## 摘要

比特币(Bitcoin)加密货币展示了跨越数千个节点的全球共识的效用，永远改变了数字交易的世界。在比特币的早期，基于概率工作证明(PoW)的共识结构(也称为区块链)的性能不是一个主要问题。比特币成为了一个成功的故事，尽管人们普遍认为比特币的延迟约为一个小时，理论上的峰值吞吐量也只有每秒7笔交易。今天的情况完全不同了，早期PoW区块链的性能可伸缩性差不再有意义。具体来说，现代加密货币平台(如Ethereum)的趋势是支持在区块链结构上执行任意分布式应用程序，需要更好的性能。然而，这种方法使加密货币平台偏离了最初的用途，进入了数据库复制协议的领域，特别是经典的状态机复制，特别是其拜占庭容错(BFT)变体。在本文中，我们将基于粉末的区块链与基于BFT状态机复制的区块链进行了对比，重点讨论了它们的可扩展性限制。我们还讨论了最近为克服这些可伸缩性限制而提出的建议，并概述了在寻求“最终”区块链结构时尚未解决的关键问题。

关键词:比特币，区块链，拜占庭容错，一致性，工作证明，可扩展性，状态机复制

## 1介绍

分布式协商一致因其有限的可伸缩性而臭名昭著，几十年来被认为是一种同步原语，只能在极度需要一致性的应用程序中使用，而且只能在少数节点之间使用(参见e.g.，[8,28])。然而，中本的比特币加密货币[48]展示了分散共识在数千个节点上的效用，永远改变了数字交易的世界。

虽然比特币协议并没有真正实现传统分布式计算意义上的共识，但它与概率协议[26]非常接近。简而言之，比特币等加密货币的目标是在分布式账本(也称为区块链)上完全订购交易。比特币区块链由区块的哈希链组成:每个区块都包含一组有序的交易和前一个区块的哈希(从最初的所谓“genesis”区块开始)。关键部分是hashchain[22]的工作证明(Proof-of-Work, PoW)方面:比特币块包含比特con挖掘器(即，试图向链中添加块的节点)必须以这样一种方式进行设置，即整个块的哈希值小于已知的目标(通常是一个非常小的数字)。事实上，在比特币中，挖掘的难度与目标成反比，在系统的整个生命周期内都是动态调整的。对块挖掘速率进行了调整，并间接地对参与系统的节点的计算能力进行了调整，以便将期望的块挖掘速率保持在大约每10分钟一个块[48]。这种10分钟的延迟(每个块)通常被称为块频率(参见[23])，是比特币中两个关键的“魔法数字”之一，另一个是块大小，在比特币中设置为1mb。

在比特币早期，其基于概率粉末的区块链的性能可伸缩性并不是主要问题。即使在今天，比特币的一致延迟约为1小时(用于推荐的6块事务确认)，峰值吞吐量最高可达每秒7(7)个事务(最小的200-250字节事务)。最重要的是，比特币网络使用了大量电能，据估计，2014年的电量约为0.1至10吉比特。

然而，区块链需求变化迅速，类比特币区块链的高延迟、低吞吐量成为[6]面临的主要挑战。相比之下，全球领先的信用卡支付公司平均每秒处理大约2000笔交易，峰值容量设计为每秒维持超过10000笔交易。此外，现代加密货币平台(如Ethereum[58])的趋势是支持以智能契约的形式在区块链结构上执行图灵完备的代码，大致来说，智能契约是自定义、自执行的程序(分布式应用程序)，自动执行数字契约的属性。事实上，智能合同区块链在许多行业被视为分布式账簿的候选技术。显然，在许多预期的智能合同用例中，分布式应用程序需要比比特币提供的性能好得多的性能。银行业是一个突出的例子，其中潜在的区块链用例远远超出了数字支付[46]，例如，证券交易结算和贸易融资。

智能契约用例将区块链带回到数据库复制协议(尤其是经典的状态机复制[54])的领域，远远超出了它最初的加密货币用途。实际上，可以将智能契约建模为状态机，并且可以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。对于区块链来说，一组状态机复制协议特别有趣，它们是拜占庭容错(BFT)[38]状态机复制协议，尽管有恶意(拜占庭)节点参与，这些协议仍然能够达成一致。在30多年的研究中，BFT协议原型已经被证明是实用的[10]，可以达到网络允许的最小延迟，支持每秒数万个事务(参见，[35,3])。但是，BFT和状态机复制协议通常在节点数量(副本)[8]方面的可伸缩性常常受到挑战，这方面对区块链至关重要，尚未经过全面测试。

总之，当今的区块链共识技术(PoW和BFT)处于可伸缩性谱的两端。粗略地说，基于powbase的区块链提供了性能较差的良好节点可伸缩性，而基于bft的区块链则为少量副本提供了良好的性能，但还没有得到很好的研究，而且直觉上可伸缩性非常有限。图1概述了区块链可伸缩性的当前状态。考虑到副本数量和性能之间看似固有的权衡，目前还不清楚最佳的区块链解决方案是什么，它适用于节点数量从几十个到1000个(或数千个)的许多用例。

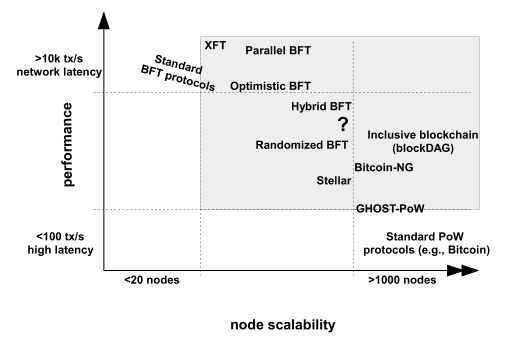


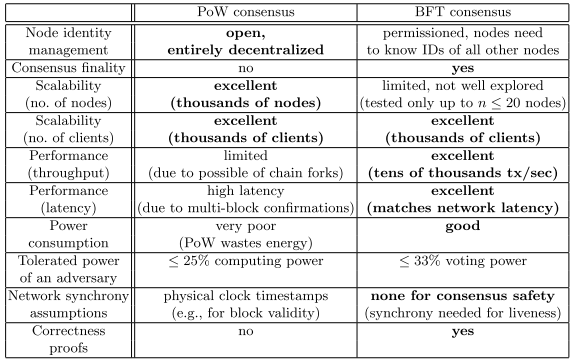
图1所示。本文讨论了不同种类的PoW和BFT协议的性能和可扩展性。涉及灰色区域的系统的实际、实际性能有待进一步研究。因此，他们目前在灰色地带的定位完全是推测性的，只是出于动机

在本文中，我们概述了近年来在提高可扩展性方面所做的努力，并重点介绍了标准PoW协议(如比特币)>1000节点比特币- ng包含区块链(blockDAG)并行BFT性能标准BFT协议的有趣方向和开放问题。

## 2 . PoW vs. BFT区块链

表1给出了一组重要区块链属性的PoW共识和BFT共识的高级比较。这些属性包括节点身份管理、共识结尾(或者,双层,临时blockchain叉)的可能性,可伸缩性的共识节点数量和客户而言,性能(延迟、吞吐量、功耗),容忍对手的力量,网络同步的假设,最后但并非最不重要,存在潜在blockchain协议的正确性证明。这组属性当然不是详尽无遗的，但是我们相信它可以用来比较两个区块链家族。在本节的其余部分中，我们将更详细地讨论表1。

表1。PoW和BFT区块链家族对一组重要区块链属性的高水平比较。粗体的条目显示了理想的特性，并突出了一个一致意见家族相对于另一个家族的优势。



节点身份管理。在PoW和BFT协议中如何管理节点标识可能是它们最根本的区别。PoW区块链的特点是完全分散的身份管理——例如，任何人都可以下载比特币矿商的代码，并开始参与协议，基本上只知道一个对等点。这是PoW区块链的一个非常强大的特性，也是他们成为所谓的“公共”区块链的区块链家族的主要原因。这样的公共区块链有时也被称为“无许可”区块链——无许可参与由PoW实现，因为PoW本质上解决了匿名网络中臭名昭著的Sybil攻击[18]。具体地说，在基于粉末的区块链中，节点的能力(resp)。影响PoW一致性结果取决于节点的计算能力(resp)。、游泳池)。

相比之下，BFT的协商一致方法通常要求每个节点都知道参与协商一致的所有对等节点。这反过来又需要(逻辑上)集中式身份管理，在这种管理中，受信任方向节点发出身份和加密证书。从直觉上讲，基于bft的区块链在这方面与PoW区块链相比处于劣势。也就是说，在许多新兴的区块链应用程序(例如，银行、金融、土地和房地产所有权分类账)中，出于法律和遵从性的原因，可能会强制要求节点的已知身份。这就解释了为什么BFT共识协议是所谓“许可”区块链的首选技术，因为区块链需要知道区块链参与者的身份。

共识的态度。粗略地说，通常非正式地称为协商一致终结性(有时也称为转发安全性[15])的属性要求永远不要从区块链中删除在某个时间点附加到区块链的有效块。在标准的分布式计算术语中，一致性的终结来自于总顺序广播[17]的总顺序和协议属性的组合，总顺序广播[17]是所有状态机复制协议构建的基础(总顺序广播等价于一致性)。转换为区块链术语后，该属性的措辞如下

定义1(共识终结)。If 正确 节点 b p 附加 块 的 复制 blockchain 之前 附加 块 b, 之前 没有 问 正确 的 节点 附加 块 b b blockchain. 副本

基于粉末的区块链不能满足协商一致的最终结果。要了解原因，请注意，除了消除身份管理的需要之外，PoW还充当了一种随机并发控制机制，在这种机制中，可以调整块频率，从而使块冲突(即，不同块的并发追加到区块链)是罕见的。然而，由于并发控制仅是概率性的，而且块在网络上的传播可能需要一些时间，因此会发生冲突，从而导致基于粉末的块链在区块链上产生临时分支，即使所有节点都是诚实的，这种分支也很容易出现。这些临时分叉(见图2)由比特币最长(最困难)的分叉规则[48]或GHOST规则[55]等规则解决，后者是Ethereum使用的变体。然而，临时分叉的存在并不意味着协商一致意见的最终结果。下面我们详细讨论,缺乏共识的结尾直接影响战俘blockchains的共识延迟交易需要跟着几个街区的概率增加事务不会被修剪和删除从blockchain(多个块确认的我们说话)。

与此相反，所有的BFT和状态机都满足协商一致的终结性

复制协议。这使得基于bft的区块链相对于PoW具有明显的优势，因为应用程序、用户和智能契约可以立即确认交易是否最终包含在区块链中。

可伸缩性。尽管脱钩blockchain可伸缩性的问题(与节点的数量和客户的系统)的blockchain性能(延迟和吞吐量)不完全是可能的,不过我们首先关注的节点数量和客户的战俘和BFT技术在实践中被证明能对感冒生效。一方面，比特币网络具有数千个挖掘节点，在实践中证明了基于粉末的区块链的节点可扩展性。尽管如此，值得一提的是，将矿商分组到矿池中(目的是为了分享采矿奖励，并让采矿成为一项财务上更可预测的事业)让比特币陷入困境，有效地集中了加密货币[27]。我们注意到，矿池集中化并不是比特币的一个特定特征，更多的是PoW区块链流行的结果，它还会影响许多替代币(类似比特币的加密货币)以及流行的区块链，比如Ethereum。另一方面。通常，BFT和状态机复制被认为是可伸缩性差的协议(参见，例如，Brewer 's CAP定理[8])。就已问世,然而在复制的背景下,传统的应用程序,比如数据库,容错,BFT协议从来没有真正彻底测试的可伸缩性,说,n = 10或20 n =节点,特别是在相当温和的光性能很多blockchain应用程序的目标。直观地说，由于BFT协议的密集网络通信通常每个块[10]包含多达O(n2)条消息，因此在数据库和系统社区中BFT协议被视为不可伸缩的(也请参见[45])。即使对于耐碰撞的同类来说也是如此。例如Paxos[37]、Zab[31]和Raft[50]等复制协议，它们在许多大型系统中使用，但实际上从来不会跨多个副本(参见[13])。

最后，当涉及到客户端数量的可伸缩性时，PoW和BFT协议都支持数千个客户端并具有良好的伸缩性。

的性能。比特币的性能非常有限，每秒最多只能进行7次交易(以当前块大小计算)，延迟为1小时，确认为6个块，除此之外，基于粉末的块链还面临着固有的性能挑战。正如我们已经讨论过的，PoW区块链的两个主要性能相关参数是块大小和块频率。以提高吞吐量为目标而增加块大小的代价是增加延迟，因为更大的块在Internet上的传播延迟更长。这些更长的延迟反过来又对区块链的安全性产生了负面影响:更长的延迟可能会增加分支的数量，并增加对[34]发起双待解决攻击的可能性，因为PoW区块链中可能存在临时的链叉，且缺乏一致的最终结论。当块频率增加时，也会遇到类似的安全挑战，目的是减少多块确认的延迟。在基于粉末的区块链中，调优块频率和块大小的确切安全性影响通常相当复杂(请参见[55]以获得分析)，应该小心处理。考虑到这一点，有限的性能似乎是PoW区块链固有的，而不是特定实现的产物。相比之下，现代的BFT协议已经被证实可以支持数万个具有实际网络速度延迟的事务，不仅作为原型(例如[35,12,3])，而且作为实用的系统[5]。

的对手。PoW和BFT考虑不同的对手。在PoW区块链中，重要的是对手控制的计算(哈希)总功率。最初，人们认为只要对手控制的散列能力不足50%，比特币就不会受到攻击。多年后，研究表明，即使只有25%的计算能力被对手[24]控制，比特币挖掘实际上也是脆弱的。相比之下，BFT投票方案最多只能容忍n/3个损坏的节点[20]。只有当网络被允许(不时地)完全异步时，这个界限才成立——增强的同步假设使提高这个阈值成为可能。经典的BFT共识的n/3阈值可以推广到一般的对手结构，对手可以控制不同的节点子集[29,57]。

网络同步。比特币依赖于一个节点的本地时间来对一个块进行时间戳。粗略地说，如果一个块的时间戳大于前11个块的中值，那么它就被认为是有效的。此外，时间戳在计算挖掘和保持块频率的难度方面起着重要作用。因此，活跃性需要松散的时钟同步。然而，时间戳操纵攻击也可能危及区块链的一致性(参见“时代精神攻击”[1])。虽然这类攻击很难针对比特币等主要的战俘区块链，但它们已经在一些战俘替代币的背景下成功实施。BFT协议通常不依赖于任何物理时钟。然而，最终需要同步通信来确保活动性，这是由于FLP协商一致不可能的结果，该结果指出，在纯异步系统[25]中，使用潜在的错误节点是不可能确定地实现协商一致的。尽管存在全球通信中断和任意长异步周期[20]，但协商一致的安全性(包括协商一致的终结性)仍然得到维护。

正确性证明。历史上，状态机复制协议，特别是它们的BFT变体，被认为是设计和实现非常具有挑战性的[11,5,3]。因此，新的协议受到了详细的学术审查，因此(或多或少)会有详细的证明，有时甚至会有需要整个博士论文的正式证明(见[14,41])。尽管比特币最初被部署的原因可能是可以理解的，但令人惊讶的是，新的PoW区块链很少附带详细的安全、分布式协议和安全分析。

## 3.提高区块链的可扩展性

在这一节中，我们将概述并讨论最近几个致力于改进PoW和BFT区块链可伸缩性方面的工作。

提高粉末区块链的性能。Sompolinski和Zohar最近提出了GHOST(贪心重的观察到的子树)规则[55]，它基本上解决了PoW区块链中的冲突，方法是通过权衡根在块中的子树，而不是根在给定块中的最长(子)链。虽然GHOST本质上是一种解决冲突的策略，但它比标准的最长(最重)比特币链规则提供了性能优势，因为它提供了更安全的方法来增加块频率和块大小[55]。在Ethereum区块链[58]中实际上实现了GHOST规则的一个变体，尽管在高负载的情况下，GHOST- pow性能还没有得到充分的强调(在2016年，Ethereum的典型吞吐量小于每天20,000个事务，即，平均约0.2 tx/s)。5 . Bitcoin-NG是Eyal等人提出的一种新颖的方案，使用标准PoW进行leader选举，声明一个节点在挖掘出一个新的key block之前，将以标准难度挖掘出的block(称为key block)作为leader。同时，leader可以将微块附加到链中，这些微块不受PoW挖掘的影响，而仅仅是哈希链在一起。因此，微块极大地提高了整个系统的吞吐量，减少了延迟(也就是说，在实践中，Bitcoin-NG还有待测试)。从某种意义上说，Bitcoin-NG将领导人选举(通常见于BFT协议)与领导人选举时代之间的以领导人为中心的协议混合在一起。然而，比特币- ng与BFT协议的不同之处在于，领导人选举是基于粉末的。因此，在Bitcoin-NG中仍有可能出现分岔，并且不能保证最终达成一致意见，这可能导致安全问题，如前面讨论的资产重复支出。

通过并行化缩放区块链。Lewenberg等人最近在PoW[39]的背景下提出了将区块链缩放为块dag(有向无环图)而不是线性区块链的方法。其思想是允许非冲突的事务(例如，那些不构成双重开销尝试的事务)最初位于不同的分支上，但最终通过挖掘一个块来合并这些分支，从而将它们都包括在分类账中。几年来，BFT和状态机复制社区也一直在深入探索并行复制的概念，利用独立请求(事务)执行的并行化(参见，例如[33,43])。

消除BFT协议中的通信和资源开销。正如我们已经讨论过的，BFT协议在区块链中阻止其广泛采用的主要挑战是其在节点数量方面的可伸缩性。star[44]是一个正在进行的努力，旨在从BFT协议中删除一致接受的成员列表，同时保持BFT相对于PoW的其他优势。其他方法的目标是BFT可伸缩性，而不需要更改成员资格假设。这些协议包括乐观的BFT协议[52,3]，它在“常见情况”下具有线性通信复杂性，只有在网络和过程故障模式特别不利的情况下，才会采用经典协议(如PBFT[10])所具有的节点之间昂贵的O(n2)通信。然而，与耐碰撞复制协议(如[37,31,50])相比，即使是乐观的BFT也有资源和通信开销，这些协议在实践中得到了更好的证明，可以作为BFT的基线。为了纠正这一问题，Liu等人最近提出了一种新的网络和节点故障模型，称为XFT[40]，该模型允许容忍最多n/2个拜占庭节点。与此同时，XFT具有消息模式的特点，以耐碰撞复制协议，即。，没有与典型BFT消息模式相关的开销。为此，XFT(“交叉”容错)挑战了BFT对手同时控制网络和拜占庭节点的既定能力，将网络故障与拜占庭节点故障解耦，将它们视为基本独立的。因此，XFT走向了一个更现实的对手模型，类似于PoW区块链，它不太关心对手控制整个通信网络的能力。最后，未来基于BFT的区块链的另一个吸引人的方向是BFT协议，它利用小型可信硬件(例如[32])来改进通信和降低资源成本。

随机BFT。随机BFT协议(如[7,56,9])是标准的、最终同步的[21]BFT协议(如PBFT)的有吸引力的替代方案。具体来说，随机BFT协议通过保证非常高的概率(即，而不是确定性地。这使得随机BFT协议完全是异步的[4]。多年来，随机BFT协议的一个问题是它们的性能。具体来说，经典的随机BFT(例如[4,7,56,9])与最终同步的确定性BFT协议相比效率非常低，这主要是因为它们使用的加密工具的开销。然而，随着新的随机BFT协议如HoneyBadger[47]显示出良好的实际性能(即通过挑选最佳可用加密工具进行随机化，以及以非常大的批处理请求，可以获得最多100个节点。显然，大批处理会对延迟产生负面影响，但是这可以通过混合BFT协议[2]来解决，它可以将非常有效的乐观和确定性BFT协议(例如[3]中描述的那些协议)与HoneyBadger等实际的随机协议结合起来。这种混合BFT协议的早期例子可以在[2,36,52]中找到，但是未来混合BFT协议的开发可以通过使用[3]中描述的模块化BFT设计框架来促进。

混合PoW和BFT。最近，Decker等人[15]提出用BFT(具体来说，就是PBFT协议[10])来增强PoW区块链，主要是通过使用BFT来保证PoW区块链的一致性最终。SCP[42]还提出了一种混合的PoW/BFT协议，使用PoW进行身份管理，使用(并行和分层)BFT协商一致进行协议。显然，上面关于按节点数量缩放BFT的重要性的讨论对于混合PoW和BFT的方法也很关键。

## 4结论和有待解决的问题

我们简要回顾了可伸缩区块链的技术现状和新兴方向。我们比较了工作证明协议(PoW)和拜占庭故障防御协议(BFT)，强调了它们各自的优点。未来的工作将是非常动态和有趣的。使图1更加清晰

准确地说,即。，相对于节点可伸缩性而言，将各种协议放在正确的位置需要进行大量的研究，但这代表了一个迫切的开放问题，需要更好地理解这个问题，以促进未来区块链可伸缩性的改进。此外，PoW和BFT之间的协作潜力很大，无论是在组合协议技术方面，还是在细化对抗模型和网络模型方面。

最后，对于要求最高的区块链应用程序，将BFT协议(例如密码学)中计算成本较高的部分移到更靠近硬件的地方将是非常有趣的。总的来说，在硬件中实现共识确实非常有吸引力，而且可能会产生令人印象深刻的性能，最近在崩溃容错上下文中探讨这一思想的建议就证明了这一点[51,30]。