以太零白皮书

EtherZero White Paper

2018. 01 版本 2.01

以太零基金会.新加坡

摘要

本文档描述了一种无交易手续费，高拓展，即时交易的通用智能合约开发平台-以太零。基于本平台，开发者能构建落地性更强的通用去中心化应用 DAPP，这些应用可以跳出当前狭隘的金融与商业应用范畴，帮助区块链和去中心化服务触达更广泛的人群，改变更多的行业。

以太零在以太坊的基础上去除了其网络核心的 gas 手续费系统，增加了交易限制策略协议层，将发起交易的门槛，频率，深度等与账户余额关联，以对抗 DDOS 类攻击。

特别的，以太零还借鉴达世币(DASH)以主节点（Master Node）交易验证网络和区块链账本层为架构的双层网络结构及其内置的社区自治系统，为用户提供实时的操作反馈和超高的交易并发，不再需要交易双方等待漫长的交易确认时间。

目录

前言

以太坊自 2015 年 5 月发布初始版本以来备受关注，但随着各个后比特币时代新型电子货币系统，尤其是 DPOS 共识机制及其变型方案的发明与应用，以太坊自身冗长的开发测试周期，巨大的历史技术包袱都导致其与新一代的平台在交易处理性能，用户使用体验上越来越多的失去竞争力。

竞争力的缺失具体表现在：全节点参与交易处理导致的低拓展性，低交易处理能力，冗长的交易结果反馈；手续费作为防止 DDOS 攻击和奖励机制而存在的同时导致的对通用应用开发的支撑缺失。

以太零去芜存菁，撷取以太坊智能合约方面成熟经验，去除其扩展性不足的以 gas 为介质的手续费系统，制定全面考量的基于账户余额的交易限定和安全策略对抗 DDOS 类攻击，最终形成以主节点和 pow 共识层为主要架构的双层网络，实现了免手续费，高并发，实时交易，自主进化等几大特性。

第 I 章. 背景

第 1.1 节 **市场状态**

即便当前加密货币总市值已超过 6 千亿美元(2017 年底)，且仍在上升，但不可否认的是，投资者中大部分人对加密货币的本身并不太了解，对于区块链能够如何改变人类的去信任化的交易也懵懵懂懂，更妄论站在外围一无所知的普通人。也就是说区块链和加密货币领域急需一类杀手级应用能帮助更多普通人以更低的门槛了解加密货币和区块链技术即将对其生活产生的巨大影响。这种杀手级的应用并非独立生成，而应该只是一个应用平台支持的个例。

第 1.2 节 **通用应用平台的需求**

这种杀手级的应用需要构建在这样一个平台上：

基础操作零交易手续费：为了能够支持更广泛意义上的去中心应用的开发和业务运营，各类基础操作，如注册，登陆，收藏，浏览，搜索，分享及各类逻辑操作不应该收取费用

超高的并发性和扩展性：能够满足全球范围的用户同时操作区块链上的合约和数据无疑是一件堪称恐怖的事情，所以这种应用平台还需要拥有足够的扩展性能够随着用户和应用的增长而成比例的扩张

即时反馈：用户绝大多数的操作在安全允许的情况下都应该是实时反馈的，这是去中心化应用具有与传统应用可比性的基础要求

版本系统：应用版本系统帮助开发者能够快速完成 bug 的修复，方便开发商完成 A/B 测试等给类用户研究。

平台进化：社区提案系统和主节点投票可以帮助完成以太零的社区驱动进化，便于各类技术迭代和平台规则的共识快速达成。

至关重要的组件功能：去中心化存储如 IPFS 协议，安全的程序热修复规程，通用底层服务如身份认证，匿名通信，通知系统等

以太零出现的目标便是解决以上问题。考虑以太坊在智能合约，代币发行等领域技术和生态最为成熟，我们决定在以太坊的基础上去除其交易手续费系统，并采用达世币以主节点和 pow 共识层双层网络架构实现高拓展性和实时交易反馈，并计划在未来引入 IPFS 协议，DAG，Plasma 分层网络等更多开创性的技术方案。这是一个长期的工作，也是整个区块链和加密货币社区的工作，在以上任务未完成之前，我们将为此目标保持持续的学习热情，研究和汲取社区一切可行的技术。

第 II 章. 零交易手续费的智能合约开发平台

第 2.1 节 零交易手续费的突破

以太零一个很大的特点便是分离了交易验证和区块的打包和同步。为了极大提高区块链的使用场景，让 DAPP 开发者，智能合约创建者能更好的发挥区块链的价值。但以比特币，以太坊为代表的项目中目前高昂的手续费很大程度上阻碍了区块链应用的普及。

Alice 在咖啡店买一杯咖啡，假定该杯咖啡 23￥，如果采用比特币付款，那么她将支付多于该价格的将近十倍的的手续费价格，显然这是非常不合理的。以太零将目前以太坊中手续费及智能合约执行的 Gas 开销去除，采用零交易手续费的策略。由于以太坊中 Gas 机制另一个重要的功能是防止 DDOS 攻击的目的，在以太零中将结合权益证明的机制采用来解决该问题。具体实现去除手续费后采用的安全策略请参考 DDOS 攻击章节。

第 2.2 节 Gas 手续费在以太坊系统中价值

在以太坊中，gas 最终会以 ETH 货币的价值计算并付给矿工作为手续费，Gas 和 ETH 在以太坊中的意义表现为：

1) *作为对对矿工工作的奖励*
2) *作为抵抗 DDOS 攻击的一种手段*
3) *作为一种增加 ETH 流动性的手段*
4) *作为一种代币交易的中间货币*

取消后如何保证矿工的奖励？ 即使除去手续费，矿工仍可以打包区块来获得货币奖励，矿工打包产生的以太零币奖励将分为三个部分，本身保留 45%，主节点保留 45%，社区预算 10%。

第 2.3 节 **零交易手续费对于通用 DAPP 开发的意义**

以一个最简单的 Todolist，待办事项应用为例，其去中心化的实现可以应用在团队任务分解的过程中，这个过程需要项目的各个参与者了解其他成员的任务，每个人任务都是团队的共识结果，具有可追溯，去信任的需求。

该应用会涉及成员的注册，任务的增删改查等需求。按照以太坊开发要求，这些所有的操作都是需要消耗 gas，也就是计费的，这对于应用的使用者来说显然是不合理的而在以太零中，交易发起频率与智能合约的执行步数将与账户中拥有的余额正相关性。这在满足免费的同时也考虑到了对于带宽的合理使用，并限制了恶意攻击者发起 DDOS 攻击需要较高的门槛和资本投入。这种从经济层面考量的限定权益机制免费将会真正的引领去中心化应用进入生活场景。

第 2.4 节 **技术实现**

1) *新增一个交易验证协议层，解决无交易费可能引起的 DDOS 攻击*
2) *根据持币量限制发起交易的频率*
3) *交易时携带 data 的大小限制与持币量成正比*
4) *引入交易等待池，交易频率和持币量等负责因素组成的动态算法*
5) *实现 0 交易费，持币越多可发起交易频率越高的创新模式*

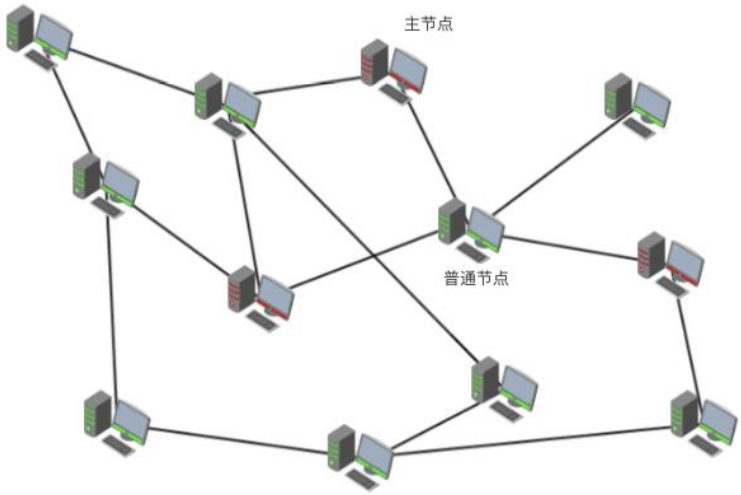
第 III 章.双层网络上的高并发和实时交易

第 3.1 节 **为何引入 Master Node**

什么是 Master Node

主节点，源于达世币的一种全节点服务器，为了保证区块链提供一定服务和基础性能而存在的必要服务设施。主节点以 POS(服务量证明)机制运行，并和负责完成 POW(工作量证明) 的矿工节点共同构成概念上的双层网络。在以太零网络主节点负责代理全链的交易有效性和区块合法性验证。主节点之间可以在共识层前构建一层仲裁层，以实现交易验证和区块链记账事务的分离。是实现高并发和实时交易特性的核心基础设施。除此之外主节点还负责社区提案的投票，参与到社区去中心化社区管理和技术迭代过程中。

需要说明的是，在物理网络连接上，主节点并不特殊于普通节点：



通过节点构建的点对点网络中各个节点，联网第一时间便需完成同步当前活跃的主节点列表的任务。

主节点职责

主节点的职责包括：

1) *交易验证：和被算法选定的其他主节点达成共识并广播结果，提供秒级实时交易反馈，这种即时的反馈区别于达世币，并不限定在特殊服务的范畴而是通用的基础服务，对所有用户的所有操作默认开放*

2) *社区自治：拥有对提案的投票权，提案会反映社区的讨论趋势和焦点，会涉及到以太零发展的方方面面，包括不限于技术迭代方向，运营计划调整，成员纠纷决议，经济运行参数变更等。*

3) *专业化服务：区别于达世币以支付为主要应用场景，以太零面向的是更为广泛的去中心化应用，这就要求主节点提供的服务在未来可能会细分化，专业化，从而满足特定的应用需求。*

工作机制

主节点的排序，选择和验证：对全球的活动主节点进行排序，并将最高排名的10%-20%主节点作为选择池。客户端将使用主节点随机生成算法从选择池中选择 10 个主节点用于交易验证，一旦 10 个主节点中的 6 个确认并达成共识，此项交易便被承认并锁定，进入后续的区块链打包记账阶段。

主节点权益

主节点的搭建和维护需要投入财力，时间，精力，技术来为全链的用户提供体验越来越优秀的服务。主节点在承担以上责任的同时，也会因此收到系统的奖励，奖励来源于矿工节点打包区块的分成。矿工每打包一个区块获得奖励的 45%自己保留，另外 45%会向全系统活跃的主节点进行分配，剩余的 10%用作社区自治和提案预算。

区块奖励向主节点的分配算法可以描述为：多劳多得。处理更多交易的节点得到更多奖励；投票和提案结果相符的节点获得更多奖励；

运营一个主节点

经济门槛

成为主节点只要关联的账户中有 2 万的 ETZ 即 可，此款项可以随时取出，但取出操作会导致主节点服务中断，帐户中锁定的 ETZ 数量一旦低于 2 万，该主节点将会被从仲裁层中剔除。此门槛值的设定意义在于

1) *保证主节点的建立和维护者具有一定的资金，能够长期维持稳定的网络服务*
2) *保证 ETZ 的稳定，保证一定的通货紧缩，保持币价的持续上升。*
3) *保证潜在的 DDOS 攻击者设立大量全节点的攻击需要巨量不可承担的经济成本*

技术门槛

主节点的部署需要一些网络部署和安全知识，并且要求服务器拥有独立的 IP 地址，24 小时在线且掉线时间不大于一小时。主节点搭建者可以自行部署也可以寻求以太零官方合作的云服务商的支持，以太零团队之后会在官网给出详细的操作文档。操作文档将描述主节点的概念，收益方式，详细的程序化和命令化操作指南，运营工具包，维护方案和 FAQ。

第 3.2 节 **双层网络**

主节点形成的仲裁层和后续的共识层共同形成了双层网络的架构，双层网络对于高并发的意义在于以近乎异步执行的方式将交易的确认和区块链记账分为两个步骤实现。交易一旦在仲裁层锁定并确认便直接返回客户端结果，无需等待共识层完成账务记录。

除主节点外，由于以太零采用的仍然是 Pow 共识算法，矿工和算力对于平台的发展仍至关重要，平台保留了对于打包区块的奖励，以太零团队将提供完善不同平台的挖矿软件，方便现有算力的简便转移。

长期来看，手续费的去除可能会对矿工造成烦恼，但是由于矿工本身拥有较多的 ETZ，垫定了其成为主节点的潜能，这种概念上和物理上的整合本身也是我们计划中获得更高拓展性和并发性的一种解决方案。基于达世币成功的运营经验，我们有理由相信双层网络长期能够形成融洽的共生关系。对于更长期的共识层建设，我们团队会考虑 DAG 技术和 Plasma 类的分层网络。

第 3.3 节 **双层网络与 DPOS 共识机制的对比**

事实上所有的 DPOS 共识机制都可以简单理解为”有钱人的游戏“。EOS 的构建者 BM 在与 Ethereum 的创始人 Vitalik Buterin 的争论中曾明确提到过这一点。这一特性的来源于 候选人被选举为委托人的概率正相关于候选人的账户余额这一处理方式。以 EOS 为例，其投票算法是在由所有节点选举出 20 个基本代理人，然后由这 20 个基本代理人再选举出一个额外代理人。这种投票权取决于账户余额，而投票选出的 21 位代理人也将在一个为期约一分钟的周期内全权代理整个区块链的区块构建工作。

对于以太零的主节点生成算法而言，所有的交易都是由客户端同步主节点列表后随机生成，每笔交易的处理代理人在概率上基本不可能重复，实现了更高程度的去中心化 。

第 3.4 节 **如何实现高拓展性**

我们将高扩展性定义为同时支持巨量用户，巨量请求，以及这种高并发附带的交易实时或近实时响应。

首先描述一个普通用户 A 向普通用户 B 发起一个交易操作的流程：

1) *用户 A 使用交易锁发送 ETZ 给用户 B*
2) *交易锁广播到整个网络，最后达到被选举出来的 N 个主节点（N>2）*
3) *被选举出来的主节点用交易锁对交易消息进行签名形成一个一致性消息，然后将这个一致性消息广播到网络*

4) *当某个节点收到一致性消息时，就可以认为这个交易是被确认过的，以此实现快速支付。用户 A 再次用这个网络中已经存在的一致性消息发起交易时，会被网络拒绝，达到防止双花攻击的目的。*

实现路径

1) *双层网络：主节点和矿工节点的分离使得交易的验证确认和打包区块记账的后续处理流程分离，配合交易锁定能够以类似异步的方式安全的实现近实时交易处理。*
2) *非全节点确认：主节点保证了不必要全链节点都参与交易的验证，只需要经过 5 个主节点的确认。结果也就是主节点越多，网络整体的交易并发处理的能力越强，此能力近线性增长。*

未来计划

增大区块容量也是一种增强扩展性的手段，以太零将支持 2M 区块容量，并会根据用户量和请求的变化有计划的发起社区预案。

随着扩展性对硬件的要求越来越强，未来的主节点和矿工有回归为单一组织的趋势。依靠专业的服务能力，合一的节点将实现中本聪提到过的节点专业化。

“当前的系统中，每一个用户都是一个网络节点，但这并非意味着它们就是系统大规模后的节点，那时的情况应该像每一个新闻组用户去运行他们自己的 NNTP 服务器一样，这种设计使得用户就仅仅是用户，当运行一个节点的负担越来越重时，节点的数量就会随之减少，那些少数节点将是那些大型的服务器场（矿场）。其余的都将是客户端节点，它们将只进行交易，而不会产出新节点。”

引用：https://medium.com/@eduffield222/how-to-enabling-on-chain-scaling-2ffab5997f8b

这或许是传统中心化经由去中心化向去中心专业化的一种嬗变，这种合一节点的角色有些类似现在的云服务商。参考当前云服务商的研发和运营，建立去中心化的分布式云服务商，我们将研究如何在这三方面增强未来这种合一节点的服务能力：

1) *定制化的高性能硬件，包括 CPU，RAM 和 硬盘*

2) *足够的带宽支撑主节点向全链的传播*

3) *主节点网络能够稳定互联并实现相互之间极为快速的广播*

第 3.5 节 **如何防止攻击**

2/3 攻击

主节点门槛值的存在使得发起基于构建大量节点的攻击方式变的极其昂贵 。以达世币的主节点网络为例，在主节点总数为 3000 时，为了获得 1.72%的攻击成功率，黑客需要控制或创造 2000 个主节点，即购买 2 百万的达世币，在现在的币价条件下，这中资金要求实在少有人能及，以这种方式攻击绝对得不偿失。加之锁定的达世币降低了达世币的大值流动性，这种攻击操作起来就变得更加不现实。

攻击节点数/总节点数	成功率 p	所需达世币数量
10/1010	3.44e-24	10,000
100/1100	2.52e-11	100,000
1000/2000	9.55e-03	1,000,000
2000/3000	1.72e-02	2,000,000

$p=\prod_{i=1}^{n}((r-(i-1))/(t-(i-1)))$

其中，n 为主节点仲裁链的长度；t 为当前网络中的激活的主节点数量；r 为攻击者控制的坏节点数量，其值≥ n。

引用：DASH WHITEPAPER –INSTANT TX

双花问题

在一个大型的可伸缩分布式网络中，一个常见的问题就是如何保证一个资源在全网中保持一致。解决一致性性的问题通常是通过调用各种一致性算法来实现，例如 Paxos。

比特币通过 POW 和区块确认数来防止双花问题，由于设计的自身限制，一个交易的确认需要等待很长的时间。以太零引入交易锁的概念，用户发起交易时，会生成交易锁广播到整个网络,该交易锁会锁定交易关联的数字资产：

Transaction Lock: (“txlock”, CTransaction, nBlockHeight, Signed Message)

未收到 Master node 的验证消息前，任何一个客户的都无法再转移资产，当网络中出现已经存在的交易时，这种情况通常发生在另一个客户端在未接受到交易锁通知的情况操作被锁定的资产时，这种情况将被认为是恶意的双花攻击而被拒绝。

女巫攻击

指通过在网络上冒充身份的一种攻击方式，Master Node 本身的备付金门槛设定以及大量的以太零币被锁定在账户中导致的低流动性导致计划依靠建立大量主节点攻击的成本变得极其高昂。

DDOS 攻击

DDOS 攻击指短时间内大量的垃圾交易请求主机，这可能导致部分主节点的脱机，服务中断。对于去除交易手续费导致的 DDOS 攻击低抗性，以太零的交易规则设定借鉴了 POS 机制，一个账户发起交易的数量，频率，执行合约的深度，

打包时的排序都会正相关与该账户的 ETZ 余额，这就导致大量的垃圾交易发起的成本非常高。包括以下：

1) *交易门槛：为了防止恶意攻击网站，将限制当账户中拥有 0.1 个 ETZ 时，才可以发起交易。且交易发起笔数在一个区块打包周期内（10s）是被限制的 。*
2) *交易顺序：账户余额越大，在区块打包时的排序优先级越高*
3) *交易深度：调用智能合约的调用链长度有限，链长随着余额的增大而增长，*
4) *交易容量：所携带的交易数据和余额有关，余额越高，可携带的交易数据越多*
5) *交易合约执行深度：为防止合约执行时陷入无限循环的状态，将限制栈的最大深度为 1024.*
6) *智能合约执行：只有当合约账户余额大于 100ETZ 时，才能发起，将在执行该笔合约时对账户余额进行验证。*

Finney 攻击

Finney 攻击由比特币的第一个用户 Hal Finney 定义, 它是一种利用比特币中未确认交易来欺诈接受比特币支付的商家的一种攻击，是双花攻击的一种变种。该攻击的前提条件是：商家信任未确认交易，并且在收到未确认交易后便立即发货，且无法撤销。

这实际上是利用了 BTC 等高延迟交易确认类支付服务的时间差，在以太零中，接近实时的交易极大降低了这种攻击的操作空间。

第 IV 章.社区自治和进化

自治源于良好的缺陷管理和责任机制，进化则源于顶层的思想，技术和经济引导。

简单的提案投票模式即可完成基本的缺陷管理。没有完美的系统，所有的系统在不同的发展阶段都会有不同的需求需要满足，这种需求变更未来将越来越多

的依赖社区的力量，包括问题的发现，提案，评审，众包，奖惩。而责任机制的形成初期依赖基金会引导社区形成评审制度，中远期将固化和合约化到区块链底层协议。

经济关系决定社会架构。预算系统占据了区块奖励的 10%，这从底层提供了一种社区自治和进化的经济激励制度。

第 4.1 节 **关于开发者**

开发者将被认为是以太零社区的核心群体，是社区资源即 DAPPs 的提供者，保证了社区对用户的粘性和生态的繁荣程度，所以以太零也会从预算或直接在经济结构底层构建对优秀 DAPP 团队的奖励系统,以繁荣整个社区的应用服务能力。

第 4.2 节 **关于提案**

当前的达世币的社区治理机制很好的促进了各种应用和活动的举办，达世币的市值也是逐渐增长之中，以太零也将引入类似的社区治理系统，但主要目前是鼓励和支持应用的开发者。

1) *申请：人人都可以发起提案，这样更需在社区中有一定贡献和名望才能获得 Master Node 的认可。*
2) *审核：审核全部在链上完成，(赞成-反对) 多于 10% 以上的主节点投票，则提案通过审核。*
3) *奖励：奖励将在每周的超级区块上挖出并按提案金额奖励提申请者。*

第 V 章. 技术参数

第 5.1 节 **POW 共识机制**

1) *区块大小：2M*
2) *区块时间：10 seconds*
3) *区块奖励：4 ETZ*
4) *难度算法：EtHash*
5) *难度调整：动态*

第 5.2 节 Master Node 主节点

1) *准入：锁定 20,000 ETZ*
2) *奖励：每个区块奖励的 45% 归矿工，45% 归主节点，10% 为社区自治预算。*

第 5.3 节 交易

1) *确认主节点数：随机 10 个主节点中的 6 个达成共识*
2) *即时交易*

第 VI 章.应用场景和市场预期

第 6.1 节 通用应用

区块链的核心任务是信任无关，也即是无论交易对手方是谁，己方无需对其产生任何信任即可直接进行交易，这种信任无关是通过智能合约实现的。以一个比赛结果对赌合约为例，其简化代码大概如下：

```
比赛结果=NBA 官方网站 API.get("总决赛")
if(骑士赢)
  pay 40 to A
else
  pay 40 to B
```

以此考虑，现实中哪些服务是需要双或多方参与的，需要中间人的存在来消弭信任的，那么这些服务都可以通过在区块链上部署智能合约代替中间人的职责。

事实上基于以太坊的智能合约本身也是通用的，但其消耗手续费的特性使得开发者编写的复杂智能合约在成本上支撑不起较大的用户量。

而以太零去除其手续费系统后，使得合理使用智能合约服务的用户不会付出任何成本，保证了大型去中心化应用在经济上的可行性和可持续性，也使得 DAPP 天然的的具有了根据账户余额差异化服务的能力。

第 6.2 节 **行业落地**

以太零作为一个底层应用开发平台，事实上是不限于合作的行业的，但有必要对一些成熟的思考做出表述，这种思考是我们未来一段时间将会着手落地的应用。

游戏道具内容协作和交易平台

一只猫搅翻了整个以太坊，也让人们认识到了区块链在一个游戏细分领域的巨大潜力：道具的唯一性在道具交易市场的重要性。

我们将设计一个内容型的去中心化道具外包和交易平台，连接设计师与编剧，数值系统设计师，游戏厂商，玩家等人群，各角色的用例如下：

1) *游戏厂商：发布需求，向智能合约锁定 ETZ 币作为预付款*
2) *设计师和编剧：领取任务， 根据游戏厂商的游戏概念设计道具；被认可后接受合约付款*
3) *数值系统设计师：设计爆率,道具效果,爆出条件,变异条件,变异规则等；被认可后接受智能合约的付款。*
4) *玩家：投票给道具设计；交易唯一道具*

通过这样的生态环路实现创意的表达，传播和变现。

行业代币支付解决方案

行业研讨会会深入各个行业，和专家讨论在这些行业内建立独立的基于以太零代币的经济体系的必要性和可行性。并探讨大数据技术和分布式记账，匿名记账技术的结合点，并基于大量可信的数据为行业的人工智能应用提供充分的养分。

中心化组织的映射

社会需要各种组织形式，社会自身的包容性和多样性正是社会自由程度的一种表现。我们计划在以太零内实现一种现实组织的虚拟映射, 相对 DAO 组织，我们称这种映射为 MRO(Map of Real world Organization)，这种实现可以涵盖匿名和实名，能帮助现有的企业快速应用区块链技术实现企业管理和商业关系管理。设想：

1) *每个组织都可以将自己的组织映射到该应用*
2) *组织管理*
    a. *招募成员，签署智能人事协议*
    b. *组织可以通过该平台发放薪酬，实现各类股权架构*
    c. *购买开发者和律师合作开发的各种基于标准可信链上数据的大数据，人工智能服务。*
    d. *发布外包任务，签署智能外包协议*
    e. *发起记名和不记名投票*
3) *组织之间*
    a. *可以和商业对手方签署无需第三方担保的智能合约*
    b. *可以和合作伙伴签署股权互持等智能协议*
    c. *发布企业债务，进行 ICO 和各类融资*
4) *更多可虚拟，协议化的场景。*

第 VII 章.　经济体系

第 7.1 节 **货币用途**

ETZ 币在整个生态中的用途按照涉及角色分类：

1) *矿工*
    a. *作为矿池奖励*
2) *社区*
    a) *作为社区被通过的提案执行的预算*
3) *主节点*
    a) *作为主节点需要一定的 ETZ 余额*
    b) *作为主节点奖励领取*
4) *开发者*
    需要锁定部分 ETZ，数量正相关于智能合约复杂度
5) *用户*
    a) *账户 ETZ 余额作为发起交易的门槛，执行交易深度，频率等的参考依据*

基于以上作用构建起的经济体系能有效激励各个角色在以太零生态内为了共同的目标努力。

第 7.2 节 **货币供应**

以太零的内生用币名字叫以太零币(EtherZero, 简写 ETZ)，初始发行总量 1.94 亿个，其中 9700 万作为糖果在分叉后向以太坊持有者 1:1 等量发放，预留 9700 万个用于早期投资者私募，以太零基金会，以太零后期开发和生态拓展。

区块产出每年大概新增 6.5%的新币，每个区块产出的 45%归矿工，45%归主节点，10%归自治社区。

第 7.3 节 **货币锁定**

主节点锁定

达世币目前有 4777 个主节点(引用 1)，每个主节点需要锁定 1000 个达世币，占达世币当前总量 7,783,295 DASH 的 61%。

以太零每个主节点需要锁定 2 万个以太零币，假设以太零运行 1 年后，达到 4000 个主节点，即需锁定 8000 万的以太零币，占以太零币总量的 41%左右。

开发者锁定

指为了保障智能合约的正常运行，开发者需要锁定在主管账户中的币值，此币值可以随时取出，但会影响合约的执行，因为系统限制了一下条件：余额 10ETZ 以上的账户发布的智能合约才可以处于服务状态。

普通账户锁定

此锁定事实上指的是一种发起交易所需要提供的权益证明，事实上用户可以随时取出余额，但限定了：账户余额 0.1ETZ 以上才可发生交易。

第 7.4 节 **货币交易**

近期上交易所，具体请保持关注官网和 twitter

第 7.5 节 **货币政策**

主节点，普通用户，开发者三种角色的锁币行为导致市场的供应量较长时间都会保持一定量的通缩。随着业务的发展，这些锁币的数值会通过通过社区的投票系统做出适当的修正。

由上可知以太零将会存在大部分以太零币 ETZ 储存在主节点和智能合约里，这种内生的经济系统，加上源源不断的新账户对以太零币的支付需求和交易平台海量的新生投资者，供求关系的倾斜将会不断推高以太零币的价格。

第 VIII 章.　以太零的未来和愿景

第 8.1 节 **工作计划**

平台的技术特性迭代将会对应生态的渐进式发展规划，在不同的时期基于不同的特性引导开发者和用户关注相应特性支撑的杀手应用。从发展的角度看待生态的壮大。

1) *2018 年 1 月，以太零测试网络对外发布，实现 0 交易费用和防 DDOS 攻击*
2) *2018 年 2 月，以太零私募发放完成，上线在线钱包，主网上线实现 0 交易费用和防 DDOS 攻击，挖出第一个分叉后的以太零区块*
3) *2018 年 3 月份，发布移动版钱包，Dapp 应用市场，促进用户端的生态发展*
4) *2018 年 1 季度，主节点 Master Node 在 Testnet 测试成功*
5) *2018 年 2 季度，完成主节点 Master Node 在 Mainnet 运行，实现实时交易和较高交易并发(大于 1000TPS)*
6) *2018 年 4 季度，主节点 Master Node 优化版上线，支持上万 TPS*
7) *2019 年 1 季度，明星 Dapp 应用比赛并推出长期的开发者奖励计划，促进开发者社区的发展繁荣*

8) *DAG 共识机制和 Plasma 分层网络等提高 TPS 的技术，将会是技术团队内部长期研究的课题，并在适当的阶段推出测试版本*

第 8.2 节 **产品愿景**

我们定位自己为区块链技术的融合者，推广者，落地者。

融合指的是现在的大部分创新技术还在实验阶段，彼此之间割裂严重，应用场景定位不清，需要一个组织站在旁观者的角度，研究这些技术在真实的应用场景中的整合可能性，并向开发者提供一个容纳各项技术，面向应用层的的操作系统 。以太零在完成主节点开发任务后，将使用私募资金招纳各项新区块链技术人员进行现有技术的整合，长期将以生产网络和实验网络并行的方式促进技术向实用场景的转化。

推广和落地针对的是真实的应用场景。任何一项技术必须有真实的可用场景，并对原有的技术体系产生了经济效益上的突破才会成为主流。我们会组织一个专门的行业应用工作组，团队成员由传统行业专家，区块链技术人员，产品化和策划人员组成，以穷举的方式对当前社会各行各业进行产业调研和场景可行性研究，以期完成区块链革命的深化和普及。

太多的概念和技术对于普通用户来说已经成为了解和享受区块链带来的红利过程中的一大障碍，我们希望通过一种认知和技术上的融合来避免用户直接接触复杂的概念，向用户输出一种成熟的产品。我们会竭尽所能引导社区开发者开发真实可触的产品。

第 IX 章.团队和社区

以太零团队

以太零作为一个全球化的开源公有链项目，由正在筹备的新加坡以太零基金会负责全球运营，是由来自中国的核心开发团队，印度和东欧的 2 个资深 DAPP 开发团队协助研发，同时有国内外数个营销团队协同推广和运营的 DAPP 底层开发平台。

以太零核心团队成员

Befree 负责人

连续创业者，先后转战网络营销，共享软件，手机游戏 到加密货币，负责过数个数字货币和 DAPP 的开发和运营。负责以太零理念设计， 开发方向，力促以太零成为通用 DAPP 底层开发平台，在 5-10 年或更长时间 内能不断进化和发展，为下一代的区块链网络社会贡献自己的微薄之力。

Rolong *技术总监*

有 10 多年开发经验的资深全栈开发工程师，精通 C++,GO,JAVA,erlang 等服 务器端开发和 web3，h5 等前段开发，资深的智能合约开发大神，对以太坊底 层网络有深入研究，更是国内顶尖的 DDOS 防御高手，其发表的技术方案仍被 其他开发人员承为技术规范。

Roger luo *开发总监*

资深以太坊底层开发工程师，是国内局指可数的对以太坊底层有过深入研究的 技术大牛，十年金融科技开发工作经验，区块链爱好者，开源社区的活跃者， 专注于以太零核心开发。

Frank *产品经理*

两年金融行业咨询，3 年金融行业产品经理，现专注研究加密货币和区块链技 术的的应用场景，以及可能的技术实现路径。

Mia *资深海外营销专家*

有过多年国外推广经验并取得过优异战绩，负责以太零全球网络的宣传和推广。

以太零社区

海外电报群 10K+用户 https://t.me/etz_official

https://t.me/etherzero_org

https://t.me/etherzero_mining

官方 QQ 群 1700+用户：438437925

第 X 章. 总结

以太零融合了以太坊，并在其基础上打造了安全可靠的免费服务，使得大型复杂的智能合约在经济上拥有了可行性和延续性。结合主节点网络实现的高扩展性和实时交易反馈更为大量用户提供了极佳的交互体验，将一改人们意识中区块链交易确认等待时间超长的印象。

鉴于区块链行业还处于技术的百家争鸣时代，唯有博采众长构建完善的技术架构，深入行业步步为营才可以降低面临的整体性风险，完成我们长期的成为社区主流区块链应用平台的目标。

但目前技术的局限性将限制区块链在日常生活中的普及，价格的炒作也将持续一段很长的时期。以太零将不忘初心，在 5-10 年或更长时间内专研技术领域，以提高区块链技术为目标，探索在各行业应用为己任，用去中心化技术和思想为提高社会运行效率，降低社会运营成本，实现更公平的社会贡献一份微薄之力。感谢大家的支持！