YEECO

YeeCo区块链
技术白皮书 2019

2019年6月

1 区块链行业发展概述

自上世纪 70 年代以来，随着密码学技术、分布式网络、共识算法以及硬件存储计算能力的高速发展，通过技术手段建立跨主体间共识协同机制的条件日趋成熟，为解决多主体环境下的中介机构信任风险、降低交易成本、提升协同效率提供了全新的、更加有效的解决思路。

近年来，区块链技术的不断发展和随之而来的技术场景化应用热潮，引发了从极客圈到 IT 技术圈、金融领域、各产业领域、政府和公共组织、媒体舆论等的广泛关注，相关各方围绕区块链技术研究、产业化应用、政策监管等开展了广泛而有益的探索实践。尽管区块链技术的成熟应用尚需时日，但它所带来的多主体共识协同的思想，将对社会治理和商业运作模式产生深刻的影响。

1.1 近年区块链行业发展情况回顾

2018 年是区块链行业发展摸索前行的一年。年初，无论是创业者还是投资人都延续着 2017 年的乐观态度，各行业、企业的区块链项目纷纷发布，表示将在区块链技术产业化中大显身手。但随后以比特币为代表的虚拟数字货币出现了断崖式下跌，区块链行业整体进入寒冬。

2018 年以来，区块链应用相对热门的行业主要集中在金融、供应链、电子存证、游戏等。尽管整个区块链产业同全球经济一样，仍然处在严冬时节，但对于那些真正沉下心来做区块链技术及应用的企业来说，经历了这一轮大浪淘沙、烈火真金的历练，必将会获得更充足的发展空间，更明确的目标方向和更务实的企业文化。

1.2 现阶段区块链行业面临的主要问题

目前人们已经广泛认识到区块链蕴藏的巨大应用价值，但是区块链技术的发展仍未达到成熟阶段，还需要一个长期的发展以及成熟的过程。

1.2.1 BTC 为代表的区块链应用存在明显的性能瓶颈

比特币作为目前区块链世界最为成功的应用类型，依然存在着固有的问题，其中最大的问题就是交易性能不足的问题。

交易效率低是因为比特币的区块大小受到限制而导致交易的数量受到限制，一般来讲，比特币交易即时在正常峰值的时候，它的每秒确认交易数也低于 7 笔。但是以互联网的典型应用为例，2018 年双十一期间，银行之间的跨行交易清算峰值接近 10 万笔每秒。这两个相较根本就不是一个数量级的，这也很明确的告诉我们，如果是按照目前的比特币的交易速度，它是不可能用于商业上的一些场景的。

针对比特币的这个缺陷，行业内一直都有努力在做对应的改进。例如 BCH 比特现金，在区块的容量上对比特币做了 8 倍扩容，也就意味着理论上每秒处理交易的速度也可以扩大 8 倍，但是这没有太大意义，因为性能还是在和比特币同样的一个量级上面。

在此之后又出现了以太坊，以太坊的挖矿速度相比特币有比较大的提升，它不是 10 分钟产生一个区块而是 10 秒钟产生一个区块，这样一来，它的处理速度相对来说也快一些（每秒 15~30 笔交易确认），但是以太坊也没有真正解决性能这个问题，它的可行性价值是在原来的基础之上添加了智能合约的功能，让我们的整个网络不仅仅可以转账，还可以完成程序的执行，大大扩大了区块链的使用场景和空间。

但是，以太坊仍未真正解决其性能不足的问题，在 2018 年以太坊应用加密猫流行的时候，就仅仅这一个游戏就造成了以太坊主链的大拥堵，更加说明其 PoW 的底层共识机制无法适应高质量商业运行的性能需求。

1.2.2 EOS 为代表的 PoS 区块链基础设施解决不了中心化的安全问题

EOS 被称为区块链的 3.0 时代，它的交易速度宣传能达到 10000 笔/秒（实际应用中峰值为 3800 左右），这就解决了困扰比特币的性能上限

的问题。

但是以 EOS 为代表的采用 PoS/DPoS 共识机制的区块链基础设施却无法解决安全性/去中心化的问题。

在 EOS 的在 DPOS 共识里，由 21 个超级节点生产区块，其中 20 个主节点，1 个轮流节点，另外还有 100 个备用节点。节点通过投票选出，为 EOS 区块链工作。

我们假设一下，如果未来 EOS 的生态完全的建立起来，那就产生了一个巨大的市场空间。那么大家就会有疑问，在这么大的利益面前，这 21 个节点会不会被操纵？这 21 个节点有无可能联合起来作恶？因此中心化的诟病就来自于此。

DPOS 的共识机制增加了权利的治理，这个治理从本质上避免了资源的装备竞争。人们从不断的购买机器算力获得竞争领先变成了人们自愿选择谁来合作，一起为区块链工作。从竞争到合作，解决了资源浪费的问题。

而人们自愿选择这件事，相当于权利回归，大众有了权利，可以选择那些能决定自己命运的节点。当所有节点都是被人们大众推举出来的，那就符合大部分人的远景，这解决了精英权利集中的问题。

如果选择的节点足够多，那自然也会解决中心化的问题。但是 EOS 的 21 个节点是否最终会形成 POW 的矿池局面，这个真的无法预测。但是可以确定的是，超级节点的利润如此诱惑必然会带来一波凶猛的竞争和拉票行为。

因此，可以这样认为，虽然 PoS 共识机制可以解决比特币的交易性能不足的问题，但是其中心化的共识机制方式却会带来相应的安全性风险，因此其可以应用的业务场景是被限制了的。

1.2.3 区块链基础设施的数据存储能力不足

在数据存储能力方面，由于区块链技术的特点，数据只有追加而没有移除，因此造成了数据量的只增不减，随着时间推移，区块链系统对数据

存储大小的需求也将持续增大，尤其在处理以几何倍数增长的企业数据时这一趋势增长更加明显。

此前区块链应用的场景集中在虚拟货币，对于这类“虚拟账户余额”式的数据内容，其数据量和数据结构的复杂性还比较简单，而对于复杂企业场景下的数据，其包含了大量的结构化和非结构化的庞杂数据，以电商供应链为例，每日数据记录条数通常都在千万级以上，如再沿着供应链条进一步展开时，每延伸一级数据量都会进一步放大。

目前典型的区块链系统在实现对账本数据的存储时，典型的方式是基于简单的文件系统或者简单的 KV 数据库存储打包在区块中，这样就导致了存储效率的低下，与复杂的商业场景的实际存储需求存在较大的差距，因此未来的区块链基础设施必将探索更为有效的大数据存储方式。

1.2.4 区块链技术的易用性和开放性

区块链由多种技术构成，学习成本高、实施难度大、人才稀缺。让用户快速理解区块链，降低学习和使用门槛，并将区块链技术快速应用到不同行业的业务中去，目前来看还有很大的挑战，但也恰恰是专注于推进区块链技术应用的企业的机遇所在。

从比特币的提出到现在，区块链的从业者们尝试了各种多样化的落地应用场景。最初是币(coin)的应用，各种虚拟货币的出现和热炒引起了广泛关注和讨论，缺乏有效监管的数据货币可能带来的泡沫危机也引起了各国重视。与此同时，人们发现，作为比特币底层技术的区块链可以尝试用来解决一些现有业务痛点，开展如身份识别、数据确权、信用管理、价值流转等多种创新业务模式，于是在金融和多个产业领域开始形成一些组织联盟，如 R3、Hyperledger 等，技术圈也逐渐将更多的关注从“币”转到了区块链的各种业务应用上来。

目前区块链技术可以大范围应用的场景比较少，无论是技术上还是业务上都还处在探索阶段。许多领域进行了广泛的尝试，如供应链管理、互联网金融、证券和银行业务、贸易融资、保险、医疗健康、资产管理、数

字版权保护、公益慈善、政府公共服务、监管合规性与审计、游戏、公益等。

业界的积极实践进一步巩固和加深了人们对区块链技术潜在应用价值的期待，但目前却仍罕有成功的、可持续的商业化落地案例，坦白来说，大多数案例还停留在理念或 POC 阶段。

1.3 区块链未来的技术发展趋势

即便区块链面临诸多挑战，但是，越来越多的人愿意相信其在未来将会发挥更加重大的作用。作为区块链技术研究与落地应用领域的从业者之一，我们认为该技术的未来发展将在如下几点：

1.3.1 创新的治理模型

现有的很多区块链项目，其治理和经济模型都是有局限性的。

对此我们认为，对于区块链项目，绝对的中心化和去中心化是一个伪命题，未来的区块链既不需要绝对的去中心化，也不是绝对的中心化，而是应该在其中寻找一个平衡点，使得去中心化和中心化有机的结合，才能使区块链这项技术发挥最大的效用。

1.3.2 各种底层核心技术的出现及区块链技术的平台化

区块链技术曾被预测为引领第五次技术革命的重要技术。在这样全球聚焦，多国鼓励的宏观趋势背景下，对区块链技术底层的研究与探索将会越来越重要。目前各家大型区块链研究机构和技术型企业均有自己的底层链技术研发。以国内为例，不光是区块链行业领域的众多初创企业，包括 BAT 等国内互联网的巨头也都纷纷投入重兵到区块链领域开展底层核心技术的研发。

未来区块链技术终将和众多企业业务相结合，企业将业务“上链”的过程势必要更加简单快捷，否则将无法跟上经济的高速发展。而区块链技术

设施的平台化可以为企业快速部署区块链提供便捷的通道。未来在大规模企业级应用中，方便、平台化的区块链基础设施、必将作为基础级设施在企业推广区块链的道路上发挥重要的作用。

1.3.3 在金融、清算领域率先实现突破

区块链技术诞生于金融场景，虽然如今很多应用已经脱离了金融领域，但是金融场景仍然是区块链技术最契合的场景，特别是在身份识别、数据确权、信用管理、价值流转、交易清算/结算等方面，利用区块链解决金融场景中的信任问题，可以为企业节省成本，提升效率，创造巨大的商业发展潜力。

1.3.4 在 5G 技术为代表的高速海量互联场景下融入实体经济

5G 技术，即第五代移动通信系统，通过提供更高的数据传输效率、更广的服务规模、更低的通信延迟，将为世界带来爆炸性的移动数据流量增长、海量的设备连接。更重要的是，5G 技术为不断涌现的各类新业务和应用场景提供技术支撑，如物联网、车联网、工业、大数据和广播类服务等，以及在发生自然灾害时的生命线通信等，移动通信技术也因此实现了从个人业务应用向行业业务应用的转变。

在具体的应用场景上，5G 技术与区块链技术拥有先天的整合优势。5G 技术的优势在于数据信息传输的速率高、网络覆盖广、通信延时低，并允许海量设备介入，其愿景是实现万物互联，构建数字化的社会经济体系，但 5G 技术依然未能完全打破目前通信技术所遇到的一些问题，如隐私信息安全、虚拟知识产权保护、虚拟交易信任缺失等。区块链技术核心优势，是能够重建当前依赖中心机构信任背书的交易模式，用密码学的手段为交易去中心化、交易信息隐私保护、历史记录防篡改、可追溯等提供的技术支持，而其缺点如延时高、交易速率慢、基础设备要求高等，恰好

在与 5G 技术结合后得到了本质提升。

区块链与人工智能、物联网、5G 技术的结合，有望推动智慧医疗、智慧交通、智慧城市、数字社会、资产上链等领域的发展。区块链技术可对现实物理资产进行确权，通过智能合约等技术，使得通证化的物理资产在链上更灵活、更自由地流转，丰富市场层次，充分激发生产力。5G 和 NB-IoT 为代表的物联网技术将会突破现有物联网的局限，广泛应用在物流、农业、自动化管理等各个领域，在生产效率、成本和安全性方面带来巨大创新优势。人工智能技术将使得工业生产、资产流转等效率更高，资源得到更优质的配置。而 5G 技术则作为上述技术的基础设施，在高速的数据传输下使得人与人、人与物、物与物之间更高效、可靠的连接成为可能。

2 YeeCo 解决方案介绍

2.1 YeeCo 的目标定位

YeeCo 的目标是成为一个去中心化的高性能万物互联网络的基础设施，在以 5G 为代表的高速海量互联场景中做价值传递载体。

YeeCo 基于全新的『分片+分层』高性能架构：采用全分片 PoW 创新方案，同时利用独创的 CRFG 最终确定性技术来解决跨分片及跨链交易的安全和效率问题。

2.2 YeeCo 的核心特性

1. 高性能：基础性能为 50000TPS（在现有主流机器的配置下），同时实现按需扩容，可通过灵活增加分片数实现高达百万级 TPS；

2. 去中心化：在实现高性能的基础上，验证节点的参与无需许可，同时将验证节点的参与门槛控制在较低水平，让 YeeCo 网络更加去中心化；

3. 高灵活性：利用 CRFG 最终确定性技术，实现 Layer1 对接多种 Layer2 的跨链方案，使得业务构建更加灵活；

4. 高安全性：继承了 PoW 共识高攻击成本及验证节点不易暴露等安全特征，CRFG 最终确定性技术能进一步防分叉，抵御长程攻击；

5. 高智能化：实现新一代智能合约，满足物联网、人工智能、智慧城市，智慧交通，智慧医疗、智慧农业、开放式金融等新领域应用需求；

2.3 YeeCo 架构概览

YeeCo 自身主要由数据层、网络层、共识层、激励层、合约层、应用层等构成，从而组成了一个完善的区块链生态体系。

YeeCo 的底层网络平台采用了 P2P 网络方式部署，是一个真正的去中心化的网络形式。网络中的每个节点并无主从之分，既能充当网络服务的提供者，又是网络服务的请求者。每个节点都可以对其它节点的请求做出响应，提供资源、服务和内容，包括信息的共享和交换，计算资源（CPU, 内存）的共享、存储资源的共享等等，具备可扩展、去中心化、健壮（ROBUST）、隐私保护、负载均衡的特点。

YeeCo 的底层数据存储能力采用了自主研发的分片存储网络服务(CDHT)，系统中所有的数据（包括文件、交易数据等等），最终都是以键值对[5]的形式被保存在去中心化的分片存储网络 CDHT 中。CDHT 就像是一个云端存储系统，架构在 YeeCo 的 P2P 网络之上，充分利用了 P2P 网络的优点，易于扩展，安全，因为数据是存储在网络中的多个节点上，

所以没有单点失效造成的数据丢失风险。

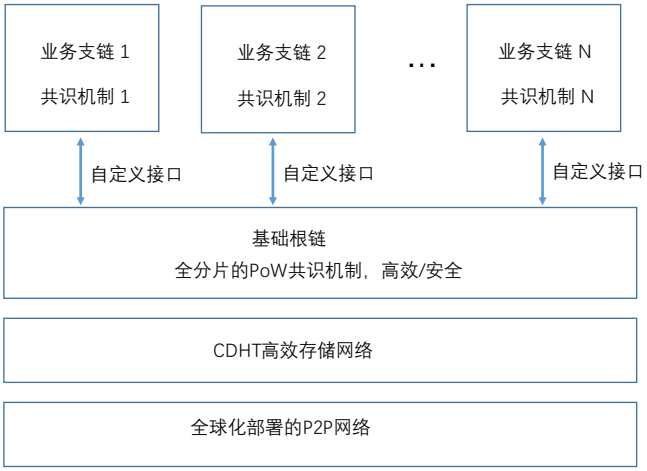
此外，YeeCo 的应用节点还内置了智能合约和 YeeCo 虚拟机，从而允许开发人员方便快捷地开发出可以和传统互联网应用相媲美的去中心化应用程序(DAPPs)。

YeeCo 的底层公链平台逻辑上将采用分层的架构，底层由一个支持高安全性（完全去中心化）和高吞吐量的基础根链构成，并通过链接多个业务支链实现业务层面的扩充和伸缩。

整体上的业务部署可以通过不断地扩充 YeeCo 的业务支链和划分多子网来进行动态扩容。

YeeCo 的基础根链坚持采用了 PoW 共识机制，但是通过全分片的机制在保留了区块链的去中心化和高安全性的基础上，同时又突破了传统 PoW 共识算法所具备的性能局限，性能上远远超过现有 PoW 主流区块链业务的交易速度，从而解决了困扰区块链的不可能三角问题。

YeeCo 的业务支链用于承载不同的业务场景，技术上使用内部消息通道和根链进行关键信息的交换。根据实际的业务需求，不同的支链可以采用不同的部署模式和差异化的共识算法，以满足不同的应用场景对于系统性能、安全、去中心化的差异化要求。

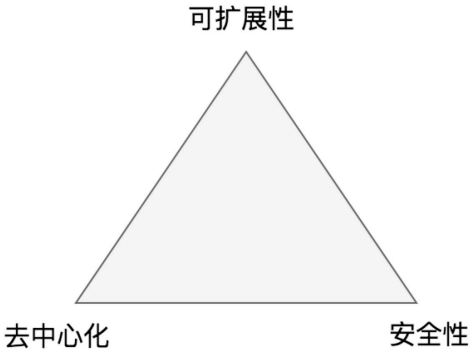


由于 YeeCo 的业务支链支持多种共识机制，因此想要良好的进行业务发展就需要良好的社区氛围以及成熟的治理模块，用于业务发展中的各种问题和规则的制定和调整。对此 YeeCo 还内置了社区治理能力和激励机制，用于推进项目的良好发展。

总体而言，YeeCo 作为区块链基础设施具备很高的业务适应性和伸缩性，能支持各种商业场景的部署需求和组网要求，并在去中心化部署的基础上实现了高性能的商业化部署能力及完善的自我管理和激励能力。

2.4 全分片架构突破区块链三角

众所周知，区块链技术存在一个不可能三角[1]，即系统的可扩展性（性能）、去中心化和安全性无法同时全部满足。



区块链系统的不可能三角

传统的中心化解决方案都是以安全性和可扩展性作为设计目标的，因为不需要考虑去中心化，数据、CPU、带宽、设备高度集中，几十万甚至上百万服务器并发服务，以淘宝为例，每秒能完成几万笔的交易。

但是区块链系统，去中心化是其最基本的特点。实践已经证明，在复杂的分布式系统中，无论用何种共识算法，只要系统的去中心化程度越高，其达成共识的速度就越慢，这是无法跨越的鸿沟。目前最快的区块链共识算法实际速度也就几千 TPS，远远不能满足实际应用的要求，而且其去中心化程度非常低，比如 EOS，仅仅使用了 21 个超级节点，这实际上是一种一定程度上妥协的中心化部署了。

另外一个问题是，业务的发展是在一开始无法就完全考虑清楚的，后续如果不限制的将所有去中心化应用都部署在唯一一条链上是根本不现实的，网络拥堵问题将无法解决。以太坊去中心化应用 DAPPS 的糟糕体验也证明了这一点。[2]

目前一种主流的解决思路就是通过分片技术来增加基础网络的吞吐量。分片技术独特于其他解决扩容的链上技术的关键特性，就是它可以进行水平扩容，也就是说，网络的吞吐量随着挖矿网络的扩展而增加，在扩展性能的同时也不会降低去中心化程度和安全性。这种特殊的特性可能使它成为推动区块链技术被快速采用的理想技术。

在底层公有链的系统内，网络上的交易将被分成不同的碎片，其由网络上的不同节点组成。因此，只需要处理一小部分输入的交易，并且通过与网络上的其他节点并行处理就能完成大量的验证工作。将网络分割为碎片会使得更多的交易同时被处理和验证，本质是通过改变网络内部各步骤之间的验证方式来增加吞吐量。因此，随着网络的增长，区块链处理越来越多的交易将成为可能。

目前主流的分片技术分为网络分片、交易分片和状态分片等三个层级，其技术难度也随之依次递增。主要的核心在于分片内节点需要达到一致，并且防止被恶意攻击者控制，而分片之间需要信息传递机制，保证交易及智能合约的状态在不同分片间达到一致。

与以上介绍的网络分片、交易分片和状态分片的方案不同，YeeCo 采用了全分片的架构设计，在确保去中心化、安全的前提下，最大程度的实现了基于 PoW 共识算法下的性能提升，有效的解决了区块链三角问题。

（1）第一角：确保安全性

区块链系统的安全性是不容妥协的，否则所有其他特性将毫无意义。区块链系统的安全性，可以用在系统中构造非法区块（破坏数据完整性或双花攻击）并得到全网认可的代价来衡量。在 PoW 共识机制中，这个代价就是实施攻击的最小挖矿算力。Nakamoto 共识算法保证恶意算力在 51%以下的时候，系统就是安全的。YeeCo 可以保证在采用分片架构之后不会引入 1%攻击问题，即保证恶意算力在全网 51%以下的时候，其也无法对任意一个分片进行攻击。

（2）第二角：坚持去中心化

作为价值互联网的基础设施，YeeCo 仍然坚持基础公链必须是一个

permissionless 的系统，并且系统中不存在不可替代的角色或者节点，这是一个根本的定性的要求。一个区块链系统的去中心化程度一方面体现在对等节点的抗合谋性，另一方面体现在对等节点的网络规模。 YeeCo 在这两方面都有较好的表现。首先，YeeCo 继承了 PoW 共识的较高的抗合谋性，不引入复杂的治理模式，保持对等节点的纯粹性和多样性，对等节点更趋于竞争而非合谋；此外，YeeCo 通过分片架构，使得每个对等节点只需要同步，验证，保存账本的一部分，降低了对等节点的参与门槛，对提升对等节点的网络规模起到了正向作用。

（3）第三角：实现高性能

YeeCo 的全分片架构将完全切分一个区块链系统的四大工作负荷，即：带宽(广播区块和交易)，计算(验证交易和更新状态)，内存(存储账本的最新状态)，磁盘读写(记录历史区块)。我们认为真正具备高可伸缩性的区块链系统必须能够突破全部四个瓶颈，而不是仅突破其中的某个或某几个。衡量性能有两个指标，一个是吞吐量，即最高每秒处理多少笔交易(TPS)，一个是容量，即可以表达的账本状态的内存总量。引入分片对于提升整个系统的吞吐量和容量，以及让系统获得高可伸缩性是易于理解的，而带来的最大挑战就是能否安全的处理跨分片交易，以及这种处理机制是否会牺牲高可伸缩性。YeeCo 的跨分片交易处理机制实现了吞吐量和容量可以随分片数 n 线性增长，在现有的互联网平均带宽约束的前提下，将分片数 n 做到数万这个量级，可以达到数万 TPS 的性能水平，足以应对主流的价值互联网应用（如转账、资产管理+交易等）的性能需求。

2.5 YeeCo 的分层方案解决业务的差异化需求

YeeCo 对 DAPP 的分层架构做了再思考，当前其他公链方案的 DAPP，往往基于性能，交易成本和存储成本的考虑，提供了与链上智能合约配合的中心化系统，这种分层架构面临如下问题：

1、中心化系统中的计算和数据面临信任问题

2、中心化系统和链上互操作的方法缺乏统一方案，研发效率和安全

性面临挑战

3、链上智能合约部分的效率仍然受限于链本身的性能

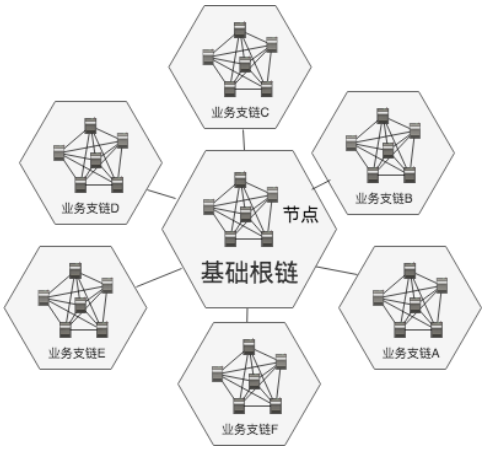
因此 YeeCo 认为在底层根链和中心化系统之间引入一层业务支链将成为 DAPP 的常规形态，业务支链具有如下作用：

1、将应用中原本只能运行在中心化系统中的部分进一步去中心化，满足公开、可信、防篡改等需求

2、支链提供了和底层根链互操作的统一方式，业务开发者可以直接利用支链的基础架构，聚焦在业务本身

3、支链可以在共识范围和所支持的计算复杂度上做取舍以满足应用的性能要求

4、支链的存在让底层根链的定位更清晰，底层根链的重点在于建立全局共识，满足交易吞吐量和状态容量的伸缩性需求，为计算和存储资源建立良性的经济模型



总之，YeeCo 设计的区块链世界的基础构成，其实就是多个 YeeCo 区块链业务平台在 YeeCo 的业务支链上的分布，每个平台都使用同样的区块链协议，通过 YeeCo 统一提供的接口规范和基础根链进行交互。各个业务支链可以动态加入或退出，并不会对整个区块链网络造成影响。

2.6 YeeCo 的特色技术介绍

2.6.1 全分片架构设计

如前文所述，YeeCo 的全分片架构将完全切分四大工作负荷，即：带宽(广播区块和交易)，计算(验证交易和更新状态)，内存(存储账本的最新状态)，磁盘读写(记录历史区块)。每个分片的工作模式和现有的单链系统完全一致，独立的完成同步交易，验证交易，打包区块，同步区块这些过程，共同维护一个账本，只不过这个账本是 YeeCo 整体系统对应的大账本的一部分。现有的 PoW 机制如何达成共识，如何激励矿工竞争记账权，如何保证安全性，如何保证去中心化在每个分片的链上也仍然是完全独立的生效的。

那么如何来切分全网的四大工作负载呢？我们限定分片数 n 为 2 的 k 次幂，即 n=2^k。只要 k 确定了，任何一个地址，根据其二进制数据的前 k 个比特，就会被分配到一个确定的分片中。而每个交易，根据交易的验证方的地址 (例如转账交易的支付方)，也会被分配到一个确定的分片中。所以 YeeCo 的分片不需要任何中心化的机制来切分地址和交易。

YeeCo 的节点工作在特定的分片上，处在同一个分片中的节点会通过独立的子网进行 P2P 通信，不同分片的子网之间互不干扰。具体而言，子网由 DHT 的 Swarm 实现，每一个广播子网对应一个 Swarm。

每个分片的节点发起的交易，广播的交易，同步的交易，验证的交易，打包的区块，同步的区块对应的数据全部都是符合分片的地址规则的，而且分片之间没有锁机制，完全并行，从而实现了工作负载的切分。

我们进一步来看 YeeCo 的全分片架构是如何满足区块链三角的情况的：

（1）安全性

YeeCo 的每个分片的链的安全机制和目前的 PoW 单链系统是一样的，每个分片的安全取决于分片内诚实节点的算力的比例。分片引入的挑战是

全网算力分散到每个分片之后，单个分片的防御壁垒将下降到 51/n %，(即所谓的 1%攻击)。针对这种风险，YeeCo 引入了并行挖矿的机制，使得攻击任何一个特定的分片，仍然需要超过全网 51%的算力。

关于并行挖矿的机制，我们将在本文的稍后章节有专门的介绍。

（2）高性能

YeeCo 通过分片架构将带宽，计算，内存，磁盘读写的工作负载切分开，获得了吞吐量和容量上的高可伸缩性。分片引入的挑战是如何安全的完成跨分片交易并且不牺牲高可伸缩性。对此 YeeCo 引入了为 PoW 共识建立绝对确定性的方案 CRFG（Conditional Reward Finality Gadget），使得跨分片交易可以拆分成可独立验证的子交易，避免了锁机制带来的和分片数相关的性能代价，而只引入了和分片数无关的数据传输量和验证交易的代价，从而保证了高吞吐量。

关于 CRFG，在本文的稍后章节中也将专门介绍。

（3）去中心化

YeeCo 保持了基于 PoW 的区块链系统的去中心化，系统是一个彻底的无许可的系统，节点参与验证的门槛较低，且具有较强的抗合谋性。

2.6.2 并行挖矿

通常情况下，在一个有 n 个分片的区块链系统中，每个分片的算力都只有全网的 n 分之一。恶意节点利用全网 51/n %的算力就可以攻击一个分片，从而使全网丧失有效性，这就是所谓的 1%攻击问题。

为了有效的抵御这样的风险，YeeCo 引入了并行挖矿的设计。

PoW 共识机制中，节点打包一个证明了和前一个区块相关联，并且证明包含了被验证过的交易的区块本身的代价并不大，而算力所做的工作量证明仅仅是为了有意增大出块难度，降低在特定时间内全网同时出大于一个块的概率（特定时间内全网出大于一个块的概率越大，越容易形成分叉从而达不成共识）。

节点打包区块时，通过构造交易的 Merkle 树，证明交易被包含在内，

而理论上我们可以在保证 Merkle 树包含需要被验证的交易的前提下，添加任意我们想证明的其他交易，甚至是其他链上的交易，形成了一份算力在多条链上并行挖矿的形态。当多个链的算力按照统一的机制在多条链上并行挖矿的时候，则既可以满足所有链的验证需求，同时总的算力开销可被大大降低。

具体而言，参与并行挖矿的算力分别构造多个链的区块，将这些区块的块头构造成一个 Merkle 树，然后探测 nonce 并计算哈希，一旦哈希满足某个链的难度要求，即完成了此链的一个新区块打包，这个新区块包含了之前构造的此链的区块，以及区块块头在块头 Merkle 树的 Merkle Proof，从而提供了区块交易的 include 证明。

YeeCo 的所有分片链都支持并行挖矿，一份算力原本只能作用在一个分片，现在通过并行挖矿，这一份算力可以作用在所有分片上，从而每个分片链的难度都会被推高到和全网算力全部都在一个链上挖矿相同的水平。所以仍然保证了只要恶意节点的算力占全网不超过 51%，就无法攻击任何一个分片。

另外一点要说明的是并行挖矿所带来的收益和付出的成本。对于矿工而言，参与并行挖矿的收益很明显，其有机会获得多个链的出块奖励，事实上矿工为了最大化收益，都会尽量启用并行挖矿，从而使其安全机制被最大程度的发挥出来。

从成本的角度来看，启用并行挖矿需要矿工运行多个链的全节点，从而带来了更多的 IT 成本支出，但是这些成本和传统 PoW 大型矿场的矿机开销来说，基本上可以忽略不计了。

2.6.3 基于 CRFG 的跨分片交易机制

在前面的介绍中指出，YeeCo 根据地址前缀进行分片划分，当分片数越大的时候，跨分片交易发生的概率也越高。经过试验数据发现，当使用以太坊 REC20 的历史交易数据，分片数为 64 时，跨分片交易的比例会超过 95%。

针对此情况，YeeCo 引入了为 PoW 共识建立绝对确定性的方案 CRFG（Conditional Reward Finality Gadget），使得跨分片交易可以拆分成可独立验证的子交易，避免了锁机制带来的和分片数相关的性能代价，而只引入了和分片数无关的数据传输量和验证交易的代价，保证了高吞吐量。

下面详细阐述 YeeCo 的跨分片交易机制。跨分片交易本质是一个跨链交易，一个交易被拆分成两个过程，第一个过程在一条链上做余额检查和减少余额操作，第二个过程在另一条链上做增加余额操作，两个过程整体要是一个原子操作。实现跨链的原子操作无外乎三种方案：

1. 两个链同步出块，这样出块成功就意味了两个过程同时成功，出块失败就意味着两个过程同时失败，从而实现了原子性，但是这种方式会引入两个分片的同步机制，从而降低了分片的独立性，会额外的增加和分片数相关的性能开销。
2. 在经典 PoW 不具备绝对最终确定性的前提下，引入回滚处理机制，第二条链能检测第一条链的回滚情况，并且对第二条链的区块进行修改，这种机制会面临更复杂的情况，比如第二条链上的通过跨链交易获得的余额被支付到第三条链上，这样会极大的增加业务应用开发的难度。
3. 为 PoW 建立绝对最终确定性，如果第一个过程对应的交易得到了最终确定，则第二个过程的交易可以实现一个确定的 SPV 验证，从而保证了整个交易要么处于完成状态，要么处于未最终确认状态，是安全的。

在实际的实现中，YeeCo 选择了第三种方案，即提出了一套叫做 CRFG 的方案为 PoW 共识建立绝对确定性。

CRFG 方案包含下列要点：

1. 出块共识和建立确定性的共识相分离

PoW 共识不要求稳定的共识范围，即允许共识参与者的自由进出，实现的是最终一致性，在出块时（高度为 n）立即建立确定性是无法实现的，

而在 k 个确认，达到足够高的概率确定性时，就具有建立绝对确定性的基础，CRFG 方案中是对 $Block_{n-k+1}$（高度为 n-k+1 的块）建立确定性。

2. 根据出块选取投票者集合，通过 PBFT 建立确定性共识

如果要对 $Block_{n-k+1}$ 建立确定性，则选取其之前 m 个块的出块节点作为投票者集合，即 $Block_{n-k-m+2}$ 到 $Block_{n-k+1}$ 的出块节点，这些节点按照一个区块一票的原则进行投票，通过 PBFT 建立 $Block_{n-k+1}$ 的确定性。首先探讨其成功率，$Block_{n-k+1}$ 是一个有 k 个确认的区块，正常节点同步到的链包含相同的 $Block_{n-k+1}$ 的概率和 k 个确认的置信水平相当，投票节点按照自身同步的链的实际情况投票达成共识的概率足够高；其次探讨公平性，引入 m 个出块节点投票对妄图从 $Block_{n-k+1}$ 开始重铸链的算力进行了限制，共识仍然以工作量证明为依据，保证了共识参与者可自由进出，但对滥用算力的行为进行了限制，具有更好的公平性。

3. 采取有条件的区块奖励（Conditional Reward）机制，解决无利害攻击问题

经典的 PoW 共识的区块奖励由出块矿工在区块中添加一条 coinbase 交易来完成，在 CRFG 中，$Block_{n-k-m+2}$ 的出块矿工 A 的奖励会延迟到 $Block_{n+t}$ 发放（t 是一个用于调节奖励延迟的系统参数）。在延迟期间，针对 $Block_{n-k-m+2}$ 到 $Block_{n-k+1}$ 的确定性的投票，矿工 A 都需要逐个参与，此投票带有矿工 A 的签名并不可伪造，如果矿工 A 有投分裂票的行为（投的区块不在一条链上），此行为可被后续区块 $Block_{n+t}$ 的矿工 B 所识别并记录。$Block_{n+t}$ 的出块矿工 B 需负责确保如下规则：如果发现矿工 A 有投分裂票的行为，则 B 会把奖励发给自己；如果没有发现矿工 A 有投分裂票的行为，则 B 把奖励发给 A。这样可以激励矿工去发现投分裂票的行为，一经发现，投分裂票的矿工将拿不到区块奖励，之前的算力投入作废，解决了无利害攻击问题。

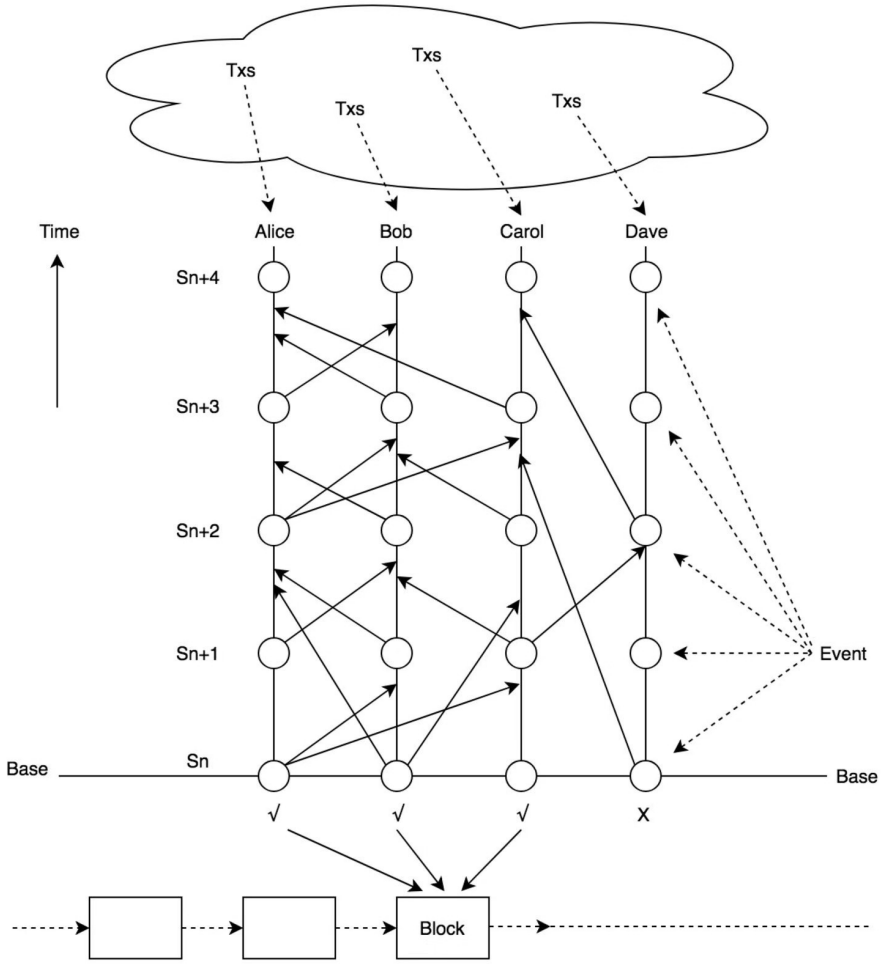
根据 CRFG 方案达成了最终确定性之后，实现跨分片交易的原子性就相对容易了。如果跨分片交易的第一个过程已经入块但还没达成最终确定性，第二个过程无法完成确定性 SPV 验证，不会入块，第二个过程的余额

增加操作处于未确认状态，不可花费；如果跨分片交易的第一个过程发生了回滚，则第二个过程的交易失效；如果跨分片交易的第一个过程达成了最终确定性，第二个过程可以完成确定性 SPV 验证，会打包交易，余额增加操作处于已确认状态，可以花费。

2.6.4 Tetris 共识算法

对于某些特定的商业场景，如果对于完全的去中心化没有特别的要求，例如某些行业场景，联盟链场景等，但是对于交易的确认速度和流量有特别高的要求，这种情况下可以在 YeeCo 的业务支链上采用 YeeCo 独创的 Tetris 共识算法来进行部署。

YeeCo 独创了高吞吐量的 Tetris 共识算法，将交易速度大幅提升到 10000 笔/秒。本质上 Tetris 共识算法是一种异步拜占庭容错(BFT) [3]，所以其具备最终确定性（Termination）、一致性（Agreement）和有效性(Validity)的优点，并不像比特币，最终确定性只是一种临时性的假设，其实理论上永远无法达成。Tetris 共识的核心思想来源于知识推理，我们认为知识推理是揭示和分析分布式系统的基本复杂性和微妙之处的最合适的工具。通过分析每个参与的验证者节点在不可靠系统中所获得的知识的状态迁移，我们可以捕获系统的一些基础信息，然后帮助我们设计有效和高效的协议。加上采用完全信息协议（FIP）和优化的消息流量模型，Tetris 最终获得了高性能，并证明了安全性。和其它共识算法相比（比如 POW），Tetris 在几秒钟就可以达成确定性共识。同时，Tetris 还实现公平性 [4]，在一些应用中这一特质是非常重要的，比如去中心化交易所。



采用 Tetris 共识算法的业务网络将是一个由多个节点构成的 P2P 网络，其中会预先选定一些节点作为验证节点并分配一个唯一的标识符：VID。验证节点负责处理数据达成共识并生成新区快。每一个验证节点会持续收到两种广播数据，一种是交易数据本身，一种是事件（Event）。

验证节点因此会周期性地产生事件并将它广播给其它验证节点。

每个事件有一个唯一的序列号：

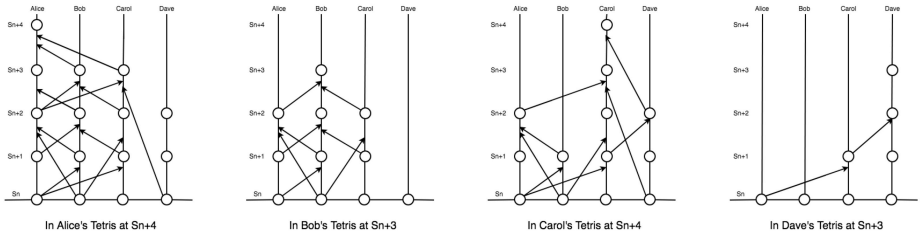
$$N = \text{Max}(\text{所有父节点的序列号N}) + 1$$

事件的数据结构如下：

$$E = \{VID, N, \{Hash\ of\ E0, E1, ...\}, \{Hash\ of\ tx0, tx1, tx2, ...\}\}$$

- E0 代表本验证节点产生的最后一个事件，我们叫做***原生父事件***。
- Ei 代表从其它节点发来的事件，我们叫做***其它父事件***。
- E 和 E0 以及 Ei（例如，E1, E2, ……）统称为 E 的***祖先***

当事件被发送的时候，会被发送节点签名，同时在被接受的时候，也会被接收节点验证。在验证的时候，验证节点会检查事件包含的数据（父事件、交易等）是否都已经收到，如果没有，验证节点会通过发送DHT请求从CDHT中将所需要的数据取回。这样在每个验证节点，所有事件就构成了一个有向图，我们称之为Tetris，标记为T。此外，我们可以用$T_{vid,n}$来表示验证节点（节点ID: vid）收到事件 $E_{vid,n}$ 时的状态。例如：$T_{alice,4,}$ $T_{bob,3,}$ $T_{carol,4,}$ $T_{dave,3}$ 表示如下：



这个有向图实际上就包含了当前节点所了解的全部信息（Full Information）。

Tetris 协议是一个全信息协议（Full Information Protocol），每个验证节点都会将自己所了解的所有信息作为事件发送给其它节点。

任何时刻，有向图的最底端都是等待被确认的事件，我们称之为基线事件（Base Event）。交易和事件不断从有向图上边落下来，因此节点知道的信息（知识）会越来越多，当满足一定的条件的时候，基线事件就可以被确认（YES/NO），所有被标记为 YES 的事件所包含的交易就是候选区块，将来就可以被打包到区块上。当基线事件被确认之后，整个基线就从有向图中被消除，之上的事件会落下来成为新的基线事件。整个过程（我们称之为 Stage，具备一个序号，该序号和区块高度一致）非常像传统的俄罗斯方块（Tetris）游戏，这也是为什么这种共识机制被叫做 Tetris 的原因。

每个业务节点都是通过不断获取新的信息，依据自己维护的有向图 T 来最终做出决定的，由于分布式网络的复杂性，虽然每个节点的有向图 T 在某一时刻可能并不相同，但是随着时间的推移，最终其底部会趋于一致，

也最终导致一致性的结果。

Tetris 是拜占庭容错模型，因此我们必须要考虑所有节点都是拜占庭节点的情况。假设存在 t 个恶意节点，那么根据拜占庭容错，总节点数至少为 3t+1 才能确保系统能够达成共识。通过操纵，恶意节点可能会把正确的事件 e 广播给系统中的一部分节点，同时把事件 e 的一个分叉 e'（错误的事件）广播给系统的另一部分。

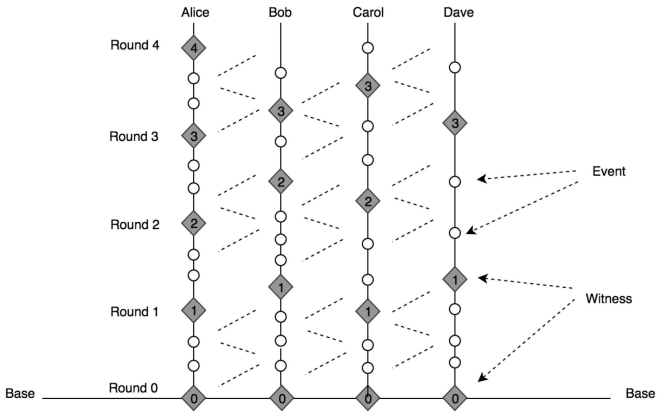
这里涉及到几个重要的概念：

- **知道（Know）**：事件 x ***知道*** 事件 y。代表 y 是 x 的祖先，同时 x 的所有祖先里都不包含 y 的创造者发出的分叉 y'。
- **众所周知（Know-Well）**：事件 x ***众所周知*** 事件 y。代表 x ***知道*** y，同时存在一个事件的集合 S，S 包括至少来自 2t+1 个节点的事件。x ***知道*** S 里所有的事件，并且 S 里所有的事件都 ***知道*** y。

我们可以证明，如果一个事件 e 存在分叉 e'，并且事件 x 在某一个验证节点 ***众所周知*** e，那么在其它节点上不可能存在任何一个事件可以 ***众所周知*** e'。

- **轮次（Round）**：在每个阶段（Stage），基线事件被定义为第 0 轮，每个基线事件之上的事件，我们定义轮次 round = r + i，r 是 e 的所有父事件的轮次的最大值，如果 e 可以被至少 2t+1 个证人在第 r 轮 ***众所周知*** 则 i = 1，否则，I = 0。
- **证人（Witness）**：代表验证节点在一个轮次里创建的第一个事件，因此基线事件被称作第 0 轮证人。

这样，我们可以把有向图 T 转化成一个相对有序的结构：



这个结构已经和同步系统的轮次概念就非常相似了，我们可以知道：

- ✧ 每个轮次 r，如果存在一个 r+1 轮次证人则一定存在至少 2t+1 个本轮次证人
- ✧ 每个轮次 r 的证人一定 ***众所周知*** 至少 2t+1 个轮次 r-1 的证人
- ✧ 证人在每个轮次不一定具备相同的序号
- ✧ 所有验证节点的有向图 T 包含的证人都是一致的

现在让我们看看共识是如何达成的：

```
function decide()

e.well-known = UNDECIDED
for each witness w in round 1
    w.vote = 1 if w know-well e, 0 otherwise.
for each witness w in round 2
    s = the set of witnesses in round 1 which w know-well
    w.vote = 1 if there are t/2 or more witnesses in s vote 1
                otherwise w.vote = 0
for r = 3 to current max round
    for each witness w in round r
        s = the set of witnesses in round r-1 which w know-well
        v = majority vote in s, 1 for a tie
        n = number of events in s with a vote of v
        if n >= 2t+1
            e.well-known = v
            w.vote = v
            return v as decided
        else
            w.vote = v
```

只要有新的证人出现在 Tetris 中，这个方法就会被调用，直到所有的基线事件被 ***众所周知。***

一旦确定了所有的基线事件，验证节点将检查这些基线事件中包含的

所有交易。如果某一交易的哈希出现在至少 t+1 个来自不同验证节点的事件（包括祖先）中，那么这个交易可以被标记为可提交。每个验证节点将为这些可提交的交易创建一个区块头，并通过其私钥进行签名并进行广播。网络上的所有节点一旦接收到由验证节点签名的 t + 1 个区块头，就可以确保生成新区块。然后，当前的基线事件将消失，上边的事件落下来形成新的基线事件重复上述所有内容以生成下一个区块。

根据 FLP 定理，在假设网络可靠、节点只会因崩溃而失效的最小化异步模型系统中，仍然不存在一个可以解决一致性问题的确定性算法。为了确保最终确定性，我们引入了一个抛硬币的随机轮来避免这个问题：

```
for each witness w in round r
    s = the set of witnesses in round r-1 which w know-well
    v = majority vote in s, 1 for a tie
    n = number of events in s with a vote of v
    c = a constant of interval of coin round, such as 10.
    if r mod c > 0
        if n >= 2t+1
            e.well-known = v
            w.vote = v
            return v as decided
        else
            w.vote = v
    else
        if n > 2t+1
            w.vote = v
        else
            w.vote = middle bit of w.signature
```

当然在现实世界，出现这个情况的可能性几乎为 0。

2.6.5 YeeCo 智能合约和 YeeCo 服务单元

YeeCo 将采用受限图灵完备智能合约，避免合约过于复杂而造成性能和安全漏洞；同时采用 Rule-based 智能合约语言，以接近自然语言便于非技术人员创建合约，为了方便开发人员，YeeCo 也提供了很多智能合约模板可供开发人员参考。由于智能合约需要全部验证节点进行验证执行，导致智能合约的运行效率受到局限，不能满足大多数复杂应用程序的需要。YeeCo 设计了独一无二的 YeeCo 服务单元来解决这个问题，YeeCo

服务单元更像是传统应用的源代码，包括核心业务逻辑，可以通过各种协议栈和 YeeCo 客户端、YeeCo 智能合约、YeeCo 应用引擎和分布式数据库引擎进行交互。通过 YeeCo 服务单元可以编写出类似传统搜索引擎、购物网站、博客一样的应用。YeeCo 服务单元一旦发布并认证，所有人都可以看到源代码，真正做到了开放、共享和协作。

2.6.6 YeeCo 虚拟机

YeeCo 虚拟机是建立在 YeeCo 区块链上的代码运行环境，其主要作用是运行系统内的智能合约。简单来说，YeeCo 虚拟机就是一个完全独立的沙箱，合约代码一旦发布对外完全隔离并且只能在 YVM 内部运行，YVM 分布在每个应用节点的计算机上。可以使用 Solidity、C++等编程语言创建运行于 YVM 的智能合约。

YeeCo 虚拟机是一个图灵完备的运行环境，并且具备可并发，快速高效、确定性、易于扩展、节省资源、安全等特点。

同时，YeeCo 虚拟机计划兼容 Ethereum 和 EOS 智能合约，可以方便开发人员将已有 APP 快速地移植到 YeeCo 中来。

2.6.7 YeeCo 的社区治理模块

虽然 YeeCo 的基础主链是基于 PoW 挖矿机制，本身就实现了高度的业务自治。但是对于众多的业务支链而言，是可以支持多种其他的共识机制的，因此对于这种情况下，想要良好的发展业务就需要成熟的治理模块，用于业务发展中的各种问题和规则的制定和调整。对此 YeeCo 设计了一套章程与治理体系来满足这个要求，主要包括以下方面：

YeeCo 的机构可以根据一定的规则从业务节点中选出若干名委员，每个委员必须持有一定量的系统通证。Token 的所有者投票选出若干个节点作为管理委员会委员，票数可以按照多种原则进行统计和确权。

任何一个管理委员会的委员都可以提出提案，管理委员会可以对提案

进行投票，从而改变预先默认设置好的系统参数（比如区块大小，出块时间等），协作更新。

同时当我们需要更新已有的系统协议或者修复系统漏洞的时候，YeeCo 也可以采取同样的策略进行投票，从而保证系统健康稳定的发展。

2.6.8 分片存储网络服务(CDHT)

YeeCo 对标准的 DHT 做了技术上的改进，来确保分布式存储在极端条件下仍然可用。在 YeeCo 网络中，每个节点都有一个节点 ID（一个 256 位的整数），两个节点之间距离并不是依靠物理距离来衡量的，事实上，YeeCo 网络将任意两个节点之间的距离 d 定义为其二者 ID 值的逐比特二进制和（xor），即，假定两个节点的 ID 分别为 a 与 b，则有：

$$\boldsymbol{d = a \oplus b}$$

在 YeeCo 中，每一个节点都可以根据这一逻辑距离来判断其他节点距离自己的“远近”。存储内容时，系统会选出节点 ID 距离其 Key 值最近的 k 个节点作为存储节点，之所以选择 k 个节点，主要是考虑到整个 YeeCo 系统可靠性而引入的冗余。

和传统的 DHT 相比，CDHT 并不是把内容简单地复制 k 份保存在 k 个节点上。YeeCo 会将内容首先按照规则分片编码成 n 份，然后再将每片内容存放在 k 个节点当中。CDHT 的内容编码算法能保证只要在 n 份内容中获取任意 m 份，就可以将整个数据内容恢复。

假设每台机器的失效概率为 p，每台机器失效的时间相对独立，则传统 DHT 数据不可恢复既所有机器同时失效的概率为：

$$\boldsymbol{prob_1 = p^k} \qquad \textit{(1)}$$

在 CDHT 中，假定 n 份中的每一份数据备份的数量同为 k，且备份的机器各不相同（即总共有 n*k 台机器）。那么，每一份数据不能恢复的概率和(1)式相同，且每一份数据能恢复的事件相互独立。当只能找到 n 份数据中的 0 份、1 份……m-1 份时不能恢复数据。使用二项式定理，可

得不能恢复数据的概率为：

$$prob_2 = \sum_{i=0}^{m-1} \binom{n}{i} (prob_1)^{n-i} (1 - prob_1)^i \quad (2)$$

在实际情况下应有：

$$prob_1 \ll 1 \quad (3)$$

则：

$$prob_2 \approx \binom{n}{m-1} (prob_1)^{n-m+1} \quad (4)$$

举例，假定 p=0.1，k=10，n=6，m=5，计算得到：

$$prob_1 = 10^{-10} \quad (5)$$

$$prob_2 = 15 \times prob_1^2 = 1.5 \times 10^{-19} \quad (6)$$

(5) 和 (6) 相比较可以知道，CDHT 可靠性的提升了大概6.7×10^8倍，这一特质使得数据不可恢复的几率几乎为 0。

2.6.9 抗量子技术

区块链技术是架构在密码学之上的，例如比特币，以太坊的数字签名都是用了椭圆曲线数字签名算法(ECDSA)。随着科学技术的不断进步，特别是量子计算理论的飞速发展，对已知的各种加密和哈希算法都提出了挑战，目前的研究表明量子计算不但对非对称加密算法安全性的影响巨大，同样对对称加密算法也有一定的影响，相比较，对于哈希算法目前的影响相对有限。[6]

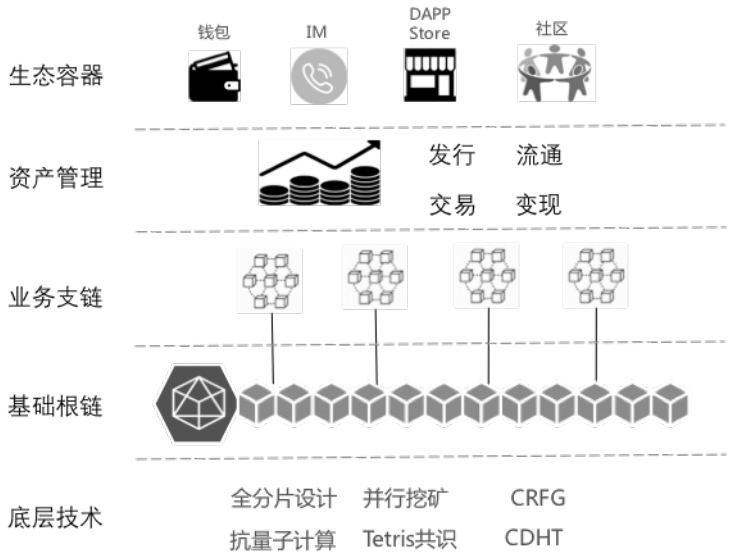
加密算法	类型	用途	量子计算的影

			响
AES-256	对称	加密	安全
SHA-256, SHA3	-	哈希	安全
RSA	非 对称	签名，密钥建立	不安全
ECDSA, ECDH（椭圆曲线加密）	非 对称	签名，密钥交换	不安全
DSA（有限域离散对数加密）	非 对称	签名，密钥交换	不安全

对于对称加密算法和哈希算法，我们一般可以通过增加位数（key sizes）就可以实现量子抵抗。但是对于非对称加密算法，我们必须对算法本身做出调整。YeeCo 系统在支持当前流行加密算法的基础上，也加入了抗量子技术模块。考虑到抗量子方案的公钥、签名长度远大于传统算法的公钥、签名长度，这将引起交易大小明显增加，导致系统吞吐量下降，造成网络拥堵，另外，签名算法的速度也是我们在系统实现时必须要考虑的问题。因此我们会根据量子技术发展的实际情况在实际部署中推荐使用相应的技术。

2.7 YeeCo 解决方案总结

以下就是 YeeCo 区块链解决方案的总体结构：



逻辑上，YeeCo 的区块链解决方案分为如下几层：

- YeeCo 的基础是一条具备高安全性的基础根链，采用了全分片架构设计，以及 PoW 共识机制，在确保去中心化和安全性的前提下，并同时实现了高性能（数万 TPS），平台上所有核心交易的数据都在这条根链上确认并进行保存
- 通过引入“并行挖矿”机制，YeeCo 解决了传统分片面临的 1%攻击问题，将算力攻击成本提升到等同于传统 PoW 共识的 51%算力，从而确保了基础根链的安全性
- 根据不同的应用场景，YeeCo 通过分层机制部署多条业务支链，用于承载不同的业务场景，支链通过内部定义接口和根链进行信息的交换。根据实际的业务需求，不同的支链可以采用不同的部署模式和有差异化的共识算法，以满足不同的应用场景对于系统性能、安全、去中心化的差异化要求
- 在 YeeCo 的基础根链和业务支链之上，YeeCo 将同时提供一个完善的数字资产交易平台，使各种数字资产可以在 YeeCo 链上进行进行全生命周期（资产的发布、托管、流通、交易、销毁）的流通和交易，从而解决价值互联网的价值流转问题

- YeeCo 也将支持各种第一方/第三方的工具（如去中心化的钱包、IM 通讯工具，社群建设和 DAPP 的应用商店等）以促进整体生态的建设，方便用户的使用
- 底层技术方面，YeeCo 采用了多种有特色的技术（如并行挖矿、CDFG 最终确定性、Tetris 共识算法、抗量子计算等），以保障 YeeCo 在技术上的整体领先

3 YeeCo 典型应用场景说明

3.1 资产证券化+全球化清算网络

ABS，即 Asset-backed Securities，资产证券化。通俗而言，就是指将缺乏流动性、但具有可预期收入的资产，通过在资本市场上发行证券的方式予以出售，以获取融资，以最大化提高资产的流动性。资产证券化是通过在资本市场和货币市场发行证券筹资的一种直接融资方式。由于银行有短存长贷的矛盾，资产管理公司有回收不良资产的压力，因此目前在资本市场，资产证券化得到了银行和资产管理公司的青睐。

区块链技术作为独立的底层数据存储和验证技术，具有去中介信任、防篡改、交易可追溯等特性，能够实现交易过程中，各节点共同维护一套交易账本数据，实时掌握并验证账本内容。各家机构间信息和资金通过分布式账本和共识机制保持实时同步，有效解决了机构间费时费力的对账清算问题。并且，区块链能够实现对基础资产全生命周期的管理能力，包括放款、还款、逾期以及交易等全流程的数据上链，以达到对现金流进行实时监控和精准预测的目的。

区块链技术在这一场景下，从业务流程多个环节切入，解决了业务中多方痛点：

对于中介机构而言，资产证券化产品尽调环节的尽调置信程度明显提升，尽调效率也得到提高，实时掌握资产违约风险。

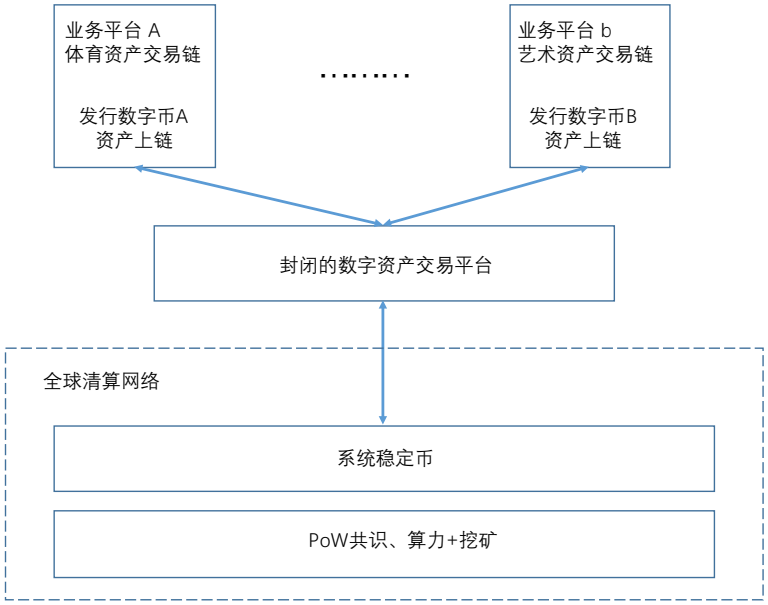
对于投资者而言，所投资产的透明程度显著增强，同时二级交易的估值和定价也变得有据可依。

对于监管机构而言，能够更大程度上满足穿透式审核和监管的要求。能够有效把控金融杠杆、提前防范系统性风险。

对于项目方而言，采用区块链技术增加了投资收益、降低了融资和沟通成本，也使得投前、投后的管理更有效。同时让资金流转速度更快，资金的分配效率更高。

目前业界有看法认为区块链的最佳实践场景之一就是资产证券化，这一技术可改变金融系统底层设计，实现所有市场参与人对资产所有权和交易信息的无差别记录，保证了底层资产数据的真实性。同时链上处理 ABS 交易信息，任何一次变动都可以同步更新到所有节点，节省了此前冗长的手续和资源的消耗。

下图是一个利用 YeeCo 作为基础设施建设一个数字资产发行+交易+全球清算网络的示意图。



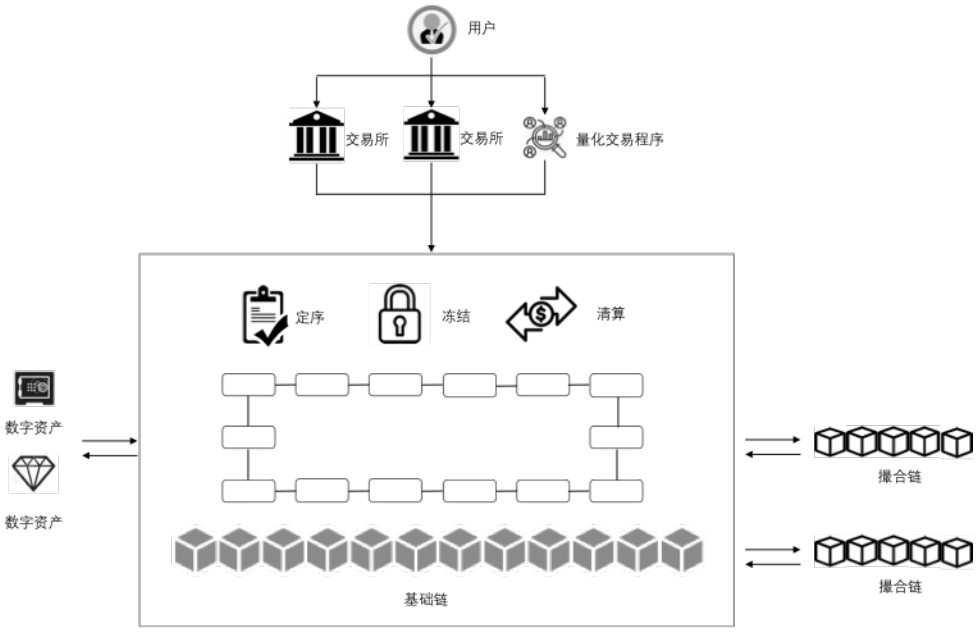
首先，利用 YeeCo 的业务支链对应不同的数字资产场景建设相应的业务链，例如针对体育内容可以建设一个单独的体育内容的链，针对艺术资产建设一个单独的艺术内容的链。由于两种业务场景的不同，因此业务链建设所选择的建设方案和模式是可以有差异的。

然后，不同的数字资产可以选择发行自己的独立的数字币，并选择在 YeeCo 提供的统一的封闭资产交易平台上进行资产流通和交易。

同时，YeeCo 为所有接入系统的数字资产发行一种数字币作为全球统一的稳定币，所有在 YeeCo 中流通的其他数字币都需要和该稳定币进行锚定，并通过和稳定币之间的兑换实现全球范围内的变现和清算能力。

3.1.1 数字资产交易平台架构

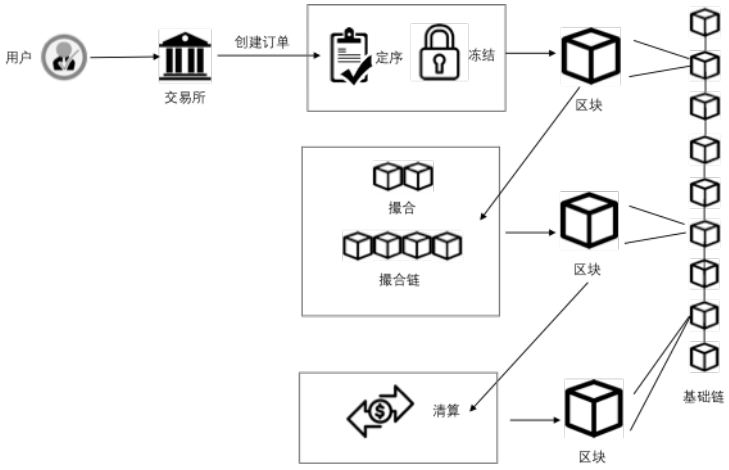
针对全球的数字资产交易+清算场景，YeeCo 将提供一个可灵活扩展的去中心化的数字资产交易智能合约平台，它的核心是一个采用了基础根链部署的去中心化交易系统，用户在保证数字资产安全的情况下，可以享受到近乎中心化交易所的交易体验。



根据本文前面章节的描述，YeeCo 全分片的架构设计，在采用 PoW 共识机制的前提下，仍然能达到数万 TPS 的系统吞吐量，因此完全可以满足去中心化交易所的性能需求。

3.1.2 数字订单类型实现过程

一个完整的订单创建流程是这样的：



1. 向基础根链发起 Create Order 的操作

2. 根链对订单进行定序，同时冻结相应的资产，将以上 transaction 打包进块

3. 业务撮合链读取主链的区块信息，进行撮合成交，将以上 transaction 打包进块

4. 基础根链读取业务撮合链的区块信息，按照撮合结果进行资产清算

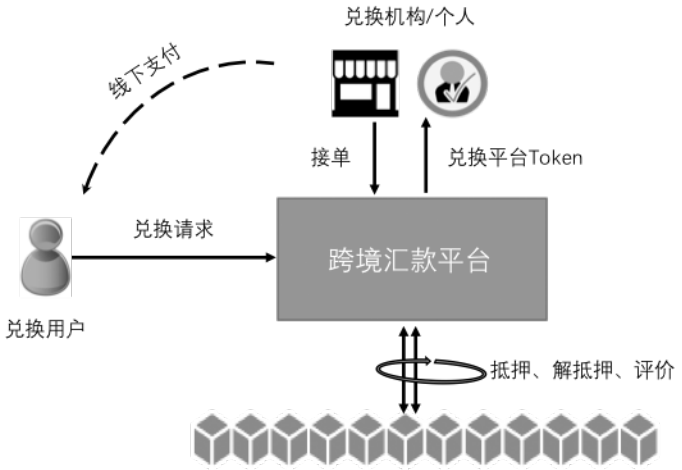
3.2 跨境汇款

在当前的实际生活中，存在着移民以及国外务工者这样的群体。对于这类群体而言，需要经常性的进行跨国汇款，但是实际上商业汇款的汇率很高，周期较长，同时家人去取款也比较复杂。

通过 YeeCo 可以构建一个跨境汇款、转账的基础公链，用户可以通过 YeeCo 在移民和移民的家人之间低成本、快速的转账，移民家人收到转账 Token 后，可以通过向 YeeCo 系统发起需求单的方式寻找换成当地货币的个人或者服务机构。需求发起后，可满足需求的个人或机构可以进行抢单。抢单成功后，即搀定汇率，同时双方都提交同等数量的系统 Token 作为担保，进而形成智能合约。当需求发起方收到本地货币后，双方都确认交易完成的情况下，抢单方将收回自己抵押的系统 Token，同时获得需求方的 Token；根据完成的时间以及需求方的评价，抢单方将获得一个不

可篡改的评价，这些评价会随着服务的次数及质量而得到不断的积累，最后在 YeeCo 的生态里形成各种换汇货币的服务提供方排名。为了促进交易均衡，有些单完成后系统会给予平台 Token 的奖励，有些单需要付出一定的平台 Token 才能抢。

业务示意如下：



3.3 5G + 区块链

3.3.1 智慧物联网

5G 技术为物联网带来了高速率、超低延迟、节能、低成本、高系统容量和大规模设备连接等特性，将大力推动物联网的爆发式增长，是智慧物联网『硬实力』的基础；区块链技术的高安全性、去中心化、防篡改及 Token 通证经济模型的特性，能够解决物联网中隐私保护、跨主体协作、可证溯源、身份鉴权等问题，让价值有序地在人与人、人与物、物与物之间自如流动，是智慧物联网『软实力』的基础。通过软硬实力相结合，智慧物联网将真正的普及到人类的日常生活及生产活动中。

YeeCo 和 5G 是天作之合。通过二者构建的智慧物联网，将拥有强大的软硬实力来满足高速海量互联场景：YeeCo 拥有高达 50000 甚至百万级 TPS 的吞吐量，可以从容应对智慧物联网大规模普及所带来的数据爆发式增长；在高性能的基础上，保持高度去中心化，同时通过 PoW 共识和 CRFG 最终确定性技术，大幅提升智慧物联网的安全性；灵活的跨链

方案和新一代的智能合约，将为智慧物联网提供丰富的应用开发基础。YeeCo 的技术特性在 5G 时代的智慧物联网场景下将被发挥的淋漓尽致。

4 YeeCo 经济模型及生态建设计划

4.1 YeeCo 的经济模型

我们将发行加密数字货币 YEE 作为 YeeCo 生态中的通行 Token，基于此 Token 的生态激励措施以及 YeeCo 基础设施的能力，我们预期将构建一个繁荣的生态系统。

本项目将发行加密数字货币 YEE，统一简称为:YEE，相比于 2018 年发布的上一版白皮书中约定的发行计划，分配方案变动如下:

YeeCo 主网上线前：

	原分配方案			现分配方案
	比例	分配方案	明细	
主网上线前	20%	预售	用于项目后续开发、人才招募、市场推广等。此部分资金的使用需要定期公示。	不变。
	10%	合作机构	用于回报现有合作机构，以及建立与相关企业的业务合作。Token 发行时被智能合约锁定，上交易所后第一个季度开始，每季度解锁此部分的 5%，	不变。

			分 20 个季度解锁完成。	
	25%	基金会	作为 Yee 基金会发展备用金，用于项目研究、开发及业务生态建设。此部分资金的使用需要基金会决议，并提前做公示。	Yee 基金会会使用基金会的份额对于 YeeCo 生态内的产品和服务进行投资，所获得权益归属 Yee 基金会所有。同时，Yee 基金会会聘请 YeeCo 生态中的核心成员担任 Yee 基金会的管理职务，共同参与 YeeCo 生态的治理。
	30%	生态激励	用户可以在 YeeCo 生态的平台上（如 YeeCall）或者 WhatsApp、Line、微信上，完成特定的行为获得奖励。该部分一共 30%，分八年解，永不增发，前四年每年释放 5%，后面四年每年释放 2.5%。	取消。 主网上线前此 30 亿 YEE 将直接销毁。
	15%	创始团队	为回报创始团队在区块链领域的探索和开发，以及今后在产品技术、运营发展、维护等方面的付出，发放 Token 做为回报。Token 发行时此部分将被智能合约锁定，1 个月后解锁，每月解锁此部分的 1/30，分 30 个月解锁完成。	不变。
主网	无			主网上线后，以 PoW 挖矿的方式，每年固定发行

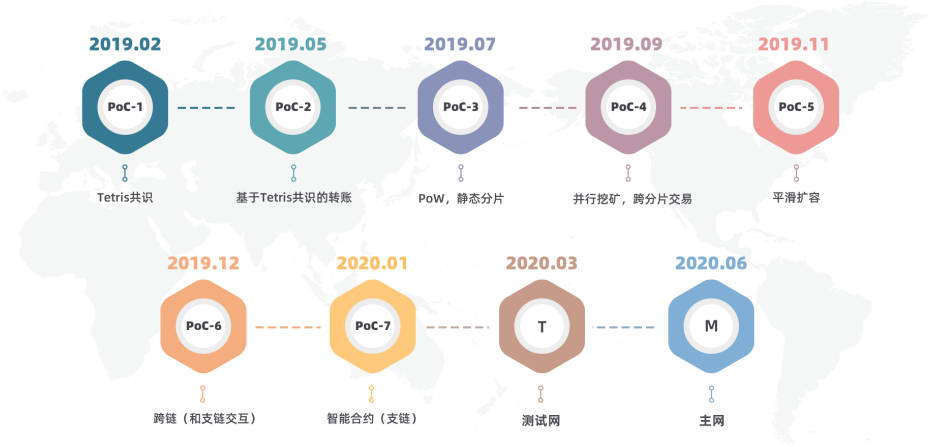
上线后		3 亿 YEE。

4.2 YeeCo 的生态建设计划

请参考 Yee 基金会后续专门提供的《YeeCo 生态建设计划白皮书》。

5 YeeCo 项目发展路线

YeeCo 项目总体发展计划更新如下，项目主网将于 2020 年中上线。



6 免责声明（Disclaimer）

本声明不涉及与证券招标以及承担 YeeCo 经营性和 YEE 的相关风险。

不涉及任何在司法管制内的受管制产品：

本文件是项目阐述的概念性文件【白皮书】，并非出售或者征集招标与 YeeCo 产品及其相关公司的股份、证券或其他受管制产品。根据本文件不能作为招股说明书或其他任何形式的标准化合约文件，也并不是构成任何司法管辖区内的证券或其他任何受管制产品的劝告或征集的投资建议。本文件不能成为任何销售、订阅或邀请其他人去购买和订阅任何证券，以及基于此基础上形式的联系、合约或承诺。本白皮书并没有经过任何国家或地区的司法监管机构审查。

不作为参与投资的建议：在本文件中所呈现的任何信息或者分析，都不构成任何参与 Token 投资决定的建议，并且不会做出任何具有倾向性的具体推荐。您必须听取一切有必要的专业建议，比如税务和会计梳理相关事务。

不能构成任何声明和保证：本文件用于说明我们所提出的 YeeCo 平台与 YEE Token，但是 Yee 基金会明确表示：1)对于本文件中描述的任何内容的准确性或完整性，或者以其他方式发布的与项目相关的内容，不给予任何声明和保证；2)在没有前提条件的情况下，不能对任何具有前瞻性、概念性陈述的成就或合理性内容给予任何声明和保证；3)本文件中的任何内容，不作为任何对未来的承诺或陈述的依据；4)不承担任何因白皮书的相关人员或其他方面造成的任何损失；5)在无法免除的法律责任范围内，仅限于所适用法律所允许的最大限度。

不是任何人都可以参与项目：YeeCo 的网络系统和平台并不是任何人都可以参与，参与者可能需要完成一系列的步骤，其中包括提供表明身份的信息和文件。

非授权公司与该项目无关：除了 Yee 基金会和 YeeCo 之外，使用其他任何公司或者机构的名称商标，并不说明任何一方与之有关联或认可，仅供说明相关内容之用。

与 Token YEE 相关的注意事项：“Yee Token”或“YEE”，是 Yee 区块链网络的虚拟密码学(Cryptographic)通用凭证。

YEE 不是虚拟货币：在本文件未完成期间，YEE 不能在交易所兑换物品、服务和交易，也不能在 YeeCo 网络以外使用。

YEE 不是投资品：没有任何人能够保证，也没有任何理由相信，你所持有的 YEE 将会一定升值，甚至有可能存在贬值的风险。

YEE 不是所有权证明或具有控制权：持有 YEE 并不是授予持有者所有权以及 YeeCo 网络系统的股权；也并不是授予其直接控制或者替 YeeCo 网络系统做任何决策的权利。

7 参考资料

[1] Vitalik Buterin 在 Sharding FAQ 提出的“不可能三角”模型，表明区块链系统只能同时拥有“去中心化、高效、安全”三种属性中的其中两种。
https://github.com/ethereum/wiki/wiki/Sharding-FAQs

[2] 一款名为 CryptoKitties 的基于以太坊的 DAPP 应用，自从上线以来，已经成为了以太坊区块链上最受欢迎的项目，一度占据了整个以太坊 20%的流量，并造成了以太坊网络的拥堵。
https://www.cryptokitties.co/

[3] 拜占庭问题(Byzantine failures)，是由莱斯利·兰伯特提出的点对点通信中的基本问题。含义是在存在消息丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的。因此对一致性的研究一般假设信道是可靠的，或不存在本问题。 https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

[4] Baird L. The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance, Swirlds Tech Report SWIRLDS-TR- 2016-01(2016)
https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

[5] 键值数据库是一种非关系数据库，它使用简单的键值方法来存储数据。键值数据库将数据存储为键值对集合，其中键作为唯一标识符。键和值都可以是从简单对象到复杂复合对象的任何内容。键值数据库是高度可分区的，并且允许以其他类型的数据库无法实现的规模进行水平扩展。
https://en.wikipedia.org/wiki/Key-value_database

[6] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, “The Impact of Quantum Computing on Present Cryptography”
https://arxiv.org/abs/1804.00200