## 区块链提升TPS技术方案选型

在区块链系统中，TPS（Transactions Per Second）是衡量系统性能和可用性的重要指标，直接影响用户体验和商业落地能力。为提升TPS，可从硬件、架构优化和拓展性方案入手：

##### 硬件

###### **芯片加速**

- 芯片加速：采用FPGA/ASIC专用硬件加速加密计算（如椭圆曲线签名验证），可提升交易验证速度，减轻节点 CPU 负担，但显著增加节点成本并可能导致中心化风险。

###### **cpu、内存、网络**

- CPU/内存升级：部署多核服务器配合大容量内存，提高交易并行处理能力，但无法解决区块链底层架构瓶颈。

- 网络优化：使用专用光纤网络和低延迟协议，将区块传播时间从秒级降至毫秒级。

**局限性：**硬件优化在小范围内提升单节点性能，无法实现数量级突破，且破坏区块链的去中心化特性。

##### **架构**

###### **减少交易数据**

通过优化交易结构、简化交易内容或压缩交易数据，可以减小每笔交易的大小，从而提升区块中能够容纳的交易数量，提高整体 TPS。例如利用交易签名聚合、状态差异更新等技术减少链上数据量。但该方法受限于数据的最小化程度，且压缩复杂度可能导致验证成本增加。

###### **增加区块大小**

增加区块的大小可以包含更多的交易，进而提高区块链的交易吞吐量，例如比特币现金（BCH）将区块从 1 MB 扩大到 8 MB，之后扩展到 32 MB。但扩大区块的同时也会增大传播延迟引发安全威胁, 比如导致分叉可能性增大和 DDoS 攻击。

###### **选择共识算法**

共识协议保证了区块链各个节点对于区块链的状态更新达成一致，已经用于区块链的共识机制有 PoW、PoS、PBFT 等。为了满足可扩展性的需求，一般高性能公链都会改进共识协议，并结合自身特殊机制，例如 Solana 基于 PoH 的共识机制，Avalanche 基于雪崩的共识机制。

###### **更换虚拟机**

虚拟机负责智能合约的执行效率，是TPS瓶颈之一。采用高性能虚拟机或对现有虚拟机进行优化（如改进字节码解释、支持并行执行、减少内存消耗）可以提升合约执行速度，进而提高区块处理能力。部分新兴区块链采用自定义虚拟机以适配特定需求，提升整体性能与开发体验。但更换虚拟机带来兼容性和生态迁移的挑战，需要综合考虑。

##### **拓展**

###### **搭配侧链**

**原理：**侧链是与主链平行运行的独立区块链，通过双向锚定（跨链桥）实现资产和数据在主链与侧链之间的流转。拥有独立共识机制和执行环境（通常基于 EVM 或兼容虚拟机），负责处理大部分交易和计算，减轻主链负载并提升吞吐量与交易速度。

**优势与不足：**技术门槛低，便于快速部署定制化功能（如支付、游戏、高频交易），支持灵活的隐私保护和业务逻辑创新，可根据需求在安全性、去中心化和性能间灵活取舍。但其安全性依赖自身共识机制，存在安全隔离风险，跨链桥容易成为攻击目标。侧链的信任假设弱于主链，在生态和用户规模较小时去中心化和安全性有限，跨链资产转移也通常存在延迟和成本。

**现状：**代表项目包括 xDai Stable Chain（以太坊侧链，通过跨链桥实现低费率稳定币支付，适用于 P2P 支付和订阅等场景）与 SKALE Network（支持高吞吐低延迟的可配置弹性侧链，满足不同 DApp 的性能和功能需求）。

###### 搭配二层网络

Layer2（二层网络）是提升区块链 TPS 的主流方案，本质是主链的“扩展执行层”，依赖主链的共识机制和安全性，并不是独立于主链的独立链。其核心做法是将大量计算和交易搬到链外处理，仅将状态根或证明提交主链保障安全，目前的方案包括以下五种：

* + 1. Optimistic Rollup

**原理：**通过假设提交的交易和状态是正确的，仅在有人质疑时在挑战期（一般 7 天）内触发欺诈证明，回滚错误状态以确保安全性。由于不需要即时生成复杂的加密证明，Optimistic Rollup 实现较简单，兼容以太坊 EVM，便于将现有合约迁移，无需修改业务逻辑即可扩容，已被 Arbitrum、Optimism 等项目广泛应用。

**优势与不足：**该方案优势在于技术成熟、兼容性好、开发迁移成本低，适用于希望快速扩容且保持与主链合约兼容的 DApp。其不足在于挑战期导致用户提款存在延迟（一般 7 天），影响资金流动性。此外，如果挑战和欺诈证明机制设计不完善，也可能引发安全风险或拖延问题。

**现状：**目前，部分项目正通过引入依赖受信任执行者或 DAC 来实现“快速提现”机制，从而缩短提款等待时间，提升用户体验。

* + 1. **ZkRollup**

**原理：**在每次提交状态时使用零知识证明（如 zk-SNARK 或 zk-STARK）验证状态和交易的正确性，主链通过验证加密证明完成即时状态确认，无需挑战期即可确认最终性，从而大幅提升用户体验和安全性。代表项目包括 zkSync、StarkNet、Polygon 等。

**优势与不足：**该方案确认速度快、无需信任第三方和挑战期、即时提现、数据可用性好，安全性依赖主链保障，抗审查性强。其不足在于零知识证明生成计算复杂，部署和维护成本较高，且目前在支持复杂智能合约和完全 EVM 兼容方面尚在持续优化，开发调试难度相对大，开发生态和工具链也在逐步完善中。

**现状：**当前，zkSync2.0（也称为 zkSync Era）、Polygon zkEVM 已提供了对 EVM 的完全兼容，逐渐成为二层扩容技术的重要方向。

* + 1. **Plasma**

**原理：**通过在主链之上构建多层级子链执行交易和计算，仅周期性向主链提交状态根（Merkle 根），减轻主链负载，提升吞吐量与计算能力。Plasma 支持智能合约执行，可运行大规模用户操作，适合用于支付和部分复杂业务场景。

**优势与不足：**通过欺诈证明机制确保安全，用户可在子链提交无效状态时挑战并追回资产。然而 Plasma 存在数据可用性问题，当子链执行者拒绝公开交易数据时，用户难以生成欺诈证明维权，且退出过程复杂并需等待较长时间，限制了其实用性和发展空间。

**现状：**目前代表项目包括支持高频支付和去中心化交易的 OMG Network、曾使用 Plasma Cash 的 Loom Network，以及采用 POS + Plasma 混合方案并支持游戏和 DeFi 应用的 Matic（Polygon 前身）。

* + 1. **状态通道（State Channel）**

**原理：**受比特币闪电网络启发，通过在固定参与者（通常两方）间开设通道，将大量交易搬到链下实时执行，仅在开启和关闭时与主链交互结算，依靠链上锁定保证金与带签名的链下状态更新保障安全，大幅降低延迟与费用。

**优势与不足：**延迟极低（毫秒级）、手续费极低、TPS 理论无限扩展，适合高频小额支付和链下游戏等即时确认场景。不足在于需预先锁定保证金，仅适用于固定参与者间交易，不支持全局状态共享和复杂合约，退出时存在争议窗口和延迟。  
 **现状：**代表项目包括 Celer Network（兼容以太坊、波卡、Near 等多链生态的状态通道平台）和 Raiden Network（以太坊上的支付通道网络）等。

* + 1. **Validium**

**原理：**同样基于零知识证明，但将交易数据存储在链下，仅将零知识证明提交至主链验证状态正确性，相较 ZkRollup 提供更高的扩展性和更低的成本，还避免了像 Plasma 依赖欺诈证明的复杂性与长退出周期，提升安全性。  
 **优势与不足：**极高的吞吐量和极低的链上数据成本，适用于对性能和费用敏感的大规模交易场景，如去中心化交易所和衍生品平台。不足在于由于数据存储在链下，安全性依赖数据可用性委员会（DAC）或运营者保证数据可用性，所以存在冻结资金风险和潜在审查问题。  
 **现状：**目前代表项目包括使用 StarkEx 提供 Validium 扩容能力的 DeversiFi（去中心化交易所）、计划集成 Validium 优化体验的 dYdX 永续合约产品等。

##### **结论**

不同扩容方案适用场景各异：状态通道适合高频小额支付但局限于固定参与者，Plasma 退出复杂且数据可用性不足，Validium 虽具高吞吐量但依赖链下数据可用性，ZkRollup 性能高但开发成本大。相比之下，Optimistic Rollup 简单可行、兼容性强、迁移成本低，是目前最易落地的 Layer2 扩容方案。综合考虑安全性、性能和兼容性，本系统最终倾向优先选择基于 **Optimistic Rollup** 的 **Arbitrum** 提升 TPS，为后续规模化落地奠定基础。