KOMA CHAIN

技术白皮书

Technical White Paper

Blockchain solutions for
WEB3 application ecosystem

KOMA Foundation
2023·06

目录

前言

区块链是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，是新一代信息技术的重要组成部分，是发展数字经济的重要技术支撑。当前，区块链底层技术研发企业及生态应用企业总会遇到来自技术、人才、用户需求等不同层次的挑战。具体来说，这些不确定性主要源于两个方面：

• 区块链技术还处于发展早期，百家争鸣、百花齐放的同时形成了一块块各自为政的区块链孤岛，尚未形成能完全统一业界共识的平台及互联互通的技术标准；

• 区块链技术如何与现有行业结合并有效地将应用场景落地仍在探索中。

智能合约平台和加密货币已引起各国政府、各领域专家的高度关注，但由于可扩展性和用户体验问题，仍未能实现被大规模采用。即使在目前被最广泛使用的智能合约平台——以太坊上，也还没有诞生国民级、杀手级的 DApps。在某些情况下，一个或几个特定应用程序暂时成功俘获了重要的用户群，但高并发经常导致短时间内整个网络严重受损。从本质上讲，这意味着即使是当今最领先的平台还没有为被大规模采用做好充分的准备。

另一方面，个别拥有更高的交易吞吐量智能合约平台，只能是以在分散化方面的妥协来换取相对快的交易速度。此外，许多即将推出的解决方案都建议开发自己的区块链，而忽略了现存的 DApps 和其他项目已经在以太坊等平台上创造的数百亿美元的市值，从某种意义上说，这些解决方案所忽视的是目前存在于像以太坊这样的平台上的庞大开发者社区和开发者生态系统。

一、KOMA 介绍

KOMA 正在致力于为 WEB3 应用生态系统提供更完整、更全面的区块链解决方案，以推动 WEB3 领域的技术革新。在 WEB3 时代，区块链技术成为了实现去中心化、信息安全、透明度、可追溯性、互操作性等众多属性的必要工具。然而，随着区块链技术的不断发展，不仅需要考虑区块链本身的安全性、性能、扩展性等核心问题，还需要更多地考虑与其他技术的结合，以及与现实世界的连接与整合。

KOMA 区块链解决方案力图在这些问题上提出更为全面、系统的解决方案。从安全协议设计、安全审计、性能优化、隐私保护、智能合约编写规范、开发工具链、跨链协议等方面入手，打造出可适用于多场景、多应用的区块链解决方案。同时，KOMA 关注的不仅仅是技术本身，在推动 WEB3 技术革新的过程中，还注重用户体验、应用场景、商业模式等对

于技术推广和应用的支撑。因此，KOMA 的区块链解决方案不仅仅强调技术层面的创新，更具有深度的商业价值和社会影响力。

自 Bitcoin 的去中心化数据库--区块链的提出以来，已经开发出了许多不同的协议来设计此类数据库。最近，基于 PoS（权益证明）建立此类系统的想法已经获得了显著的流行度。在最初的 PoW（工作证明，如比特币所使用的）机制中，用于激励参与和确保系统安全的投票权是与参与者拥有的计算能力成比例的，而在 PoS 中，投票权是与代币数量（特定于此系统的数字货币）成比例的。在这种系统中，一个常见的选择是定期委派一个由固定大小的参与者委派委员会，该委员会负责运行共识，确定应将哪些块添加到区块链中。这种构建区块链的方法与普通的 PoW 系统（如比特币）相比有两个重要的优点：

1）它允许运行在过去 几十年中开发的经典的基于授权的共识协议之一。

2）它不仅允许奖励节点参与，还可以通过削减违规委员会成员的担保保证金来惩罚不当行为。

最近，在这种 PoS 区块链中可以用作核心引擎的基于授权的共识协议设计方面取得了巨大的进展。其中绝大多数是在部分同步的 BFT 模型下设计的，该模型断言节点之间的通信最终变得同步，并且任何节点中不会有超过给定比例（例如 1/3，在该模型中是最优的），且这些节点可能以

任意方式违反协议。Hotstuff，Tendermint 和 Streamlet 等最先进的协议接近最优，可以在带宽、最终确认时间和实现简单性方面实现最佳。然而，这类区块链系统的实际属性中有一些重要性质没有被经典模型所包含，因此仍有很大的改进空间。其中一个重要方面是节点的分区可能无法准确反映它们的真实态度。实际上，根据模型，即使是因为 DDoS 攻击或临时网络故障而错过了几个协议消息的“诚实”节点也被视为是拜占庭式节点。在超过 1/3 的节点（即使只有几秒钟）遭受这种网络问题的情况下，经典 BFT 模型中的协议不能保证正常运行，这是一个实际问题。

另一方面，除了这些偶发的离线期外，在现实世界的系统中，可以合理地假设绝大多数节点，如果不是全部，都诚实地遵循协议规则。这是诚实参与的财务激励的结果。实际上，委员会成员最好确保他们积极参与共识协议，因为他们会因为诚实工作而得到奖励，并因为离线或没有为协议进展做出足够的贡献而受到惩罚。事实上，由于协议违规的惩罚，几乎不可能有对手尝试一次不保证成功的攻击，否则它可能面临重大损失。因此，除了旨在摧毁整个系统的大规模协调攻击之外，我们应该始终期望几乎所有节点都表现得诚实。

在这个认识的基础上，已有几项研究设计了在经典意义下是安全的协议，同时在“典型”情况下力图提供更好的保证。在本文中，我们提出了一种新的协议— KoMaBFT，有益于此方面的工作。KoMaBFT 的安全

性仍然是基于部分同步 BFT 模型来形式化的，因此特别是在最严格的 1/3 节点为拜占庭节点的情况下，它实现了安全性和灵活性。但是，在此基础上，KoMaBFT 提供了以下两个功能，使它在实际部署中特别具有吸引力。首先，在大量节点诚实参与的时期，它允许以比 1/3 更高的“置信度”达到块的最终性。举个例子，如果一个块达到了 0.8 的最终化置信度（在 KoMaBFT 中是可能的），那么至少 80%的节点需要违反协议才能从链中回滚该块。这与传统的最终化概念形成对比，后者是相对的：一个块要么被最终化（这意味着最终化置信度为 1/3），要么没有。KoMaBFT 的第二个实际改进是其实现了与中定义的类似的灵活性概念。参与 KoMaBFT 的节点可以配置不同的安全权衡，允许在协议中有不同数量的拜占庭节点和崩溃节点（可能会离线但仍是诚实的节点）。灵活性意味着尽管存在这些配置差异，所有节点都运行单个版本的协议并执行相同的操作，只有最终化决策取决于所选的参数。一个实际的结果是，具有较低安全阈值的节点可能比具有较高阈值的节点更快地达到最终性，但只要这些节点的假设都得到满足，它们都会最终确定相同的块并保持一致。

在技术上，KoMaBFT 可以被归类为 DAG(Directed Acyclic Graph)协议，其中节点共同维护协议消息的公共历史，形成表示因果关系排序的有向无环图。在设计上，KoMaBFT 来源于以太坊 Casper 协议，并通过使用新的最终性机制、消息创建计划和垃圾邮件防止机制等方面进行了显

著改进。我们相信 DAG 协议的概念简单性以及 KoMaBFT 协议的优越实用特性使其成为基于权益证明的区块链一致性引擎的可靠选择。

KOMA CHAIN 致力于解决可扩展性和可用性问题，同时不会影响权力下放和利用现有开发人员社区和生态系统。它是现有平台的扩展解决方案，可为 DApps/用户功能提供可扩展性和卓越的用户体验。KOMA 基金会计划提供 KOMA 钱包，支付 API 和 SDK，产品，身份解决方案和其他支持解决方案，使开发人员能够设计，实施和迁移基于 Ethereum 等基础平台的 DApp。

二、KOMA 架构

2.1、基础模型

我们考虑一个具有固定集合 x 的 n 个验证者的系统，每个验证者都装备有其他节点知道的公钥。这个模型符合“许可制区块链”的场景，但是通过旋转验证者集合，该协议也可以应用于半许可场景。我们的模型做出以下假设：

- （可靠的点对点网络）我们假设通道不会丢失消息，并且协议中的所有消息都由发送者的数字签名进行身份认证。

•（部分同步网络）存在一个公开已知的界限Δ和一个未知的全局稳定时间（Global Stabilization Time GST），因此在 GST 之后，无论何时验证者发送消息，都在Δ时间内到达接收者。

•（拜占庭故障）我们假设 n 个验证器中有 f 个完全受到对手控制，因此可以任意偏离协议。对于 f 和 n 之间的全局假设，我们没有做出任何假设，因为安全性和灵活性需要不同的界限，而后者也与崩溃节点的数量有相互作用。

•（崩溃性故障）我们假设 n 个节点中有 c 个在协议执行的某个时刻可能永久性失去响应。

2.2、KOMA 区块链主体共识

在一个典型的区块链系统中，验证者的任务是对他们从外部环境中接收到的一个不断增长的交易链进行迭代共识。在这个过程中，他们将交易封装到块中，形成一条区块链，每个块通过哈希值引用其前一个块。第一个块是创世块，是协议定义的一部分。在 KoMaBFT 中，由于验证者的集合要么保持不变，要么只受到极端受控制的变化，特定的验证者被直接任命在指定的时间段内构建一个块。他们通过将本地队列中的交易封装和认为应该是前一个块的哈希值来实现这一点。由于验证者可能不会引用最后构建的块（无论是故意这样做还是由于网络故障），因此块的集合 B 是一棵树，每个块都有一条通往根（创世块 G）的唯一路径。在这种情况下，

共识协议的主要目标是从这棵树中选择一个单一的分支。对于块 B，我们把所有在其他分支上的块都称为与 B 竞争的块，因为如果选择它们中的任何一个，就无法选择 B。

2.3、共识实际挑战

自 Dwork、Lynch 和 Stockmeyer 最初定义部分同步模型以来，已经创造了大量的研究来优化该设置中协议的各种参数，但其中大部分都是在半正式的假设下编写的，即存在超过 n⁄3 个不诚实的节点的存在在任何可以证明协议的情况下之前。这种假设源于最初的论文的证明，即如果 n < 3f + 1，则不可能保证部分同步协议同时保证存活和最终性。尽管存在这种负面结果，但在对于长时间期间，即使不诚实的节点不从协议中偏离，积极地工作以完成块的情况下，仍然可以为提供额外的最终性保证。尽管从经典安全模型的角度来看，这似乎不是一个重要的观察结果，但我们强调它具有重大的实际影响——在大多数区块链部署的情况下，可以假定大多数时间基本上所有节点都会积极协作以达成共识。因此，在这些时间段内创建的块可以提供更强的最终性保证，因此要撤销它们，需要更多于 n⁄3 的验证者共谋。

灵活性，一旦传统的 n < 3f + 1 界限不再适用，最终性和存活性之间会自然产生一种权衡。我们需要越强的最终性保证，就需要更多的验证

者诚实合作以完成具备此保证的块。所有验证者就使用的共同最终性阈值达成一致可以解决这种权衡，但这种解决方案会有重大的限制。

然而，在 KoMaBFT 中，不存在达成共同阈值的必要性，因此每个验证者都可以使用不同的阈值，甚至是多个不同的阈值。除了消除对该超参数进行额外共识的需求外，这种特性的一个重要意义是，它允许验证者在生态系统中扮演略微不同的角色——例如，一些验证者可能主要处理一些小的交易并进行最终化，这种情况下小的延迟比非常高的安全性更重要（而且，正如在协议被介绍后将明显的是，达到更高的阈值通常需要更长时间），而其他验证者则可以将安全性置于延迟之上。

2.4、KoMaBFT

我们介绍 KoMaBFT 协议—— 一个实现强乐观最终性且灵活的共识协议，它允许验证者使用不同的置信阈值来确信某个块已经“最终化”。

除非一些验证者积极违反协议，否则对于给定的验证者来说，块的最终性只能增加，这类似于 PoW 场景下块的确认数不断增加的情况。然而，与 PoW 不同的是，在 KoMaBFT 中，对于一个给定的块，置信水平可以直接解释为需要多少个验证者才能做出不良行为以翻转这样的块，我们将其形式化为以下定理：

定理 1（最终性）：如果某个诚实验证者对于一个给定的有效块 B 达到了置信阈值 t ≥ f，则没有任何其他诚实验证者会使用置信阈值 t 最终化与 B 竞争的块。

需要注意的是，尽管由于先前提到的不可能性结果，不可能证明置信阈值高于 n/3 时的存活性，但在实践中，绝大多数验证者大部分时间都不会偏离协议。在这样的时候，可以达到任意高的置信阈值，这使得在这段时间内构造的块几乎不可能被回滚。

接下来，我们提供了一种保证协议将继续最终化给定置信阈值块所需的诚实验证者数量的上限。我们指出，这与传统的 n ≥ 3f + 1 边界一致，并加上了“崩溃错误”这一概念（由 c 表示），它破坏了共识过程，但不像拜占庭错误那么严重。

定理 2（存活性）：对于每个置信阈值 0 ≤ t < n/3，如果满足 f ≤ t 且 c < n-3t/2，那么对于每个诚实验证者来说，经过 t 置信的块组成的区块链将无限增长。

三、构建 KoMaBFT 协议

在区块链中，我们称初始区块为“创世块”，该块被视为协议定义的一部分。除了创世块，其它的区块都由其父块的引用和该块的内容组成，父块用 prev(B) 来表示。通常情况下，一个块包含了交易列表等内容。B

中的父引用通过在 B 中包含 prev(B) 的哈希来实现，因此块图中不可能存在环。我们还用 next(B) 表示所有以 B 为父块的块的集合。我们递归地定义块的高度 H：创世块 G 的高度 H(G) 为 0，对于任何其它块 B，H(B) = 1+H(prev(B))。我们说块 B1 是块 B2 的后代，如果我们可以通过遵循父链接从 B2 到达 B1，则称 B2 ≤ B1（特别地，H(B2) ≤ H(B1)）。

在 KoMaBFT 协议中，验证者通过交换消息来就提议的区块达成共识，并验证生产的区块链中的可能存在的多个分支之一。为了捕获并传播不同验证者对已经存在的消息的知识，它采用 DAG 框架，其中每个由验证者广播的消息都引用了此前由验证者发送的某些消息集。我们将此类在正常协议操作期间广播的消息称为单元，并将其中包含的引用称为引用。更正式地说，每个单元包括以下数据：

- Sender.：单元的发送者（创建者）的 ID。
- Citations.：一个哈希列表，其中包含创建者想要证明的其他单元。
- Block.：如果此单元是由指定在给定时间内产生块的验证器生成的，则会将它包含在单元中。

四、为什么选择 KOMA?

分散的应用程序正在大量提出，但目前的区块链生态系统还没有准备好扩展以满足大规模采用的最终用户应用程序的需求。此外，DApps

的用户体验非常差，对普通用户来说无益。缓慢的块确认，高交易费用，低可扩展性和糟糕的用户体验是大规模采用区块链应用程序的一些主要障碍。以下部分解释了当前区块链生态系统中存在的问题以及 KOMA CHAIN 是如何解决这些问题。详细的技术规范在白皮书的其他部分中提供。

4.1 解决当前区块链网络拥堵的问题

区块链交易通常非常缓慢，吞吐量非常有限。大多数基于 PoW（Proof-of-Work）的区块链协议都对块大小有限制，并且生成块需要一定的时间。由于潜在的连锁重组，每笔交易还必须等待多个区块确认。

基于 PoS（Proof-of-Stake）的区块链尝试使用铆接机制来抵消这些限制，但是能够以 PoS 实现高吞吐量的区块链能够以分散化为代价来实现。这些限制通常是公共区块链确保安全性和分散化的必要条件，其中块需要通过网络传播并由所有节点验证以实现最终性。

KOMA CHAIN 通过使用高吞吐量区块链解决了这个问题，该区块链由一组选定的区块生产者提供，由一组 Stakers 为每个 CheckPoint 选择。然后，它使用 ProofOfStake 图层来验证块，并将区块生产者生成的块的周期性证明（merkle 根）发布到以太坊主链。这有助于实现高水平的分散，同时保持极快（<2 秒）的块确认时间。

4.2 解决当前 POS 交易吞吐量低的问题

公共区块链必须在相邻块的产生之间保持一定量的时间滞后，以便确保块传播的充足时间。此外，块大小需要很小，以确保块通过网络快速传播。这需要特定块中的事务数量需要相当有限。

4.3 提供侧链可扩展性

从理论上讲，KOMA 网络具有使用多个侧链每秒数百万次交易的能力。此外，已经通过第一个 KOMA 概念证明了第一个 KOMA 侧链的机制，并且可以在某些特定协议(例如新增的 NFT\SFT 协议，或一些企业化的独立验证机制)需求下扩展并添加新的侧链。

在基于智能合约的区块链的情况下，区块链和/或计算状态上的每个块必须由多个节点验证。每个节点都必须管理状态和块的副本。虽然随着时间的推移，链条的规模会增加，但维护和验证整个区块链变得困难，并导致公共区块链中的完整节点数量减少，从而导致分散化的风险。

对于 KOMA 网络，提供分散的主要层可以选择仅存储从前一个 CheckPoint 到下一个 CheckPoint 的 KOMA CHAIN 块。所有先前的交易/块证明都已提交给主链。这可以实现极低保真度的 PoS 节点，这些节点可以在低成本的低存储机器中运行。未来 KOMA 还将推出基于移动设备的 PoS 验证节点。

4.4 多个微支付渠道与跨链解决方案

一些支付渠道解决方案提出了解决微支付问题的解决方案。但是，使用多个 DApp 或用户打开和管理频道的过程很复杂。此外，通过渠道进行中介支付的速度和便利性仍有争议。

由于 KOMA CHAIN 在 EVM（以太坊虚拟机）上使用基于状态的体系结构，因此不需要在双方之间打开支付渠道。实际上，任何有效的以太坊地址都是有效的 KOMA 地址。当他们想要检索主链上的付款或设法加入 KOMA 生态的时候，他们只需要有一个 KOMA 钱包即可。

4.4.1 解决传统区块链高交易费用问题

随着区块链生态系统的快速发展，新的加密资产越来越多地被创建，转移和销售，通常涉及多个加密令牌。此外，大多数分散的应用程序都有自己的令牌和经济模型。为区块链支付服务代币或进行任何类型的交易需要进行链转移。每个区块链都有一个交易成本（GAS 费用）。

费用金额是激励验证者和防止某些类型的安全攻击（如 DoS）的重要因素。但是，由于块大小有限，存在费用变化的问题（取决于待处理的事务队列）。KOMA 通过在区块生产者层上进行大量交易来实现低成本交易，从而实现低成本交易，确保低成本，然后使用块的 Merkle 根对高

度分散的 KOMA 块的证明进行批处理主链（例如以太坊）使用分散的 PoS Stakers 层。

4.4.2 解决传统区块链可用性差问题

与集中式对应物相比，DApps 上的用户交互通常较差。对于实现大规模采用的权力下放革命，DApps 的用户体验必须与其集中式同行相提并论，即使不是更好。

4.4.3 KOMA 系统架构包括以下组件

跨链分区（Zone）指运行着同一类业务的区块链集合。KOMA 可以对这个区块链集合本身和内部的区块链资源进行命名和寻址，根据业务需要，跨链操作会产生分区和分区之间，以及分区内部的链和链之间。

跨链路由（Router）指用于桥接业务系统与区块链的服务进程。多个跨链路由之间可以相互连接，相互转发请求。用户通过向跨链路由发起请求来访问跨链分区中的资源。跨链适配器（Stub）指连接一个区块链的接口实现，可由跨链路由加载。跨链路由可以配置多个区块链适配器，达到连接多条区块链的效果。跨链路由间会自动同步区块链适配器的配置信息，从而帮助用户寻址位于其他区块链上的资源。

跨链资源（Resource）指区块链上的智能合约、数字资产等用户可访问的数据对象。类似于区块链适配器的配置信息，跨链资源的元信息也

在跨链路由之间同步。用户通过统一的接口对跨链分区中的资源进行寻址和调用。为了满足未来多样化的业务互联需求，针对海量数据跨链的典型业务特征，KOMA 为网络交互和部署架构设定了以下关键设计目标。

跨地域互联：作为多方参与的区块链应用，通常涉及多个服务机构，业务部署在多个跨地域的数据中心。KOMA 为跨地域场景设计安全、可靠和高效的网络架构，基于 TCP 长连接、心跳、自动重连和加密通信技术的网络机制来保证大范围跨地域互联的稳定性、及时性和安全性。

部署架构灵活：由于跨链需求通常源自成熟的区块链应用项目，跨链部署架构需要具备兼容现存区块链实例的能力。KOMA 采用 “非侵入式”设计，跨链路由以独立进程的方式与区块链节点分离部署，无需变更既有的区块链网络架构，即可实现灵活的架构部署。跨链路由间使用网络传输跨链消息和区块链消息，结合网络自动寻路功能，只要跨链路由间有直接或间接可触达的网络链路，就能完成跨链交互。

可自由定制：现实业务场景中的跨链需求千差万别，接入的区块链平台多种多样，因此定制化可裁剪的跨链能力不可或缺。KOMA 的区块链适配器和跨链资源支持自由定制，根据接入的区块链类型、系统资源和网络情况，选择不同的区块链适配器和跨链资源。

KOMA 开发团队还将开发各种移动和 Web 浏览器集成工具，并且是该领域的先驱协议。它打算构建一个无处不在的移动/浏览器应用程序，

它将作为区块链交互的安全交互层。KOMA 开发团队将很快发布这些设计和原型。

五、介绍 KOMA 网络

正如上文简要讨论的那样，KOMA CHAIN 旨在通过使用适应版本的 DAC 框架构建分散式平台来解决区块链生态系统所面临的问题。这提供了在主链上具有最终性的快速且极低成本的交易。

KOMA 开发团队还在构建产品生态系统，包括用户友好的移动应用程序，桌面钱包和浏览器扩展，这将为所有用户提供无缝体验。设想用户将能够支付，转移或保存加密资产而不必担心底层系统的复杂性。

5.1 KOMA 网络架构

由于 KOMA 的核心重点是大规模用户采用，因此深入了解 KOMA 的技术架构应该从用户旅程开始。

当用户在以太坊网络上传输 ETH 或 ERC20 令牌时，他们必须等待块的确认，范围从 14 秒到 20 秒。即使这样，用户也必须等待多个块确认才能确保交易的最终结果。假设您正在购买咖啡或支付代币来观看电影。在每笔交易中，您不仅要支付高额费用，还要等待确认。

此外，在高峰负荷期间，大量交易会阻塞以太坊网络，并且每笔交易都会增加 GAS，以便获得更快的确认。提出 KOMA 网络作为克服这些问题的解决方案。

5.2 KOMA 角色定位

KOMA 的生态系统将有以下参与者：

1. 终端用户

2. DApp 开发人员：开发人员应该使用 KOMA 来扩展他们的应用程序，并为他们的最终用户提供更好的 UI/UX

3. Stakers：Stakers 需要存入/持有令牌才有资格并在 KOMA 中扮演非常重要的角色。他们使用具有三分之二以上的 PoS 共识机制验证交易并在主链上提出 CheckPoint。他们还选择满足一定标准的区块生产者，在侧链上生产块。

4. 区块生产者：这些是由 Stakers 选择的区块生产者，而 Stakers 又可以更快地生成区块链。他们必须提供完整的资产证明（KMC）才能获得提名。

5.3 KOMA 共识

KOMA 使用 CheckPoint 层的双重证明策略和区块生产者层的区块生产者来实现更快的阻塞时间，同时通过使用 CheckPoint 和防欺诈机制在主链上实现最终结果来确保高度分散。

通过这种机制，KOMA CHAIN 实现了高转换速度，并在主链上实现了高度的分散和终结。在仅将以太坊作为基链的第一个版本中，以太坊根合约通过标题栏（CheckPoint）非常有效地强制执行偿付能力和终结性。系统的各种元素和机制如下所述：

CheckPoint 层

基本上，任何人都可以在根合同上放置他们的 KMCs，成为 PoSCheckPoint 层的一个 Staker（在以太坊链上部署合同）。这为 KOMA CHAIN 提供了高度分散的基础层。

验证节点

在 KOMA 的区块链层，有一些 BlockProducers，由基础层上的 PoS Stakers 选择，他们将创建 KOMA 区块。为了实现更快的块生成时间，这些块生成器的数量会很少。预计该层将以极低至可忽略的交易费用实现约 1-2 秒的块生成时间。

CheckPoint 机制

在 KOMA CHAIN 的 CheckPoint 层，KOMA 网络的 PoS 机制的基础上，对于 KOMA 网络的块层上的每几个块，将在利益相关者中选择提议者以在主链上提出 CheckPoint。这些 CheckPoint 由提议者在验证 KOMA 网络的块层上的所有块并创建自上一个 CheckPoint 以来的块哈希的 Merkle 树之后创建。然后将 Merkle 根广播到 Staker 网络以进行签名。其他利益相关者也验证了证据。如果提议的块有效，它们将通过提供签名来批准它们。

系统需要得到利益相关者的批准才能向根合同提出“Title Block”。一旦在主链上提出 CheckPoint，以太坊主链上的任何人都可以在指定的时间段内挑战建议的 CheckPoint。如果没有人质疑它并且挑战期结束，则 CheckPoint 被正式列为主链上的有效 CheckPoint。

除了在主链上提供终结性之外，CheckPoint 在提款中起着非常重要的作用，因为它们包含在用户撤回时的令牌的销毁证明。它使用户能够使用 PatriciaMerkle 证明和标题块证明在根合约上证明其剩余的令牌。请注意，要证明剩余令牌，必须通过 PoS（利益相关者）将标头块提交到根链。

通过这种机制，KOMA CHAIN 在主网上实现了高交易速度，高度分散化和终结性。在以以太坊为基链的第一个版本中，以太坊根合约通过标题栏（CheckPoint）非常有效地强制执行偿付能力和终结性。

验证节点选择

通过主链上的投票，Stakers 在 CheckPoint 层中选择区块生产者。在预定的时间间隔内选择区块生产者，直到网络共识机制削减/删除，或者由于任何外部问题而无法参与块生产。

P2P 网络

1. KOMA Network will ask for applications from the public to run the Block Producer nodes 2. It will also run 3 Block Producer nodes itself during the seed stage of the network 3. At the epoch, the public stakers will select a total of 5-7 block producer nodes 4. These nodes will be kickstarted with a KOMA Chain N(number of) genesis configuration

验证节点申请流程

1. The Block Producers have to apply by staking the Block Producer Stake requirement amount in KOMA Tokens on the mainchain 2. The Network will maintain a pool of interested Block Producers (An incentive system for the Block Producer nominees would be devised to keep ample number of Block Producers in the pipeline)Criteria on the basis on which Stakers will decide to vote for a particular nominee Block Producer are as follows:- Uptime history

- Technical specifications - Dynamic scaling capability - Location persity - Other factors under consideration

在任期完成时通过投票选择

1. Voting process is scheduled and completed one week before the completion of one tenure 2. Existing Block Producers can re-appear in the elections 3. Stakers vote for Block Producers from the pool of Nominees

在正在进行的任期内更换 BlockProducer

如果区块生产者不合时宜地移除/无法参与块生产，将招募来自临时池的新区块生产者。根据投票者的投票，将设计一个适当的激励机制来确定优先/优先的验证节点名单，以维持一个健康的验证节点库。

5.4 多链支持

KOMA CHAIN 公共 CheckPoint 层通过设计支持多个侧链。从理论上讲，可以在安全和分散的 CheckPoint 层下工作无限数量的侧链。企业可以将其专用侧链连接到公共 CheckPoint 层，完全控制其执行环境，同时通过 CheckPoint 机制保留交易的不变性，可证明性和安全性。

影响这种分片过程设计的关键因素预计是：

1. 调度点层的调度以周期性地提出不同侧链的 CheckPoint

2. 跨越多个侧链的资产流动

3. 用户将能够使用链 ID 和收据跨侧链发送资产

4. 将为用户提供直观的钱包界面以执行链间交易

5. 将为开发人员提供 API/SDK，以便为链间事务构建可编程接口

6. 资产从一个链到另一个链的移动将在 CheckPoint 层进行管理，并且可能不需要与主链进行任何交互。目前正在进行研究以促进更快（可能是即时）的侧链转移。

5.5 互通性

如前面白皮书中所述，以太坊主链是 KOMA CHAIN 安全集成的第一个基本/主链，使用了 DAC 框架的改进实现。此外，KOMA 网络打算整合多个领先的智能合约平台加密货币（如比特币等），为用户提供通用平台，以便能够使用/交换各种区块链中的资产，打破区块链孤岛魔咒，真正实现区块链全网互联互通。

它还可以为托管来自多个区块链的资产的大型 DEX（分散交易所）提供坚实的基础。此外，拥有来自多个区块链的资产的单一平台也可以产生大量新的用例，开发者生态系统可以将其未来产品概念化。对于 KOMA 开发团队来说，这是一个令人兴奋的探索领域。

总的来说，如果能够有效地识别有问题的 EVM 状态转换以进行验证，通过 EVM-in-an-EVM 结构，可以使其受到挑战，从而保护它。

5.6 安全

欺诈证据，为了增强交易的安全性，KOMA CHAIN 还在主链上提供欺诈证明。该机制使主链上的任何个人能够提交他/她认为是欺诈的交易的细节。如果挑战成功，参与欺诈的各方的利害关系就会被削减，挑战者会收到大幅削减的资金作为检测欺诈的动机。对于希望调查 KOMA 网络上交易真实性的任何一方，这可以被视为一个始终运行的高奖励赏金计划。

基本证明，必要时，每份证明必须提交以下相应的证明：

1. 交易包含的 Merkle 证明：需要此类证据来证明给定的交易包含在块中
2. 块包含的 Merkle 证明：需要这种类型的证明来证明块包含在给定的 CheckPoint 中块需要此证明来证明该块与有效的引用哈希序列一致。

交易

单级 txn 证明

// validate ERC20 TX function validateERC20TransferTx(uint256 headerNumber, bytes headerProof, uint256 blockNumber, uint256 blockTime, bytes32 txRoot, bytes32 receiptRoot, bytes path, bytes txBytes, bytes txProof, bytes receiptBytes, bytes receiptProof) public { // validate tx receipt existence }

Nonce 验证

- 检查是否存在具有重复 nonce 的事务
- 检查缺少 nonce 值的事务（跳过其间的多个 nonce）这是一个交互式欺诈证明。在对此类交易提出质疑时，区块生产者必须在一定时间内提交缺失的随机数交易。
- 检查与非订购的 nonce 的交易

function validateMisMatchedNonce(bytes tx1, bytes tx2) public { // check if both transactions are not the same ... // validate first transaction ... // validate second transaction ... // check if sender is the same in both transactions ... // make sure 2 is included after tx1 ... // check if both nonce values are same or nonce2 < nonce1, just call slasher ... // revert the operation ... }

验证

- 检查给定收据中的收货字段，事件，主题和数据类型

存款

- 验证存款交易验证主链上的存款交易，看它是否与根链中的 DepositBlock 对象匹配。

- 重复存款交易此证明验证是否存在具有相同 DepositID 的重复交易，并且每个 DepositID 仅包含一次

- 验证存款金额和存款人地址

ERC20 转让

- 验证 ERC20 交易数据，收货日志和值

- 检查日志收据日志中的 UTXO 样式输入是否等于最近事务日志收据的 UTXO 样式输出

5.7 专注于用户体验

KOMA 开发团队正在通过实施 WalletConnect 协议开发钱包，该协议是一种将基于 Web 的分布式应用程序连接到移动加密资产的开放协议。

此钱包将帮助用户轻松与 DApps 交互并签署交易，同时仍可帮助用户在移动设备上保护其私钥安全。这对于使主流用户可以访问区块链有很大帮助。

除此之外，该团队还在寻找特定于上下文的无以太网账户和身份上的气体中继抽象，以实现无以太网标志交易，这可以大大提高主流用户的采用率。

5.8 KOMA 智能合约

主链上的 KOMA 智能合约为 KOMA 网络提供了核心逻辑。合同包含各种机制，例如从主链到侧链的存款和退出，反之亦然。它们还包含退出优先级队列，来自 Validator 层的周期性状态承诺，防欺诈机制，绑定退出质询逻辑和各种其他组件。

5.9 KOMA CHAIN Bridge（跨链，链桥）

KOMA CHAIN 的桥接器是区块生产者节点的一部分，它们监听主链上的 RootContract 事件并监视发生在 RootContract 上的任何令牌/以太传输事件。链桥方案使用了 KOMA CHAIN 的 Dagger 工具。一旦桥检测到主链上的存款，它就会在 KOMA 链上触发存款事件，并且在 KOMA 网络上的用户地址被分配存款金额。

5.10 KOMA PoS

KOMA 网络的 CheckPoint 机制是一个支持 PoS 的层，它有一些 Stakers，它们向主链提出 CheckPoint。在 CheckPoint 层将有大约 100-150 个 Stakers 开始。随着以太坊区块链上更有效的签名机制的出现，KOMA CHAIN 将能够显着增加 CheckPoint 层上的 stakers 数量，这有望进一步提高其分散度，极有可能超越以太坊和比特币这样的区块链。

5.10.1 区块生产者层

在基础层，KOMA 网络具有由 PoS 层的 Stakers 通过对每个 CheckPoint 间隔进行投票而选择的区块生产者节点。

区块生产者通过 KOMAVM 接受交易，预计每隔约 1 秒创建一个块。BlockProducer 图层的更多技术和代码级细节将添加到白皮书的更高版本中。

5.10.2 KOMA EVM 虚拟机

KOMA 使用基于标准 EVM 的状态机，由 BlockProducer 节点运行以生成块。使用 EVM，KOMA CHAIN 可以构建和部署协议，如 ERC 协议以及其他协议，如 KyberNetwork，ZRX 等。

KOMA 网络架构的优点在于，由于它使用了与 EVM 兼容的状态机，因此将以太网区块链上运行的 DApps 和智能合约移植到 KOMA 网络变得非常容易。KOMA 开发团队打算支持 KOMA 网络上的广义状态转换，这种架构为构建提供了一个平滑的基础。

5.10.3 KOMA 撤销桥

当 KOMA 网络上的地址向网络提交撤销请求时，相应的令牌将在 KOMA 链上被烧毁（撤销），并且此交易将被推送到 KOMA 链。在指定的 CheckPoint 间隔之后，PoSCheckPoint 层将 CheckPoint 发布到主链，

其中将包括 KOMA 链上这些令牌的刻录（撤销）证明。一旦在主链上提交了该 CheckPoint，用户就可以声明他们的撤销令牌。

5.11 DDos 保护

运行 KOMA 的区块生产者层的区块生产者将监视资产的转移状态以识别冗余的交易。他们拒绝任何支付金额为零的传入交易，从而挫败任何 DoS/垃圾邮件攻击，并进行零成本交易。即使 KMC 的成本非常低且费用非常低，由于 KOMA 网络的高 TPS，在 KOMA 网络上运行持续的 DoS 攻击在经济上是不可行的。

KOMA 将支付转移事件日志保存在类似 UTXO 的数据结构中，从而可以有效地验证输入和输出。这允许各种安全措施。

运行其他检查以基于此减轻垃圾邮件：

- 对于每个输入，引用的输出必须存在且不能已用完
- 检查输入值的总和是否小于输出值的总和。
- 检查交易费用是否过低。
- 检查事务池中具有相同输出的重复事务。
- 检查池中具有相同交易费用的重复交易。

5.12 潜在案例

KOMA 基金会致力于为第三方分散式应用程序提供可扩展且用户友好的生态系统。管理机构，如以太坊和其他平台基金会，将推广各种基链 DApps（如目前在以太坊上构建的 DApps，以及未来的 NEO，EOS），以在 KOMA 网络上构建和迁移面向用户的应用程序/交易。它还将向第三方应用程序开发人员授予资助和资金，以便在 KOMA CHAIN 之上构建各种用例，例如：

5.12.1 支付

KOMA CHAIN 将为 DApps、商家和用户提供支付 API 和 SDK，以便立即接受或支付加密资产（例如，ERC20 令牌，Ethers，ERC721 令牌）。

5.12.2 TOKEN 生态

KOMA 合同允许用户使用他们喜欢的任何加密令牌付费，接收者将收到他们喜欢的资产付款。KOMA CHAIN 可以通过跨链加密资产之间的 TOKEN 交换来处理交易。

5.12.3 流动性提供者

第三方可以通过利用 0x 流动资金池或其他流动性提供商在转移加密资产时使用 KOMA CHAIN 来交换任何其他令牌的令牌。在法定的情况下，KOMA 开发团队计划与主要国家货币的法定流动性提供商合作。

5.12.4 分散交换（DEX）和市场支持

预计 KOMA 将拥有交易平台应具备的所有特征-更快，更便宜的交易。KOMA CHAIN 能够支持分散式交换，实现无信任，可靠，简便的加密交易。分散交换是数字资产的未来，提供比集中交换更好的安全性和偿付能力。

5.12.5 贷款和信用评分平台

KOMA 将使商家平台能够通过其交易历史评估关联用户的信誉。这使得商家能够在与没有足够资金的用户进行交易时向网络上的用户提供令牌。KOMA CHAIN 期望使用 Dharma 协议为用户提供标记化的债务。

5.12.6 数字身份

用户需要一个实用且用户友好的界面，不需要 MetaMask 或支持 web3 的浏览器。他们不需要了解区块链节点如何在幕后工作。

分散式应用程序需要一种签署交易的方式，但必须在 Web 浏览器或移动应用程序上的每个 DApp 上提交私钥的情况下进行。KOMA 开发团队认为，用户必须能够控制他们的私钥，而不必担心安全问题。KOMA CHAIN 将通过 Open-Identity 系统解决这个问题，并为用户提供无缝体验。

该系统还将提供一种根据用户选择的标准自动批准某种交易的方法。这将推动 KOMA 网络上的定期付款。

5.12.7 游戏

我们希望游戏成为 KOMA CHAIN 的重要组成部分。代表 NFT（ERC721）的游戏内资产预计将在我们的侧链上大量购买，出售和交易。如果他们愿意，开发人员还可以在侧链上保存游戏状态。随着我们将启用的 NFT 市场，开发人员和用户将真正拥有一个快速，高效和安全的侧链来构建和玩游戏。

5.13 基础设施

KOMA 开发团队将采用简单的口头禅-简单而无缝。为此，该团队将围绕 KOMA CHAIN 提供新的基础架构，包括针对个人用户和商家的用户友好型钱包，工资单仪表板，支付 SDK 和其他开源工具。

KOMA Dagger 工具

从 Dagger 开始，KOMA 开发团队已经开始为开发人员构建基础架构。Dagger 是一种实时跟踪以太坊帐户和事件的工具或引擎。

开发人员可以使用 Dagger 跟踪他们自己的智能合约，帐户和交易。他们可以通过 IFTTT 或 Zapier 创建自定义服务或与第三方服务集成。

KOMA 钱包

KOMA 开发团队正致力于构建易于使用的等离子钱包移动应用程序，与 WalletConnect 集成，以确保密钥的安全存储，直观访问 KOMA CHAIN 提供的功能，以及连接浏览器的无缝机制基于 DApps 的移动应用程序。用户可以在浏览器和未来的更多设备上与 DApps 进行交互，同时仍然可以将密钥保存在他们的移动钱包中。

KOMA 钱包将作为 DApp 开发人员的一个现成工具，让他们的用户可以快速高效地使用 KOMA 侧链。

六、KOMA 原生代币（KMC）

KOMA 代币（KMC）是 KOMA 网络上生态系统的主要组成部分，旨在用作网络上的主要令牌。KMC 将作为 KOMA 区块链上符合 ERC-20 标准的数字通证发行。

KMC 被设计成一个实用程序令牌，作为在 KOMA 网络上的生态系统内交互的参与者之间的支付和结算单位。

KMC 不以任何方式代表管理机构，发行人，其关联公司或任何其他公司，企业或企业的任何股权，参与，权利，所有权或权益，KMC 也不会授予令牌持有人任何承诺。费用，股息，收入，利润或投资回报，并不构成香港或任何相关司法管辖区的证券。除了 KOMA CHAIN 和/或可能

使用此类令牌的任何其他第三方可能提供的权利之外，KMC 的所有权不具有任何明示或暗示的权利。

预计 KMC 将提供经济激励措施，鼓励参与者在 KOMA 网络上贡献和维护生态系统。在 KOMA 网络上执行各种功能需要计算资源，例如验证块和发布证据，因此这些服务/资源的提供者将获得用于向网络提供这些资源的 KMC（即，在 KOMA 网络上“验证奖励”）保持网络完整性。KMC 将用作交换单位来量化和支付消耗的计算资源的成本。KMC 是 KOMA 不可或缺的一部分，因为没有 KMC，用户无需花费资源参与活动或为 KOMA 网络上的整个生态系统提供服务。只有实际为网络维护做出贡献的用户才会获得令牌激励。KOMA CHAIN 的用户和/或未积极参与的 KMC 持有者将不会收到任何 KMC 作为奖励。

为了参与 KOMA 网络的共识流程，用户需要将 KMC 作为该用户对该流程承诺的指示。因此，KMC 也将被用作阻止各种违法行为（如无效区块，非法验证区块或无效交易执行）的威慑，要求他们在有权参与生态系统之前首先放置 KMC 代币。如果犯规者犯下了违法行为，将扣除 KMC。

七、KMC 法律声明

7.1 不可退款且不得以管理机构，发行人或任何关联公司兑换现金（或其他任何虚拟货币的等值）或任何付款义务;

7.2 不代表或授予代币持有人对管理机构，发行人（或其任何关联公司）或其收入或资产的任何形式的任何权利，包括但不限于获得未来股息，收入，股份的任何权利，所有权或股权，股份或担保，任何投票，分配，赎回，清算，专有（包括所有形式的知识产权或许可权），或其他金融或法律权利或同等权利，或知识产权或任何其他形式参与或与 KOMA，管理机构，发行人和/或其服务提供商有关的;

7.2.1 并非旨在代表差价合约或任何其他合约的任何权利，其目的或假定目的是确保盈利或避免亏损;

7.2.2 并非旨在代表货币（包括电子货币），证券，商品，债券，债务工具或任何其他类型的金融工具或投资;

7.2.3 不是向管理机构，发行人或其任何关联公司提供的贷款，并非旨在代表管理机构，发行人或其任何关联公司所欠的债务，并且不存在利润预期;

7.2.4 不向代币持有人提供管理机构，发行人或其任何关联公司的任何所有权或其他权益。

代币销售中的供款将由代理销售后由发行人（或其附属公司）持有，并且在代币销售之后，供款人对这些供款或该实体的资产不具有经济或法律权利或实益权益。如果 KMC 的二级市场或交易所确实发展，它将完全

独立于理事机构，发行人，KMC 和 KOMA CHAIN 的销售和运营。管理机构和发行人都不会创建这样的二级市场，也不会将任何一个实体作为 KMC 的交换。

八、风险

您承认并同意购买 KMC，使用 KMC 以及使用 KMC 参与 KOMA CHAIN 有很多风险。在最糟糕的情况下，这可能导致丢失已购买的全部或部分 KMC。如果您决定购买 KMC，您明确承认，接受并承担以下风险：

8.1 不确定的法规和执法行动：许多司法管辖区的 KMC 和分布式分类帐技术的监管状态尚不清楚或尚未解决。虚拟货币的监管已成为世界所有主要国家监管的主要目标。无法预测监管机构如何，何时或是否可以应用现有法规或针对此类技术及其应用制定新法规，包括KMC和/或KOMA。监管行动可能以各种方式对 KMC 和/或 KOMA 产生负面影响。如果监管行为或法律或法规的变更使得在该司法管辖区内运营成为非法，基金会，分销商（或其关联公司）可以停止在司法管辖区内的运营，或在商业上不受欢迎以获得在该司法管辖区内经营的必要监管批准。在咨询了广泛的法律顾问并对虚拟货币的发展和法律结构进行持续分析后，将采用谨慎的方法来销售 KMC。因此，对于代币销售，可以不断调整销售策略，以尽可能避免相关的法律风险。对于代币销售，基金会和分销商正在与香港的一

家精品公司律师事务所TzedekLawLLC合作，在区块链领域享有良好的声誉。对于 KMC 的出售，将采用谨慎的方法。因此，对于代币销售，可以不断调整销售策略，以尽可能避免相关的法律风险。对于代币销售，基金会和分销商正在与香港的一家精品公司律师事务所TzedekLawLLC合作，在区块链领域享有良好的声誉。

8.2 信息披露不充分：截至本文发布之日，KOMA 仍处于开发阶段，其设计概念，共识机制，算法，代码以及其他技术细节和参数可能会不断更新和更新。虽然本白皮书包含有关 KOMA 网络的最新信息，但它并非绝对完整，可能仍会由 KOMA 开发团队不时调整和更新。KOMA 开发团队没有能力和义务让 KMC 的持有人了解有关开发 KOMA 网络的项目的每个细节（包括开发进度和预期里程碑），因此信息披露不充分是不可避免和合理的。

8.3 竞争对手：各种类型的分散式应用程序正在迅速崛起，行业竞争日益激烈。有可能建立使用 KMC 和/或 KOMA 的相同或类似代码和协议的替代网络，并尝试重新创建类似的设施。可能需要 KOMA 网络与这些替代网络竞争，这可能对 KMC 和/或 KOMA 网络产生负面影响。

8.4 未能发展：由于各种原因，包括但不限于任何数字资产，虚拟货币或 KOMA 价格下降的事件，KOMA 网络的开发可能无法按计划执行或实施令牌，不可预见的技术困难，以及活动开发资金短缺。

8.5 安全漏洞：黑客或其他恶意组织或组织可能会以各种方式干扰KMC 和/或 KOMA，包括但不限于恶意软件攻击，拒绝服务攻击，基于共识的攻击，Sybil 攻击，smurfing 和欺骗。此外，存在第三方或基金会成员，经销商或其附属公司可能有意或无意地将弱点引入 KMC 和/或 KOMA 的核心基础设施的风险，这可能会对 KMC 产生负面影响。或者 KOMA。此外，密码学和安全创新的未来是高度不可预测的，密码学或技术进步（包括但不限于量子计算的发展）的进步，

8.6 其他风险：此外，上述简要提及的潜在风险并非详尽无遗，而且您购买，持有和使用 KMC（包括基金会或其他人）的其他风险（更具体地说，在条款和条件中有所规定）经销商无法预料到。这些风险可能进一步成为上述风险的意外变化或组合。您应该对基金会，经销商，其附属公司和 KOMA 开发团队进行全面的尽职调查，并在购买 KMC 之前了解 KOMA 的整体框架，使命和愿景。

附录 A：独立性（与利益相关方无关联）

本标准适用于战略决策委员会和顾问委员会的独立成员。

满足相关入选标准的独立性要求且符合下列所有分类标准的成员应视为“独立成员”：

成员本人及直系亲属均不担任基金会的合伙人、重要利益相关者，或任何利益相关者的高管。

成员本人及直系亲属均不大量持有 KMC。本标准下所称的 KMC 持有者应为重要的 KMC 持有者。

成员本人及直系亲属均不担任基金会的高管。

上述标准所称的“直系亲属”包括：配偶、父母、子女、兄弟姐妹、配偶的父母、子女的 配偶、养子养女、配偶的兄弟姐妹及任何共同居住人（家政服务人员除外）。

此外，在评估独立性时，战略决策委员会还会考虑其他相关事实和情况。

附录 B：参考文献

[1] V. Buterin. A next generation smart contract & decentralized application platform (Ethereum white paper), 2014.

[2] G Wood. Ethereum: A secure decentralised generalised transaction ledger (Ethereum yellow paper), 2014.

[3] S. Nakamoto. Bitcoin: a peer-to-peer electronic cash system, 2008.

[4] POA Network. Proof of Authority: consensus model with identity at stake, Medium (https://medium.com/), 2017.

[5] M. Castro and B. Liskov. Practical Byzantine fault tolerance, in the Proceedings of the Third Symposium on Operating Systems and Implementation, 1999.

POS Network. PROOF-OF-STAKE: Proof-of-stake underlies certain consensus mechanisms used by blockchains to achieve distributed consensus., Ethereum (https://ethereum.org/), 2023.