文献引用格式：潘业达，陈恭亮，郭乃网等 . 区块链吞吐率提升研究 [J]. 通信技术，2019，52（01）：134-140.
PAN Ye-da,CHEN Gong-liang,GUO Nai-wang,et al.Research on Block Chain Throughput Improvement[J].Communications Technology,2019,52(01):134-140.

doi:10.3969/j.issn.1002-0802.2019.01.024

区块链吞吐率提升研究 *

潘业达[1]，陈恭亮[1]，郭乃网[2]

（1. 上海交通大学，上海 200240；2. 国网上海电科院，上海 200232）

摘　要：近年来，区块链作为一门新兴技术得到了广泛关注。但是，区块链技术离真正的投入使用还有相当长的一段路程需要走。目前，区块链无法投入生产的一个重要因素，是现存的区块链系统的低吞吐率无法满足现实生产的需要。例如，理论上，比特币是 7 TPS，以太坊是 15 TPS，而传统的中心化系统如 VISA，支持上千的 TPS。因此，分析限制区块链扩展性的主要因素，抽离出提高吞吐率的模型，并且针对每个方面进行具体分析，为以后的研究奠定基础。

关键词：区块链；吞吐率；安全；扩展性

中图分类号：F821；TP311.13　　**文献标志码**：A　　**文章编号**：1002-0802(2019)-01-0134-07

Research on Block Chain Throughput Improvement

PAN Ye-da[1], CHEN Gong-liang[1], GUO Nai-wang[2]

(1.Shanghai Jiaotong University, Shanghai 200240, China; 2.Shanghai Institute of Electrical Technology, China Network, Shanghai 200232, China)

Abstract: In recent years, blockchain has received extensive attention as an emerging technology. However, blockchain technology still has a long way to go before it is actually put into use. At present, an important factor that the blockchain cannot be put into production is that the low throughput rate of the existing blockchain system cannot meet the needs of real production. For example, in theory, Bitcoin is 7TPS, Ethereum is 15TPS, and traditional centralized systems such as VISA support thousands of TPS. Therefore, the main factors that limit the scalability of the blockchain are analyzed, and the model for increasing the throughput rate is extracted. And each of the above aspects is specifically analyzed to lay the foundation for future research.

Key words: block chain; throughput; security; scalability

0　引　言

随着数字货币的火热，区块链技术逐步进入公众的视野，并引起了广泛的讨论和研究。目前，虽然区块链各个方面的研究火热，但是距离真正投入使用、影响并改变人类现有的生活生产方式还很长的路需要探索。影响区块链投入使用的一个重要原因在于目前的区块链系统性能无法满足日常生产生活需求，其中最重要的瓶颈在于其低下的吞吐率。因此，本文分析限制区块链吞吐率的因素，分别举例说明如何突破这些瓶颈以提升区块链吞吐率，以期区块链更早投入生产。

* **收稿日期**：2018-09-09；**修回日期**：2018-12-14　Received date:2018-09-09;Revised date:2018-12-14
基金项目：国家重点研发计划“电子货币新算法与新原理研究”（No.2017YFB0802505）
Foundation Item: National Key Research and Development Program of China “Research on New Algorithms and New Principles Of Electronic Currency” (No.2017YFB0802505)

1　区块链概述

区块链技术是中本聪 [1] 构建比特币系统的底层技术，随着密码货币市场的火热，逐渐被学术界所关注和研究。区块链技术是集分布式系统、点对点网络、密码学于一体的新兴技术，主要解决了在没有引入可信第三方的基础上，在相互不信任的节点之间达成共识的问题。突出贡献在于，能够在拥有大量参与者的情况下（比特币十几万个节点），无准入且可以随时退出的情况下达成共识。这相较于传统的基于投票的 BA 类共识协议有了巨大的突破（在 PBFT 中，参与节点不能超过 100 个，且所有的节点需要引入可信第三方对节点身份进行认证，同时在协议开始运行后不能有新的节点加入）。

同时，区块链通过使用 Hash 函数、Merkle Tree、数字签名等密码学方法，构造出了一条证据链，使得上链的数据在经过有限的时间等待后无法被篡改，在各个节点之间形成一个公共的账本。区块链技术通过其开创性的共识协议，为互不信任的节点提供了一种信任机制，即由对传统意义上人、企业、政府等实体的信任，转移到对点对点网络、密码学等技术的信任，可能带来下一次的信息技术等革命。

2　区块链扩展性限制

虽然区块链技术的前景十分广阔，但目前技术发展并不成熟，无法支撑现阶段业务的正常运行，其中区块链的低扩吞吐率是最大的瓶颈。相较于比特币理论上的 7 TPS 和以太坊的 15 TPS，日常系统可能每秒转账（交易）量需要上千上万。如此低的吞吐率，在实际应用中杯水车薪。

如图 1 所示，区块链可以根据功能由低到高划分为密码基础层、网络层、共识层和应用层四个层次，分别对应于数字签名、Merkle 树等密码算法，点对点网络，POW、POS、PBFT 等共识协议，智能合约等上层应用。其中，密码基础层对于区块链的性能等影响主要体现在签名和验签过程，可以使用更加轻便的签名算法如 BLS 短签名；网络层性能瓶颈主要在于点对点网络的性能瓶颈，其突破需要点对点网络的进一步发展；应用层是构建在底层区块链网络上的具体应用，因此暂时不予考虑其对吞吐率的影响；而相较于其他三层，共识层是目前吞吐率的短板，限制了区块链性能的提升。因此，本文在主要讨论共识层提高吞吐率的模型，并举例分析如何实现吞吐率的提升。

图 1　区块链层次结构

共识层中，限制区块链吞吐率的主要因素是其链状的结构，因为只有被记录到区块链上的交易才是有效交易。决定交易吞吐量的因素有三点——出块速率、块的大小以及是否可以通过并行提高系统的吞吐率。因此，如果想要提高区块链的扩展性，要从这三个方面入手。但是，由于区块链的安全性限制，如果过度提高出块的速率或者区块的大小，会导致安全性的下降。同时，由于区块链的链式结构，通过并行来提高吞吐率十分困难。后续章节中，本文分析了限制上述三点的主要因素，提出了可能的解决办法，并且通过例举现存项目分析比较其优缺点。

3　通过提高出块速率提高吞吐率

由于区块链的链式结构，如果出块速率过快，会导致产生过多分叉，进而影响系统的安全性，如图 2 所示。从直觉上看，如果两个区块之间的时间间隔短于整个网络的网络延迟，会出现这种情况。假设将所有的节点进行线性排列，当第一个节点在高度 i 发出一个区块 B_i^1，然后逐个向后面的区块进行传递。如果在 B_i^1 到达所有节点前，最后一个节点在同一高度也产生了一个区块 B_i^n，并且向前传播。这样前一部分节点在高度 i 的区块为 B_i^1，剩余的节点在高度 i 的区块为 B_i^n，区块链产生了分叉。此外，随着出块速率的提高，分叉的可能性也在提高，其安全性呈指数下降，无法提供 50% 的安全性，攻击者可以用更少的资源攻陷区块链系统。如图 2 所示，随着出块速率的增加，安全系数呈指数下降，这在文献 [2] 中有具体说明。

如果想要提高出块速率而不影响吞吐率，则需要解决分叉问题。这里主要提出两种解决分叉的方

法：一是通过改进传统的拜占庭共识协议，二是通过改变区块链的结构，从传统的链式结构转换为有向无环图结构（DAG）[3]。

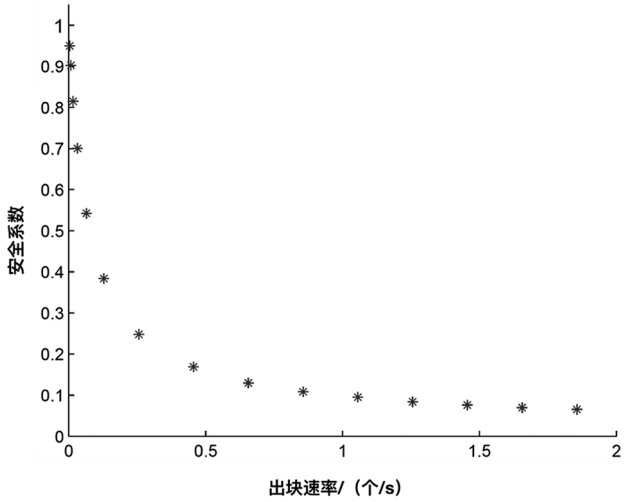

图 2 安全性与出快速率关系

3.1 改进的拜占庭共识

首先，区块链产生分叉的原因在于，节点可以在区块链的任意位置向后延伸，即在区块链的同一高度可以产生多个区块，而哪一个区块被最终确认是概率性事件。如果在区块链的相同高度只能产生一个区块，那么就不会产生分叉。而传统的共识协议对于一个事件的共识只有达成共识和不达成共识两种状态，因此如果使用基于传统拜占庭共识协议，并不会因为出块速率的提高而导致分叉的产生。但是，传统的共识协议并不支持大规模共识。例如，PBFT[4] 参与的节点数理论上不能超过 100，这在公链系统要求全网参与的情况下杯水车薪。因此，基于拜占庭共识的协议通常做法是通过某种算法，均匀采样产生一个委员会和一个备选区块。在委员会中对备选区块进行投票，如果投票成功产生区块，如果投票失败，这一轮不产生区块。需要注意的是，为了委员会中好人占的比例大致同整个网络中好人的比例相等，要求委员会的大小不能太小，需要远大于 100，这样传统的拜占庭共识协议无法满足需求，需要对现有的拜占庭类协议进行改进，以支持更大的参与者。这类协议中较优秀的是 Micali 教授提出的 Algorand[5] 算法，通过 VRF[6] 随机产生备选区块和委员会，并通过一个其称为 BA^* 的二元输出的拜占庭共识产生一个一致的输出。Algorand 算法的公平性体现在每一轮都会产生一个新的委员会，以保证委员会的代表性。

Algorand 在实验环境下 50 000 个节点参与，区块大小为 2 MB 的情况下，出块的时间间隔约为 12 s，吞吐率约为 327 MB/h，相较于比特币的 6 MB/h 提升了 50 倍以上。同时，实验表明，区块的大小在 Algorand 中对确认时间几乎没有影响，因此可以通过提高区块的大小进一步提高吞吐率。例如，在区块大小为 10 MB 的情况下，Algorand 的吞吐率大约为 750 MB/h，是比特币吞吐率的 125 倍。

通过使用改进的拜占庭共识的问题在于，为了使委员会中的坏人比例大致等于全网中的坏人，委员会的大小需要得到保证。在 Algorand 实验中，委员会的大小为 5 000 个节点，在委员会中需要进行多轮投票，导致网络会产生大量的投票信息而出现网络拥塞。

3.2 有向无环图（DAG）

传统的区块链中，同时有多个参与者在区块链的不同位置向后扩展，但是最终只有一条链会被接受，即从全局来看，全网生成的是一棵树状的结构，但为了能够为其中的区块提供一个不可篡改的顺序，即抽象出一个公共账本，区块链选择只接受其中一条链，其余分支将被舍弃。因此，不管用何种方法选取这条链，都会不断产生分叉。如果分叉的速率和数量太多，会影响系统的安全性。DAG（有向无环图）的思想是，如果将网络中的所有的区块全部包含到最终的状态图中，那么将不存在分叉。此外，还可以从两个方面提高系统的扩展性。第一，出块的速率可以更高，因为系统存在分叉，出块速率的加快不会带来安全性的降低。第二，在链式结构中，部分产生的区块被忽略了。在 DAG 结构中，所有的合法区块最终都会被包含在最终的系统中，所有参与者对于打包交易的贡献最终会体现在最后的系统状态中，实现了某种意义上的并行。

有向无环图同传统链式结构的主要区别在于，每个区块中不仅包含一个父区块的 Hash 值。有向无环图应当包含多个区块的 Hash 值，从而构成一个有向无环图的结构，且其包含的区块的 Hash 值应为在其本地视图下最新的没有子区块的区块。DAG 的结构如图 3 所示。

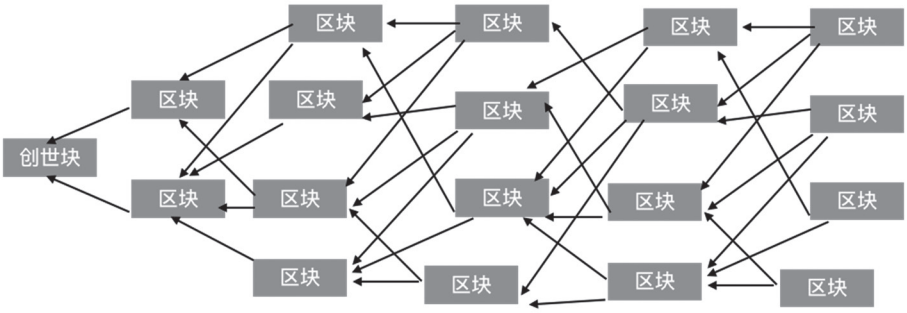

图 3　DAG 结构

如果使用 DAG 结构，其主要的挑战在于如何在一个有向无环图中提取出一个公共账本，或者说如何比较任意两个区块之间的先后顺序。目前，有两种方式。一种方式是对任意两个区块，通过直接或者间接连接到或被其连接的区块进行投票，获得票数多的区块被认为顺序更靠前。这里，计票过程在各个节点根据本地的视图中进行的。投票的原则在 SPECTRE[7] 中有具体描述，这里不再赘述。第二种方式是，在 DAG 中通过某种方法提取一条主链来为全视图中所有的区块给出一个唯一的序列号，进而构造出一个公共账本。这种方式在文献 [3] 中提出，假设有一个算法能够在 DAG 的视图中提取出一条主链，这条链需要满足区块链的安全属性，即链的增长性，公共前缀和链的质量 [8]。通过这条主链为全视图中的所有区块提供一个全视图唯一的序列号。目前，较为可行的办法是通过 Ghost[9] 方法进行主链的选择 Conflux[10]。Conflux 在构造有向无环图时，将连接前向区块分为父节点和叔节点，连接父节点的边为主边，连接叔节点的边为从边，父节点的选择是根据 Ghost 中的最重链原则进行选择。首先，去掉所有的从边，将视图从一个图退化成一棵树，在这棵树中使用 GHOST 算法，选择出一条主链。在 Conflux 中，在网络节点个数为 20 000、区块大小为 4 MB、出块速率为 0.4 个 /s、网络带宽为 40 Mb/s 的情况下，吞吐率为 6 400 TPS。

需要注意，目前 DAG 还处于基于 POW 阶段，使用 POS 的协议多存在安全性隐患，失去了区块链去中心化的意义。同时，由于 POS 的 DAG 不需要消耗资源，它可以在 DAG 的任何节点后产生区块，并且最终都会被包含在所有参与者的视图中，这样 DAG 的视图可能无法收敛。因此，目前 DAG 并不适合使用 POS 一类的不需要消耗资源的协议选取主链。同时，由于所有的合法区块都会被包含，区块中的数据有大量重复，造成了大量的数据冗余，其对扩展性的提高无法达到预期效果，且增大了存储负载。

4　通过变相提高块的大小提高吞吐率

一味地扩大块的大小会带来两种问题。一是随着块的增大，其广播到全网中所有节点的时间（网络延迟）会线性增长，如图 4 所示。出块速率是相对于网络延迟而言的，在出块速率不变的前提下，增加网络延迟变相地提高了出块速率，导致了更加频繁的分叉，进而影响了系统的安全性。二是当区块大小增大，则出块的节点所拥有的权利（打包交易的数量）随之增大，会导致某种意义上的中心化。可以想像，如果块大小无限大，那么这就是一个中心化系统。单纯提高区块的大小，会导致网络延迟的增加，因此可以将一个大区块拆分成许多小区块。小区块的确认独立于大区块，即小区块的接收可以随时停止，且全网都会同步到相同的小区块上。在现有的协议中，康奈尔大学博士后 Ittay Eyal 等人提出的 bitcoin-ng[11] 协议最具代表性。

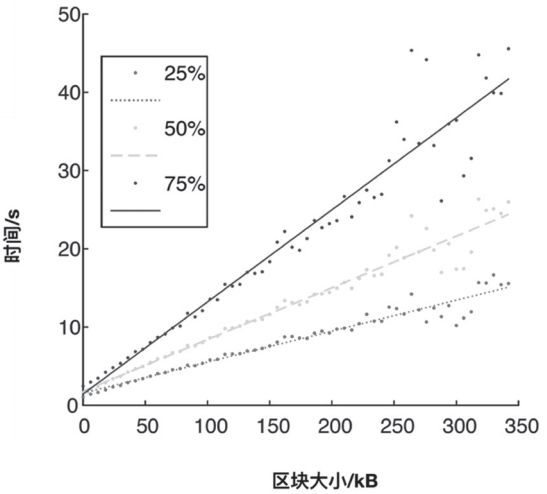

图 4　区块大小同网络时延关系

Bitcoin-ng 将区块分为主区块和微区块两种角色。主区块中包含工作量证明信息，微区块中包含

具体交易信息和产生主区块的节点签名。主区块之间的时间间隔需足够长，防止出现过多的分叉。从创世区块开始，所有的节点基于创世区块进行POW。成功算出 POW 的 nonce 值的节点首先产生一个主区块，其中包含 POW 的验证信息和自己的签名，广播到整个网络中。收到这个主区块的其他节点停止基于创世区块的 POW 工作。产生主区块的节点不断打包网络中的交易成为一个个微区块，将微区块广播到网络中去；其他的节点选择基于某个微区块进行下一轮的 POW，产生新的主区块，结构图如图 5 所示。

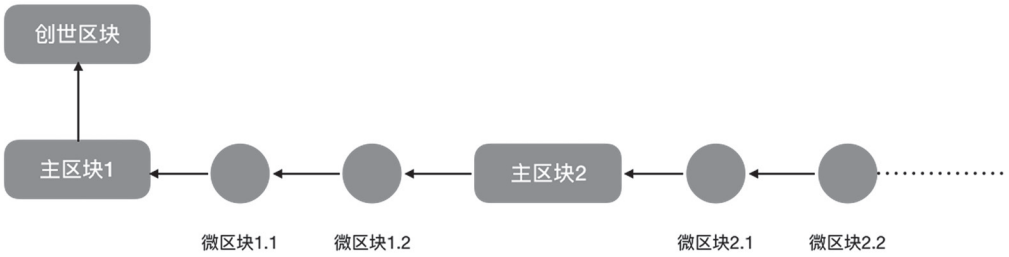

图 5 bitcoin-ng 结构

理论上，bitcoin-ng 的吞吐率只受单个节点处理速度的限制，因为高的吞吐率不会产生分叉。虽然微区块之间的时间间隔可以远小于主区块，但是其时间间隔不能够无限小。微区块的出块速率非常快时，会导致在主区块出块附近出现非常多的分叉，分散了算力，严重影响系统的安全性。

另一种拆分区块的方法是首先选出一个领导者，领导者不断打包交易直到产生新的领导者。这种协议中具有代表性的是康奈尔大学的 Elaine 教授提出的 Thunderella[12] 协议，主要过程为：

（1）选出一个加速节点；

（2）选出一个委员会；

（3）加速节点收集网络中的交易信息，将交易的信息进行排序后签名发送给委员会；

（4）委员会对交易进行投票，如果一条交易收到的票数超过了 3/4，那么这笔交易就被确认；

（5）否则，交易进入底层的区块链系统，等待足够长的时间，进行确认。

相较于 bitcoin-ng 在微区块之间需要有一定的时间间隔，Thunderella 中的领导者在两个交易之间不需要等待，可以连续向委员会发送交易，这样在领导者为诚实的且委员会中超过 3/4 是诚实的情况下，系统的性能瓶颈被限制在领导者的单节点处理速度和委员会投票的通信复杂度上。同 Algorand 一样，这种使用投票的共识协议会大大增加网络中路由交易信息的数量，造成网络拥塞。

5 通过并行提高吞吐率

区块链单条链的结构使得打包交易过程只能够串行进行，串行的模式导致难以通过并行提升效率。在串行模式下，吞吐率的上界被单节点的网络速度和处理性能从物理上被限制，且随着网络规模的增大，系统的性能不能同比上升，甚至会有所下降。为了使得区块链能够实现并行，可以有两种方法。一是将区块链系统分层，底层是区块链网络，只存储关键信息，上层负责具体交易的处理，上层之间相互独立，可以并行处理数据；二是借助分片技术，拆分系统中的资源，各个分片单独处理各自的交易。

5.1 分层

区块链的主要优势在于能够在互不信任的网络中提供一个较可信的环境，并且将所有的交互信息进行存储。但是，在实际的生产生活中，交易完整的处理过程不需要都在可信环境下，所有的数据也无需无差别存贮。事实上，只要在交易的重要过程能够提供一个安全环境，且对关键数据进行存储，就可以满足日常生产生活的需求。分层的思想是关键的交易和信息在底层的区块链执行和存储，非关键交易的具体执行和中间结果由参与方线下执行，线下的交易可以并行处理。从全局来看，这大大提高了系统吞吐率。

在分层的解决方案中，较具代表性的是闪电网络 [13]。在闪电网络中，需要进行交易的双方需要向区块链提交一个智能合约来创建交易通道，在智能合约中需要将一定量的代币锁定。在创建好支付通道后，交易双方在线下进行交易，交易的安全性通过多方签名来保证。交易结束后，将最后的状态提交到主链上，并且释放通道关闭交易。主要流程如图 6 所示。

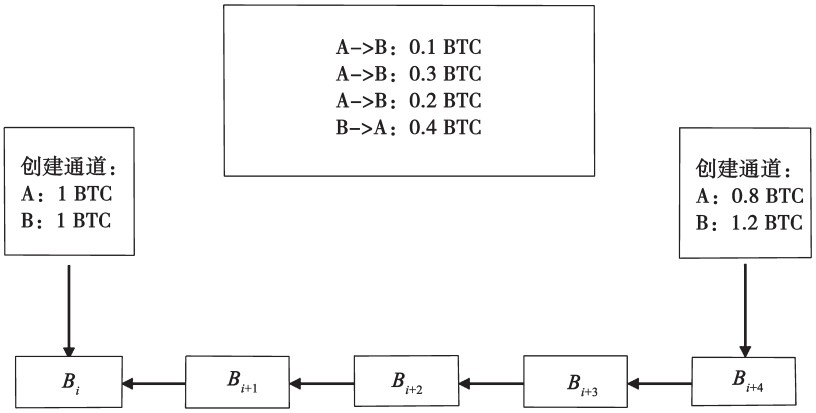

图 6　闪电网络交易过程

虽然闪电网络将多个交易简化成了两个交易，但是其使用范围十分受限。在闪电网络中，线下交易只能在已有直接或者间接通道的用户之间进行，同时只有在交易频率较高的情况下才能够体现出其优势。但是，在网络中存在大量的一次性交易，即 A 向 B 发送一笔交易后，后续长时间内 A 和 B 之间不会发送交易。在这种情况下，单笔交易会被扩展为两笔交易，得不偿失。

5.2　分片

分片技术是一种应用于数据库分片的传统扩容技术。它将数据库分割成多个碎片，并将这些碎片放置在不同的服务器上。在区块链情境中，网络上的交易将被分成不同的碎片，由网络上的不同节点单独处理。每个节点只需处理一小部分传入的交易，并且通过与网络上的其他节点并行运算，可以同时完成对交易的验证和处理。因此，随着网络规模的增长，区块链同步提升将成为可能，这种属性也称为水平扩容。

在区块链中，通过将参与者分片，每个分片单独处理，存储不同的交易信息。可以将每个分片想象成一个子链，所有的子链构成了完整的区块链。区块链中，分片的技术难点在于保证跨分片交易的原子性。一笔交易如果被接受，在所有的分片中都会被接受；如果不被接受，所有的分片都会拒绝这比交易。即状态的改变是原子性的，全网中的状态是相同的，如何实现在文献 [14–15] 中有具体的描述。同时，在分布式系统中，分片由中心节点来决定。但是，在区块链系统中，没有一个中心的系统来进行分片。要保证分片的随机性，需要有一个随机源来产生随机数进行分片。庆幸的是，区块链所要解决的问题是随机选取一个节点来打包交易完成出块，因此在现存的一些共识算法中可以提供这样一个随机源。例如，Algorand 中通过 VRF 产生随机数，或者通过 POW 产生的符合要求的 nonce 值（虽然这不是一个随机数，但是也是一个不可预测的值）。

6　结　语

本文总结了限制区块链吞吐率提升的主要因素，抽离出提升区块链吞吐率的架构，并从三个方面描述了提高区块链吞吐率的模型，举例进行了具体分析。在同一协议中可能会使用其中一种或多种，表 1 中例举比较了各个协议中提高吞吐率的情况。其中，Y 表示该协议拥有该特性，N 表示没有。

表 1　提升吞吐率协议对比

共识协议	提高出块速率	提高块的大小	并发
Bitcoin–ng	N	Y	N
Conflux(DAG)	Y	N	Y
Thunderlla	N	Y	N
Algorand	Y	Y	N
Ghost	Y	N	N
RapidChain	Y	N	Y

相信随着技术的发展，当吞吐率不再是限制区块链实用的主要影响因素时，区块链作为可能的下一代信息革命的优势将真正展现出来。

参考文献：

[1] Sompolinsky,Yonatan,Aviv Z.Secure High–Rate Transaction Processing in Bitcoin[C].International Conference on Financial Cryptography and Data Security,2015.

[2] Pass,Rafael,Lior S,et al.Analysis of the Blockchain Protocol in Asynchronous Networks[C].Annual

International Conference on the Theory and Applications of Cryptographic Techniques,2017.

[3] Sompolinsky,Yonatan,Aviv Z.Accelerating Bitcoin's Transaction Processing[Z].Fast Money Grows on Trees, Not Chains,2013.

[4] Castro,Miguel,Barbara L.Practical Byzantine Fault Tolerance[Z].1999.

[5] Gilad,Yossi.Algorand:Scaling Byzantine Agreements for Cryptocurrencies[C].Proceedings of the 26th Symposium on Operating Systems Principles ACM,2017.

[6] Micali,Silvio,Michael R,et al.Verifiable Random Functions[C].Foundations of Computer Science,40th Annual Symposium on IEEE,1999.

[7] Sompolinsky,Yonatan,Yoad L,et al.SPECTRE:A Fast and Scalable Cryptocurrency Protocol[Z].IACR Cryptology ePrint Archive,2016:1159.

[8] Garay,Juan,Aggelos K,et al.The Bitcoin Backbone Protocol:Analysis and Applications[C].Annual International Conference on the Theory and Applications of Cryptographic Techniques,2015.

[9] Sompolinsky,Yonatan,Aviv Z.Secure High-Rate Transaction Processing in Bitcoin[C].International Conference on Financial Cryptography and Data Security,2015.

[10] LI Chen-xing.Scaling Nakamoto Consensus to Thousands of Transactions per Second[Z].2018.

[11] Eyal,Ittay.Bitcoin-NG:A Scalable Blockchain Protocol[Z].2016.

[12] Pass,Rafael,Elaine S.Thunderella:Blockchains with Optimistic Instant Confirmation[C].Annual International Conference on the Theory and Applications of Cryptographic Techniques,2018.

[13] Poon,Joseph,Thaddeus D.The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments[Z]. DRAFT,2015.

[14] Kokoris K,Eleftherios.OmniLedger:A Secure,Scale-Out,Decentralized Ledger via Sharding[R].Cryptology ePrint Archive,Report 2017/406,2017.

[15] Zamani,Mahdi,Mahnush M,et al.RapidChain:Scaling Blockchain via Full Sharding[C].Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security ACM,2018.

作者简介：

潘业达（1993—），男，硕士，主要研究方向为网络空间安全、区块链技术；

陈恭亮（1961—），男，博士，教授，主要研究方向为应用密码学、信息安全、区块链技术；

郭乃网（1984—），男，硕士，高级工程师，主要研究方向为网络安全。