DOI：10.19729/j.cnki.1009-6868.2018.06.001
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20181203.1012.002.html

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]。

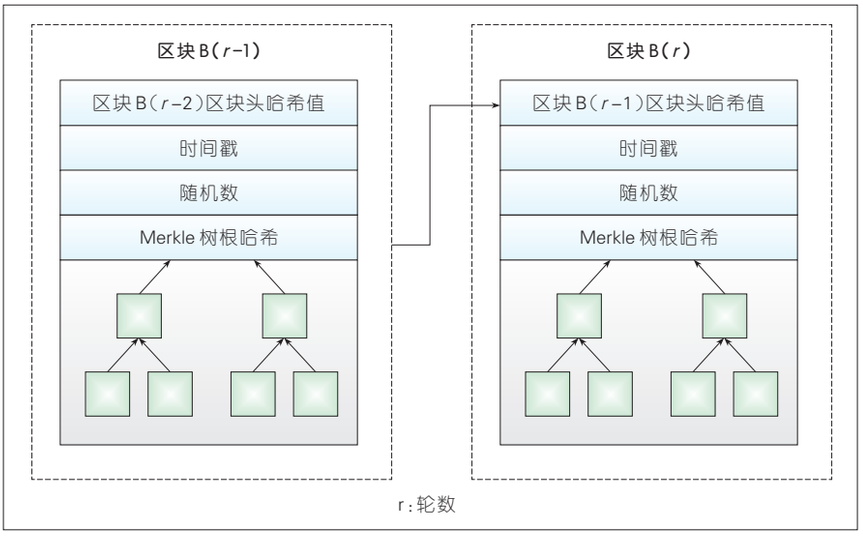
2.2 典型方案

（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$Merkle_{TX}$、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$H(A_{r-1}, Merkle_{TX}, Nonce) < D$，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。



▲图1 比特币区块结构图

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

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相关，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相关。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，可以同时在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来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, AI-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, Al-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] SOMPOLINSY 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] DAVAROANAH 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, JOVANOVIC 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, JOVANOVIC 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, JOVANOVIC 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。