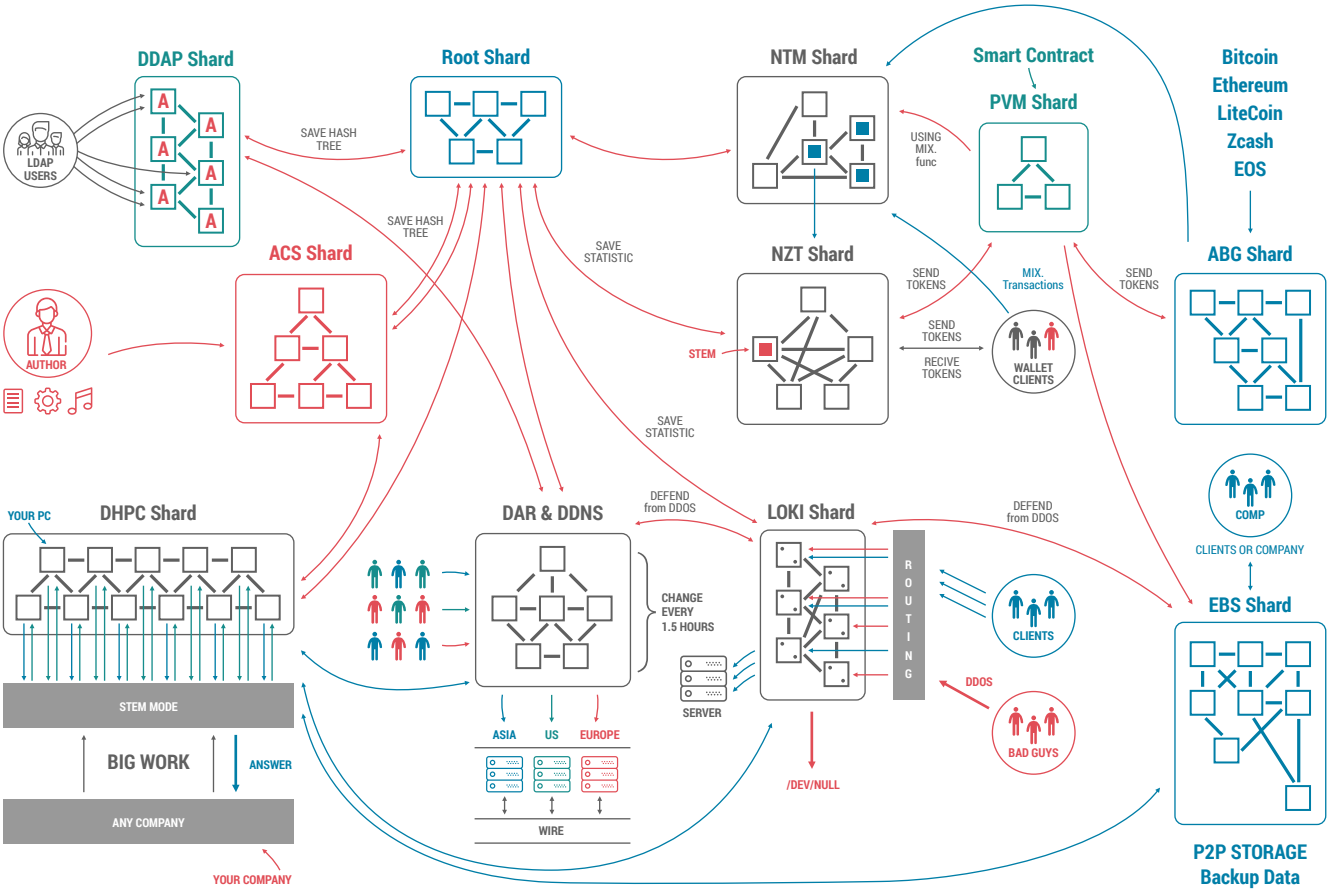

Noosphere
技术百度书

目录:

1 摘要

NOOSPHERE ECOSYSTEM



智能圈是一种分散式区块链云平台，是借助服务导向的分割技术实现的一种分布式网络服务和计算系统的新型组成架构。智能圈的每个分片都是可被用户售卖和使用的独立区块链的服务。所有的分片共同组成了一个计算生态系统，该系统具备以下特点其中包括：可扩展性、高速性、分散性、跨服务兼容性和容错性。智能圈被视作首个既可新建各种复杂程度的网络服务和计算系统，亦可将现有网络服务和计算系统纳入自身管理的区块链平台。

请注意：本白皮书中提到的加密代币是指采用NOOSPHERE软件中已启动的区块链上的加密代币。并没有涉及到与NOOSPHERE代币分布所相关的，且在以太坊区块链上分布的ERC - 20兼容代币。

2 免责声明

本Noosphere技术白皮书第4版仅供参考。Noosphere Foundation不保证本白皮书或其得出结论的准确性，且“按原样”提供本白皮书。Noosphere Foundation不做任何明示、默示、法定或其他陈述和保证，包括但不限于：（I）适销性、特定用途适用性、适用性、所有权或非侵权性的保证；（ii）本白皮书的内容没有错误；（iii）此类内容不会侵犯第三方权利。Noosphere Foundation及其附属机构对因使用、引用或依赖本白皮书或本白皮书所包含的任何内容而产生的任何类型的损害不负任何责任，即使被告知有可能会发生此类损害。在任何情况下，Noosphere Foundation或其附属机构均不对任何个人或实体因其所使用、引用或信赖的本白皮书或其中任何内容而遭受的任何形式的损害、损失、债务、成本或开支（无论是直接、必然、赔偿、偶然、实际、惩戒性、惩罚性或特殊）承担任何责任，包括但不局限于任何业务损失、收入、利润、数据、使用、商誉或其他无形损失。

3 区块链平台的实际要求

不论其他信息技术领域如何，当前区块链技术在不断发展。区块链技术的到来开辟了开发和完善现有数据存储和传输方法的新路径。然而，伴随着发展，对商人、政府以及全球人士为代表的终端用户提出了新的要求。从长远角度考虑，当今不能满足全新需求的平台会大大被削减其可信度。

3.1 定向服务的体系架构

区块链具有众多利于经营的优势。主要体现为强大的计算功能、安全可靠、可容错以及技术简单清晰的方面，但是现有的区块链云平台会提供超过其自身架构的私人商业逻辑实现机制。它们的功能性受支付功能和智能合约的限制，加之这两者会导致产生微乎其微的作用。该因素明显地限制着行业的发展——我们无法将现有的区块链云平台用作创建新服务和改进现有服务的基础。因此需要一种新型的定向服务架构。未来的系统应该能够提供可实现服务建构的API，这类服务能够超越单一计算网络发挥作用并具备跨服务数据交换的功能。

3.2 有效可扩展性

区块链网络内部的用户数量及数据流强度与日俱增。大众平台的工作能力无法满足日益增长的需求。每天都会诞生新的想法以及对其进行调试的算法——将会增大区块容量、改写共识算法以及使用侧链解决方案等。由于该原因是显而易见的，上述方法仅具有短暂的效果。设计新平台时应考虑与今日相比之下，用户数量和数据流将会扩大数十倍。实现该目标的唯一方法是高效扩容。与中心化系统不同，区块链能够依靠自身的去中心化而轻松达到此目的。分割输入数据流可使系统能够平均高效地为上万直至上千万的用户服务 并在大量在分片中平行处理数据。

3.3 定向业务的执行

比特币平台的整体哈希率达到4ekzahash/秒。仅有为数不多的超级计算机才能够达到如此的工作效率。然而所有的计算机仅仅是用于维持PoW老旧共识算法的运行。据统计，90%以上的公司倾向使用虚拟云技术代替购买个人计算机。使用区块链网络中利于计算的资源，包括利于实现定向服务架构的资源能够吸引更多的意向用户，此外还可将区块链技术的应用领域拓宽数十倍。

3.4 安全性和活跃度

去中心化系统对于安全性、自我修复性和更新进程有特殊的要求。没有数据的平台只可依靠分叉而改变，这还会给用户带来更多问题。还应注意到，业务中是无法使用分叉的。应当研发一种能够确保系统在无分叉和无临界延迟的情况下运行的特殊方式。如果没有这种机制，系统将不会拥有竞争力和使用吸引力。

4 定向服务的分片

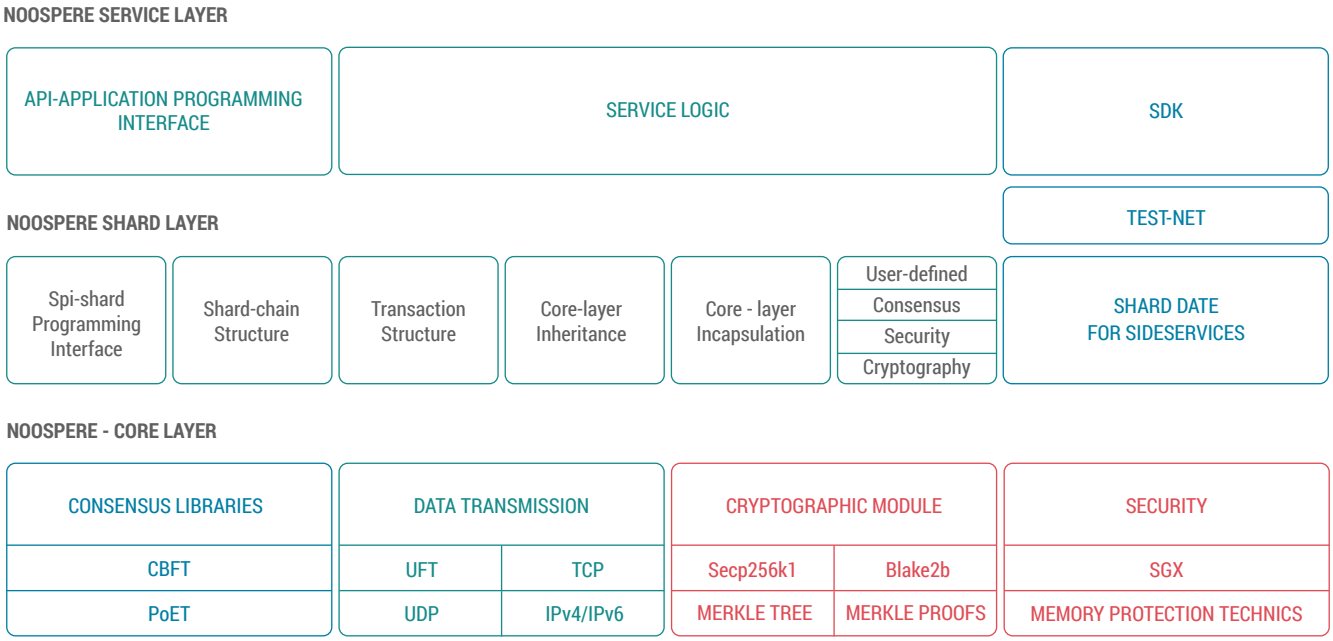
Adam Efe Gence首次在 的对于区块链的服务导向的分割研究中提出定向分片服务技术的构想。将分片用作服务器是该构想的最大与众不同之处。每个分片都是一个独立的服务器，能够执行既定的功能并且可与系统的其它分片（或其他文本和服务）交换信息。智能圈与其他分片使用系统的主要区别在于既可支持转让交易和履行智能合约的标准功能，还可支持所有能够在区块链技术中实现的服务或者能够将区块链技术用作监控模块的服务。换言之，它不仅仅是传统分片技术理念的复制替代品，而是智能圈是组建去中心化网络服务架构的新型方法。DNS、DAR、LDAP、人工神经网络、路由选择、代理、分布式计算和负载分配属于该类服务器，它们验证了中心、直接支付功能以及商业的定向服务，后者包含自定义交易规格以及可实现不具备私有计算能力的公司和集团商业逻辑的区块结构。

对于该类服务而言，可将分片随时补入系统进而扩大整个系统的功能性。此外，定向服务分片技术能够轻松地实现任意侧链也可将任意现有的侧链用作分片。此种情况下，专业服务分片仅应于确保数据的路径选择功能，并还可以确保数据的可靠性。

在智慧圈平台，分片分为两种——静态分片和动态分片。系统定义的分片称为静态分片，其负责维持系统的工作能力和可扩大内核的功能。用户定义的分片称为动态分片，所有用户都可创建动态分片以实现个人的逻辑。此外，当系统功能和社区的正面决策达到临界状态时，所有的动态分片都可变为静态分片无需考虑作为一组维持社区运行的独立物理服务器的每个单独的分片。许多分片会有单一的虚拟架构，为它们受管理本质或监控本质的约束而实现自身的高负荷。总之，静态分片保障垂直可扩展性，动态分片保障水平可扩展性。

智慧圈内核没有可处理智能合约以及实现交易加密和负荷平衡的内置机制，因为上述都是服务器，应当分出独立的分片。可见，智慧圈具备了其他平台没有的优势。系统的架构十分灵活，可在任何时刻改变功能原理，而且可以改变和新建分片。此外，智慧圈并无限制，每个用户都可以随意使用自己的智能合约类型还有自己的虚拟服务器去处理智能合约，而且还能够创建自己的交易混合器以及扩大整个系统功能性的其他服务，这都是独立的分片。

5 Noosphere 剖析



5.1 设计原则

5.1.1 KISS – 保持简单易懂

如果保持简单易懂的话，系统可更好的运行。这不仅会降低入门门槛，还可轻松进行改写和升级。系统应当透明且易于掌握，不应繁琐陈旧令用户和设计人员望而却步。

5.1.2 成为社区的一部分

带有公开源代码的系统设计人员社区是推动系统持续良性发展的绝佳因素。因理念和目标一致而聚在一起的人们是在进步道路上的最强动力。如充分给予了这些人包括财务方面的支持的话，他们的创意将能够建立起可与封闭商业架构一较高下的真正基础性平台。

5.1.3 灵活优于刻板

打造每天都可高效发展且极具竞争性系统的方法之一是将内置功能数量降至到最低，依靠可轻易从系统安装/卸载的灵活模块提供实现新功能的机制。

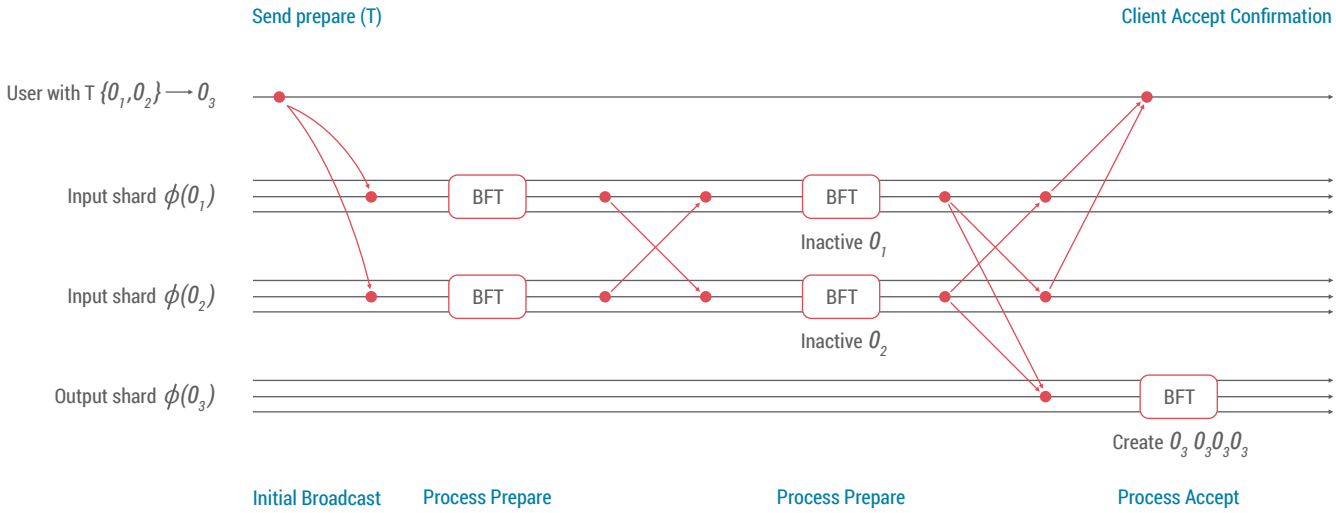
5.1.4 了解您的用户需求

只有用户了解当今需要何种功能以及明日的需求时，系统才会发展唯一正确的矢量，其矢量就是与用户的对话。如果没有这种交流，系统就会冒着偏离道路的危险，可能会成为不被需要的无用之物。

5.1.5 安全性

对于用户而言，最重要的迫切需求之一是个人数据的绝对安全性。尽管这一忧虑已经在区块链哲学中得到了落实，但许多开发出的平台没有给予应有的关注，而是沿着错误道路继续前行，简单复制过往项目中的成分。我们有经验丰富的开发人员、工程师、数学家和密码译员团队，所以能够开发出完全满足该需求的系统。

5.2 分片



智能圈平台架构的基础是分片技术。分片技术的标准使用方法为分别处理交易，按照某种特征在服务分片之间对交易进行分类。相较于将节点划分为系统间区块链的唯一副本而言，这可显著提高系统的工作能力和运行速度。在智慧圈平台上的每一个分片都是一个完全能够独立运行的微型区块链，它的运行不需要时刻与其他分片保持关联。因此，系统的主要区块链就是分片。可见，智慧圈的基本组成单位即为分片。每个分片的架构都是唯一的，只是它们履行的功能不同。

5.2.1 分片技术

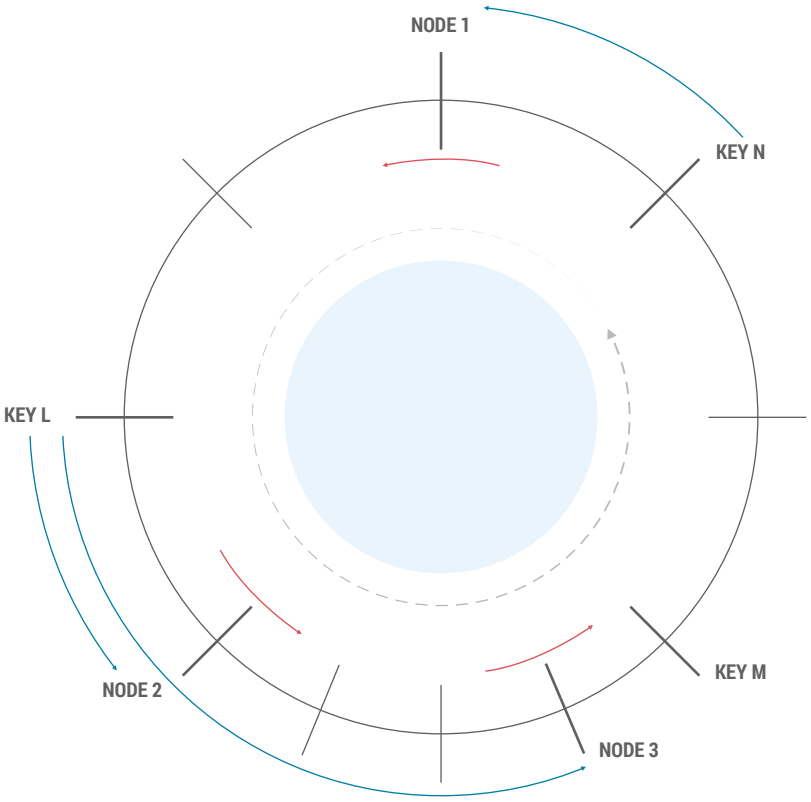
分片技术是水平分割数据的一种方法。分片技术过程本身可分为三部分:

- 选择分片技术的功能;
- 重新分片-数据再分割过程;
- 数据路径选择（确定数据的物理位置）。

数据路径选择（确定数据的物理位置）。$f(x_1, x_2, x_3,..., x_n) = y$ ，类型函数，式中 x_n 式中是分片技术的密钥，y是分片。正确选择分片技术的密钥对分片效果有直接影响。通常这些密钥由运行中用到的节点和用户标识符数量组成，数据也在此列之中。分片技术的函数 f 本身是一个特殊的哈希算法。这可能是一个相容哈希算法或者 HRW (Highest Random Weight) hashing。被选择函数的效果能够在数据再分割时体现，当 K 节点中的n从结构中脱离，数据应当在剩下的在线节点中再次分割，网络负荷急剧增加，继而形成新的分片来分配负荷。现有的区块链平台分片技术忽略了该问题的重要性，认为网络负荷是固定的，一开始分片架构被选择了那么在今后将不会被更改，因此仅仅只能选择哈希算法。相容哈希算法是一种特殊类型的哈希算法，特点在于当哈希表改变时，只有密钥的 $\frac{K}{n}$ 平均值改变，式中的K为密钥数，n 为位数。与此相反，在绝大多数传统哈希表中，位数的改变几乎会引起所有密钥的改变。使用相容哈希算法能够使我们避免在改变一组活跃节点（添加/去除）时重新对密钥进行哈希式算法。相反，这组进行哈希算法的密钥和数据将被置于闭环中，无需再次进行哈希算法，加入新节点就可动态分配负荷。

HRW hashing是一个类似的函数，但是它的功能性更强大，相容哈希算法在特定情况下可视作一种个别情况。HRW哈希算法会使用统一的哈希函数分配闭环中的几组密钥。不同于相容哈希算法，HRW不要求事先计算或者保存密钥。对象 O_i 取节点 n 中的值计 $N_1,...,N_n$ 算 n 哈希值 $h(O_i, N_j)$ 并选择令哈希函数取最大值的节点 N_k。如果加入新的节点 N_{n+1}，新的放置点或对象要求将计算 $n+1$ 哈希值并选取其中最大值。如果对象已经在系统中为 N_k，与其对应的是新节点 N_{n+1}，对象将被再次启动并以 N_{n+1} 进行哈希计算全部客户将随后从该节点获得一个数值，最终以 N_k 的旧哈希副本将被局部哈希算法代替。如果去掉 N_k，它的对象将等于剩下的 $n-1$。HRW算法的变型skeleton能够缩减时间 $O(n)$ 以便通过最小的全局同质性来放置对象 $O(log(n))$。然而，如果n不大，基础HRW的 $O(n)$ 的安置成本将是一个问题。HRW完全避免了附加开支，并且避免了与正确处理各节点和相关元数据密钥有关的繁琐事宜。

NOOSPHERE
HRW HASHING



当n突然增大，skeleton类型的 HRW算法能够显著降低对象分布时间。这种方法能够建立一个虚拟的分层架构并达到运算时间 $O(log\ n)$，启动时按层级在各分层采用HRW。第一步提取常项 m 并在 $c=n/m$ 分片中构成节点 n，

$S_1 = \{N_1, N_2,..., N_m\}, S_2 = \{N_{m+1}, N_{m+2},..., N_{2m}\},...$

第二步从虚拟节点树叶 T 的分片中建立虚拟分层，虚拟节点的子节点为 f。

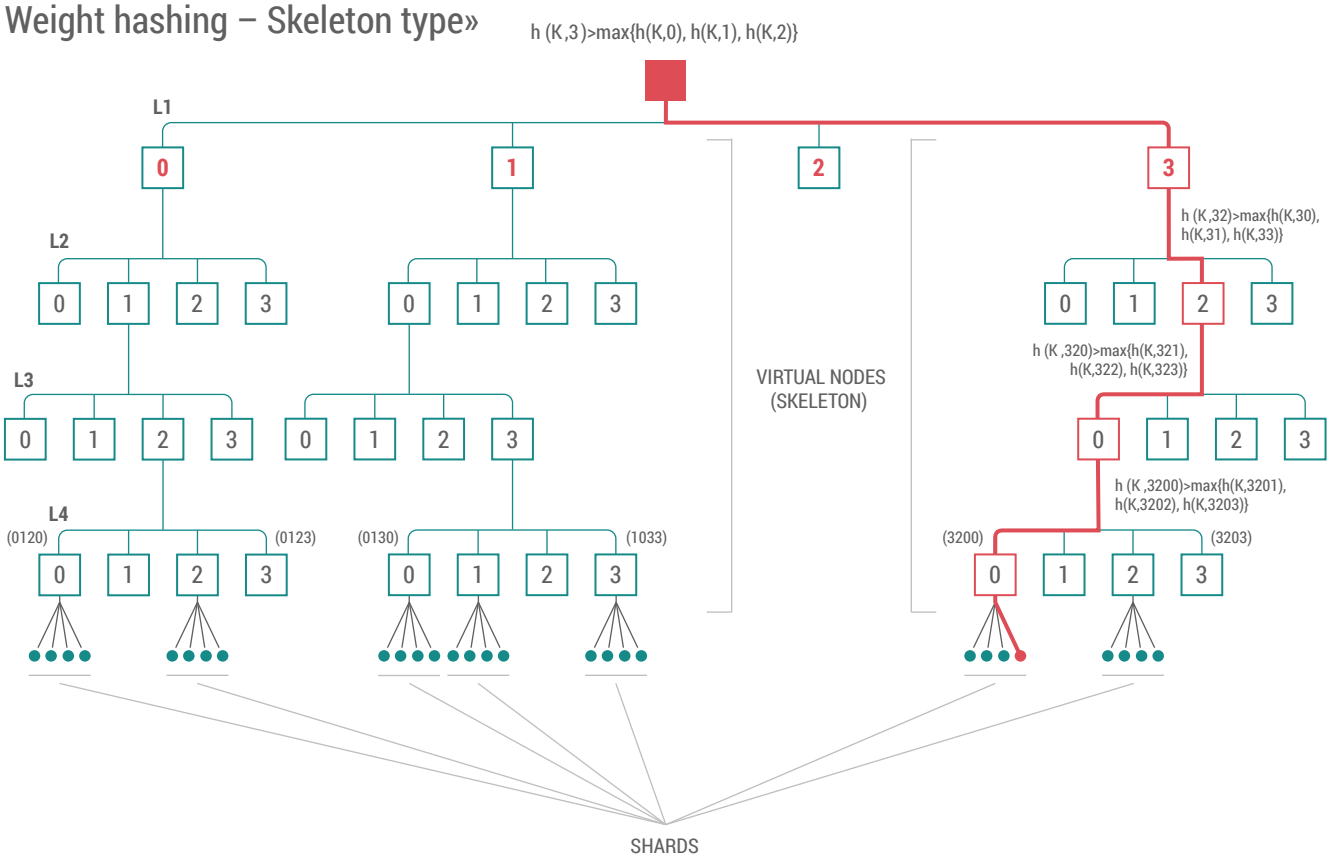
假设分片阈值 $m = 4$，架构的子节点 $f = 4$，实际节点总数为128。

与其对128个实际节点采用HRW，开始我们可以在选择一个实际节点后对32个最小虚拟节点采用HRW 。然后对分片中的4个实际节点采用HRW并选择易于发现的节点。我们仅需要 32 + 4 = 36哈希，而不是128。

我们可以从虚拟分层的任何层级而非仅从底层开始。在下部层级启用需要更多的哈希，却可在故障时改善负荷的分配。此外，不需要保存虚拟层级——可按要求建立层级，因为虚拟节点的名称只是普通的概念base-f。显然， T 有高 $h = O(\log c) = O(\log n)$，因为 m 和 f 均为常量。每个分层完成的运算 $O(1)$ 和 f 是常量。

显然，对于任何对象 O，方法与每个分片对应，因此，n节点中的每一个节点具有同样的概率。如果被选择的节点无法使用，我们可以在分片内部简单选择其他节点。作为代替，我们可以在架构中上升一层或多层，从该分层的相邻虚拟节点中选择替代节点，然后再次根据层级按照上文所述方式启用实际节点。可根据预期故障频率和预期负载平衡度等因素选择 m 值。故障情况下，依靠更高的检索费用高 m 值可降低负荷。

NOOSPHERE «Highest Random Weight hashing – Skeleton type»



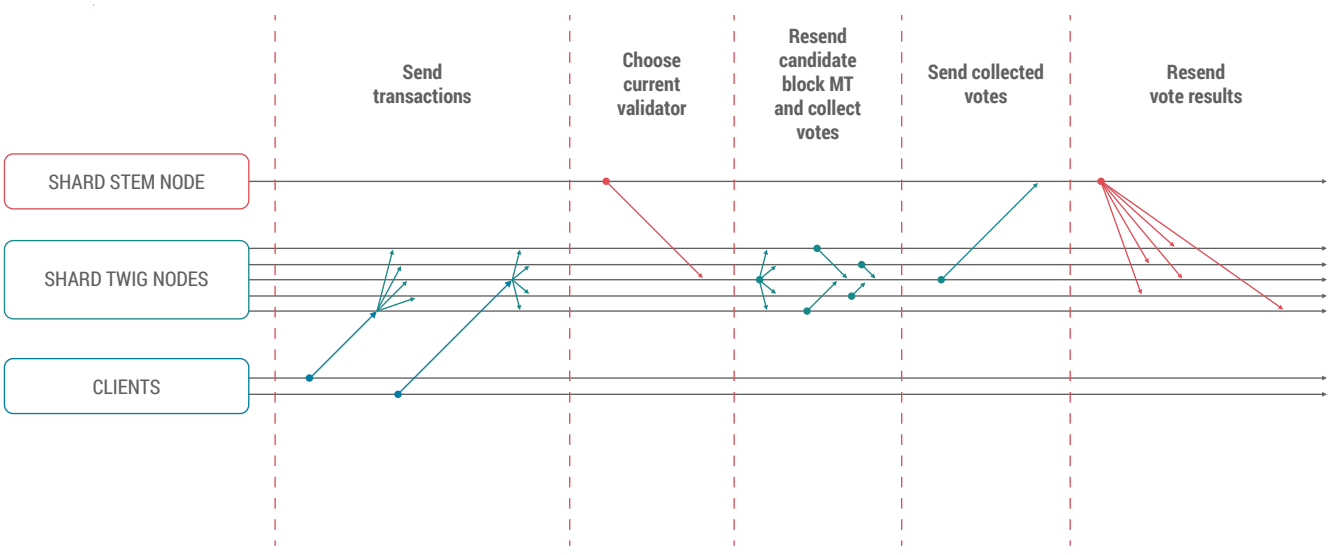
数据的路径选择问题也同样重要。向终端用户传输数据的速度以及分片之间的数据交换均取决于路径选择。最普通无效的方法是保存客户的路径选择表。但是这种方法牺牲了可拓展性。由于区块链系统的去中心化架构，使用独立划分的协调器也不可能够实现。因此，数据的路径选择问题归于系统节点本身。将相邻节点的信息和有限节点集的信息保存到节点中是在对数时间logn内找到所需源数据的最简单解决方案。因此，任何请求下，如果请求数据未被在当前节点中所保存，则会向相邻节点（如果它们有密钥）或者随机相邻节点提出请求。

5.3 分片架构

NOOSPHERE ELEMENTS STRUCTURE

TYPE	FUNCTIONS	NEEDED POWER
END CLIENT	• TRANSATIONS • CONTRACTS • VOTING	LOW
TWIG NODE	• SAVE CHAIN • COLLECT TRANSACTIONS • CHECK TRANSACTIONS • BUILD BLOCKS • RESEND TR. & BLOCKS • GATE FUNCTION • VOTING	MEDIUM / HIGH
STEM NODE	• SAVE CHAIN • SYNCHRONIZE • EXCLUDE • CHOOSE	MEDIUM / HIGH
ROOT SHARD	• SAVE ALL CHAINS • GIVE DATA TO WORLD • ROUTING	HIGH

NOOSPHERE SHARD STRUCTURE



智慧圈的每一个分片由具有不同功能的一组节点组成。参与共识算法、交易集、区块形成和验证的节点统称为枝节点。参与CBFT共识算法并加快运行的节点称之为茎节点。茎节点仅是一个辅助功能，没有它系统仍可以正常平稳运行，但是会使用另一种共识算法（详见“一致性”章节）。如果在提交申请之中并通过了选拔（详见“一致性”章节），任何意向者都能够成为分片的枝节点。 如果为了系统运行而当需要使用快速高效的CBFT共识算法时，则茎节点将作为分片的创建方。在无茎节点情况下使用PoET分片也可独立运行如果对数据选择并无重要要求。

5.4 基础分片

智慧圈的基础分片称为根碎片 - 当它与其他分片间进行数据交换时，它会调节其他分片的工作。通过以下功能可以进行调节:

1. 确定从其他分片中接收数据的真实性;
2. 提交活跃分片列表;
3. 提交分片活跃枝节点s列表;
4. 提交关于分片的服务数据

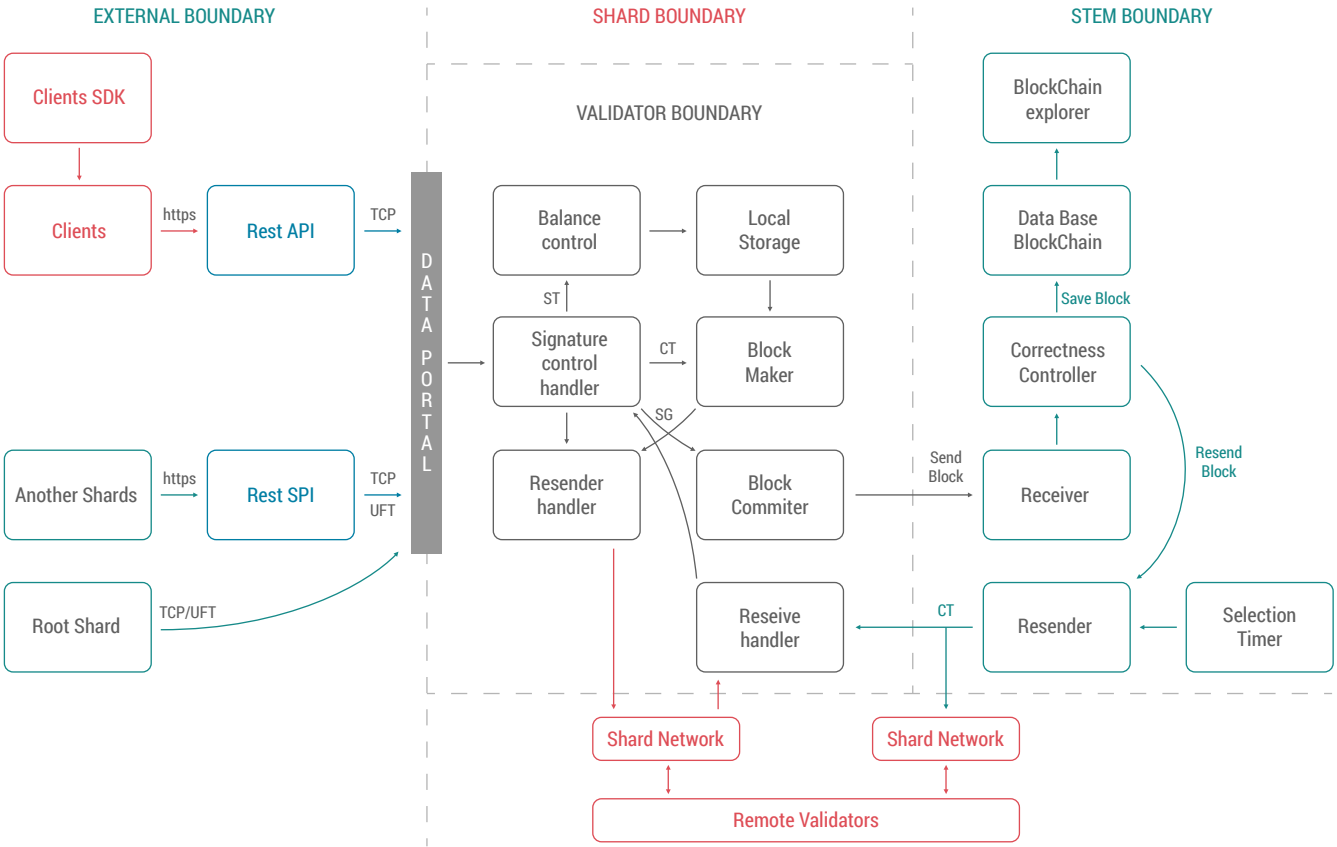
T为了实现上述功能，根碎片在自己的区块链中保存并按以下类型引用数据:

1. 分片名;
2. 独一无二的分片标识符;
3. 分片类型;
4. 访问修饰符 (公开/ 私人/ 加密);
5. 分片活跃性标志;
6. 各分片全部区块链的默克尔树架构。根碎片不会保存全部区块的副本 ——它会使用Merkle Proof 验证数据;
7. 描述分片及其提供的API服务

根碎片 支持以下类型的交易:

1. 新分片登记事务;
2. 分片删除事务;
3. 分片区块Merkle Tree保存事务;
4. 当前分片验证枝节点的s 保存事务。

5.5 NZT 分片

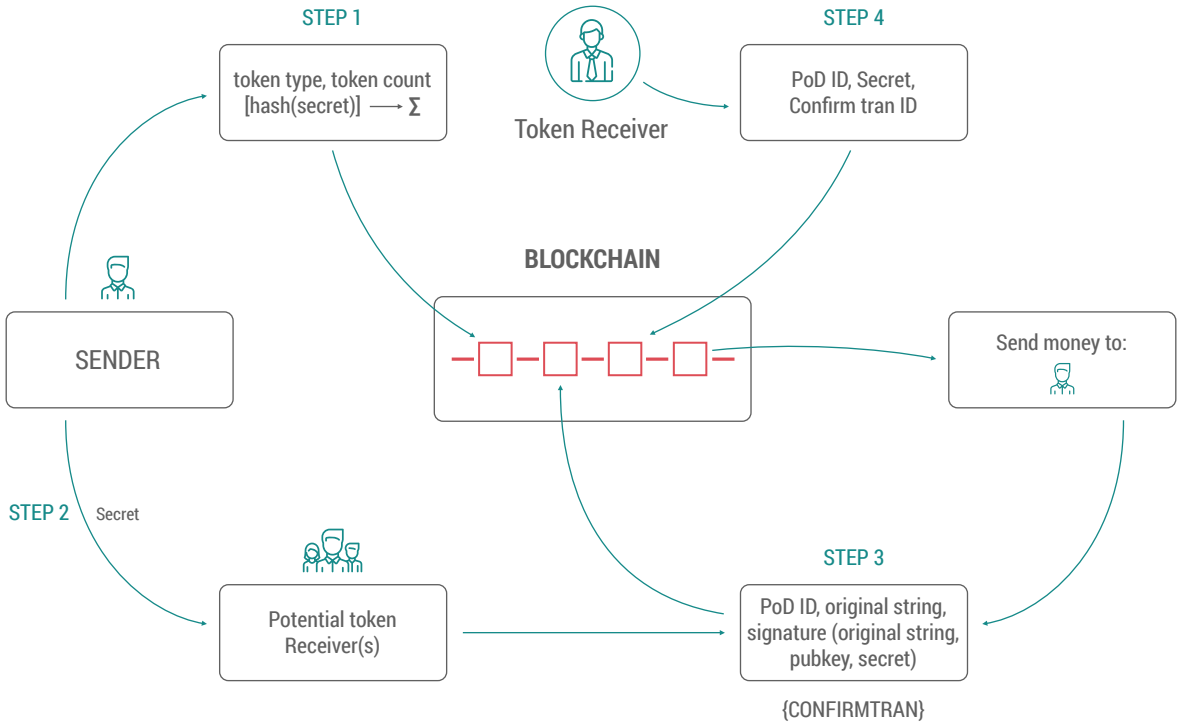


NZT碎片提供的服务伴随着系统的主要货币NZT。这是一种在系统用户之间汇款的功能，支持一系列特殊事务:

1. 递交作为枝节点参与当前验证的申请交易;
2. 提款交易(PoD);
3. 汇款交易;
4. 利用多重签名的汇款交易。

5.6 PoD - 按需支付

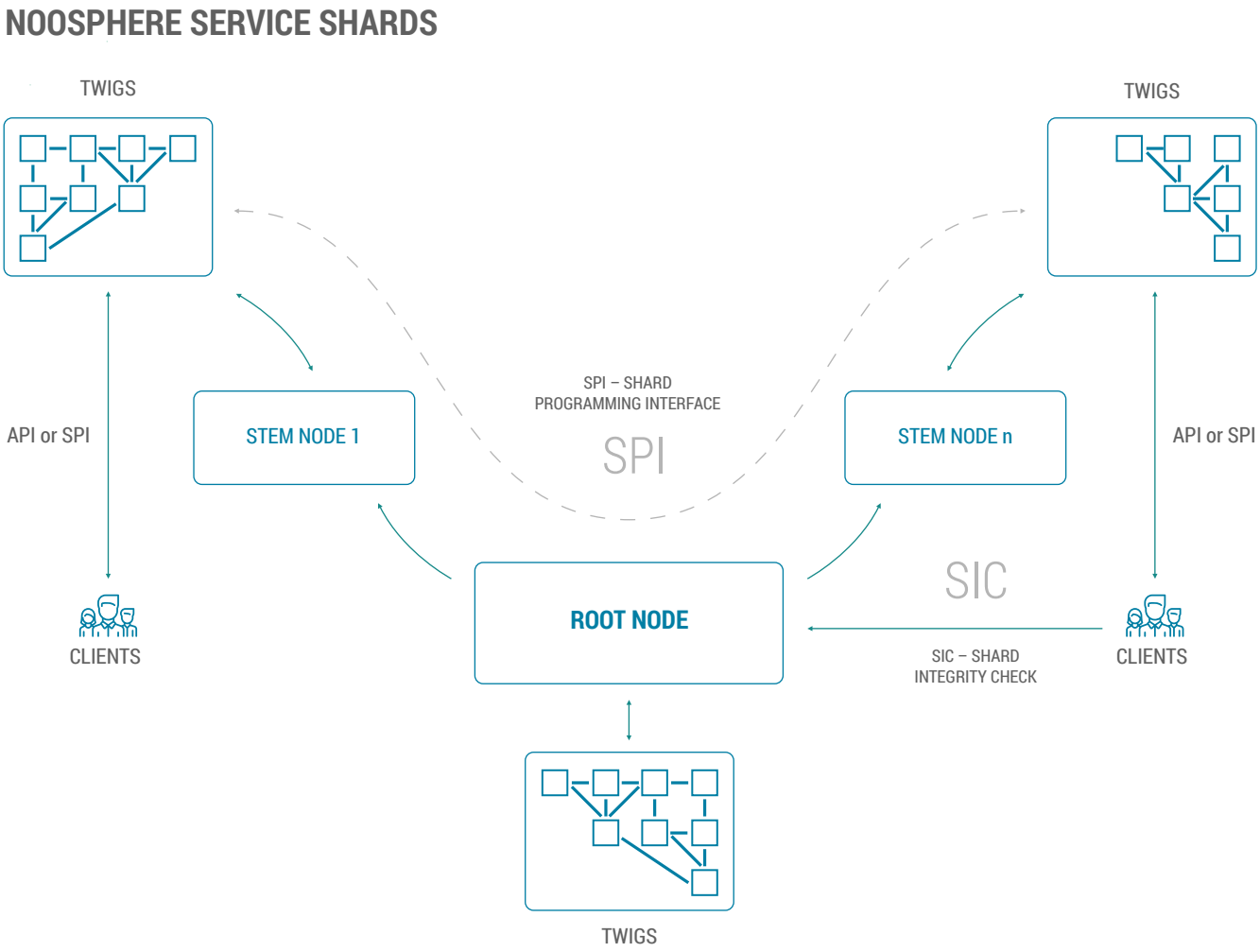
NOOSPHERE PoD – payment on demand



此种类型的交易会在NZT碎片中实现，提供用户间汇款和参与/拒绝的功能。用户能够将任意数量的货币转为“存储”的特殊状态，它们仅可在密钥发布后从这种状态下取款。该密钥可由网络的任意参与者发布，因为货币在“存储”状态下与付款方和潜在收款方均无关系。交易创建者能够创建所需数量的密钥，它会在此之间分到自己所需的份额。

5.7 服务分片

定向服务分片技术理念指的是从分片构想向服务分片过渡。智慧圈平台上的每一个分片就是服务分片，并且这些文本是可替换的。在传统分片技术实现过程中，每一个分片都会处理总交易流中的一部分，这可加快区块链的运行。对于智能圈来说，这只是使用方案之一，因为接收交易流负荷的分配是一种服务器，这种服务器应当被专门为该种服务分片所创建。



可以分出两种在分片中实现服务的方法。第一种方法是直接使用分片区块链的架构，在此之中按照既定规则保存密钥值的记录，它们可以确定服务的功能性。经中心验证的DNS，路由选择服务器是该方案的典型示例。第二种方法整合性较强且可提供资源密集型服务。
对于第二种方法而言，需要对工作的结果进行运算，继而确定区块链的内容（智能合约），或者不要求将输出数据保存在区块链中时（透视图、科学研究和dApps），则区块链只完成行政功能。当进入系统时，在上述两种情况下，每一个分片都应提交自己的API的介绍以便自行使用。

在创建服务分片时，可以创建与其伴生的货币。当在根碎片登记时，应当提供货币在分片运行期间的生成规范。

5.8 分叉

智慧圈平台不受分叉概念的限制。对于一般区块链而言，分叉是整个系统中内嵌关键功能算法的交替。依靠智慧圈的模块架构，可以通过新建服务分片以扩大自身的功能性。终端用户可自由选择他所信任的服务器，以及两种或两种以上具有统一功能但能与不同实现方式的服务分片并存（例如交易混合器），这就是智慧圈的标准功能图。

5.9 分片安全

在茎节点参与分片运行的情况下， 茎节点会控制选择例行验证的参与者并管控删除不稳定的验证器。茎节点仅参与辅助功能，分片区块链自身的形成并无任何参与项，因此茎节点不会影响数据的安全性。如果分片按照PoET算法运行，所有参与者将处于平等的关系之上，则他们之间将会在独立中达到共识。此外，如果网络参与者发现可在当前验证中证实非验证区块的不稳定枝节点，则参与者个人将会锁定该枝节点。当分片之间交换数据时，参与者能够通过根碎片校验所获数据的真实性，根碎片保存了所有分片的相关数据。根碎片 中有所有分片整个区块链的Merkle Tree，它能够100%正确地验证并确认数据的存在和真实性。同时， 根碎片 保存了所有活跃可靠的并且可用于数据查询服务的分片节点相关数据。如果发现了分片参与者提供了虚假数据，根碎片可对其进行检验并删除

5.10 分片设计者

特殊程序工具的推出是为了简化智慧圈平台私人服务分片的创建 — 碎片设计者可借助易用的图形用户界面或组态文件去形成分片及其区域模块所需的交易架构，从而规划外部服务API以及与计算所消耗的资源（包括与外部正在运行的系统）与其联络的机制。除此之外，如果在需要与标准形式不同的且网络异常终止还能够设定共识算法与其功能参数。内嵌测试能够避免设计错误，测试网能够校验工作中以及其他分片周围的新分片。

5.11 Noosphere 测试网

智慧圈平台的测试网由两部分组成。第一部分该网在一台计算机中模仿智慧圈网络的运行时，碎片设计者会提供的纯粹虚拟网。第二部分是由Noosphere Foundation创建和支持的真实测试网，它能够全面测试新的分片，特别是候选者向静态分片过渡的时期。

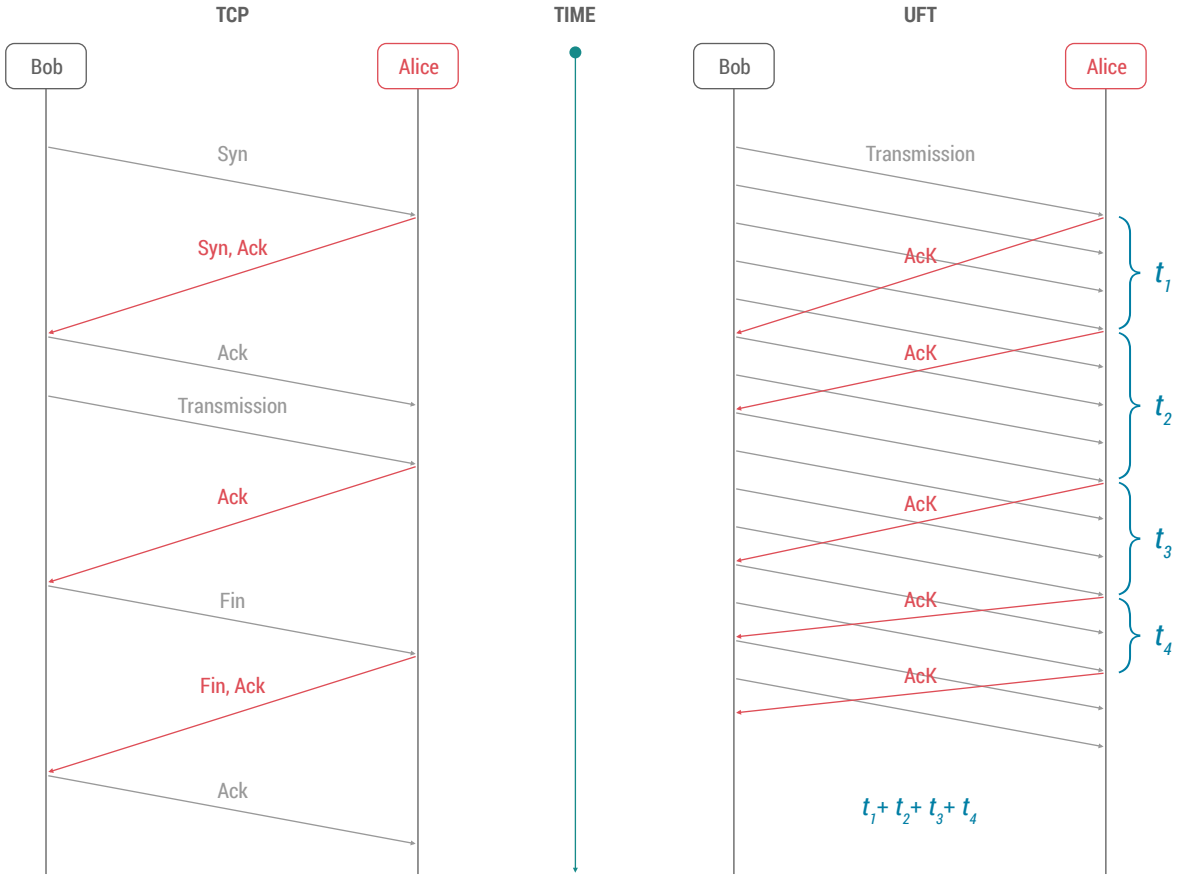
5.12 并行交易处理

为避免形成队列而采用输入数据流平行的处理，智慧圈平台的高速运行对接受交易处理算法提出了特殊要求。交易的分配根据平行的服务数据流运行，取决于数据流的类型以及从发送人地址收到的数据流标识符的特殊值。当启动校验器时，软件确定系统中可用于交易服务的数据流可能数目。根据这个数值形成具有独一无二标识符的对应处理池数量，随后启动输入的交易。从发送人地址收到的数据流标识符接收类型很多。最普通的类型是将地址空间分为数据流数量。与后续处理相比，这不但显著提升了工作效率，还可避免双倍的花费。

5.13 UFT – 超高频流传输

基于分片参与者之间（以及直接在分片之间）数据传输和转发的UDP 协议(UDP流传输)能够避免TCP（是英特网数据传输的实际标准）的典型问题包括：数据包丢失时传输速度降低以及过载（当用户不能接收发送者发出的全部数据时）。这其中任何一个问题都会使发送验证交易这样的操作大幅降低其网速，这主要是由于额外附加费用会导致区块链中每一个中枢的网络资源被再次利用。

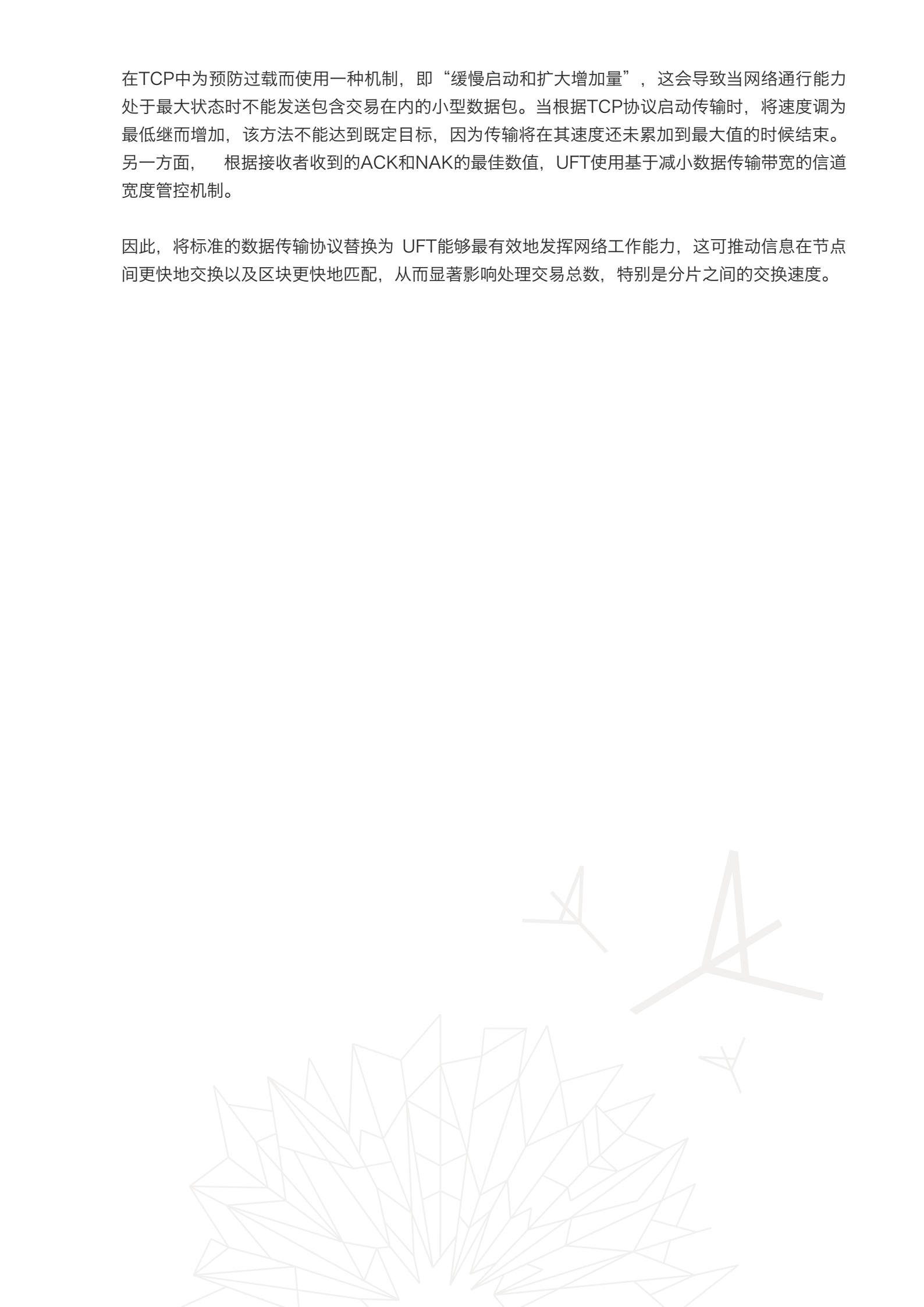
NOOSPHERE UFT



在TCP协议情况下，当消息发送队列超载时，主路由器的可能性过载会导致传输速度降低。随着网络链路中路由器数量的增加，丢失概率也会增长，当存在个别损失时会导致传输速度大幅下降。TCP协议指的是传输数据流中数据包的相互认证，发送者未收到认证信号(TCP ACK) 将导致从数据包丢失位置的传输再次初始化。UFT 指的是建立发送者和接收者之间的双向联系，其中发送者-接收者联系用于已发送的数据流，反之联系则是独立的，需要确认接收。TCP和UFT之间的原则性差别在于UFT需要经过短暂的时间间隔后选择确认接收到的数据流(SACK)。当数据传输速度高，周期性的ACK可简化返回检查信息的动态控制，因为这种情况下，ACK的数量与时间成正比，不同数据包数量成正比，如同TCP的情形。如果丢失数据包，接收者将发送否定应答(否定ACK, NAK)，这会导致选择性转发输出数据流的特定部分。

在TCP中为预防过载而使用一种机制，即“缓慢启动和扩大增加量”，这会导致当网络通行能力处于最大状态时不能发送包含交易在内的小型数据包。当根据TCP协议启动传输时，将速度调为最低继而增加，该方法不能达到既定目标，因为传输将在其速度还未累加到最大值的时候结束。另一方面，　根据接收者收到的ACK和NAK的最佳数值，UFT使用基于减小数据传输带宽的信道宽度管控机制。

因此，将标准的数据传输协议替换为 UFT能够最有效地发挥网络工作能力，这可推动信息在节点间更快地交换以及区块更快地匹配，从而显著影响处理交易总数，特别是分片之间的交换速度。



5.14 共识

5.14.1 CBFT 共识

卷积拜占庭容错是智能圈平台的主要共识算法。与普及的PoS不同，CBFT不会根据存款数值分配节点。所有节点处于平等条件下，对其进行选择时，仅会按照一组标准来进行:

- 计算能力;
- 网络连接数量;
- 具有必要数额的存款货币。

系统使用该笔存款，作为节点可靠性的担保。运用随机选择的方式，按照既定周期从递交的申请中选择节点。使用特殊交易类型递交申请以确保进程的透明性，所有候选和枝节点s的相关数据保存在区块链中。当前验证期间同时运行的枝节点s数量取决于网络负荷。验证持续时间为10000 个区块。

无需在枝节点s网络之间大量发送候选区块是CBFT的标志性特点。相反，节点完全可以交换有关交易的压缩元数据组从而达成共识并进行表决。仅在新出现并需要区块链真实副本的验证器时使用区块文件。此外，使用UFT协议能够避免在传统BFT算法使用过程中出现的转送传输被迫延迟。当前区块创建进程的开始由茎节点控制，它会从活跃的枝节点s队列中随机选择一个当前枝节点 。区块创建时间为1.5秒，此时仅有一个验证器有权创建区块。如果在1.5秒内未能创建区块，茎节点会将时间间隔扩大一倍后管理下一个枝节点。如果验证器连续三次不能在分配给它的时间内创建区块，则它会从当前验证器组中删除。如果创建具有虚假交易的区块，验证器会被删除，系统会保留其存款。

5.14.2 CBFT 技术

现有区块链平台共识系统的网络架构基于系统运行周期的平稳性原理，仅使用泊松事件流建立此架构。在许多情况下，分析输入数据流分配法则的类型和转换周期的持续时间的必要性决定了后者能够组成系统运行周期的实质部分，而输入数据流分配法则可对系统输出参数的统计性产生显著的影响。因此，如果不考虑非平稳性周期和输入数据流分配法则类型的影响并不能彻底优化系统的工作性能。

一起看一个系统输入申请流模型，该模型规定当取确定的平均强度 λ，输入流强度取决于时间 ，$\lambda_g(t)\ (g=\overline{1, period})$ 即使用输入流平均强度值 λ 和反映输入申请流在较长时间内(周期 - 系统功能周期)变化的统计数据。在大规模服务理论中，通常规定根据指数法则，输入申请流强度为 λ 的申请进入系统，并不受时间t限制。申请输入时间间隔ξ有连续的随机变量，此变量指数分布参数 $\lambda > 0$。ξ只取非负值，其密度$f_\xi(x)$ 和分布函数 $F_\xi(x)$ 分别为以下类型:

$$f_\xi(x) = \begin{cases} \lambda e^{-\lambda x}, x \geq 0, \\ 0, x < 0; \end{cases}$$

$$F_\xi(x) = \begin{cases} 0, x \leq 0, \\ 1 - e^{-\lambda x}, x < 0; \end{cases}$$

式中 λ - 输入流的强度。

ξ 偶然值的数学期望与输入流强度比 $M_\xi = \frac{1}{\lambda}$. 偶然值的方差也由输入流强度 $D_\xi = \frac{1}{\lambda^2}$ 决定。实际情况中，系统输入流强度并不是定值，它会随时变化。它的变化与系统活跃参与者在达成共识过程中大量发送候选区块的周期以及系统中申请服务的时间有关，即与分析由当前验证期内事务集组成的候选区块有关。

在开发CBFT共识算法构成中收集到了能够反映分布式网络中由于候选区块转发时间引起的输入数据流强度变化的统计资料以及处理容量和时间的相关统计资料。借助带有既定边界条件的三次样条内插分段多项式 $S_g(t)$ 可对收到的统计数据执行近似算法，即在每个有j号的部分 $[t_j, t_{j+1}]$ 近似函数 $S_g(t)$用多项式表示。

$$P_j(t) = \sum_{i=0}^{k-1} a_i^{(j)} (t - t_j)^i, k - 1 = 3$$

边界条件在周期性条件下，即间隔范围内 $[T_1, T_n]$. 第一个派生值和第二个派生值一致。
建立样条能够借助线性方程式系统方案确定系数集 $a_i^{(j)}$。针对于既定函数 $S_g(t)$ 履行内插条件 $S_g(t_i) = y_g(t_i)$ $i = 1, ..., N$ 对于表格函数 y_g
当平均强度 λ 确定，为了求得输入流强度对时间 $\lambda_g(t)$ 的具体依赖性，需要用得到的样条 $S_g(t)$ 到的样条 乘以平均强度，随后分割成样条平均值$S_g(t)$:

$$\lambda_g(t) = \frac{\lambda}{\overline{S_g(t)}} S_g(t)$$

$$\overline{S_g}(t) = \frac{\sum_{i=1}^{N} S_g(t_i)}{N}$$

式中 λ 输入流的实际平均强度。

提到的输入流模型要求接收申请的时间间隔 ξ 是一个连续的随机值，它可按照诸如指数法则、泊松法则、常规法则和平均法则等不同的法则分布。

5.14.3 运行时间证实机制 (PoET)

如果智能圈任意一个分片的控制节点出现故障，则会转换为另一个共识算法——PoET。该算法运行方式如下。分片的每一个节点会激活内部计算随机时间的计时器。计时器最早运行的首个节点会成为当前区块的验证器。但是为实现该项功能需要校验两个条件：偶然选择的等待时间的及节的数量点是取决于等待计时器是否启动。使用英特尔软件防护扩展(SGX)技术就可校验这两个条件。确保履行上述两个条件是PoET 共识算法的受信任代码，SGX 会使应用程序能够在中央处理器层级的加密环境下启用受信任的代码。SGX使网络参与者能够互相检验加密的是否是正确的代码，代码是否正确执行，以及排除非法用户的欺诈行为。与CBFT的基本算法相比，此种条件下的共识停留时间延长至4秒。如果分片对提高交易处理速度并无要求或它的功能不要求具备 茎节点，则可使用此种共识算法。

5.14.4 混合SGX-CBFT算法

对于攻击概率十分高的关键服务而言，用户可以使用SGX混合共识协议——CBFT。它的运行方式类似于前文介绍的卷积拜占庭容错，但是网络参与者还可以借助英特尔SGX技术远程校验所有相邻节点的可靠性。

5.15 攻击防护

如同任何一种在因特网中运行的信息系统一样，区块链是黑客们的目标。除了众所周知的DDoS攻击类型，还新出现了许多对区块链平台的攻击方式。对所有威胁的分析（包括分析被攻击区块链系统的架构缺点）可在智能圈子系统中植入有效的反黑客防御手段。

5.15.1 DDoS – 分布式拒绝服务攻击

此攻击的成功基于工作能力的限制，后者是所有共享网络的性能之一。在DDoS 攻击期间，向共享网络发送大量请求，旨在终止其处理数据的能力并破坏它的常规功能。为防止此类威胁可以使用Loki这种特殊的服务分片。它的任务是连续监控并分析数据，当发现 DDoS迹象时，流量会转到专门的节点，随后进行虚拟处理。因此，攻击看似成功，但受保护的服务却继续正常运行。

5.15.2 女巫攻击

这是一种非法用户将大量受其操控的节点投入网络并试图“包围”被攻击节点，即占有全部相邻网络节点的攻击行为。在 CBFT共识协议算法运行中此种攻击类型不易察觉，因为当试图破坏网络正常运行时，节点都会禁用并且它的存款将由系统保管。即使当非法用户持有能够恢复攻击的足够资金时，这可显著降低攻击的成功概率。也会为每轮验证随机选择节点。

5.15.3 日食攻击

日食攻击。2015年由伊坦·海尔曼领导的波士顿大学和欧洲大学的专家团在报告中详细介绍了这种软杀伤类型，随后在以太坊网络中进行了示范。当正确操作时，黑客可“覆盖”对等网络上的节点，使这些节点只和受攻击节点接触，从而影响新区块的创建进程。对于智能圈大多数都使用共识算法，所以此种攻击并未真正地实现。 通过英特尔SGX技术，PoET算法能够校验周围节点的真实性，而通过随机替换每轮验证的验证器，CBFT可以迫使黑客每次都从新攻击中进而消除攻击作用。

5.15.4 51% 攻击

这种攻击是最普遍的类型之一，会不断攻击挖矿机的区块链。对于包括智能圈在内的非挖矿机系统，这种攻击将难以实现，因为这需要更多的经济资源。当使用混合SGX-CBFT时候，攻击完全不可能，因为即使是占领其中一个节点，得益于远程校验的可靠性，这个节点也将会立刻被隔绝和禁用。

5.15.5 双花攻击

指的是如果区块链非同步化，两次成功使用同一个工具。这种攻击只针对网络参与者有权创建新区块的系统。对于 CBFT 共识算法，这种攻击不可能实现，因为只有一个节点负责在特定时间单位内创建区块，网络非同步化并不可能。

5.16 路由

已经建立了针对在中心化系统中使用的现代网络路径选择协议。由于缺少类似协议和替代协议，现有去中心化平台仍在使用上述协议。此外，这些协议并不能有效解决去中心化系统中数据路径选择的相关问题，因为它们使用了完全不同的实质，十分需要在动态网络节点之间对数据进行快速路径选择。

去中心化网络包含大量交易节点——这比中心化网络多出许多。解决去中心化网络中的路径选择任务不仅需要采用复杂的数学仪器，并且没有专业化软件，独立计算路径并不可能。为了解决这类问题而开发了Swift Torus 路由协议。使用此种协议能够显著提高动态节点间数据的传输效率和速度，特别是在不同分片节点间传输数据并且没有可实现服务分片的系统中心入口点。

以网络节点作为极值，以节点间的联系作为数据传输加权信道的图解法是借助网络动态拓扑在系统中建立动态路径的方法之一。同时，代替标准算法，避开图解法，为了找到最短的路径使用基于节省空间的图形表示法 - Hilbert-ordered tiles的计算算法。这种方法在现代图形处理引擎，即 MOSAIC中使用。为了比较，使用Hilbert-ordered tiling scheme，根据700000000余个极值的图解法计算路径仅在4个Xeon Phi处理器中耗时1秒钟。

采用离散时间模型直接创建图表。在这种模型中，网络拓扑的变化表现为拓扑快照的周期性重复序列S，公用时间间隔 $\Delta t=T/S$ ，式中T 表示组拓扑状态的重复周期。拓扑G = (V, E)对应每一个快照，式中V表示节点组，E表示信道组。 对于在周期 T内重复的拓扑有限集{G}，提前设计路径选择表。表格数据按照节点发送，在必要时刻 使用。

设计出的系统数学模型能够以图表体现的常态序列反映连续的拓扑变化:

$$\forall t \in [0; +\infty) \exists \Delta t_n = t_n - t_{n-1}$$
$$t \in (t_{n-1}; t_n)$$
$$G_n(t) = G(\Delta t_n)$$

考虑到网络的拓扑状态会受外部事件的影响而变化:

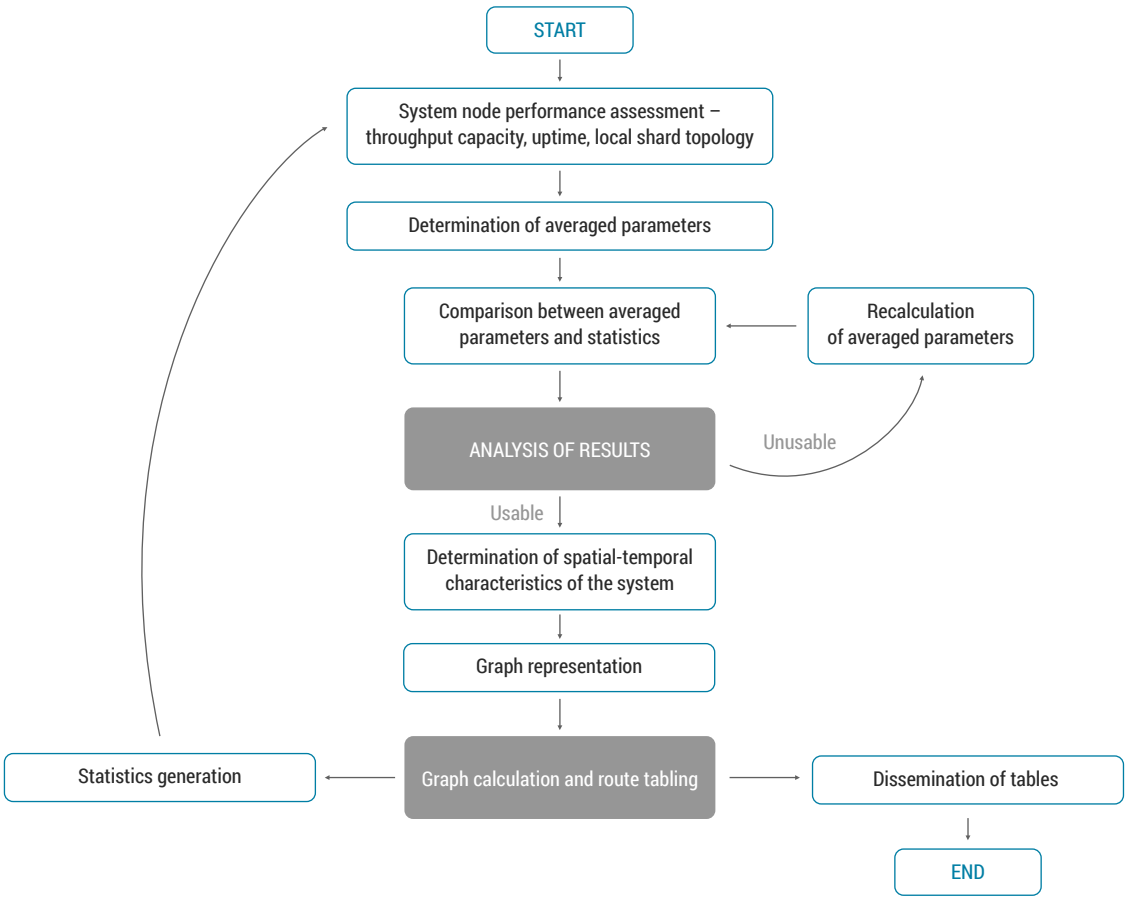
$$G(\Delta t_0) \rightarrow G(\Delta t_1) \rightarrow \ldots \rightarrow G(\Delta t_n)$$

预测网络拓扑在一定时间 T_p - 预测时间内的未来状态。

$$\sum_{1}^{n} \Delta t_n = T_p$$

式中 Δt 为一个时段，在此期间认为系统参数不会恶化; $G(\Delta t_n)$ 网络拓扑在 时段内具有极值V的有限集和边集E。T_p 为通信系统被预测状态的时间。

考虑到上述准则，节点和信道的工作统计以及设备的技术性能是模型的基本输入参数。下方展示路由选择图预先计算算法结构图。



5.17 Noosphere 服务-分片应用

Noosphere Foundation 设计人员社区本着去中心化和安全性原则打造了基本的关键事务服务器。这类服务器的任务是成为由相关人员研发的更复杂服务的功能基础。

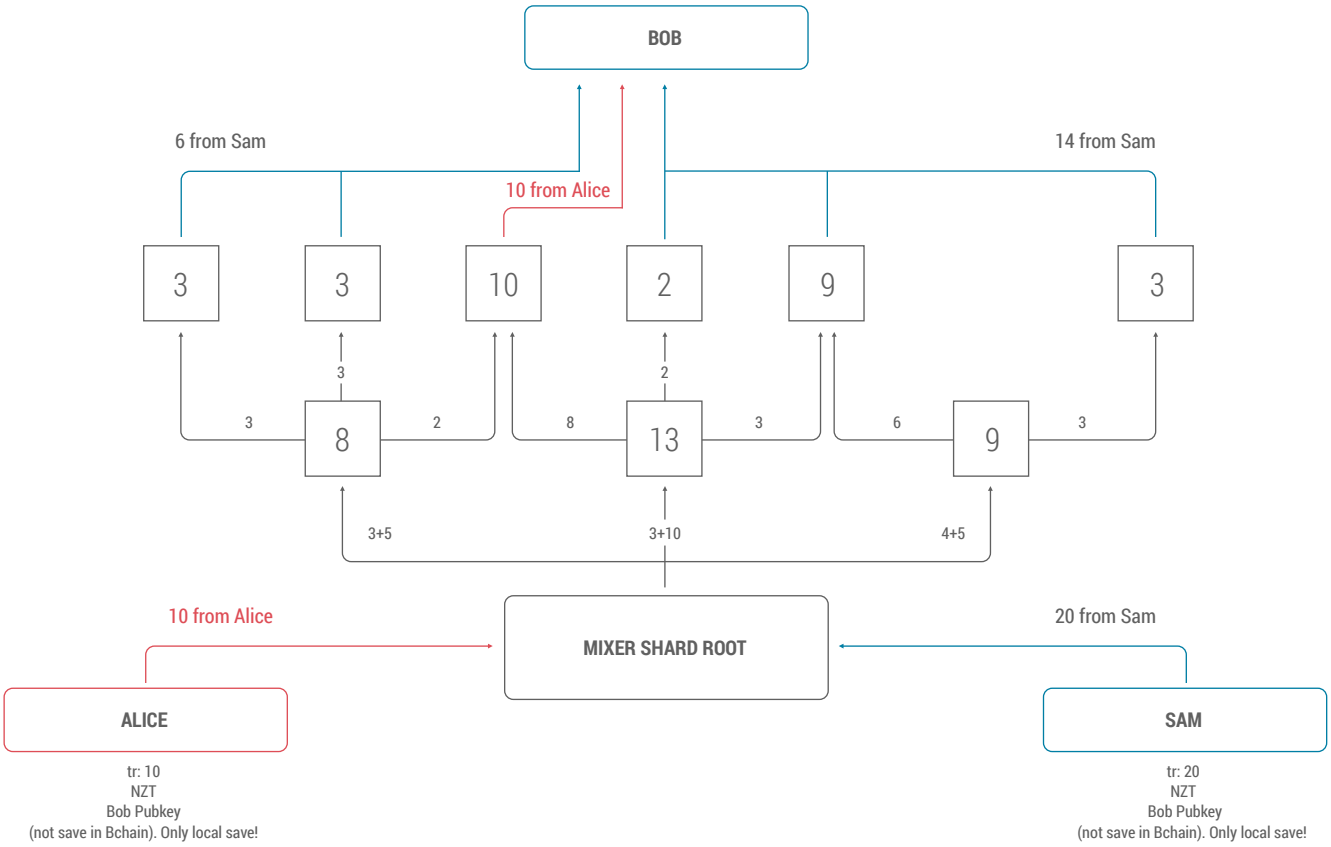
5.17.1 DAR & DDNS – 动态应用程序路由和动态域名系统

服务导向的分割使用的可行性方案之一是将网络计算资源用作数据传输的分配仓库或者分配路径选择。使用Noosphere Foundation 研发出的动态应用路由协议能够实现这种路径选择。该协议指的是利用每位网络参与者的工作能力，根据I2P 或Tor网络类型创建高于英特网的去中心化网络，并非在IP包一般传输层面，而是在客户和服务器间按照具体软件协议交换数据的层面。该协议的执行可以使用终端服务器间负载平衡算法，还可选择地理分布式数据中心之间的用户数据流路径。该协议的执行可以作为已适应Noosphere 秘密信使的客户与服务器之间数据包的随机路径选择方式。

每一个分片节点都是路径选择单位，IP地址和接入特点（响应时间和工作能力）的相关信息保存在区块链的特定分片中。为了实现地理分配的路径选择，在区块链中保存着一串密钥-数值，其中密钥是用户标识符哈希，数值是必要的系统入口点。并且每一位网络参与者都会持有明确的指令：向哪一个服务发送具体用户的数据。出现一个问题，与区块链分片没有联系的聊天工具的用户如何确定接通哪一个路由器。解决方案相当简单。DNS协议可在5秒钟内更新一次域信息。实际更新时间的全球纪录约为25分钟，能够设计该应用碎片并组建包含路由器信息的区块，时间为5-10分钟一次。区块链会在此期间形成DNS域的相关信息，上传进行整体加工并在网络内部发送DNS解析。此外，建立连接的聊天工具用户通过DNS请求、DNS服务询问路由器的有效IP地址，该地址可从区块链接收已经更新的数据并转入钱包中，上交分片参与者的其中一个地址。用户获得路由器地址后就可接通本地区的服务器，开始交换数据。这种方法的主要优势是基于动态应用 路由，因为来自聊天工具客户的流量是按照包含不断变化入口点的标准 https协议请求和应答。

5.17.2 NTM – Noosphere 交易混币器

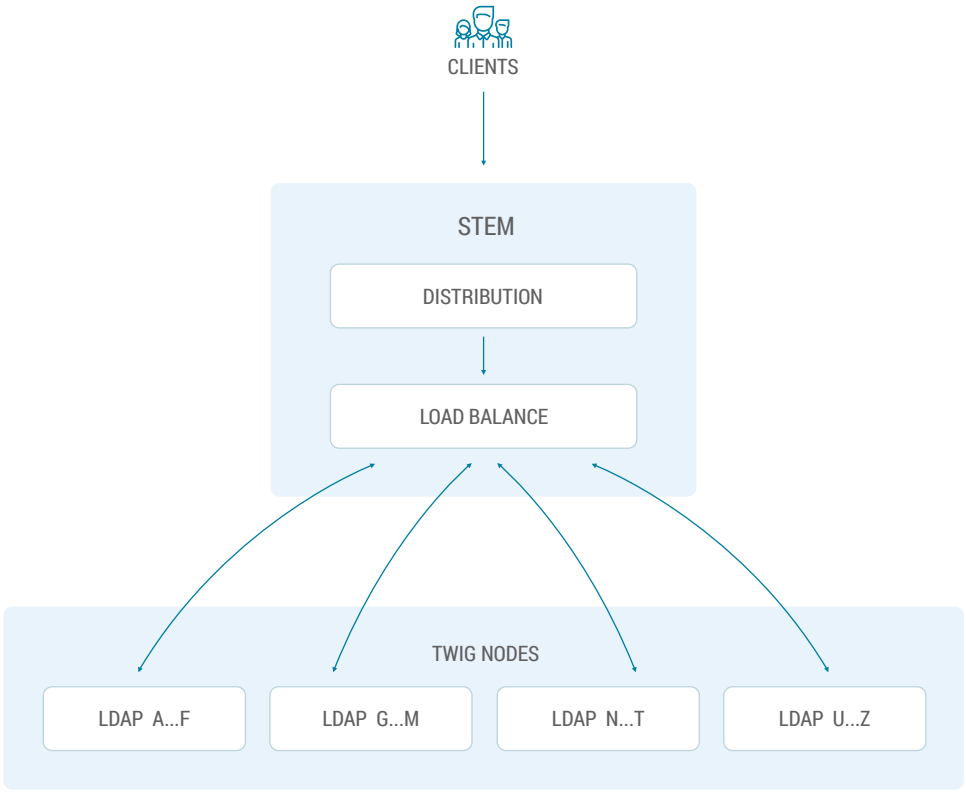
NOOSPHERE NTM



在智能圈平台能够轻松提供最受区块链平台用户欢迎，旨在提高转账匿名性的交易混币器。用户将数字货币转入分片茎节点　并注明资金的终端接收者。茎节点将其分割成多笔小额款项发送已注明终端用户的款项枝节点s，网络节点在用户已选择的时间内交换数字货币的数据，随机向接收者转款。分片茎节点可监控所有资金转账。不会在分片中保存任何发出方和接收方的相关信息。由于不同的用户能够同时使用混币器的多个变型，因此连续使用这些混币器并不困难，这可在保密用户个人信息的同时将转账匿名性提高数倍。

5.17.3 DDAP – 分散式目录访问协议

NOOSPHERE DDAP



DDAP是支持LDAP协议功能的一种服务器，对运行安全性、容错性和速度有更高要求。在分片节点中分割所有保存目录，可以单独设置每种数据类型的储存级别。分片节点的茎节点会考虑分片的当前符合以及包含查询信息的分片清单，随后确定将接收用户请求的分片节点。

5.17.4 ACS – 自主版权制度

区块链系统的架构能够创建防注销和改变的自治版权系统。任何二元数据——图像、文本以及语音等都可作为版权保护对象。ACS服务可针对每个对象建立一系列特征，这些特征能够精准识别该对象，随后在整个数据库中进行快速检索。数据库中的每个对象都可收到防复制和侵权的证书。

5.17.5 Loki – DDoS 保护系统

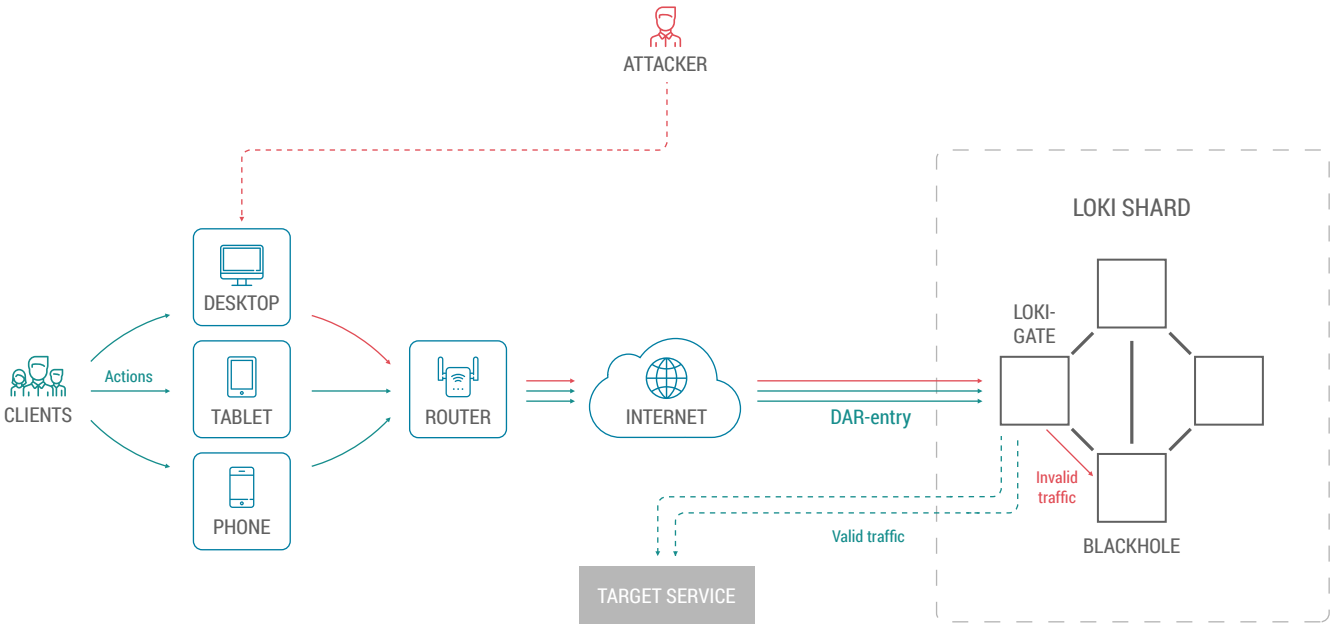
DDoS (Distributed Denial of Service)是分布式“拒绝服务”攻击。网络资源由于从僵尸用户组织的不用节点发送的大量请求而被占用。 (维基百科)

发送类似攻击的原因相当多，不需要了解与保护区建立有关的细节，如该攻击来自哪里以及为什么。此外存在相当多的攻击方式，保护方法也同样多。
Loki可同时在OSI模型的多个层面运行，对输入请求、通信对话时间和数据流进行分析并整合，以便最准确地发现来自合法用户的流量，去除不可靠的误报。

在这些设备中，使用的Loki可以分出多个要点:

- 过滤不可用的数据流 (英文 - malformed)
- 分析数据流并从中发现异常
- 分析网站用户的行为

NOOSPHERE LOKI



如果第一个设备包括一组防火墙过滤规则，那么第二个和第三个则使用 DPI (深度数据包检查)，可以进行统计并根据机器训练的统计数据执行，以便进一步发现异常并快速做出反应。这种情况下，区块链用于保存可识别流量异常的围绕神经网络的比重，这能够在过滤节点之间同步CHC训练结果。

如果在数据流、用户行为统计或控制序列故障统计中发现异常，用户请求会自动转发要求额外验证，这首先能够依靠用户验证和识别来训练神经网络，如果攻击检测有保障，流量转发到可以模仿成功攻击的特殊节点。

使用本组技术并结合该文件中介绍的DAR技术能够创建独立于服务器自身的最可靠服务，该类服务器主要是聊天服务器，网站以及 VPN之门等。

5.17.6 EBS – 有效的备份服务

相较于使用中心化系统，将区块链用作分布式数据库更加有利。询问和数据下载的速度会高出很多，因为会立刻从众多来源下载，文件在这些来源里直接分配。共同缺点是在分布式网络参与者出现故障或者压缩时，数据的完整性和安全性。使用基于范德蒙行列式的正向纠错(FEC)就可轻松消除这一缺点。有效备份服务是 消除恢复和错误纠正功能，能够保留数据的完整性和安全性，甚至是丢失部分数据时。存在一系列错误校正代码，可在FEC中使用这些代码。主要是 Reed-Solomon码、Hamming码、Reed-Muller码和binary Golay码等。

5.17.7 DHPC – 分散式高性能⌧算

网格系统是分布式计算方法之一。网格是一种地理分布式计算平台，该平台由能够通过统一接口访问的异构节点组成的。当没有数据资源中心化管理时，平台可以协调资源使用，使用标准协议、公开协议和万能协议以及接口，还可用独特方式确保高质量服务。根据资源类型，Grid-系统可以分为:

- 数据网格;
- 信息网格;
- 计算网格。

网格程序包括:

- 远程超级计算机的复杂升级;
- 共同显示大量科学数据;
- 针对数据分析的分布式处理

网格系统的主流解决方案的基础是OGSA - Open Grid Service Architecture开放式架构。OGSA是服务器中的一种分布式计算和协作架构，能够保证多相系的互操作性不受运行、位置以及平台的影响，确保不同类型的资源能够交流并交换信息。

智能圈在OGSA基础上开发出DHPC服务器，目的是方便计算资源在已有的HTCondor、Globus项目和BOINC平台，以及在OGSA基础上新出现的平台上使用。
DHPC包括:

- 分布式程序前端，是所有分布式网格计算平台的统一门户;
- 在HTCondor基础上执行计算任务的SDK ;
- 控制点机制;
- 数据复制服务器。

DHPC不仅可以租借自己的计算设备，还可以使用网格平台的设备完成个人任务。

5.17.8 PVM – 虚拟机

智能圈平台限制了将在其服务器-分片中执行的功能。因此，未限制特定类型的虚拟机，它们将在分片中用来履行智能合约和dApps的功能。Noosphere Foundation 提供了可以根据类似Python的 语言处理智能合约的新型虚拟机。选择Python编程语言作为基础，因为根据Github 统计，它是最受欢迎的可快速高效创建脚本的编程语言。该服务分片不是处理智能圈智能合约关键分片，它同其他类似服务-分片一样，仅向愿意者提供该项服务。

5.17.9 ABG – 任何区块链门

所有区块链都会基于自身拥有统一抽象功能——处理根节点的代码和数据API询问。内部实施不同，但是访问架构是同一个。针对这一目标，使用ABG模板服务，它能够将任何间接区块链导入智能圈生态系统。对于终端用户而言，将会提供统一的访问API，这能够在创建智能合约和dApps时灵活使用任意系统，dApps可在运行中使用大量数据源。

6 结论

目前基于前沿区块链技术的综合研究成果以及密钥学和控制论的研发成果获得丰富经验，在此基础上设计了智能圈平台。得益于服务定向方式，智能圈建立了首个区块链生态系统，这是信息技术发展的新举措，将会改善每位地球居民的生活。