Tachyon field Chain

快子公链技术白皮书

Version 1.1.0

https://www.tafchain.com/

摘 要

区块链作为构建在互联网之上的新一代可信的数据关系系统，通过其核心价值，为数字领域塑造了信任关系。其解决了传统互联网时代无法解决的重大问题，如数据的所有权问题、数据的隐私问题、数据的质量和真伪问题等。另外，区块链作为数据经济的基础设施，成为数据市场的核心，将对现有的商业社会产生深远的影响。然而，拥有透明、去中心化、安全、信任等诸多优势的区块链系统在解决了众多传统互联网无法解决的难题后，依然无法在各行各业里大规模商业应用，究其原因在于目前主流的区块链性能低下所致。一项技术究竟能否大范围应用于日常的生产、生活，除了功能完备以外， 性能显然是一项极其关键的指标。

另外，阻碍商业级用户核心商业数据上链的重要原因在于数据所有权及隐私问题。区块链的透明、账本共享等特点，导致商业级用户无法把核心商业机密数据上链。上链就意味着公开。例如，商业用户的战略发展规划、研发计划、投资规划、经营收益规划等，市场分析、经济分析等形成的综合性报告、调研资料、行业及竞争对手的研究材料等，这些重要机密材料由于隐私问题无法上链，严重影响了区块链对于商业用户领域的拓展。

为了解决目前区块链领域所存在的，导致其无法大规模商业应用落地的核心问题，TAF Chain 团队从链的本身开始设计并重构各基础模块，在达到高性能的同时，满足特殊用户数据隐私的要求。另外其作为一条高性能的区块链基础设施，为商业级用户提供了隐私保护套件，打通了商业级用户核心隐私数据上链通道。

TAF Chain 独创的引入了双层网络共识机制和 VRF（Verifiable Random Functions）算法，优化了目前主流项目的 DPoS 共识机制存在的算力过于集中问题，并解决了社区活跃度不足等相关选举问题。TAF 的投票选举方案，具有一定的随机性，攻击者无法预先推测出选举的最终结果，大大提高了整个网络的安全性。另外，VRF 机制的引入，使得选举的最终获胜者不一定是持有代币最多者，解决了持有绝大多数代币者（如交易所）长期处于垄断位置的问题，一定程度上激活了社区参与度，保证了选举过程的长期公平性。另外，TAF Chain 独创的采用双层网络来实现全网节点数据一致性的机制。可以有效提高整个网络的性能，解决了目前主流的 DPoS 共识机制算力过度集中的问题。在其网络中，参与竞选的节点需要质押一定数量的 TAFT 资产，如若当选节点有不作为或作恶情况，会扣除部分或全部质押代币作为惩罚。在节点参与竞选时质押资产，引入了惩罚机制，增加了节点作恶的成本。一定程度上保证了网络的长期稳定和安全。

未来，TAF Chain 也将继续专注于高性能区块链网络，为商业级用户数据隐私上链提供创新与实践。为商业级区块链市场提供高性能、共治、安全、隐私的区块链底层基础服务，成为全人类的可信数字化时代的公共基础设施。

目 录

1. 背景

区块链解决了传统互联网时代无法解决的重大问题，如数据的所有权问题、数据的隐私问题、数据的质量和真伪问题等。这也使得其作为数据经济的基础设施，成为数据市场的核心。因此，区块链技术的核心价值--塑造数字信任，将对现有的商业社会产生深远的影响。然而，拥有透明、去中心化、安全、信任等诸多优势的区块链系统在解决了众多传统互联网无法解决的难题后，依然无法在各行各业里大规模商业应用，究其原因在于性能问题。一项技术究竟能否大范围应用于日常的生产、生活，除了功能完备以外， 性能显然是一项极其关键的指标。何为区块链的性能呢？区块链的性能指标主要包括交易吞吐量和交易延时。交易吞吐量表示在固定时间能处理的交易数，一般常规的用 TPS（每秒处理交易的数目）来计量；延时表示对交易的响应和处理时间。在具体应用中，吞吐量和延时两个指标需要综合进行考察。如果只考虑交易吞吐量而不考虑延时会阻碍用户使用，从而影响用户体验；如果只考虑延时而不考虑吞吐量，则会被那些必须处理大量并发交易的平台直接抛弃。

“区块链没能大规模应用的一个重要原因是物理性能不高（特别对公有链）。”中国人民银行 2018 年 11 月发布的题为《区块链能做什么、不能做什么？》的 1.5 万字篇幅工作论文曾这样表述。这篇论文同时也称，“目前真正落地并产生社会效益的区块链项目很少”的原因之一也是区块链物理性能不高。在上述央行工作论文中，研究人员举例称：比特币每秒钟最多支持 6 笔交易，而 Paypal 平均每秒钟能支持 193 笔交易，Visa 平均每秒钟能支持 1667 笔交易。另据可查的资料显示，金融系统的交易吞吐量至少是万次 / 秒的量级。这就对区块链系统的确认时间、每秒处理交易的能力（TPS）要求也非常高。然而，很多区块链技术平台每秒只能处理几百笔交易。相比之下，微信钱包在最高峰时候能处理 20 万 tps，支付宝在双 11 的时候到了 54.4 万 tps。假如 TPS 太低，很容易造成网络严重拥堵，从而使得区块链在高价值的高并发业务领域无法落地。此外，由于 TPS 太低，比特币、以太坊都存在交易费用高、确认时间长、扩展性差等短板。

此外，阻碍商业级用户核心商业数据上链的重要原因在于数据所有权及隐私问题。区块链的透明、账本共享等特点，导致商业级用户无法把核心商业机密数据上链。上链就意味着公开。例如，商业用户的战略发展规划、研发计划、投资规划、经营收益规划等，市场分析、经济分析等形成的综合性报告、调研资料、行业及竞争对手的研究材料等，这些重要机密材料由于隐私问题无法上链，严重影响了区块链对于商业用户领域的拓展。

如果有更好的方案，能够在多方面解决区块链的性能问题，以及针对商业级用户需求的隐私问题，不但可以获得广泛的普通用户生态，也同样可以拥有大规模的商业级用户生态，以商业级机密数据上链作为突破口，使得大规模商业应用落地成为可能。

2. TAF Chain 技术架构

2.1. 什么是 TAF Chain

为了解决目前区块链领域所存在的，导致其无法大规模商业应用落地的核心问题，需要重构其核心算法及数据交换方式。目前影响性能的技术因素主要存在于广播通信、信息加解密、共识机制、交易验证机制、存储机制等多个环节。更具体的说，为了解决目前影响大规模商业应用上链的问题，我们需要从链的本身开始，设计并重构各基础模块，在达到高性能的同时，满足特殊用户数据隐私的要求。

TAF Chain 就是这样一条高性能的区块链基础网络，其基于区块链的分布式特性、密码学、共识机制等技术手段和通证设计，为商业级用户提供了隐私保护套件，打通了商业级用户核心隐私数据上链通道。未来，TAF Chain 也将继续专注于高性能区块链网络，为商业级用户数据隐私上链提供创新与实践。为商业级区块链市场提供高性能、共治、安全、隐私的区块链底层基础服务，成为全人类的可信数字化时代的公共基础设施。

2.2. 核心技术

TAF Chain 相对于其他 DPoS 共识机制的公链，社区节点为了成为候选者，需要根据当时实际的通证 TAFT 流通量，质押一定量的 TAFT。这一改进举措使得网络中候选者节点冗余更少，选举效率更高。进一步，引入了当选节点的惩罚机制及激励机制，在任期内没有完成区块打包任务（或作恶）的节点，TAF 网络会对其质押的通证扣除部分或全部。另外，在 TAF Chain 的选举过程中，引入了 VRF 机制，一定程度上解决了传统 DPoS 垄断性高的问

题，由于攻击者无法事先推算出选举结果，避免了被集中攻击的风险，安全性更高，在一定程度上激活了社区参与竞选及投票的积极性，可保证整个 TAF 网络的长期公平性。

2.2.1. 节点选举

在 TAF Chain 网络的治理生态中，参与共识的节点分为以下四个类型：

委任打包节点

负责区块原始数据的计算及创建，如交易验证、Merkle 树等，该节点需要提供教大的计算能力。其工作在 TAF 共识的 Layer1 层。

委任验证节点

该类型节点负责已经完成原始数据计算的区块在整个链条上的一致性工作。其工作在 TAF 共识的 Layer2 层。

备选委任打包节点

负责在委任打包节点出现问题或受到干扰，无法正常完成区块打包任务时，该类型节点顶替上，以维系整个区块链网络的稳定性。

备选委任验证节点

委任验证节点的备选节点。当 TAF 网络中出现“不合格”委任验证节点时，该类型节点将其替换。

TAF Chain 作为开放的公链系统，所有的节点都可以参与到生态的治理中来。项目初期我们将采用“27+21+43+49”的形式进行节点的选举。

选举过程如下

1. 全网所有持有 TAFT 代币的用户，均可以参与进来，根据持有代币的数额，可获得相应的投票权力。
2. 根据得票率，前 140 名的节点将成为 VRF 候选者节点。
3. 以候选者的代币质押量和得票数作为权重，进行 VRF 运算：
    a. 首先在 140 个候选者节点中，计算出 27 个节点作为委任打包节点；

b. 去除 a 计算出的节点后，接下来计算 21 个节点成为委任验证节点；

c. 去除 a 和 b 所得后，第三次需要进行 43 个备选委任打包节点的计算；

d. 去除 a、b 和 c 所得后，剩下的 49 个节点被标记为备选委任验证节点。

TAF 网络的选举过程，引入了 VRF（Verifiable Random Functions）过程，该投票选举方案，具有一定的随机性，攻击者无法预先推测出选举的最终结果，大大提高了整个网络的安全性。另外，VRF 机制的引入，使得选举的最终获胜者不一定是持有代币最多者，解决了持有绝大多数代币者（如交易所）长期处于垄断位置的问题，一定程度上激活了社区参与度，保证了选举过程的长期公平性。

2.2.2. 共识机制

TAF Chain 研发团队，从性能、安全、社区治理等多个领域系统分析了目前主流的 DPoS 共识机制。

首先在节点选举上，主流项目的 DPoS 共识机制，选择验证人的方式简单粗暴的参考了目前的选举制度，得票率最高者既为获胜者。这样带来了过于集中化的问题，项目后期资产逐渐的集中，例如，大多数用户的代币都存在交易所里。最终的获胜者无法反映出生态用户的实际意愿。大量的出块奖励被少部分人垄断，最终导致代币的流动性越来越小，形成穷者越穷，富者越富的局面。另外，简单粗暴的选举策略，非常的容易被恶意攻击者预先推算出选举结果。

在性能方面，目前主流的 DPoS 共识机制，在选举结束时，所有的出块节点排序后，轮流进行区块生产和确认。由于区块的运算需要非常大的算力，才能在指定的时间内完成。某一时刻算力过度集中，是性能无法提高的关键因素。例如 hash 运算非常消耗 CPU 的计算能力，在 Merkle 树的计算过程中，要进行大量的 hash 运算，才能完成。

治理方面，目前主流的 DPoS 机制，本身就是一种制度性门槛。拥有少部分资产的用户无法从选举中获胜，以获取出块奖励，导致社区用户的参与度越来越低。直到最后，出块奖励将被少部分人垄断，社区很难有人再愿意参与，此时的去中心化网络治理模型就会被少部分人所占有。

TAF Chain 中采用自研 DPoS2.0 共识机制，来实现节点账本状态的一致性。理论上每秒可进行数十万笔交易，TAF Chain 的共识机制分为两层：

Layer1，称为预处理层，由所有的委任打包节点共同完成区块元数据，如交易 Hash、Merkle 树、签名、可信时间戳等的计算，形成一个预处理区块。该层在项目初期拥有 27 个委任打包节点，同时系统开放投票接口。随着 TAF 网络的逐渐稳定，社区用户可通过治理的形式，发起改进提案，由治理委员会严格审查后，可最终确认并执行。

Layer2，称为共识层，由所有的委任验证节点，根据节点所处地域距离形成排序后，依次负责 Layer1 层已创建区块的排序、区块 hash 计算、交易验证及最终结块。并把区块通过 P2P 网络广播给所有委任验证节点，一旦 2/3 以上节点校验并确认区块有效后完成最终区块的确认，此时的交易就成为了不可逆交易。

Layer1 层的委任打包节点受到网络延迟、各节点之间交易一致性等诸多因素影响，并非数目越多越好。Layer2 层的委任验证节点，受到交易确认效率和去中心化程度等条件影响，数目也并非越多或越少约好。TAF 研发团队经过大量第三方 DPoS 项目分析和实验测试计算，项目初期暂定委任打包节点数目为 27 个，委任验证节点数目为 21 个，以达到性能和去中心化的平衡。同时会在社区治理部分设计合约，提供社区用户投票的接口，通过社区投票的形式来决定 TAF 网络在不同的运行阶段共识节点的合理数目。

TAF Chain 独创的采用双层网络来实现全网节点数据一致性的机制。可以有效提高整个网络的性能，解决了目前主流的 DPoS 共识机制算力过度集中的问题。

在 TAF Chain 网络中，参与竞选的节点需要质押一定数量的 TAFT 资产，如若当选节点有不作为或作恶情况，会扣除部分或全部质押代币作为惩罚。在节点参与竞选时质押资产，引入了惩罚机制，增加了节点作恶的成本。一定程度上保证了网络的长期稳定和安全。

TAF Chain 首次在 DPoS 共识机制的选举层，融入 VRF 算法，解决了“得票率最高者既为获胜者”问题，使攻击者无法事先推算出选举的结果，增加了整个网络的安全性。由于选举的获胜者并不一定是资产最多者，在一定程度上激活了社区的参与度。

TAF Chain 在 DPoS 的基础上，独创的引入了双层网络共识机制和 VRF 算法，优化了目前主流项目的 DPoS 共识机制存在的算力过于集中问题，并解决了社区活跃度不足等相关选举问题。

2.2.3. 智能合约

智能合约在区块链项目的生态中扮演着至关重要的角色，同时作为区块链的重要组成部分，TAF Chain 网络中包含两种类型的智能合约：系统合约和用户合约。

系统合约是由 TAF 研发团队为了网络的稳定运行而开发的，在区块链网络启动部署即全网生效。若区块链网络运行期间需要重新部署变更升级，则需要通过链上治理委员会进行发起提案、投票表决最终在未来某个区块高度生效来完成变更。系统合约的模块既可以供区块链内部核心调用也可以对 DApp 提供服务，系统合约主要有入网合约、选举合约、投票合约、原生通证 TAFT 合约、工作量（stake 算力）统计合约、惩罚合约、链上治理合约（链上宪法制定、升级、重要参数确立等）等组成，它们用来保持 TAF Chain 链内部业务的正常有序执行，同时为生态建设更加趋向于良性运作提供保障。

用户合约允许生态内的用户在 TAFChain 主网上通过编写智能合约代码来发行各种数字资产，也可以编写智能合约实现各种复杂的业务逻辑。这使得 TAF Chain 变成了一个自动化、可编程的去中心化平台，任何 DApp 开发者在支付或者质押相应 TAFT 之后即可在链上编写一套完全去中心化的业务系统，完成商业应用的落地，这对 TAF Chain 来说具有重大意义。

TAF Chain 主链采用 C++语言开发，合约机采用轻量级通用智能合约语言(Wasm)，支持 C++语言编写智能合约，追求效率的同时兼顾兼容性。Wasm 是一种为栈式虚拟机设计的二进制指令集，其拥有众多技术优势，如性能高效、内存安全、存储成本低、平台独立和多语言支持等特点。

针对目前大多数区块链智能合约开发者，由于历史的原因，比较熟悉采用 EVM 虚拟机进行智能合约的开发，其已经拥有众多的合约实现，因此 TAF Chain 研发团队会在网络稳定后的第一时间推出 EVM 虚拟机兼容，使得 TAF 用户可以编写 Solidity 智能合约，方便未来的各种 Solidity 实现迁移到 TAF 网络。

2.2.4. 网络通讯

TAF Chain 在 P2P 网络通信方面进行了深入的研究，使得网络通信速度更快，本地办公电脑测试可达每秒 200

万条消息，并且在硬件性能提升以及集群之后的消息并发量还将上升，处理性能也将提高，P2P 网络通信的性能提升也是 TAF Chain 能支撑起高性能、低延时的商业场景的重要前提。

TAF Chain 中的 P2P 网络通信使用无阻塞，纯异步调度的模式，并且在基于传统的 TCP 通信的基础上，按顺序预分配网络套接字，对网络套接字进行缓存，通过哈希表快速查找并使用套接字。另外增加对消息的缓存，并且对传输的消息进行内部协议的高效编码压缩，提高传输的效率。在整体 TAF Chain 网络中，所有的消息都由内部协议编码传输，在保证效率的同时兼顾了安全性。

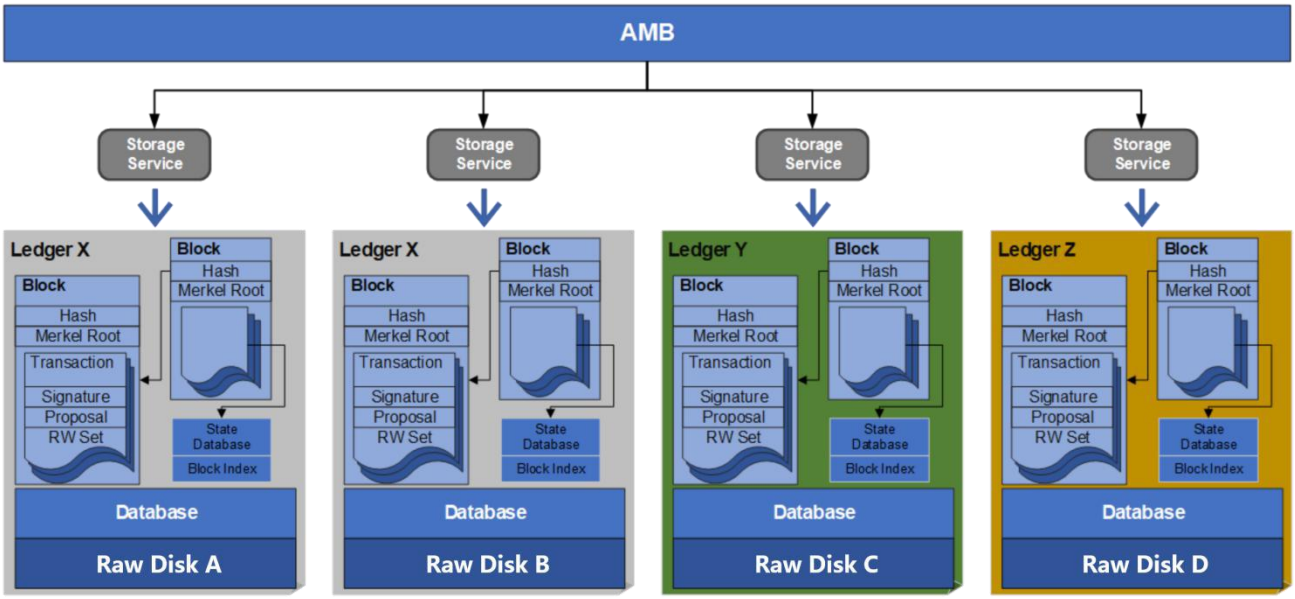
另外，TAF Chain 系统对内部服务间的通信进行了改进，基于整体系统的程序框架，不同功能的服务可以运行在同一个进程上，也可以运行在不同的进程上，但是不管是否在同一个进程中，都可以通过查找服务类型以及 ID 的方式进行直接通信。让开发者在进行消息通信的时候，不用去关心底层的网络消息。不同进程之间会在进程启动的时候，建立本地的 socket 连接，相互之间共享服务，当有需要的时候，就可以直接找到相关服务，让进程间通信的调用体验接近本地通信，提高通信质量。

2.2.5. 存储技术

TAF Chain 网络中的数据存储技术，有别于其他公链的存储技术，例如一些公链，为了追求存储的性能，把状态数据存放在内存中，导致内存资源消耗过大，该类型区块链对共识节点硬件要求极高。另外，还有很多区块链系统是把存储直接放在了第三方的开源数据库，如 LevelDB、RocksDB 等。TAF 的数据存储，不依赖于文件系统，不依赖于任何 SQL、NOSQL 存储搜索引擎，并且做到了事务支持、并行 IO，实现 IO 性能的最大化。

同一账本可以一式多份，分别存储于不同设备，交叉保护、自我修复、并行读取。

TAF Chain 同时支持文件系统、raw 设备和第三方开源存储数据库系统作为其状态及块链数据的存储系统。



针对区块链的特点，在数据读取更新时通过映射的方式快速找到磁盘内的目标位置，大大提高了数据读取更新性能。

该存储技术应用于 TAF 区块链的数据读取更新方法，其特征在于，区块链中的数据存储在磁盘中，磁盘分成多个大小相同的文件 file，该些文件 file 根据需要被分配给对应的业务，在业务内以及磁盘内进行连续编号后分别得到逻辑文件 id 和物理文件 id，这里的物理文件 id 和逻辑文件 id 存在映射关系。文件 file 包含多个大小相同的页 page，页 page 包含多个大小相同的记录 record；该方法包括以下步骤：

1) 根据需要读取更新数据的 record id 计算 page id；

2) 根据 page id 计算逻辑文件 id；

3) 根据逻辑文件 id 和映射关系找到磁盘中物理文件 id；

4) 执行数据读取更新操作。

在计算上述 page id 之前，首先判断需要读取更新数据的 record id 的合法性，在确定需要读取更新数据的 record id 合法后，再计算 page id。上述的 page id 和逻辑文件 id 分别通过下式计算获得：

$$page\ id = record\ id / n$$

$$逻辑文件\ id = page\ id / m$$

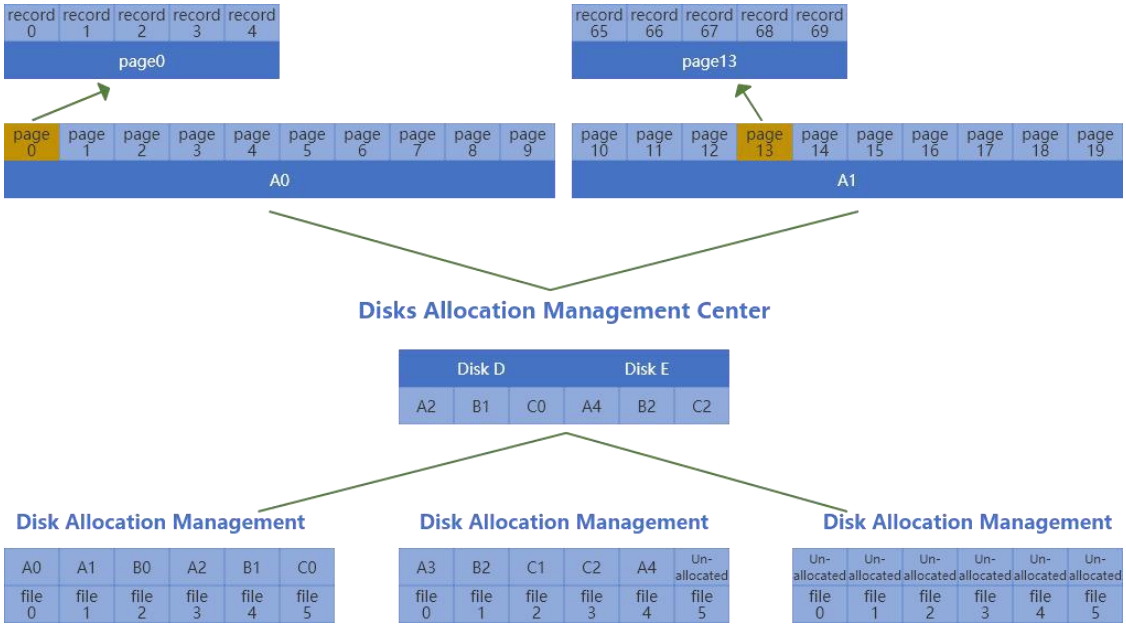
其中 n 为一个页 page 中记录 record 的数量，m 为一个文件 file 中页 page 的数量。得到物理文件 id 后，根据对应的偏移和长度，在物理文件 id 位置进行数据读取更新操作。该系统包括：

page id 计算模块，用于根据需要读取更新数据的 record id 计算 page id；

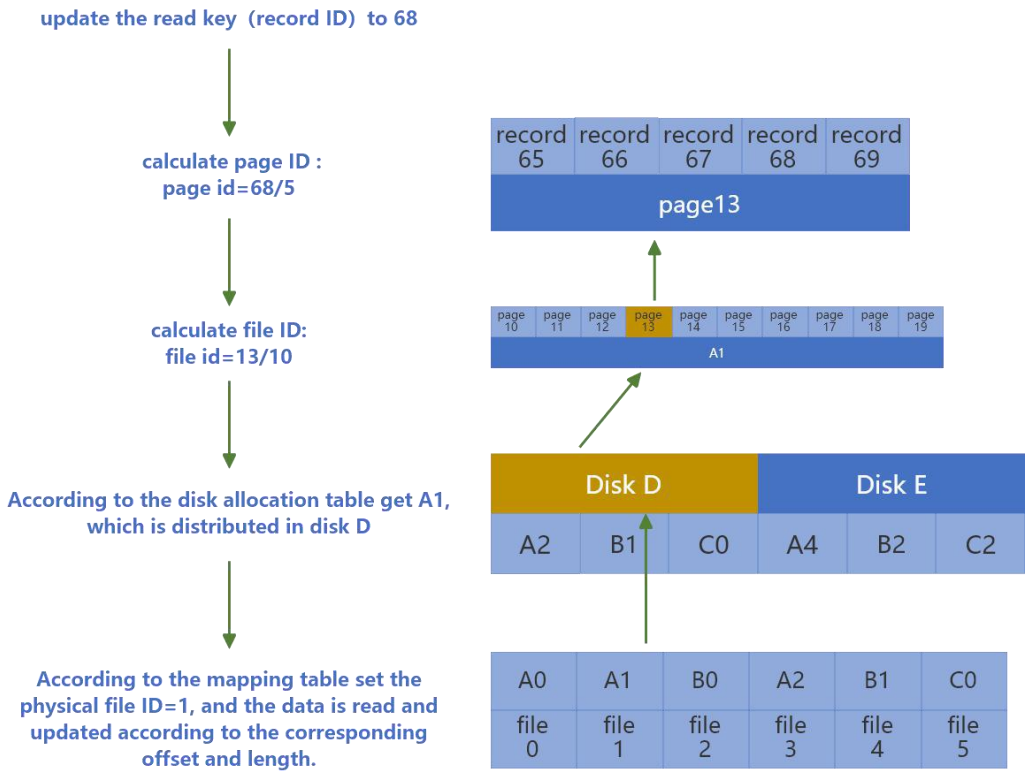
file id 计算模块，用于根据 page id 计算逻辑文件 id；

磁盘位置确定模块，用于根据逻辑文件 id 和映射关系找到磁盘中物理文件 id；

读取更新执行模块，用于执行数据读取更新操作。



磁盘存储结构图



数据读取更新方法的流程图

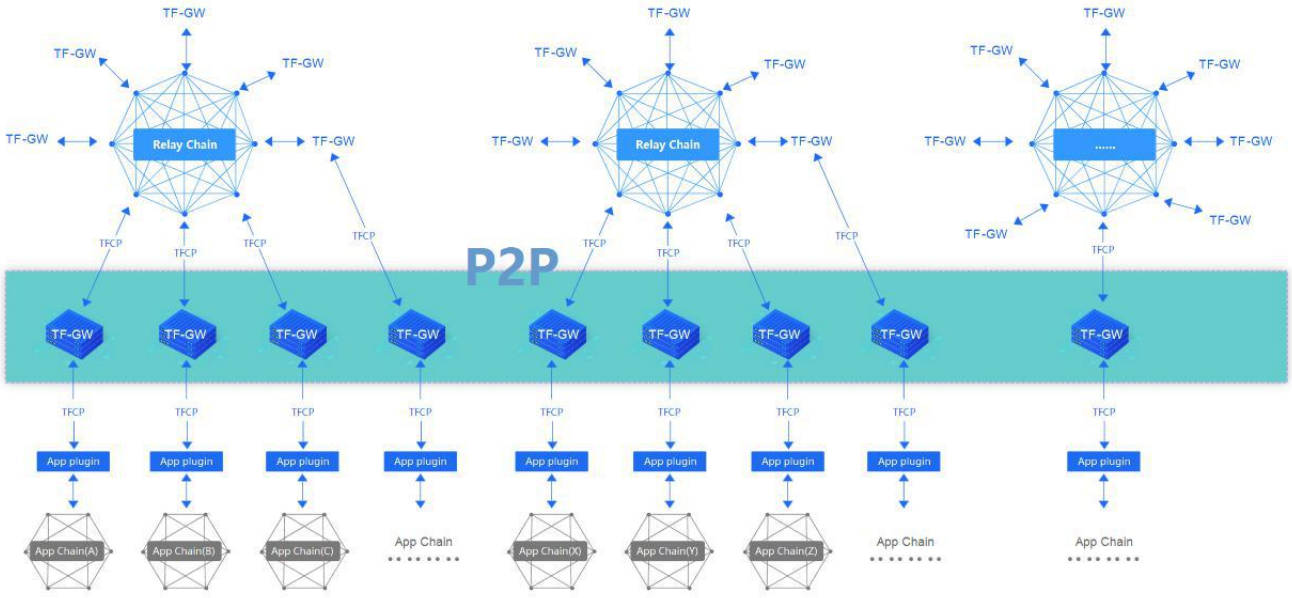
该存储方式，支持动态扩容，如上所描述，当一个物理 id 指定的存储区域写满了之后，可以配置新的逻辑的 id 对应的物理 id，存储可以无缝衔接的到新的物理地址。

基于以上原理，存储的关键在于给逻辑 id 指定物理 id，只需要将逻辑 id 和物理 id 绑定，就可以直接寻址存储，实现真正的不依赖于设备的分布式存储，带来高效的存储体验。并且基于这种方式，也可以更灵活对存储进行扩容。另外为加大存储效率，存储的位置要和存储功能更好的适配，在存储使用之前，需要对存储的位置进行格式化，将物理地址和逻辑地址做适配。

2.2.6. 跨链技术

目前区块链项目平台百花齐放，主流的区块链平台像是一个独立的封闭体系。每个区块链项目就像是一个孤岛，都有独特的技术和生态。但是区块链项目之间无法进行业务的往来。在业务形态日益复杂的商业应用场景下，这严重限制了区块链业务生态的健康发展。例如比特币的持有者无法进行以太坊的去中心化 DeFi 活动、以太坊上的去中心化交易所无法进行比特币交易等。

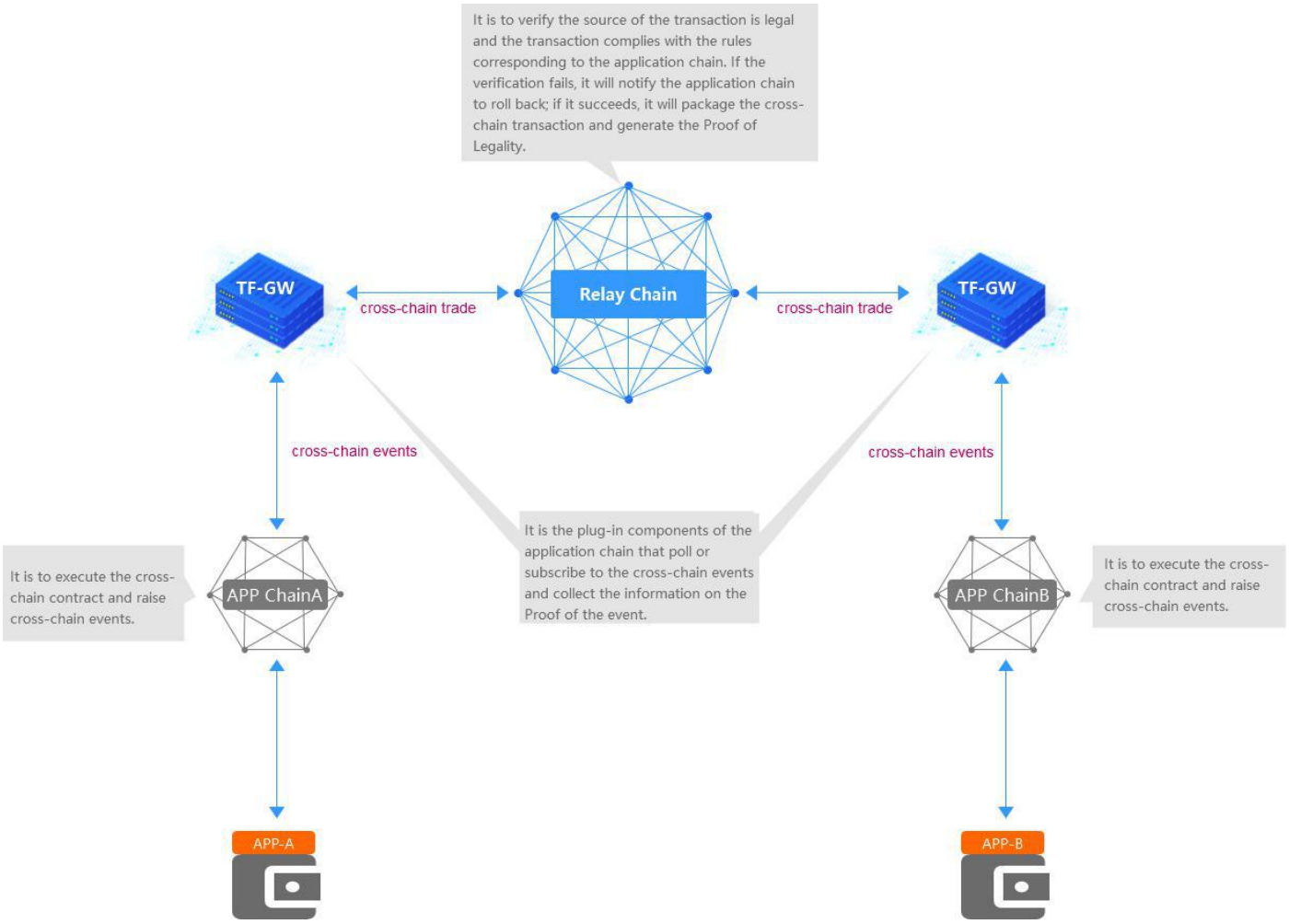
TAFChain 团队基于跨链互操作需求，设计了一种通用的链间消息传输协议 TFCP（Tachyon field Cross Chain Protocol），该协议支持异构区块链之间的跨链交易路由和可信验证，允许资产、数据、服务等进行跨链调用。最终基于 TFCP 实现了异构区块链之间交易的跨链技术平台。打破了不同区块链之间数据无法互通的孤岛效应。



总体架构图

TAF 跨链平台是由中继链（Relay-Chain）、跨链网关（TF-GW）、应用链（APP-Chain）所共同构成的链间互操作平台。在如上 TAF 跨链平台总体架构图里，中继链的作用在于跨链交易的可验证性与可靠路由。跨链网关担任的是区块链间收集交易并进行传播的角色。应用链负责具体的业务逻辑，如比特币、以太坊等公链。

跨链网关（TF-GW）作为整个平台的核心，可分布在任何地区，多个跨链网关之间通过 P2P 网络互通数据，是对接具体类型区块链和转发跨链消息的重要组成部分。它提供了应用链适配器、TFCP 协议探测器、跨链交易路由器等核心模块。另外，该跨链网关支持中继和直连两种模式，中继模式也就是通常所说的通过中继链来进行跨链操作，该模式适合较多区块链进行跨链互操作的场景。直连模式的作用在于该网关可以直接与其他跨链网关建立连接，并进行跨链交易的传递。



跨链交易执行流程

如上图为典型的跨链交易执行流程，应用链 A 上的 APP-A 的用户发起了一笔交易发送到应用链 B 上的 APP-B 的用户。最终这笔交易在应用链 A 和应用链 B 上分别得到确认。以下为该笔交易的整个流转过程。

1. 跨链交易由 APP-A 发起到应用链 A 上，执行相关业务逻辑后，调用事先部署在该应用链 A 上的跨链合约。跨链合约在收到跨链交易请求后，立即抛出一个跨链事件。该跨链事件会及时的被应用链 A 上的插件模块捕获到，此时应用链 A 的插件模块会将相应的跨链交易通过 TFCP 协议发送到跨链网关（TF-GW）网络中去。

2. 与应用链 A 直连的跨链网关在接收到该跨链交易后，将对该交易进行基本的检查操作，如跨链交易有效性检查等。如果该跨链交易有问题，将通知应用链 A 做相应的回滚操作。若检查通过，该交易会被提交到该网关的交易分发模块。

3. 交易分发模块首先确认该笔跨链交易所属于的跨链模式。在中继模式下，交易分发模块会把该笔交易分发到中继链。如果是直连模式，该笔交易将通过 P2P 网络被分配到应用链 B 所直连的跨链网关中。此时的跨链网关 B 进行着交易的同步操作。

4. 在中继模式下，该笔跨链交易将参与中继链的共识过程。将被打包进中继链的区块中。此时，跨链网关 B 将同步与自身相关的中继链区块中所有的跨链交易。对于中继链同步的交易，跨链网关将在自身节点对跨链交易进行验证，确保跨链交易的有效性。如果是直连模式，跨链网关通过 P2P 网络转发跨链交易，应用链 B 的跨链网关接收来自于应用链 A 的跨链网关发来的跨链交易，并对其进行有效性检查。

5. 对于所有同步自其他链的跨链交易，都需要进行交易有效性检查。在中继模式中，由于已经在中继链的交易验证引擎进行验证确认，并参与了中继链的共识过程，中继链会对参与共识的跨链交易进行签名，所以交易检查时只需要验证跨链交易是来自于中继链即可。在直连模式下，由于跨链交易是通过 P2P 网络获取，所以检查跨链交易的过程更加复杂，应用链需要定制跨链交易的验证规则后进行跨链交易检查。

6. 在交易检查完成后，即该笔跨链交易为有效交易，来自于中继链或其他跨链网关的跨链交易，由应用链 B 的插件模块，与应用链 B 对接，在调用跨链合约之前需要确认交易防止重放攻击等。在应用链 B 上执行结果返回后，将把执行结果通过跨链回执的方式，返回到应用链 A。回执过程与跨链交易过程类似。

3. 治理与激励机制

“治理”是公链的核心命题，有效合理的去中心化治理机制对于公链的长久发展至关重要。TAF Chain 通过链上与链下治理相结合的形式，在实现治理的去中心化的同时保证其有效性。每一个 TAFT 资产持有者都拥有参与去中心化治理 TAF Chain 的权力。

3.1. 选举制度

3.1.1. 节点类型

为了完成节点选举有序进行，按照节点类型进行命名，保障节点各司其职，不同节点类型在不同的节点池，完成不同的工作进而达到协作上的统一，为主链内部业务逻辑的解耦提供了依据，为将来进行分片技术，平滑扩容性能奠定了基础。在 TAF Chain 网络的治理生态中，参与共识的节点分为以下 4 个类型：

委任打包节点

负责区块原始数据的计算及创建，如交易验证、Merkle 树等，该节点需要提供教大的计算能力。其工作在 TAF 共识的 Layer1 层。

委任验证节点

该类型节点负责已经完成原始数据计算的区块在整个链条上的一致性工作。其工作在 TAF 共识的 Layer2 层。

备选委任打包节点

负责在委任打包节点出现问题或受到干扰，无法正常完成区块打包任务时，该类型节点顶替上，以维系整个区块链网络的稳定性。

备选委任验证节点

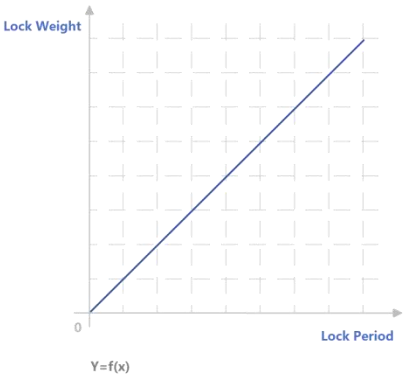
委任验证节点的备选节点。当 TAF 网络中出现“不合格”委任验证节点时，该类型节点将其替换。

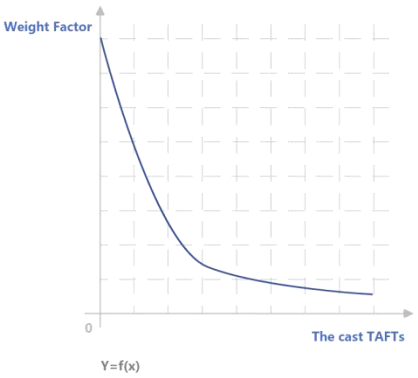
选举类型	选举委员会	中选节点角色	节点池

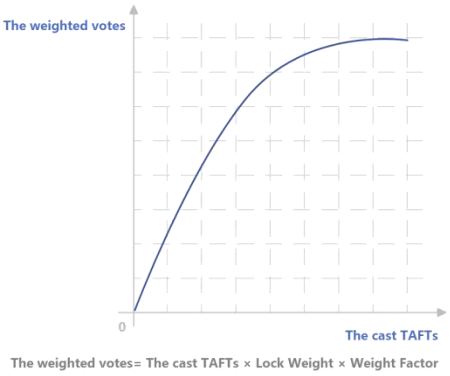
新入网选举	NEC（newnode election committee）	候选节点	候选者池
打包者选举	PEC（packager election committee）	打包节点	打包节点池
验证者选举	VEC（verifier election committee）	验证节点	验证节点池

3.1.2. 节点选举与投票

在 TAF 生态中，权益证明以及委托权益证明通过原生代币 TAFT 兑换选票进行投票来达成，作为选举最重要的介质之一被用做节点的选举投票。TAF Chain 采取的是非线性锁仓权重机制，1 币按照权重获票，1 票 1 投。全体持币用户都可以通过锁定 TAFT 兑换一定数量的选票，获得选票后即可对节点进行投票。为了防止持币大户对整个生态的影响，TAF Chain 设计了投票机制-“非线性锁仓权重机制”。根据不同的投票数量计算不同的锁仓权重以产生不同的得票率。







相比传统投票治理模型，高持币者能轻松参与决策层影响整个生态发展，在 TAF Chain 投票治理中竞选委任打包节点和委任验证者节点的组织或者个人，为了拉开差距必须质押更多 TAFT，获得更多票，锁仓期限更久。长时间持币用户的参与比短期持币用户更重要，锁定期越长，兑票越多。锁定期结束后，选票失效才能兑换回 TAFT。投票人可以随时发起赎回 TAFT 的申请，申请发起后 48 小时（待定）到账，同时支持部分赎回和全部赎回。

举例：假入 A 组织拥有 100 个持币投票，每个投票的锁仓周期为 1 年（假设 1 年的权重是 4），那么 A 组织将获得 100*4=400 的得票。此时，如果 B 组织拥有 400 个持币投票，每个锁仓周期为 1/4 年即 90 天（假设 90

天的权重是 1，但是因为机制的原因，权重系数降为 0.9，那么综合权重为 1*09=0.9），那么 B 组织将获得 400*0.9=360 的得票。所以 TAF Chain 最终发现高持币者的得票相对减少，这就要求高持币者参与竞选需要投入更多的币及进行更多的锁仓期限。那么在关键事件的二次投票上，将明显削弱高持币者优势，甚至毫无优势，那么显而易见的是提高其他持币用户的参与度，赋予更多用户参与选出打包者节点和验证者节点的决策权利。

每一个候选节点获得出块/验证奖励需要对投票者进行分红，按占票数进行比例分红。持币用户给节点投票，固定周期统计出节点获得的总投票数，进而统计出节点的占票率，得票率越高则越大概率入选成为获胜节点，那些给入选节点投票的用户将按用户占票率分红。

节点选举机制的高可用性可以确保整个网络安全和稳定长久运行。通过资质和能力证明的节点具备参与选举资格，同时要求节点质押一定数量的 TAFT 作为保证金，节点保证金适用于所有的选举场景，节点的选举包括新节点入网选举，打包节点选举，验证节点选举，BFT leader 选举。

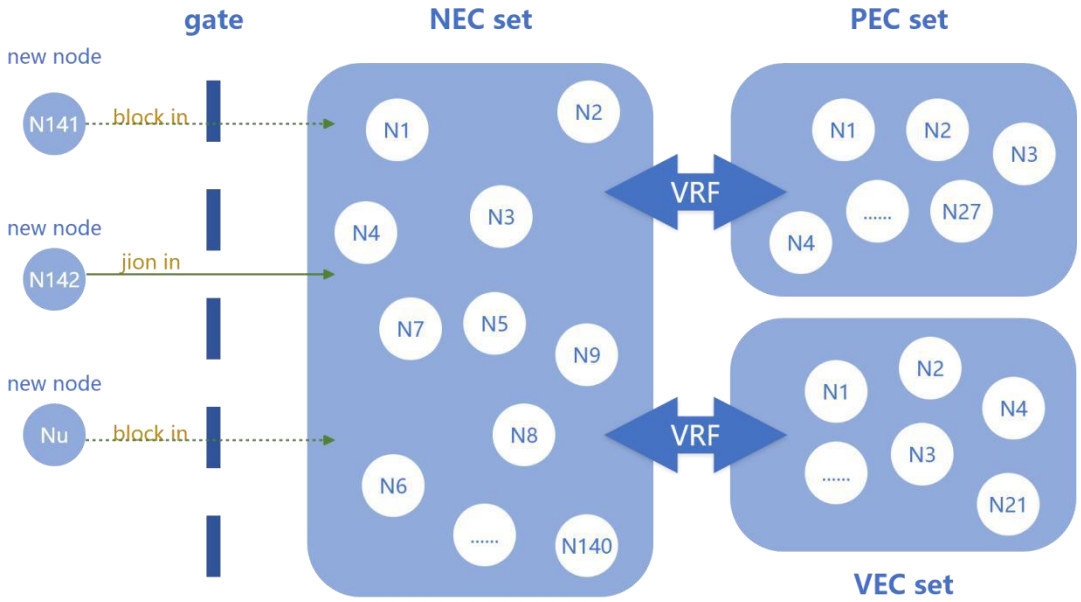
新节点入网时如果保证金小于约定 TAFT 数量，新节点入网将无法选入候选节点池进行选举，只有满足保证金 TAFT 大于要求最小数量节点才能参与选举，同时保证金越高入选在候选节点概率越大。打包节点和验证节点的选举取决于选民的选票和保证金数量，候选池根据选民选票和保证金通过 VRF 进行选举，最终选举出打包节点和验证节点。TAFT 作为保证金，节点可按需抵押保证金，保证金可以持续增加，在抵押时需要验证用户钱包地址是否确定绑定了打包节点和验证节点。在发起赎回保证金时会立即从节点账户中扣除赎回数量，TAFT 到账时间需要等待 48（待定）小时。

节点准入通过质押等方式进入候选池，候选节点通过动态选举产生打包节点和验证节点，同时不同的轮次打包者节点池和验证者节点池的节点有效有序的更新，保障打包节点和验证节点池轮入轮出满足 stake 最大化。TAF Chain 的打包节点和验证节点由全体持币者投票选出，具体规则按照选举业务流程规范。如果打包节点或验证节点在出块或验证周期中作恶，被识别为攻击者抵押 TAFT 将会被没收。例如广播双花交易。

3.1.3. 选举业务规范

启动网络，由基金会节点和社区节点共同发起，新节点入网需要满足基础的入网条件，新节点包括从未入网的

节点以及入网掉线后需要重新进入网络的节点，同时为了保障节点全天候在线，不反复掉线入网，需要抵押一部分资产。所有基金会节点和社区节点历经完成了所需要准备工作任务，确保准备条件满足，启动这些节点，构建初始网络。然后入网的新节点也需要基础算力测试，网络能力测试，提交入网申请后，才有可能进入新节点候选池。由于初始网络已经启动，通过 VRF 选出 leader 收集入网新节点的测试结果广播全网，通过 BFT 共识后出块广播全网，将满足入网标准的节点放到 NEC 选举委员会作为打包者和验证者候选池。



新节点一旦完成入网，就可以获取节点被投票，获取 stake(选票)，某个节点获得的 stake 占全部节点投票的比例为节点占票率，节点占票率越高，入选委员会的概率越高。按照 stake 最低数量标准投出的结果进行 VRF 选出 27（待定）个委任打包者节点组成 PEC 委员会，27 个委任打包者节点组成委任打包节点池；同时选出 21（待定）个验证者节点组成的 VEC 委员会，21 个验证节点组成委任验证节点池。通过在 PEC 委员会的委任打包者节点进行打包的区块按照时间进行排序，投递给 VEC 委员会，最终完成区块验证上链。举例：TAF Chain 社区一共有 2000 个新节点完成入网，从 2000 个节点中选 140 (待定) 个组成包含打包者和验证者的 NEC 选举委员会，此过程 stake 越高通过 VRF 越大概率入选打包节点池和验证节点池。再从 140（待定）个节点的候选池中选 27（待定）个节点组成 PEC 委员会和 21（待定）个节点组成的 VEC 委员会，此过程与节点 stake 排序和保证金相关。VEC 委员会再从 21（待定）个节点中选出 BFT leader 进行验证区块上链。

3.1.4. 节点/leader 更新

由于节点选举和投票的定期更新，为了保障网络安全性和公平性，每轮对 NEC 选举委员会的 1/15（待定）节点进行更新，采用先进先出（待定）的方式。每轮对 PEC 选举委员会和 VEC 选举委员会的 1/5（待定）节点进行更新，采用 VRF 可验证随机。每轮对 VEC 委员会选举 leader 进行更新，时间待定。

3.2. 治理委员会

3.2.1. 链上链下治理

作为一条去中心化的公有链，有效“治理” 是公链长久运行的保障。如何确保区块链在完全自治、离散节点各自为主的环境下消除没有中央机构控制而带来的无序隐患，这是值得深思的议题，TAF Chain 治理委员会一共 7 个席位，TAF Chain 基金会拥有 3 个席位，技术创世团队共拥有 1 个席位，另外 3 个席位由社区投票产生。其中基金会的 3 个席位任期为 3 年，其他均任期为 1 年，到期进行重新投票选出，任何机构与节点均可参选，任期内代表所有持币用户和社区行使表决最高权力。

TAF Chain 治理方案提供了双投一致策略。全体持币用户通过质押一定 TAFT 获得票，1 账户 1 票，用户通过投票联署参与 TAF Chain 公链治理权力。同时通过治理机制，用户也可以发起提案，通过治理委员会投票进行联署，当联署票数过半时，即可触发治理委员会对联署的提案进行投票表决，最终确定提案是否执行，什么区块高度以及条件下通过智能合约自动执行。完成表决后，用户质押的 TAFT 会自动被赎回回退到用户账户中。例如升级共识算法、选举节点数量参数、集群大小、区块大小、交易大小、出块时间、奖励参数等，影响公链运行和生态治理的重要参数的修改权交给全体持币用户进行投票表决确定，通过后根据设置系统智能合约自动执行，最终完成治理。

对于治理委员会决策层 7 个席位的选举，用户拥有选举和被选举的权利同时应尽执行公链治理义务，为公链的发展规划及执行在关键事件决策上起到治理作用。所有链参数更改通过公链治理决定，而非仅局限于部分参数以及创始团队的初始链创世所决定。将管理的治理与技术的治理同时应用到整个 TAF Chain 的治理体系中，从而实现区块链去中心化治理。

3.2.2. 基金会（在全球公售后根据公链发展情况择机成立）

TAF Chain 计划在全球公售后分别在瑞士和阿联酋本地监管机构的支持下设立基金会，作为第三方的中立机构负责公链的社区治理，旨在通过科学、合理、有效的治理机制推动并维系 TAF Chain 的生态建设和健康发展，帮助社区治理的日常事务。

3.3. 通证经济模型

TAFT 是 TAF Chain 主链上发行的原生通证，是公链的核心资产，为生态内构建的基础虚拟加密通证权益证明。公链项目在产品设计、研发上需要大量技术人才引进和社区建设等多方面需求，为了更好更快的落地项目和发展社区生态。TAFT 稀缺性以及未来构建的强应用需求支撑其巨大的生态内流通价值。

TAF Chain 的 TAFT 总量为 30 亿，基金会及其团队持有一定比例的 TAFT，以确保 TAF Chain 在初期发展阶段平滑过度到中期稳定运行，其中节点打包奖励占比总量的 X%，分为 N 年增发完。

出块/验证块（工作量）时间：T 秒
每个工作量奖励：n TAFT
所有节点每日获得奖励总是：S = n*(60/T)*60*24
投票分红比例：K%
所有节点分红：S*(1-K%)
所有投票人分红：S*K%
投票年化利率：(S*K%)/所有节点得票数总和 * 天数 (年)

3.3.1. 出块和验证奖励

每生产一个区块，那么系统都会奖励区块打包者一定数额的 TAFT，这部分的 TAFT 从尚未对外发行的剩余数量按照一定比例规则进行发行，同理验证块的验证节点也将获得一定数量的 TAFT 奖励。每年固定从基金会账户拿出固定数额 TAFT，进入奖励池，出块和验证块奖励从系统的奖励池进行奖励，按照出块数/验证块数占全网比例进行分配。

3.3.2. 奖励发放

链上完成奖励汇总、结算、发放。按照打包节点出块数占比把出块奖励发放到节点所在的“投票合约”地址，“投票合约”按照分红比例将 TAFT 奖励发放到“投票管理合约”账户地址，“投票管理合约”按照投票人按占票权重比将 TAFT 奖励定时发放到投票人账户和节点账户。同理按照验证节点验证区块的数量占比进行奖励发放。

3.3.3. 交易免手续费

在 TAF Chain 上进行转账本身是完全免费的，仅开发者在调用合约等需要占用系统资源时需要持有代币冻结和支付。

4. 商业级公链

为商业级用户量身打造，提供公链基础设施支持、开发套件支持、链上运行环境支持。拥有可以落地商业应用支撑海量用户的高并发性能，不会因为网络堵塞等问题影响到商业用户的正常链上行为。同时支持多种主流的隐私保护策略，商业级用户可根据特殊的行业进行链上数据隐私保护，在满足数据上链后不可篡改等特性的同时，解决商业用户数据泄密隐患。支撑商业用户应用落地海量数据的分布式存储。该项目将成为全球首条商业级公链，商业用户需要支付一定的手续费后，可稳定、高效、可靠的使用链上资源。

4.1. 基础设施

4.1.1. 模块组件化

TAF Chain 在开发初期就采用了组件化的开发模式，有利于快速开发出最小可运行版本，解决了区块链公链项目过度复杂导致组件之间高耦合的问题，使开发和维护成本大幅降低。同时组件化可以快速迭代版本，在添加修改组件的时候也不需要担心影响其他组件，还可以解决业务模块划分不清晰。 TAF Chain 不单单作为一条链，而且还会将用到的相关组件作为基础设施为相关领域提供组件化服务。改进的共识机制、丰富的智能合约、高效的分布式存储网络、P2P 网络、跨链组件等都可以作为单独的应用来服务。

4.1.2. 高性能分布式开发运行平台

TAF Chain 提供了高性能的开发运行平台，使开发更加高效、成熟，运行更加快速。

(1) 采用了分布式的开发运行平台，各个服务之间独立开发运行，互不影响，并且各个服务又具备高扩展性和可移

植性；

(2) 微内核设计，不同于现在主流发行的 Linux 版本，TAF Chain 开发运行平台对 Linux 内核进行了优化，提供操作系统核心功能的精简版本，设计在很小的内存空间内，增加了可移植性，提供了模块化设计，各个模块按需加载。微内核具有很好的扩展性，并可简化应用程序开发，用户只运行需要的服务，这有利于减少磁盘空间和存储器的需求；

(3) 微服务化的开发，每个微服务都很小，这样能聚焦一个指定的业务功能或业务需求。所有服务是松耦合的，平台上的各种服务，无论是在开发阶段或部署阶段都是独立的。由于服务的独立性，微服务能使用不同的语言开发。而且微服务允许开发者利用融合最新技术，提高本服务的性能和稳定性。另外易于开发人员的理解，便于开发人员的加入，开发人员只要专注于自身的业务逻辑就可以为整个项目的开发带来很高的价值。

(4) 任务采用了无阻塞、纯异步调度，可以立即给调用方返回初步的结果，在执行的过程中，可以释放占用的线程等资源，避免阻塞，等到结果产生再重新获取线程处理，充分利用操作系统资源。并且 TAF Chain 团队在使用异步调度技术的同时，解决了异步调度中的“回调地狱”的问题。

(5) 上层应用开发无需关注平台是如何运转的，只需根据平台开放的接口，专注于自己的业务逻辑开发即可，如果上层应用出问题，整个区块链网络并不会受影响，并且上层应用的性能也不会影响区块链网络，上层应用也可以通过对自己的应用系统的优化，提高整个系统的运行性能；

(6) 平台内部内置了集群功能，具有很强的可伸缩性。随着需求和负荷的增长，可以通过配置向集群系统添加更多的服务器。在这样的配置中，可以有多台服务器执行相同的应用和数据操作。另外还具备高可用性，在不需要操作者干预的情况下，防止系统发生故障或从故障中自动恢复的能力。通过把故障服务器上的应用程序转移到备份服务器上运行，集群系统能够把正常业务系统运行时间提高到 99.999%，大大减少服务器和应用程序的停机时间。并且具有高可管理性，系统管理员可以从远程管理一个、甚至一组集群，就好像在单机系统中一样。

(7) 分布式开发运行环境上的各项应用，都是独立开发，高内聚，低耦合，各个应用之间的问题不会相互影响，可以独自优化，在各自调优的同时，兼顾做到整个平台的调优开发。另外分布式的开发运行平台，各个服务可以跨平台、跨数据库使用。每个服务都专注于自身的服务细节，对自身服务性能的提升，那么在整个平台运行各

项服务的时候，整体性能就会提升。

4.1.3. API 和 SDK

系统将提供一整套完善的 API 及 SDK，用于身份创建、Token 创建、智能合约、跨链交互、可信数据、可信存储等场景进行调用。SDK 可支持主流编程开发语言，如 Golang，C++，js，Python 等主流开发编程语言。

4.1.4. 区块链浏览器

TAF Chain 将搭建与主链配合工作的区块链浏览器，以提供各类区块链信息的检索和使用。

4.1.5. 钱包

我们将配套与主链配合工作的钱包软件，用于链上账户及资产管理，并向第三方开放 API 及文档。

4.2. 商业性能优势

区块链自问世以来就被形容成一项无所不能的科技，被看好能影响各行各业，甚至重塑生产关系。然而区块链自身，却存在着著称为“不可能三角”的技术瓶颈，至今仍远远无法施展它的潜能。在区块链 1.0 时代的 BTC 交易系统，区块大小和出块时间制约着性能（扩展性），而到了区块链 2.0 以 ETH 为代表支持通用智能合约的区块链系统，除了区块大小和出块时间之外，串行计算方式依然也制约整体性能，另外以 PoW 共识机制较慢的出块时间来降低分叉概率以换取安全的做法也限制了性能。性能低下是目前区块链行业里亟需解决的重大问题。影响区块链性能的因素众多，如共识机制、P2P 网络通讯效率、存储效率、出块时间、区块大小、事务执行速度和事务大小等。

面对区块链的性能问题，目前普遍的做法就是将更多的计算从区块链网络中分离出来，采取 On/Off Chain 的方式进行计算和数据分离，只将最主要的关键数据上链，减少区块链网络的计算以及存储。但是，将一些操作从链上转移到链下操作，链下的操作也面临的一系列的信任问题、稳定性问题等。

从扩展区块大小或者减少出块时间来提高性能和吞吐量，是在单链结构中所采取的通用方式，比如比特币分叉出来 BCH，BCD，BSV 等都采取这样的方式进行扩展。从 PoW 到 PoS，这次改进解除了能耗高的要求，交易数据确认速度和系统吞吐主要依赖的是网络通信能力。PoS 主要时间花在投票过程，而与区块大小或出块时间关系不大，这样增加区块大小和缩短出块时间变得更有空间。当然这些好处也带来了潜在的安全性风险。PoS 共识机制下，验证者始终诚实可信变得至关重要。

另外一种通用方案是有向无环图 DAG，解决区块链可扩展性问题的一种可行而且极具前景的去中心化技术。DAG 的组成单元是交易，每个单元记录单个用户交易，交易单元组成的网络，可以异步并发写入交易，类似开启多核多线程并行处理。在区块链网络中可以完成并发写入，并行意味着交易数量的倍增。

目前新兴的扩容方案是采用 sharding 分片技术，将全网的节点进行分组，每一组同时处理一个分解后的任务，这样就从原先单一节点处理全网的所有任务变成了多组节点同时并行处理。通过改变区块链网络验证的方式来增加吞吐量，关键策略是把单一共识主体的流程分离成多个子步骤串行，针对不同步骤的实现机制优化，同时不同共识主体并行执行，降低分叉回滚的可能性。分片技术独特之处在于它可以大规模的进行水平扩容，网络的吞吐量随着网络的扩展而增加。

TAF Chain 通过最先进的 P2P 双层分片网络消息通讯，以及自研并行存储 IO 系统，和高性能改进的 DPoS2.0+BFT 共识算法作为一个整体机制来解决区块链性能问题。预计网络上线时将达到 20,000TPS，随着公链四个阶段的不断优化演进后，最终交易性能会突破 100,000TPS。

4.3. 隐私保护和权限

支持多种主流的隐私保护及安全机制，多方位多渠道构建安全体系，让企业及个人用户在实际应用中兼顾安全

和隐私，包含但不限于以下：

(1) 支持 ECC 公私钥对及国密算法。

(2) 引入分层加解密技术，降低秘钥被泄露和破解的可能性。

(3) 采用高度的散列和摘要算法来保证用户地址的合法性。

(4) 采用安全多方计算、零知识证明保证数据的机密性。

(5) 运用环签名、群签名机制保证身份隐私。

4.4. 商业应用分布式存储

对于商业用户来说，数据安全性和易访问性的权衡是一个难题。商业活动产生的海量数据（文本、图片、音频、视频等），存储在链上会提供易访问性，但会大大增加数据暴露的风险。同时链上存储需要巨大的成本，对于区块链来说不现实。基于传统的中心化存储 安全性、隐私性有保证，但是数据不易访问。

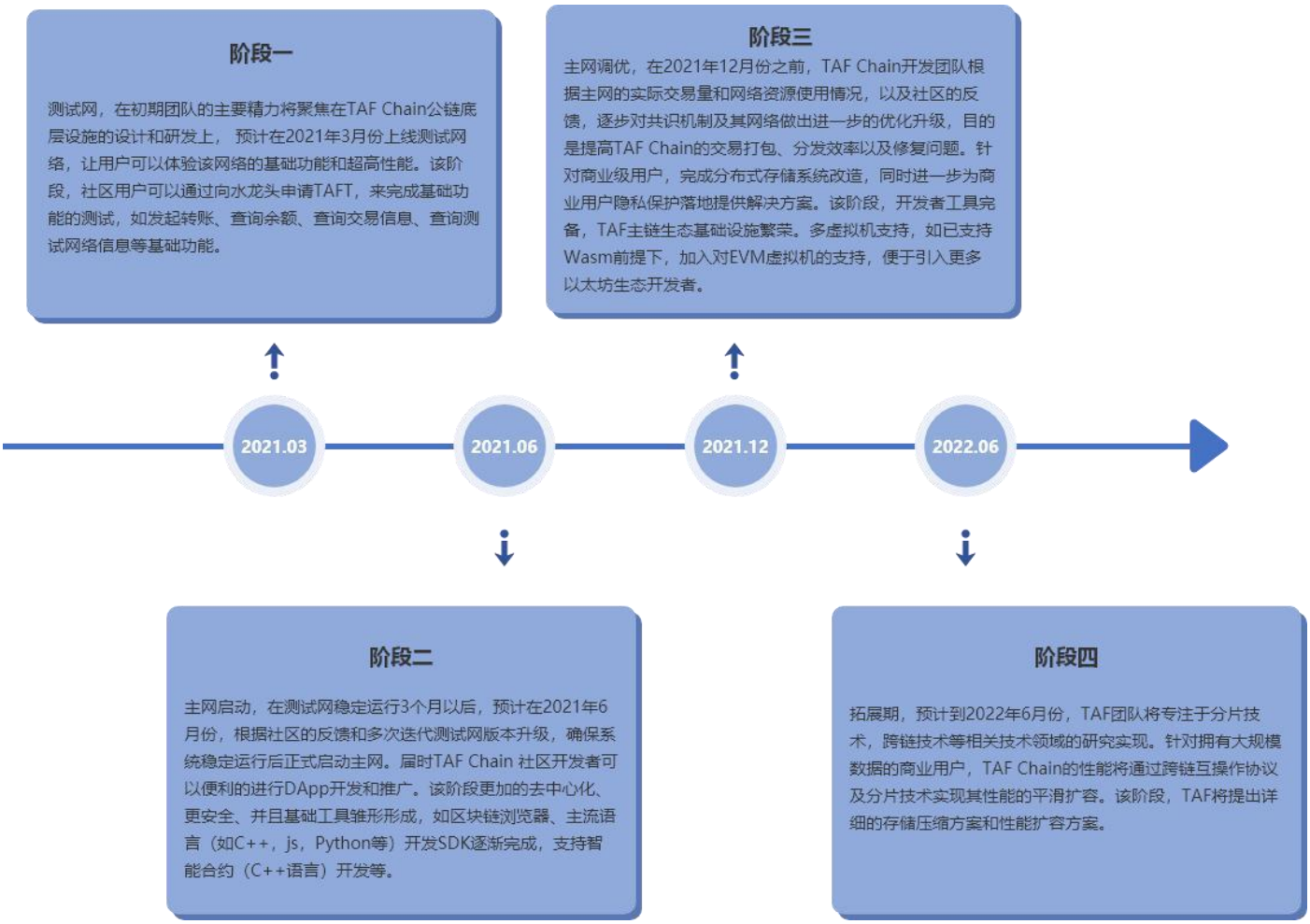
TAF 为商业级用户提供文件存储，基于 gossip 协议，以合约的形式实现。提供了一个 p2p 的网络用于文件的发现和分享。其特点是文件名和文件内容强关联，协议的内容寻址体系结构能够确保数据的完整性和可验证性的。

用户在本地或者商业合作方上部署存储节点（节点集），生成文件的链接，并对该链接进行加密（密钥不同于用户的密钥），随后打包成交易并签名，调用合约保存数据。这样文件的索引信息就以加密的形式存储在链上。当需要分享给合作方时，用户的存储节点需要在线，并授权相应的权限给合作方访问合约，合作方会通过 gossip 协议构成的 p2p 网络复制相应的文件，完成文件的分享。

由于数据是存储在本地节点，并且链上存储的是加密过的文件链接，数据的安全性得到保证。对于私密性和安全性需要更高的要求，可以以加密的形式存储文件内容在本地节点。

5. TAF Chain 的技术路线图

TAF Chain 项目的设计初衷是建立高性能的商业级公链，其既有公链的安全性、公平性、不可篡改性、隐私保护等特性。同时，针对大规模商业场景目前很难落地的事实。TAF 团队计划在其网络内引入商业应用所必须的组件，如二层的分布式存储网络，数据隐私权限等。形成可以应用于大规模商业场景的通用的区块链底层基础设施。



TAF Chain 的四个阶段：

阶段一

测试网，在初期团队的主要精力将聚焦在 TAF Chain 公链底层设施的设计和研发上， 预计在 2021 年 3 月份上线测试网络，让用户可以体验该网络的基础功能和超高性能。该阶段，社区用户可以通过向水龙头申请 TAFT，来完成基础功能的测试，如发起转账、查询余额、查询交易信息、查询测试网络信息等基础功能。

在该阶段，TAF 团队预计完成以下相关项目。

1. 预计会在测试网上线时，完成水龙头（TAFFaucet1.0）网站的开发并上线，普通用户可以通过该网站，获

取测试所需的 TAFT。

2. 预计在该阶段区块链浏览器（TAFScan1.0）第一个版本完成上线，其中包含常用区块链查询信息，如查询区块信息、查询交易信息、数据浏览（如最新区块高度、交易总数、账户总数、合约总数、已流通 TAFT 总数）等。

3. 预计在该阶段会完成 Taf 钱包（UvToken1.0）的开发，用户使用该钱包可创建账户地址、导出和导入私钥、查询余额、发起交易、查询交易等。

阶段二

主网启动，在测试网稳定运行 3 个月以后，预计在 2021 年 6 月份，根据社区的反馈和多次迭代测试网版本升级，确保系统稳定运行后正式启动主网。届时 TAF Chain 社区开发者可以便利的进行 DApp 开发和推广。该阶段更加的去中心化、更安全、并且基础工具雏形形成，如区块链浏览器、主流语言（如 C++，js，Python 等）开发 SDK 逐渐完成，支持智能合约（C++语言）开发等。

在该阶段，TAF 团队预计完成以下相关项目。

1. 预计在该阶段会陆续上线开发者中心，该网站包含 TAF 链的常用基础操作向导，SDK 调用帮助手册，RPC 接口等相关操作文档。

2. TAF 团队在该阶段会定期更新 TAF 官方网站，使用户了解到 TAF 项目的最新进展。

3. 预计同步上线区块链浏览器（TAFScan2.0）版本，该版本可支持 TAF 链相关高级操作的展示，如投票情况，参与投票用户数量、投票票数、投票参与比例、投票的进度等。另外，该官方 TAF 链浏览器也会支持得票情况查看、分红比例查询、奖金池情况等。

4. 预计该阶段会推出 UvToken2.0 版本，该版本新增相关高级功能，如抵押、赎回、投票，申请候选人、得票率等，以及相关链上治理功能，如发起提案、提案表决等。

阶段三

主网调优，在 2021 年 12 月份之前，TAF Chain 开发团队根据主网的实际交易量和网络资源使用情况，以及社区的反馈，逐步对共识机制及其网络做出进一步的优化升级，目的是提高 TAF Chain 的交易打包、分发效率以及修复问题。针对商业级用户，完成分布式存储系统改造，同时进一步为商业用户隐私保护落地提供解决方案。该阶

段，开发者工具完备，TAF 主链生态基础设施繁荣。

在该阶段，TAF 团队预计完成以下相关项目。

1. 多虚拟机支持，加入对 EVM 虚拟机的支持，便于引入更多 Solidity 生态开发者。

2. 预计在该阶段完成二层分布式存储网络创建，使其进入商用阶段。

3. 在该阶段会引入更多隐私保护算法，如零知识证明、环签名等，作为可选项防止用户敏感信息泄露。

4. 不断完善现有工具集，如合约机、编译器、区块链浏览器、钱包等及相关二次开发套件。

5. 预计会在开发者中心增加用户隐私、分布式存储网络、合约虚拟机等相关内容，构建完整的开发者社区。

阶段四

拓展期，预计到 2022 年 6 月份，TAF 团队将专注于分片技术，跨链技术等相关技术领域的研究实现。针对拥有大规模数据的商业用户，TAF Chain 的性能将通过跨链互操作协议及分片技术实现其性能的平滑扩容。该阶段，TAF 将提出详细的存储压缩方案和性能扩容方案。

在该阶段，TAF 团队的工作重心在以下相关项目。

1. 不断完善 TAF 分片技术方案，实现第一条分片 TAF 测试网络。到时，不同的业务场景可通过分配到不同网络分片的形式，实现性能扩容。

2. 不断完善 TAF 可信跨链方案，落地 TAF 跨链技术。到时，可打通不同网络分片之间数据互通。解决网络孤立性，使得不同网络分片协同工作。

3. 不断完善 TAF 存储技术，进一步提高数据压缩比例，以减少网络数据传输量。该阶段，TAF 公链可兼容主流的存储系统，如裸设备、Linux 文件系统、HDFS、第三方数据库等。

6. TAFChain 商业级公链与主流公链对比分析

区块链拥有众多优势，如可信及可靠网络，去中心化、不去篡改、变更历史可追溯等。但是，其从诞生到现在经历十年依然无法大规模商业化应用。通常只能在一些业务逻辑及其简单、数据量非常小的场景中使用。究其原因是大规模的商业化场景对区块链网络有较为苛刻的要求，如高性能、数据隐私等问题。下表列出了常见的区块链平台和 TAF Chain 在主要指标上的比对情况。

平台名称	合约语言	Oracle	共识机制	性能	出块时间	商业链	隐私保护
Bitcoin	不支持	不支持		6tps	10 分钟	不支持	不支持
Ethereum	Solidity, vyper	不支持	POW	40tps	15 秒	不支持	不支持
EOS	C/C++	不支持	DPOS	3000tps	0.5 秒	不支持	不支持
TRON	Solidity	不支持	DPOS	2000tps	3 秒	不支持	零知识匿名交易
NEO	C#, Java, Python, GO, JavaScript	不支持	DBFT	1000tps	15 秒	不支持	不支持
Zcash	不支持	不支持	POW	25tps	150 秒	不支持	零知识
Monero	不支持	不支持	POW	1700tps	120 秒	不支持	环签名
Hyperledger Fabric	Golang, JavaScript	不支持	Kafka, raft	2500tps	可配置	不支持	不支持
TAFChain	C/C++, JavaScript, Golang， Python, Solidity	内置预言机	DPOS2.0	20,000tps 理论可达到 100,000tps	0.5 秒	为商业应用提供稳定性能、及隐私支持	零知识 环签名 商业应用可选

性能方面：TAFChain采用最先进的消息通讯底层，自研的并行存储IO系统，和高性能的共识算法。预计主网首期上线时将达到20,000tps，经过后期逐步优化后，预计交易性能会突破100,000tps。从上表可以看出，目前市值较高的主流区块链平台，交易性能最高者，在2000到3000之间。通常来说，金融系统的交易吞吐量至少是万次 / 秒的量级。而微信钱包在最高峰时候能处理20万tps，支付宝在双11的时候到了54.4万tps。很容易看出，目前主流公链项目交易性能较低，这是影响其大规模商业应用落地的重要因素。

智能合约：TAF Chain首先支持开发者采用C++语言进行合约开发，同时也支持其他主流的开发语言进行合约开发。根据上面图表可以发现，有些公链不支持智能合约编写（如Bitcoin、Zcash、Monero等），有些链虽然支持了图灵完备的合约语言（如Ethereum、TRON、EOS等），但是其只支持单一的合约开发语言。对

于商业用户来说一方面学习成本过高，另外由于对其相关生态不熟悉，导致合约编写各种漏洞，引入安全隐患。例如，2018年12月27日，以太坊智能合约Fountain(FNT)出现整数溢出漏洞，导致其币价一夜归零。为了简化开发者编写智能合约的难度，TAFChain将陆续支持C/C++, JavaScript, Golang，Python，Solidity等主流编程语言编写智能合约。TAF Chain研发团队会在网络稳定运行后的第一时间推出EVM虚拟机兼容，使得TAF用户可以编写Solidity智能合约，方便未来的各种Solidity生态应用迁移到TAF网络。

预言机：由于区块链是确定性的、封闭的系统环境，目前的主流区块链项目都只能获取到链内的数据，区块链与现实世界是割裂的。TAFChain团队会陆续推出链上合约访问外部资源的内建预言机。完成区块链与现实世界的数据互通。从上图表可发现，目前主流区块链平台都不支持预言机。如目前火爆的DeFi领域，由于合约无法获取外部数据源，导致链上的去中心化DeFi项目受限于链内数据源，只能应用于当前链的生态。该属性对于定位于商业级公链的TAFChain来说至关重要，其智能合约和去中心化应用（DAPP）对外界各种数据拥有交互需求。可以说一切需要链上与链下进行数据交互的DApp都需要预言机，如去中心化交易所项目需要通过外部接口获取到实时的币价信息等。举例来说，比如EOS上面的掷色子游戏或以太坊上面的FOMO3D游戏，因为他们没有满足智能合约/Dapp场景对安全伪随机数的要求，因为随机即不可预测。因此这类DAPP因随机数问题而遭受黑客的攻击。

共识机制：相对于其他主流公链，TAFChain摒弃了耗费资源多且效率低下的POW共识机制，采用开发团队自研的DPoS2.0共识算法。另外，目前主流的DPoS共识机制，首先在节点选举上，选择验证人的方式简单粗暴的参考了目前的选举制度，得票率最高者既为获胜者。这样带来了过于集中化的问题，项目后期资产逐渐的集中，最终导致代币的流动性越来越小，形成穷者越穷，富者越富的局面。另外，简单粗暴的选举策略，非常的容易被恶意攻击者预先推算出选举结果。在TAF网络中，引入VRF后，选举结果具有一定的随机性，攻击者无法预先推测出选举的最终结果，大大提高了整个网络的安全性。同时在一定程度上解决了资产过度集中的问题。

商业链：TAFChain 对商业级用户提供分布式存储网络。该网络提供了一个 P2P 的文件存储、发现和分享。其协议的内容寻址体系结构能够确保数据的完整性和可验证性。针对商业用户隐私性需求，用户可以把原始数据加密后提交到该分布式存储网络中。通过 TAF 智能合约分享给商业合作方后，后者通过 TAF 文件的索引信息可拥有该

数据的完整拷贝及解密方式。由于目前主流区块链系统无法满足商业用户的隐私需求，使得大规模的商业应用无法很好的应用于其平台。另外，TAF 研发团队会继续专注于高性能区块链网络，为商业用户提供多种隐私保护策略，使 TAF 生态在满足数据上链后不可篡改等特性的同时，彻底解决商业用户数据泄密隐患。