CESS

Cumulus Encrypted Storage System

去中心化云存储

基础网络设施

开启一个去中心化的数据云存储时代---CESS

https://cess.cloud

摘 要

从石刻到竹简，从帛布到纸张，从印刷到电子打印数字记录……人类文明的承载，从实体转移到数据虚拟空间。文明的记录，是人类社会的宝贵财富，是人类文化和文明的传承，它得益于科技日新月异的进步，人类对于记录数据有着天然的执着，技术更迭，亘古不变的是人类对数据存储更安全，更高效，更便捷的不懈追求。

人类社会正在迈入数字化时代，在互联网这条快速连接的高速公路上，海量数据实现了快速传输、接收、存储、挖掘和分析，如果说活字印刷是人类文明的播种机，那么大数据则是人类未来发展的新能源、新技术和新的组织方式，将引领人类社会发展的新纪元。

人类社会正在受到数字化世界的冲击，在数字化的世界里，数据需要被安全保护，数据隐私、使用权属只能属于数据创造者，记录人生点滴的各种数据必须保证其私有性。现今，大量个人数据的价值并没有被充分挖掘且让数据创造者获益。人类正逐渐构建一个以数据为基础的新文明秩序。

区块链被认为是下一代互联网——“价值互联网”的基础，区块链技术的出现将推动 Web3.0 互联网的加速实现。基于区块链等技术，在网络世界、虚拟空间里将建立一个数字化新世界，这个新世界可能蕴藏着比物理世界更大的财富和潜在的行业机遇。

CESS 建立的去中心化分布式云存储基础网络设施致力于保护数据安全，不被泄露、丢失、篡改、盗取，个体隐私和权益获得保护，个人牢牢掌握个人数据的分享和交易的权利。

CESS 去中心化云存储生态解决困扰人类许久的数据存储安全问题，它还是对存储安全强需求的基于区块链的商业系统操作平台，是一个开放、透明、共建、共享、共荣的生态。

CESS 致力于推动数据和价值互联，建造更加开放、公平和安全的分布式的网络世界，必将重新定义存储系统，这也将对未来万物互联的数字世界的发展形成深远的影响。这就是 CESS 的存在意义，也是推动 Web 3.0 发展的强大动力！

目 录

1、项目概述

随着计算技术、虚拟现实及人工智能等新型技术的发展，人类社会已逐渐迈进了数字化时代，而伴随而来的是网络空间中的数据量呈现出爆炸式增长。据世界经济论坛估算，仅 2020 年全世界的数据量就将达到 44 垓(ZB)。其中，据不完全统计，仅谷歌搜索的日访问量就高达 40 亿次，社交媒体脸书的月活跃用户量甚至比中国人口总量还要多，每天产生 4 兆比特的数据，包含 100 亿条消息、3.5 亿张照片和 1 亿小时的视频浏览。毫无疑问，依托大数据、机器学习等技术，可以从这些海量数据中挖掘出数据价值出来，也就是所谓的“数据价值”。但如何存下当下与日俱增的数据，却是一个相当棘手的问题。为克服传统独立数据存储介质可靠性、易丢失等方面的不足，云存储技术被广泛接受和应用。借助云存储技术，人们可以做到随时随地访问自己数据，而不用担心存储空间够不够、数据会不会丢、方不方便携带，但是，过度中心化的云存储同样面临着数据丢失、隐私泄露的问题。基于此，我们将构建一种基于区块链技术的分布式云存储基础设施——Cumulus Encrypted Storage System （CESS），具备云存储的存储效率和使用体验，同时有效解决了当前数据存储过度中心化的问题。

CESS 是一群在致力于探索实现去中心化的分布式数据云存储的开拓者，努力建设基于区块链和云存储特性的云存储基础设施。基于区块链技术，CESS 将线上闲散存储资源有效利用起来，构建庞大的分布式存储网络，同时，借助虚拟化技术、云计算技术，将这些资源实施有效管理，构成统一的、海量

的数据存储湖，为用户提供高效地数据存储服务。CESS 系统具备极强的数据存储可靠性，每份数据在 CESS 上将会以三份副本形式存在，且每份数据被切分成多份，分散到 CESS 的网络中，而任何一份数据的损坏并不会带来数据文件丢失。除此之外，CESS 基于区块链特性构筑了一套高效、透明、平等的存储交易市场，让数据所有者可以在 CESS 网络上，围绕数据构建数据要素市场，进行数据共享和数据交易，便于用户挖掘数据内在价值，从其中带来收益。

2、背景与挑战

2.1 Web 2.0 的达摩克利斯之剑

当前的互联网处于 Web2.0 阶段。Web2.0 时代的巨头是谷歌、脸书、亚马逊、推特等，在这些巨头前赴后继的不懈努力下，互联网变得更容易访问，全世界有近三分之二的人口实现上网，对人类社会产生了巨大深远的影响。

在 Web2.0 时代，每个人用以前无法想象的方式与数以万计的个人、企业与机构时刻进行互动，产生大量由 0 和 1 组成的二进制数据。据 IDC 统计，2018 年全球产生的数据量达到 33 ZB，到 2025 年将达到 175 ZB。全球云存储市场规模从 2017 年的 307 亿美元增长到 2020 年的 889.1 亿美元，年均增速 20%以上。IBM 公司的研究人员提出，当今世界 90%的数据是在过去 2 年中产生的，而且随着新的设备和技术的出现，数据增长会进一步加快，万亿规模的储存市场会很快变成现实。但随着近年来数据规模的增大及其重要性日益凸显，号称安全的 Web 2.0 中心化云存储的安全不断被质疑。其中最著名的例子就是 Facebook 的 5000 万用户数据被泄露，用户数据遭到了很大的侵害。数据安全和主权就是悬在 Web2.0 头上的达摩克利斯之剑。

2.2 数据存储的困境

2016 年美国学者出版的《平台革命：改变世界的商业模式》提出 Web2.0 的本质是平台经济，并宣称“平台正在吞食整个世界”。平台是通过促进不同使用者群体间的交易/交互来创造价值。由于垄断平台持续地寻租，获取的收益分配比重才越来越大，整个社会都在为平台打工，平台获取了大部分的经济增值。

互联网公司垄断市场的手段是掌握大量服务提供方和服务使用者的数据。Web2.0 的科技巨头凭借他们对所有数据的控制，掌握了巨大的权力，数据被视为企业最核心的资产，数据及数据的使用规则，完全由企业来掌控，普通用户完全没有权力参与其中，巨头控制了游戏规则。

具体来说，数据完全由企业或者中心机构掌控，会有如下问题：

数据易泄露。外界的攻击，导致数据易被盗取。特别是很多企业内部数据用明文存储，一旦被盗，所有信息相当于完全公开。

数据易丢失。两千年前，亚历山大图书馆被焚毁。大火烧毁了我们历史上成千上万的珍贵文件。所有人都认为这是人类的悲剧。然而，这种事情每天都在 Web2.0 发生。企业运维的事故性丢失或者黑客攻击性丢失，或者企业倒闭服务关停都能导致数据丢失。

数据会被审查。对于中心化的服务器，中心机构就很容易阻止对它们的访问。例如，土耳其近两年来一直禁止访问维基百科。有些国家访问不了国外网站，因为有些持不同意识形态的网站被认为对国家造成了威胁。

数据可被篡改。企业对其内部的数据库，有至高无上的权利，理论上来说，工程师、算法师、管理员可修改任何数据，比如删除做恶的记录，即使是用的所谓纯增量数据库也是如此。

数据会被打包售卖。当前网络数据售卖的黑产已呈现国际化、公司化、智能化、匿名化的特点趋势。黑灰产团伙开始通过利用暗网、Telegram 等多种工具平台，实施数据的窃取、流转、整合和交易。部分黑灰产利用公司化的外衣，从事数据交易的不法行为，并且存在黑产人员将多渠道获取的数据进行数据清

洗整合，自动化对外提供服务。

数据孤岛。在多数的工业/制造业企业，现有信息化的应用系统大多按传统的 IT 系统垂直架构，以项目制而独立构建，开放性比较低，相对封闭，整合困难，生死难往来，形成多个烟囱式的应用系统，以及多个数据孤岛。同时这些系统一般沿用传统的应用开发模式，导致功能大而全，内部功能模块紧耦合，可复用性低，造成开发工作量繁重，更新困难。这种状况，要打通上述跨越业务边界、部门边界、甚至企业边界的数据主线、价值链主线，实现信息联通和流程联通，以及敏捷开发和迭代更新众多的业务应用软件，以应对日益多变的业务和创新需求，面临着很大的挑战。

2.3 数据存储的破局

当前，各国已经深刻认识到 Web 2.0 的数据存储问题，并制定和数据安全相关的法律和规定。2016 年 4 月，欧盟正式通过《通用数据保护条例》（General Data Protection Regulation, 简称 GDPR）并于 2018 年 5 月正式施行，这条被称为“史上最严”的法规整合了隐私保护指令、电子通信隐私保护指令以及欧盟公民权利指令，规定现行或未来将跨越国界的商业经营模式及企业组织需遵循个人数据保护原则，对包括记录、保存、下载、组织等有可能引发个人隐私泄露的行为或产品进行严格把控，且数据主体有权要求企业组织更正、清除并停止处理其个人数据，这对于当前高速发展的大数据时代，推动用户掌握个人隐私所有权起到至关重要的护航作用。

然而数据存储安全光靠法律保护还不够，还需要基于新技术创新的基础设施的支持，人们认识到当前的互联网并不完美，其固有缺陷靠技术上的小修小

补已经不能解决问题，需要一次更新迭代。

呼唤 Web3.0 的呼声越来越强烈，那什么是 Web3.0？简单的说，Web3.0 是对下一代互联网的设计和设想。

如果说互联网 Web 1.0 和 Web 2.0 带来了信息流量自由流动的爆炸，互联网 Web 3.0 则将会带来信息价值自由流动的爆炸。

Gavin Wood 博士在 2014 年提出了一种革命性的 Web3.0 设想，他的愿景之一是 Web3.0 能实现用户掌握自己身份、数据和命运的互联网；Web3.0 将启动新全球数字经济系统，创造新业务模式和新市场，打破平台垄断，推动广泛的、自下而上的创新，建造一个更加开放，去中心化，分布式的网络世界，数据创造者能够保护自己的数据，个人隐私和权益获得保护，个人牢牢掌握个人数据的交易和分享的权利，这对未来的生产关系产生巨大的改变。

无论是互联网，还是区块链、人工智能、物联网，所有的存储、计算、传输，一切仍旧是围绕数据展开。基于区块链的去中心化分布式存储，具有数据确权的领先优势，让数据存储安全成为可能，实现数据的跨平台、跨协作、跨格式的互操作。去中心化存储的技术特性，包括数据隐私的不可篡改、私有化、资产化，以及可信的底层基础设施、未来的数字经济等，都是分布式存储在未来应用上的“可扩展性”。同时，分布式存储可以为底层基础建设提供后助力，必然衍生出很多应用。分布式存储网络可以更好地推动 web3.0 到来，是 Web3.0 的底层技术架构基础之一。

CESS 作为一个去中心化的云存储基础设施，利用了区块链技术的分布式存储、不可篡改、可追溯、多方维护、交叉验证等特性，能有效界定数据权属，

追踪监管数据流通，合理分享数据收益。

CESS 打造的分布式存储生态，其账户系统、智能合约以及底层的分布式存储底层设施，可建立起规模化的分布式存储网络。它能够根据不同的应用需求，推出多种交易策展机制和共识机制，打造 CESS 存储生态建设的具体方案。当前，人工智能、远程医疗、物联网、5G 都需要稳定安全的 CESS 去中心化云存储系统，在互联网上运行的数字创作、直播、视频、音乐、小说、漫画、电商等应用都可以在 CESS 生态中呈现。CESS 为海量增长的数据量提供了强大可延展的存储基础设施，确保其上层的商业大厦的稳定构建。

3、基于区块链的应对新方案

区块链技术的蓬勃兴起已经彻底改变了互联网发展路径，它允许数据分布在整个分类账中，没有任何中央管理机构，但基本要求是参与者验证数据，这为数据变得更加开放与安全提供了无限可能。建立数据存储的“自由交易市场”，似乎不再遥不可及。

基于区块链技术的去中心化云存储将充分发挥区块链技术的优势功能，满足存储大量数据的实际需求。去中心化云存储，顾名思义，是把数据切成小块加密后分散到多个网络节点。提供去中心化云存储的服务商仅负责管理与维护分散的区块链网络，而非控制其存储数据。存储技术均为开源，没有公司可以完全控制区块链网络中的数据。智能合约进行自动化交易并负责下达存储数据的指令，数据一旦上链在区块链网络便无法删除与更改。

正因如此，与集中式网络相比，基于区块链的去中心化云存储数据安全性更高。所有数据均会被加密且被复制以保证冗余，每个用户拥有自己的加密私钥来控制自己的数据，这极大程度地保证数据上传者对自身信息的可控度。此外，存储文件的节点仅负责一小块文件的内容，这也意味着通过攻击存储节点获取文件信息是毫无意义的。

去中心化云存储的理念实现了允许普通人在点对点网络中通过租用经济实惠的硬盘空间来实现数据存储的需求。为了盘活此类新兴云存储的使用场景，多数项目方从“供给—需求”两个层面入手：即存储挖矿（供给）方面，用户可将闲置的存储空间添加到分布式网络中，并允许存储空间提供者接收存储需求，并以 Token 作为激励机制。在存储服务（需求）方面，客户利用区块链网络来

存储数据，这些数据会被发送到世界各地许多不同的矿工，雇佣矿工进行存储与分发数据。但是大部分都还处在实验阶段。

CESS 结合了去中心化云存储的理念，构建去中心化云存储新生态，并落地到商业应用中满足商业应用对大量数据存储的实际需求，它将实现以下目标：

（1）低成本存储：存储成本过高导致互联网企业在选择业务数据存储周期和存储质量方面面临的重大挑战。CESS 精心设计的激励措施为矿工提供了有吸引力的经济回报，并鼓励他们为存储网络做出贡献。与此同时，它惩罚作恶的参与者。基于奖惩分明的 CESS 存储网络可以建立一个大型、高质量的存储市场。这使 CESS 能够利用现有大量未使用的带宽和存储资源，并以更低的成本提供强大的存储服务。CESS 打造了一个分布式的云存储平台，提供各种存储类型产品，为了使系统易于使用，它还提供了完善的 API 和 SDK，方便开发者对接和用户使用，给用户带来更好的产品体验。

（2）隐私、安全和稳定：数据安全和隐私保护是 CESS 分布式文件系统设计的首要要求。通过使用数据分片和加密算法，单个存储节点不会存储数据所有者的全部数据，而是分散到多个节点存储，矿工在打包存储数据的过程中只获得一部分信息，用户数据只能由拥有用户唯一私钥的人检索。系统允许用户轻松地将其数据分享给其他人。CESS 采用了高效的分布式 Hash 算法，以保持其存储内容的完整性和可靠性；开发了可用存储服务证明算法（PoAs），以提供节点或矿工提供可用资源的有效验证；优化了时空证明算法（PoSt），可确保节点或矿工在指定时间内确实存储了指定的数据；使用复制证明算法（PoRep）保证节点或矿工复制用户的数据；使用流量证明算法（PoF）保证了

节点与节点流量交互的数据。

（3）数据确权：明确数据所有权一直是内容应用所面临的巨大挑战之一，传统的确权手段采用提交权属证明和专家评审的模式，但是缺乏技术可信度，且存在潜在的篡改等不可控因素。为解决这些问题，我们提出区块链+分布式存储网络+内容识别的解决方案，系统的内容所有权认证主张：认证即确认所有权。系统也引入申诉机制，当某用户认为平台内内容侵权，经认证后，系统可将该内容下架或转移数据所有权。

数据确权内容过程为：用户提交内容，内容认证，所有权判定，结果上链。确权内容过程中的核心为所有权判定，基于此，系统引入内容判定节点，该节点类似认证节点，区别为不使用单认证节点模式，系统引入大量认证节点，所有认证节点对用户上传内容进行判定，当 50%以上节点认为该内容为当前用户所有，即判定所有权归属该用户，将用户所属内容特征上传至区块链。

- 用户使用系统，上传内容至特征网关。
- 特征网关判断系统是否已经存储该内容，若无存储，再依据当前在线节点数量，随机抽取对应节点数量的文件内容特征，分发至认证节点。
- 认证节点获取随机的文件内容特征，对比内容特征数据库。
- 认证节点对比完毕数据库，依据判定结果，对内容所有权投票。
- 智能合约依据投票结果，对数据确权，确定数据内容归属，将文件所有权保存至区块链，完成整个内容确权过程。

特征数据库包含对内容文本的采样或音频的采样。

（4）数据权益保护：在这个共享经济时代，数据的拥有者的权益是否能够

得到保障是所有用户比较关系的一个问题，CESS 作为一个去中心化的内容存储和发布网络，提供一套机制来保护数据拥有者的权益不受侵犯。首先 CESS 借助于区块链网络，对每一份数据都进行着 24 小时不间断的监测，确保数据的每一次使用都记录在案，为数据收益分配提供了完整、可靠、可验证的证据服务。然后 CESS 通过智能合约，确保了数据拥有者能够实时的收到因数据共享产生的权益。CESS 系统默认提供两种经济模型的系统合约供用户选择。一种是固定收益模式：数据每次使用，都会固定支付拥有者设定的费用，此收益及时发放。另一种是股权收益模式：周期性的统计数据使用者的收益，按比例提取部分收益，然后按照使用数据的数量以及频率按比例分配给各个数据拥有者，此收益周期发放。

（5）构建强大的应用生态：CESS 提供了一组类似于亚马逊，苹果，阿里等云服务的存储 API，使得从这些服务迁移数据变得更加容易。CESS 提供其他的云存储产品，以更好地支持分布式应用程序，包括对象的存储，音视频转码和文件访问管理等。CESS 有一个全面的计划来开发一个完善、可持续的生态系统，来促进开发应用程序和服务，并鼓励开发人员参与 CESS 生态应用的开发。

4、应用场景

4.1 分布式网盘

CESS 能上线分布式网盘，基于 CESS 分布式基础设施，打造去中心化云存储系统。

CESS 网盘不需要云端服务器，有效地避免了对主干网和中心化服务器的依赖。用户数据能够分散存储到多个存储节点，下载资源不再受制于网盘服务提供商，数据传输速度得到大幅提升。基于区块链的加密算法，存储的数据都可以被加密，保证了存储的隐私性，不用担心数据丢失和中心服务器关停。CESS 网络支持无限扩展，因此无需担心网盘扩容问题。可以根据实际的需求进行动态扩容，打破了传统网盘的存储限制，让广大用户享受新一代云存储，享受科技进步的乐趣。

4.2 NFT 存储

在过去的一年，NFT 逐渐成为了加密世界中最热门的领域之一，吸引了来自艺术界、奢侈品、社会名流和其他公众人物的高度关注。NFT 的安全存储是 NFT 艺术价值和商业价值的核心底座，CESS 能为 NFT 创作者们提供安全可靠的存储。用户只需将 NFT 文件上传 CESS 中，系统将对其进行哈希处理分配地址即可，通过向量空间建模技术综合知识结构特征、主题特征、语义特征等，对 NFT 作品特征信息进行自动匹配，其他人便可以使用用户给他们的私钥来请求文件，形成 NFT 自由流通的良好生态。比如在 NFT 的交易中，美国艺术家创作了 NFT 艺术品售卖给英国的买家，交易过程中版权转让，时间戳生成都在

公开透明可追溯的 CESS 链上系统完成，掌握 CESS 私钥就掌握了数据资产分享分配交易的专属权益，杜绝了仿制、伪造、盗版，同时交易可以在瞬间完成。

CESS 不仅能够存储 NFT 数字资产，也能交易 NFT 数字产品，还可以在 CESS 上开发多种应用，成为 NFT 的生态孵化器，通过智能合约，对利益进行重新分配，真正让 NFT 的生产者和分发者得到回报。同时，不断降低传统平台接入区块链的门槛，用户并不需要深入了解链上技术，通过调用友好的 API 即可发布自己的应用。CESS 创造了一个开发者和创作者共同建设的平台，创作者在互联网上创作游戏，文学作品，绘画，音乐，视频和直播等都可以基于 CESS 系统对 NFT 数据存储，让每一个创作者都有机会拥有自己的 NFT 作品，CESS 不但给创作者提供理想安全存储空间，还支持创建一个确权，存储，分享，交易，传输，保存和使用的商业平台，交易过程版权确认，时间戳生成都在 CESS 链上公开透明完成，掌握 CESS 私钥就掌握看数据资产分享，分配和交易的权利。专属令牌促进粉丝互动经济，社群互动分享和促进消费，使分享，交易，流通和使用成为社群文化的一种新颖的令牌经济模式。

4.3 分布式存储

CESS 将开始建设的一个分布式存储系统，这必将使我们成为分布式存储领域的拓荒者和前行者。CESS 利用区块链技术，通过存储证明算法构建多策略存储能力证明机制，可充分利用闲置的带宽和存储资源，以更低成本、提供相比传统云存储更强大、更高效的存储服务；同时实现数据确权和权益保护，并提供更好的数据安全和隐私服务，打造一个去中心化、奖励机制完善、灵活可扩展、链上可验证可信的区块链云存储平台，建立自由交易的数据存储市场。

具体而言，CESS 在数据存储方面能给数据产业链条带来如下改变：

数据生产链的改变。CESS 的分布式存储能够在生产过程中将非线性化和网络化，即所有生产要素可以网络化多点配置；生产方式完全协同化，在人—机—人的协同中完成产品，实现众产（crowd-production），区块链技术提供了这样的“网状协同”的技术条件，提供了非线性生产平台。

数据流通链的改变。数据 CESS 可以使基于存储的交易、流通的原有中介渠道消失或重组，这种去中介化的特征使得数据产品可以在任何时空与任何用户见面，并且都有记录；数据产品和服务流通将出现新模式，如非线性的流通、垄断渠道和平台地位将更加式微，生产者、产品与用户之间的智能合约使得产品和服务点对点之间的可信任传播变得可能，从而降低价值的流通成本，提高价值的效益与效果。

数据消费链的改变。不再是巨头或者数据中心主导数据消费，而是每个数据存储者和应用者主导，数据消费主权已发生了变化。通过数据存储、过滤、整合、优化、匹配、参与等满足用户对数据的需求，实现供给和需求的完美匹配。

5、技术实现

5.1 设计架构

CESS 是一个高速、安全、可扩展的去中心化的云存储项目。它通过并行技术，可以处理每秒钟上万笔的交易；通过切片技术，能够完成海量数据的安全存储，同时它具备数据确权和数据权益保护等功能，提供了强大的数据服务能力；为 Dapp 提供无限可扩展的存储能力的同时，具备完善的数据权益保护能力。

如图所示，CESS 采用分层、松耦合的设计方式，分为分布式存储资源层、分布式内容分发层、区块链服务层及应用层。其中，分布式存储资源层利用虚拟化技术实现存储资源的整合、池化，为上层应用提供海量的、弹性可伸缩的云存储资源，由存储容量矿工和存储调度矿工构成基础设施；分布式内容分发层利用内容缓存技术，实现存储数据的快速推送，由数据索引矿工和数据分发矿工组成；区块链服务层为整个网络提供区块链服务，包括激励闲置资源加入两种存储网络，达到构建高质量存储网络的目的，同时也为应用层提供数据交易、数据确权存证等服务。

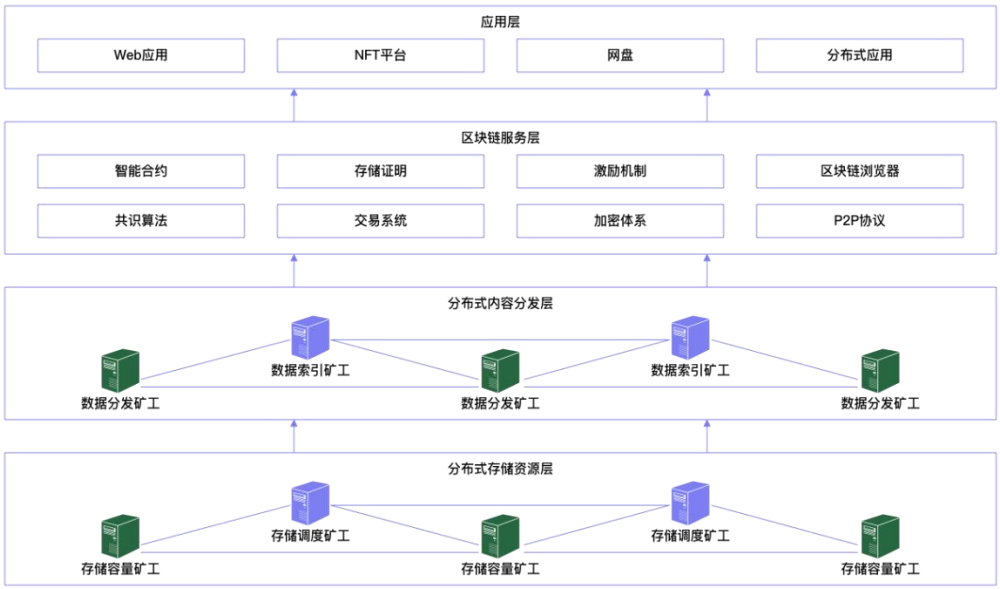

图 1 设计架构图

分布式存储资源层：利用区块链的激励机制，将具备存储能力的服务器、台式机及笔记本等存储能力的设备，有效的管理起来，为全球提供海量的数据存储能力，是全系统最为关键的硬件基础设施层，该部分由存储调度节点和存储容量矿工两类矿工组成，其中，存储调度节点存储数据元数据，提供数据快速索引，存储容量矿工提供数据存储空间。用户存储到分布式存储资源层的节点上数据，通常是以加密后切片的形式存储到存储容量矿工上，故不会造成用户数据泄密。

分布式内容分发层：采用去中心化的云存储技术会导致数据相比传统的云存储数据中心更为分散，从而带来用户访问数据过慢的问题。CESS 如何解决这一难题呢？我们借鉴了 IPFS 的设计思路，引入了内容缓冲技术，为全球提供高效数据存储服务。本层网络是一个高效的内容分发网络，由数据分发矿工和数据索引矿工组成，其中，数据分发矿工负责缓冲数据，数据索引节点负责高

效查询数据。

高性能区块链公链服务：除了激励闲散的计算资源、存储资源加入分布式存储网络和分布式内容缓冲网络外，还可以提供高效区块链服务。CESS 将利用异步拜占庭共识算法技术，提供高 TPS 的访问能力，同时具备图灵完备的智能合约、跨链交易能力等。值得兴奋的一点是，针对当前区块链系统缺乏数据治理能力，CESS 将引入去中心化的可编辑区块链技术，允许链上数据在共识基础之上实现数据治理。

应用层服务：为用户提供接口友好、使用方便的数据存储和区块链服务，例如网盘、云盘等。

5.2 区块链层设计

CESS 采用多分层架构，具备可扩展和鲁棒性，并提供了完善的 API 接口和 SDK，方便开发者进行对接。

如图 2 所示：整体架构共分为六层，分为数据层、网络层、共识层、激励层、接口层和应用层。其中，数据层支持可扩展的数据存储，并利用了一些算法技术来优化资源的使用和利用以及数据的安全；网络层用于节点连接，数据传输，提供负载均衡和 P2P 网络协议和算法；共识层利用共识算法实现交易快速形成共识，具备上十万级别 TPS 处理能力；激励层将应用多种存储算法，通过智能合约实现收益公平分配，从而形成正反馈，激励整个 CESS 社区向前发展；接口层提供丰富的 API 接口和完善的 SDK，便于开发者对接；应用层，支持第三方开发商开发的 DAPP 或者 APP 应用。

图 2 整体技术栈

5.2.1 数据层

数据层包含了区块数据、P2P 网络中存储的数据等。为保证数据的安全性和完整性，将采用加密算法进行数据的传输、存储和验证，如数字签名、哈希算法、默克尔树等。

区块数据：即链的数据，它记录了整个公链网络上的交易记录数据；一部分节点需要保存区块数据并运行全节点，以保证公链的安全稳定。

分布式存储：将数据分散存储在多台独立的设备上。它可以提供高效率的、鲁棒的和负载平衡的文件存取功能。如下图 3 所示：

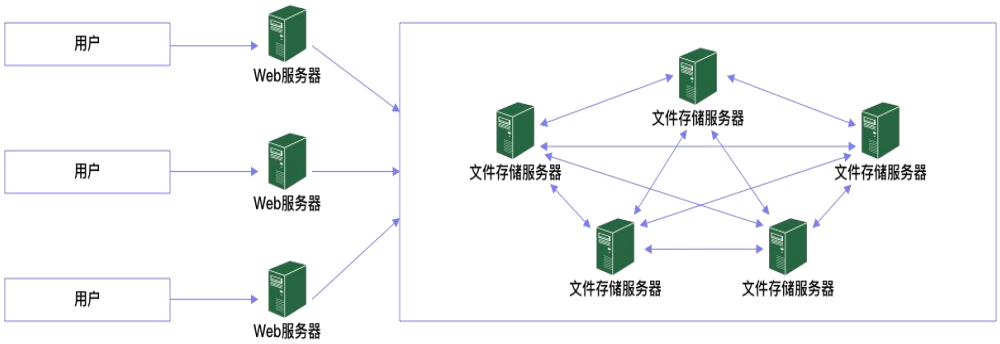

图 3 分布式存储系统

数字签名：数字签名（又称公钥数字签名）是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。它是在法律效力上等同于纸上的物理签名和签章，使用公钥加密算法技术实现的用于验证数字信息的方法。数字签名的实现包括两种配合使用的算法，一个用于签名，另一个用于验证。我们用数字签名进行系统中身份认证、数据完整性验证等。

哈希算法：哈希是一种单向密码体制，即它是一个从明文到密文的不可逆的映射，只有加密过程，没有解密过程。哈希函数可以将任意长度的输入经过变化以后得到固定长度的输出，但是不同的输入哪怕只存在一个比特的不同，形成的输出都是不同的。哈希函数的这种单向特征和输出数据长度固定的特征使得它可以生成供验证消息——称为哈希值或 HMAC 值。常用的哈希算法有 MD5、SHA-1、SHA256 等。我们使用哈希算法来唯一标识数据，并保证数据的不可篡改。

非对称加密：指加密和解密使用不同密钥的加密算法，也称为公私钥加密。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密。

因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。常用的有 RSA、ECC 等。

Merkle Tree：即默克尔树（又叫哈希树），就是存储 hash 值的一个树形数据结构。Merkle 树的叶子是数据块（例如，文件或者文件的集合）的 hash 值。非叶节点是其对应子节点串联字符串的 hash。在 p2p 网络下载数据之前，先从可信的源获得文件的 Merkle Tree 树根。一旦获得了树根，就可以从其他从不可信的源获取 Merkle tree。通过可信的树根来检查接受到的 Merkle Tree。如果 Merkle Tree 是损坏的或者虚假的，就从其他源获得另一个 Merkle Tree，直到获得一个与可信树根匹配的 Merkle Tree。我们可以直接下载并立即验证 Merkle Tree 的一个分支。因为可以将文件切分成小的数据块，这样如果有一块数据损坏，仅仅重新下载这个数据块就行了。

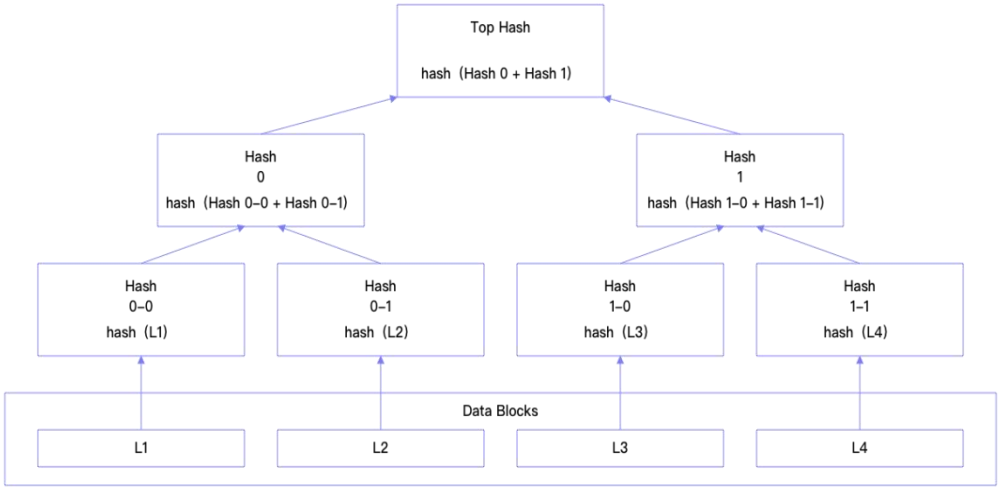

图 4 默克尔树数据结构

5.2.2 网络层

为保证网络中数据的高效存取，将构建一个基于 DHT 的 P2P 存储网络。

P2P 网络：即对等计算机网络，是一种在对等者（Peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。在 P2P 网络环境中，彼此连接的多台计算机之间都处于对等的地位，各台计算机有相同的功能，无主从之分，一台计算机既可作为服务器，设定共享资源供网络中其他计算机所使用，又可以作为工作站，整个网络一般来说不依赖专用的集中服务器，也没有专用的工作站。网络中的每一台计算机既能充当网络服务的请求者，又对其它计算机的请求做出响应，提供资源、服务和内容。

DHT：分布式哈希表，是一种分布式存储方法。在不需要服务器的情况下，每个客户端负责一个小范围的路由，并负责存储一小部分数据，从而实现整个 DHT 网络的寻址和存储。连入 DHT 网络的用户叫做节点(node)，节点之间互相有路由记录，因此只要和任何一个已经在 DHT 网络中的节点连接上，客户端就可以寻找到更多的节点，从而连入网络。DHT 技术就是可以使得网络中的任何一个机器都实现服务器的部分功能，使得用户的下载不再依靠于服务器。

ICE：ICE 是一种针对节点之间进行通信的面向对象的中间件平台。ICE 提供了一种 RPC 协议，既可以把 TCP/IP、也可以把 UDP 用作底层传输机制。节点并不需要了解其具体实现。ICE 还允许把 SSL 用作传输机制，让节点间的所有通信都进行加密。

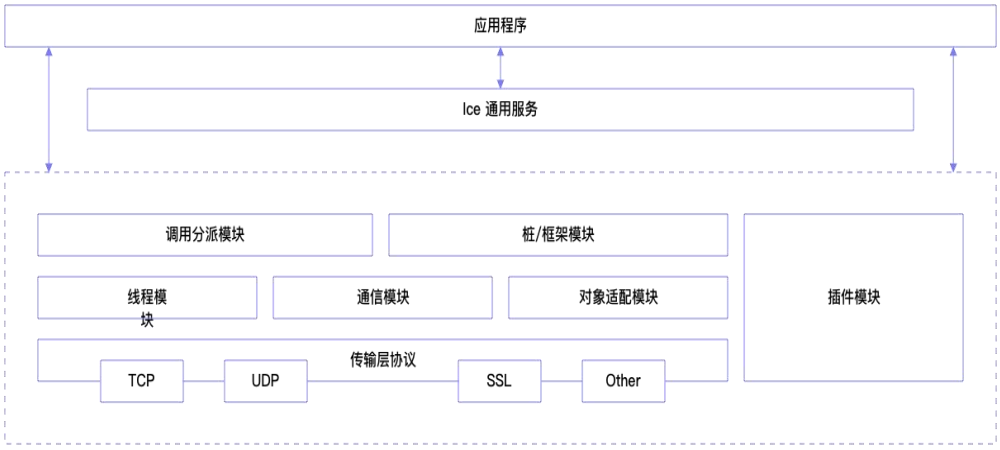

图 5 ICE 框架

5.2.3 共识层

为了确保区块链网络上交易和事件快速达成共识，CESS 将采用一种基于拜占庭容错改进的共识机制，进一步提高了系统的性能和可扩展性。

信誉度评分：该共识机制采用健康分数评估模型。该模型对分布式能源节点在平台中的共识行为进行健康分数评估，表现出诚实行为的节点健康分数就会越高，为进行视图更换时共识节点委员选举提供依据，从而提高共识节点的可靠性，保证上链数据的真实性。

可验证随机函数：利用基于可验证随机函数的出块节点选举协议，对传统 PBFT 取余选举出块节点的方式进行改进，增加节点选举的随机性和不可预测性，提高主节点的抗攻击能力，保证基于区块链的 CESS 平台的安全性。

共识分片：采用共识分片协议，有助于减少整个联盟链的整体负载，减少了网络中交易过程的通信开销，降低了时延，提高交易吞吐量。相比于链下扩容方案，分片方案保证了交易链上进行，一定程度上兼顾了非中心化。

动态节点：构造动态共识节点协议，该协议包括新节点加入协议和主动退出协议，系统共识节点的加入和退出机制是对共识算法流程的补充，实现了联盟链网络集群不停机的场景动态增删节点的功能，提高 CESS 的鲁棒性，进一步扩展 CESS 实际应用性。

5.2.4 激励层

CESS 作为分布式文件系统，使用的系统资源主要存储和网络。在 CESS 网络中，将存在两种类型的挖矿节点，一种为存储内容挖矿节点(Content Storage Node，CSN)，一种是加速内容传播的内容缓冲节点(Content Delivery Node, CDN)。CSN 节点存储负责文件的存放，CDN 节点负责文件的传播。因此，用户可以通过提供两种类型的资源加入 CESS 网络建设，而 CESS 系统则会根据节点所作的贡献奖励 CESS。

为了鼓励用户长期稳定的加入到 CESS 网络中，需要为 CESS 网络设计激励机制，根据用户节点所做的贡献来给予奖励。

- 如何参与 CESS 网络

对用户来说，奖励有点类似于“挖矿”。CESS 提供的奖励是考量用户对 CESS 分布式网络所做的贡献来分发奖励，贡献证明算法（Contribution of Proof, CoP）则是对 CESS 贡献判断的证明算法。贡献证明算法是一种综合共识算法，主要考察矿工存储容量、网络带宽及机器配置等因素，计算一个综合分数，根据分数，获得 CESS 网络的奖励。

- 如何获取 CESS Token

为了促进 CESS 的网络发展，除了在技术层面的激励制度以外，CESS 引入了主节点激励机制，符合激励机制的用户将发放 CESS。

1. 节点挖矿：矿工可以加入分布式存储网络、分布式内容分发网络获取 CESS ，具备方法是通过是相应的带宽及存储容量即可获得对应的激励。
2. 社区贡献：为了推广 CESS 应用，开发者和社区成员，合作者等都可以通过预案的形式提交申请，获得社区投票，并获得通过后，将会从区块链系统中发放对应的奖励。
3. Token 治理将采用 DAO（Decentralized Autonomous Organization ）达成共识的群体产生共创，共建，共治和共享的协同行为，充分展现社区协作能力，更加体现公正性和公平性，

- Token 分发

由于 CESS 是分布式的，去中心化的网络存储系统。所有与激励相关的的操作都采用基于智能合约实现。它包含：用户的时空证明认证结果的上链操作及奖励发放。确保 CESS 激励机制的公开化，透明化。

5.2.5 接口层

CESS 的核心设计目标之一是提供可编程的分布式存储，也可以称为分布式存储服务(DSaaS)，为了对开发者更友好，它提供：

- SDK

  它为各种平台上提供 api，如 iOS、Android、Mac 和 Windows。

- Web API

帮助开发人员开发基于 web 的应用程序。

- json-rpc 接口

允许 DApps 调用 CESS 节点上的功能，轻松集成 CESS 存储系统。

- 应用程序沙箱

CESS 可以支持在其存储网络中并发运行大量应用程序。开发人员可以在他们的应用程序中配置文件。

1) 每个应用程序都有自己的加密密钥。应用程序开发人员可以指定如何加密其应用程序中的数据对象:

2) 仅使用应用程序的加密密钥进行加密。

3) 使用应用程序和用户的加密密钥进行加密。

CESS 提供两个类别的 api，系统级 api 为开发人员提供了更大的灵活性和对 CESS 各种功能的更好控制，合约级 api 为开发人员提供各种对存储购买查询的功能。

- 系统级 api

1) get: 获取指定 hash 值的资源对象。

2) cat: 获取指定 hash 值的资源对象数据流。

3) delete：删除指定 hash 值的资源。

4) add: 增加资源。

5) push: 增加并备份资源。

6) Callback：获取下载资源的 url。

- 合约级 api：

1） Get_account:获取合约内账户相关信息。

2） Get_table_rows：获取激励及存储相关信息。

5.2.6 应用层

CESS 的 API 旨在使第三方开发人员能够构建各种应用程序，包括以下内容:

- 存储应用程序:

私人数据存储。由于其去中心化，CESS 存储网络非常适合于私有网络存储应用。个人数据被分区、加密并存储在不同的节点上，以确保隐私被保护。与此同时，对数据的访问受到用户私钥的限制，使得个人数据更加安全。

- 企业数据存储:

CESS 可以在提供企业数据存储高性能服务的同时为其显著的成本节约。

- DApps:

对于去中心化应用程序来说，在区块链上存储应用程序数据非常昂贵。智能合约或其他应用程序的数据可以通过使用 CESS 的 api 存储在 CESS 存储节点上，从而实现显著的成本节约。

- 媒体应用

CESS 提供具有经济的带宽资源，可以有效的降低内容分发的成本。CESS 还配备了专门优化的调度和传输算法，以实现流畅的数据传输，可以为媒体应用程序实现和维护高质量的用户体验。

- 数据交换

文件资产可以在 CESS 的网络中进行交易。CESS 可以提供方法来匹配卖方和买方，并安全地可靠地处理交易，而不需要中间方。常用的应用程序，如应用程序市场和内容平台可以受益于 CESS。

- 数据库

CESS 可以用作企业数据库，存储大量的历史数据，替代传统的本地数据存储或昂贵的云存储。除了企业数据，CESS 还可以用来存储公共数据库。

对于其他类型的存储需求，CESS 也将提供必要的支持。此外，CESS 将很快开放源代码。届时，应用程序爱好者和开发人员将能够参与 CESS 的开发，并为更多的应用程序增加支持。

5.3 分布式存储资源层设计

与现有 IPFS 等项目不同的是，CESS 旨在构建基于区块链的分布式云存储系统，关注的重点是如果将分散的资源利用虚拟化技术有效管理起来，对外提供统一高效的分布式存储服务。CESS 强大之处在于，具备全球高效数据存储能力，支持用户通过分布式身份信息实现无差别的数据访问。在具备实现上，CESS 将构建分布式内容缓冲和分布式云存储两类基础设施，其中，分布式内容缓冲网络会将根据用户地理位置，将数据投送到最近的内容缓冲节点，达到访问速度加速的目的；分布式云存储网络主要是提供海量的、可靠的及弹性可伸缩的云存储服务。

- 数据存储流程

用户存储数据到 CESS 网络的流程将经过生产、上传、处理、存储、分发及销毁等几个阶段。在生产阶段，用户可以通过 restful api、SDK 等方式植入

应用之中，实现数据的上传；在存储阶段，基于 CESS 网络资源，将可以搭建面向图片、视频、文档的智能服务，支持用户在线处理数据；在分发阶段，通过内容分发网络，可以实现超过 10T 的网络带宽。另外，CESS 支持用户在线删除数据。

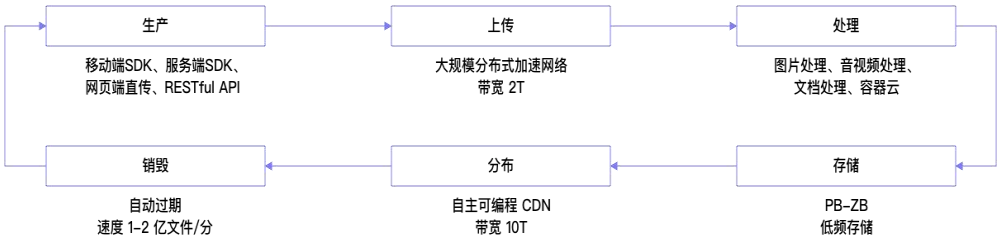

图 6 数据存储流程

- 分布式内容缓冲网络

为了实现高效的文件访问，系统有效的结合了 CDN 和 P2P 的两种技术的优点，形成了内容分发网络技术，它通过 P2P 技术有效地减少了系统所需得代理服务器的数量，增大了系统的容量，从而降低了总体成本，又利用 CDN 技术将媒体内容转移到客户所在的自治域内，使客户访问媒体的质量大大提高，同时由于是在一个较小的自治系统范围内，P2P 网络性能也会有很大提高，而高性能缓存代理服务器的存在，也避免了纯 P2P 网络中的“种子”问题。

同时在应用端，应用中的存储内容会首先在发布源节点上进行发布，在源节点不下线的前提下，能够持续提供下载服务。然而当从同一个源节点下载的用户数增加后，该节点的带宽将被消耗殆尽，而每个用户的下载速度也会降低。通过内容分发网络的设计，网络中的大量租户节点开始保存和提供同样内容的

下载。用户因此可以从多个节点下载内容，用户体验大幅提高。

分布式内容分发网络层的整体设计与区块链技术进行了完美结合，存储节点与各区域的代理节点组成 CDN，代理节点与下面无公网 IP 的存储节点形成了相对独立的 P2P 网络，节点贡献奖励通过智能合约发放，形成了一个开发自治的网络。如下图所示：

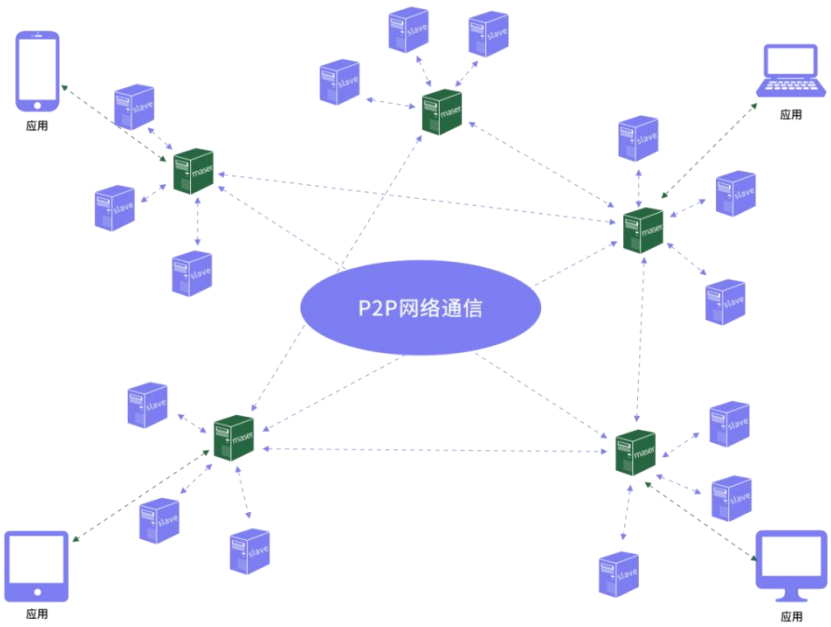

图 7 分布式内容缓存网络

- 分布式云存储网络

为了满足不同存储需求，我们将设计实现多态数据存储访问接口，以 API 的形式提供满足多种应用的存储服务。如下图所示，在统一的分布式对象存储引擎之上，多态数据访问服务以标准 API 的方式对上层应用提供对象存储、块存储、文件系统存储三大类存储服务方式，为顶层应用提供了全面友好的数据存储服务支持，是 CESS 平台乃至整个应用生态提供了统一的高性能数据存储

服务解决方案。

CESS 将提供高可靠的对象存储服务，上层应用调用对象存储服务接口，由对象存储模块自动完成用户对象存储空间到底层统一的分布式对象存储空间的映射，用户数据以对象数据的形式存储在分布式对象存储引擎。

CESS 将提供块设备存储服务，上层应用调用块设备服务接口，由块存储模块自动完成用户的块设备操作、数据读写操作到底层统一的分布式对象存储空间的映射，用户在块设备上的数据最终以对象数据的形式存储在分布式对象存储引擎，支持快照、克隆等功能。

对于通用文件系统，POSIX 文件系统模块，提供兼容 POSIX 标准的文件系统接口，同时支持内核文件系统和用户空间文件系统（FUSE）两种模式，上层应用调用 POSIX 文件系统接口，由 POSIX 文件系统模块及 POSIX 文件系统元数据管理器（负责 POSIX 文件系统空间到对象存储空间的映射和转换）共同完成用户的 POSIX 文件操作到底层统一的分布式对象存储空间的映射，用户在 POSIX 文件系统中的数据最终以对象数据的形式存储在分布式对象存储引擎。

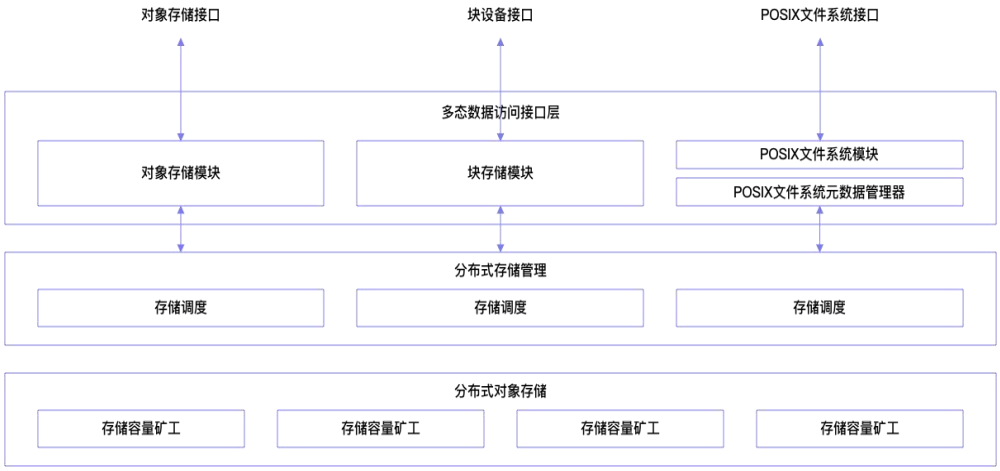

图 8 分布式存储网络架构设计

5.4 关键技术一：数据防篡改机制

基于区块链技术，CESS 设计实现融合数字水印生成和数据指纹提取算法的数据防篡改机制，为数据的安全流转提供支撑。同时，利用区块链链上数据可追溯防篡改特性，加强链上数字指纹的权威性，解决 CESS 平台数字指纹易丢失、难监管、怕掉包等难题。不同类型的数据应采用合适的技术方案以及匹配的处理流程，CESS 平台数据主要可分为文本数据、图像数据、音频数据和视频数据。

- 文本数据

重点突破潜在语义特征提取、二进制数据指纹转换、哈希算法防篡改检验等关键技术，实现 CESS 文本数据基于潜在语义的防篡改与信息内容修改程度检测。文本数据指纹提取算法基本过程包括文本集合、文本预处理、向量空间标识、潜在语义空间构造与指纹生成。

- 图像数据

重点突破图像全局特征提取、二进制数据指纹转换和强鲁棒性图像指纹检测等关键技术，通过 CESS 区块链系统服务，实现基于多全局特征的高效率图像数据指纹提取与检测。主要研究基于颜色直方图的特征提取算法，通过分别计算视频帧 YUV 分量的直方图，量化线性融合提取特征；研究基于颜色矩的特征提取算法，将几何矩思想应用于图像的的特征提取中，通过计算其一阶矩、二阶矩和三阶矩来精确描述图像整体颜色特征分布；研究基于颜色熵的特征提取算法，利用灰度熵进行图像阈值选取，提高图像中光线和运动对象的鲁棒性。

- 音频数据

重点突破基于谱熵的音频指纹提取、最大公共子串、编辑距离和动态时间规整等关键技术，增强对于噪声、失真等因素的鲁棒性。基于熵的音频指纹提取算法主要可分为三部分。首先 CESS 对音频每一帧进行汉宁加窗操作，再对加窗后的数据进行快速傅里叶变换，使得音频信号由时域转换为频域。然后，采用临界频带划分方法将结果划分为若干个临界频带。最后，分别对每个临界频带计算求出熵值。

- 视频数据

重点突破视频指纹上链、视频数字水印嵌入和提取、全局特征视频指纹生成等关键技术，实现可追溯高准确率的视频篡改检测。具体实现上，首先，CESS 利用基于分块离散余弦变换的视频水印技术，完成对视频所有帧的数字水印嵌入，同时具有强鲁棒性。其次通过视频篡改主动检测技术，通过对视频的颜色、纹理、形状以及亮度等特征的提取，实现视频指纹特征的强鲁棒性与区分性。

5.5 关键技术二：跨链机制

多链并存乃至多链协作，是单链落地后的必然趋势。然而，由于各私有、公有区块链的技术架构各异、互不连通、独立运行，网络孤立性阻碍了不同区块链之间的协同操作，极大程度的限制了区块链的发挥空间。对于区块链来说，跨链技术是为区块链间通信提供服务的重要一环，是实现价值网络的关键，是区块链向外扩展和彼此连接的桥梁。基于对跨链技术的研究，CESS 系统实现了一种支持同构链间和异构链间跨链交互的集成性跨链机制，支持不同的区块链平台之间的资产流转、信息互通、应用协同，它类似于不同公链之间的桥梁，实现不同区块链网络间的数据传输，并极大降低传输成本。

在 CESS 系统中，跨链中继和平行链分别是实现同构链间和异构链间跨链交互的基础设施。同构链之间安全机制、共识算法、网络拓扑、区块生成验证逻辑都一致，它们之间的跨链交互相对简单。通常来说，基于跨链中继的出入口可以实现不同链之间的交易转发和数据交换。而异构链的跨链交互相对复杂，基于平行链的状态验证方法和同步共识可以实现异构链间消息的有效性验证和无需信任的跨链交互。CESS 系统的跨链交互机制如下图所示。

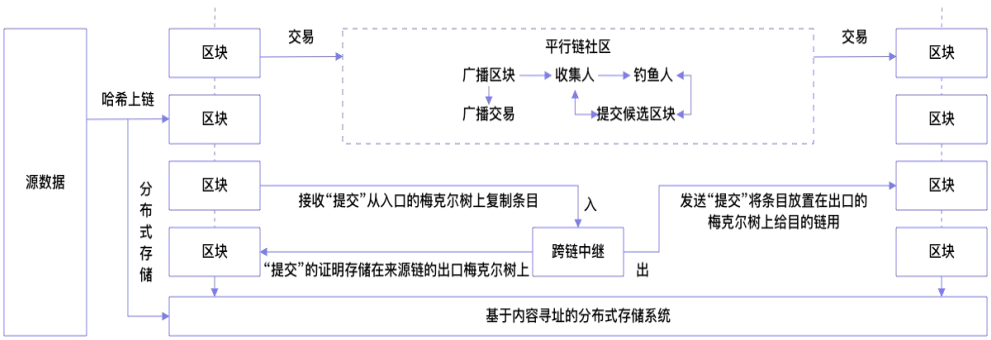

图 9 CESS 跨链机制

通过跨链中继的路由转发、交易监听、交易执行和锚定撮合功能，可以实现同构区块链之间的安全连接和自由交易。通过平行链的交易验证、交易核验、交易收集、交易检举等机制的保障，可以实现异构区块链的互认互信。CESS 系统的跨链机制聚焦基础跨链协议标准，在跨链消息的输入和输出口径、跨链消息的真实性证明、跨链消息的统一格式、消息的有效性证明和跨链执行结果证明等多个方面实现了标准化建设，为跨链安全共享提供了坚实的技术支撑。

5.6 关键技术三：链上/链下数据治理机制

基于区块链技术的去中心化云存储平台极大地降低了隐私、数据泄露等风险，解决了中心化存储中信任缺失的问题。然而当前尚未成熟的区块链技术，仍然面临着平台安全和应用安全等的严峻挑战。层出不穷的智能合约漏洞事件表明了不可篡改性并非绝对，反而在一定程度上限制了基于区块链的平台进一步发展。CESS 平台通过引入自主可控公链技术加强数据治理，解决数据冗余、错误、混乱等问题。在实现公有链主体功能的同时，支持对链上新型内容的管理，为防范和管理区块链信息安全风险提供支撑，为区块链技术应用的安全发展提供示范。为 CESS 平台设计的公链系统在数据结构上支持交易信息和内容信息的可分离，确保交易、智能合约的执行以公有链形式正常进行，同时可以对内容信息进行管理，实现了链上链下相结合的数据治理。

链上数据治理：现有区块链系统通过哈希函数保证链上数据的不可篡改性，链上数据将永久存储。CESS 平台中将用变色龙哈希函数替代哈希函数，实现可编辑的区块链技术。可编辑区块链技术可以在不影响其他区块数据、不改变区块链结构的情况下，删除失效或非法交易，减少资源浪费和营造健康的公链

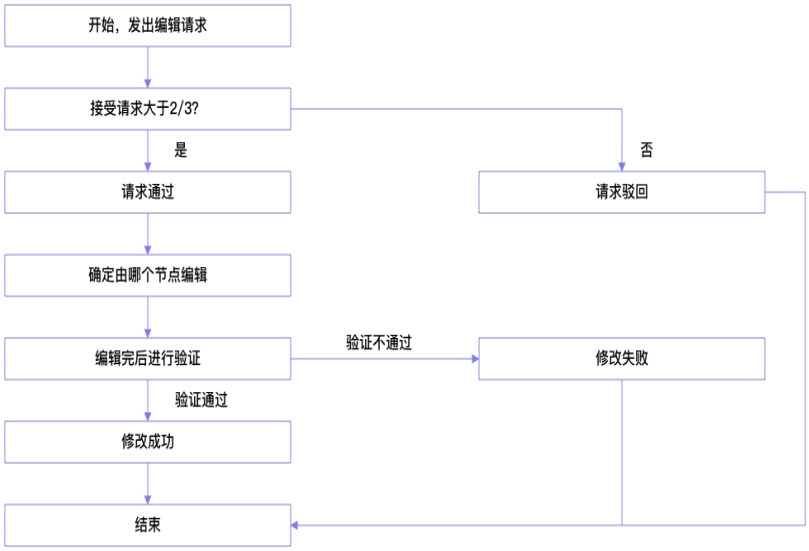

图 10 链上数据修改流程

环境。我们将区块链系统的节点分为三种角色。密钥持有节点负责保管变色龙哈希的私钥；计算节点负责计算新的区块；共识节点负责对编辑请求和编辑结果投票，这种分布式的管理方式增强了编辑行为的安全性。CESS 平台链上数据治理机制的流程如下图所示：区块链系统中所有用户都可以监控链上数据，当监测到错误、有害、过期等信息时，某个节点首次发出区块链编辑请求，并向向全网广播；系统中所有节点对请求进行验证，检查该请求的合理性；当同意该请求的节点数达到一定数量时，方可认为该请求通过，否则驳回该请求；系统根据特定策略选取一个节点编辑区块链；具有修改权的节点按照请求内容编辑区块信息，并向全网广播；其余节点验证操作结果，验证通过后更新自己的账本。这样既保留了平台分布式的特点，又保证了链上数据的有效治理。

链下数据治理：首先，我们将链上区块与链下数据分离。链下数据存储平

台采用统一分布式存储系统 CESS(Cumulus Encrypted Storage System)和基于内容寻址的分片技术，可以有效提升区块链的存储能力和交易速度，并通过友好 API 为用户提供超大文件存储支持。其次，我们建立了激励机制和和黑名单机制，对于共享存储资源或贡献的流量数据质量较好的用户给予存储奖励；而对于用户投诉的文件，确认如果是非法文件，则删除该文件并将此文件记录到黑名单列表。激励用户上传规范、合法的数据文件。另外，我们的安全机制是根据内容寻址，合法的内容不会存在丢失的情况，内容加密且分片存储保证了内容的强安全性。最后，我们还进行了主动备份，将上传的文件主动备份到 2 个 Master 节点，所有对象拥有相同的内容只存储一次，节约了存储空间。

6、独有技术

6.1 可编辑区块链机制

现有的区块链系统由哈希函数的抗碰撞性保证不可篡改性，该特性在为区块链打下安全基础的同时，特定情况下也限制了区块链的发展。因此，CESS 平台引入基于变色龙哈希的可编辑区块链机制。变色龙哈希函数具备陷门碰撞性，即对于掌握陷门的节点可以很容易计算出哈希碰撞，而对于不知道陷门信息的节点则依旧是安全的。如下图所示：首先，我们初始化变色龙哈希函数，得到密钥、陷门等参数；当需要对交易的 payload 进行修订时，只要通过变色龙哈希函数计算出一个新的 Nonce 值，就能根据该值计算出与原来交易相同的哈希值；然后我们对变色龙哈希函数（CH）的陷门实行分布式管理，即将陷门通过秘密分享算法分成多份，分别由多个节点掌握，编辑过程还采用 PBFT 共识机制，保证编辑的过程的安全性。

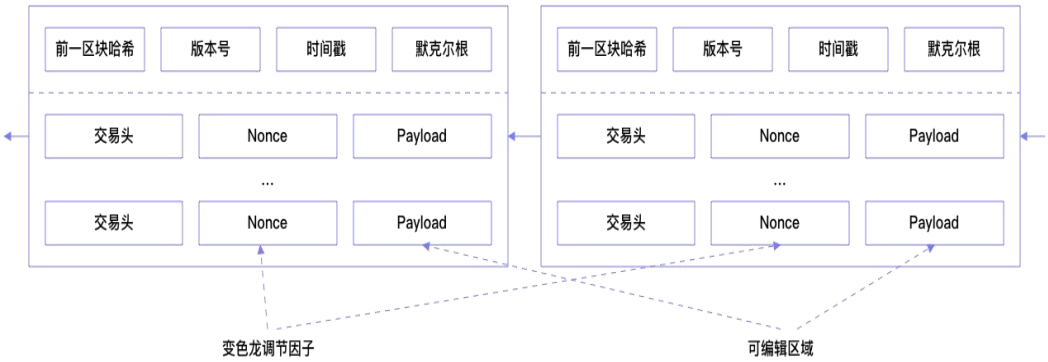

图 11 可编辑区块链机制

6.2 异构链数据跨链流转方法

CESS 提出了一种基于跨链中继的异构链数据跨链流转技术，该方法不仅支持同一网络条件下的区块链之间的通信，还支持面向内、外网络的数据跨链流转需求。发起链在目的链上完成注册后，跨链中继主要提供了跨链单元和网络处理单元，跨链单元负责跨链交易监听、跨链交易执行、跨链交易转发等核心功能，在跨链体系中是一个对接具体类型区块链以及转发跨链消息的重要组成部分；网络处理单元包括内网处理模块、外网处理模块和隔离与交换控制单元等，保障面向内、外网的隔离网络环境中数据交换的安全性。

面向异构链的数据跨链流转体系架构如下图所示，跨链中继作为连接发起链和目的链的桥梁，拥有三类接口：交互接口肩负了跨链可信验证及跨链事务保证的使命，服务接口实现了跨链资源初始化和信息获取与更新的功能，网闸接口为两个网络之间的数据交换提供了通道。

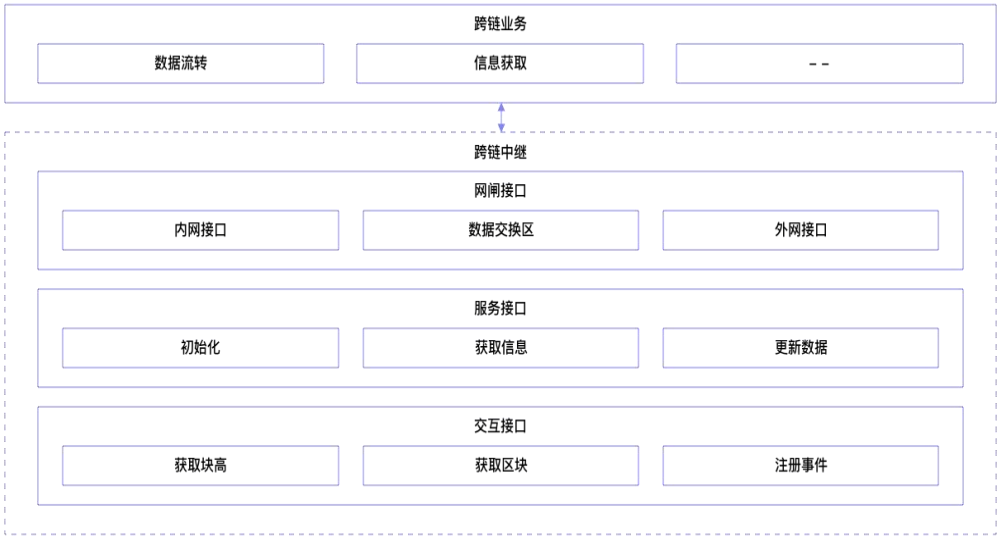

图 12 跨链中继总体架构图

其中，内网接口负责与内网的连接，完成接入网络的用户身份认证，确保数据的安全通道，外网接口处理的是与外网的连接，内网接口与外网接口共同配合实现同一时刻下跨链网闸只与一个网络连接，通过物理隔离内、外网络，阻断来自外网对内网的恶意攻击；数据交换区作为交换数据的中转，受内、外网连接接口控制形成内外网的隔离；初始化接口指的是跨链资源初始化，从源链获取跨链数据并变换格式实现对跨链资源的统一规范；获取信息接口是面向只读场景下链上信息的获取；更新数据接口是面向跨链交易场景下链上数据的更新；获取块高实现了区块头同步的锚定；获取区块指的是查询区块头等信息完成跨链交易验证；注册事件接口用于监听跨链事件，通过构建的区块链事件响应机制完成事件捕获。基于跨链中继的转发路由功能，跨链中继在验证消息来源的可信后通过内外网异步连接通道锚定目的链并转发信息，最终实现异构链之间的通信交互。

6.3 基于全局特征的数据篡改技术

相较于传统中心化云存储，CESS 中的数据分布式地存储在各个节点上，不可避免地，存储数据的生命周期涉及多方法人单位，流动性强，数据的可信与审计成为一个不可忽略的问题。因此，我们基于 CESS 机制的各项特征，创新结合区块链系统，提出基于全局特征的数据篡改技术，实现数据的高效篡改检测功能，多角度提高数据的存储安全。

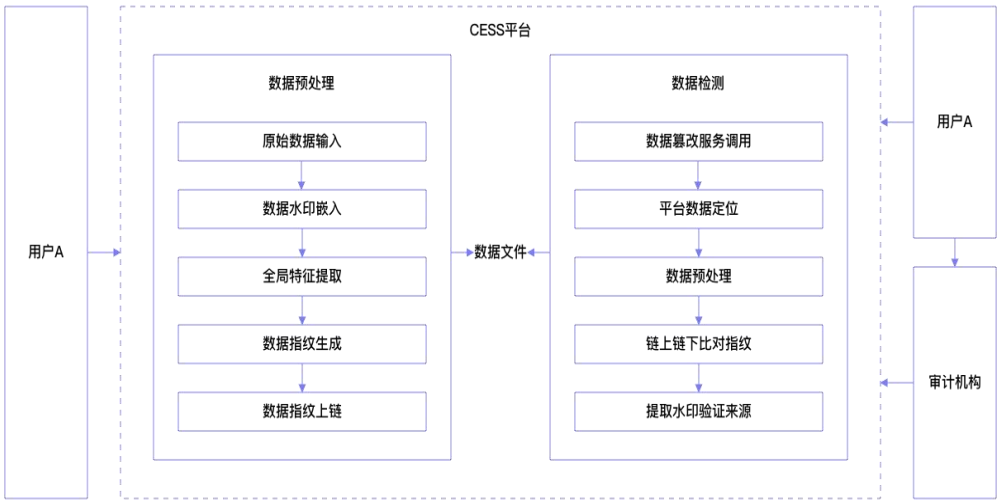

图 13 数据篡改检测服务流程示意图

首先，用户在发布数据至 CESS 之前，针对该数据进行数据预处理。系统集成了包括文本数据、图像数据、音频数据和视频数据等不同数据类型的预处理算法，各算法分别提供定制的基于全局特征的数据指纹提取以及数据水印嵌入功能。对于文本数据可提取文件属性、分词词频直方图、潜在语义等特征；图像数据则可提取如图片 RGB 及灰度直方图和亮度直方图等特征；音频数据同样可提取音频采样频率、频谱图等特征；而视频数据则利用视频关键帧进行全局特征提取。在数据正式发布时，一并将数据指纹信息通过 CESS 上链存储，

随时为用户或第三方审计机构提供数据篡改检测服务。当用户需要验证数据是否被篡改时，可自行或委托可信第三方机构来对数据进行主动检测。1）用户或审计方通过使用 CESS 数据篡改检验服务，利用与上传数据时的预处理阶段相同的算法对待检测数据进行处理来得到该数据的指纹信息 2）同时通过智能合约访问 CESS 平台待检测数据块对应的链上数据指纹。3）利用汉明距离进行检测来判定数据是否存在篡改痕迹，若汉明距离小于设定的阈值，则说明待检测数据为原始数据，若汉明距离大于阈值则判定数据存在篡改痕迹。4）通过读取数据水印信息可验证数据来源。

6.4 多策略存储能力证明机制

确保系统的安全性尤其是完整性是任何信息系统都需关注和着力解决的问题。在 CESS 这样一个去中心化的存储系统中，去中心的属性天然为数据存储带来了更强的隐私性，降低了存储成本，并且提高了传输速度。我们希望 CESS 是一个具有良性的、自主管理的生态系统，因此，我们将采用非中心化的算法来保证系统的正常运行，同时确保系统中奖惩机制的公平公正和很大程度上确保数据的完整性。CESS 主要用以维持整个系统安全稳定使用的存储证明算法有复制证明（PoRep）、时空证明（PoSt）、流量证明（PoF）、存储可用性证明（PoAs）等。

首先，当用户存储文件至 CESS 网络时，系统将采用复制证明算法（PoRep）来确保用户文件的一致性和完整性，复制证明算法（PoRep）是一种交互式的证明算法，存储节点提供存储证明给验证节点，证明用户的数据已经被复制存储到存储节点的专用物理存储设备上。该算法具有抵御女巫攻击、外

源攻击和生成攻击的能力。

系统不仅会在文件上传时进行文件的相关验证，在文件存储的合同期内，还会使用时空证明算法（PoSt）来保证文件的完整性和可恢复性。时空证明算法（PoSt）是衡量并计算存储在网络中的数据存储时间及空间的算法，时空证明可以理解为持续的复制证明。存储节点必须不断的生成证明，并周期性的提交存储证明，如果存储节点没有在提交周期内及时提交证明，则节点无法获取到该周期内的奖励，同时会降低节点在系统中的信用积分。除复制证明算法和时空证明算法外，CESS 系统将对节点的流量也进行分析和统计，从而确定节点在网络传输和分享过程中所作出的贡献。因此，CESS 系统将使用流量证明算法（PoF）来衡量并计算网络中节点贡献的流量。流量证明算法（PoF）采用节点相互进行证明的机制，每个节点需要定期向验证节点提交流量数据（本节点和其他节点交互的数据记录），验证节点将根据这些数据进行统计和分析，以此判断节点在系统流量方面做出的贡献。

CESS 作为一个去中心化分布式网络，系统中节点具有很强的自主性，同时，考虑到网络环境容易波动，系统将采用存储可用证明算法（PoAs）来保证节点具有足够的存储能力和稳定性，该算法一方面通过周期性的监测节点以判断节点状态，同时，系统会结合节点的信用积分进行存储能力评估。用户存储文件时，系统将选择评分更高的节点存储数据。

6.5 基于智能合约的数据权益保护机制

从用户端看，CESS 可作为一个理想的、去中心化、用户自主管理能力强的内容分享平台，它致力于将用户的数据的所有权归还给用户，让用户享受到

自己的数据带来的价值，保护好用户的数据隐私权。为此，CESS 实现了一种自动执行的、公正透明的基于区块链和智能合约的从确权、权益跟踪、到维权的一整套完善的数据权益保护系统。

首先，CESS 为每一份数据都准备了两种收益模型的智能合约供用户选择，用户在发布数据时，只需要按照自己的意愿设置好数值。系统会按照用户的设置，生成数据的权益属性。数据的权益属性主要包括收益模型、白名单、黑名单等。这些策略作为数据的权益属性与数据一同发布。每次数据被访问时，都会执行数据的权益属性中的智能合约，以此来保证按照数据拥有者制定的策略来执行。

当其它用户需要访问数据时，需要先申请数据权限，系统将会更具数据的权益属性，检查申请者账户是否可以访问该数据，如果检查通过，系统将按照数据权益属性中的收益模型执行收费，并返回数据给申请的用户。

CESS 为了促进数据的流通性，当用户申请数据访问权限时，也可以自己设定收益模型合约的数值。系统将按照数据拥有者设定的白名单策略，或者等待拥有者自己判定，如果通过，将会把申请者、申请者的收益模型记录到数据的白名单属性中。通过这种灵魂的模式来促进数据的交流。

如下图所示，CESS 的数据权益保护系统借助于区块链的溯源性，通过扫描随意交易，设有一个专门的证据库模块。证据库提供了一套接口，方便用户随时查看数据的访问记录。为解决数据权益纠纷提供公开、准确的证据。

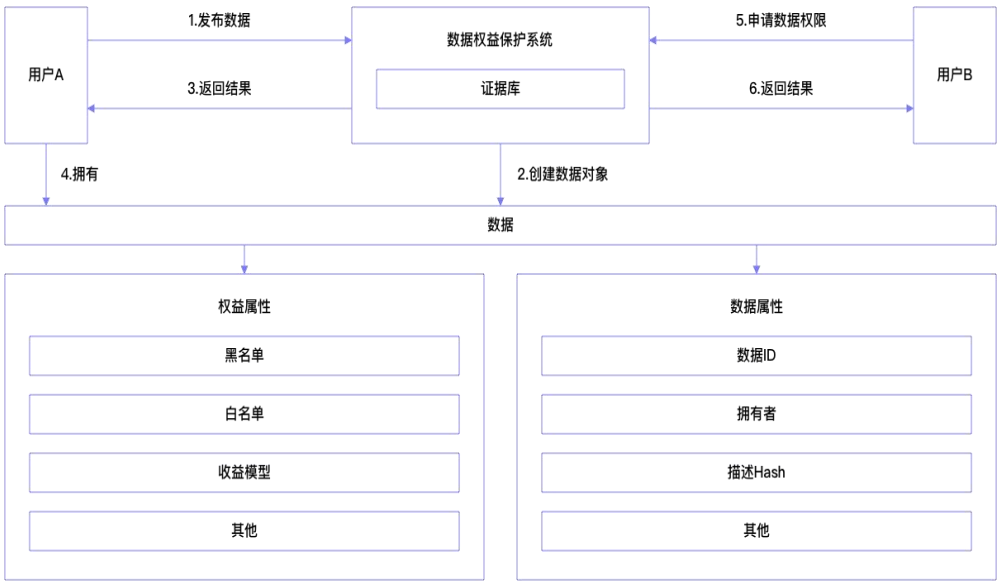

图 14 数据权益保护系统用例示意图

7、安全机制

CESS 是一个基于区块链的分布式存储系统，除了需要构建稳定存储基础网络之外，还需要维护用户数据安全。因此，CESS 采取了严格的安全措施，来确保其存储数据的完整性和可靠性。

7.1 数据安全

为了为用户提供高可靠的数据存储服务，CESS 从数据可用性、数据完整性及数据隐私性三个维度保护用户数据安全。如下图所示，首先，客户端软件对数据进行条带化，利用纠删码机制对数据编码，让数据子层具备一定的纠错能力，避免存储物理节点因黑客攻击、物理设备故障等问题而导致数据不可使用的要素；然后，利用数据完整性验证机制、时空证明机制确保存储节点在合约周期内用户数据是完整的、可用的；第三，对于用户数据隐私问题，我们利用高效的加密算法对用户数据进行加密，确保存储放到存储节点上的数据不是明文存储，有效防止数据泄露的问题。

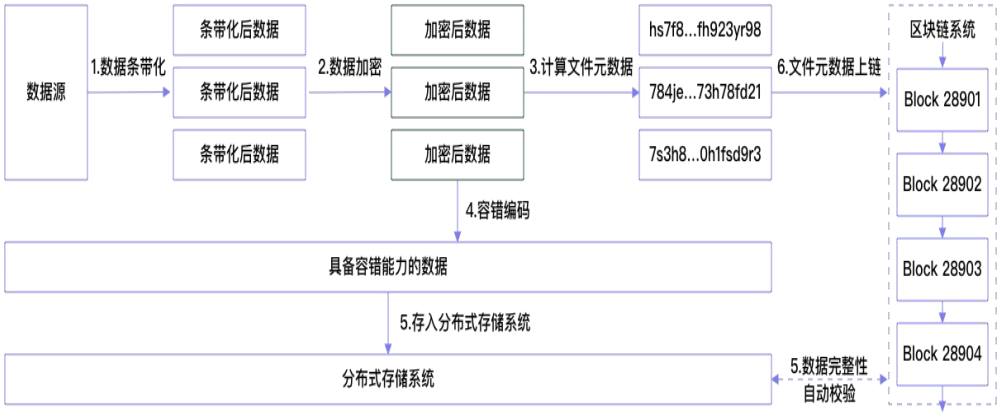

图 15 数据存储流程

7.2 共识安全

区块链作为一种去中心化的分布式公共数据库，通过分布式节点利用密码学协议共同维护。拜占庭攻击是指通信网络中攻击者控制若干授权节点并且任意干扰或破坏网络的攻击方式，会使得区块链节点无法达成共识。CESS平台在治理链上数据的过程中，可能存在节点恶意清除链上数据的行为。

为此，CESS平台搭建混合高效的共识模块。其中，PBFT算法是一种有效的容错共识算法，最多可以容纳网络中存在1/3的恶意节点。当系统中存在f个拜占庭节点（恶意节点）的时候，整个网络中必须拥有3f+1个副本节点才能保证整个网络做出正确的判断。可以有效防止恶意行为上链。

7.3 多副本攻击

任意一个存储矿工需要及时跟验证服务器证明自己确实存储了所分发的数据，但可能存在以某种方式临时生成该数据，并提供证明，获得存储奖励。通过这种攻击，攻击者获得了不公平的存储奖励，更为严重的是，攻击者提供的存储数据，用户无法正确获得原始数据，导致存储系统的可靠性出错。

CESS 的复制证明算法，为一份数据创建多个存储副本时，同步生成 Merkle 树，当存储矿工需要证明自己存储有该数据副本时，必须提供正确的 Merkle 树的路径，保证了矿工不能按照自己的方式存储数据副本，导致数据不可用，同时矿工也无法再获得额外的存储奖励。

8、经济模型

8.1 角色与职能

CESS 网络运行需要多种角色参与运营维护，主要包括：存储矿工（storage-miner）和共识节点（consensue-node）。

- **存储矿工**

  包括存储内容矿工、内容分发矿工，负责存储网络建设工作，存储挖矿，参与存储市场交易。

- **共识节点**

  负责全网交易打包，存储矿工的存储能力模型验证工作。

8.2 存储能力模型

为了保障存储矿工的合理收益，真正做到存储矿工的收益公平和公正，CESS 网络构建了一套完整的存储能力模型测评体系，并根据每个矿工的存储能力模型进行科学的评分，系统将这个分数叫做信用值，并根据信用值所在的区间进行奖励。影响信用值大小的指标如下：

- 基本运行情况指标

  1. 机器配置
  2. 机器在线时长
  3. 机器的运行带宽

- 资源贡献指标

  1. 存储文件的大小

2. 节点网络贡献流量的大小

以上几种是现有建立模型的指标，后续根据项目运转的情况，会不断丰富指标来完善存储的能力模型，并通过人工智能机器学习的方式，自我调整和改进。

8.3 存储奖励

1） 基本情况运行指标评定

通过可用存储服务证明算法（PoAs）来进行验证，并对节点的可用存储服务打分。

2） 资源贡献指标评定

存储文件的大小：系统采用时复制证明算法(PoRep)和时空证明算法（PoSt）。

节点网络贡献流量的大小主要是节点与节点之间流量的大小，采用流量证明算法(PoF)。

CESS 网络的存储节点和存储矿工的奖励通过其做出的贡献来进行合理的分配，贡献值大小 R 是由其累计的存储证明来确定的，公式如下：

$$R = (\alpha f(PoSt) + \beta f(PoRep) + rf(PoF) + df(PoAs)) * x$$

x 为抵押参数，如果两个矿工累计的贡献相等，则未来服务更长的矿工将被分配更高的抵押参数，因此获得更高的采矿奖励。每个证明的比例因子的默认值如下表 1 所示：

比例因子	描述	默认值
α	时空证明算法	40%
β	复制证明算法	20%
r	流量证明算法	30%
d	可用存储服务证明算法	10%

表 1 每个证明的比例因子默认值

在 CESS 的早期部署期间，预计存储的数据量和存储量交易将比较低。为了鼓励新矿工或者节点加入网络并提供可用存储服务，在此期间将提高 PoAs 的比例因子。随着存储量的增长，PoAs 的比例因子将逐渐减小，而其他存储证明的比例因子将增加。

8.4 代币分配模型

总量 100 亿 CESS。

角色	分配比例	分配数量	释放方式
初期贡献者	15%	15 亿	6 年线性释放
矿工	45%	45 亿	25 年挖完，矿币 25%即刻释放，75%在 180 天线性释放（每四年减产一次）
社区激励	10%	10 亿	KPI
合作伙伴	11%	11 亿	开发，合作
预留	9%	9 亿	DAO
融资	10%	10 亿	公众投资和战略投资。（1–36 个月线性释放）

8.5 各角色收益模型

CESS 网络在创建初期阶段，存在两种角色，如下：

- 存储矿工：存储挖矿收益+质押挖矿收益+用户支付收益。
- 共识矿工：验证存储数据，生成区块，获得部署区块奖励。

9、去中心化交易和存储挖矿

9.1 存储交易市场: 可验证可信的交易市场

在存储应用的商业行为上，存在着“存储供应商 to 应用 to 用户”这样一条产业链条。CESS 将改善这条产业链，打造存储供应商 to 用户的自由交易市场。在 CESS 经济体中，存储交易市场是可验证、可信的交易市场，客户（买方）可以直接向存储矿工（卖方）购买低价的存储空间来存储数据。

系统根据以下要求设计存储市场协议：

- 订单上链：

订单价格公开透明，客户可以根据全网订单的情况来制定适合自己的订单，并将订单提交上链，只有上链成功的订单才能够被网络所接受，上链成功后不能进行修改。

- 参与者投入资源：

为了保证存储市场的稳定，防止存储矿工不提供服务或者提供服务超时，存储矿工必须抵押与存储量大小成一定比例的抵押金放到存储的验证池中，客户支付订单的费用也会先进入验证池中，只有验证通过，订单费才会打入存储矿工的账户中。从而保证交易的流畅和安全。

- 自组织处理：

存储矿工需要在约定的时间内多次提交订单向验证矿工证明它们的存储行为，验证矿工必须能够及时准确的进行验证，并及时返回结果。

9.2 存储挖矿：去中心化存储的商业实现

CESS 去中心化存储是基于 CESS 共识网络实现的。存储矿工需提交存储数据的数据持有证明给验证矿工，验证矿工验证通过后才可以获得相应奖励。

去中心化存储的商业实现需要矿工存储有效数据而不是无效的随机数据，存储矿工需要获得资格并质押一部分 CESS 奖励作为订单赔付金，随着订单时长减少线性返还卖方，存储矿工需在存储交易市场接受存储需求方的存储订单，系统通过订单进行验证，验证成功后，存储矿工获得存储挖矿奖励和用户支付的费用。

9.3 存储资产做市商：提升经济体内的资源整合

去中心化不等于去中介化，尤其在企业级资源分配等场景下，个体存储矿工和存储需求用户在交易市场上的匹配明显是低效和不经济的。存储资产做市商的出现，则解决了效率问题，可以通过市商规模化集中提供存储资源，并交易给存储需求方（应用），做市商的存在将极大的提升经济体内的资源整合能力，进一步提高产业链效率。

10、展望未来

开启一个去中心化分布式云存储的时代，从 CESS 开始。

随着分布式存储技术的日新月异，热点频出。云存储行业和区块链行业的发展总是有各种崭新的增长点和时代性的革命。就像苹果手机重新定义了手机，CESS 将重新定义区块链存储系统。

数字经济之父、全球著名新经济学家唐·塔斯考特（Don Tapscott）曾说：“在未来几十年，带来巨大影响的可能并不是社交媒体，也不是大数据和机器人科学。如果我们不仅能将价值互联，还能让价值互联，让大量的、全球性的分散式账本可以在数千万台电脑上运转，每个人都有访问权，无论什么样的资产，从金钱到音乐，都可以进行存储、移动、交易和管理，而且不经过强大的中间商，能将这些实现的科技就是比特币等数字货币的技术基础，也就是区块链。区块链并不是什么华丽的辞藻，但我相信它将是互联网的未来，并且给每一次交易、每一个社会、每一个人带来光明的前景。”

基于区块链的去中心化云存储基础网络设施，CESS 致力于推动数据和信息互联，构建更加开放、公平和安全的网络环境，推动 Web3.0 的发展。CESS 必将重新定义存储系统，而这也将对未来万物互联的数字世界的发展形成最为深远的影响。

人们对自己的个人数据宣誓主权，自己的数据是自己的资产！自己的数据自己做主！

这就是 Cumulus Encrypted Storage System(CESS)努力追求实现的核心价值和意义，也是致力于推动 Web 3 发展的强大动力！

我的数据我做主!

参考文献：

1. Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto,2008.

2. Proof of space from stacked expanders.Ling Ren, 2016.

3. Practical byzantine fault tolerance, M Castro, B Liskov – OSDI, 1999.

4. Practical Byzantine fault tolerance and proactive recovery, Miguel Castro, Barbara Liskov, 2002.

5. Secure and efficient proof of storage with deduplication, Qingji Zheng,Shouhuai Xu, 2012.

6. Comparative analysis of blockchain consensus algorithms, LM Bach, B Mihaljevic, M Zagar, 2018.

7. From blockchain consensus back to Byzantine consensus, Vincent Gramoli, 2020.

8. Proof of luck: An efficient blockchain consensus protocol, Mitar Milutinovic, 2016.

9. An innovative IPFS-based storage model for blockchain, Qiuhong Zheng, 2017.

10. Ethereum: A secure decentralised generalised transaction ledger[J]. Wood G.， 2014.

11. Data object store and server for a cloud storage environment, including data deduplication and data management across multiple cloud storage sites, 2012.

12. Cassandra: a decentralized structured storage system, Lakshman A, 2010.

13.Enabling public auditability and data dynamics for storage security in cloud computing, Wang Q, 2010.