

Hyper Speed Network

全球首个公链 + 5G 应用架构的价值生态网络体系



2019 – 04 (Cn) V0.9.7.1

目录

摘要

1、5G 产业发展趋势 P1

概述
关键技术和应用场景
商业前景

2、5G 时代的区块链视角 P3

区块链发展历程
区块链为 5G 赋能
5G 给区块链技术带来的挑战

3、HSN 解决方案 P5

技术要求
总体架构
部署结构

4、HSN 核心技术 P8

超级节点
边缘节点
分层共识机制
文件加密去重
· 数据加密去重算法
· 用户间数据分享算法
· 用户组数据共享算法
分块技术
侧链技术
核心优势

5、应用场景 P17

视频流场景
车联网和无人机
软件定义广域网和网络附加存储 (SD-WAN+NAS)
无线 Mesh 产品
边缘计算

6、经济模型 P21

价值体系
通证分配

7、发展规划 P22

8、管理团队和投资机构 P23

核心成员
顾问
投资机构

9、风险提示 P28

司法监管相关的风险
HSN 应用缺少关注度的风险
黑客或盗窃的风险
漏洞风险或密码学科突飞猛进发展的风险
缺少维护或使用的风险
未保险损失的风险
应用存在的故障风险
无法预料的其它风险

摘要

作为引领数字经济创新的重要推动力，5G 技术正以其高吞吐、低延迟、高并发、低功耗等优质特性，与人工智能（AI）、区块链（Blockchain）、云服务（Cloud）、大数据（Big Data）一起，构建新时代的全球 IT 基础设施。5G 所延伸出的万物互联将有利于提升整个社会效率，促进物联网、人工智能、边缘计算、AR、VR、超高清视频流等应用的大规模兴起和繁荣。

但是，伴随着设备的大规模接入、数据的海量增长及计算需求的剧增，以下问题也接踵而至，引起人们的广泛关注：

- 数据缺乏安全保障，容易被黑客窃听
- 海量数据采集、GDPR 法例生效突显隐私保护责任
- 在 5G 网络上开发各种物联网应用的成本高昂
- 除了通信以外，终端之间难以实现价值的交易和互换

为解决这些问题，HSN 应运而生。Hyper Speed Network（HSN，简称超速网络），是全球首个公链 +5G 应用架构的价值生态网络体系，主要特性包括：

- 利用区块链技术，构建了 5G 架构下终端上链的网络安全和信任机制
- 实现高吞吐、低延迟、高并发、低功耗的价值生态网络体系
- 能够支撑未来数字时代大数据上链的多源信息互联交换，以及多元化的资产登记、交换、交互及流动
- 实现万物互联、构建链上数据世界，促成信息获利的新经济体

作为面向 5G 数字经济时代的基础公链，HSN 旨在利用区块链技术实现复杂的应用场景业务上链，为 5G 数字时代的产业发展助力。在主网上线之后，HSN 将广泛应用于 5G 环境的云 VR/AR、智慧安防、车联网、智慧城市、智能制造、无人机、SDWAN+NAS、Mesh 产品、边缘计算模块等应用领域。

1、5G 产业发展趋势

1.1 概述

5G 即第五代移动通信系统 (5th Generation Mobile Network)，是新一代的无线通信网络标准。相比 4G，5G 在移动宽带、时延可靠和海量连接等方面都产生了质的飞跃，具体表现为：

- 能以 10Gbps 的数据传输速率支持数万户
- 能以 1Gbps 的数据传输速率同时提供给在同一楼办公的许多人员
- 能支持数十万的并发连接以用于支持大规模传感器网络的部署
- 频谱效率相比 4G 显著增强
- 覆盖率比 4G 有所提高
- 信令效率得到加强
- 延迟显著低于 LTE

1.2 关键技术和应用场景

根据 IMT-2020 发表的《5G 概念白皮书》，5G 的创新技术包括大规模天线阵列、超密集组网、新型多址、全频谱接入和新型网络架构。

其中大规模天线阵列、超密集组网、新型多址和全频谱接入等技术是业界关注的无线领域创新焦点；基于软件定义网络 (SDN) 和网络功能虚拟化 (NFV) 的新型网络架构是网络架构领域的未来标准。

此外，基于滤波的正交频分复用 (F-OFDM)、滤波器组多载波 (FBMC)、全双工、灵活双工、终端直通 (D2D)、多元低密度奇偶检验码、网络编码、极化码等也是 5G 重要的潜在无线关键技术。

5G 通过融合上述关键技术，能应对多样化场景的极端差异化性能需求，其适用的应用场景包括连续广域覆盖、热点大容量、低时延高可靠和低功耗大连接等四个 5G 典型适用场景，包括云 VR/AR、智慧安防、车联网、智能城市、智能制造、无人机、SDWAN+NAS、Mesh 产品、边缘计算模块等应用领域。

1.3 商业前景

作为未来创新技术的标准，全球各国给予高度重视，制定了明确的 5G 商用时间表。 这当于所

有美国消费者在 2016 年的全部支出，并超过了 2016 年中国、日本、德国、英国和法国的消费支出总和。

到 2035 年，全球 5G 价值链将创造 3.5 万亿美元产出，同时创造 2200 万个工作岗位。上述数字超过了今天整个移动价值链的价值。5G 价值链平均每年将投入 2000 亿美元，持续拓展并增强网络和商业应用基础设施中的 5G 技术基础。

此外，5G 部署将支持全球实际 GDP 的长期可持续增长。在 2020 年至 2035 年间，5G 对全球实际 GDP 增长的贡献预计将相当于一个与印度同等规模的经济体。

简而言之，5G 将会通过以极高的速度实现各种设备之间的实时通信，成为 AI、大数据、云服务 etc 新一代创新技术的推动者，最大限度地发挥这些创新的影响。数字领域的数据爆炸可以帮助大规模转变业务，并为用户提供丰富、有意义和身临其境的体验。随着 5G 数据经济的充分发展，人们的工作和生活方式将发生根本性的变化，全球经济也将迈向新的数字时代。

2、5G 时代的区块链视角

2.1 区块链发展历程

区块链是分布式数据存储、点对点传输、共识机制、加密算法等新型计算机技术，具有去中心化、全网记录、低成本、高效率、安全可靠等技术特点。

从 2009 年 1 月 3 日中本聪挖出创始区块开始，比特币不间断运行至今，用长达 10 年的不间断安全运行成果，比特币证明了其背后区块链技术的可行性。2014 年 1 月 23 日，年仅 19 岁的以太坊创始人 Vitalik Buterin 发布了以太坊白皮书。2015 年，经济学人报一篇《区块链：信任机器》的报道，将区块链技术引入了全球风口。2017 到 2018 年迎来了区块链概念大爆发，越来越多的公司、创业者开始涉足区块链，区块链项目呈井喷式增长。

大型企业也开始纷纷涉足区块链领域。2018 年 8 月 10 日，中国深圳开出第一张区块链电子发票，由腾讯 FiT 区块链团队提供底层技术。2018 年 10 月 10 日，IBM 宣布 IBM Food Trust 正式商用。2019 年 2 月，摩根银行宣布将发行银行系统稳定币 JPM，一个 JPM 锚定一美金。2019 年 3 月，彭博社报道拥有 20 亿用户的 Facebook 正在战略转移区块链，研究利用 WhatsApp 推出一款稳定币，瞄准汇款市场。

区块链技术潮流不可逆转，并正在以其自身的运行规律不断地完善和优化，分片技术、侧链、跨链、共识算法、抗量子等领域技术也在不断突破中。从区块链产业看，随着行业龙头的出现，市场向精细化划分，再加上法律法规的逐步健全，未来三年内，区块链产业格局将基本形成，区块链对社会经济各领域的推动作用快速显现，区块链在全球范围内对人类的生活产生广泛而深刻的影响。

2.2 区块链为 5G 赋能

5G 是未来网络的基础设施架构，区块链是业务开展的新框架，区块链如何与 5G 技术紧密融合，是区块链设计者们目前重点研究的课题。

1、5G 创造的万物互联为区块链带来万亿市场机遇

当前全球上万亿的商品中，有 99.99% 的商品都没有接入区块链网络，其中一个原因是受制于终端的不成熟，众多依赖于物联网终端的区块链产业应用无法商业化，其中包括云 VR/AR、智慧安防、车联网、智能城市、智能制造、无人机、软件定义广域网 + 网络附加存储 (SDWAN+NAS)、

无线 Mesh 产品、边缘计算模块等。

而 5G 技术能够给物联网带来更广的覆盖、更稳定的授权频段、更统一的标准，从而对基于物联网的区块链应用提供有力的支持。因此，依托高速的 5G 通信技术，以及物联网、大数据和人工智能等各项技术的发展，区块链将能为全球上万亿的商品，提供稳定的跟踪、溯源能力和分布式的点对点交易功能。

2、区块链为 5G 应用场景提供数据保护能力

5G 时代对数据的保护能力提出了更高的要求。5G 出现后网络速度将大幅度提升，数据量也将随之急速增长，此外，更多计算和存储将由智能终端和边缘计算节点来承担。

区块链技术旨在打破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、可追溯等提供技术支持，天然适用于对数据保护要求严格的场景。

3、区块链促使 5G 实现真正的点对点的价值流通

5G 重点布局分布式的场景，比如车联网、远程视频、智慧城市等。区块链可以做到在分布式部署的架构下，无需中心机构做确权，而由去中心化的节点在链上来确权和分发。这就促使点对点的价值交换成为可能，而不需要通过中心化的中转、提成，大大提升了终端交易的效率，降低交易成本。比如 5G 带宽租赁服务、新能源电表交易等等商业模式，很适合通过区块链来完成点对点的交易，实现价值交换。

2.3 5G 给区块链技术带来的挑战

5G 依托光纤网络，比现在的 4G 快 10 倍，并提供更低的延迟和更大的带宽，面向 5G 的应用场景通常具有高性能、低延时的并发存储、协同网络、并发计算的技术需求。要管理这样复杂的“生态系统”，需要更高的计算能力和存储容量。

而区块链不可能三角的问题成为制约其技术发展的关键瓶颈。当前区块链的共识技术、交易处理能力、数据吞吐能力还无法应对复杂的应用场景需求。此外，随着区块链平台的不断丰富，更多的终端接入区块链世界，必然出现多种区块链平台共存的情况，5G 时代的跨链需求更加迫切。

3、HSN 解决方案

HSN 是全球首个专注于 5G 应用场景的公链项目。针对以上挑战，HSN 提出了下列技术要求，并设计了完善的“区块链 +5G”解决方案。

3.1 技术要求

1、支持海量设备并发接入

为了支撑终端设备产生的海量数据上链需求及复杂应用的边缘计算需求，HSN 需能够处理海量用户设备所产生的并发数据。

2、支持海量数据存储

5G 网络对传输带宽的大幅提升，使得大数据应用、超高清视频应用向区块链存储数据成为可能，HSN 需具备高存储能力，以便承载复杂的 5G 数据存取需求。

3、超高性能

为实现 5G 时代链上存储和链上计算的目标，HSN 需要提供超高的性能，包括网络访问、数据存储、顺序计算、并行计算等各方面的超高性能指标。

4、极具竞争力的运行总成本

伴随云计算、云存储以及区块链等技术发展，以 AWS、阿里云、Azure 为代表的传统云计算公司，和以 EOS 为代表的第三代区块链应用公链，正在不断降低开发者和企业的使用和运营成本。HSN 需要从技术架构、经济模型层面设计一套自适应的运营体系，允许用户免费访问网络，开发者免费发布应用，并为开发者和企业创建有效的盈利模式。

5、支持新型软件开发流程 —— 敏捷开发和 DevOps

随着 5G 应用需求的不断多样化，以及区块链基础设施的不断更新换代，完全不依赖于中心服务器的复杂场景应用将成为主流。因此，基于智能合约开发的 DAPP 应用应能满足用户需求快

速迭代，满足开发者使用现代化软件开发流程和运维流程的需求，比如互联网流行软件开发流程——敏捷开发和 DevOps。

3.2 总体架构

为了满足上述技术要求，HSN 采用了以下架构：



HSN 技术架构

HSN 提供了无缝接入 5G 网络的一体化的分布式账本体系，包括完整的分布式部署架构、智能合约体系、安全体系、分层共识机制，能够满足 5G 高吞吐量、高性能的复杂去中心化应用场景需求，催生 5G 区块链商业生态。

HSN 采用了超级节点（PBFT-DPoS 共识机制）和边缘节点（Edge Node）分层共识机制，既保障了整个 HSN 生态系统的安全运行，又促进了边缘计算和物联终端的繁荣生态。同时，HSN 对底层复杂的技术体系及异构的系统进行了封装、抽象，实现分布式的隐私保护、多维身份认证，并支持跨链和侧链交互映射。

HSN 突破性地提出了基于区块链的自动设备认证技术，在基于会话和特征识别的基础上，通过智能合约和挑战应答（challenge-response）的通讯方式实现自动设备绑定请求、设备认证，并支持用户级别的身份绑定，使得终端设备信息无法被篡改，为万物互联和边缘计算应用提供最基础的终端设备认证。

为支持 5G 环境高并发和网络存储需求，HSN 选用了 IPFS 为其存储基础架构。IPFS 的网络提供了动态的、细粒度的、分布式的网络存储支撑，可以更好地适应 5G 内容分发网络（CDN）的要求。HSN 大文件会被切分成小的加密分块，下载的时候可以从多个服务器同时获取。在对象层和文件层，大部分数据对象都是以 Merkle DAG 的结构存在，并具备双重哈希去重，能够灵活支持内容寻址和去重存储。

在此基础上，HSN 网络提供了一系列应用框架，包括分布式数据交换协议、分布式流程管理协议等等，使用通用 API、SDK 以及各种应用功能组件，能够实现开发部署的便捷化，支持互联网产品敏捷开发。

HSN 这种高度封装化的分布式账本架构、快速地支持大量并发进程的存储结构，使得 HSN 具备了应对 5G 复杂应用场景需求的能力。

3.3 部署结构

HSN 的总体部署架构如下图所示：5G 网络构成基础设施，超级节点负责执行智能合约和出块，边缘节点则负责涉及智能终端的分布式计算和存储平台，提供海量计算和存储能力。分布式账本负责链上及链下核心处理。

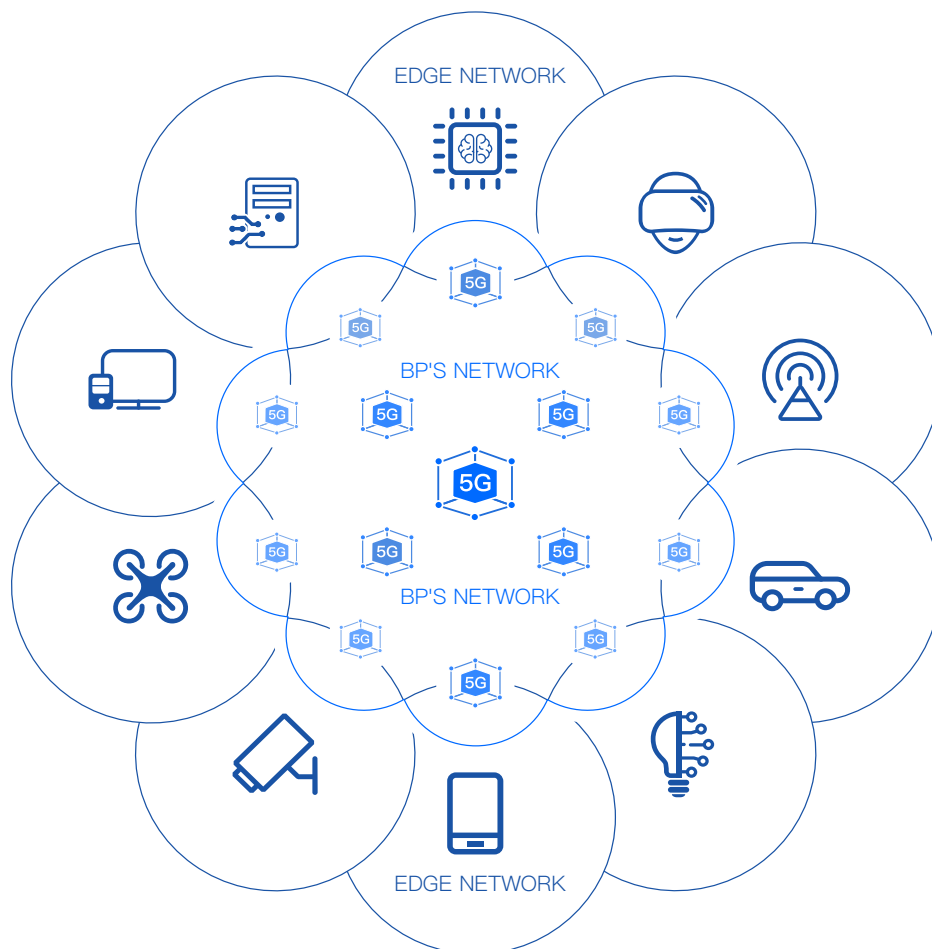


4、HSN 核心技术

4.1 超级节点

HSN 对超级节点机制进行了优化，使其可以更好地管理核心网络和系统功能的任务，包括在侧链上运行多种服务，支持 5G 模块组扩展，跟踪并测量设备的正常运行时间，并为矿工安排节点报酬支付时间表。

与 EOS 超级节点不同的是，HSN 超级节点除了执行智能合约和出块，还为整个网络的海量数据提供存储服务，作为类 IPFS 分布式存储网络的主节点，确保整个 HSN 网络提供高效、可靠、可信的区块链网络服务。此外，HSN 超级节点还具有设备模块，能够接入智能终端设备，适应视频、网络等多种终端接入模式。在共识机制上，超级节点采用 PBFT-DPoS 共识机制，负责区块产生和存储关键数据。智能合约和运算量小的计算工作在超级节点上执行。



4.2 边缘节点

海量计算需求会给超级节点带来严重的负载。经过对超级节点模式的压力测试，团队认为超级节点不适合处理万物互联环境下复杂的长时间计算任务，因此需要边缘计算节点接入来执行计算密集型任务。另一方面，在一些高响应要求的物联网应用中，云端响应的延时会造成整体效率的低下。

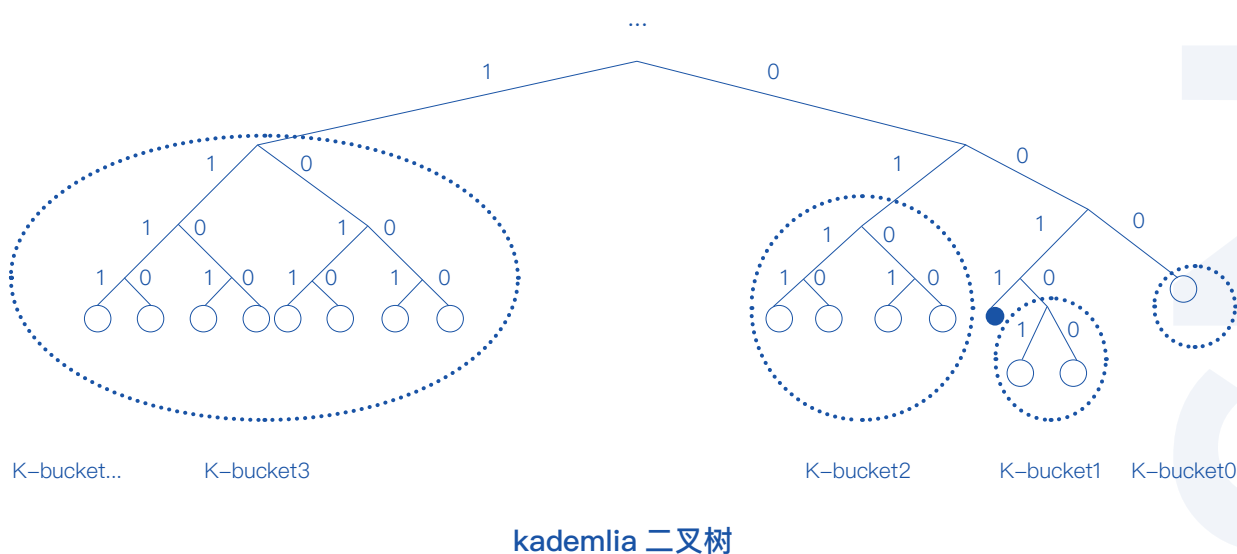
HSN 引入了边缘节点（Edge Node）的概念，边缘节点机制作为超级节点的必要补充，可以将密集计算业务下沉至边缘节点，这有助于降低响应时延和带宽成本，满足去中心化架构模型下各类智能场景的需要。

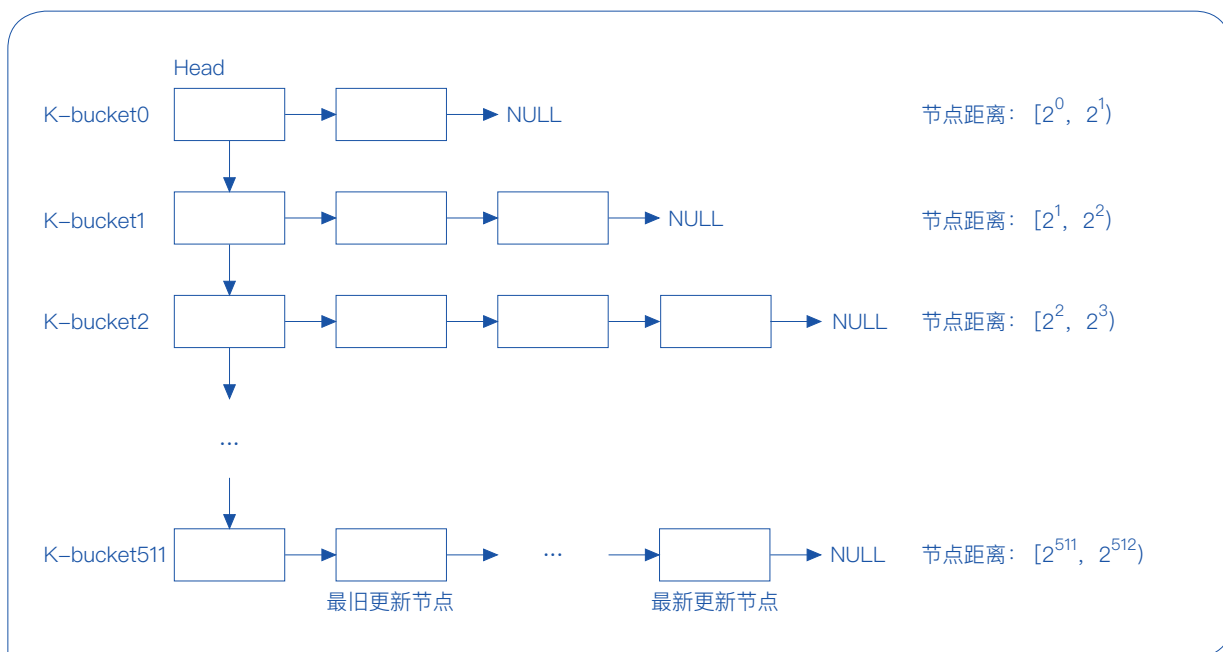
边缘节点作为 HSN 网络海量计算和海量存储资源的来源，可以是未来所有的具备一定计算或存储能力的终端设备，通过让超级节点为边缘节点担保，确保边缘节点为大数据存储和超高速智能合约边缘计算处理提供高效、可靠、可信的区块链网络服务。

通过将海量的边缘节点的闲置计算能力和存储能力组成一个分布式计算和存储平台，执行耗时较长的计算任务，包括 AI 应用，图片处理，基因测序等使用边缘节点的场景，把密集计算任务从云端卸载到边缘之后，整个系统对能源的消耗减少了 40% 以上，数据在整合、迁移等方面可以减少 90% 以上时间。

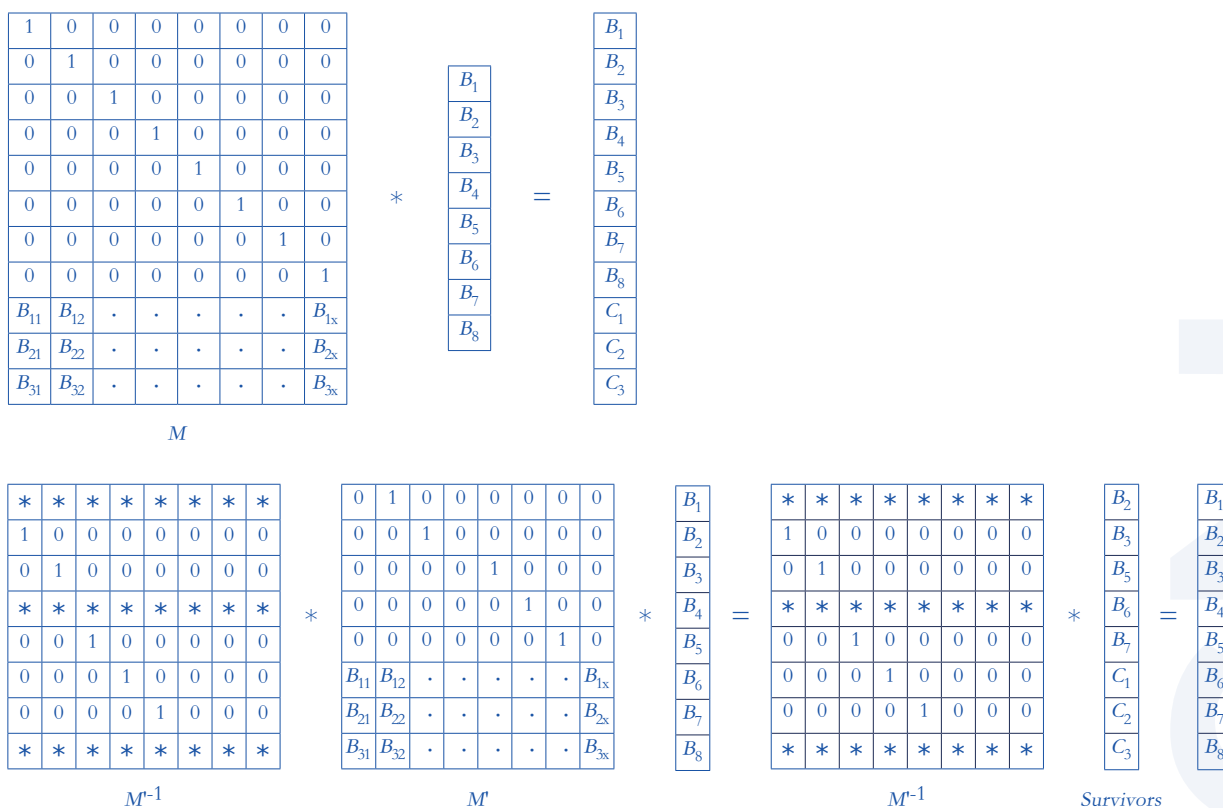
边缘节点数据存储采用如下算法：

HSN 采用 kademlia 算法改进版实现数据存储与检索。在 HSN 中节点 *Nid* 长度 取值 512；节点冗余参数 *k* 取值 32；





每个节点内部 k-bucket 存储示意图



Reed-solomon 数据还原示意图

- 1) 边缘节点 E_1 加入 HSN 后向 HSN 超级节点请求节点 id, 临近超级节点 H_1 从 id 池中选择未使用 id_1 节点分配给该边缘节点 (节点 id 一旦分配其整个生命周期内维持变);
- 2) 边缘节点 E_1 收到 id_1 后计算 $Nid_1 = sha3 - 512(id_1)$ (即本节点标识)。
- 3) E_1 收到终端设备发来数据 $Data_1$ 存储要求时, 根据 $Data_1$ 大小将其切分, 假设节点长度为 L , 切分后长度结果表示为 $L = \sum_i n_i \cdot b_i$ (其中 b_i 依次取 256M, 256K; n_0 为 256M 分块数, n_1 为 256K 分块数); 相应的数据切分为 B_j , 即 $Data_1 = \sum_j B_j$;
- 4) 根据用户支付 HSN 通证情况, 选择矩阵 M , 根据 M 生成冗余数据:
 - a. 用户选择普通安全模式, 系统按 10% 比例生成冗余数据: $m_i = \lceil n_i * 10\% \rceil, (i=0,1)$
 - b. 用户选择中等安全模式, 系统按 20% 比例生成冗余数据: $m_i = \lceil n_i * 20\% \rceil, (i=0,1)$
 - c. 用户选择强安全模式, 系统按 30% 比例生成冗余数据: $m_i = \lceil n_i * 30\% \rceil, (i=0,1)$
 - d. 新生成的整体数据记为: $Data'_1 = \sum_j B'_j (i \leq n_0 + n_1 \text{ 时 } B_j = B'_j, i > n_0 + n_1 \text{ 时 } B'_j \text{ 为冗余数据})$
- 5) 针对每个 j , 计算 $Nid'_j = h_j = sha3 - 512(B'_j)$, 根据 h_j 在边缘节点查询相关数据表项是否已存在, 若已存在则扣除相关 HSN 通证后继续下一 j 处理; 否则转入 a. 处理:
 - a. 计算待存储节点 E_{1,i_0} 与本节点 E_1 距离 $d = Nid_1 \oplus Nid'_j$, 根据 kademlia 二叉树路由表查找其位置;
 - b. 通过 ping 命令探寻 E_{1,i_0} 是否存活;
 - c. 如果存活向 E_{1,i_0} 发送 store B_j 指令; 下一 j 处理;
 - d. 如果节点 E_{1,i_0} 非存活 (将该非存活节点则上报超级节点扣除相关 HSN 奖励), 则在相应 K-kucket 集合 $\{E_{1,i_1}, E_{1,i_2}, \dots, E_{1,i_k}\}$ (这里 i_t 表示待存储节点与本边缘节点距离, $2^i \leq i_t < 2^{i+1}, t=1,2,\dots,k, k$ 最大选取 32, 超过该值还未找到则将本次数据丢弃) 中选取第一个存活节点进行存储;

4.3 分层共识机制

共识机制是所有公链的技术核心。共识机制存在一个 CAP 原则，即一致性、可用性和分区容错性难以同时得到保障。同时，还需要确保所有诚实节点都保持一致性，避免分叉。对于 HSN 而言，由于存在边缘节点，使得共识算法更加复杂。

为此，HSN 采用分层共识机制：

- 超级节点通过投票机制产生，使用 PBFT-DPoS 机制轮流打包出块，获得奖励。
- 边缘节点使用 PoT（即 Proof of Telecommunication，通信证明），每个节点依据其提供的通信服务获取奖励。请注意，这里的通信服务不是单纯的存储容量、网络流量、计算能力等，而是所有与通信有关服务的集合。
- 为保证边缘节点的服务质量，边缘节点需要向超级节点获取担保，担保过程采用投票和抵押机制。

4.4 文件加密去重

传统存储网络中，如云盘、CDN 甚至 IPFS，对于明文文件的去重技术已相当成熟，只需要对比两个文件的指纹信息，即可判定是否内容相同。但在加密存储应用中，上述方法已经失效，两个相同文件使用不同的公钥加密后产生的密文内容并不一样，无法简单地基于密文的指纹信息实现去重，同时数据的分片存储也使得去重变得更加复杂。

HSN 利用非对称加密和零知识证明技术，研发了一套文件加密去重技术。利用零知识验证方法，基于二次哈希，实现了密钥与文件分离、完整所有权认证、不使用第三方传递密钥等功能，解决了“收敛加密（CE）对重复数据的无用加密操作使计算开销随着数据负载去重率的提高而增加”的问题。即使是不同的用户同时在 HSN 网络上存储相同文件，整个网络也只需要保存一份加密后的内容拷贝，而不用担心内容和隐私泄露，从而提升整个网络的存储效。

4.4.1 数据加密去重算法

- 1) 用户 A 存储数据时将待存储数据 $Data_A$ 进行从大到小切分（256M,256K），（即：文件大于 256M 时按照每块 256M 切分，文件不足 256M 时每块按 256K 切分；不足 256K 时补 0 对齐），这里假设切分后分别为 $B_1, B_2, B_3, \dots, B_n$ （即 $Data_A = \sum B_i$ ），分别计算每个块 hash： $h_i = hash(B_i)$ ；
- 2) 根据 h_i 在映射表中查找相关表项是否存在，若存在，则扣除用户 A 相关 HSN 通证同时更新映射表项 h_i 与 $Node_{E_{1i}}$ （ E_{1i} 计算见 4）步骤）对应关系后返回；若不存在转入 3) 操作；

- 3) 针对每个块计算密钥种子: $seed_i = hash(B_i + salt)$;
根据种子计算加密密钥 $K_{1i} = Key_expansionbyseed(seed_i)$; 为防止 rainbow 攻击, salt 取 $seed_{i-1}$ ($i=0$ 时 salt 取 "\$#ADFGHFJ&^*678679&*")(\$^Gfg*^!!!@#@#\$\$%XCGH^%&**(&(") ;
- 4) 用户 A 计算 $E_{1i} = E_{K_{1i}}(B_i)$ (即采用密钥 K_{1i} 对数据块 B_i 进行加密存储), 边缘节点对加密数据进行存储;
- 5) 计算 $E_{PAK} = E_{P_A}(K_{1i})$ (即用户 A 公钥 P_A 对密钥 K_{1i} 进行加密), 并将其存储于节点 $Node_{E_{PAK}}$;
- 6) 在映射表中添加映射表项 h_i 、 $Node_{E_{1i}}$ (E_{1i} 的存储节点)、 $Node_{E_{PAK}}$ (E_{PAK} 的存储节点) 对应关系;
- 7) 用户 A 扣除相关 HSN 通证;

4.4.2 用户间数据分享算法

设 p 为大素数; 且 $a < p$ 为模 p 的一个原根; a, p 公开;

- 1) 用户 A 选择随机数 $R_A < p$, 计算 $Y_A = a^{R_A} \bmod p$, 并将 Y_A 发送给 C;
- 2) 用户 C 选择随机数 $R_C < p$, 计算 $Y_C = a^{R_C} \bmod p$, 并将 Y_C 发送给 A;
- 3) A 计算 $K_{share} = Y_C^{R_A} \bmod p$;
- 4) C 计算 $K_{share} = Y_A^{R_C} \bmod p$;
- 5) A 计算 $E_{1i} = E_{K_{share}}(K_{1i})$ 并发送给 C;
- 6) C 计算 $K_{1i} = D_{K_{share}}(E_{1i})$, 然后用 K_{1i} 对原始存储数据进行解密;

4.4.3 用户组数据共享算法

- 1) 用户 A、B、C 加入用户组 G_1 时, 系统为其分配组密钥 KG_1 , 每个用户分别计算: $E_{AKG_1} = E_{P_A}(KG_1)$, $E_{BKG_1} = E_{P_B}(KG_1)$, $E_{CKG_1} = E_{P_C}(KG_1)$ (该步表示每个用户用自己公钥对 KG_1 进行加密); 加密数据存储于该用户接入边缘节点的映射表中;
- 2) 用户 A 将原始数据加密存储后, 计算 $D_{AKG_1} = E_{KG_1}(K_1)$ (该式表示使用组密钥 KG_1 对 K_1 进行加密, K_1 为用户 A 存储数据时产生的密钥), 将其存储于边缘节点映射表中;
- 3) B 读取 A 分享数据时:

- a. 计算 $KG_1 = D_{P_B}(D_{AKG_1})$ (即 B 用自己私钥 P_B 对加密数据 D_{AKG_1} 进行解密得到组密钥);
- b. B 根据文件 hash 值在 HSN 映射表中查找原始存储文件 $Data_A$ 及 D_{AKG_1} ;
- c. 计算 $K_1 = D_{KG_1}(D_{AKG_1})$ (即用组密钥 KG_1 对 D_{AKG_1} 进行解密);
- d. 计算 $Data_1 = D_{K_1}(Data_A)$ (即用密钥 K_1 对原始存储文件 $Data_A$ 进行解密得到原始存储数据);

4.5 分块技术

HSN 对待存储数据进行预处理, 即将数据文件分割成多个碎片, 并将其存放在不同的节点上。每个节点只需处理一小部分传入的交易, 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。

在 HSN 网络中, 分块技术具有多层含义: 在超级节点网络中, 利用分片技术提升 TPS 和智能合约执行速度; 在边缘节点网络中, 通过将计算密集型和存储密集型任务进行分片, 提高整个网络的计算能力和存储能力。

4.6 侧链技术

侧链技术可以提供交易效率, 还可以在 HSN 主链的基础上提供隐私保护等新功能。用户在使用这些新服务的时候, 不会对主链产生任何影响, 以满足未来 5G 时代不同的行业应用需求。

以侧链锚定的方式在更多的区块链上进行流通。开发者们可以根据业务形态的需要开发不同的侧链来接入 HSN。侧链技术进一步扩展了区块链技术的应用范围和创新空间, 使 HSN 可以支持多种资产类型, 并可以在侧链上建立智能合约开发 DAPP。

4.7 核心优势

综上所述，HSN 具备以下核心优势：

- **高吞吐**：通过改善 HSN 的 TPS 实现，结合分片及侧链技术，目标 TPS 可达千万级别；
- **大容量**：通过改善 HSN 的底层网络文件系统实现，结合加密去重技术，理论可以提供无限存储空间；
- **高可靠**：通过改善 HSN 的区块链网络结构，结合超级节点和边缘节点双重分层共识，构建可靠可行的价值体系，确保整个网络稳定运行；
- **多样性**：通过改善 HSN 的智能合约实现机制以及任务调度模型，结合边缘计算网格，使得智能合约适应大数据计算的应用场景；
- **高兼容**：智能合约编写规范兼容市面主流公链，结合多重合约虚拟机机制，使得智能合约跨链兼容，降低开发者的入门门槛；
- **低成本**：通过优化 HSN 经济模型，结合多重激励机制，实现消费体系和生产体系的良性循环，提供具有其他中心化设计和竞品所无法比拟的运行成本。

5、应用场景

在 4G 时代，数据通常以接入层、汇聚层、核心层接入，业务数据在核心网集中处理，这种中心化工作方式难以满足 5G 应用场景对于低时延、大带宽和多连接的要求。5G 时代，针对不同的业务场景，业务将在不同节点分布式处理；以去中心化的工作方式提高效率和可靠性。随着分布式 AI 的崛起，5G 边缘网络平台将承载更多的算力和数据流量。

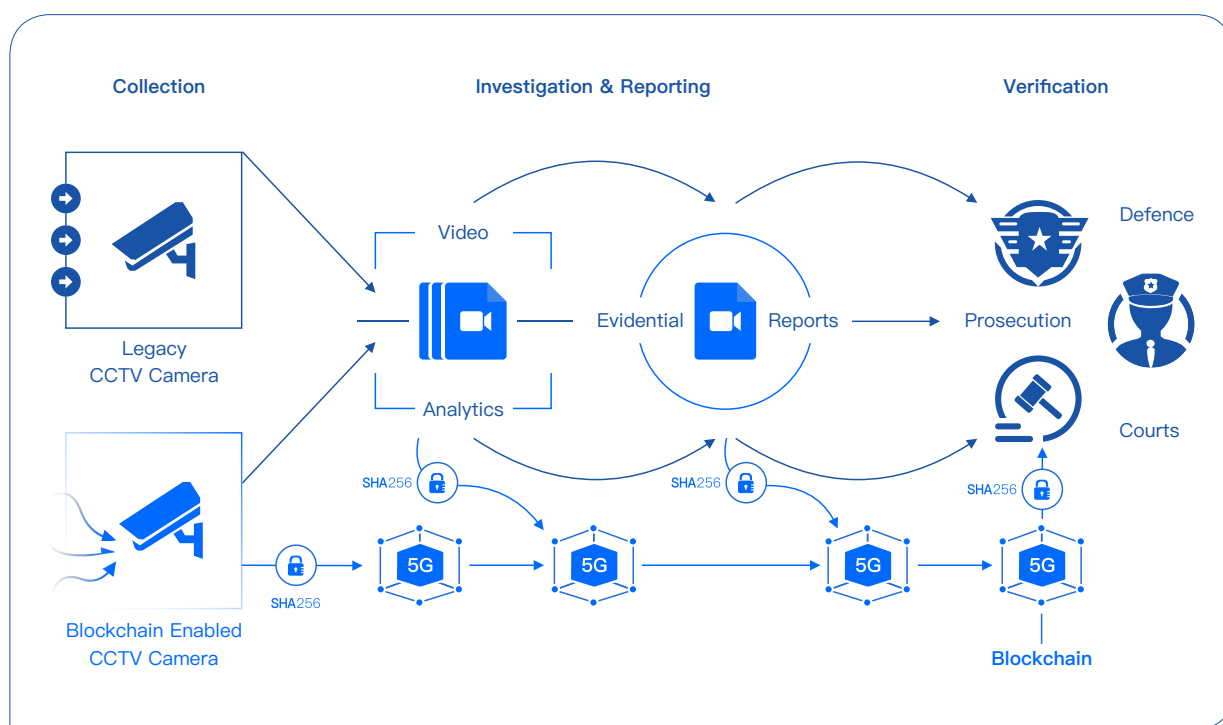
5.1 视频流场景

4G 技术促进了手机视频的普及。曾经有文字、静态相片的地方，现在有摄像头、视频博客、YouTube 频道、Facebook 直播、Snapchat 和 TikTok 等各种传播渠道。现在，5G 技术为超高清视频提供了基础。随着 5G 的普及，实时视频流在移动应用和社交媒体上将变得更加流行。

HSN 支持 5G 架构下的视频流上链，HSN 将视频内容分块转换为哈希值，存储在 HSN 网络上，支持视频索引变量、储存变量置换，采用基于内容索引的方式，能够实现视频流的上链和智能合约操作，实现海量视频和图片的智能化解析。

HSN 能够支持 5G 架构的以下视频场景：

- 支持摄像头多场景应用，例如可以对视频上的人脸进行 100 多个关键点的分析，生成每一个人脸的性别、年龄、服饰等详细信息。
- 将信息存储在 HSN 网络上，利用区块链提供精准、高效的图像分析。
- 支持各种视频直播节目应用，提供去中心化视频版权保护，打破现有的应用中心化版权运作，真正保护原创直播视频的版权收益，并可以提供点对点的价值交换。
- 激励更多的终端贡献视频存储空间，通过通证激励机制盘活闲置视频存储资源。



Blockchain for Chain of Evidence Management in CCTV

5.2 车联网和无人机

5G 技术支持设备与设备之间的直接通讯，构建 D2D (Device to Device) 网络，因而各类物联网将迅速普及，首当其冲的便是“杀手级”应用——车联网领域。HSN 在大数据管理、安全性、透明性和点对点交易方面具有独到优势，使得在车联网的自动驾驶、无人驾驶等领域设备协作成为可能。

HSN 可用于整个汽车价值链，从供应链管理、汽车硬件制造到自动化驾驶，以及车辆生命周期数据跟踪，继而为自动驾驶提供数据，也能创造成本节约和优化运营流程。通过 PoT 模块将车辆数据接入链上后，如果车辆发生事故，未来 HSN 能够保证数据及时采集，基于实时传输的物联网数据，完成保险赔付、二手车交易等金融场景使用。在车联网应用场景中，HSN 支持自主身份，即将一个独特的身份标识存储于 HSN 上，构成唯一的身份标识。另外，借助设备的可编程逻辑（智能合约）控制器机制，可以利用区块链为芯片提供加密接口，从而在去中心化的环境下，保证系统的安全性。

5.3 软件定义广域网和网络附加存储 (SD-WAN+NAS)

SD-WAN (Software Defined WAN, 即软件定义广域网) 是当前企业和企业之间、企业和分支机构以及家庭应用的流行网络解决方案。根据咨询机构 Gartner 的预测, 到 2019 年底, 将有 30% 的企业采用 SD-WAN 专线。5G 的发布将进一步简化网络连接策略, 比如为企业间的视频会议提供高可靠性。

在 5G 架构下, 企业级、家庭级用户可以通过 SD-WAN+NAS (Network Attached Storage, 即网络附加存储) 的方式, 利用超融合技术一起提供服务。SD-WAN 在应用层实现 5G 数据流的加密和流向控制, NAS 接入 HSN 网络, 可以实现存储的共享和备份。

在 SD-WAN+NAS 的应用场景中, HSN 将提供高度的隐私性、点对点的交易, 简化了信任构建, 为高度自治、敏捷和简化的应用铺平了道路。HSN 具备安全且固有的容错性, 使用公钥加密和时间戳来验证每个记录或操作。利用 HSN 的智能合约, 通过公共分类账验证产品或交易的真实性, 并减少监管和审计相关风险, 同时在双方建立了可信机制。

5.4 无线 Mesh 产品

无线 Mesh 是应用于 5G 网络连续广域覆盖和超密集组网场景中重要的无线组网技术，能够构建快速、高效的基站间无线传输网络，提高基站间的协调能力和效率，降低基站间进行数据传输与信令交互的时延。

有激励机制的无线 Mesh 被以太坊创始人 Vitalik 认为是区块链应用的最佳领域之一。基于通证的激励，借助物联网终端，HSN 可以配合自组织，形成一个具有灵活性、去中心化、分布式、能够自我修复的无线 Mesh 网络，提供比互联网更高的速度和宽带，并且它通常是免费的，以便更加快捷方便、低耗能地为社交、娱乐、商业服务。

5.5 边缘计算

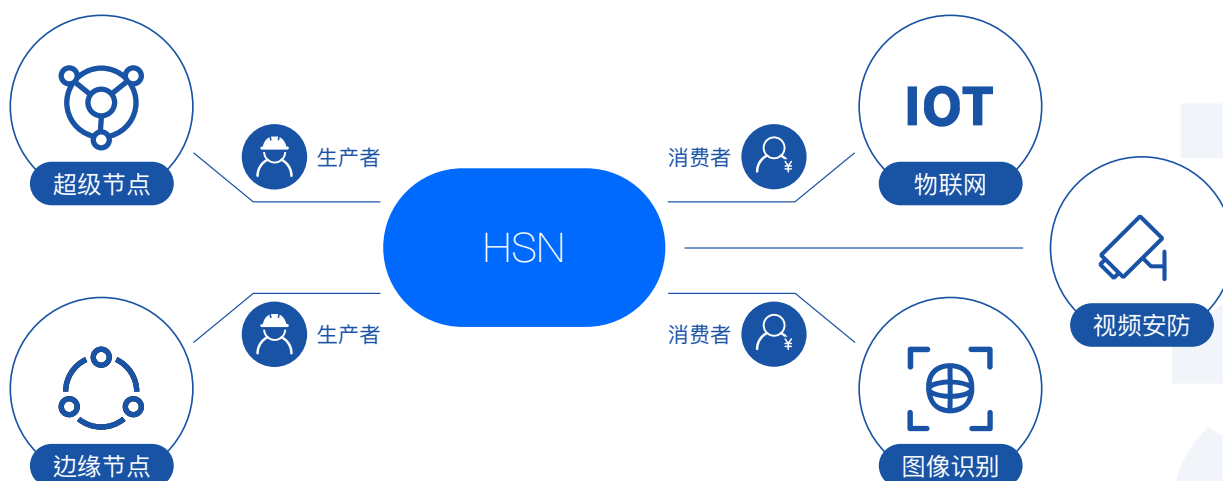
伴随着智能终端的发展，边缘计算的兴起，大量实时的需要交互的计算将在边缘节点完成。边缘计算的核心理念就是将数据的存储、传输、计算和安全交给边缘节点来处理，HSN 网络恰好符合边缘计算架构，可以充分利用节点本身所具备的计算能力，就近完成物联网设备计算存储的对接需求，提升物联网感知 - 计算 - 响应这一过程的时效性。在物联网应用中存在大量需要低延时响应的使用场景，当云计算在这些领域一筹莫展时，HSN 的边缘计算方案是一个新的解决途径。

6、经济模型

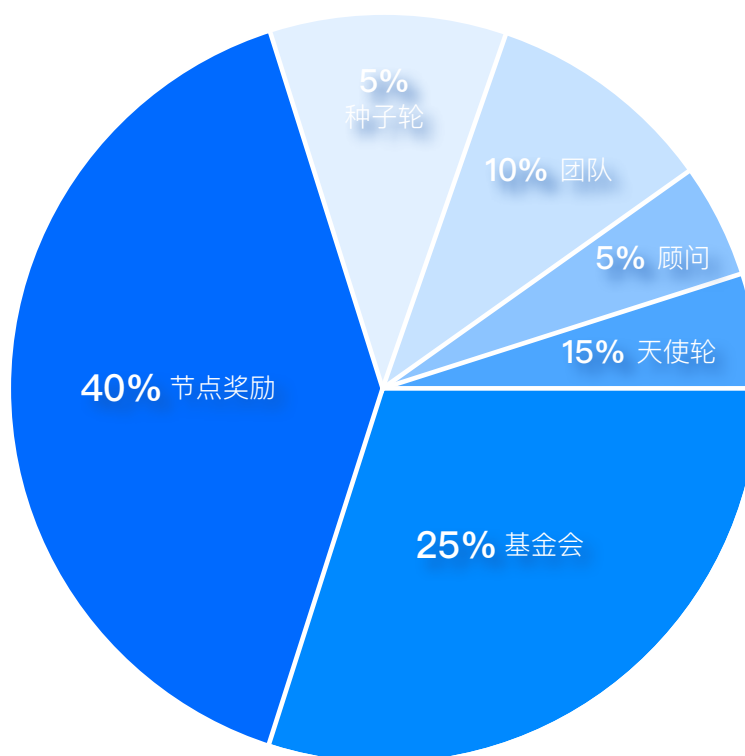
6.1 价值体系

作为面向 5G 应用场景的公链，HSN 的主要目标是支持 5G 复杂应用场景下的区块链应用，因而 HSN 的通证将扮演非常重要的角色。它体现了 HSN 的下列价值主线：

- 价值载体：每一个应用场景接入或直接使用一定量的 HSN，或定义自己的通证，并与 HSN 进行一定比率的兑换。随着应用场景的逐渐丰富，HSN 使用和消耗越来越多，HSN 的价值也越来越大。
- 交易属性：与 EOS 类似，HSN 上的每笔交易都无需要支付交易费用，其上的 DAPP 应用也需要使用 HSN 抵押和购买资源，HSN 支持智能合约，合约上的 HSN 将通过交易进行原子级别的交易交互。
- 激励机制：通过积极的激励计划，HSN 激励人们主动提供系统验证交易，创造区块，利用经济手段产生积极的反馈可以促进系统的不断发展。通证将作为奖励，激励社区持续为系统做出贡献。



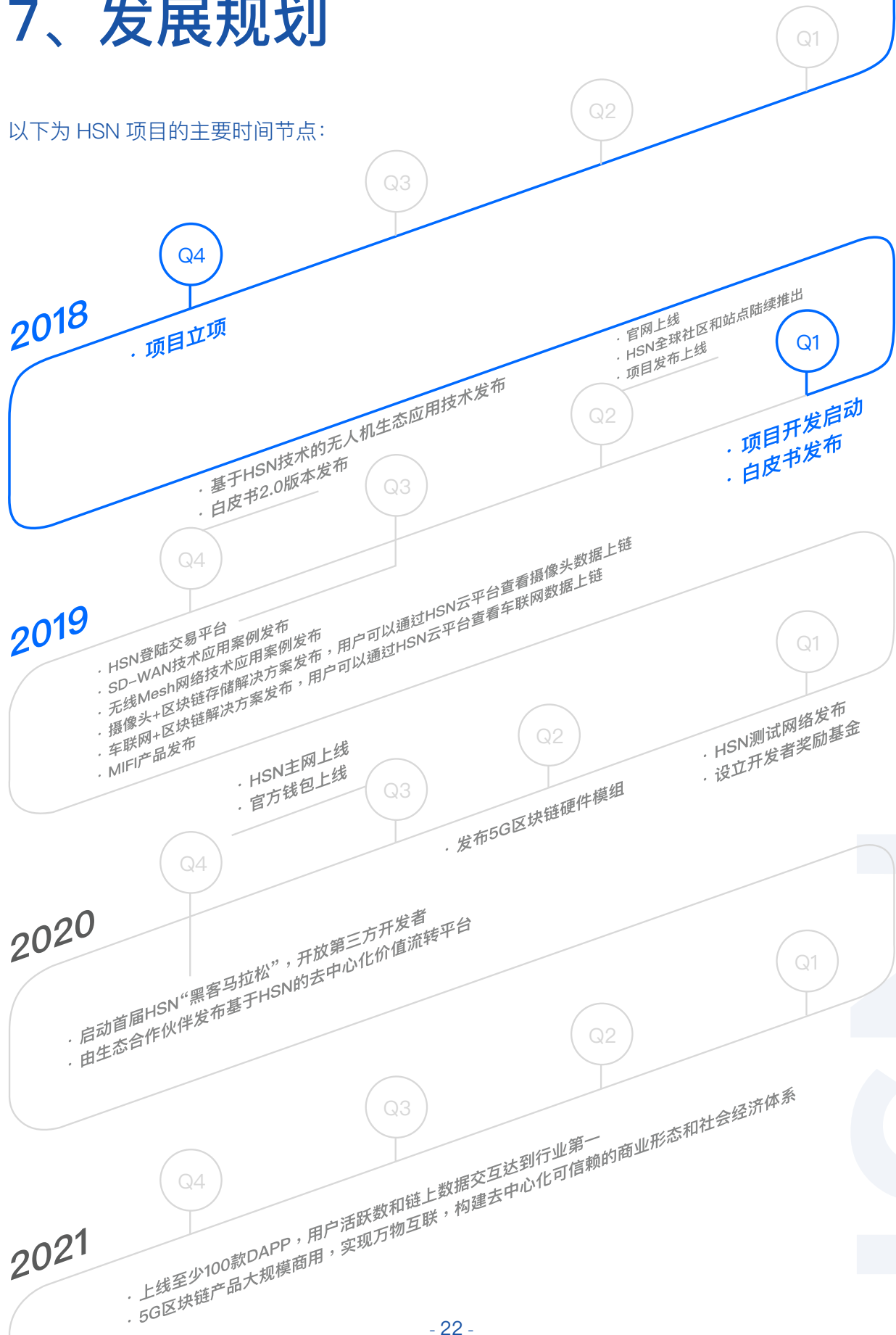
6.2 通证分配



HSN 通证分配	数量	释放规则
总量	10 亿	/
种子轮	5000 万	交易平台上线后半年后开始释放 6 个月全部释放完成
天使轮	1.5 亿	交易平台上线前释放 20% 交易平台上线后 1 个月释放 40% 交易平台上线后 2 个月释放 40%
团队	1 亿	项目启动研发一年后线性释放
基金会	2.5 亿	用于技术研发，市场推广，社区激励
顾问	5000 万	交易平台上线后半年后开始释放 6 个月全部释放完成
节点奖励	4 亿	主网上线前根据节点活动奖励 50% 主网上线后根据规则奖励 50%

7、发展规划

以下为 HSN 项目的主要时间节点：



8、管理团队和投资机构

8.1 管理团队



Richard Sheh

计算机专业硕士，大数据和物联网专家，10 年以上通信行业从业经验，曾就职于深信服科技从事数据通信和安全产品的研发管理工作，担任公司核心产品项目负责人。曾担任腾达科技高性能无线通信产品线主管，领导开发的《超高速大容量智能无线接入控制器关键技术》荣获深圳市科技计划项目 400 万现金奖励。2017 年进入区块链行业，主导开发过溯源跟踪系统、数字钱包、数字交易所等区块链行业关键应用，具备丰富的区块链行业从业经验。



Tommy Chai

10 年以上数据通信行业经验，曾创办数据通信品牌 Tenhot 并担任 CEO，负责全球化品牌行销，曾和中国领先的 IoT（物联网）解决方案提供商 -- 酷宅科技联合创办物联网 + 通信公司开维科技并担任 CEO。2017 年开始从事区块链行业，有丰富的区块链项目运营管理经验，对比特币等数字货币有深入的研究和独特见解。



Daniel Sun

计算机专业硕士，数据安全专家，曾多次获得全国大学生数学建模竞赛国家级及省级奖励，保送研究生，读研期间发表论文多篇，毕业后曾就职于华为和启明星辰从事密码和通信系统的研发管理，具有丰富的区块链产品开发与管理经验，曾领衔开发过多套系统并成功广泛商用。



Peter Jia

上市科技公司资深研究员，10 年互联网连续创业者，2013 年接触并进入区块链领域开始创业投资，《风口区块链》主笔人。



Daren Yuen

Clicknews 创始人，早期数字货币投资者，多年区块链行业生态运营经验，生态运营涉及数字货币矿场运营、项目筛选、市场分析、孵化及公关运营，商务投资等，先后成功参与 Cardano(ADA)、UGChain、Loopring、Hcash、WaltonChain 等区块链项目国内早期投资及相关推广运营。

8.2 顾问



Robert Van Aert

拥有蒂尔堡大学（荷兰）法律硕士学位和商业法专业硕士学位。与多个为进入中国的财富 500 强公司合作并担任公司顾问，包括 Apple, Clorox 和 Oakwood, 在房地产和高科技领域引领中国投资和欧洲并购方面经验丰富。是区块链媒体平台 China Crypto News 以及 China Blockchain Partners (CBP 中欧区块链合伙人) 的创始人，同时也担任多个欧洲和中国区块链项目的商业顾问。



Mr. Michael Ott

早期的区块链传道者，专注于超高速交易和图表分析，欧洲加密社区的建设者和意见领袖。



曾子涛

资深区块链技术专家，ET 钱包联合创始人，ETH 智能合约开发者，2013 年进入区块链行业，成功领衔开发过数字钱包、数字交易平台、公链等多个产品和项目，具有丰富的区块链技术开发和应用经验。



Alexander Jiung

加密熊猫资本创始人，前戴尔国际计算机公司 BSD 经理，IT 行业连续创业者以及区块链行业先行者，参与过多个知名区块链项目投资以及矿场投资，曾协助组建中国最大区块链线下社群联盟。关注区块链 DeFi 金融方案以及区块链落地项目。



白宝明

西安电子科技大学教授、博士生导师，中国电子学会会士，中国电子学会信息论分会主任委员，美国加州大学戴维斯分校（UC Davis）访问学者，曾任中国通信学会青年工作委员会副主任委员，IEEE ICCAS'04、ICCCAS'06 无线通信分会技术程序委员会共同主席，IEEE ITW'06 技术程序委员会成员，美国加州大学戴维斯分校（UC Davis）访问学者，主要从事信息与编码理论、编码调制技术、无线通信和量子通信等领域的的科研工作。



王家恒

德国高级洪堡学者，IEEE 高级会员，东南大学移动通信国家重点实验室教授，博士生导师，5G 移动通信系统专家，区块链技术专家，中国通信学会青年工作委员会委员，长期从事区块链与无线通信融合技术研究，提出了区块链无线接入网（B-RAN, Blockchain Radio Access Network）概念，并建立了分布式无线接入网的新型架构，现主持国家自然科学基金、江苏省自然科学基金、973 子课题等研究项目，并与华为、中兴、NEC、海信等国际知名企业保持长期合作关系。



Christina Chan

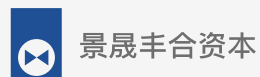
浙江大学管理科学与工程硕士，高级咨询师，前埃森哲高级咨询顾问，陶氏化学高级分析员，十年以上企业管理咨询和项目管控经验，曾服务过的客户涉及美国、印度、南非、德国等全球五百强企业，行业涉及金融、能源、化工制造业等。



Chiyu Yu

中国执业律师、专注区块链和数字资产法律业务研究、柬埔寨《数字资产交易法》起草团队成员，自 2017 年初开始研究区块链产业相关的法律制度，主要业务领域为数字资产交易平台的合规服务及海外资质申请，Token 项目的框架设计及法律尽职调查，数字货币投资领域的法律服务等。已服务客户涵盖交易所、代币项目和 Token Fund 等区块链各产业。

8.3 投资机构



9、风险提示

9.1 司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体施加影响则 HSN 可能受到其影响，例如法令限制使用，销售，电子通证诸如 HSN 有可能受到限制，阻碍甚至直接终止 HSN 应用的发展。

9.2 HSN 应用缺少关注度的风险

HSN 应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发

展这些相关分布式应用，这样一种缺少兴趣的现象可能对 HSN 应用造成负面影响。

9.3 黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 HSN 功能的可能性，包括服务攻击，Sybil 攻击，游袭，恶意软件攻击或一致性攻击等。

9.4 漏洞风险或密码学科突飞猛进发展的风险

密码学的飞速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给加密通证和 HSN 平台，这可能导致 HSN 的丢失。

9.5 缺少维护或使用的风险

首先 HSN 不应该被当作一种投资，虽然 HSN 在一定的时间后可能会有一定的价值，但如果 HSN 缺少维护或使用的話，这种价值可能非常小。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对 HSN 是非常不利的。

9.6 未保险损失的风险

不像银行账户或其它金融机构的账户，存储在 HSN 账户或以太坊网络上通常没有保险保障，任何情况下的损失，将不会有任何公开的个体组织为你的损失承保，但诸如 FDIC 或私人保险公司将会为购买者提供保障。

9.7 应用存在的故障风险

HSN 平台可能因各方面的原因故障，无法正常提供服务，严重时可能导致用户 HSN 链的丢失。

9.8 无法预料的其它风险

密码学通证是一种全新且未经测试的技术，除了本募集说明书内提及的风险外，此外还存在着一些 HSN 团队尚未提及或尚未预料到的风险，此外，其它风险也有可能突然出现或者以多种已经提及的风险的组合的方式出现。



Hyper Speed
Network