旮晃云分布式加密存储网络

GalaCloud Distributed Encryption Storage Network

（Zeepin Chain 生态分布式应用）

White Paper V1.0

July 27, 2018

Zeepin 基金会提供支持

目 录

1. 简介

由于中心化数据存储很容易受到各种安全威胁和攻击，让很多个人和公司数据遭到泄漏和丢失。为了彻底解决数据安全问题，Zeepin 社区团队将致力于建立具有明显优势的分布式加密云存储网络。文件数据通过 GalaCloud 客户端加密，被切碎成多个碎片并存储于由大量分布式节点形成的网络中，通过检索和备份维护数据的完整性，在很大程度上避免了存储故障和安全漏洞。因为加密私钥由个人保管，网络中的数据将无法进行未经授权的访问和篡改，即便拿到文件的部分碎片也无法解密。同时数据存储市场向所有人开放，让更多的参与者提供存储空间以降低各种存储服务的成本。

旮旯云分布式加密存储网络，是 Zeepin 生态重要的分布式应用，他为生态应用提供分布式存储空间和服务，是 Zeepin 公链的重要基础设施之一。同时为 Gala 代币的应用提供极为广阔的发展空间。

旮旯云提供的分布式文件存储系统称作 GalaCloud DESNet，主要由多个 GalaHub 节点和众多 GalaBox 节点组成。GalaHub 在整个网络中起到文件分片的调度、寻址作用，协调所有的 GalaBox。GalaBox 加密文件分片数据存储客户端，主要是提供数据块存储的服务；接收上传和下载的请求，并把接收的加密文件分片存储在磁盘中。

GalaCloud 旮旯云将提供安卓、IOS、WEB 等客户端应用，跨多个终端。Gala 将作为 GalaCloud 的共享权益凭证，存储文件用户需要支付 Gala 获得存储空间，收入的 Gala 将分配给各个节点。

2. 为什么要用 GalaCloud？

如今大型云存储供应商大都是中心化的，容易受到各种安全威胁和攻击，让很多个人和公司数据遭到泄漏和丢失。另外客户端加密标准和中心化管理私钥仍然无法真正保证数据的保密和安全。因此近年来大型网站用户数据和云存储供应商的数据安全问题层出不穷。中心化存储被认为无法很好解决以上问题。

为了彻底解决数据安全问题，Zeepin 社区团队将致力于建立具有明显优势的分布式加密云存储网络。GalaCloud 作为分布式加密存储系统的主要优势如下：

A．分布式存储

因为它是分布式存储的，所以不存在中心节点，也就是不需要第三方中心系统及组织，可以随时随地的上传或者下载文字、图片、音频、视频等文件。

B．安全加密

云存储通过第三方的中心机构来管理，等于是把文件的安全管理交给了第三方，所以安全性存在着很大的问题，GalaCloud 云存储是去中心化的，所有的文件都存在于一个分布式的网络中，文件被切碎并加密，同时进行动态备份。你绝对是你信息的唯一拥有者，除非你把私钥给了别人。

C．分布自治网络

GalaCloud 采用一致的标准治理协议，基于 Zeepin 公链的智能合约进行治理，节点间按照统一的协议标准自动运行，使得对中心的信任改成了对协议的信任，实现了全网的自治。

D．挖矿收益

本项目得到 Zeepin 基金会的支持，Gala 将作为 GalaCloud 的共享权益凭证，存储文件用户需要向 GalaCloud 治理合约支付 Gala 获得存储空间，收入的 Gala 将通过合约分配给各个提供存储服务和空间的节点。

E．信息防灾

所有存储到分布式网络中保存的信息分布于各个分散的 GalaBox 节点上，所有的加密数据碎片会生成 Hash，并由节点自动维护。例如当碎片冗余度低于安全阈值时，会启动生成新的碎片，分发至新的数据节点。数据通过个人保存的私钥加密，在使用期限中除非本人删除，否则数据永不丢失。

F. 应用对接

基于区块链的去中心化应用不断增多，用户对数据隐私和安全的需求日益提高。GalaCloud 将被用于 Zeepin 公链作为提供分布式存储的区块链基础设施，将通过合约实现与多个 dApp 的数据存储对接。例如 ZeeRights 版权源码存储将与 GalaCloud 实现无缝对接，为创意者提供安全加密的分布式云存储服务。

3. DESesNet

（Distributive Encrypted Storage Network）

3.1 网络组成说明

- GalaCloud DESNet: 分布式加密存储网络

- GalaHub: 在整个网络中起到文件分片的调度、寻址作用，协调所有的 GalaBox 同时在服务中缓存所有 GalaBox 的活跃状态、磁盘使用率等信息，每个 GalaHub 之间完全对等。

- GalaBox Pro: 强大的数据存储磁盘集群，主要是提供数据存储的服务；接收上传文件和下载文件的请求，并把接收的加密文件分片存储在磁盘中。预计将在 2019 年推出 GalaBox Pro。

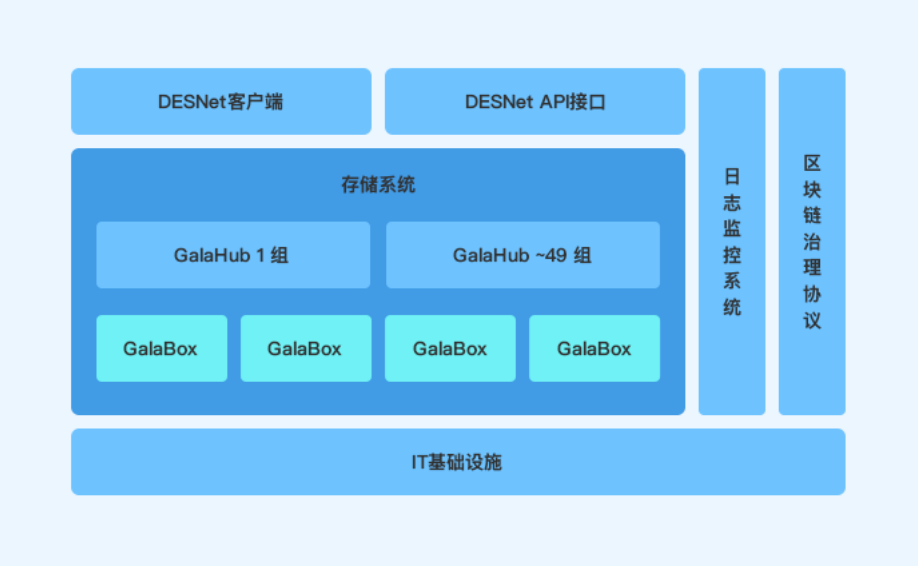
- GalaBox : 加密文件分片数据存储客户端，主要是提供数据块存储的服务；接收上传和下载的请求，并把接收的加密文件分片存储在磁盘中。

- GalaCloud API：客户端以外，更适合大规模接入 dApp 应用的合约接口，为 Zeepin 生态去中心化应用提供基础服务设施。

3.2 DesNet 整体结构设计

DESNet 文件存储系统主要由多组 GalaHub 节点和众多 GalaBox 节点、GalaBox Pro 节点组成，同时通过 Zeepin 公链上的治理合约进行治理 .。GalaHub 通过心跳对 GalaBox 的状态进行监测，GalaBox 会通过心跳，把本身的状态广播给 GalaHub，包括存活时长、磁盘状态、服务状态等。每个 GalaBox 都会定时向 GalaHub 广播，每个 GalaHub 的信息是对等的，每个 GalaHub 都可以提供服务，所以某个 GalaHub 停止服务后 GalaBox 可广播给活跃的 GalaHub，同理如果一台 GalaBox 离线后，GalaHub 监测到并移出服务队列。

图 1. DESNet 整体结构设计



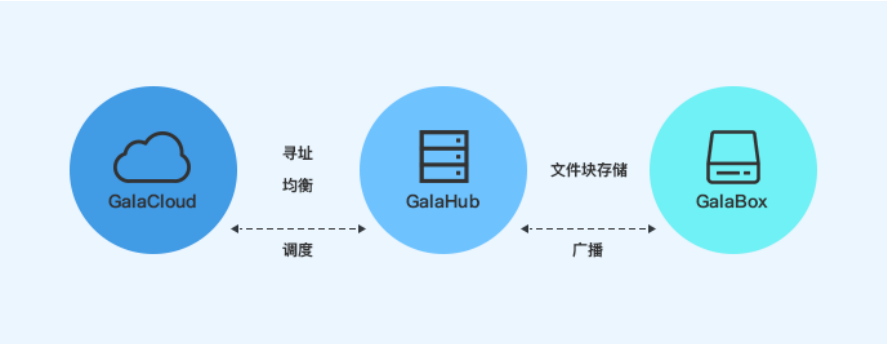
3.3 DESesNet 整体存储结构

GalaCloud 的客户端首先向 GalaHub 发起写请求，GalaHub 会根据每个 GalaBox 的容量、负载、状态等情况来就近选择当前高效运行的多个 GalaBox；接着，客户端向选择的 GalaBox 写入加密文件分片数据，GalaBox 支持流式数据写入。

每个写操作过程中 GalaHub 会记录 GalaBox 信息，标示加密文件分片存储到哪个 GalaBox 上；GalaBox 上会记录文件 hash，并把文件 hash 返回给客户端，客户端根据文件 hash 访问文件。

客户端读取文件的时候，首先访问 GalaHub，GalaHub 查找出加密文件分片所在的一系列 GalaBox；客户端得到可以读取文件的 GalaBox 信息，连接 GalaBox 根据文件 hash 读取文件数据。

图 2. DESNet 整体文件存储结构



3.4 GalaBox 节点

GalaBox 是数据存储集群的节点，每一台 Galabox 节点都是一台加密文件数据存储设备，设备上会存储用户上传的加密文件分片，文件按规则存放在相应目录，GalaBox 通电后会自动连接 GalaHub，定期广播心跳信息。

GalaBox 还担当文件备份的功能，根据 GalaHub 的指令来判断是不是需要备份本地的某些文件，将这些文件备份到附近的 GalaBox 上，保证文件的安全和可用性。

3.5 GalaHub 节点

GalaHub 由节点申请者提供网络服务器，并配置相应的存储空间和优质带宽；GalaHub 相当于寻址及调度设备，负责与 GalaBox 进行通信，GalaHub 会获取 GalaBox 心跳信息，收集供客户端服务和 API 服务调用。

3.6 文件编码

文件编码不仅可以降低数据冗余，还可以提高数据的访问速度。由于 DESNet 搭建在各个节点之上，虽然 GalaBox 数据节点较为稳定，但仍然可能会由于掉网、断电、损坏等各种因素脱离分布网络，随之造成存储在该 GalaBox 节点的数据暂时不可访问。因此 DESNet 设计了一种数据冗余机制来保证文件数据在部分节点失效的情况下仍然完整。在对文件分片加密处理之后，访问数据时可以从上百个节点中同时获取文件数据分片，通过少量的冗余保证数据的可用性。DESNet 通过文件的 hash 值、私钥、GUID 来保证编码的唯一性。同时获取碎片，而获取其中任意部分碎片就可以解码恢复出原始数据。这样避免了部分数据节点网络的不可靠带来的木桶效应，同时获取了剩余节点的上行带宽累加，带来了流畅的访问速度。DESNet 通过文件的 hash 值、私钥、GUID 来保证编码的唯一性。

4. GalaBox 矿机硬件

GalaBox 矿机主要用来作为提供加密文件分片的存储空间，通过众多 GalaBox 分布联网保证存储文件的安全和稳定，GalaBox 由 Zeepin 社区团队 BrandSky 设计。

图 3. GalaBox 设计图

4.1 GalaBox 矿机主要特点如下：

A. 可拆式设计

抽插式硬盘结构，方便用户自行购买硬盘装入并取出。

B. 健康提醒

设备内模块化组合方式，任一模块出现故障，可让用户直观地在指示灯上体现。（如硬盘、风扇、主板的健康状况）

C. 质保与售后

整机质保时间（1 年），长时间提供售后服务。

D. 智能标签

通过智能标签技术，让文件自动分类，方便用户更快找到。

E. 升级维护

系统定期升级，保障运行稳定

F. Gala 奖励

客户端有效的被读取和被写入，可获得 Gala 奖励。通过奖励机制来引入用户，有效拓宽用户群。

G. 手机端实时监测

手机端 APP，UI 系统定制开发，多语言支持，满足全球化用户的使用。通过手机客户端实时监测，有利于用户随时随地知晓 GalaBox 矿机的工作状态、收益动态以及最新的区块链资讯。

H. 家居化、科技感

符合家庭使用环境，兼具科技产品的属性

4.2 如何获得 GalaBox

GalaBox 矿机将通过 ZeeFund 众筹平台分阶段众筹。 ZeeFund 是 Zeepin 生态的重要 dApp 之一，主要为全球文创产业的创意项目提供众筹服务。预计第一年 GalaBox 数量在 6 万台以内，以后将根据存储空间的需求逐步增加。

GalaBox 将通过邮寄的方式寄送给用户，用户自行插入硬盘即可加入分布式存储网络并开启存储挖矿，多个 GalaBox 可以绑定在一个客户端上组成集群，便捷管理的同时大幅提高收益。

5. 数据安全

5.1 数据智能迁移

数据智能迁移的主要作用是为了防止某一个节点因为 GalaBox 物理上的损坏，导致数据节点的数量减少，影响系统性能及文件的完整性，为了免受节点失效的影响，采用数据迁移的方法。主要的做法是将某一个失效的 GalaBox 节点从系统中移出服务队列，并且当一个新的 GalaBox 节点加入系统时，将存储在原失效的 GalaBox 节点上的文件通过运算还原、迁移到新加入的 GalaBox 节点上。

5.2 目录管理

目录管理的主要功能是为了支持对分布式文件系统内存放文件的管理以及支持用户对信息的查询功能。

5.3 加密管理

文件分为公开文件和私有文件，公开文件会使用公共的公私钥进行加密和解密；私有文件会使用用户自身的公私钥进行加密和解密。

5.4 私钥管理

每个用户都必须在客户端上创建或绑定自己的公私钥，私钥只存储在用户客户端中，丢失后无法恢复。

5.5 防作弊方案

每一次文件的存取都是通过算法进行文件分片的不等数量切割、加密后存入不同 GalaBox 节点，要获得大量的资源进行作弊需要消耗大量的 Gala，理论上无法通过作弊获得奖励。

5.6 大文件操作

分布式文件系统对大文件的支持主要是集中在对于文件分块的处理，本系统对大文件的支持也是通过将大文件进行分割成小的文件分片，然后对每一个文件分片进行加密处理、分散存储。

大文件传输时，为了提高传输的效率，通过链表来排序下载数据块，保证图片、音频、视频等类型文件的展现。

6. 节点参与和激励机制

6.1 GalaHub 节点参与和退出流程

若 ZPT 持有者希望竞选加入 GalaHub 集群，可通过 GalaHub 竞选页面发起抵押申请，第一阶段计划招募不超过 49 个 GalaHub 节点，依据抵押额度进行排名，如进入前 49 位，则直接进入候选池列表，进入候选池列表后需向社区治理委员会提交节点拥有者信息进行真实性审核。

若 GalaHub 节点申请退出，则不能再继续参与成为下一轮 GalaHub 网络的节点。在 GalaHub 申请周期结束后，节点才可以退出。

6.2 节点激励机制

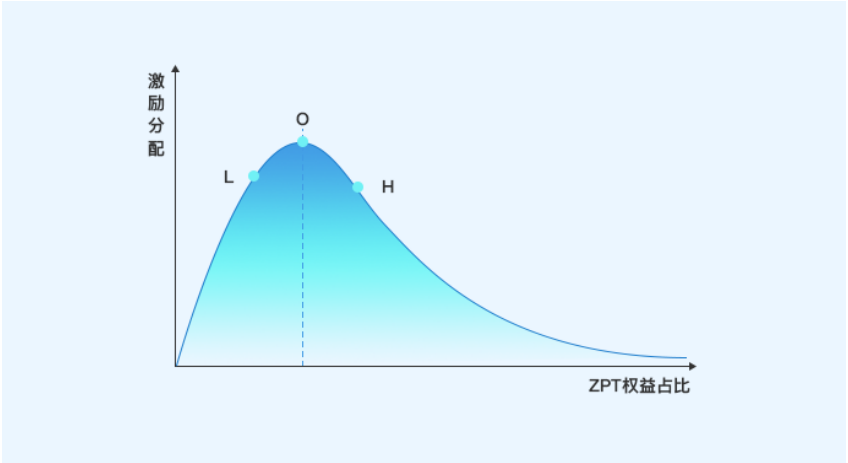
存储文件用户需要支付 Gala 获得存储空间，收入的 Gala 将分配给各个节点，其中 70% 发放给 GalaBox 节点，20% 发放给 GalaHub 节点，10% 用于建立 GalaCloud 基金。同时 Zeepin 基金会在早期对各个节点进行补偿。

节点	节点数	激励方案	收益占比
GalaHub	49	Gala Hub 激励曲线	20%
GalaBox	～ 60000	按优化系数分配	70%

6.2.1 GalaHubBox 激励模型简介

图 6 为 GalaHub 激励曲线，表示参与共识的 GalaHub 节点其权益占比激励分配的关系。节点 ZPT 权益抵押开始随着数量的增加激励分配比例也会随之增加，但当 ZPT 权益抵押超过 O 点后，在过多的情况下会降低 Gala 的激励。只有“恰当”的 ZPT 抵押才能获得最大的收益，由激励曲线形成的动态平衡，为公平和去中心化治地治理整个节点网络提供了更好的双重博弈机制。

图 6. GalaHub 激励曲线



单个 GalaHub 激励分配系数 H_j

通过各个 GalaHub 抵押的 Gala 数量可以根据激励曲线查询对应的激励分配系数 H_j

全网 GalaHub 激励分配总系数 H_t

所有 GalaHub 节点的激励分配系数 H_j 相加可以得到总系数 H_t

$$H_t = \sum_{j=1}^{m} H_j$$

单个 GalaHub 激励分配比例 $P_j\%$

$$P_j\% = \frac{H_j}{H_t}$$

单个 GalaHub 节点每周总收益 R_j

$$R_j = P_j\% \times [(G_r \times 20\%) + G_{f1}]$$

G_r：一周内 GalaCloud 全网存储收入 Gala 分配总数

G_{f1}：一周全网基金会激励补偿 GalaHub 节点的 Gala 总数

m：一周内 GalaCloud 全网 GalaHub 的总有效节点个数

6.2.2 GalaBox 激励模型简介

所有通过众筹获得的 GalaBox 存储矿机都可以联网加入 GalaCloud 旮旯云存储网络 , 并成为存储矿工。通过 GalaBox 矿机获得 Gala 挖矿权，根据矿机优化系数每周结算。系统启动后 Zeepin 基金会每周补偿发放 Gala 补偿金，每两年减半。

GalaCloud DESNet 会统计每个 GalaBox 节点的总在线时间、本周在线时间、共享总空间、已用空间、上传总量、下载总量、24 小时下载速率、24 小时上传速率等参数。

GalaBox 日贡献系数计算方案如下：

定义：

S：一周平均设备存储空间，单位 TB

U：一周平均上行带宽，单位 Mbps。U_0 为建议带宽，若 $U>U_0$ 时，U/U_0 取值为 1.

D：一周平均下行带宽，单位 Mbps。D_0 为建议带宽，若 $D>D_0$ 时，D/D_0 取值为 1.

T：一周设备在线时长，单位小时

C_i：单个 GalaBox 周贡献系数

$$C_i = \left(\frac{S}{4T}\right) \times \left(\frac{U}{U_0}\right) \times \left(\frac{D}{D_0}\right) \times \left(\frac{T}{168}\right)^2$$

C_t：全网所有 GalaBox 周贡献总系数

$$C_t = \sum_{i=1}^{n} C_i$$

单个 GalaBox 节点每周总收益 R_i

$$R_i = \frac{C_i}{C_t} \times [(G_r \times 70\%) + G_{f2}]$$

G_r： 一周内 GalaCloud 全网存储收入 Gala 分配总数

C_{f2}：一周全网基金会激励补偿 Gala 总数

n： 一周内 GalaCloud 全网 GalaBox 的总有效节点个数

使用 GalaBox 的存储设备时，系统每天会根据 GalaBox 的存储空间、在线时长、上下行带宽综合评估权重进行计算出每周贡献系数，并进行全网代币收益结算，每周向绑定 GalaCloud 客户端的 Zeepin 钱包进行分配。分配记录可以通过 GalaCloud 客户端查询。

7. Roadmap


2020.1 对外提供企业级商用服务网络平台
2019.5 Zeepin dApp平台和Galaxy dApp娱乐生态应用接入GalaCloud
ZeeRights接入GalaCloud
2019. 1~3第一批GalaBox加入节点
GalaCloud全网正式运行
2018.12 GalaHub节点组网测试
GalaCloud全网测试
2018.10 开始部署GalaHub节点
2018.8 GalaBox开始众筹
GalaHub启动节点竞选
2018.7 完成GalaCloud白皮书 V1.0
2018.6 完成DESNet网络测试
2018.5 完成GalaCloud客户端原型设计
2018.4 GalaBox设计和DESNet分布式框架设计
2018.3 GalaCloud启动项目