区块链技术与原理

一、区块链的工作原理(上) 区块链体系结构

区块链是一种分布式账本技术，依靠智能合约等逻辑控制功能演变为完整的存储系统。其分类方式、服务模式和应用需求的变化导致核心技术形态的多样性发展。为了完整地认知区块链生态系统，设计了一个层次化的区块链技术体系结构，进一步深入剖析区块链每层结构的基本原理。

区块链概念

2008 年，中本聪提出了去中心化加密货币——比特币（bitcoin）的设计构想。2009 年，比特币系统开始运行，标志着比特币的正式诞生。2010—2015 年，比特币逐渐进入大众视野。2016—2018 年，随着各国陆续对比特币进行公开表态以及世界主流经济的不确定性增强，比特币的受关注程度激增，需求量迅速扩大。事实上，比特币是区块链技术最成功的应用场景之一。伴随着以太坊（ethereum）等开源区块链平台的诞生以及大量去中心化应用（DApp,decentralized application）的落地，区块链技术在更多的行业中得到了应用。

由于具备过程可信和去中心化两大特点，区块链能够在多利益主体参与的场景下以低成本的方式构建信任基础，旨在重塑社会信用体系。近两年来区块链发展迅速，人们开始尝试将其应用于金融、教育、医疗、物流等领域。但是，资源浪费、运行低效等问题制约着区块链的发展，这些因素造成区块链分类方式、服务模式和应用需求发生快速变化，进一步导致核心技术朝多样化方向发展，因此有必要采取通用的结构分析区块链项目的技术路线和特点，以梳理和明确区块链的研究方向。

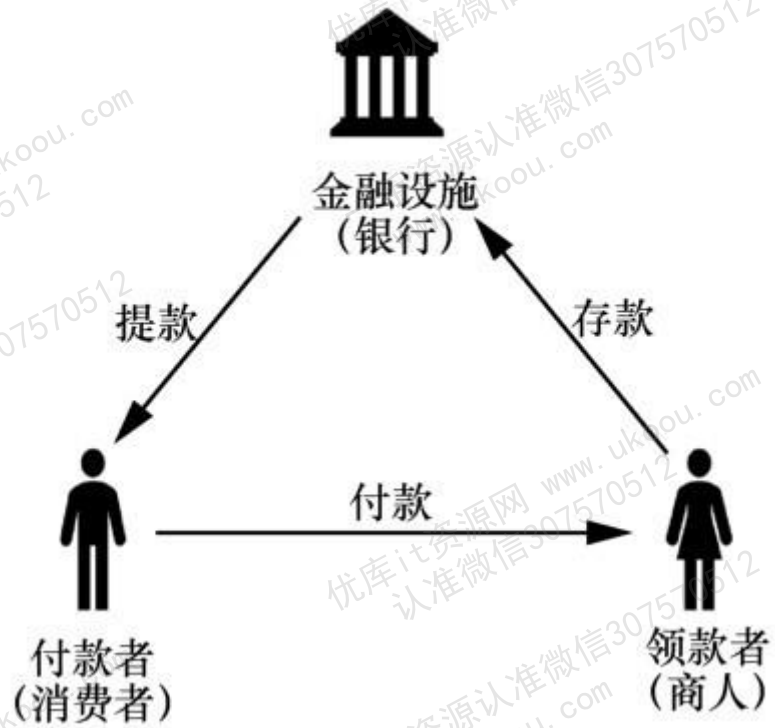
中心化与去中心化

随着区块链技术的深入研究，不断衍生出了很多相关的术语，例如“中心化”“去中心化”“公链”“联盟链”等。为了全面地了解区块链技术，并对区块链技术涉及的关键术语有系统的认知，我们将给出区块链及其相关概念的定义，以及它们的联系，更好地区分易使人混淆的术语。

加密货币

加密货币（cryptocurrency）是一类数字货币（digital currency）技术，它利用多种密码学方法处理货币数据，保证用户的匿名性、价值的有效性；利用可信设施发放和核对货币数据，保证货币数量的可控性、资产记录的可审核性，从而使货币数据成为具备流通属性的价值交换媒介，同时保护使用者的隐私。

加密货币的概念起源于一种基于盲签名（blind signature）的匿名交易技术，最早的加密货币交易模型“electronic cash”。



最早的加密货币构想将银行作为构建信任的基础，呈现中心化特点。此后，加密货币朝着去中心化方向发展，并试图用工作量证明（PoW,poof of work）或其改进方法定义价值。比特币在此基础上，采用新型分布式账本技术保证被所有节点维护的数据不可篡改，从而成功构建信任基础，成为真正意义上的去中心化加密货币。区块链从去中心化加密货币发展而来，随着区块链的进一步发展，去中心化加密货币已经成为区块链的主要应用之一。

区块链及工作流程

一般认为，区块链是一种融合多种现有技术的新型分布式计算和存储范式。它利用分布式共识算法生成和更新数据，并利用对等网络进行节点间的数据传输，结合密码学原理和时间戳等技术的分布式账本保证存储数据的不可篡改，利用自动化脚本代码或智能合约实现上层应用逻辑。如果说传统数据库实现数据的单方维护，那么区块链则实现多方维护相同数据，保证数据的安全性和业务的公平性。区块链的工作流程主要包含生成区块、共识验证、账本维护 3 个步骤。

1. 生成区块。区块链节点收集广播在网络中的交易——需要记录的数据条目，然后将这些交易打包成区块——具有特定结构的数据集。

2. 共识验证。节点将区块广播至网络中，全网节点接收大量区块后进行顺序的共识和内容的验证，形成账本——具有特定结构的区块集。

3. 账本维护。节点长期存储验证通过的账本数据并提供回溯检验等功能，为上层应用提供账本访问接口。

区块链类型

根据不同场景下的信任构建方式，可将区块链分为 2 类：非许可链（permissionless blockchain）和许可链（permissioned blockchain）。

区块链体系结构

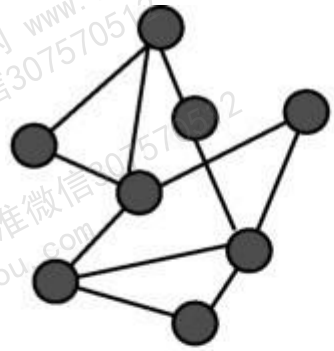
现有项目的技术选型多数由比特币演变而来，所以区块链主要基于对等网络通信，拥有新型的基础数据结构，通过全网节点共识实现公共账本数据的统一。但是区块链也存在效率低、功耗大和可扩展性差等问题，因此人们进一步以共识算法、处理模型、交易模式创新为切入点进行技术方案改进，并在此基础上丰富了逻辑控制功能和区块链应用功能，使其成为一种新型计算模式

网络层

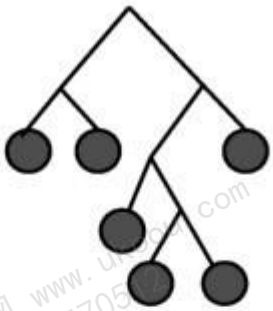
网络层关注区块链网络的基础通信方式——对等（P2P,peer-to-peer）网络。对等网络是区别于“客户端/服务器”服务模式的计算机通信与存储架构，网络中每个节点既是数据的提供者也是数据的使用者，节点间通过直接交换实现计算机资源与信息的共享，因此每个节点地位均等。

1. 组网结构

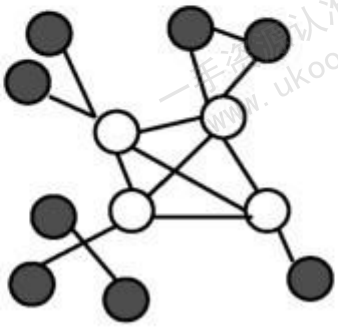
对等网络的体系架构可分为无结构对等网络、结构化对等网络和混合式对等网络，根据节点的逻辑拓扑关系，区块链网络的组网结构也可以划分为上述 3 种.



(a) 无结构对等网络



(b) 结构化对等网络
(以Kademlia为例)

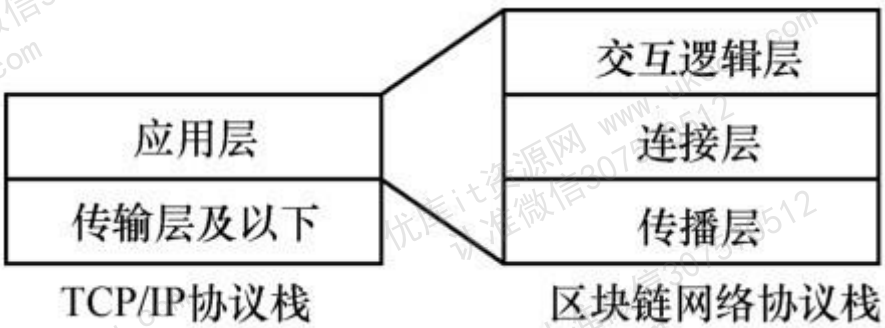


对等节点
特殊中继

(c) 混合式对等网络

2. 通信机制

通信机制是指区块链网络中各节点间的对等通信协议，建立在 TCP/UDP 之上，位于计算机网络协议栈的应用层。该机制承载对等网络的具体交互逻辑，例如节点握手、心跳检测、交易和区块传播等。由于包含的协议功能不同（例如基础链接与扩展交互），我们将通信机制细分为 3 个层次：传播层、连接层和交互逻辑层。



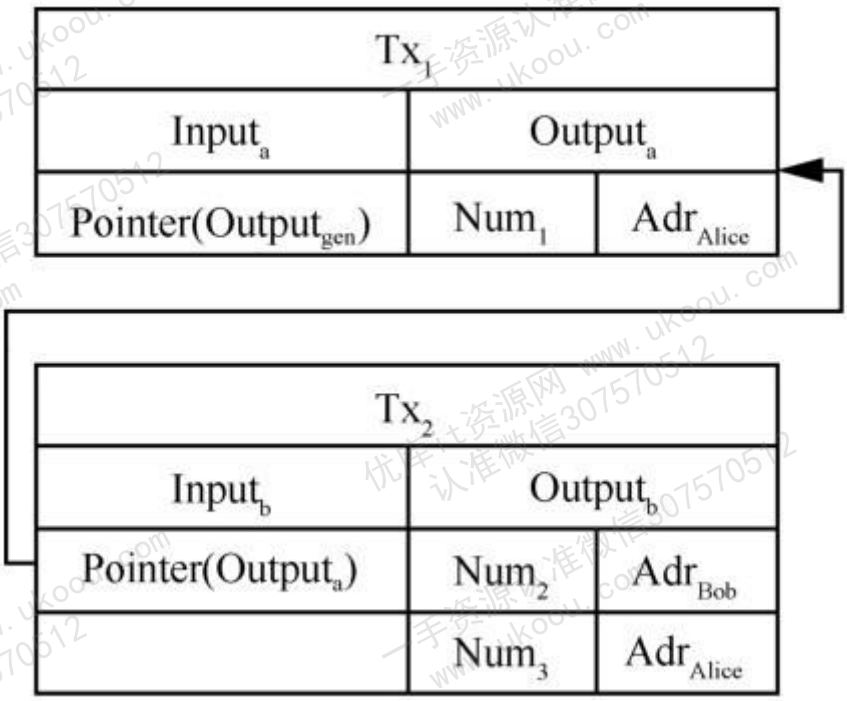
3. 安全机制

安全是每个系统必须具备的要素，以比特币为代表的非许可链利用其数据层和共识层的机制，依靠消耗算力的方式保证数据的一致性和有效性，没有考虑数据传输过程的安全性，反而将其建立在不可信的透明 P2P 网络上。

数据层

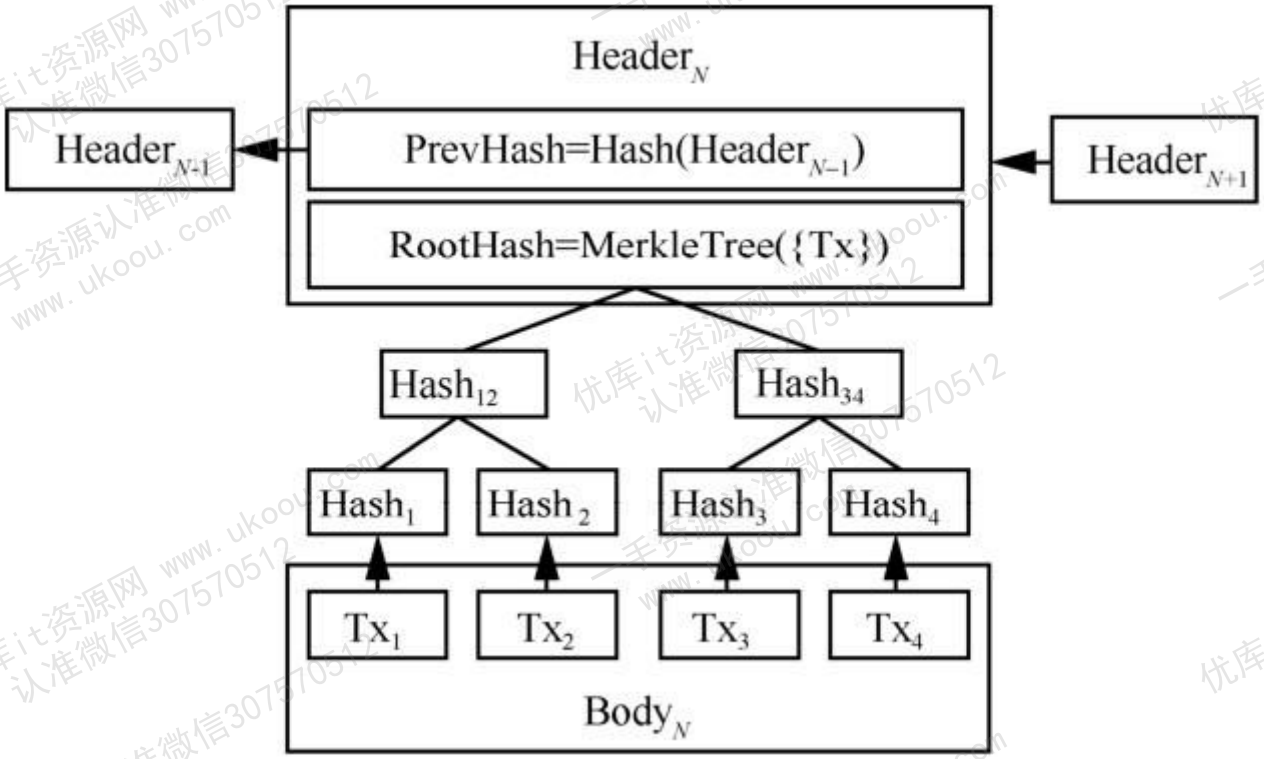
1. 信息模型

区块链承载了不同应用的数据（例如支付记录、审计数据、供应链信息等），而信息模型则是指节点记录应用信息的逻辑结构，主要包括 UTXO （unspent transaction output）、基于账户和键值对模型 3 种。需要说明的是，在大部分区块链网络中，每个用户均被分配了交易地址，该地址由一对公私钥生成，使用地址标识用户并通过数字签名的方式检验交易的有效性。



2. 关联验证结构

区块链之所以具备防篡改特性，得益于链状数据结构的强关联性。该结构确定了数据之间的绑定关系，当某个数据被篡改时，该关系将会遭到破坏。由于伪造这种关系的代价是极高的，相反检验该关系的工作量很小，因此篡改成功率被降至极低。链状结构的基本数据单位是“区块（block）”。



3. 加密机制

由上述加密货币原理可知，经比特币演变的区块链技术具备与生俱来的匿名性，通过非对称加密等技术既保证了用户的隐私又检验了用户身份。非对称加密技术是指加密者和解密者利用 2 个不同秘钥完成加解密，且秘钥之间不能相互推导的加密机制。常用的非对称加密算法包括 RSA、Elgamal、背包算法、Rabin、D-H、ECC（椭圆曲线加密算法）等。Alice 向 Bob 发起交易 Tx2，Alice 使用 Bob 的公钥对交易签名，仅当 Bob 使用私钥验证该数字签名时，才有权利创建另一笔交易，使自身拥有的币生效。该机制将公钥作为基础标识用户，使用户身份不可读，一定程度上保护了隐私。

共识层

区块链网络中每个节点必须维护完全相同的账本数据，然而各节点产生数据的时间不同、获取数据的来源未知，存在节点故意广播错误数据的可能性，这将导致女巫攻击、双花攻击等安全风险；除此之外，节点故障、网络拥塞带来的数据异常也无法预测。因此，如何在不可信的环境下实现账本数据的全网统一是共识层解决的关键问题。实际上，上述错误是拜占庭将军问题（the Byzantine generals problem）在区块链中的具体表现，即拜占庭错误——相互独立的组件可以做出任意或恶意的行为，并可能与其他错误组件产生协作，此类错误在可信分布式计算领域被广泛研究。

1. PoX 类协议
2. BFT 类协议
3. CFT 类协议

4. 奖惩机制

控制层

区块链节点基于对等通信网络与基础数据结构进行区块交互，通过共识协议实现数据一致，从而形成了全网统一的账本。控制层是各类应用与账本产生交互的中枢，如果将账本比作数据库，那么控制层提供了数据库模型，以及相应封装、操作的方法。具体而言，控制层由处理模型、控制合约和执行环境组成。处理模型从区块链系统的角度分析和描述业务/交易处理方式的差异。控制合约将业务逻辑转化为交易、区块、账本的具体操作。执行环境为节点封装通用的运行资源，使区块链具备稳定的可移植性。

1. 处理模型

账本用于存储全部或部分业务数据，那么依据该数据的分布特征可将处理模型分为链上（on-chain）和链下（off-chain）2 种。

链上模型是指业务数据完全存储在账本中，业务逻辑通过账本的直接存取实现数据交互。该模型的信任基础建立在强关联性的账本结构中，不仅实现防篡改而且简化了上层控制逻辑，但是过量的资源消耗与庞大的数据增长使系统的可扩展性达到瓶颈，因此该模型适用于数据量小、安全性强、去中心化和透明程度高的业务。

链下模型是指业务数据部分或完全存储在账本之外，只在账本中存储指针以及其他证明业务数据存在性、真实性和有效性的数据。该模型以“最小化信任成本”为准则，将信任基础建立在账本与链下数据的证明机制中，降低账本构建成本。由于与公开的账本解耦，该模型具有良好的隐私性和可拓展性，适用于去中心化程度低、隐私性强、吞吐量大的业务。

2. 控制合约

区块链中控制合约经历了 2 个发展阶段，首先是以比特币为代表的非图灵完备的自动化脚本，用于锁定和解锁基于 UTXO 信息模型的交易，与强关联账本共同克服了双花等问题，使交易数据具备流通价值。其次是以以太坊为代表的图灵完备的智能合约，智能合约是一种基于账本数据自动执行的数字化合同，由开发者根据需求预先定义，是上层应用将业务逻辑编译为节点和账本操作集合的关键。智能合约通过允许相互不信任的参与者在没有可信第三方的情况下就复杂合同的执行结果达成协议，使合约具备可编程性，实现业务逻辑的灵活定义并扩展区块链的使用。

3. 执行环境

执行环境是指执行控制合约所需要的条件，主要分为原生环境和沙盒环境。原生环境是指合约与节点系统紧耦合，经过源码编译后直接执行，该方式下合约能经历完善的静态分析，提高安全性。沙盒环

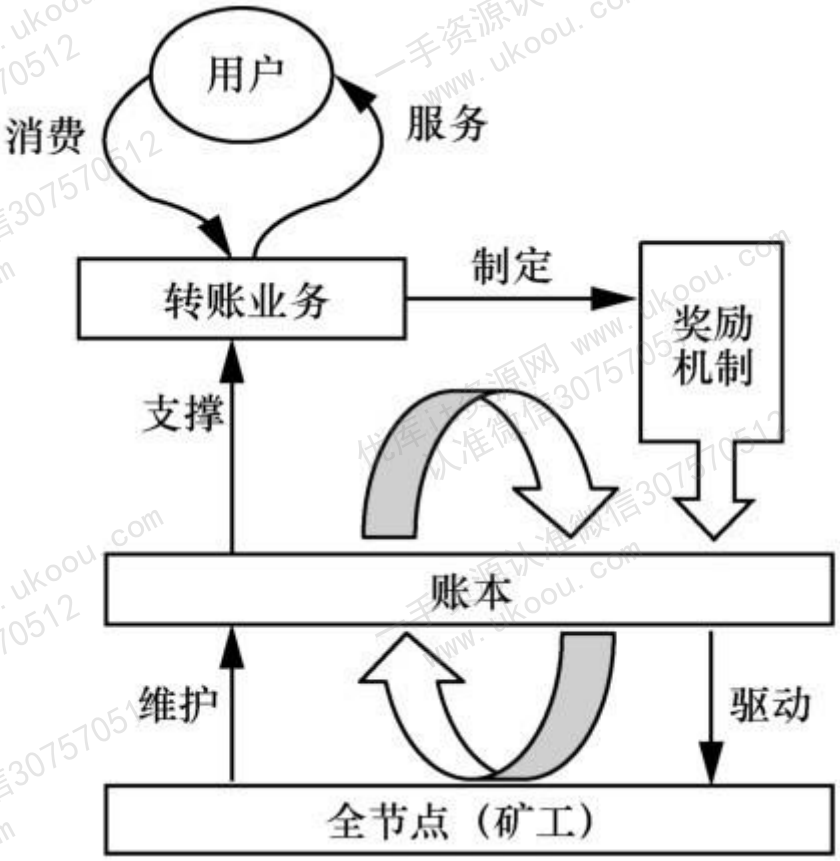
境为节点运行提供必要的虚拟环境，包括网络通信、数据存储以及图灵完备的计算/控制环境等，在虚拟机中运行的合约更新方便、灵活性强，其产生的漏洞也可能造成损失。

二、区块链的工作原理(下) 技术选型分析 Bitcoin 和以太坊

区别于其他技术，区块链发展过程中最显著的特点是与产业界紧密结合，伴随着加密货币和分布式应用的兴起，业界出现了许多区块链项目。这些项目是区块链技术的具体实现，既有相似之处又各具特点，我们将根据前文所述层次化结构对比特币、以太坊和进行分析，然后简要介绍其他代表性项目并归纳和对比各项目的技术选型及特点。

比特币

比特币是目前规模最大、影响范围最广的非许可链开源项目。为比特币项目以账本为核心的运行模式，也是所有非许可链项目的雏形。比特币网络为用户提供兑换和转账业务，该业务的价值流通媒介由账本确定的交易数据——比特币支撑。为了保持账本的稳定和数据的权威性，业务制定奖励机制，即账本为节点产生新的比特币或用户支付比特币，以此驱动节点共同维护账本。



1. 网络层

比特币在网络层采用非结构化方式组网，路由表呈现随机性。节点间则采用多点传播方式传递数据，曾基于 Gossip 协议实现，为提高网络的抗匿名分析能力改为基于 Diffusion 协议实现。在安全机制方面，比特币网络可选择利用匿名通信网络 Tor 作为数据传输承载，通过沿路径的层层数据加密机制来保护对端身份。

2. 数据层

比特币数据层面的技术选型已经被广泛研究，使用 UTXO 信息模型记录交易数据，实现所有权的简单、有效证明，利用 MKT、散列函数和时间戳实现区块的高效验证并产生强关联性。在加密机制方面，比特币采用参数为 Secp256k1 的椭圆曲线数字签名算法（ECDSA,elliptic curve digital signature algorithm）生成用户的公私钥，钱包地址则由公钥经过双重散列、Base58Check 编码等步骤生成，提高了可读性。

3. 共识层

比特币采用 PoW 算法实现节点共识，该算法证明依据中的阈值设定可以改变计算难度。计算难度由每小时生成区块的平均块数决定，如果生成得太快，难度就会增加。该机制是为了应对硬件升级或关注提升引起的算力变化，保持证明依据始终有效。目前该阈值被设定为 10 min 产出一个区块。除此之外，比特币利用奖惩机制保证共识的可持续运行，主要包括转账手续费、挖矿奖励和矿池分配策略等。

4. 控制层

比特币最初采用链上处理模型，并将控制语句直接记录在交易中，使用自动化锁定/解锁脚本验证 UTXO 模型中的比特币所有权。由于可扩展性和确认时延的限制，比特币产生多个侧链项目如 Liquid、RSK、Drivechain 等，以及链下处理项目 Lightning Network 等，从而优化交易速度。

以太坊

以太坊是第一个以智能合约为基础的可编程非许可链开源平台项目，支持使用区块链网络构建分布式应用，包括金融、音乐、游戏等类型；当满足某些条件时，这些应用将触发智能合约与区块链网络产生交互，以此实现其网络和存储功能，更重要的是衍生出更多场景应用和价值产物，例如以太猫，利用唯一标识为虚拟猫赋予价值；GitCoin，众筹软件开发平台等。

1. 网络层

以太坊底层对等网络协议簇称为 DEVP2P，除了满足区块链网络功能外，还满足与以太坊相关联的任何联网应用程序的需求。DEVP2P 将节点公钥作为标识，采用 Kademlia 算法计算节点的异或距离，从而实现结构化组网。安全方面，节点在 RLPx 协议建立连接的过程中采用椭圆曲线集成加密方案（ECIES）生成公私钥，用于传输共享对称密钥，之后节点通过共享密钥加密承载数据以实现数据传输保护。

2. 数据层

以太坊通过散列函数维持区块的关联性，采用 MPT 实现账户状态的高效验证。基于账户的信息模型记录了用户的余额及其他 ERC 标准信息，其账户类型主要分为 2 类：外部账户和合约账户；外部账户用于发起交易和创建合约，合约账户用于在合约执行过程中创建交易。用户公私钥的生成与比特币相同，但是公钥经过散列算法 Keccak-256 计算后取 20 B 作为外部账户地址。

3. 共识层

以太坊采用 PoW 共识，将阈值设定为 15 s 产出一个区块，计划在未来采用 PoS 或 Casper 共识协议。较低的计算难度将导致频繁产生分支链，因此以太坊采用独有的奖惩机制——GHOST 协议，以提高矿工的共识积极性。具体而言，区块中的散列值被分为父块散列和叔块散列，父块散列指向前继区块，叔块散列则指向父块的前继。新区块产生时，GHOST 根据前 7 代区块的父/叔散列值计算矿工奖励，一定程度弥补了分支链被抛弃时浪费的算力。

4. 控制层

每个以太坊节点都拥有沙盒环境 EVM，用于执行 Solidity 语言编写的智能合约；Solidity 语言是图灵完备的，允许用户方便地定义自己的业务逻辑，这也是众多分布式应用得以开发的前提。为优化可扩展性，以太坊拥有侧链项目 Loom、链下计算项目 Plasma，而分片技术已于 2018 年加入以太坊源码。

应用研究

区块链技术有助于降低金融机构间的审计成本，显著提高支付业务的处理速度及效率，可应用于跨境支付等金融场景。除此之外，区块链还应用于产权保护、信用体系建设、教育生态优化、食品安全监管、网络安全保障等非金融场景。

1. 智慧城市

智慧城市是指利用 ICT 优化公共资源利用效果、提高居民生活质量、丰富设施信息化能力的研究领域，该领域包括个人信息管理、智慧医疗、智慧交通、供应链管理等具体场景。

2. 边缘计算

边缘计算是一种将计算、存储、网络资源从云平台迁移到网络边缘的分布式信息服务架构，试图将传统移动通信网、互联网和物联网等业务进行深度融合，减少业务交付的端到端时延，提升用户体验。

3. 人工智能

人工智能是一类智能代理的研究，使机器感知环境/信息，然后进行正确的行为决策，正确是指达成人类预定的某些目标。

三、密码和钱包

要完全理解加密钱包，我们必须了解一些关于区块链的概念，这将有助于我们理解钱包如何帮助我们。让我们开始吧。

什么是地址？🤨

地址是使用加密技术生成的一串文本，用于表示您在区块链上的帐户。这个地址可以与其他人公开共享，这样做是完全安全的。您可以从您的钱包地址发送和接收资金。基本上，地址是您在区块链上的唯一标识符，代表您的“帐户”。以太坊地址的一个例子是：`0x01573Df433484fCBe6325a0c6E051Dc62Ab107D1`.

什么是私钥？🔐

私钥是地址的对应物。每个地址都有一个关联的私钥。顾名思义，这意味着保密，不与任何人共享。

你可以把它想象成一个密码，一个非常强大的密码，它包含一堆字母和数字，可以让你证明对你的地址的所有权。任何拥有私钥的人都可以从您的地址进行交易，即从您的地址向他们的地址汇款。

私钥看起来像这样：

```
E9873D79C6D87DC0FB6A5778633389F4453213303DA61F20BD67FC233AA33262
```

如果您将您的地址视为您帐户的用户名，那么私钥就是它的密码。因此，分享您的地址是可以的，但永远不要分享您的私钥，否则有人可能会窃取您的资金——然后就无能为力了。

注意：由于区块链是去中心化的，因此没有“忘记密码”选项。如果您丢失了您的私钥，您将无法访问您的帐户。同样，如果有人窃取了您的私钥并窃取了您的资金，您将无能为力。保持此私钥的安全非常重要。

对于开发人员，我们经常使用私钥作为代码库的一部分来执行某些交易，例如将我们自己的智能合约部署到以太坊网络。当您仍在学习时，我们强烈建议您完全使用单独的帐户进行开发，而不是用于存储任何类型的资金。不幸的是，初学者开发人员经常使用他们拥有资金的同一个帐户，并且不小心公开共享他们的代码库 - 黑客可以在代码库中看到您的私钥并最终窃取资金。请把它当作一个谨慎的故事。

什么是助记词？👮‍♀️

助记词就像一个主密码 - 密码的密码！

想想密码管理器，比如 Lastpass 或 1Password。这些应用程序在其中安全地存储您用于其他应用程序的用户名和密码，并且它们本身也有密码。因此，如果有人破解了您的密码管理器，他们还可以访问存储在其中的所有帐户。

加密钱包有点像密码管理器，您可以在其中管理多个区块链帐户。如果私钥是单个帐户的密码，则种子短语有点像该钱包的主密码。

当你创建一个新的加密钱包时，你会看到一个助记词，你应该绝对安全地存储和备份。您从该钱包中生成的任何新帐户都将链接到助记词。那一个助记词将始终生成相同的帐户，每个帐户具有相同的私钥和地址。

因此，例如，如果您创建了一个钱包，然后在其中创建了 5 个帐户，则您的助记词管理所有 5 个帐户。如果您想切换到新钱包，您可以单独导入 5 个钱包 - 通过使用它们各自的私钥 -或者只是使用助记词导入，它会重新生成相同的 5 个帐户。

种子短语的一个例子是：dove lumber quote board young robust kit invite plastic regular skull history

那么什么是加密钱包呢？😛

加密钱包是您账户的管理者，主要是他们的私钥。它们还允许您与去中心化应用程序交互，并允许通过钱包连接到 dApp，充当构建在区块链上的所有应用程序的单点登录。

在 LearnWeb3 上，您也可以进入仪表板并连接您的加密钱包（在您设置之后），这将让我们知道您的地址是什么，这样我们就可以在您从我们的轨道毕业时向您发送一些生病的 NFT！

设置钱包 🎉

对于以太坊，有许多可用的钱包选项。Metamask 或 Coinbase 钱包是最容易上手且对开发人员最友好的。

两者都是以太坊加密钱包，可以作为浏览器扩展或移动应用程序安装。您可以在下面找到下载链接。我们建议下载其中任何一个并进行设置，然后再继续进行跟踪。

加密钱包是个人和加密世界之间的桥梁。

钱包被用于存储大量加密资产，而钱包本身也多种多样，令用户目不暇接。人们对投资加密货币持犹豫态度的原因之一便是安全风险。虽然进行加密货币交易存在风险，但安全措施实施起来也并非难事，而且有数百万人在加密货币领域安全地进行交易。

在努力打造一款完美钱包的过程中，我们也了解到，在面临琳琅满目的钱包选择时，挑选一款完美的钱包是困难的。任何在互联网上尝试寻找完美加密钱包的人都应知道，选择钱包意味着在安全、隐私和便捷之间做出决定。

用户“被迫”进行选择，因为没有一个钱包是完全安全和可靠的。用户要么通过信任交易所，要么自己掌握安全措施，但冒着可能犯错的风险。尽管这一现实为现在的加密钱包描绘了一幅黯淡景象，但

解决方案却显而易见——我们需要一个结合一流安全性和优秀可用性的加密钱包，并为用户提供安全有效的备份选项，而不需要他们放弃对资金的控制。

在首次选择钱包时，用户必须考虑其安全功能，如钱包的开发者是谁，以及用户是否可以访问自己的私钥。在使用新钱包之前，用户应尝试找到有关其安全性能的可用信息。此外，当查看加密钱包背后的团队时，应该确保其由信誉良好的项目开发，如若是匿名团队，则其极有可能在策划一个骗局。

加密圈有句广为流传的谚语，“私钥不属于你，代币也不属于你。”这是指用户是否掌控着自己的私钥，否则便等同于将自己的数字资产委托给第三方。拥有私钥也意味着要对其安全负责。管理自己的私钥似乎听起来很有吸引力，但如果你的私钥或助记词被盗或丢失，资金也会随即消失。没有什么比意识到自己忘记私钥更可怕的事情。

如何选择加密钱包也取决于你的用途。你是打算做日常交易吗？还是主要是为了“拿住”？

过去的钱包安全事件告诉我们，黑客会以多种方式窃取加密货币，从窃取或猜测你的密码，到通过网络钓鱼尝试引诱你泄露信息。其中，网络钓鱼攻击是黑客最常见的数据窃取技术。

1. 恶意空投

这种方法经常用于开展网络钓鱼活动。用户会收到一封电子邮件、短信或社交媒体信息，表明某些代币已经通过空投被添加到他们的钱包中，然后将用户导向一个出售加密货币的平台。获得空投者被要求连接他们的钱包地址。一旦连接，他们就会发现所有的资金都被黑客掏空。

2. 助记词钓鱼

加密用户都知道，助记词是提供访问钱包中所有加密资产的密钥。这就是为何许多网络钓鱼诈骗欺骗用户分享他们的助记词。在助记词网络钓鱼中，最常见的诈骗方式之一是通过假钱包应用程序。假钱包应用程序的主要受害者是安卓手机的用户，因为 GooglePlay 的审核规则没有 AppStore 严格。黑客可以滥用这一规则，通过上传假钱包应用来模仿知名钱包应用程序来“钓鱼”用户输入助记词。

3. 恶意电子邮件、网站和消息

钓鱼邮件、短信和社交媒体信息是最常见和已知的技术。然而这些也是最有效的骗局。高仿网站、社交媒体账户和欺诈性电子邮件每日都会出现，并欺骗用户参与各种广告宣传和营销活动。

总的来说，我们建议用户应确保自己使用了正确的 URL，而不是将钱包连接到可疑的 Dapp 上。除此之外，我们还建议您确保钱包具有多重身份验证和设置强密码，以确保进一步安全。一些钱包还会启用生物识别功能，这也使得在没有指纹的情况下难以登录。

以下是 FoxWallet 安全团队总结的一些技巧，以帮助您防止上述诈骗。

- 不要重复使用电子邮件和加密帐户的密码。
- 使用多重身份验证。
- 将加密货币与个人/工作账户分开。
- 留意最新骗局和威胁。
- 使用 VPN。

四、NFT 与铭文

最近，铭文 NFT 无疑是最火热的叙事。那么铭文 NFT 的优势有哪些？又应该如何选择呢？这节课我们将跟大家讲清楚

- 与以太坊 NFT 比，优势在哪？

全部上链：

由于铭文 NFT 全部内容是铭刻在 bitcoin 网络上的，你的心爱的 NFT 将永久的存于世界上最安全的链上。这和大部分 ETH NFT 将内容存储在 IPFS 有较大不同。

- 什么是铭文号，递归铭文，诅咒铭文，稀有聪？

铭文号：

由于每个铭文 NFT 都会按照铭刻顺序被赋予一个铭文编号（从 0 开始依次递增），随着时间推移，当前铭文号已达数千万，这增加了收藏的乐趣与价值判断的依据。

通常大家认为铭文号靠前的铭文 NFT 会有更大的收藏价值，比如 sub10k 系列（最靠前一万个铭刻的铭文）

递归铭文：

由于 taproot 隔离见证对内容的限制为 4M，这样就限制了铭文内容的大小，为了突破这个限制及引入更大的灵活性。铭文协议设计了一种相互引用的格式，被称为「递归铭文」。

这样你可以在铭文中看到更丰富的更高清的表现，比如 ordibots 3D 就采用了递归铭文的方式完成了 AR 与高清，且每个铭文 NFT 铭刻费用非常低。

诅咒铭文：

诅咒铭文原本是协议 bug，一些铭文没有「正常」的被编入原本的序号系列。因此，被称为「被诅咒」的铭文，从而被赋予了负数编号。

当前已经修复了这些协议 bug，未来也不会再新增编号为负数的诅咒铭文 NFT。

稀有聪：

由于铭文 NFT，每一个都被刻在聪上，为了增加趣味性，铭文协议定义了一些特别的聪，叫做「稀有聪」，比如每个区块第一个被开采的聪。刻在这些聪上的 NFT，通常会价格高一些，因为稀有聪的价格高于普通聪，我头像就是一个铭刻在稀有聪上的巫师。

如何选择铭文 NFT?

由于铭文 NFT 的各种趣味性，选择铭文 NFT 会是一个比较偏主观而个人的过程。

比如铭文号靠前的有收藏价值，递归铭文有不断技术创新价值，诅咒铭文类似错版邮票且不再新增，稀有聪则有一个价值的地板（就算 NFT 不值钱，还可以把聪卖了）。

看起来眼花缭乱，但其实万变不离其中，看谁的「共识」更强。

在我看来，目前共识最强的有三类：

1. 强社区

如大巫师，一系列的社区事件与传播，让铭文 NFT 不断出圈；以及近期狐狸的快速飙升，大家能看到社区的力量。长远看来，我认为是最重要的，没有社区就会不断被新的概念和系列稀释掉关注和流量。

2. 铭文号靠前 First is First

sub10k 系列里面，一些比较好的系列；当前龙头小青蛙，被认为是第一个 10k 系列（其实另有一个，口碑有问题，不介绍了）。

3. 各细分领域龙头

这种会汇聚喜欢这类细分领域的关注和流量。比如：技术创新类的 ordibots3d，艺术家类大鹅，稀有聪类 ohm 等。

五、跨链技术

Abstract

跨链技术本质上是一种将 A 链上的数据 D（或信息 I，或消息 M）安全可信地转移到 B 链并在 B 链上产生预期效果的一种技术。因为区块链系统本来就是一种特殊的分布式账簿数据库系统，所以这个转移的数据，最常见的就是资产的数据，如代币余额。

目前主流的区块链跨链技术方案按照其具体的实现方式主要有：公证人机制、哈希锁定、侧链&中继链、分布式私钥控制。

目前最有名的跨链项目有 Cosmos 和 Polkadot，两者采用的都是基于中继链的多链多层架构。由此可见，侧链&中继链技术将会是未来跨链技术的主力。

本文首先简要介绍跨链的技术原理。其中会简要介绍公证人机制、哈希锁定，详细介绍侧链&中继链技术。然后本文将介绍几个相关的跨链项目，包括基于 ETH 的 Plasma、基于 Polkadot 的达尔文网络，基于 Cosmos 的 IRIS。

公证人机制及哈希锁定

跨链交互根据所跨越的区块链底层技术平台的不同可以分为同构链跨链和异构链跨链。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。而异构链的跨链交互相对复杂，如 Bitcoin 采用 PoW 算法而 Fabric 采用传统确定性共识算法，其区块的组成形式和确定性保证机制均有很大不同，直接跨链交互机制不易设计。异构链之间的跨链交互一般需要第三方辅助服务辅助跨链交互。

跨链要达到安全可信必然对跨链机制、步骤等有一些要求，其中最重要的就是跨链事务的原子性。对于普通的链内交易来说，交易需要支持原子性——交易如果失败则需要回滚。而跨链的交易也是如此，其失败时要回滚涉及本次交易两条或多条链的交易。

2.1 公证人机制（Notary schemes）

公证人也称见证人机制，其是一种中介的方式。设区块链 A 和 B 本身是不能直接进行互操作的，那么他们可以引入一个共同信任的第三方作为中介，由这个共同信任的中介进行跨链消息的验证和转发。很多时候，这个公证人/中介就是交易所。其优点在于支持异构的区块链跨链，缺点在于有中心化风险，只能实现交换不能实现转移。

跨链交易实例：假设 Alice 想和 Bob 进行 1 个 BTC 换 50 个 ETH 的交易

Alice 将自己的 1 个 BTC 存入交易所的比特币地址;Bob 将自己的 50 个 ETH 存入交易所的以太坊地址；

Alice 在交易所上挂单：1 BTC for 50 ETH；

Bob 通过交易所完成与 Alice 的交易，Alice 得到 50 ETH，Bob 得到 1 BTC

这里会有不少的形式。一种是 Bob 挂出购买比特币的单子，然后交易所撮合。一种是 Bob 直接看到 Alice 挂出卖单，然后直接要这个卖单。 4. Alice 将交易所得的 50 ETH 提币到自己的以太坊账户；Bob 将交易所得的 1 BTC 提币到自己的比特币账户；

通过引入中介完成了 Alice 和 Bob 的 BTC 和 ETH 的交换。通过该例子可以看出交易所的方式目前仅能够支持资产的交换，且资产交换的原子性、安全性完全由中心化的交易所保障，故存在一定的中心化风险。

2.2 哈希锁定（Hash-locking）

哈希锁定的典型实现是哈希时间锁定合约 HTLC(Hashed TimeLock Contract)。哈希时间锁定最早出现在比特币的闪电网络。哈希时间锁定巧妙地采用了哈希锁和时间锁，迫使资产的接收方在 deadline 内确定收款并产生一种收款证明给打款人，否则资产会归还给打款人。收款证明能够被付款人用来获取接收人区块链上的等量价值的数量资产或触发其他事件。哈希锁定只能做到交换而不能做到资产或者信息的转移，因此其使用场景有限。

跨链交易实例（仍以前一节中的交易需求为例）：

Alice 随机构建一个字符串 s，并计算出其哈希 h;

Alice 将 h 发送给 Bob;

Alice 通过合约锁定自己的 1 个 BTC 资产，设置一个较长的锁定时间 T1, 再设置了获取该 BTC 的条件：Bob 提供 h 的原始值 s;

Bob 锁定 50ETH 到自己的合约，设置一个相对较短的锁定时间 T2(T2 < T1)。再设置 50ETH 的获取条件：Alice 提供 h 的原始值 s;

Alice 将字符串 s 发送到 Bob 的合约获得 50 个 ETH;

Bob 观察到步骤 5 中 Alice 的 s 值，将其发送给 Alice 的合约成功获取 1 个 BTC; 至此完成资产的交换。

如果超时，则锁定的资产返回原主。

从上述的过程可以看出哈希时间锁定合约有一些约束条件：

双方必须能够解析双方的合约内部数据，例如 s，例如锁定资产的证明等;

哈希锁定的超时时间设置时需要保证存在时间差，这样在单方面作弊时另一方可以及时撤回自己的资产。

2.3 分布式私钥控制

国内关于分布式私钥控制的博客真的烂到窒息了，cure Multi-Part Computation）和门限密钥共享机制（Threshold Key Sharing Scheme）的技术。分布式私钥控制其实和跨链并没有什么关系，也没有解决跨链 2 个难点中的一个。其将中继链账户的私钥分为冗余的多份，然后分发给验证人，可以防止某个验证人在在跨链资产交换的解锁锁定阶段的单方作恶，因为只有多个验证人集合起来才拥有私钥。

国内关于分布式私钥控制的博客真的烂到窒息了，想深入了解分布式私钥控制建议之间看 Wanchain 的白皮书。

3 侧链/中继链

3.1 侧链的含义及意义

首先，什么是侧链?

在一开始，主链特指比特币主网区块链。所以所谓侧链就是除了比特币区块链以外的，任何能遵循侧链协议并和比特币互通的一切区块链。侧链使得比特币有更好的流动性；而在比特币主网上开发应用很困难，现在通过再侧链上开发应用再使用互通方式与主链连接可以解决这个问题——间接使用了比特币，进一步巩固了比特币的中心地位。

不过，现在自然已经不能说主链特指比特币了。根据维基百科上的说法：“侧链用来指代与主区块链并行的那条区块链。来自主区块链的 entries 可以向侧链连接，也可以被侧链连接；这样一来，侧链就可以独立于主区块链进行操作（例如，通过使用备用的记录保持方式）。一个侧链模型是驱动链。”

这个说法包含三个要点：

侧链是相对的。我们不能单纯的说某条链 B 是侧链，而必须说这条链 B 可以是链 A 的侧链。

侧链与主链是独立的。链 B 可以有自己的功能，在它自己运行时不需要链 A 的支持。如果 B 链发生运行故障或被中心化控制，不会直接影响到 A 链本身的运行（但可以间接影响，比如 B 链被控制后，A 链还依旧与之交互）。

侧链与主链可以连接互通，即跨链。当要实现跨链的功能时才需要 B 链和 A 链进行互通。因为侧链的互通机制是其最主要的功能，所以常常将侧链与主链的互通叫做侧链技术。至于侧链本身是否包含在

侧链技术之中，不同的项目有不同的看法。

其次，侧链的意义?

从主链单链角度讲，侧链可以虚拟化地横向和纵向提升主链的性能。所谓横向，就是将多个侧链与主链互通，将大部分交易放到侧链上，然后再通过与主链互通实现，可以虚拟地提升主链的 TPS。所谓纵向，就是侧链可以有主链不具有的功能，通过侧链，主链看上去也像是支持了这些功能。所谓虚拟化，就是虽然有横向和纵向的提升，但是主链本身并任何没有变化，只是通过众多侧链小弟帮其起到类似代理的作用，使其看上去性能提升。

从全局角度讲，侧链作为跨链技术的一种，自然是为万链互连做出了重要贡献。实现万链互联有两者架构：1. 任何一条链，既有主链的功能，又有侧链的功能（一些资料将拥有侧链功能叫做遵循侧链协议），这就像计算机网络中任何计算机既是主机又是路由器。2. 只有特定的几条链作为主链，其他所有链都只支持侧链功能，就和现在的计算机网络类似，有网络核心部分——单纯的路由器，也有网络的边缘部分——单纯的主机。

3.2 侧链的技术

侧链实现是通过双向锚定技术。将暂时的数字货币在主链中锁定，同时将等价的数字资产在侧链中释放。实现双向锚定的最大难点在于协议改造需兼容现有主链，也就是不能对现有主链的工作造成影响。其具体实现方式有：单一托管模式、联盟模式、SPV 模式、驱动链模式、混合模式。

单一托管模式就是类似交易所做中介完成锁币放币，其实和。联盟模式即公证人模式，由多个公证人的多重签名来对转移资产的交易进行签名，避免了中心化。

SPV 模式是通过将交易发给本链的一个特殊地址，由此会自动创建一个 SPV 证明给侧链上并发起一个交易在侧链上解锁对应的资产。驱动链模式是用矿工来作为资金托管方，将资产的监管权发放到数字资产矿工手上，矿工进行投票决定何时解锁资产及将资产发送到何方。混合模式就是将这些侧链机制进行有效结合，对结构不同的链，为其使用最适合其结构的模式，如主链使用 SPV，侧链使用驱动链。

这里 SPV 模式是使用得最多的，也是最有前途的。SPV 就是简单支付验证（Simplified Payment Verification），其能验证交易是否存在。

BTC-Relay 是号称的史上第一个侧链，其通过以太坊构建了一个比特币的侧链，运用以太坊的智能合约允许用户验证比特币的交易。SPV 交易实例（仍以之前的交易需求为例）：

Bob 将 50ETH 发送到 BTCSwap 的合约进行冻结(该合约若确认 Bob 接收到来自 Alice 的 1BTC 就自动将 50ETH 转给 Alice)；

Alice 确认 Bob 冻结信息后，将 1BTC 转到 Bob 比特币账户；

BTC-Relay 将比特币区块头推送到 BTCSwap 合约；Alice 将自己转 BTC 给 Bob 的交易 tx 发给合约 BTCSwap 合约，请求 50ETH;

BTCSwap 合约结合 tx 和比特币区块链进行 SPV 验证，验证通过则将 50ETH 转到 Alice 的以太坊地址。

侧链的机制相对哈希锁定而言能够提供更多的跨链交互场景，侧链以及类 SPV 验证的思想适合所有跨链的场景。

3.3 中继链

中继链算是公证人机制和侧链机制的融合和扩展，目前社区内最活跃的两个跨链项目 Cosmos 和 Polkadot 采用的都是基于中继链的多链多层架构，其中 Cosmos 目前支持的是跨链资产交互；而 Polkadot 则宣称提供任意类型的跨链交互，但具体实现还有待观察。

- 3.3.1 Cosmos 的中继链机制

为了支持平行链之间的跨链操作，Cosmos 提出了一种跨链交互协议 IBC(Inter-Blockchain Communication Protocol)。

以链 A 到链 B 转账 10token 为例说明使用 IBC 的跨链交互：

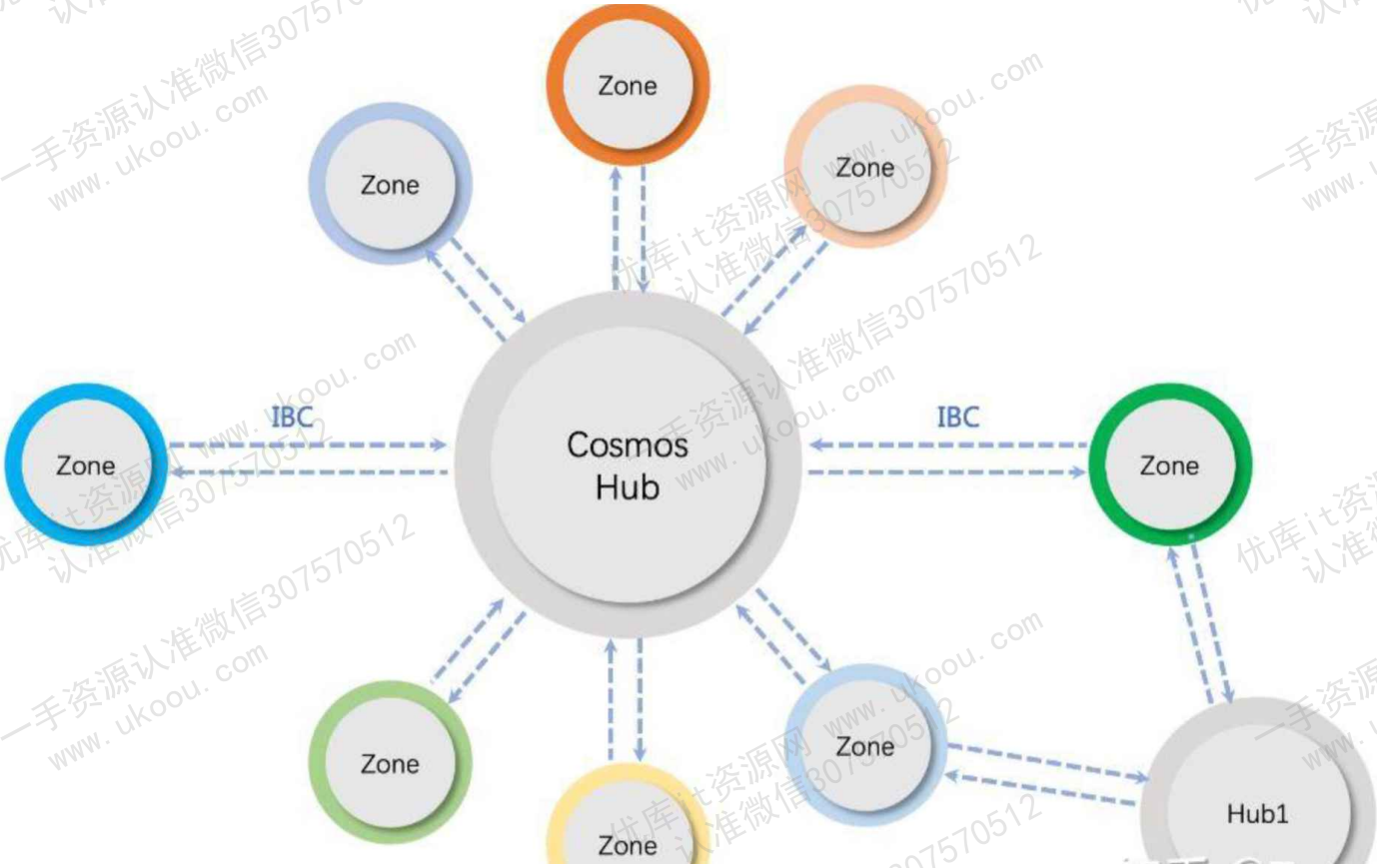
互相跟踪。如果 A 要和 B 进行跨链交易，那么 A 和 B 链需要分别运行相当于对方区块链的轻节点，这样可以实时接收到对方的区块头信息（方便后续执行类 SPV 验证）；链 A、链 B 初始化 IBC 协议。

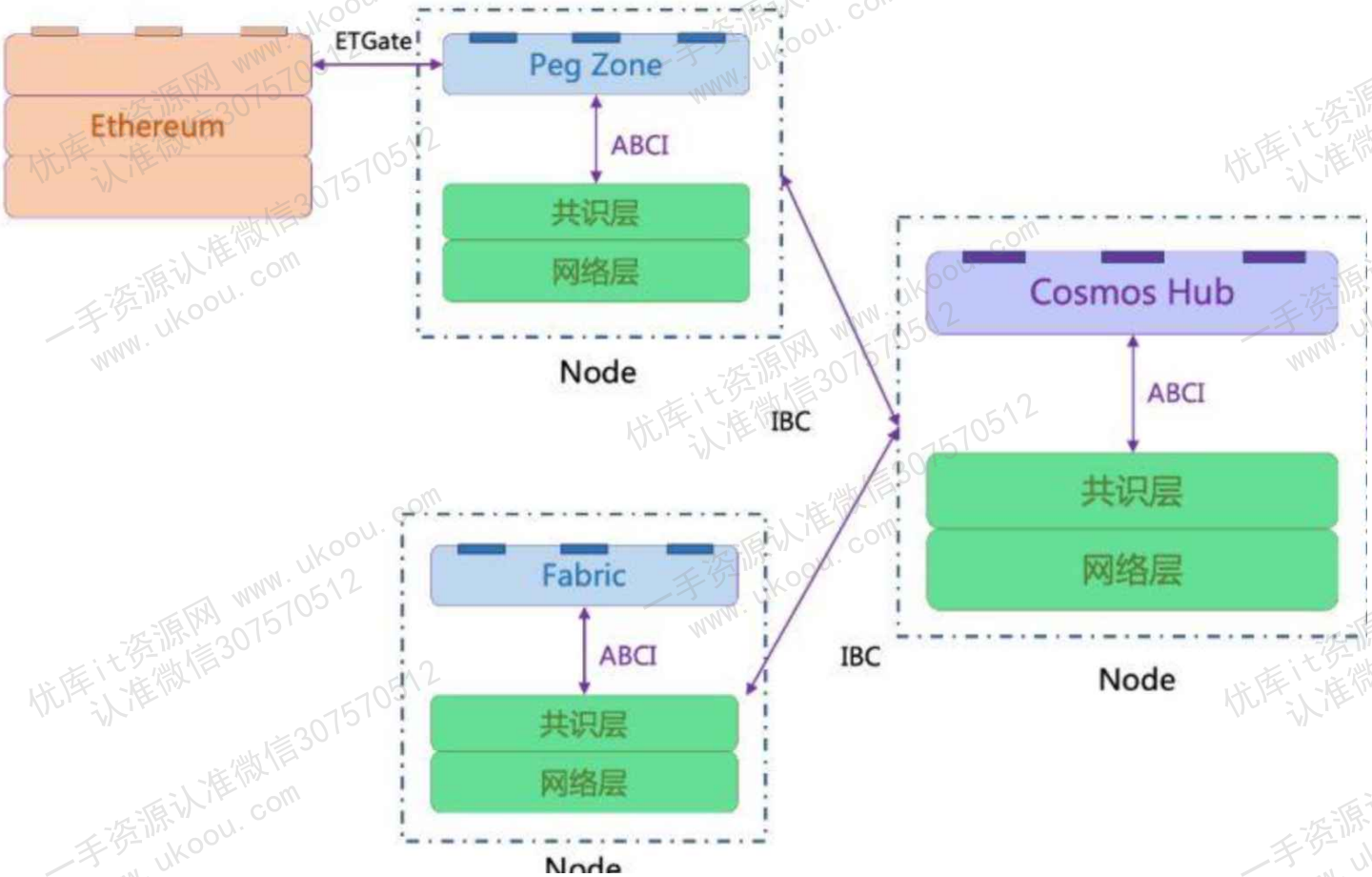
链 A 冻结 10token, 并生成相应的证明发送给链 B。

链 B 接收到相应的 IBC 消息，通过链 A 的区块头信息确定链 A 确实进行相应的资产冻结，然后链 B 会生成等价 10token 的资产。

以上是使用 IBC 协议的两个平行链直接进行跨链的基本过程，如果区块链很多，那么这种方式的两两跨链复杂度会呈现组合级别增加。因此 Cosmos 网络又引入了一种 Hub 的中继链，所有的平行链都通

过 IBC 连接到 Hub，让 Hub 辅助跨链交易的验证和资产转移（于是乎，某链能与 Cosmos 体系中的链进行交互=某链能连接到 Hub）。目前 Cosmos 实现了一个官方的 Hub 称为 Cosmos Hub。





上图是 Cosmos 网络的详细架构图。一条链从层次结构上讲，分为网络层、公式层、应用层。为方便平行链开发，Cosmos 提供了 tendermint core（简称 tendermint） 和 Cosmos SDK（Go 语言）。其中 tendermint 是指网络层、共识层的封装，而 Cosmos SDK 是应用层中常用的模块：账户、治理、Staking、IBC 等等的封装。因此，自己开发一条新链可以使用 Cosmos SDK+ tendermint，并且由此开发出来的链能直接与 Cosmos Hub 连接（Cosmos Hub 自己本身也是用 Cosmos SDK+tendermint 开发的）。

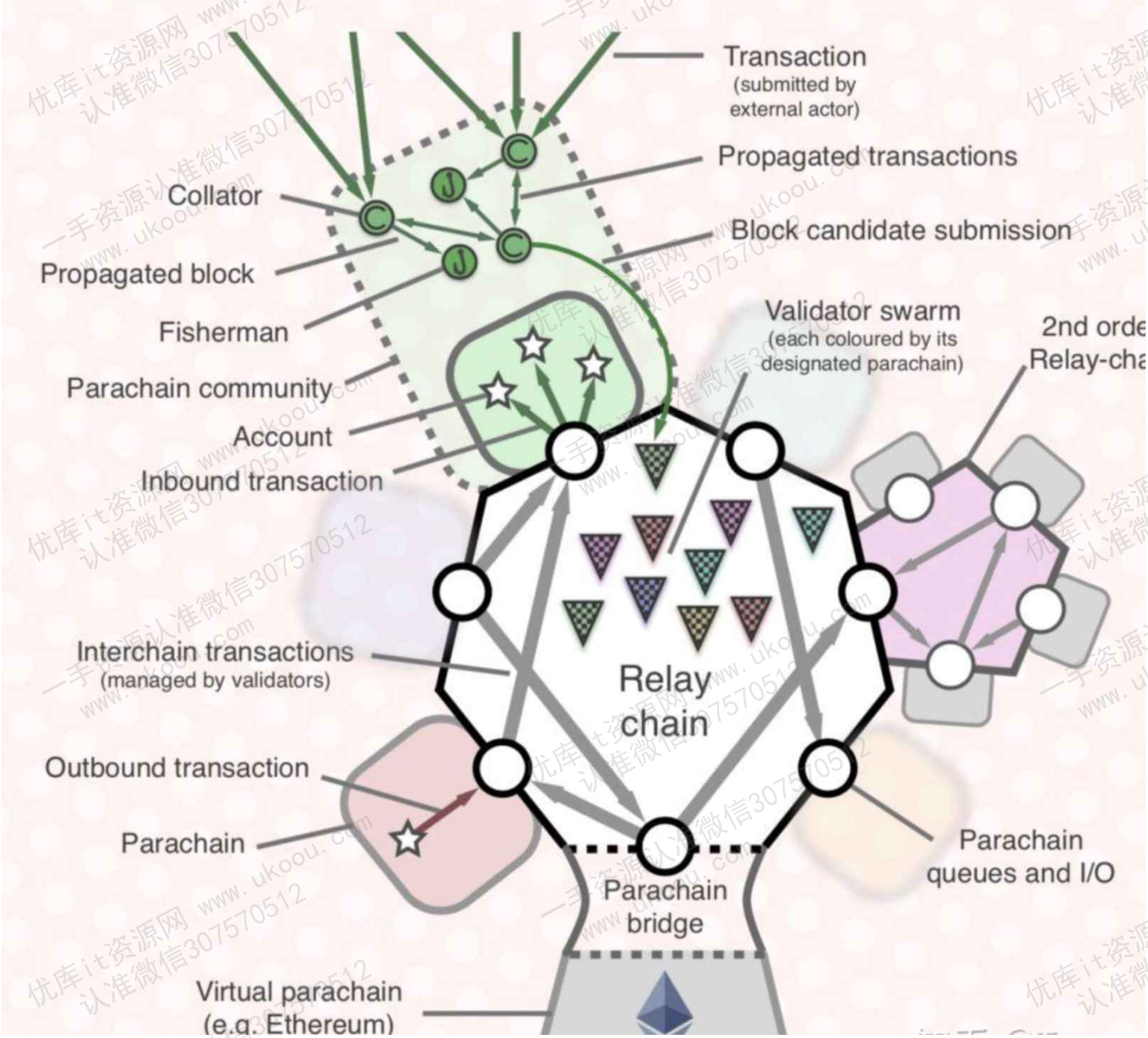
而对于非 Cosmos SDK 开发的区块链（如已经存在的这些区块链），如果要与 Cosmos 体系中的链进行交互（即能与 Hub 连接），需要使用 Peg Zone 进行桥接，所谓的 Peg Zone 就是使用 Cosmos SDK 开发的，既能接入 Hub 的，又能和原链进行交互的一条链。如图中的 Ethereum，如果要接入 Cosmos Hub，则需要专门使用 Cosmos SDK 开发一条起 Peg Zone 作用的新链。

所谓 Cosmos 主网是指由 Cosmos 团队自己开发的第一个官方版 Hub，也就是不同链进行跨链操作时的第一个中央枢纽。以太坊将是 Cosmos 最先连接的非 Cosmos SDK 开发的公链，目前有两个项目去实现这种连接： Cosmos 开发团队主导的 Ethermint 项目，以及由 Loom Network 主导的 PlasmaChain。这两个项目其实就是开发一个连接以太坊和 Cosmos Hub 的、起 Peg Zone 功能的一条链。

协议应该是各方达成共识的，在 3.1、3.2 小节中说到的“侧链协议”其实并不是真正的协议，因为侧链技术目前没有像计算机网络一样有一些共识的协议，所以其实只能说是侧链机制。而 Cosmos 为跨链带来的最大贡献在于 IBC 协议的设计，IBC 协议提供了一种通用的跨链协议标准。IBC 的设计使得跨链交易可以在多个 Hub 之间进行安全路由和转发，类似目前互联网的 TCP/IP 协议。但是遗憾的是目前的 Cosmos 设计也只能够支持资产的跨链，而且由于不同区块链的业务不同其共识速率的不一致也会影响跨链交易有效性的证明。

这里只讲了 Cosmos 的侧链技术，关于 Cosmos 更多的内容，请看其他参考文献。

- 3.3.2 Polkadot 的中继链机制



Polkadot 的平面体系结构有三种链链角色和四种参与方。

1. 三种链角色：

中继链（Relay chain）：中继链位于 Polkadot 的体系的核心地位，主要是为整个系统提供统一的共识和安全性保障；

平行链（Parachain）：在 Polkadot 中平行链负责具体的业务场景，平行链自身不具备区块的共识，它们将共识的职责渡让给了中继链，所有平行链共享来自中继链的安全保障，中继链是 Polkadot 组成的一部分（中继链有可能不是一条链，Polkadot 对其定义是 App 的数据结构，因此可以是 DApp 甚至是一般的 App；不过大部分情况下还会是一条链）；

转接桥(Bridges）：在 Polkadot 中转接桥其实有三个含义，其中最重要的含义是：为 Polkadot 体系之外的区块链(如 Bitcoin, Ethereum)提供不同的 Bridge 与 Polkadot 连接在一起进行跨链交互。

三种链角色和 Cosmos 体系中差不多。

2. 四种参与方：

验证者(Validator): 验证者负责 Polkadot 的网络出块，会运行一个中继链的客户端，在每一轮区块产生中会对其提名的平行链出的块进行核验。当平行链的块都被他们的验证者集合确定好之后，验证者们会将所有平行链区块头组装到中继链的区块并进行共识。

收集人(Collator)，也叫核对人: 帮助验证者收集、验证和提交备选平行链区块，维护了一个平行链的全节点。

钓鱼人(Fisherman):钓鱼人主要靠检举非法交易或者区块以获取收益；

提名人(Nominator):拥有 stake 的相关方，维护和负责验证者的安全性。

用户在平行链发起交易，交易被收集人收集，打包成区块，交给一组验证人去验证。这组验证人并不是来自平行链，而是来自中继链统一管理的验证人池，通过随机分组指定给平行链。

每条平行链都有一个消息输出队列和一个消息输入队列。如果用户发起的是跨链交易，交易就会被放进输出队列。再被目标平行链的收集人放入其输入队列。目标平行链的收集人执行交易，生成区块，由验证人组敲定。

提名人是 Polkadot 基础通证 DOT 的持有者，他希望质押 DOT 获得收益。但是要么是因为 DOT 数量少，要么是缺少运行维护验证人节点的专业技能。因此系统提供了另一个参与途径，就是持币者选择他信任的验证人，把自己的 DOT 通过验证人来质押，分享验证人收益。

渔夫是个软件进程，它监控网络上的非法行为，一旦发现就会向区块链提交举报交易。举报交易也要经过共识过程，通过 2/3 以上验证人验证，打包进区块，惩罚和奖励也都是区块链交易。

在 Polkadot 中如果 Parachain A 需要发送一笔交易到 Parachain B 的过程如下：

链 A 将跨链交易放到自己的消息输出队列 engress。

链 A 的 Collator 收集 A 链的普通交易以及跨链交易并提交给链 A 的验证者集合。

链 A 的验证者集合验证成功，将本次链 A 的区块头信息以及链 A 的 engress 内信息提交到中继链上。

中继链运行共识算法进行区块确认以及跨链交易路由，中继链上的验证者会将链 A 的相应交易从链 A 的 engress queue 中移动到链 B 的消息输入队列 ingress queue 中。

链 B 执行区块，将 ingress queue 中相应交易执行并修改自身账本。

以上便是 Polkadot 跨链交易的主要步骤。Polkadot 为应用链提供的工具是 Substrate，目前支持 Rust 语言开发。

4 跨链相关项目

4.1 ETH.Plasma

以太坊的 Plasma 是 Layer2 扩容的一个方案。Plasma 其原理是将交易移到 off-chain 并在一条次链（Secondary Chain）中进行处理，其想法来自 side chain，但完全一样。但 Plasma 不如 State Channel 来的成熟，目前只有在支付上的应用，数量也很少，正在进行支付以外领域的使用研究。

4.2 Polkadot.Darwinia

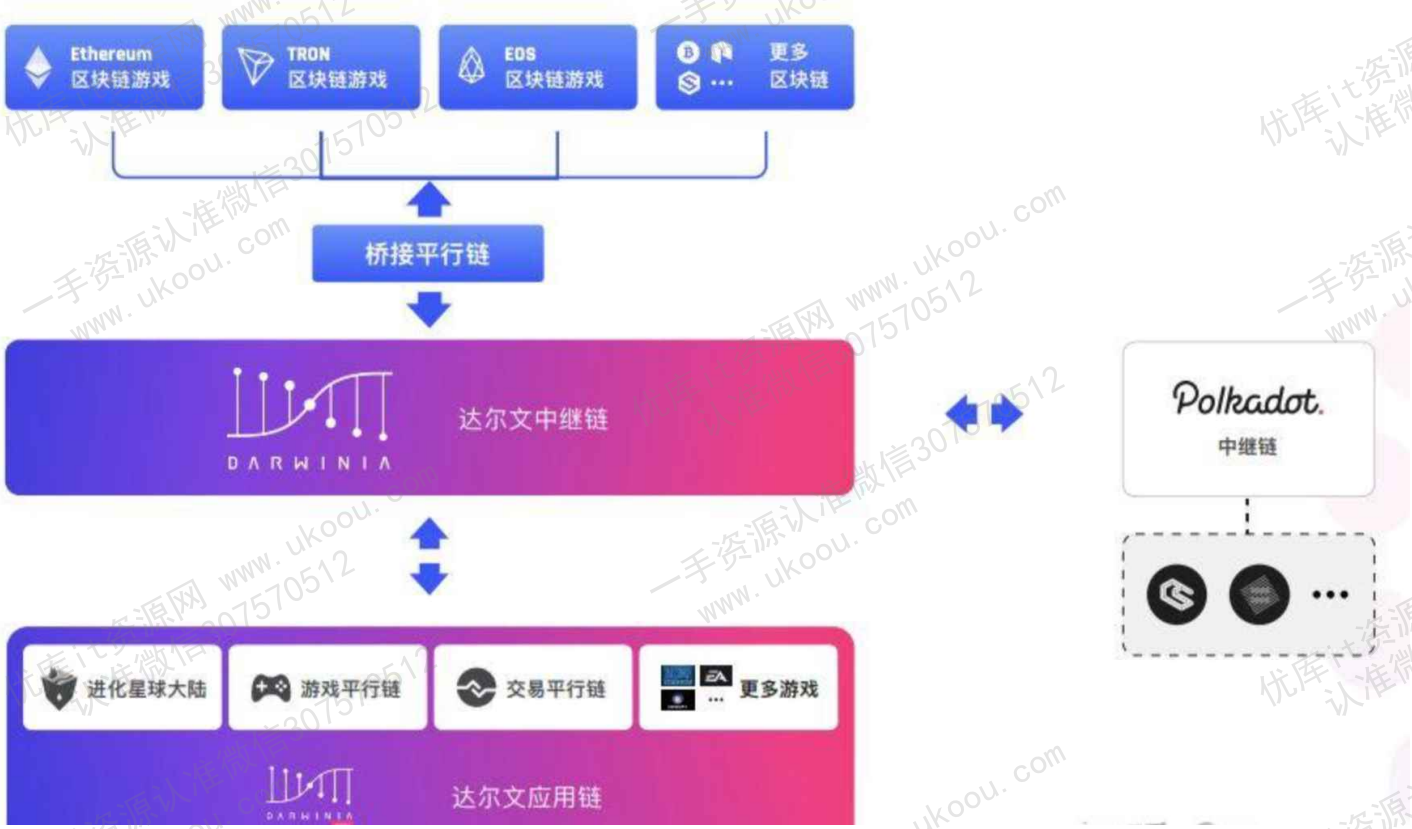
- 4.2.1 达尔文网络概述

达尔文网络，是使用 Polkadot 的 Substrate 的技术构建的跨链游戏网络。达尔文网络的技术其实可以看成是在 Polkadot 的 Substrate 之上的二次开发，将其改进成专门用于游戏资产和游戏操作的跨链交互。目前主要用于支撑进化星球及相关的业务体系（进化星球是一个建立在区块链上的游戏虚拟世界，也是一个 DAO，类似于区块链上的《我的世界》）。主网 Token 是 RING。

达尔文网络的运行模式有 Solo 模式和 Polkadot 模式（值得注意的是，在不同的运行模式下具体的激励方案会有所不同。）。

1. solo 模式。其实，达尔文网络本身自己就是一个的网络，其有自己的中继链。在这个网络中，各种游戏成为达尔文的子世界（子大陆），这个子世界可以是一条使用 Polkadot 的 Substrate 开发的平行链，也可以是 ETH 或者 EOS 上的智能合约。这些子世界接入达尔文网络的中继链的方式和 Polkadot Parachain 接入 Polkadot Relay-chain 一样。

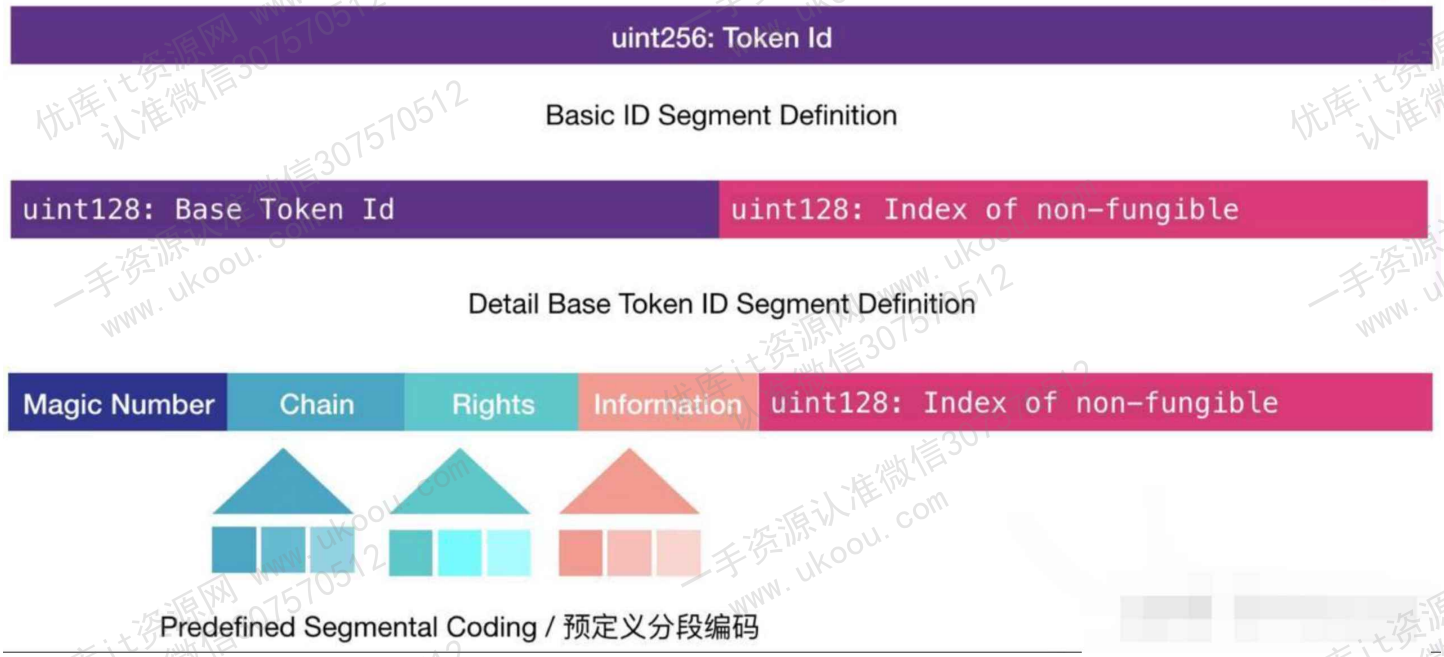
2. Polkadot 模式。达尔文网络整体也可以看做是 Polkadot 的一个 Parachain，并接入 Polkadot 的 Relay-chain。从这个意义上讲，达尔文网络可以被看做是 Polkadot 的一个二阶 Relay-chain (2nd order Relay-chain)



在达尔文网络结构中，我们看到有一个东西叫做达尔文应用链，达尔文应用链之于达尔文网络等于 Parachain 之于 Polkadot 网络。达尔文应用链是基于 Substrate 和达尔文网络区块链内核（Darwinia Kernel）设计开发的一套应用区块链的框架。

- 4.2.2 星际资产标准

对于游戏资产跨链而言，最重要的自然是资产的数据结构及操作的定义。在达尔文网络官网的中的“NFT 可识别性”部分大致叙述了其星际资产编码标准。其认为在单一网络中，域内的 Token ID 在域内能标识唯一的物品，但是到了互连的环境下则不行。因此其设计了一个星际资产编码标准，让不同公链、不同游戏的资产在达尔文网络可以得到唯一标识，让游戏资产可以方便的跨链转移。☒ 星际资产编码标准的字段含义如下。



4.3 Cosmos.IRIS

前面的达尔文网络是 Polkadot 生态中的项目（主网 Token 为 IRIS），而 IRIS 则是 Cosmos 生态下的项目。其旨在解决的主要挑战有两个：

分布式账本上链外计算和资源的集成与协作

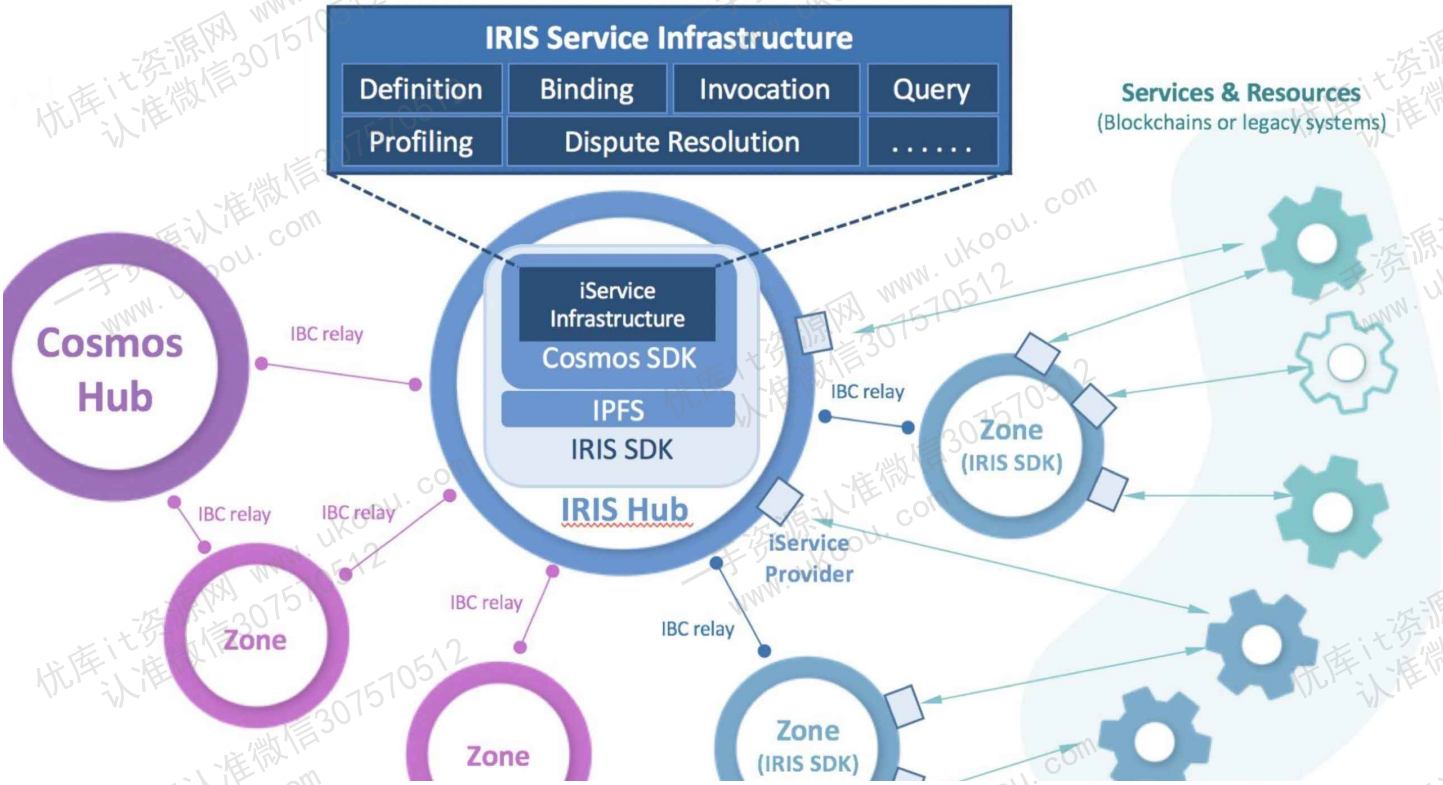
解释：IRIS 认为很多事情不应该放到链上或以智能合约的方式来解决，比如一些计算问题

解释：IRIS 认为跨链的不应该只是资产，而应该是各种各样的资源（那为什么还选 Cosmos? Cosmos 只支持资产跨链=_=） 2. 跨异构链的服务的互操作性

之前的达尔文网络面向的主要是游戏，而 IRIS 面向的是商业应用(其团队有一位曾在中科院计算技术研究所担任过研究员的博导站台)。IRIS 预设企业和 IRIS 以 Consumer(服务消费方)/Provider(服务提供方)的方式进行合作：IRIS 为企业和项目方提供了更易用的 SDK，来帮助他们利用分布式账本所带来的好处。

说完了 IRIS 的愿景，来看看其网络拓扑结构。

在拓扑结构上，IRIS 和达尔文网络差不多。IRIS 用 Cosmos SDK+ Tendermint 开发的，本身是一个网络，有 Hub，也能接入 Cosmos 生态作为其 Zone。当然 IRIS 是 Cosmos 生态下的，而达尔文网络是 Polkadot 生态下的。



iService 其实是 IRIS Services 的简称，其是用来弥合区块链世界与非链应用世界之间的鸿沟的。弥合的方式是协调 Off-Chain 服务的完整生命周期（从其定义、绑定（提供者注册）、调用到其治理（分析和争议解决），就是蓝色表格中的几个内容）。通过增强 IBC 处理逻辑以支持服务语义，IRIS SDK 旨在允许分布式业务服务在整个区块链互联网上可用。

另外，其网络包含三种角色：

消费者（Consumers）：通过向网络发送请求并从网络接收响应来使用 Off-Chain 服务。

提供者（Providers）：可以提供一个或多个 iService 定义的实现。并且通常充当位于其他公链和企业遗留系统中的基础服务和资源的适配器。提供程序监视并处理传入的请求，将响应发送回网络。通过将请求发送给其他提供者，提供者可以同时充当消费者。

Profiler：是代表 IRIS Foundation Limited（“基金会”）的特殊用户，IRIS Foundation Limited 是在香港成立的一家有限责任公司。该基金会将领导 IRIS 网络的建设。Profiler 是唯一被授权以配置文件模式调用 iService 的用户，该服务旨在帮助创建和维护目标提供者配置文件，供消费者选择合适的提供者。

4.4 其他项目

ChainX、Edgeware 是 Polkadot 生态中非常重要的两个项目，可以说是 Polkadot 生态中的一哥和二哥。基于 Polkadot 生态的项目在 Teams building on Polkadot 中有列出。这里暂时只作简要介绍。

ChainX 是基于 Polkadot 的 Substrate 的资产跨链项目。ChainX 通过去中心化的方式将链间资产进行统一转化，任何链只要建立与 ChainX 的连接，就可以与所有链进行资产互通。Polkadot 旨在做底层基础建设，实现任意消息跨链，而 ChainX 则专注于资产跨链。ChainX 的主网 Token 为 PCX。

Edgeware 是一个智能合约平台。一旦 Polkadot 上线主网，用户可以使用 Edgeware 在 Polkadot 上快速部署智能合约。支持 WebAssembly，用户可以使用 Rust 编写 Edgeware 智能合约，在 WASM 中执行合约相比大部分虚拟机更快、更高效。

六、共识机制 POW、POS

区块链是去中心化的，没有中心记账节点，所以需要全网对账本达成共识。目前有 POW、POS、DPOS、POOL 四种共识机制。

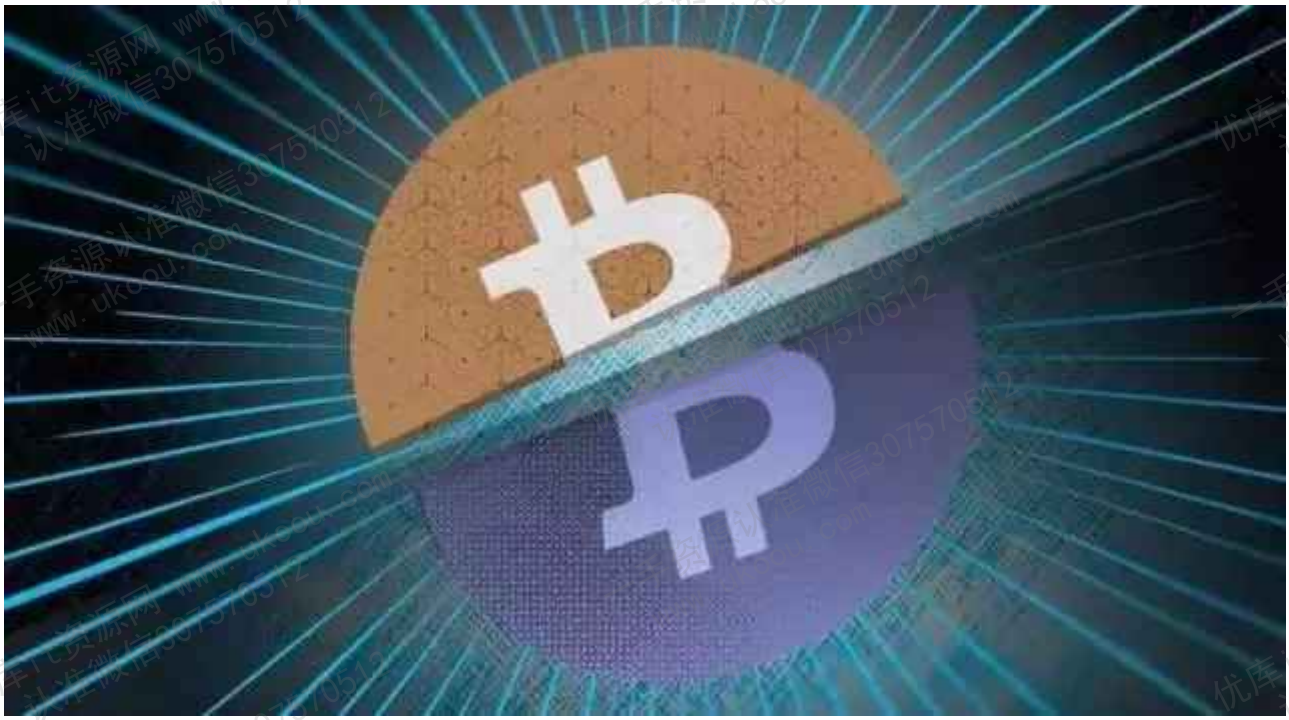
今天我们用通俗的例子来分析下其中的两种：POW、POS。

POW：有一道数学题非常难算

POW（Proof of Work），工作量证明，引入了对一个特定值的计算工作。

比特币采用的共识算法就是 POW，矿工们在挖一个新的区块时，必须对 SHA-256 密码散列函数进行运算，区块中的随机散列值以一个或多个 0 开始。随着 0 数目的上升，找到这个解所需要的工作量将呈指数增长，矿工通过反复尝试找到这个解。

在这其中，如果想要对业已出现的区块信息进行修改，攻击者必须完成该区块外加之后所有区块的工作量，并最终赶上和超越诚实节点的工作量。



用一个通俗的例子来说：

你上学的时候，班级里发生的行为需要被记在班级的一个大家公用的账本（区块链）上。

老师或者同学们用这个公用的账本进行记录，并且有一种专门用来支付这个账本上大家记录的、需要支付的代币，我们暂且把它叫做 Good 币。这些币可以兑换成钱。你们班级的公共账本不是一个大本子，而是由很多个小本子中间连接一条线组合成的。

每个小本子的启用需要进行一个数学运算，如果一个同学算出了某个小本子附带的数学题，就开启了一个新的小本子连着前面小本子，大家就会开始用新本子记账。

每个小本子开头都留一页，写上与其他小本子关联的信息、小本子的启用时间和开启这个小本子时算的数学题的答案。

因为同学们学习都很忙，如果没有报酬的话，就没有人会花费大量时间去班级的小本子上帮大家记账，因此老师做了一个规定：最先算出新的小本子附带的数学难题、开启小本子的人获得 Good 币，用币来奖励维持班级账本正常运转的同学。

一个期末，你得了奖，A 同学算出了一个新小本子——第 N 个小本子带着的数学难题的解，然后帮你得奖的信息记在了小本子上，A 同学获得了一笔奖励。

B 同学一直不喜欢你，他想把记录在小本子上的信息修改成 B 同学得奖，这样老师就会把奖金发给他。

B 同学开始计算第 N 个小本子上的数学难题，当他重新计算完第 N 个上面的数学题，其他同学已经计算出和第 N 个小本子连着线的第 N+1 个小本子的解了。

（因为 b 同学算的慢，其他同学只认最长链，所以 b 同学算的无效）

其他记账的同学根据最长链原则都跟在了第 N+1 个小本子的后面，所以 B 同学除非计算的速度变得很快，跟上另一条并超过，否则没办法将自己修改的错误信息的区块纳入整个账本系统中。

所以 POW 共识机制的优点之一：B 在攻击公共账本的时要耗费大量的时间精力和脑力，但结果却很难成功，所以如果他选择攻击，不仅得不到奖励，还会对自己造成大量的消耗，就会得不偿失——即降低不诚实节点的攻击意图。

但，不得不说的是，攻击存在成功的可能性，如果 B 同学说服班上超过 50%的同学一起承认错误他修改的错误的账本，那么被篡改的账本就会被达成共识。当然，就攻击这个公共账本而言，除非，超过 50%的同学用被 B 同学的一己私欲说服。

以这个例子来看，缺点也很明显，为了维护这个公共账本的运作，班级的同学花费了大量的时间来算这些哈希函数的难题，浪费了大量的时间和精力，表现在比特币上就是：花费了大量的电力，浪费了大量的能源。

POS：拥有的币越多，有记账权的概率就越大？

POS（Proof of Stake），权益证明，试图解决 POW 机制中大量资源被浪费的情况。这种机制通过计算你持有占总币数的百分比，包括你占有币数的时间来决定记账权。

预告：在该处会引起不适的可能有 1、2、3、4 段，请大家稍作忍耐……

在 POW 机制中，由于想要找到符合条件的 nonce 值往往需要大量的电力和时间成本，为了避免这种浪费，PoS 机制采用更快速的算法：

SHA256（SHA256（Bprev）,A ,t）≤balance(A)m

这其中，H 为某个哈希函数；t 为 UTC 时间戳；Bprev 指的是上个区块；balance(A)代表账户 A 额余额。

唯一可以不断调整得到参数是 t，等式右边 m 是某个固定的实数，因此，当 balance(A)越大，找到合理 t 的概率越大，网络中，普遍对 t 的范围有所限制，如可以尝试的时间不能超过标准时间戳 1 小时，也就是一个节点可以尝试 7200 次，来找到一个符合条件的 t。因此在 PoS 中，一个账户的余额越多，在同等算力下，就越容易发现下一个区块。

这实在是太复杂了，不知道该怎么理解……（哭脸）

我们还是用上一个“你上学的时候，班级里发生的行为需要被记在班级公用的账本（区块链）上，老师或者同学们用这个账本进行记录”例子来说，这个时候规则变了。

假设同学们经过前一阶段都已经持有一定数量的 Good 币，老师觉得大家为了争夺记账的机会，浪费的时间和精力都太多了，所以就修改了规定：

不采用之前那种特别难的数学题的方法。通俗的来说，根据你持有币的多少和时间长短给你发利息。

币龄（每个币每天产生 1 币龄）越高的人和持币越多的人越有机会得到启用小本子和帮别人记账的权利，记账又可以得到奖励。

在期末的时候持有更多币的人会有更多的奖励，所以同学们都很勤奋地去争夺记账权。

假设班级 Good 币的年利率是 5%（不同的币的年利率不一样，点点币的年利率是 1%；）

现在你们班级的 A 同学拥有的币最多，在 POS 机制下，每个币每天产生 1 币龄，A 同学拥有 100 个 Good 币，他已经持有这 100 个币 30 天，此时 A 同学的币龄为 30✖100=3000。每产生一个区块，币龄就会被清空为 0，每被清空 365 个币龄，就会从区块中获得 0.05 个币的利息。

A 同学拥有 3000 币龄，他通过计算启用了一个小本子，他得到的利息就是=3000✖5%➗365=0.41 个 Good 币。

通过持有币的数量和时间长短来决定记账的节点，这样就省略了竞争记账造成的资源浪费。如果在 POS 机制中想要发起攻击，必须要收集全部币量的 50%以上，不仅成本会非常大，并且执行难度非常高。

通过这些机制，使得区块链网络之间达成共识，以此来解决去中心化网络的信任问题。

七、IPFS

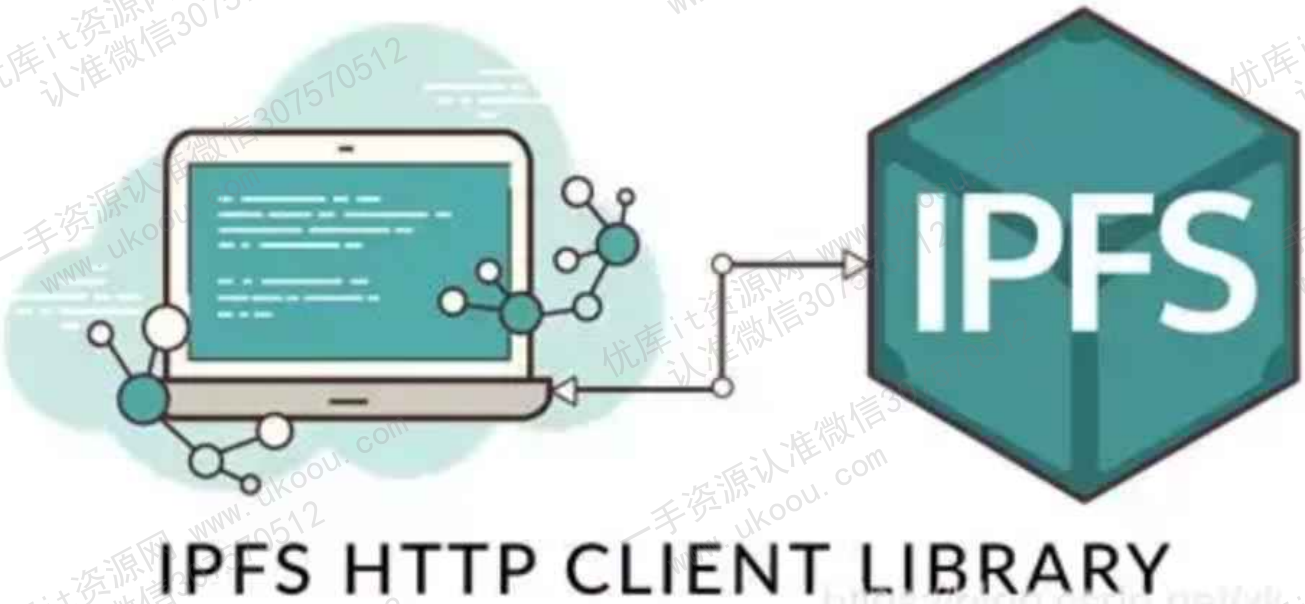
IPFS 项目介绍

IPFS 介绍：星际文件系统 IPFS（Inter-Planetary File System）是一个面向全球的、点对点的分布式版本文件系统，目标是为了补充（甚至是取代）目前统治互联网的超文本传输协议（HTTP），将所有具有相同文件系统的计算设备连接在一起。原理用基于内容的地址替代基于域名的地址，也就是用户寻找的不是某个地址而是储存在某个地方的内容，不需要验证发送者的身份，而只需要验证内容的哈希，通过这样可以让网页的速度更快、更安全、更健壮、更持久。

IPFS 是什么

星际文件系统 IPFS(The InterPlanetary File System),是一种点对点的分布式文件系统,可能大部分互联网用户对它都很陌生,不过就像很多人使用了十几年的超文本传输协议(HyperText Transfer Protocol,简称 HTTP),每次打开网页都需要输入也不清楚它具体是什么。

IPFS 也是一种底层协议,通过底层协议,可以让存储在 IPFS 系统上的文件,在全世界任何一个地方快速提取,不受到防火墙的影响,让用户访问数据的速度更快,更加安全,并且更加开放。



IPFS 是什么

互联网得以快速发展建立在 HTTP 协议上的,超文本传输协议(HTTP)的设计目的是保证客户机器与服务器之间的通信,打个比方,客户端的浏览器向服务器提交 HTTP 请求,然后服务器向客户端再返回响应,这是互联网诞生以来沿用至今的一种方式。但随着互联网用户量级的改变,以及越来越多的网络安全问题的凸显,互联网发展到了今天,HTTP 也开始逐渐暴露出不足。

HTTP 作为一种底层协议并不是非常安全的,它是一种明文传输协议,但它并无法加密数据。大部分的普通互联网用户其实都没有足够的能力对自己的浏览行为进行安全性的保护。因此当浏览器用户与网站进行 HTTP 链接时,两者之间传输的数据容易被窥视、窃取甚至篡改。

IPFS 是使用内容寻找地址,内容作为唯一的表示去进行访问,并且会提前检验这个标识是否被储存过,如果它之前已经被存储过了,那么就直接从其他节点读取,这样就不需要重复存储,解决了存储空间浪费的问题。

IPFS 的特性在应用层面让它与当下大热的区块链完美结合。区块链的本质是分布式账本,解决的传统账本的存储能力,可以在一定程度上为传统应用程序提供分布式缓存方案。

IPFS 的产生背景及应用

HTTP 超文本传输协议从 1999 年创立以来，对整个互联网行业的发展起到了无法替代的作用。但是中心化存储的互联网运行机制下，运营成本高、效率低、安全性差、数据易丢失等缺陷也是无法避免以及正在解决的问题。

为了改变现在互联网的种种弊端，斯坦福大学毕业的胡安·贝尼特于 2015 年创立协议实验室，发布了 IPFS（星际文件系统），目标就是取代 HTTP，成为下一代互联网底层通信协议。

IPFS(Inter-Planetary File System)即星际文件系统，是一种基于内容寻址、版本化、点对点的超媒体传输协议，集合了 P2P 网络技术、BitTorrent 传输技术、Git 版本控制、自证明文件系统等技术，对标 Http 的新一代通信协议。

IPFS 从根本上改变了用户搜索的方式。我们知道，通过 HTTP 浏览器搜索文件的时候，首先找到服务器位置，然后使用路径名称在服务器上查找文件，但是通过协议 IPFS，用户可以直接搜索内容。这里是怎么实现呢？

首先，IPFS 网络里的文件，会被赋予一个哈希值，这个哈希值类似于我们的身份证号，他是独一无二的，它是从文件内容中被计算出来的。

然后，当用户向 IPFS 分布式网络询问哈希的时候，它通过使用一个分布式哈希表，可以快速地找到拥有数据的节点，从而检索到该数据。简单来讲，就是以前我们是通过跳转多层网站才能找到一个文件，但是在 IPFS 上存储的文件，我们只需查询它的哈希值，便能快速找到。

IPFS 对于一些大的文件，它会自动将其切割为一些小块，使 IPFS 节点不仅仅可以像 HTTP 一样从一台服务器上下载文件，而且可以从数百台服务器上进行同步下载。所以，只要所存储的节点通电且网络正常，那么这个访问速度就可以非常快。

IPFS 和区块链有什么区别？

IPFS 和区块链的区别主要包括：

1. 区块链是一种记录交易数据并在区块中维护历史的技术。IPFS 旨在取代 HTTP，它是一种协议和网络，设计用于共享和存储媒体的点对点方法。

2. 区块链技术不适合存储大量数据。IPFS 由需要可公开访问的数据库的区块链应用程序使用，IPFS 将大量数据存储在不同的节点上，它使用区块链的通证经济（其激励层 Filecoin）来保持这些节点在线。

3. 在区块链上输入数据后; 它无法更新或删除，使用先前块散列函数的链接创建新块。在 IPFS 中，只有在另一个节点选择不重新托管时，才能删除网络数据。同时，IPFS 支持版本控制。

4. 区块链将数据存储在具有数据，哈希函数和先前哈希的块中。文件存储在 IPFS 对象中。这些对象可以存储高达 256kb 的数据，还可以链接到其他 IPFS 对象文件存储在 IPFS 对象中。这些对象可以存储高达 256kb 的数据，还可以链接到其他 IPFS 对象。

这些特性使 IPFS 成为分布式存储数据的理想场所，可以使用区块链技术进行参考和时间戳。

区块链

IPFS 不是区块链项目，但其激励层 Filecoin 是名副其实的区块链项目。

Filecoin 是运行在 IPFS 上的一个激励层，是一个基于区块链的分布式存储网络，它把云存储变为一个算法市场，代币（FIL）在这里起到了很重要的作用。代币是沟通资源（存储和检索）使用者（IPFS 用户）和资源的提供者（Filecoin 矿工）之间的中介桥梁，Filecoin 协议拥有两个交易市场—数据检索和数据存储，交易双方在市场里面提交自己的需求，达成交易。IPFS 和 Filecoin 相互促进，共同成长，解决了互联网的数据存储和数据分发的问题，特别是对于无数的区块链项目，IPFS 和 Filecoin 将作为一个基础设施存在。这就是为什么我们看到越来越多的区块链项目采取了 IPFS 作为存储解决方案，因为它提供了更加便宜、安全、可快速集成的存储解决方案。

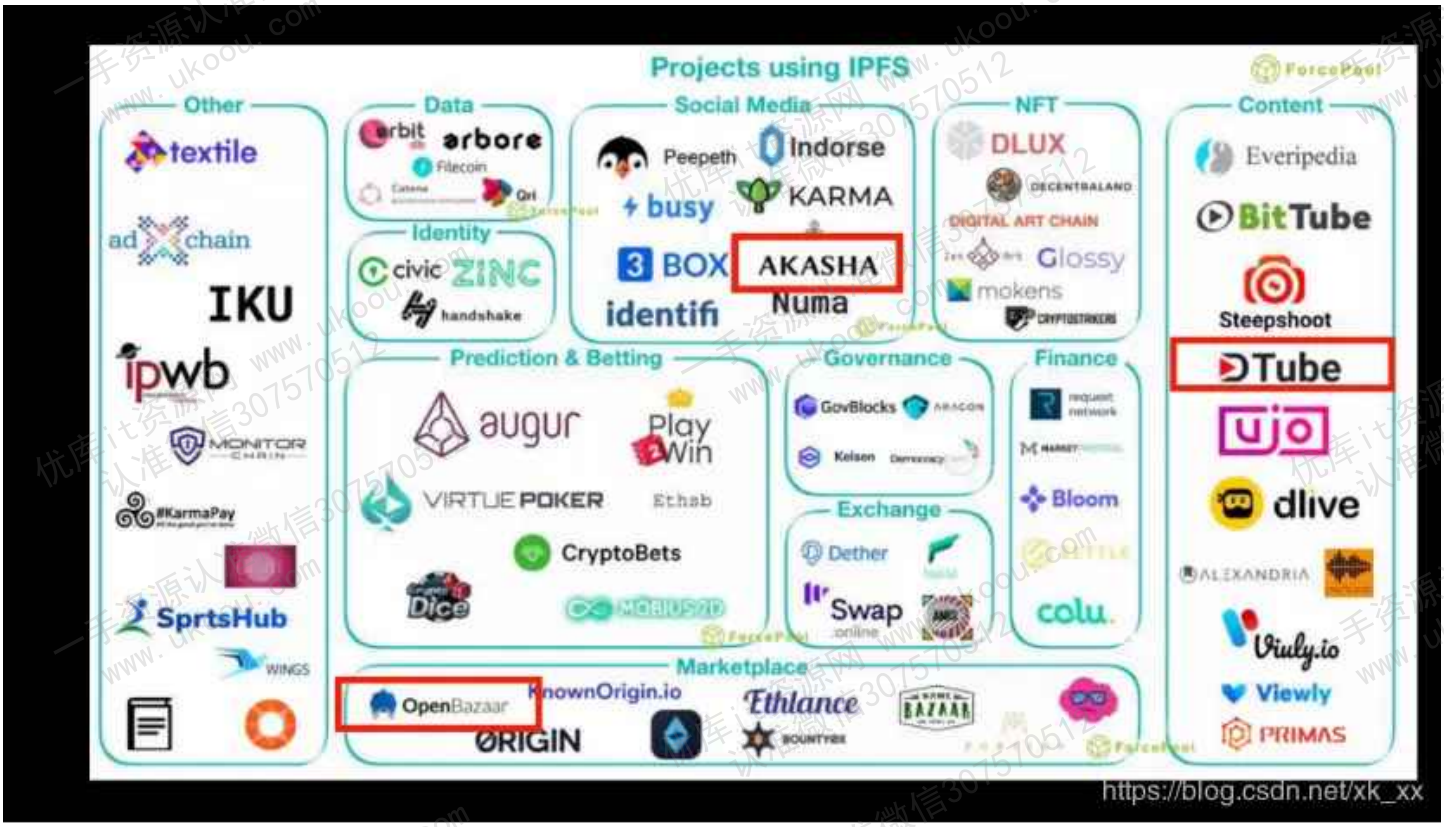
IPFS 为区块链带来什么变化?

区块链的诞生本是为了做到去中心化，在没有中心机构的情况下达成共识，共同维护一个账本。它的设计动机并不是为了高效、低能耗，抑或是拥有可扩展性（如果追求高效、低能耗和扩展性，中心化程序可能是更好的选择）。

IPFS 与区块链协同工作，能够补充区块链的两大缺陷：一是区块链存储效率低，成本高；二是跨链需要各个链之间协同配合，难以协调。

IPFS 生态

应用层 Dapp



采用 IPFS 技术的 DAPP 示意图

DAPP 示例

1. Openbazaar 是个开源的开放集市（c2c），没有中心服务器，靠的是分布式节点自动维护，交易付款用 BTC，交易双方是匿名；网站没有没有域名，它并不是使用域名访问的，而是使用类似区块链技术的 onename。

在 1.0 版本，OpenBazaar 被称之为“黑市”，那时没有应用 IPFS，利用 ZeroMQ 来实现 P2P 交易，把交易的手续费作为红利给到用户，同时它用比特币作为支付渠道而轰动一时，用户数量在短时间内迅速提升。

在 2.0 版本发布后，加入了一层审查机制，同时支持了比特币之外的 BCH 等数字货币，并且整合与重构 IPFS，取代了之前的 ZeroMQ。

现在，集市上众多的商店在没有用户上线的情况下，也可以在主机上就被运行。以前必须同时登陆才可以交易，现在利用 IPFS 相当于实现了离线店铺，这意味着，访问你店铺的人越多，店铺数据被复制越多，有利于优质的店铺宣传和推广，这也是一定意义上的价值回归。

2. PeerPad 是协作的实时编辑器，它不使用第三方，所有参与节点直接对话，不需要中央服务器。同时 Peerpad 开源，展示了开发者如何使用 IPFS 建立自己的无服务器的、实时的、离线优先的多人协作的分布式应用程序，由协议实验室和 IPFS 社区建立。可实现四种功能：

1. 会议笔记

无论是使用纯文本、Markdown 还是富文本，你都可以实时地与同事分享会议记录。

2. 协作或共享代码片段

Peerpad 有一个内置的代码编辑器，可以在编辑同一个文件时使用它与同事协作。

3. 写文章并分享

您可以发布一个 pad 的快照到 IPFS，使其在 internet 上可用。通过共享解密内容的读取密钥来选择与谁共享。

4. 与多个用户同时协作

Peerpad 可以与许多用户同时修改文档，实时处理彼此的变化。

IPFS 应用层目前还多为当前互联网商业业务突出的产品的区块链版，有音视频娱乐服务、电子商务等，但结合 IPFS 特性及中心化社会的痛点，未来但凡涉及‘数据量大’、‘带宽压力’、‘数据安全’、‘文件版本’等基本诉求的业务，皆向去中心化甚至 IPFS 靠拢，在这里做个窥探性前瞻。

网络激励层–Filecoin

目前 IPFS 激励层应用在国内外有多个项目在探索，最受关注的还是协议实验室自搭建的 Filecoin（文件币），它的出现旨在提升 IPFS 协议在全球范围内被应用的广度，这个普及推广的过程需数年甚至数十年，Filecoin 自身也形成了一个应用生态，包含了存储网络、经济体系、技术架构等。

IPFS 与 Filecoin 的关系

IPFS 星际文件系统（InterPlanetary File System ），是个旨在创建持久且分布式存储和共享文件的网络传输协议。它是一种内容可寻址的对等超媒体分发协议。

我们现在常用的这些 APP、网站、朋友圈的数据都是放在中心化的服务器集群中存储的，然后通过 URL、URI、域名系统定位资源去访问，而 IPFS 呢，不是基于这种域名寻址，而是内容寻址，它会从一个资源的内容计算出一个哈希值，这个值直接反应这个资源的内容。一个 IPFS 客户存储一个大文件资源到 IPFS 网络，当该资源较大时 IPFS 通过对资源文件进行分片，分别计算哈希，并通过 Merkle DAG（Git 数据格式）对该资源文件进行组织，每个分片可能存在一个节点或多个节点，并且可能是多个副本来保证某些节点失效时还可以在其他节点取得文件分片。

Filecoin 是一个去中心化存储网络，也叫做 Filecoin 的区块链，Filecoin 的代币名称为 FIL。Filecoin 与 IPFS 是两个项目，IPFS 是底层协议。FIlecoin 区块链中的矿工可以通过为客户提供存储来获取 FIL。相反的，客户可以通过花费 FIL 雇佣矿工来存储或分发数据。

Filecoin 是基于 IPFS 进行 ICO 的另外一个项目，本质上来说 Filecoin 是对 IPFS 网络的一个激励层 IPFS 可以理解为一个 BT 软件，那么 BT 软件多年来一直未解决的问题就是如何激励资源的贡献者，如何激励参与者提供更好的磁盘、更好的网络，提供给使用者更好的使用体验和稳定质量。

Filecoin 去中心化存储网络 (Decentralized Storage Network，简称 DSN)，在这个网路中准备构建两个市场分别为「存储市场」和「检索市场」，以此来奖励存储矿工提供更好质量的存储服务，同时在检索市场激励网络较好或响应性能较好的矿工获取奖励。

附录

区块链概念

- 区块链（Blockchain）：一种分布式账本技术，通过加密方法保障数据安全、完整和不可篡改性。
- 加密货币（Cryptocurrency）：利用区块链技术创建的一种数字或虚拟货币，通过加密保障安全。

- 智能合约（Smart Contracts）：存储在区块链上的自动执行合同的代码，当预定条件满足时自动执行合约条款。

中心化与去中心化

- 中心化（Centralization）：数据或资源控制集中在单一实体或位置。
- 去中心化（Decentralization）：去除中央控制权，数据或资源分布在网络中多个节点。

区块链类型

- 公链（Public Blockchain）：任何人都可以参与的开放式区块链网络。
- 联盟链（Consortium Blockchain）：受限的区块链网络，仅允许特定组织的成员参与。

区块链工作流程

- 生成区块：收集交易数据，形成区块。
- 共识验证：通过某种共识机制验证区块的有效性，以达成网络共识。
- 账本维护：将验证通过的区块添加到链上，更新区块链数据库。

区块链体系结构

- 网络层：关注区块链网络的基础通信方式，如对等网络（P2P）。
- 数据层：定义了区块链的数据结构和存储方式，包括信息模型、加密机制。
- 共识层：解决在不可信环境下如何实现账本数据全网统一的问题。
- 控制层：提供了区块链与上层应用之间的接口和逻辑控制功能。

共识算法类型

- 工作量证明（Proof of Work, PoW）：通过解决复杂计算问题来达成共识。
- 权益证明（Proof of Stake, PoS）：根据持币量或年龄来选择创建新区块的节点。
- 拜占庭容错（Byzantine Fault Tolerance, BFT）：允许网络中有一定比例的节点失败或恶意行为仍能达成共识。

比特币

- 比特币（Bitcoin）：最早的非许可链加密货币，依靠区块链技术实现去中心化的资金交易系统。

以太坊

- 以太坊（Ethereum）：支持智能合约的开源区块链平台，允许开发者构建和部署去中心化应用（DApp）。

网络层技术

- Gossip 协议：一种网络协议，通过节点间的简单信息传播机制保证网络中的信息能够迅速且广泛地分散。
- Diffusion 协议：用于改善网络的匿名分析能力，通过随机的路径传播信息，增强数据传输的安全性。
- Tor（The Onion Router）：一种匿名通信网络，通过多层加密的方式实现用户的匿名上网。

数据层技术

- UTXO（Unspent Transaction Output）模型：比特币区块链中的交易输出模型，代表尚未被消费的交易输出。
- Merkle Tree（MKT）：一种数据结构，用于高效且安全地验证内容的完整性。
- ECDSA（Elliptic Curve Digital Signature Algorithm）：一种使用椭圆曲线密码学的数字签名算法。

共识机制

- PoW（Proof of Work）：一种共识机制，要求节点完成一项工作以证明其对网络的贡献，通常涉及计算复杂的数学问题。
- GHOST 协议：用于提高区块链网络中的交易吞吐量和确认速度，允许非主链区块的某些信息被纳入到主链的共识过程中。

控制层技术

- 智能合约（Smart Contract）：存储在区块链上的代码，当预设条件被触发时自动执行合约条款。
- EVM（Ethereum Virtual Machine）：以太坊虚拟机，执行智能合约的运行环境。
- Solidity：一种高级编程语言，专为编写智能合约设计，运行在以太坊虚拟机（EVM）上。

跨链技术基本概念

- 跨链技术：允许不同区块链网络之间安全可信地传输数据（如资产数据）并在接收链上产生预期效果的技术。
- 公证人机制（Notary schemes）：通过引入第三方中介（如交易所）来验证和转发跨链消息的机制，适用于异构链的跨链交互，但存在中心化风险。
- 哈希锁定（Hash-locking）：使用哈希时间锁定合约（HTLC）技术，结合哈希锁和时间锁，实现交易的安全性和原子性。主要用于资产交换，不能直接实现资产或信息的转移。
- 分布式私钥控制：通过分布式密钥生成（如门限密钥共享）技术，提高跨链资产交换过程中的安全性，防止单点作恶。

具体跨链技术

- 侧链&中继链技术：通过建立侧链（与主链并行的区块链）和中继链（连接多个侧链和主链的中心链）实现跨链互操作性。侧链技术使得资产能够在不同区块链之间流动，而中继链技术则进一步扩展了跨链交互的范围和效率。

主要跨链项目

- Cosmos：采用中继链架构，通过IBC（Inter-Blockchain Communication Protocol）协议实现区块链间的互操作性。
- Polkadot：通过中继链和平行链（Parachain）架构实现跨链互操作，支持任意类型的跨链交互。
- ETH.Plasma：以太坊的Layer2扩容方案，通过在主链外进行交易处理来提高系统吞吐量。
- Polkadot.Darwinia：基于Polkadot技术构建的跨链游戏网络，支持游戏资产和操作的跨链交互。
- Cosmos.IRIS：旨在解决链外计算和资源集成以及跨异构链服务互操作性问题的跨链项目。

IPFS 基本概念

- IPFS（InterPlanetary File System）：一个面向全球的、点对点的分布式版本文件系统，目标是补充或取代当前互联网的超文本传输协议（HTTP），实现更快、更安全、更健壮和更持久的文件存储、访问和共享方式。

IPFS 组件与技术

- 内容寻址（Content Addressing）：IPFS 用文件内容的哈希值作为文件的地址，而不是传统的基于域名的地址。这意味着用户查找的是存储在某处的内容，而非某个特定的服务器地址。
- 分布式哈希表（Distributed Hash Table, DHT）：一种用于高效数据查找的技术，IPFS 通过 DHT 快速定位存储内容的节点。
- Merkle DAG（Directed Acyclic Graph）：IPFS 使用 Merkle DAG 来组织数据，每个文件或数据块都有一个唯一的哈希，保证了数据的完整性和唯一性。
- BitTorrent：一种 P2P 文件共享协议，IPFS 在文件传输层面借鉴了 BitTorrent 的技术，实现了高效的文件分发。

IPFS 与区块链的关系

- Filecoin：IPFS 的激励层，一个去中心化的存储网络，通过区块链技术激励用户提供存储空间，使用 Filecoin 代币（FIL）作为交易媒介。

应用案例

- OpenBazaar：一个去中心化的市场，使用 IPFS 来存储商品信息和用户数据，通过去中心化方式保证交易的安全性和匿名性。

- PeerPad：基于 IPFS 的实时协作编辑器，允许用户无需中心服务器即可共同编辑文档，保证了数据的即时同步和安全性。

IPFS 的意义

- 去中心化存储：IPFS 通过去中心化的方式存储文件，解决了中心化存储的诸多问题，如运营成本高、效率低、安全性差、数据易丢失等。
- 高效文件分发：IPFS 允许同时从多个节点下载文件片段，提高了文件传输的效率和可靠性。
- 持久性存储：IPFS 的设计确保了数据的持久性，只要在网络中有节点存储着文件的副本，该文件就可以被访问。