翻译：Tang wei　X：tangyujie2002

X1 技术文档

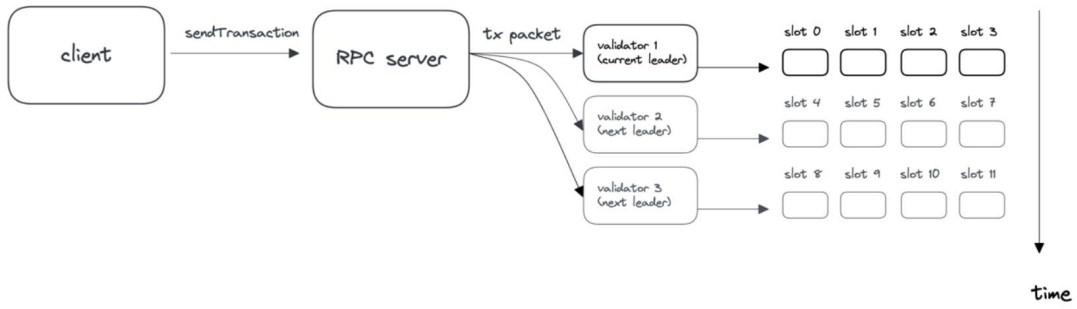
1、SVM 容量扩展

解锁硬件潜力：X1 区块链执行调度程序中的动态线程缩放

调度流程

初始化交易

一旦用户在其钱包中签署了交易，钱包就会将交易发送到 RPC 服务器。RPC 服务器可以由任何验证器运行。在接收到交易后，RPC 服务器检查领导者（leader）调度(每个 epoch 确定一次，大约 2 天)，并将交易转发给当前领导者以及接下来的两个领导者。领导者负责为当前的槽（slot）生产一个区块，并被分配四个连续的槽。插槽通常持续大约 400 毫秒。一旦签名的交易到达当前领导者，领导者就会验证该交易



多线程并发

EVM 是单线程运行时环境，这意味着它一次只能处理一个合约，而 SVM 是多线程的，可以在更短的时间内处理更多交易。每个线程包含一个等待执行的交易队列，交易随机分配到一个队列中。

默认的调度器实现是多线程的，每个线程都维护一个等待执行的交易队列。交易被随机分配给单个线程的队列。每个队列按优先级费用（以每个请求的计算单位支付的费用计价）和时

间进行排序。

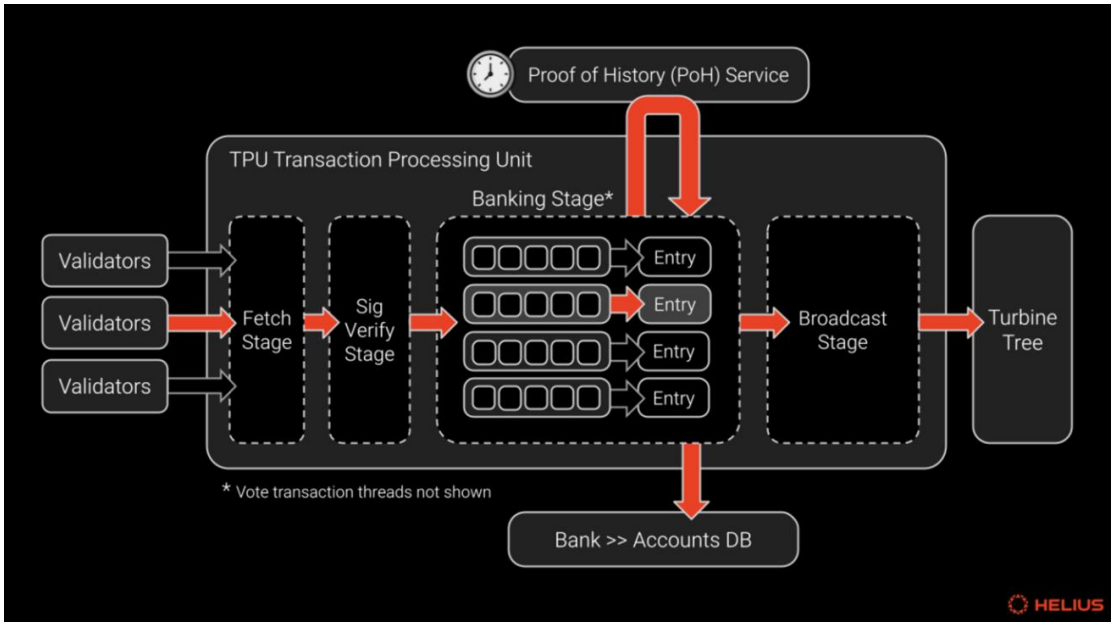
请注意，排队等待执行的交易没有全局排序；每个线程的队列中只有一个本地排序。

区块构建和银行阶段

许多区块链网络在广播它们之前构建整个区块，称为离散区块构建。相比之下，Solana 采用连续区块构建，这涉及在分配的时间隙内创建区块时动态组装和流式传输区块，从而显著减少延迟。

每个插槽(slot)持续 400 毫秒，每个领导者(leader)被分配四个连续的插槽（1.6 秒），然后轮到下一个领导者。要使区块获得接受，其中的所有交易都必须是有效的，并且可以被其他节点复制。

在担任领导节点之前的两个槽，验证者会停止交易转发，为即将到来的工作负载做准备。在此时间内，入站流量会达到峰值，每秒超过 1 GB，因为整个网络将数据包定向到新任领导者。



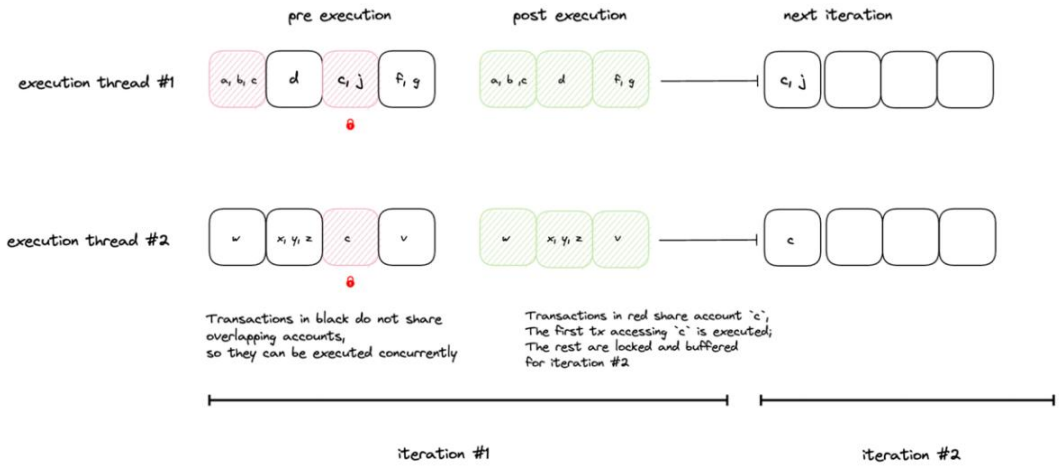
收到交易消息后，进入交易处理单元（TPU），这是验证者负责区块生产的核心逻辑。在这里，交易处理序列从 Fetch 阶段开始，通过 QUIC 接收交易。

随后，交易进入 SigVerify 阶段，并接受严格的验证检查。在这里，验证者验证签名的有效性，检查签名数量是否正确，并消除重复交易。

银行阶段(Banking Stage)可以被描述为区块构建阶段。这是 TPU 最重要的阶段，它的名字来源于“银行”。银行只是给定区块的状态。对于每个区块，Solana 都有一个银行，用于访问该区块的状态。

当一个区块在足够多的验证者投票后最终确定时，他们会将账目从银行更新到磁盘，使它们永久存储。链的最终状态是所有已确认交易的结果。这种状态总是可以确定性地从区块链历史中重新创建。

交易被并行处理并打包到领导者“条目”中，这些是 64 个不冲突的交易批次。Solana 上的并行交易处理变得容易，因为每笔交易都必须包含它将读取和写入的所有账户的完整列表。这种设计选择给开发人员带来了负担，但允许验证者轻松地只选择每个条目内不冲突的交易来执行，从而避免竞争的情况。如果两个交易都尝试写入同一帐户（两次写入），或者一个交易尝试从同一帐户读取，另一个尝试写入同一帐户（读取 + 写入），则交易将发生冲突。因此，冲突的交易进入不同的条目并按顺序执行，而不冲突的交易则并行执行。



在上图中，每个框代表一个交易。每笔交易都标有它锁定的账户。线程 1 锁定账户 [a，b，c]、[d]、无法锁定 [C，J] 和 [F，G]。线程 2 锁定账户 [w]、[x，y，z]、无法锁定 [c] 和 [v]。剩余的交易将被重新安排以备将来执行。

这是 X1 和 Solana 实现比竞争链更高性能的一种方式。当多个交易不需要触及相同的状态时，它们可以并行执行，这提高了链的吞吐量。但是，这会给开发人员带来负担，因为必须预先指定交易可能需要的任何状态。

六个线程并行处理交易，其中四个专门用于正常交易，两个专门处理投票交易，这些都是 Solana 共识机制不可或缺的一部分。所有处理的并行化都是通过多个 CPU 内核实现的，验证者节点不需要使用 GPU。

一旦交易被分组到条目中，它们就可以由 Solana 虚拟机（SVM） 执行。交易所需的账户被锁定；运行检查以确认交易是最近的，但尚未处理。加载帐户，执行交易逻辑，更新帐户状态。条目的哈希值将被发送到历史证明服务进行记录（下一节将对此进行更多介绍）。如果记录过程成功，所有更改都将提交到银行，并且解锁第一步中锁定的帐户。

Solana 架构当前的限制

Solana 的高吞吐量和快速交易处理能力很大程度上归功于其并行处理架构。但是，此体系结构中的一个重大限制是为调度交易执行分配的银行线程数量是固定的。目前，Solana 将

银行线程的数量限制为仅 4 个，无论底层硬件的功能如何。这种限制导致现代多核处理器的利用率不足，而现代多核处理器在节点环境中越来越普遍。

Solana 中的银行线程负责执行交易、管理状态更改和处理智能合约。虽然 Solana 架构中的并行性理论上支持高吞吐量，但人为限制四个银行线程会导致一些效率低下：

1、多核处理器利用率不足：现代处理器通常具有 16、32 或更多 CPU 内核。在这种硬件上限制为四个银行线程无法充分利用全部计算潜力，从而导致大量的空闲处理能力。

2、执行瓶颈：线程数量有限会在交易处理管道中导致瓶颈，限制网络处理峰值交易负载的能力。这会导致延迟增加和吞吐量降低。

3、未达到最佳并发性：Solana 并行处理的可行性受到线程限制。因此，并发交易处理的全部优势没有得到实现，从而降低了网络的整体效率。

X1 的方案：动态线程扩展

为解决这些限制，X1 引入了一个动态扩展的执行调度器。这项创新允许根据节点上可用的 CPU 核心数来扩展银行线程的数量，从而优化硬件的利用率。

自适应线程分配：X1 的执行调度器根据检测到的节点 CPU 核心数动态调整银行线程数。例如，在具有 32 核处理器的节点上，调度器可以分配多达 32 个银行线程，从而显着提高交易处理能力。

增强并行性：通过利用额外的线程，X1 最大限度地提高了并行交易处理能力。这种方法最大限度地减少了与有限线程数的瓶颈，从而实现更高效的执行管道。

提高吞吐量：同时处理更多交易的能力与网络吞吐量的提高直接相关。随着使用更多线程，交易确认时间会减少，尤其是在高网络负载条件下。

可扩展性和面向未来：X1 的动态线程扩展机制旨在随着硬件技术的进步而扩展。随着多核处理器变得越来越强大和普遍，区块链可以无缝扩展其执行能力，确保长期可行性和性能。

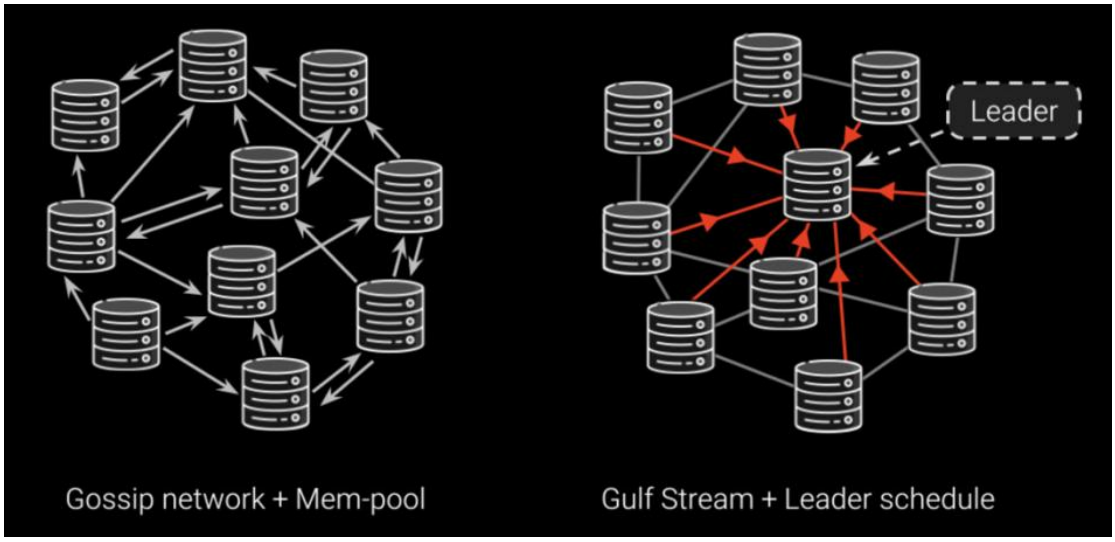
通过将线程分配与可用的硬件资源保持一致，X1 旨在消除当前区块链架构中阻碍交易吞吐量的瓶颈。这种方法增强了网络的敏捷性，并使区块链能够抵御当今系统的局限性，确保它能够随着硬件技术的发展而有效扩展。

2、基于绩效的领导者选择

为高性能验证者节点创建激励措施

领导者（Leader）

Solana 之所以脱颖而出，是因为它从一开始就被设计为在没有内存池的情况下运行。与使用八卦协议（Gossip Protocols）在网络上随机和广泛传播交易的传统区块链不同，Solana 将所有交易转发给每个插槽的预设主要验证者，称为领导者。一旦 RPC 收到要包含在区块中的交易消息，就必须将其转发给领导者。



领导者选择

在每个纪元（Epoch）之前（大约每两天）生成一个领导者计划。即将到来的纪元被划分为多个插槽（Slot），每个插槽固定为 400 毫秒，并且为每个插槽选择一个领导者。领导者的顺序是提前确定的，验证者知道他们何时会成为领导者。这种轮转发生得非常快，领导者每隔几百毫秒就会更换一次。

拥有较高质押比例的验证者在每个纪元被选为领导者的可能性更高。在每个插槽期间，交易消息被转发给领导者，领导者有机会生产一个区块。当轮到验证者时，他们切换到“领导者模式”，开始积极处理交易并将区块广播到网络的其余部分。

验证者性能

Solana 的“跳过率”——未产生区块的插槽百分比——从 2%到 10%不等。虽然分叉是跳过插槽的主要原因，但验证者性能是另一个重要因素。目前，成为领导者的唯一选择标准是质押权重，未考虑验证者的表现。

如果验证者被选为领导者，但由于网络连接问题或硬件问题而表现不佳，他们就有可能跳过他们本应获得奖励的插槽。这不仅会减慢网络的速度，还会增加交易被丢弃的风险，从而不利于链的整体性能。

在 Solana 上，有一些节点具有相当大的质押权重，尽管历史表现不佳，但它们经常被选为领导者。其中一些节点的跳过率超过 50%，但它们仍继续在领导计划中被选中。Solana 目前不会从领导者计划中拒绝表现不佳的验证者，这会导致网络效率低下。

基于绩效的领导者选择

为了优化系统，很明显，领导者的选择不应该仅仅基于质押权重。除了质押权重外，X1 还将在领导者计划中引入新的资格标准。质押权重将被虚拟化为一个数值，该数值可以根据验证者的历史表现进行调整。如果验证者的数值因表现不佳而下降，他们将被从领导者计划中移除或完全拒绝成为领导者。

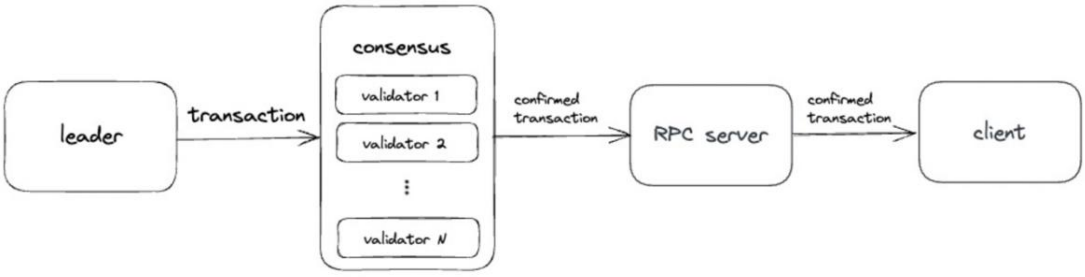
该解决方案利用现有的经济激励措施，鼓励验证者维护高效和高性能的节点。通过将质押权重和历史表现纳入选择过程，X1 旨在确保只有最有能力的验证者被选为领导者，从而提高网络的整体效率和可靠性。

3、简化扩展

优化验证者小组委员会共识

共识

一旦交易被领导者执行，它就会立即被记录到验证者的账本副本中，并传播到网络的其余部分。在区块获得必要的共识投票后，该交易被视为“已确认”。最后，当一个区块之上已经构建了 31+ 个已确认的区块时，它被“最终确定”。这些过程通过 RPC 返回前端，使用户能够查看其交易的状态。



许多区块链网络在广播区块之前构建整个区块，称为离散区块构建。相比之下，Solana 采用连续区块构建，这涉及在分配的时间段内创建区块时动态组装和传输区块，从而显着减少延迟。

要使区块被接受，其中的所有交易都必须是有效的，并且其他节点可以复制。领导者将块分成较小的部分，称为“碎片”。每个碎片都包含区块数据的一部分，并使用加密哈希链接到其他碎片。

领导者将碎片广播到集群中的验证者节点。这通常是通过八卦协议完成的，以确保数据的广泛和高效的传播。验证者收集碎片，并从收到的碎片中重建整个区块。

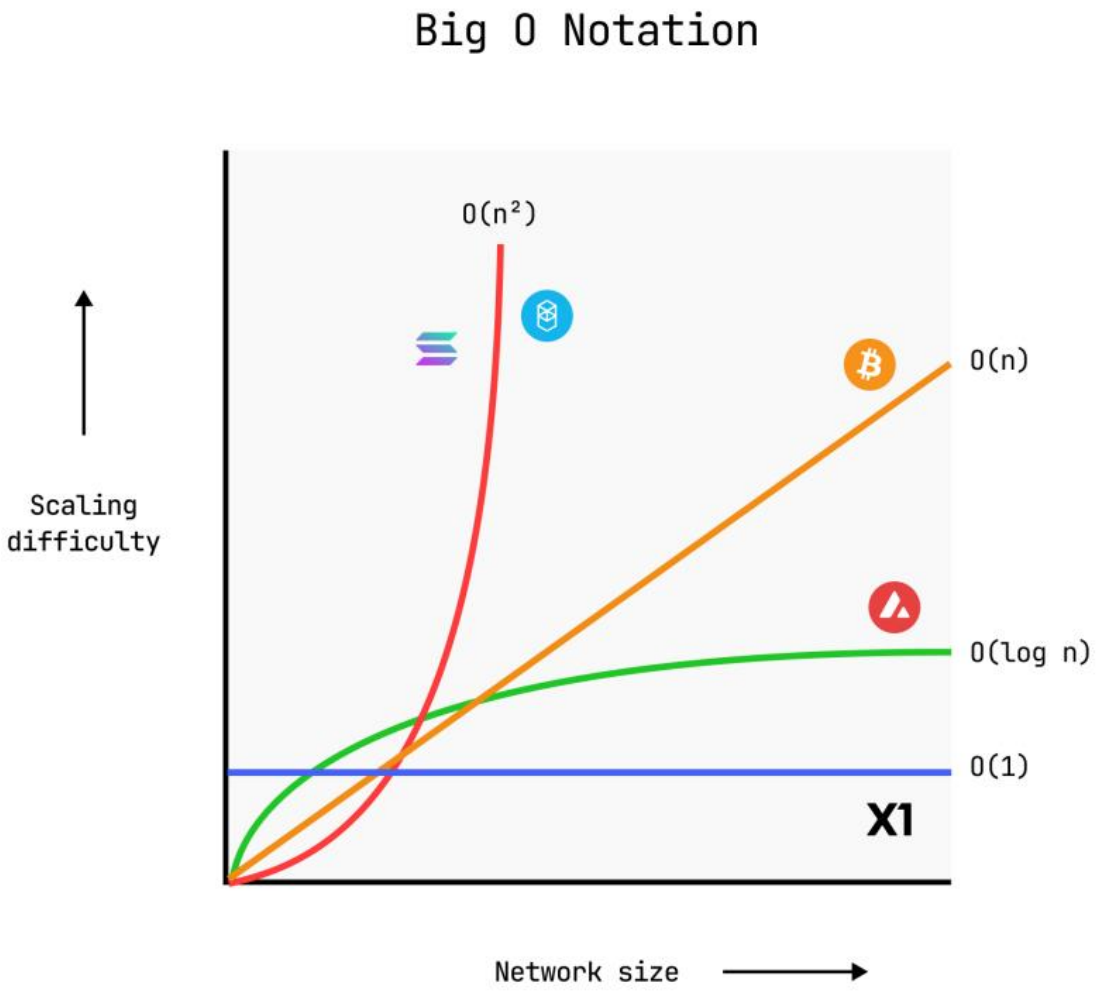
验证者通过检查 PoH 哈希值并确保交易有效且没有被双重花费来验证区块的完整性和有效

性。

一旦验证者验证了一个区块，它就会向网络的其余部分发送投票交易，表明该区块是有效的。当收集到足够的选票时，网络达成共识，并将区块添加到区块链中。
在 Solana 区块链中，要确认一个区块，需要集群中验证者的绝对多数票。具体来说，这种绝对多数被定义为网络中总投票权的三分之二（或 66.6%）。

网络规模小时模型运行良好，但随着时间的推移会导致扩展挑战，通过算法复杂性的概念更好应对。

算法复杂性



区块链技术中的共识可扩展性困境

在保持安全性和去中心化的同时解决可扩展性问题对区块链技术来说是一个重大难题。比特币和以太坊等传统区块链在这一领域遇到了挑战，随着网络规模和活动的扩大，经常遇到瓶颈。这些网络利用中本聪式的共识机制，需要最终用户通过交易费用来竞争写入区块。

由于区块大小的静态属性和区块创建的固定频率，与不断增长的网络使用需求形成鲜明对比，这种机制导致交易费用增加，并在需求高峰期延长确认时间。

共识复杂性：二次元难题

与比特币和以太坊不同，像 Fantom 和 Solana 这样的区块链采用了一种替代方法，即实施异步区块投票机制。这种方法至少需要三分之二的网络节点参与消息交换，以便于投票。这个过程的结果是一个二次增长的共识复杂度，在数学上表示为 O（n^2）。尽管这种策略对于用户的交易来说可以非常敏捷和快速，但它本质上限制了网络的可扩展性，因为节点数量不断增加。

雪崩链（Avalanche）：社区

Avalanche 采用了一种新颖的策略，通过引入社区来降低复杂性。通过采用类似八卦的结构机制，Avalanche 将其共识复杂度巧妙地降低到对数尺度，即 O（log（n））。这一进步标志着在不按比例增加共识复杂性，并且保持快速交易执行时间，向增强可扩展性迈出了重大一步。

X1 区块链：通过简化法进行扩展

X1 通过整合子委员会投票来改进其共识算法，这是一个借鉴了 HotStuff2 共识模型的概念。此增强功能解决了传统区块链网络（例如 Solana）中发现的不可避免的问题，由于平面网络拓扑要求所有节点参与投票，因此投票过程为 O（n^2）。这种过度的沟通会造成瓶颈，减慢共识进程。

相比之下，X1 区块链采用了一种更简化的方法，通过选择较小的节点子集或子委员会来处理投票和验证。这减少了整体通信开销和计算负载，从而能够以更少的资源更快地达成共识。通过支持无限数量的节点（n），同时只需要有限的组（x）进行投票，X1 区块链保持恒定的时间复杂度 O（1），以实现共识操作。

这种对小组委员会的战略性使用增强了 X1 区块链的可扩展性和敏捷性，使其能够处理更大的网络和更高的交易量，而没有传统共识方法的缺点。采用小组委员会投票可确保网络保持可扩展性和安全性，为未来的增长奠定坚实的基础。

4. 全局收费市场

X1 中的全局费用市场和动态费用调整

Solana 当前收费市场的局限性

Solana 目前的交易费用市场主要由本地费用市场管理，这些市场专注于优先考虑各个区块内的交易。这种方法在保持高效的网络性能方面带来了一些挑战，尤其是在高需求下：

1. 静态经济压力：Solana 上交易签名的基本费用静态设置为至少 5,000 lamports。这种固定的费用结构不足以在网络需求旺盛的时期施加强大的经济压力。因此，网络更容易受到垃圾邮件交易的攻击，这可能会降低整体网络的效率并降低服务质量。

2. 没有全局手续费调整：Solana 不采用全局块计算单元 （CU） 会计机制。否则，交易费用不会根据网络计算资源的整体需求动态调整。在高峰期，缺乏全局调整机制可能导致网络拥堵和性能瓶颈，因为低优先级交易持续争夺空间，而没有任何经济抑制因素。

3. 统一的基本费用制定：Solana 当前模型中的基本费用统一应用于所有交易，无论网络条件如何。这种方法限制了区块链适应不同需求水平的能力，导致资源分配欠佳，并且在高流量时期服务质量可能下降。

X1 的方法：动态的全局收费市场

X1 通过引入全局费用市场机制，结合动态费用调整来解决这些限制，旨在提高网络性能和适应性。该方法包括以下关键创新：

动态基础费用，门槛更低

X1 实施了灵活的基本费用结构，将较低的门槛设置为每个签名 500 lamports。与 Solana 的静态费用不同，此基本费用会根据网络上的全局负载动态调整。随着需求的增加，费用会随着需求的增加而增加，从而确保费用结构对网络的运行状态保持响应。

全局块计算单元计费

X1 集成了一个全局块计算单元（CU）记帐系统，该系统持续监控网络的总计算负载。该系统能够根据实时使用情况动态调整交易费用，使费用结构与网络的当前需求和计算能力保持一致。

动态收费阶梯机制

受以太坊 EIP-1559 模型的启发，X1 采用了类似的动态费用调整流程。这种机制根据区块计算能力的追踪利用率调整基本费用。当网络负载增加时，基本费用会逐渐提高，从而对优先级较低的交易施加经济压力。这有助于确保在需求高峰期间仅处理高优先级交易，从而防止网络拥塞。

经济背压与资源配置

X1 中的动态费用缩放机制旨在提供经济背压，使交易优先级与网络容量保持一致。随着网络负载的增加，交易费用的相应上涨会激励用户仅提交必要的交易。这种方法降低了网络拥塞的可能性，优化了资源分配，并确保区块链即使在不同的条件下也能保持高性能。

X1 实施全局费用市场和动态费用缩放，引入了更具适应性和响应性的交易费用模型。通过结合实时网络负载监控和灵活的费用调整，X1 旨在提高网络性能，减少拥塞，并在各种条

件下保持高效的运营。

5、同态加密

执行加密计算

什么是同态加密？

同态加密是一种加密类型，允许对加密数据执行计算，而无需先解密。这些计算的结果在解密时与对原始未加密数据执行相同操作的结果相匹配。此属性允许处理和分析数据，同时保持其机密性。

同态加密很重要，因为它允许对加密数据执行计算，而无需先解密它。此功能非常重要，原因如下：

1. 隐私保护：通过同态加密，敏感数据即使在处理过程中也可以保持加密状态。这在云计算等场景中至关重要，在这些场景中，用户可能需要将计算外包给第三方，但希望确保他们的数据保持机密。

2. 安全性：由于数据在处理过程中永远不会被解密，因此由于违规或内部威胁而暴露的风险大大降低。这增强了处理数据的系统的整体安全性。

3. 合规性：许多行业（例如医疗保健和金融）都受到有关数据隐私的严格规定的约束。同态加密可以使组织能够以加密形式处理数据，从而帮助组织遵守这些法规。

4. 数据实用程序：它允许对加密数据进行有意义的分析和计算，而不会影响其安全性。这在协作环境中特别有用，在这些环境中，不同的各方需要在不泄露实际内容的情况下处理共享数据。

凭借线性带宽扩展和数十毫秒的解密运行时间，加密更加高效和轻量级。

同态加密可以用来做什么？

可编程加密和条件解密可用于广泛的用例，包括加密的链上意图（限价单、止损单、可编程交易）、不良 MEV 预防、私有治理、审查和抗抢先运行共享排序、汇总、链上游戏、法律合同、随机生成预言机，以及任何不对称信息限制去中心化应用程序使用的场景。

运作方式

从任何应用程序前端，用户都可以通过声明其解密条件来加密交易。然后，加密的交易被提交到网络。可以在相同条件下对多笔交易进行加密，并批量解密。

一旦满足解密条件，验证者就会收到通知，并共同生成阈值解密密钥。然后，私钥被发送到目标链以解密加密的交易。
私钥用于解密每个解密条件的所有加密交易，然后在应用程序所在的网络上执行这些交易。