区块链性能提升：链上设计之道

The Road to Scalable Blockchain Designs

Author	Shehar Bano ,Mustafa Al-Bassam and George Danezis
Translator	Taosheng Shi
WeChat Contact	data-lake
Mail Contact	tshshi@126.com
Organization	NOKIA
Document category	Distributed System
Document location	https://github.com/stone-note/articles

Version	Status	Date	Author	Description of changes
0.1	Draft	10/2/2018	Taosheng Shi	Initiate
0.2	Draft	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere
1.0	Approved	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere

Contents

1 引言

由于区块链的固有缺陷，比特币系统已经变得越来越中心化，并且越来越低效。 为了解决这个问题，大量替代解决方案被提了出来。Off-chain（链外）解决方案允许小型和频繁的交易发生在与主链并行并由主链背书的侧链实例上。 On-chain（链上）解决方案直接修改区块链设计以支持高性能。 我们专注于后者，并总结和讨论近期 On-chain（链上）性能提升方面的研究进展。

尽管建立在信息开放和自由的理想之上，互联网已经变得越来越中心化：只有少数大公司可以控制谁可以访问信息。 为了抵消这一趋势，一些建议被提出，以便信息存储和处理不集中在任何单一实体中。 其中，区块链前途广阔，吸引了主流媒体，研究机构和政策界的广泛关注。

区块链是一个不可更改、去中心化的数据库，有利于数据透明和审计管理。 区块链首次获得关注是作为 2009 年提出的比特币[文献 8]的基础技术。但由于其弹性，完整性和透明性，区块链已经独立发展。 然而由于区块链的性能问题，阻碍了比特币的广泛应用。 在过去的一年里，由于交易区块已经达到了容量极限，导致交易费暴涨，比特币社区就比特币应该如何扩容出现了重大分歧。 分歧争论的核心是扩容和中心化之间的 tradeoff：区块链越大，越少的设备有能力存储和审计完整区块链，从而导致网络变得更加中心化。

一些人认为只将比特币区块链用作大额交易的结算网络——小规模交易由区块链之外的支付中心处理（off-chain scaling，链外扩展），而另一些人则主张增加区块链本身对所有交易类型的容量 （on-chain scaling，链上扩展）。 作为这一主张的附带结果，链上扩展（on-chain scaling）的支持者最近推出了比特币区块链的支链作为自己的网络，称为比特币现金。 在本文中，我们综述了区块链链上扩展（on-chain scaling）的关键主题和选项。

2 区块链的功能组件(Functional Components of a Blockchain)

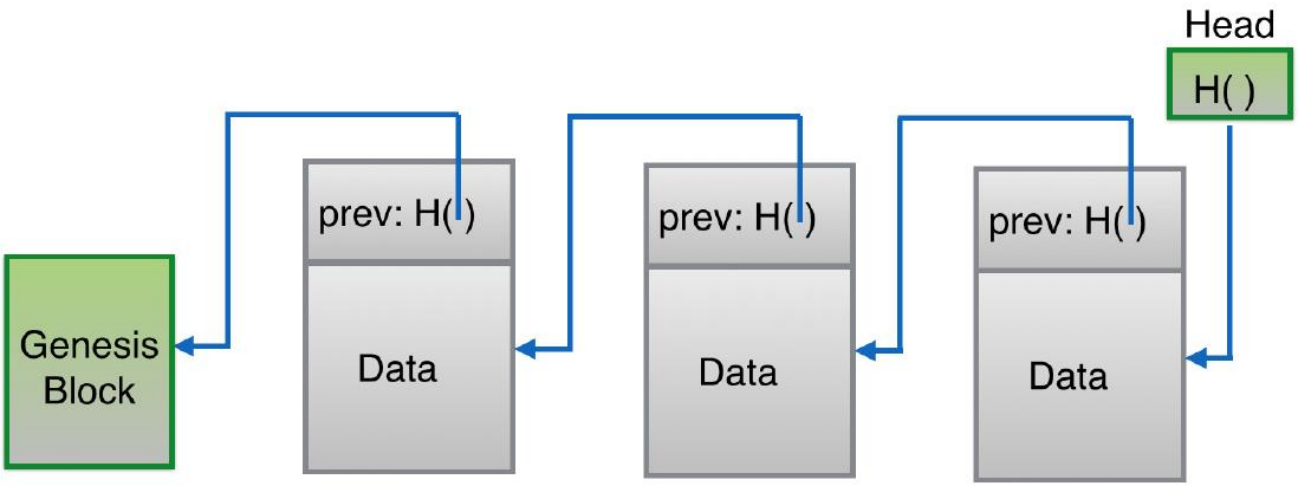

Figure 1: A blockchain is implemented as a linked list of hash pointers.

区块链充当去中心化的数据库——或者分布式总账——代表同步、分布式和复制数据（称为区块，代表交易集）的共识。区块链的内部实现为链表，其中指向前一个区块的指针替换为加密哈希指针(Figure 1)。指针仅仅是一些信息（例如，这里指前一个区块）的哈希，这个哈希用于识别信息以及验证其完整性。区块链中的每个区块都包含前一个区块的哈希和当前区块的特定信息。由此产生的哈希链确保每个区块隐式验证之前整个区块链的完整性。因此，区块链可以作为防篡改日志：可以将数据附加到日志的末尾，并且以前数据的篡改是可检测的。区块链有两个关键功能组件：交易验证组件和区块链增长组件。我们将分别讨论这两个组件。

2.1 交易验证(Transaction Validation)

交易指定了总账本状态的转变。这些交易在通过有效性验证之后，将被包含在一个候选（将要添加到区块链中）区块（一组交易）中。作为一个具体的例子，我们描述一个典型的（简化的）比特币交易——涉及从付款人向收款人转移货币。付款人和收款人通过其公钥进行标识，付款人对交易进行数字签名——涉及他们控制的在区块链先前区块中编码的价值。根据比特币网络规则，网络中的节点在接受交易之前必须执行一系列检查，以确保其有效。首先，他们必须检查交易是否完整。其次，他们必须验证付款人是否有权来进行交易（通过检查其数字签名是否与付款人的公钥对应）。第三，节点必须验证交易输出的总和低于输入的总和——付款人不能支付超过他们自己拥有的价值，但交易费可以包含在支付中。最后，节点必须确保没有任何输入被双重支出。这可以通过下面的方法进行验证：在区块链中回溯到输入值创建时，然后再向前遍历到当前交易，确保这笔输入之前没有支出过。

2.2 区块链增长(Extending the Blockchain)

事实上，交易产出(例如， X bitcoins)没有物理存在：Bob 拥有交易输出的事实基于这样的事实：大多数节点认为这是事实。 节点之间关于如何增长区块链的协议是通过一个称为共识的协作过程达成的。

2.2.1 共识(Consensus)

早在被区块链重新讨论之前，存在缺陷或恶意节点的共识问题在分布式系统社区已经有了广泛的研究。 在具有 n 个诚实节点的网络中，每个节点接收输入值并将其与网络的其余节点共享，共识协议使得所有 n 个诚实节点就诚实节点生成的输入值集合达成一致。 在比特币环境中（节点——作为对等（p2p）网络的一部分——广播交易信息），节点需要就哪些交易发生以及按什么顺序发生达成共识——也就是说，节点必须就区块链的状态达成一致。

2.2.2 分叉(Forks)

实现共识具有挑战性。节点可能具有区块链（分叉）的不同视图：p2p 网络上的交易传播延迟；节点随机失败；恶意节点试图抑制有效交易并将无效交易推送到区块链。分叉对抗共识，因此需要一种机制来解决冲突，并让大部分节点就区块链的状态达成一致。

2.2.3 领导者(Leader)

共识协议通常依靠领导者。 领导者节点负责协调其他节点达成共识，并为区块链追加最终的承诺价值。 领导者节点通常只在一段时间内有效，称为一个 epoch。在 epoch 之后或者领导者节点发生故

障，则选出一个新领导者。 领导者节点的一个重要属性是它应该诚实行事。 这一点很重要，因为尽管区块链的设计是“防拆封的”（tamper-evident），但将坏的区块添加到区块链中，可能会导致分叉。为了使节点重新收敛到区块链分叉之前的有效视图，将导致系统资源的浪费。 领导者行为的诚实通常通过激励和审计来强制保证。

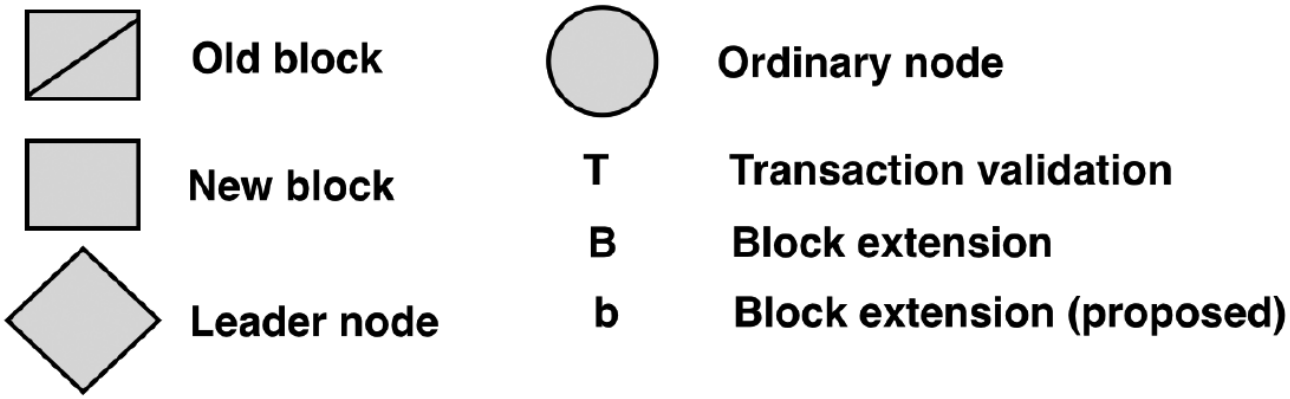

Figure 2: Legend used in the figures

图 2(Figure 2)显示了其中一些概念的可视化表示，这些概念后文用于解释各种设计主题。

3 比特币及其扩展问题 (Bitcoin and Its Scalability Issues)

2009 年比特币的出现激发了人们对区块链的兴趣。区块链是比特币的基础技术，比特币也是后续出现的无数区块链变种的先驱。因此，基于比特币的上下文，对于理解区块链的性能问题是非常有用的。

3.1 比特币区块链(The Bitcoin Blockchain)

比特币是一个 P2P 网络，任何节点都可以加入并成为网络的一部分。 如果一个节点收到一个新的区块，它会将其广播到网络的其余节点(Figure 3)。 所有节点都可以接收和发送广播，但只有领导者节点才可以向区块链追加信息。为了阻止不诚实的领导者将系统带入泥潭——例如频繁创建分叉——每个 epoch 的领导者都是通过工作量证明随机选择的。 这涉及求解希难题——也称为挖矿，这也是领导者节点被称为矿工的原因。 如果矿工幸运地找到哈希难题的答案，它会提出要追加到区块链下一个区块。为了激励矿工解决哈希难题并提出下一个区块，允许成功的矿工为自己支付一些金钱作为报酬（区块奖励，随着时间的推移而减少）或扣除交易输出的一部分作为交易费用。

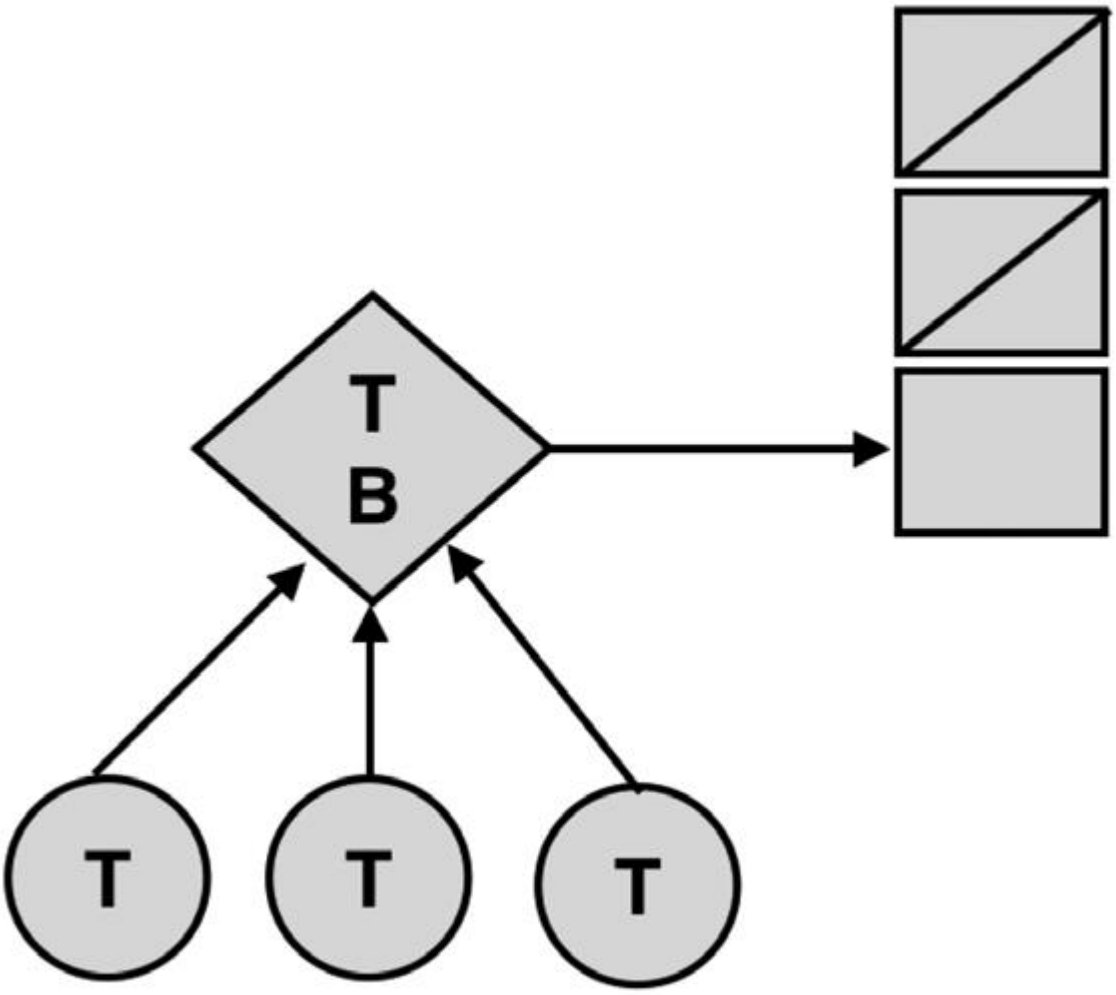

Figure 3: The Bitcoin blockchain model

3.2 区块链的扩展性(Blockchain Scalability)

有两个测量指标与区块链扩展性直接相关：交易吞吐量（区块链可以处理交易的最大速率）和延迟（确认交易已包含在区块链中的时间）。虽然以前的工作已经确定了额外的指标[文献 4]，但吞吐量和延迟是瓶颈问题，从研究的角度也更具挑战性。比特币的交易吞吐量是其区块大小和块间间隔（时间）的函数。在当前块大小为 1MB 和 10 分钟块间间隔的情况下，最大吞吐量限制在每秒约 7 个交易；而创建交易的客户必须平均等待至少 10 分钟以确保交易包含在区块链中。相比之下，像 Visa 这样的主流支付处理公司可以在几秒钟内确认交易，并且每秒处理吞吐量高达 24,000 次[文献 9]。目前的研究集中在开发显著提高区块链性能的解决方案，同时保持其去中心化特性。对比特币区块大小和块间间隔的参数化可以在一定程度上提高性能——基于最近一项研究[文献 4]：每秒 27 次交易吞吐量和 12 秒延迟。然而，性能的显著提升需要重新对区块链范型进行根本性的设计。

4 重新设计区块链(Redesigning Blockchains for Scalability)

现在我们来看看为提高区块链的扩展性而开发的重要设计方案。 我们的研究范围仅限于区块链设计核心（链上解决方案）的方法，而不是将信任委托给并行旁路区块链实例（例如 sidechains 侧链[1]（off-chain 解决方案））的技术。 主题和示例系统的列表并不是全面的，而是指示接近这一主题的主要方法，并为未来的研究工作提供高层次路线图。图 2 (Figure 2)显示了我们在后续章节中将要讨论的设计主题的基本构建块。

4.1 多区块单一领导(Multiple Blocks per Leader)

Bitcoin-NG[文献 5]分享了比特币的信任模型，但将领导者选举（通过工作量证明随机且偶尔执行）与交易序列化(Figure 4)解耦。然而，与比特币不同的是（比特币领导者节点只能提出一个区块来追加区块链），Bitcoin-NG 将时间划分为 epoch，领导者节点可以在其 epoch 期间单方面向区块链追加多笔交易，直到新领导者节点被选出。 Bitcoin-NG 中有两种区块：密钥区块和微区块。 密钥区块包含一个难题答案，用于领导者选举。密钥区块还包含一个公钥，用于签署由领导者节点生成的后续微区块。每个区块都包含对前一个微区块和密钥区块的引用。费用会在当前领导者（40%）和下一个领导者（60%）之间分配。与比特币类似，通过增长（聚合所有密钥区块的）最长分支来解决分叉问题。请注意，由于这些微块不包含工作量证明，所以微区块不会影响分支的长度。为了对微区块中创建分叉的领导者节点进行惩罚，后续的领导者节点可以在其关键块（包含被剪枝分叉中的第一个块的头部）之后插入特殊的有毒交易作为欺诈证据。这使恶意领导者节点的报酬无效，报酬的一小部分支付给告发领导者。当一位新领导者选出但前任领导者还没有收到，并继续产生微区块时，分叉也会出现。然而，一旦新领导者选举的宣布达到所有节点，这些分叉就会得到解决。

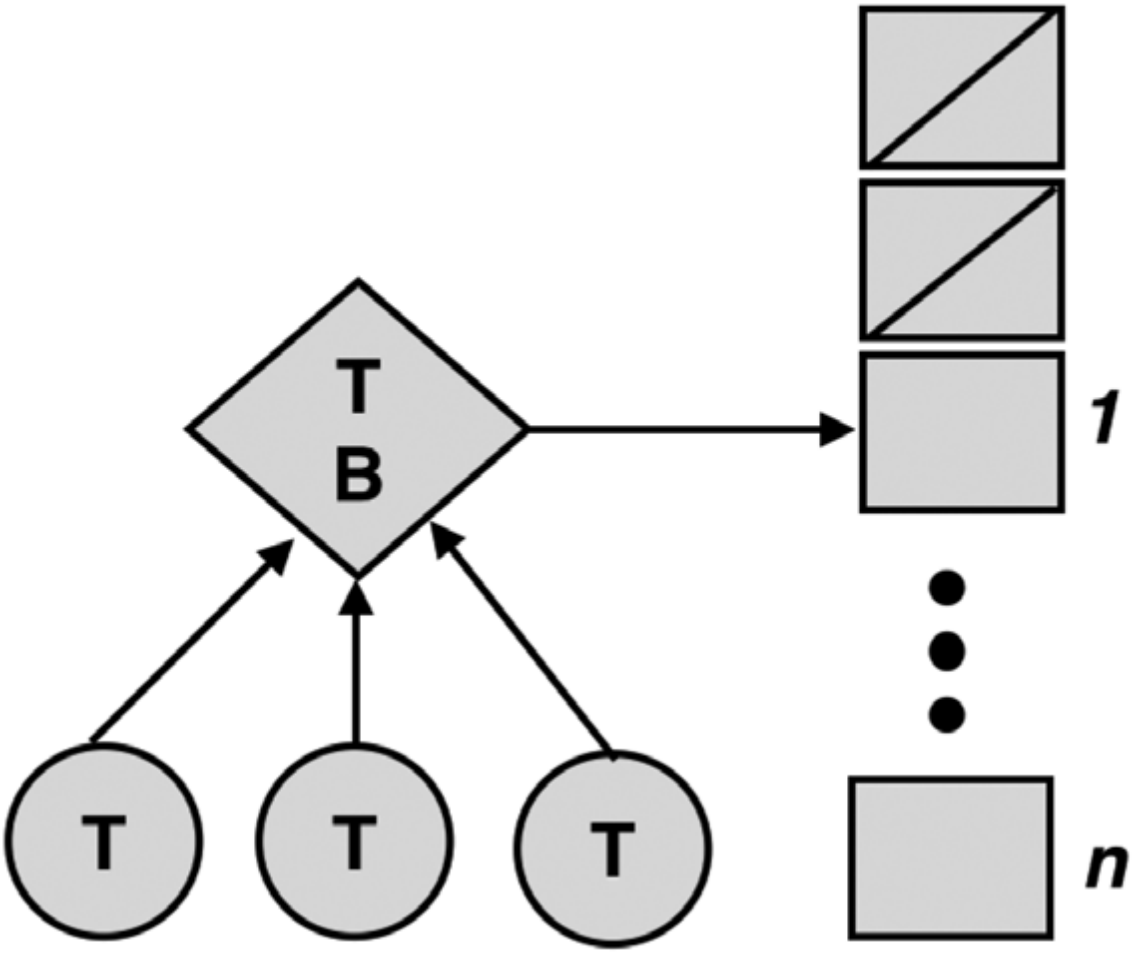

Figure 4: Multiple blocks per leader

4.2 集体领导(Collective Leaders)

该方案采用多个领导者共同快速决定是否应该将区块添加到区块链中(Figure 5)。ByzCoin [文献 6]通过扩展 Bitcoin-NG（参见前面的章节）取代比特币的概率性交易一致性保证（具有强一致性），以实现高交易吞吐量。这有一个好处，即客户提交的交易将被添加到区块链中，区块链仍然是无分叉的，因为所有领导者都立即就区块有效性达成一致。 ByzCoin 修改了 Bitcoin-NG 的密钥区块生成机制：一组领导者，而不是单个领导者，产生一个密钥区块，然后是微区块。领导者小组由近期时间窗口的矿工动态组成。每个矿工的投票能力与其在当前时间窗口的挖矿区块数量成正比，这是其哈希能力。当一位新矿工解决难题之后，它将成为现任领导小组的一员，更进一步，替换出最老的矿工。ByzCoin 使用与比特币相同的激励模式，但报酬由领导者小组成员按其比例分摊。

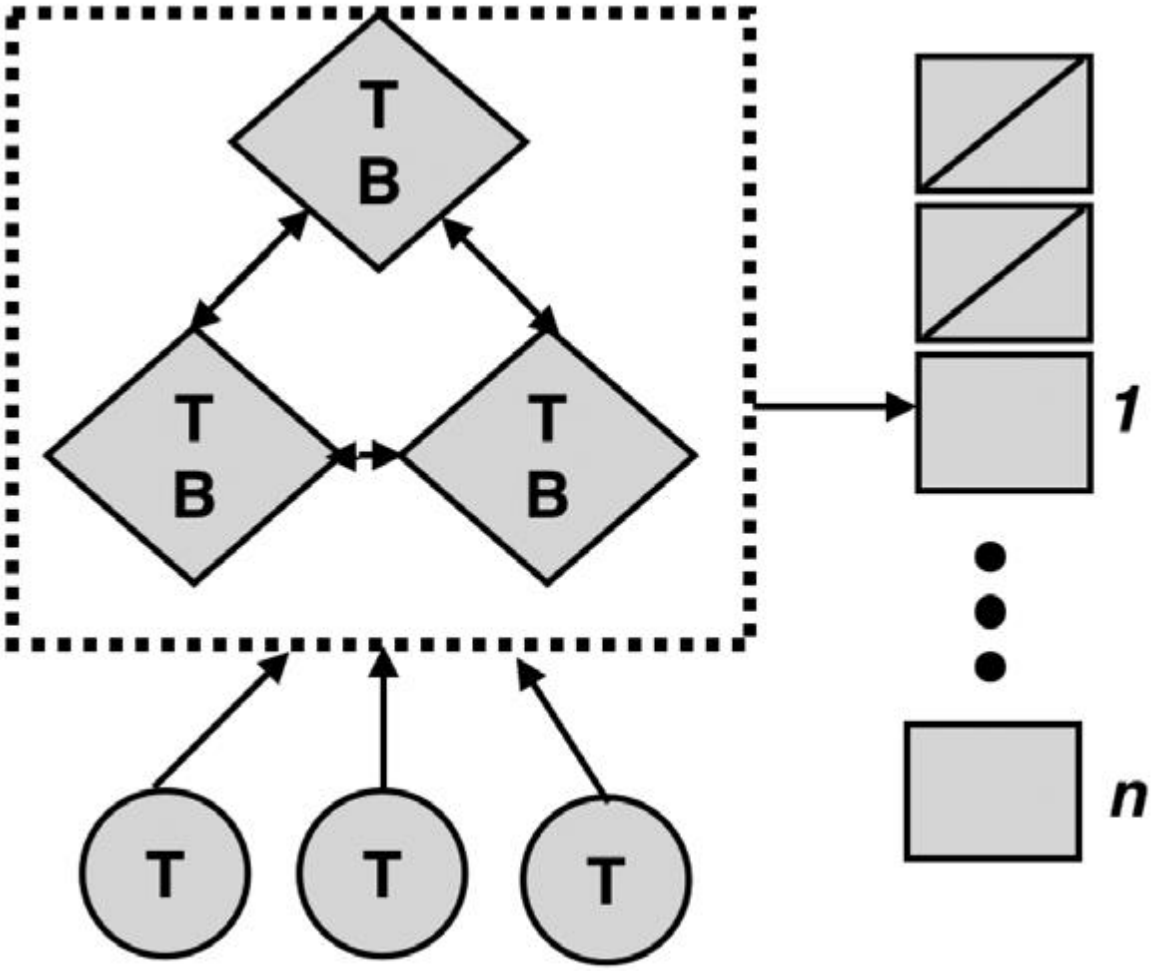

Figure 5: Collective leaders

领导者小组被组织成一个消息通信树，其中最新的矿工（领导者）在树的根部。领导者运行一个具有线性消息传递复杂度的实用拜占庭容错（PBFT）协议[3]的修改版本，以生成一个集体签名，证明至少三分之二的共识小组成员见证并验证了该微区块。网络中的节点可以以 O(1)时间复杂度验证该微区块已被共识小组验证为有效。这种设计解决了 Bitcoin-NG 的限制——恶意领导者节点可以创建微区块分叉：在 ByzCoin 中，这要求领导者小组成员的三分之二多数为恶意节点。此外，Bitcoin-NG 遭受竞争条件困扰：一位尚未收到新领导者的老领导者节点可能会继续错误地在较早的微区块上进行挖矿。在 ByzCoin 中，领导者小组成员确保新领导者建立在最新的微区块之上。

4.3 并行区块链增长(Parallel Blockchain Extension)

如图 6(Figure 6)所示，在这种方法中，多个领导者并行增长区块链的不同部分（例如，交易图）。比特币具有增长区块链的线性过程：矿工尝试解决难题，找到答案的矿工追加下一个区块。由 Boyen，Carr 和 Haines [文献 2]提出的框架通过放弃“区块”和“链”的概念来并行化这个过程（支持交易的图式交叉验证，而不是线性，可以理解为“区块图”）。每笔交易确认两笔交易（其双亲）并包含一些有效负荷（例如，加密货币）和工作量证明。

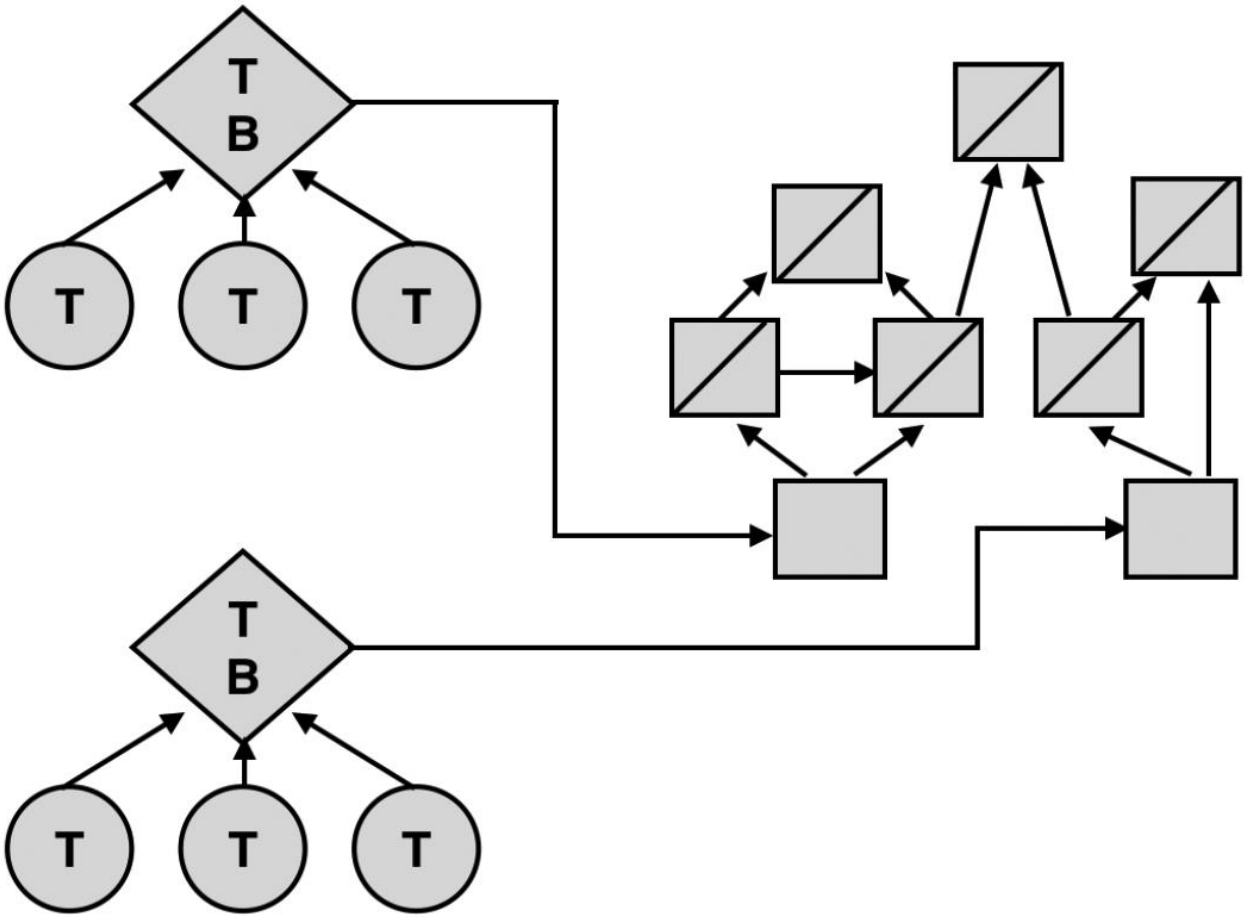

Figure 6: Parallel blockchain extension

交易可以由多个子节点进行潜在的验证。此外，每次交易还会包含一笔报酬，这笔报酬由验证该交易的交易收取。随着更多的节点直接或间接地验证它，报酬值会降低，因此新节点有更多的动机来验证最新的交易。该系统已被证明是收敛的，这意味着在某一时刻有一个交易连接到（并且因此隐式地验证）之前的所有交易。作为这种图结构的结果，矿工可以并行地增长交易图的不同分支。系统中的正常（非矿工）节点在收到交易时验证它们。除了对交易及其双亲的工作量证明正确性和结构有效性进行标准检查之外，节点还验证该交易不是双重支出（通过接受附加有最大工作量的良好格式的交易验证）。

4.4 分片交易(Sharding Transactions)

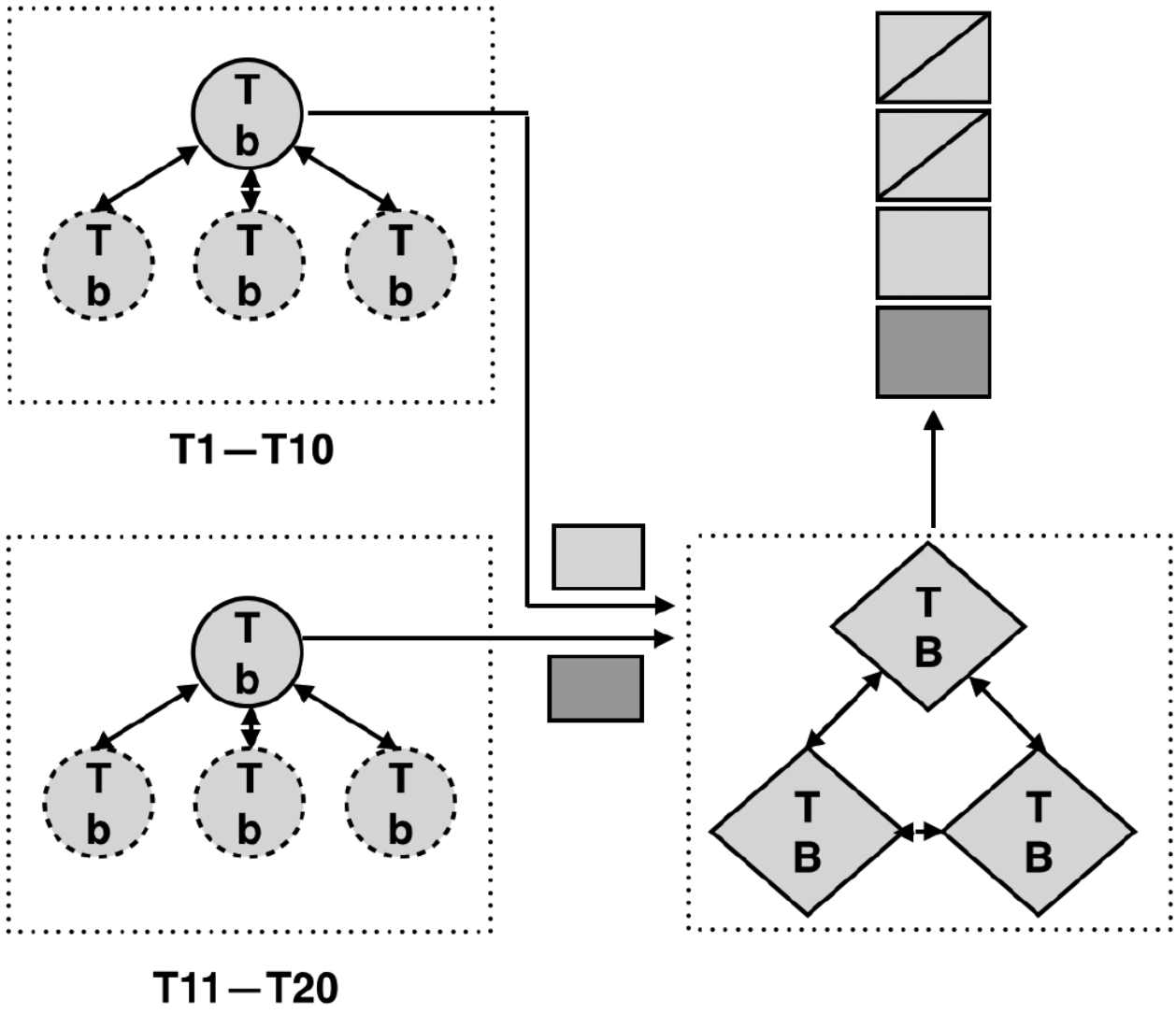

Figure 7: Sharding transactions

Elastico [文献 7]将节点分成称为“委员会”的组，每个委员会管理交易的一个子集（分片）。在图 7(Figure 7)中，上部分片处理前 10 个交易，而下部分片处理后续 10 个交易。在委员会内，节点运行拜占庭一致性协议（例如，PBFT）以协定交易区块。如果该区块已被足够的节点签名，委员会将其发送给最终委员会。最终委员会将从委员会收到的一系列交易整理到一个最终区块中，然后在其成员之间运行拜占庭一致协议以增长区块链，并将附加区块广播给其他委员会。系统按 epoch 运行：分配给委员会的节点仅在 epoch 期间内有效。在这个 epoch 结束时，这些节点解决当前最终委员会产生的随机字符串难题，并将求解答案发送给下一个最终委员会。因此，在每个 epoch，一个节点与委员会中的不同节点搭档，管理一组不同的交易。委员会数量与系统中可用算力成线性比例关系，但一个委员会内的节点数量是固定的。因此，随着更多节点加入网络，交易吞吐量增加而延迟不会增加，因为这里有一个解耦：一致性协议所需的消息与添加到区块链的最终区块的计算和广播之间的解耦。

5 结论 (Conclusion)

我们框架性的介绍了区块链的性能问题，并概述了区块链 on-chain（链上）性能提升的关键方法。本文揭示了用于构建可扩展区块链的设计模式。事实上，一些模式已经在使用：ByzCoin 在 Bitcoin-NG 的“多区块单一领导者”设计的基础上建立了集体领导机制。集体领导是通过在多个领导者之间分散责任和利益来强化诚实行为（并避免分叉）的有用原语。 分片(Sharding)通过将共识委托给（部分地）可以有效运行经典 BFT 协议的节点小组，并且成立负责增长区块链的领导者节点小组（领导者之间运行可能还仍然是 BFT 共识协议）来加速交易吞吐量。用集体领导机制取代领导者节点之间的共识机制也许是可行的，因为集体领导机制的信息传递复杂度低于原来的 PBFT 协议，并具有更高的信任度。并行区块链扩展的想法可以与分区相结合，使得区块链在独立的分片上以部分连接的树存在。不同树中的区块，仅在发生交易且交易消耗不同分片管理的区块时，才会发生连接。

挖矿中心化是比特币中一个众所周知的问题：最大矿工在决定区块链发展方面具有巨大优势。Bitcoin-NG 和 ByzCoin 等系统继承比特币挖矿共识的系统遭遇同样的中心化问题，并有利于最大矿工。总的来说，比特币的低效的挖矿领导者选举机制已经转变为经典共识协议的新颖组合或变体。经典共识协议不能直接在区块链中使用，因为它们最初是为局域网实现的，并且它们的吞吐量随着节点数量增加而减少。看看有什么新设计会出现，以及如何将现有的共识协议重新应用于去中心化广域网(WAN)环境和各种攻击模型中，这将非常有趣。这方面的研究重振了拜占庭共识领域，并有可能对大规模部署的对等系统有重大作用。

6 致谢(Acknowledgments)

The authors are supported in part by EPSRC Grant EP/M013286/1 and the EU H2020 DECODE project under grant agreement number 732546, as well as The Alan Turing Institute.

7 作者简介

Shehar Bano is a Postdoctoral Researcher at University College London. Her research interests center on networked systems, particularly in the context of security and measurement. She received her PhD from the University of Cambridge in 2017 where she was an Honorary Cambridge Trust Scholar, and was awarded the Mary Bradburn Scholarship for her research work.

Mustafa Al-Bassam is a PhD student at University College London, working on scalable distributed ledger technology and peer-to-peer systems.He received a BSc in computer science from King’s College London, where his final-year project focused on public-key infrastructure implemented with smart contracts.

George Danezis is a Professor of Security and Privacy Engineering at University College London and a Turing Faculty Fellow, where he heads the Information Security Research group. He researches privacy-enhancing technologies, decentralization, and infrastructure security and privacy. In the

past he worked at Microsoft Research, KU Leuven, and the University of Cambridge, where he also studied.

8 参考文献(References)

[1] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell,A. Miller, A. Poelstra, J. Timón, and P. Wuille, “Enabling Blockchain Innovations with Pegged Sidechains,” Blockstream.com,2014: https://www.blockstream.com/sidechains.pdf.

[2] X. Boyen, C. Carr, and T. Haines, “Blockchain-Free Cryptocurrencies:A Rational Framework for Truly Decentralised Fast Transactions,” Cryptology ePrint Archive, Report 2016/871,2016: https://eprint.iacr.org/2016/871.

[3] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” in Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI ’99), USENIX Association, 1999, pp. 173–186: http://bit.ly/2fjh6dN.

[4] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A.Kosba, A. Miller, P. Saxena, E. Shi, and E. G. Sirer, D. Song, R.Wattenhofer, “On Scaling Decentralized Blockchains,” 3rd Workshop on Bitcoin and Blockchain Research, 2016: http://bit.ly/2xfz5Jl.

[5] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse,“Bitcoin-NG: A Scalable Blockchain Protocol,” in Proceedings ofthe 13th USENIX Conference on Networked Systems Design and Implementation (NSDI ’16), pp. 45–59: http://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf.

[6] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, “Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing,” in Proceedings of the 25th USENIX Security Symposium (USENIX Security ’16),pp. 279–296: http://bit.ly/2wziEbl.

[7] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P.Saxena, “A Secure Sharding Protocol for Open Blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS ’16), pp. 17–30: https://www.comp.nus.edu.sg/~loiluu/papers/elastico.pdf.

[8] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” December 2008: https://bitcoin.org/bitcoin.pdf.

[9] https://usa.visa.com/run-your-business/small-business-tools/retail.html).