标准链

打造去中心化世界的基石

2017.12.31

创世纪

创区块链之革命 自中本聪（Satoshi Nakamoto）2008 年发明比特币以来，其作为“一个去中心化电子现金系统”，把计算机领域成熟的技术（如：P2P 通信，密码学，块链数据结构等）创新的组合在一起，形成了一种去中心化、非信任和基于博弈的自治体系---区块链。随之以以太坊为代表的系统提出了具有图灵完备性的智能合约概念，使区块链既能实现价值的传递，又具有一定的逻辑判断和处理能力。自此以后，越来越多的人意识到区块链技术的巨大价值和潜力，开始关注和研究区块链技术，促进了区块链的基础设施的持续发展。

但是我们看到由于当前区块链平台的局限性，还很少有区块链系统实现和现实社会的连结，在各实体行业的广泛应用仍然受限：区块容量受限，难以处理和记录海量交易，容易造成系统拥塞；共识机制本身缺乏灵活性，无法随意在共识机制中引入不同的因素以动态的衡量用户的贡献力；同时现有区块链系统具备很大的封闭性，目前大多数智能合约仅接受链上数据作为触发条件，缺乏与现实世界的交互。

我们希望可以构建一个全新的区块链生态系统----标准链，把区块链技术推向更高维空间的进化和演变，使其最终作为未来世界可选的互联网价值传输协议。通过对分布式技术、P2P 通信、共识机制和智能合约的创新，在芯片物理层及协议层上进行革命，最终使得标准链成为区块链世界连接现实世界中的桥梁。

立雾联网之标准 标准链技术从底层驱动科技从物联网（IoT）向雾连网（FoT）

的转变。物联网中各个设备虽然分布于不同的区域，但是它们之间的交互和所有的运算都通过云端的服务器进行。从本质上来说，物联网仍然是中心化的架构，在大规模拓展时会遇到很多瓶颈：成本飙升、系统拥塞、可靠性降低、服务器容易受到攻击。另外，设备的数据也归属于服务商所有，用户无法全面的获取自己的数据。

标准链驱动的雾联网采用去中心化的架构。基于去中心化的需求，标准链重新设计了传统区块链中的一些元素：

- 共识机制中引入了设备计算能力、存储能力及通信能力的贡献度（第 3.1 章节）。
- 全新的合约设计，链下和链上数据的共同输入作为触发条件，实现线上线下的价值交换（第 3.2 章节）。
- 引入新的交易费率机制，实现区块链社区资源的最优分配（第 3.3 章节）。
- 新的加密结构和访问权限，设备可开放链上数据给指定用户（第 3.4 章节）。
- 广泛集成现有的如分布式文件系统、分布式数据库等第三方软件，将他们的优点和区块链技术结合，取长补短（第 3.5 章节）。
- 优化了和硬件连接的接口，允许不同特性的硬件无缝接入标准链（第 3.6 章节）。
- 在协议层内置币币互兑系统，方便运行在雾联网中的不同 DeOS（Decentralized Operating System）之间进行价值传递

通过这些创新，人与人、人与物、物与物的相连不通过中心服务器而在标准链所架构的分布式结构里完成，前面所述的中心化问题均可以得到完美的解决，并最终发展成为一个软硬一体的生态：所有运行在标准链共识机制上的设

备或系统都可视为标准链里的公民：他们向其他个体购买生产资料；他们贡献自己的生产力获取报酬；他们缴纳一定的税收；他们在法规的约束中博弈。

构可持续之生态 参与标准链的开发公司、运营基金会并不保障整个标准链项目是否能够最终实现我们的愿景，我们所能保证的一点是：在整个项目一旦执行后，基于网络及社区的维护将生生不息。

社区建设和代码开源：标准链致力于通过社区、第三方开发者和技术上的创新，打造一个在全球具有影响力的开源社区生态，通过开源鼓励第三方的开发者一起推动标准链技术渗透不同的应用和产业。最终目的是将区块链融入万物相连的世界，成为现实世界个体信息传递和价值交换的媒介。

雾联网基金会：为实现标准链的可持续性发展，避免散沙式的发展结构和底层构架分化，标准链基金会将制定完善的治理架构，对一般轶事、代码管理、财务管理、薪酬管理和特权操作范围等事务进行管理。同时，治理架构会随着基金会和社区的发展不断更新，并引入监察和监督功能，规则制定和变更控制管理等。

商业应用：标准链基金会通过与合作伙伴的通力合作，将企业、商界、技术和政府等多方面资源进行整合，最大化实现资源共享，最高效利用资源，实现社会协同发展。

目录

1 概述

1.1 标准链和雾联网

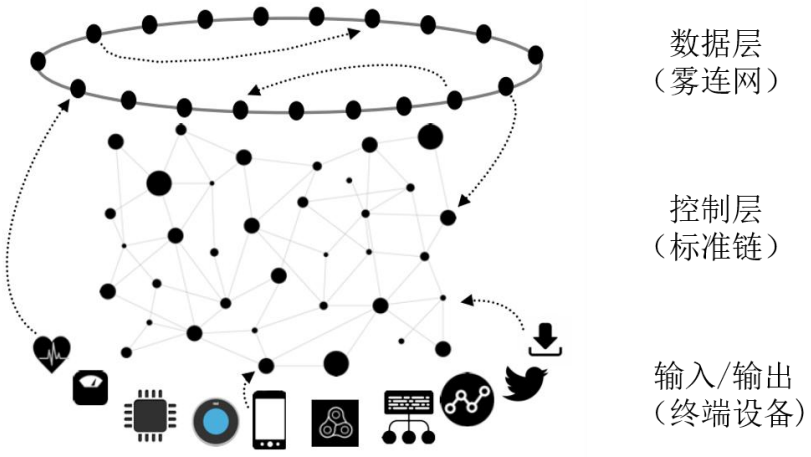

图 1 标准链与雾联网

从技术层面上讲，标准链是通过区块链思想形成的一个去中心化的超级计算机，这个超级计算机是由标准链规范的协议上运行的，任何可联网的设备（如：电脑、手机、手表、车辆、游戏手柄、路灯、智能家居等）或 DOS（如以太坊、EOS 等）在标准链上运行并建立连接，互相提供服务。简单的说，在超级计算机中，终端设备提供输入/输出服务，数据在雾联网中处理，由标准链协议层控制。第 1.2.2 章节详细论述了超级计算机的结构。

对应于实体世界而言，标准链便是一个便捷、安全可信任的去中心化运营组织。所有连接设备或系统都可视为标准链里的公民：他们向其他个体购买生产资料；他们贡献自己的生产力或生产资料获取报酬；他们缴纳一定的税收；他们在共识的规范中博弈。

和目前物联网设备不同，设备或系统在标准链中运营的服务都是分布式的。

一个标准链设备或系统所获取的服务是由标准链中的一个设备/系统或者其他多个设备/系统合作提供，且无法确认来源，因此我们称之为雾联网。

标准链主要为雾联网设计了一个基于价值激励的自进化系统，主要在以下几个层面进行：

- 定义价值尺度：标准链定义了衡量雾联网中的设备贡献的价值尺度和激励方法。通过对设备的激励，引导并挖掘雾联网的最大价值。
- 建立社区生态：建设社区，为开发者提供友好的正向反馈机制，建立一个繁荣的去中心化应用生态。
- 实现自我进化：标准链的自我进化治理模式可以引导雾联网向更快的计算、更强的系统、及更好的体验进化，避免过多人为干涉。

通过标准链不仅可以实现当前传统的互联网和物联网服务：如：社交、电商、游戏、家庭安防、医疗报警等。它还可以将现有的很多区块链项目直接应用在标准链之上：

- 需要大量分布节点交互和合作的服务：自组建 Mesh 网络、车联网中的场景检测等。
- 需要大量计算能力的项目的开发。如：大数据科学运算、人工智能的训练等。
- 遵循标准链共识机制的其他区块链项目或区块链操作系统。

1.2 标准链的产品及技术特点

1.2.1 标准链中的几何哲学

在数学的百花园中，几何是最美丽的奇葩，它既有优美的、令人赏心悦目的图形，又有众多论证严谨而优雅、美丽而精致的命题。几何这个词最早来自

于希腊语“γεωμετρία”，在中国古代叫作“形学”，就是研究空间结构及性质的一门学科。在远古时代，人们在实践中不断积累和掌握了的各种平面、直线、方、圆、长、短等概念，并且逐步认识了这些概念之间以及它们之间位置关系和数量关系，这些就成为了几何学的基本概念。现代几何学又发展出了微分几何、拓扑学和解析集合等多个分支，并被应用于测绘、建筑、天文和计算机等不同领域中。我们的世界就是一个几何的世界，充满了几何的规律，只不过我们习以为常、熟视无睹罢了。

和其他学科一样，区块链作为计算机科学中一门新的学科，它的设计与几何知识有极大的相关性和相似性。区块链中个各个节点组成的 P2P 的网络即涉及拓扑学的知识；区块链中矿工之间的合作和竞争可以用博弈论和微分几何学来研究；当一个链增长到一定的体量覆盖达到一定的广度之后，各个区域的发展会具有统计自相似性，可以归入分形几何的范畴；如果在区块链共识机制中引入算力之外的因素，如存储和带宽等，则进入更高维度的空间，我们姑且可以称之为“区块网”或“雾联网”。

标准链旨在将分散性的存储、计算、带宽等能力，通过区块链及分布式技术，建立一个基于区块链思想的超级计算及网络系统，这是一个异常复杂的工程。为了能够简化设计并使标准链的概念更抽象化，我们引入了几何中“尺”和“规”的概念，在标准链中设计了标准玄尺(CZR)和标准玄规(CZC)作为开发和研究标准链的工具。尺和规作为几何里面最基本的研究工具，尺用来度量，规用来作图。在我们的设计里，玄尺**度量**标准链世界中个组件的**性能**，而玄规则**规范**标准链世界中组件交互的原则，玄尺和玄规试图寻求不同场景下标准链的最优解，是推动标准链世界发展和进化的引擎。

1.2.2 标准链+雾联网 = 超级计算机

图 2 显示了标准链和雾联网结合成为一台超级计算机的结构：

- 玄尺和玄规为整台计算机的运行核心，他们定义了整个标准链和雾联网的运行方向和核心的安全机制，可以把他们类比为普通计算机里面的 BIOS。
- 标准链里面的其他组件如共识机制、智能合约等定义计算机的运行机制，协调雾联网中设备和资源管理，可以类比为普通计算机里面的 CPU。
- 雾联网为超级计算机处理数据提供算力，可以类比为普通计算机里面的 GPU。
- 雾联网设备之间通过 P2P 的网络架构相连，可以类比为普通计算机里面的系统总线。

图 2 标准链超级计算机

在标准链和雾联网组成的超级计算机上，我们安装和集成了分布式 Web 服务器、分布式数据库等软件，并提供了应用开发 API。开发者可以在此基础上进行应用开发和生态建设。

表 1 总结了标准链/雾联网中各组成部分和计算机部件的对应关系：

计算机	标准链+雾联网	功能
BIOS	玄尺/玄规	提供标准链运行的核心机制
总线	P2P 网络架构	各节点之间的数据传输
GPU	雾连网设备	数据处理
CPU	标准链	逻辑处理，各节点协调和资源管理

表 1 标准链/雾联网中各组成部分和计算机部件的对应关系

1.2.3 区块链协议及芯片

标准链区块链协议旨在定义一个雾联网（即未来的区块链网络）的运行模式，其中主要包含治理模式、共识机制、价值传递规范等，并通过开源的芯片解决方案，为区块链的广泛应用提供有力的基石。

区块链协议将提供一系列的关键性规范文件，是形成所有共识的基础，基于协议之上采用层次结构，可以很容易的讨论和学习协议的规范细节，并创建了一个更好的互连环境，降低了整个雾联网的复杂度，使共识更容易达成，发展及进化的速度更快。

而专业的可编程区块链芯片，将共识机制从应用程序层下沉到芯片内核层，使标准链在性能及安全性上更能发挥价值。

1.2.4 区块链网关

对于普通用户而言，区块链似乎是一个高深的技术，同时，到目前为止，普通用户几乎没有接触过区块链应用（除 Token 外）。

标准链区块链网关的出现，革命性的降低了普通用户使用享受区块链所带来的改变，使得普通用户获得了一把开启通往区块链世界之门的钥匙。

1.2.5 标准玄尺 (CZR) 和 标准玄规 (CZC)

玄尺是在标准链和雾联网中多维度衡量元素价值尺度的组件；玄规是在标准链和雾联网中规范各方面行为的组件。目前已有的或者已被提出的区块链解决方案都主要以改进区块链本身的技术为主，寻找的只是区块链中局部的最优解。而标准链以雾联网的为出发点，把区块链里面的底层技术（链上）和雾联网的特性（链下）结合做跨层的优化(cross-layer optimization)，寻找区块链加雾联网全局的最优解，如图 3 所示。

玄尺对于衡量标准链和雾联网的性能，增强标准链的安全性和稳定性起到关键作用。玄尺在链上度量的性能有：标准链中区块大小、区块生成时间、矿工的参与度等；玄尺在链下度量的性能有：雾联网中设备 P2P 传输时延、设备带宽、设备存储空间、设备负载和业务能力等；雾联网上应用的稳定性、应用的使用频度、应用的传播性、应用中价值流动的频次和规模。基于上述指标，玄尺对获取的数据进行分析和处理，然后提供给玄规。

玄规获取玄尺提供的数据之后，着手构筑标准链的价值体系，建立更完善的模型，挖掘更多元的价值维度，采用更加节能环保和稳定的共识机制。玄规在确定标准链价值体系的变化之后，可以向社区提议进行标准链升级。

玄规还定义了标准链的治理原则（第 1.2.4 章节）。标准链利用玄规在签名用户之间建立 P2P 服务协议或约束性合约。玄规内容定义了仅依靠代码无法完全执行的用户间的义务，同时结合相互间的公认规则，确立司法权和适用法律。

每一个在网络中签名广播的交易，其签名信息中必须包括玄规的哈希值，以明确约束合约签名者。

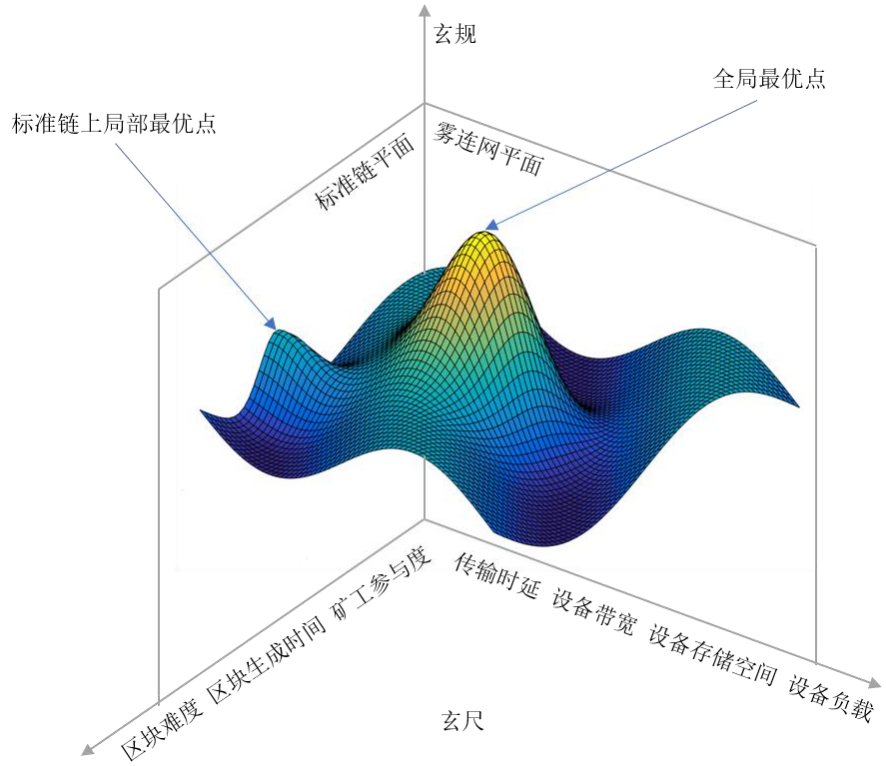

图 3 玄尺和玄规对标准链和雾连网作全局性的优化

1.2.6 标准链的治理

在对区块链协议进行升级或者当出现某些安全漏洞时，我们经常可以看到区块链社区出现一些临时的、非正式的、经常有争议的治理过程，从而产生硬分叉或导致不可预知的结果。如：比特币和比特大陆因为对区块大小定义的分歧而出现了硬分叉；以太坊因为 DAO 被黑客所攻破而出现了硬分叉。标准链系统通过玄规实现了一个社区共同治理过程，可以解决一些目前不能完全被软件算法所解决的问题（事实上在任何事物的发展初期均无法预知在后期发展过程中将出现的分歧）。

在标准链系统中，治理权力源来自于经过社区共识产生的区块生产者（第3.1.3.1章节）。区块生产者拥有有限的和被监督的权限来冻结账户，更新有缺陷的应用程序，并提出对底层协议的变更。区块生产者必须代表标准链社区中所有账号的广泛利益，如果他滥用权力或者拒绝对社区期望的改变做出投票，那么社区就可以通过选举替换区块生产者。

1.2.6.1 标准链参数确立

在玄规确立标准链的基本原则之后，由社区投票产生标准链上的各项参数，在社区投票通过过后写入这一版本的玄规。这些参数包括：

- 交易费率：链上为每笔交易收取的交易费。为了参与者的积极性，此费率为建议值，并非强制执行。
- 区块时间和最大区块尺寸
- 衡量设备贡献度的方法
- 产生区块生成者候选人的原则
- 区块生成者的数量
- 区块生成奖励的分配
- 不同区块链操作系统互通的接口定义

1.2.6.2 标准链升级

玄规定义了标准链的更新方法，需要完成以下步骤：

1. 社区开发者提交一个变更动议，并获得四分之三以上的赞成票，并把所有的赞成票维持连续7天。

2. 要求所有用户都必须使用新玄规的哈希值确认交易。
3. 社区开发者提交修改的源代码并提交测试网络，测试网络区块链上的哈希值改变。
4. 社区开发者继续将四分之三以上的赞成票维持连续 7 天。
5. 源代码修改测试通过后，所有节点需要在 7 天时间内完成升级，没有升级为新代码的节点将自动剔除。

2 标准链的场景展望

根据不同服务对于时延和计算能力要求的不同，标准链的应用场景可以分为几类。不同场景对于区块链技术提出了不同的要求和挑战，而标准链也为之提供了相应的技术和解决方案。

2.1 平台性应用

我们把类似于 Windows、Linux 等系统对于电脑芯片而言的区块链操作系统类应用模式称之为“平台性应用”。

在遵循标准链雾联网协议的基础上，任何区块链底层操作系统均可以运行于标准链系统之上，比如现在的比特币网络、以太坊、EOS 等，只要愿意遵循标准链的共识机制或互操作协议，那么也可以运营在标准链里面，并使用、调度链上资源。

此类平台性应用我们称为“DeOS”。

2.2 交互性应用

我们把具有低延时高可靠性要求的应用称之为交互型应用。主要包括车联网、Mesh 组网、医疗诊断、安防报警等。此类应用的服务需要在较低（可能在毫秒级）的时延内获得确认，确认时间远远小于目前一般区块链技术的区块确认时间。

2.2.1 车联网

车联网是由车辆位置、速度和路线等信息和周边信息构成的巨大交互网络。通过 GPS、RFID、传感器、摄像头图像处理等装置，车辆可以完成自身环境和状态信息的采集。

在传统的实现上，车辆通过无线技术将自身的各种信息快速传至云端中央服务器，中央服务器分析和处理所有周边车辆上报的信息，推算出当前的路况和场景，计算出不同车辆的最佳路线、及时汇报路况和安排信号灯周期。

在标准链的实现上，任意一个周边的设备都可以参与到车联网中，通过分布式处理周边车辆的信息推算当前的路况和场景。接入标准链后，路灯可以成为一个帮助车辆 GPS 定位的信标；所有路边餐馆收银台的电脑可以成为计算路况和场景的运算中心；行人过马路时的手机可以为车辆防撞系统发送警报。在标准链中，这些设备为车联网的场景提供计算力和服务，同时也从中获取收益。

2.2.2 Mesh 组网

Mesh 组网可以突破蜂窝网络结构的局限性，构建低成本的下一代无线网络，同时因其所具有的宽带性、无线汇聚功能、自组织、自管理、鲁棒性等独特的

性能，正受到越来越多的关注。目前它已被业内普遍认为是无线网络技术的一个发展方向。

在 Mesh 网络中，采用网状 Mesh 拓扑结构，是一种多点到多点网络拓扑结构。在这种 Mesh 网络结构中，各网络节点通过相邻其他网络节点，以无线多跳方式相连。在 Mesh 网络中，任意一个设备既可以是用户端，也可以是路由器。在设备自身应用和其他设备相连时，就是用户端；当设备为其他设备作中继转发时，就是路由器。

Mesh 网络的物理层技术（如：蓝牙，WiFi 等）和网络层技术都已经非常成熟，但是如何让一个用户设备牺牲自己的资源（处理器、内存、电池等）为其他设备作为路由器使用，一直是一个难题。

如果把 Mesh 网络建立在标准链之上，则可以利用标准链里的共识机制，衡量设备贡献度为设备分配一定比例的奖励，使 Mesh 网络在经济上能够持续发展。

2.3 大数据应用

我们把需要高运算力和高数据吞吐量要求应用称之为大数据应用。主要包括人工智能、药品的研制、计算机视觉渲染等。此类应用的服务节点之间数据量的交互远远超过目前一般区块链技术的区块大小。

2.3.1 人工智能训练

机器学习算法特别是神经网络在近几年越来越流行，当前神经网络已经应用到计算机视觉识别，语音识别，自然语言处理，股市的预测和分析等领域。

为了让神经网络驱动仿效生物大脑的工作，给电脑赋予像人类一样的行为，

有时甚至超越人类的能力。必须在神经网络里面多达几百甚至上千层的节点，又被称之为深度学习网络。在深度学习网络上的项目需要为其部署，训练和调整提供巨大的计算能力。现代的个人电脑（例如，Core i5 芯片，8Gb 内存）可以在合理的时间内训练拥有数以万计样本的网络，支持维度高达数百的输入数据。但是深度学习网络需要更大样本的数据，这些目前都是通过数据处理能力更强的 GPU 实现。

标准链为实现机器学习算法和深度学习网络提供了经济而高效的解决方案。通过把深度学习网络中的层次合理的分配到不同的节点中，节点之间仅交互层与层之间的参数，可以加快学习过程，提高学习质量。标准链中根据设备的运算能力合理分配深度学习网络中的数据，并提供它们相应的收益。

3 标准链技术

3.1 PoP 共识算法

3.1.1 节点贡献度

设备节点可以衡量自身对于设备资源，如 CPU,内存，带宽和存储空间的占用，和事务属性等定时以合约的形式记录到链上。事务属性是为了表示事务的紧急和重要程度。

共识算法会以这些数据为依据，对不同节点的贡献度排名，挑选出区块验证者。即使两个节点的资源贡献完全相同，但是不同的事务属性也会导致两个节点的贡献度不同。

事务（R）	CPU（C）	内存（M）	带宽（B）	存储（D）	重要性（I）
车联网	低	低	低	低	高
Mesh 网络	低	低	中	中	中
CDN	低	中	高	高	低
数据库查询	中	中	中	高	中
科学计算	高	高	中	高	低

表 2 不同事务设备贡献度的比较

在衡量事务重要程度时，同时也考虑边际效应。例如在 CDN 事务中，如果一个节点已经在一定时段内处理了足够多的 CDN 业务，那么之后相同资源的价值会随边际效益而降低，从而降低了节点的贡献度。

用字母 P 来代表设备贡献度，P 是 CPU 使用率(C)、内存使用率(M)、带宽(B)、存储（D）和事务重要性(I)的函数。以标准链中的区块时间作为单位时间。对于特定事务 s，设它的开始时间为t_0^s，当前时间为 t,那么该事务当前的贡献度为 $P_s\left(t^s, t_0^s\right) = \gamma^{t-t_0} P(C,M,B,D,I)$，其中$\gamma$就是由边际效益而产生的衰减指数。如果某设备同时服务于多个事务，那么整个设备在 t 时刻的贡献度则为所有事务的贡献度之和 $P(t) = \sum_{\{s \in S\}} P_s\left(t, t_0^s\right)$.

以上仅是一个简单公式，实际应用中的玄尺会考虑到更多的维度，决定设备的重要性是一个复杂的动态过程。我们以 Mesh 网络的应用为例，设备贡献度还和网络结构有关。在此例子中有两个 Mesh 网络，都具有良好的联通性，里面的设备都有很大的活跃度和贡献度；但是这个两个网络之间却只有一个设备分别于之相连，所有在 Mesh 网络 1 里面的设备和 Mesh 网络 2 里面的设备通信都需要通过此设备。在此情况下，该设备所贡献的物理资源可能没有其他两个

Mesh 网络内部的多，但是它的贡献度却超过了他们，因为它是保持这两个 Mesh 网络联通的必要设备。需要注意的是，Mesh 网络中的设备具有移动性，因此设备的重要性也会随之改变，这就需要玄尺非常智能的动态的去衡量设备的重要性。

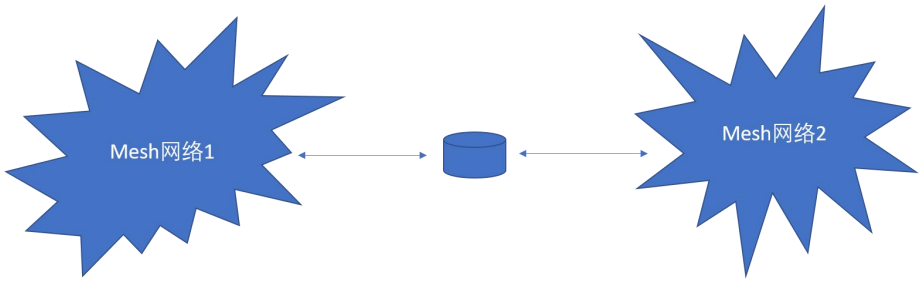

图 4 设备贡献度和网络结构有关

3.1.2 设计目标

共识算法随区块链的发展过程不停的进化，表 3 是对当前流行的共识算法的优缺点和特性比较。标准链的共识算法设计以快速、不可逆、民主性、对雾连网下设备的公平性和普适性为设计目标。

最初的共识算法设计主要以不可逆为目标，当有一个或几个记账人无法记账或者作假时，剩余的记账人仍能在账本上达成共识。比特币和第一代以太坊采用的 PoW (Proof of Work) 工作量证明算法就是一种不可逆的共识算法。PoW 采用竞争性哈希计算来确定记账人，导致了整个生态每次出块时都有大量电能在竞争中被无端消耗，挖矿成本越来越高，速度逐步受限。因此，随着参与挖矿的节点增加，在 PoW 协议下维持生态健康发展的成本将会持续升高。

为了解决 PoW 的弊端，降低记账能耗，提升记账速度，区块链研究者提出了两种不同的解决方案：PoS(Proof of Stake)和 PoI(Proof of Importance)。

PoS 股权证明共识算法采用资产的多寡来取代算力的作用，按照记账者的押金数额来分配获得记账权的概率。这种算法解决了 PoW 的弊端，但放大了资本对记账权概率分配的影响，导致大资本更容易占据生态的话语权，形成寡头垄断，丧失了记账的公平性。PoI(Proof of Importance)重要度证明共识算法引入了账户重要程度的概念，使用账户重要性评分来分配记账权的概率。但是账户重要度经常缺少社区共识。

之后诞生的 DPoS(Delegated Proof of Stake)算法作为 PoS 的改进，由社区通过选举产生记账者。记账者数量的减少，可以让整个共识算法运行速度更快；记账者得到社区的承认，让整个记账过程更民主化，更公平。

共识算法	工作原理	优缺点	应用
PoW	竞争性哈希计算来确定记账	优点：BFT， 不可逆 缺点：消耗大量电能，记账成本高，记账速度慢	比特币，以太坊
PoS	用资产的多寡来取来分配获得记账权的概率	优点：低能耗，速度快，不可逆 缺点：寡头优势，失去公平性	以太坊 Casper
DPoS	选中一小群节点做为代表进行 PoS 记账	优点：速度更快，更民主化 缺点： 没有考虑账户重要性	Bitshare, EoS.io
PoI	使用账户重要性评分来分配记账权的概率	优点：低能耗，速度快，公平 缺点：缺少社区共识，账户重要性 ≠ 设备贡献度	

表 3 目前流行共识算法比较

但是对于标准链和雾联网来讲，上面几种共识算法都有各自的缺陷。在 PoI 中，账户重要度主要通过链上账户的活跃程度和交易数量来判断，无法满足标

准链中对链上链下全面衡量设备贡献度的需求，而且记账者缺乏社区的共识。在 DPoS 中，由于雾联网的体量巨大，设备分布广泛，社区无法观察到所有的设备，社区的共识无法完全体现设备对标准链生态的贡献度。

我们提出了基于账户参与度的 PoP(Proof of Participation)算法，PoP 将 PoI 和 DPoS 的思想结合，既能确保对设备的公平性，又拥有社区的共识。当前 PoP 算法并非按照雾联网的终极目标而设计的，仍是在当前区块链技术之内优化共识算法。标准链是对区块链技术和雾联网需求的联合优化。如前面例子所示，雾联网中设备的重要度和账户重要度有很大的区别，仅仅利用账户重要度来分配记账权并不是最优方案，因此，标准链的共识算法将随着项目的发展和推进，将逐步进化，并在社区形成共识后采用。

3.1.3 PoP 算法设计

3.1.3.1 选举区块生成者

在 PoP 共识机制中，系统将首先选取生态中广泛的具有代表性的账户作为候选账户。选择候选账户时，系统同时考虑多种因素：如，账户的地域分布；账户的业务类型；和此账户关联的设备贡献度。候选账户是具有广泛的代表性，这个方法非常接近于人民代表大会制度，每个人民代表具有相同的投票权力，而他们又是各自的省份和各自行业中的佼佼者。

社区对系统生成的候选账户进行投票，按照所得票数的多少，系统从中按照概率挑选总共 N 个账户作为区块生成者,其中 N 由社区投票决定，并被写入到标准链玄规中（第 1.2.4.1 章节）。候选账户所获得的投票数越多，被选中成为区块生成者的机会就越大。因此最终所选取的区块生成者既具有了广泛的代表

性，又拥有社区的共识。通过社区投票可以剔除那些虽然具有设备贡献力，但是却对社区建设不够活跃的或者恶意破坏标准链生态的账户。

3.1.3.2 区块生成

标准链每隔固定 T 秒产生一个区块，其中 T 由社区投票决定，并被写入到标准链玄规中（第 1.2.4.1 章节）。以每 N 个区块的时间为一个周期。在一个周期的 N 个间隔内，区块生成者以一定的次序依次产生区块。如果其中一个区块生成者没有在规定的时间间隔内生成区块，那么这个时间间隔将被跳过，由下一个区块生成者产生区块，这样两个区块之间的间隔就变为 2T 秒。

在下一个周期内，区块生成者产生区块的次序将被随机切换，使区块生成者之间保持良好的互通性，避免较小概率下区块链的分叉进入到一个固定的发展模式而无法合并。

在两种情况下，社区需要重新投票选举新的区块生成者：

- 系统意识到设备的状态出现了较大的变化，提交了新的候选人到社区。
- 某些区块生成者没有尽到职责，长时间没有生成区块。

3.1.3.3 交易确认

在区块生成者的参与度是 100%的情况下，区块链不会出现任何分叉，一笔交易平均在几秒内就可以得到确认。但是如果出现了软件错误、网络不够顺畅、或者某些区块链生成者恶意而为之而造成分叉，一笔交易就需要至少（2/3*N+1）个区块生成者的确认后才能被保证是不可逆的。

3.2 智能合约

智能合约程序不只是一个可以自动执行的计算机程序：它自己就是一个系统参与者。它对接收到的信息进行回应，它可以接收和储存价值，也可以向外发送信息和价值。这个程序就像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。在图 5 从左到右显示的是一个普通智能合约模型：一段代码（智能合约），被部署在分享的、复制的账本上，它可以维持自己的状态，控制自己的资产和对接收到的外界信息或者资产进行回应。

标准链的智能合约在此基础上一方面引入了设备事件，设备在一定条件下可以触发合约的执行或者状态的改变；另一方面，设备也可以向合约写入回调函数，当合约进入某个特定的状态时通知设备，而设备作出相应的操作。

标准链的智能合约是链上和链下价值流动的渠道，通常用于设备与公链之间，或者设备与设备之间的一些频度不高的交互。以下面两个合约为例：

- 合约 1：当多个设备合作处理一项业务时，互相签署合约保证向项目贡献一定的资源，同时向合约中存入保证金。如果一个设备想退出，设备可以通过事件触发提前通知合约解约请求，合约将保证金还给设备账户；反之，如果合约看到如果其中有一个设备的资源贡献没有达到承诺的目标，可以执行回调函数通知设备，同时没收保证金。
- 合约 2：在标准链设备上面进行商业推广，和推广者签署合约，每个设备拓展一个新用户，从推广者的账户向设备账户转入一定的资金。

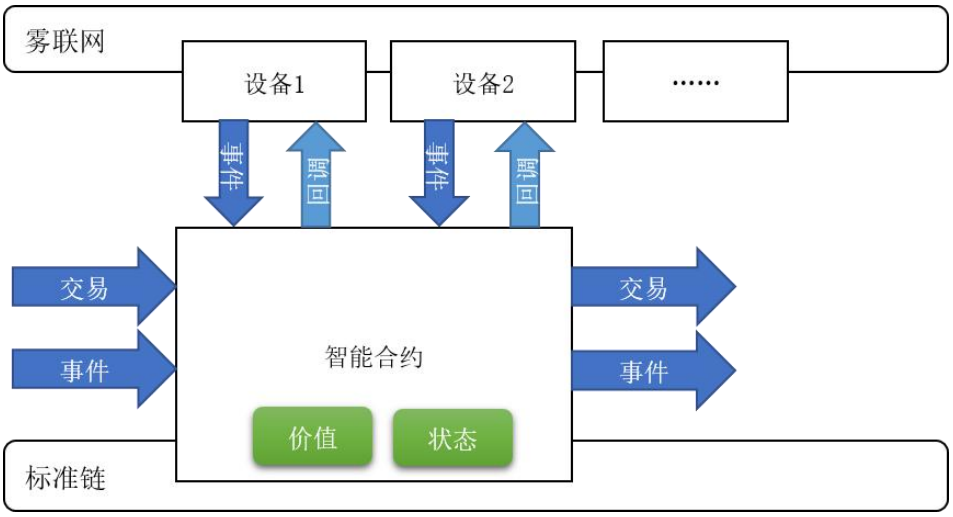

图 5 标准链智能合约引入线下事件

3.3 交易费率机制设计

为了维护区块链生态的健康，区块链中交易的过程一般需要支付一定量的手续费，手续费是对矿工在区块链中处理交易所占用资源的一种补偿。发起交易的账户需要指定自己愿意为这笔交易支付的手续费；而矿工则可以指定自己愿意处理的最低的交易手续费，只有手续费高于这个最低值的交易才会被该矿工处理。矿工会优先打包交易手续费高的交易，如果一笔交易所愿意支付的交易手续费过低，这笔交易可能要等很久才会被打包确认。交易费的设计可以鼓励更加高效的合约代码，减少不必要的计算，避免系统遭受攻击，毕竟攻击者要为他们消耗的资源付出一定的代价。

从经济学的角度来讲，交易的发起者们通过竞价向矿工购买了确认交易的服务，而矿工通过价高者得的原则销售自己的服务。因此我们可以通过经济学中的机制设计理论(Mechanism Design) 来指导矿工费率的设计。简单的讲，经济机制设计理论是研究在自由选择、自愿交换、信息不完全及决策分散化的条件下，设计一套机制(规则或制度)来达到既定目标的理论。

图 6 阐述了矿工在处理交易时的两种不同情况。图中矿工对所收到的交易的价格从高到底排序为 $p_1 > p_2 > \ldots > p_n > \ldots > p_N$，每个区块最多可以容纳 N 笔交易。如(a)所示，矿工设置的费率低于最后一条交易，也即$p_m \leq p_N$. 这样所有交易都被打包进区块，而总的交易费为$\sum_{\{i=1\}}^{N} p_i$. 在(b)里面，矿工设置的费率仅低于前 n 个交易，因此只有 n 个交易被打包进了区块，而总的交易费为$\sum_{\{i=1\}}^{n} p_i$.

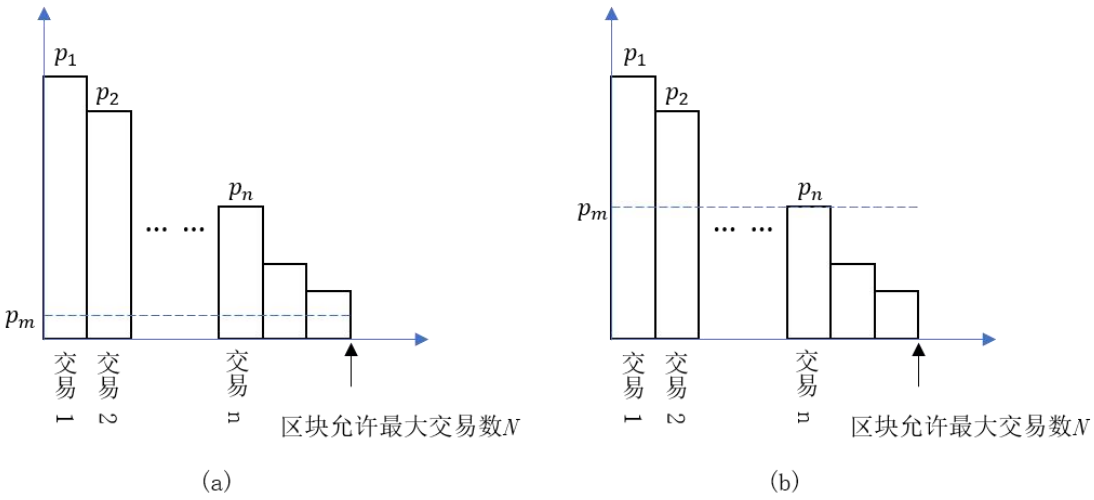

图 6 交易费率机制设计

在这样的设置里面，一个交易的发起者最终支付给矿工的交易费是和他的竞价价格一样的：如果他的出价是 p,最终交易被确认后，必须支付给矿工 p 的交易费。这种方式在竞价理论里面被称为“第一价格拍卖(The first-price auction)”。第一价格拍卖虽然简单易于理解，但是考虑到不同买家（也即交易发起者）之间的博弈，一个买家的出价很可能背离他对标的（也即交易的确认）的真实估价，出价最高的买家并非是真正估价最高的人，因此最终的分配从社会价值上考虑并非是最优的。

在机制设计理论里面，这个问题可以通过“第二价格拍卖(The second-price auction”来解决，一个交易的发起者最终支付给矿工的交易费并非他的

竞价价格 p,而是取竞价未成功的所有交易者中最高价格和矿工保留价格两者之间的较大值。在图 6 中，显然所有被确认交易最终的价格是矿工所提出的价格 p_m. 通过在交易费率机制设计中引入第二价格拍卖，可以让交易发起者的竞价不会背离交易确认的真正价值，在整个区块链中交易确认的分配达到社会化的最优。

3.4 新的加密接口和访问权限

传统区块链上所有的交易都被记录在公链上，所有的用户都可以查询到每一笔交易的来龙去脉，这种机制确保了交易的公开和透明，对金融应用更是极大的推进。但是在标准链和雾联网的应用中，并非所有的数据都是公开的，某些数据属于用户个人所有。这也是我们把物联网改变成雾连网的初衷之一，把属于用户的数据从服务提供商归还给用户。

以此为出发点，我们设计了全新的用户访问权限。在标准链设备中，每个用户的数据都用自己的密钥加密存放，同时受标准链访问权限的保护，在用户没有授权的情况下，其他人无法破解。而用户对服务商或其他用户的每次授权都被公开保存在标准链上，这样可以用标准链的不可逆特性记录他人对用户数据的访问，确保安全性。

数据所有者在标准链上授权他人访问自己的数据主要分两步：第一步，数据所有者发送一个交易，里面包含了数据的 ID（数据摘要的哈希值），把当前已有数据注册到标准链上；第二步，如果数据所有者要把数据授权分享给他人，他再发送一个交易，交易里面包括了数据流的 ID 和用被分享人的公钥地址。

当一个设备获取数据请求时，会先从标准链上通过请求人的地址获取授权，

如果数据所有者没有把授权记录在标准链上，则把请求拒绝；反之则接收请求。

3.5 第三方工具集成

标准链是为处理雾联网的异构业务而优化设计。为了能够处理高吞吐量和低时延的业务，标准链还需要借助于其他的软件和开发工具。

3.5.1 分布式文件系统 IPFS

IPFS（InterPlanetary File System，星际文件系统）是永久的、去中心化保存和共享文件的方法，这是一种内容可寻址、版本化、点对点超媒体的分布式文件协议。

内容可寻址：通过文件内容生成唯一哈希值来标识文件，而不是通过文件保存位置来标识。相同内容的文件在系统中只会存在一份，节约存储空间。

版本化：可追溯文件修改历史

点对点超媒体：P2P 保存各种各样类型的数据

可以把 IPFS 想象成所有文件数据是在同一个 BitTorrent 群并且通过同一个 Git 仓库存取。

总之，它集一些成功系统如分布式哈希表、BitTorrent、Git、自认证文件系统等的优势于一身。

标准链将在 IPFS 开源的基础上进行改进，将加入安全性、去中心化、抗灭失性等特征。

3.5.2 分布式数据库 NoSQL

分布式数据库和区块链的特性比较：

需求	区块链	分布式数据库
高吞吐量	-	√
低时延	-	√
快速查询	-	√
权限多样化	-	√
分布式控制	√	-
操作不可逆	√	-
支持资产创建和转移	√	-

为了能让应用能够用传统的分布式数据库的方式访问数据，让标准链同时具有区块链和分布式数据库技术的优点，在标准链上建立对分布式数据库 NoSQL 的支持，使标准链在数据业务上具有可扩展性，能够支持高速的并发数据库读写，同时在链上记录用户行为，保持数据库数据的不可逆。

3.5.3 闪电网络

闪电网络是为了区块链技术适应海量微支付场景而设计。通过为交易双方建立一个微支付通道网络，双方大量的支付都可以在链外直接多次、高频、双向地通过轧差方式实现瞬间确认。当交易结果需要结算时，再把最终结果提交到区块链确认，以此来解决公有链网络的扩展性问题。理论上闪电网络技术可以实现每秒百万笔的转账。闪电网络在比特币和以太坊上都已经有概念性的验证。

不光在金融领域，即使在雾连网领域也存在海量微小交易的场景。如前所述的车辆网应用场景，几辆相邻的汽车需要以极短的时延快速的多次交换相互

信息来判断周边环境，实现安全驾驶功能。

同时，在标准链上运行的 DeOSes，由于 DeOSes 上的 Dapps 有大量的跨链交易产生，也需要闪电网络来支持此类碎片化的交易。

因此，标准链把闪电网络当做区块链的基础设施予以实现，并且提供足够的灵活性设计。任何第三方开发者，都可以在标准链上利用闪电网络的基础服务，做高频交易场景的应用开发。

3.5.4 开发者工具

为了支持标准链开发者，标准链开发组将提供丰富的开发者工具，包括独立的智能合约开发 IDE，区块浏览器，各种流行IDE 的插件支持，调试器，模拟器，智能合约形式化验证工具，各种高级语言的后台 SDK，移动端 SDK 等。同时在标准链社区以讲座和讨论的形式推广开发者工具。

3.6 硬件开发及开源

在标准链和雾联网中，因为其彻底的开放性，数据的安全显的尤为重要。链上的数据安全可以通过标准链的共识机制来保证，而链下的数据安全则要通过硬件的重新设计和加密算法来得以确保。

一个能安全在标准链中使用的硬件设备必须包括:1）安全的 P2P 的通信机制； 2）安全的电子钱包存储空间； 3）入侵检测系统； 4）篡改证据记录等。目前市场上一般的硬件产品显然无法达到这一要求。如在标准链团队正在开发的一款标准链智能手机中，即在普通智能手机硬件之上添加了安全沙盒，具有极高的安全性。标准链用户的电子钱包即存放在安全沙盒之中。

标准链团队已有多年的通讯协议及芯片设计、智能网关、智能路由器等硬件的开发经验。在标准链的生态建设中，将快速的利用我们的优势开发出支持标准链协议并对其产生贡献度的智能硬件。在稳定的测试一段时间后，开源我们的硬件设计，推出参考设计，可以让第三方开发者根据自身需要定制标准链硬件，实现价值最大化。同时开源也可以使标准链的节点快速增长，促使生态发展。

4 标准链团队

4.1 标准链团队

杨嗣超

雾联网区块链科技核心创新及应用开发者，标准链 core 团队发起人；

美国伊利诺伊大学数学系硕士和电子与电气工程系博士；美国自然科学基金课题研究者；博士课题为分布式网络中的资源分配和优化。

曾担任世界领先的无线通信芯片和服务提供商高通公司（NSQ：QCOM）高级主管工程师，参与了第四代移动通信 LTE 芯片的设计和开发，是高通公司在目前无线通信领域保持领先地位的重要贡献者之一。 并领导了高通公司在车联网项目的研究，在分布式网络、车载通信、用户行为感知和智慧城市等方面拥有多项发明专利；其中基于 DSRC 通信的行人安全系统（与本田公司合作开发）为世界首创。

麻省理工大学、斯坦福大学、康乃尔大学和英国剑桥大学等地的世界知名学者多次引用杨博士论文(Google scholar 显示目前总引用次数超过 500 多次)；Mathematics of Operations Research, IEEE Transaction on Networking,

Games and Economics Behavior 等国际知名权威科学杂志审稿人；

曾在美国新泽西州立大学(Rutgers University)担任客座教授。

金海龙

标准链创始发起人，雾联网区块链实践者；

国内第一家第三方支付平台创始人；

中国电子商务协会中国支付行业专家委员会成员；

“通用搜索”关键词精准营销软件创始人，装机量超过 3000 万台，同时在线超过 600 万。

浙江搜道网络技术有限公司创始人，全国最大的美女网红机构，年交易额超过 5 亿。

WiFiSONG 创始人，公司在智能 WiFi、iBeacon 等领域具备领先优势影响力。

Joe Thong　标准链联合创始人

马来西亚人，工商管理硕士；

Popify、Twinova、雷神资本联合创始人；

三星，SAP，Total（道达尔），斐济旅游局等世界 500 强企业合作伙伴；

单志浩　　标准链联合发起人

中国第一部互联网地方性法规撰写者；

原杭州互联网安全协会秘书长；

密码学与加密技术反向研究者与实践者；

4.2 专家顾问团队

MICAEL SAUNDERS　迈克尔.桑德斯教授：首席数学家

斯坦福大学终身教授、数学家、世界算法专家

桑德斯教授目前是SIAM(工业与应用数学学会)院士；斯坦福大学发明名人堂成员；新西兰皇家学会院士；曾获得包括“SIAM Linear Algebra Prize”等众多奖项。

在斯坦福大学管理科学与工程系/运筹学/系统优化实验室/计算与数学工程/科学计算与计算科学等学科研究与教授，特别是在数值优化、数值线性代数、线性/非线性规划、稀疏矩阵、迭代求解器、约束优化、稀疏线性方程组、稀疏最小二乘法的算法设计与实现，系统生物学中的多尺度优化问题等方面的研究处于世界领先水平。

刘亦浩：首席金融顾问

诺亚控股（NYSE：NOAH）战略基金合伙人，诺亚财富香港CEO；

原世界最大证券交易所——纽约证券交易所北京代表处首席代表，任职期间辅助阿里巴巴（NYSE：BABA）在纽交所上市；

曾任世界最著名的证券零售商和投资银行——美林证券(Merrill Lynch ，NYSE：MER, TYO: 8675)亚太区首席运营官及中国区核心领导。

潘越飞

锌财经创始人。

wemedia联合创始人

原猎豹移动全球内容总监、搜狐科技主编。

4.3 战略投资人

孔剑平

长三角人工智能实验室发起人

中国区块链应用研究中心发起人

恒通云(838316)董事长

嘉楠耘智联席董事长

傅政军

香港上市公司天鸽互动（1980.HK）董事会主席；

中国视频直播第一人，9158 创始人；

2011 年起任金华市六届政协委员；

获得 2012 年度“文化新浙商”；

2014 年获得由《创业家》杂志社主办的“2014 年度十大创业家”；

2017 年，受邀出任“浙商经济发展理事会主席团副主席”。

李成博士

原华欧创投副总裁， 2015 年浙江省股权投资行业年度优秀投资人。

董源

天使合伙人社群创始人

浙商杂志 2015 年杭州十大天使投资人

2016 年杭州市“十佳创业导师”荣誉称号

徐张生

杭州微巴信息技术有限公司创始人，国内首批微信公众平台开发先行者；

曾与孙海涛共同创建 E 都市、房途网、租房宝等互联网项目。

钱永忠

钱先生是互联网及通信领域的专家，先后创办及投资多家公司。

第二办公室、印助理、客家行创始人

名优金融、木梯商旅等联合创始人。

5 标准链路线图

2018 年 1、2 月　　ERC20 代币发行，CZR 登录交易所

2018Q2　　PoP 共识机制基本完成，标准链代码开源、主网上线

2018Q2　　全球首款支持 PoP 共识机制的区块链网关（雾联网节点）发布

2018Q2　　发布标准链 API

2018Q3　　全球标准链开发者社区对外正式开放，雾联网联盟启动

2018Q4　　发布标准链智能手机（区块链手机），并开始预售

2019　雾联网协议 V1.0 发布

2020　首款雾联网芯片出现并开源

2021~ 低成本微功耗雾联网适配规范及适配器出现，人类社会全面进入雾联网时代

6 标准币：CZR

6.1 CZR 功能

在标准链上，所有的贡献均会获得 CZR 激励，同时，所有的对于资源的使用，都需要消耗 CZR。

CZR 激励由共识机制根据贡献权重进行分配，而消耗 CZR 则由对于资源的具体使用度来衡量。

CZR 是衡量价值传递的一个标准，同时也是建立在标准链上众多 DOSes 及 Dapps 的基础资产。

6.2 CZR 分配方案

CZR 总量为 1,618,033,988Є。

其中：

面向早期投资人及私募 40%

创始团队、开发团队　10%

社区激励、全球推广、合作激励预留 20%

POP 激励预留（即传统区块链项目中的“矿池”）30%

6.3 CZR 发行模式

CZR 初期在以太坊以 ERC20 Token 形式发放，在主网上线后提供互兑方案。

用户可以通过参与私募、交易所购买、场外转让等方式获得 CZR。

私募期间 CZR 兑换比例：1ETH=6000CZR

6.4 团队 CZR 合约

创始团队、开发团队分配的 CZR 在每次分配后分三年逐步投放市场，规则如下：

首次释放：25%，

一年后解锁：25%，

二年后解锁：25%，

三年后解锁剩余部分：25%。

其余开发者社区、全球推广、合作激励等所获得的激励，在每次获得后分四次投放市场，每季度释放 25%

6.5 私募用途

主要用途：

全职工作人员报酬；

市场推广支出；

基于生态建设的再投资。