Beacon: A Peer-to-Peer Data Stream Grid

烽火: 一种点对点的数据流网格

Urna Semper *

2019年9月27日

非公开初稿 中文版 0.9

本白皮书仅供参考，不构成要约或任何形式的投资建议。

摘要.

烽火Beacon是一种大规模的去中心化数据流服务网格，可称之为基于发布/订阅模式的全球“超级计算机总线”，为种类繁多、规模庞大的设备、机器、应用、服务、系统、平台等，提供数据传送和控制逻辑的一种安全的通用方式。它由分散在全球不同区域可自由加入或退出的云节点、雾节点组成，基于高扩展的委托权益共识机制、无权限门槛设置的分布式分类帐本技术，针对参与各方提供多种激励(如节点运营、数据块交换、转发量工作证明、网络扩张等)机制的一种新经济运作模式，也是面向未来普适计算[22]环境的一种安全的全球性基础型公共服务设施。与聚焦片段化结果(实质是快照机制，例如提供增删改功能的数据库)的静态范式不同，它是聚焦完整过程(时间线机制，例如仅提供追加功能的区块链)的动态范式的某种低延迟准实时系统。

1. 背景

2008年，中本聪发布的比特币白皮书[1]，提出了一种不依赖信任的电子交易系统，这项发明带来了：①不依赖可信任第三方，解决双重支付问题的方案；②基于哈希计算的工作量证明PoW[23]链，即“最长链竞争”的共识机制[25]；③不可更改记录的后被世人称为“区块链”的分布式公开分类账本技术；④“无中生有”称为挖矿的经济激励/铸币机制；⑤基于极简架构，节点可自由参与无需授权的一种点对点网络。

2014年，最初由Juan Benet设计的星际文件系统IPFS[15]，它是：①采用Git仓库分布式存储的一个Bittorrent集群；②结合了分布式哈希表，带激励机制的块交换BitSwap协议和自我认证命名空间，采用广义Merkle DAG数据结构构建的一种内容可寻址、版本化、点对点的超媒体协议；③期待成为让WEB更快、更安全、更开放的，无单点故障、无需信任、去中心化保存、永久的一种点对点文件共享网络。

在比特币基础上的加密货币，如达世币[2]，除了添加提高可互换性的匿名支付，不依赖中心权威的即时支付功能外，最大亮点在于与比特币只奖励矿工工作量证明的哈希计算不同，它添加了双层激励制次级网络--也称为主节点网络。主节点是运行全节点服务的有着显著流量带宽、大存储空间的高可用性服务器。在抵押一定数量币的基础上，为全网的客户端提供一定的服务，在很大程度上可缩短网络广播的时间，提升网络健康度、网络相应给予币奖励。可以说比特币引入“挖矿”业，达世币引入了“节点运营”业，这两者都是新经济生态模式的重大创新。（这里重点强调一下，有些号称“主节点”的山寨币项目有可能是骗局。）

基于零知识工作量证明的ZEN币[3]，提出基本和超级两种主节点激励，后者需确保节点之间的所有网络通信被加密，并提供基于证书的加密连接，从而进一步拓宽了主节点类型和使用用途。

同样基于零知识工作量证明的ZEL币[4]，其ZelNode[5]依据服务器的CPU、内存、存储、网络带宽、服务有效性等方面的不同基准要求、和不同抵押币数量的三种类型节点[6]，从而引来一种新型计算力资源投资模式。这些节点不仅用于区块链账本，还可进一步提供去中心化的各种服务，如去中心化身份、去中心化交易服务等。

不同于以上基于工作量证明(PoW)的主节点币[2][3][4]，普维币PIVX[7]，是采用零币股权证明(zPoS)共识的主节点币，此外与其它币不同的一个地方，就是在交易费用花费的约束下，可以动态地校准硬币供应量。

以太坊[8]作为智能合约和去中心化的应用平台，引发了代币化服务浪潮，一些项目认为中心化云服务将会逐渐被代币化、去中心化的解决方案取代。如: Golem[9]立足于利用用户的闲置机器资源，构建一个去中心化的廉价算力市场，提供诸如CGI渲染、科学计算、机器学习等方面的计算服务，同时利用以太坊的支付转账系统，实现算力买家(需求方)、卖家(供应商)、软件开发者之间的直接支付；SONM[10]利用Docker容器技术，提供IaaS/PaaS栈服务，并利用其代币实现基于智能合约的去中心化计算租赁市场；Streamr[11] 是基于以太坊平台[8]、有可能采用IPFS[15]、BigChainDB[16]等作为其事件存储组件、借助于Golem[9]作为其算力资源提供商，结合Streamr自有技术栈(智能合约、对等网络、数据市场、事件处理和分析引擎、编辑器)，为消息传递和事件处

* c8d0e24ffe41a39f350a54c2a4876b637d282472e1f7611880ec981bf573fb46
za13fcph4zr4rptwdl6nnyuvx57w9w5whc0tzv3k2r88td8le9c4zkrz3s682tfwf67ky4uxsfkm8h(ZEL)
0x8f7b89d8f4d5a3e3402049d05374da7576123d55 (ETH)
1LcVX9m6TUfbsGuXu8knbBfJKBNqPBVw4T (BTC)

理提供去中心化解决方案，期待达到如Golem替代Azure Virtual Machine，IPFS替代Azure Blob Storage，Streamr替代Azure Event Hub, Azure Stream Analytics等平台那样的效果。

Blockstack[12]作为一个去中心化计算网络和App生态系统，认为更强劲的客户端设备、边缘计算和全球连接将会减少对中心化平台的依赖，而云计算将会朝着去中心化计算演进，这是计算机工业自从大型机转向桌面电脑以来最重大的技术变迁。它通过Stacks区块链，一方面扩展安全、隐私的去中心化应用，它们在客户端运行绝大部分业务逻辑和数据处理，而不像传统Web应用是在中心化服务器上。Blockstack希望通过这种端对端设计将复杂性推送到系统边界(用户设备和用户控制的存储)，而另一方面激励开发者在网络上开发多种应用程序。

物联网是一个价值8000亿美元的产业，在线连接设备超过84亿，预计到2021年，支出预算将达到1.4万亿美元[13]。而物联网跟区块链的结合催生了一些有趣项目，如Helium[14]定位于一个去中心化的无线网络，它期望使得世界上任何地方的设备能无线连接到互联网并自己进行地理定位，而无需耗电的卫星定位硬件或昂贵的蜂窝计划。Helium热点提供无线覆盖服务，并充当生产Helium代币的矿机。通过设置热点，为低功耗物联网设备提供连接。利用区块链，激励一个覆盖供给者和消费者之间的双边市场。

至比特币问世以来，它从不同角度启发后来者，催生了越来越多的新技术和应用。这些角度大致可分为：①以加密货币为基础的电子交易或去中心化金融系统；②不断改进或革新的加密算法、隐私保护技术；③推陈出新的共识机制或算法；④不可篡改的分布式分类账本技术；⑤不同于链状结构的技术，如DAG；⑥以区块链概念为基础的各种商业项目；⑦新型的经济激励机制或投资模式；⑧去中心化的无需授权的点对点网络；⑨去中心化的应用/系统/平台等；⑩区块链与物联网、边缘计算、机器学习等其它领域的融合。

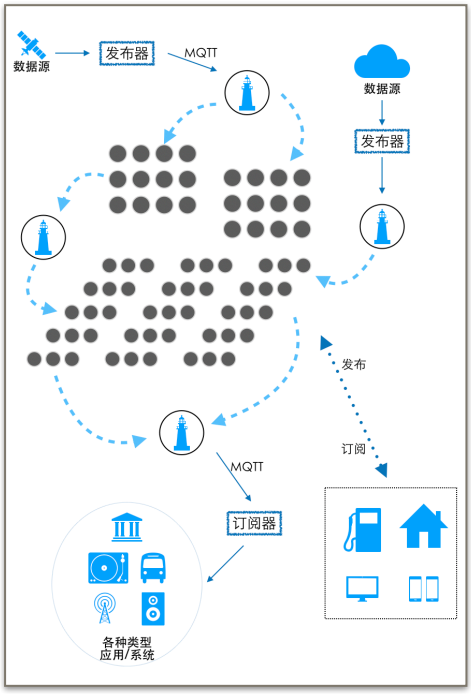
现在互联网传输文件的事实标准HTTP协议，由于与浏览器结合，拥有巨大的技术和社会影响力，但它并没有采用最近15年发明的数十种先进的文件分发技术。而旨在提升Web的IPFS[15]在某些领域，其影响力正在不断提升，也在不断启发后来者持续创新。

2. 重新思考

在新技术浪潮或变革来临之际，一方面，我们认为内置激励机制的去中心化的网络服务或计算范式将会是传统中心化网络服务或计算范式有力的竞争者，必定在未来发挥越来越重要的影响力；另一方面，我们认为“时间”是物理世界中的核心要素，基于时间序列机制的数据流网格(DSG)服务将会更容易成为普适计算[22]环境中的一个核心支撑。

我们观察基于中心化传统型的数据流网络(DSN)服务，如PubNub[17]公司提供的在线服务，已在很多场景下发挥了巨大作用：①聊天与社交；②实时在线消息推送；③远程系统日志采集；④金融行情数据流；⑤多人游戏交流与协作；⑥健康与安全领域；⑦家居自动化；⑧供应链应用；⑨跨组织的实时协作、审计、跟踪等方面；⑩IoT/IoV/IoE等领域的设备监测、消息控制、持续性测试等方面。此外，可从网站PubNub.com显示的月活跃单一设备达3.3亿台，月交易数达2万亿次来看，其相应的市场潜力可见一斑。

当我们重新思考数据流网络DSN时，一个新的构想：“烽火网格”，便由此孕育而生。它是一个无需额外授权，可随时加入退出，且在不可信的环境下依赖权益证明PoS[24]的共识机制[24]，提供多方位的经济激励尤其是云与边缘的节点奖励，实现基于主题的发布/订阅模型的去中心化点对点数据流网格。它本质上是基于互联网的一种覆盖网络，同时具有对等网络、开放异构、虚拟资源(如数据流)共享、多链路冗余传递和存储等网格计算技术[18]的众多特点，因而我们把它归类为一种数据流网格服务。（请参见图一）



图一：数据流网格服务示意图

本白皮书并没有描述完整的相关细节，有些内容也会随着相关编写或研发的进度而发生一些变化。

作为后来者，我们认为可以重新定义数据流网络DSN：

❖比特币通过激励“矿工”的方式，将物理世界的电力等代价注入到加密货币网络中，形成其背后“价值存储”的信用背书。采用“节点运营”模式，可将服务器算力、网络带宽、电力等可见代价注入到网络中，为网络提供起始的源动力。成功的网络，可以集聚全球化的投资/投机资源，催

生一个诸如挖矿的一个产业，形成拥有成千上万个节点，其数量规模远超于传统的中心化组织运作的网络。这在传统模式下，对于小型的初创团队来说是难于想象的。能否充分利用好这种全新的投资运营生态，将是点对点数据流网络/网格能否成功的一大要素。

❖作为构建在互联网之上的覆盖网络[34]，一种数据流网格，一种高效的生产力工具，它的真正价值体现来自于其使用成本的大幅度降低、大量应用场景需求(如上文提及的多种DSN应用场景)的满足、更高的安全性保障、更好的隐私保护措施、数据拥有权的回归、更高效的跨组织协作赋能、基于全球化的资源配置优化、超大规模的服务能力、以及超精细化的服务运营。而实现这些价值的核心要素，就是分散在全球不同计算中心的云节点，遍布世界各个角落的边缘节点，随处可见的终端设备与应用，支持不同级别的信道设计，实现纳米支付、微支付的高性能可扩展分布式分类账本，绿色环保的共识机制与极简的网络架构，超级灵活自由的竞争市场(如节点经营)与生态系统等。

❖虽然比特币的代码一直在优化升级，但总体来说，它是属于一经上线，无需外界干预即可自我运转的系统，基本符合物理学第一性原理特点：简单、美、普适。这是应当秉承的核心哲学理念。由此，我们主张烽火网格采用一体化而非庞杂组件支撑的极简轻量化架构设计理念，如将接口、加密、共识、路由、分发、存储、信道、协议等精简化后紧耦合融为一体，完全聚焦于最核心的普适功能(针对消息与控制这类数据流的汇聚、存储、分发等)满足各种场景需求，使之具备普适计算[22]雏形的一个关键组件，这个雏形如果比作一台巨大的“超级服务器”，那么烽火网格将是一个巨大的“安全的超级总线”的关键存在。而在万物互联(IoE[19])的概念中，它将扮演极简主义的轻量级组件角色。我们期望这个规模庞大的轻量级组件，依赖于开放协议(如CoAP[20]、MQTT[21])，能实现其特定的普适计算功能。

3. 简要阐述

跟Golem[9]、SONM[10]、Blockstack[12]这类去中心化计算网络不同，烽火是一个有特定目标的去中心化网络，因而不会采用容器/虚拟机这类能扩展系统可编程性、应用灵活性等方面的技术，从技术角度上来看属于能提供大规模服务能力的高性能、高扩展、普适化的垂直性轻量级融合系统，而非通用化计算/服务平台。

3.1.分布式分类账本

◉采用基于权益质押证明PoS[24]的高扩展分布式分类账本技术，其负责：①铸造新币；②烽火云节点或烽火边缘节点的运营奖励；③烽火代理转发量证明(PoF: Proof-of-Forward)的奖励；④诸如提供方/消费方/推荐方/先行者奖励等；⑤多种类型的烽火币支付，包括纳米支付、微支付、小额支付等；注：相关细节请看下文段落

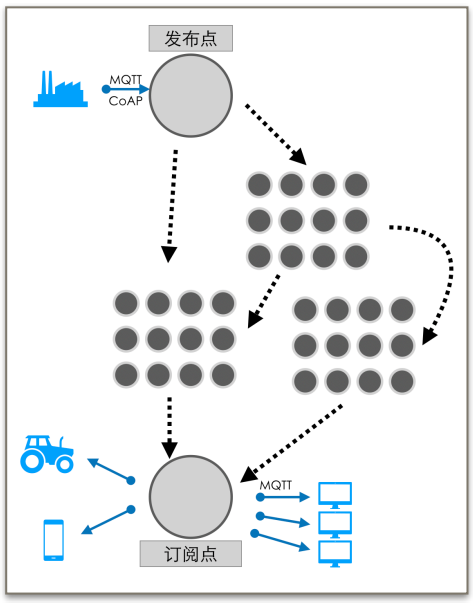
◉烽火权益质押证明PoS[24]分类账本，采用图技术，而不是链技术，使得它拥有高扩展，高吞吐的能力，同时它也构成了烽火网络的底层支撑。无论是节点代理中的数据流转发机制，还是时序数据流存储机制中涉及的数据块交换，诸如这种节点间“交易”行为，都依赖于分布式分类账本机制的支撑。（请参见图四）

◉采用PoS而不是PoW，是基于两个方面考量：①重点强调计算机服务算力取代Hash算力的代价注入；②避免Hash算力成本对于币价格的影响因素，从而凸显其网格服务价值对于币价格的影响力；③鼓励节点而非矿机的大规模扩张；

◉烽火网格是通用基础型应用类项目，它不是对外公开的区块链平台，也不是主打加密货币的交易系统，因而权益质押证明PoS[24]分类账本，主要以纳米支付、微支付、小额支付为主体，采用快速确认机制，同时设置大额转账机制。

◉秉承极简轻量化架构设计理念，烽火与大多数区块链项目不同，将不支持图灵完备的智能合约(虚拟机和合约语言)，选择采用硬编码方式实现与支付相关的内置合约逻辑。注：除非随着项目的进程发现智能合约是必须的功能选项才考虑添加

3.2.数据流代理的核心机制

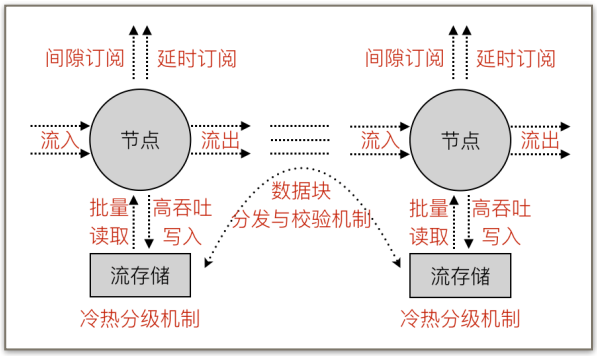


图二：发布/订阅模式示意图

◉采用基于主题的发布/订阅机制，支持开放协议(MQTT、CoAP等)，那样支持此类协议的编程语言、开发包、应用、微服务、设备与系统，均可连接到“超级总

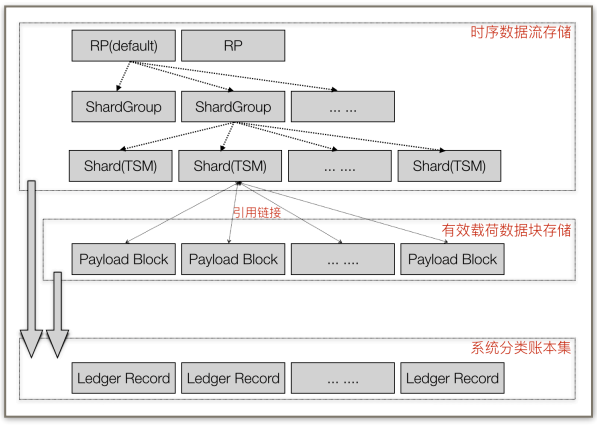
线”服务上，类似访问传统的消息代理服务或计算机集群系统。（请参见图二）

◉发布/订阅机制可以支持一对一(如私聊、分析管道)，一对多(如新闻渠道、股票行情、消息推送)，多对一(数据采集、日志监控、投票)，多对多(群聊、多人游戏)的使用场景[11]。



图三：延时订阅与数据块分发示意图

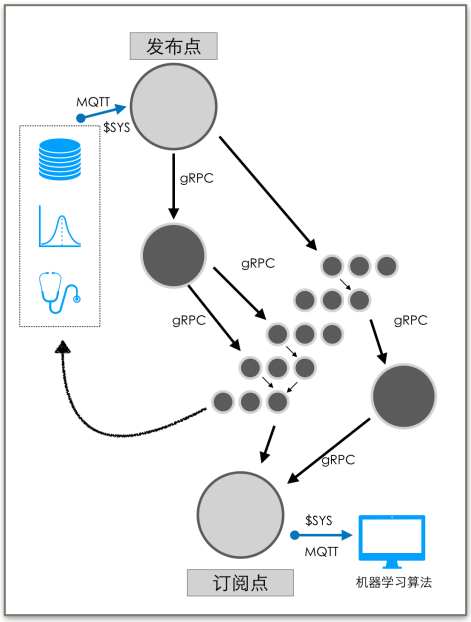
◉数据流发布并不意味着一定需要客户端订阅，也就是说存在延时多重备份的场景需求[11]。当节点接受发布的数据流时，不同于传统的单点消息代理服务或某个集群只负责消息的分发，它首先将数据流保存到本节点，然后伺机通过数据块分发到其它节点备份，是本网格天然的亲密选项。这是立即保存比实时分发的代价要小的性质决定的。实时分发消息，会消耗更多的计算和带宽资源，因而将优先处理此类需求，而延后无订阅的冗余备份。（请参见图三）



图四：时序数据流存储结构示意图

◉基于时间序列的轻量级数据流存储模型，其：①采用类似于IPFS[15]的设计原理，将一定时间间隔或容量大小的数据块分散在不同的节点中(与数据流直接转发不同，这是一种延时的数据块分发机制)，但实现需兼顾轻量化的设计要求；②拥有默认的失效时长，一种数据保留策略的一部分，类似于InfluxDB[52] 的Retention Policy(RP)，但可通过支付一定量的币作为代价，即可延长相关存储的失效时间；③采用类似于InfluxDB[52]的TSM引擎机制，作为存储引擎实现设计；④流数据中的非公开有效载荷将先用数据源拥有者的私钥加密签名后存储与转发，网格系统无法感知具体负载内容，但数据流的元信息可按时间戳进行查询、下载等操作；⑤不同于中心化服务，利用加密技术，发布者拥有完整的数据所有权；⑥流数据存储会保留一些元数据，如分发时长、网络延时、数据包大小等，有利于网络性能的进一步优化或分析；⑦采用冷热数据分级机制，而冷数据将会通过数据块交换协议，进行分发与传播；（请参见图三、图四）

◉烽火网格核心消息传播，将通过诸如grpc机制完成。但属于业务层的流数据，比如烽火节点日志流，烽火节点的CPU等资源运行数据流，就是一序列$SYS主题的发布者和消费者。节点经营者可以观察和分析相关节点运行状况。开发者也可以针对与系统性能、资源消耗相关的数据，进行分析。未来的机器学习算法，可作为消费者，也可以利用这些数据进行异常侦测，及时发现网络攻击等。（请参见图五）

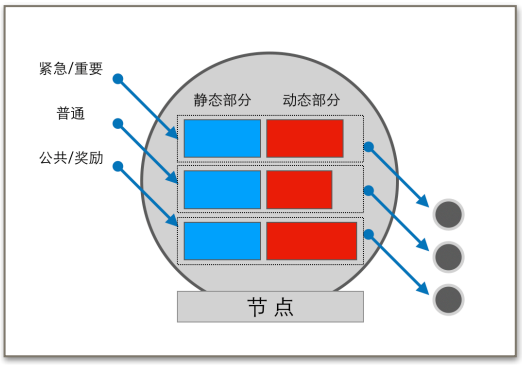


图五：$SYS主题示意图

◉烽火代理直接内置分紧急/重要、普通、公共/奖励三种等级的渠道，分别按一定比例占有静态部分的CPU与内存资源，动态部分的CPU与内存资源，将根据动态阈值(类似于比特币挖矿中的难度系数)进行调节，分配给不同等级的渠道。这三种等级渠道的分配，消费者和供给者均需要支付不同量的烽火币。但公共等级可采用纳米级支付，其代价接近于零，相当于互联网公共服务中的“免费”模式，其它等级无论是发布方还是订阅方，都属

于付费模式，其中订阅方付费，将按照一定比例支付给烽火参与方(如烽火节点)做为转发奖励和发布方。三渠道分离设计目的，是确保渠道能独立运作，互不干扰影响。不同于按支付高低来确定服务优先级的设计方式，它能保障各种支付代价都能有机会得到对应等级的服务响应。

◉针对紧急/重要，普通这两级渠道，恶意发布者很难发动攻击，试图消耗节点资源，因为对方需要支付使用成本(按市场价格支付)，对烽火网格来说，它就是正常的数据流发布者。（请参见图六）



图六：独立分级通道示意图

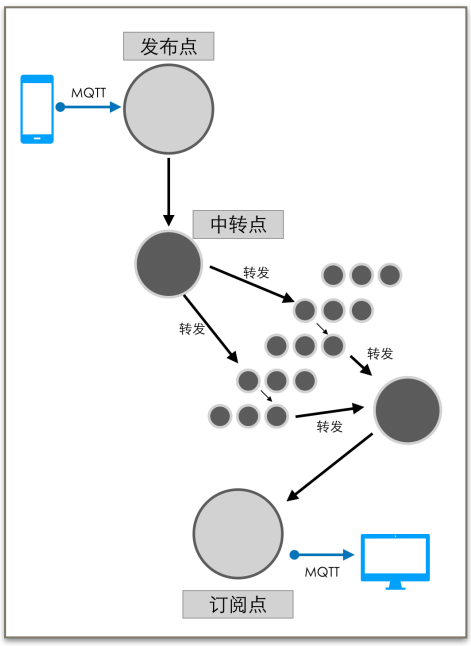
◉公共/奖励这个等级，基于超低价或额外奖励的情况，会有恶意发布者和恶意订阅者利用无价值有效载荷消耗烽火节点资源(CPU、内存、流量、存储等)或骗取奖励。①可通过延迟奖励发放或设置时间锁定机制，或者订阅者产生消费支付后，发放或解锁；②根据发布者/订阅者的地址，设置动态的限定阈值，限定同一公开地址的连接数、设备数、数据流时长与容量大小。

3.3.节点服务

◉烽火节点特指类似于ZelNode或达世币主节点的能够通过节点运营获取额外奖励的那类，而不是烽火股权质押证明PoS节点，前者拥有具体规格限制和在线可用性要求，后者没有这类硬性规定。

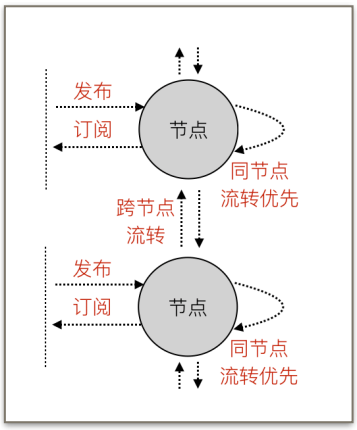
◉烽火节点上拥有完整的分类账本记录集，也对外提供账本数据同步服务，尤其是分块的二进制账本数据，缩短新加入节点的分类账本记录集同步时间和所需的网络流量。

◉烽火节点代理转发量证明(PoF: Proof-of-Forward)，是在数据流路由路径上，其不包括发布节点和消费节点的节点，属于被动选中(类似于随机，不受发布者和消费者影响)，避免恶意节点、恶意发布方、恶意订阅方的作弊行为。不同于工作量证明PoW，这类节点不参与共识机制，主要作为烽火节点奖励的组成部分。当然不排除作为随机抽样过程中的加权因子，降低新加入节点被抽中的概率，延迟新节点攻击，这种情况只出现在共识节点与服务节点一体时。（请参见图七）



图七：数据流转发路径示意图

◉基于同一烽火节点的发布和订阅，将优先处理，这对于边缘节点或与其它节点通信延时大的节点，性能表现尤为明显。（请参见图八）



图八：优先机制示意图

◉烽火网格各类节点需要报告有效性，一种特殊Ping机制，只有符合抽样条件阈值设置，才能获得对应奖励。而这运作状况数据，通过匿名化手段后，将会存储到网格中，为网格性能提升提供数据支撑。

◉烽火云节点特指网络中，能够提供代理接入、存储与分发等服务，这些节点主要部署在云上，如云服务提供商提供的云主机，能够满足特定规格要求，如CPU内核数量、内存大小、磁盘容量大小、网络带宽要求、及持续在线服务要求等，这些节点构成烽火网格服务的主体

骨干。

◉烽火雾/边缘节点特制网络中，普通企业或家庭用户，利用企业或家庭带宽，在普通计算机或单板计算机上，或者租用Golem[9]、SONM[10]这类去中心化雾服务的虚拟主机，能够为周边设备与应用提供代理接入、存储与分发(连接云节点)等服务。这些节点通过抵押一定数量币后，同烽火云节点一起，参与节点激励计划。与这些节点接入的应用、设备在边缘部分，构成了一个个微中心化的客户端/服务器模式的网络，让浏览器、客户端应用透明化的访问烽火去中心化网络，是通过部署在雾/边缘节点中的特定网关服务(如Proxy代理、DNS服务等)实现。

3.4.构成点对点网络的核心技术

◉保密与安全机制

‣ 采用Ed25519，这种使用SHA-512和Curve25519[46]的爱德华曲线数字签名算法(EdDSA[47])的签名方案。在密码学中，Curve25519是一个椭圆曲线，提供128位安全性，设计用于椭圆曲线迪菲-赫尔曼(ECDH)密钥协商方案。它是不被任何已知专利覆盖的最快ECC曲线之一[48]。在公钥加密学中，EdDSA是一种数字签名方案，使用基于扭曲爱德华曲线的Schnorr签名变体，它的设计比现有的数字签名方案更快，而且不会牺牲安全性[49]。

‣ 烽火网格将会严格遵守数据保密机制，对属于终端用户/设备/应用这类数据源的非公开流的事件有效载荷将使用非对称密钥进行强加密，只有持有授权私钥的一方才能读取数据。

‣ 构建烽火对等虚拟专属网，加密运行在承载网之上的烽火节点间通信数据包，防止网络嗅探等行为。

◉采用安全键路由的S/Kademlia方法

‣ S/Kademlia[33]作为一种分布式哈希表DHT，可被应用于协调和维护对等系统的元数据。

‣ S/Kademlia[33]协议通过在多条不相交的路径上使用并行查询抵抗常见攻击，并用隐式密码来限制节点ID自由生成。它的静态和动态密码学谜题强制所有节点ID均匀分布，每个节点维护的路由表都被均匀的分区，跨越了诚实子网的通信也能延续。即使网络中存在一半以上的不诚实节点，也能达到85%的成功率。另外，这种节点ID的均匀性使得仅需要一个可靠的引导节点，新用户很容易的加入成为网络成员。

‣ S/Kademlia[33]承载网[34]具有De-Brujin网络拓扑结构[35]，能够高效的发送消息到指定的接收方。它不仅仅在分类账本通信中发挥作用，也在烽火节点之间建立可靠的分布式路由，高效传递包含数据流载荷的消息。

‣ S/Kademlia[33]的网络拓扑决定了它并不会区分对待节点，跟奖励发放、消息转发等结合时，不会引发马太效应困境[43]。

‣ 这种分类账本节点和服务节点，采用相同的路由方法，也是秉承一体化设计的理念，也构成了烽火网络的核心技术之一。

◉采用Coral[51]分布式稀松哈希表DSHT

‣ 在块数据交换机制中，采用Kademlia分布式哈希表DHT，会存在忽略“远”节点可能拥有数据，而强制“近”节点存储，这种浪费存储和带宽的现象。而Coral存储了地址，通过该地址的对等节点就可以提供相应的数据块。

‣ Coral用户只需要一个可工作的对等体，而不是完整的列表。这样可以仅将子集分配到“最近”的节点，从而避免热点(当密钥变得流行时，重载所有最近的节点)。

‣ Coral根据区域和大小组织了一个成为群集的独立DSHT层次结构，这使得节点首先查询区域中的对等体，也就是说“查找附近的数据而不查询远程节点”，那样大大减少查找的延迟。

◉通过构造MerkleDAG对象，一种有向无环图，为数据流存储提供了有用的属性，包括①内容可寻址：所有内容都被多重Hash校验和唯一识别；②防止篡改：所有内容都用它的校验和来验证；③重复数据删除：所有的对象都拥有相同的内容并只存储一次，而这对于数据的公共部分非常有用；

◉基于Snowball[30]协议变体的有向无环图DAG共识.

‣ 融合了经典共识协议(强一致性、高效)、中本聪协议(开放性、无权限)两者优点的基于亚稳态机制的分布式拜占庭容错协议Snowball[31]，采用概率性的安全保证，使用可调的安全参数使得共识失败的概率任意小，另外加入了BFT属性，增加系统效率和安全性。

‣ 具备静态绿色、低通信成本、高拓展性等特点。这种多次重复抽样的方式(灵感来源于1961年Snowball抽样[38])使节点之间达成共识，在消息转发、数据同步中，也将在数据流代理中发挥作用，这也体现了一体化设计的好处。

‣ 由于工作量证明PoW共识，一方面不具备伸缩性，另一方面我们希望注入代价到节点上，而不是Hash挖矿上。基于最长链的权益质押PoS[24]，或委员会权益质押DPoS[28]，同样不具备可伸缩性。鉴于烽火网络的愿景，是拥有超大规模数量节点构成的网络，则可

伸缩性是它的核心要素。

4. 伸缩性困境

采用最长链法则的分类账本技术，如工作量证明，是通过竞争的方式，解决交易冲突，而节点数量的增加，协调节点网络来维护分布式分类账本，将会带来额外的通信和处理开销。并导致指数级的处理时间复杂度，因而存在伸缩性困境，它需要在性能、一致性、可用性之间作出平衡。而采用委员会模式的分类账本技术，如典型代表Algorand[29]、Tendermint、Ouro-boros Praos、Dfinity[39]和EOS，无论是通过权益委托[28]，可验证验证函数[29]，还是去中心化投票[30]，但在节点数量极少的情况下，降低了网络的安全性，如要扩大节点数量，则降低了性能，就面临着伸缩性困境。但值得关注的是，采用最长链竞争性的iChing[45]协议，基于概率竞争的一种PoS共识协议，它拥有极高的可扩展性，共识节点可便捷地加入退出。

基于有向无环图DAG，在节点间复制交易的共识协议家族Avalanche[31]，拥有极佳的伸缩性，可以应用于大规模节点网络中。另外引用其Snowball协议[31]，并做了相关改进的Wavelet共识[32]，可保证交易的不可逆、全局一致性顺序，而不会对安全性、性能或活性产生任何影响。

5. “鸡与蛋”困境

从互联网演变历史中，我们可以发现诸如Google这样的中心化互联网服务公司，提供一个公共的采用客户端/服务器模式的通用化服务，客户端以浏览器为主，比如邮箱、即时通讯、文稿处理、文件存储等，而这些以往的付费软件往往运行在客户的计算机中。采用如广告这类的“三方付费”商业模式，它有别于供应/消费的传统经济模式。当Google提供免费搜索服务时，它要收录互联网上的海量网页、这就需要研发网页排序算法、提供超级庞大的互联网接入与大量的服务器，在全球不同区域设立众多规模庞大的数据中心。这在未产生大笔收入之前，就需要远远超过传统企业的前期资金投入。这在互联网泡沫时期，这类风险投资驱动的亏损经营现象被称之为“烧钱运动”，但它极大缓解了“鸡与蛋”式困境[26]。然而小型互联网公司，则没那么幸运，深陷其中。他们只有达到一定规模后，才有可能实现盈利，否则要么被收购、要么倒闭。

某种程度缓解该困境的“免费”[40]商业模式，一方面使得“赢家通吃”现象比传统行业愈发明显，另一方面大规模的中心化互联网服务的数据泄漏，如雅虎公司的黑客入侵事件，全球近三十亿用户账户受到影响[41]，这对用户而言，就是以牺牲数据所有权和隐私权作为代价换取“免费”服务的某种证据。

如要提供大规模安全的，注重用户隐私与数字产权的公共“数据流总线”网格服务，跟其它通用化互联网服务一样，照样存在从零到一的冷启动过程，即“鸡与蛋”困境[26]，它是首当其冲的战略因素，除了软件代码研发之外，一项重要的资金投资领域，就是各种云服务器、边缘服务器、网络带宽等方面的基础性设施投资。如同PubNub[17]这样的垂直性业务公司也需上亿美元的持续投资，从而维持其相应的市场地位。此外，目标用户到种子用户的转换难题，这个对连接供应和消费的双边市场，如Golem[9]、SONM[10]、Streamr[11]而言，就显得格外明显和尖锐。

烽火采用“节点经营”模式，激励其基础设施投入。采用铸币方式，让面向未来的有信仰的投资者，看中未来的价值变现(与其它替代币不同的地方在于烽火的重心不在于能提供一个可以转账的加密货币，而在它能提供的基础性普适服务。如今加密货币圈已存在大量的资金可进行投机或投资，这是一个自由的开放市场。我们认为对于一些初始项目来说，它是一个时代机遇)，投入大量资金经营去中心化的点对点网络节点(云节点和雾节点)。从梅特卡夫定律(Metcalfe's law)[37]可以看出，当节点数量规模超过某临界点，以至于达到传统行业组织无法企及的那种数量级，它会像现在的互联网服务一样，发挥爆发性的巨大作用。

诚如中本聪所言的那样，通过注入物理世界有价值的算力/电力，一方面为烽火经济体系提供价值支撑(虽然大规模的成本投入，不代表一定能够创造价值，但确实能帮助项目渡过临界点)，另外一方面可解决“从无到有”的冷启动困境(即大规模网络的基础设施投资)。

6. “群体鸿沟”

我们看到很多基于以太坊协议的ICO项目，购买通证的人群，绝大多数都是以投机或投资为目的，而非项目的用户或客户。这就造成了项目的使用者只是极少数一部分人，项目的应用状况跟早期的互联网项目没法比，用户极少就会大大限制项目发展。这样，ICO仅是一种新的融资方式，而没有发挥通证这一核心存在的基础，也就是通证的使用。这种现象同样也反应在比特币上，它并没有成为一种加密货币，在不同用户间用作支付货币的大规模转账，同时实现支付手续费和新铸币的合理平衡，而变成了一种“数字黄金”，作为投资者的某种类型的储值工具，从而远离了中本聪的最原始的那个加密货币愿景。而后续立志成为电子现金的项目，同样也面临着这个挑战。随着时间的推移，也许是二十年以后，如果越来越多的人群开始接受加密货币、加密资产及其底层技术，形势也许会变得愈发明朗。

我们可以观察到，在加密货币领域，已经存在加密货币钱包服务、中心化交易所或去中心化交易所、加密资产的金融服务等，由于针对一个特定用户群体，从而显得非常活跃。而引入“区块链”技术，并注重于应用生产领域的，恰恰

是另外一个群体。而更加广泛的普通大众、企业则是远离以上两类群体的大多数，这从一个侧面，印证了“群体鸿沟”这一社会现象。

如同常见的产业链合作共赢那样，在加密货币领域，由于存在普遍的群体认知共识，彼此间的各种合作，比比皆是，从而形成某种小生态，但突破这个“群体鸿沟”，扩展到现有群体之外，仍然有待时日。

要缓解上述挑战，需要尽可能引入早期用户，就需要对这类先锋用户给予适当激励。这个在某些试点项目中，也呈现良好势头的端倪，如PI币[27]。但过度激励，也会带来负面作用，如恶意的垃圾用户，因而激励平衡就非常重要。不能像互联网服务那样，采用全免费的模式，只能借鉴互联网服务中的免费加收费的混合模式，也就是纳米支付(无限接近于免费)、微支付(小额支付)、紧急支付三类混合的方式，同时也借鉴现有经济模式中常见的推荐奖励，使用奖励，资深用户回馈等常规的市场营销手段(使得纳米支付、微支付手段在早期发展过程中，达到“相当于免费”的事实)。随着新一代用户在付费使用、数据产权、隐私保护等方面意识的不断增加，种子用户转化的成功率也会不断提高。另外也需要等待合适的第三方服务(如法币转换、服务置换)时机，以便于更多圈外人士容易使用或消费相关的公共服务。

也真是由于上述挑战的存在，迫使我们思考，如何让烽火更轻量、更简单、更普适，使得它能够像比特币一样，一上线就能持续化的自我运行，而无需更多的功能迭代。随着用户的不断增加、网络规模的不断扩大直至它突破临界点，使得它能够具备传统中心化系统或服务所不具备的特性，而成为很多第三方应用或设备、产商、组织的一种优选的解决方案。

通过一个投机/投资群体的超大规模的基础设施提供，为群体以外的个人、企业、组织提供一个更加注重安全与隐私、更加注重数字产权、更加去中心化、更加具备规模化与性价比优势的可替代生产工具/生产资料.从而逐步弥合这一“群体鸿沟”，实现“信用背书”到“价值生产”的一个演进案例。

7. 价值共识

刚接触加密货币的人，其中有一个困扰：“开源的比特币代码，可通过复制，搞一个克隆币，那岂不是可以无代价复制，反过来也说明比特币不值得投资”。实际上，市场上充满了各种替代币，也存在各种垃圾币与骗子币。但最后结果是，剥离比特币核心部分或其它克隆代码后，唯有那些有自主创新与内在价值的那些品种，才会被市场认可和接受，才有机会生存下来。这也可初步印证自由市场[42]，它自身就具备某种价值认定的共识机制。

8. 激励机制

创始之初，就设立一个明确的激励机制。它采取总量恒定，在三十六年时间跨度内，按季度线性通缩的方案，直至停止铸币后转变为百分百用户消费驱动。

此外，新币奖励的分发机制：

①按固定比例，横跨完整周期的共识节点奖励；

②按固定比例，横跨完整周期的云/边缘节点奖励；

③按固定比例，横跨完整周期的转发量证明奖励；

④按固定比例，创建头四年逐年解锁的初创激励池；

⑤按固定比例，创建头六年逐年缩减早鸟用户激励池；

⑥按固定比例，创建头八年逐年缩减用户推荐激励池；

⑦按固定比例，创建头十年逐年解锁开发基金池；

⑦按固定比例，创建头十五年逐年解锁市场基金池；

⑧按固定比例，创建头二十年单节点缩减总额递增的节点扩张动态激励池；

这里仅提出一个轮廓性设计构想，不涉及具体细节。

9. 机器与人

早期用户(被激励主体)在进行消费支付后，奖励池通过机器算法对支出方进行一定数额的延时回馈活动，通过这种游戏机制，取代那类免费无成本模式，并兼顾人类心理的一种有趣方式。

庞式骗局[44]那种现象屡见不鲜，首先是人性的贪婪与侥幸赌博心理，其次也是分散化个体资本的泛滥表现。如能疏导这种天生的人性需求，使之成为一种风险投资力量，借此构造一种创造价值、造福于人类的生产工具与生产关系，激发其内在的潜力和爆发力。

科技不断进步的将来，机器的价值创造总量呈现指数级增长，将在很多领域超越人类，这种状况使得在整个常规价值创造体系(不包括高创新性的人类经济活动)中机器的角色愈发重要。当它们变成价值创造主体时，就会出现机器与人融合的新经济形态，大多数普通人将扮演“投资人”、“雇主”、“经理”、“管理者”、“策划人”等新角色，而开展实际工作的“雇员”将会是机器。当“人机混合微型商业体”不断涌现时，较低准入门槛的去中心化模式，将会扮演某种重要角色。

通过观察优步[50]的经营模式，就会发现“司机”和“车”之间这种新颖的生产关系，而随着智能驾驶技术的来临，上述构想，将越来越成为可能。

10. 总结

在计算机体系结构中,“总线”就是一种通信通道，它是为计算机内部或计算机之间的组件，提供数据传送和控制逻辑的一种通用方式。如将主板比喻成一座城市，总线就像是城市里的公共汽车，车上乘客就是数据，按照各种线路传送乘客，使之快捷顺利地到达目的地[36]。

目前各种苹果设备，如iPhone、iPad、Mac之间，就可以进行互操作，如数据同步、消息提醒、屏幕显示、接听电话、寻找苹果设备等，其背后就由这类机制所驱动，它已经让用户感受不到其背后的计算服务的存在，它是当下非常好的普适计算[22]雏形范例，并已初步展示了其强大的交互能力，代表着未来的某种趋势。

可以想象未来，定位于普适计算模型/新一代价值互联网，这一巨大的“超级计算机”中的“安全的超级总线“角色的大规模点对点数据流网格，为“超级计算机”内的各种组件，也就是种类繁多的设备、应用、系统、服务等，提供数据传送和控制逻辑的一种安全的通用方式。无论是在加密通信、私密社交、物联网、车联网、工业互联网、供应链、普惠金融、智能家居、智慧城市、大数据分析、人工智能、还是其它各种跨界服务的应用场景中，伴随着5G通信技术，和更多普适计算案例的不断涌现，这类遍布全球的基础型公共服务设施，将会扮演越来越重要的角色。换句话说，“无所不在的计算”、离不开“无所不在安全的数据流通道”的服务支撑。

11. 致谢

任何一项创新的活动，都离不开前辈们所开创的局面，没有这些，烽火的任何设想都不可能实现。中本聪不仅仅发明了比特币，更是开启了一个全新的时代。伴随着星际文件系统IPFS的出现，也启发了后来者重新审视以HTTP为基础的WEB体系。

12. 参考

1. Satoshi Nakamoto et al.Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
2. Evan Duffield, Daniel Diaz. Dash: A Payments-Focused Cryptocurrency, 11revisions, 2018.
3. Pier Stabilini,Robert Viglione,Alberto Garoffolo. Horizen Application Platform:Tiered Node System and Sidechains to Decentralize the Network, 2018.
4. https://zel.network/zel/
5. ZelNodes — The decentralized, scalable, high-availability computing network, 2018. https://medium.com/@ZelOfficial/zelnodes-the-decentralized-scalable-high-availability-computing-network-57c1b4245fbd
6. ZelNodes — Dates, Specs, Network Upgrade, Payout Cycles, etc. 2019. https://medium.com/@ZelOfficial/zelnodes-dates-specs-network-upgrade-payout-cycles-et-al-8c5b84fbbf70
7. https://pivxmasternode.org white-paper, 2018.
8. Vitalik Buterin. Ethereum, 2014 3.1, 6.1, 7
9. https://golem.network white-paper, 2016.
10. https://sonm.com white-paper, 2017.
11. https://www.streamr.com Unstoppable Data for Unstoppable Apps: DATAcoin by Streamr, 2017.
12. Muneeb Ali, Jude Nelson, Aaron Blankstein, Ryan Shea,Michael J. Freedman. The Blockstack Decentralized Computing Network, 2019.
13. Marcus Torchia, Monika Kumar. IDC - Worldwide Semiannual Internet of Things Spending Guide, 2017 (document)
14. Amir Haleem, Andrew Allen,Andrew Thompson,Marc Nijdam, Rahul Garg. Helium A Decentralized Wireless Network, 2018.
15. https://ipfs.io A peer-to-peer hypermedia protocol designed to make the web faster, safer, and more open.
16. https://www.bigchaindb.com/whitepaper/ 2018.
17. https://www.pubnub.com/
18. https://en.wikipedia.org/wiki/Grid_computing
19. https://www.bbvaopenmind.com/en/technology/digital-world/the-internet-of-everything-ioe/
20. https://en.wikipedia.org/wiki/Constrained_Application_Protocol
21. https://en.wikipedia.org/wiki/MQTT
22. https://en.wikipedia.org/wiki/Ubiquitous_computing
23. https://en.wikipedia.org/wiki/Proof_of_work
24. https://en.wikipedia.org/wiki/Proof_of_stake
25. https://en.wikipedia.org/wiki/Consensus_(computer_science)
26. https://en.wikipedia.org/wiki/Chicken_or_the_egg
27. https://minepi.com
28. Dan Larimer. Delegated Proof-of-Stake Consensus, 2018.
29. Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, pages 51 – 68. ACM, 2017.
30. Ethan Buchman. Tendermint: Byzantine fault tolerance in the age of blockchains. PhD thesis, 2016.
31. Team Rocket. Snowflake to Avalanche: A novel Metastable Consensus Protocol Family for Cryptocurrencies, 2018.
32. Kenta Iwasaki, Heyang Zhou. Wavelet: A decentralized, asynchronous, general-purpose proof-of-stake ledger that scales against powerful, adaptive adversaries, 2019.
33. Ingmar Baumgart and Sebastian Mies. S/kademlia: A

practicable approach towards secure key-based routing. In 2007 International Conference on Parallel and Distributed Systems, pages 1 – 8. IEEE, 2007.
34. https://en.wikipedia.org/wiki/Overlay_network
35. https://en.wikipedia.org/wiki/De_Bruijn_sequence
36. https://en.wikipedia.org/wiki/Bus_(computing)
37. https://en.wikipedia.org/wiki/Metcalfe%27s_law
38. Leo A Goodman. Snowball sampling. The annals of mathematical statistics, pages 148 – 170. 1961.
39. Timo Hanke, Mahnush Movahedi, Dominic Williams. DFINITY Consensus, DFINITY Technology Overview Series Consensus System Rev.1, 2018
40. https://en.wikipedia.org/wiki/Free:_The_Future_of_a_Radical_Price
41. https://en.wikipedia.org/wiki/Yahoo!_data_breaches
42. https://en.wikipedia.org/wiki/Free_market
43. https://en.wikipedia.org/wiki/Matthew_effect
44. https://en.wikipedia.org/wiki/Ponzi_scheme
45. Lei Fan, Hone-Sheng Zhou. A Scalable Proof-of-Stake Blockchain in the Open Setting, 2018.
46. Bernstein. "Irrelevant patents on elliptic-curve cryptography". cr.yp.to. Retrieved 2016.
47. Josefsson, S.; Liusvaara, I. Edwards-Curve Digital Signature Algorithm (EdDSA). Internet Engineering Task Force. doi:10.17487/RFC8032. ISSN 2070-1721. RFC 8032. Retrieved 2017.
48. https://en.wikipedia.org/wiki/Curve25519
49. https://en.wikipedia.org/wiki/EdDSA
50. https://www.uber.com
51. https://en.wikipedia.org/wiki/Coral_Content_Distribution_Network
52. https://www.influxdata.com/products/influxdb-overview/