者提出将区块链技术应用到IoT平台中,用以解决IoT中安全性差和低效率的问题。体域网作为IoT的一部分,可将区块链技术与体域网结合展开研究。目前中国尚无该方向的研究,本文中我们对区块链应用到体域网中进行身份认证展开研究和分析。

智能医疗利用先进的体域网技术,实现患者与医务设备、医疗人员和医疗机构之间的信息沟通,进而达到信息化的效果。智能医疗能够良好地结合区块链技术,实现数据在体域网中安全和高效的传输。

3.1 系统架构设计

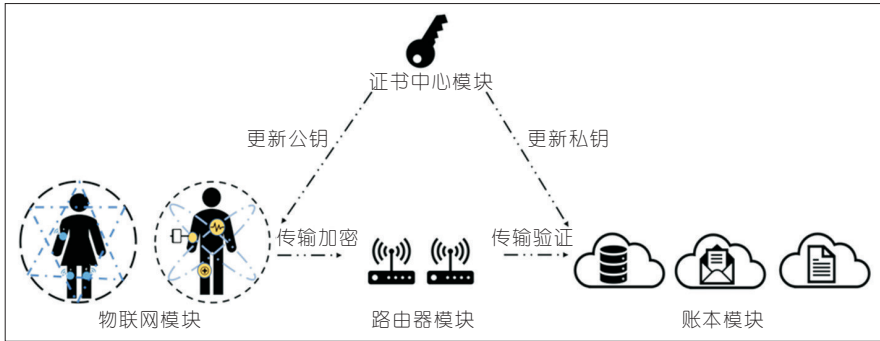
本文中我们设计的适用于体域

网平台的区块链身份认证系统框架,将传感器、路由器和可信中心构成一个区块网络,如图2所示。由于传感器的资源受限,无法进行数据的计算工作,因此传感器只参与数据的简单加密和传输。然后把数据作为数据交易块发送给路由器,路由器使用验证机制对接受到的数据进行验证。最后,将数据发送给可信中心,可信中心根据共识机制将数据记入帐本。

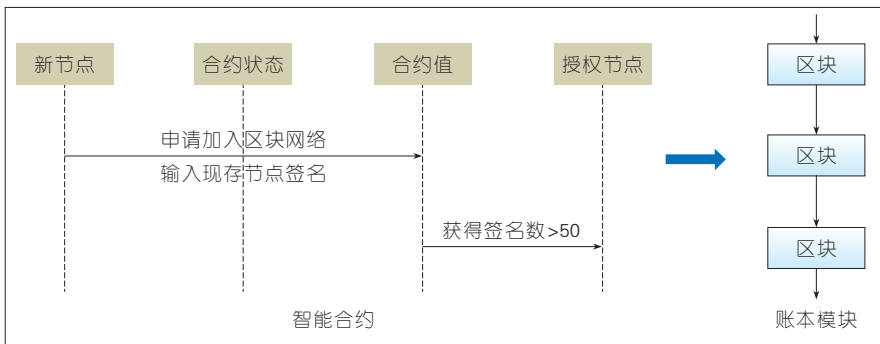
在使用可穿戴传感设备前,每个用户的手机需要与设备借助轻量级认证协议完成用户与传感器之间的身份认证。其次,再利用区块链技术实现体域网中多方身份认证过程。在传感器端生成数据后,使用证书中心生成的公钥将数据加密,传输给路由器。这期间,为保证新加入的节点身份的正确性和真实性,账本端启用共识算法,用于验证新节点身份。新节点需经过智能合约的判断:当有半数以上的节点通过审核时,系统自动认可该节点被记入帐本,并记录到主链上;否则,本次请求视为无效,该节点不被放入主链中。本系统架构能有效地防止恶意节点的加入,确保了节点的正确性和安全性。新节点加入区块的智能合约流程如图3所示。

本文所提的区块链结构如图4所示,区块头包含了版本号、前区块哈希值、时间戳、随机数和该区块哈希值。前一区块哈希值又称为父哈希,用于和前一个区块进行连接,形成链式结构;生成每一个区块的时间就是时间戳;最先找到并正确验证随机数的矿用拥有该区块的记账权;Merkle根中记录了所有交易时所用的信息。

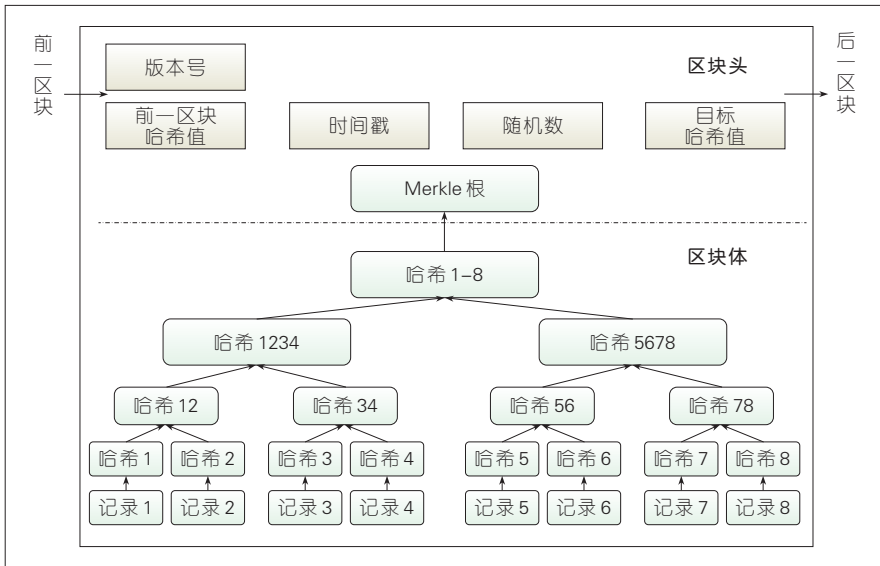
区块链中第一个区块被称为创始区块,起始于创始区块,每一个新生成的区块严格按照时间戳的先后顺序,通过区块哈希地址连接到上一个区块中,形成链式结构。同时,前一个区块的加密结果会被用于当前区块的加密,也就是说,任意1个区块数据的改变将会影响2个区块中的信息。所以,区块链技术能够有效地



▲ 图2 系统框架图



▲ 图3 智能合约流程图



▲ 图4 区块结构

防止恶意对手对数据的篡改,保证了数据的安全性。

3.2 适用于体域网平台的区块链

身份认证

在本节,我们提出了2个身份认证的阶段:用户和传感器之间的群组

轻量级认证阶段,传感器与证书中心、传感器与路由器之间的基于区块链技术的身份认证阶段。

3.2.1 密钥分配阶段

区块链技术使用的是非对称加密算法。非对称加密是由唯一一对

私钥和公钥组成的加密方法。加密算法遵从公钥 K 加密,使用其对应的私钥 K' 进行解密。在区块链中,区块头中的随机数就是私钥,使用不可逆的加密算法生成其对应的公钥,用公钥的哈希算法生成该区块的哈希地址。为了保证数据的隐私性和密钥的安全性,证书中心的公钥和私钥会定时更新,并对应生成其密钥版本号。与此同时,将密钥的版本号提供给传感器和账本模块,以便于用户对数据进行加解密。

3.2.2 群组轻量级认证阶段

初始化时,在用户使用智能医疗服务前,会分别在用户手机端和其传感器的芯片中添加用户标记 δ_i 和传感器标记 s_i ,且两方均可以使用如公式(1)的哈希函数:

$$H_i\{0,1\}^* \rightarrow \{0,1\}^L. \quad (1)$$

在个人可穿戴传感器中,存在资源相对较大的传感器,在该传感器中集成其余设备的信息,用公式(2)进行信息集成:

$$id = id_1 || id_2 || \dots || id_n. \quad (2)$$

为验证传感器与用户的身份,用户首先向传感器发送验证请求。该传感器计算如公式(3)~(5),其中 T_i 是时间戳:

$$U_i = H_i(\delta_i || T_i), \quad (3)$$

$$M_i = U_i \oplus V_i, \quad (4)$$

$$V_i = H_i(id || T_i). \quad (5)$$

将计算结果 (U_i, M_i, V_i) 发送给用户,用来验证传感器的身份。用户在手机端的计算如公式(6)~(7):

$$U'_i = H_i(\delta_i || T_i), \quad (6)$$

$$V'_i = U'_i \oplus M_i. \quad (7)$$

公式(8)如果成立,则完成对传感器身份的验证;否则终止服务:

$$V_i = V'_i. \quad (8)$$

其次,用户端向传感器端发送验证传

传感器的身份的请求。用户端的计算公式为(9)–(10),其中 R_1 是随机数, T_1' 是时间戳:

$$M_2 = (T_1' \| R_1) \oplus U_1', \quad (9)$$

$$V_2 = H_1(s_i \| T_1' \| R_1), \quad (10)$$

将计算结果(M_2, V_2)发送给传感器端,用来验证用户的身份。传感器的计算如公式(11)–(12):

$$M_2' = U_1 \oplus M_2, \quad (11)$$

$$V_2 = H_1(s_i \| M_2'). \quad (12)$$

如果传感器端的验证公式(13)成立,则完成对用户身份的验证;否则终止服务。

$$V_2 = V_2' \quad (13)$$

3.2.3 区块链身份认证阶段

(1) 传感器——证书中心身份认证阶段

在使用传感器前,需要在系统中执行注册阶段。首先,证书中心生成传感器的公钥 K_1 ,并发送给相应的传感器。其次,传感器使用公钥 K_1 加密其身份信息 id_i 和随机数 R ,并将加密结果 E_1 返回给证书中心。最后,证书中心收到加密结果 E_1 后,用其私钥 K_1' 来解密,并对其中的信息进行审核。如果审核通过,则向传感器发送其使用的公钥和私钥(K, K')。

在注册阶段完成后,传感器和密钥生成中心进行相互认证。首先,传感器使用加密算法对公钥 K 、随机数 R 、时间戳 T 和请求服务内容 M 进行加密,并将结果 E_s 发送给证书中心。然后,证书中心用私钥 K' 对加密信息 E_s 进行解密,验证时间戳的准确性并判断传感器的真实性。最后,如果传感器信息为真实可靠的,则再用公钥 K 加密请求服务内容 M 和随机数 R ;否则,终止服务。

(2) 传感器——路由器身份认证阶段

在路由器进行数据传输之前,需要在系统中完成注册阶段。首先,路由器将其和传感器的公钥(K, K')和随

机数 R_2 发送给证书中心。然后,证书中心核实2个公钥的身份信息,如果信息真实可靠,则生成路由器和传感器间的会话密钥 $K_{s,r}$ 。最后,使用传感器公钥对会话密钥和路由器公钥进行加密 E_s ,并返回给路由器。

在注册阶段完成后,传感器和路由器进行认证。路由器用其私钥对加密信息 E_s 进行解密,对传感器身份的真实性进行认证。然后,路由器用会话密钥 $K_{s,r}$ 对随机数 R_2 加密 E_s' ,返回给传感器。最后,传感器用自己的私钥对 E_s' 解密,完成对路由器身份的认证。

使用区块链技术完成身份认证,能够有效地防止恶意用户对数据的篡改。同时,将计算过程进行简化,降低了计算开销,提高了计算效率。

3.3 安全性分析

在本文提出的2个认证阶段中,群组轻量级认证阶段用预先设置随机数的方式,将秘密值提前安全存储在用户移动端和传感器端,并借助发起验证时的时间戳,对用户和传感器群组进行身份认证。无论用户还是传感器群组都无法在自身硬件中篡改或伪造随机数,即使恶意用户对时间戳进行成功伪造,也仅能完成单向认证过程。在该阶段中,用户和传感器群组需要完成双向认证才能证明其身份的真实性。

区块链身份认证阶段使用了区块链的加密方法和结构特征。一个区块中既存有自身的哈希值,也存有前一个区块的哈希值的特征,保证了区块的不可篡改。一旦某一个区块中的数据被篡改或者某一个区块被恶意替换,则会立刻被区块网络所获知。因此,本阶段借助区块的特征对身份进行认证是安全的。

4 结束语

本文主要针对IoT平台中存在的问题展开了研究和分析,并提出使用

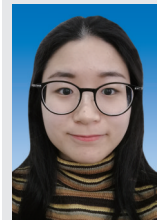
区块链技术来解决上述问题。体域网作为IoT的一部分,将其与区块链技术相结合实现身份认证,是本文的研究重点。通过研究发现:数据能够有效地实现防恶意用户或者服务器的篡改,保证数据的分散性,符合现实生活对数据存储的需求;数据间的传输、加密、验证过程不再需要过于冗杂的计算,提高了数据操作过程中的计算效率,节约了计算开销。与此同时,如何保护在公共信道中的公钥不被他人用于共谋攻击等问题,仍需要日后解决。此外,随着IoT平台的进一步发展,区块链技术实际应用于智能医疗、智能家居等实际场景中将是未来发展方向。

参考文献

- [1] 何渝君, 龚国成. 区块链技术在物联网安全相关领域的研究[J]. 电信工程技术与标准化, 2017, 30(5): 12–16
- [2] SHEN J, ZHOU T Q, CHEN X F, et al. Anonymous and Traceable Group Data Sharing in Cloud Computing [J]. IEEE Transactions on Information Forensics and Security, 2018, 13(4): 912–925. DOI:10.1109/tifs.2017.2774439
- [3] 赵阔, 邢永恒. 区块链技术驱动下的物联网安全研究综述[J]. 信息安全, 2017(5): 1–6
- [4] SHEN J, ZHOU T Q, HE D B, et al. Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing [J]. IEEE Transactions on Dependable and Secure Computing, 2018: 1–1. DOI:10.1109/tdsc.2017.2725953
- [5] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481–494
- [6] XIONG H. Cost-Effective Scalable and Anonymous Certificateless Remote Authentication Protocol [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(12): 2327–2339. DOI: 10.1109/tifs.2014.2363553
- [7] SHEN J, WANG A X, WANG C, et al. Content-Centric Group User Authentication for Secure Social Networks [J]. IEEE Transactions on Emerging Topics in Computing, 2017: 1–1. DOI:10.1109/tetc.2017.2779163
- [8] WANG C, SHEN J, LIU Q, et al. A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things [J]. Security and Communication Networks, 2018, 2018: 1–7. DOI:10.1155/2018/3680851
- [9] CHERUKURI S, VENKATASUBRAMANIAN K K, GUPTA S K S. Biosec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body [C]//The Workshop on International Conference on in Wireless Networks of BIOSENSORS Implanted in the Human Body. USA: IEEE, 2003: 432–439

- [10] BAO S D, POON C C Y, ZHANG Y T, et al. Using the Timing Information of Heartbeats as An Entity Identifier to Secure Body Sensor Network[J]. IEEE Transactions on Information Technology in Biomedicine, 2008, 12(6): 772–779. DOI:10.1109/titb.2008.926434
- [11] VENKATASUBRAMANIAN K K, BANERJEE A, GUPTA S K S. PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks [J]. IEEE Transactions on Information Technology in Biomedicine, 2010, 14(1): 60–68. DOI:10.1109/titb.2009.2037617
- [12] ZHENG G, FANG G, ORGUN M A, SHANKARAN R. A Comparison of Key Distribution Schemes Using Fuzzy Commitment and Fuzzy Vault within Wireless Body Area Networks[C]//IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications. USA: IEEE, 2015:2120–2125. DOI: 10.1109/PIMRC.2015.7343648
- [13] ZAGHOUBANI E K, JEMAI A, BENZINA A, ATTIA R. ELPA: A New Key Agreement Scheme Based on Linear Prediction of ECG Features for WBAN[C]//2015 23rd European Signal Processing Conference (EUSIPCO). USA: IEEE, 2015:81–85. DOI: 10.1109/EUSIPCO.2015.7362349
- [14] ZAGHOUBANI E K, BENZINA A, ATTIA R. ECG Based Authentication for E-Healthcare Systems: Towards a Secured ECG Features transmission[C]//International Wireless Communications and Mobile Computing Conference. China: WICOM, 2017:1777–1783. DOI: 10.1109/IWCMC.2017.7986553
- [15] LAMPORT L. Password Authentication with Insecure Communication [J]. Communications of the ACM, 1981, 24(11): 770–772. DOI:10.1145/358790.358797
- [16] LIU J, ZHANG Z, SUN R, KWAK K S. An Efficient Certificateless Remote Anonymous Authentication Scheme for Wireless Body Area Networks[C]//IEEE International Conference on Communications. USA: IEEE, 2012:3404–3408. DOI: 10.1109/ICC.2012.6363786
- [17] LIU J W, ZHANG Z H, CHEN X F, et al. Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 332–342. DOI:10.1109/tpds.2013.145
- [18] XIONG H. Cost-Effective Scalable and Anonymous Certificateless Remote Authentication Protocol [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(12): 2327–2339. DOI: 10.1109/tifs.2014.2363553
- [19] SHEN J, CHANG S H, SHEN J, et al. A Lightweight Multi-Layer Authentication Protocol for Wireless Body Area Networks [J]. Future Generation Computer Systems, 2018, 78: 956–963. DOI:10.1016/j.future.2016.11.033

作者简介



杨惠杰, 南京信息工程大学在读硕士研究生; 研究方向包括信息安全、密码学和安全多方计算。



周天祺, 南京信息工程大学在读硕士研究生; 研究方向包括信息安全和密码学; 参与主持江苏省研究生科研与实践创新计划项目、信息安全国家重点实验室项目、桂林密码学和信息安全重点实验室项目等; 已发表论文 10 余篇。



桂梓原, 南京信息工程大学在读硕士研究生; 研究方向包括信息安全、密码学和轻量级认证; 参与主持江苏省研究生科研与实践创新计划项目; 已发表论文 5 篇。

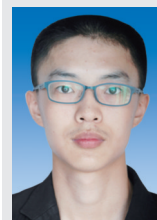
上接第 12 页

的并且消耗资源量小的信任对象是当前共识机制改进的重要问题。

参考文献

- [1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. (2017-06-04) [2018-10-17]. https://github.com/GammaGao/bitcoinwhitepaper/blob/master/bitcoin_en.pdf
- [2] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(04): 481–494
- [3] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J/L]. 自动化学报, 2018: 1–12. DOI:10.16383/j.aas.2018.c180268
- [4] LESLIE L. The Part-Time Parliament [J]. ACM Transactions on Computer Systems, 1998, 16(2): 133–169
- [5] ONGARO D, OUSTERHOUT J K. In Search of an Understandable Consensus Algorithm [C]// Proceedings of the USENIX Annual Technical Conference. USA: USENIX ATC, 2014:305–319
- [6] CASTRO M, LIISKOV B. Practical Byzantine Fault Tolerance[C]//Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. USA: OSDI, 1999:173–186
- [7] DWORK C, NAOR M. Pricing via Processing or Combatting Junk Mail[C]//Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Germany: Springer-Verlag, 1993:139–147
- [8] GIBERT 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. DOI: 10.1145/564585.564601
- [9] Proof of Stake [EB/OL]. (2017-11-10) [2018-10-17]. https://en.bitcoin.it/wiki/Proof_of_Stake
- [10] DUONG T, FAN L, ZHOU H S. 2-Hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely [EB/OL]. (2016-07-19) [2018-10-17]. <https://eprint.iacr.org/2016/716>
- [11] ANTONOPOULOS A M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [M]. USA: O'Reilly Media Inc
- [12] 白帽信息安全研究院. 区块链安全分析报告[R/OL]. (2018-05-08) [2018-10-17]. <https://bcsec.org/report>
- [13] DOUCEUR J R. The Sybil Attack [C]// Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS '01). Germany: Springer-Verlag, 2002. DOI:10.1007/3-540-45748-8_24
- [14] Bitcoin Energy Consumption Index [EB/OL]. [2018-10-17]. <https://digiconomist.net/bitcoin-energy-consumption>

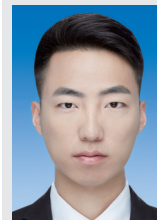
作者简介



王李笑阳, 中国人民大学信息学院在读研究生; 主要研究领域为区块链技术及其应用。



秦波, 中国人民大学副教授; 主要研究领域为新兴信息系统安全、数据安全与隐私保护、云计算安全、应用密码学; 发表论文近百篇。



乔森, 中国人民大学信息学院在读研究生; 主要研究领域为信息安全、区块链等。

一种基于区块链的身份识别技术

An Authentication Technology Based on Blockchain

苏宣瑞/SU Xuanrui
邹秀清/ZOU Xiuqing
丁勇/DING Yong

(桂林电子科技大学, 广西 桂林 541004)
(Guilin University of Electronic
Technology, Guilin 541004, China)

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0041-008

摘要: 基于以太坊的智能合约技术提出一种新型身份识别系统的设计方案, 其中平台架构设计分为数据层、网络层、共识层和接口层, 采用点对点(P2P)技术将数据分布存储在各个节点, 实现了分布式认证, 可抵抗黑客的攻击; 采用椭圆曲线数字签名算法(ECDSA)和改进的Merkle树, 确保数据的真实性。本设计具有高拓展性、高可靠性、高安全性的特点, 支持不同平台进行统一的身份认证。

关键词: 区块链; 以太坊; 智能合约; 身份识别

Abstract: A new authentication system design based on Ethereum smart contract technology is proposed. The platform architecture includes a data layer, a network layer, a consensus layer, and an interface layer. The point to point (P2P) technology is used to distribute data to each node, then a distributed authentication mode can be implemented, and hacker attacks can be resisted; the elliptic curve digital signature algorithm (ECDSA) and the improved Merkle tree are applied to ensure the authenticity of the data. This design is highly scalable, high reliability and high security, and supports unified authentication on different platforms.

Keywords: blockchain; Ethereum; smart contract; authentication

随着互联网行业的发展, 越来越多的新型的网络平台融入到了人们的生活, 人们日常生活都要用到淘宝、京东等交易平台, 使用支付宝、小米钱包、微信等来支付。这些平台都有一套独立的注册、登录、认证和权限管理的系统, 每一个用户在系统中都充当不同的角色, 并拥有不同的权限, 这种中心化系统给人们带来的弊端有以下几点:

(1) 如果有多个系统需要进行登录、认证, 管理员的维护和管理成本将会大幅增加, 并随着规模的增加, 维护难度会增加。

(2) 用户必须记住自己的多个账号、密码, 如果账号很多, 使用起来将非常不便捷。

(3) 容易被黑客攻击, 带来损失。

(4) 中心化系统不可信, 管理员可以随时篡改数据。

区块链技术是一种利用去中心化共识的机制维护一个完整的、分布式的、不可篡改的账本数据库的技术, 它能够让区块链中的参与者在无需建立信任关系的前提下实现一个统

一的账本系统。近年来, 区块链以成分布式数据存储、点对点(P2P)传输、新型加密算法和共识机制等技术的特点, 已越来越成为许多国家政府和国际组织研究讨论的热点, 依靠互联网的产业也纷纷加大了对投入的力度^[1], 但是目前全球还没有政府大力推广将该技术应用于物联网的身份识别系统。

如今新型的区块链技术给人们带来了解决方案: 区块链建立了动态的P2P网络, 没有了中心化服务, 账本均分布在每个节点中, 所有的节点一同维护; 账本上记录了该区块链自创建以来的记下的所有交易记录, 通过密码学的安全机制, 使得所有记录不可修改、真实可信; 每个人都是一个节点, 通过彼此之间的信任来建立区块链的信任。区块链网络没有传统的

中心管理员, 整个网络的运作由线上的电脑共同进行维护, 使得运营成本大幅降低。

本设计组成的框架主要包括四大模块: 数据层模块、网络层模块、共识层模块和接口层模块。通过接入到同一个区块链网络中, 使用统一的接口层进行交互, 同时接口层还能和网络层和共识层通过底层协议进行交互, 网络层负责发现区块链网络中的P2P节点和数据的传输, 共识层负责身份认证, 数据层负责存储数据。

1 关键技术

1.1 区块链技术

1.1.1 区块链技术基本原理

假设Bob要在互联网上向Alice转

收稿日期: 2018-10-30
网络出版日期: 2018-11-27

账,每次转账都会产生交易记录,将所有交易记录进行连接,生成总帐单,总账单包含每个人的余额。记账时,应需保持公平、诚信的态度,使得双方能够相互信任;但记账人可能会作假,使得双方的信任程度降低,这是很典型的欺诈行为。区块链技术则可以很好地解决这一问题,没有人可以作假。

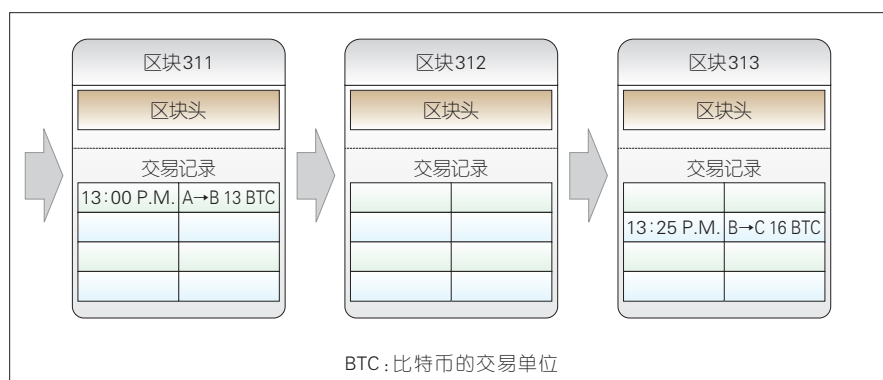
现把账单模型进行缩小,规定:每次更新、修改数据必须在原有的账单中进行,并且新账单包含时间戳、前一个账单的哈希值等数据。将这些帐本累加起来称为总帐本,总帐本将所有的块链接起来,组成区块链,图1表示一条区块链中的3个区块。

1.1.2 区块链的去中心化

在2008年的金融危机中,比特币的创始人中本聪发明了比特币,它成为了第一个去中心化的数字货币。区块链是一个分布式网络,每个节点都会存放所有交易的副本,并自动同步。节点可以是用户的电脑、手机,或是其他设备。如图2所示,区块链网络节点是扁平化的,每个节点的地位相等、公平,并以扁平拓扑的方式进行数据交互^[9]。

假设Bob想给他人转账,Bob就得向全网广播他要转账的消息,并需全网达成共识,才能认为他的消息是合法的,且每个节点都会保存他转账信息。全网没有中心服务器,没有人能拥有管理的权力,只要规则定好了,就必须照着规则做,没有人可以改变,这其实就是区块链去中心化的魅力所在。

所有节点都相当于“校验员”,它们无时无刻不在检查区块中的交易信息是否正确,并且在检查交易的时候,不断尝试产生随机数,计算哈希值,使数据具有很强的安全性,黑客无法入侵,无法修改账户余额。随着用户的增加,越来越多的后续节点(用户)加入到了比特币网络中,共同完成共识的过程^[9];而整个过程中网



▲ 图1 一条区块链中的3个区块

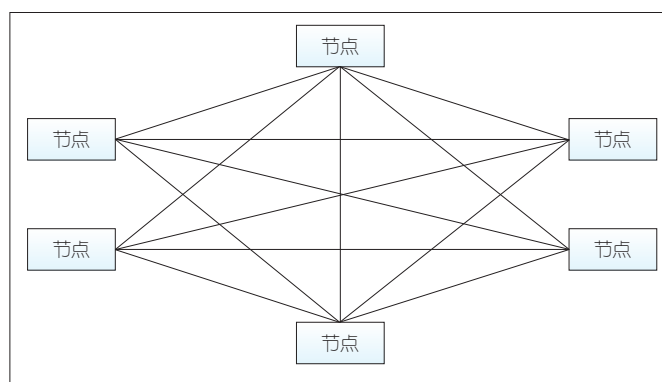


图2
去中心化的节点图

络中每个节点的地位是相同的。比特币不是凭空产生,而是通过消耗了电力、物力并应运算而产生的,因此具有价值,可以兑换成现有的货币。

1.2 加密哈希函数和哈希指针

哈希函数也叫做哈希算法,不论输入字符串的长短,生成签名的长度都是固定的,因此可以作为一段数据的数字指纹,便于区分每个消息。生成的摘要可作为签名,以确保数据的真实性。账户的创建需要一个非对称加密密钥对,以太坊选择的是椭圆曲线加密算法(ECC)中的Secp256k1,依据速度、安全性等参数确定账户的地址,具体的方法如下:

- (1) 创建一个随机私钥,由64个十六进制的字符构成;
- (2) 从私钥中导出公钥;
- (3) 从公钥中导出地址。

使用Secp256k1生成256位公钥/密钥,然后编译成64位长度的十六进制字符串;采用公钥的Keccak-256哈

希算法,得到一个32字节的字十六进制字符串,接下来对该字符串进行截取,取字符串的最后20个字节(即删除前12个字节),得到了40个字节的字符串,在签名加上0x前缀,就可以得到一个42个字节长的地址,该地址就是以太坊用户全网唯一的账号。

1.3 Merkle树

Merkle树在区块链中尤其重要,相当于用大量的数据块来进行哈希运算。Merkle树将2个相邻的认证请求进行哈希计算,逐步堆积到Merkle树根。这种哈希算法的好处就是让历史数据不可篡改、真实可信^[10]。节点的值是它相连2个叶子节点的哈希,这就导致整个Merkle树中的数据都是互相关联的,改动其中一个数据,将会彻底改变整个区块的结构,因此给身份的证明提供了一个非常简洁的机制。

Merkle树的最初应用是在比特币中,即使用了Merkle树来存储每个区

块的交易。每个Merkle树从块到根都是由哈希的分支组成,如图3所示。由于Merkle树采用了非常强的哈希算法,且哈希后的摘要要求逆几乎不可能实现,因此Merkle树提供了真实可信的数据验证方法。

每个区块头包含如图4所示的内容。将相连的数据区块的数据进行相连,通过上一区块的哈希值和当前区块的哈希值将所有的区块请求进行关联。如果修改了其中一个数据,将影响所有在当前区块链网络上的区块,因此数据不可能被篡改,所有的认证请求不可伪造,极大提高了区块链的安全性。

1.4 ECDSA

ECDSA是数字签名算法(DSA)的其中一个例子。和非对称加密算法(RSA)进行对比,在相同的安全强度下,ECDSA可以使用的密钥更短,从而节省网络和存储空间,具有较高的

研究价值^[5]。

在本设计方案中,首先要避免数据明文传输的极大不安全因素,同时要保证交互双方的身份真实性,因此需要利用公钥加密算法中非对称加密的优势。使用本设计方案进行数据传输时,将服务器的公钥输出在客户端,客户端使用公钥加密,在信息交互时数据以密文方式传给服务器端,再由相应私钥得到明文数据^[6]。

Alice将要给Bob发送一条消息,要求消息包含数字签名来进行身份识别,那么可以定义一组参数($CURVE, G, n$),其中 $CURVE$ 表示椭圆曲线的点域以及它所使用的几何方程, G 表示椭圆曲线基点,大素数 n 是椭圆曲线的阶数^[7]。接下来我们介绍数字签名的具体过程和验证数字签名的具体过程。

(1) 数字签名的过程

如果Alice要发出认证请求,她希望能对消息 m 进行签名,因此将椭圆

曲线的参数设计为 $D=(p, a, b, G, n, h)$,其中对应的密钥对为 (k, Q) , Q 为公钥, k 为私钥。Alice将按照如下步骤进行签名:

- 1) 产生一个随机数 $d, 1 \leq d \leq n-1$;
- 2) 计算 $dG=(x_1, y_1)$,将 x_1 转化为整数 \bar{x}_1 ;
- 3) 计算 $r=\bar{x}_1 \bmod n$,若 $r=0$,则转向第1步;
- 4) 计算 $d^{-1} \bmod n$;
- 5) 计算哈希值 $H(m)$,并将得到的比特串转化为整数 e ;
- 6) 计算 $s=d^{-1}(e+kr) \bmod n$,若 $s=0$,则转向第1步;
- 7) (r, s) 即为Alice对消息 m 进行的签名。

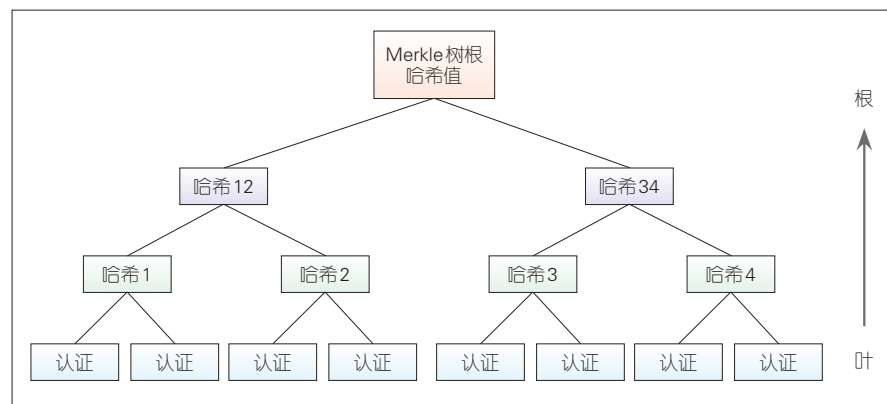
(2) 验证数字签名的过程

如果Bob收到消息 m 之后,他需要验证消息 m 的签名 (r, s) ,在得到椭圆曲线参数和 Q 之后,将按以下步骤操作来验证数字签名^[8]:

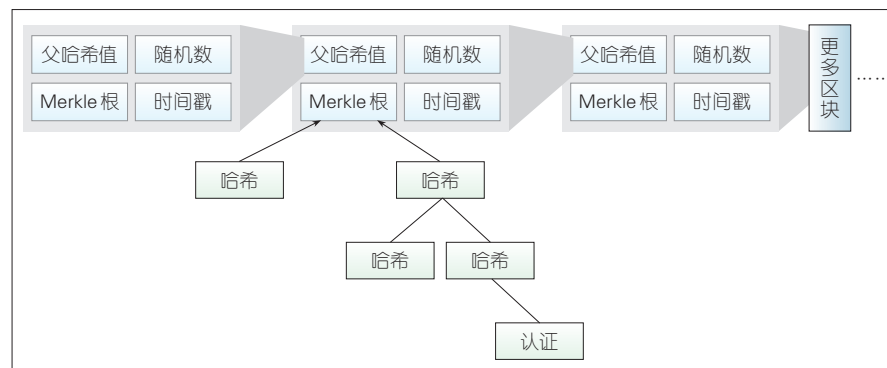
- 1) 首先验证 r 和 s 是区间 $[1, n-1]$ 上的整数;
- 2) 计算 $H(m)$ 并将其进行转化为整数 e ;
- 3) 计算 $w=s^{-1} \bmod n$;
- 4) 计算 $u_1=ew \bmod n$ 以及 $u_2=rw \bmod n$;
- 5) 计算 $X=u_1G+u_2Q$;
- 6) 若 $X=0$,则拒绝该签名的有效性,否则将 X 的 x 坐标 x_1 转化为整数 \bar{x}_1 ,并计算 $v=\bar{x}_1 \bmod n$;
- 7) 当且仅当 $v=r$ 时,签名验证可以通过。

利用ECDSA算法,将认证信息进行数字签名,确保了每条认证消息都是由正确的用户发表的,防止他人假冒,还可以保证数据的完整性。在整个认证请求中,将不会有人对数据包进行恶意篡改。

每个节点用户再发起认证请求时,都会利用自己的私钥签名,其他节点收到认证请求,也会一同参与签名认证的操作。如果认证成功,将会将账单记录下来,完成认证;否则将



▲ 图3 Merkle树的结构



▲ 图4 数据区块头的结构

拒绝认证请求。

1.5 共识方法

1.5.1 Gas——以太坊系统计算工作量的单位

Gas 是以太坊系统中执行交易所需要的计算工作量单位。所有的交易不论是转账交易,还是执行智能合约,都要消耗 Gas。Gas 的价格由交易的发起人和矿工的工作量决定,交易打包进区块中需要矿工们进行哈希运算,矿工们付出了劳动,因此需要收取一定的费用。如果交易发起人设置的 Gas 价格过低,矿工们基本不会将交易打包进区块里;如果交易设定较高的 Gas,该交易将会得到较高的优先级。

1.5.2 以太坊的工作量证明和挖矿原理

工作量证明(PoW)的目的是阻止网络攻击,如当今网络环境下常出现的分布式拒绝服务攻击(DDoS),就是用来发送许多假的请求以耗尽计算机网络系统资源,导致服务器宕机,真正的用户则无法登录到中心服务器上^[9]。

PoW 被定义为花费计算机算力来进行数据校对的要求,俗称“挖矿”。挖矿的目的有以下几点:

- (1) 验证交易的合法性,避免出现多重交易的情况;
- (2) 用来奖励矿工所做出的计算工作;
- (3) 维护以太坊系统的正常安全运转。

通过挖矿的方式解决 PoW 的数学难题具有不可逆的特征。从技术角度来说,挖矿的过程就是一个不断进行的哈希运算过程,它通过尝试产生随机数,找到满足条件的随机数后立即将区块进行打包并全网广播,找到该随机数的节点也是赢得本轮记账权利的节点。该区块将在整个区块链网络广播,进行共识的达成。如果

达成共识,每个节点将会将该区块添加到自己的区块链中,同时该矿工将会得到以太坊奖励。

随机数的条件取决于系统设定的难度,例如:要求整个区块加上随机数计算出的哈希值要小于给定的值才算成功;而哈希值的产生没有规律可循,只有算力越高的计算机才能更快得到符合条件的随机数。

2 核心框架

2.1 数据层

2.1.1 数据区块和链式结构

首先,区块是以太坊网络的核心,所有的交易、数据存储都是在区块头中进行的。不同的区块头之间通过头指针(ParentHash)函数指向前一个区块的头指针,将它们串联起来,形成单项链表。

区块结构分为区块头和区块的数据部分这2个部分,源码在以太坊的/core/types/block.go中,数据层的函数关系如图5所示。

其中,区块的结构体定义为:

```
type Block struct
```

```
{
//表示一次交易的结构体
header *Header      //区块头
transactions Transactions //交易
}
```

区块头的结构体定义为:

```
type Header struct
```

```
{
    ParentHash common.Hash //头指针,指向前一个区块
    Number *big.Int        //代表当前区块的编号
}
```

在上面的结构体中提到了交易指针,简称tx,表示一次以太坊交易的结构体。相应的代码在/core/types/transaction.go中。

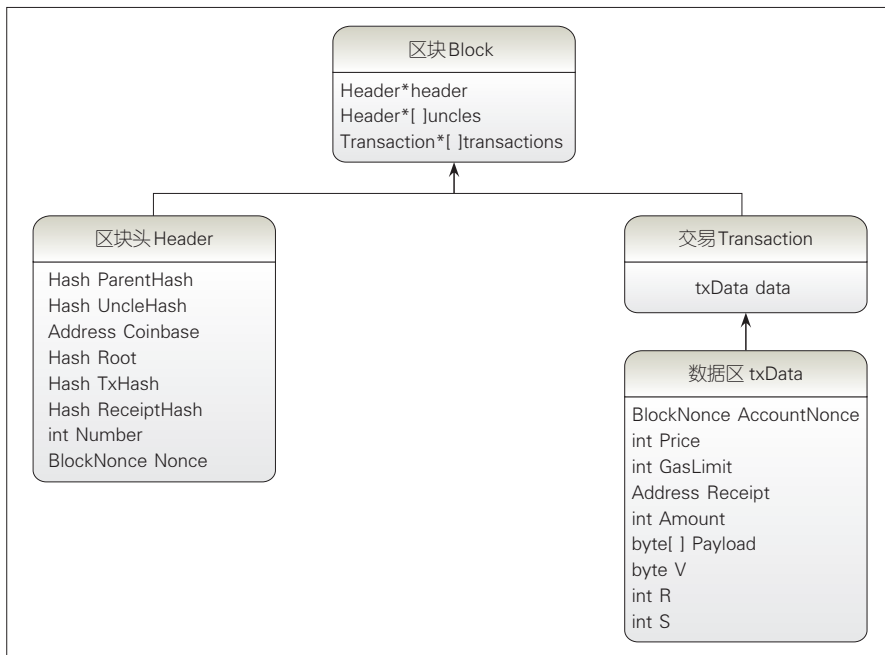
交易的结构体定义为:

```
type Transaction struct
```

```
{
    data txdata //交易的存储数据
    Hash, size, from atomic.Value //在内存使用
}
```

数据区(txdata)的结构体定义为:

```
type txdata struct
```



▲图5 数据层函数关系图

```

{
    AccountNonce uint64 //随机数
    Price *big.Int      //交易所产生
    的费用
    GasLimit *big.Int   //当前以太
    坊网络 gas 的限制
    Recipient *common.Address //
    转账转出方的账户地址
    Amount *big.Int
    Payload []byte
    V, R, S *big.Int    // 数字签名的值
    Hash *common.Hash   // Hash 的
    封装处理
}

```

2.1.2 Merkle 树的使用

在以太坊中使用的是 Merkle 树的改进树 (MPT), 也是二叉树的一种。节点的值是它相连 2 个叶子节点值的哈希。Merkle 树用于所有交易正确性的验证, 而 MPT 则大大提高了查找效率。树的构造代码在以太坊源码的 trie/trie.go 中, 关键代码如下。

首先是从根节点进行遍历:

```

func (t *Trie) HashRoot(db
DatabaseWriter) (node, error)
{
    if (t.root == nil) {...}
    //如果节点不存在子节点了, 直接
    返回
    h := newHasher(t.cachegen, t.
    cachelimit)
    //否则会对节点进行折叠, 继续
    遍历
    return h.Hash(t.root, db, force:
    true)
}

```

通过调用下面的函数跟父节点进行交互, 进行数据存储:

```

func (t *Trie) Commit() (root Hash,
error)
{
    if (t.db == nil) {...} //如果数据
    已经存在数据, 返回
    return t.CommitTo(t.db) //父节点
    没有数据, 就调用下面的函数写数据
}

```

```

}
func (t *Trie) CommitTo(db
DatabaseWriter) (root common.Hash,
error)
{
    Hash, cached, error := t.HashRoot
    (db) //对数据进行 Hash, 存放到父节
    点中
    t.root = cached //把当前遍
    历的位置存放到内存中
    ...
}
    查找、插入、删除都是在 trie/trie.go
    里进行使用的。

```

2.1.3 数据存储的实现

以太坊的数据存放在 StateDB 中。StateDB 是以太坊的数据库, 负责本地存储数据及业务, 还负责连接到底层的数据库, 它使用二级缓存机制来存储账户的相关数据。

StateDB 的相关代码在 core/state/statedb.go 中, 其定义的结构体以及作用为: DataBase 类型的 DB 用于存放数据, Tire 类型的 tire 用于存放 MPT 树, stateObject 表示以太坊账户, 其中在 stateObject 中也有二级缓存机制, 主要用来缓存和更新以太坊帐户。

整个以太坊网络的运作结构如图 6 所示。

2.2 网络层

2.2.1 网络层传输协议

当一个节点有新的数据区块产生, 该节点将会进行全网广播, 其他

收到请求的节点将会进行验证。一个节点创建一个新的区块, 该新区块很快会被发到网络上所有的节点, 然后每个节点都要验证这个新的区块, 验证其真实性。经验证后, 每个节点才会添加这个新的区块到区块链, 区块链网络中的所有节点达成共识, 一起决定哪个区块有效而哪个无效, 擅自篡改的区块会被网络上其他节点拒绝^[10]。

在节点之间传播数据时, 采用加密网络和传输协议 (RLPx) 加密握手协议。该协议在网络层的上层, 在以太坊网络中新的节点建立后, 首先进行端口监测侦听、节点间连接及通信交互, 当节点间都建立了连接, 将会通过 Msg 的格式进行通信。每次在通信的过程中, 都会做出如图 7 所示的判断, 以确保握手协议运作正常, 如果运作不正常, 将会失去对该节点的连接。

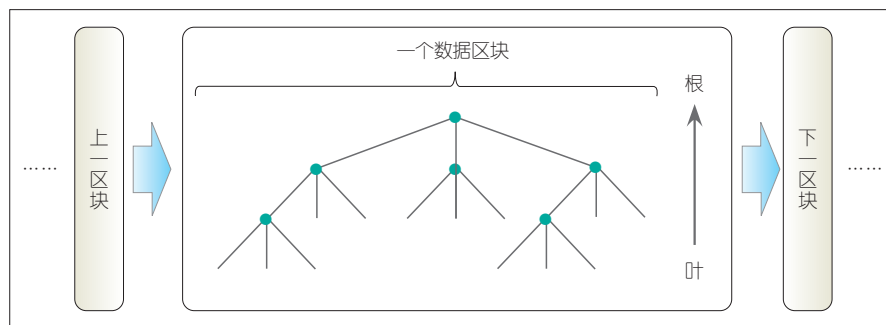
RLPx 加密握手协议的具体流程如图 8 所示。

2.2.2 数据验证机制

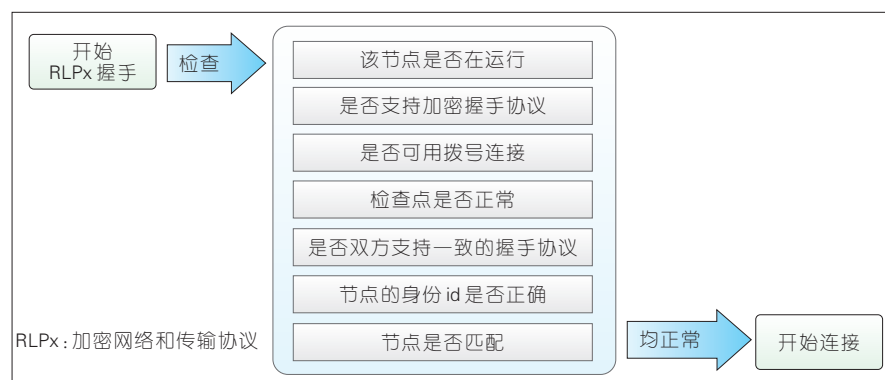
P2P 网络中的每个节点, 只要在线, 都在随时监测侦听其他节点的认证请求, 验证区块数据的具体一些步骤如下:

(1) 负责识别网络中广播的数据和区块;

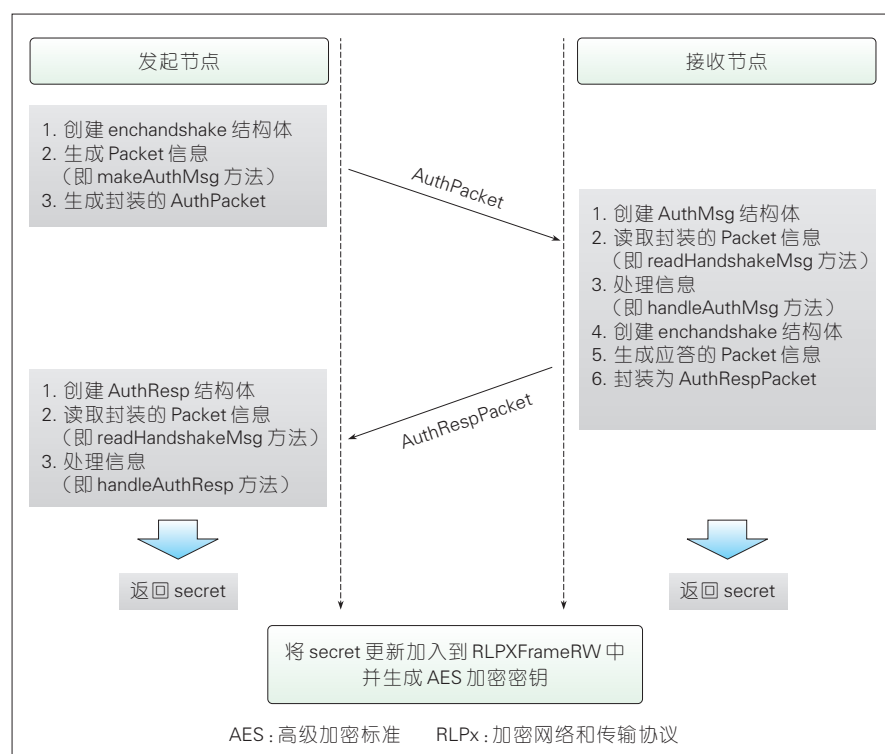
(2) 如果接收到相邻节点发来的认证, 将会对认证请求进行分析, 将检查数据的完整性、语法的规范性、数字签名是否正确等方面来校验交易数据是否有效;



▲ 图 6 以太坊网络的运作结构



▲ 图7 RLPx 加密握手协议的建立



▲ 图8 RLPx 加密握手协议的流程

(3) 如果数据有效,将会把数据放入存储池中,即将认证请求记录到本地,同时向相邻节点转发数据;

(4) 如果数据无效,将会立即放弃该数据,确保数据不会在区块链网络中传播。

2.2.3 P2P 网络的具体实现

以太坊的 P2P 网络主要使用以下几个工具实现。

(1) Discover: 使用了 Kademlia 协议,用于使用 UDP 的 P2P 节点发现的

协议;

(2) discv5: 用于发现新节点;

(3) nat: 网络地址转换工具;

(4) netutil: 有关网络连接的工具;

(5) simulations: P2P 网络测试工具。

P2P 网络非常复杂,如果要使用它,就必须包含节点查找、节点维护、节点建立连接的功能。在 database.go 文件中, newNodeDB 函数用来存储节点数据,存储节点数据采用了 Keccak-256 的签名哈希算法。以下是一些关键函数。

(1) 查找节点的函数: func(db *nodeDB)node(id NodeID)*Node;

(2) 插入数据的函数: func(db *nodeDB)updateNode(node*Node);

(3) 删除数据的函数: func(db *nodeDB)deleteNode(id NodeID)。

连接超时的处理办法,即如果发现有个节点接收消息的时间超出了设定的值,那么就删除节点不再连接,关键代码如下:

```
func (db *nodeDB) expireNodes()
error
{
    threshold := time.Now().Add(-
nodeDBNodeExpiration)
    //将节点最后接收的时间和当前的
    时间进行比较
    it := db.lvl.NewIterator(nil, nil)
    defer it.Release() //初始实例化,
    先将指针指向头部,接下来准备开始
    遍历
    for it.Next() //循环查找节点
    {
        .....
        if !bytes.Equal(id[:], db.self[:]) //
        找到对应的节点
        {
            if seen := db.lastPong(id); seen.
            After(threshold)
            //如果节点
            在规定时间内更新,继续查找
            Continue
            db.deleteNode(id) //否 则
            释放该节点,不再连接
        }
        return nil //返回最新
        的节点
    }
}
```

2.3 共识层

2.3.1 PoW 的机制

PoW 通过计算机进行数学运算得到记账权,但是每次要达成全网共识,都需要全网一起参与运算。本设计系统作了以下规定,使认证步骤准

确进行:

(1)所有连接到以太坊网络的地址都应该分为已被认证的和未被认证的;

(2)已认证的节点可以变成没有经过认证的,没有经过认证的节点也可以变成已认证的;

(3)一条认证请求包括认证的地址、认证的状态等;

(4)认证成功之后不能再进行第2次认证。

2.3.2 共识记账的设计方案

本设计方案的认证流程如下:

(1)请求的生成。以太坊的客户端持续监测侦听,如果网站调用了认证请求,那么客户端将会向全网进行广播。Alice使用她的私钥对认证请求进行签名,并在认证请求的末尾处添加签名,以便能够让其他节点来进行校验。

(2)请求的广播。Alice将认证的请求向全网节点广播,其他的节点将会收到并将共同参与数字签名的校验。若正确,则将其纳入到矿工自己的区块中;若不正确,则丢弃。

(3)区块的生成。每当间隔一段时间,所有的节点通过挖矿进行PoW,通过解决数学难题来赢得记账的权利,此过程也是所有节点进行区块同步校对的过程。

(4)区块的广播。如果有节点通过算力找到了符合条件的随机数,将会向全网广播,该节点将是下个区块的创建者,并会获得奖励;

(5)区块写入账本。将对所有节点成功解出数学难题的广播答案进行验证,如果正确,它会将该区块纳入自己的账本中,每个节点同步进行;否则,将丢弃该区块。

2.3.3 共识记账的实现

共识层的代码在 consensus/路径中,本节具体介绍共识记账的实现。

prepare函数主要用来处理区块头部信息,其定义如下:

$$\text{diff} = (\text{parent_diff} + (\text{parent_diff} / 2048 * \max(1 - (\text{block_timestamp} - \text{parent_timestamp}) / 10, -99))) + 2^{(\text{periodCount} - 2)}$$

其中parent_diff表示上一区块的难度;block_timestamp表示当前区块的时间戳;parent_timestamp表示上一区块的时间戳;periodCount表示区块数量。

结合官方的文档,在测试阶段,调节区块难度的值为一个较低的值,让登录认证的交易尽快被矿工打包,避免用户长时间等待,同时方便调试和使用。难度设定需基于创世区块(创世区块是指区块链的第1个区块,它是构建整个区块链系统的基础)。

seal函数用于处理挖矿的工作,需要一直递归调用,直到解决问题,解决问题之后退出。seal函数具有以下几点作用:

(1)根据区块头部的信息中的挖矿难度系数来处理计算目标值。

(2)选取随机数和区块头的哈希值,进行哈希运算。如果结果小于目标值,那么表示挖矿成功,自动退出;否则,则继续循环进行哈希运算。

(3)如果从外部收到了这个块,表示其他人已经挖矿成功并且已经得到了块,那么就会马上放弃打包当前块。

(4)Finalize函数表示挖矿成功之后奖励的事,它可以计算矿工的奖励,使矿工得到奖励。

verifyHeader函数主要用来校验区块的时间戳、校验难度值、校验区块的gas。

VerifySeal函数主要用来验证区块头部的签名信息。

2.4 接口层

本设计系统使用的是以太坊的go-ethereum客户端来连接到自己搭建的以太坊私有网络,它提供的应用程序编程接口(API)可以给本设计系统进行调用,并用来创建新地址,验证数字签名、支付和转账、查看余额等。接口层包含了以太坊智能合约

脚本、分布式计算、验证加密签名和数据存储的技术。所有的请求数据通过post传递,使用json参数传递。

解析一个请求的具体的实现步骤如下:

(1)首先要对json数据进行实例化,使用NewJSONCodec编码器;

(2)通过NewJSONCodec编码器将请求转换为jsonRequest,并且获取参数有关服务名(service_name)、服务方法(service_method)和数据片段(params);

(3)通过服务名(service_name)和服务方法(service_method),查找已经注册的rpc服务;

(4)向rpc服务进行请求,之后的操作都在rpc服务中进行;

(5)rpc返回结果,接着对json序列化,返回结果值。

例如:本设计系统使用Ethereum客户端账,在向rpc服务发送请求时,设定service_name为指定以太坊的服务名,并设定service_method为sendRawTransaction,通过调用rpc服务,返回的结果是TxnHash字符串的json数据。

3 结束语

本设计方案最大的创新之处在于身份识别系统基于以太坊智能合约技术,立足于传统互联网行业的现状,解决了中心化管理的麻烦,以及用户信息容易被篡改、被黑客盗用,中心服务器被攻击等事关国家信息安全痛点的问题。

在本设计中,认证请求者向系统提出认证请求,服务器节点在收到请求后,采用认证方案对识别认证者的请求,同时将认证信息加入到认证区块链中。这个过程解决了分布式账本的一致性和安全性问题,不需要第三方中介的引入。

该系统具有以下创新特点:

(1)去中心化,防止伪造。根据当今互联网产业的需求,本系统使用P2P技术,改善了数据的存储。所有

的数据通过分布式存储保存在各个节点,每个用户都是一个节点,通过节点的共识,完成身份识别,不依赖第三方。

(2)数据校验,真实可信。结合以太坊改进之后的MPT树,以及通过RLPx加密握手协议,并充分利用ECDSA的非对称加密的优势,避免了黑客通过网络传输作弊的行为。整个认证过程由节点们共同完成,使数据真实可信。

(3)安全性高,黑客止步。基于区块链的去中心化特点,每个节点的地位都是对等的,即使某个或者部分节点被摧毁都不会影响整个系统的安全,也不会造成数据的丢失。黑客如果想篡改数据,需要攻击、修改一半以上的节点数据,这几乎是无法实现的。

(4)调用方便,拓展性高。本系统设计的接口层,通过json传递参数到以太坊客户端,基于接口层方便调用的特点,可快速搭建更多不同开发语言的网站和程序,同时客户端支持多个网站和程序,并调用获取账号的信息,实现了账号的统一身份认证。

(5)部署简单,用途广泛。本设

计方案可以部署在企业、政府机构、教育结构等,例如:在企业中,多个部门可以使用同一套以太坊网络,无需在每个部门都进行部署,支持跨多个部门,适合部署在大型企业中。

本设计仍然有很多的可拓展之处,除了身份认证,还可以通过以太坊智能合约开发更多功能,例如:房屋出租、契约、贷款平台等,能给使用者带来显著的安全效益、经济效益、管理效益、科研效益。

参考文献

- [1] 韦康博. 解读区块链——重新定义未来经济[M]. 北京: 人民邮电出版社, 2017
- [2] 申屠青春. 区块链开发指南[M]. 北京: 机械工业出版社, 2017
- [3] 徐明星, 田颖, 李霁月. 图说区块链[M]. 北京: 中信出版社, 2017
- [4] 杨波. 密码学中的可证明安全性[M]. 北京: 清华大学出版社, 2017
- [5] MANN C, LOEBENBERGER D. Two-Factor Authentication for the Bitcoin Protocol[J]. International Journal of Information Security, 2017, 16(2): 213-226. DOI:10.1007/s10207-016-0325-1
- [6] 陈志德, 黄欣沂, 许力. 身份认证安全协议理论与应用[M]. 北京: 电子工业出版社, 2015
- [7] 虞小忠. 区块链在身份认证中的应用[J]. 科技经济导刊, 2017(3): 26-27
- [8] 邓迪. 区块链技术最新的认识和成果[J]. 新经济, 2016, (19): 90-91
- [9] 康双勇. 区块链中的身份认证问题研究[J]. 保

密科学技术, 2018(5): 32-35

- [10] 陈烨, 许冬瑾, 肖亮. 基于区块链的网络安全技术综述[J]. 电信科学, 2018, 34(3): 8-16.
DOI:10.11959/j.issn.1000-0801.2018135

作者简介



苏宣瑞, 桂林电子科技大学在读本科生; 主要研究方向为信息安全以及区块链等。



邹秀清, 桂林电子科技大学在读硕士研究生; 主要研究方向为信息安全、区块链等。



丁勇, 桂林电子科技大学计算机与信息安全学院教授、副院长, 广西密码学与信息安全重点实验室主任; 主要研究方向为公钥密码理论、同态加密、密码安全协议、区块链等; 主持国家自然科学基金、中国密码发展基金、国防预研基金、广西区自然科学基金等项目10余项; 发表论文60余篇, 其中SCI/EI检索30余篇, 出版学术专著1部、工信部规划教材1部。

区块链的理想与现实

Vision and Reality of Blockchain

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0049-003

摘要: 认为区块链是互联网的又一块补丁, 弥补了价值传递时的不足。去中心、匿名性和不可篡改, 一起构成了区块链的三大技术支柱, 这些技术特征在实际的商业应用中, 还需要做很多的妥协和再平衡工作。区块链作为一种新兴的数据库技术, 还处于非常早期的阶段, 多个方面的技术都有待改进。

关键词: 区块链; 去中心化; 工作量证明(PoW); 权益证明(PoS); 区块链即服务(BaaS)

Abstract: Blockchain is the new patch to enhance the shortage for the Internet when transferring the value. Decentralization, anonymity and non-tampering are three technical pillars of the block chain. These technical features need to be compromised and rebalanced in practical commercial applications. It is in the very early stage as a kind of new database technology, and waiting for optimizing in several technical aspects.

Keywords: blockchain; decentralized; proof of work (PoW); proof of stake (PoS); blockchain as a service (BaaS)

何宝宏/HE Baohong

(中国信息通信研究院, 北京 100045)
(China Academy of Information and
Communications Technology, Beijing
100045, China)

1 区块链是块补丁

互联网是一个还没有完成的科学实验, 它过早离开实验室的襁褓来到了人世间。自传输控制协议(TCP)/网际协议(IP)应用的30多年以来, 不断有人预言互联网会崩溃, 会被新技术所替代, 从IP地址耗光、垃圾信息、视频流量、路由表爆炸到安全攻击, 原因不一而足; 但互联网因其良好的开放性和扩展性, 不断自我完善, 既没有崩溃更没有被替代。

与内容分发网络(CDN)、对等网络(P2P)应用、软件定义网络(SDN)、网络地址翻译(NAT)、云计算和移动互联网等类似, 区块链是针对互联网

在价值传递方面的缺点, 新打的一块补丁。

在传统互联网上, 数据主要用来表示信息, 核心要义是传播、复制和分享。随着互联网与实体经济融合的不断深化、大数据的兴起, 数据正在资产化, 资产正在数据化。现在的数据, 很多已经是用来表示价值而不是信息了。数据表示价值, 核心要义是所有权、控制和交易。

互联网与传统电话网、广播电视网类似, 主要用于传递, 尤其是数据信息。数字化的价值, 比如货币、凭证和权益等Token, 不能直接在互联网上传递, 需要通过权威的中心节点做信任背书。这带来了在互联网上交易时, 建立信任的成本高、效率低, 以及中心节点可能造假等问题, 于是就有了基于区块链的价值传递技术,

希望用区块链来代替传统的中心节点, 从信任机构转向信任机器。

区块链的基本思路是将价值数据按时间顺序排列成一条链, 只有某数据的最后一个拥有者, 才是该数据的价值拥有者。链上该数据的曾经拥有者, 都只是价值的过客, 是用来证明最终拥有者的。

这就是所谓的价值互联网, 是互联网的又一次延展。区块链的核心是做数据管理和价值传递, 只是信息技术的一个“区块”, 还必须与其他信息技术和场景“链”起来, 才可能占据互联网世界的一个生态位。

2 区块链是一种数据库技术

传统数据库、大数据和区块链, 都是用来管理数据的, 都可以认为是数据库管理技术^[1]; 但它们追求的目标不同, 因此应用场景也不同。

传统数据库针对的是高价值的结构化数据, 大数据针对的是海量和更多类型的数据。二者都假设, 虽可能会存在数据质量等问题, 但可以相信输入数据的机构以及数据管理员, 相信他们不会故意捏造或篡改数据。

区块链面向的也是高价值数据, 但针对的是数据机构或数据管理员, 以及可能造假的问题。区块链不信

收稿日期: 2018-10-16
网络出版日期: 2018-11-06

任数据机构和数据管理员,不信任他/她写入的数据,除非多个相关方能够根据事先达成的协议(共识机制),集体同意录入。传统数据库为追求一致性而牺牲了效率,大数据为追求效率而牺牲了一致性,而区块链为追求更高的一致性而牺牲了更多的效率。

区块链集成了分布式网络、密码学、共识算法和智能合约等技术,采用了一种集体维护数据的思路。这带来了区块链能够防篡改的特点,但也会严重损耗性能和扩展性等。虽然通过隔离见证、分片、多链和增加块大小等手段,能够加以改善,但理论上性能和扩展性都无法与集中式的数据库技术相比。

当然,区块链还引入了一些数据管理之前没有过的概念,比如共识算法、智能合约和激励机制等,超出了传统数据库的概念范畴,但我们认为本质上还是数据库技术。

3 区块链的技术魔咒

去中心、匿名性和不可篡改,一起构成了区块链的三大技术支柱。因为区块链正处于从比特币实验走向市场试商用的阶段,因此这些技术特征在实际的商业应用中,还需要做很多的妥协和再平衡工作。

3.1 去中心化

比特币和区块链等希望去掉央行和交易中心等中心组织,核心理由是这些权威的中间组织可能会伪造自己的资产负债表,只能做事后审计,并且不容易发现。

但当区块链技术逐步“堕入”商业世界时,去中心化的信仰正在逐步沦丧,架构开始走向了集中。比如区块链的企业操作系统(EOS)项目,就设计了21个中心节点。事实上,如果以最典型的区块链应用,比特币和以太坊等为例做观察,就会发现已经形成了3个中心:代码中心、算力中心和财富中心。

(1)代码中心。2018年3月伦敦大学的研究人员发现:Bitcoin Core软件中所有文件的7%是由一名开发人员编写的,而以太坊中的大约20%的文件是由单一编码人员编写的。对比特币社区影响最大的最初是创始者中本聪,现在是Core小组的5个人。以太坊社区,基本由其创立者BUTERIN V说了算。

(2)算力中心。工作量证明(PoW)和权益证明(PoS)是目前应用最为广泛的2种共识机制,分别基于算力大小和财力大小来分配记账权。PoW的基础是算力,曾经超过70%的算力由一家公司生产,集中在一个国家挖矿,这已形成了算力中心。

(3)财富中心。区块链技术的一大创新,是将激励机制内置化。PoS的基础是代币,全世界代币持有者联合起来就是财富中心。而PoW的算力,又是可以通过资本购买的。有研究表明:比特币是高度集中的,40%的比特币集中在1000人,96.53%的比特币归属4.11%的地址。另外,PoW和PoS只是创造了所谓的数字资产,还需要做数字资产的交易,于是交易所也成了财富中心。

3.2 匿名性

在传统金融系统中,账户名是可以公开的,但账本内容是必须保密的。为储户保密指账户中的记录,不是账户号。区块链的设计反过来了,账户号是匿名的,但账本内容是公开的。区块链匿名性说的是账户名匿名,不是账户中的记录。

首先,为了交易的便利性,区块链的账户(地址)标识需要一定的稳定性和一致性。又因为所有账户的内容是公开性的,交易时的IP地址是公开的,因此实际上掩盖交易身份是非常困难的。

其次,早期的区块链应用记录的是源于母体的数字货币,区块链自产自销的是原生虚拟资产。这是一个封闭的数字价值世界,不需要与物理

世界打交道就可以运转,匿名也是完全可行的。但到了区块链的2.0时代(具备智能合约和平台化等),区块链上记录和交易的不再来自区块链,而是来自物理世界的股权、版权和产权等。如果区块链上所映射的是匿名资产,从法律意义上就是无效合同。

3.3 防篡改

根据数据库理论,所有的数据库管理技术都会包含“Insert”,“Select”,“Update”和“Delete”等。但一些组织或个人把数据库所具备的“修改”能力,当作可以篡改能力来用了,导致假账频发,于是就有了区块链。它去除“Update”和“Delete”等数据库的功能,变成只能单向“Insert”和“一次性写”的数据库技术。

有人的地方就可能出现误操作,有利益的地方就可能出现欺诈;但区块链只是一种技术,认为误操作也是操作,欺诈交易也是交易,修改和篡改没什么区别。技术无法处理道德和管理层面的问题,区块链只能用下一个不可修改的操作,来弥补前一个错误操作。

区块链缺乏类似会计制度中的差错处理机制,已经带来了一些问题,例如:2016年的The DAO事件,已经让区块链陷入了程序正义还是内容正义的陷阱。

4 区块链要自证清白

不能因为一个应用系统引入了区块链,就可以相信它了。一个区块链应用系统要获得更多的信任,一是所使用的区块链要自证清白,二是区块链应用的环境也要值得信任,例如:入出链的数据和镜像关系也要自证真实性。

4.1 基础设施

区块链不是天然值得信任的。在许可链(比如联盟链和私有链)中,用户的授权和访问控制,需要由值得信任的管理员来执行。虽然无需许

可的公有链中,去掉了管理员这个角色。但无论是公有链、联盟链和私有链,都还需要信任自己的组成部分^[2]:

(1)必须信任所选用的加密技术。但是,加密算法或实现可能会有缺陷,智能合约也可能会有漏洞。

(2)必须信任所运行的软件。要祈祷程序员是个天才,所开发的软件没有BUG。

(3)必须相信用户之间不会共谋。如果一个群体或个人控制了PoW系统中51%的算力,或者PoS系统中51%的投票权,整个区块链的防篡改根本就不成立了。

(4)必须相信节点的中立性。要假设节点会公平地接受和处理每笔交易,类似于“网络中立”的法律原则,但“链中立”但还没形成标准和法律制度。

4.2 应用环境

区块链应用要依存于外部环境和整个生态。环境中的一些不可信因素,也必然会被带入到区块链的生态系统中。区块链具有防篡改能力,但只是数据已经在链上的时候。在数据写入链之前,在数据离开区块链之后,是否被篡改了,区块链都是无能为力的。

不像区块链的虚拟币是一个闭环应用,区块链上的数据在一些溯源、存证等非闭环的应用场景下,虽然是不可篡改的,但链上的数据与物理世界物品的“关联关系”不能上链,区块链可以防止篡改数据,但无法防止篡改映射关系。

5 区块链发展趋势展望

区块链技术还在持续演进中,扩展性有待进一步提升,性能还无法满

足高频交易的需要,对共识算法还没有共识,智能合约的“智商”还有待提升,新业务模式还在探索中。总的来看,区块链技术演进趋势呈现如下几个特点^[3]。

(1)架构方面:公有链和联盟链融合持续演进。联盟链是区块链现阶段主要的落地方式,但相对于公有链而言,扩展性、隐私性和社区激励还有待完善。随着应用场景趋于复杂,公有链和联盟链的架构模式开始走向融合:以面向大众的公有链做基础设施,通过隔离和加密等手段,面向企业构建基于公有链的联盟链。这种模式与业界之前的虚拟专用服务器(VPS)、虚拟专用网(VPN)、虚拟专用数据库(VPD)和虚拟专用云(VPC)等非常相像,因此可以称为“虚拟专用链(VPB)”。

(2)部署方式:区块链即服务(BaaS)加速演进。区块链的实现可以是基本传统IT的,也可以是基于云计算的。现在,越来越多的区块链开发者和用户意识到了新兴的云计算带来的好处。基于云计算搭建BaaS,不仅可以带来快速开发、敏捷部署和成本较低等优势,还可以让区块链企业将重点转向面向垂直行业,以更好地对接用户。

(3)技术层面:跨链及高性能的需求日益凸显。不同的区块链适用于不同的应用场景,跨链技术可以让区块链适于更加复杂的场景,以实现多个区块链之间的价值转移、存证和授权管理等,如金融质押、资产证券化、溯源防伪和征信等。目前典型的跨链技术,如公证人机制(Notary schemes)、侧链/中继(Sidechains/relays)、哈希锁定(Hash-locking)、分布式私钥控制(Distributed private key

control)。

(4)共识方面:共识机制从单一向混合方式演进。导致区块链性能降低的重要因素之一是共识算法。PoW、PoS、股份授权证明(DPoS)和拜占庭容错等,各据优势,各有最适用的场景。为提升效率,需在安全性、可靠性、开放性等方面进行取舍,根据场景切换共识机制成了新趋势,并且将从单一的共识机制向多类混合的共识机制演进,运行过程中支持共识机制动态切换,或系统根据当前需要自动选择相符的共识机制。

(5)智能合约方面:可插拔和易用性成为关注的重点。更具体而言:一是可插拔的执行环境架构,二是明示化的调用关系,三是可链外存储的合约代码,四是低耦合度的设计,五是完整安全的防护体系。

参考文献

- [1] 何宝宏.别拿着区块链找钉子[EB/OL].(2018-05-20)[2018-00-00]. https://mp.weixin.qq.com/mp/profile_ext?action=home&__biz=MzAxMjlyMjYxOA==&scene=126&subscene=0#wechat_redirect
- [2] ROBACK E. U.S. Department of Commerce [R]. USA:National Institute of Standards and Technology, 1990. DOI:10.13039/https://doi.org/10.13039/100000161
- [3] 中国信息通信研究院. 区块链白皮书(2018年)[R]. 北京: 中国信息通信研究, 2018

作者简介



何宝宏,毕业于中国科学院计算技术研究所,获计算机博士学位,目前担任中国信息通信研究院云计算与大数据研究所所长;从事互联网研究20余年,现主要研究方向为互联网技术哲学;出版《互联网的基因》等书。

区块链:描绘物联网安全新愿景

Blockchain: New Vision for Security of Internet of Things

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0052-004

摘要: 认为物联网(IoT)安全防护技术是保障IoT快速、健康发展的重要基础。从IoT自身的特征及局限性入手,重点剖析了区块链与IoT两种技术结合的可能性、优势及发展趋势,提出了基于区块链的去中心化IoT安全防护新思路,对其中的基于区块链的IoT系统安全检测、分布式信任机制及隐私保护进行了相关分析与探讨,指出区块链在保证IoT系统安全方面的重要意义。

关键词: 区块链; IoT; 安全防护; 去中心化管控

Abstract: It is considered that the safety protection technology of Internet of things (IoT) is an important foundation to ensure the rapid and healthy development of IoT. Starting with the characteristics and limitations of IoT, the possibility, advantages and development trends of the combination of the blockchain and IoT are analyzed emphatically. In this paper, a new idea of decentralization of IoT security protection based on blockchain is proposed. The security detection, distributed trust mechanism and privacy protection of IoT system based on blockchain are then analyzed and discussed. The importance of blockchain in ensuring the security of IoT system is finally pointed out.

Key words: blockchain; IoT; security protection; decentralized management and control

徐恪/XU Ke¹
吴波/WU Bo¹
沈蒙/SHEN Meng²

(1. 清华大学, 北京 100084;
2. 北京理工大学, 北京 100081)
(1. Tsinghua University, Beijing 100084, China;
2. Beijing Institute of Technology, Beijing 100081, China)

1 物联网技术发展现状与挑战

近年来,以智能家居、智慧城市、车联网等应用场景为代表的物联网(IoT)技术已成为新型动态网络发展的核心技术之一。从美国政府的“智慧地球”,到中国倡导的“感知中国”;从智能设备的快速发展,到网络性能的日益提升,“万物互联”已成为当前不可阻挡的趋势,也展现了

IoT在下一代互联网技术发展中举足轻重的地位。

IoT技术的愈发成熟带来用户资源与互联设备数量的爆炸式增长。2017年,IoT设备数量首次超越全球人口总数75亿,而到2020年,这个数量预计将会增长到300亿以上。届时,平均每人将具有4个左右的IoT设备,人们的生活也会朝着便利化、智能化的方向发展。

尽管市场不断扩大、业务不断增长,IoT仍处于技术发展的初期,依旧面临一系列的安全隐患,庞大的数量和自身的脆弱性使得IoT设备极易成为黑客的首选目标。电影《速度与激情8》中数以万计的智能车辆被“天眼”系统恶意操控,进而组成“僵尸车

联网”围剿国防部长;再如,2016年下半年,Mirai病毒控制超过30多万台的IoT设备对Dyn公司、OVH公司发动大规模分布式拒绝服务(DDoS)攻击,致使164个国家或地区受到影响。因此,IoT产业化的日益加速与技术的可信之间的矛盾成为该领域急需解决的重要问题,也是推动新型IoT技术发展的重要因素之一。

为解决系统面临的安全威胁,提升生态系统的安全可信,当前的IoT技术面临着诸多安全挑战,但归根结底是以下2方面的特性所致:

(1) 设备数量庞大的分布式系统。IoT系统由多种感知设备(如传感器、射频识别(RFID)等)通过网络相互连接而成。不同于当前的互联网结构,IoT包含数以亿计的网络节点,庞大的设备数量增加了安全检测的难度;不同于软件定义网络(SDN)的架构,IoT实际上是一种大型的分布式系统,去中心化的网络特征增加了IoT集中式安全管控的难度。

(2) IoT设备自身的资源受限。IoT节点主要由一些嵌入式的传感设备组成,这类设备的计算能力、存储空间和通信效率极其有限。由于这

收稿日期: 2018-10-16
网络出版日期: 2018-11-06

基金项目: 国家重点研发计划(2018YFB0803405)、国家杰出青年科学基金(61825204)、国家自然科学基金(61472212, 61602039)、欧盟CROWN基金(FP7-PEOPLE-2013-IRSES-610524)

种限制,当前互联网的诸多安全解决方案(例如:漏洞检测、流量审计、访问控制等)不能很好地迁移到IoT系统中,导致IoT设备在面对形如Mirai病毒时却无能为力,这种因设备资源受限而导致安全检测能力的降低(甚至丧失)给IoT系统的安全造成了严重的威胁。

2 基于区块链的安全防护新思路

2.1 区块链技术概述

近几年,以比特币为代表的数字货币成为众多投资者趋之若鹜的对象,它最早起源于中本聪2008年发表的一篇名为《比特币:一种点对点的电子现金系统》^[1]的论文。比特币共有2 400万个,当前已经挖出超过1 700万,预计在2040年剩余的比特币将全部挖光。2017年12月,比特币价格接近20 000美元,足见其火爆程度。姑且不论比特币是否真的具有价值,但其核心技术——区块链已经吸引了互联网、金融界足够多的眼球。简单来说,比特币是区块链的成功产物,区块链是比特币的底层技术,两者相辅相成。

从技术核心来看,区块链是一种基于密码学原理的分布式共识账本技术^[2]。从组成结构来看,区块链是由一个个区块依次连接而成,而每个区块中包含多个以默克尔树的形式组织的交易记录。严格意义上讲,区块链并不是一项新的技术,而是现有多种技术的融合。就密码学而言,区块链使用了基于SHA-256和RIPEMD-160的哈希算法、基于椭圆曲线加密的密钥生成算法和非对称加密算法;就分布式结构而言,区块链使用了基于P2P网络的通信机制与验证方式;就共识账本而言,区块链使用了基于工作量证明(PoW)、权益证明(PoS)和股份授权证明(DPoS)等共识算法的分布式存储机制。从安全角度来讲,区块链利用去

中心化的点对点(P2P)技术实现分布式共识机制,完全摆脱了传统的集中处理方式,在保证共识机制的同时,将系统的安全性提升到新的层次。

2.2 区块链与IoT结合的优势

区块链能够很好地弥补当前IoT技术在安全领域方面的缺陷,为IoT技术提供底层安全防护,推动其设备、系统和生态朝着更加安全可信的方向发展;而IoT同样能够为区块链技术的升级提供动力,使区块链能够为更多的应用场景提供安全验证与防护,如图1所示。

首先,区块链的去中心化特性与IoT的分布式结构能够较好地融合。区块链系统是一种完全的去中心化结构,不依赖于任何形式的集中式管控,这恰恰与当前IoT系统的分布式架构具有较高的契合度。基于区块链的IoT技术不仅能够依靠共识机制实现对IoT设备的分布式管控,同时还可以使用智能合约技术实现对相关感知信息的自动反馈。

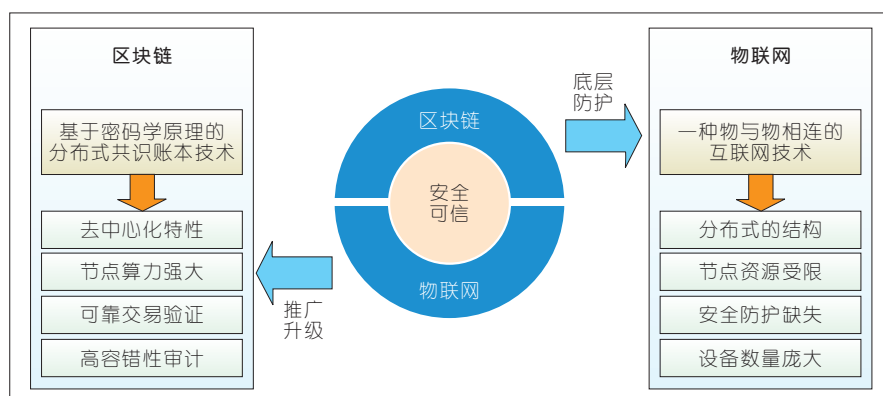
其次,区块链强大的节点算力能够较好地弥补IoT设备的资源受限。当前区块链矿工节点具有较强的算力,以比特币系统为例,目前的总算力已经超过5 500万TH/s。区块链技术能够为IoT提供较强的算力支持,设备的资源受限不再是制约IoT技术发展的关键因素,依托算力支持的安全验证等技术会进一步推动新型IoT技术朝着更加安全可信的方向发展。

再次,区块链可保证智能IoT交易的安全可信。随着人工智能领域的异军突起,IoT技术也朝着智能化的方向发展,智能化设备将满足更加人性化的需求,而价值互连与智能传输将会成为新型IoT技术的一大特色。基于区块链的去中心IoT安全增强技术将极大程度地保障智能设备间交易的安全性,防范双花攻击与恶意欺诈,推动IoT智能经济的健康稳定发展。

最后,基于区块链的去中心化安全基础设施能够对庞大数量的IoT设备进行安全审计与验证。区块链可以作为去中心化的安全基础设施为新型IoT技术的发展提供真实可信的安全保障,基于区块链的IoT技术具有较强的容错性,保证只有少数设备发生故障或被恶意控制时依然保持健壮性。去中心化的安全基础设施能够对数以亿计的IoT设备进行安全验证与审计,有利于增强IoT系统抵御攻击的能力,提升生态安全性。

在未来几年,IoT的规模将变得更加庞大,设备也会变得更加智能化、人性化和多元化;同时,安全性与隐私性也会逐渐成为IoT用户的迫切需求。如何提升IoT设备抵御恶意攻击的能力,如何保证IoT用户的隐私不受侵害,如何增强IoT生态中智能化交易的安全性等都成为新型IoT技术需要解决的难题。

区块链的去中心化特征与内生的安全防护属性能够很好地弥补当



▲图1 区块链与物联网技术

前 IoT 技术的缺陷,有助于推动新型 IoT 安全增强技术的发展。一方面,基于区块链的去中心化安全基础设施可以增强对 IoT 系统的安全监测控制能力,提升系统的对恶意行为的抵抗力,保障系统的安全可信;另一方面,基于共识机制的分布式管控可以保证 IoT 策略与行为验证的一致性,提升系统的容错力,保障系统的健壮性。由此可见:IoT 与区块链技术的融合将会是未来发展的一种趋势。

3 基于区块链的去中心化 IoT 安全防护系统

区块链技术可以为 IoT 提供较强的安全防护。首先,区块链内生的激励机制可以吸引更多的安全服务商加入到 IoT 系统的检测中来,有利于形成更加系统权威的检测报告;其次,区块链衍生的大规模去中心化系统可以为 IoT 提供分布式信任机制,保障 IoT 跨域互联互通的安全性;最后,区块链自身的隐私防护特性可使得 IoT 智能交易更具匿名性,有效地保护用户的隐私信息不受侵害。

3.1 基于区块链的 IoT 系统安全检测

当前 IoT 系统面临较大的安全威胁,其主要原因在于 IoT 设备中的高危漏洞。而设备旧化、系统防护较弱、安全设计缺失等问题都是众多安全漏洞频现的原因,这导致 IoT 系统在面对网络攻击时表现得不堪一击。针对上述问题,多数 IoT 厂商通过修复漏洞、更新版本的方式来提升系统的安全可信,但这也引入了 2 个问题:系统版本的更新可能引入新的未知漏洞;集中式的安全厂商由于检测能力的差异并不一定能发现所有的漏洞^[9]。

如图 2 所示,基于区块链的 IoT 系统安全检测技术可实现以下几方面的优势:(1)通过创建激励机制可吸引众多检测者参与到 IoT 系统的检测中来,基于多方协同检测的安全增强技术可以较为容易地获得完整、全

面的检测结果;(2)通过创建惩罚机制可进一步约束 IoT 厂商的行为,恶意系统的发布会致使相关厂商受到相应的制裁;(3)通过创建公开透明的检测结果账本可较好地指引 IoT 设备对系统安装的选择,安全级别更高的系统更容易得到普及。这样,IoT 系统中出现漏洞的概率大大减小,也有利于创建更加安全可信的 IoT 生态系统。

3.2 基于区块链的 IoT 分布式信任机制

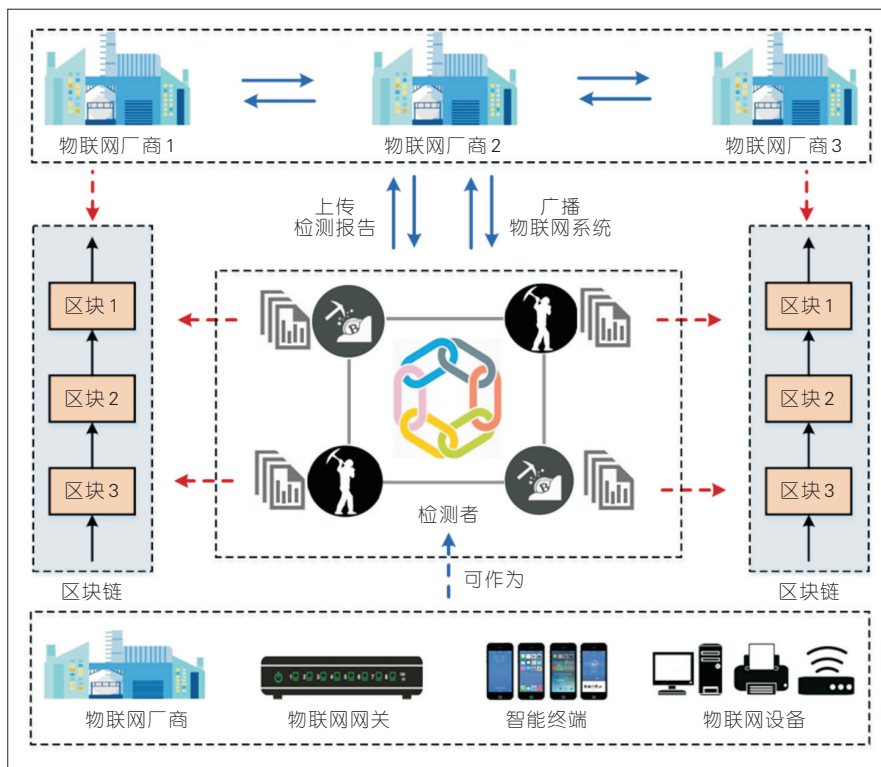
当前 IoT 系统普遍存在多个管理域,如智慧小区、智慧学校、智慧医院等,出于安全考虑,不同管理域之间是彼此“绝缘”的,如何实现 IoT 跨域的互联互通及相关安全协议的研究成为新型 IoT 安全增强技术的重要目标之一。

IoT 更高级别的安全防护都是以密码学为基础的,而当前安全密钥的创建与分发都是过度依赖集中式的基础设施,而这类设施极易成为黑客攻击的首选目标,成为威胁 IoT 系统

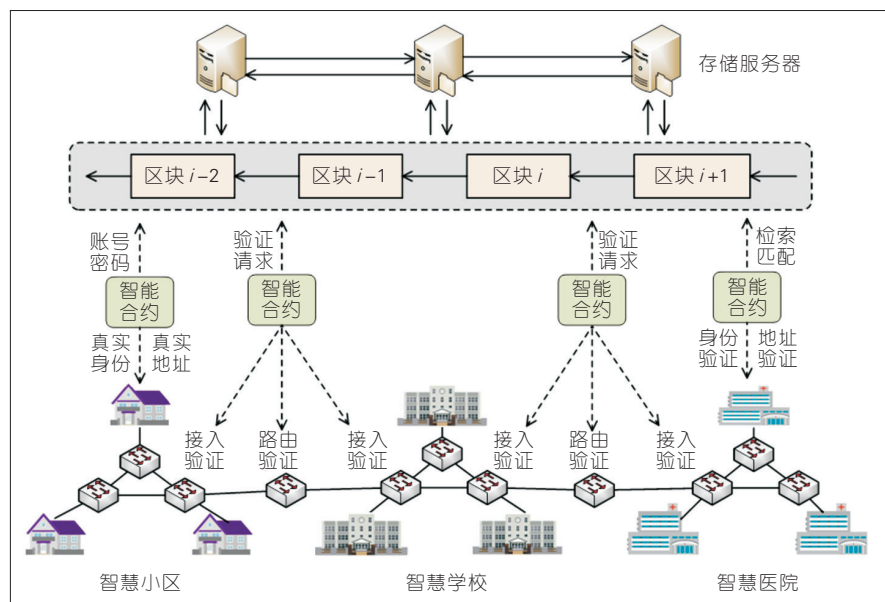
安全的重要因素。基于区块链的去中心化密钥基础设施可以更好地保障系统密钥的安全,为 IoT 密钥的创建、管理和分发提供鲁棒性更强、容错率更高的安全保障。

真实身份与真实地址是实现 IoT 互联互通的关键因素,而当前身份伪造、地址哄骗等都是造成信息泄露、隐私窃取的重要原因。如图 3 所示,针对 IoT 的大规模分布式异构问题,基于区块链的去中心化真实身份与真实地址生成与验证技术可以有效地保证 IoT 设备的真实性,有利于防止跨域用户的越权访问,降低数据隐私泄露的风险,也为 IoT 互联互通提供重要的安全保障。

IoT 系统策略的安全性是保障其正确运行的重要基础,也是各类 IoT 设备行为一致性验证的重要前提,而基于 SDN 架构的安全策略分发已不再适应日益扩大的 IoT 规模。相比较而言,基于区块链的 IoT 去中心化安全管控不仅能够实现庞大 IoT 设备数量下安全策略的分发,更能为异构



▲图 2 基于区块链的物联网系统安全验证技术



▲图3 基于区块链的去中心化信任机制

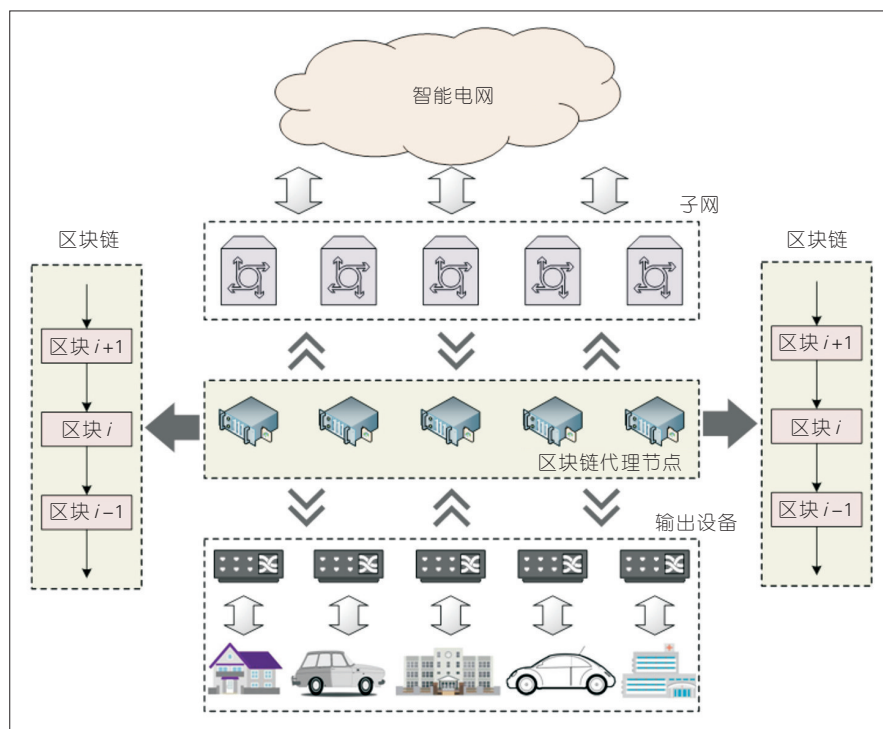
IoT系统提供较高的容错性,是新型IoT技术发展的一个很好趋势。

3.3 基于区块链的IoT匿名支付隐私保护方案

IoT的智能化趋势势必会带来频繁的交易行为,而基于这类交易的隐私泄露也给IoT用户带来一定的安全隐患^[3]。以智慧小区为例,供电公司可以轻易地获取每个家庭的用电记录,进而推测出业主的用电规律、用电行为等隐私信息;再如,车联网中电动汽车的充电记录也会暴露车主的驾车习惯、行车轨迹等私密信息。仔细分析不难发现,隐藏交易记录是不现实的,因为供电机构无法确认应该给哪个家庭或电车供电;所以,最有效的方式应该是隐藏用户的身份标识信息。借助区块链技术的节点标识策略,基于区块链的IoT匿名支付方案将有利于防止各类交易信息中用户隐私的泄露,将IoT的安全防护提升至一个新的台阶。

为了实现上述的IoT匿名支付方案,可在IoT支付双方(即供给方与需求方)之间引入区块链代理节点。以智能电网供电为例,如图4所示,无论是家庭业主还是电动车车主,都

具备独一无二的加密身份标识,而该标识不能反映其他信息。当业主或车主向智能电网购买电力资源时,双方的交易信息通过区块链代理节点进行确认。在此期间,智能电网无法识别业主或车主的身份,因为它只需向对应的电力输出设备供电即可。



▲图4 基于区块链的物联网匿名支付方案

在这种情况下,IoT用户的身份信息、用电规律、驾车习惯等隐私在没有暴露给智能电网的同时,仍然有效地获取了电力资源。

4 区块链与IoT技术融合的挑战与趋势

虽然IoT与区块链技术在各自的领域已经得到快速发展,但2种技术的融合仍然面临很多的挑战,总结起来主要有以下几个方面:

(1)效率问题。基于区块链的新型IoT安全增强技术主要依赖区块链作为分布式账本来存储各类IoT信息,而区块时间和共识效率将会是制约数据存储、安全验证、信息获取等的效率的关键因素。

(2)存储问题。以比特币为例,当前矿工针对交易记录的存储已经达到100 G以上,而拥有大量设备的IoT势必需要更多的存储空间才能容纳各类交易记录、验证结果等信息。

(3)资源浪费问题。仅就比特币、以太坊而言,每年挖矿所消耗的

►下转第64页

NG-PON 技术背景、应用和展望

The Technical Background, Application and Prospect of NG-PON

陈爱民/CHEN Aimin

(中兴通讯股份有限公司, 广东 深圳 518057)
(ZTE Corporation, Shenzhen 518057, China)

1 技术背景

宽带网络已经成为各国信息化的战略性公共基础设施, 宽带光接入网具有投资大、建设周期长、网络复杂的突出特点, 是宽带网络的重要组成部分。随着云计算、高清视频等新业务网络的迅猛发展, 用户带宽以每 5~6 年 10 倍速度增长, 面对用户对带宽不断增加的市场需求, 当前运营商已经开始规模部署 10 G 无源光纤网络 (PON), 为用户提供高带宽业务。其中, 住宅用户带宽将会达到 1 Gbit/s, 企业用户带宽超过 1 Gbit/s。未来随着增强现实 (AR)/虚拟现实 (VR) 业务的加速应用, 运营商计划采用下一代 (NG)-PON 技术为每个用户提供最高 10 Gbit/s 带宽。同时随着 5G 时代的到来, 高频基站的导入导致基站密度将大为增加, 基于同一光纤接入 (FTTX) 光配线网 (ODN), 实现 5G 前传或回传的统一承载。NG-PON 由于节省了大量光纤资源, 成为运营商研究热点。

宽带接入网是一个点到多点的网络架构, PON 技术是主流宽带的网络架构, PON 技术是主流宽带的重要接入技术, PON 网络技术已经历了

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0056-004

摘要: 10 G 无源光纤网络 (PON) 标准已成熟多年, 并逐步进入规模商用。随着增强现实 (AR)/虚拟现实 (VR) 等技术应用及 5G 时代的到来, 使得建设固移融合 (FMC) 的光接入网成为趋势, 并且对 PON 技术未来带宽和时延等提出了更高的要求。下一代 (NG)-PON 有单波长提速和多波长叠加 2 个技术路径。认为 NG-PON 已成为研究热点, 运营商、设备商及标准组织都在该领域积极投入。NG-PON 将有着广阔的应用前景。

关键词: 10 G PON; FMC; NG-PON; 50 G PON; 波分复用 (WDM)-PON

Abstract: 10 G passive optical network (PON) standard has matured and commercialized. With the application of augmented reality (AR), virtual reality (VR), and the arrival of 5G era, the constructing of the optical access network of fixed and mobile convergence (FMC) has become a trend, and higher requirements for the future bandwidth and delay of PON technology are needed. Two technical paths are considered in next-generation (NG)-PON: single wavelength speed increase and multi wavelength stacking. NG-PON technology which operators, equipment providers and standard organizations are actively invested in, has become a research hotspot, and will have a broad application prospects.

Key words: 10 G PON; FMC; NG-PON; 50 G PON; wavelength division multiplexing (WDM)-PON

从以太网无源光网络 (EPON) 和吉比特无源光网 (GPON) 到 10 G PON 的发展历程。随着 AR/VR 和 5G 技术的加速发展, 10 G PON 技术也难以满足未来的驻地接入和移动前传/回传的带宽需求, 因此下一代更高速率的 PON 技术正逐步成为业界研究热点。

2 技术进展

从技术路线角度看, NG-PON 分成单波长提速和多波长叠加 2 条路线演进, 具体如图 1 所示。对于下一代单波长提速技术路线, 考虑到当前产业链现状以及未来低成本规模商用, 基于 25 Gbit/s 基础速率可以复用现在数据中心 25 G/100 G 以太网产

业链, 并可以通过高阶调制技术实现 50 Gbit/s 的速率。对于有更高带宽的需求, 可以采用多波长的叠加方式扩展实现。一些特殊高带宽和低延迟需求 (如 5G 前传) 可以采用密集波分复用 (WDM)-PON 方式, 其中每个通道实现了点对点 (P2P) 直连。当前电气和电子工程师协会 (IEEE) 和国际电信联盟电信标准分局 (ITU-T) 就是基于这个思路演进^[1]。

其中, IEEE 率先启动了 NG-PON 技术的标准制定, 单根光纤上支持 25 Gbit/s 下行速率, 同时也可以支持 10 Gbit/s 或 25 Gbit/s 的上行速率, 并且可以和 10 G EPON 兼容。而对于 50 Gbit/s 需求带宽, 采用多波长叠加

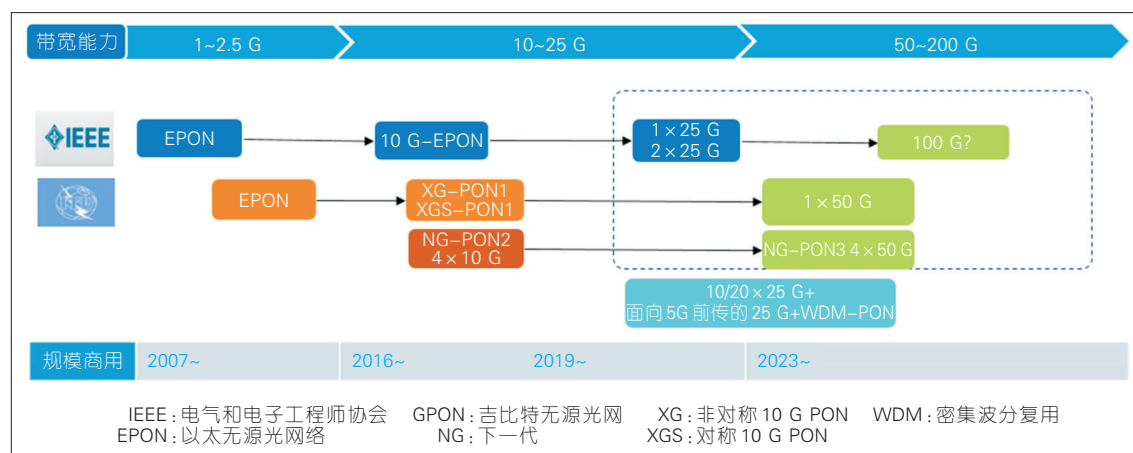


图1
无源光纤网络技术
演进趋势示意图

技术和通道绑定技术可以提供 2 个 25 Gbit/s 通道, 实现 50 Gbit/s 带宽, 其标准预计 2019 年中提交发布。

同时, ITU-T 也在考虑 10 G PON (XG-PON1 和 XGS-PON) 后的技术。基于前期 G.sup.hsp 后 10 G PON 技术研究白皮书, 并考虑了家庭用户、企业用户、移动回传和前传的需求, 运营商和设备商等产业链逐步形成了对于 NG-PON 的需求, 于 2018 年 1 月立项了 50 G PON 的相关标准, 同时立项的还有基于多波长叠加的 NG-PON2 下一代, 其中每个通道的速率约为 50 Gbit/s。

3 应用场景

NG-PON 将极大地扩展 PON 技术的应用领域, 为各类用户提供低成本、高带宽的接入业务。当前 NG-PON 聚焦在固网新业务挖掘和 5G 承载新领域的扩展, 具体包括:

- (1) AR/VR 高带宽应用;
- (2) 5G 回传业务;
- (3) 5G 前传业务。

AR/VR 技术对于带宽有着极高要求, 以 VR 技术为例 (具体如表 1 所示), 进入规模商用阶段的高级 VR, 带宽需要近 500 Mbit/s, 依照 1:64 分光比计算, 即使考虑实际用户并发率, 10 G PON 也难以满足要求; 而对于极致级 VR 的 1 G 带宽需求, 则需要 PON 口带宽近 50 Gbit/s。另外, 还对 NG-PON 的带宽演进提出了明确

表 1 VR 几个阶段带宽需求表

指标	入门级 VR	高级 VR	极致级 VR
连续体验时间/min	小于 20	20 ~ 60	大于 60
帧率	30	60	120
分辨率	480 P	2 K	4 K
色深	8	10	12
带宽需求	100 Mbit/s	近 500 Mbit/s	1 Gbit/s

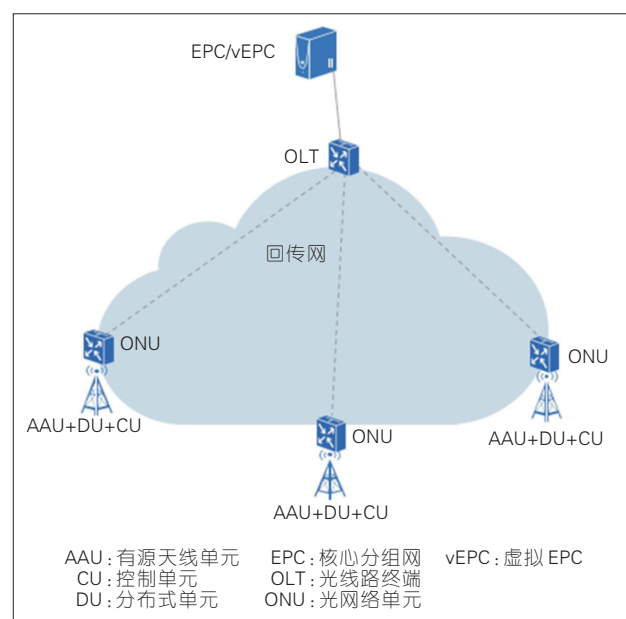
VR: 虚拟现实

的需求。

5G 基站回传组网如图 2 所示, 其对于带宽需求远远大于 4G 基站, 单站回传带宽需求从 4G 的数百兆到 Sub6G 低频 5G 基站的近 5 Gbit/s, 高频基站要大于 10 G。依照正常 PON 回传应用的分光比 1:8 来计算, 需要

至少大于 40 Gbit/s 以上带宽, 这就需要 NG-PON 来满足 5G 的带宽需求。为此, 下一代单波 50 G PON 技术可以承载 Sub6G 的低频 5G 基站回传, NG-PON2 可以支持大于 100 Gbit/s 带宽, 用于高频 5G 基站回传。同时, 5G 业务对延迟要求更高, 增强型移动带

图2
无源光纤网络无线回传
场景



宽(eMMB)需要1~4 ms,高可靠超低时延通信(uRLLC)业务需要0.5 ms。相比现在10 G PON,NG-PON在动态带宽分配(DBA)方面会进一步优化,满足5G低时延业务的要求^[2]。

如图3所示,对于5G前传,WDM-PON技术基于FTTX ODN的点多点树型网络拓扑,实现了单纤10~20通道的密集波分,能大量节省光纤布线资源,且每个通道提供25~50 Gbit/s的带宽,满足5G前传通用公共无线电接口(eCPRI)的带宽需求。对于采用集中化无线接入(C-RAN)架构,需要在城区实现5G基站密集连续覆盖,同时骨干光纤资源非常紧张的场景,WDM-PON是一个非常合适的技术。

4 关键技术

NG-PON技术中单波长提速技术路线沿用现在TDM-PON技术,具有下行广播连续发送和上行时分多址突发传输的特点,其主要关键技术包括调制技术、光模块大功率收发技术、高性能前向纠错码(FEC)、突发接收、超低延时转发等技术。对于多波长叠加技术路线,尤其是WDM-

PON技术,其核心技术聚焦于无色ONU技术。

4.1 调制技术

关于50 G PON调制方案,目前业界仍在研究中,具体包括不归零码(NRZ)、NRZ+均衡和四级电平脉冲幅度调制(PAM4)等。为了更好地实现50 Gbit/s速率,NRZ需要50 Gbit/s的速率器件,当前产业链不够成熟。NRZ+均衡和PAM4基于25 Gbit/s速率器件,器件相对成熟,是50 G PON调制技术的研究热点。

4.2 光模块大功率收发技术

PON已经历了好几代技术变革,ODN网络也已基本完成部署,功率预算达到32 dB。50 G PON需要兼容已有ODN网络,功率预算是重大挑战。数据中心使用25 G激光器,其发射光功率在0 dBm左右,不能满足32 dB光功率预算要求。25 G雪崩光电二极管(APD)接收50 G PAM4时的接收灵敏度大约为-20 dBm @1E-3,通过均衡补偿高频响应。虽然当前灵敏度有所改善,但要满足32 dB功率预算仍存在挑战,需要产业链进行

突破。

4.3 高速突发接收技术

PON系统上行采用突发机制,不同ONU占用不同时间隙突发发射,光线路终端(OLT)接收机需要突发跨阻放大器(TIA)快速建立工作电平,并需要突发模式时钟与数据恢复(BCDR)快速恢复时钟,才能正确接收信号。目前还没有针对50 G PON应用的突发TIA和BCDR,需要产业链加大研究。

4.4 高性能FEC技术

高性能FEC是为了解决功率预算问题而提出新技术方向。目前PON采用的是冗余度为7%左右的里所码(RS)编码,能够将1E-3误码纠正到1E-12。低密度奇偶校验码(LDPC)、Turbo乘积码(TPC)、Polar码等高性能FEC技术可以将1E-2误码率纠正到1E-12以下,但需要更高的编码冗余、更高计算复杂度和更大的处理时延。

4.5 超低延迟转发

当前GPON/XG(S)-PON技术存在

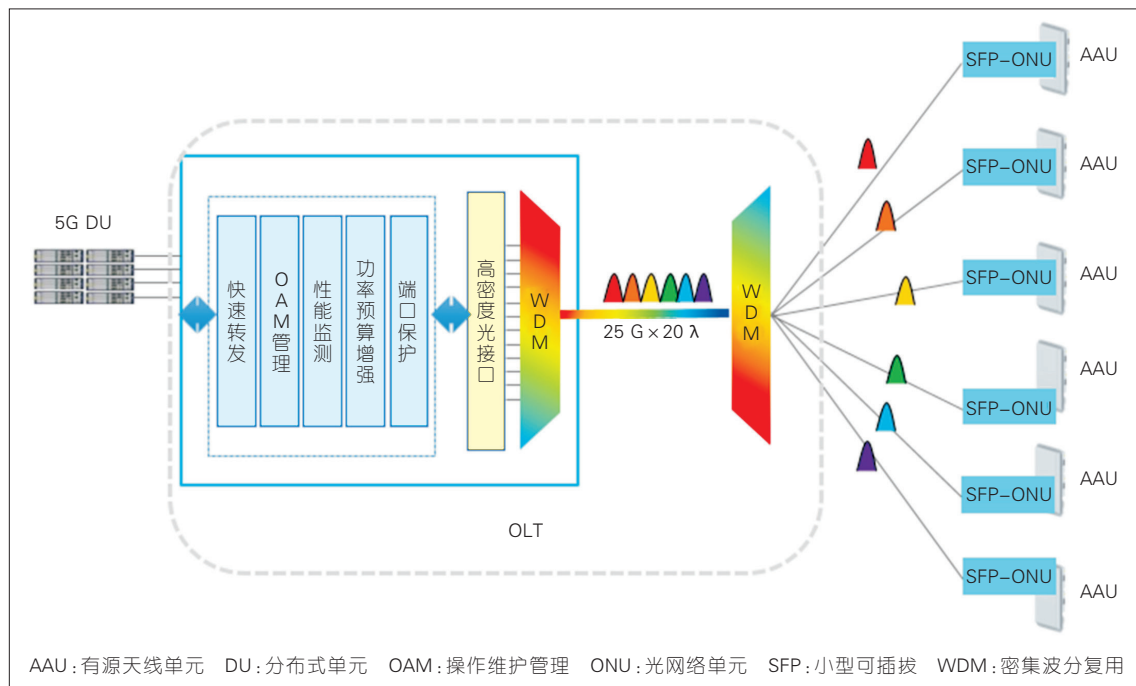


图3
25 G WDM-PON 5G
前传场景

上行转发时延过长的问题,主要原因是:PON 数据依照 125 us 周期进行传输,一般 DBA 调度在 4 个周期左右。考虑到数据包分片,如果不做特殊处理,上行时延将达到 1 ms,这样不能满足 5G 回传对接入段最低数百微秒的时延要求。同时,ONU 开窗发现需要 PON 下面所有 ONU 在较长时间内停止数据传输,导致时延达到数个毫秒以上,从而使得时延和抖动更加恶劣。NG-PON 技术将在数据转发延迟和 ONU 开窗发现这 2 个方面做深入优化,满足 5G 回传的要求。

4.6 无色 ONU 技术

作为 WDM-PON 系统的关键技术,无色 ONU 一般采用波长可调 ONU 技术方案,该方案采用可调谐激光器,实现在 ONU 侧波长的灵活配置。激光器波长调谐采用电流调谐、温度调谐或微机械调谐等方式来改变增益介质折射率或者外腔反馈条件,以保证每一个 ONU 均工作在特定波长上。直接调制可调谐激光器速率可达 10 Gbit/s,与外调制器集成时能实现 25 Gbit/s 速率传输。波长可调方案部署方式灵活,带宽可扩展性高,光信号质量高,利于长距离传

输,是应用最为成熟的无色 ONU 技术方案。目前业界有多种已商用的可调激光器技术方案,如:分布布拉格反射激光器(DBR)、数字超模 DBR 激光器(DS-DBR)、采样光栅 DBR 激光器(SG-DBR)、外腔激光器(ECL)等。当前可调激光器成本过高,影响规模商用,同时对于 5G 前传的应用场景,还面临着功耗和工作温度范围挑战,对模块自身温度控制提出了较高的要求。

5 结束语

庞大的 FTTX ODN 光纤资源是运营商的巨大财富,充分利用这个资源实现用户接入的低成本/高带宽/低延迟普遍覆盖,满足各种业务的服务质量,是 NG-PON 的主要目标。NG-PON 技术将实现现有 PON 技术在同一个 ODN 下共存,不仅满足当前普通家宽业务,还可以提供满足 AR/VR 应用的更高带宽家宽业务、更高带宽/低延迟的企业业务,还可以实现 5G 基站回传和前传。NG-PON 技术面向这些未来应用,以更高速率、更低时延、更低成本和功耗等为技术目标。标准组织、运营商和设备厂家以及产业链各个方面都在积极努力,以

实现 NG-PON 技术的早日成熟。由于 5G 时代的到来,预计 25 G WDM-PON 技术将在 2020 年左右实现规模商用,下一代单波 50 G PON 将在 2023 年产生商用产品,开始试商用,2025 年进入规模商用。下一代 PON 技术的应用必将有利于促进未来固移融合新一代光接入网的规模建设。

参考文献

- [1] 黄新钢. 单波 50G PON 实现和应用前景分析[J]. 中兴通讯技术简讯, 2018, (7): 27-29
- [2] 李玉峰. 25G WDM-PON 承载 5G 前传的技术研究[J]. 中兴通讯技术简讯, 2018, (7): 5-7

作者简介



陈爱民,中兴通讯股份有限公司固网产品线光接入规划总工;现负责新一代 OLT 产品和解决方案的规划,自 1998 年进入中兴通讯以来,先后从事光传输产品、BRAS 产品、DSLAM 产品和光接入 OLT 产品研发和商用规模交付工作,历任软件开发工程师、软件开发组长、系统研发工程师、项目经理、研发总工;先后参与“863”计划“光接入网络演进技术研究”与示范、“光纤同轴混合接入系统演进技术研究”等多项国家和地方项目课题,负责项目的光接入系统架构设计,并多次获得奖励。

专题预告

《中兴通讯技术》2019 年专题计划

期次	专题名称	策划人
1	5G 商用支撑理论及关键技术	中兴通讯股份有限公司 CTO 王喜瑜
2	云网一体化技术	中国联通网络技术研究院首席专家 唐雄燕
3	边缘计算技术及其应用	清华大学教授 郑伟民 佐治亚州立大学教授 潘毅
4	5G 通信安全技术	清华大学教授 李军
5	新型光互连与光接入技术	北京大学教授 李红滨
6	5G 通信系统示范应用	中国信息通信研究院科技委主任 蒋林涛

基于BGP的域间二维路由方案

A Design of Inter-Domain Destination and Source Routing Based on BGP

中图分类号: TN929.5 文献标志码: A 文章编号: 1009-6868 (2018) 06-0060-05

摘要: 提出了基于边界网关协议(BGP)的域间二维路由方案。该方案在进行路由决策时同时考虑目的地址和源地址,实现灵活和细粒度的流量控制。给出了二维路由的部分应用场景,设计了二维路由的控制层,修改了部分报文格式用来传递二维路由信息,同时保证二维路由与传统路由的兼容;还给出了二维转发表的方案,解决二维转发匹配造成的三态内容寻址存储器(TCAM)空间爆炸的问题。

关键词: 域间二维路由;源地址;报文设计;二维转发表

Abstract: In this paper, an inter-domain destination and source routing scheme based on border gateway protocol (BGP) is proposed. This scheme makes routing decisions considering both destination address and source address, which achieves flexible and fine-grained flow control. Some application scenarios of the scheme are presented. The control layer of the scheme is designed. Some message formats are modified to transfer two-dimensional routing information, and they are compatible with the traditional routing protocol. A practical design of two-dimensional forwarding table is then given, and the problem of ternary content addressable memory (TCAM) space explosion caused by two-dimensional matching is solved.

Key words: inter-domain destination routing; source address; message field design; two-dimensional forwarding table

耿男/GENG Nan¹
金飞蔡/JIN Feicai²
徐明伟/XU Mingwei¹

(1. 清华大学, 北京 100084;
2. 中兴通讯股份有限公司, 广东 深圳 518057)
(1. Tsinghua University, Beijing 100084, China;
2. ZTE Corporation, Shenzhen 518057, China)

由于互联网发展的历史原因,以传输控制协议(TCP)/网际协议(IP)为核心的互联网模型将“尽力而为”的可达性作为网络的首要任务,这使得报文携带的目的地址在路由过程中成为了唯一的决定因素。这种仅依靠目的地址的路由方式,大大限制了对报文转发控制的灵活性。并且随着互联网规模的迅速增长和用户业务的多样化,传统路由协议越来越难以满足许多业务对服务质量

的要求。

陆续出现的多协议标签交换(MPLS)^[1]、软件定义网络(SDN)^[2]等技术,试图寻找除目的地址之外的新的路由计算维度。MPLS通过标签交换提前建立好一条专门的转发路径,指定的流量可以按照MPLS建立的路径进行传输,然而这种源路由方式存在的安全性差、复杂性高以及开销大等问题,使得网络服务提供商(ISP)部署MPLS的积极性不高。SDN彻底解放了路由计算维度的限制,最新的OpenFlow协议^[3]支持44个匹配域,能够实现对网络流量的精细控制;但是这也造成了SDN流表空间爆炸的问题,使得SDN扩展性不高,另外集中式控制方式降低了网络的鲁棒性,因

而广泛部署SDN仍是一个很漫长的过程^[4]。

域间路由是互联网路由体系结构的重要组成部分,自治系统(AS)之间构成的域间路由具有管控难度大、路由因素复杂等特点。由于可扩展性等原因,MPLS、SDN等方案在域间难以实际部署,当前广泛应用的域间路由协议仍然是边界网关协议(BGP)^[5],那么能否在传统BGP的基础上,实现更加灵活的转发控制?

本文设计了一种基于BGP的域间二维路由方案,其在进行路由决策的时候,不仅仅考虑目的地址,而且考虑了源地址,这一思想弥补了传统BGP中源地址语义缺失的问题,可以实现对网络流量更加细粒度的控制,为满足用户和ISP的多样化需求提供了新的解决方案。整个方案包括控制层和数据层,控制层主要是协议设计,基于现有的多协议BGP(MP-BGP)^[6]进行扩展,实现二维路由信息的传递、管理和使用,并保证二维路由协议与传统路由协议的兼容性;数据层面主要是给出了支持二维匹配域的转发表结构方案,并进行了存储

收稿日期: 2018-09-23

网络出版日期: 2018-11-13

基金项目: 国家自然科学基金(61625203)、国家重点研发计划(2017YFB0803202, 2016YFC0901605)、北京市科技计划项目(Z171100005217001)

空间压缩。

1 二维路由简介

1.1 二维路由的概念

二维路由是一种新型路由协议,它在进行路由决策的时候,不仅仅考虑目的地址,还要考虑源地址。传统路由协议中,去往相同目的地址的报文的下一跳往往是相同的(不考虑等价多路径);但是在二维路由中,目的地址相同、源地址不相同的报文的下一跳可能不同。二维路由的这种特性带来2方面的好处:一是流量控制的粒度变细,网络管理者可以更加灵活地管理网络,如进行流量调度、策略路由等;二是用户的多样化需求可以被更好地满足,例如:享受专门的转发通道等。

本文介绍的是基于BGP的域间二维路由设计方案,它可以利用路径属性(如本地优先级和多出口分辨器)实现二维路由策略。简单来说,域间二维路由为所有可达的目的地址前缀设置一套默认的路径属性,然后再为<目的地址前缀,源地址前缀>这样的前缀对儿设置专门的路径属性,这种设置只作用于对应的前缀对儿,这样就可以生成一条区别于默认方式的转发路径。

1.2 域间二维路由的应用场景

本节通过2个例子来展示文中提出的域间二维路由的应用场景,每个场景都用域间二维路由来解决传统网络遇到的难题。

图1所示是一个多宿主场景,一个站点同时与2个上游ISP相连接,分别用ISP₀和ISP₁表示。其中ISP₀为该站点分配地址前缀为P₀的地址,ISP₁为该站点分配地址前缀为P₁的地址,因而网络中的终端系统具有2个地址,其中地址A属于P₀,地址B属于P₁。在传统的路由协议中,对于去往同一个目的地址的报文,无论终端系统使用地址A或是B作为源地址,

其都将会被转发至同一个上游ISP,假设是ISP₀,此时,如果ISP₀实施了源地址过滤机制,则有可能将来自源地址B的报文过滤掉,从而造成丢包。使用域间二维路由,可以根据报文的源地址选择合适的出口路由,即来自源地址P₀的报文将会通过路由器E₀转发至ISP₀,来自源地址P₁的报文将会通过路由器E₁转发至ISP₁,从而保证了多宿主环境下正常的数据通信。

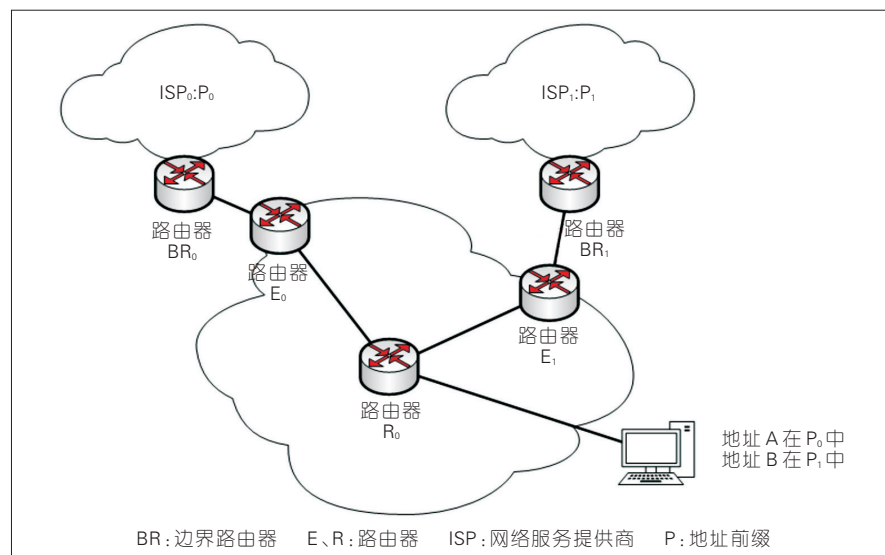
图2所示是一个负载均衡场景,网络中有2个源端AS,分别带有地址前缀P_{s1}和P_{s2},还有1个目的端AS,带有地址前缀P_d,源端AS和目的端AS通过中间的ISP相连。默认情况下,2个源端AS发出的报文可能选择了同一个ISP出口,如路由器E₂,这样可能

会造成与E₂相关联的设备或链路负载比较重,而E₃则负载很轻,出现了网络负载不均衡的情况。负载不均衡会造成网络应对突发问题的容忍性下降、资源利用率降低等问题。使用域间二维路由,可以区分报文的源地址,为不同的源端AS选择不同的出口路由,比如源前缀为P_{s1}的报文通过E₂到达目的端AS,源前缀为P_{s2}的报文通过E₃到达目的端AS,从而实现负载均衡。

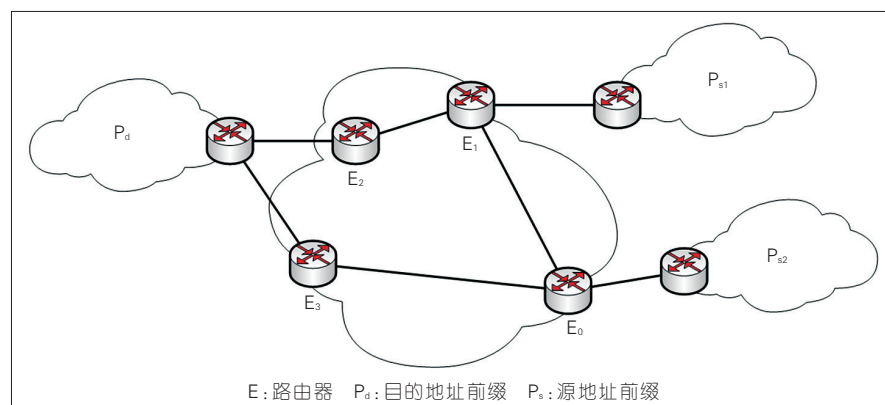
2 域间二维路由协议设计

2.1 基于BGP的二维路由动态学习过程

传统的BGP是通过4种报文完成



▲ 图1 多宿主环境下的域间二维路由应用



▲ 图2 负载均衡场景下的域间二维路由应用

路由信息交互的,分别为:OPEN、KEEPALIVE、UPDATE 和 NOTIFICATION。假设路由器 A 向路由器 B 已经建立了 TCP 链接,此时路由器 A 向路由器 B 发送 OPEN 报文,携带自己的协议版本等信息,如果路由器 A 在约定时间内(计时器计时)收到路由器 B 返回的 OPEN 报文,路由器 A 就会向路由器 B 发送 KEEPALIVE 报文保持刚刚建立的连接。如果在另一约定时间内路由器 A 收到对端发送的 KEEPALIVE 报文,则进入 ESTABLISHED 状态,在此状态下两个路由器可以任意传送 UPDATE 报文来更新路由或者撤销路由。整个过程中,路由器可以通过 NOTIFICATION 报文报告可能出现的错误信息。

基于 BGP 的二维路由协议与传统 BGP 的信息交互过程一样,只不过需要对信息交互报文进行必要的扩展,使其能够支持二维路由相关信息的传递。另外为了能够支持二维路由的增量部署,在设计 BGP 二维路由协议的时候,需要保证二维路由协议与传统路由协议的兼容。在本文中,我们是基于 MP-BGP 实现的域间二维路由协议。

域间二维路由器建立协议连接时,会向对端路由器其发送携带二维路由标识的 OPEN 报文。如果对端路由器支持域间二维路由则回复携带有相同标识的 OPEN 报文,如果对端路由器不支持二维路由即无法识别标识信息,则返回常规的 OPEN 报文。发起连接的域间二维路由器会根据返回的 OPEN 报文是否携带特定标识来识别和记录对端路由器是否支持二维路由,将来二维路由相关信息只会发给建立连接的二维路由器,而不会发给传统路由器。

进入 ESTABLISHED 状态后,域间二维路由器间使用 UPDATE 报文传递网络层可达信息(NLRI),该信息位于 MP-BGP 的可选属性 MP_REACH_NLRI 和

MP_UNREACH_NLRI 的 NLRI 字段,域间二维路由扩展了该字段使其除了包含目的地址信息外,还包含源地址信息。与传统 MP-BGP 类似,MP_REACH_NLRI 负责携带二维路由更新信息,MP_UNREACH_NLRI 负责携带二维路由撤回信息。

需要说明的是:域间二维路由在引入地址信息的时候,默认引入传统路由协议中的所有一维网络层可达信息,即目的地址信息,来保证最基本的可达性,在此基础上可以通过路由器指令等方式引入二维的网络层可达信息,实现进一步的二维路由策略。域间二维路由协议的选路规则同传统 BGP 相同,传统 BGP 的属性例如本地优先级等在域间二维路由协议中同样适用。此外,当需要使用 AGGREGATOR 等属性进行路由聚合的时候,只聚合目的地址而不用不聚合源地址^[7]。

2.2 基于 BGP 的二维路由的报文设计

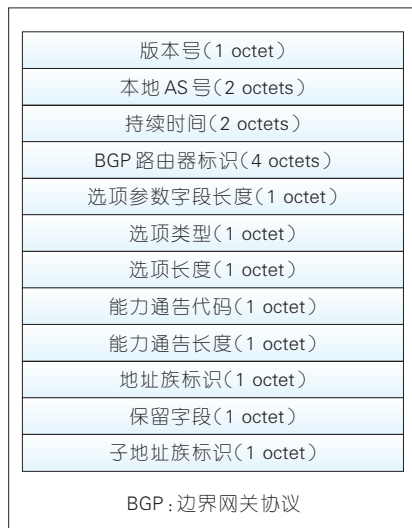
域间二维路由协议的报文设计主要是涉及 OPEN 报文和 UPDATE 报文,剩余的 KEEPALIVE 报文和 NOTIFICATION 报文不做修改,保持与传统路由协议一致。

2.2.1 域间二维路由协议 OPEN 报文

域间二维路由协议的 OPEN 报文跟原始的 OPEN 报文结构基本一致,不同点在于前者需要通过可选参数字段携带二维路由标识。本文中我们通过定义新的子地址族标识来作为二维路由标识,子地址族标识位于报文可选参数部分 Capability 属性包含的多协议扩展字段,具体携带方式如图 3 所示。该标识的具体数值需要向互联网数字分配机构(IANA)进行申请。

2.2.2 域间二维路由协议 UPDATE 报文

域间二维路由协议的 UPDATE 报文用于通知对端路由器有新的路由

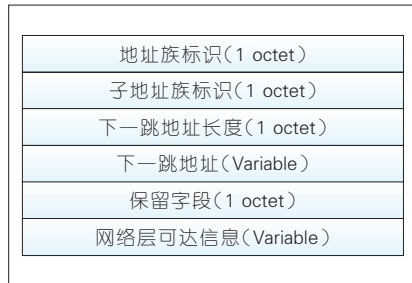


▲图 3 域间二维路由的 OPEN 报文结构图

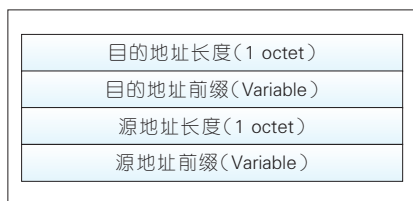
条目需要更新和撤销,协议格式同 MP-BGP 类似。域间二维路由协议使用可选属性 MP_REACH_NLRI 更新路由,使用可选属性 MP_UNREACH_NLRI 撤销路由,其中可选属性 MP_REACH_NLRI 字段结构如图 4 所示,其子地址族标识需要使用同 OPEN 报文一样的二维路由标识,另外其包含的 NLRI 字段(即图 4 中网络层可达信息字段)需要进行扩展。原始的 NLRI 字段只存放目的地址长度和目的地址前缀信息,域间二维路由协议对该字段扩展后,还存放了源地址长度和源地址前缀信息,扩展后的 NLRI 字段结构如图 5 所示。MP_UNREACH_NLRI 字段结构与 MP_REACH_NLRI 字段一致,不在此赘述。

3 域间二维路由转发方案

域间二维路由器收到报文时,不



▲图 4 MP_REACH_NLRI 字段结构图



▲图5 域间二维路由网络层可达信息字段的结构图

仅需要匹配目的地址,还要匹配源地址,因而转发表需要有2个地址匹配域。实际上,只有通过二维路由配置生成的转发表项才需要二维的匹配,其他由传统路由方式(仅基于目的)生成的转发表项只需要匹配目的地址。一个很直接的转发层设计方案为:路由器分配2个转发表,一个是二维转发表,另一个是传统的一维转发表。当路由器收到报文时,需先在二维转发表中进行最长前缀匹配,二维的最长前缀匹配规则是:先进行目的地址的最长前缀匹配,然后在匹配结果中进行源地址的最长前缀匹配,若找到匹配的表项,则终止查找,若无匹配表项,则寻找下一个最长前缀匹配的目的地址,然后再进行源地址的最长前缀匹配,这样重复下去直到找到匹配结果或查完所有表项^[8]。如果在二维转发表中找到匹配表项,就按照其下一跳转发报文,否则就查找传统的一维转发表。一维转发表的查找只进行目的地址的最长前缀匹配。这样的转发层设计十分简洁,但存在一个问题:当二维路由策略很多时,就会生成很多的二维转发表项,消耗大量的转发表空间。转发表一般使用三态内容寻址存储器(TCAM)实现高速匹配,但是TCAM成本高、能耗高,大大限制了二维转发表的空

间大小。

幸运的是:杨术等人提出的企业转发表结构(FISE)^[9]能够较好地解决该问题。FISE结合TCAM和静态随机存取存储器(SRAM)压缩了二维转发表所需的TCAM空间,同时保证报文的线速处理。

如图6所示,新型的转发表结构FISE有2张TCAM表和2张SRAM表。一张TCAM表存储目的表,每条表项是一个目的前缀到目的索引号的映射;另一张TCAM表存储源表,每条表项是一个源前缀到源索引号的映射。一张SRAM表存储所有转发规则的下一跳的索引号,该表被称为二维(TD)表,表里的每个单元格被称为TD单元。通过一个目的索引号和一个源索引号,可以定位到一个TD单元并获得一个下一跳索引号。另一张SRAM表中存储了下一跳索引号和下一跳接口信息之间的映射关系,该表被称为映射表,它能缓解

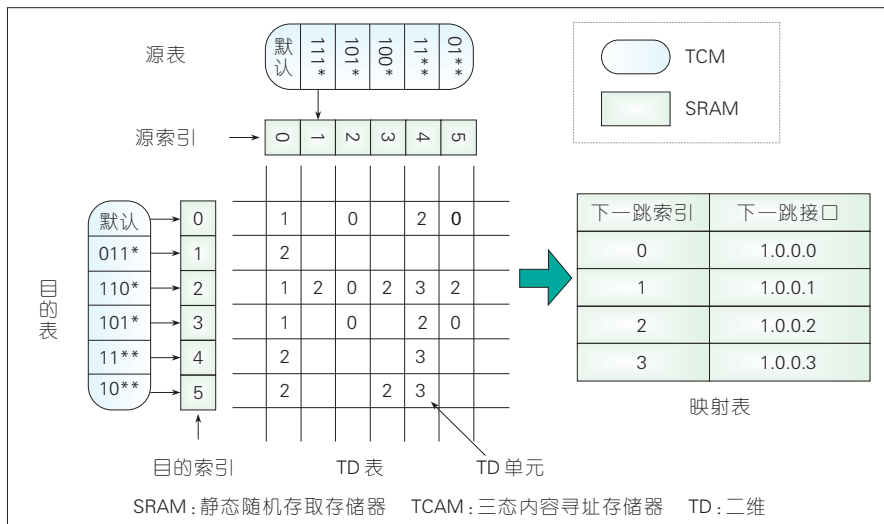
下一跳信息占用存储空间过大、冗余信息过多的问题。

可以看到:FISE将二维转发表的大部分开销从TCAM中移到了SRAM中。这是因为SRAM要比TCAM便宜得多(TCAM成本大概是SRAM的10~100倍),能耗也相对低得多(TCAM能耗大概是SRAM的几十倍到100倍)。FISE借助TCAM的高速匹配和SRAM的空间压缩大大降低了二维转发表的开销并保证了匹配性能。

图7展示了FISE的查找流程。当一个报文到达时,FISE首先在TCAM中分别匹配目的前缀和源前缀,通过目的表和源表可得指向TD单元的目的索引号和源索引号,最后利用TD单元存储的下一跳索引号,在映射表中查找到下一跳的信息。

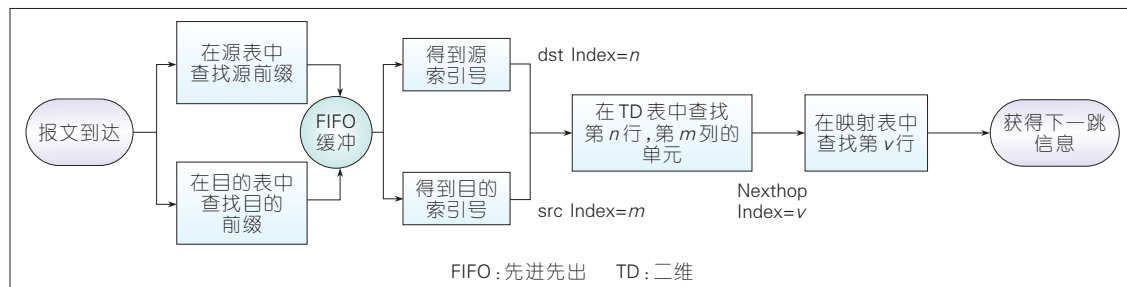
4 结束语

本文中我们提出了一个基于



▲图6 FISE的结构图

图7 FISE的查找流程图



BGP 的域间二维路由的设计方案,域间二维路由在进行路由决策的时候同时考虑目的地址和源地址,实现了灵活的流量控制,能够满足用户的多样化需求。本文中我们设计了域间二维路由协议的控制层,使用 MP-BGP 的可选属性携带二维路由的配置信息,同时兼容传统路由协议,方便 ISP 进行增量部署。我们还给出了适用于域间二维路由的数据层设计,使用前人提出的 FISE 转发表结构,可以解决二维转发表造成的 TCAM 空间爆炸的问题。整体而言,域间二维路由是一种新型路由方式,灵活和细粒度的流量控制使得其具有很好的应用前景。

参考文献

- [1] Framework for Multi-Protocol Label Switching (MPLS)-Based Recovery: RFC 3469[S]. IETF, 2003

- [2] McKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow [J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74. DOI:10.1145/1355734.1355746
- [3] RUCHANSKY N, PRPSEPIO D. A (not) NICE Way to Verify the Openflow Switch Specification [C]// ACM SIGCOMM 2013, ACM Special Interest Group on Data Communication 2013. China: ACM, 2013. DOI:10.1145/2486001.249171
- [4] VISSICCHIO S, TILMANS O, VANBEVER L, et al. Central Control over Distributed Routing [J]. ACM SIGCOMM CCR, 2015, 45(4): 43-56
- [5] A Border Gateway Protocol 4 (BGP-4): RFC1771[S]. IETF, 2005
- [6] Multiprotocol Extensions for BGP-4: RFC4760[S]. IETF, 2007
- [7] XIAO L, WANG J, NAHRSTEDT K. Optimizing IBGP route reflection network [C]// IEEE ICC 2003, IEEE International Conference on Communications 2003. USA: IEEE, 2003: 1765-1769. DOI: 10.1109/ICC.2003.1203903
- [8] SMIRNOV A. Draft-ietf-Rtggw-Dst-Src-Routing-06[R]. Internet Draft, 2017
- [9] YANG S, XU M W, WANG D, et al. Scalable forwarding Tables for Supporting Flexible Policies in Enterprise Networks[C]//IEEE INFOCOM 2014, IEEE Conference on Computer Communications, 2014. USA: IEEE, 2014: 208-216. DOI:10.1109/INFOCOM.2014.6847941

作者简介



耿男,清华大学计算机系在读博士生;主要研究方向为流量工程、二维路由、路由协议等。



金飞蔡,电子科技大学计算机学院在读硕士生;现任中兴通讯股份有限公司承载网产品线平台系统部项目经理;主持研究了“863”计划项目,国家重点研发计划和省重点研究项目4项;发表专利10余篇。



徐明伟,清华大学教授、博士生导师;主要研究方向为互联网体系结构、互联网路由、高性能路由器、网络安全等。

上接第55页

电力远远超过全球一些小国家(如约旦等)一年的用电量,相比于IoT设备的低耗能,区块链技术带来的安全防护可能远远小于它的资源浪费。

(4)跨链访问问题。可以预见,未来将会有更多的基于区块链的IoT平台出现,如基于区块链的车联网平台和基于区块链的智慧小区,而如何保证不同区块链平台的互通/互操作将会是促进区块链快速部署的重要条件。

(5)区块链自身的安全问题。区块链在为IoT提供安全防护的同时,自身也面临着一些安全威胁,如eclipse攻击、路由劫持攻击、51%攻击、智能合约漏洞等,这同样为2种技术的融合带来一定的安全隐患。

未来,区块链与IoT这2种技术将进一步融合,面向IoT安全的区块链技术也将逐渐兴起。共识效率更高、存储空间更小、绿色环保的安全区块链技术更能适应新型IoT技术的需求;而容错率高、鲁棒性强、去中心

化的IoT安全管控势必会推进区块链应用技术的发展。

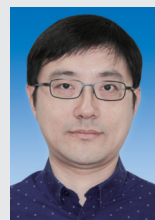
5 结束语

基于区块链的新型IoT技术还处在“萌芽”阶段,对学术界与工业界来说既是机遇又是挑战。区块链与IoT两种技术的融合势必会推动IoT安全的迅猛发展,并由此带来技术的巨大升级。研究适合IoT特征的区块链安全防护技术是未来的一种趋势,但也存在各种挑战而任重道远。

参考文献

- [1] NAKAMOTO S. A Peer-to-Peer Electronic Cash System[EB/OL].(2008-10-31)[2018-10-16].<https://nakamotoinstitute.org/bitcoin/>
- [2] 徐恪,李沁.算法统治世界[M].北京:清华大学出版社,2017
- [3] WU B, LI Q, XU K, et al. SmartRetro: Blockchain-Based Incentives for Distributed IoT Retrospective Detection[C]//IEEE MASS 2018. USA:IEEE, 2018
- [4] GAO F, ZHU L, SHEN M, et al. A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks [EB/OL].(2018-07-04)[2018-10-16]. <http://www.x-mol.com/paper/635775>

作者简介



徐恪,清华大学教授、博士生导师、计算机系副主任,国家杰出青年科学基金获得者,中国计算机学会理事;主要从事计算机体系结构、网络空间安全和网络经济学等方面的研究;获国家技术发明二等奖1次、国家科技进步二等奖1次、中国电子学会电子信息科学技术奖一等奖1次,其他省部级一等奖3次等;发表论文20余篇,完成著作6本,获得中国发明专利20余项,美国发明专利授权8项。



吴波,清华大学在读博士研究生;主要研究方向为网络体系结构、网络安全和区块链等;发表论文6篇,获中国发明专利5项,参与制定中国通信行业标准3项。



沈蒙,北京理工大学副教授、硕士生导师,并担任多本国际期刊的审稿人,以及IEEE ICC、IEEE Globecom等国际会议的程序委员会委员;主要研究领域为区块链与数据隐私保护;已发表论文30余篇,获得中国发明专利授权12项,美国发明专利授权2项。

《中兴通讯技术》第24卷总目次

卷·期·页

卷·期·页

卷首特稿

5G商用,蓄势待发.....徐慧俊 24-1-02

专题

专题:5G承载网技术和优化组网

5G无线网络架构对传输网影响.....许森,高程,卞宏梁 24-1-06
5G移动业务OTN承载解决方案.....孙志勇 24-1-13
面向5G的承载网需求及关键技术.....师严,王光全,王海军 24-1-17
面向5G的MEC系统关键技术.....宋晓诗,闫岩,王梦源 24-1-21
网络切片:构建定制化的5G网络.....任驰,马瑞涛 24-1-26
基于增强学习的5G网络切片资源动态优化方案.....任语铮,谢人超,黄韬 24-1-31
移动边缘计算的移动性管理研究.....王秋宁,谢人超,黄韬 24-1-37
5G承载网技术和优化组网.....张宝亚 24-1-42

专题:大数据智能化无线网络技术

大数据驱动的“人工智能”无线网络.....张琰,盛敏,李建东 24-2-02
大数据驱动的无线网络资源管理及控制.....刘媛妮,赵国锋 24-2-06
基于强化学习的无线网络智能接入控制技术.....严牧,孙耀,冯钢 24-2-10
移动边缘计算中数据缓存和计算迁移的智能优化技术.....汪海霞,赵志峰,张宏纲 24-2-15
TD-LTE网络中大气波导干扰的分析与预测.....孙天宇,周婷,杨旸 24-2-19
基于数据驱动深度学习方法的无线信道均衡.....杨旸,李扬,周明拓 24-2-25
mMTC网络中基于空口流量的入侵检测.....卢楠,杜清河,任品毅 24-2-30
5G网络人工智能化的基本框架和关键技术.....

专题:毫米波和太赫兹通信

5G高低频无线协作组网及关键技术.....赵军辉,杨丽华,张子扬 24-3-02
5G高低频协作组网场景下小区范围动态扩展优化技术.....方思赛,魏品帅,刘聪 24-3-10
太赫兹高速通信系统前端关键技术.....樊勇,陈哲,张波 24-3-15
面向5G毫米波通信系统的本振源设计与实现.....胡蒙筠,周健义 24-3-21
毫米波大规模MIMO系统中的预编码技术.....张钰,赵雄文 24-3-26
车载雷达通信系统综述.....朱伏生 24-3-32

专题:5G回传网络光电子器件技术

5G回传的分组切片网络架构和关键技术研究.....赵福川,温建中 24-4-02
基于CMOS平台的硅光子关键器件与工艺研究.....赵瑛璇,武爱民,甘甫烷 24-4-08
半导体前置光放大器的设计和制作要点.....李洵,左成亮,董智星 24-4-15
面向5G通信的高速PAM4信号时钟与数据恢复技术.....廖启文,Patrick Yin CHIANG,祁楠 24-4-21
高速高密度光电共封装技术.....孙瑜,刘丰满,薛海韵 24-4-27
PAM4技术在光通信应用中的系统分析.....朱梅冬,陆建鑫 24-4-33
数据中心的高速光互联技术.....余建军,方凯博 24-4-38
基于硅基集成的可重构微波光子前端.....霍元东,于鸿晨,陈明华 24-4-42
高速光器件封装技术发展趋势.....张一鸣,刘宇,张志珂 24-4-46

专题:可再生能源供电的无线通信与网络

电力基础设施薄弱地区的基站自供电技术研究.....王亚会,周振宇,贾云健 24-5-02

可再生能源供电无线通信的最优链路传输策略·····杜林松,黄川	24-5-06
可再生能源供电下射频单元的基带功能分割和功率控制·····王刘猛,周盛	24-5-12
无线数据与能量协同传输中的游程限制编码设计·····胡杰,李梦媛,杨鲲	24-5-18
部分自供电的非正交多址接入技术·····龚杰,陈翔	24-5-24
基于摩擦纳米发电机的自驱动微系统·····陈号天,宋宇,张海霞	24-5-28
摩擦纳米发电机等效电路模型研究·····魏子钧,耿来鑫,边森	24-5-35

专题:区块链技术及其物联网应用

区块链共识机制研究:典型方案对比·····刘懿中,刘建伟,喻辉	24-6-02
区块链共识机制发展与安全性·····王李笑阳,秦波,乔鑫	24-6-08
比特币生成原理及其特点·····林成骏,伍玮	24-6-13
区块链概念剖析及其在物联网中的部分应用·····田海博	24-6-19
基于区块链的物联网密钥协商协议·····张佳妮,何德彪,李莉	24-6-23
基于区块链的电子数据存证的设计与实现·····冒小乐,陈鼎洁,孙国梓	24-6-28
区块链技术在物联网中的身份认证研究·····杨惠杰,周天祺,桂梓原	24-6-35
一种基于区块链的身份识别技术·····苏宣瑞,邹秀清,丁勇	24-6-41

专家论坛

5G 承载的挑战与技术方案探讨·····李俊杰,唐建军	24-1-49
面向 5G 的传送网新架构及关键技术·····李晗	24-1-53
智能物联网技术和应用的发展趋势·····杨旸	24-2-43
关于毫米波与太赫兹通信的思考·····洪伟	24-3-39
发展中国太赫兹高速通信技术与应用的思考·····陈智,张雅鑫,李少谦	24-3-43
5G 无线光模块的需求分析和关键技术·····张华,黄卫平	24-4-51
绿色通信:如何笑到最后·····牛志升	24-5-40

无线数据与能量协同传输技术:编码与调制设计·····胡杰,金石	24-5-43
区块链的理想与现实·····何宝宏	24-6-49
区块链:描绘物联网安全新愿景·····徐恪,吴波,沈蒙	24-6-52

专家视点

封装天线技术最新进展·····张跃平	24-5-43
--------------------	---------

企业视界

面向 5G 承载的网络切片架构与关键技术·····王强,陈捷,廖国庆	24-1-58
5G 传送标准进展·····张源斌,杨剑,占治国,周严伟	24-1-62
免调度非正交多址技术及其接收机设计·····邱刚,田力,王沙,袁志锋	24-2-47
RRU 关键技术及创新·····王永贵,张国俊,崔晓俊	24-3-48
VR 的技术发展趋势和行业应用·····尹芹,吕达	24-4-54
OGC 视频直播新时代展望·····尤琰,张东卓,孟晓斌	24-4-58
大数据已成为基础通用技术·····王德政,汪绍飞,王梅	24-5-54
NG-PON 技术背景、应用和展望·····陈爱民	24-6-56

技术广角

新一代无线定位技术研究与发展趋势分析·····陈诗军,王慧强,陈大伟	24-2-54
软件定义天地一体化网络:架构、技术及挑战·····许方敏,仝宗健,赵成林,秦智超	24-2-59
LTE-V 和 DSRC 共享频谱资源的研究·····陈沛吉,马伟,张琳	24-3-54
基于结构特征的时序聚类方法研究·····孟志浩,刘建伟,韩静	24-3-61
基于卫星的流媒体应用技术研究·····黄泽武,韩桂鲁,李双全	24-5-57
基于深度卷积神经网络的视觉 SLAM 去模糊系统·····缪弘,张文强	24-5-62
基于 BGP 的域间二维路由方案·····耿男,金飞蔡,徐明伟	24-6-60

《中兴通讯技术》杂志(双月刊)投稿须知

一、杂志定位

《中兴通讯技术》杂志为通信技术类学术期刊。通过介绍、探讨通信热点技术,以展现通信技术最新发展动态,并促进产学研合作,发掘和培养优秀人才,为振兴民族通信产业做贡献。

二、稿件基本要求

1. 投稿约定

- (1)作者需登录《中兴通讯技术》投稿平台:tech.zte.com.cn/submission,并上传稿件。第一次投稿需完成新用户注册。
- (2)编辑部将按照审稿流程聘请专家审稿,并根据审稿意见,公平、公正地录用稿件。审稿过程需要1个月左右。

2. 内容和格式要求

- (1)稿件须具有创新性、学术性、规范性和可读性。
- (2)稿件需采用WORD文档格式。
- (3)稿件篇幅一般不超过6000字(包括文、图),内容包括:中、英文题名,作者姓名及汉语拼音,作者中、英文单位,中文摘要、关键词(3~8个),英文摘要、关键词,正文,参考文献,作者简介。
- (4)中文题名一般不超过20个汉字,中、英文题名含义应一致。
- (5)摘要尽量写成报道性摘要,包括研究的目的、方法、结果/结论,以150~200字为宜。摘要应具有独立性和自明性。中英文摘要应一致。
- (6)文稿中的量和单位应符合国家标准。外文字母的正斜体、大小写等须写清楚,上下角的字母、数据和符号的位置皆应明显区别。
- (7)图、表力求少而精(以8幅为上限),应随文出现,切忌与文字重复。图、表应保持自明性,图中缩略词和英文均要在图中加中文解释。表应采用三线表,表中缩略词和英文均要在表内加中文解释。
- (8)所有文献必须在正文中引用,文献序号按其在文中出现的先后次序编排。常用参考文献的书写格式为:
 - 期刊[序号]作者.题名[J].刊名,出版年,卷号(期号):引文页码.数字对象唯一标识符
 - 书籍[序号]作者.书名[M].出版地:出版者,出版年:引文页码.数字对象唯一标识符
 - 论文集中析出文献[序号]作者.题名[C]/论文集编者.论文集名(会议名).出版地:出版者,出版年(开会年):引文页码.数字对象唯一标识符
 - 学位论文[序号]作者.题名[D].学位授予单位所在城市名:学位授予单位,授予年份.数字对象唯一标识符
 - 专利[序号]专利所有者.专利题名:专利号[P].出版日期.数字对象唯一标识符
 - 国际、国家标准[序号]标准名称:标准编号[S].出版地:出版者,出版年.数字对象唯一标识符
- (9)作者超过3人时,可以感谢形式在文中提及。作者简介包括:姓名、工作单位、职务或职称、学历、毕业于何校、现从事的工作、专业特长、科研成果、已发表的论文数量等。
- (10)提供正面、免冠、彩色标准照片一张,最好采用JPG格式(文件大小超过100kB)。
- (11)应标注出研究课题的资助基金或资助项目名称及编号。
- (12)提供联系方式,如:通讯地址、电话(含手机)、Email等。

3. 其他事项

- (1)请勿一稿两投。凡在2个月(自来稿之日算起)以内未接到录用通知者,可致电编辑部询问。
- (2)为了促进信息传播,加强学术交流,在论文发表后,本刊享有文章的转摘权(包括英文版、电子版、网络版)。作者获得的稿费包括转摘酬金。如作者不同意转摘,请在投稿时说明。

编辑部地址:安徽省合肥市金寨路329号凯旋大厦1201室,邮政编码:230061

联系电话:0551-65533356,联系邮箱:magazine@zte.com.cn

本刊只接受在线投稿,欢迎访问本刊投稿平台:tech.zte.com.cn/submission

中兴通讯技术

ZTE TECHNOLOGY JOURNAL

办刊宗旨:

以人为本,荟萃通信技术领域精英
迎接挑战,把握世界通信技术动态
立即行动,求解通信发展疑难课题
励精图治,促进民族信息产业崛起

双月刊 1995 年创刊 总第 143 期
2018 年 12 月 第 24 卷 第 6 期(卷终)

主管:安徽省科学技术厅
主办:安徽省科学技术情报研究所
中兴通讯技术杂志社
出版:中兴通讯技术杂志社

总编:王翔
常务副总编:黄新明
责任编辑:徐烨
编辑:卢丹、朱莉
排版制作:余刚
发行:王萍萍
编务:王坤

《中兴通讯技术》编辑部
地址:合肥市金寨路 329 号凯旋大厦 1201 室
邮编:230061
网址:tech.zte.com.cn
投稿平台:tech.zte.com.cn/submission
电子信箱:magazine@zte.com.cn
电话:(0551)65533356
传真:(0551)65850139

编辑、发行:《中兴通讯技术》编辑部
发行范围:公开发行
印刷:合肥添彩包装有限公司
出版日期:2018 年 12 月 10 日
中国标准连续出版物号:ISSN 1009-6868
CN 34-1228/TN
定价:每册 20.00 元