arXiv:2305.01232v1 [cs.DC] 2 May 2023

TangleSim：一种用于基于有向无环图的分布式账本技术的智能体式模块化模拟器

Bing-Yang Lin*、Daria Dziubałtowska*、Piotr Macek *、Andreas Penzkofer*、Sebastian M¨uller†
*IOTA 基金会，德国柏林，电子邮箱：research@iota.org
†艾克斯-马赛大学´，法国国家科学研究中心（CNRS），I2M，UMR 7373，13453 马赛，法国，电子邮箱：sebastian.muller@univ-amu.fr

摘要——基于有向无环图的分布式账本技术支持对账本进行并行、异步的写入。因此，不同节点对最新区块的认知可能存在显著差异，而点对点层底层网络的属性会直接影响协议性能。此外，多个核心组件之间更强的相互依赖关系，使得研究此类分布式账本技术需要采用更复杂、更全面的方法。

本文介绍了一款面向大规模网络的开源智能体式模拟器，用于模拟实现无领导者 Tangle 2.0 共识协议的网络。其模拟范围包括底层点对点通信及其网络拓扑、数据包丢失、异构延迟、具有可靠广播特性的 Gossip 协议、底层有向无环图数据结构，以及共识协议。

该模拟器使我们能够探索协议在不同网络环境以及不同攻击场景下的性能。

I. 引言

分布式账本技术（DLT）是一类应用于分布式系统的协议，其核心组件是共识算法 [1]。由于大规模分布式账本技术系统复杂度很高，对这些协议进行性能评估通常既困难又耗费成本 [2]。此外，若未进行适当的性能评估便盲目开发分布式账本技术系统，可能会在实际部署阶段引入漏洞 [3]。为了在开发早期评估分布式账本技术系统，并在不同环境和参数设置下对系统进行验证和测试，分布式账本技术模拟器是设计安全协议的必要工具。

直到最近，区块链模拟器的开发和应用才受到广泛关注 [2]。例如， [4]，收集并研究了各领域专家对于创建面向物联网区块链应用的仿真环境的意见。研究表明，目前缺乏可用于体现不同需求并开展必要分析的模拟器。 [5] 和 [6] 通过将系统抽象为五层（包括网络层、共识层、数据层、执行层和应用层），迈出了模拟器概念设计的一步。即使采用这种模块化架构，开发通用区块链模拟器仍然具有挑战性。目前，还没有模拟器能够全面涵盖现有区块链技术广泛的运行特性和功能。考虑到其复杂性，为各种区块链技术开发通用模拟器并不现实。然而，开发具备有价值功能、适用于特定分析的模拟器仍然可行。

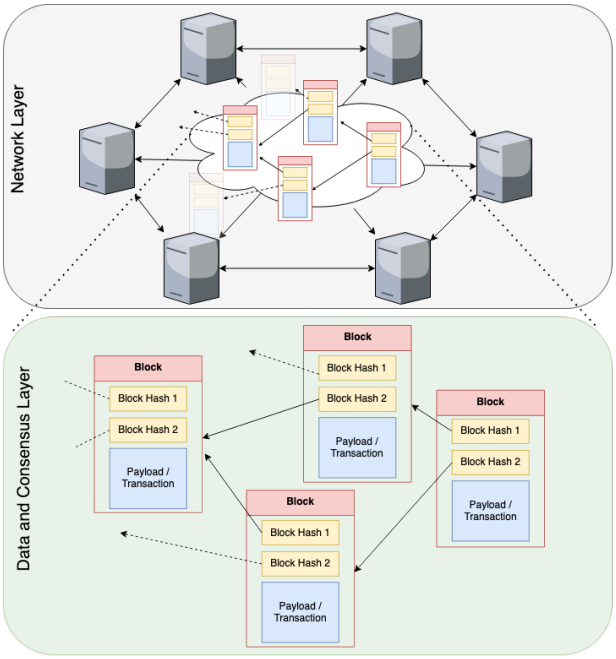


图 1. 模拟器中树层的概览：网络、数据和共识。由于共识基于数据层，因此这两个层合并显示为一层。

而应用具有实用价值，并能为设计稳健且高性能的协议带来显著益处。

A. 相关工作

首个区块链模拟器在 2013 [7]中提出，用于评估比特币中的用户隐私。随后，2019 年，BlockSim[8] 提出了一个适用于各种区块链系统的仿真框架，并将其作为框架和软件工具推出。为了比 BlockSim 提供更真实的结果，Block-Perf [9] 应运而生，对引言中提到的五层进行了更全面的覆盖。 [10]通过引入隔离见证 [11], [12], ——最重要的软分叉升级实现之一，进一步增强了 BlockSim。 [13] 根据 [1] 中定义的五个区块链流程对 Blocksim 进行了模块化，以实现高性能和可扩展性。

最近， [14]提供了一份聚焦于可用性、可靠性、功能和支持的特性的模拟器系统性映射综述。

文献[13], [15]中调查并评述了更多区块链模拟器。然而，迄今为止，只有三种有向无环——

图（基于有向无环图）的模拟器见于相关文献。首个基于有向无环图的模拟器是 TangleSimulator[16] ，于2018年推出，用于研究 Tangle白皮书版本 [17]。作为首个提出的基于有向无环图的模拟器，它仅支持有限的配置选项。为改进 TangleSimulator，同年推出了第二个基于有向无环图的模拟器 CIDDS [18]，用于研究网络层和吞吐量对系统的影响。第三个基于有向无环图的模拟器是 DAGSim [19]。它是一个面向基于DAG的加密货币的连续时间多智能体仿真框架。然而，所有节点都是按串行方式模拟的，因此无法模拟异步特性的关键方面。

上述基于DAG的模拟器分析了过时的 IOTA 协议 [17], 的行为，但没有一个实现并支持冲突分析或任何不利场景。此外，迄今为止，这些模拟器只展示了少数几项指标，包括交易附加概率和基本统计数据。区块确认时间是最关键的指标之一，但尚未得到探讨。

B. 贡献

我们提出了 TangleSim，这是首个能够分析网络、数据和共识层及其相互作用的基于DAG的模拟器。TangleSim 支持最新的 IOTA 共识协议 [20], ，并提供各种性能指标，以研究基于DAG的协议行为细节。虽然在多核服务器环境中进行仿真是一种常见做法，但我们将模拟器的易用性视为一项重要的设计标准。因此，我们提出了一种减速机制，使用户无需使用高性能硬件，即可在一台本地机器上进行大规模仿真。

II. 协议基础

在区块链中，每个区块都包含多笔交易的记录，并通过密码哈希函数与链中的前一个区块进行加密链接。这就形成了一条区块链，若不同时修改链中所有后续区块，就无法更改其中的内容；这需要获得网络共识。随着新交易不断加入网络，区块链持续增长，从而形成一份记录所有已发生区块链交易的不可篡改记录。

在基于DAG的分布式账本技术中，区块可以链接到多个先前的区块，从而形成区块有向无环图，而非区块链；另请参见图 1。该数据结构由区块组成
以及从较新的区块指向较旧区块的引用；较新的区块称为子区块，较旧的区块称为父区块。由此形成的区块有向无环图也称为*Tangle*。尖端 是没有任何引用指向它们的区块，也就是说，它们尚无子区块。Tangle 从创世区块开始，节点根据称为尖端选择的算法将新区块附加到先前的区块上。

与区块链类似，这些对 DAG 先前部分的引用能够为区块纳入最终数据结构的可信度设定一定等级。在 Tangle 2.0 共识协议的示例中， [20], 该等级由 批准权重 定义区块及其相关交易获得认可的程度。更确切地说，一个区块（或其包含的交易）的批准权重，是所有直接或间接引用该区块的区块发行者的累积权重。这是区块链中最长链规则或原始 Tangle 提案中的累积权重的自然延伸。区块的累积权重达到阈值 θ 时，即视为已确认。

III. 模拟设置与定义>定义*A.* 模拟器的数据流

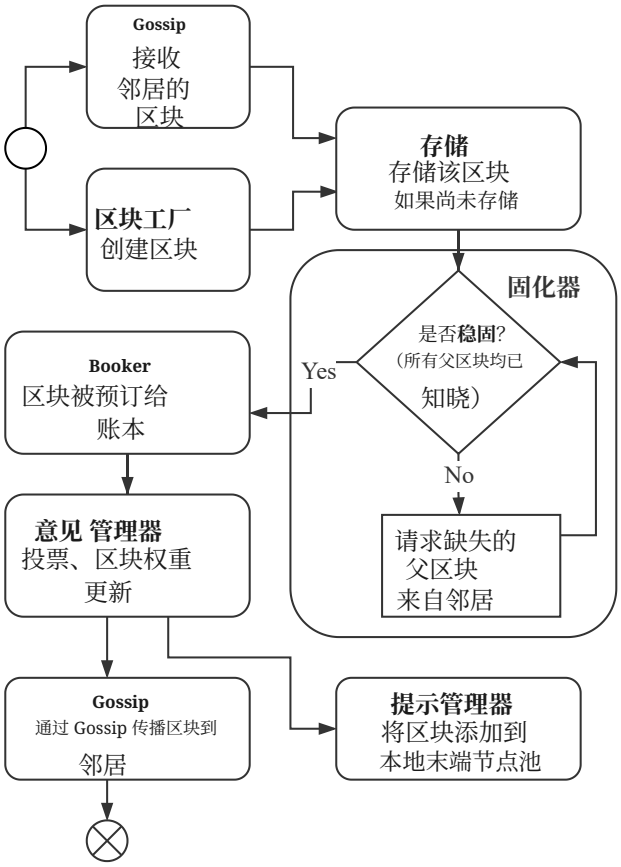


图 2. 模拟器中的区块流转图，展示区块从处理生命周期的开始（◯）到结束（⊗）的过程。

模拟器的设计侧重于与主要性能指标相关的核心组件。具体而言，我们实现了必要的组件，以支持基本的网络功能，例如 Gossip、调度和请求缺失区块，支持基于有向无环图的数据结构属性，以及共识层。

下文将介绍已实现的组件，并参见图 2 了解部分组件之间的交互。

区块工厂。 区块工厂会创建有效区块。它使用尖端选择算法来选择有效提示。在完整节点实现中，它还负责区块签名，并在适用时执行工作量证明。在这 亚洲欧美

模拟器，最后这两个操作被省略了。我们注意到，这两个操作会导致选择引用与其他参与者看到区块之间的延迟增大，从而影响协议的性能。不过，我们可以通过相应地增加网络延迟来模拟这一影响。

存储。 存储模块将区块存储在磁盘上的数据库中。在模拟器中，所有区块都存储在内存中，这提升了性能，但限制了可存储的区块有向无环图的大小。

固化器。 固化是请求缺失区块的过程。通过检查已接收区块所引用的区块是否存在于节点的数据库中，可以识别缺失区块。如果缺少任何父区块，该模块就会向邻居发送请求，请求缺失的区块。对于给定区块，当其直接或间接引用的所有区块都存在于数据库中后，该区块便会被标记为已固化。

Booker。 Booker 是一个负责将区块添加到 Tangle 中的模块。它负责识别和管理双重花费。

意见管理器。 意见管理器指出节点当前支持哪些冲突。它无需持续跟踪所有冲突及其批准权重，而是在节点需要发起投票时才延迟计算。在模拟器中，由于仅支持一个冲突集，其逻辑大大简化。

Gossip。 Gossip 模块负责在底层 P2P 网络中的节点之间传播新区块。

提示管理器。 提示管理器负责跟踪可用的有效提示，并将提示返回给区块工厂模块，用于新创建的区块。

IV. 设计与特性

我们在模拟器设计中纳入了网络、数据和共识这三个层。我们简要介绍每一层所实现的功能，详细说明请参阅 [21] 。

A. 网络层

节点数 N 是模拟中节点的数量。每个节点或对等节点都具有一定权重，用作女巫攻击防护、控制写入权限，并用于共识确定。模拟器支持使用参数为 s 的齐夫定律对节点权重进行建模。例如，可以使用 $s = 0$ 对同质网络进行建模；而当 s 显著大于 1 时，则可以研究更中心化的权重分布。默认情况下，假设节点的区块发行速率与其权重成正比，但也可以选择其他设定。我们使用 Watz-Strogatz 图 [22] 对 P2P 网络的拓扑进行建模。这类图可以高度控制各种参数，例如每个节点的邻居数、网络随机性和网络直径。为模拟现实世界中的行为，模拟器会指定相邻对等节点之间的数据包延迟，以及每个节点连接的丢包情况。区块通过 Gossip 算法进行分发。

表 I 网络层参数

符号	描述	默认值
N	节点数	1,000
s	权重分布的齐夫参数	0.9
γ	瓦茨-斯托加茨重连概率	100%
k	邻居数量	8
d_{min}	最小延迟	50ms
d_{max}	最大延迟	150 毫秒
p_{loss}	丢包	0

其速率由调度器模块控制。此外，我们还实现了一个固化器模块，用于向节点的邻居请求缺失区块。

如 [23], 所示，对协议性能更为微妙的影响因素是延迟的随机性。P2P 通信之间的延迟由区间 $[d_{\text{min}}, d_{\text{max}}]$ 内的均匀随机变量建模，并且每个数据包都有 p_{loss}的概率丢失。不同参数的概览请参见表 I。

B. 数据层

数据层，尤其是有向无环图的结构，取决于每个区块所引用的尖端数量 n_{tips} 。另一个重要参数是系统的吞吐量，该参数由每秒区块数 BPS 控制。此外，我们假设节点的区块发布时间间隔服从泊松分布 [24]。这些变量的概览请参见表 II。

表 II 数据层参数

符号	描述	默认值
n_{tips}	尖端数量	8
BPS	每秒区块数	100
IMIF	区块间延迟的分布	“泊松”

C. 共识层

确认阈值 θ 控制区块的确认；如果一个区块获得的批准权重大于 θ，就会被确认。模拟器支持对各种拜占庭环境进行建模。对抗权重 q_a描述了攻击者控制的比例，d_q则表示对抗性消息的延迟。这使我们能够模拟影响 P2P 层的攻击者。概览请见表 III。

表 III 共识层参数

符号	描述	默认值
θ	确认阈值	66%
d_q	对手延迟	100 毫秒
q_a	对手权重	5%
N_a	对手节点数	2

我们实现了一种特别高效的对手策略，正如 [20] 中所指出的。在这种所谓的诱饵与调包攻击中，

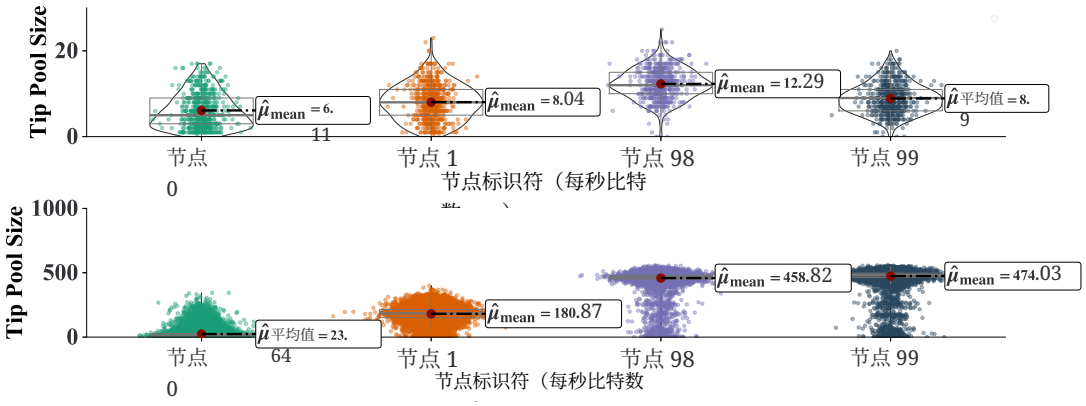


图 3. BPS 取不同值时，局部 tip 池的不同视图。

攻击者不断发出无穷无尽的冲突交易，以阻止“诚实权重”累积到同一笔交易上。

V. 性能指标

A. 确认时间

在分布式账本技术中，交易的确认时间可能是最重要的性能指标。本文将其定义为从区块发行时刻到该区块累积的批准权重超过确认阈值 θ 所经历的时间。通过分析不同场景下的确认时间，可以确定 Tangle 的最优配置，即能够实现最短确认时间的参数集合。例如，在图 4 中，我们研究权重分布的中心性对确认时间的影响，同时将其他参数设为默认值。每组参数均进行 100 次模拟运行。

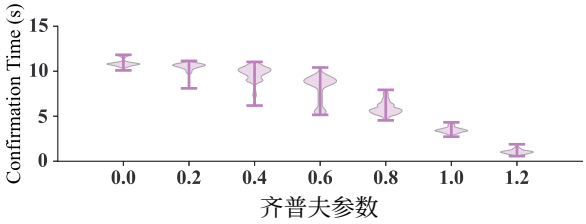


图 4. 确认时间对节点权重分布的依赖关系。

B. 尖端池大小

对于基于有向无环图的分布式账本技术而言，一个特别值得关注的性能指标是尖端的数量。这些尖端池的本地认知差异可能导致性能下降或同步问题。例如，在图 3 中，我们研究了 100 个节点、每秒比特数取两个不同值时尖端池的变化情况；所有其他参数均设为默认值，并进行了 100 次模拟运行。有关尖端池本地认知的更详细分析，请参阅 [25] 。

C. 共识时间

在存在冲突的情况下，我们关注解决冲突所需的时间，并将其称为共识时间。例如，在图 5 中，我们给出了诱饵转换攻击下共识时间随对抗权重变化的关系；齐普夫参数设为 2，其他参数均设为默认值。不同对抗情形下的共识时间研究较为复杂，关于使用我们的模拟器对 Tangle 2.0 共识鲁棒性进行的初步研究，请参阅 [26] 。

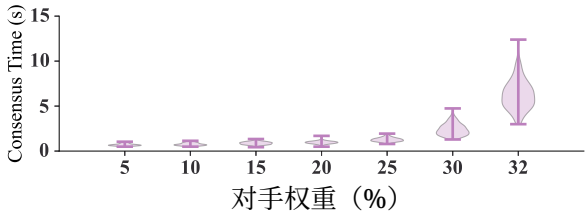


图 5. 共识时间对抗权重的依赖关系。

VI. 总结与讨论

我们提出了一种基于智能体的模拟器，可帮助我们了解 IOTA 2.0 协议在各种网络情境下的性能，并评估拜占庭环境中的共识协议。我们还展示了最具代表性的性能指标示例。模拟器的模块化设计使其能够无缝纳入其他组件和攻击策略。此外，它还可以轻松调整，用于研究其他基于有向无环图的分布式账本技术，并可作为比较不同基于有向无环图的分布式账本解决方案的通用框架。

致谢

作者谨此感谢 Hans Moog 编写了该模拟器的第一个版本。

引用

[1] Y. Xiao、N. Zhang、W. Lou 和 Y. T. Hou，“区块链网络分布式共识协议综述”，IEEE Communications Surveys Tutorials，第 22 卷，第 2 期，第 1432–1465 页，2020 年。[2] R. Paulavi˘cius、S. Grigaitis 和 E. Filatovas，“区块链模拟器概述及当前状态”，载于 2021 IEEE 区块链与加密货币国际会议（ICBC），2021 年，第 1–3 页。[3] S. Smetanin、A. Ometov、M. Komarov、P. Masek 和 Y. Koucheryavy，“区块链评估方法：现状与未来展望”，Sensors，第 20 卷，第 3358 页，2020 年 6 月。[4] A. Albshri、B. Awaji 和 E. Solaiman，“研究构建物联网应用区块链模拟器的必要性”，载于 2022 IEEE 智能物联网国际会议（SmartIoT），2022 年，第 232–240 页。[5] M. Belotti、N. Bo˘zi´c、G. Pujolle 和 S. Secci，“区块链技术指南：何时、选择哪种以及如何使用”，IEEE Communica-tions Surveys & Tutorials，第 21 卷，第 4 期，第 3796–3838 页，2019 年。[6] Z. Qingyi、S. Loke、R. Trujillo-Rasua、F. Jiang 和 Y. Xiang，“分布式账本技术在物联网中的应用：综述”，ACM Computing Surveys，第 52 卷，第 1–34 页，2019 年 11 月。[7] E. Androulaki、G. Karame、M. Roeschlin、T. Scherer 和 S. Capkun，“评估比特币中的用户隐私”，载于金融密码学与数据安全——第 17 届国际会议，FC 2013，修订精选论文，系列：计算机科学讲义（包括人工智能讲义和生物信息学讲义子系列），第 7859 LNCS 卷，2013 年，第 34–51 页。[8] M. Alharby 和 A. van Moorsel，“Blocksim：区块链系统仿真框架”，ACM SIGMETRICS Performance Evaluation Review，第 46 卷，第 135–138 页，2019 年 1 月。[9] J. Polge、S. Ghatpande、S. Kubler、J. Robert 和 Y. Le Traon，“Block-perf：混合区块链模拟器/模拟框架”，IEEE Access，第 9 卷，第 107 858–107 872 页，2021 年。[10] M. Basile、G. Nardini、P. Perazzo 和 G. Dini，“ 隔离见证扩展及比特币 Blocksim 模拟器的改进 ”，载于 2022 IEEE 区块链国际会议（Blockchain），2022 年，第 115–123 页。[11] （2022）Bip：141。 [在线]。可访问：https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki [12] （2019）Bip：144。 [在线]。可访问：https://github.com/bitcoin/bips/commits/master/bip-0144.mediawiki [13] X. Ma、H. Wu、D. Xu 和 K. Wolter，“Cblocksim：模块化高性能区块链模拟器”，载于 2022 IEEE 区块链与加密货币国际会议（ICBC），2022 年，第 1–5 页。[14] A. Albshri、A. Alzubaidi、B. Awaji 和 E. Solaiman，“区块链模拟器：系统化映射研究”，载于 2022 IEEE 服务计算国际会议（SCC），2022 年，第 284–294 页。[15] R. Paulavi˘cius、S. Grigaitis 和 E. Filatovas，“区块链模拟器的系统综述与实证分析”，IEEE Access，第 9 卷，第 38 010–38 028 页，2021 年。[16] M. N. Nguyen。（2018）Tanglesimulator。 [在线]。可访问：https: //github.com/minh-nghia/TangleSimulator [17] S. Y. Popov，“Tangle”，2016 年。[18] M. R. Abdul Lathif、P. Nasirifard 和 H.-a. Jacobsen，“Cidds：可配置的分布式基于有向无环图的分布式账本仿真框架”，2018 年 12 月，第 7–8 页。[19] M. Zander、T. Waite 和 D. Harz，“DAGSim：基于有向无环图的分布式账本协议仿真”，ACM SIGMETRICS Performance Evaluation Review，第 46 卷，第 118–121 页，2019 年 1 月。[20] S. M¨uller、A. Penzkofer、N. Polyanskii、J. Theis、W. Sanders 和 H. Moog，“Tangle 2.0：基于最重有向无环图的无领导者中本聪共识”，IEEE Access，第 10 卷，第 105 807–105 842 页，2022 年。[21] （2021）TangleSim。 [在线]。可访问：https://github.com/iotaledger/tanglesim [22] D. J. Watts 和 S. H. Strogatz，“‘小世界’网络的集体动力学”，Nature，第 393 卷，第 6684 期，第 440–442 页，1998 年。[23] A. Cullen、P. Ferraro、C. King 和 R. Shorten，“智慧出行的分布式账本技术：可变延迟模型”，载于 2019 IEEE 第 58 届决策与控制会议（CDC），2019 年，第 8447–8452 页。[24] A. Penzkofer、O. Saa 和 D. Dziubałtowska，“延迟类别对 IOTA 数据结构的影响”，载于 DPM/CBT@ESORICS，2021 年。[25] S. M¨uller、I. Amigo、A. Reiffers-Masson 和 S. Ruano-Rinc´on，“本地尖端池大小的稳定性”，2023 年。 [在线]。可访问：https://arxiv.org/abs/2302.01625

[26] B.-Y. Lin、D. Dziubałtowska、P. Macek、A. Penzkofer 和 S. M¨uller，《Tangle 2.0 共识的稳健性》，2022 年。 [在线]。可访问：https://arxiv.org/abs/2208.08254