KardiaChain – The First Decentralized Interoperable and Self-Optimised Blockchain Ecosystem

区块链(Blockchain) 技术提供了前所未有的去中心化(decentralization)和交易透明度， 并在性能和跨链之间做出权衡。在不久的将来，我们相信区块链提供的解决方案，尤其是智能合约(smart contract), 将帮助人们在所有的日常活动中轻松地达成协议与合作，并不需要相互之间先达成信任。但是目前实现这个目标的方法倾向于取代其他区块链项目，或者要求这些区块链项目根据标准进行大规模地修改。KardiaChain 使用了“求同存异”的方法，专注于为用户和开发人员构建简单易用的解决方案。KardiaChain 开发了一种无创性解决方案 --- 双网络主节点(Dual Master Node) (简称为双主节点)， 使得现有的区块链以及未来的区块链之间实现交互。KardiaChain的终极目标是创建一个统一的生态系统，开发人员可以轻松创建能够在许多不同区块链上运行的智能合约(Smart contract) 。此系统可以大大降低成本，减少网路拥堵的现象，并在不需要信任的前提下, 通过智能合约在多个区块链系统之间实现安全的通信。

I. KardiaChain *的哲学*

KardiaChain 认为下一个新阶段很快会到来，人们将通过区块链技术，尤其是智能合约(smart contract)来帮助人们在所有的日常活动中轻松地达成协议与合作，而不需要当事人双方事先建立信任作为前提。

许多区块链项目的当前做法是完全取代旧的区块链系统并让自己成为一个多方位集成的系统。与这些项目不同的是，KardiaChain 团队希望在现实世界中以不同的方式发展。就像互联网连接了许多内部局域网络而形成一个大型网络，我们对区块链网络的设想是许多公有链和私有链之间的链接。每个区块链都为了达到特定的目标而具有独特的设计，人们应该充分利用每个区块链各自的特性。

因此，应该有一个能够利用和优化区块链系统优势的智能生态系统解决在区块链之间的互操作性(interoperability)和独立性(independence)问题。我们将这个智能生态系统视为一个人体：每个区块链系统都是一个器官，KardiaChain 是人的心脏，它根据需要以一定的速率支持血液的流动（例如：交易）。

虽然有很多项目旨在解决区块链之间的交互问题，但它们都需要这些区块链系统在底层上做出改变或要求这些系统以某种模式进行集成。

相比之下，KardiaChain 使用了一套独特的方法，可以简单快速地在区块链之间建立链接， 而无需对各个区块链底层进行更改。
KardiaChain 追求“求同存异”的方法，专注于从用户和开发人员的角度进行简化。

我们很自豪地介绍 KardiaChain 的跨链智能生态系统，并且我们每天都在努力地工作使其适用于绝大多数的区块链系统。

II. *项目背景*

A. 单链

区块链技术提供了前所未有的去中心化(decentralization)和交易透明度，并可以在性能和跨链之间做出权衡。对于大部分的单链，主要目标是提高系统的可扩展性 (Scalability), 即提高交易处理速度(TPS)。 现在最常用的方法之一是分片。其目的是把区块链系统分成几个小块(子链) 并同时处理每个部分/链上的交易， 这种方法可以实现每秒处理数百万次的交易。但是，即使基于上述理论的预估，没有任何单一的区块链项目能够达到所需的速度和性能。比如，我们在 Facebook 上的主要互动需要每秒处理 16,000 笔交易，因为每分钟都有 510,000 条评论，293,000 条新状态更新和 136,000 张照片上传。Instagram 一天有 40 亿个点赞意味着在 1 秒内有 46,000 个点赞（TPS）。在 Youtube平台上，如果 1 天 内观看了 100 万小时的视频，意味着在 1 秒内处理了近 700 万笔交易 (假设在用户的YouTube 访问期间每 6 秒访问一次视频信息)。

阻碍交易处理速度的原因是区块链以单链的形式运行，它们无法相互沟通，因此，计算处理过程不能在许多区块链上同时运行。缺乏区块链的互通性会

阻止很多企业在区块链平台上找到解决自己问题的方案。例如，有许多区块链系统支持智能合约，但每个区块链都有自己的处理性能。举个例子，比特币网络甚至都不支持智能合约。这意味着，很难有一个单链可以处理企业遇到的所有问题。由于没有适用于所有应用的简单解决方法，导致学习在许多不同的区块链上运行智能合约变得非常困难。

B. 跨链

1) 多维区块：

如果我们将单链视为一个计算机或本地网络，当许多这些计算机连接在一起并共享数据处理请求时，处理性能将变得更高，而不是只使用一台具有高处理速度的超级计算机。在这里，我们使用多维区块的概念，以便更容易地理解当今扩展区块链性能的方法。

X 轴= 水平复制=交易方向: 数据同时存储在多个节点(nodes)上以尽量减少拥堵。

Y 轴 =功能扩展=不同的区块链处理不同的要求: 这意味着每个服务使用单独的数据库。因此，某个区块链上的拥挤不会影响其他区块链处理交易的能力。

Z 轴 =数据分工=在多个区块链之间共享数据处理需求(例如，分片算法): 同时在多个节点上运行相同的代码副本以分担工作负载。

目前，许多单链都在寻求的解决方案是通过应用分片算法专注于扩展 Z 轴。比如以太坊2.0就专注于使用分片技术。我们的目标是扩展所有三个维度，重点关注 X 和 Y 轴同时利用生态系统中其他区块链的分片技术。由于跨链技术，区块链之间可以合作完成工作，实现了 X 轴的扩展。如果按照 Y 轴扩展，我们可以将工作拆分为更小的操作并在许多不同的区块链上运行。这就是 KardiaChain 带来的跨链互联优势。

2) 相关研究：

虽然许多项目都声称要开发区块链之间的跨链技术，但是每个解决方法都对区块链提出了修改的要求，以便可以与通用标准集成，甚至需要对区块链进行分叉（软分叉或硬分叉）。尝试对区块链系统结构做出更改可能会导致两个主要后果：1) 对旧区块链进行硬分叉来以满足集成要求; 2) 当着力改变如上所述的区块链系统结构时，可能会带来安全问题。

接下来，我们将分析目前使用的一些常用的跨链方法。

a) *侧链* (Sidechain)

侧链是一个与主链系统并行运行的区块链系统，使用作为一种方法以增加主链的功能通过区块链的互连能力。该系统允许在两个区块链之间以去中心化的方式交换和转换加密代币。换句话说，你可以将加密代币转移到侧链， 然后切换回主链。

侧链经常遇到的问题就是你想要从主链转移到侧链（反之亦然）的资产将会被锁定一段时间，称为参赛期(contestant period)，然后才能交易。虽然这个使用侧链的想法在 2014 年已经被提出，但到目前为止，没有太多成熟的应用程序使用侧链。

b) *消息传递层*(Message layer)

这个消息传递层被设计为从外部区块链接收数据的中介部分。每个交易将视为一条信息要求系统创建一个单独的分层以按顺序过滤并对这些信息进行排序。简单地说，当这些信息在记账前需要通过网络的筛选。此过程可能会影响网络性能。我们认为， KardiaChain可以直接从外部链中选择重要数据通过区块链交易不可改变的性质删除这不必要的一层。

c) *电源模块/ 连接模块/ 转换模块*(Hub/Connector/Adaptor)

电源模块设计作为每部分区块链之间的通信通道。通过它，这些区块链可以相互交互以交换资产。使用这一方法的著名项目是波卡。这个方案遇到的关键问题是每个区块链需要与电源模块进行同步才能实现跨链交互，这意味着现有的区块链必须更新才能加入该系统。换句话说，电源模块不与区块链系统集成。相反，需要区块链系统与它集成在一起(Confusing

sentence)。在我们看来，这种方法是一个违背交互操作定义和实际应用的例子。

3) KardiaChain *的“求同存异”方法*

简单来说，KardiaChain与其他区块链集成方法。我们最大的目标是提供一个实用的系统， 准备投入运行并确保满足以下要求：

· 不改变区块链系统的前提下实现集成，包括从解决方案的设计到实际应用的操作过程。

· 保持区块链各自的特性和它们自己的共识机制。

· 为 Dapp 开发人员考虑，KardiaChain负责处理跨链业务，同时仍然为开发人员提供设计和构建自己想法的能力。

III. KardiaChain *的解决方案（申请专利中）*

为了解决可互操作的挑战以及提高区块链系统的性能，KardiaChain 旨在提供一种同步基础架构，其中应用程序可以通过区块链链接功能在不同的区块链上运行，同时简化开发人员的开发流程。KardiaChain的技术亮点之一是允许用户激活一个区块链上的交易，但其交易的结果可以在另外一个区块链上出现。

KardiaChain 是一个区块链生态系统，链接区块链和应用程序。该项目的目标是创建一个同步的生态系统，其能够集合其他区块链上的优点，为大家将来广泛使用区块链技术铺平道路。
KardiaChain 使用的主要工具是双网络主节点(简称为双主节点) 包括 3 个主要部分： 翻译模块， 协调模块和聚合模块 (Translator, Router，和 Aggregator). 这些工具提供了实用性，非侵入性(non-invasive) 让区块链链接能够在安全和去中心化的环境中运行，从而降低了成本并提高了处理速度。

A. 技术优势

KardiaChain 的解决方案在以下技术方面进行了改良：

· 定向交易的接近算法最大限度地降低了成本并提高了处理速度。

· 同步智能合约系统在术语方面增加了广泛扩展的能力。

· 区块链系统之间非侵入性的解决方法：如果你想在 KardiaChain 的生态系统中进行交互，它将提供向后交互并且不需要改变其他区块链。

· 有效的实际应用

· 安全和去中心化

B. 重要部分：

- ***双主节点***可以依次访问两个区块链系统(KardiaChain 和一个可选的区块链) 总帐的数据。此双主节点可以从外部区块链系统接收交易并安全地将其更新为 KardiaChain，而无需从两个区块链中更改任何内容。双主节点实现了分散性，因为任何人都可以运行(没有分散/permissionless) ，还有双主节点之间存在共识机制以确认每个区块链系统的数据。双主节点非常安全，因为来自 KardiaChain 的区块链之间的所有交易数据是不能造假的，它们受多重签名功能的保护，例如 Schnorr 加密签名系统。
- ***翻译模块*** 将优化智能合约系统和在不同的区块链上同步 Kardia 的语言 (Kardia unified Smart contract language KSML)，打破智能合约之间的编程语言障碍，并在 KardiaChain 和外部区块链系统之间建立“共识”。
- ***协调模块*** 将确定哪个区块链系统最适合将用户请求移动到该区块链并加以处理，协调模块可以根据已定位交易的数据提高在特定时间执行系统交易的能力，交易费，交易完成的时间和容量。
- ***聚合模块*** 将从部分区块链总结更新以减轻 KardiaChain 的压力。以上部分之间的协调将为区块链系统创造无限潜力，并为全球区块链技术打下坚实的基础，以便普及在日常应用中。

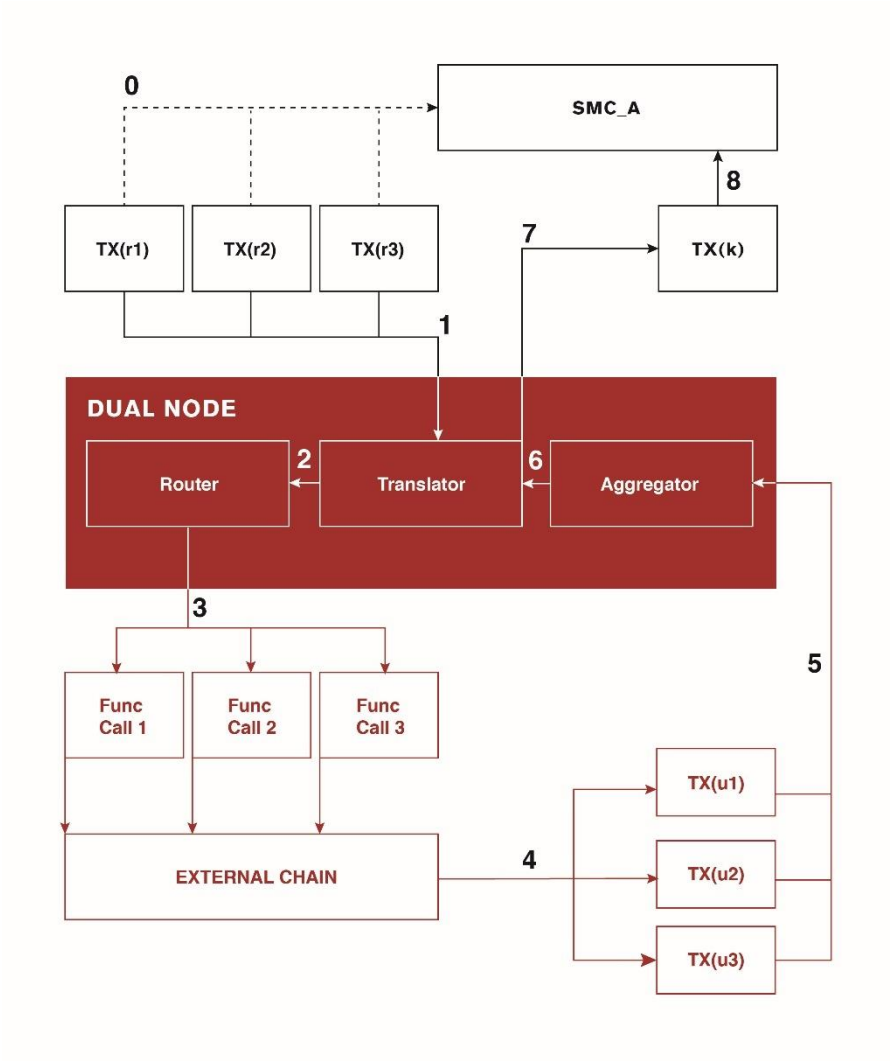
Chart

- **第 0 步**：用户激活交易 TX(r(i)) 与 i=1,2,3 以使用智能合约 SMC_A
- **第 1,2 步** 协调模块和翻译模块将定位交易并处理它
- **第 3 步** 双主节点执行命令 Func_call(j)与 j=1,2,3 以针对外部的区块链系统
- **第 4 步** TX(u(l)) 与 l=1,2,3 的结果从外部区块链转移到双主节点
- **第 5 步** 双主节点可转换 TX(u(l)) 结果回归外部区块链系统的标准
- **第 6,7 步** 聚合模块和翻译模块将执行单个交易 TX(k)=[value:(1,2,3)]

- **第 8 步** 更改（1,2,3）在 SMC_A 进行并记录在总账

如上所见， Kardia 的新处理方法允许我们综合所有部分区块链的交易绩效并在 1 秒内重新定义交易处理速度的概念 (TPS)

$$\text{KardiaTPS} = \sum_{i=0}^{n} K_i + \min(R, E, K_i\, t) \times \left(1 - \frac{1}{t}\right)$$



Ki: Kardia 可以实现交易处理性能 (i=0)

Ki: Kardia can achieve transaction processing performance (i-0)

R: 从部分区块链交易中获得的交易性能(i=1,...,n)

R: Transaction performance from some blockchain transactions (i-1,...,n)

E: 双区块的路由能力

E: Two-block routing capability

t: 区块的组合比率

请注意，当越来越多的区块链获得 KardiaChain 的支持，t 和每个区块链的Block_Size 和Block_Time将会改变。具体地，t 的范围从 1 到绝对值。

(1…)是所有部分区块链的组合

*t=1 是仅 1 个交易/命令被发现和处理的特殊情况，导致对 Kardia 的单一更新，因此组合为 1

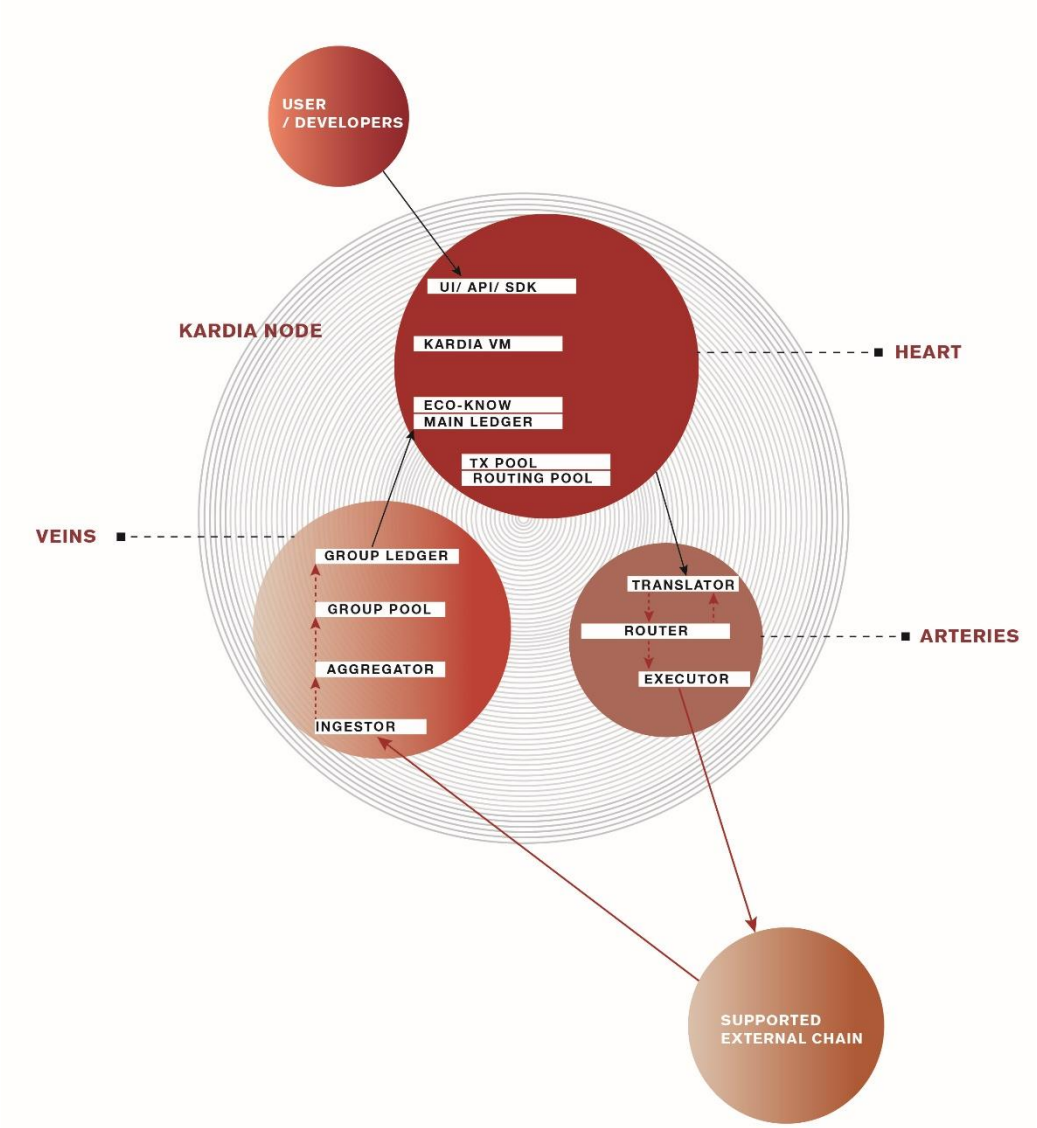
$$t_{\max} = \frac{\sum_{i=1}^{n} TPS_i}{\sum_{i=1}^{n} \frac{1}{\text{Block\_Time}\, i}},$$

IV. KardiaChain *的技术*

A. 网络节点的部分

为了更清楚地描述，我们将节点的结构分为 3 个部分，如人的生物器官结构是：心脏，动脉和静脉。双主节点直接使用这 3 个部分来维持区块链之间的链接。心脏的性能是存储交易并通过动脉转移交易到成员链，这些交易将会通过静脉转回 KardiaChain。如果出于任何原因，做出选择的节点将不会在链接区块链的生态系统，它只会使用心脏部分并成为能够处理源区块链中交易的标准节点。

1) 心脏



a) Kardia *的发展工具：*

Kardia 的目标是简单化学习其他区块链系统的其他智能合约结构的过程。为了简化学习Kardia 智能合约的结构，我们将提供一组 UI，API 和SDK。这套工具被称为引导系统，可以使心脏持续运行。

· 用户友好的 UI 系统将提供模板以建立 Kardia 的智能合约。该模板将帮助缺乏经验的开发人员或掌握智能合约编程语言的深入知识（Confusing）可以自行决定更改合约的更多细节。

· 高性能的 API 将直接构建更复杂的 Kardia 智能合约。该工具面向更专业的开发人员，允许他们同时在多个区块链应用部署任何类型的逻辑应用。

· 高性能的 SDK 允许 Dapp 的开发者随意研究和调整 Kardia 智能合约中的所有细节。SDK 允许程序员完全控制 Kardia 智能合约的所有相关活动： 从在外部区块链中创建附录合约的能力， 到随意更新新信息的方法，所有都将由程序员自由选择。

b) Kardia *的虚拟机*(KVM)

Kardia 虚拟机 是以太坊虚拟机的升级版，更集成了区块链之间的操作功能。在 Kardia 虚拟机上运行的智能合约可以从部分区块链处理外部交易并在 总账记录而不需要改变Kardia 的共识机制。

Kardia 虚拟机维护两个收费系统，分别在主链的交易和侧链的交易。适当的收费机制将适用于连链交易以鼓励部分节点在处理连链式交易时更加活跃 为了确保整个系统的顺利运行。

Kardia 虚拟机还支持一组特殊工具帮助管理与处理相关的连链交易，并总结来自外部字符串的更新

c) 生态系统的智慧(EcoKnow)

EcoKnow 存储 Kardia 正在链接的区块链系统指数。EcoKnow是帮助 Kardia 胜过其他系统的部分，它提供大量信息帮助 Kardia 通过智能算法为面向交易的机制提供出色的解决方案。除了交易更新，参数更新也将立即收集和分析。 EcoKnow 将这些参数压缩并存储到综合数据点中并允许生态系统使用它们来提供最佳选择。 EcoKnow 被认为是整个系统的知识来源, 甚至新的网络节点也可以访问它以获取整个系统的信息

d) *总账*

总账存储在所有节点上（标准节点和双主节点）并包含主链的数据(阅读更多关于块的结构以便更好地理解). 当每个主链保存一条指令到从双主节点生成的二级分类帐时，总账结构化为树状结构。总账显示了 Kardia 虚拟机的一般状态，其中任何在 Kardia 和外部区块链的交易将都改变总账的状态。总账的目标是提供系统历史数据的连续概览而不在乎哪个区块链系统执行任何交易。

e) *主钱包*

主钱包是一个安全的地方，用于存储具有高保密性的用户资产。它还允许用户执行跨链交易并且无需为每个区块链拥有多个个人密钥或公钥。

2)　动脉

动脉允许交易从 Kardia 顺利流向其他区块链同时确保跨链操作无缝完成。这是一个多步骤的过程，其中有翻译模块和协调模块之间的双向交换，以及通过处理模块的 smc 命令

a) 翻译模块

翻译模块使用算法转换可用的 Kardia 智能合约成一个二进制码的编译器包含与部分区块链匹配的 SMC，以升级 Kardia 的智能合约并处理部分区块链上的错误。

b) Kardia *智能合约语言系统*(KSML)

KSML 旨在成为程序员的有效工具。在 Kardia 系统上建立智能合约，并且无需大量的知识或深入的编程经验。通过提供由基本语言系统（比如 JSON 和 YAML）组成的全面的综合编程指南，程序员可以轻松构建自己的想法而不需要使用特定语言来编写某个区块链的指令（例如，以太坊需要 Solidity 或Neo 需要 C＃，Java 或Python 以及许多其他语言）。

与 KSML 语言并行发布是测试应用程序帮助程序员可以快速检查和验证他们刚刚构建的智能合约是准确的，并在 Kardia 平台上顺利运行。KSML 和工具将集成到 SDK 中为程序员提供一套完整的工具，让他们在 Kardia 上自由构建产品。

将来，我们的目标不仅是支持 Kardia 智能合约语言系统，还允许开发人员为每个区块链上安装特定的编程方法(例如，以太坊智能合约的 Solidity). 这一发展将消除障碍并允许程序员在 KSML 提供的所有语言和逻辑系统中构建解决方法

c) *跨链研究机模块*(CMNR): Cross-chain Machine-learning Network Router

跨链研究机模块使用基于 SON 的选择算法为了找到最合适的区块链参与跨链交易过程。选择算法基于许多因素，包括成本，确认时间，每条链上

的交易金额。该模块使用灵活的分级算法，从最好的分析结构建造，为了确定交易R 在时间t 的一区块链 X 的总点数如下：

ScoreXt = f(h,f,v,d)

h: 块的高度

f: 记录最新交易的成本

v: 时间形成一块X

d: 难度指数是根据智能合约的难度差异计算出来的
如上所述，从 EcoKnow 直接连续获取数据量，跨链研究机模块能够在智能合约的指导下做出有效决策，能够在智能合约的指导下做出有效决策，从而实现最高性能和竞争性运营成本。由于能够自动化管理和自动优化，所有更改和升级到SON 的关键算法无需人工干预即可自动部署。

跨链研究机模块将有两个表面层：内部表面是 JSON-RPC 应用程序编程表面提供节点的定向功能以指示 Kardia 的交易， 外部表面或称 RESTful 应用程序编程表面允许程序员为他们的智能合约获得最有效的方向

d) 处理模块

处理模块负责计算最少的部分那就是上传智能合约的 二进制码编译器，按照 CMNR 的详细说明，通过相应的 JSON-RPC 到目标区块链。

3) 静脉

静脉负责收集生态系统的更新，有效地处理它们并安全地将它们发送到总账。静脉有如下几个部分：

a) 吸收模块

吸收模块从特定区块链系统，双网络主节点发送信息的地方，获取新区块。相关更新将被压缩并实时发送到聚合模块。

b) 聚合模块

聚合模块从吸收模块接收在线更新，并将：

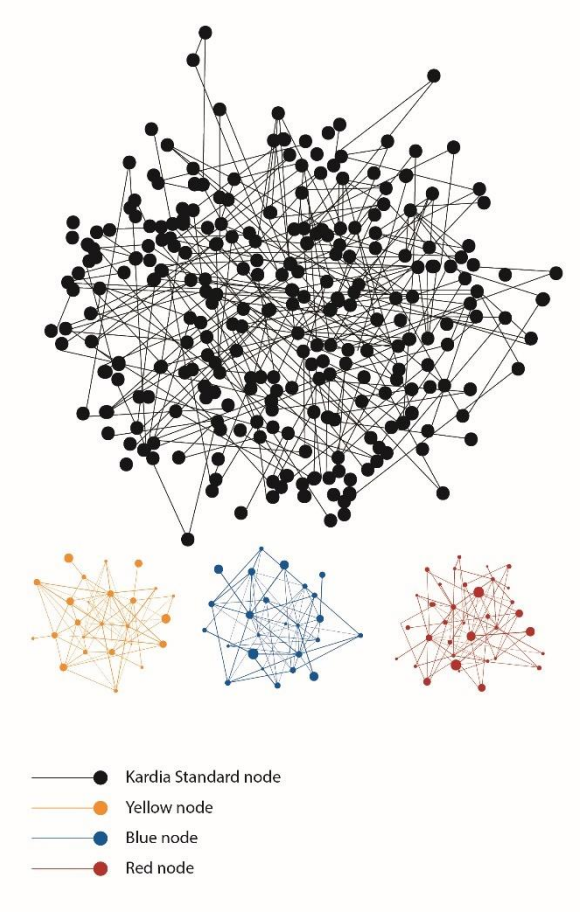
(1) 把定向的交易和来自外部区块链的标识号序列合起来

(2) 总结一系列可以相互集成的交易成 Kardia 的新交易并将把此交易发送到交易结合地方

c) 组合和分组账

(Group Pool and Group Ledger)

交易结合地方是双主节点收集定向交易的地方以在下一个块处理。分组账记下这些交易。重新阅读“块构造”部分，以了解有关分组账如何连接到总账的更多信息。

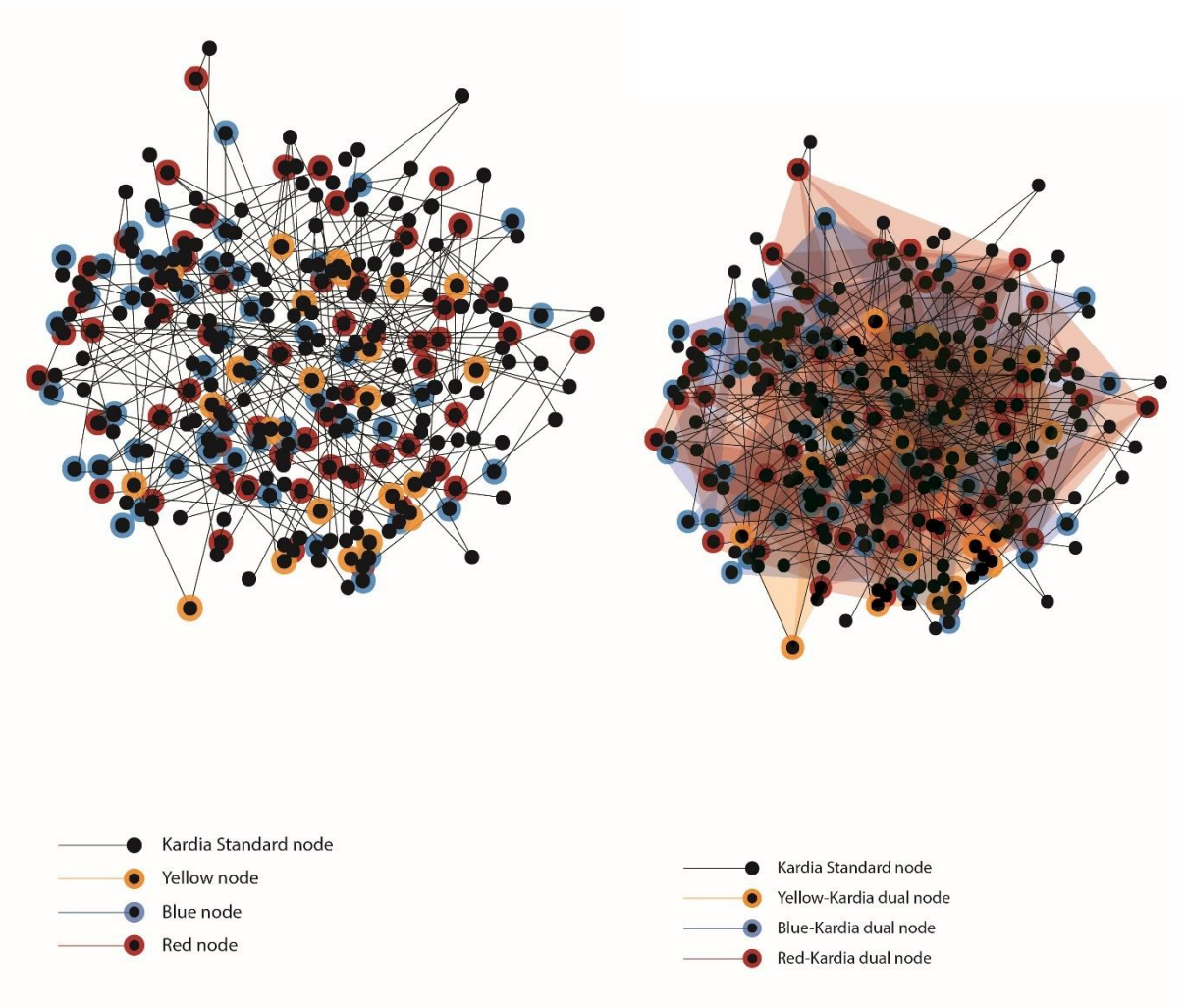


B. 系统机构

所有加入了系统的新节点将默认为标准节点。他们可以存放主代币成为双主节点以及帮助选择一个外部区块链。根据组合运行的双主节点支持类似的区块链。需要注意的是，有时双主节点仅附加到特定的区块链。这是因为，对于一个单节点，同时处理多个外部区块链的性能是无效的，也是不可行的。关于多链节点的可行性，未来还需要进一步研究。

下图显示了同一组中的双主节点，它们之间的距离很远的，因为每个节点

选择一个区块链来任意支持，整个系统将定期运行优化算法(根据参与者的利益的流动机制的一部分) 确保节点之间的最大链接。



C. *参与者的利益的流动机制*(ESWIM)

当收到块形成总额和总交易成本以补偿其复杂的工作频率的大部分时间，建议使用双主节点。参与者的利益的流动机制(ESWIM) 目标是确保系统发挥最佳作用，通过在每组中保持适当的双主节点数量并确保系统的保密性，和通过划分验证者在组和整个系统中的影响

ESWIM 机制鼓励在一组中的标准节点和双主节点之间灵活切换节点通过一些公式，如：更改区块的奖励分区，交易成本和每个链的节点改变的特定要求。例如，最低定金被增加将帮助节点移出一个太过重的组，最小化此级别可以吸引更多节点加入短缺的组。

如图所示，在时间段 t1 和 t2 之间在蓝色和红色链上执行交易成本的变化导致 Kardia 双主节点组的改变。因为在红链上运营的成本变得更加昂贵，

所以把交易指向红链的需求会减少，与绿色链条相反。Kardia 使用的机制将适当调整 A 组和 B 组中的双主节点数量根据预期的交易数量指向这两个链。请注意，交易执行成本只是众多因素中的一个，由参与者利益的流动机制以计算相应的改变。

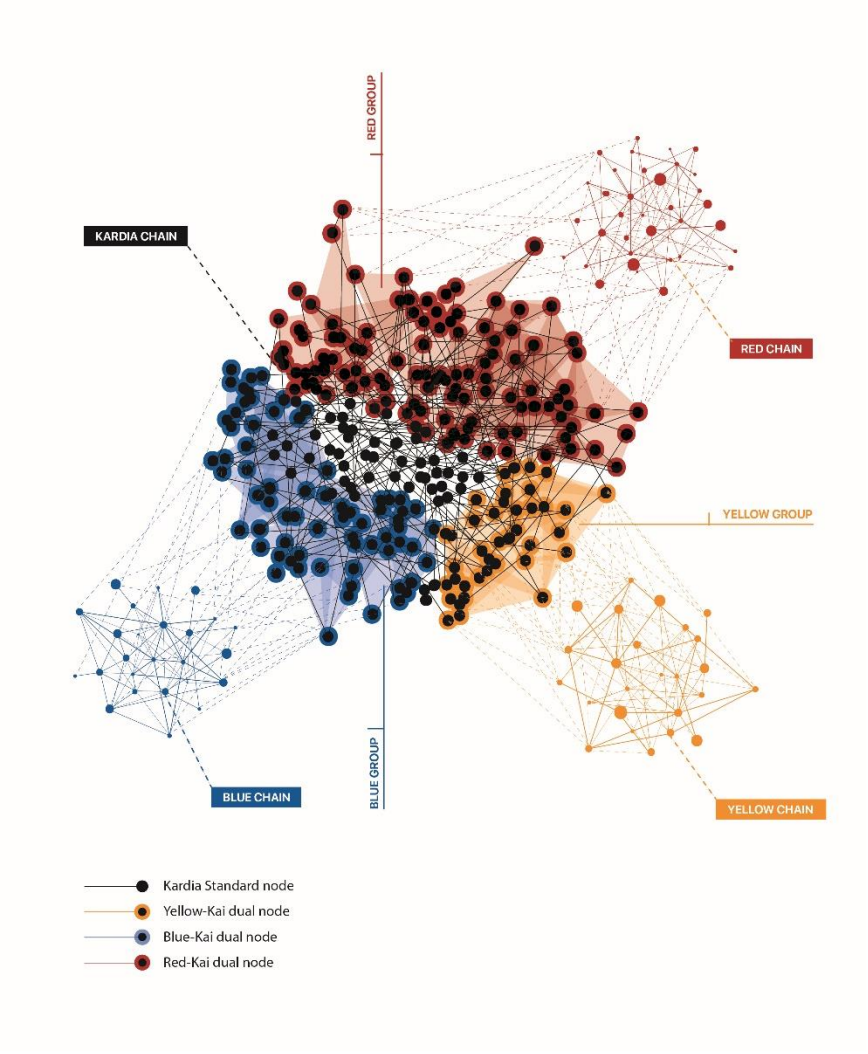


Fig 6: Optimised distribution of Dual Groups

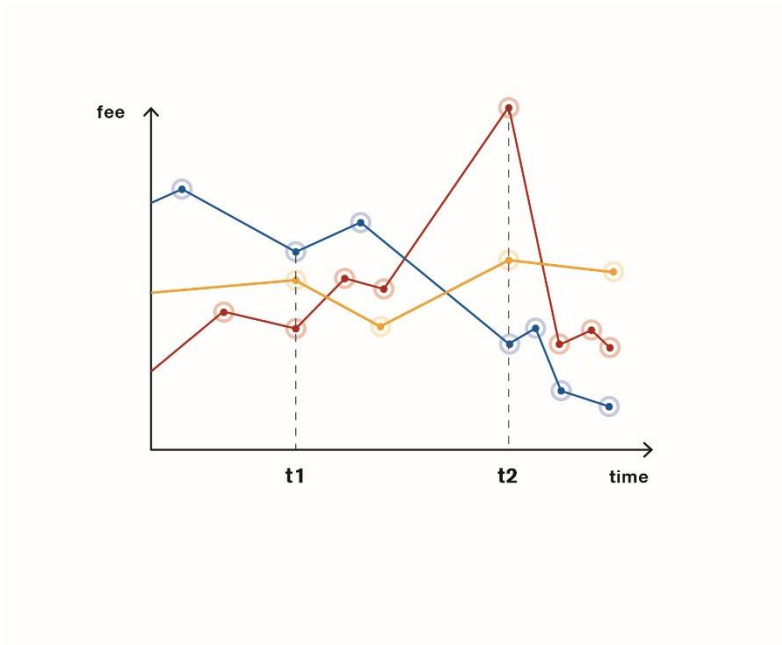


Fig 7. Transaction fee on Blue and Red chain overtime

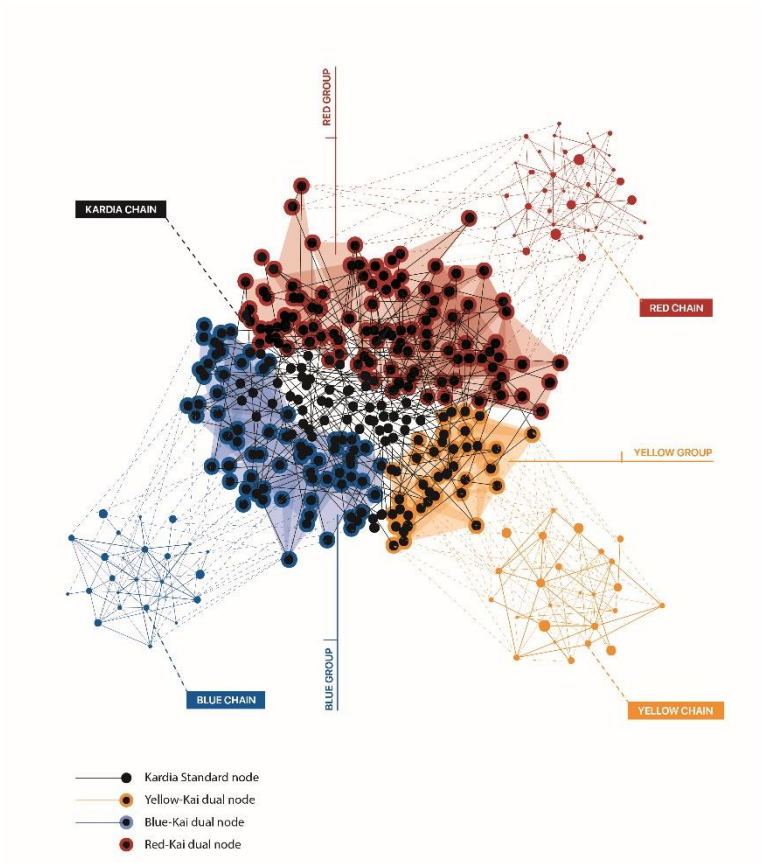


Fig 8. Group distribution at time t1

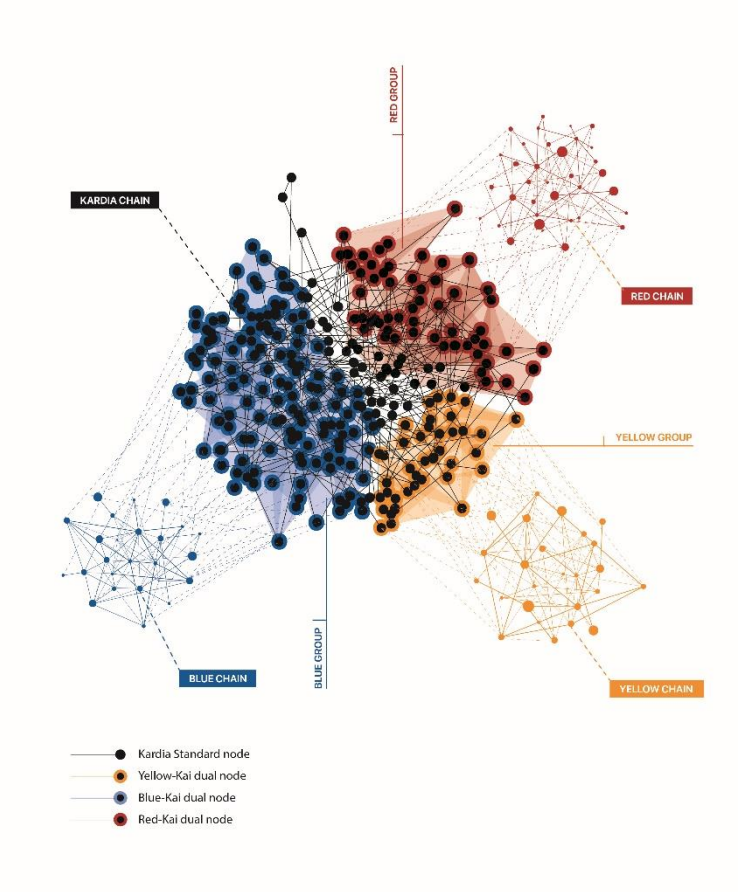


Fig 9. Group distribution at time t2

D. 共识机制

KardiaChain 使用两个共识机制 BFT + DPoS: 主要的共识机制(MCon) 和小组共识机制(GCon)。主要共识机制的成员称为密钥验证者(Main Validators - Mvals), 是那些负责维护 Kardia 总账的人。小组共识机制的成员称为小组核查员 (Group Validators - Gvals), 是那些负责批准连链交易的人并将它们添加到相应的总账

1) 过程:

小组共识机制的 5 个步骤如下:

- 选举：验证者在他们之间做出选择。
- 提案：提议者设置了一个区块并将此块发送到组中的其他节点。如果提议者无法在允许的时间内创建区块，无论区块的结果如何，系统都将继续进行下一步。此外，提议者将这些交易移动到下一个区块（1）。
- 验证：验证者接收建议块时，用选项<批准/拒绝/无投票>开始选举

过程以确定区块的有效性，然后通过交换仪式发送他们的投票。

- 批准：当提议者获得三分之二的选票时，他们会将此块发送到主要提议者(2). 主区块批准后，所有双主节点将批准此区块。
- 总结：如果系统上批准了新区块，区块的高度将增加 1 个单位以显示这个新区块已经完全批准。主要的共识过程采取相同的步骤，但有一些细微差别，例如：

在主要的共识机制中实施了相同的步骤：

- 选举：验证者在他们之间做出选择一名主要提议者。
- 提案：主要提议者将从他们收到的区块组建构一个主要区块并合理化
- 批准：当建议的区块收到足够的投票以供批准时，所有节点将开始接受该区块

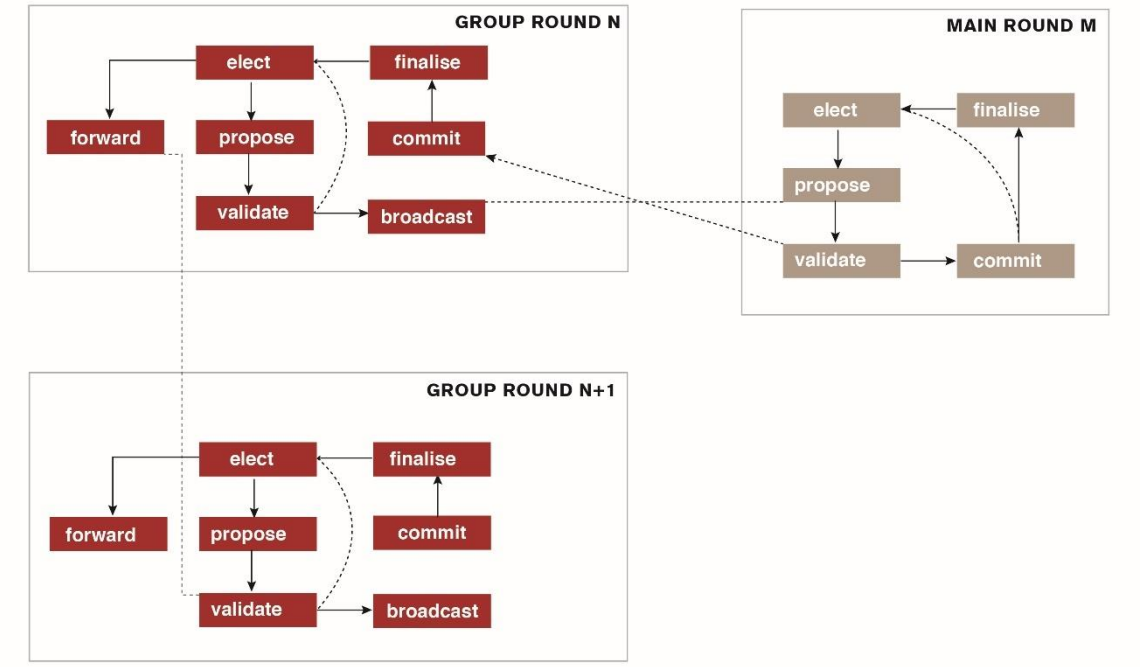


Fig 10. Consensus Protocol

(1)　发送交易：该组的提议者跟交易总结地方有关，可以定位并在待机模式下处理已定向的交易并已经有对这交易的现在区块链适当的目标区块链。被允许发送后，提议者将把这些 RTX 交易转移到聚合双主节点，双主节点将保存的位置并在下一个区块链形成的区块链中更新这些交易。

(2)　显示批准的区块：建议的区块获得三分之二的选票后，提议者会将这些区块发送到其他节点，专注于主要提议者将这些区块链进入他们的提

案中。

2) 区块结构

- Timestamp: Creation time of the block
- Height: the length of the blockchain. Genesis block starts from 0
- Vote: Record of all the BFT votes from this block, including the signatures for the block
- PreviousHash: Hash of its parent block
- StateRoot: Hash of trie root, representing the global state after the block transactions are finalized
- GasLimit: current gas limit for one block
- GasUsed: total gas used by transaction in this block
- Data: transactions data in the block. MainBlock keeps the transaction on the Kardia mainchain. DualBlock keeps the event happened on the dual group

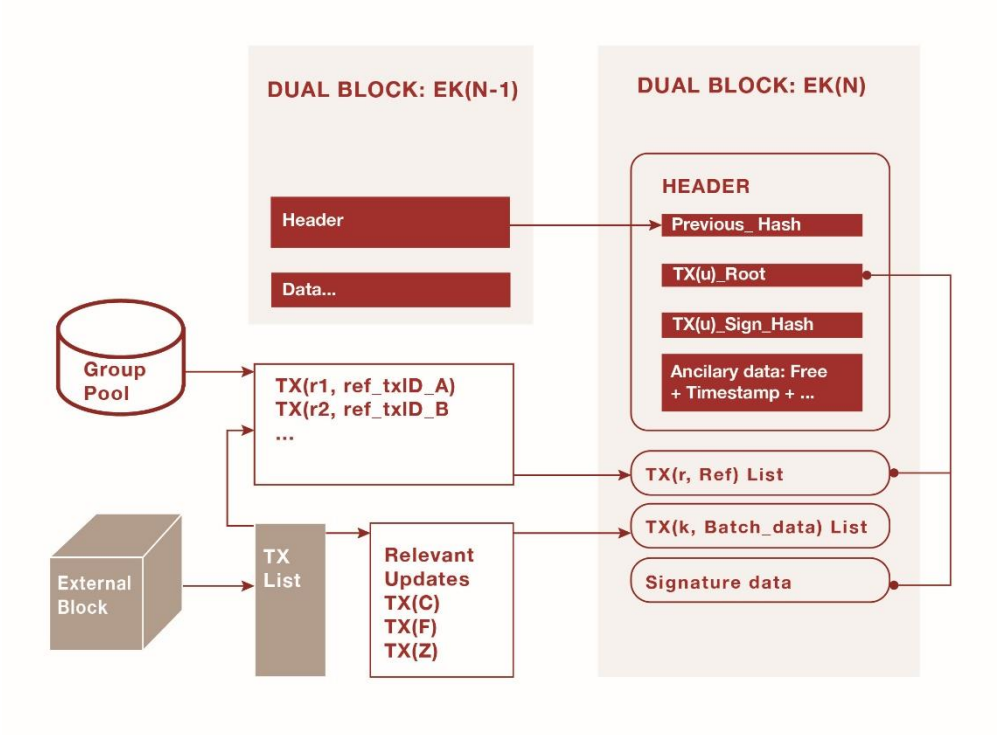


Fig 11. Connection between Dual blocks and Main block

双区块的结构可以如上所示。自不同群体的双区块将以自己的身份标记，例如
EK 代表Eth-Kardia，NK 代表Neo-Kardia（*此标记可以更改）

主要提议者会总结已从所有双主节点集成 TX（u）的交易和已从标准节点集成 TX（n）的交易以形成交易的汇总数据。主要提议者将使用从双区块收集的签名数据和发送交易的标准节点来确认这些交易。主要提议者在原始系统上记录这些交易。主要区块将根据主要提案获得的必要数据和签名形成。

E) 定金模型

1) 节点操作者需要锁定钱包中的所有 Kardia（KAI）代币，使用帐户锁定 （lockBalance）成为验证者。主要节点验证者所需的定金是 s(M)，双主节点的是 s(M+D)。我们使用“金钱时代”的概念以评估定金的可信度，意味着准备好用于 lockBalance 之前，定金必须通过一定数量的区块保存在账户中(符号mature_time) 。该模型包括许多保护系统免受攻击的点。一方面， mature_time 帮助延长攻击所需的时间，当新交易的代币不允许用于定金时。另一方面，在 mature_time 时间, 定金的总额可能会有所不同， 因此， 达到大多数所需的定金可能需要适当增加。比如， 总定金现在为1,000,000 KAI，数基于上述 BFT 共识机制，黑客必须拥有 2,000,001 KAI 才能获得超过 66%的总票。在经历了 Mature_time 之后, 一些新帐户作 为新验证者加入系统，并将总储备增加到额外的 100,000 KAI 多。这意味 着黑客需要增加 200,000 KAI 再等下一 mature_time 以能够攻击系统。因此，无法保证对系统的攻击能够成功，使打算攻击系统的用户感到困难。

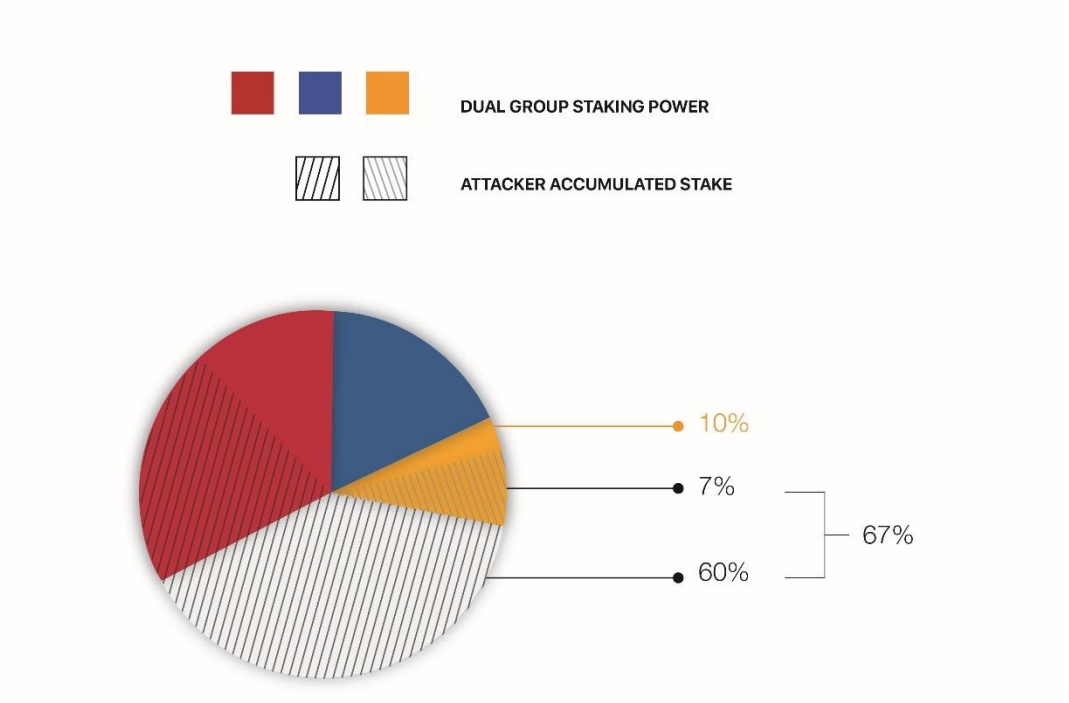


Fig 12. Total network staking power required to take control over a small dual group

对双主节点组的攻击也需要控制主系统因为主要验证者需要先验证外部区块链的更新，然后才能将其记录在总帐中。如第 13 图所示，以控制一组有 10%的定金将需要总定金的 7%，例如，从金链做出个假更新。但是，要将此更新记录在 Kardia 的总账，它需要通过主要验证者的验证。这意味着需要另外 60%的定金以有机会进行攻击。如果攻击失败批准此交易的所有节点上的定金或有害的区块会被取消（这笔钱将被烧掉），让针对 Kardia 进行任何攻击都会变得更加昂贵。

2) ***主要代币的功能***

KardiaChain 的加密公用事业代币（KAI）是 KardiaChain 建立的生态系统的重要组成部分，它的设计功能使其成为系统中唯一的代币。KAI 是一种无法偿还的公用事业代币，仅用作参与 KardiaChain 生态系统的成员之间的交换单位。KAI 的诞生旨在为在与 KardiaChain 生态系统交互时，成员之间沟通时提供一种方便、安全和简单的支付方式。KAI 对基金会(Foundation)，代理商(the Distributor)或其任何附属公司， 企业或代表不代表 KAI 所有者的任何所有权(shareholding)， 参与(participation)，权利(right)，职位(title)或利益(interest) 。同时，KAI 也没有代表的价值或向其所有者提供任何义务或承诺关于成本(fee)，股息

(dividends)，收入(revenue)，利润(profits)或任何投资收益(investment returns)， 也不构成， 不属于新加坡或任何相关领域的任何证券(securities)。KAI 只能在 KardiaChain 的生态系统使用，KAI 所有权没有权利或能力给出任何意见除了能够使用 KAI 作为与 KardiaChain 交互的工具。

网络资源(computational resources) 用于在验证区块链系统上的新区块或信息，因此，网络资源提供商将使用网络资源活动收费（例如：KardiaChain 的“mining” ）为了保持系统的公平性和透明度，在使用网络资源后，KAI 将在付款过程中用作支付单位。KardiaChain 要求 miners 在被允许参与 mining 过程之前付一定数量的 KAI 定金。KAI 是 KardiaChain 不可分割的一部分，因为当没有 KAI 出现时用户使用网络资源以开展活动或提供有助于 KardiaChain 生态系统发展的服务没有任何利益。

KardiaChain 的用户和 KAI 所有者不会从 KAI 获得利益如果不积极参加 KardiaChain 的活动。具体而言，KAI 被理解并接受为：

- 无法退款并且不能兑换成现金(或其他加密代币的任何价值) 或来自本组织，分销商或其任何关联公司的任何付款方式;
- 不代表或允许 KAI 所有者没有任何权利对组织，代理商（或任何下属单位） 或收入(revenue)， 资产(assets)， 包括任何接收 股息(dividends)，收入 (revenue)， 股 票 (shares) 权 利， 所 有 权 (ownership)，股票 (shares)或证券(security)，投票权，分配，赎回，付款，所有权（包括所有与知识产权相关的形式），或其他财务和法律权利包括知识产权或以任何参与形式与 KardiaChain，组织，代理商或上述单位的服务提供商；
- 不代表任何不同合同形式的权力，或为了获取利润或避免损失而签订合同;
- 不是一种货币（或电子货币）， 证券(security)， 大宗商品(commodity)，债券(bond)，债务工具(debt instrument)或与之相关的任何其他形式 金融工具(financial instrument)或投资;
- 不是来自组织，代理商或下属单位的贷款，不代表本组织，代理商

或其下属单位的贷款，不会产生利息预期;

- 不要向 KAI 所有者授予对组织，代理商或任何附属实体的任何所有权或利益。

代币销售过程中的贡献将在代币销售过程后由代理商（或属于其代理商的单位）存储。参与者在销售过程中在代币销售过程之后，上述贡献或贡献者的贡献资产将不会带来经济，法律或利益。对于 KAI 交易所二级市场 (secondary market) 的发展的情况下，该市场将由一个单独的单位维护和管理，与 KAI 和 Kardiachain 的组织，代理商或销售流程无关。组织和代理商不会在上面提到创建二级市场，也不会成为 KAI 的交换单位。

V. KardiaChain *的优势*

我们提出的任务是简化程序员的工作，使其不受单个区块链操作的限制。Kardia 允许程序员创建分散的应用程序能够同时在多个区块上运行，而不需要为每个区块链编写不同的智能合约。Kardia 旨在创建一个全面的系统包括私有和公有链。在这个系统中，区块链可以与系统中的任何其他区块链进行交互而不需要改变每个区块链的沟通方式。因此，我们可以轻松提高可扩展性，互操作性和灵活性。

- **可扩展性**

当智能合约被送到 KardiaChain 时，它将被集成并发送到系统中指定的区块链。最合适的区块链会被选择来接收和处理该交易提供在发送交易时在系统中处理交易最佳级别的能力。这也被称为减少区块链负载的解决方案，在某些时候避免局部拥挤。

- ***链接可能性***

通过 Kardia, 系统中的所有区块链都能够使用其他区块链上的数据和资产进行交互。跨链功能允许分散的应用程序应用于许多不同的区块链，这将有助于在给定时间里特定链上的拥塞

- ***发展能力***

程序员可以轻松集成新的区块链技术通过 Kardia 的智能合约编程接口 来自他们熟悉的工具和语言系统。KSML 采用易于阅读的语言设计，语言系统可用于支持智能合约涉及的大多数活动。通过 KSML 改变智能合约，程序员可以轻松地将他们构建的解决方案应用于所有支持的区块链。

- ***整合能力***

任何组织或个人都可以拥有区块链技术应用的第一次经验通过智能合约 API，提供了一套易于使用的工具并完全支持语言系统帮助程序员可以构建，测试和应用他们构建的第一个智能合约而不遇到任何困难。所有步骤都可以在简单的网络平台上完成，不需要高级设置。

- ***成本***

当你在某个系统中操作时， 你必须以固定的变化率支付费用。关于 Kardia, 用户使用 CMNR 选择最合适的区块链在一段时间内处理交易。包括 Kardia 的交易费，平均成本总是低于单个区块链的平均成本

VI. *分散应用的新视野*

这部分将概述分散应用程序在我们的系统上运行时的三个典型功能：

A. 具有大流量的简单 Dapp*：*

公众投票就是这 Dapp 类的一个很好的例子。在一段固定的时间内，我们期望获得与一个国家人口相对应的大量选票。但是，安装过程非常简单当组织者只需要调整 Kardia 提供的可用 SMC 表格的一小部分时，然后在 Kardia 系统上使用命令 Vote_smart contract_ABC（K）。除非进行进一步修改， CMNR 将分析上述命令并提供命令 Vote_smart contract_ABC（K）可以运行的区块链系统列表。之后，这部分将转 SMC 代码以与选定的区块链集成，例如，为以太坊集成的 Vote_smart contract_ABC（Eth）。

以下组织将收到在多个区块链上的一些 Vote_smart contract_ABC 一些命令的列表并可以选择适当的使用它们。选民可以提交投票在任何命令 Vote_smart contract_ABC 的区块链上运行。但是，我们建议通过最初的 Kardia 区块链系统发送投票以优化加密的智能导体减少整个系统的拥

塞。

比如，Kardia 在选举期间支持两个区块链系统（E 和 N）。第一个区块链能够处理每秒 2000 个交易，每个区块在 10 秒内形成，而剩余的区块链可以在一秒内执行 1000 个交易，区块形成时间为 5 秒。此外，Kardia 的原始区块链系统可在 1 秒内处理大约 3100 个交易，总的来说，整个系统可以确保完全接受 5000 万人的选票(只要所有人在 8 小时内发出投票，在同一天，导致平均需求在一秒钟内完成 1700 个交易)。

B. 多功能的 **Dapp*:***

一个简单的例子是 CryptoKitties 游戏软件，该软件包含玩家使用的每个动作比如喂养猫，改变猫的名字将在以太坊链系统上使用 1 个交易并消耗时间和金钱。我们可以节省大量的时间和成本如果可以将这些小型操作移至交易较少的区块连系统并要求降低成本。主要业务，如买卖猫将在主要和可靠的区块链系统上实施。这种方法有利于利用操作频率的差异。例如， 喂养猫会要操作很多次，而玩家之间的猫交换将以更低的频率完成。那么为什么这两个操作都应该在同一个区块链系统上运行呢？在软件设计中， 我们知道为每个目的使用不同的参数（例如速度和连续性）的多个数据点是一种值得考虑的方法并应用此软件时可以创造许多好处。

C. *彼此沟通的* **Dapp:**

Kardia 为 Dapps 提供基础设施这样他们就可以安全无缝地交换数据并相互沟通。下面的图表有助于我们理解银行阵列中 Dapp 的操作模式，当这个 Dapp 使用另一个 Dapp 的 KYC 数据时而这两个 Dapps 运行在两个不同的区块链链系统（KardiaChain 和 ChainX）上。用户A 将KYC 个人信息上传到 ChainX，用户 A 可以使 Banking_Dapp 应用程序使用 KYC_A 数据从 KardiaChain 上的 KYC Dapp 数据字典。这个过程安全和分散运行以最大限度地减少软件工程师的工作量并增强用户体验.