Galaxy Network

基于区块链的分布式加速存储网络

目錄

1. 摘要 4

2. Galaxy 网络定义 5

2.1 系统组成 5

2.2 网络协议 6

2.3 系统属性 7

3. Galaxy 网络构建 8

3.1 系统概述 8

3.1.1 参与者 8

3.1.2 基础网络 9

3.1.3 交易市场 9

3.1.4 存储证明 10

3.1.5 流量证明 10

3.1.6 共识算法 10

3.2 基础网络 10

3.2.1 矿工架构 11

3.2.2 信道编码 12

3.2.3 存储格式 13

3.2.4 安全存储策略 14

3.2.5 索引结构 14

3.3 交易市场 15

3.3.1 订单 15

3.3.2 存储市场 15

3.3.3 加速市场 19

3.3.4 PUSH 协议 20

3.4 存储证明 (Proof of Capacity) 22

3.4.1 动机 22

3.4.2 存储证明 24

3.5 流量证明(PROOF-OF-FLOW) 24

3.5.1 动机 24

3.5.2 流量证明 25

3.6 共识与出块 25

4. 需求实现……26

5. 治理结构……27

5.1 非营利组织设立……27

5.1 非营利组织原则……27

5.1 非营利组织目标……28

6. TOKEN 经济模型……28

6.1 “一链双币”设计……28

6.2 分配方案……29

7 应用场景……30

8. 里程碑……32

9 风险提示和免责声明……33

9.1 关于本白皮书……33

9.2 免责声明……33

9.3 风险披露……34

10 参考文献……38

1. 摘要

本文提出了一种去中心化的存储和传输网络，通过聚合过剩的闲置智能设备，使得客户可以实现低成本及高体验的数据存储和传输服务；通过良好的 Token 经济模型，激励用户提供存储和带宽资源。

公有云存储及CDN 是当下主流的云计算解决方案，但云计算存在如下问题：

① 云计算主要投入是X86 服务器、电费及垄断的电信基础设施，导致硬件和基础设施成本居高不下；

② 指数增长的需求与有限供给的云计算资源之间存在巨大的鸿沟，未来无法支撑增长的需求，导致需求不能得到有效满足；

③ 集中式云计算模式导致数据的上传和下载瓶颈无法解决；

④ 大数定律昭示着高度集中的模式一定会单点失效，系统可靠性下降

⑤ “守夜人”的随时窥探，让数据隐私无从保护，且易受干扰。

其它去中心化存储网络如IPFS[6] 和FileCoin[5]提出了新思路，以 Token 作为激励手段，聚合存储矿工，成为去中心化存储的标杆。但IPFS 依赖分布在全球的大型存储矿机及服务器，其矿机全部为新增设备投入，无法利用过剩的智能设备，相比于雾计算，成本没有绝对下降。IPFS 没有突破存储与传输技术，BitTorrent 从效率层面无法承担下一代去中心化基础设施引擎的使命。具体而言，IPFS 有如下缺陷：1）IPFS 采用原始数据分块存储，为了增加可靠性及提供CDN 服务， 复制数量过多，全网存储效率低；2）IPFS 采用bitswap 策略在存储矿工上随机部署数据， 数据分布与用户需求不匹配，文件缓存有空洞，导致下载速度低；3）没有解决 NAT 穿透和UDP 传输，直接复用底层传输协议并采用中继模式，导致传输速度极其不稳定，体验极差；4）无法有效 对抗由于设备不稳定带来的网络抖动问题，需要更多的冗余来对抗不稳定，系统开销大。类似的，Sia[7]重点在于智能合约的创建，Storj[8]则提供现收现付的机制要求用户一直在线， MaidSAFE[9]对效率的关注也比较弱。

20 多年来，没有解决方案在P2P 效率层面作出真正的突破，相应的，当下不存在能与中心化云存储相匹敌的去中心化存储解决方案。

另外，去中心化存储网络依赖区块链实现去中心化的交易，交易 TPS 正比于存储网络中的文件数量，文件数量的无限性与区块链交易性能低下形成尖锐的矛盾。

Galaxy Network 为解决上述问题，提出了如下解决方案：

① 低成本：矿工保存经信道编码[1,16]后的条带，条带存储格式对加速矿工存储空间需求降低几十到百倍；闲置设备构成的雾计算模式，其特征是共享过剩闲置资源，成本为 0，所有闲置设备资源总和远大于所有IDC 资源总和

② 高可靠性：文件编码后存储，形成 2.5 倍备份方案，提供 99.99999%的存储可靠性，超越 3 倍备份方案 99.9%的可靠性，存储可靠性提升 10000 倍；如果存储 3 倍冗余，可以达到 99.9999999%的存储可靠性

③ 冗余备份潮汐效应：通过潮汐效应控制冗余倍数，冷数据保存 2.5 倍到 3 倍，维持99.99999%的存储可靠性；对于热数据，复制几十倍到几千倍的冗余，形成可靠的 CDN 服务

④ 100Mbps 高速下载：条带保存在几百个甚至几万个矿工上，文件可从几百个矿工同时下载，几百个矿工的上行带宽总和远大于下行带宽，这种技术模式可以实现超高速下载

⑤ 高并发：链下交易市场以及以DPoS为共识算法的区块链网络，解决超大并发交易的瓶颈

Galaxy Network 是一个比IPFS 快 100 倍的商用级去中心化存储和传输网络：

① 高效率

a) 采用信道编码[1,16]，全网存储效率提升了几十倍到百倍

b) 这是雾计算，降低设备加入门槛，符合共享经济的精髓：过剩产能、人人参与

c) 达到商用级服务水平的系统，未来传输峰值速度可突破 500Mbps ~ 1000Mbps

② 激励相容

a) 经济系统自洽，有效激励矿工加大投入，提高网络的整体价值

b) 提升交易，促进需求的爆发

c) 提升Token 价值

③ 丰富的应用场景

a) 开放源代码，与社区形成共识

b) 集成Merkle DAG 文件系统，形成一个以去中心化文件系统为基础、多场景的生态系统

c) 包括但不限于：数据库、去中心化网站、文件分享系统、去中心化社交网络、去中心化电商网络、Git 版本管理系统、大数据计算平台、永不丢失的存储系统、版权分发系统、超高速流媒体分发系统、实时加密通讯等

2 Galaxy 网络定义

去中心化存储和传输网络聚集了由多个独立存储矿工和加速矿工提供的存储和加速服务，并且能自我协调的提供存储和加速服务给客户。这种协调是去中心化的、无需信任的：通过协议的协调与个体参与者能实施验证操作，系统可以获得安全性操作。

2.1 系统组成

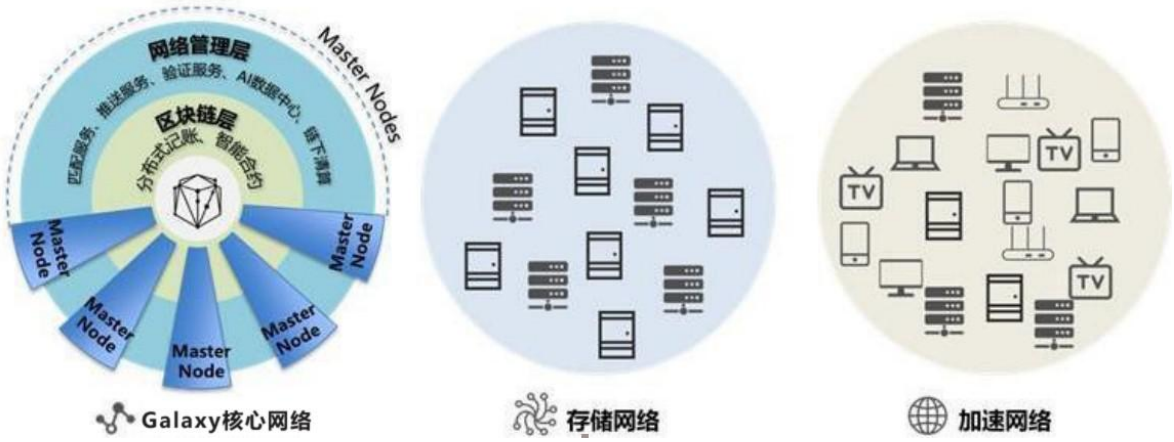


图 1. Galaxy Network 系统组成

Galaxy Network 由下面三个部分组成：

Galaxy 核心网络一方面作为区块链，提供公开不可篡改的记账能力；另一方面作为 AI 数据平台，动态感知用户需求及网络状态的变化，进行全局资源调度，满足全网体验最优，成本最 低。

存储网络聚合存储矿工的存储能力，提供近乎无限的存储空间，信道编码[1,16]进一步降低冗余备份数量，存储可靠性提高到 99.99999%。存储网络以冷数据为主。

加速网络聚合过剩闲置资源的带宽能力，提供 100Mbps 的超高速传输服务，加速矿工最小剩余存储空间只需 50MB；由 AI 算法基于全网状态完成缓存数据在全网加速矿工的调度。加速网络以热数据为主。

Galaxy 核心网络：

- 区块链层
  - 提供分布式记账及智能合约服务
  - 由多个Master Node 组成，DPoS+PoC 共识机制，支持 10000 TPS
  - 出块即挖矿，参与出块并获得奖励
- 网络管理层
  - 提供订单匹配服务、存储证明验证服务、链下可审计的清算服务
  - 基于AI 算法的缓存调度、推送服务及存储修复服务

存储网络：

- 百万级带硬盘的存储矿工，要求Token 抵押、7*24 小时在线、公网IP 地址
- 为用户提供可靠存储服务
- 向核心网络提供存储证明，获得Token 回报
- 前 40%最大实际存储量矿工获得存储挖矿奖励

加速网络：

- 亿级加速矿工，支持所有接入网络的设备，包括PC、手机、机顶盒、智能电视、路由器、Pad、光猫、智能音箱等，剩余存储空间大于 50MB，对设备在线稳定性没有硬性要求
- 为客户提供加速服务
- 向核心网络提供流量证明，获得Token 回报
- 比 IPFS 快 100 倍，提供大于 100Mbps 的实时传输服务

2.2 网络协议

Galaxy Network 由核心网络、存储网络、加速网络及客户运行的协议元组(Put ，Get，Push)：

- Put(data) → key：客户端执行Put 协议将数据存储在内容Hash 值key 下
- Get(key) → data：客户端执行Get 协议提取保存在键值 key 下的数据

- Push(data) → key： AI 数据平台指令推送服务向加速网络推送缓存数据，形成分布在加速网络上的缓存数据，这些缓存数据是Get 协议运行的前提

2.3 系统属性

成本:

成本分为存储成本及加速成本。在同等条件下，存储成本比公有云存储成本降低 80%，加速成本比传统CDN 成本降低 90%~95%。

体验:

客户关注数据的可提取性及传输体验，其它分布式存储网络由于数据分布的数量、完整性及地域的不确定性，无法和公有云在体验上进行竞争，不具备主流场景的商用能力。Galaxy Network 在传输体验上超越公有云，我们定义下载速率大于 100Mbps，比 IPFS 快 100 倍，未来突破 500Mbps ~ 1000Mbps 的传输能力。

数据完整性：

如果有任意成功的Put 操作将数据D 保存在键 key 下，那不存在有限的对手A 能使得客户在对键 key 执行Get 操作接受D', 其中D' 不等于D。

存储可靠性:

一个成功的Put 操作的定义是(D，f, m), 它的输入数据被存储在m 个独立的存储矿工中，并且它可以容忍最多f 个故障存储矿工。如果有小于f 个故障存储矿工，则对存储数据Get 操作成功。

例如数据经过信道编码[1,16]后，编码条带存储在 25 个存储矿工和加速矿工上，第一个存储矿工存储 1 份完整数据D 的编码副本R，第 2~25 个矿工保存编码后的 1/16 数据量副本。这个方案为 1+16+8 冗余备份，m = 25, f = 10，小于 10 个矿工故障，Get 操作成功。

公开可验证：

对于每个成功的Put 操作，存储网络的存储矿工可以生成数据正在被存储的证明。这个存储证明必须说服任何只知道 key 但并不能访问 key 所对应的数据的有效验证者。

公开可审计:

公开可审计代表如果所有存储证明的操作轨迹被公开存储，并且在未来能被检查在正确的时间上数据确实被存储了。

激励:

如果存储矿工和加速矿工由于成功提供了存储和加速服务而获得激励，或者因为作弊而得到惩罚。所有存储矿工和加速矿工的优势策略是存储数据和缓存数据，并且保持在线状态。

3 Galaxy 网络构建

Galaxy Network 是可升级，可公开验证和激励式设计的去中心化存储和传输网络。客户为了存储数据和下载数据，向存储矿工及加速矿工付费。存储矿工和加速矿工提供磁盘空间和带宽来赚取Token。存储矿工和加速矿工只有在他们提供的服务被验证正确时才会收到付款。

在本节中，我们介绍基于Galaxy Network 定义的构建过程。

3.1 系统概述

Galaxy Network 由下面这些角色组成和定义：

3.1.1 参与者

任意用户都可以作为客户、DAPP、存储矿工、加速矿工、Master Node 参与Galaxy Network。

- 客户

客户通过DAPP 向Galaxy Network 发起Put 协议存储数据，或Get 协议请求数据。客户和矿工签署交易订单，存储及流量费用由为客户提供服务的DAPP 支付。因此，客户通过DAPP 使用Galaxy Network 的服务时，拥有和其它互联网服务一致的用户体验：无需拥有区块链钱包。

- DAPP

DAPP 通过预支付Token 使用 Galaxy Network 的存储及带宽资源，并向其客户提供服务。DAPP 使用Galaxy Network 可以得到如下优势：1）较低的存储及带宽价格；2）获得Galaxy Network 的Token 激励，鼓励DAPP 的繁荣发展；3）DAPP 的客户在没有安装钱包时，客户作为加速节点参与到Galaxy Network，其加速收益为 DAPP 所得。

- 存储矿工

存储矿工通过提供存储空间并且响应客户的Put 请求参与到Galaxy Network。要想成为存储矿工，客户必须提供与存储空间成比例的抵押，并且为了获得更多的订单，存储矿工必须提供稳定在线时长、足够的存储空间、以及高质量的宽带连接。存储矿工与客户达成存储订单后，必须生成存储证明以证明存储矿工在特定时间存储了客户的数据。如果存储证明验证成功，客户会支付小额费用给存储矿工。如果存储证明失败或不能提供证明，存储矿工将被取消订单或者被罚没部分抵押。实际存储量前 40%的存储矿工，获得存储挖矿激励。

- 加速矿工

加速矿工为客户提供数据加速服务。加速矿工通过响应Get 请求来参与Galaxy Network，通过 Push 协议向加速矿工快速部署数据。和存储矿工不同，加速矿工不需要抵押，不需要提供存储证明。存储矿工也可以作为超级加速矿工参与加速服务。与其它去中心化存储网络不同的地方在于，几乎任意设备均可作为加速矿工参与Galaxy Network，以零成本赚取加速收益；高质量的加

速矿工，如拥有公网IP 地址、高质量的带宽、稳定在线，则可以提供更优质的加速服务，可以通过提高报价赚取更高的回报。

- Master Node

Master Node 拥有三部分职责：

- 交易账本及智能合约
- 交易市场：存储订单匹配、存储证明验证及链下清算系统
- 存储管理系统：用于缓存管理及推送、存储故障修复

Master Node 通过出块及提供存储管理服务获得挖矿回报。

3.1.2 基础网络

由存储矿工及加速矿工组成了 Galaxy Network 的基础网络，基础网络在逻辑上包含存储网络和加速网络。存储网络及加速网络使用统一的节点架构：即统一在改进的 IPFS 架构上。但 IPFS 的 P2P 引擎被替换，用于改进IPFS 在存储效率及传输能力的不足。效率的提升是基础网络的核心优势。

由于存储网络和加速网络共享统一架构，本质上是统一的 P2P 引擎，因此，存储网络及加速网络统一了底层的存储格式：

- 采用信道编码[1, 16]，对文件D 先编码后存储， 具体定义见 3.2.2 节
- 采用条带的格式进行存储，具体定义见 3.2.3 节
- 存储网络的安全存储策略，具体定义见 3.2.4 节
- 存储和加速网络统一以条带为寻址对象，而不再以块为寻址对象，具体定义见 3.2.5 节

3.1.3 交易市场

Galaxy Network 有两个交易市场：存储市场和加速市场。存储市场允许客户为存储矿工存储数据而付费。加速市场允许客户为加速矿工提供加速服务而付费。交易市场由 Master Node 运行，保证矿工在提供服务时可以得到客户的奖励，同时也要保证客户数据真实存储在存储矿工上。因此，交易市 场是一个可验证的市场，一个基本的交易流程被分解为两个阶段：订单匹配阶段和结算阶段。

存储市场运行 Put 协议：

- 订单匹配：
  - 客户和存储矿工分别提交订单到交易市场
  - 匹配服务根据质量导向原则对客户及存储矿工的订单进行匹配
  - 当订单匹配成功后，客户发送数据碎片给存储矿工
  - 双方签署交易订单并提交到区块链
- 结算：
  - 验证服务定期向存储矿工发起存储证明挑战
  - 存储矿工生成存储证明，提交给验证服务
  - 验证服务验证存储矿工生成的存储证明，验证失败则罚没存储矿工部分抵押
  - 基于有效的存储证明， 验证服务生成向存储矿工支付的指令

加速市场运行 Get 协议：

- 订单匹配 ：
  - 客户向加速矿工广播订单
  - 加速矿工返回报价订单
  - 客户决定是否与加速矿工建立交易订单
- 结算：
  - 加速矿工发送小部分碎片给客户，同步发送一个经加速矿工签名的流量证明(收据)
  - 客户对接收到的流量证明签名，然后返回给加速矿工
  - 加速矿工继续发送碎片数据给客户
  - 加速矿工向交易市场提供流量证明，获得奖励

Push 协议：

Push 协议是加速市场的支撑协议，通过 AI 数据平台动态感知客户加速需求及网络状态的变化，快速高效在加速网络中部署客户需要的缓存数据，形成有序的数据缓存分布是超高速传输的基石。Push 协议由存储矿工和推送服务器承担，根据其推送的流量，获得加速矿工售卖带宽的分成。

3.1.4 存储证明

存储矿工必须让他们的客户相信，客户付费的数据已经被存储矿工存储。因此，我们提出的存储证明(Proof-Of-Capacity) 允许存储矿工证明数据已经被存储到了唯一专用的物理存储设备上。存储唯一的物理副本使客户或Galaxy Network 能够检查存储矿工是否不存在将多个数据副本重复拷贝到同一存储空间。存储矿工只有正确提供了存储证明，才能得到客户的支付。

3.1.5 流量证明

在加速市场，加速矿工和客户端之间交换数据是在没有第三方信任的中介情况下进行。因此加速矿工不能在加速服务完成后才得到客户的支付，而必须在加速服务过程中，加速矿工在确认上一个流量碎片得到支付后，再继续提供流量服务。这种模式导致了海量的碎片化交易。为解决这个问题，我们定义了流量证明(Proof-Of-Flow)方案，解决高并发交易的问题。

3.1.6 共识算法

PoS 和 PoW 是当前最为流行的两种共识机制。Galaxy Network 定位为去中心化存储网络，交易量正比于存储网络中的文件数。 以PoW 和PoS 共识算法为基础的区块链交易性能无法支撑 Galaxy Network 的交易需求。 我们选择DPoS 共识算法作为解决方案的一部分。

3.2 基础网络

3.2.1 矿工架构

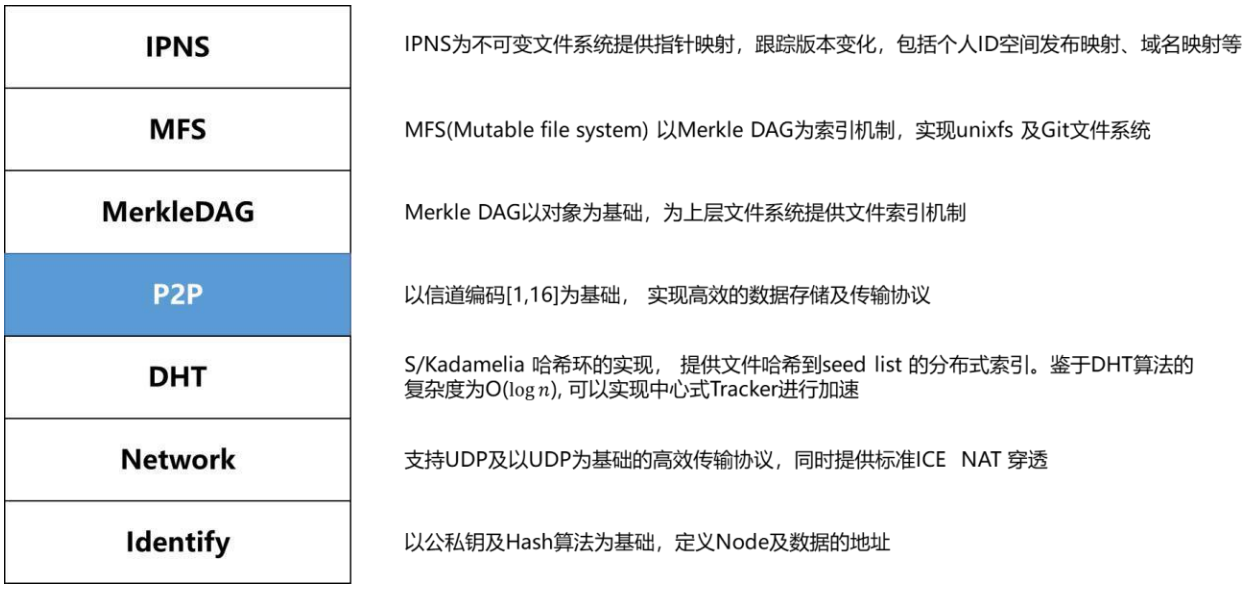


图 3. 矿工节点系统架构

矿工节点架构继承IPFS[6]的整体架构，Merkle DAG、IPLD、IPNS 等上层功能被保留，但 P2P 引擎被替代，用于改进IPFS 的低效及体验差的缺点，下表是Galaxy Network 与 IPFS/Filecoin [5, 6]的对比：

机制	IPFS/FileCoin	Galaxy Network
信道编码	没采用纠删码	采用信道编码算法[1,16]
存储格式	以块为存储对象，存储效率及索引效率低	以条带为存储对象，存储效率及索引效率、传输效率高
索引结构	Merkle DAG + DHT	Merkle DAG + DHT + Tracker
数据分发	基于信誉、账本的bitswap 策略，随机性强，数据无序分布，不具有全局合理性	主动进行缓存分布管理，缓存分布（缓存数量和地域分布）能完美响应客户加速的需求，每个加速矿工保存百分之一数据量
存储效率	节点保存块数据，存储效率低，不能被有效删除，冷数据占用大量存储空间	保存条带，但数据量是块的百分之一，存储效率高，如果数据长期无人访问，条带被删除；全网存储成本低
矿机成本	专用矿机，成本高	矿机门槛低，只需大容量硬盘及优质带宽接入；对于加速网络，几乎任意 0 成本智能设备均可加入网络
传输体验	乱序下载，下载体验不稳定，下载速度慢，不适合流媒体； 没有 NAT 穿透，连接效率及实时性差，无法适应中国复杂网络环境	超过百个矿工同时提供数据顺序下载，实时传输速度大于 100Mbps, 传输能力上超越CDN 及BBR TCP [14,15], 并且在弱网条件下卡顿率比BBR TCP 降低 20 倍以上
存储故障恢复	通过存储证明验证存储是否失效，	存储矿工通过心跳汇报在线状态，根据

	不能在业务层面执行存储恢复策略； 在P2P 层面，通过bitswap 扩散缓存数据，有一定的保护作用；	全局存储矿工在线概率计算修复门槛，低于门槛则启动故障存储的修复
订单匹配	链上订单撮合，交易并发能力受限于区块链	链下订单匹配， 交易并发无上限
存储证明	PoRep 及PoST 证明，交互比较少，但证明复杂度高	PoC存储证明，能防止女巫攻击、外包攻击和生成攻击
验证存储证明	链上保存存储证明，由于文件数量巨大，区块链存储空间及并发是巨大的挑战	Master Node 发起挑战及验证存储证明
支付服务	利用闪电网络[9,10]完成微支付，用户提现时，从闪电网络提交区块链进行记账	加速矿工收集流量证明，并由清算系统合并碎片化交易生成账单，由智能合约完成支付，清算系统能极大降低业务的交易频度，提升交易系统容量；清算系统还可以执行复杂交易，譬如免费额度和客户费用转移到DAPP 支付等功能
出块者	存储矿工	Master Node+存储矿工
共识算法	时空证明PoST	DPoS + PoC

3.2.2 信道编码

IPFS[6]以分块的方式存储，文件 D 被分成M 块，每个块离散分布在不同的节点。与IPFS 不同，Galaxy Network 采用了空间变换，将文件以块为单位变换到信道编码空间，每个块包含 N 个piece, 条带（stripe）包含M*X 的piece 矩阵，M 为文件包含的块数，X 为每个块包含的piece 数，X≤N。Galaxy Network 统一以条带为存储对象。从任意N/X 个节点获得数据后，即可解码恢复原文件。

下图描述了文件D 编码的过程：

对文件 D 以块为单位通过信道编码算法[1,16]进行编码，输入 N 个 piece, 输出 K 个编码 piece, 编码 piece 各不相同，可以从 K 个 piece 中任意选取 N 个 piece, 即可恢复原始块。K > N。 信道编码的算法复杂度为 O(n), 解码性能在苹果 A5 芯片上超过 200Mbps, 比 Reed Solomon 码(O(n^2)) [4] 快 100 倍以上。

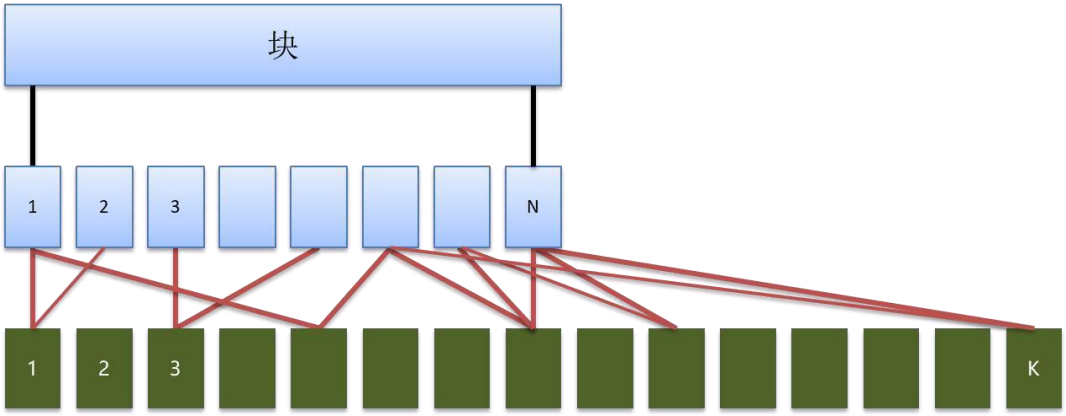


图 5. 信道编码块生成piece 的过程

文件D 编码输出的集合如下图：

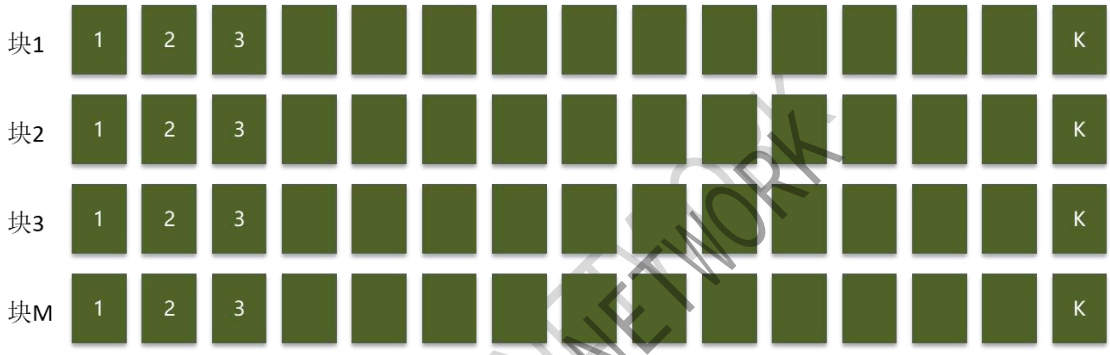


图 6. 文件输出K 个piece 的集合

3.2.3 存储格式

条带为矿工存储格式，条带的定义如下：

- 每个条带包含文件D 的所有块, 从块 1 到块M
- 每个块从K 中随机选择X 个piece, X ∈ {1，2，…, N}
- 条带是一个M * X 的piece 矩阵
- 所有条带, 均不能出现重复piece

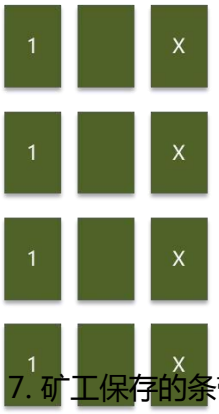


图 7. 矿工保存的条带

3.2.4 安全策略

为了保证Galaxy Network 的存储高可靠性，必须对存储数据进行一定的冗余备份，我们定义了一种 2.5 倍冗余存储方案：

- 存储矿工 1 存储数据D 的一份完整副本R，R 为M * N 的条带
- 存储矿工 2~25 存储数据D 的副本R′，R′ 为 M * N/16 的条带
- 从存储矿工 1 下载数据或者从加速矿工 2~25 中随机挑选 16 个存储矿工即可恢复D
- 上述形成 1 + 16 + 8 的冗余存储方案

矿工的在线率分布差别极大，在部分矿工在线率低的情况下，1+16+8 冗余存储方案并不能保证存储可靠性达到 99.99999%。因此 Galaxy Network 根据矿工在线率的实际分布，动态决策数据冗余的倍数，维持存储可靠性大于 99.99999%。

3.2.5 索引结构

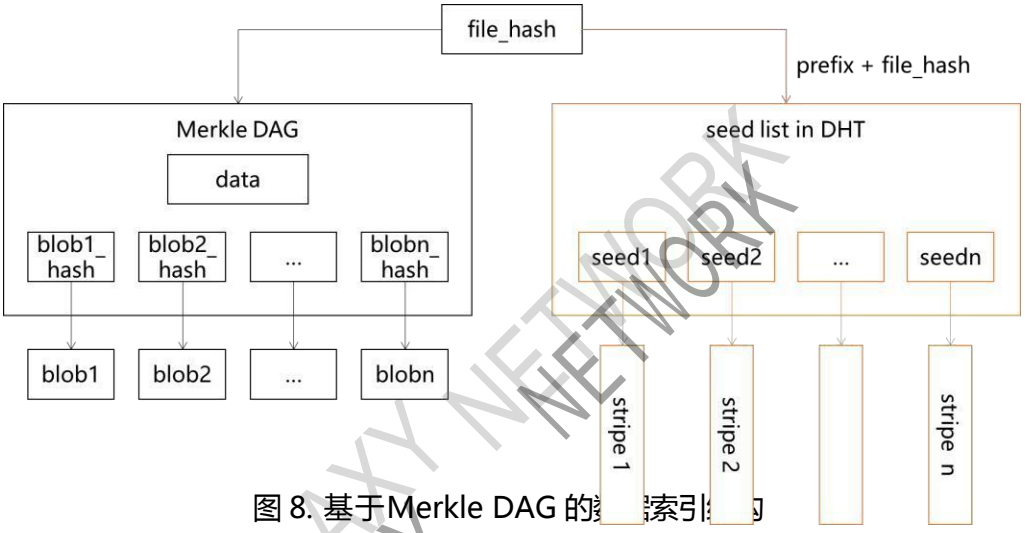


图 8. 基于Merkle DAG 的数据索引结构

在 IPFS 的实现中， 以Merkle DAG 作为数据的统一索引结构。

其中：

- blob_hash = Hash(blob)
- file_hash = Hash(blob1_hash || blob2_hash || ... ||blobn_hash)
- 通过key=file_hash 在DHT 网络中寻址对应Merkle DAG 对象，找到 Merkle DAG 中包含的 blob 列表
- 通过key=blob_hash 在DHT 网络中寻址到对应的blob

IPFS 的索引结构有如下致命的性能缺陷：

- Merkle DAG 是一种数据块的间接索引机制，当一个文件被分成很多blob 时，需要多次寻址
- DHT 网络的寻址时间复杂度为 O($\log n$), Merkle DAG 基于 DHT 寻址导致寻址时间非常长
- blob 被分散在多个存储矿工，导致连接效率和传输效率极低

在Galaxy Network 中， 基于IPFS Merkle DAG 的索引结构，做出如下改进：

- 保留Merkle DAG 的索引结构不变
- blob_hash 键值到seed list 的映射保存在DHT 网络
- blob_hash 只用于数据去重及验证数据的完整性，不再用于寻址
- 寻址以prefix+file_hash 为键值建立到seed list 的映射，增加prefix 便于区别file_hash 到merkle DAG 的映射关系，这种寻址映射可以一次查询，返回所有矿工列表
- 存储矿工及加速矿工存储条带，客户无需与矿工频繁交换存储状态及切换矿工，连接效率及传输效率高。

3.3 交易市场

3.3.1 订单

下列数据结构与交易市场相关，是交易市场的核心数据结构：

存储订单：

- size, 提交存储的文件大小
- funds, 客户充值金额
- time， 客户存储文件的最大时长，单位秒
- price, 客户报价
- sign, 客户签名

询价订单：

- space, 存储矿工剩余的存储空间
- price, 存储矿工的报价
- sign, 存储矿工签名

交易订单：

- 存储订单
- 询价订单
- timestamp, 被存储矿工签名的时间戳
- file_hash, 存储文件的hash 值
- sign, 客户及矿工签名

3.3.2 存储市场

存储市场是可验证的市场，它允许客户请求他们的存储数据和存储矿工提供他们的存储空间。存储市场运行Put 协议：

客户端

1. 充值：客户为存储订单充值

输入：

- 文件哈希
- 文件大小
- 充值金额

输出：

- 返回 0 则表示区块链成功接收充值交易

2. 添加订单

输入：

- 存储订单

输出：

- 存储矿工的询价订单列表

处理：

- 客户从DHT 网络中查询是否存在重复块
- 如果存在重复块，把<file_hash, 存储矿工>添加到DHT，为该文件创建索引
- 重新计算所有未重复块的文件大小，这些块是需要提交存储的
- 客户向匹配服务提交存储订单
- 匹配服务返回存储矿工的询价订单列表

3. 发送数据

输入：

- 存储订单
- 询价订单
- 数据p
- file_hash

输出：客户签名的交易订单

处理：

- 发送数据<file_hash, p, 存储订单, 询价订单>到存储存储矿工
- 接收到存储矿工的交易订单
- 验证交易订单的有效性
- 客户签名交易订单，发送交易订单到区块链

存储矿工

1. 抵押

输入：

- 抵押金额

输出：

- 输出 0 表示成功

2. 接收数据

输入：

- 存储矿工私钥
- 存储订单
- 询价订单
- 数据p
- file_hash

输出：

- 存储矿工签名的交易订单

处理：

- 验证存储订单的合法性
- 编码数据 R= entropy_encode(p), 保存R
- 签名交易订单，发送给客户
- 把<file_hash, 存储矿工> 添加到DHT 网络，创建索引

3. 生成存储证明

输入：

- N: 表示该文件被分割成多少块
- k：表示每一个存储矿工在存储后必须上报的存储证明文件子块数
- Z: 表示当前区块链最后一个区块的哈希值
- s: 表示为随机数
- pk/sk 存储矿工公私钥对

输出：

- 输出存储证明到验证服务，输出结果见 3.4.2 节

匹配服务

4. 匹配订单

输入：

- 存储订单

输出：

- 存储矿工询价订单列表

处理：

- 在所有存储矿工中找出符合条件的询价订单
  - 存储矿工剩余存储空间大于存储订单文件大小
  - 存储矿工报价小于等于存储订单的报价
- 在满足上述条件的存储矿工中执行如下算法，找出score最大的存储矿工提供存储服务
  - 在线率 online_ratio: 存储矿工24小时在线率
  - pledge：存储空间抵押
  - pledge_avg: 所有存储矿工抵押的平均值
  - NAT类型评分 nat_score：

- ✓ 公网IP地址 ：100
- ✓ Full coneNAT ： 50
- ✓ IP 限制型NAT ：30
- ✓ 端口限制型NAT：10
- ✓ 对称型NAT ：0

➢ proof_succ_score：存储矿工所有存储证明成功率
➢ score = online_ratio * 40 + (pledge / pledge_avg) * 30 + nat_score * 20 + proof_succ_score * 10

- 返回score 最大的 3 个询价订单列表

验证服务

5. 存储挑战

输入：

- 交易订单
- k：表示每一个存储矿工在存储后必须上报的存储证明文件子块数
- Z: 表示当前区块链最后一个区块的哈希值
- s: 表示为随机数

输出：

- 0：成功，1：失败或超时

处理：

- 根据交易订单生成存储挑战
- 接收存储矿工的存储证明
- 验证存储证明是否合法，超时没接收到存储证明判定失败
- 把存储证明验证结果发送给清算系统

清算服务

6. 接收存储证明

输入：

- 存储证明验证结果

输出：

- 无

处理：

- 接收存储证明验证结果
- 归并成功的存储证明，生成账单，发送给智能合约进行支付
- 失败的存储证明，发送给智能合约扣除存储矿工部分抵押

推送服务

7. 安全备份策略

输入：

- file_hash ：文件的加密哈希值，用于索引该文件
- 存储矿工列表
- 条带中每个块包含的piece 数

输出：

- 无

处理：

- 推送服务执行 1+16+8 安全备份策略，其中一份完整数据副本已保存在第一个存储矿工上，另外 24 份条带推送到 24 个存储矿工或加速矿工
- 推送服务根据file_hash 下载该文件的完整数据副本R
- 对下载的数据进行解码，恢复原始数据，D=entropy_decode(R) [1,16]
- 对 D 进行编码，生成存储矿工需要的条带
- 以 piece 为单位增加 1 字节校验码
- 推送条带到存储矿工

3.3.3 加速市场

Get 协议运行周期:

客户端

1. 下载订单

输入：

- file_hash

输出：

- 文件D

处理：

- 客户向智能合约充值
- 客户根据file_hash 从DHT 网络获取矿工列表（存储矿工、超级加速矿工、加速矿工）
- 客户发送订单请求到矿工，获得矿工报价
- 为提升启动阶段的响应速度，优先挑选存储矿工及超级加速矿工下载数据，在存储矿工及超级加速矿工列表中挑选价格低的提供服务
- 加速矿工连接建立成功后，利用加速矿工替换存储矿工及超级加速矿工
- 在加速矿工中选择报价低的提供服务
- 接收加速矿工数据及流量证明
- 客户签名后，发送签名后的流量证明到加速矿工
- 收到流量证明后，加速矿工继续推送数据到客户
- 客户发现部分加速矿工的传输质量不能满足实时性时，终止与该加速矿工的交易，重新挑选其它加速矿工提供服务
- 如果出现加速矿工攻击行为，伪造及篡改数据，客户编码接收数据成功后，校验哪些加速矿工提交伪造数据，把加速矿工加入黑名单
- 客户下载数据成功后提交给上层应用

加速矿工

2. 接收下载订单
输入：
- 客户下载订单

输出：
- 询价订单

处理:

- 加速矿工接收到客户的下载订单后，发回询价订单
- 加速矿工接收到客户的下载请求，发送小片数据，同时发送经加速矿工签名的流量证明
- 接收到客户签名的流量证明
- 加速矿工继续向客户发送小片数据
- 加速矿工提交流量证明到清算系统

清算
3. 接收流量证明
输入：
- 加速矿工流量证明

输出：
- 无

处理：
- 接收加速矿工流量证明
- 归并碎片化流量证明，生成账单
- 归档流量证明到Galaxy Network 存储网络，供第三方公开审计
- 提交账单到智能合约，完成支付

3.3.4 Push 协议

AI 数据平台
1. 接收状态汇报
输入:
- 加速矿工汇报剩余存储空间、条带列表、NAT 类型
- 客户端汇报下载文件列表
- P2P%（P2P%=加速矿工流量/(加速矿工流量+超级加速矿工流量+存储矿工流量)

输出：
- 无

处理：
- 对接收到的数据进行清洗，存入本地LevelDB
- 把清洗后的数据保存在Galaxy Network 存储网络，可以供第三方公开访问

2. 智能决策

输入:

- 清洗后的数据

输出：

- 增加推送
- 删除缓存

处理：

- 根据下述维度进行决策
  - 文件访问频度
  - 客户访问地理分布
  - 加速矿工剩余存储空间
  - 加速矿工在线时长
  - 加速矿工NAT 类型
  - P2P%
- 删除缓存
  - 统计全网加速矿工剩余存储空间，剩余存储空间< 10% * 总存储空间，执行删除策略
  - 基于LRU 算法筛选冷文件
  - 删除加速矿工上保存的冷文件条带
- 增加推送
  - 根据文件访问频度、P2P%、该文件条带数量决策是否要增加推送及推送数量
  - 决策推送后，根据客户访问地理分布、加速矿工在线时长、加速矿工NAT 类型、加速矿工剩余存储空间，挑选出合适的加速矿工列表
  - 把决策结果通知到推送服务

推送服务

3. 接收推送命令

输入：

- file_hash ：文件的加密哈希值，用于索引该文件
- 加速矿工列表
- 条带中每个块包含的piece 数

输出：

- 无

处理：

- 推送服务根据file_hash 下载该文件D 的完整数据副本R
- 对下载的数据进行解码，恢复原始数据，D=entropy_decode(R) [1,16]
- 对 D 进行编码，生成推送给加速矿工的条带
- 以 piece 为单位增加校验码
- 推送条带到加速矿工

加速矿工

4. 接收数据

输入：

- 编码后的条带
- 条带中每个块包含的piece 数量
- file_hash ：文件的加密哈希值，用于索引该文件

输出：

- 无

处理：

- 校验接收到的piece，校验失败则丢弃
- 保存校验成功的条带
- 提交<file_hash, 加速矿工>到DHT 网络

3.4 存储证明 (Proof-Of-Capacity)

在 Galaxy Network 中，存储矿工必须让他们的客户相信，客户付费的数据已经被存储矿工存储，因此，存储矿工必须接受客户或Galaxy Network 的挑战，存储矿工基于挑战生成存储证明给Galaxy Network 或客户来验证。

3.4.1 动机

存储证明允许用户（验证者V）将数据外包给存储矿工（即证明人 P），用户（验证者 V）可以反复检查存储矿工是否依然存储数据D。用户可以用比下载数据高效的方式来验证保存在存储矿工的数据完整性。存储矿工（证明人P）通过对一组随机数据块进行采样和提交小量数据来生成拥有的概率证明作为给用户的响应。

我们需要强大的算法阻止作恶矿工利用下面三种类型攻击而获得奖励：女巫攻击(Sybil attack)、外包攻击(outsourcing attacks)、生成攻击（generation attacks）

女巫攻击：

作恶矿工可能通过创建多个女巫身份假装物理存储很多副本，但实际上只存储一次。

外包攻击：

作恶矿工在挑战时可以快速从其他存储矿工获取数据，作恶矿工可能承诺能存储比他们实际物理存储容量更大的数据。

生成攻击：

作恶矿工可能宣称要存储大量的数据，但是他们使用小程序有效地生成数据。如果这个小程序小于所宣称要存储的数据，则作恶矿工获得的奖励增加。

3.4.2 存储证明

容量证明(PoC)[5, 10]是一个新型的存储证明。它允许存储矿工（即证明人 P)说服用户（即验证者V）一些数据D 已被存储到它唯一的专用物理存储上了。我们的方案是一种交互式协议。当证明人 P:

a) 承诺存储数据D 的n 个不同的副本R（独立物理副本），然后
b) 通过响应协议来说服验证者V，P 确实已经存储了每个副本。

下面的方案能有效阻止了女巫攻击、外包攻击和生成攻击。

第一步：生成数据D 的在存储矿工P 的唯一副本R

- 数据D 为用户的原始输入数据
- 采用信道编码进行编码，R = entropy_encode(D)
- 保留R，删除数据D
- R 全局唯一，与保存在其它存储矿工的副本不同，也无法通过再次调用编码器生成相同副本R

第二步： 存储矿工提供证明 [10]

参数定义：

N: 表示该文件被分割成多少块
k：表示每一个存储矿工在存储后必须上报的存储证明文件子块数
Z: 表示当前区块链最后一个区块的哈希值

s: 表示为随机数
R[n_i]副本R 第 n_i块pk/sk
存储矿工公私钥对sign:
签名函数

π_{n_i} 为 R[n_i] merkle 证明

σ_0 = 0
n_1 = Hash(pk || Z || s) mod N
for i=1,2,...k
Do:

h_i=Hash(pk || Z || σ_{i-1} || R[n_i])

$\sigma_i = sign_{sk}(h_i)$

n_{i+1}=Hash(pk || Z || σ_i) mod N

Done
所有n_i形成了一个集合 Gn = {n_1, n_2, n_3, ..., n_k}
存储矿工交付下面的ticket 供验证者验证：

ticket=(pk, s, {R[n_i], σ_i, π_{n_i}}) ∀i∈Gn

第三步：验证
验证者V 根据pk, s, Z, k 等参数生成集合G'n
G'n != Gn，校验失败

G'n == Gn 则：
验证者 V 根据 ticket 中的{R[n_i], σ_i, π_{n_i}}∀i∈Gn 中提供的文件子块索引以及π_{n_i}来校验 merkle 树，一直校验到树的root，root 相等则验证成功

3.5 流量证明(Proof-Of-Flow)

3.5.1 动机

加速市场存在着海量请求、数据碎片化请求的问题，针对加速市场的订单匹配及支付存在着巨大的挑战。

加速订单匹配：

客户端必须找到提供所需要数据碎片的加速矿工，并且在定价之后直接交换数据。这意味着订单簿不能通过区块链来运行，因为这将成为加速请求的瓶颈。因此，加速订单只能在链下保存。我们要求双方传播自己的订单。

无信任方的加速市场：

在不存在双方都信任的第三方中介的情况下，是不可能进行公平交换的[11]。在加速市场，加速矿工和客户端之间交换数据是在没有第三方信任的中介情况下进行。加速矿工通过将数据分割成多个碎片，发送一个碎片到客户端，要求客户端支付，然后再发送后续碎片。在这种方式中， 如果客户端停止付款，或者矿工停止发送数据，任何一方都可以终止这个交易。

小额支付通道：

客户端收到数据碎片后需要立刻支付，加速矿工只有在确认收到付款后才提供数据碎片，通过区块链来确认交易在性能上是不可能实现的。所以，其它类似系统发展了一种链下微支付的解决方案[12,13], 这种以侧链为机制的闪电网络性能约为 2000~3000TPS。

在 Galaxy Network 中，每个加速请求会向几百个加速矿工下载数据，并且同时生成几百个小额支付。这个小额支付量级比其它类似去中心化存储系统增加百倍以上，即使是中心化的支付系统也难以承受这样的并发压力。因此，通过提升支付通道的性能不可能真正解决小额支付带来的问题。

3.5.2 流量证明

对于加速市场，由于客户的海量请求和支付的碎片化，这个支付量级不可能上链交易，即使闪电支付网络也不可行。为了解决海量支付的问题，我们引入了可公开审计的清算服务来归并碎片化交易，指数级降低交易的频度。当加速矿工向客户发送一段碎片后，要求客户生成经双方签名的流量证明，只有客户正确返回流量证明给加速矿工，加速矿工才继续向客户发送下一段碎

片。加速矿工持有该流量证明，提交给清算服务，由清算服务周期性生成账单，供区块链智能合约支付。加速矿工把流量证明归档到Galaxy Network 的公开存储区，供第三方审计。

加速矿工持有的流量证明：

Proof-Of-Flow=(pk_a, pk_c,L, price, $sign_{sk\ c}(sign_{sk\ a}(L, price))$)

式中：

pk_a, sk_a ：加速矿工公私钥对

pk_c, sk_c ：客户端公私钥对

L ：发送的数据片段长度

price : 流量价格

3.6 共识与出块

区块链的共识机制，是系统参与各方的纽带，将系统整体与各参与方的利益协调一致，具体规则反应各方的利益分配。Galaxy Network 共识机制的目标是：10000 TPS，10 秒出块，并以参与者对系统的贡献程度获取对等的收益。高TPS 满足 10 亿级文件存储规模，10 秒出块满足收益快速到账，收益分配使Galaxy Network 的各方获取公平激励。

共识算法需要实现上述目标。系统的参与者，都是系统的贡献者，其中：

存储用户：得到安全可靠的存储服务，与快速高效的全球加速服务；

存储矿工：以提供存储基础服务作为贡献，存储服务费用反应了这个基础服务的收益，整个系统的繁荣发展离不开众多稳定优质的存储矿工，因此额外分配收益给到提供服务的存储矿工， 鼓励对系统的建；

加速矿工：类似的，加速服务费用反应了其加速基础服务的收益；

Master Node：Master Node 完成出块，以提供一个公开透明，不可篡改，安全可信的区块链基础设施，会得到挖矿的收益。

Galaxy Network 共识算法，即 DPoS + PoC（委托权益与存储证明），兼顾出块与矿工的权益。具体来说：

一方面，推选 Master Node 作为出块者，用户通过投票的方式，推举多个Master Node ，服务于 Galaxy Network 网络进行轮流出块，出块间隔为 4分钟，出块后需要传播到区块链网络，其它Master Node 进行验证并回复签名证据，得到超过 2/3 其它 Master Node 的认同后，区块得以被确认，Master Node 作为出块者会得到回报，回报正比于其得到的投票，此为DPoS。实现 10000 TPS 与 4分钟确认。

另一方面，存储矿工通过复制证明 PoC的方式证明其工作量，加速矿工通过流量支付的方式证明其工作量，工作量以用户支付的 Token 为量化表征。存储矿工也会随着出块得到回报，回报正比于其被证明了的工作量。

4 需求实现

下面论证Galaxy Network 如何实现成本、体验、完整性、存储可靠性、公开可验证性、公开可审计、激励。

① 实现低成本

成本分为存储成本和加速成本：

成本结构	描述
存储成本	1+16+8 冗余备份方案 总存储数据量为 2.5 倍原始数据量，小于 3 备份存储成本; 同时由于在加速网络中的缓存相比其它网络降低几百倍，全网总存储成本降低约百倍
加速成本	5~10%流量来自于存储矿工和超级加速矿工 90~95%流量来自于加速矿工 总成本比传统CDN 降低 90% ~ 95%

② 实现体验

- 启动阶段：
  - 缩短连接建立时间, 建立到存储矿工和超级加速矿工连接数量不超过 17 个
  - 要求存储矿工及超级加速矿工有静态IP 地址或full cone NAT 类型
  - 启动时间小于 1 秒

- 正常下载阶段：
  - 建立百个加速矿工连接，客户从加速矿工下载数据
  - 这种极度碎片化和极度分散化带来几点好处：
    - ✓ 百个节点形成的上行带宽总和远大于下载所需
    - ✓ 百个节点形成负载均衡，对加速矿工上行带宽冲击非常小
  - 高效调度多个加速矿工，实时传输能达到客户网络的上限

③ 实现完整性

数据碎片以加密哈希寻址。一个Put 请求后，客户只需要存储哈希即可通过Get 操作来加速数据，并可以验证收到的数据的完整性。

④ 实现存储可靠性

只要存储矿工 1 在线或存储矿工及加速矿工 2~25 中有 16 个节点在线，客户下载数据即可恢复，其可靠性概率公式：

$$P = p + (1-p)\sum_{k=m}^{n}\binom{n}{k}p^{k}(1-p)^{n-k}$$

其中：

P 为存储可靠性概率

K 为每个存储矿工在线概率

n 为存储冗余份数

m 为恢复数据D 所需最小节点数

存储冗余份数n	最小节点数m	矿工在线概率p	存储可靠性P
24	16	90%	99.9967873%
24	16	95%	99.9999936%
24	16	96%	99.9999992%
24	16	97%	99.9999999%

⑤ 实现公开可验证和可审核性

复制证明、流量证明均被提交到Galaxy Network 的公开存储区，网络中的任意用户都可以访问备档的复制证明和流量证明验证这些证明的有效性。另外由于这些证明都不可以被篡改和删除，所以操作痕迹可以随时审核。

⑥ 实现激励

通过提供存储及流量而获得奖励。当矿工承诺存储一些数据的时候，它们需要生成证明。如果矿工忽略了证明就会被惩罚（通过损失部分抵押），并且不会收到存储的奖励。

5 治理结构

5.1 非营利组织设立

Galaxy Network 非营利组织（以下简称“非营利组织”）是在新加坡成立的非营利性公司，非营利组织致力于Galaxy Network 的开发建设、社区治理透明度倡导及推进工作，促进生态社会的安全、和谐发展。

为避免有违区块链精神的事件出现，非营利组织将通过制定良好的治理结构，帮助管理社区项目的一般轶事和特权事项。

5.2 非营利组织原则

Galaxy Network 非营利组织有三个结构性原则：

公正

进行单独管理以开发Galaxy Network 的技术体系和社区体系

非盈利

管理Galaxy Network GN的发行和分配

专业

由专业团队管理的独立法律实体

5.3 非营利组织目标

非营利组织（以下简称“组织”）的使命是发展基于区块链的分布式存储和传输生态系统，使生态用户可以享受基于信用的高可用存储和高速传输的产品和服务，同时为开发者提供一个开放平台，以进行开发、交付与增强这些产品或服务并吸引生态用户建立丰富的生态场景。

为了完成上述使命，组织将把资源投入到管理、研究和开发相关的三个目标中。管

理目标

组织将建立一个公平透明的管理流程，并积极听取生态系统内所有参与者的意见和需求，通过社区投票机制来进行技术和治理决策。开放的管理机制将能监督会员参与流程和规则的制定、GN发行、定价规则、法律事项、以及内容与合规准备相关的决策。组织将负责管理和监督Token 保存的安全性，以及Token 收支的透明度。

研究目标

组织通过与科研机构和合作伙伴合作来培育创新环境，保持 Galaxy Network 在技术指标和应用场景上的领先。合作内容包括共识算法、同态加密算法、零知识证明、再生码[2,3]、传输协议的研究、探索生态应用的新模式、推动价值创造和网络效应。组织将资助研究工作，以支持一个安全有效、提供商业交易服务的自主网络。

开发目标

组织计划指导并资助Galaxy Network 本身的开发，以及Galaxy Network 生态系统合作伙伴的培训和合作等赋能工作，确保各项研究能够快速而广泛地落地。

6 Token 经济模型

6.1 “一链双币”设计

文件存储周期通常都是按月或者年来计，考虑到用户是预付费，而存储矿工是按天结算，为了避免Token 价格波动对生态内部结算体系的冲击，故采用“一链双币”设计。

Security Token：GN

为了有效激励早期投资者、社区建设者与参与者，实现平台的生态增长，Galaxy Network 将基于以太坊ERC20 协议发放Galaxy 通证；随着未来主网上线，将按照 1：1 的兑换规则将所有基于以太坊ERC20 的Galaxy GN映射为Galaxy Network 原生币，保障所有参与者的权益。

Galaxy Network 将是一个高速增长的生态平台，未来将由百万级的存储矿工和亿级的雾计算加速矿工构成，同时将承载海量的文件和数据。随着节点的增加、存储的增加、流量的增加、文件的增加，总量恒定的GN 的单位价值和价格将持续上升。

Utility Token：GNS

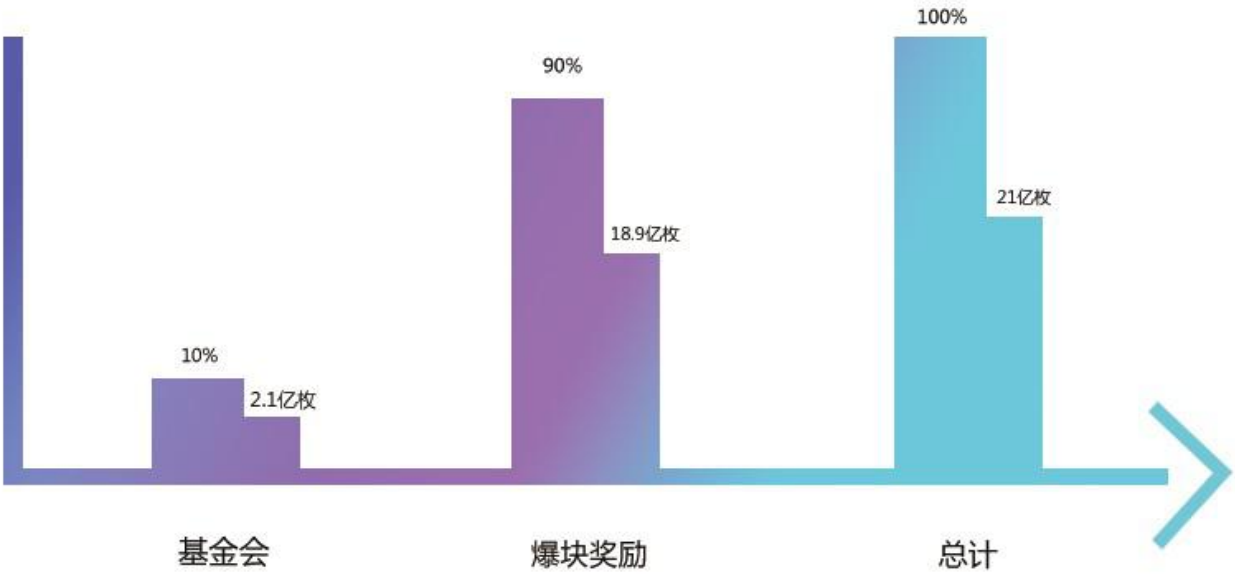
GNS与法币锚定，1GNS 等于 0.1 美分，向使用 Galaxy Network 的用户提供了一种价格稳定的支付手段。GNS 不能在交易所流通，只能在Galaxy Network 平台内部用法币购买或者与GN进行双向兑换。

平台为避免超发GNS，所有GNS在发行时都会质押当时等价的GN, 在G N S 使用完毕回流到平台时，平台释放当时等价的GN。这样的发行规则类似央行发行货币，背后需要储备等额的外汇储备和国债。

6.2 分配方案

Galaxy Network 将总共发行Token 21 亿枚，具体分配方式如下：

分配对象	比例	数量	说明
非营利组织（预挖）	10%	2.1 亿枚	• 用于非营利组织合规运营、未来发展，包括但不限于返还生态、投资合作等用于社区运营、社区发展、DAPP 建立等 • 用于奖励合伙人、合作伙伴、生态价值贡献方、保 持生态活跃 • 用于在冷启动阶段对生态用户的激励等
爆块奖励	90%	18.9 亿枚	• 爆块奖励，（加速矿工、存储矿工）获得的奖励
总计	100%	21 亿枚	



6.3 挖矿收益

GN总量:21亿枚

爆块奖励：18.9亿枚

区块间隔时间：4MIN

初始单区块产量：3600枚/BLOCK

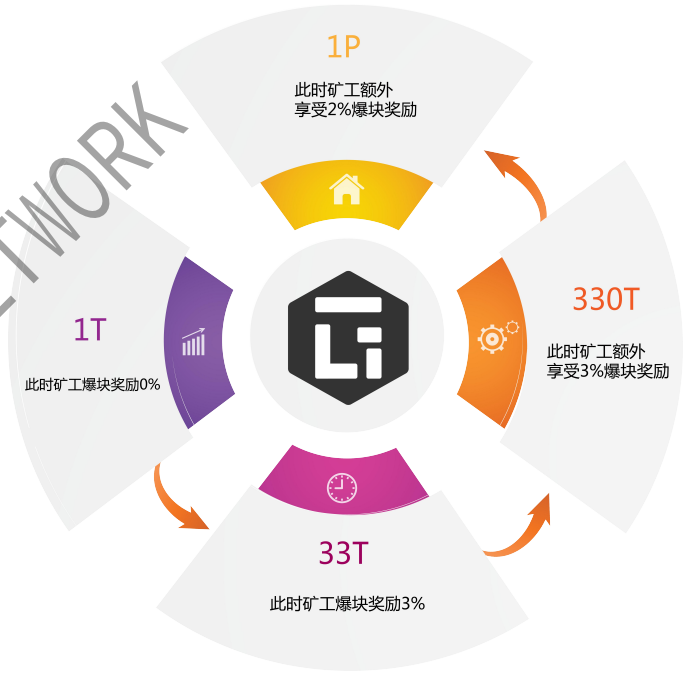
24H产量：1296000枚

抵押：1500枚GN/T

减产周期及幅度：
全网容量达到300PB后，爆块奖励减产50%；
全网容量达到900PB后，爆块奖励减产50%；
全网容量达到2700PB后，爆块奖励减产50%；

补充说明:
容量以300PB为基准，每达到3倍，爆块奖励减产幅度为50%。

矿池抵押币调整幅度：1500枚GN/T（弹性抵押）
根据全网容量增速及市场表现，九大矿池商议后，适当增减抵押币数量。



爆块奖励：

1.容量达到33T的矿工:
均享该矿池挖币量的3%奖励
2.容量达到330T的矿工:
均享该矿池总挖币量的3%奖励
3.容量达到1P的矿工:
均享该矿池总挖币量的2%奖励

矿工须知：

1.33T，330T,1P类似于矿工A,B,C群体，A矿工群体数量众多，均分奖励较少（奖励快速降低），B矿工群体数量较少，均分奖励较多（平稳降低）C矿工群体稀缺，均分奖励丰厚（缓慢降低）

大矿工申请条件：

330T（行星矿）申请条件：
（1）容量达到330T
（2）缴纳报名费1000枚GN
（3）等待该星系矿池审核通过

1P（恒星矿）申请条件：
（1）容量达到1P
（2）缴纳报名费3000枚GN
（3）等待该星系矿池审核通过

7 应用场景

Galaxy Network 拥有和IPFS 相同的应用场景，在如下场景中可以使用Galaxy Network 完成目标：

DAPP 是使用一种或多种去中心化技术的无服务器HTML5 应用程序，利用以太坊区块链、Galaxy Network、以及分布式通信平台，即可轻松开发和部署 DAPP。通过Galaxy Network，可以轻松存储和检索DAPP 上的数据，并将完整的DAPP 部署在Galaxy 上。

② 去中心化数据库

去中心化数据库是一个无服务器、分布式、P2P 数据库。它是一个最终一致的数据库，它使用CRDT 进行无冲突的数据库合并，使去中心化数据库成为DAPP，区块链应用程序和离线优先Web应用程序的绝佳选择。去中心化数据库可以依靠Galaxy 的高可靠性存储、超高速传输能力以及强大的去重能力，构建商业化的数据库服务。

去中心化数据库为不同的数据模型和用例提供各种类型的数据库：

- log：仅追加、可遍历、不可更改日志记录。对最新条用例或作为消息队列有用。
- feed：具有可遍历历史记录的可变日志。可以添加和删除条目。对购物车类型的用例有用，或者例如作为博客帖子或微博。
- key/value：键值数据库。
- docs：一个文档数据库，JSON 文档可以通过指定的键值存储和索引。用于构建搜索索引或版本控制文档和数据。
- counter：用于计算与日志/源数据分开的事件。

③ 实时聊天系统

基于Galaxy Network 构建分布式对等聊天应用程序。

④ 图片托管网站

基于Galaxy Network 构建图片托管网站。整个应用程序运行在去中心化的概念上，这意味着不是将信息托管在我们的中心服务器上，而是由想要的每个人存储数据。当图片放在Galaxy Network 上时，会给出一个散列，一个 46 个字符的长数字指纹。没有其他文件可以拥有它，如果相同的文件被添加两次，那么它们的哈希将完全相同，这意味着即使图片托管网站关闭，只需知道哈希就可以在网络上找到图片。

⑤ 去中心化邮件系统

去中心化邮件系统允许客户将文件作为电子邮件的连接发送，由于文件使用 Galaxy Network 存储， 因此文件无法被删除。这是向世界各地发送无限量文件的最简单方法。

⑥ 点对点加密文件系统

一种点对点加密文件系统，具有安全的文件共享，旨在抵御数据内容或朋友圈的监视。它将是一个安全的电子邮件替代品，与电子邮件有一些互操作性。还将有一个完全私密且安全的社交网络，用户可以控制谁看到了什么（以加密方式执行）。

⑦ 去中心化编辑器

去中心化编辑器，允许同时写入文本。除了对给定文档进行实时更改外，它还允许只读节点实时跟踪更改。它还允许将文档的自包含快照发布到Galaxy Network。

⑧ 超高清 4K 视频平台

基于Galaxy Network 的存储和超高速分发能力，构建基于机顶盒和智能电视的 4K 视频分发应用。并且允许用户自己上传视频并分享给其他人。

⑨ 基于Galaxy Network 的搜索引擎

Galaxy Network 的搜索引擎。嗅探DHT 内容并索引文件和目录哈希值。提取元数据和内容， 使用ElasticSearch 5 进行搜索，使用RabbitMQ 进行排队。

⑩ 去中心化Web 发布系统

基于Galaxy Network 进行Web 内容的部署，并且指定自己的域名进行发布。

⑪ Git 存储系统

使用Galaxy Network 部署 Git 版本系统，在客户端利用 Git 兼容协议从Galaxy Network 推送和拉取数据。

⑫ 文件分享系统

基于Galaxy Network 构建朋友间的文件分享系统。

⑬ 去中心化博客

构建基于Galaxy Network 的博客系统。

⑭ 去中心化Log 系统

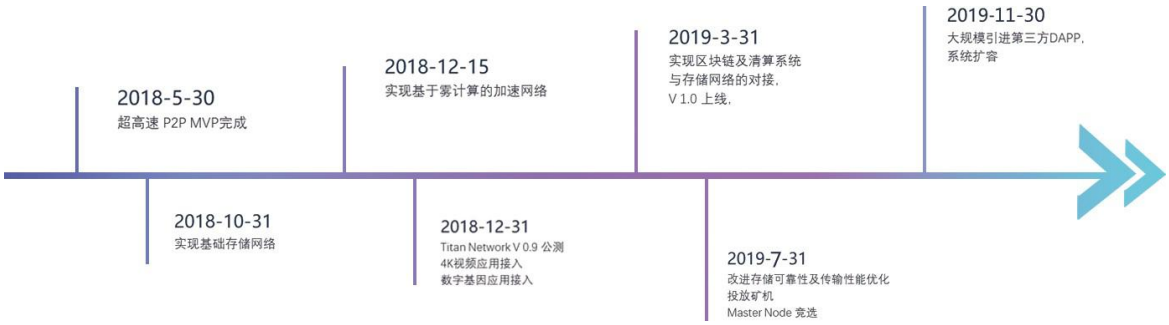
去中心化 log 系统是一个用于分布式系统的不可变的，基于操作的无冲突复制数据结构（CRDT）。它是一个仅附加日志，可用于模拟p2p 应用程序中对等体之间的可变共享状态。

日志中的每个条目都保存在Galaxy Network 中，每个条目都指向形成图形的先前条目的哈希值。日志可以分叉并重新连接在一起。

⑮ 超高速CDN

低成本的音视频超高速CDN 解决方案

8 里程碑



2018-5-30：

完成超高速P2P 网络的开发，成功证明在公网环境下流畅播放超过 20M 4K 视频的技术指标

2018-10-31:

完成存储网络的第一版开发，在兼容IPFS 接口的基础上，实现基于信道编码的可靠存储、下载、存储证明、订单管理、订单修复、块去重、高效UDP 传输协议及NAT 穿透等功能。

2018-12-15：

实现基于雾计算的加速网络，初步实现 20~50Mbps 的实时传输能力，并上线公测

2018-12-31：

存储网络 V0.9 线公测，开始接入 4K 应用及数字基因应用

2019-3-31：

实现基于区块链和链下清算系统的交易市场，与底层存储网络对接，完成存储网络与激励系统的闭环，V1.0 上线公测

2019-7-31：

改进存储的可靠性，包括去重、订单失效修复、订单过期修复、基于最低存储可靠性门槛的存储修复、以及传输能力的进一步优化。同时开始投放存储矿机及竞选Master Node。

2019-11-30：

大规模引入第三方DAPP，随着存储容量的增加，对系统进行扩容。

9 风险提示和免责声明

9.1 关于本白皮书

本白皮书只做交流之用，其中包含的信息或分析不构成购买提议或劝导。本白皮书不构成也不应被理解成为提供任何买卖的行为，或邀请买卖任何形式虚拟商品的行为， 也不是任何形式上的合约或者承诺。

9.2 免责声明

除本白皮书所明确载明的之外，Galaxy Network 基金会不作任何其它陈述或保证（尤其是对其适销性和特定功能）。任何人参与 Galaxy Network Token 的购买行为均基于其自己本身对项目的知识和本白皮书的信息。在无损于前述内容的普适性的前提下，所有参与者将在 Galaxy Network 项目启动之后按现状接受 Token，无论其技术规格、参数、性能或功能等。

Galaxy Network 基金会在此明确不予承认和拒绝承担下述责任：

① 任何人在购买Token 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；
② 任何人在购买Token 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取Token；
③ 由于任何原因Token 的购买计划被放弃；
④ Galaxy Network 的开发失败或被放弃，以及因此导致的无法交付Token；
⑤ Galaxy Network 开发的推迟或延期，以及因此导致的无法达成事先披露的日程；
⑥ Galaxy Network 源代码的错误、瑕疵、缺陷或其他问题；
⑦ Galaxy Network 平台或以太坊区块链的故障、崩溃、瘫痪、回滚或硬分叉；
⑧ Galaxy Network 未能实现任何特定功能或不适合任何特定用途；
⑨ 对所募集的资金的使用；
⑩ 未能及时且完整的披露关于Galaxy Network 开发的信息；
⑪ 任何参与者泄露、丢失或损毁了数字加密货币或GN的钱包私钥（尤其是 其存放Token 钱包的私钥）；
⑫ Token 的第三方众筹平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或歇业；
⑬ 任何人与第三方众筹平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾；
⑭ 任何人对Token 的交易或投机行为；
⑮ Token 在任何交易所的上市或退市；
⑯ Token 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制
⑰ 本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

9.3 风险披露

Galaxy Network 基金会相信，在 Galaxy Network 的开发、维护和运营过程中存在着无数风险， 这其中很多都超出了 Galaxy Network 基金会的控制。除本白皮书所述的其他内容外，每个 Token 购买者还均应细读、理解并仔细考虑下述风险，之后才决定是否参与计划。

每个 Token 的购买者应特别注意这一事实：尽管 Galaxy Network 基金会是在新加坡共和国设立的，但 Galaxy Network 只存在于网络虚拟空间内，不具有任何有形存在， 因此不属于或涉及任何特定国家。

参加本次购买计划应当是一个深思熟虑后决策的行动，将视为购买者已充分知晓并同意接受了下述风险：

① 购买计划的终止

本次 Token 购买计划可能会被提前终止，此时购买者可能仅被部分退还其支付的金额。

② 不充分的信息提供

截止到本白皮书发布日，Galaxy Network 仍在开发阶段，其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了Galaxy Network 最新的关键信息，其并不绝对完整，且仍会被 Galaxy Network 基金会为了特定目的而不时进行调整和更新。Galaxy Network 基金会无能力且无义务随时告知参与者 Galaxy Network 开发中的每个细节（包括其进度和预期里程碑，无论是否推迟）， 因此并不必然会让购买者及时且充分地接触到 Galaxy Network 开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

③ 监管措施

加密GN正在被或可能被各个不同国家的主管机关所监管。Galaxy Network 基金会可能会不时收到来自于一个或多个主管机关的询问、通知、警告、命令或裁定，甚至可能被勒勒令暂停或终止任何关于本次购买计划、
Galaxy Network 开发或GN 的行动。Galaxy Network 的开发、营销、宣传或其他方面以及本次计划均因此可能受到严重影响、阻碍或被终结。由于监管政策随时可能变化，任何国家之中现有的对于 Galaxy Network 或本次计划的监管许可或容忍可能只是暂时的。在各个不同国家，TOKEN 可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，TOKEN 可能被禁止交易或持有。

④ 密码学

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明）可能给基于密码学的系统（包括 Galaxy Network）带来危险。这可能导致任何人持有的 TOKEN 被盗、失窃、消失、毁灭或贬值。在合理范围内，Galaxy Network 基金会将自我准备采取预防或补救措施，升级 Galaxy Network 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的， Galaxy Network 基金会将尽力迎合密码学和安全领域的不断变化。

⑤ 开发失败或放弃

Galaxy Network 仍在开发阶段， 而非已准备就绪随时发布的成品。由于 Galaxy Network 系统的技术复杂性，Galaxy Network 基金会可能不时会面临无法预测和/或无法克服的困难。因此，Galaxy Network 的开发可能会由于任何原因而在任何时候失败或放弃（例如由于缺乏资金）。开发失败或放弃将导致 TOKEN 无法交付给本次购买计划的任何购买者。

⑥ 投资资金的失窃

可能会有人企图盗窃 Galaxy Network 基金所收到的投资资金（包括已转换成法币的部分） 。该等盗窃或盗窃企图可能会影响 Galaxy Network 基金会为 Galaxy Network 开发提供资金的能力。尽管 Galaxy Network 基金会将会采取最尖端的技术方案保护投资资金的安全，某些网络盗窃仍很难被彻底阻止。

⑦ 源代码瑕疵

无人能保证 Galaxy Network 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏漏洞，这可能使得用户无法使用特定功能，暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害 Galaxy Network 的可用性、稳定性和/或安全性， 并因此对 TOKEN 的价值造成负面影响。公开的源代码以透明为根本，以促进源自于社区的对代码的鉴定和问题解决。Galaxy Network 基金会将与紧密 Galaxy Network 社区紧密合作，今后持续改进、优化和完善Galaxy Network 的源代码。

⑧ 无准入许可、分布式且自治性的账本

在当代区块链项目中，有三种流行的分布式账本种类，即：无准入许可的账本、联盟型账本和私有账本。Galaxy Network 底层的分布式账本是无准入许可的，这意味着它可被所有人自由访问和使用，而不受准入限制。尽管 Galaxy Network 初始时是由 Galaxy Network 基金会所开发，但它并非由 Galaxy Network 基金会所有拥有、运营或控制。自发形成的 Galaxy Network 社区是完全开放、无中心化且无准入 槛即可加入的，其由全球范围内的用户、粉丝、开发者、TOKEN 持有人和其他参与者组成， 这些人大都与 Galaxy Network 基金会无任何关系。就 Galaxy Network 的维护、治理以及甚至是进化而言，该社区将是无中心化且自治的。而 Galaxy Network 基金会仅仅是社区内与其他人地位平等的一个活跃成员而已，并无至高无上或专断性的权力， 哪怕它之前曾对 Galaxy Network 的诞生做出过努力和贡献。因此， Galaxy Network 在发布之后， 其如何治理乃至进化将并不受到 Galaxy Network 基金会的支配。

⑨ 源代码升级

Galaxy Network 的源代码是开源的且可能被 Galaxy Network 社区任何成员不时升级、修正、修改或更改。任何人均无法预料料或保证某项升级、修正、修改 或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料料或非预期的结果，从而对Galaxy Network 的运行或TOKEN 的价值造成重大不利影响。

⑩ 安全弱点

Galaxy Network 区块链基于开源软件并且是无准入许可的分布式账本。尽管Galaxy Network 基金会努力维护 Galaxy Network 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入Galaxy Network 的核心基础设施要素之中，对这些弱点或缺陷

Galaxy Network 基金会无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的TOKEN 或其他数字GN丢失。

⑪ “分布式拒绝服务”攻击

Galaxy Network 设计为公开且无准入许可的账本。因此，Galaxy Network 可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 Galaxy Network 系统遭受负面影响、停滞或瘫痪， 并因此导致在此之上的交易被延迟写入或记入Galaxy Network 区块链的区块之中，或甚至暂时无法执行。

⑫ 处理能力不足

Galaxy Network 的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过 Galaxy Network 区块链网络内届时节点所能提供的负载， 则Galaxy Network 网络可能会瘫痪和/或停滞，且可能会产生诸如“双重花费”的欺诈或错误交易。在最坏情况下，任何人持有的TOKEN 可能会丢失，Galaxy Network 区块链回滚或甚至硬分叉可能会被触发。这些事件的余波将损害 Galaxy Network 的可使用性、稳定性和安全性以及 TOKEN 的价值。

⑬ 未经授权认领待售TOKEN

任何通过解密或破解 TOKEN 购买者密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意获取 TOKEN 购买者所购买的待售 TOKEN。据此， 购买者所购买的待售 TOKEN 可能会被错误发送至通过购买者注册邮箱或注册账号认领 TOKEN 的任何人士，而这种发送是不可撤销、不可逆转的。每一 TOKEN 购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性：(i) 使用高安全性密码；(ii) 不打开或回复任何欺诈邮件；以及 (iii) 严格保密其机密或个人信息。

⑭ TOKEN 钱包私钥

获取 TOKEN 所必需的私钥丢失或毁损是不可逆转的。只有通过本地或在线 TOKEN 钱包拥有唯一的公钥和私钥才可以操控 TOKEN。每一购买者应当妥善保管其TOKEN 钱包私钥。若 TOKEN 购买者的该等私钥丢失、遗失、泄露、毁损或被盗， Galaxy Network 基金会或任何其他人士均无法帮助购买者获取或取回相关TOKEN。

⑮ 通 胀

可能会由于采纳 Galaxy Network 源代码补丁或升级（这将由 Galaxy Network 社区决定而不是 Galaxy Network 基金会决定），导致 TOKEN 数量发生增加。由此产生的TOKEN 供应量通胀可能导致市场价格下跌，从而 TOKEN 持有者（包括购买者）可能遭受经济损失。TOKEN 购买者或持有者并不能被保证会由于 TOKEN 通胀而获得赔偿或任何形式的补偿。

⑯ 普及度

TOKEN 的价值很大程度上取决于Galaxy Network 平台的普及度。Galaxy Network 并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，Galaxy Network 甚至可能被 期边缘化，仅吸引很小一批使用者。相 之下，很大一部 TOKEN 需求可能具有投机性质。缺乏用户可能导致 TOKEN 市场价格波动增大从而影响 Galaxy Network 的 期发展。出现这种价格波动时，Galaxy Network 基金会不会（也没有责任）稳定或影响TOKEN 的市场价格。

⑰ 流动性

TOKEN 既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的货币，也没有任何硬资产或其他信用所支持。TOKEN 在市场上的流通和交易并不是Galaxy Network 基金会的职责或追求。TOKEN 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 TOKEN 持有者处兑换或购买任何 TOKEN， 也没有任何人士能够在任何程度上保证任何时刻 TOKEN 的流通性或市场价格。TOKEN 持有者若要转让 TOKEN，该 TOKEN 持有者需寻找一名或多名有意按共同约定的价格购买的买家。该过程可能花费甚巨、耗时 并且最终可能并不成功。此外，可能没有加密GN交易所或其他市场上线TOKEN 供公开交易。

⑱ 价格波动

若在公开市场上交易，加密GN通常价格波动剧烈。短期内价格震荡经常发生。该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。

无论是否存在 TOKEN 交易的二级市场，Galaxy Network 基金会对任何二级市场的 TOKEN 交易不承担责任。因此，Galaxy Network 基金会没有义务稳定 TOKEN 的价格波动，且对此也并不关心。TOKEN 交易价格所涉风险需由 TOKEN 交易者自行承担。

⑲ 竞争

Galaxy Network 的底层协议是基于开源电脑软件。没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用Galaxy Network 的源代码和/ 或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台、虚拟机或智能合约从而与 Galaxy Network 竞争， 或甚至赶超或取代 Galaxy Network 。Galaxy Network 基金会对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台与 Galaxy Network 产生竞争关系。Galaxy Network 基金会在任何情况下均不可能消除、防止、限制或降低这种旨在与Galaxy Network 竞争或取代 Galaxy Network 的竞争性努力。

10 参考文献

[1] 分布式存储中的纠删码容错技术研究, 王意洁, 许方亮, 裴晓强
http://cjc.ict.ac.cn/online/onlinepaper/wyj-20171494406.pdf

[2] K. V. Rashmi, Nihar B. Shah, Kannan Ramchandran, Fellow, IEEE, and P. Vijay Kumar, Fellow, IEEE "Regenerating Codes for Errors and Erasures in Distributed Storage"
https://arxiv.org/pdf/1202.1050.pdf

[3] Steve Jiekak∗†, Anne-Marie Kermarrec‡ , Nicolas Le Scouarnec∗ , Gilles Straub∗ and Alexandre Van Kempen∗ ∗Technicolor, Rennes, France †EPFL, Lausanne, Suisse ‡ INRIA Rennes - Bretagne Atlantique, France "Regenerating Codes: A System Perspective"

[4] Reed Solomon code wiki,
https://en.wikipedia.org/wiki/Reed%E2%80%93Solomon_error_correction

[5] "Filecoin: A Decentralized Storage Network", https://filecoin.io/filecoin.pdf

[6] IPFS whitepaper,
https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

[7] Sia white paper, https://www.sia.tech/whitepaper.pdf

[8] Storj white paper, https://storj.io/storj.pdf

[9] maidsafe white paper, https://github.com/maidsafe/Whitepapers/blob/master/Project-Safe.md

[10] Andrew Miller, Ari Juels, Elaine Shi, Bryan Parno and Jonathan Katz
"Permacoin:Repurposing Bitcoin Work for Data Preservation"
http://soc1024.ece.illinois.edu/permacoin.pdf

[11] Henning Pagnia and Felix C G¨artner. On the impossibility of fair exchange without a trusted third party. Technical report, Technical Report TUD-BS-1999-02, Darmstadt University of Technology, Department of Computer Science, Darmstadt, Germany, 1999.

[12] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chaininstant payments. 2015.

[13] Andrew Miller, Iddo Bentov, Ranjit Kumaresan, and Patrick McCorry. Sprites: Payment channels that go faster than lightning. arXiv preprint arXiv:1702.05812, 2017.

[14] BBR: Congestion-Based Congestion Control, https://queue.acm.org/detail.cfm?id=3022184

[15] google bbr github，https://github.com/google/bbr

[16] Forward Error Correction Scheme for Object Delivery, http://www.rfc-base.org/rfc-6330.html