



白皮书

2020年3月12日

中国社区志愿者翻译整理

中文白皮书翻译自Thinkium基金会白皮书英文版
如有表述不一致的地方，欢迎指正。

目录

1 缘起	2
1.1 从无到有	2
1.2 平行世界	3
1.3 新起点	4
2 THINKIUM 世界	7
2.1 THINKIUM 新世界	7
2.2 THINKIUM 生态	9
2.3 THINKIUM 世界机制设计原则	12
3 THINKIUM 核心引擎技术	13
3.1 系统及模型分析.....	13
3.2 系统架构.....	14
3.3 共识协议实现.....	16
3.4 跨链消息和验证.....	19
3.5 网络算法.....	19
3.6 多链并行模型.....	20
3.7 身份及认证.....	21
3.8 隐私计算.....	23
3.9 开发体系.....	24
4 THINKIUM 上构建行业公链	26
4.1 优势和特点	26
4.2 搭建一条行业公链	29
5 THINKIUM 分布式商业	29
5.1 分布式商业的定义.....	29
5.2 分布式商业的发展路径.....	31
6 THINKIUM 生态发展和治理	38
6.1 THINKIUM 生态发展	38
6.2 THINKIUM 生态治理	40
7 THINKIUM 之约	43

1 缘起

1.1 从无到有

“人类的思想是由自私的基因构成的”，这是本能。

“基于深度认知的协作，是人类区别于其它物种的关键”，这是进化。

宇宙从大爆炸开始，从基础规则“一”开始，一生二、二生三、三生万物，基础规则的无穷力量不言而喻，只有永恒不变的规则“一”才能演变成现在的浩瀚宇宙。

生命也是来自那最初的规则“一”。地球的形成将近 46 亿年，35 亿年前单细胞生物出现、9 亿年前多细胞生物出现、700 万年前人科动物出现、20 万年前智人出现。个人、人类、地球、太阳系、银河系、宇宙，在这个链条中，每个后者都是由无数个前者组成。当我们再往链条的前面追溯，个人可以再细分到宇宙的基本组成，器官、细胞、分子、原子；原子还可以再往下分几层到基本粒子，这些最基本粒子之间遵循一些基本的规律相互作用，一花、一叶、一世界。

单个“一” 整体“一”

每个生物都是独立的个体，都自成体系。由于物质和能量的有限，每个个体内在机制的首要目标是延续生命，因此人生来是以自我为中心运转的，而且生物进化使得生命体越来越复杂、遗传信息越来越多。每个个体内部不断的进行物质和能量的更新，但同时又和环境进行物质和能量的交换，形成个体新陈代谢、种群生态、生物生态。种群内部协作也是无数年进化的结果，并融入到先天基因和后天传承中，故蜂群能够修建复杂的蜂窝，候鸟集体迁徙，狼群集体捕猎。

独特的“一”

人类是地球上生命进化的顶端，具备比其它生物高很多的智商。人类强大的思考能力加上高效的信息工具（语言、文字），沉淀了强大的人类文明，并形成人类共同的追求，使得人类的创造力真正无限，并具有主动改变和创造世界的的能力，但这不是单个人的能力，而是整个人类的能力。

整体“一”的发展

人类通过对宇宙不断的认知，并创造新事物来使自己变得更加强大，创造新事物的能力也越来越强。从石器、青铜、铁器、蒸汽、电气到信息，工具越来越强大。人类创造世界越来越依靠智力而不是体力，让一切为人类所用，让事物按照人类的意图运作。人类基于宇宙原有规则创造了一套新规则和世界，并不断加大对原来宇宙的改造和融合。在整个过程中，起到基础作用的是人类社会自身的基本制度。社会制度不断的演变和发展，目的就是协调和激励每个人都发挥自己的作用，并对整体人类带来最好的效果。社会制度反映的是人的利益，是每个时期社会认知上的公平与正义。

1.2 平行世界

计算机世界是人类基于物理世界创造的“平行世界”。早期人类发明算盘、计算尺、机械计算机等都是计算机，只是靠人力、机械来驱动。现代计算机的底层计算其实是逻辑计算，虽然计算与逻辑密不可分，但逻辑并不等于数学计算，数学计算可实现加法乘法，而逻辑主要是与或非等。二进制的发明将逻辑学和数学计算进行融合，可以把数学计算转化为逻辑运算。但这些都只是理论，直到二进制数字电子电路设计和逻辑应用，将二进制运算与电子器件相结合实现逻辑运算功能，这才真正是电子计算机的实现。它成功将人类思维和物理世界关联在一起，使得人类思维可以脱离人而单独运行；同时，人类将物理世界的各种信息数字化并编码成二进制，也可以通过反编码把二进制翻译成物理信号，开启了“平行世界”。

单台计算机就像单个人，能力有限，互联网技术的出现彻底改变了这一格局。互联网技术最早来自美国国防部支持的技术，也就是后来的互联网通信协议TCP/IP，计算机使用这种协议互联互通。最开始，计算机的主要目的不是给个人用的，是用来解决军事、科研等重要问题的。到了商业互联网，有了数量庞大的个人计算机，上层逐渐演化出搜索、社交、网上购物等应用场景。随着移动互联网、大数据、AI、物联网的发展，人类基本生活行为都开始融入到计算机世界中，真正开始了人类的“平行世界”。

“平行世界”的社会制度

“平行世界”发展到今天，基本沿用的是人类物理世界中部分制度的子集，但是“平行世界”中“人”的主权、利益和物理世界已经发生了根本性的变化。虽然全球人类一直也在不断的探索，例如反垄断、数据主体、隐私保护等，但是都没有找到很好的解决办法。“平行世界”其实是由割裂的、可能突然消失的部分组成，是少数人控制的世界，里面对“人”利益的定义非常原始，更加无法体现公平正义。曾经打着协作、自由、共享、反垄断的互联网巨头，为了自己的商业利益，成为了新的更大垄断者，垄断了本该属于用户自己的绝大部分利益，无所不用其极地争抢用户时间、行为、思想以及源源不断的数据，并将这些封闭在自己的平台中，以达到把用户锁定在自己平台上的目的，甚至用这些反过来操纵和伤害用户。社会生产力和生产关系的发展是社会制度发展的根本原因，而当前这些都严重阻止了人类生产协作效率的进一步提升，同时也抑制了全人类创新效率的提升，因此需要在平行世界中进行基础规则的重构。

1.3 新起点

在“平行世界”中，我们希望有一个底层制度能够给我们一个更加公平、更有希望的未来，“人”不再是“木偶”。在新世界中，底层制度能够清楚的定义每个“人”的利益，并提供一个公平公正的规则演化的土壤环境。这是一个可信的世界，每个人都有一个不断积累和成长的“我”的存在，这个“我”、“你”、“它”“基于不同的”规则“协作，并延伸到物理世界。这样，人类能够更加信任地进行协作，而不是各种勾心斗角、尔虞我诈。

这一切在遇到区块链的那一刻发生了变化，开始了一个新世界。

什么是区块链？到现在，还没有让大家满意的统一答案，原因主要有三点：一是区块链的起源问题，区块链是由比特币系统发展而来，比特币系统的重点在比特币，功能单一，早期相信和研究它的人更多专注在金融属性，后来慢慢演化到关注技术，人们才了解比特币只是第一个区块链应用，因此影响力比较大；二是区块链涉及的内容较多，既有金融、社会组织等社会学内容，也有计算机、密码学等自然科学内容，不同的研究者会把它归到不同层面来讨论，会有不同的话语体系出现；三是区块链现在的发展正处于百家争鸣的阶段，出现很多不同的派别，而且谁也无法说服其他人。这些原因导致普通用户对区块链的理解出现混乱，

同时也被部分人利用来进行虚假宣传。

通过一些典型系统来看区块链的基本发展，可以理解过去，思考未来。

比特币系统是基于中本聪论文设计（名字为《一种点对点的电子现金系统》，2008 年底）的开源软件，用户基于该软件建构一个点对点网络系统，比特币是这个网络系统上依据特定算法（共识算法、PoW）产生的一种总量恒定的加密数字资产，这个算法促使点对点网络中的节点构成不可篡改的分布式账本来确认并记录所有比特币转移支付行为，基于非对称加密算法的账户体系使比特币只能被真实（掌握私钥）的拥有者转移支付。

以太坊是基于以太坊白皮书设计（2013 年 11 月初版）的一个有智能合约功能的开源区块链平台，以太坊系统通过提供虚拟机来处理智能合约。和比特币系统比，它允许用户在上面运行比交易更加复杂的业务。

Hyperledger Fabric 是一个联盟链开源构架，提供一个模块化的构架，允许组件即插即用，如节点用户、共识算法等，在 2015 年底由 Linux 基金会启动，早期由 IBM 等企业贡献代码。

这三个系统，一个是区块链的起源，一个是区块链由单一功能转向支持二次开发的标志性系统，一个是联盟链的标志性系统。前两个是公链系统，允许用户无需许可成为系统网络中的节点，联盟链是节点需要允许才能加入系统。

早期区块链系统基本设计逻辑

在区块链系统中，节点一般指的是运行区块链系统程序的网络计算机，由用户自发购买服务器、安装运行系统、连接到系统网络中，通常情况下每个节点运行的都是同一个程序，这些节点通过点对点网络通信技术相互连接。不需要许可意味这个系统的节点是用户自发搭建的，不是由一个中心化的个人或者公司来搭建，只要有人运行节点并加入到系统网络中，这个系统就会一直运行下去，同时无法被特定的人控制；需要许可意味着这个系统是由确定的个人或者组织来负责搭建这套系统，并被这些节点控制。

从时间线来看，是先有了不需要许可的公链，后有需要许可的联盟链，这是对区块链技术的一种扩展，也是业务场景的延伸。公链系统的基本思想是由不需许可的节点运行同一程序组成一个系统。与中心化系统区别很明显，普通用户随

时可以参与到系统的构建中，系统的运行权不再是单个主体。需要许可的联盟链系统和中心化系统的区别主要在于，系统的运行权不再是单个主体，而是多个主体共同运行，但是普通用户无法参与。

区块链通过共识算法来确保不同节点记录的信息都一样，算法机制写在区块链系统的代码中，每个节点都按照这个机制来运行；算法确保在每一轮，这些节点都往各自系统中写入同样的数据；节点每一轮写入的数据用区块方式存储，同时通过密码学和链式结构确保节点上上一轮区块也是大家认可的，并形成可验证的链式关系，最终确保每个节点存储的这条不可篡改的区块链是一样的。公链主要采用的共识算法有 PoW、PoS、DPoS 等，而联盟链主要的共识算法是 raft、pbft 等，因为节点数量相对固定，而且安全性相对可控，所以联盟的这些共识算法都是传统分布式算法中的经典算法。

传统共识算法主要通过相互多次通信的方式来解决，但是支持的节点规模数量有限，比特币通过引入经济机制（PoW 算法），能有效的解决节点去中心化问题，但降低了共识效率。引入经济机制的共识算法同时也解决了公链节点加入的动力问题。搭建节点是要付出成本的，但公链系统中是没有一个中心化组织为大家付费，也不能有这样的组织（否则公链系统就会被这个组织控制），所以公链节点只能靠自愿，而联盟链的节点和上层业务提供者一般是同一组织，有明确的商业逻辑。比特币共识算法融入了去中心化经济机制，既解决了节点数量和安全性问题，也激励节点自愿加入，这种创新的设计造就了区块链技术。

从前面这些区块链的概念、产品和逻辑来看，十分局限，“平行世界”需要的是一个永不停息的可信核心引擎，为“平行世界”提供运行支撑，引擎上运行着不可更改的各种规则，引擎的当前和历史状态都可被验证，永远可信。“平行世界”基于这个引擎重新定义“人”，重新定义底层制度。这个引擎就是我们对区块链的定义。

2 Thinkium 世界

2.1 Thinkium 新世界

新世界的诞生

世界是指某个时空中所有的集合，通常是指地球、宇宙。人类在物理世界之外又创造了“平行世界”，但“平行世界”更像是物理世界的简单延伸，充满着不确定，而且时空混沌。

Thinkium 世界（后面简称 Thinkium 或者新世界）是从混沌“平行世界”孕育出来的一个新世界，原点来自支撑这个世界的 Thinkium 核心引擎，这就是我们一直寻找的不一样的“区块链”。为了支撑这个世界，Thinkium 核心引擎必须足够强大，不仅能够永不停息的可信运行，同时要无限制的支撑这个世界的成长、演化、变化。

新世界有着底层的时空元规则，并由 Thinkium 核心引擎执行并辐射到世界内部任何地方；新世界由原点开始，并基于元规则演化成长，整个过程按照时间轴被完整不可篡改的记录，形成稳定的四维时空；新世界基于底层元规则演化创造出无数的上层规则，并基于 Thinkium 核心引擎的稳定执行，来保障 Thinkium 的成长和繁荣。

传统“平行世界”的网络空间是割裂的，人的信息和思维被存储在不同的碎片空间，而且碎片空间随时可能消失；时间在“平行世界”随时可被修改，任意时刻的信息可以被任意篡改，世界中的“主体”可被任意抹杀。这一切在 Thinkium 中不再发生，让人类思想世界不再混沌，全人类思想在 Thinkium 中有序、高效成长，共同创造无数的经典信息和思想，整个 Thinkium 高度统一、协调，并因此帮助人类在物理世界中的成长和繁荣。

Thinkium 核心引擎

Thinkium 核心引擎是 Thinkium 的核心和源动力，在新世界诞生之前，它是一套由“设计者”创造的机制，并用计算机语言实现。当第一台计算机运行 Thinkium 核心引擎后，新世界就此开始诞生，成为那个“一”，随着越来越多的计算机运行 Thinkium 核心引擎，新世界变得越来越强大和稳定。Thinkium 核心引擎把所有加入的计算机凝聚成一个可信计算平台，为 Thinkium 世界提供永续

的可信计算运行能力。当 Thinkium 开始运行后，允许人类通过二次开发接口在底层规则上制定新的规则，并由它来协调管理这些规则和底层计算资源，同时提供交互接口。

新世界必然会有大量的创业者、开发者来重构升级现有“平行世界”的规则制度逻辑，同时也会衍生出无数的新业务，因此需要一个无限可扩展、安全可信、方便易用的引擎来承载各种规则、资产、数据和业务逻辑，支撑起互联网级的海量应用与用户。要做到这一点，就必须站在更高的维度、以更远的视角来进行设计。

Thinkium 核心引擎的设计是站在前人的肩膀上，在一颗永不放弃追求的“人心”支持下，融入对客观世界理解、对人类社会的期望、对人性的尊重、对科技的渴望而不断迭代而成。

在 Thinkium 核心引擎的设计过程中，我们暂时沿用传统的“公链”概念来描述其基本逻辑。Thinkium 核心引擎运行着无数的公链，公链一般包括上层和下层，下层是公链底层，定义基础规则，保障链上各节点共识得以达成，上层是应用层，部署各种业务逻辑规则，解决不同场景的业务需求。公链从协作角度看，是一群达成共同认知的人，共同遵循的一套行为规则；从建设角度看，无需许可就可以成为这个公链的建设者；从使用角度看，每一个人可以自由创建由自己掌控的账户，使用链上服务；从经济角度看，需要创建一套支撑自己永不停息运行的经济机制。

比特币创建第一个应用，很多人效仿，但需建立新的区块链网络；以太坊让发行数字货币变得简单，很多人尝试在以太坊上部署业务，但受限于性能瓶颈转头搭建自己的区块链，由此诞生万链并存，进一步催生跨链技术；但各链间巨大的不同，互通成本高，且链的可扩展性严重不足，发展空间受限。由此诞生“三难”问题：建链难、跨链难和扩链难。

首先是建链难，单链无法满足实际需求，故需要搭建很多不同的链，目前建链成本很高，需要承担巨大研发成本和安全风险，经常发生黑客攻击事件，轻则社群共识急剧萎缩，重则价值归零；其次是跨链难，很多区块链在设计之初没有考虑链间互通，导致跨链交互困难，难以形成统一区块链网络和繁荣生态，跨链技术出现后，也因为所跨链自身性能问题等，导致跨链生态应用发展受限；最后是扩链难，区块链项目都面临一个致命问题，就是网络性能（TPS），这直接决定

可承载的业务复杂度和用户规模大小。

Thinkium 核心引擎在解决去中心化、一致性、可扩展的“不可能三角”问题的基础上，为行业公链建设提供了针对“三难”问题的完美解决方案，并称之为“公链的公链”。Thinkium 核心引擎这种“公链的公链”方案，让任何人能够独立自由在其上搭建各种行业公链，且行业公链具备互通、可扩展的基础能力，为 Thinkium 扩展到各行各业，为大规模应用落地、服务社会中的每一个人提供可能，推动社会各个领域的深度高效协同，并最终产生更大的社会价值和经济价值。

Thinkium 是一个开放的世界，其规则会层层延伸，影响物理世界。在很多场景下，规则的延伸需要集中式系统、联盟链和公链三者共存。Thinkium 核心引擎基于统一的协议能够很好的支持联盟链和公链的可信融合，一方面，公链和联盟链互相同步有限数据证明数据的可信；另一方面，联盟链也可以确保自身数据的隐私性，数据必须在获得授权的情况下才可以访问。这样的架构能够很好的将两个世界规则进行连通，在利用区块链的同时，符合物理世界当下的商业、法律等方面的规则，来确保更多场景更快的落地。

2.2 Thinkium 生态

Thinkium 给所有主体提供一个自由、平等、开放、公正的环境，为每个主体提供非常友好的参与“接口”和“界面”，尊重每一个主体在 Thinkium 中的“权利”。

Thinkium 中不同的主体基于不同的规则相互作用，并延伸到物理世界，随着更多的主体和规则加入，这些主体及相互之间的关系变得更为复杂，我们称为 Thinkium 生态，也是当前这个阶段 Thinkium 的主要内容。

2.2.1 Thinkium 生态概述

Thinkium 生态遵循自然成长与进化，生态成员之间相互促进、相互制约。

底层系统是区块链的支撑系统，为整个生态提供储存能力、计算能力、通信能力，运行着由链开发者加密编程写入的规则，为开发者提供安全、可信、便捷的操作平台。开发者不需要从头开始构架或分叉代码，免受底层区块链技术开发的巨额成本负担，通过调用系统合约或开放接口即可开发行业公链、分布式商业

应用、DAO 应用、通用工具等。

随着一批批开发者的参与创造，Thinkium 生态将会扩展更广的应用范围，各类分布式商业及 DAO 应用必将涌现，诸如：去中心化的社交、媒体、搜索、娱乐、游戏、电商、租房、出行等，产生更多能量、更多用户、更多资产、更多需求，推动生态发展。

Thinkium 把数据控制权还给用户。个人所有的行为、信息、数据等数字资产都得到有效保护，个人数据储存在分布式的数据中心，由区块链进行访问控制，任何机构或个人读取都需获得本人的授权；资产以通证的方式存储在链上，能够在整个生态中自由流通，随时可验证、可追溯、可交换。

每个用户通过私钥 ID 成为生态的住民，不仅可以更加自主、安全地使用各类应用，还能够以无地域限制、不依赖个体间信任的方式进行生态内协作。基于通证激励机制，用户组成一个个的分布式经济体，在生态内部进行充分的互动和流转，并演化成一张巨大的共享生态价值网，与现实世界互相辉映、共同发展，成为现实世界的一个“映射”和延伸。

2.2.2 Thinkium 生态系统结构

Thinkium 生态系统是开放的，激励和吸引越来越多的成员参与其中，主要包括以下组成部分。

底层系统：是整个 Thinkium 生态的支撑系统，以分布式的方式运行着不可更改的各种规则程序，负责数据储存、信息交互、验证等，提供安全、便捷、高效的部署环境，支撑海量应用和用户的发展。

行业公链：是基于 Thinkium 核心引擎构建出来的行业区块链基础设施的集合，通过其上建立的各种行业基础规则和 Token 发行，组织、人、程序等基于这些规则公平协作、降低成本、高效创造，重构行业生态。

联盟链：是为分布式商业应用落地而搭建的，分布式商业主体可以自行搭建、也可以通过 bass 平台租赁使用。通过指定多个预选的节点为记账人，每个块的生成由所有的预选节点共同决定，与 Thinkium 核心引擎的底层进行信息交互，任何第三方可以通过授权进行访问查询。

通用工具：是开发者针对用户的需求或者想要提供的服务，基于底层系统或

行业公链开发的各种智能合约、跨链协议、行业协议、节点软件、钱包、D-store、DAO 工具、交易软件等，为个人应用或上层场景应用提供工作框架或相关支持。

DAO 应用：是通过 Thinkium 核心引擎的底层系统或行业公链的开放接口，对原住通用工具的大量移植并衍生新的物种，开发迭代海量 APP、Web、小程序、PC 产品等，为用户提供个性化的服务。账户、数据、资产均在链上、控制权归用户所有，用户通过私钥可自由选择应用进行数据迁移。

数据中心：是分布式商业及 DAO 应用的核心枢纽，对生态用户在使用过程中产生的数据进行存储、分析、计算、分发等，由独立的数据链进行访问控制，通过区块链规则让用户的数据权益得到有效保障，用户在使用过程中产生的数据都归属于自己，任何主体调用都需要经过用户的授权并支付相应的报酬。

通证：是指 Thinkium 生态中可流通的数字权益凭证，包括底层资产 TKM、行业公链发行及分布式商业主体发行的 Token，通过跨链技术在 Thinkium 生态内可以进行直接流转和交易。

链开发者：是指参与区块链底层系统的研发、迭代、维护，或提供相关技术服务的研发人员或科研机构。

应用开发者：是指基于合约或操作平台进行开发的组织或个人，通过提供的开发工具，完成包括行业公链、通用工具、DAO 应用、分布式商业应用等软件或工具的开发。

节点：是指运行区块链系统程序的网络计算机，通过自行购买服务器、安装运行系统、连接到系统网络中，分为数据节点、共识节点、普通节点三种。数据节点负责其所在链全部数据的存储以及链与链之间信息的交互；共识节点负责其所在链的运算、打包以及共识；普通节点只是承载业务，不参与共识。节点从数据存储、打包交易、生成区块或其他过程中获得 TKM 奖励。

社区：是 Thinkium 生态的入口和重要推动者，每个企业或个人都可以组建自己的社区，开展或提供节点部署、发行公链、开发应用、推广用户、生态咨询、金融投资等生态建设工作，或者协同开发者进行应用推广，通过有参与感、有激励性的市场方案，让更多的人参与应用共建。

用户：包括生态资产通证的持有者及各类应用的使用者。每一个用户可以根

据自己的能力和喜好加入不同的社区，为生态提供服务、协同创造或参与生态建设，根据贡献得到公平、公正的奖励。

2.3 Thinkium 世界机制设计原则

Thinkium 有其底层的基础规则制度，也有基于基础规则制度演化和制定的新规则制度，Thinkium 的演化成长和制度的设定变迁是分不开的。

制度是内生演化和人为设计共同作用的结果。“自然”演化与有意识的设计，在许多制度的产生与变化方面，均起着十分重要的作用，两者是一种互补而不是竞争的关系。在 Thinkium 中，单靠制度自身演化有时会耗时过长，成本过大，需要用新的制度设计来纠错、矫正，促进新发展。

制度变迁是一个动态博弈的过程，前一个博弈的结果构成后一个博弈的前提，如此迭代下去，后一个博弈的规则由前序博弈累积的规则而决定的。Thinkium 的基本规则和根本制度会内嵌于世界上层的各种规则之中，它们构成了规则的规则。表层制度机制的可实施性源于基础性的元制度，即元博弈的结果决定了后续博弈的结构，前者中的博弈者随之变为后者中的执行者。

资源的有限性和欲望的无限性是经济学的一个基本矛盾，这个矛盾在 Thinkium 中同样存在。需要通过治理，设定激励机制与制度约束，在“理性人”假设下，每个人都从自己利益最大化的利己角度考虑和决策，也会让整个世界变得有序和更好。

在 Thinkium 的机制设计里，会有“设计者”或者“治理者”的角色存在，其目标即为整个 Thinkium 的目标，是整个 Thinkium 的用户达成的一种共识、约定、规则。

3 Thinkium 核心引擎技术

3.1 系统及模型分析

Thinkium 核心引擎通过共识协议确保在不同计算节点上运行相同的内容，并允许任何节点在无需获得权限许可的情况下加入。同时一个有效的系统应具有以下两个基本属性：安全性，所有结果是正确的；活跃性，每个有效请求都会在一个固定（小）的时间内处理。

Thinkium 核心引擎从解决现实商业中的问题出发，必须能够支撑起海量用户级别的应用，必须解决公链的去中心化、一致性和可扩展性问题，并满足分层多链并行能力、快速交易确认能力、高频交易承载能力、极高系统安全性与可用性、智能合约的图灵完备性、系统的高灵活性与高可扩展性、方便易用的开发能力、数据隐私保护能力等。

我们通过定义基于交易的区块链模型，量化去中心化、一致性、系统吞吐量、可扩展性等参数指标，并提出相关的函数，构建可量化分析的区块链模型，最后设计了一个高效的共识协议模型。

1、区块链系统的去中心化关键是共识的去中心化。去中心化的主要目的有两个：系统的结构分散，使其不会因为少数节点的掉线、叛变或遭受攻击而失效；共识由系统参与者共同完成，增加了系统的透明度和可信度，避免系统被寡头控制。

2、区块链是一个去中心化系统，没有中心节点来维护区块集合。共识算法使不同节点维护同一个集合，从而达成一致。然而系统中可能存在节点作恶，从而影响其他节点的操作和全网的一致性。同时由于网络延迟和共识等因素，无法保证任意时刻全网节点数据的强一致性，只能保证弱一致性。

3、区块链系统的性能主要体现在系统确认交易所需的时间，一般用两个参数刻画：确认时间（一笔交易确认所需时间）和吞吐量（单位时间内最多可完成确认的交易数量）。确认时间是用户进行一笔交易的最短周期，如果一个系统的确认时间很长会造成用户体验不佳，限制系统的应用场景。如果吞吐量太小，不足以处理所有交易请求，就会有一些交易被堵塞或丢弃，造成整个系统的延迟提高。对性能的讨论只有在系统满足去中心化和一致性才有意义。区块链系统确认

一笔交易，需要保证所有参与者达成共识，为了优化性能，应该改进共识算法的计算复杂度和通讯复杂度。

4、当区块链系统达到其处理瓶颈时，它必须丢弃多余请求，使系统可用性降低，因此需要可扩展性突破系统限制。区块链可扩展性包括系统吞吐量可扩展、负载可扩展性、功能可扩展性和更新可扩展性。我们设计了一个评估区块链系统可扩展性的模型，并分析得出区块链系统应通过并行性来达到可扩展性。

5、共识算法效率的因素主要包括共识计算延迟、共识通讯延迟和共识权限分配延迟，为了提高共识机制的效率，需要在确保系统去中心化和安全性的前提下，对上述因素进行优化。我们通过分析具体优化方法，得出在一个性能需求快速增长的系统当中，仍然可以通过增加链数目来满足系统的性能要求。

6、基于上面的理论模型分析，我们系统设计了一套高效的、可扩展的、去中心化的、安全可靠的共识协议模型。在该模型中区块链系统为树形结构，树的每个节点代表一条链，非叶子节点代表结构区块链，负责对其所有子节点对应的区块链的节点集合和区块集合进行共识；叶子节点代表交易区块链，负责对交易数据子集进行共识。区块链的条数随着数据交易集合大小的变化而动态调整。通过证明，该区块链系统满足去中心化条件，且性能不随着系统节点数目和交易数据集合大小的增加而下降。

3.2 系统架构

3.2.1 分层多级链结构

Thinkium 核心引擎的链结构是分层多级链结构，链按功能分为主链和业务链两种，每条链都是具有自己状态的完整独立系统。主链充当整个系统的领导者和协调者，它作为业务链的切入点和信任来源，记录每条业务链已确认区块的元数据和摘要，产生所有链的委员会选举中使用的随机种子，并记录选举结果。同时，来自业务的工作负载由所有业务链共同承担，并使用基于 Actor 模型的消息驱动协议进行合约并行计算。系统中的所有节点都保持主链的状态，通过更新和验证主链的区块，节点可以验证已经包括在主链中的业务链的任何区块数据。该结构具备以下主要优点：

- 节点加入系统只需要从可信源获取主链的当前状态，或者从创世块重建，

并不需要同步整个系统的所有数据，这使得整个系统的负载大大降低。

- 每条链的共识是独立和并行执行的，大大降低了对网络带宽和计算处理要求。
- 主链可以充当系统的协调器，它提供跨链同步，并允许整个系统拓扑是动态调整的。
- 节点可以使用主链中的摘要和 Merkle 证明来验证从另一个业务链发起的事务。因此，业务链的区块生成者不需要来自其他业务链的任何信息来处理链间交易。

可以按照不同的事务类型或商业主体，划分出不同的业务链进行单独运行。他们之间可以完全无关的独立运行，通过主链提供的佐证进行跨链通信，也可以把有从属关系的链组成有依赖的父子关系链，其中子链继承部分父链的属性，例如在这条链上的账户余额的货币类型、链的选举方式等。

Thinkium 核心引擎允许每条业务链向下扩展自己的子链，但实际使用中，基本会在三层以内都可以解决问题。无论是主链还是业务链，都有可能因为请求过多而拥堵变慢。当发生拥堵时，可以通过将该链分片的方式，把请求分散到不同的分片上，以求提高该链的吞吐能力，随着分片的数量增加，该链的吞吐量线性增加。分片本身也是一条独立运行的链，分片之间会有针对跨分片交易请求的并行模型，大大提高分片链间的跨片交易执行速度。

这种分层多级的结构具有很好的灵活性和可扩展性，并且可以动态调整，因此每个链都不会成为整个网络的性能瓶颈。此外，随着链的数量增加，整个系统的吞吐量线性增加，而不会产生太多的冗余消息。

3.2.2 四层系统结构

基于上面的分层多级链结构，设计了一种四层实现框架，以方便系统将来的可扩展和升级。

第一层主要解决全系统总体共识，主要负责划分请求和节点，并将不同的请求分配给特定的委员会进行处理。所有请求首先发送到任务层，在那里它们将被分割并分配给不同的委员会进行并行处理。由于并非所有请求都可以并行处理，因此需要根据其类型进行划分。此外，所有活动节点都在任务层注册。这些节点

以随机方式被划分到不同的委员会，并被分配不同的请求。我们需要确保每个委员会都是可信的，即每个委员会内部的恶意节点比例不会超过系统设定的某个阈值。

第二层主要解决单链共识问题，需要处理分配的请求并生成日志。每个委员会包含一组节点，当委员会收到给定请求时，它需要处理请求，达成共识并生成日志。由于每个委员会的可信度由上层保证，因此该层只需要考虑如何尽快在委员会中达成共识。

第三层主要解决多链之间的共识，每个委员会生成的日志和请求数据会根据特定的编码方法进行聚合，以形成单一的日志。系统的目标是每个节点生成一致的日志。因此，需要聚合算法来集成委员会中节点生成的所有日志，并达到统一日志。还需要编码方法来减少每个节点的存储。此外，由于节点会不时地加入和离开委员会，因此必须使来自数据层的相应数据进行同步。

第四层是网络层，它是在节点之间建立连接并提供通信的基本层。该层是整个系统的基础，为计算节点之间建立通信。在网络层内，我们可以构建一个多层网络，为每个委员会建立一个共识网络层。

3.3 共识协议实现

在 Thinkium 核心引擎中，每一条链中都存在三类节点：数据节点，共识节点，普通节点。数据节点负责其所在链全部数据的存储以及链与链之间信息的交互，共识节点的主要职责为所在链的运算、打包以及共识，普通节点不参与共识可以验证数据，一般用来承载业务。每次参与的共识节点是随机分配的，他们会随着时间的变化而不断重新选拔。

3.3.1 委员会选择

为了抵制对无权限系统模仿出多种身份进行的女巫攻击，我们使用基于股权证明（PoS）的选举算法。在 PoS 机制中，共识参与者的记账权取决于其拥有的资产。在我们的共识算法中，共识参与者通过提交押金的形式证明自己的权益。系统通过随机算法，定期按照押金的比例选取一定数量的参与者组成委员会负责一段时间的出块。

由于每次出块只需要选出来的委员会成员参加，因此在多链系统中，每条链

的委员会可以同时存在，相互独立地运行。随着网络中的节点数量增加，可以支持同时运行更多的子链，从而高效地利用节点的资源。

选择算法需要以下安全属性：

(1) 每次选举中当选的委员会成员中诚实比例不能低于共识算法的安全要求，算法应该是公平的，每个参与者投入越多，被选择的概率越高。

(2) 委员会成员应该是流动和不可预测的，以便对手不能通过腐蚀委员会成员来攻击系统（假设腐败的时间超过了委员会的寿命）。

首先，在选举之前，由于所有节点只监听主链，所以当需要选择下一个委员会时，子链必须在主链上发出信号。所有链的选举都在主链上进行，通过主链上的摘要信息，主链可以收集到各条链的选举状态，进行汇总发布。同时，主链上会周期性地生成随机种子，用以保障各条链选举的随机性。

愿意参与共识的节点需要通过发送特殊类型的交易在主链上注册，质押要求。主链发布选举信息后，共识参与者可以在主链上看到选举信息，使用对应的随机种子和自己的私钥计算一个可验证随机函数的值，以此决定自己是否被选中。当一个节点发现自己有权力加入某条链委员会，它会先加入这条链的网络，在其中发送自己的 ID 和可验证随机函数证明，这些信息会被当前的委员会记录。同时，新加入的委员会成员需要加入委员会的网络，同步子链的状态等，使用主链上的摘要进行验证等，为参与共识进行准备。选举的公平性对于系统的安全至关重要：如果攻击者可以在一个委员会中占据多数席位，这个委员会就没有办法正常出块，需要保证随机种子不能被操纵。

3.3.2 委员会的共识

我们假设委员会内部存在部分同步通信模型，其中存在有效的拜占庭容错算法，并为此设计量身定制的 PBFT 变体 TBFT 算法。委员会只占全网节点的一小部分，并且他们会自己组建一个规模更小的网络以降低广播的延迟，因此得以稳定高效地出块。由于 PBFT 算法的性质，当委员会中的节点满足弱同步假设时，在恶意节点不超过一半的情况下，出块算法就能安全地运行。因此，在选举算法安全的前提下，每个委员会出块的活性、正确性和唯一性可以得到保证。此外，我们的押金和惩罚机制，使得委员会成员作恶需要付出很高的代价，由此鼓励用户不作恶并举报其他人的恶意行为。

节点的执行可以以轮划分。每轮包括三个阶段：提案，准备和确认。状态转换是事件驱动的。为了在出现网络故障或恶意攻击时保持系统活跃性，本地时钟可能会触发超时。

提案阶段：委员会的负责人向其他委员会成员广播拟议的议案。

准备阶段：每个委员会成员收到建议的块后，会广播一条包含该块的签名的消息。如果在收到建议的块之前触发超时，则委员会成员签署并向其他委员会成员广播特别消息（表明领导者有缺陷）。

确认阶段：在准备阶段结束时，每个委员会成员签署并广播一份在准备阶段收到的签名。签名聚合可用于显着减少确认阶段中的消息大小。

根据在确认阶段收到的消息，每个委员会成员可以决定是否已达成关于该块的协议，并广播商定的区块或空块以及其决定的证据。

恶意节点惩罚。在检测到明确行为不当的节点的情况下（例如，在同一阶段向不同节点发送不同消息的节点），该轮将通过输出空块而中止。但是，行为不端的节点将受到大量的经济惩罚，使得这种攻击不可持续。如果在准备阶段收到的签名数量意味着大多数诚实的委员会成员已收到相同的提议块，委员会成员可能会达成“早期共识”：成员可以在确认阶段之前使用签名输出该块作为协议的证明（与常规协议相比的不同形式），节点仍需要参与确认阶段。

3.3.3 安全分析

设 N 是节点数， n 是委员会中期望的节点数， m 是委员会的数量。恶意节点的数量是 λN 。当委员会中的超过比例 ρ 的节点是恶意节点，我们说委员会选举失败。不失一般性，我们设置 $N = n \cdot m$ 。假设有一个完全随机的 oracle $O: [N] \rightarrow [m]$ 。固定一个委员会，定义 A_i 成为委员会中恶意节点的比例 $i > \rho$ 的事件。那么对于每一个 $i \in [m]$ ，我们都有

$$\Pr[A_i] = \sum_{x=\rho n+1}^n \frac{\binom{\lambda N}{x} \cdot \binom{(1-\lambda)N}{n-x}}{\binom{N}{n}}$$

通过 union bound，我们可以得到

$$\Pr[\cup_{i \in [m]} A_i] \leq m \cdot \Pr[A_i]$$

对于适当的参数设置，我们可以确保事件发生的概率是可以忽略不计。

3.4 跨链消息和验证

在多链系统中，跨链操作是不可避免的。每个链都需要处理由其他链生成的一些消息。我们的系统中有两种跨链消息（参见后面的多链并行）。第一种是从 C_i （链 i）到 C_R （链 R）的消息 m_i ，其包含 C_i 块的摘要。消息 m_i 用于 C_i 块的最终确认，并且每个区块只有唯一一个这样的消息。第二种是从 C_i 到 C_j 的外部中继消息 $m_{i,j}$ 。在 $m_{i,j}$ 被发送到 C_j 之前，它被记录在 C_i 的区块上。

在处理这些消息之前，我们应该先验证它们。验证链产生的消息有两种方法：（1）验证签名；（2）验证消息哈希。这两种方法都很有用，具体取决于消息的类型。对于从 C_i 到 C_R 的消息 m_i ，它附加了 C_i 委员会成员的签名，可用于验证真实性。由于 C_i 的委员会成员记录在 C_R 中，因此 C_R 中的每个节点具有 C_i 的当前委员会成员的公钥，并且可以验证 m_i 的签名。

对于从 C_i 到 C_j 的消息 $m_{i,j}$ ，它带有可以验证的证明 $\pi_{i,j}$ 。在 $m_{i,j}$ 被发送到 C_j 之前，它被记录在 C_i 的区块上。在 C_i 的区块上，有一个 Merkle 树 T_i 用于记录所有外部中继消息。证明 $\pi_{i,j}$ 指的是从 Merkle 树根到其入口的路径上的所有兄弟节点的哈希值。 T_i 的根哈希包含在 C_i 的摘要中。由于 C_i 块的摘要记录在主链 C_R 中，并且 C_j 中的每个节点也是 C_R 中的节点，因此 C_j 中的每个节点都可以获得 T_i 的根哈希并且通过证明 $\pi_{i,j}$ 。

不使用签名来验证 $m_{i,j}$ 的原因是为了防止 C_i 委员会成员不完全可靠的情况。此区块生成的消息只有在其块最终被 C_R 确认时才会生效。但是，对于同一子链 C_i 的交叉分片消息，其验证速度可能更快，只需等到摘要记录在其子链 C_i 上，而不是主链 C_R 。

3.5 网络算法

作为高吞吐量区块链的瓶颈，P2P 技术作为区块链网络的潜在技术已经引起越来越多的关注。在区块链中，由于需要大量的数据广播操作，效率和冗余是所

有区块链 P2P 网络设计必须注意的关键问题。

传统的区块链 P2P 网络(例如比特币和以太坊)通常基于非结构化设计思想。在广播时,部分广播机制适于减轻消息冗余问题,但是对更高吞吐量和点对点传输的要求将变得不足。在这种情况下,结构化网络(例如 DHT)是可用于进一步优化的解决方案。但是,在区块链中,特别是在公链项目中,存在节点可以任意加入和退出的假设。频繁更换的网络将导致结构维护的巨大成本。因此,采用结构化 P2P 网络的挑战之一是处理复杂网络的不稳定性和不确定性。在 Thinkium 核心引擎中,我们使用结构化和非结构化方法的组合。某些场景(例如点对点传输)使用结构化 P2P 网络方法来减少冗余并提高效率,同时将非结构化传输作为稳定性的保证。

3.6 多链并行模型

对于多链系统,当前单链系统的账户模型(例如,UTXO 或者以太坊账户)不再适应新的需求,特别是在处理大量跨链操作时。我们设计了一种新的帐户模型,它允许我们以异步和无锁的方式在多链系统上实现复杂的逻辑。在此模型中,我们将涉及到一组帐户的交易以消息形式分离为多个步骤。每条消息都由唯一的主体接收,并由相应的链执行。最终执行所有消息就能实现交易。

我们设计一种基于 Actor 的并行模型作为我们的基本框架。该结构主要包含以下信息:

- 地址: 区块链帐户的唯一标识符。
- 余额: 帐户的当前余额。
- Nonce: 标量值, 等于从该地址发送的外部消息数。
- 代码: 处理消息的编程逻辑。
- 存储: 帐户的内部状态, 可以为空。

每个帐户都由私钥控制。在代码中,帐户为其收到的消息定义了自己的处理方法,允许向其他帐户发送消息,创建新帐户并修改内部状态。对于某些规范消息,每个帐户都有相同的通用处理方法(例如“tran”和“add”)。每个帐户还可以自定义其他消息的方法。

消息有两种类型：外部消息(external message)和中继消息(relay message)。外部消息由使用其私钥对其签名的帐户创建。中继消息由在执行过程中执行 send 命令的帐户产生。我们模型中的这些消息支持跨链传播。

消息主要包含以下信息：

- 发件人：消息发送人地址。
- 收件人：消息接收人地址。
- Nonce：标量值等于发送方发送的外部消息数，对于中继消息为空。
- 输入：指定消息调用的输入数据组。
- 验证数据：标识发送者外部消息的签名，或中继消息的证明。

对于外部消息，可以通过签名和 nonce 进行验证。对于中继消息，它可以通过证明进行验证。

在我们的并行模型中，对于链C上的每个区块，有三种消息：

输入消息。这些消息当前未被确认，并且接收者账户都是在链C上，它们可以是外部消息或由其他链产生的中继消息。

内部中继消息。这些是在执行整个区块期间生成的中继消息，并且接收器同样位于链C上，因此它们在本区块上就会被确认。

外部中继消息。这些是在执行整个块期间生成的中继消息，它们的接收器位于其他链上，这些消息将由其它链确认。

我们设计了一些优化方法来降低通信成本和帐户存储。相比同样被用来做并发的其他方法，我们的模型具有更高的灵活度和效率。

3.7 身份及认证

Thinkium 核心引擎为用户提供一个通用、可控、安全的身份认证体系。Thinkium 区块链系统的地址账号不直接与用户身份关联，支持用户对账号进行身份认证。认证方式包括：具有公信力的 CA 向账号签发证书、在认证主体的信息主体上发布认证信息、其他账号对用户帐号进行授权等。账号的身份认证信息

可以存储在链上，可以被快速地查询和访问；账号所有者可以自行添加和维护认证，也可以将维护的权限授予其它账号。Thinkium 核心引擎允许灵活的认证方式，每个账号可以经过多条信任链的认证，每种方式的信任锚和安全程度不同，用户和应用可以根据自己的需求，对可靠性进行判断。

用户可以使用可验证声明（Verifiable Claim）对账号的身份和其他属性进行认证。可验证声明由签发者账户签名创建，验证者通过签发者的公钥可以确认声明的真实性和完整性，在签发者主动吊销声明或者声明有效期结束之后，该可验证声明将会失效。除签发和吊销过程外，其余过程都不需要签发者参与。

可验证声明中可能会包含一些敏感的信息，用户可以通过对可验证声明进行加密来保护隐私。Thinkium 核心引擎支持三类声明方式，使得用户可以在安全性、成本和效率之间权衡，选择最适合自己的需求的协议。在实现可验证声明的过程中，区块链由于具有不可篡改的性质，适合作为一个可信任、可追溯的公告板。

明文声明：声明没有经过任何加密，以明文的形式发布或保存。

加密声明：声明的内容被加密，验证者需要持有者提供的密码学信息才能读取。通过对声明的每一部分使用不同的密钥进行加密，可以在每次出示声明时，只让验证者看到相关的那部分。需要注意的是，如果恶意的验证者公开解密密钥，声明的内容就会被公开。

另一个方法是使用零知识证明：持有者可以选择性地向验证者证明一些性质，验证者不会获得声明的原文或者任何额外的信息。零知识证明不仅可以证明属性的值，还能证明关于属性的函数，例如“价格高于 100 元”或者“国籍不为美国”这种形式的命题。使用交互的随机证明，可以使验证者无法向其它人重复相同的证明（证明是需要持有者参与的随机算法）。

匿名声明：加密声明虽然可以隐藏声明的内容，但并不能隐藏持有者的身份。即使验证的过程中没有出示账号，验证者在两次看到同一个声明时，就知道两次验证的是相同的用户。如果验证者和签发者串通，他们可以得到签发者所知道的关于持有者的所有信息。在隐私高度敏感的应用中，应该使用匿名声明来保护持有者的身份。匿名声明结合零知识证明和盲签名，验证者即使和签发者串通，也无法区分满足验证条件的不同声明。IBM 的 Idemix 和微软的 U-Prove 是两个成熟的开源匿名证书协议，前者更符合匿名声明的需求。

明文声明可以公开放在链上（例如第三方机构的认证），也可以由持有者保存，在使用时出示（例如适合公开的职业和从属信息）。另外两类的声明一般由持有者保存。签发者可以通过在指定的链上发布通知来吊销一个声明，因此，对于支持吊销的声明，验证者需要读取链上的吊销信息，才能确认声明的有效性。

用户和应用亦可以选择使用 Thinkium 核心引擎外的可验证声明，这是为了兼容已有的声明和认证系统。但是在这种情况下，使用者需要自己管理和检验声明的有效性。

3.8 隐私计算

在一些特定场景中，一方面需要对用户数据进行计算，另一方面又需要保护用户数据的安全和隐私。在数据使用者不能被信任时，需要设计一种机制使得用户的数据不被窃取或滥用，这就是密码学中的安全多方计算问题。在安全多方计算的过程中，用户的输入以加密的形式被使用，任何人都无法获得除了计算结果以外的与输入有关的信息。安全多方计算的安全性来自于其中使用的密码学方法，在密码学构件的安全性的前提下，是可以严格证明的。

目前的安全多方计算方案，理论上可以实现任何的算法。但是由于极高的通讯复杂度，目前并没有办法大规模地应用。尽管如此，对于一些数据很敏感的行业，即使只能进行简单的运算，也能获得很有用的结果。这种情况最典型的例子是医疗和基因数据。伴随着密码学技术的发展，会出现更多可行的应用场景。

区块链是一个数据发布和交流的平台，而安全计算提供了一个将数据与计算分离的方式，不仅拓宽了区块链应用可以实现的功能，同时使用户能更好地保护数据的隐私。使用安全计算可以实现一些需要隐藏数据或身份的功能，例如拍卖（隐藏除了最高出价以外的竞价）、不记名投票、匿名评价等。安全计算允许用户用自己的数据参与特定的计算，例如用于（具有公益性质的）研究或指定目的的数据出售，同时可以防止计算方将数据用于其他用途或者转卖。

因为安全多方计算的通讯复杂度较高，计算过程适合在链下进行。而计算的发起、协调、记录、支付等步骤可以在区块链上进行，计算的结果也可以上链以便后续的调用。对于一些需要证明计算结果正确性的应用（例如投票、拍卖），可以使用可审计的安全多方计算算法，并使用区块链作为公告板：计算的参与者在公告板记录计算过程中的信息，之后，所有人（即使是没有参加计算的人）都

可以通过公告板上的信息验证计算过程的正确性。

3.9 开发体系

Thinkium 核心引擎设计特有开发体系架构，为使用者隐藏了各种晦涩难懂的概念及工具，可以整合在一个 Thinkium 桌面应用中，使得每一个人都可以简单上手，同时，也为开发者提供从去中心化应用到智能合约开发所需的全栈 SDK，快速开发目标应用。

3.9.1 Thinkium 桌面

Thinkium 核心引擎提供一个标准桌面应用——Thinkium 桌面，它拥有对应用的检索、下载，以及运行的能力，桌面可运行于 PC、移动终端上，使用户能够在不同设备上轻松使用区块链。

1、应用展现

每一个 Thinkium 桌面均连接到 Thinkium 公共区块链网络上，再通过 Thinkium-API 对 Thinkium 区块链上的 D-Store 后端进行数据读取，最终在桌面上展现出整个应用市场。在这里，用户不仅可以通过分类、排行榜、搜索等方式对 Thinkium 应用进行快速定位，将感兴趣的应用下载到本地，直接点击运行即可。还可以对每个自己使用的应用进行评定与打分。

2、应用运行

Thinkium 桌面包含一个基于 Thinkium-API 的 Thinkium 应用运行环境 (Thinkium-desk runtime)，用户下载到本地的 Thinkium 应用，可以在 Thinkium 桌面中直接打开在该环境中运行。每一个 Thinkium 应用均由经过严格控制的类 JavaScript 语言进行编写并打包。由 Thinkium 应用运行环境负责解析执行，这包括了应用界面展现、应用逻辑运行以及 Thinkium 服务和传统互联网服务的调用。

3.9.2 开发框架

Thinkium 核心引擎具有友好的开发者框架，这包括：Thinkium 智能合约 SDK，合约开发者用来快速调试开发智能合约的工具集合；Thinkium 应用开发 SDK，应用开发者用来快速开发应用的工具集合，并使之能够发布在 D-store 上，运行于 Thinkium 桌面。

1、Thinkium 智能合约 SDK

为方便合约开发者的使用，Thinkium 核心引擎将发布智能合约语言 T 的编译器，可以把 T 语言编译成为虚拟机语言，降低学习成本。编译器之外，Thinkium 智能合约 SDK 还包括原生开发库，通过原生开发库为智能合约提供 Thinkium 区块链原生数据的读取能力。Thinkium 核心引擎会提供智能合约在线 IDE 和通用编辑器插件，以方便开发人员的快速转换。

2、Thinkium 桌面应用开发 SDK

为了让用户以最方便的方式使用 Thinkium 公共区块链，Thinkium 核心引擎提供应用开发语言及运行环境。使用这套开发 SDK，应用开发者可以像开发一款 Web 应用一样，开发 Thinkium 去中心化应用。通过使用它对 Thinkium 公链 API 层功能的封装，可以调用区块链核心能力和各种已发布的智能合约，同时还可以对外部资源进行访问。

最后，通过 SDK 中的发布工具，将代码打包并发布到 D-Store，这样，用户即可以通过 Thinkium 桌面查找到新应用并使用。D-Store 让开发者更方便的获得应得的劳动收益，同时也能更好的刺激优秀 Thinkium 应用的产生，营造优胜略汰的良好生态环境。

3、API

API 建筑在区块链核心能力与智能合约之上，将底层接口、智能合约、D-Store 后端逻辑封装在基于 HTTP 的标准协议之下，对外提供远程调用的能力。Thinkium 核心引擎通过将功能封装在 API 层的标准接口上，使用者只要使用 Thinkium-API，就可以通过远程调用获得区块链的全部能力。

4、D-Store 后端

D-Store 后端不仅提供对应用的分类索引及搜索，还能够通过区块链数据统计每个应用的使用情况，从而自动生成各类排行榜（如：最新、最热、最喜爱等）。D-Store 后台与区块链节点部署在一起，能够快速访问区块数据，同时共享 P2P 网络，形成了一个去中心化的高可用的与区块链共生的应用商店。D-Store 通过多维度的组织方式，解决现有公链上智能合约的散乱现象。从而避免了因重复开发导致的资源浪费。同时，使更多的使用者聚集在同一个合约上，使得合约开发者获得更大利益，从而催生更高质量的合约功能，正向推动区块链的发展。

4 Thinkium 上构建行业公链

4.1 优势和特点

4.1.1 优势

基于 Thinkium 底层基础设施搭建行业公链，有以下三大优势：

第一，低成本搭建、专注聚焦。相比于完全自己搭建，且承担高昂安全风险，利用 Thinkium 已有基础设施快速搭建自己的公链，并将精力更加专注在自有公链的生态发展、应用建设、社群建设等特定领域问题，而无需投入巨大精力与财力重复建设区块链底层基础设施。

第二，跨链互通、网络效应。基于 Thinkium 基础设施上搭建的公链，从一开始就不必为跨链间互通问题而烦恼。另外，随着更多公链的加入与成长，不断沉淀可信数据，链与链之间可以形成强大的网络效应，从而提升所有公链的竞争力。

第三，无限扩展、无限可能。Thinkium 从根本上解决了在确保一致性和安全性基础上的无限可扩展问题，为其上每条公链的生态发展打开了天花板，能真正意义上允许互联网级别区块链应用的诞生。

4.1.2 特点

Thinkium 作为“公链的公链”具备以下六大特征：

第一，底层统一，能降低公链的建设与维护成本。作为底层基础设施，Thinkium 公链提供统一的底层能力，允许各条公链在其上得以运行；在分层的模式下，Thinkium 公链不断升级迭代，为其上的所有公链赋能，降低了公链的建设与维护成本。

第二，独立自由，发展自身行业公链生态。每一条行业公链虽然在统一的底层基础设施上搭建，但并不意味着“吃大锅饭”，Thinkium 允许各个链独立自由发展，包括自由建链、增加与减少节点数，使得各条链自由扩展收缩。

第三，去中心化发展，生态共同成长。长期来看，公链最终应进化为不受任何中心化组织的约束，以去中心化方式发展各自链内生态节点，以公链内部激励体系实现各自链的自发成长，同时底层 Thinkium 公链的生态也会共同成长。而

且，只要满足最低需求，Thinkium 其上的公链即可存在不会消亡。

第四，无限扩展，打开成长天花板。随着各条公链上应用的复杂度和用户规模的增长，势必对链的性能及存储等服务能力提出了更高要求。基于 Thinkium 底层基础设施搭建的各条行业公链，能够通过扩充节点的方式线性扩容服务能力，满足行业公链的发展要求。

第五，跨链互通，提供统一高效、可迭代定制的跨链互通方案。公链天生对跨链互通性提出了要求，即：能够通过互相访问不同链上的数据，形成更加丰富的应用生态。Thinkium 通过底层公链的基础服务和统一高效、可迭代定制的跨链方案，让其上各条公链间的用户、数据、资产等跨链互通，充分享受各条公链服务，形成各公链间的网络效应，为更加深度的基于区块链生态治理的社会打下坚实的基础。

第六，安全保障，发挥安全性的网络效应。相比传统独自建链，独自承担链的底层安全风险，在 Thinkium 底层公链上搭建的所有链，安全性可以共同发展、相互促进。即，当更多节点加入网络后，在安全性上可以同步提升；对于规模较小或初建的公链，也能拥有大型公链所拥有的安全性；伴随各行业公链的成长，Thinkium 公链生态也会同步成长，安全性持续提升。

4.2 搭建一条行业公链

相比于传统的从零搭建公链的方式，基于 Thinkium 底层基础设施搭建一条行业公链，包括以下六个方面：

第一，行业公链启动。任何人可以很方便的利用 Thinkium 底层基础设施，以相比传统公链建设方式低的多的成本与时间投入，通过简单设置与开发部署，即可启动一条功能完备、安全的行业公链。公链的发起方无需担心从零研发所带来的巨大研发成本，无需投入大量精力在底层公链技术细节中，无需担心上线后所面临的潜在安全风险，使团队更加专注于公链上层行业规则的设计、开发及公链生态建设，从而降低了行业公链的进入门槛。

第二，行业公链生态建设。行业公链生态建设初期，Thinkium 底层生态允许行业公链发起方采用预付账户形式，在链上直接支付公链节点运行费的方式，来完成生态节点的搭建。当经历初期验证和社群搭建后，可以逐步转变为社群共

建搭节点的方式，即：Thinkium 节点都可以通过支持指定行业公链的方式来加入，并允许此行业公链使用更多节点资源，扩容此行业公链的服务能力。

第三，设定行业公链的激励机制。激励机制事关行业公链的生死与发展。行业公链通过发行自己的公链币，设定加入规则（例如抵押币、POW 工作量证明，POC 存储证明，建立自己的矿机生态等方式），设计基于自己公链币的激励分发规则，来激励更多的用户参与此行业公链的生态建设中来。由于 Thinkium 底层共识机制已经被解决，因此可以专注在行业公链上层的激励机制设计上，而无需担心对底层共识算法的影响。从而构建更加灵活和有吸引力的激励机制，促进行业公链自身生态的发展。

第四，使用底层公链的基础服务。行业公链可以充分利用 Thinkium 不断沉淀迭代的底层基础服务，例如：ID 系统、资产交易、社交服务、数据服务等，丰富自己链上服务的深度与广度，将 Thinkium 生态内的用户、数据、资产与自身行业公链服务打通，加速行业公链成长。

第五，行业公链币的成长。从用户角度看，由于建立在 Thinkium 底层基础设施之上的行业公链拥有畅通的用户与资产跨链互通的能力，行业公链社群用户除了使用链上服务并消耗公链币外，也能同时享受整个 Thinkium 生态下其他行业公链发展所带来的成长红利，增大了持币和需求币的用户群体。从服务角度看，由于方便的跨链数据互通可以构建丰富的应用服务场景，提升整个行业公链生态的服务深度与粘性，增加公链币的使用范围和频次。从技术角度看，行业公链不仅安全性随着整个 Thinkium 生态繁荣不断加强，而且由于行业公链的服务能力可以线性扩容，从而允许更多的用户加入到行业公链生态中来，为行业公链中诞生大规模互联网级的应用提供了技术上的保障，也为公链币的价值增长扫清了障碍。

第六，行业公链的治理。每条行业公链可以根据自身的发展节奏开展行业公链的治理。从行业公链的发展来看，往往会经历内部测试验证、外部测试、主网上线、后续迭代，期间会不断发现问题并解决。在内部测试验证阶段，行业公链建设者可以选择回滚或关闭并重建新链的方式来修复或修改链上规则；当主网上线后，Thinkium 其上的行业公链可以通过 Thinkium 底层基础设施提供的基础社群治理规则或自定义治理规则，进行整个行业公链的治理。

5 Thinkium 分布式商业

Thinkium 的设计目标之一就是构建和支撑现实商业。它的技术特点决定了它能够完美支持复杂任务的高并发处理，让区块链能够更高效承载大规模的交易，能够支撑起海量用户规模的应用运行，使得原本由于受限技术成熟度的区块链商业项目的落地变为可能。

Thinkium 搭建的底层基础设施和基础服务，可以比拟为一个互信商业协作引擎，催生出一个个参与者共建的、可信、又安全的商业环境。在这样的商业环境中，用户、数据、资产可以互通，跨商业主体分布式协作成本大幅度降低，同时也能促进更加充分的市场竞争，提高供需双方信息匹配度和协作可能性，达到多边激励相容，整个商业生态更加繁荣、有序和可持续发展。

5.1 分布式商业的定义

分布式商业是商业的又一次进化。基于个体需求的演化与发展，基于区块链技术建立可信商业世界，能够大大降低协作成本、促进价值创造、更有利于社会中每个个体的发展，是一种全新的商业形态。

分布式商业是基于区块链技术构建的一种新型生产关系。多方商业主体基于区块链可信网络及新的数字主体权益，将业务逻辑、分利规则等进行代码编程，商业链条中的各个主体通过预设的、可被强制自动执行的透明规则进行组织管理、协作生产、经营推广、利益结算等，任何商业活动的参与方都公平公正、互信安全的协作、交易，最终实现共建共赢、高协同的社会生产生活目标。

分布式商业的三个特征：

第一，数据成为“主体”及非常重要的资产，且所有权和交互记录都能在链上被清晰的记录、可追溯，确保协作、交易的内容和过程是可信的、安全的。

在互联网时代，一旦创造主体生产了数据，会很容易被复制、传播，个人用户的数据权益更是无法得到保证，甚至连数据隐私权都被侵犯。大量数据和数据交互记录被中心化平台垄断，且平台之间互不开放，严重阻碍了信息的流动，用户创造了数据却只能被企业无偿使用。

区块链技术首先解决的是数字资产的确权和可追溯问题。数据的产权主体在链上被清晰确认，协作和交易的过程信息记录在链上、且不可篡改，真正实现“我的数据我做主”。任何一方主体想要获取数据，无需经过任何第三方平台，可以直接与数据主体进行平等价值交换，因此基于区块链的商业协作是可信的。

第二，基于可信的商业协作和价值交换，交易成本也必然会极大的降低。

从后端生产协作来看：协作主体之间基于事先定义的行业规则，记录在公链或联盟链上，上下游企业都能通过链上实时、安全的访问所需信息，并与集中化生产系统及物联网同步数据，可以实现“全网节点自动化生产协作”，不仅能降低协作多方的信息沟通成本，上下游之间的协作订单也更加可信；交易结算基于智能合约自动执行，能降低财务成本，会很大程度上提高生产协作效率。

从前端市场交易来看：一方面，通过紧密的社群关系，用户获取价值信息的决策成本更低；另一方面，基于链上可信的用户数据、透明的交易规则，交易双方的交易执行成本也能大大降低。另外，基于通证经济体系将参与方利益绑定，还能产生更多商业合作，如品牌共建、服务共建等；消费者可以成为供给方的推广大使、投资人、品牌设计师、售后服务等角色，这能极大的降低供给方的运营成本，社群关系也更强。这在互联网电商是很难实现的。

第三，基于链上可信的分配规则、透明执行的过程，及通证经济激励机制，参与方之间能最终构成真正的商业利益共同体。

在互联网时代，用户数据集中在各大互联网平台，平台是最大的赢家；“马太效应”使得中小微企业及个体经营者的生意越来越难做，用户的个性化需求也不能被很好的满足。虽然社交电商、IP 电商等新模式逐渐涌现，但仍然只是表面，无法解决中心化组织或个人的信用问题，参与方之间的利益分配和透明度难以得到保障。

区块链彻底解决用户的信任问题和规则执行的可信问题。传统模式下的利益分配规则，基于链上合约自动执行且信息透明，多边商业主体获得利益有了保障。另外，基于通证经济系统，经济活动不再是相互之间的摩擦或竞争，反而变成共同合作完成的一项事业，传统商业及互联网商业中的零和博弈最终会被区块链时代的多赢局面所取代，推动商业生态的可持续发展。

5.2 分布式商业的发展路径

5.2.1 Thinkium 分布式商业生态

Thinkium 分布式商业生态，是基于 Thinkium 区块链基础设施，构建的商业生态体系；是区块链链接人与物理世界的重要窗口，包含链上原生商业、链下传商业等。

所有参与商业生态的用户主体、数据和资产在底层公链的公链上记录。每一个用户主体就是一个链上的账号，可以是人，也可以是机器，也可以是虚拟主体。结合 Thinkium 的数据确权和保护体系，用户主体产生的数据归属于自己，成为个人重要资产，授权使用、记录可追溯。基于 Thinkium 底层基础设施，可以实现跨链和跨应用之间的数据交互，避免了传统互联网商业中不同商业生态之间的“数据孤岛”，从而能产生更多更大的商业价值。

案例：符合每个学生个性化需求的铅笔，将如何在分布式商业生态中运行？

一、商业场景：铅笔是学生的日常消耗品，每个学生都期望能买到符合自己个性偏好的铅笔，且经常变换需求。

二、忠诚用户快速繁殖，自发形成分布式社区：假设某学生（Elsa）买到一款迪士尼电影 Frozen 系列的定制铅笔，会很容易自发推荐给其他同学（Kitty, Nimo 等），并形成多个不同主题的学生社群，如冰雪奇缘群（Frozen 社群）、小马宝莉群（MyLittlePony 社群）等。社群成员围绕主题会有更多包括电影、电视和书籍等相关主题的其他交流等，商家也能基于社群需求产生新的业务增长点。

三、激励机制下社群裂变效应：推荐下单得奖励，所有线上行为自动累积为信用积分，积分能“挣钱”，还能当“投资人”，例如：某企业新增或扩产某主题系列的铅笔生产线，可以发行该生产线的通证面向市场流通，获得该通证的用户可以与厂商分享未来经营收益；群主与商家达成共识，建立“推广合作的智能合约”，社群 KOL 自带“第二职业”。

四、“市场-生产-供应链”全网节点自动化协作：供给端服务商经授权访问 IM 信息，将其进行结构化数据分析，辅助供给端经营决策；群主使用专用统计工具，定期发送社群对铅笔的个性化需求，自动同步到商家后台管理系统，与铅

笔需求有关的结构化信息在链上互通访问。铅笔各生产厂家、上游原材料供应商、油漆等配套材料供应商、迪士尼 IP 版权方等商业主体，随时可以经授权访问市场信息、下游伙伴需求和订单信息等，各自生产管理系统和生产一线即时收到排产信息和物流需求，并进行即时响应。

五、结算、分利等规则自动执行：当期铅笔生产线完成后，上下游企业链上智能合约自动执行，完成数字资产转账结算。

六、企业融资透明、可信，监管更便利：铅笔产业某企业要融资，融资机构可基于链上可信的动态经营数据，与其建立融资合约，甚至根据链上动态经营结果设定融资激励机制；所有企业都可以基于其量化资产发行通证，进行“自融资”，通证资产在生态中能自由流动。同时，社会及政府监管机构，可以通过访问链上公开、透明的信息来实施法律、税务等监管。

Thinkium 从多个领域出发做了大量研究、探索和实践，致力于提供底层技术基础设施的同时，为整个商业生态赋能，支持例如分布式电商、分布式金融、分布式生产协作、分布式组织、分布式虚拟经济等大规模商业应用落地。参与商业生态的用户包括开发者、消费者、生产商、供应商、品牌主、金融组织、监管机构等，通过分布式的账户体系，在遵循一定的商业规则下参与平等自由的商业活动，发挥各自的贡献和才能并从中获益。

下面分别概述基于 Thinkium 分布式商业生态的几种典型商业应用。

1. 分布式电商

分布式电商指的是，基于 Thinkium 区块链技术构建的可信平权的供需网络。在这个互信网络中，各参与方的行为按照共识的标准被资产化，同时可按照共识的规则进行自主协作并交换价值。

这是一种新型的“需求-供给”关系。所有参与方的用户数据记录在链上，商品或服务的供给方（价值创造者）可以直接与消费者通过可信社区进行交流、协作和交换价值，消费即投资的理念让协作双方成为紧密的利益共同体。在这样新的互信分布式电商网络中，参与各方的协作摩擦大大减小，进而大大提升协作效率。基于 Thinkium 构建的可信协作网络、真实 ID 系统等，使得各个角色的价值被更合理的分配，以及被持续存储下来，从而实现各自的能力升级和角色转化。

消费者（用户）：同时也是营销推广者、品牌设计者、内容生产者、服务者、投资者等多重角色，享受多重收益。首先，基于链上溯源系统，消费者可以获得品质更优的产品与服务；第二，用户的各种消费、推广行为等累计积分并获得通证，基于通证经济体系参与品牌和商城的收益分红；第三，用户个人数据资产确权，跨商城、跨品牌主、跨商业应用被授权使用，安全性得到保证，数据资产变现方式多样；第四，用户自由选择参与社群共建、品牌共建、服务共建等，通过做贡献获得更多收益；比如，社区成员进行更加专业化的分工，发挥各自在设计、服务、选品等方面的专长，创造的内容、提供的服务等都可以被资产化，在分布式商业网络中发挥更大价值。

供给方：尤其是众多中小微企业、产地源头直供方、个体经营者、小品牌主等。首先，供给方直接触达用户，营销推广成本大幅度降低的同时，供给方能更加专注于产品本身；第二，以前是先营销后卖货再收钱，现在是收钱之后再分钱，供给方现金流更充足，结算方式也更可信；第三，供给方精细化运营用户社群，通过提供更多增值服务，带来更多增量收益；第四，融资逻辑发生本质变化，供给方用实际经营结果作为品牌背书，获得更低成本的信贷服务；第五，零成本分布式品牌建设和服务建设，通过分享收益的机制，激励社群成员参与品牌共建和服务共建，满足消费者个性化需求。

2. 分布式生产协作

分布式生产协作指的是，基于 Thinkium 区块链技术整合供给端形成全网协同、高效运转的研发生产制造网络。在原材料、生产、加工、设计、研发、定价、品牌推广等各个环节，各参与方进行自主协作提供产品与服务，并根据各自贡献的价值决定最终的收益。

这是一种新型的生产协作网络关系。协作网络中的各个供应商，和服务提供商都是一个独立的生产节点，各自的生产运行数据可以在集中式服务器存储管理，关键业务数据、结算信息、节点信息及摘要等可以通过链上（联盟链或公链）记录，并通过授权访问，从而形成各个供给端之间、与需求端之间链上高度互联，数据动态调控和精准匹配，实现按需生产、按需定制。上下游之间无需大量的沟通成本和物理契约就能达成合作，就可以实现供应链动态协作生产，相互之间的回款结算，根据链上共识规则协议自动完成，供应商货款账期能极大的缩短，同时也保证了足够的生产效率和极低的资源浪费。另外，基于上下游之间的可信关系，以及需求端信息的共享、透明、可信，生产商可以用货品融资方式提前获得

上游材料供给，上游也可以通过发行通证和通证资产流通来锁定下游订单，生产协作的各方构成多方互利可信的生产联盟。

利用 Thinkium 区块链底层基础设施，商业主体可以根据自身的业务需要进行业务拆分，将一部分必须严格保密的业务放在可信的联盟链中，将另一部分需要在更大范围流通的业务放到行业公链中，可以同时满足保密和业务上链的需求。商业主体的区块链技术落地路径将因为 Thinkium 的出现而大大缩短，可以吸引更多的商业主体参与到区块链变革中来。

3. 分布式金融

分布式金融指的是，基于 Thinkium 提供一个无需许可的金融服务生态系统，任何金融活动的发生无需任何中心化权威，可以在供需双方直接完成，任何人都可以使用。

基于 Thinkium 底层基础设施的分布式金融，可以实现：

允许金融服务在去中介下完成。一般大众对金融服务的需求包括：储蓄、贷款、交易、保险及其他金融服务，都可以在基于 Thinkium 上开发的 DAPP 应用来实现，并且支持海量用户，实现高效金融服务。

链上资产可以自由互换。基于 Thinkium 的任何行业公链上的资产，可以在 Thinkium 生态内自由流动，不受资产种类、地域、行业等的限制，如此可以使得整个分布式金融的效率更高，不仅高于传统金融服务效率，而且高于目前分布式金融领域任何相关应用，真正实现去中心化的金融。

助推大规模分布式商业生态创造更好的产品和服务。例如，对于一些中小微企业品牌或个体经营体而言，其信用及价值可以基于链上记录的可信经营数据进行更加精确的衡量，使其更容易获得金融服务来促进生产力的提升；对于参与生产协作的供应链上的各方参与者，上下游之间可以通过货品融资方式解决中小企业融资难、融资贵的问题。

降低企业财务成本和财务风险。由于供应链生产协作和商品市场流通的每一笔交易都能在链上发生和被确认，因此可以节省传统商业中对账等大量财务结算成本；同时，可以降低企业的应收账款风险，提高企业的资金周转效率。

金融流动性透明化，为金融监管提供了良好的基础。

4. 分布式虚拟经济

互联网的虚拟世界，数字资产属于中心化平台组织。在分布式虚拟经济下，账号体系、数据等数字资产真正归属于用户自己，因此可以诞生更多的可能性。比如，传统游戏开发主要由中心化组织来运营，而在分布式虚拟经济中，游戏内的资产在链上被确权，游戏里的金币、积分等可以在游戏内外进行互通，从而构建开放式游戏生态。组织或个人可以基于现有游戏进一步开发衍生内容，甚至在原有游戏开发组织已经关停的情况下也有机会继续维护游戏的运行和迭代。

Thinkium 的线性可扩展的技术特点，可以支撑分布式虚拟经济中互联网级游戏应用的诞生。

5.2.2 Thinkium 分布式商业路线图

分布式商业是未来商业发展的必然趋势。当前及未来一段时间，传统商业、互联网商业和分布式商业也会彼此共存，互联网商业与分布式商业在很长一段时间还会“此长彼长”。

结合大量实践和理论研究，Thinkium 致力于提供底层基础设施的同时，为生态参与者提供低成本的区块链技术服务，赋能生态落地大规模商业应用。目前，Thinkium 分布式商业落地已经开启，并将经历以下几个阶段：

第一阶段：基础夯实和社区启动，重点包括：

1. 建立强健稳固的底层商业基础环境，包括 Thinkium 底层基础设施和底层核心基础服务；
2. 同步启动全球各地区的 Thinkium 生态社区建设。

目前，该阶段已经初步完成，底层核心基础服务正在完善中，搭建行业公链和联盟链的技术条件也已经具备。全球各地区的个人、社区组织、技术开发者和开发者社区等，都可以参与到 Thinkium 底层生态节点搭建、底层通用工具开发中来。

第二阶段：基于“单位价值密度上链”原则，优先聚焦单位价值密度足够高的行业或行业信息上链，进行全球大规模商业落地，行业生态社区也会同步建设。单位价值密度是指，单位字节数（存储）的价值高低，价值包括资产、协作过程

中的关键信息等。

分布式电商：互联网电商的核心数据是交易订单信息、交易双方用户和商户信息、产品和服务页面信息等，这些数据的单位价值密度很高，对实体经济的价值贡献也非常大，对“用户数据资产回归”的意识变革有非常大的社会价值。

分布式金融：金融的核心数据是交易信息、账户信息，金融数据的单位价值密度非常高，且对安全、保密性的要求也非常高，与区块链的天然属性、Thinkium 底层基础设施的强大技术能力也非常匹配。

分布式游戏：游戏的核心数据是道具、金币、积分等资产和用户信息，虚拟资产的单位价值密度很高；而且，传统互联网游戏中的用户资产相对较为封闭，不同游戏之间无法互通，用户对资产的开放流动性诉求不能被满足，而这在区块链世界里是很容易得以实现的。

分布式内容版权：内容包括文字、视频、音频、专利等，其版权信息的单位价值密度较高，且对安全、保密性要求较高。基于 Thinkium 上可以搭建专有的细分行业公链，内容数据可以放在中心化服务器存储，而内容信息摘要通过哈希记录在链上，产权主体被唯一确认且不可篡改，产权使用过程可追溯，用户的内容知识产权得到极大的保护。

第三阶段：深度融合人工智能、大数据、物联网等前沿信息技术，让全球更多有价值的资产、数据、信息等，在基于 Thinkium 统一的底层基础设施上的各行业公链生态中高效互联、互通，让区块链全面融合渗透到全球及全社会各产业经济中。随着各行业生态社区的发展，Thinkium 底层生态也更加繁荣。

5.2.3 Thinkium 分布式电商已落地解决方案

基于以下四个方面的因素，Thinkium 首先赋能的领域是线上零售行业，即分布式电商。

第一，电商的核心数据是交易信息、交易双方的用户信息，其“单位价值密度”非常高，上链投入产出率较高；

第二，电商用户和交易规模足够大，资产上链能对社会每个个体用户更有价值；在传统互联网电商中，用户数据资产所有权并没有得到应有的价值回报；

第三，电商核心数据上链后，流量会自动流向价值更高的商品，“谁的产品和服务好、流量就会自由往哪去”，流量获取更公平、消费者个性化需求能更好的被满足，还能解决大量中小微企业及个体经营者的融资难问题；

第四，电商与实体经济紧密结合，能够创造更大的社会经济价值。

目前，亚洲地区分布式电商社区已经启动，第一个分布式电商系统已经开始运行。基于 Thinkium 的分布式电商落地解决方案包括：链上基础设施、分布式商业系统平台和分布式电商社区组织三大部分。

一、完善的链上基础设施，包括底层公链、底层公链基础服务、行业公链和联盟链、上链信息的数据存储。底层公链基础服务包括去中心化账户体系、去中心化资产交易平台、去中心化即时通信服务、去中心化行业公链建设等。

二、分布式电商系统平台，由三部分构成：

1. 设置通证发行总额，确定通证发行机制，并进行管理；比如：零预挖模式或提前售卖再挖矿模式。

2. 设定推广规则和激励方式、激励策略等激励机制内容，包括：推广消费返佣、行为资产兑换通证及通证权益规则等，确保收益分享；

3. 确保产品订单信息、产品详情、库存信息、支付方式、优惠措施等产品与服务信息记录在链上，确保交易可执行、交易被真实的履约执行、交易前后信息一致。

三、分布式电商社区组织。参与 Thinkium 底层生态社区建设的用户，可以自由参与其上各类商业活动，并成为分布式电商社区的种子用户；同时，传统电商的用户也可以平移到区块链世界，参与分布式电商不仅能拥有一个区块链世界的可信数字 ID，还可以分享更多的生态收益，共享 Thinkium 生态繁荣带来的数字资产收益。

6 Thinkium 生态发展和治理

6.1 Thinkium 生态发展

6.1.1 动力模型

Thinkium 世界从无到有，从简单到复杂，从底层架构到公链发行，从系统合约到上层应用，会形成的一个相互联系、相互作用、相互依存，具有自动调节机制的生态系统。这个自动调节机制，就是 Thinkium 生态的动力模型。

该动力模型中包含的主要角色包括：生态节点、各行业商业主体、社区建设贡献者、社区传播者、开发者、DAPP 用户、投资者等。Thinkium 世界原生数字资产，是模型中连接各个角色经济活动的关键，也是每一个用户进入生态社区的入场券。

Thinkium 生态节点是其上行业公链的基础建设者，通过持续质押原生数字资产，提供算力、存储、网络等必要的设备资源，为生态提供合约及交易的验证、数据存储等服务，从而换取更多资产激励。节点所提供服务的用户是 Thinkium 分布式商业的各商业主体，需要支付生态一定的原生数字资产，来实现其商业目的。生态中的终端社区用户，使用 DAPP 应用服务、分布式商业活动等，也都需要消耗更多的原生数字资产。随着 Thinkium 分布式商业生态的繁荣，越来越多的社区用户参与到生态中来，对原生数字资产的需求也越来越大。在资产总量恒定下，使其资产价值能获得持续的成长空间，这给整个生态中的各种角色带来资产持续增值的动力，最终促进整个生态的持续繁荣。

Thinkium 的种子用户同时也是 Thinkium 生态推广和布道者，为后续行业公链的启动，提供了用户基础和节点建设基础。随着社群用户裂变增长，更多的用户通过链上公开透明的治理规则和激励机制获取到相应奖励，加入并运行节点，节点的数量逐步增大。随着行业公链成本越来越低，底层公链安全性越来越高，行业公链、应用实现落地、用户及链上数据越来越多。

各行业公链的成长也带来 Thinkium 自身的节点增长和用户增长，从而可以为其上各行业公链提供更好的安全性与性能扩展空间，也为跨链融合发展提供了基础。Thinkium 不断完善公链底层基础设施，沉淀通用的公链部署、治理、应用规则，完善跨链技术与链上资产交易等，使各个链上的用户能方便的使用整个 Thinkium 生态中任意行业公链的应用。各行业公链可以利用其他链上数据，拓

宽自有行业公链生态应用范围，丰富自有生态应用；可以引导建立激励机制，让其他社群用户愿意尝试使用自身链上服务；可以激励自身社群参与资产兑换等跨链基础服务，提升自身行业公链资产流动性，因此社群用户在持有自身资产情况下还能方便使用其他链上服务，也能提高自身行业公链资产的持有率，用户的资产能够在各链间自由无缝的兑换，同时也反哺整个 Thinkium 底层公链生态呈指数级的增长。

Thinkium 最终与其上的所有参与者形成开放、共享、共建、共治的大生态体系，共同为整个社会、商业、产业、经济及个体的发展带来更大的价值。

6.1.2 发展路径

第一阶段：底层基础设施的建设

最初的 Thinkium 先是一个操作系统的建立，由少数的社区用户部署节点搭建而成，用于全球链开发者进行区块链核心系统的架构及编程，经过三年多时间科研人员及全球社区的共同努力，目前 Thinkium 已完成全球更多范围节点的部署，自动运行成为一个庞大的网络操作系统，并完成了在保证分布式、安全的基础上性能无限可拓展的成功测试，进化成为一台永不停息的可信计算机。

第二阶段：行业公链应用的落地

Thinkium 不断完善和降低行业公链的搭建门槛，沉淀通用的公链部署、治理、激励以及应用规则，吸引越来越多的行业组织或开发者基于 Thinkium 底层基础设施进行行业公链搭建，并组织行业内社区进行公链节点部署、行业应用落地、应用通证发行等，同时多链之间实现信息互通、价值互通、用户共享，让整个生态具有了更加顽强的生命力，Thinkium 成为真正意义上的区块链基础设施。

第三阶段：Thinkium 数字生活

Thinkium 生态随着各类原生及传统应用的落地，人类开始创建自己的数字身份，基于各种规则进行消费或者协作，并拥有了各种链上资产，各资产在链上进行流转，不断产生价值，推动人类正式迈入链上可信生活，Thinkium 生态用户呈指数级增长。Thinkium 彻底将靠底层技术来确保规则可信执行的区块链新世界与靠政府、靠法律法规，靠某个中心化平台来背书的旧世界链接起来。

6.1.3 生态未来

Thinkium 带领我们进入一个全新的世界，一个分布式自治体系的世界，在这个新世界里，让不可信的虚拟世界变的有章可循，每个人或物都可以拥有一个属于自己的数字身份，你的成长、学习、工作、生活、资产、活动轨迹等都被真实地记录在链上，所有的数据都被得到有效的保护；你可以无比信任地使用这个世界里的各种应用或工具、购买各种需要的商品或服务、管理自己的各种资产或信息，开启属于自己的数字生活；你也可以加入各种社区、基于各种规则参与商业协作，链接更多的人或物（机器），为别人提供更好的产品或服务，获得相应的 Token 奖励作为报酬。甚至成为某个领域规则的制定者，发行自己的行业公链或场景应用，组织供应链上下游行业或社区进行创造，创造属于这个世界的产品或服务，输出更多的能量及价值，链接物理世界与 Thinkium，共同推动可信社会新经济制度的建立，人类逐步走向规则社会。

Thinkium 生态的未来，属于每一个人，每一个有理想、有智慧的创造者、贡献值，都可以加入进来编辑自己的人生、贡献自己的力量，同时每一位贡献者都将在生态建设过程中获得巨大的财富。

6.2 Thinkium 生态治理

6.2.1 生态治理的意义

Thinkium 生态无人拥有却人人可用，是个典型的“公共产品”，需要持续维护升级。开放的系统构建起各行各业都能参与的全球大生态，生态中既存在竞争也存在合作，既存在着相互独立的个体运作，也存在着相互影响的整体协作。Thinkium 生态的特殊性，必须要有科学完善的生态治理解决公共产品效率问题，以保障技术持续的迭代升级和生态的发展繁荣，协调生态内竞争合作关系使生态运行稳定有序，确保共同利益目标的实现。

6.2.2 生态治理的原则

开放透明原则是生态治理的基础。Thinkium 生态只有足够的开放，才能使生态更加繁荣；只有治理透明，才能获得生态成员的认可。

相互协作原则是生态治理的内在要求。在 Thinkium 生态有竞争有合作，必须以相互协作原则进行治理，让生态从混沌、无序状态走向统一、有序状态。

民主公平原则是生态治理的执行保障。只有采用民主公平的治理原则，让所有生态参与者积极主动参与治理，才能确保 Thinkium 发展既能满足生态和用户的需求，也能符合整体生态系统的价值要求。

制度有效原则是生态治理的保障，完善制度也是治理的目标。要保证 Thinkium 的庞大复杂生态按照统一的目标运转并且相互协作，必须要有统一完善的制度作为依据，同时在治理中根据生态的发展不断完善和巩固制度。

6.2.3 生态治理的体系

Thinkium 生态秉持“共建、共治、共享”的理念，在生态治理中，构建由用户社区、专业自组织委员会、及基金会为主体的治理组织方式，形成由生态所有参与者共同投票决定 Thinkium 底层基础设施和上层生态重大事项的决策机制，打造技术平台支持进行链上投票的治理方式。各生态主体都可以对生态发展提出改进建议方案，所有改进的建议方案由基金会统一收集并做初步筛选分层投票。对于影响整个生态发展的技术和生态改进方案，由基金会提交链上平台由全体生态参与者进行投票决定；对于行业公链或是单个应用生态层面的改进方案，由基金会组织对应行业公链或是应用的生态进行投票决定。

Thinkium 基金会

Thinkium 基金会担负生态治理的官方主体和日常执行机构。基金会主要担负生态治理制度和决策机制的拟定、Thinkium 底层基础设施技术的升级迭代方案的拟定，Thinkium 生态在全球市场发展规划方案的拟定，生态发展中争议纠纷和问题解决方案的拟定，生态发展激励和处罚方案的拟定，生态重大问题应急方案的拟定等重大决策拟定；以及作为日常治理的执行机构，主动提出技术迭代升级和生态发展的建议方案，落实和监督各项重大决策、维护底层系统、服务生态、协同生态竞争协作问题等日常事务管理。

Thinkium 基金会是一个非营利性质的组织，基金会成员由技术极客、网络节点、各行业企业、生态用户或学术机构等共同组成构成。基金会下设理事会作为日常执行机构，设立监事会负责基金会运作的监督管理。基金会内部可成立专业委员会以提高治理专业度，各专业委员会可提出对应专业领域的治理方案通过基金会提交决策，也可参与对专业生态发展的服务和指导。

专业社区自组织

Thinkium 生态治理组织方式倡导和鼓励各个成立各生态、参与者或是专业自治组织，比如开发者委员会、网络节点委员会、用户委员会、行业公链或应用

委员会、技术委员会等。生态治理鼓励自组织间进行各种专业交流，支持这些自组织向基金会提交对 Thinkium 底层基础设施或生态发展的建议方案，由基金会提交决策机构进行投票决定，共同促进生态的发展和繁荣。专业委员会自治是 Thinkium 生态治理的润滑剂和专业保障。

用户社区

在治理 Thinkium 生态中方式中，赋权于用户，允许和鼓励用户积极参与生态事务，倡导培育和提升用户参与生态治理的意愿、能力和参与方式，构建用户社区为用户参与治理提供便利。用户可以对生态发展提出建议方案，也能对重大生态发展改进方案进行投票治理。

在 Thinkium 生态治理组织方式中，由基金会牵头和引导解决了公共产品的“代理问题”和“搭便车”问题，同时为生态进化提供引导资金，是生态治理的基础主体；专业化为委员会自治一方面能为生态治理进化提供专业技术保障，另一方面也有利于为生态进化提供规划需求和方向；而用户社区则是生态的基础，用户的参与让生态变成有意义和有价值。因此构建以基金会、专业委员会自治和用户社区的治理合作网络治理方式，相互协作，相辅相成，为 Thinkium 生态的繁荣有序发展，达成生态利益最大化目标而努力。

7 Thinkium 之约

528 年前，克里斯托弗·哥伦布率领 3 艘船、90 名水手勇敢地扬帆起航，发现新大陆，极大拓展了人类生存发展的空间和边界。

58 年前，约翰·费茨杰拉德·肯尼迪掷地有声地讲：在未来的十年要把人类送上月球，我们选择登月，不是因为它简单，而是因为它很难。自此人类探索的脚步迈入了月球。

3 年前，来自全球的几个技术极客因为“用技术改变世界”的信仰而达成共识，并诞生了 Thinkium。Thinkium 通过一个永不停息的可信核心引擎，重新定义“人”、重新定义底层规则，并辐射到世界的任何地方，帮助每一个参与者在“自由、平等、开放、公正”的 Thinkium 新世界中获得成长和价值回报。

比特币的出现，为我们打开了通向区块链世界的大门，引领区块链领域十二年的发展，同时也点燃了少数人的财富梦想。在 Thinkium 世界，每一个有理想、有智慧、有才能的价值创造者和贡献者，都可以自由加入各种生态、编辑自己的数字人生、贡献自己的一份力量，同时拥有巨大的财富，梦想实现的路径也不再有限。

“伟大的事业都始于梦想”，梦想的实现都是一点一滴的成长。成长的过程不会总是那么的一帆风顺，毛竹会用最初的 4 年长仅仅 3cm，从第五年开始每天长 30cm。远见、坚毅、勇敢是创造者的品质，价值和荣誉最终属于拥有伟大梦想的创造者。

播种是一瞬间，生根、发芽、成长是漫长的，但每一步都是坚实的，成长的过程是迭代、演化的，过程中的每一个小段都是自我的提升。今天的 Thinkium 还是小芽，不久的将来就是一棵小树，然后有更多的树木，终将是一片森林。

每个人都有眼睛，但不是每个人都有眼光；

每个人都有双手，但不是每个人都能把握机会；

每个人都有机会，但不是每个人都有勇气去追求梦想；

来到 Thinkium 新世界，你准备好了吗？