基于聚合签名的共识算法优化方案

苑 超 徐蜜雪 斯雪明
(解放军信息工程大学 郑州 450001) (数学工程与先进计算国家重点实验室 郑州 450001)

摘 要 随着比特币以及以太坊、超级账本等系统的兴起,区块链技术受到越来越多的关注。区块链是众多技术结合的产物,共识算法在区块链中起着至关重要的作用,共识算法的优劣直接影响着区块链系统的优劣。针对不同特点的区块链系统,采取的共识算法也不相同,不同的共识算法各有优劣。目前,效率问题是区块链中共识算法面临的主要问题之一。为了提高区块链系统中共识算法的运行效率,首先介绍了区块链中共识算法的各种潜在的优化方案,然后以联盟链中常用的PBFT共识算法的改进算法dBFT为研究对象,结合聚合签名技术以及双线性映射技术对dBFT的共识过程进行优化,并与原方案进行比较。优化后的聚合dBFT共识算法可以有效降低区块链系统中签名的空间复杂度。

关键词 区块链,共识算法,聚合签名,优化,双线性映射
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.02.009

Optimization Scheme of Consensus Algorithm Based on Aggregation Signature

YUAN Chao XU Mi-xue SI Xue-ming
(PLA Information Engineering University, Zhengzhou 450001, China)
(State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China)

Abstract With the rise of Bitcoin, Ethernet, Hyperledger and so on, blockchain has been paid more and more attention. Blockchain is the product of many technologies, and the consensus algorithm is an important standard to adjudicate a blockchain system. The adopted consensus algorithm should be different from the blockchain system to another for the different features. Different consensus algorithms have their own advantages, but they also have shortcomings. Currently, efficiency problem is one of the main problems faced by the consensus algorithm in the blockchain. In order to improve the efficiency, the potential optimization scheme of the consensus algorithm in the blockchain was introduced. Then, the dBFT consensus algorithm commonly used in the alliance chain was taken as the research object, and through combining with the aggregation signature and the bilinear mapping technology, the consensus process was modified. At last, compared with the original scheme, the space complexity of the signature in blockchain system can be effectively reduced with the aggregated dBFT.

Keywords Blockchain, Consensus algorithm, Aggregation signature, Optimization, Bilinear pairings

1 引言

区块链是近来来金融领域及其他众多领域研究的热点,除了在传统的金融货币领域有应用,其在数字货币、票据、清算、数字资产交易、供应链金融以及政务、民生和商业的底层架构方面也具有很好的应用潜力。随着区块链技术的不断发展与完善,越来越多的应用项目落地,而区块链也已摆脱了比特币的底层技术的局限,其应用范围日渐广阔。

但区块链的发展也面临着挑战,其中性能优化无疑是重要挑战之一。区块链的性能优化问题仅仅处于研究初期,很多问题还不成熟。

共识算法[1-4]是指在一个节点或者多个节点提议一个值后,整个分布式系统对这个值达成协定的算法。共识算法的选择是区块链的核心设计考量之一。在公有链中,以工作量证明(Proof of Work, PoW)[5]、权益证明(Proof of Stake, PoS)以及股份权益证明(DPoS)[6]为主要共识算法。而在私有链和联盟链中,他们多数直接采用了传统的拜占庭容错算法(BFT),其中又以经典的实用拜占庭容错算法(PBFT)及其变体最为常见。在恶意节点数不超过限制的前提下,BFT类算法可以支持较高的吞吐量,其正确性可被严格证明。

到稿日期:2017-05-15 返修日期:2017-08-27 本文受国家重点研发计划(2016YFB0800101,2016YFB0800100),国家自然科学基金创新研究群体科学基金(61521003)资助。

苑 超(1992—),男,硕士生,主要研究方向为密码学、区块链、信息安全;徐蜜雪(1993—),女,硕士生,主要研究方向为密码学、区块链、信息安全;斯雪明(1966—),男,教授,主要研究方向为密码学、数据科学、计算机体系结构、网络安全、区块链,E-mail:sxm@fudan.edu.en(通信作者)。

本文首先从硬件加速、异步并行、分层共识的角度介绍了区块链中共识算法的潜在优化方案，然后基于聚合签名和双线性映射给出了改进的 dBFT 共识算法。

本文第 2 节对区块链系统中常见的共识算法进行了介绍；第 3 节介绍了区块链中共识算法的潜在优化方案；第 4 节介绍了 PBFT 算法的改进方案 dBFT 算法[9]，然后给出了基于聚合签名和双线性映射的改进方案；最后总结全文并对未来的研究方向进行初步探讨。

2 准备知识

2.1 常用的共识算法

共识算法是区块链技术的关键。共识算法的核心是在分布式网络中利用一种算法来保证全网对于块的创建是一致的。目前，区块链中主流的共识算法以工作量(PoW)、PoS、实用拜占庭容错 PBFT 以及 PBFT 的各种变形算法为主。当然，不同的共识算法具有各自的优势，适用于不同的场景和环境，同时各算法也都存在缺陷。本文对目前区块链系统中的主流共识算法进行简要的介绍。

2.1.1 工作量证明(POW)

1997 年，Adam Back 设计的 Hashcash 中首次提到了工作量证明，其最开始的目的是预防垃圾邮件。2009 年，Satoshi Nakamoto 设计比特币时，使用了工作量证明作为共识算法，是可重复使用的 Hashcash 工作证明。生成工作证明是一个概率意义上的随机过程。工作量证明的优点是去中心化和分布式，缺点是浪费资源，同时也存在相应的安全问题，例如，假设攻击者掌握了全网 51%的算力，他便可以在网络中伪造、阻碍区块的产生，甚至不需 51%的算力就可以对区块链网络进行攻击，如自私挖矿攻击、日蚀攻击、顽固攻击等都是基于这种条件的攻击方式。

2.1.2 权益证明(PoS)

权益证明最初是为了辅助工作量证明而被提出的。2011 年 7 月，Quantum Mechanic 在 bitcoin 社区提出了权益证明，但并没有独立运用。权益证明是在 Sunny King 发明的 peercoin 中真正实现的。其核心思想是通过网络参与节点掌握资产的数量以及利用时间来决定参与节点的记账权。其优点是不需要消耗资源，核心权益掌握者有能力改变网络而不需要得到所有网络参与者的认可。其缺点是核心权益掌握者对网络的垄断控制在一定程度上破坏了分布式账本的去中心化的功能。

2.1.3 委托权益证明(DPoS)

委托授权权益证明是权益证明的一种改进，这种共识算法由 Dan Larimer 于 2014 年 4 月提出。其使用声誉系统和无耗损的实时投票来生成代表，这些代表有权创建区块并将其添加到区块链中，同时可以禁止不信任参与者的参与。这种共识算法的优点是参与者达成共识的速度快。

2.1.4 实用拜占庭容错算法(PBFT)

PBFT 是由 Miguel Castro 和 Barbara Liskov 于 1999 年提出[10,17]，该算法解决了原始拜占庭容错效率不高的问题，将复杂度由指数级降低到多项式级，使得拜占庭容错算法在实际系统应用中变得可行。这种共识机制可应用于不需要大的吞吐量但需要处理许多事件的数字资产平台。在达成共识的过程中每个节点发布公钥，通过节点的消息由节点签名来验证其格式。一旦达到相同的足够数量的响应，则交易达成共识。在 PBFT 中，由 N 个节点构成的区块链网络可以接受 f 个拜占庭节点，其中 $f=(N-1)/3$。

2.2 聚合签名[11,19]

聚合签名是一种支持聚合特性的数字签名变体，即给定 n 个用户 $u_i\in U(1\leqslant i\leqslant n)$，其中 U 为用户集合，对于 n 个消息，$m_i\in M(1\leqslant i\leqslant n)$，其中 M 为消息集合。对于 n 个签名，聚合签名的生成者(可以不同于 u_i 或是不被信任的用户)可以将这 n 个(单一)签名聚合成一个唯一的短签名 σ，并给定该聚合签名、参与生成聚合签名者的身份 u_i 及其签名的原始消息 m_i，可以使验证者确信是用户 u_i 对消息 m_i 做的签名[20]。

$AS=(Setup,Key,Sign,Verify,Aggs,Aggv)$ 是多项式时间算法六元组，具体说明如下：

$DS=(Setup,Key,Sign,Verify)$ 是普通的签名方案，亦称为聚合签名的基准签名。

$Aggs$：聚合签名生成算法，可至少实现 3 个子功能。

(1)实现普通签名功能；

(2)实现 3 个向量组，即消息向量$(m_1,\cdots,m_n)$、用户向量$(u_1,\cdots,u_n)$和个体签名向量$(\sigma_1,\cdots,\sigma_n)$的聚合功能；

(3)聚合追加新的签名 σ_{n+1}。

$AggV$：聚合签名验证算法，假设每个用户拥有私钥 sk 和公钥 pk，若 $AggV(pk_1,\cdots,pk_n,m_1,\cdots,m_n,AggS(pk_1,\cdots,pk_n,m_1,\cdots,m_n,Sign(sk_1,m_1),\cdots,Sign(sk_n,m_n)))=1$，则输出 1，否则输出 0。

2.3 双线性映射

定义 $\xi=(n,G_1,G_2,G_T,e,g_1,g_2)$，其中$G_1=\langle g_1\rangle$，$G_2=\langle g_2\rangle$，$G_T$是 n 阶循环群，定义映射 $e:G_1\times G_2\rightarrow G_T$，如果映射 e 满足以下 3 个条件，则称 e 是双线性映射。

(1)对于任意 $a,b\in Z_n$，$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$；

(2)存在 $u\in G_1$，$v\in G_2$，使得 $e(u,v)\neq 0$，其中 O 是单位元；

(3)对于所有的 $u\in G_1$，$v\in G_2$，可以简单计算得到 $e(u,v)$。

3 共识算法的潜在优化策略

目前，区块链上的共识算法面临的主要挑战是其共识过程中的效率问题，其受到交易数量、交易频率以及事务处理效率要求的影响，共识算法的效率是制约区块链技术应用的一个问题，因此对区块链上共识算法的优化策略的研究显得尤为重要。本文对目前区块链上共识算法的主要优化策略进行了简要介绍。

3.1 硬件加速

硬件加速对于优化方案具有普适性，对于共识算法的优化也不例外。比特币挖矿方式的改进就很好地说明了这一点。从最开始的 CPU 到 GPU 和 FPGA，再到现在的挖矿芯

片,SHA256 难题被解决的速度越来越快。在区块链的共识算法的性能优化上,硬件加速能发挥作用,例如在签名验证过程中利用 FPGA 的并行和寄存器多的特点可以并行验证多个签名,进而提高了签名验证的效率[7]。

3.2 打包操作

区块链中的区块通常包含多笔交易,因而通过打包操作来对共识过程进行优化较容易。打包可以将共识节点间进行签名和验签的开销平摊在块中的每笔交易上,从而降低总体开销。假设之前共识节点以单笔交易为对象进行签名验证,现在共识节点可以将 n 笔交易进行打包。

4 共识算法的改进方案

dBFT[9]是在 PBFT 的基础上提出的一种改进的拜占庭容错算法,适用于区块链系统。本文首先介绍 dBFT 的一般流程,然后基于聚合签名技术提出针对 dBFT 算法的改进方案。

4.1 dBFT 的一般流程[9]

参与共识的节点需要维护一个状态表,用于记录当前的共识状态。一次共识从开始到结束所使用的数据集合被称为视图。如果在当前视图内无法达成共识,则需要更换视图。每一个视图分配一个编号 v,编号从 0 开始,并逐渐递增,直到达成共识为止。

每一个参与共识的节点被分配一个编号,从 0 开始,最后一个节点的编号为 $n-1$。每一轮共识都需要一个节点来充当议长,其他节点则为议员。议长的编号 p 由如下公式来决定:假设当前共识的区块高度为 h,则 $p=(h-v)\bmod n$。

每一次共识产生一个区块,并附有至少 $n-f$ 个记账节点的签名。一旦有新的区块产生,则立即开始新一轮的共识,同时重置 $v=0$。

假设系统要求每次产生区块的时间间隔为 t,则在一切正常的情况下,算法按照以下流程执行:

(1)任意节点向全网广播交易数据并附上发送者的签名;

(2)所有记账节点均独立监听全网的交易数据,并将其记录在内存中;

(3)议长在经过时间 t 后,发送$\langle PerpareRequest,h,v,p,block,\langle block\rangle_{\sigma_i}\rangle$;

(4)议员 i 在收到提案后,发送$\langle PerpareResponse,h,v,i,\langle block\rangle_{\sigma_i}\rangle$;

(5)任意节点在收到至少 $n-f$ 个$\langle block\rangle_{\sigma_i}$后达成共识并发布完整的区块;

(6)任意节点在收到完整区块后,将包含的交易从内存中删除,并开始下一轮共识。

4.2 视图更换

若节点 i 在经过 $2v+t$ 的时间间隔后仍未达成共识或接收到包含非法交易的提案,则进入视图更换流程:

(1)令 $k=1$,$vk=v+k$;

(2)节点 i 发出视图更换请求$\langle ChangeView,h,v,i,vk\rangle$;

(3)任意节点收到至少 $n-f$ 个来自不同节点 i 的相同 vk 后,视图更换达成,令 $v=vk$ 并开始共识;

(4)如果经过 $2vk+t$ 的时间间隔后视图更换仍未达成,则 k 递增并回到步骤(2)。

随着 k 的增加,超时的等待时间也会呈指数级增加,这样可以避免频繁的视图更换操作,并使各节点尽快对 v 达成一致。

而在视图更换达成之前,原来的视图 v 依然有效,由此避免了因偶然性的网络延迟超时而导致的不必要的视图更换。图 1 将以流程图的形式对 dBFT 的整个过程进行展示,使 dBFT 的共识过程更加容易理解。

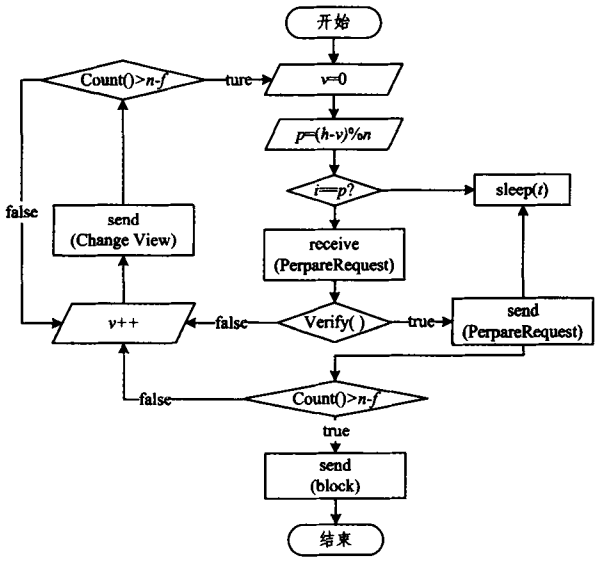

图 1　dBFT 算法的流程图

Fig. 1　Flow chart of dBFT algorithm

4.3 共识算法的改进方案

令 q 为大素数,选择生成元 $P\in\mathbb{G}_1$,$Q\in\mathbb{G}_2$,定义阶均为 q 的加法群 $\mathbb{G}_1$ 和乘法群 $\mathbb{G}_2$,双线性映射为 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$,定义散列函数 $H_0:\{0,1\}^*\to\mathbb{Z}_q^*$,$H_1:\{0,1\}^*\times\mathbb{G}_1\to\mathbb{G}_2$,$H_2:\{0,1\}^*\to\mathbb{G}_1$,$H_{DV}:\{0,1\}^*\to\mathbb{G}_1$。

(1)利用当下的视图计算 $P_v=vP$,结合已有参数,得到系统参数 $Params=\{\mathbb{G}_1,\mathbb{G}_2,e,q,P,Q,P_v,H_0,H_1,H_2,H_{DV}\}$。

(2)用户 u_i 选择随机值 $x_i\in\mathbb{Z}_q^*$ 作为用户的秘密值,计算 $P_i=x_iP$,$Q_i=H_1(ID_i\parallel P_i)$,$D_i=vQ_i$,生成用户的私钥 $S_i=(D_i,x_i)$。

(3)用户 u_i 执行以下过程:

1)选择 $r_i\in\mathbb{Z}_q^*$,计算 $R_i=r_iP$,$h_i=H_0(ID_i\parallel m_i\parallel P_i\parallel R_i)$,$T=H_2(P_v)$。

2)计算 $V_i=D_i+h_ir_iT+x_iQ$,输出 u_i 对 m_i 的签名 $\sigma_i=(V_i,R_i)$并将其发送给聚合者 u_A。

(4)若要验证 u_i 对 m_i 的签名 $\sigma_i=(V_i,R_i)$的有效性,计算 $h_i=H_0(ID_i\parallel m_i\parallel P_i\parallel R_i)$,$Q_i=H_1(ID_i\parallel P_i)$ $T=H_2(P_v)$,并验证下列等式是否成立:

$$e(V_i,P)=e(Q_i,P_v)e(T,h_iR_i)e(Q,P_i)$$

(5)*Aggregate-Sign*:输入用户 u_i 对 m_i 的签名为$\{(m_1,\sigma_1=(V_1,R_1)),\cdots,(m_n,\sigma_n=(V_n,R_n))\}$,然后聚合者 u_A 计算 V 和 R,$V=\sum_{i=1}^{n}V_i$,$R=\sum_{i=1}^{n}h_iR_i$,输出最终的聚合签名 $\sigma=(V,R)$。

(6)若需要验证聚合签名 σ 的有效性,可以执行该算法。输入系统参数 $Params$、用户 u_i 对应的身份列表 $ID=\{ID_1,\cdots,ID_n\}$、公钥列表 $P=\{P_1,\cdots,P_n\}$、消息列表 $M=\{m_1,\cdots,m_n\}$和签名列表 $\sigma=\{\sigma_1,\cdots,\sigma_n\}$,计算 $Q_i=H_1(ID_i\|P_i)$和$T=H_2(P_v)$,验证等式[12]:$e(V,P)=e(\sum_{i=1}^{n}Q_i,P_v)e(T,R)e(Q,\sum_{i=1}^{n}P_i)$是否成立,若成立,则验证通过,否则验证不通过。

下面说明此基础框架的正确性。定理 1 和定理 2 分别给出了单个签名验证过程的正确性和聚合签名验证过程的正确性。

定理 1 单个签名验证过程是正确的。

证明:每个签名者 u_i 对 m_i 的签名 $\sigma_i=(V_i,R_i)$的验证过程如下:

$$\begin{aligned}e(V_i,P)&=e(D_i+h_ir_iT+x_iQ,P)\\&=e(D_i,P)e(T,h_ir_iP)e(x_iQ,P)\\&=e(Q_i,P_v)e(T,h_iR_i)e(Q,P_i)\end{aligned}$$

定理 2 聚合签名验证过程是正确的。

证明:聚合签名 $\sigma=(V,R)$的验证过程如下:

$$\begin{aligned}e(V,P)&=e(\sum_{i=1}^{n}V_i,P)=e(\sum_{i=1}^{n}D_i+x_iQ+h_ir_iT,P)\\&=e(\sum_{i=1}^{n}D_i,P)e(\sum_{i=1}^{n}h_ir_iT,P)e(\sum_{i=1}^{n}x_iQ,P)\\&=e(\sum_{i=1}^{n}Q_i,P_v)\prod_{i=1}^{n}e(T,h_iR_i)\prod_{i=1}^{n}e(Q,P_i)\\&=e(\sum_{i=1}^{n}Q_i,P_v)e(T,R)e(Q,\sum_{i=1}^{n}P_i)\end{aligned}$$

在得到以上基础框架以及对此基础框架的正确性进行验证之后,本文将此框架运用到 dBFT 共识算法的共识过程中,得到了如下改进的共识过程:

(1)任意节点向全网广播交易数据并附上发送者的签名;

(2)当未入块的消息数量达到 m 后,聚合签名者通过集合签名算法得到聚合签名;

(3)所有记账节点均独立监听全网的交易数据,并将其记录在内存中;

(4)议长在经过时间 t 后,发送$\langle PerpareRequest,h,v,p,block,\langle block\rangle_{\sigma_i}\rangle$;

(5)议员 i 在收到提案后,发送$\langle PerpareResponse,h,v,i,\langle block\rangle_{\sigma_i}\rangle$;

(6)任意节点在收到至少 $n-f$ 个$\langle block\rangle_{\sigma}$后达成共识并发布完整的区块;

(7)任意节点在收到完整区块后将包含的交易从内存中删除,并开始下一轮共识。

改进的共识算法将原来的 m 条消息的签名聚合成 1 条,其空间复杂度降低为原来的 $1/m$。但与此同时增加了一个聚合签名的过程,其计算复杂度有所增加。在聚合签名的过程中,进行了 $2m$ 次加法和 m 次乘法,其计算复杂度提升了 $O(3m)$。目前,在比特币区块链系统中,扩容问题是迫在眉睫的问题,在其他区块链系统中这一问题也同样突出,本文给出的改进共识算法可以在一定程度上解决该问题。

结束语 共识算法是区块链的重要构成模块,区块链中共识算法的研究进展也直接影响着区块链技术的研究。目前区块链中使用的共识算法以工作量证明、权益证明、PBFT 算法以及其改进算法为主。在工作量证明和权益证明中,设计者有以效率换取安全性和稳定性的倾向,因此对这两种共识算法的效率进行优化并不是明智的选择,但是对于 PBFT 算法以及它的各种变体来说,效率优化就显得尤为重要了。本文在共识算法 dBFT 的基础上,基于聚合签名和双线性映射,给出了改进的共识算法。当然这仅仅是对共识算法优化方案研究的开端,我们认为在今后的研究中环签名[15]和私有外包技术[16]等可以有效地优化区块链中的共识算法。

参 考 文 献

[1] PEASE M, SHOSTAK R, LAMPORT L. Reaching Agreement in the Presence of Faults[J]. Journal of the ACM, 1980, 27(2): 228-234.

[2] LAMPORT, LESLIE, SHOSTAK, et al. Byzantine Generals Problem[J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401.

[3] FISCHER M. The Consensus Problem in Unreliable Distributed Systems (a Brief Survey)[C]// International Fct-conference on Fundamentals of Computation Theory. 1982: 127-140.

[4] CHANDRA T, TOREG S. Unreliable Failure Detectors for Reliable Distributed Systems[J]. Journal of the ACM, 1996, 43(2): 225-267.

[5] SATOSHI N. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. https://bitcoin.org/bitcoin.pdf.

[6] Delegated Proof-of-Stake Consensus[EB/OL]. http://bitshares.org/technology/delegated-proof-stake-consensus.

[7] BRASSAI S T, BAKO L, DAN S. FPGA Parallel Implementation of CMAC Type Neural Network with on Chip Learning[C]// International Symposium on Applied Computation Intelligence and Informatics. 2007: 111-115.

[8] DANEZIS G, MEIKLEJOHN S. Centrally Banked Cryptocurrencies[OL]. https://arxiv.org/abs/1505.06895.

[9] 张铮文. 一种用于区块链的拜占庭容错法[EB/OL]. [2016-04-07]. http://www.onchain.com/paper/66c677 3b.pdf.

[10] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]// OSDI. 1999: 173-186.

[11] YANG T, KONG L B, HU J B, et al. Survey on Aggregate Signature and Its Applications[J]. Journal of Computer Research and Development, 2012, 49(S2): 192-199. (in Chinese)
杨涛, 孔令波, 胡建斌, 等. 聚合签名及其应用研究综述[J]. 计算机研究与发展, 2012, 49(S2): 192-199

[12] ZHANG Y L, ZHOU D R, LI C Y, et al. . Certificateless-based efficient aggregate signature scheme with universal designated verifier[J]. Journal on Communications, 2015, 36(2): 1-8. (in Chinese)
张玉磊, 周冬瑞, 李臣意, 等. 高效的无证书广义指定验证者聚合签名方案[J]. 通信学报, 2015, 36(2): 1-8.

[13] SCHUBERT S. Simple BFT [EB/OL]. http://jira.hyperledger.org/browse/FAB-378.

(下转第 83 页)

[15] GIRVAN M, NEWMAN M E J. Community structure in social and biological networks [J]. Proceedings of the National Academy of Sciences of the United States of America, 2002, 99(12): 7821-7826.

[16] NEWMAN M E J. Fast algorithm for detecting community structure in networks[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2004, 69(6 Pt 2): 066133.

[17] NEWMAN M E J, GIRVAN M. Finding and evaluating community structure in networks[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2004, 69(2): 026113.

[18] LANICHINETTI A, FORTUNATO S, RADICCHI F. Benchmark graphs for testing community detection algorithms [J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2008, 78(4): 046110.

[19] MOLLOY M, REED B. A critical point for random graphs with a given degree sequence [J]. Random Structures & Algorithms, 1995, 6(2-3): 161-180.

[20] SESHADHRI C, KOLDA T G, PINAR A. Community structure and scale-free collections of Erdös-Rényi graphs[J]. Physical Review E Statistical Nonlinear & Soft Matter Physics, 2012, 85(5): 056109.

[21] KOLDA T G, PINAR A, PLANTENGA T, et al. A scalable generative graph model with community structure[J]. Siam Journal on Scientific Computing, 2014, 36(5), C424-C452.

[22] AMARAL L A, SCALA A, BARTHELEMY M, et al. Classes of small-world networks [J]. Proceedings of the National Academy of Sciences of the United States of America, 2000, 97(21): 11149-11152.

[23] ECKMANN J P, MOSES E. Curvature of co-links uncovers hidden thematic layers in the World Wide Web [J]. Proceedings of the National Academy of Sciences of the United States of America, 2002, 99(9): 5825-5829.

[24] BARABÁSI A L, ALBERT R, JEONG H. Scale-free characteristics of random networks: the topology of the world-wide Web [J]. Physica A Statistical Mechanics & Its Applications, 2000, 281(1-4): 69-77.

[25] ALBERT R, JEONG H. Diameter of the World Wide Web [J]. Nature, 1999, 401(6): 130-131.

[26] DOROGOVTSEV S N, MENDES J F. Language as an evolving word web[J]. Proceedings Biological Sciences, 2001, 268(1485): 2603-2606.

[27] RIPEANU M, FOSTER I, IAMNITCHI A. Mapping the gnutella network: properties of Large-Scale Peer-to-Peer systems and implications for system design [J]. IEEE Internet Computing, 2002, 6(1): 50-57.

[28] JEONG H, TOMBOR B, ALERT R, et al. The large-scale organization of metabolic networks [J]. Nature, 2000, 407(6804): 651-654.

[29] HUXHAM M, RAFFAELLI D. Do parasites reduce the chances of triangulation in a real food web [J]. Oikos, 1996, 76(2): 284-300.

[30] CANCHO R F I, JANSSEN C, SOLÉ R V. Topology of technology graphs: small world patterns in electronic circuits [J]. Physical Review E, 2001, 64(4): 046119.

[31] BLONDEL V D, GUILLAUME J L, LAMBIOTTE R, et al. Fast unfolding of communities in large networks [J]. Journal of Statistical Mechanics Theory & Experiment, 2008, 2008(10): 155-168.

(上接第 56 页)

[14] SOXT E. Ethereum[M]. Wiesbaden: Springer Fachmedien Wiesbaden, 2017.

[15] CHANDRAN N, GROTH J, SAHAI A. Ring signatures of sublinear size without random oracles[C] // International Colloquium on Automata, Languages, and Programming. Springer, 2007: 423-434.

[16] ZHANG Y Q, WANG X F, LIU X F, et al. Survey on Cloud Computing Security[J]. Journal of Software, 2010, 27(6): 1328-1348. (in Chinese)
张玉清，王晓菲，刘雪峰，等. 云计算环境安全综述[J]. 软件学报，2010，27(6)：1328-1348.

[17] CASTRO M, LISKOV B. Practical Byzantine Fault Tolerance and Proactive Recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

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

[19] CHEN H, WEI S M, ZHU C J, et al. Security Certificateless Aggregate Signature Scheme[J]. Journal of Software, 2015, 26(5): 1173-1180. (in Chinese)
陈虎，魏仕民，朱昌杰，等. 安全的无证书聚合签名方案[J]. 软件学报，2015，26(5)：1173-1180.

[20] LU H J, YU X Y, XIE Q. Provably Secure Certificateless Aggregate Signature with Constant Length[J]. Journal of Shanghai Jiaotong University, 2012, 46(2): 259-263. (in Chinese)
陆海军，于秀源，谢琪. 可证安全的常数长度无证书聚合签名方案[J]. 上海交通大学学报，2012，46(2)：259-263.