对可扩展的区块链构架的探索

——工作量证明区块链与拜占庭故障容错区块链的对比

Marko Vukolic

**摘要**

比特币展示了基于无数节点的全球共识之功效，这也永远改变了全球的数字事务处理方式。在比特币刚刚出现的时候，它表现为基于共识机制的盖然论的工作量证明，也被称为区块链，而在当时这不是一个主要课题。比特币获得了成功，尽管它的共识延迟被定为一小时，且它的理论生产量峰值仅为每秒7个节点。

而今天的情况则全然不同，早期的基于工作量证明的区块链已毫无可扩展性。特别地，现代电子加密货币平台的流行，例如Ethereum，正对随意分布式的区块链应用的执行产生支持，而它们则需要更好的表现。然而，这种趋势使得电子加密货币平台偏离了它们最初的目标，并进入了数据库复制协议领域，尤其是经典的状态机复制和拜占庭故障容错的变种。

本文将对基于工作量证明区块链（以下简称PoW）和基于拜占庭故障容错的状态机复制的区块链（以下简称BFT）进行对比，关注它们在可扩展性上的限制。本文也会讨论目前对于区块链的有限可扩展性的解决方案，并且概述未完成的对于探索区块链理想构架的关键开放性问题。

**关键词**

比特币，区块链，拜占庭故障容错，共识，工作量证明，可扩展性，状态机复制

**1.介绍**

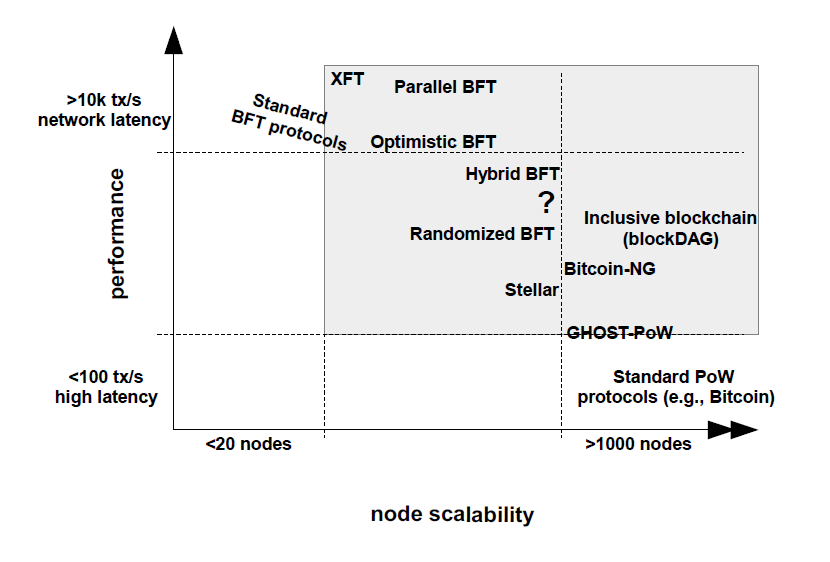
分布式共识算法，因其有限的可扩展性而不受重视，几十年来仅用于极度需要连贯性的应用的原始同步，并且仅基于少量节点存在（见[8,28]）。然而，中本聪的比特币[48]证明了基于无数节点的分布式共识算法的功效，而这将永远地改变电子交易市场。

尽管比特币协议实际上并没有实现传统的分布式算法的一致性，但它很接近于基于概率的共识算法[26]。简而言之，像比特币这样的电子加密货币的目标是全部整理为一份分布式账本，这也被叫做区块链。比特币的区块链基于一系列的哈希链:每个区块包含了一笔特定的交易和上述的区块碎片（从所谓的起始区块开始）。关键部分是哈希链的工作量证明部分[22]：每个比特币区块由一个特殊的比特币矿工（一个尝试增加区块的节点）所构成，这种比特币矿工必须使整个区块小于可知目标，而这通常是个很小的数字。实际上，比特币矿工进行开采的困难在于要使系统能从始至终地动态适应，并与目标成反比例。调节器根据开采率来制造，然后间接地关系到系统中节点的计算能力，以此来保持每10分钟一个的区块开采率。这十分钟（每个区块）的延迟经常被成为块频率（见e.g.,[23]），这也是比特币的两个重要的“魔法数据”的其中之一，而另一个则是被设定为1MB的块大小。

在比特币技术刚出现时，它盖然论的、基于工作量证明的区块链的性能可扩展性并不是一个主要课题。即使是今天，比特币形成共识的周期为大约一小时（用来完成所推荐的六区块的交易确认），工作量峰值则是每秒七笔交易（200-250比特大小的交易）。因此比特币网络需要大量电力，在2014年，这个量估计在0.1-10GW。

然而，区块链的需求迅速改变，像比特币这样的高延迟、低产出的区块链迎来了巨大的挑战。作为比较，全球领先的信用卡支付公司平均每秒可大约支持2000笔交易，最高甚至可支持超过10000笔交易。此外，随着像Ethereum这样的现代电子加密货币平台的流行[58]，正对由智能合约组成的区块链构造的图灵完全代码的执行产生支持，通俗地讲就是，自执行程序（分布式的应用）有着自动执行数字合约的属性。事实上，在很多行业中，智能合约型区块链被视为分布式账本的替代技术。很明显，在大量的已定的用例智能合约中，分布式的应用表现得远比比特币更好，银行业是一个显著的例子。在银行业中潜在的用例区块链表现得比数字支付更好[46]，比如证券交易结算和贸易融资。

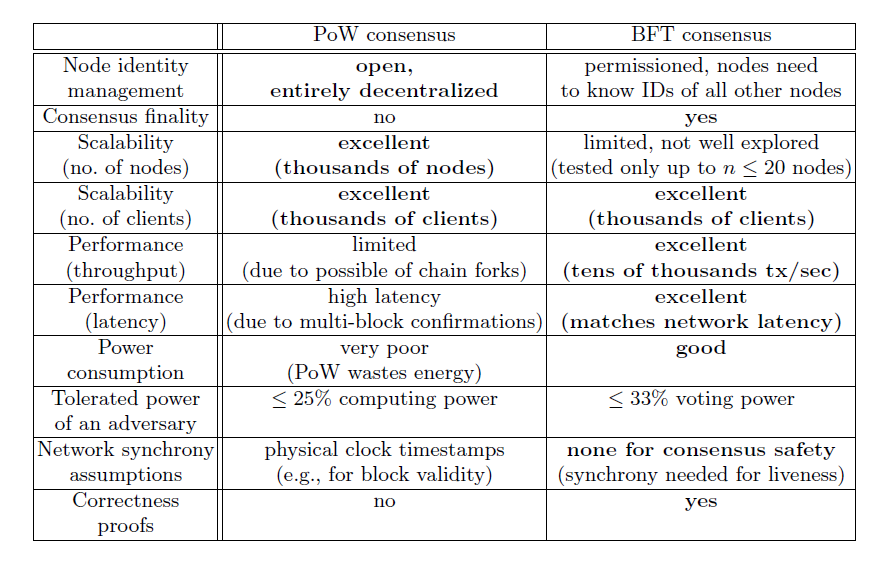
区块链最初被设计为电子加密货币，而回到数据库复制协议的领域，特别是经典的状态机复制，用例智能合约的表现远远地超出了预期[54]。实际上，可以将一个智能合约建模为一个状态机，并使用状态机复制实现分布式环境中跨多个节点的一致执行。有趣的是，区块链的一系列状态机复制协议就是一系列的拜占庭故障容错的状态机复制协议，这保证了一致性但会出现故障（拜占庭故障）节点。在超过三十年的研究中，BFT的原型已被证明是实用的[10]，达到了几乎是网络所允许的最小延迟，并且支持每秒完成数千笔交易（见[35,3]）。然而，拜占庭故障容错和广义的状态机复制协议经常受限于它们在节点（副本）数上的可扩展性，并且还没有在这对于区块链来说十分重要的方面被彻底测试过。

总的来说，现今的区块链共识技术——PoW和BFT——在可量测性范围的两端。粗略地讲，前者有更好的节点扩展性但是较差的性能，而后者则能提供更好的少量副本和较差的可勘测性和有限的可量测性。这一关于区块链可扩展性的现状草拟与图一中。鉴于在副本数量和性能之间看似固有的平衡，至今还不清楚对于这些数量不等的用例节点的最优解。

**图一**是对本文所讨论的PoW和BFT在性能和可扩展性两个方面的图解。事实上，涉及灰色区域的系统的真实性能有待进一步研究。因此，它们在灰色区域的定位目前来说完全是推测性的，只是出于动机目的。

在本文中，我们将看到近来为改善两者的频谱扩展性而做出的努力，并强调关于追求理想的区块链结构的关键方向和问题。首先，在第二部分我们将比较上述的两种区块链协议。而在第三部分中，我们会将概述定标两种协议的有效方法。在第四部分，我们将通过一些会在不久的将来获得解决的开放性问题来进行总结。

**2.工作量证明协议和拜占庭故障容错协议区块链的比较**

表格1给出了上述两种区块链协议的一系列重要指标的高层次比较。这些特性包括了节点身份管理、共识的终结（或是区块链短暂交叉的可能性）、共识节点和客户数量的可扩展性、性能（延迟、生产量、功耗）、容错率、网络同步假设和关于协议潜在区块链的存在性证明。这组属性当然不是详尽无遗的，但我们相信它能有代表性地对比两种区块链。在余下部分中，我们将对表格1的细节进行讨论。

**表格1**两种区块链协议的一系列重要指标的高层次比较。粗体条目显示了令人满意的特性，突出了一个协议相对于另一个的优势。

**节点身份管理**

如何对节点的身份进行管理大概是两种区块链协议间最根本的区别。PoW具有完全分散的身份管理功能——比如，任何人可以为比特币款共下载代码，然后开始参与这串协议并基本知晓开始的那一个对等点。这使PoW有一个光明的未来，任何人都被允许参与便是它被称为公共区块链的原因。这种公共区块链有时也被叫做无需许可的区块链——无需许可的参与可能由PoW产生，因为其天生可以解决在匿名网络中臭名昭著的女巫攻击（the Sybil attack）[18]。另外，在PoW中，节点（或节点池）影响区块链产出的能力取决于节点的计算能力。

与此相反，BFT达成共识通常需要每个节点知道整个组的节点参与的共识。相应地，这需要一个（逻辑上）集中的身份管理系统，在这之中一个可信的同伴

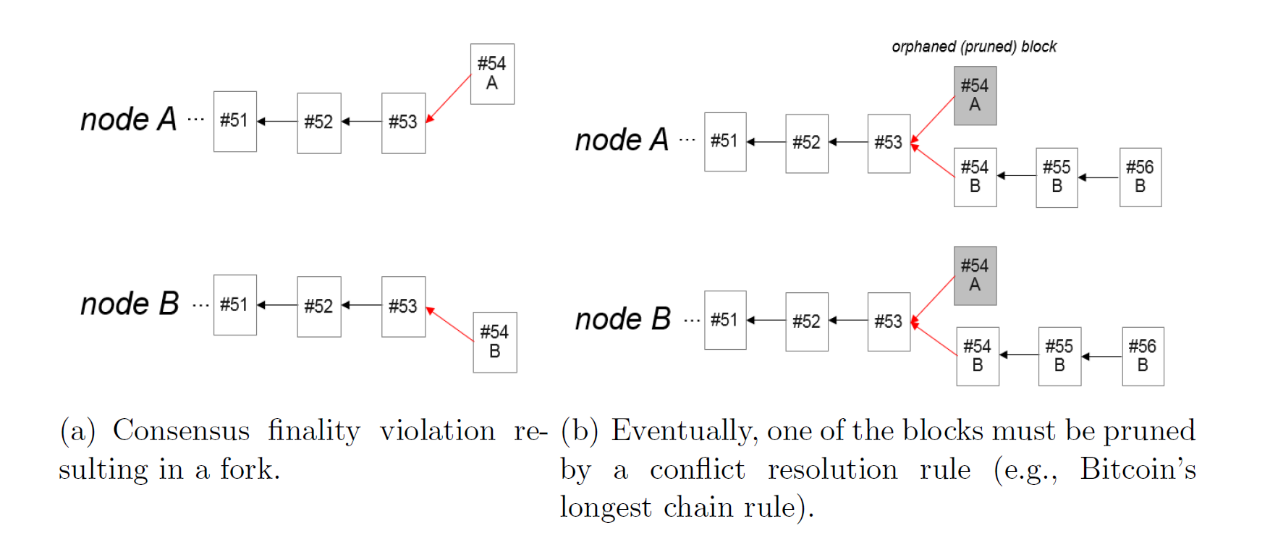
发布节点的身份和加密证书。1直观地说，在这方面BFT是弱于PoW的。也就是说，在许多新兴的区块链应用中（如银行业、金融业、土地和房地产行业的所有权分类账），节点的身份信息会因为法律和承诺的原因而被强行要求。这就解释了为什么BFT共识协议是所谓的准入区块链的技术选择，这种区块链要求参与者的身份需被知晓。

**共识的终结**

大致来说，共识的终结（有时叫做前行安全性[15]）是一种属性的非正式称呼，而这种属性是指有效块会在某个时间点被强制添加到区块链上，并再也不能被移动。在标准的分布式计算术语中，共识终结出现在全序和全序（原子）广播的一致性联合之后[17]，而这则是原始的全状态机复制协议的根基。而转化为区块链的术语后，这个特性可以表述如下：

**定义1（共识终结）。如果一个正确节点P在添加块B’前，将块B添加到它的复制链上，然后错误节点Q则以相反的顺序添加块B和块B’于它的复制链上。**

共识终结是不利于PoW区块链的。需要注意的是，除去对于身份管理的需求之外，PoW也是一种随机的并发控制机制，在这种机制中块频率将是动态的，因此块冲突（即同时添加不同的块于区块链上）将会很少发生。然而，由于并发控制只是概率性的，网络上的块传播可能需要一些时间[16]，冲突确实会发生，并导致BFT倾向于产生短暂的链交叉，尽管所有的节点都是可信的。这些短暂的链交叉（举例见图2）由规则来解决，比如比特币最长（最困难的）交叉法则[48],或幽灵法则（一种在Ethereum使用的变体）[55]。然而，临时链交叉的存在不意味着共识终结。正如我们在以下所讨论的更多细节中所显示的，共识终结的缺失直接影响着PoW的共识延迟，因为一笔交易需要紧跟着一些块来防止其最终

被从区块链上删除（我们称之为多块确认）。

**图2**共识终结、链交叉和冲突解决的例子

相反地，共识终结被所有的BFT和状态机复制协议所满足。2这给了BFT一个相对PoW来说很大的优势，因为应用、用户和智能合约能够拥有将交易转化为区块链的即时确认性。

**可扩展性**

尽管脱离了性能（延迟和产出）来解耦区块链的可扩展性（根据系统中节点和客户的数量）问题是不完全可行的，不过我们首先着眼于已被证明在实际工作的PoW和BFT技术中节点和客户的数量。

一方面来说，比特币网络在无数的矿点中起主要作用，并在实践中证明了PoW节点的可扩展性。也就是说，值得一提的是，将矿工分组进入矿池（伴随着分裂挖矿奖励和使得挖矿在经济上更可预测的努力目标）的工作给比特币带来了麻烦，但使电子加密货币的集中更为有效[27]。我们注意到，矿池的集中不是比特币的一个特殊特征，而是PoW区块链普及的结果，这影响着许多山寨币（比特币型的替代电子加密货币）以及流行的区块链，比如Ethereum。

另一方面来说，BFT和状态机复制大体上被认为是可扩展性差的协议（见， Brewer’s CAP theorem[8]）。然而，基于传统应用（比如数据库）的再创造而被

发明的、目标为容错的BFT协议的可扩展性永远不会被真正地彻底测试，最多只会测试10个或20个节点，特别是在许多的区块链应用表现的公平谦虚的情况下。直观地说，由于它们密集的网络通信（每一块包含了无数的信息）[10]，在数据库和系统社区中的BFT协议被视为不可扩展的（也见于[45]）。3即使是对它们的容错同行（比如Paxos[37]，Zab[31]和Raft[50]这样的复制协议）来说也是正确的，这些则在许多大型系统中被使用但实际上从来不会超过几个副本（见e.g., [13]）。

最后，当谈到客户数量的可扩展性时，两种区块链协议都支持上千客户的规模。

**性能**

由于每秒七笔交易的限制（按现有的区块尺寸来计算）和六区块确认机制导致的一小时延迟，PoW区块链正面临着内在的性能挑战。正如我们已经讨论过的，两个PoW的与性能有关的参数分别是区块尺寸和区块频率。因为在因特网上，更大的区块意味着更长的延迟，所以以提高生产量为目标而增加区块大小，随之而来的代价就是更长的延迟。因为短暂链交叉和缺乏共识终结的可能性，在PoW区块链中，延迟的增长会对区块链的安全造成负面影响：更长的延迟会导致更多的链交叉和增加发生双重支付攻击的可能性[34]。若以减少多块确认的延迟为目标而增加区块频率，也会导致相思的安全问题。在PoW区块链中，调整块频率和块大小而产生的真正安全问题一般是相当复杂的（见， [55]作为分析），需要被认真对待。在此基础上，对于PoW区块链来说，有限的性能似乎是固有的。

相比之下，现代的BFT协议已经被证实能够以实际网络速度的延迟维持成千

上万的交易，不仅是作为原型（见[35，12，3]），更作为实际的系统[5]。

**敌对**

PoW和BFT考虑不同的敌对。在PoW区块链中，重要的是敌对方控制的总计算（哈希）功率。最初，只要敌对方控制散列能力低于50％，比特币就被认为是无懈可击的。多年以后，事实表明，即使只有25％的计算能力被敌对方控制，比特币挖掘实际上也是脆弱的[24]。相比之下，BFT协议已知最多可允许有n/3个破坏的节点[20]。这种限制只有在网络允许（随时间而改变）完全异步时才能成立——加强同步假设使得提高这个门槛成为可能。经典的BFT共识的n/3阈值界限可以推广到一般的敌对结构，其中攻击者可以控制不同的节点子集[29,57]。

**网络同步**

比特币依靠节点的本地时间来标记时间戳。粗略地说，如果一个块的时间戳大于最后11个块的中间值，则该块被认为是有效的。此外，时间戳在计算挖矿和维护块频率的难度方面也起着重要作用。因此需要宽松的时间同步限制。但是，时间戳操纵攻击也可能会破坏区块链的一致性（可参见“时代精神攻击”[1]）。虽然这种类型的攻击难以对付像比特币这样的主流区块链，但它们已经在一定量的PoW区块链中被成功地执行了。

BFT协议通常不依赖于任何物理时钟4。然而，由于FLP共识的不可能性，最终需要同步通信来保证活跃性，这表明一致性不可能以纯异步方式确定性地实现具有潜在故障的节点系统[25]。尽管有全球通信中断和任意时长不同步的情况，协商共识的安全性仍然能得到保持。

**正确性证明**

从历史上看，状态机复制协议，尤其是BFT变体，其的设计和实现已经被认为是非常具有挑战性的[11，5，3]。因此，新协议需要经过详细的学术研究，因此需要（或多或少）详细证据，有时甚至需要通过整个博士论文的方式来证明（见[14,41]）。即使可以理解当初比特币没有经过类似的研究就被部署，新的PoW区块链很少伴随详细的安全分布式协议和安全分析的情况还是相当令人惊讶的。

**3.改善区块链的可扩展性**

在本节中，我们将概述并讨论一些最近致力于改善PoW和BFT区块链的可扩展性方面的工作。

**提高PoW区块链的性能**

最近，Sompolinski和Zohar提出了GHOST（Greedy Heaviest-Observed Sub-Tree）法则[55]，它基本上通过平衡根植于块中的子树而不是根植于给定块的最长（子）链来解决PoW区块链中的冲突。尽管GHOST本质上是一个冲突解决策略，但是它比比特币标准的最长（最重）链规则提供了更好的性能优势，因为它给出了更加安全的提高块频率和块大小的方法[55]。不过，遵循GHOST法则的PoW区块链的性能还没有在高负载的情况下进行充分的压力测试（在2016年，典型的Ethereum吞吐量每天少于20,000次交易，也就是说，平均约0.2tx / s）。5

Bitcoin-NG是由Eyal等人提出的新颖提议[23]，它使用标准的PoW协议进行领导选举，并宣布一个能够找出标准难度块（称为密钥块）的节点成为领导者，直到找出新的密钥块为止。同时，与此同时，领导者可以将微块添加到链中，这些链不受PoW挖掘的限制，而只是被拼凑在一起。因此，微块锁可以显著增加

整个系统的吞吐量，并减少延迟（实际上Bitcoin -NG还在实践中进行压力测试）。从某种意义上说，Bitcoin -NG将领导者选举（通常在BFT协议中看到）和在领导者选举时期以领导者为中心的协议混合在了一起。但是，基于BFT区块链协议的Bitcoin-NG的困难之处在于，领导者选举部分是基于PoW的。因此，在Bitcoin-NG中，链交叉依旧可能发生，也不能保证达成共识，这可能导致如前面讨论的资产双重支出一样的安全问题。

**通过并行化缩放区块链**

Lewenberg等人最近提出，在PoW协议背景下，通过使区块链DAG（有向无环图）而不是线性链块来缩放区块链[39]。这个想法是允许非冲突交易（例如，那些不构成双重支出尝试的交易）最初在不同的分支上，但最终通过挖掘它们包含在分类账中的块，以此合并分叉。6BFT和状态机复制社区还利用独立请求（事务）执行的并行化（参见[33,43]）深入探索了几年来的并行复制思想。

**消除BFT协议中的通信和资源开销**

正如我们已经讨论过的那样，阻碍了BFT协议在区块链中被广泛应用的是它们在节点数量方面的可扩展性。Stellar [44]是一个持续的尝试，其旨在从BFT协议中删除一致接受的成员列表，同时保持其他BFT优于PoW的优势。而其他方法则希望在不改变成员假设的情况下来改善BFT的可扩展性。这些方法包括积极的BFT协议[52,3]，其特点是在“通常情况”下的线性通信复杂性，并且仅在网络和传统协议（如PBFT[10]）过程故障模式下特别不利。然而，即使是积极的BFT协议，与容错复制协议（见[37,31,50]）相比，也会有资源和通信开销，这在实践中得到了更好的证明，并且可以作为BFT的基准。

为纠正这一点，刘等人最近提出了一个新的网络和节点故障模型，称为XFT

模型[40]，它使得区块链能容错高达n/2的拜占庭节点。同时，XFT具有消息模式的特征，以适应崩溃容错的复制协议，即没有与典型的BFT消息模式有关的开销。如此，XFT（“交叉”容错）能够挑战BFT的攻击者同时控制网络和拜占庭节点的能力，将网络错误从拜占庭节点故障中解耦出来，并基本上将他们隔离。因此，XFT成为了一个攻击者更为逼真的模型，和PoW区块链一样，对手控制整个通信网络的能力将不再是重点。

最后，基于BFT的区块链的另一个吸引人的未来方向是BFT协议，它利用部分可信硬件（见[32]）来改善通信并降低资源成本。

**随机BFT**

随机BFT协议（见[7,56,9]）是最终同步的[21] BFT协议（如PBFT）的标准替代品。具体而言，随机BFT协议通过保证非常高的概率（总是除了可忽略的概率以外）而不是确定性来避免FLP一致性的不可行结果[25]。这允许随机BFT协议完全异步[4]。

多年来，随机BFT协议的一个问题就是它们的性能。具体而言，与最终同步的确定性BFT协议相比，经典的随机BFT（见[4,7,56,9]）效率非常低，这主要是因为他们使用的密码工具。然而，随着新的随机化BFT协议（如Honey Badger）的出现，这种情况可能会很快发生变化。通过选择最好的随机密码工具，Honey Badger展示了具有高达约100个节点的良好实际性能（即相当高的吞吐量）作为非常大批量的处理请求。很明显，大量的批次会对等待时间产生负面影响，但这可以通过混合BFT协议来解决[2]，这种协议可以将非常有效的积极和确定性BFT协议（如[3]中描述的协议）与实用随机协议（如Honey Badger）结合起来。这种混合BFT协议的早期例子可以在[2,36,52]中找到，但是通过使用[3]中描述的模块化的BFT设计框架，可以促进未来混合BFT协议的发展。

**混合PoW和BFT**

最近，Decker等人[15]已经提出用BFT（具体来说，PBFT协议[10]）来增强PoW区块链，主要是通过使用BFT来确保PoW区块链的共识终结。SCP[42]也提出了一种混合PoW / BFT协议，这种协议使用PoW进行身份管理，使用（并行和分层的）BFT来获得协商的共识。显然，上述关于按照节点数来缩放BFT的重要性的讨论对于混合PoW和BFT的这种方法也是至关重要的。

**4.结论和开放性问题**

我们简要介绍了最新的技术发展状况以及可伸缩区块链的新兴方向。我们对比了工作量证明（PoW）和拜占庭容错（BFT）共识协议，指出了它们各自的优点。

未来的工作将是非常有活力和有趣的。为了使图1能够更加精确，即，使各种协议放置在正确的位置，这与其节点的可伸缩性相比需要进行大量的研究，但是这代表了一个需要更好理解的即时性开放问题，这将促进未来区块链可伸缩性的改善。此外，PoW和BFT之间的协同作用还有很多潜力，无论是在协议技术方面，还是在改善对抗性和网络模型方面。

最后，对于要求最苛刻的区块链应用来说，探究如何应用硬件成本巨大的BFT协议（例如，密码术）将是很有趣的。一般来说，在硬件上实现共识确实是很有吸引力的，并且可能获得令人印象深刻的性能，正如最近在碰撞容错方面探索这个想法的提议所证明的那样[51,30]。

**参考文献列表略**