概览

YEECO 不仅仅是区块链技术的进一步革新，而且是构建新一代去中心化互联网的基石。YEECO 主要由革命性的区块链平台 YEECO BlockChain、高效大吞吐量 P2P 网络 YeeNet 和编码分片存储网络 CDHT 这三个主要部分构成，新一代分布式互联网逻辑上可以表示为由无数个 YEECO 区块链平台构成的去中心化云计算平台，可以通过不断地扩充 YEECO 区块链平台和划分子网来动态扩容。YEECO 区块链平台主要由认证节点、应用节点和存储节点构成：认证节点负责对网络交易达成共识，应用节点运行下一代去中心化应用，存储节点用以存储所有交易数据。YEECO 首创的基于知识推理的 Tetris 共识算法可以将交易速度提升到 10K+TPS 以上，远远超过现有所有主流区块链的交易速度；另外，应用节点内置的智能合约服务单元、YEECO 虚拟机以及强大的应用服务引擎（DAPPEngine）和分布式数据库引擎（DSQL）能够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）；所有交易数据都是以区块链分布式账本的形式保存在编码分片存储网络 CDHT 中的存储节点中，安全可靠，不可篡改。同时，在社区共识的基础上建立 Meta 管理和可升级机制，确保公链的演进能力。

1 目录

2 前言

随着世界上第一台通用计算机“ENIAC”于 1946 年 2 月 14 日在美国宾夕法尼亚大学诞生，计算机技术已经经历了从主机时代、PC 时代到互联网时代的巨大变革，每个时代都飞速推动着人类文明的进步和发展。然而到了今天，互联网的发展已经进入一个死胡同，越来越多的资源（包括人力资源、数据、财务等）、应用和服务被垄断在 Google、 Facebook、Apple、Tencent 等少数几家大公司手中，用户个人信息对这些垄断企业来说，基本没有什么秘密而言，随着人工智能在大数据领域的飞速发展，通过分析这些数据，很容易根据使用者的性别、年龄、职业、性格等个人信息定制化出各种各样的应用和服务来一点点消耗用户的时间和生命，从广告、娱乐、购物、饮食等方方面面彻底绑架用户的生活，将用户碎片化。这些企业完全有能力使用用户的数据危害到用户自身甚至整个社会。这一切都似乎偏离了原来的轨道，与众所周知的互联网精神（自由、开放、平等、协作、分享）背道而驰。人们经常会这样思考 - 我们看到的世界可能并不真实，我们看到的世界其实是别人想要我们看到的世界，我们的生活轨迹都是被设计出来的，并且没有选择权。历史呼唤新的技术来摆脱这些垄断性的束缚，建立一个真正互信、共享、自治的价值互联网经济。2008 年，中本聪（Satoshi Nakamoto）[1] 发表了一篇名为《比特币：一种点对点式的电子现金系统》[2] ，描述了一种被他称为“比特币”的电子货币及其算法，并且在 2009 年发布了比特币系统，从此拉开了区块链技术革命浪潮的序幕。随着时间的推移，区块链技术以去中心化、数据不可篡改、匿名、自治等特质被越来越多的人接受并认可，各种区块链项目也如雨后春笋般加入进来，比较知名的项目有：以太坊、RIPLE、EOS 等。然而人们在探索的道路上也遇到了一个不可跨越的鸿沟，除了投机相关应用（ICO、博彩、交易），到目前仍然没有真正意义的区块链应用项目落地，加密猫项目[3] 的迅速成功和没落也让人们更清醒地认识到了一点。分析

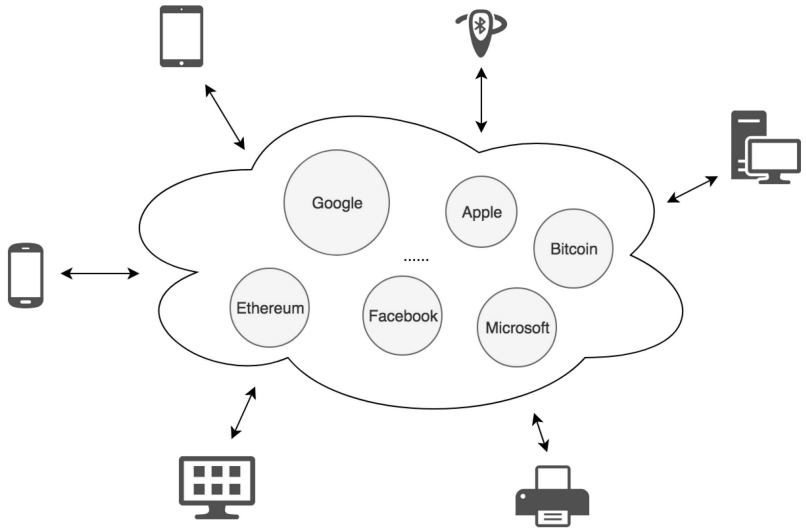
根本原因，除了已知的各种系统自身缺陷之外（比如：交易速度），一个最重要的原因是区块链技术还没有被行业巨头所拥抱，因为去中心化明显和这些企业自身的利益相矛盾。现在所有区块链系统几乎都是以互联网的一个补充形式存在，去中心化和中心化世界并存，而且互不干扰。然而我们相信历史的车轮不可阻挡，也决心通过 YEECO 项目做出自己的努力，用区块链技术彻底改造互联网，重塑互联网精神。

3 介绍

人们普遍认为区块链的演进方式可以划分三个阶段：

- 数字货币
- 数字资产与智能合约
- 各种行业分布式应用落地

从 2008 到 2018 年，区块链的发展也经历了大约 10 年的时间，出现了各种各样的区块链系统，从一个相对简单的电子货币系统（Bitcoin）到支持图灵完备的智能合约系统（Ethereum），从 PoW 共识到各种共识算法（PoS、 DPoS、 PoA、 DAG、PBFT）百花齐放，交易速度从几个 TPS 到几十 TPS 再到几百、几千，相对简单的去中心化应用（Decentralized Application）也随之诞生。但是各个区块链系统和其它中心化系统都是自成体系，孤立地存在于系统之中。



资源不共享，应用逻辑不透明，少数一些企业垄断着整个互联网，用户的权益得不到真正的保护，这些都严重影响着互联网的持续发展。和绝大多数人的想法不同，我们建议充分利用区块链的特点来彻底改造互联网，发展路径如下：

我们希望实现的去中心化互联网具备如下特点：

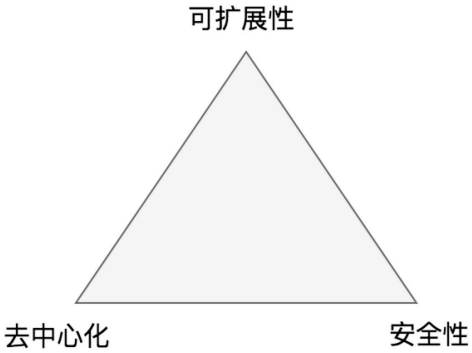
- 数字货币
- 数字资产与智能合约，简单的去中心化应用
- 基于区块链技术的去中心化互联网，分布式应用落地

我们希望实现的去中心化互联网具备如下特点：

- 分布式，去中心化
- 公共数据共享，不可篡改
- 商业逻辑透明
- 保护用户隐私，数据安全
- 资源货币化，数据流转的同时也包括价值的流转
- 共识自治
- 系统安全可靠

- 节能环保
- 维护简单，模块化节点动态加入和退出
- 私有/联盟/公共服务并存

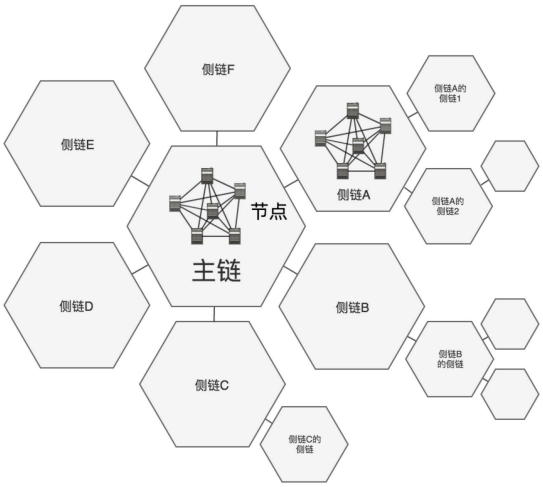
实现上述要求的挑战是巨大的，众所周知，区块链系统存在一个不可能三角[4] ，即可扩展性、去中心化和安全性只能同时满足两点。



区块链系统的不可能三角

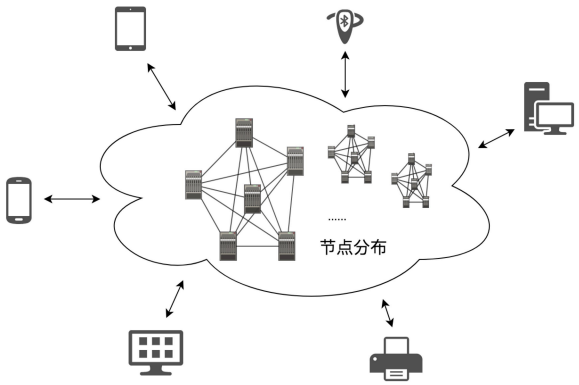
传统中心化解决方案都是以安全性和可扩展性作为设计目标的，因为不需要考虑去中心化，数据、CPU、带宽、设备高度集中，几十万甚至上百万服务器并发服务。比如淘宝，每秒能完成几万笔的交易。但是区块链系统，去中心化又是一个最基本的要素。实践证明，在复杂的分布式系统中，无论用何种共识算法，去中心化程度越高，达成共识的速度就越慢，这是不可跨越的鸿沟。目前最快的区块链共识算法实际速度也就几千 TPS，远远不能满足实际应用的要求，而且其去中心化程度非常低，比如 EOS，仅仅使用了 21 个超级节点。另外一个问题是，互联网上的应用不计其数，如果将所有的去中心化应用都部署在一条主链上是根本不现实的，网络拥堵问题将根本无法解决，以太坊去中心化应用 DAPPs 的糟糕体验也证明了这一点。因为考虑到主链安全性不可妥协，导致我们只能从去中心化和可扩展这两个方面来想办法。为了确保较高的去中心化，我们建议采取多链架构来满足可扩展的要求，将扩展性用区块链第二层解决方案（Layer2 solution）来解决。主链只维护关键核心数据状态（交易、账户等），将所有的应用和服务都部署在不同的侧链中去，每个侧链可以跑一个或多个应

用，侧链可以自己通过平衡去中心化、安全性和可扩展性这三个要素来满足特定需要。

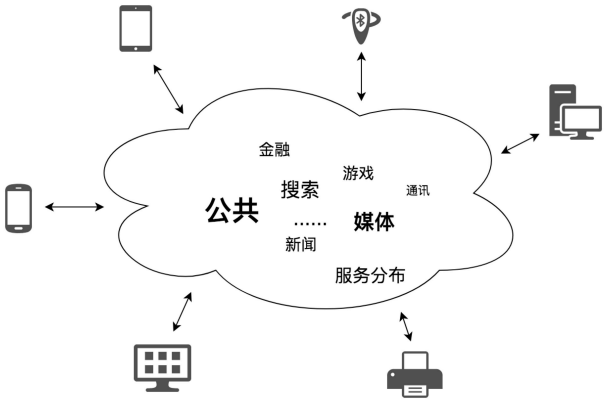


YEECO 多链架构组成的去中心化互联网

因此，我们设计的互联网的基础构成，其实就是多个 YEECO 区块链平台（由应用节点、验证节点和存储节点组成）在云中的分布，每个平台都使用同样的区块链协议，通过侧链技术（例如 Plasma、状态通道）进行交互。平台可以动态加入或退出，并不会对整个网络造成影响。



从互联网的功能来看，其实就是各种 YEECO 去中心化服务在云中的分布。Google、Apple、Facebook 在新的生态里只是服务的代名词，不再是一个个垄断性的中心化组织和实体，所有这些服务的公共数据、内容、业务逻辑都是去中心化、开放、共享、透明的。同时，现有的属于各个公司的私人服务器在统一的协议栈之下，变成侧链上一个个节点的集合，可以简单任意地扩容，单个节点的失效对系统没有任何影响。



为了支撑这个宏大的设计目标，我们不仅对区块链支撑网络和存储等进行了优化和改进，使用了分片和子网技术，建立了编码分片存储网络 CDHT，还对共识算法进行了高度创新，我们独创的 Tetris 共识算法，无论从效率、速度还是实用性和安全性方面，将全面超越已知的 PoW、PoS、PBFT、DPoS 等共识算法。

YEECO 建议的系统逻辑架构如下图：

主要分成以下几个组件：

1. YEECO BlockChain 平台

- Tetris 共识算法
- BlockChain
- 智能合约和应用代码
- YEECO 虚拟机（YVM）
- 应用引擎
- 分布式数据库引擎
- 社区自治模块

- 激励模块
- 抗量子技术
- 节点动态管理模块（应用节点、验证节点、验证节点匿名管理）

2. P2P 网络 YeeNet

- 子网管理
- 代理节点
- 编码分片存储网络服务（CDHT）
- 分布式哈希表
- 存储节点矿机

3. YEECO 域名系统（YDNS）

- 域名登记
- 域名解析
- YDNS 节点

4 YEECO 解决方案

4.1 YEECO BlockChain 平台

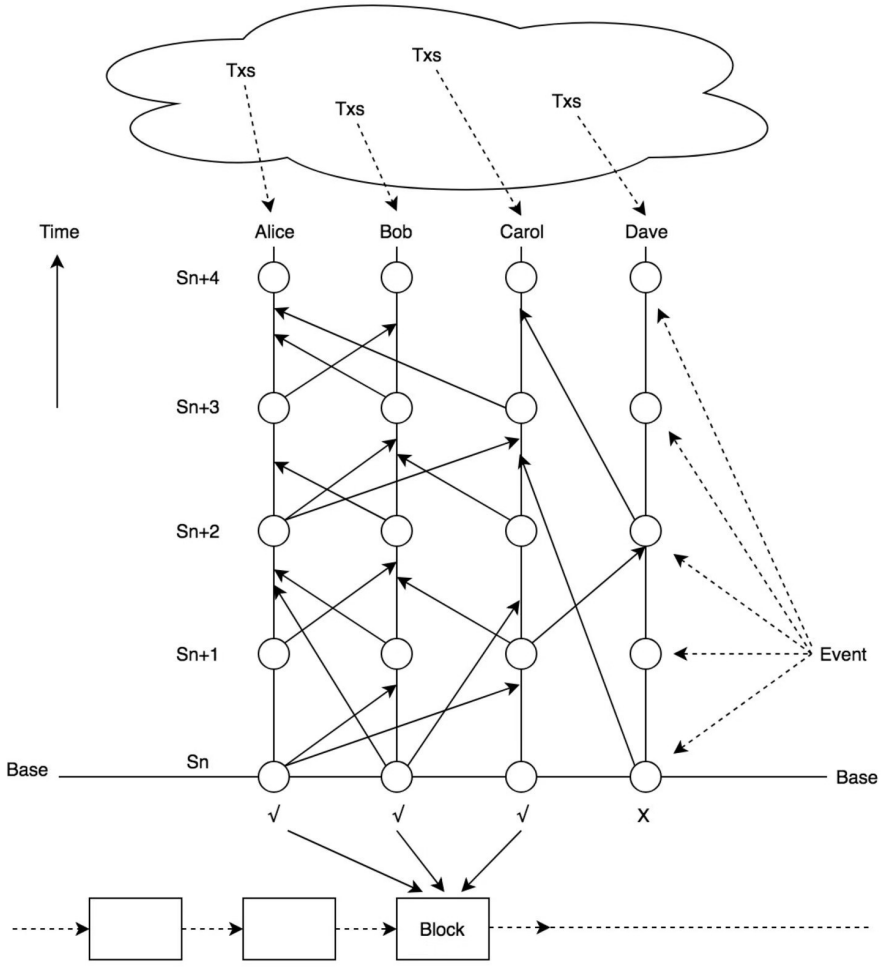
4.1.1 Tetris 共识算法

YEECO 独创的高吞吐量 Tetris 共识算法，将交易速度大幅提升到 10K+TPS，本质上 Tetris 共识算法仍然是异步拜占庭容错（BFT）[5] ，所以仍然具备中止性（Termination）、一致性（Agreement）和有效性（Validity）的优点。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（Full Information Protocol）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，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。

很多共识算法，包括一些新的技术比如 VRF 等，最终为了确保安全性都会增加一个 BFT 策略，比如：TON 的 PoS + BFT、EOS 的 DPoS + BFT、Algorand 的 VRF + BFT 等等。这些通过使用 BFT 策略打补丁来满足非许可网络的方式会造成各种潜在的问题。另外，对于 PBFT、Hashgraph 等共识机制，虽然能够获得高性能，但是由于系统模型的局限性，最终只能应用于许可网络。

YEECO 使用独特的方法来实现在非许可网络环境下的拜占庭容错，YEECO 通过可插拔的上层协议选出一些节点作为验证节点，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）。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了解的所有信息作为事件发送给其它节点。每个节点都会将了

解的信息形成一张有向图。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，当满足一定条件的时候，基线事件就可以被确认，所有被标记为可确认事件所包含的交易就是候选交易，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消失，之上的事件会落下来成为新的基线事件。因为整个过程非常像传统的俄罗斯方块（Tetris）游戏，这也是为什么我们的共识叫做 Tetris 的原因。



每次基线事件等待确认到被确认的过程我们叫做阶段（Stage）。正因为阶段（Stage）的存在，我们的验证节点是动态可替换的，验证节点可以自由加入和退出，对共识没有影响。

1. 性能

我们在测试环境下已经实现了 10K+的 TPS，Tetris 具备以下特质：

- 因为下层 P2P 覆盖子网（Overlay sub-network）的设计，当节点越多的时候，越多的子网会被划分，从而导致更多 TPS
- 每个时刻的交易数量越多，事件产生的就越多，达成共识越快

2. 扩展性

基于 Tetris 的区块链具备如下特点：

- 支持无限节点
- 支持无限账户
- 10k+TPS
- 普通节点只需满足最小存储需求

3. 最终确定性

Tetris 系统中，一旦共识达成，就是确定性共识，系统状态将被锁定，不可更改。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。这个特性的优点是很明显的。首先，新加入的节点不需要同步整个区块历史，只需要同步最近的区块状态，节省了大量的存储空间。其次，最终确定性可以大大简化跨链和分片策略。

4. 公平性

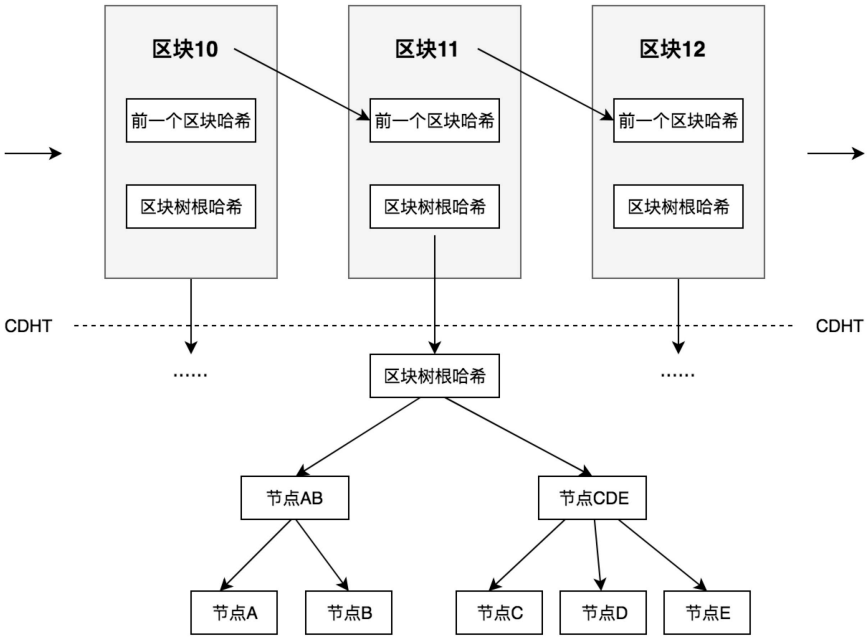
同时，Tetris 还实现公平性[6] ，在一些应用中这一特质是非常重要的，比如去中心化交易所。

详细内容请参看《Tetris 共识机制白皮书》。

4.1.2 区块链 （BlockChain）

YEECO 所有的交易数据都是以区块链的方式存储在系统中的，具备安全可靠，不可篡改，可追溯等特性。

在每一个区块头中，都包含了一个交易树根哈希的指针，交易树包括区块中发生的所有交易。



每个区块里指向的交易树都是一个梅克尔-帕特里夏树（Merkle Patricia Tree）[7] ，为了满足实际需要，YEECO 在实现上会做一些改进。

YEECO 中的梅克尔树由空节点、分支节点、扩展节点、叶子节点组成。这些节点数据都会以键值对（key-value）[8] 的形式被存储在编码分片存储网络 CDHT 中。

4.1.3 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 也提供了智能合约模版库可供开发人员参考。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。YEECO 服务单元是以包的形式发布的，类似于 java 的 jar 包，可以包含源码、图片、文本等等。源代码会发布到应用引擎中形成可执行文件，同时源代码文件、音视频、图片和文本等静态信息会被自动保存到编码分片存储网络之中去，将来可以通过唯一的 hash 指针来访问资源。因为合约的发布和执行都需要消耗区块链系统资源（带宽、CPU、内存），YEECO 也会锁定 Token 来实现这一过程。

4.1.4 YEECO 虚拟机（YVM）

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。

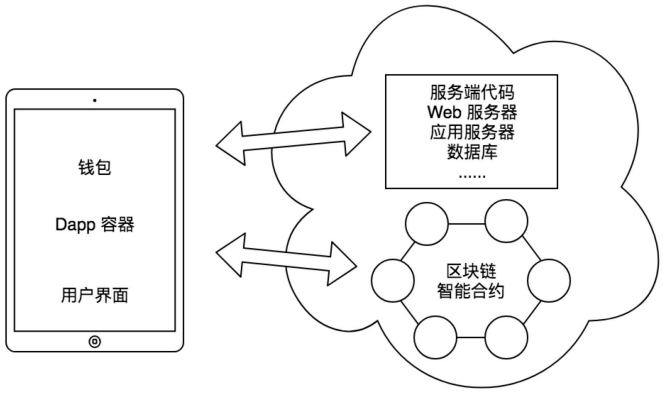
YEECO 虚拟机是一个智能合约的运行环境，并且具备可并发、快速高效、确定性、易于扩展、节省资源、安全等特点。

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。

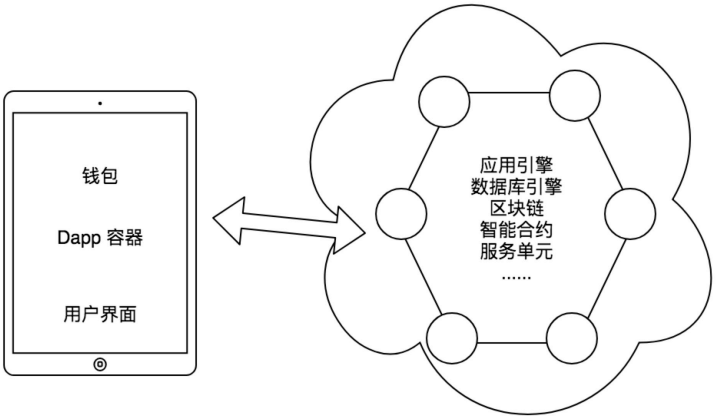
4.1.5 YEECO 应用引擎

目前主流 DAPPs 实现跟传统 APP 一样仍然需要自己在链外部署各种 web 服务器、应用服务器和中间件，只有需要链上数据的时候才和链打交道，区块链的角色仅仅是一个分布式数据存储系统。从应用架构上说，以以太坊为例，因为智能合约的性能和设计上的局限性，整个 DAPP 的

核心业务逻辑大部分还是在链外运行的，智能合约更关注的是核心交易数据的流转和存储，比如 Ether、Erc20 Token 和 Erc721 Token 等等。因此可以这样认为，现有的去中心化应用和中心化应用主要区别只是数据是否存储在区块链上或者是中心化服务器上，并不能称之为真正意义的去中心化应用。而且如果和中心化解决方案来比较，维护成本仍然很高，性能和效率确反而是问题。另外最重要的是，如果链外的这些应用逻辑不受智能合约的控制，服务仍然不对用户透明，没有解决真正互信的问题。



YEECO 应用引擎就是为了解决这个问题而诞生的，YEECO 应用引擎是由应用节点负责维护和提供服务的，YEECO 应用引擎采取可插拔的架构，可以通过统一协议来更新和升级。应用引擎通过与 P2P 网络、CDHT、智能合约和 JSON-RPC 交互，提供一整套类似于传统 web 服务器和应用服务器的功能，所有核心业务逻辑都可以无缝地运行在应用容器之内，实现真正的去中心化应用程序。



4.1.6 YEECO 分布式数据库引擎

传统区块链目前的本质实际上是分布式账本，一种分布式数据库，但是现有的链式结构的效率低下，实现不了现代数据库的高并发性能。实际使用的时候，需要开发人员专门对区块链分布式账本处理成结构化数据库，就像 etherscan [9] 一样。YEECO 专有的分布式数据库引擎就解决了这个问题，架构在 CDHT 之上，YEECO 分布式数据库引擎可以提供跟传统数据库一样的功能和性能。大大提高了应用开发的效率。也保持了对传统应用开发的兼容性。和传统数据库不同的是，除了缓存数据之外，最终所有的数据改变都是永久的保存在编码分片存储网络之中的。即便 YEECO 分布式数据库数据损坏失效，也可以通过链上数据很方便的重建，不需要像中心化数据库那样，需要各种各样的备份策略。

4.1.7 社区治理模块

由于数据是真正去中心化、分布式地存储在网络上的，如果没有任何监管和限制，违反伦理、低俗、犯罪等内容可能造成巨大的社会隐患，系统设计上的漏洞或者软件缺陷一旦被发现，遭到恶意使用和攻击可能导致硬分叉（例如，因为没有自我修复功能，以太坊不得不硬分叉成 ETH 和 ETC 来解决 The DAO 漏洞问题 [10] ），这些都是我们不希望看到的。因此一个成熟的系统必须具备一个治理模块，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 管理委员会从一年内担任过验证节点的所有者中选出，一共 n 名委员，每个委员必须持有一定量的 Token。所有验证节点的所有者投票选出 n 个节点作为管理委员会委员，票数按照所有者持币数（币天）进行换算来计数。

任何一个 YEECO 管理委员会的委员都可以提出提案，YEECO 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），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。

除此之外，对于违反伦理、低俗、犯罪等内容可以通过同样的策略，将这些内容永久从系统中移除。

具体细则请参看未来发布的《YEECO 社区治理白皮书》。

4.1.8 激励机制

YEECO 的激励机制主要包括以下几点：

1 没有交易费（Gas）

与以太坊不同，YEECO 的所有交易是不向用户收取交易费（Gas）的，以太坊的 Gas 机制存在设计上的缺陷，因为矿工需要竞争记账权，当竞争成功后，为了利益最大化，它一般会选取支付 Gas 最多的交易优先打包，这可以能会造成以下两个问题：其一是恶意用户在同一时刻可以连续提交高 Gas 的交易将以太坊网络整个阻塞住。其次，在一个购买中，A 用户先付了款，过了一段时间 B 用户才付了款，但是由于 Gas 费用比 A 用户设的高，很可能 B 用户的交易比 A 用户的先确认，这就涉及到一个公平性的问题。另外，每次确认 Gas 严重影响了应用执行的效率和体验。鉴于这些原因，YEECO 在设计上取消了交易费。

2 资源使用费

虽然取消了交易费，由于 YEECO 系统的资源（带宽、CPU、存储）属于有限资源，用户在使用 YEECO 节点提供的服务，根据资源的使用量（例如智能合约的发布和运行需要消耗带宽和 CPU、保存智能合约需要消耗系统存储等），开发者需要锁定一定的 Token，同理，用户使用 YDNS 域名服务、域名登记，也需要锁定一定的 Token。锁定的 Token 在资源不使用的时候，可以由系统解锁，从而回到用户手中。对于使用带宽和 CPU 而锁定的 Token，在不使用之后一段时间内会由系统自动返还给用户。因为节点的加入和退出是动态不可控的，因此锁定 Token 的数量也是一个

动态算法，会根据整个系统容量动态给出。

3 挖矿

YEECO 系统的挖矿激励分为节点的记账激励和存储激励。当节点提供记账服务的时候，系统会根据协议对每个节点给一定的 Token 作为激励。YEECO 主网正式上线之后，会将 Yee 项目里 30%即 30 亿的 YEE Token 作为对节点和开发者及用户的激励费用，前四年每年分发 5 亿，之后四年每年 2.5 亿。8 年之后，在系统所有 Token 都激励完成后，由 YEECO 管理委员会来决定是否增发 Token 作为激励。

当存储节点提供存储服务的时候，系统会根据文件大小和存储时间给出动态定价，用户需要锁定相应的 Token 在系统中，当文件被销毁或者被使用时，会根据存储的时间扣除费用后，将剩余的 Token 解锁给用户。存储节点在这个过程中，除了会收到用户支付的存储费用，还会得到系统的挖矿激励。

4 惩罚

对于节点可能的恶意行为，系统会将节点预先锁定的 Token 扣除部分或者全部作为惩罚，同时将节点从系统中排除出去。

以上只是激励机制的概览，具体内容请参看《YEECO 激励机制白皮书》。

4.1.9 节点动态管理模块

YEECO 节点类型主要包括验证节点、应用节点、存储节点和 YDNS 节点这四种类型，YEECO 节点是系统中提供服务的服务器的统称。YEECO 网络中的每一个节点均拥有一个专属 ID，该 ID 的具体形式与 SHA256 散列值一样，为一个长达 256bit 的整数。YEECO 节点类型只是逻辑上的区分，有的节点可能同时具备四种类型。当节点加入和退出网络的时候，会在系统中登记/取消注册，系统资源的总容量也会因此改变。

成为 YEECO 节点的基本要求主要有以下几点：

- 需要锁定一定数量的 Token
- 为了防止恶意攻击，需要经过一个 PoW 的过程通过节点资格认证
- 对节点有配置要求（内存、带宽、存储、CPU）
- 必须保证长时间在线，低于系统预设阀值会被取消节点资格

由于分布式系统的复杂性，验证节点越多，达成共识需要的时间就会越长，交易速度变慢。当节点过少，共识加快，交易速度提升，可能安全性又是一个问题。因此通过权衡，YEECO 缺省会选择 100 个节点作为备选节点，当有节点退出，系统会选择候补节点自动补位。

4.1.10 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。[11]

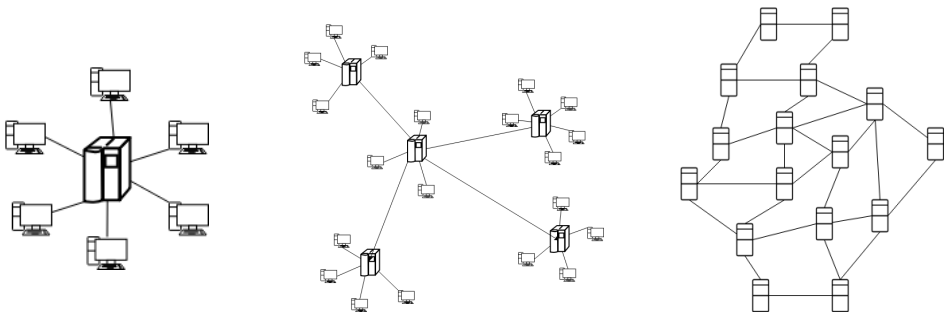
加密算法	类型	用途	量子计算的影响
AES-256	对称	加密	安全
SHA-256、SHA3	-	哈希	安全
RSA	非对称	签名、密钥建立	不安全
ECDSA、ECDH （椭圆曲线加密）	非对称	签名、密钥交换	不安全
DSA （有限域离散对数加密）	非对称	签名、密钥交换	不安全

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 size）

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（对于算法的研究超过了本文的范畴。详细内容请参看《YEECO 抗量子技术》）。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推荐使用。

4.2 P2P 网络 YeeNet

P2P 网络作为 YEECO 的底层网络平台，是一个真正的去中心化的网络形式。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。



Centralized 中心化　　Distributed 分布式　　Decentralized 去中心化

4.2.1 子网管理

每个验证节点主要会收到两类数据，一种是交易数据，一种是共识 Event 数据。因为分布式系统的复杂度，为了帮助我们估算网络流量，我们可以用一个简化的模型，给定一些前提假设来帮助进行估算，如下：

- 一共有 n 个验证节点

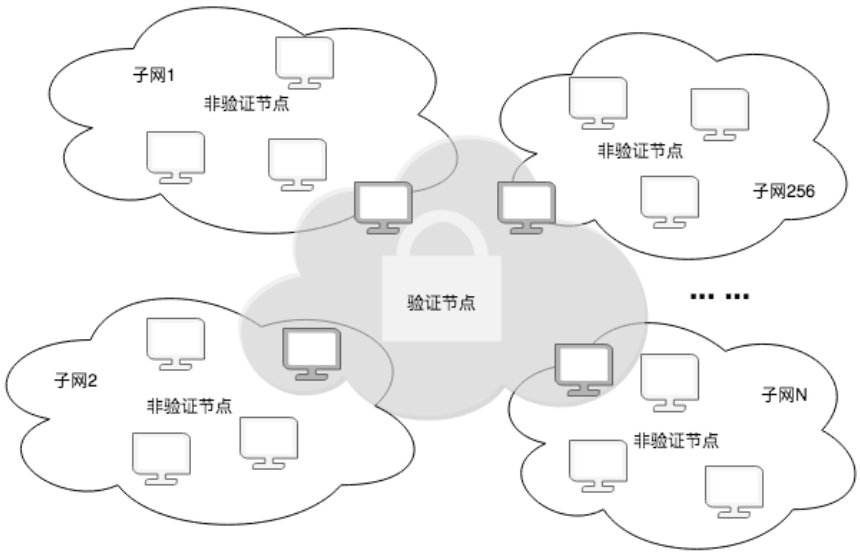
- 交易速度大约 s TPS
- 每个交易大小大概 c 字节
- 每个交易的 Hash 是 32 字节 （256 位）

如果没有划分子网，每个节点的每秒的流量 t 计算如下：

$$t = n \times s \times 32 + c \times s$$

当 n = 100， s = 10000 TPS， c = 200 字节的时候，t = 34M 字节/秒。

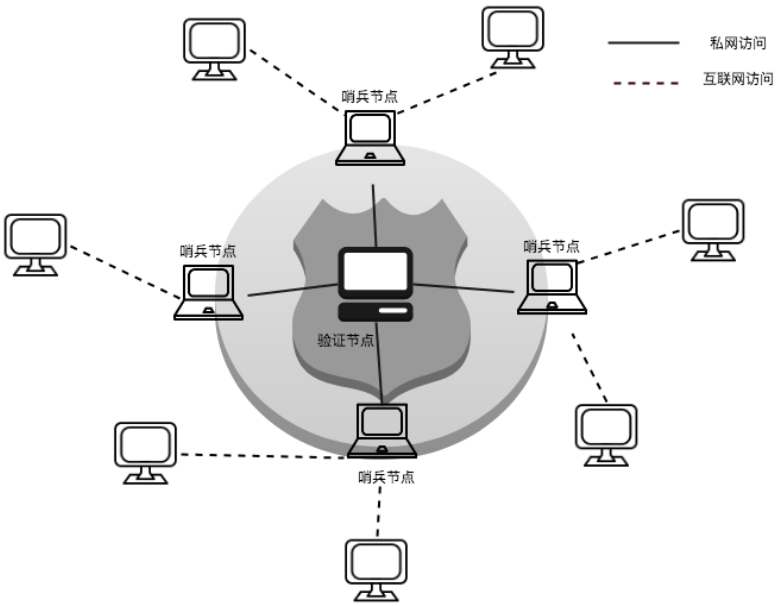
这个流量对于高端配置的计算机来说，在 1G 网络带宽下是可以满足的，但是考虑到分布式系统上存在各种配置的计算机，我们从设计上要确保低性能的计算机仍然正常工作，因此我们要求每个非验证节点的吞吐量不超过 200K 字节。因此 YEECO 设计了子网管理模块，将整个网络虚拟的动态划分成 N 个子网，消息只在子网内广播。同时，所有验证节点确保在一个虚拟子网之内，快速有效地达成共识。子网划分是动态和实时的，可以根据网络节点的增减快速作出相应。



对于上面的假设，我们只需要将整个网络划分成 34M/0.2M = 170 个子网就可以实现。为符合子网掩码实现要求，我们最终划分成大约 256 个子网，这样每个子网普通节点的流量就可以控制在 130K 左右。

4.2.2 哨兵节点（Sentry Node）

因为验证节点的重要性，为了防止各种恶意攻击（DDoS，女巫攻击等），我们要求节点尽可能的不暴露自己在网络中 IP 地址，一个可行方案就是可以通过哨兵节点的方式隐藏验证节点，每次会有不同的哨兵节点负责处理输入和输出。哨兵节点并不负责实际处理逻辑，只是收集信息和输出信息，最终的处理逻辑仍然由验证节点完成。这样大大降低了验证节点被攻击的可能。



4.2.3 编码分片存储网络服务（CDHT）

编码分片存储网络服务（CDHT）是 YEECO 自主研发的分布式文件管理系统。相对于传统的 DHT 网络，CDHT 可靠性至少提升大概10^9倍。

YEECO 所有的数据（包括文件、交易数据等等），最终都是以键值对的形式被保存在去中心化的编码分片存储网络 CDHT 中。CDHT 就像是一个云端存储系统，架构在 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。

4.2.4 YEECO 分布式哈希表

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：

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

在实际情况下应有：

$$prob_1 \ll 1 \tag{3}$$

则：

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

举例，假定 p=0.1，k=10，n=6，m=5，计算得到：

$$prob_1 = 10^{-10} \tag{5}$$

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

(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。

具体内容请参看《YEECO 编码分片存储网络 CDHT 白皮书》。

4.2.5 CDHT 矿机

存储节点对系统的性能要求相对比较简单，主要涉及到带宽和存储容量两个方面。同时，由于带宽和存储容量在 YEECO 生态里都是货币化的资源，当有应用使用到这些资源的时候，会根据使用量锁定或消耗用户的 Token，系统也会给予节点一定的挖矿奖励。同时，矿机可以根据需要随时加入网络中提供服务。未来 YEECO 将推出相应的存储矿机产品。

4.3 YEECO 域名系统（YDNS）

传统的互联网中，域名系统 DNS（Domain Name System）是互联网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住那些只能被机器识别的 IP 地址。IP 地址只是一串数字。例如，人们很容易记住 www.yeefoundation.com，相反对于 13.35.125.14 确没有任何概念。同理，因为在 YEECO 系统中，所有资源都是一个 Hash 字串，没有任何实际意义，我们也需要一个类似的系统来帮助人们来访问资源。

4.3.1 域名登记（Registrars）

用户可以跟注册互联网域名一样，申请注册 YEECO 域名，这样可以通过域名系统提供服务，应用等。域名登记是以智能合约的方式提供服务的，除了支付一点点 Token 作为资源使用费之外，用户还需要锁定一定的 Token 作为登记费，只要没有人登记过该域名，你就可以进入该域名候选人列表。域名登记是一个竞价的过程，采用维克里拍卖（Vickrey auction）[12] ，整个竞拍流程分为三个阶段：

1. 从域名开标到竞价截止共 72 小时，此阶段接受任何竞标，所有人竞标价格保密
2. 之后进入揭标环节：揭标开始至揭标结束共 48 小时，在第 1 阶段所有参与竞价者必须揭标，否则 99.5%竞价金将被销毁
3. 出价最高者以第二高价获得域名，退回多余款项并结标。此后可在两年的域名持有期内设置域名解析或转让给他人

4.3.2 域名解析（Resolvers）

在 YDNS，域名对应的是一串 Hash 字串，当修改网页内容之后，这个 Hash 字串会改变，我们只需要修改这个映射关系就可以，用户仍然能够通过同一域名访问到改变后的资源，当然实际应用可能比较复杂。

4.3.3 YDNS 节点

为了确保高性能，YDNS 节点会将 YDNS 实际的去中心化存储数据（注册表 registry）转换成结构化数据库，在网络中会有一些这样的服务器专门提供 YDNS 服务。这些节点提供服务的同时，也会从系统收取一定的 Token 作为奖励。

5 结论（Conclusion）

YEECO 是一个高吞吐量、安全和自治的基于区块链的去中心化互联网基础设施，之上可以架构新一代去中心化互联网。去中心化互联网的高速发展可以最终打破传统垄断性企业对用户的束缚，重塑互联网精神。所有应用和服务在 YEECO 都是去中心化应用，业务逻辑透明，开发和部署变的简单，高效。系统可以通过动态的加入节点扩容，社区治理可以确保系统能够不断更新来满足发展的需要，激励机制可以确保提供服务的节点积极地维护系统的安全和稳定。

6 免责声明（Disclaimer）

本声明不涉及与证券招标以及承担 YeeCall 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 Yee 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 Yee 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：Yee 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 YeeCall 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 Yee 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 YeeCall 和 Yee 网络系统的股权；也并不是授予其直接控制或者替 YeeCall 和 Yee 网络系统做任何决策的权利。

7 参考资料（References）

[1]: 中本聪（英语：Satoshi Nakamoto），自称日裔美国人，日本媒体常译为中本哲史，此人是比特币协议及其相关软件 Bitcoin-Qt 的创造者，但真实身份未知。

https://en.wikipedia.org/wiki/Satoshi_Nakamoto

[2]: 中本聪于 2008 年发表了一篇名为《比特币：一种点对点式的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）的论文，描述了一种被他称为“比特币”的电子货币及其算法。

https://bitcoin.org/bitcoin.pdf

[3]: 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/

[4]: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

[5]: 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

[6]: 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

[7]: 梅克尔帕特里夏树（Merkle Patricia Tree），简称 MPT，一种数据结构，它会存储每个帐户的状态。这个树的建立是通过从每个节点开始，然后将节点分成多达 16 个组，然后散列每个组，然后对散列结果继续散列，直到整个树有一个最后的“根散列”

https://github.com/ethereum/wiki/wiki/Patricia-Tree

[8]: 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

[9]: 以太坊区块浏览网站

https://etherscan.io/

[10]: The DAO 事件是区块链历史上的著名事件，由于智能合约的漏洞造成资金被黑客转移，最终导致以太坊硬分叉。

https://en.wikipedia.org/wiki/The_DAO_(organization)

[11]: Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, “The Impact of Quantum Computing on Present Cryptography”

https://arxiv.org/abs/1804.00200

[12]: 维克里拍卖，又称集邮者拍卖、第二密封拍卖，是指所有买家

通过密封投标的方式竞价，出价最高的投标者获得被拍卖的商品，并支付第二高的出价

https://en.wikipedia.org/wiki/Vickrey_auction