

# YET 云存储生态白皮书

Yotta Ecological System White Paper

---

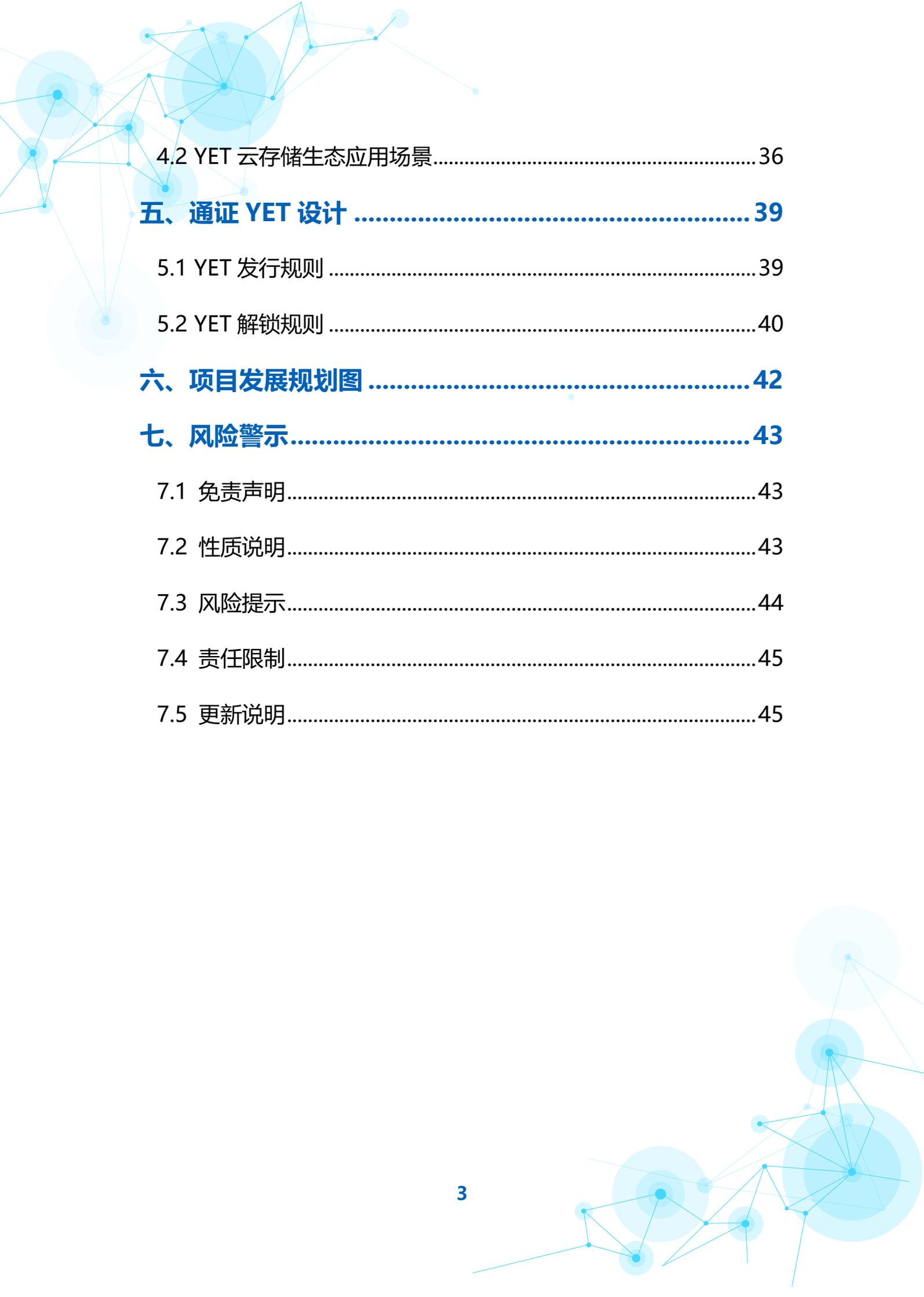
**全球顶尖的区块链存储技术服务提供商**



YET 基金会 V1.0

# 目录

摘要.....	4
<b>一、YET 云存储生态体系.....</b>	<b>6</b>
1.1 区块链结合分布式存储：颠覆传统互联网的革命.....	6
1.2 YottaChain 走在区块链云存储时代前沿 .....	13
1.3 基于 YottaChain 开发的 YET 云存储生态.....	15
1.4 YET 云存储公链 .....	18
<b>二、技术阐述.....</b>	<b>19</b>
2.1 区块链技术阐述 .....	19
2.2 区块链存储技术阐述.....	21
2.3 YottaChain 核心技术阐述 .....	26
2.4 YET 云存储生态技术阐述.....	29
<b>三、网络架构设计.....</b>	<b>30</b>
3.1 分布式存储架构 .....	30
3.2 YET 生态系统结构.....	32
<b>四、应用场景.....</b>	<b>33</b>
4.1 区块链存储应用场景 .....	33



4.2 YET 云存储生态应用场景.....	36
<b>五、通证 YET 设计 .....</b>	<b>39</b>
5.1 YET 发行规则 .....	39
5.2 YET 解锁规则 .....	40
<b>六、项目发展规划图 .....</b>	<b>42</b>
<b>七、风险警示.....</b>	<b>43</b>
7.1 免责声明.....	43
7.2 性质说明.....	43
7.3 风险提示.....	44
7.4 责任限制.....	45
7.5 更新说明.....	45



## 摘要

从传统的工业模式到如今的信息浪潮，我们都处于一种不断更新资源的环境中。同时，随着智能化带给人类爆炸性的影响后，数据成为当下的主流，也是最宝贵的资源，而信息也从集中存储转变成现在的分布式存储。

与现有云存储解决方案相比，基于区块链的分布式存储更便宜，更安全，更快，更具审查性，并且分布更广。它充分利用了这样一个事实：大量的存储空间在世界各地的人们的硬盘上未被使用。为此创造允许人们把他们备用存储空间货币化的市场。全球存储市场的涌入将降低存储价格。

在大数据时代，区块链存储正在慢慢渗透我们的生活，并且应用范围也愈加广泛。可以预见，区块链存储是颠覆传统互联网的、未来必不可少的技术之一。

建立在区块链存储技术的基础上，立足于 YottaChain 区块链存储的前沿技术，YET 团队打造区块链云存储生态。同时，围绕通证经济打造云存储公链，以及基于区块链技术打造云存储平台，YET 团队旨在成为全球顶尖的区块链存储技术服务提供商。



YET 云存储生态应用场景包括但不限于云盘 DAPP, 内容共享 DAPP, 账号代理 DAPP, 以及第三方 DAPP 等等, 应用场景十分丰富。YET 团队将服务全球用户, 为其提供全球尖端的区块链存储技术, 共享更大规模的云存储空间。

YET (全称 Yotta Ecological System) 是 YET 云存储生态中对参与者的贡献量通证, 是生态圈的价值核心, 其价值来源于生态成员的价值贡献。区块链中的矿工可以通过为客户提供存储来获取 YET。相应地, 客户可以通过花费 YET 来雇佣矿工来存储或分发数据。和比特币一样, 矿工们为了巨大的奖励而竞争式挖区块。

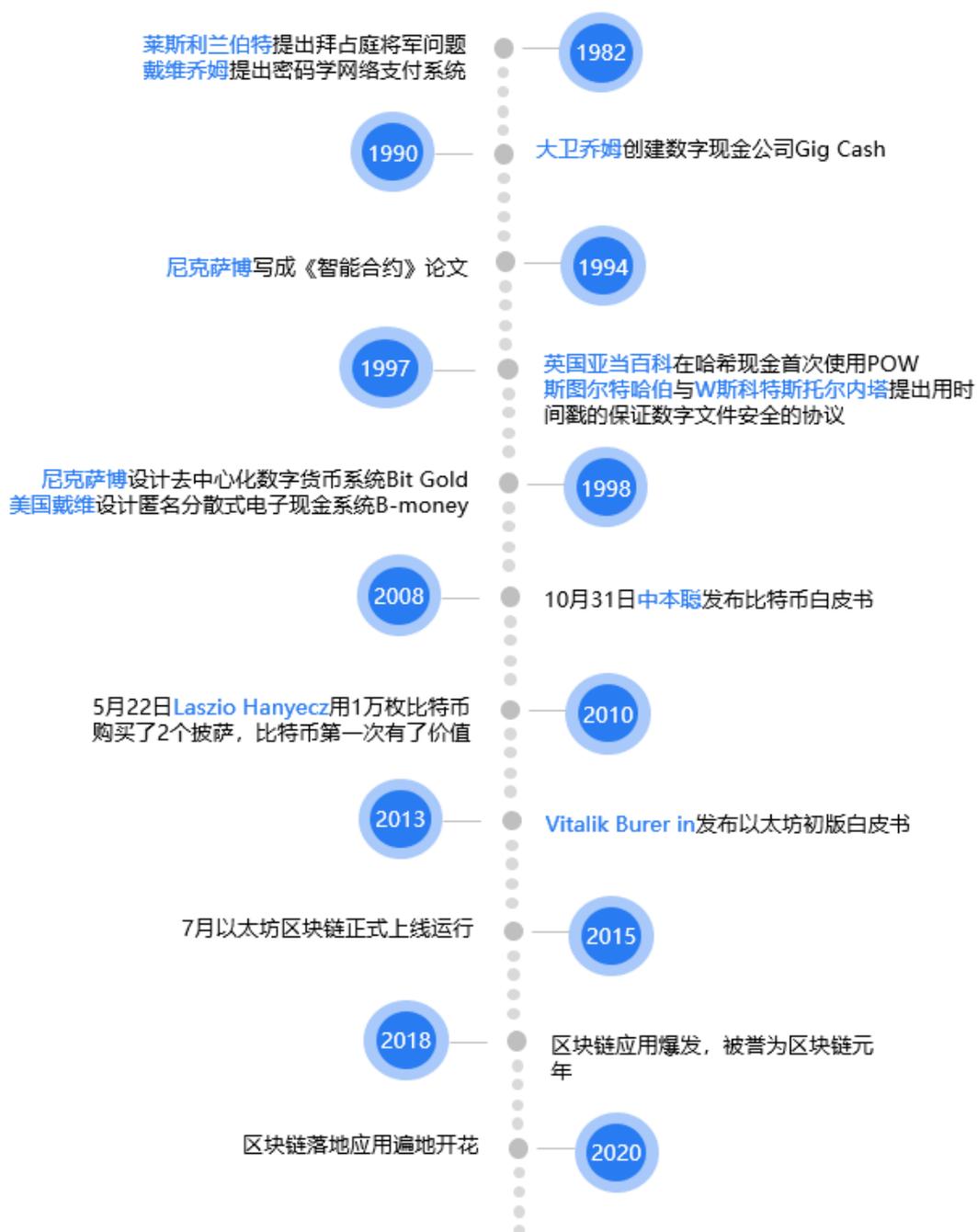
在生态发展上, YET 可直接迁移现有数百万种应用, 共享最前沿的云存储技术。第三方区块链存储系统加入 YET 云存储生态, 即可快速获得关键技术, 共享云存储空间, 实现合作共赢。

存储将是区块链技术的最佳落地应用场景, 下一个区块链时代也将是云存储时代, YET 云存储生态顺势而为, 应运而生。

# 一、YET 云存储生态体系

## 1.1 区块链结合分布式存储：颠覆传统互联网的革命

### 1.1.1 区块链技术的发展历程





### 1.1.2 存储从传统到现代：实现云端

伴随着计算机规模的扩大，将所有的业务单元集中在一个或若干个大型机上的体系结构已然不能满足当今计算机系统的需求，尤其是互联网的快速发展，致使系统构架模型灵活多变，层出不穷，我们现在正在经历一场前所未有的由传统存储（以集中存储（本地存储）为主）到分布式存储（（云存储）以软件定义存储为主）的蜕变。

所谓集中式系统就是指由一台或多台计算机组成中心节点，数据集中存储于这个中心节点中，并且整个系统的所有物业单元都集中部署在这个中心节点上，系统所有功能均由其集中处理。也就是说，集中式系统中，每个终端或客户端及其仅仅负责数据的录入和输出，而数据的存储与控制处理完全交由主机来完成。

集中式系统最大的特点就是部署结构简单，由于集中式系统往往基于底层性能卓越的大型主机，因此无需考虑如何对服务进行多个节点的部署，也就不需要考虑多个节点之间的分布式协作问题。

分布式系统是一个硬件或软件组件分布在不同的网络计算机上，彼此之间仅仅通过消息传递进行通信和协调的系统。

### 1.1.3 分布式存储系统的特性

- 
- 1.高可用性
  - 2.高可靠性
  - 3.高扩展性
  - 4.数据一致性
  - 5.高安全性
  - 6.高性能
  - 7.高稳定性

#### (1) 高可用性

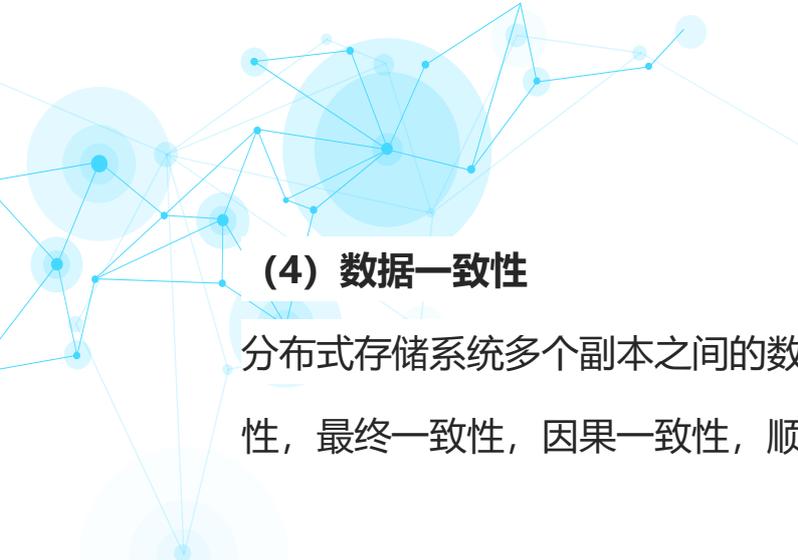
分布式存储系统在面对各种异常时可以提供正常服务的能力。

#### (2) 高可靠性

重点指分布式系统数据安全方面的指标，数据可靠不丢失，主要用多机冗余、单机磁盘 RAID 等措施。

#### (3) 高扩展性

分布式存储系统通过扩展集群服务器规模从而提高系统存储容量，计算和性能的能力，业务量增大，对底层分布式存储系统的性能要求越来越高，自动增加服务器来提升服务能力，分为 Scale Up 与 Scale Out。



#### **(4) 数据一致性**

分布式存储系统多个副本之间的数据一致性，有强一致性，弱一致性，最终一致性，因果一致性，顺序一致性。

#### **(5) 高安全性**

分布式存储系统不受恶意访问和攻击，保护存储数据不被窃取，针对现存的和潜在的各种攻击与窃取手段，要有相应的应对方案。

#### **(6) 高性能**

衡量分布式存储系统性能常见的指标是系统的吞吐量和系统的响应延迟，系统的吞吐量是在一段时间内可以处理的请求总数，可以用QPS (Query Per Second) 和TPS (Transaction Per Second) 衡量。系统的响应延迟是指某个请求发出到接收到返回结果所消耗的时间，通常用平均延迟来衡量。这两个指标往往是矛盾的，追求高吞吐量，比较难做到低延迟，追求低延迟，吞吐量会受影响。

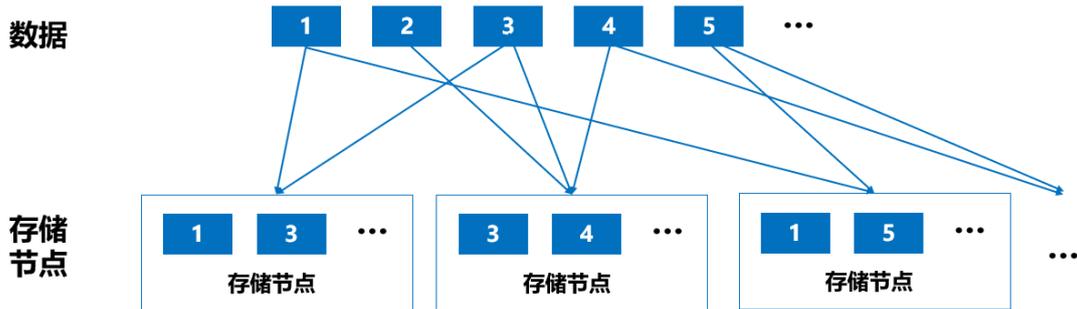
#### **(7) 高稳定性**

这是一个综合指标，考核分布式存储系统的整体健壮性。任何异常，系统都能坦然面对，系统稳定性越高越好。

## 1.1.4 区块链存储是什么？

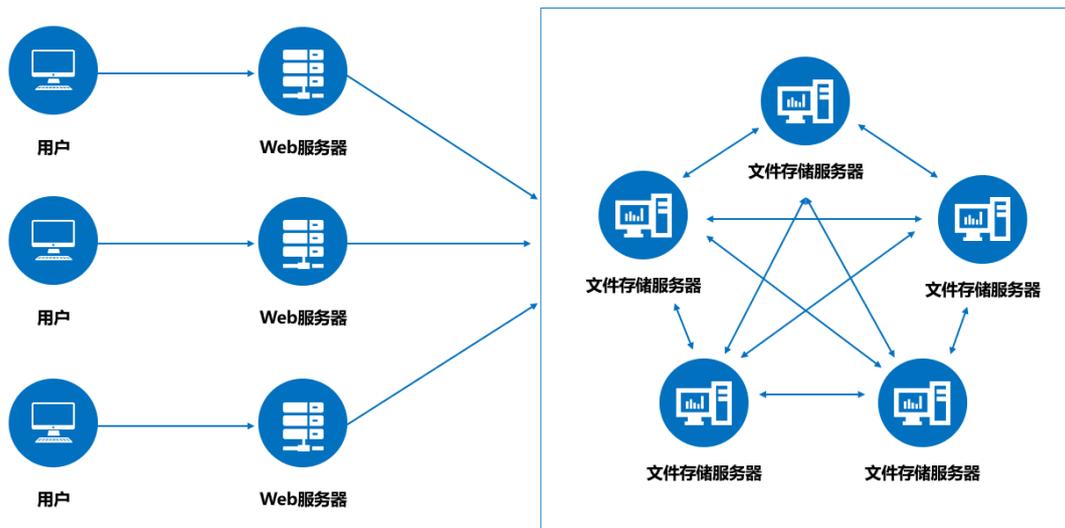
### 1.1.4.1 去中心化+存储

去中心化被理解为权力从中央实体转移到更加本地化和“自由”的体系。



### 1.1.4.2 分布式存储

分布式存储是一个能够存储文件的系统，无需回复大量集中的数据孤岛，这些数据孤岛不会破坏隐私和信息自由等重要价值。



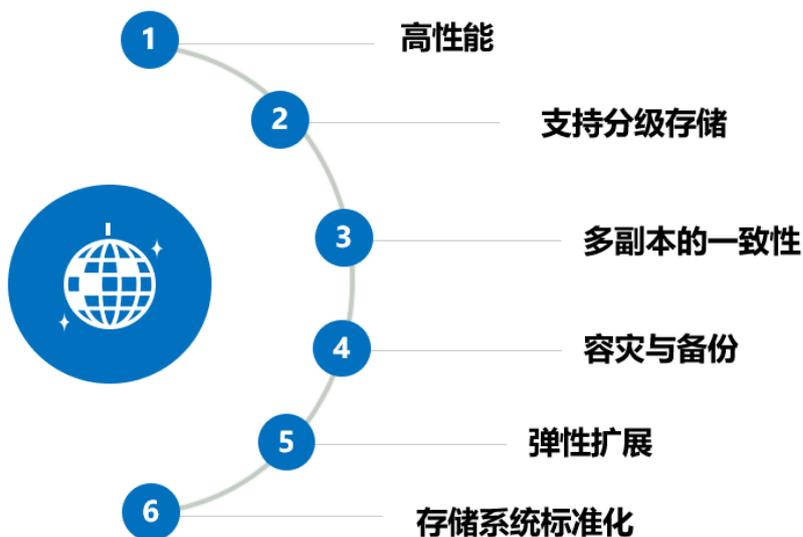
### 1.1.4.3 区块链存储

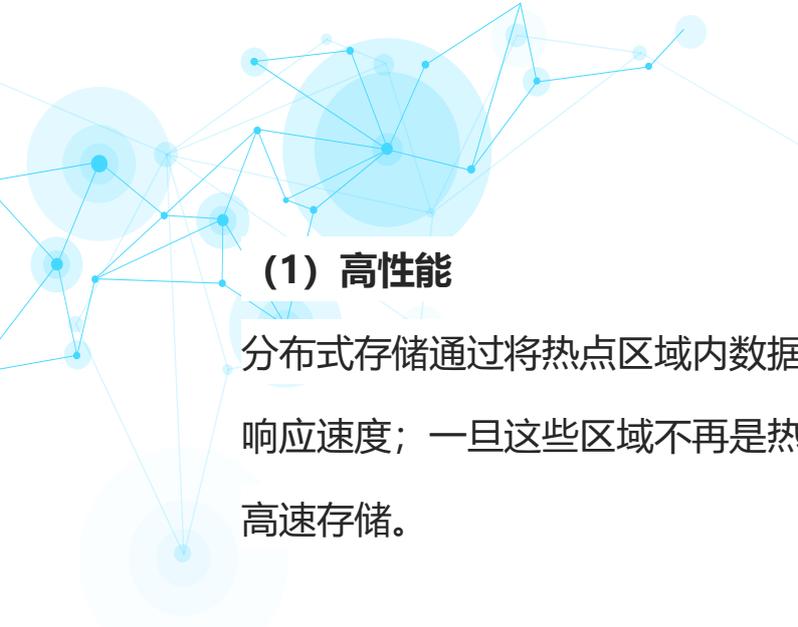
区块链技术不仅是加密通证的基础技术，也可以实现分布式存储；不仅能够存储加密货币的交易记录，还能存储其它类型的数据，这在许多行业都能有所应用。

区块链、大数据等已然变成新一代科技潮流的代名词，已经是公平、透明、自由的象征。尤甚在遇到文件和数据存储时，区块链的原始目的变得尤为明显。

### 1.1.5 区块链结合分布式存储：解决传统痛点

分布式存储技术是区块链的基础也是关键所在，分布式存储技术正在逐渐渗透进我们的生活，应用范围愈加广泛，它的高可用性，高扩展性，数据一致性等充分弥补了传统存储方式的痛点。区块链结合分布式存储具有以下优势：





### **(1) 高性能**

分布式存储通过将热点区域内数据映射到高速存储中，来提高系统响应速度；一旦这些区域不再是热点，那么存储系统会将它们移出高速存储。

### **(2) 支持分级存储**

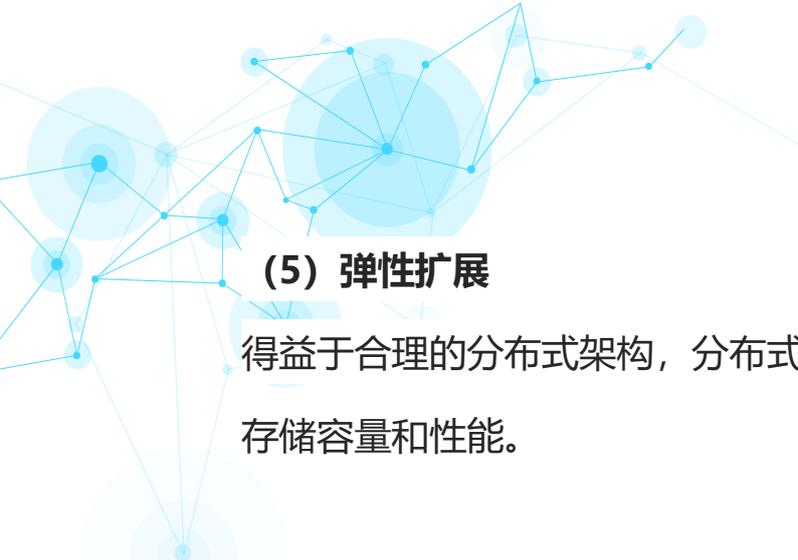
分布式存储允许高速存储和低速存储分开部署，或者任意比例混合。解决了目前缓存分层存储问题——当性能池读不命中后，从冷池提取数据的粒度太大，导致延迟高，从而给造成整体的性能的抖动的问题。

### **(3) 多副本的一致性**

分布式存储采用了多副本备份机制。在存储数据之前，分布式存储对数据进行了分片，分片后的数据按照一定的规则保存在集群节点上。当数据长时间处于不一致状态时，系统会自动数据重建恢复，同时租户可设定数据恢复的带宽规则，最小化对业务的影响。

### **(4) 容灾与备份**

在分布式存储的容灾中，一个重要的手段就是多时间点快照技术，使得用户生产系统能够实现一定时间间隔下的各版本数据的保存。



## (5) 弹性扩展

得益于合理的分布式架构，分布式存储可预估并且弹性扩展计算、存储容量和性能。

## (6) 存储系统标准化

随着分布式存储的发展，存储行业的标准化进程也不断推进，分布式存储优先采用行业标准接口（SMI-S 或 OpenStack Cinder）进行存储接入。基于异构存储整合的功能，用户可以实现跨不同品牌、介质地实现容灾，如用中低端阵列为高端阵列容灾，用不同磁盘阵列为闪存阵列容灾等等，从侧面降低了存储采购和管理成本。

## 1.2 YottaChain 走在区块链云存储时代前沿

### 1.2.1 数据存储和防护工作势在必行

“互联网+”时代社会各行各业生产和人们生活模式都发生了颠覆性改变，引发巨大变革，数据资产价值愈加凸显。享受红利的同时，危害也随之而来，数据泄漏事件层出不穷，国家、企业和个人利益接连受损，衍生的灰色产业愈演愈烈，屡禁不止，国家安全发展受到严重威胁。在这样的背景下，该如何加强对数据的防护，成为了摆在社会一大难题。

移动互联网应用程序得到广泛应用，在促进经济社会发展、服务民生

等方面发挥了重要作用。同时，App 强制授权、过度索权、超范围收集个人信息等现象大量存在，违法违规使用个人信息的问题突出。因而数据存储和防护工作势在必行。

## 1.2.2 YottaChain 蕴藏巨大优势

### 1.2.2.1 区块链存储的局限性

尽管区块链存储具有无可比拟的优越性，但仍然存在不足之处。

#### 区块链分布式存储的局限性



缺乏数据安全机制



数据可靠性不够



不支持动态网页



服务稳定性不够

### 1.2.2.2 YottaChain 完善了区块链存储技术

YottaChain 是基于颠覆性的技术和深厚的行业资源打造的区块链存储公链，完善了诸多区块链存储技术的缺点，为原中心化存储的用户提供端到端无缝衔接的高品质低成本持久化存储和网络加速解决方案，还制定区块链存储协议 BSP，打造区块链存储开放平台，为 DAPP 提供可靠、廉价、大容量、高性能的去中心化存储，为其它区块链存储系统提供核心能力并共享去重放大效应。

相对于市面上常见的区块链存储项目，YottaChain 得出了极大的改进。

### YottaChain与常见区块链分布式存储项目简单对比

	网络加速市场 (几十亿美元规模)	持久化存储市场 (几百亿美元规模)	加密去重	区块链存储开放平台	中心化存储市场迁移
市面上常见的区块链分布式存储项目	✓ 适用	× 不适用	× 只去重不加密，不适用于存储个人和企业数据	× 无	× 无
YottaChain	✓ 适用	✓ 适用	✓ 零知识加密+跨用户去重，既能适用个人和企业数据还不影响数据去重的商业模式	✓ 通过BSP协议赋能所有区块链存储系统（包括IPFS），依靠核心技术和网络效应覆盖到所有区块链存储系统	✓ 拥有相关行业资源，技术上可无缝迁移中心化存储的应用

## 1.2.3 基于 YottaChain 打造 YET 云存储生态

YET 云存储生态，正是基于 YottaChain 的区块链技术，而打造的。可链接多个分布式存储生态，实现云存储空间和技术的共享。

YET 云存储生态系统架构包含三层，分别为应用层、YET 公链和底层技术。

## 1.3 基于 YottaChain 开发的 YET 云存储生态

### 1.3.1 YET 云存储平台应运而生

YET 云存储平台正是在这样的背景下诞生。YET 云存储平台为各区块链存储系统提供核心技术赋能，并为上层应用提供各类存储服务，包括至关重要的加密去重技术，去中心化静态持久存储、去中心化动态



持久存储、本地缓存、CDN 等存储服务，存储管理、跨链调度等管理功能，还包括账号管理、密钥管理等数据安全机制。所有这些都通过 BSP 区块链存储协议开放给所有区块链存储系统和上层应用。

去中心化静态持久存储适宜存储静态数据，存储所采用的数据，可靠性远高于最好的中心化存储，是通过数据的 hash 值来访问的；

去中心化动态存储的数据可靠性与去中心化静态存储相似，但是需要通过 ID 来访问，一个文件无论内容发生多少变化，其 ID 都不会发生改变。同一 ID 的文件，新内容会覆盖旧内容；

本地缓存使用本地存储资源，性能较高但不能用于持久化存储；

CDN 适于网络加速，只保存最热门的内容，对没有命中的内容回源；

存储管理根据市场供需状况自动分配各存储服务所占用的存储资源，以保证矿工利益和用户利益的最大化，并根据各资源通证和第三方区块链存储系统的市场行情、当前平均数据重复率和税率自动计算各存储服务的报价。

跨链调度根据用户需求分配存储流量，评估各存储系统的可靠性，并



在用户许可的前提下尽量做到跨链存储,以最大程度隔离故障域、提高系统冗余性,从而提高数据可靠性。

数据安全机制基于 TruPrivacy 技术,用于对持久化存储的数据进行加密和密钥管理,确保只有数据的 owner 及其授权者才能使用数据,其他人都无法看到数据;而且读写权限分离,可以分开单独授权。

### 1.3.2 BSP 协议

一个区块链存储系统,通过对接 BSP 协议,可以享有 YET 云存储平台的全部功能,包括加密去重等对区块链存储起到决定性作用的核心技术,直接带来市场收益的对中心化应用的无缝对接,也包括非常专业的各种类型的存储服务,专业的密钥管理和账号管理功能等。除此之外,所有运行在 YET 云存储平台之上的区块链存储系统还都可以共享“去重效应”的红利,获得远大于自身的存储放大系数(这是因为用户越多数据越多则放大系数越高),从而可以销售更多的数据存储空间,多挣几倍的钱。例如,假设某第三方区块链存储系统有 1 万个存储节点,合计 10PB 存储空间,单独自己的去重放大效应是 1.8 倍,可销售 18PB 存储空间,加入 YET 云存储生态可获得 5 倍放大效应,销售 50PB 空间。

调用 YET 云存储平台需要消耗一定的 YET,但数量是很少的,相当于



各种 ERC20 通证在以太坊平台上需要消耗一定的 ETH 作为 Gas。

与 YET 云存储平台带来的收益相比, 其比例是很低的, 从而达到生态共同发展共同收益的目标。

## 1.4 YET 云存储公链

### 1.4.1 YET 云存储公链

YET 云存储公链实现基于 DAG 的区块链系统, 通过 DPOS 共识算法实现对矿工的激励, 并提供 YET 双向兑换各类资源通证以及用户使用资源通证购买各类存储服务或计算服务的内部交易市场。



## 二、技术阐述

### 2.1 区块链技术阐述

#### 2.1.1 区块链技术特征

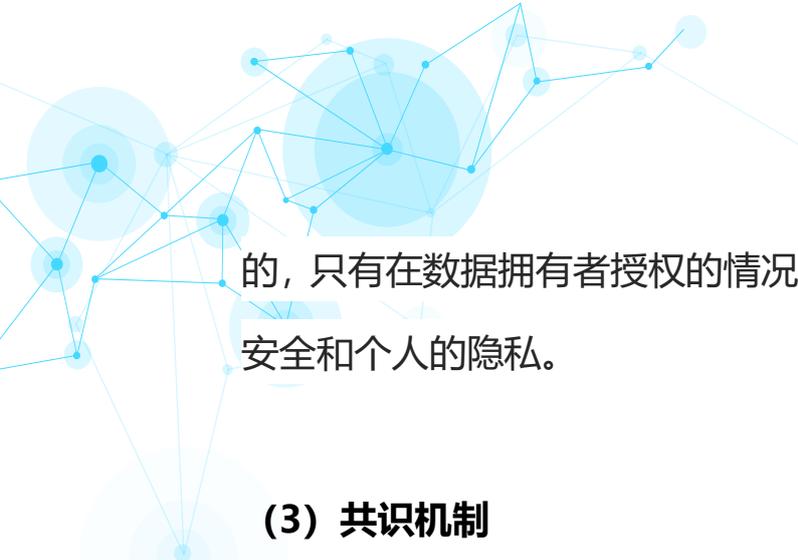
##### (1) 分布式账本

分布式账本指的是交易记账由分布在不同地方的多个节点共同完成，而且每一个节点记录的是完整的账目，因此它们都可以参与监督交易合法性，同时也可以共同为其作证。

跟传统的分布式存储有所不同，区块链的分布式存储的独特性主要体现在两个方面：一是区块链每个节点都按照块链式结构存储完整的数据，传统分布式存储一般是将数据按照一定的规则分成多份进行存储。二是区块链每个节点存储都是独立的、地位等同的，依靠共识机制保证存储的一致性，而传统分布式存储一般是通过中心节点往其他备份节点同步数据。没有任何一个节点可以单独记录账本数据，从而避免了单一记账人被控制或者被贿赂而记假账的可能性。也由记账节点足够多，理论上讲除非所有的节点被破坏，否则账目就不会丢失，从而保证了账目数据的安全性。

##### (2) 非对称加密

存储在区块链上的交易信息是公开的，但是账户身份信息是高度加密



的，只有在数据拥有者授权的情况下才能访问到，从而保证了数据的安全和个人的隐私。

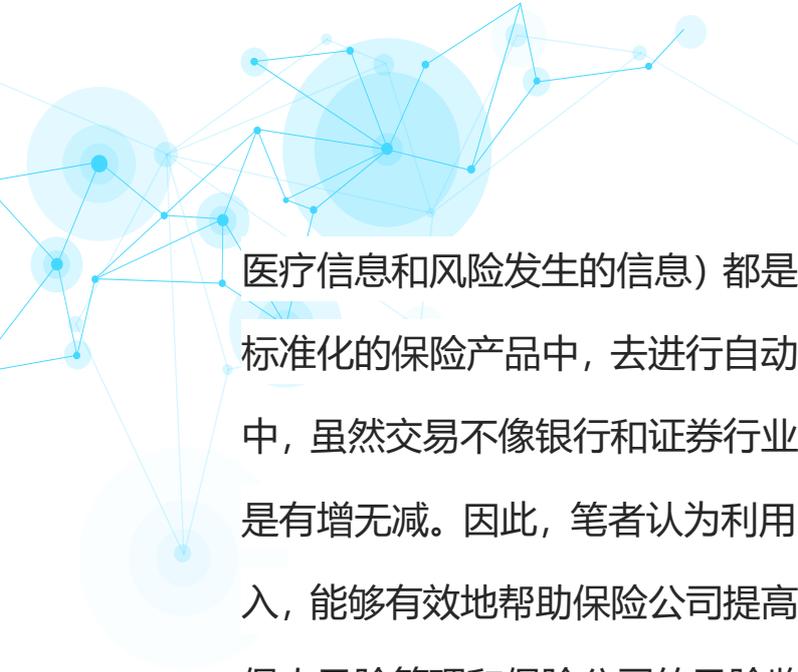
### **(3) 共识机制**

共识机制就是所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了四种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。

区块链的共识机制具备“少数服从多数”以及“人人平等”的特点，其中“少数服从多数”并不完全指节点个数，也可以是计算能力、股权数或者其他的计算机可以比较的特征量。“人人平等”是当节点满足条件时，所有节点都有权优先提出共识结果、直接被其他节点认同后并最后有可能成为最终共识结果。以比特币为例，采用的是工作量证明，只有在控制了全网超过 51%的记账节点的情况下，才有可能伪造出一条不存在的记录。当加入区块链的节点足够多的时候，这基本上不可能，从而杜绝了造假的可能。

### **(4) 智能合约**

智能合约是基于这些可信的不可篡改的数据，可以自动化的执行一些预先定义好的规则和条款。以保险为例，如果说每个人的信息（包括



医疗信息和风险发生的信息) 都是真实可信的, 那就很容易的在一些标准化的保险产品中, 去进行自动化的理赔。在保险公司的日常业务中, 虽然交易不像银行和证券行业那样频繁, 但是对可信数据的依赖是有增无减。因此, 笔者认为利用区块链技术, 从数据管理的角度切入, 能够有效地帮助保险公司提高风险管理能力。具体来讲主要分投保人风险管理和保险公司的风险监督。

## 2.2 区块链存储技术阐述

### 2.2.1 区块链存储工作原理

区块链分类账作为一个去中心化的数据库, 用于保存每个事务的详细信息。交易按时间顺序添加到分类账, 并存储为一系列的块, 每个块引用前面的块以形成一个互连的链条。分类账分布在多个节点上, 每个节点都保存一个完整的副本。区块链自动同步和验证所有节点上的事务。分类账对所有参与成员都是透明的, 可以验证, 无需中央机构或第三方验证服务。

由于其分布式特性, 区块链技术被评价为“天然适合 P2P, 去中心化存储”。在这个场景(数据存储)中, 区块链提供了创建一个地理上分散的存储资源的逻辑存储池所需的结构, 其中, 这些存储池可充当区块链节点。基于区块链的存储系统, 会为存储准备数据,



然后通过一个去中心化的基础架构进行分发，这个过程可以分为以下六个步骤：

(a) 创建数据分片。存储系统将数据分成更小的片段，这个过程称为分片(Sharding)。这一步将数据分解为可管理的块，这些块可以分布在多个节点上。具体的分片方法取决于数据类型和进行分片的应用程序，对关系数据库进行分片，与 NoSQL 数据库或文件共享上的文件是不同的。

(b) 加密每个分片。分片之后，存储系统需要加密本地系统上的每个数据分片。内容所有者可以完全控制此过程。目标是确保内容所有者以外的任何人都无法查看/访问分片中的数据，无论数据位于何处、该数据是静态还是动态。

(c) 为每个分片生成哈希(Hash)。区块链存储系统根据分片的数据或加密密钥生成唯一的哈希——即固定长度的加密输出字符串。哈希将添加到分类账和分片元数据，以便将事务链接到存储的分片。生成哈希的确切方法因系统而异。

(d) 复制每个分片。存储系统会复制每个分片，因此有足够的冗余副本，可确保可用性和性能，并防止性能下降和数据丢失。由内容



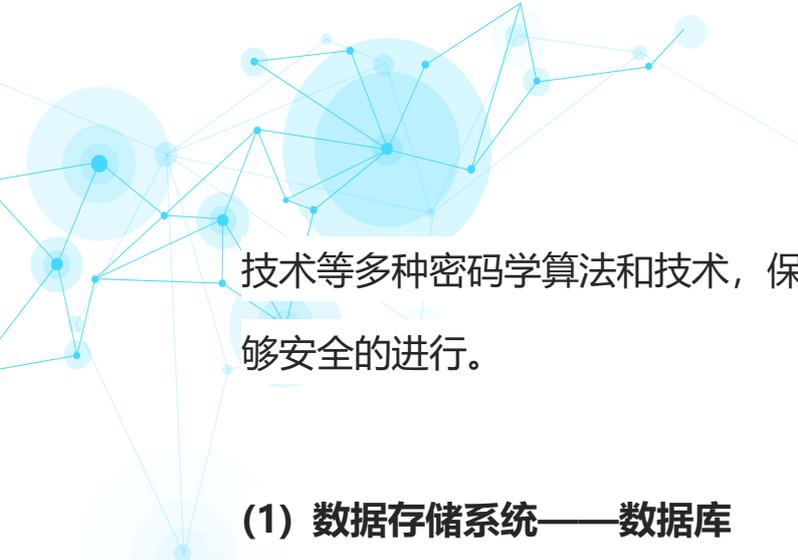
所有者来决定每个分片的副本数量以及这些分片所在的位置。此过程中，内容所有者应该为需要维护的最小副本数建立阈值，以确保不会丢失数据。

(e) 分发复制的分片。P2P 网络将复制的分片分发到地理上分散的存储节点，无论是区域还是全局。多个组织或个人(有时也称作 farmer)拥有存储节点，通过租用额外的存储空间可换取某种类型的补偿，通常是加密货币。没有一个实体能够拥有所有存储资源，或者控制存储基础架构。只有内容所有者才能完全访问其所有数据，无论这些节点位于何处。

(f) 将交易记录到分类账。存储系统记录区块链分类账中的所有事务，并在所有节点之间同步该信息。分类账存储与事务相关的详细信息，例如分片位置，分片哈希和租赁成本等等。由于分类账基于区块链技术，因此它具有透明性、可验证性、可追溯性以及防篡改性。

## 2.2.2 区块链存储技术分析

数据层是最底层的技术，主要实现了两个功能：数据存储、账户和交易的实现与安全。数据存储主要基于 Merkle 树，通过区块的方式和链式结构实现，大多以 KV 数据库的方式实现持久化。账户和交易的实现与安全这个功能基于数字签名、哈希函数和非对称加密



技术等多种密码学算法和技术，保证了交易在去中心化的情况下能够安全的进行。

### **(1) 数据存储系统——数据库**

数据层的一大功能是存储，存储系统的选择原则是性能和易用性。一个网络系统的整体性能，主要取决于网络或本地数据存储系统的 I/O 性能。

### **(2) 区块数据 (Block)**

区块数据主要是保存交易数据，不同的系统采用的结构不同。区块链的数据结构成员分散存储在底层数据库，最终存储形式是[k,v]键值对，使用的[k,v]型底层数据库是 LevelDB；与交易操作相关的数据，其呈现的集合形式是 Block；如果以 Block 为单位链接起来，则构成更大粒度的 Blockchain.

### **(3) 链式结构 (chain)**

从上面的区块结构中可以看到，每一个区块都保存了上一个区块的 hash 值，这样就将这些区块连接起来。



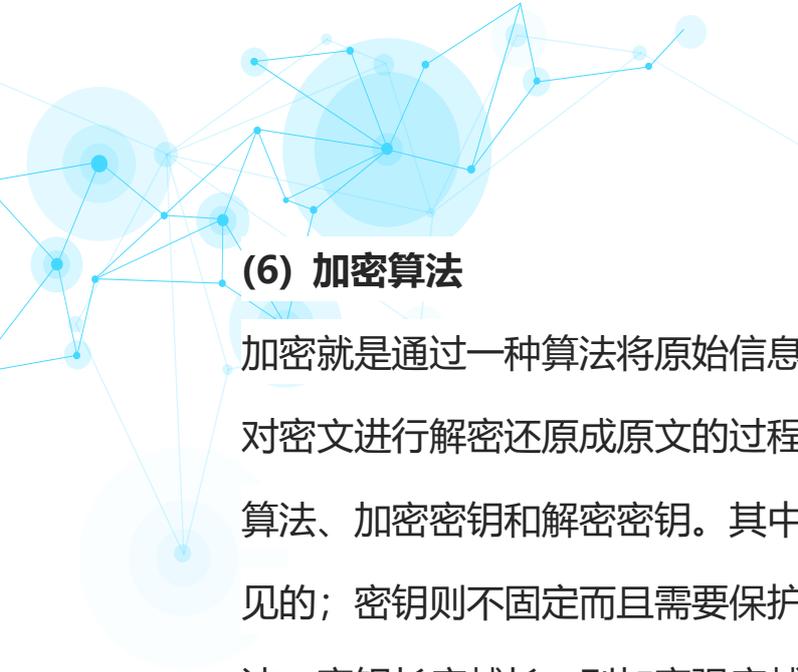
#### (4) Merkle 树

默克尔树 (Merkle tree, MT) 是一种哈希二叉树, 1979 年由 Ralph Merkle 发明。在计算机科学中, 二叉树是每个节点最多有两个子树的树结构, 每个节点代表一条结构化数据。通常子树被称作“左子树” (left subtree) 和“右子树” (right subtree)。二叉树常被用于实现数据快速查询。

#### (5) 哈希函数

Hash, 一般翻译为“散列”, 也有直接音译为“哈希”的, 就是把任意长度的输入 (又叫做预映射 pre-image) 通过散列算法变换成固定长度的输出, 该输出就是散列值。这种转换是一种压缩映射, 也就是, 散列值的空间通常远小于输入的空间, 不同的输入可能会散列成相同的输出, 所以不可能从散列值来确定唯一的输入值。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

哈希能够实现数据从一个维度向另一个维度的映射, 通常使用哈希函数实现这种映射。通常业界使用  $y = \text{hash}(x)$  的方式进行表示, 该哈希函数实现对  $x$  进行运算计算出一个哈希值  $y$ 。



## (6) 加密算法

加密就是通过一种算法将原始信息进行转换，接收者能够通过密钥对密文进行解密还原成原文的过程。加密算法的典型组件有加解密算法、加密密钥和解密密钥。其中加解密算法是固定不变和公开可见的；密钥则不固定而且需要保护起来，一般来说，对同一种算法，密钥长度越长，则加密强度越大。

## (7) 数字签名

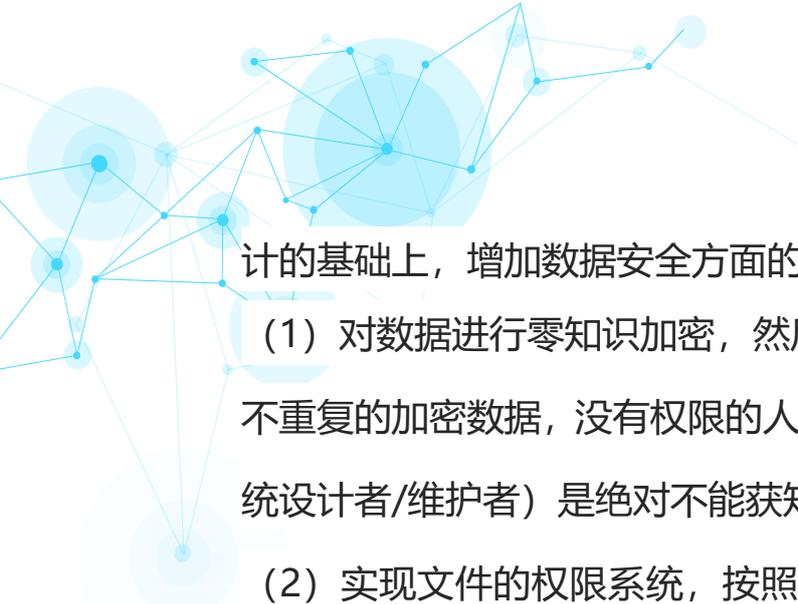
数字签名又称之为公钥数字签名，是一种类似于写在纸上的物理签名。数字签名主要用于数据更改的签名者身份识别以及抗抵赖。数字签名包含三个重要特性：

- 只有自己可以签署自己的数字签名，但是他人可以验证签名是否是你签发；
- 数字签名需要和具体的数字文档绑定，就好比现实中你的签名应该和纸质媒介绑定；
- 数字签名不可伪造。

## 2.3 YottaChain 核心技术阐述

### 2.3.1 TruPrivacy 技术分析

YottaChain 独家拥有 TruPrivacy 技术,将在继承 IPFS 现有存储设



计的基础上，增加数据安全方面的机制，主要体现在三个方面：

(1) 对数据进行零知识加密，然后做数据去重，使得最终存储的是不重复的加密数据，没有权限的人（包括所在存储节点的拥有者、系统设计者/维护者）是绝对不能获知数据内容的；

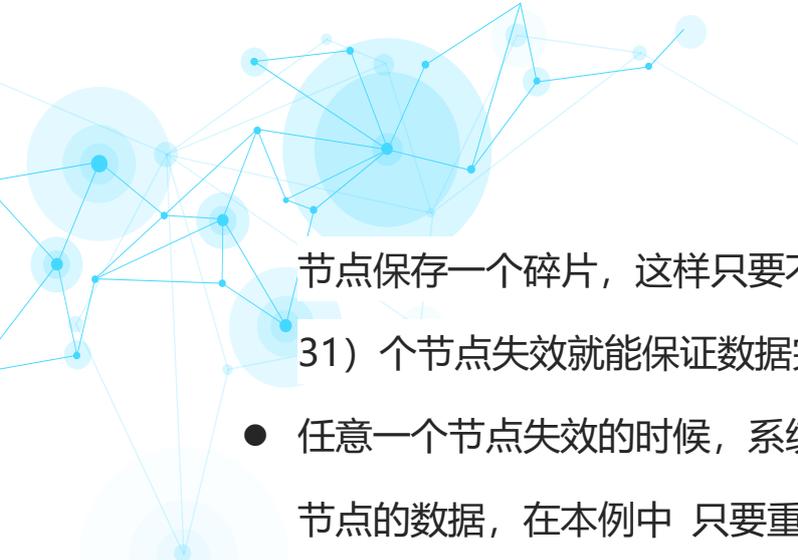
(2) 实现文件的权限系统，按照文件的 Owner、所在 Group 和 Everyone 三个维度定义文件的访问权限；

(3) 在数据级实现文件的授权机制，使得文件只能被授权人打开，不管各个节点如何作恶（包括恶意修改代码）都无法突破授权机制。这种机制的可靠性和区块链一样，是用密码学为基础的数学公式来保障的。

采用后，在保障数据安全的前提下可以实现数据去重，YottaChain 相当于成为一个“空间魔方”，即矿工投入 1GB 的空间，YottaChain 可以产生 5-10GB 的存储容量，这样就产生了资源供应者获得的通证的购买力超过其供应的资源的奇迹效应。

### 2.3.2 持久化存储服务技术分析

- YottaChain 的持久化存储服务统一采用冗余编码，任何数据自动编码成分成  $N$ （例如 100，具体数字将来由社区治理委员会确定）个碎片，其中只要有任意  $M$ （例如 70）个碎片即可恢复出数据，然后将这  $N$  个碎片分别存储到  $N$  个存储节点中，每个



节点保存一个碎片，这样只要同时有  $N-M+1$ （本例中为 31）个节点失效就能保证数据完整不丢失

- 任意一个节点失效的时候，系统将会立即另选其它节点重建失效节点的数据，在本例中 只要重建第一个失效节点完成之前不会有另外 30 个节点也相继失效，就可以保证数据永远不丢
- 各节点之间会互相监控、互相校验，任何节点一旦失效都能被快速发现
- 重建一个失效节点的数据时，会分成很多个节点同时重建以加快重建速度。例如失效节点上存储了 1 万个文件的各一个碎片，重建一个碎片平均需要 0.5 秒钟时间（主要是网络传输花时间），选 100 个节点参与重建，每个节点只需要重建 100 个碎片，平均 50 秒钟完成全部重建工作。只要 50 秒钟内不会有同一个文件的另外 30 个节点同时失效，该文件数据就不会丢
- 由于冗余性好且地理位置分散，不用担心因为硬盘损坏、个别节点运维失误（2018 年 8 月曝光腾讯云因为运维失误丢失用户数据）、雷电天气（2018 年 9 月，Microsoft 因为雷击导致部分地区的 Azure 服务停机 20 多小时）、停电、光纤被挖断、地震火灾等原因而数据失效
- 由于节点分散而且冗余性好，不怕 DDOS 攻击



## 2.4 YET 云存储生态技术阐述

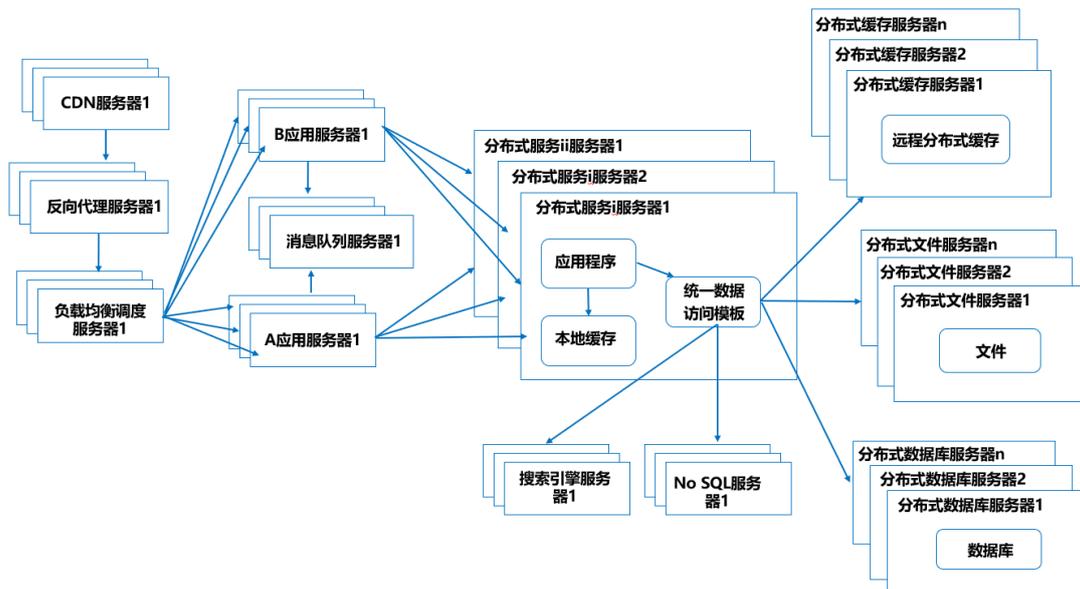
YET 云存储生态将继承区块链存储技术和 YottaChain 现有的存储设计优势。建立在于 YottaChain 前沿技术的基础上，可链接绝大部分分布式云存储系统。

YET 云存储生态将使得拥有存储资源的人与其用来存自己数据，不如用 YET 挖矿，用挖矿所得的通证再来买存储空间存数据，不仅可以存更多的数据还能富余一些通证。这种机制可以激励更多的人来参与挖矿，贡献自己的存储资源。

## 三、网络架构设计

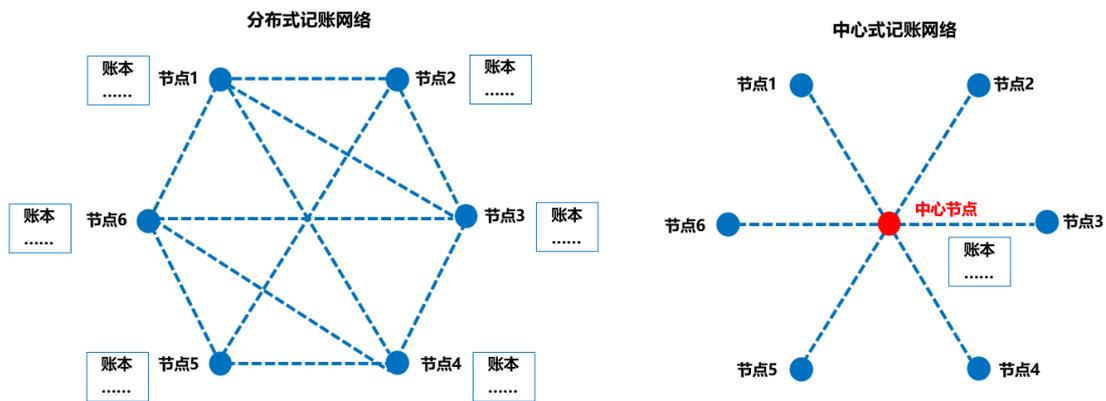
### 3.1 分布式存储架构

分布式存储架构由三个部分组成：客户端、元数据服务器和数据服务器。客户端负责发送读写请求，缓存文件元数据和文件数据。元数据服务器负责管理元数据和处理客户端的请求，是整个系统的核心组件。数据服务器负责存放文件数据，保证数据的可用性和完整性。该架构的好处是性能和容量能够同时拓展，系统规模具有很强的伸缩性。



尽人皆知，比特币区块链是区块链技术的 1.0，尽管比特币区块链基本上是账户和余额的分散数据库，但由于容量问题，将这些信息保存到分散的分类账中已经是一个挑战。每当我们聊及分散账本技术 (DLT) 和数据存储之间的互惠关系是，区块链最常使用的就是激

励机制，这意味着数据不会存储在区块链本身，但手边的网络能够利用区块链作为自动支付和价值交换的分类账本，并且可以收取用户在访问或存储文件时产生的费用。区块链没有被用于数据存储，它为构建分散网络提供了基础，无中央管理机构，因此有了更快的结算时间，更低的交易费用，更高的隐私性，保持透明度和不变记录的能力。



## 3.2 YET 生态系统结构

YET 云存储生态系统架构主要包含三层，分别为应用层、YET 公链和底层技术。



## 四、应用场景

### 4.1 区块链存储应用场景

- ✓ **场景一：内容创作**  
区块链是信用制造机器，保护和鼓励创作内容版权
- ✓ **场景二：网络视频平台**  
大幅度降低存储和带宽成本
- ✓ **场景三：互联网信息安全**  
提升用户互联网信息隐私的存储安全性
- ✓ **场景四：数据存储**  
让数据的存储更安全更快速且能永久保存



#### (1) 场景一：内容创作

区块链是信用制造机器，保护和鼓励创作内容版权。

AKASHA 是一个基于以太坊和星际文件系统（IPFS）的去中心化社交网络，是以太坊创始人 Vitalik Buterin (V 神) 和 IPFS 创始人 Juan Benet 共同担任顾问的一个项目。以太坊提供了身份系统、微支付等支持，IPFS（星际文件系统）提供了内容存储、分发等支持，这些构建了一个去中心化的社交网络。

用户在这个网络创作的内容通过 IPFS 网络进行发布，同时绑定了以



以太坊的钱包，用户可以对优质内容进行 ETH 的打赏，内容收益直接归创作者所有，没有中间商。作为一个去中心化的应用程序，AKASHA 部署了由以太坊和 IPFS 融合而诞生的下一代信息架构。

## **(2) 场景二：网络视频平台**

大幅度降低存储和带宽成本。

作为去中心化 YouTube 的实现基础，DTube 以 STEEM 区块链为核心构建而成。与现有主流视频共享网站类似，DTube 属于一款浏览器内应用程序，允许内容创作者通过上传素材获得收益。

传统在线视频网站采用的是中心化存储服务，这需要高额的储存费用和带宽费用，当然这些费用最终都转化为观看长时间的广告和非会员限制等转移到用户的身上。而 DTube 使用了 IPFS 作为主要的存储方式，大大降低了相同资源的冗余，同时节约了大量用户播放视频时产生的带宽成本。

## **(3) 场景三：互联网信息安全**

提升用户互联网信息隐私的存储安全性。

最近这几年，国际社会也发生过多次因黑客入侵而导致的大规模用户



信息泄露的事件，都对用户造成了很大的损失或影响，如当年的苹果 iCloud 和今年的 Facebook 数据泄漏事件。

而 IPFS 采用的是区块链的技术，去中心化概念天生就拥有抵抗攻击的能力，所有的数据访问都分布在不同的节点，想要入侵就要攻击所有的节点，这有效的保证了数据的安全，保护了用户的隐私。

#### **(4) 场景四：数据存储**

让数据的存储更安全更快速且能永久保存。

古亚历山大图书馆——古老的知识生活的中心，在一场大火中被摧毁了。据说，大量的书籍和卷轴在一场战争中不幸遗失，这一事件使得人类知识的进步倒退了几个世纪。自古人类一直都在探寻能更有效更长久的保存信息数据的介质。

IPFS 分布式存储为此而生，没有了中心化的数据管理，数据的安全性将更高，很难被窥探或者复制。全网分布式的数据存储，降低了因为自然灾害、战争、黑客攻击等原因造成的数据遗失或损坏，让珍贵的有价值的数据和资料得以永久保存。

## 4.2 YET 云存储生态应用场景

### 4.2.1 YET 云存储生态应用场景



#### (1) 兼容 IPFS 所有应用场景

YET 云存储生态本身就采用 IPFS 作为去中心化静态持久化存储模块的一部分，可以兼容 IPFS 的所有应用场景，包括静态网页、CDN 等。

#### (2) 为个人和企业数据提供安全、低成本存储

YET 云存储生态提供完善的数据安全机制，保证不管数据保存在多么不可信任的节点上，都不用担心数据被泄露，在任何情况下都只有数据的拥有者或其授权者能看到数据，对任何其他人来说都只是乱码，而且不存在被攻破的风险，从实践意义上来说可以视为绝对安全的。



### **(3) 充分利用闲置资源，打造真正的共享经济**

YET 云存储生态利用独有的区块链激励模型能调动存储空间和计算能力的所有者将暂时闲置的资源贡献出来挖矿，为他人所用，充分共享社会资源，从而落地实现一个规模庞大的共享经济系统。

### **(4) 将自用存储空间用来挖矿**

对 YET 云存储生态来说，除了将闲置资源用来挖矿外，正在使用和即将使用的存储资源也是可以用来挖矿换取奖励的，并且可以做到数据存储和挖矿换取奖励的两不误。

### **(5) 作为其他区块链项目的基础架构**

作为一条基础公链，YET 云存储生态将为其它区块链项目提供坚实、安全可靠、低成本的基础架构支撑。

### **(6) 作为低成本对象存储**

YET 云存储生态将提供 S3 兼容的对象存储服务，而且存储成本更低，这样 AWS/S3 或其它云平台对象存储的用户无需修改代码即可马上降低每月的费用。

### **(7) 作为具备容灾能力的持久化存储**



YET 云存储生态的去中心化存储是天然具备异地容灾能力的, YET 云存储生态将提供标准块存储接口和 NAS 存储接口, 可以作为常规企业级存储的低成本方案, 而且自动具备容灾能力。

将来, 所有的中心化存储 (包括 AWS、阿里云、EMC、华为) 都不会被视为持久化存储, 而只能被作为本地缓存使用。只有去中心化存储才能作为持久化存储使用。



## 五、通证 YET 设计

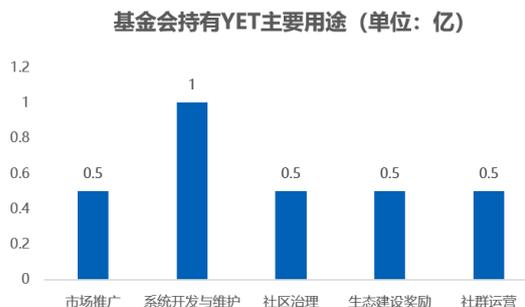
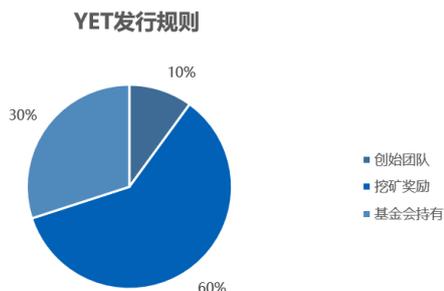
### 5.1 YET 发行规则

YET (全称 Yotta Ecological System) 是 YET 云存储生态中对参与者的贡献量通证，是生态圈的价值核心，其价值来源于生态成员的价值贡献。区块链中的矿工可以通过为客户提供存储来获取 YET。相应地，客户可以通过花费 YET 来雇佣矿工来存储或分发数据。和比特币一样，矿工们为了巨大的奖励而竞争式挖区块。

总发行量 10 亿，永不增发；

- (1) 创始团队持有 10%，总量 1 亿；
- (2) 挖矿奖励持有 60%，总量 6 亿；
- (3) 基金会持有 30%，总量 3 亿，主要用途包含如下部分：
  - 市场推广：0.5 亿（用于项目的整体市场活动、品牌宣发、市场合作等）
  - 系统开发与维护：1 亿（用于项目的 APP 研发、技术升级等）
  - 社区治理：0.5 亿（用于项目启动后针对社区拓展、管理等社区化工作的补贴）
  - 生态建设奖励：0.5 亿（用于应对早期矿工由于通证价格增长所带来的销售行为，所导致的二级市场供应不足的情况）

- 社群运营：0.5 亿（用于早期参与项目投资的相关机构的  
通证兑换）；



## 5.2 YET 解锁规则

### (1) 创始团队

- 通证上线交易所整一年开始解锁释放，随用户挖矿产出数量，同比例进行解锁；
- 过往一年应释放的部分，按照上所一年整解锁过往一年应释放部分的 20%，剩余部分每个月解锁三十六分之一；
- 创始团队在一整年解锁期后，每个月释放部分，继续与挖矿奖励释放数量同比例释放，
- 释放部分也按照每个月三十六分之一解锁。

例如：用户在上锁满一整年的时候，挖矿释放通证为挖矿奖励通证总量 8 亿的 10%，则释放创始团队 4 亿总体的 10% 4000 万，先



期解锁释放总量的 20% 800 万，剩余部分按照每个月三十六分之一解锁。

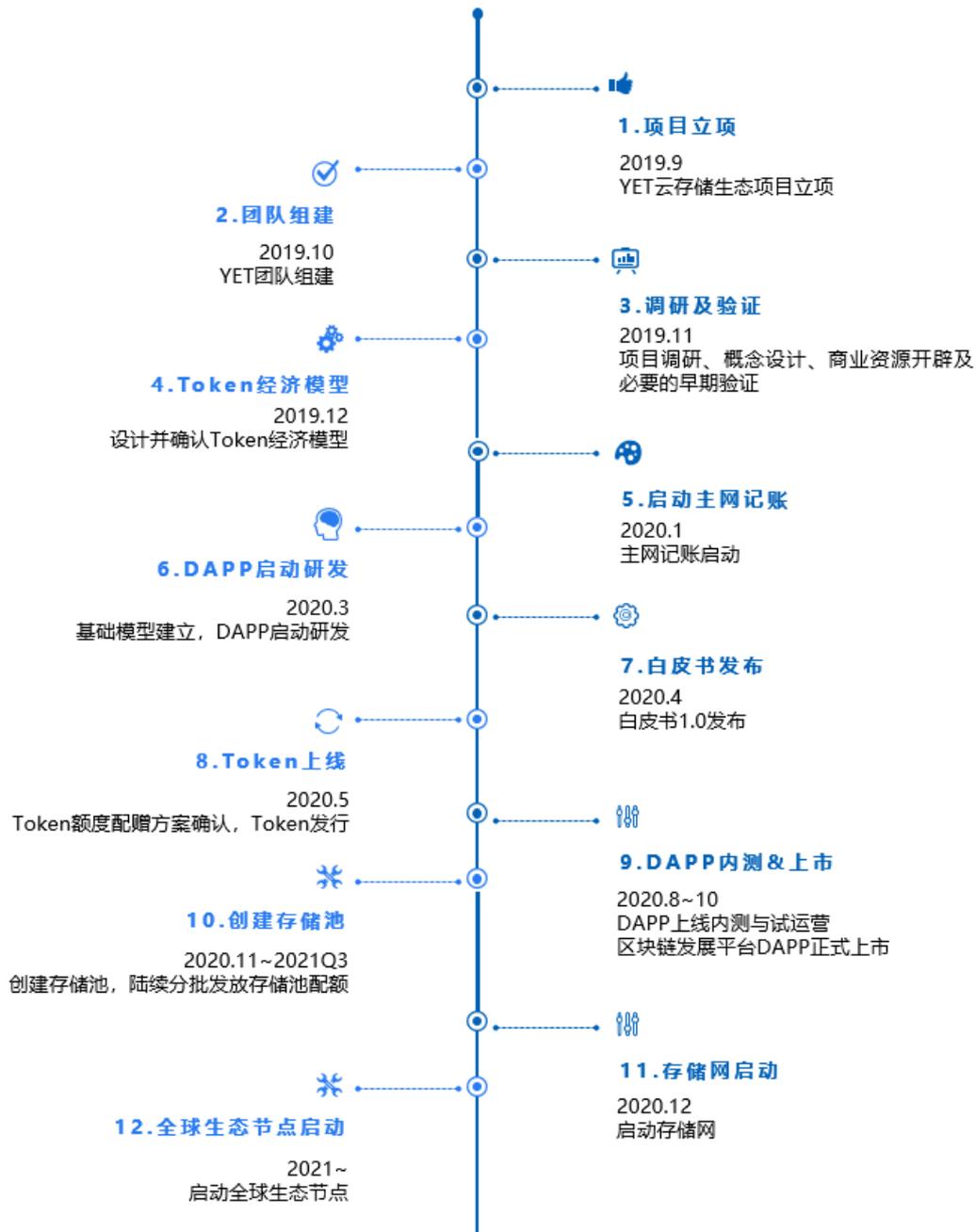
## (2) 挖矿奖励

- 用于用户购买存储空间使用权用户之挖矿奖励，不锁仓；
- 释放规则：按照用户实际挖矿数量进行行行释放；

## (3) 基金会持有：不锁仓

## 六、项目发展规划图

YET云存储生态项目发展规划图





## 七、风险警示

### 7.1 免责声明

本白皮书所使用的所有文本资料、图片、标志、技术分析、时间预估、链接和参考文献等（以下简称“资料”），仅供参考，本白皮书将会随时修改资料。虽然本白皮书已经尽力确保资料的准确性，但本白皮书不包含任何明示或暗示去保证这些资料均准确无误。本白皮书不会对任何错误或遗漏承担责任。

本白皮书不会对使用或任何由于使用本白皮书而造成的损失（包括但不限于资料失实、理解错误、产权使用等）承担任何责任。本白皮书可能会设计其他项目所提供的信息，但这些信息并不受本白皮书的约束。本白皮书不会对这些信息所带来的效果做出任何保证或承担任何责任。所有使用本白皮书提供信息的人，将要自行承担后果。

### 7.2 性质说明

本白皮书不是任何性质、任何形式的要约文件或招股书。本白皮书

(a) 不涉及任何形式的证券内容，(b) 不涉及任何意义和种类上的货币，(c) 不涉及任何股票、股权及债权，(d) 不涉及任何基金



相关内容。所有适用或涉及上述 a~d 的任何法律法规将不适合于本白皮书和 YET 的发行运作。本白皮书不是任何形式的招股说明书或要约文件，也不构成对任何司法管辖区证券投资的报价或试图招揽投资。本白皮书和 YET 尚未获得任何管辖机构的任何监管机构的批准。不应认为本白皮书和 YET 云存储生态产品符合任何司法管辖区的任何法律，法规或立法。

### 7.3 风险提示

本白皮书不形成任何形式的投资建议，不对 YET 的潜在持有者的决策进行任何干扰。对任何人的收益不做任何保证。

YET 是一种长期投资工具，其主要功能是，给予通证持有者参与项目的权利。YET 不同于银行储蓄和债券等能够提供固定收益预期的金融工具，持有通证，既可能分享投资所产生的收益，也可能承担基金投资所带来的损失。

通证在投资运作过程中可能面临各种风险，既包括市场风险，也包括项目自身的管理风险、技术风险和合规风险等。通证市场行情不可能只涨不跌，有投资收益的同时必然伴随着投资风险，您应当在操作前对自身的经济承受能力和心理承受能力做出客观判断，对于自己投资的资金金额做出谨慎决定，对于任何因阅读本白皮书产生



的损失，本白皮书不承担任何责任。

通证市场是一个风险无时不在的市场。您在进行通证投资时存在盈利的可能，也存在亏损的风险。本白皮书并不可能揭示从事通证投资的全部风险及市场的全部情形。您务必对此有清醒的认识，认真考虑是否对 YET 云存储生态项目进行投资。

## 7.4 责任限制

在任何情况下，本白皮书及 YET 云存储生态团队及合作方不须就任何人士由于直接或间接使用本白皮书，并参考本白皮书的所有内容或任何产品、资讯或服务，而导致的任何损失或伤害负上任何责任（包括并不限于基于智能合约、侵权行为（包括疏忽）或其他形式）。在符合或不符合本白皮书的一般性原则及任何情况下，本白皮书及 YET 团队及合作方并不需要对任何阅读或使用本白皮书的任何附带引起、特殊或相应而生的任何种类的损失作出赔偿，包括并不限于利润损失、营业受限、资料损失或其他法律经济损失、人身伤害等。

## 7.5 更新说明

在给予或不给予事先通知的情况下，本白皮书保留随时更新的权利



利。任何更改在项目官方网站发布时，立即生效。请各位在关注项目的同时，务必查看本免责声明。若投资人决定参与 YET 云存储生态项目，则视为阅读并认可本白皮书的所有内容。