

不断发展



Noosphere
百度书



内容:

总结

1. 概念 3-4

1.1 一个新的区块链模式: Noosphere 区块链即服务 4

1.2 Noosphere 是基于面向服务的区块链分片 4

2. Noosphere - 高端区块链 5

2.1 定制安全性 5

2.2 容错 5

2.3 成本效益 6

2.4 遍布全球 6

2.5 适用性 6

3. 多功能 7

3.1 开发自由 7

3.2 采用速度 7

3.3 SDK - 软件开发工具包 8

3.4 区块链互操作性 8

3.5 服务生态系统 8-9

4. 构架与技术 10

4.1 面向服务的分片 10

4.2 分片技术 10-12

4.3 可扩展性和共识 13

4.4 区块链建块方法技术 13-14

4.5 英特尔软件防护扩展指令 15

4.6 软件防护扩展指令 - 区块链建块方法 15

4.7 服务间的交换 15-16

4.8 速度 16

5. NOOSPHERE FOUNDATION 17

6. 路线图 18-19

参考文件 20



总结

Noosphere Foundation提出了一个新的愿景，即现今区块链技术如何应用于各行各业的企业。Noosphere是一个专有的开发项目，它拥有一个现代区块链平台和一个名为异构蒲公英的全新生态系统。

Noosphere是一个以区块链为基础，面向服务的环境，旨在托管位于分片中的大量软件即服务。许多建立在区块链之上的创新解决方案相继在不断完善中，包括面向服务的分片、灵活的共识机制和服务间的交换使Noosphere与其他区块链相比下具有更多的优势。

Noosphere Foundation拥有其专有的区块链平台，为生态系统的用户提供一系列广泛的工具和服务，包括从分散的数据存储和计算能力到定制安全性和用Python编写的智能合约。此外，我们欢迎第三方开发人员能够在蒲公英生态系统中构建属于他们自己的服务，并且能够融入自己的加密协议和数字签名。

优先考虑信息安全：包括生态系统采用的特殊算法来抵御最常见的区块链威胁，如遭遇到Sibylla、Eclipse和51%的攻击等等。

特别关注的是该系统将第三方区块链解决方案整合到异构蒲公英生态系统的能力：这是通过一个开放的Noosphere应用程序编程接口和一组连接器接口来实现的，允许用户使用所有类型的加密货币进行交易。

Noosphere Foundation通过运营一个内部的技术中心去大力支持驱使异构蒲公英生态系统的发展，并鼓励第三方开发者通过创建他们自己的平台内软件服务来做出相应的贡献。



1 概念

Noosphere是云技术发展中新的一步，云计算为全球传统企业提供区块链即服务。尽管市场上有大量大型的云平台可供使用，并且其资源和服务的价格在不断地逐年下降中，但所有这些平台仍然是处于集中管理状态。自然而然地，其集中化无形中会带来许多问题包括：数据隐私、数据安全和对服务提供商的依赖，后者的严重程度会危及到所有企业的商业自由。

Noosphere是一个基于区块链与面向服务的分片式平台，旨在提供云服务和广泛的云计算能力之上。Noosphere平台整合了一个名为异构蒲公英的多区块链云生态系统，其中区块链技术和云解决方案可以被所有传统企业充分利用。

Noosphere创新的分布式构型为用户提供了突破性的企业云体验，如Azure、AWS和Google Cloud，这将会把可扩展性和数据安全性提升至一个新的高度。

Noosphere平台的能力可以帮助用户直接访问云计算、并且提供了一系列定制产品和服务的入口，它能够快速处理世界各地企业和公司所面临的一系列任务难题并且分析和处理大量数据、帮助公司建立内外沟通与创建业务应用程序等等。

1.1 一个新的区块链模式：Noosphere区块链即服务



并不是每个企业都有能力聘请专门的开发人员将最新的技术解决方案整合到公司的运营工作流程中的。这就是为什么今天的企业不仅需要一个区块链系统，还需要定制的平台和现成的服务，以便容易地嵌入公司的管理架构。

区块链的技术和意识形态发展是一个非常快速的过程，新版区块链更好地满足传统商业的当前需求。Noosphere区块链是迎合任何行业（包括金融科技、医疗保健、物流等）的下一代区块链，通过提供一个基于面向分片的服务的有价值的合作模式，很容易融入到当前真实业务的IT环境中。

Noosphere区块链即服务（NBaaS）模式使最终客户/客户和专业开发人员能够在测试阶段绕过任何资本成本，立即部署和测试基于区块链技术的解决方案。这种经济可靠的解决方案是基于云平台，允许公司使用最新技术进行交互。

在公司层面，区块链用作公用数据层，在其上可以创建新类型的应用程序。基于分散和数据可靠性的原则，应用程序允许降低成本和将欺诈风险减至最小限度。

随着Noosphere继续扩展其开发，新的基于云的分散式服务和应用程序将会出现，这将有助于优化SMB（中小型企业）运行的大多数日常流程。Noosphere的目标是持续改进托管跨平台DApps和服务的分散云生态系统。通过利用区块链的创新架构，所有实施的解决方案都将拥有无限的可扩展性和前所未有的安全性。上述优势在技术上是通过对改进当前的区块链和消除以前版本的区块链的遗留的问题而实现的。Noosphere优势是由特殊生态系统服务支持，确保前所未有的安全性（Loki和DDAP服务）和可扩展性（DAR & DDNS、ABG和PVM服务）。

1.2 Noosphere 是基于面向服务的区块链分片



Noosphere是基于面向服务的区块链分片，这项技术将为包括中小企业在内的企业释放无限能力，从而获得易于扩展、高通量的区块链。

多亏了Noosphere，区块链将会适应组织或公司的任何需求。无论区块链的内部规范如何，提出的概念的关键价值在于解决基础设施问题：可扩展性、兼容性和总体安全性。Noosphere为用户提供方便、高效的场地，用于区块链技术和智能合约的商业应用。



2 Noosphere - 高端区块链

2.1 安全性定制



处理业务关键型数据高度重视安全性和机密性。用户必须确保他们的数据不会在其不知情的情况下传输给第三方或以其他方式处理。如果数据集中存储在单个所有者终端，那么数据将成为工业间谍、黑客的目标，甚至可能引起政府组织的注意。

像其他在线信息系统一样，区块链是黑客的热门目标。除了作为最普遍的攻击类型的DDoS之外，我们知道有多种新的方法专门用来影响区块链平台：Sibylla、Eclipse攻击、51 %攻击和许多其他攻击。Noosphere在分析所有这些威胁和当前暴露现有区块链架构的缺陷后，能够为其子系统提供最有效和最积极的补救措施。

鉴于潜在的威胁，Noosphere配备最先进、最成熟的加密数据保护技术：secp 256 k1 aBLAKE 512，然而，考虑到使用X25519密钥、SHA256、Keccak 512实施ED25519，生态系统有很大的发展潜力。此外，Noosphere提供的算法确保广泛的灵活性，允许用户创建加密协议、数字签名，如果需要，还可以运行后量子密码算法。

2.2 容错



由于Noosphere的分散架构，Noosphere为分布式计算资源提供接近零增长的失效概率。在Noosphere平台中应用分散原则保证整个系统的高容错性：即使在单个节点完全或部分中断的情况下，系统自身仍可运行。

已对此进行了实验，结果表明，即使Noosphere 30 %的关键节点出现故障，也不会影响构建新模块的速度、共识机制以及区块链的任何其他关键特征。



2.3 成本效益



Noosphere平台是在Noosphere Foundation管理下所创建的，Noosphere Foundation是一个促进和支持自由区块链开发者社区发展的非营利组织。Noosphere开发的所有服务都作为共享软件交付给终端用户。与商用的集中式云服务相反，分散式解决方案维护硬件基础架构所需的开销要少得多，因此需要灵活且有竞争性的财务政策。

向Noosphere平台提供新服务的第三方开发人员可能会对其使用收费。所有平台内服务和应用程序都使用代币进行支付；在创建相关服务时，将被链接到主要的Noosphere代币上。也就是说，服务开发商独立决定财务政策：支付频率、奖金和特价。这种方法为最终用户带来超出想象的便利性，能够更有效地计划他们的开支，并在一系列支付计划中进行选择。

2.4 遍布全球



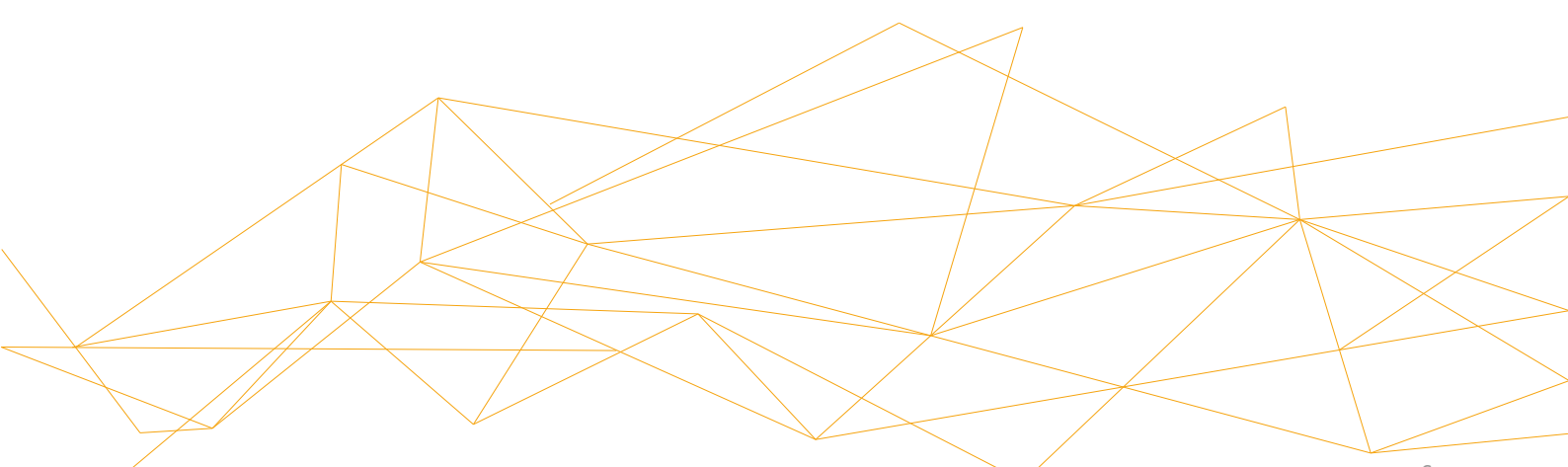
分布式分散架构使得Noosphere能够出现在世界的每一个地方。其他云服务供应商并不具备在世界各地部署数据中心的资源和能力水平，无法与Noosphere相比。

当创建新服务或使用现有服务时，开发人员或终端用户可以选择数据处理所需的资源、特定的存在区域中以及告知他们的数据应该存储在哪个地理区域里。

2.5 适用性



Noosphere平台不限制开发人员使用的工具和他们创建平台内服务时探究的应用领域。可应用区块链技术和智能合约的领域不计其数包括：金融、物流、医药、选举和其他数以千计的领域，在这些领域中，必须严格要求数据安全性和真实性。Noosphere超越区块链平台的传统用途，开发了一个智能合约向导和一个用于执行外部ICOs的工具包。





3 多功能

Noosphere创建一个开创性的架构——异构蒲公英生态系统。由于开放的设计和开发原则以及所使用的核心技术，Noosphere系统中的所有服务都有无限量的使用前景。

这个生态系统由一系列服务组成，这些服务已经投入使用或正在开发中，系统还将包括在Noosphere Foundation帮助下，由大量的三方开发的服务所承揽。

异构蒲公英生态系统为IT和区块链市场参与者提供使用Python智能合约构建自己的分散解决方案的大好机会。生态系统的灵活架构简化集成或构建新的软件服务，服务增效使其对第三方开发团队更具吸引力。默认情况下，这些团队及其服务可能会使用蒲公英生态系统的所有当前功能，例如分散数据存储或云计算。该系统能够理解各种编程语言和算法，因此，可以在区块链的每一分片中构建第三方应用程序。大数据处理、分布式神经网络、数据备份和存储系统、高性能计算只是Noosphere能为用户提供的一小部分。虽然Noosphere采用的每项服务都成为其不可或缺的一部分，但它与其他平台内服务交换数据，从而将Noosphere转变成一个成熟的分布式云生态系统，释放无限的可能性。

3.1 自由性开发



目前可用的云服务平台受到一系列功能工具的限制，这些工具往往不能满足消费者的需求。

Noosphere系统的核心和Noosphere Foundation开发的所有服务都是开放的，任何想研究和它们的人都可以使用。

自由社区对创建新的分散服务和应用程序的投入推动Noosphere的进一步发展，因此该平台对开发人员工具包没有任何限制。服务软件可以在任何平台上运行——Linux、Unix、Microsoft Windows、MacOS，并且可以用任何编程语言编写——C、c++、Java、Python、JavaScript、Go、c#等。

通过为异构蒲公英生态系统中的所有核心服务创建一个成熟的应用程序编程接口，这种灵活性已经成为可能。这意味着未来外部团队的服务将会在各个层面上提供且彼此交互：数据、事务、同步请求等。

3.2 采用速度



Noosphere测试网络拥有一个扩展工具包，用于在沙箱中测试服务，其中开发和采用的新功能几乎不费任何时间。内置的服务监控软件可高度定制且易于更改，同时也已考虑到监控系统负载和容错值。

应牢记最终用户更愿意选择易操作的解决方案。为此，Noosphere创建DApps & Services的NooStore——一个所有基于平台的解决方案的门户网站，也是开发者可以用来推广和销售其应用和服务的媒介。

3.3 SDK - 软件开发工具包



专门为Noosphere架构设计标准，以简化其上服务的开发。这些标准既方便又易于读取，包括应用到程序编程接口构建原则、服务到服务之间的链接、访问Noosphere系统核心、路由选择等。由于现有的服务种类繁多，这些标准包括了使用这些服务的通用机制，从而确保加速采用和运行。为了给第三方开发者一些指示，将创建Noosphere 开放性知识库，其中包含简短的指南和系统交互示例。

与所有现有云解决方案相比，Noosphere拥有一个额外的优势就是具备了一个多功能工具包，可供任何用户开发和实施新服务。每一项这样的服务一经开发，就成为扩展Noosphere能力的整体生态系统的一部分。所有创建的服务不仅仅是用户应用程序；它们是基于云的分散技术而实施，通过向最终用户提供服务，开发者可以将他们的研发产品货币化（有关服务生态系统的更多细节，请参见第3.5节）。

3.4 区块链互操作性



Noosphere创建一个相互操作的系统来解决区块链多元化和孤立的全球问题。由于不同的区块链之间没有通信，这项技术在应用领域受到严重阻碍。任何企业都不能脱离外部世界独立经营。与交易对手、合作伙伴、审计员和监管机构的互动要求企业在沟通方面有更大的灵活性。

Noosphere的服务的提供有助于第三方区块链整合的应用程序编程接口。此外，可以既方便又快捷地为关键集成创建网关。

在技术上，Noosphere的生态系统能够容纳所有第三方区块链。为确保使用的方便性和透明度，每个平台都可以通过特殊服务网关（连接器接口）访问，为用户提供统一的数据交换协议。利用这种方式替换惰性的集中式结构，允许来自不同业务环境的组织快速高效地构建优化的区块链解决方案，满足他们的需求。

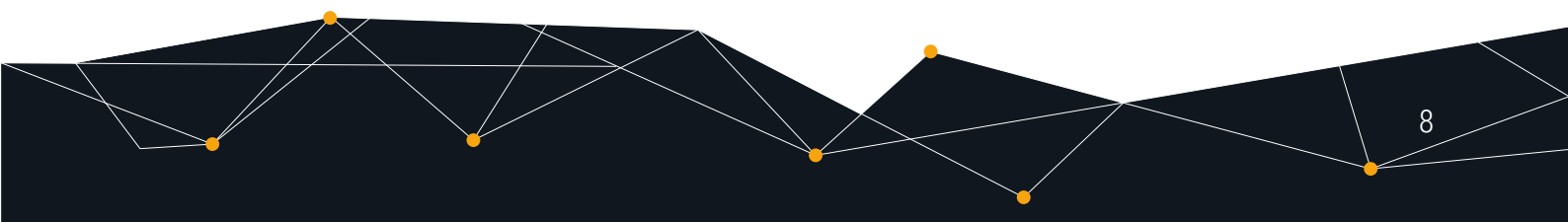
3.5 服务生态系统



在异构蒲公英生态系统中，Noosphere Foundation的开发者社区基于分散和安全原则创建了基本的关键业务服务。他们的目标是奠定坚实的基础，使得有关各方（包括开发人员的第三方团队、Noosphere社区等）开发出的更复杂服务能够运行。

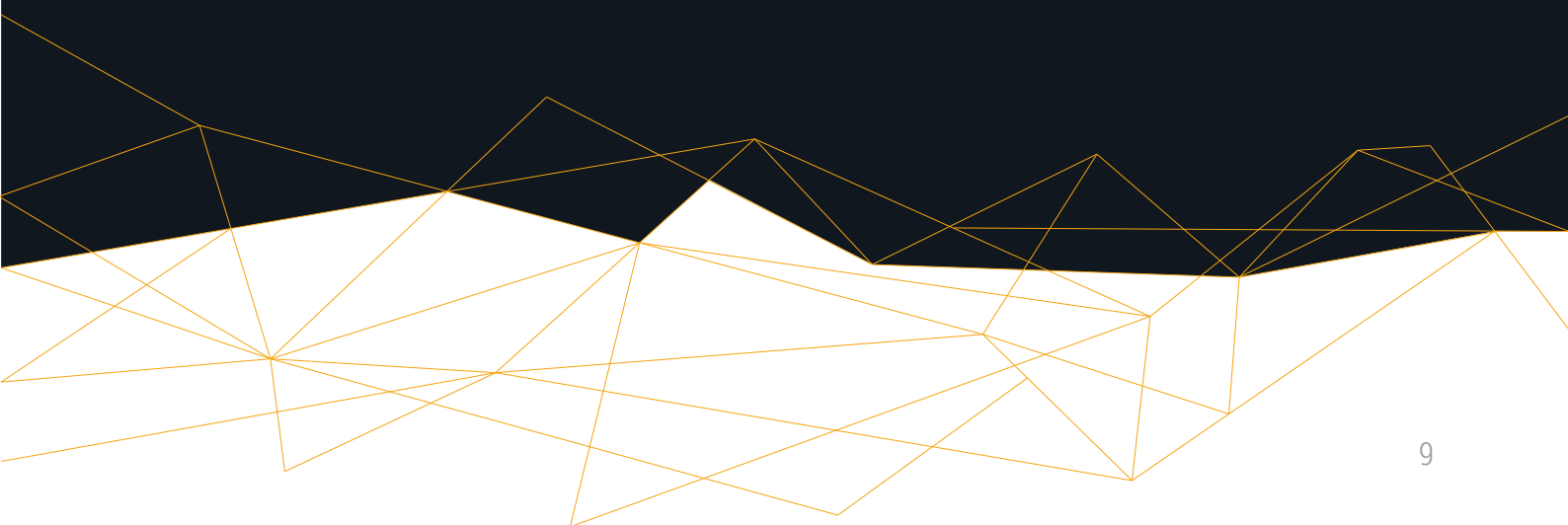
异构蒲公英生态系统是一个集成方案，由一组基于分散的区块链碎片的软件服务组成。Noosphere Foundation创建了核心碎片，支持生态系统的协同作用，并为第三方开发团队提供了一个快速启动模式。

生态系统的每个组成部分都是一个单独的服务性碎片，在与其他服务碎片密切相关的过程中可以独立于其他服务碎片的运行，反之亦然。整个生命周期中某个时刻，这样的碎片可以作为生成大量其他碎片的基础。





- 1 **DAR & DDNS** ——动态应用路由和动态域名系统——一项可确保负载平衡、数据流路由和IP级容错，并为应用程序提供集成的动态DNS功能的服务。
- 2 **NTM** - Noosphere 事务混合器 - 一种额外的事务动画服务，不仅可用于加密货币，还可用于传输机密数据
- 3 **DDAP** ——分散目录访问协议 - 一种提供LDAP功能的服务，安全性和容错性要求增强。
- 4 **ACS** ——自主版权系统 - 版权保护服务。
- 5 **Loki** ——一种针对DDoS攻击的保护服务，通过持续的通信信道监控和将通信量重定向到特殊节点，能够及时检测出威胁，以模拟攻击者的成功。
- 6 **EBS** - 有效备份服务——一种快速高效的数据备份服务，由于在传输过程中备份节点之间自动共享数据，因此与集中式服务相比，可以提高备份速度和快照生成速度。
- 7 **DHPC** - 分散式高性能计算——一项有助于将现有的计算任务和软件转移到Noosphere系统中，并适应分布式计算能力的使用，同时也参与此类计算的服务。
- 8 **PVM** - Python 虚拟机——基于类Python语言的虚拟智能合约处理机，包括每个内置模板中的智能合约设计器。此服务包含以下两种机制：基于模板编写智能合约，无需任何编程，或者使用Python语言编写的智能合约编程代码。
- 9 **ABG** - 区块链之门——一种模板服务，提供标准化的API来整合第三方区块链的运营。





4 构架与技术

尽管分散式区块链技术比传统的集中式系统存在很多优势，但也有一些弱点。主要涉及相对较低的吞吐量和可扩展性有限。一旦上述问题得到解决，区块链系统即可成功与中央平台进行竞争。

4.1 面向服务的分片



分片是Noosphere平台架构的核心。使用碎片的标准方法是单独处理事务，这些事务根据特定标准分布在服务碎片中。与其他系统相比，将大大提高系统的吞吐量和运行速度，其他系统中，区块链的单个副本存储在节点中。

Noosphere平台的每个碎片都是一个区块链，能够完全独立运行，不需要与其他碎片的永久连接。此外，碎片是系统的基本区块链。因此，Noosphere的基本复合单元是碎片。

Adam Efe Gencer在其针对区块链进行的面向服务的分片研究中首次提到了面向服务的分片的概念。这种想法的主要显著特征是使用碎片作为服务。

每块碎片代表一个独立的服务，执行某些规定的功能，并且能够与系统中的其他碎片共享信息。基于碎片的新服务动态添加到系统中，并扩展了系统范围的功能。除此之外，面向服务的分片可以轻松实现任一侧链，并以上述方式使用任一第三方区块链作为碎片。

4.2 分片技术



分片是一种划分水平数据的方法。可分为三个部分：

- 选择分片函数；
- 重新分片或重新分发数据；
- 数据路由（确定其物理位置）。

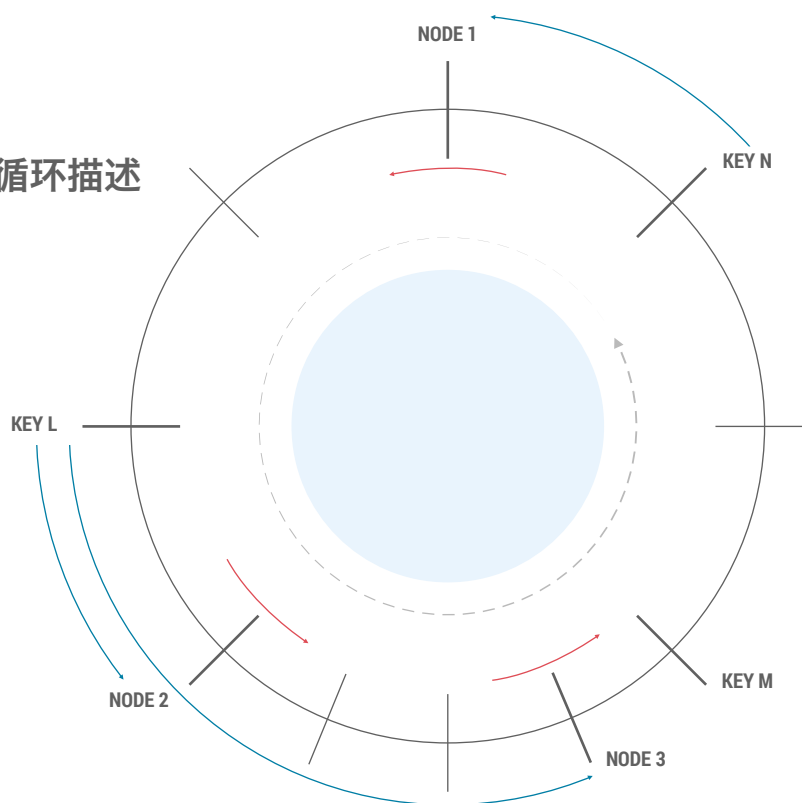
在其最简单的形式中，分片函数是 $f(x_1, x_2, x_3, \dots, x_n) = y$, x_n 是分片键, y 是碎片。

分片键的正确选择直接影响分片效率。这些键通常由多个可用节点和拥有数据的用户的ID组成。分片函数 f 是一种特殊的哈希函数。可以是一致性哈希或HRW哈希。

n 从 K 节点禁用时，所选函数的效率在数据重新分片时显而易见，而且数据必须在保持在线的节点之间重新分配，反之亦然，网络负载急剧上升，且必须生成新的碎片来实现负载分配。区块链平台上现有的分片方法忽略了这个问题的重要性，只选择哈希函数，因为网络负载是恒定的，所以不会认为随着时间的推移而改变最初选择的分片配置

一致性哈希是一种特殊类型的哈希，特征是调整哈希表时，只有平均的 $\frac{K}{n}$ 键必须重新分配，其中 K 是键的数量， n 是插槽的数量。相比之下，改变大多数传统哈希表中的插槽数量将导致几乎所有键重新分配。当活动节点的选择发生变化（增加/删除）时，通过一致性散列消除对重散列键的需要。相反，节点和数据的哈希键选择是在一个闭环中，随着新节点的增加，负载可以动态分配，而不需要再散列。HRW哈希是一个类似的函数，但它的功能更广泛，一致性哈希可认为是在特定情况下的一种特殊情况。HRW哈希还使用统一的哈希函数在圆圈中分配键集。与一致性哈希不同，HRW不需要任何预计算或键存储。将对象 O_i 置于 N 个节点 N_1, \dots, N_n 之一，计算 n 哈希值 $h(O_i, N_j)$ 并选择节点 N_k 于是产生哈希函数的最高值。如果增加一个新节点 N_{n+1} ，对象的新位置或查询将计算 $n+1$ 个哈希值并选择其中的最高值。如果将已经位于系统中 N_k 位置的对象与这一新节点 N_{n+1} 位置的对象进行比较，将重新加载并在 N_{n+1} 位置兑现。将来，所有客户都可以从这一节点，而 N_k 位置的旧兑现副本最终将被本地现金控制算法取代。如果 N_k 禁用，则其对象将均匀地重新分配给剩余的 $n-1$ 个位点。由于出租人放置安排的全局同质性，HRW算法的骨架式变体可以将对象放置时间从 $O(n)$ 缩短到 $O(\log(n))$ 。但如果 n 不太大，基本HRW的放置成本 $O(n)$ 几乎不会造成任何问题。HRW可完全避免与正确处理每个节点若干个键和相关元数据相关的所有费用和困难。

HRW哈希键的循环描述



n 非常高时，HRW算法的骨架式变体可以大大缩短对象放置时间。这种方法创建了一个虚拟层次结构，并通过在向下层次结构的每一层应用HRW来达到 $O(\log n)$ 的运行时间。第一步，选择常数 m ，并在 $c=n/m$ 碎片 $S_1 = \{N_1, N_2, \dots, N_m\}, S_2 = \{N_{m+1}, N_{m+2}, \dots, N_{2m}\}, \dots$

处形成 n 节点第二步，使用放置在虚拟节点T形树叶上的碎片创建虚拟层次结构，每个虚拟节点都有分支 f 。

附表显示了大小为 $m = 4$ 的碎片，骨架式分支 $f = 4$ ，实际总节点数等于128。

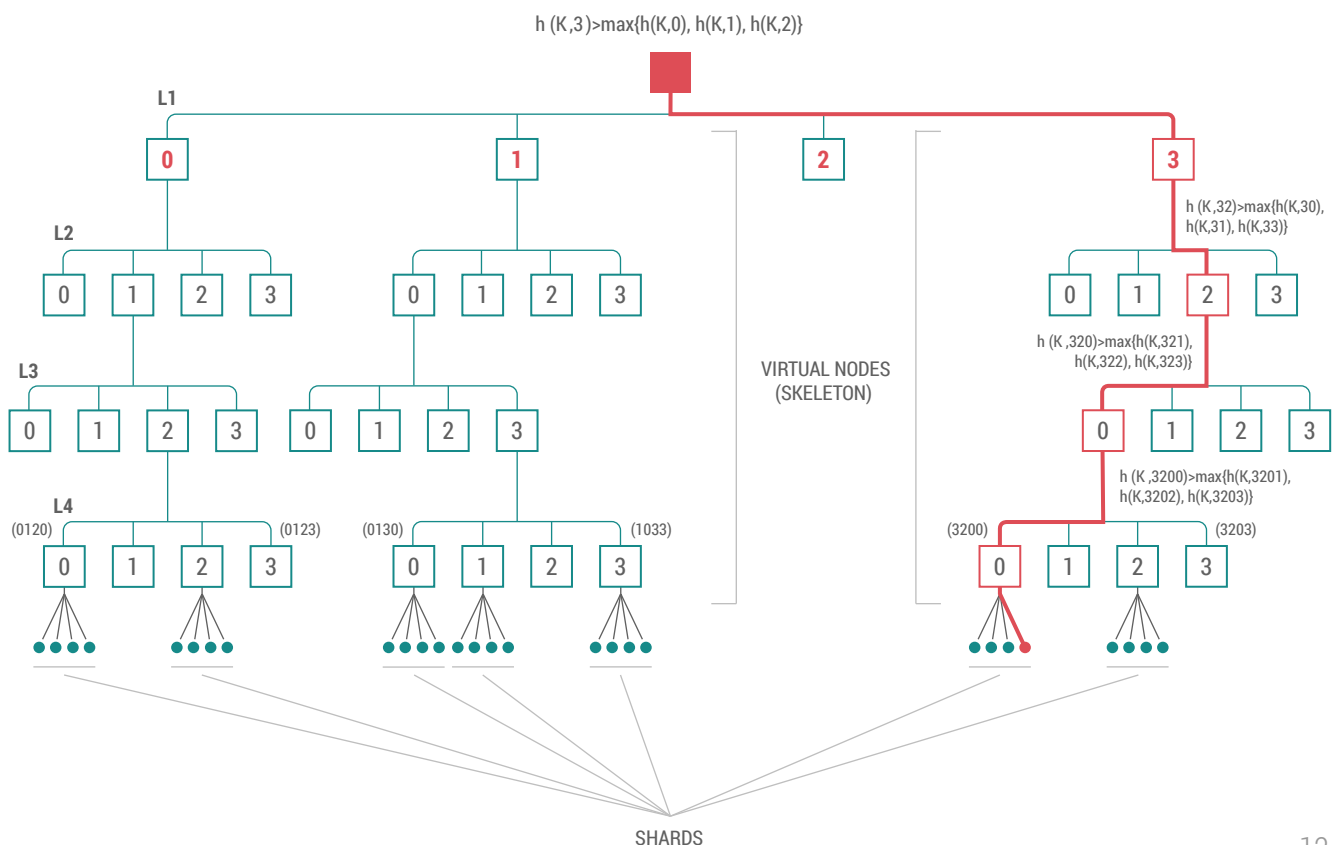
首先，我们可以选择32个最低虚拟节点之一应用HRW，而不是将HRW应用于所有128个真实节点。然后，将HRW应用于所拥有碎片中的四个真实节点，并选择获胜节点。我们只需要 $32+4 = 36$ 个散列，而非128个。

我们可以从虚拟层次的任一层开始，而不仅仅是从根开始。低层次启动需要大量散列，但如果出现故障，则可以改善负载分配。此外，虚拟层次结构不需要保存。可以根据需要创建，因为虚拟节点的名称只是加上 $base - f$ 前缀。很明显，因为 m 和 f 都是常数，T的高度 $h = O(\log c) = O(\log n)$ 。因为 f 是常数，所以每一层执行的作业为 $O(1)$ 。

对于每个给定的对象 O ，很明显，这种方法选择了每个碎片，从而以相等的概率选择 n 个节点中的每一个。如果选定节点不可用，则可以用传统方式在同一碎片中选择另一个节点。或者，我们可以在骨架中向上一层或多层，在同一层的虚拟姐妹节点中选择一个替代节点，然后到下层中的真实节点，如上所述。

可以基于诸如预期故障频率和预期负载平衡比等因素来选择 m 值。由于查找成本较高， m 值越高，故障时负载越低。

图 “最高随机权重哈希 - 骨架式”



数据路由问题也一样重要。它是向终端用户呈现数据和碎片之间数据交换速度的决定因素。最简单且效率最低下的方法是与客户一起存储路由表。但是这种方法剥夺了可扩展性。由于区块链体系结构的分散化，不可能使用单独分离的协调员和代理的变体。

因此，由节点系统自行处理数据路由。使得在对数时间 $[\log]_n$ 内找到所需数据源成为可能的最简单解决方案是让节点存储关于相邻节点和有限的一组不相邻节点的信息。因此，收到请求时，如果所请求的数据没有存储在当前节点上，则将请求发送到相邻节点（如果按住键）或者进一步发送到随机的不相邻节点。

4.3 可扩展性和共识



分片是Noosphere体系结构的基础。创建的每个服务都是一个单独的碎片，有自己的一组计算资源。服务碎片既能够自行独立存在，又能够通过划分它们之间处理的输入数据流来交换数据。

为了加速每个碎片内的数据处理，Noosphere Foundation开发了一种特殊的一致性算法——卷积BFT。核心的区别性特征是，当信息块出于共识在参与者之间进行分配时，能够有效地进行数据卷积。与以传统方式实现的区块链共识相比，每个信息块不是以其原始形式传输，而是以复杂形式传输，占用的体积相对较小并能够降低数据传输成本。

4.4 区块链建块方法技术



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则，并且完全是利用事件的泊松流构建。由以下事实决定需要分析输入数据流的分布规律类型和过渡期的长度，即后者可能占系统运行周期的相当大一部分，而输入数据流分布规律可能对系统输出参数的统计指标产生重大影响。一般而言，如果在未适当考虑非平稳期和输入数据流分布规律类型的影响的情况之下，则不会实现系统运行特性的优化。CBFT算法基于23个节点共识，其中每个节点（除了主节点）都是外部用户进入系统的入口点。每个节点都向其他节点发送数据。23个节点通过投票选出主节点（茎节点），该节点偶然选出区块链中下一区块的节点验证器。

验证器节点形成来自于输入事务的下一个区块，并将其发送给CBFT共识的其他参与者。每个节点都验证区块并使用自己的签名（EDS）投票。验证器节点使用计时器总结投票的结果，如果达成共识，则会将新的区块发送给主节点（茎节点）。重复循环直到茎节点和所有活动节点。那么共识参与者都因区块链平台的新选举而发生变化。

虽然CBFT算法使用了PoS原理，但是证明节点可靠性的证据是它们拥有Noosphere代币（NZT）。当在区块链平台开始运行时和在系统中定义验证器节点时，持有足够份额代币的代币持有者才在他们的第一选择时选择可信节点。

设想投票过程中共有N个候选节点，算法的重点在于从N个候选节点中选择23个获胜者 - M1、M2……M23。此外，我们还有代币持有者的W名投票人，他们可以将他们在Noosphere中的代币总数Y中X个代币投票给任一Mn候选。然后，投票分配的结果R（时间t）可以定义为：

$$R(t) = f(X, Mn, W);$$

$X > L$ 时, L ——投票的最小份额。

共识中选出 $M1 \cdots M23$ 节点是投票人 (W) 给出 X 个代币, 并由候选节点 (Mn) 接收时, $R(t)$ 函数最大化的结果。

$$X = > 0.15 * Y \text{时};$$

当前的CBFT算法仅从主节点 (茎节点) 开始, 这就是在下一轮才开始选择茎节点的原因。在共识的23个节点中选择主节点 (茎节点) Mo 使用相同的最大投票原则; 23个验证器节点每一个只能投一票。然后, 投票分配的结果 Rsn (时间 $t1$) 可以定义为:

$$Rsn(t1) = f(Mo, M1 \cdots M23);$$

禁止为自己投票, 每个节点在每轮选举中只有一票可投。此外, 为了避免平局, 还采用了决胜算法。

实际上, 随着时间的推移, 系统输入流强度并非恒定值。达成共识的过程中, 这些变化与候选区块在系统的活跃参与者之间发送大量邮件的期间和系统中请求处理的持续时间有关, 即, 对候选区块的分析, 包括当前验证周期的一组事务。

CBFT一致性算法的发展已经产生了一些统计信息, 反映了分配系统中输入数据流强度的变化, 取决于候选区块的分配时间、大小和处理持续时间。收集到的统计数据使用规定边界条件的分段多项式形式的插值三次样条 $S_g(t)$ 逼近, 即在每个区域 $[t_j, t_{j+1}]$, 编号为 j 的近似函数 $S_g(t)$ 都采用多项式形式

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

边界条件位于周期性条件, 即区间 $[T_1, T_n]$ 边界上一阶和二阶导数值的重合。样条构造相当于通过求解线性系统来确定一组系数 $a_i^{(j)}$ 。构建插值样条 $S_g(t)$ 以满足表列函数 y_g 的插值条件

$$S_g(t_i) = y_g(t_i) \quad i = 1, \dots, N$$

为了确定输入流数据强度在平均强度 λ 时对 $\lambda_g(t)$ 的特定依赖性, 得到的样条 $S_g(t)$ 应乘以平均强度, 再除以样条本身 $\overline{S_g(t)}$ 的平均值:

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

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

其中 λ 是输入流的实际平均强度。

所提出的输入流模型意味着请求 ξ 到达之间的时间是一个连续的随机值, 可以根据各种分布规律分配, 例如指数定律、泊松定律、正常定律或统一定律等。

泊松定律决定将流数据输入系统并分析候选区块的主要共识机制。其功能可能因主要因素而异: 网络活动、网络负载和服务间交互速度。

4.5 英特尔软件防护扩展指令



处理要求安全标准更高的数据（包括密码、密钥、个人信息等）时，Noosphere使用英特尔的软件防护扩展技术。这是目前市场上唯一能够在计算机中央处理器级别保护用户数据的技术。

相比之下，其他技术仅在操作系统级别提供保护，只能作为防范恶意行为的第一道防线。此外，当在不能使用卷积BFT或速度要求不高时，可以使用英特尔SGX技术实现特定的算法PoET和云计算。HyperLedger项目中证明一致性算法PoET是有效的。

4.6 软件防护扩展指令 - 区块链建块方法



对于具有极高攻击风险的关键服务，可以使用混合一致性协议SGX - CBFT。它的操作类似于前文描述的卷积BFT，但是由于采用了英特尔SGX技术，市场参与者还能够远程验证所有相邻节点。

4.7 服务间的交换




网络越宽，快速数据路由需求对数据传输的影响就越大。现有的通过互联网发送数据的协议，如OSPF、BGP、IGRP等，不适用于分散系统，因为它们基于现有的数据处理中心，默认情况下，对于分散系统是 unacceptable 的。

为了构建服务碎片的生态系统Noosphere架构，我们已经开发了Swift Torus路由协议。在很多因素中，它不同于现有的互联网数据路由协议，因为它能够与完全不同的实体并道一同运行，并且会当快速发送数据产生的需求时，动态节点之间的运作会成倍的增长。服务间有效路由的搜索算法基于包括拓扑结构、图论和排队论的研究，以及当代图形处理引擎都是最佳的实践，如Mosaic、Chaos、Giraph等。作为比较，对于四个Xeon Phi处理器，基于大约700,000,000个点的图形使用Hilbert排序切片方案进行路由计算需要一秒钟。

至于网络图设计，使用离散时间模型。在这些类型的模型中，网络拓扑变化表现为拓扑快照 S 的周期性重复序列，除以间隔大小 $\Delta t = T/S$ ，其中T指节点组拓扑状态的重复期间。将每张快照与图 $G = (V, E)$ 进行比较，其中V是一组节点，E是通信信道的数量。为每个有限图集 $\{G\}$ 初步计算周期t内重复出现的路由表。这些表分布在节点之间，并在需要的时间点 Δt 使用。

服务间交换（Swift Torus路由协议）采用的当前算法是使用OSI模型在传输层和网络层连接不同分片的简单且智能的方法。Swift Torus路由是异构蒲公英的核心系统之一，因为它使用上述方法即加快服务间的交换：又促使了快速数据快照和路由表的运行。

4.8 速度



标准和普遍接受的数据传输协议不能满足当今平台的需求。这不仅适用于分散的系统。集中式平台依赖宽带数据传输通道，而分散式平台则专注于新的一致性算法。这两种情况下开发都会受到限制，因为这些解决方案不能确保长期可持续性发展或无法满足不断增长的吞吐量要求。

Noosphere Foundation开发了一种全新概念的数据传输协议，有效地结合了TCP和UDP协议。称为UFT - UDP流传输。区块链的基本数据传输单元是事务。UFT旨在实现事务或具有预定结构的短信息消息的传输。这样，可用带宽可以100 %用于保证传输。



5 Noosphere Foundation

Noosphere Foundation是一个在瑞士注册的公共、自律、非营利组织。

我们的使命是通过结合科学进步与能源、技术和人力资源的可持续消费，开发和推广新的区块链技术。

NOOSPHERE FOUNDATION的主要目标包括：

- 促进和改进区块链技术；
- 发展和支持区块链开发人员的自由社区；
- 开发和维护Noosphere平台；
- 信息技术产业中的应用研究与开发；
- 支持和开发以生产可再生能源为重点的新技术。
- 通过使技术人性化和提高公众对区块链优点的认识，发展和普及区块链。

根据瑞士法律，非政府组织必须以完全独立的方式行事，因此在ICO期间筹集的资金只能用于组织。创始人与非政府组织运作不存在相关的间接或个人经济利益。

Noosphere Foundation的主要不同之处在于，它使用建立智能合同的技术来确保平台财务运营的透明度，使得项目从经济方面更具吸引力。

代币销售的收益将分配用于开发一个开放的区块链协议，随后用作分散的云区块链平台的基础。一部分收益将捐给Noosphere Foundation，以支持应用程序、工具和协议的生成，从而确保项目基础设施的开发。资金将进行分配以支持分散应用和服务的开发。

Noosphere Foundation负责Noosphere平台的开发和战略定位。Foundation拥有一个稳定的行政结构，确保区块链社区所有参与者之间的迅速沟通。其包括一个行政中心、一个技术开发中心和一个战略中心。

行政中心负责组织活动的一般事务，包括财务、法律和人力资源问题。其计划预算和编制财务报表，对项目进行尽职调查，监督运营所在国法律的遵守情况以及通常管理Noosphere Foundation的活动。

战略规划中心的优先任务是对Noosphere平台的发展前景进行管理和决策。其下属部门负责组织项目营销支持、确保社区参与者之间的沟通，并举办主题会议、研讨会和培训课程。

技术开发中心负责Noosphere平台的开发、测试和推广。其将为平台上的第三方服务开发人员提供咨询和工程支持。



6 路线图

本节描述了Noosphere平台开发的各个阶段，以及相关技术和主要服务碎片，这些碎片将成为生成新用户碎片的基础，并扩展其功能。

每个开发阶段都将使用开发人员的测试网向公众展示所取得的进展。

由于自由开发者社区也参与了开发，所以如果某一功能在某个时候存在优先重要性，将对此路线图进行调整。Noosphere平台的所有开发阶段都将在github.com公布。

根碎片和碎片设计器 - 2018年第三季度

- A. 茎节点和枝节点 - 允许在独立模式下启动茎节点和枝节点的基础功能。
- B. CBFT - 开发Noosphere平台的主要一致性算法。
- C. 节点API文档 - 节点交互界面文档。
- D. 区块链浏览器的Rest API。
- E. 区块链浏览器 - 平台主要监控工具的实现。
- F. 启动Noosphere平台开发人员的测试网。

NZT碎片和核心功能 - 2018年第四季度

- A. 并行事务执行 - 开发节点功能，以便并行处理整个输入流的事务。
- B. UFT - 开发一种网络协议，侧重于分布式分散网络中的事务处理，以提高平台操作的速度。
- C. Swift Torus路由 - 开发一个Swift Torus路由协议来加速碎片之间的数据同步。
- D. SPI - 碎片编程接口 - 开发Rest API以统一碎片之间的数据交换协议。
- E. NZT碎片 - 开发Noosphere平台碎片，实现了NZT硬币的主要支持功能。
- F. NZT碎片的Rest API - 开发一个接口访问NZT碎片。
- G. 茎节点和枝节点全功能的实现。

III Noosphere测试网 - 2019年第一季度

- A. 在公共接入中推出Noosphere平台的测试网。
- B. PoET - 基于英特尔SGX技术的附加一致性算法的实施。
- C. 基于英特尔SGX和CBFT的一致性算法的实现。
- D. PoD - 事务类型的实现 - “按需付款”。
- E. 在PoET&SGX - BFT一致性算法上公开展示Noosphere平台的运行速度。
- F. 碎片设计器 - 在Noosphere平台上设计和创建新碎片的工具。

IV Noosphere服务 - 2019年第2季度

- A. Noosphere平台主网的启动。
- B. Noosphere - 实现存储, 用于访问在Noosphere平台上创建的服务。
- C. NTM - Noosphere事务混合器
- D. PVM - Python虚拟机和智能合约设计器
- E. 碎片设计者的文档编制 - 碎片设计者的文档。

V Noosphere服务 - 2019年第四季度

- A. DAR和DDNS - 动态应用路由和动态域名系统。
- B. DDAP - 分散式目录访问协议。
- C. ACS - 自主版权制度。
- D. Loki - DDoS保护服务。

VI Noosphere服务 - 2020年第一季度

- A. EBS - 有效的备份服务
- B. DHPC - 分散式高性能计算
- C. ABG - 任一区块链门



如果您有任何疑问, 请参阅技术WP (链接)

参考文献



Bitcoin - NG: 可扩展的区块链协议, Ittay Eyal、Adem Efe Gencer、EminGünSirer和Robbert Van Renesse, 第13届Usenix网络系统设计与实现大会论文集 (NSDI 2016) 。

M. Castro和B. Liskov, “实用拜占庭容错”, 第三届操作系统设计与实施研讨会论文集, ser.OSDI '99.美国加利福尼亚州伯克利: USENIX应用, 1999, 第173 - 186页。

Chain Inc.区块链开放标准: 用于大规模金融网络的安全区块链协议。 <http://chain.com/os/>, 2016年9月检索。

CoSi: 保持当局“诚实或失败”和分散见证连署保证, Ewa Syta、Iulia Tamas、Dylan Visser、David Isaac Wolinsky和Philipp Jovanovic、Linus Gasser、Nicolas Gailly、Ismail Khoffi和Bryan Ford, 第37届IEEE安全和隐私研讨会 (SP 2016) 。

Elastico: 开放区块链的安全分片协议, Loi Luu、Viswesh Narayanan、Kunal Baweja、Chaodong Zheng、Seth Gilbert、Prateek Saxena、ACM计算机和通信安全会议 (CCS 2016)

A.Efe Gencer, R.van Renesse, E. Gün Sirer, “面向服务的区块链分片”计划, 用于加密货币和合同 (IC3) 康奈尔大学计算机科学系, 2016年。

L. Luu、V. Narayanan、K. Baweja、C. Zheng、S. Gilbert和P. Saxena.开放区块链的安全分片协议。2016年奥地利维也纳计算机与通信安全会议。ACM.

PBFT: 实用拜占庭容错和主动恢复, Miguel Castro和Barbara Liskov, ACM计算机系统事务 (TOCS), 第20卷, 第4期, 2002年11月, 第398 - 461页。

F. Amirjavid和H. McKeck.面向服务的分布式计算, 第二届IEEE软件技术与工程国际会议论文集 (ICSTE 2010), 美国波多黎各圣胡安, 2010年10月3日至5日。