**上海大学“区块链”课程论文考试**

**Mirror项目分析**

姓名：陈晓奕 学号： 21726095

**字数：4644**

**摘 要：Mirror 去中心化组织**

随着区块链技术的发展，去中心化的概念开始拓展到各个方面：金融、游戏、虚拟货币，甚至是组织形式。去中心化组织DAO，也称分布式组织，就是这一技术发展下的产物。区别于传统公司形式的集权管理，DAO强调社区治理，依托于智能合约以更直接和智能的方式进行资源的分配。目前，以太坊上有关DAO的项目有很多，大致可以分为八类：孵化器DAO、协议DAO、投资DAO、服务DAO、收藏DAO、社交DAO、媒体DAO、基础设施栈DAO。本文选取基础设施栈DAO中的一个项目：Mirror为例，对其经济模型和技术模型两个角度进行分析，归纳出Mirror现存的优点和缺陷，进而对于投资该项目提出相应的建议。

**关键字：去中心化组织 Mirror 经济模型 技术模型**

**论文评语：**

成绩： 任课教师：吴建刚

随着区块链技术的发展，去中心化的概念开始拓展到各个方面：金融、游戏、虚拟货币，甚至是组织形式。去中心化组织DAO，也称分布式组织，就是这一技术发展下的产物。DAO的全称是Decentralized Autonomous Corporations，传统的治理是以公司为形式的，而DAO是以类似于社区的方式来运营的。周卫华、康伟婷（2022）基于区块链的组织特征：分布式组织结构、加密信任与共识机制、并行生产、社区互动，提出区块链的治理机制:决策机制、执行机制、激励机制、监督机制。

和传统的公司集权式治理不同，DAO强调社区治理，依托于智能合约以更直接和智能的方式进行资源的分配。

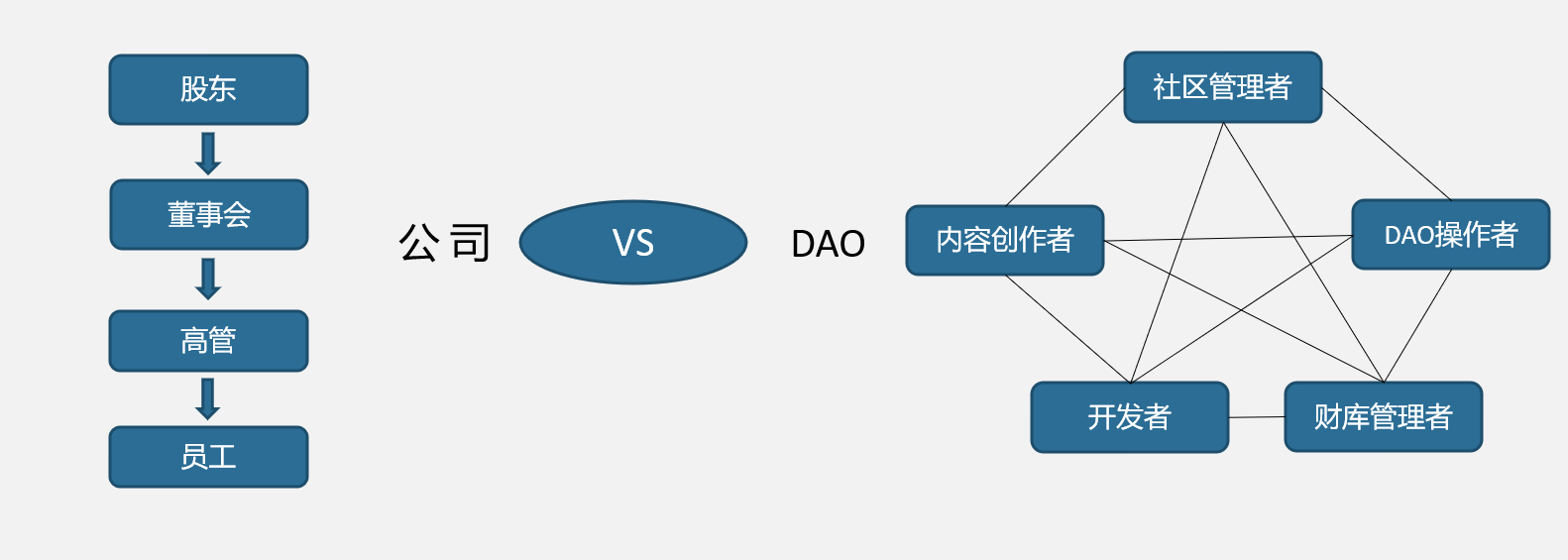


图1 DAO与公司治理架构区别

目前，以太坊上有关DAO的项目有很多，大致可以分为八类：孵化器DAO、协议DAO、投资DAO、服务DAO、收藏DAO、社交DAO、媒体DAO、基础设施栈DAO。本文选取基础设施栈DAO中的一个项目：Mirror为例，对其经济模型和技术模型两个角度进行分析，归纳出Mirror现存的优点和缺陷，进而对于投资该项目提出相应的建议。

1. 经济模型分析
   1. 项目、创始人及团队简介

Mirror 类似于 Medium，通过为创作者提供代币发行工具来帮助创作者众筹，基于以太坊运行，任何人都可以通过 Mirror 链接价值。2020年11月16号，Mirror 由 a16z crypto 合伙人 Denis Nazarov 发起Beta版，2021年1月7号推出简化可实行产品。2021年1月29号，Snapchat前软件工程师在Mirror上发起首次众筹，1小时内以10 ETH超额完成众筹目标。2021年6月2日，Union Square Ventures （USV）以1亿美元估值投资。

* 1. 项目想要实现什么

Mirror想要实现的目标主要有两个：一是采用Arweave区块链实现内容的永存，颠覆现有的内容创作平台，做到内容的不可删除；二是围绕每个不同内容，通过众筹代币分发，形成不同的DAO组织，以推动链上的社区治理，用智能合约的执行来代替传统治理形式中的人的角色作用。

为了实现上述两个目标，目前Mirror上有10个功能模板,如下表所示：

表1 Mirror功能模块

|  |  |
| --- | --- |
| **Mirror10个功能模块** | |
| NFT 展示 | 目前支持图片、音讯、影片和文本 NFT 的插入。Mirror 支持 EthBlock.art、Foundation、Rarible、SuperRare和 Zora 平台的 NFT。 |
| 众筹模块 | 任何人都可以通过 Mirror 发起或参与众筹。支持者可以存入 ETH 来资助发起者并换取 Token。 |
| 拍卖模块 | Mirror 支持使用储备拍卖来拍卖 NFT。保留拍卖配置有两个主要参数：保留价格和拍卖持续时间。 |
| 链接及预览 | Mirror 显示的是基于 OpenGraph 标签通用标准的所有链接的渐进式增强预览。 |
| Twitter 预览 | 通过任意一个推特 URL 可插入一条单独的推文或整个 thread。 |
| 视频类多媒体 | 通过插入一个外部托管视频文件的链接来插入一个mp4 视频。还可以通过设置相关的查询参数来设置自动播放、静音、循环和控制。 |
| 分账 | Mirror 上的分账是一种自动与多个实体分享你产生的价值的方式。分账是一个应付的智能合约，将价值传送到以太坊的多个地址。分账可以作为奖励你的合作者、激励你的人的一种方式，或捐赠你的作品的收益。 |
| 多版 NFT | 多版 NFT 是创作者以固定价格铸造有限供应的相同的 NFT 的一种方式。 |
| 多版文章 | 多版文章是一种通过限量版 NFT 使 Mirror 上的写作具有收藏价值的方式。 |
| Token Race | Mirror 支持创建 Token Race，这是$WRITE Race 的衍生品。代币竞赛是一个简单的基于期限的治理工具，允许上传提案，并允许社区根据他们在某个时间点持有的特定 ERC20 代币或 ERC721 代币（NFT）。 |

* 1. 为什么需要分布式记账

Mirror想要实现内容的不可篡改，而传统的互联网平台由于内容存储在数据库，由中心化的企业平台操控，因此，要想信息不被篡改和删除，需要分布式记账。Mirror用到的是Arweave区块链技术。Arweave是一种新型的存储方式，用可持续和永久的禀赋来支持数据，使用户和开发者能够永远存储数据。Arweave 设计了一个全新的共识机制——访问证明Proof of Access（在本文的2.1处会详细介绍该机制如何实现分布式记账）。因此，传输数据时就会获得更多的资源和连接权限，这样就用经济手段，促进了数据的分享效率。不仅能达到数据的均衡分布，而且能够真正实现去中心化的存储。

* 1. 代币机制

Mirror平台里有众多不同的代币。围绕每一个内容项目，Mirror通过众筹代币的分发，形成了一个个利益相关的DAO（去中心化自治组织）。其中作者作为生产者，通过发布内容众筹挣取启动资金，并保留部分 NFT 份额；投资者通过投资NFT持有文章部分所有权，所有权以DAO的代币份额来体现。每一次NFT的转手都可为全部代币持有人带来相应比例的收益，包括作者和各投资者。

除了每个内容项目都有属于自己的代币系统，Mirror还有一个代表平台自身的代币$WRITE： 2021年3月，团队开启了一个竞赛（Mirror's $WRITE Race），每周投票，获得票数最多的10个作者每人获得一个$WRITE。只有得到这个代币的人才能开通Mirror账号。一直到2021年8月1日的4个月期间，有200名大V抢到了$WRITE。大V们燃烧$WRITE开通Mirror账号然后在Twitter上炫耀。这时市场上完全没有$WRITE流通，$WRITE相当于Mirror账户的邀请码。2021年8月19号，Mirror空投总量302枚$WRITE给5千名社区活跃用户。2021年10月6日，Mirror.xyz 正式对外开放。开通Mirror账号不再需要燃烧$WRITE。但$WRITE并没有消失，而是功能上有了变化：燃烧1枚$WRITE可以成为Mirror DAO成员，同时获得一个Mirror子域名。Mirror DAO 它本质上是一个和Mirror团队保持密切联系的精英用户组织，有一些Mirror社区治理的权力，比如Mirror DAO可以提名投票评选Mirror生态的优秀项目，奖励1枚$WRITE。因为每期只有个位数项目入选，所以$WRITE还是非常稀罕，而且，只有燃烧1枚$WRITE才能获得一个Mirror DAO成员名额。$WRITE代币的新一次功能变化是在2021年11月底，Mirror Spotlight启动，Mirror DAO成员提名和投票，从每周阅读量最高的原创文章作者中选择并奖励$WRITE。平台代币$WRITE从一开始的平台账户入场券，逐渐演变成投票权和核心玩家俱乐部的入场券，以吸引更多玩家的加入以扩大平台的内容量。

1. 技术模型分析
   1. 共识机制

由于Mirror是基于Arweave技术上的应用，其共识机制采用的是一种全新的机制：访问证明Proof of Access。它类似于工作量证明，但它有一些重要的区别。与工作量证明不同，访问证明的方法不依赖于前一个区块来验证交易。相反，它使用链中的前一个块和随机块。将这种方法与他们的块编织结构相结合，这是一种构建区块链的新方法。这样，矿工就不需要整个区块链，只需要一个称为“召回区块”的现有区块。然后，此召回块中的事务将针对当前块进行哈希处理，以生成新块。当矿工解决问题并找到合适的哈希值时，他们可以与网络共享新区块和召回区块。具体做法如下：每次出新区块的时候必须同时验证一个以前的区块。这个以前的区块数随机产生，只有拥有随机区块的节点才能进行 POW 出块。因此，每个节点都必须保存够多的区块，才能有机会参与 POW 出块得到报酬。由于存储有成本，会随着数据的指数级增长，如果每个节点都要保存所有区块的话，会使得运行很难。随机区块的存在可以调节每个节点所保存的数据量，每次对外发布新区块时，只需要给出一个类似区块头的哈希值，以及交易发生的钱包地址列表，然后每个节点通过这个列表从自己的交易池里把交易找出来验证。如果跟哈希值一致，验证就成功，区块就可以被写入自己的本地数据库。每个节点都可以跟相邻的节点分享文件，并对相邻节点的表现进行评分。如果从相邻节点那里得到的可靠的文件越多，评分就越高。其他成员可以验证新块是否有效，即使没有召回块也是如此。对于平台用户来说，相比于工作量证明机制，它消耗的能量要少得多，速度更快，更便宜。

* 1. 帐户机制及智能合约

Mirror中所有条目都由用户的签名密钥签名。这是一个非以太坊密钥对，不包含任何直接经济价值，然后将签名连同已签名的摘要以及进入摘要的内容一起发布到 Arweave。签名密钥本身被放入声明作者权的消息中，然后由作者的以太坊地址签名。所有这些信息与条目的内容一起存储在 Arweave 上——用于每个条目和更新。因此，任何人都可以验证条目是否由给定的以太坊帐户创作。

智能合约的运行通过提案人和众筹投资者享有的代币比例对应投票权，提案人上传执行代码并发起投票，通证持有人可以在链上投票，这共同构成治理合约，当投票通过后自动执行代码实现功能迭代，形成功能合约。但这种形式下执行较慢，且油费较贵，导致有些内容并未上链。因此，智能合约目前还未能覆盖所有内容，需要用户、通政持有人和项目团队的链下治理来补充。

* 1. 隐私保护和身份验证

Mirror使用 ENS 向作者提供域所有权，作者在入职期间通过销毁邀请$WRITE来声明此所有权。该过程涉及与 $WRITE ERC20 代币合约进行交互，该合约授权 ENS 注册商合约在注册 ENS 标签之前销毁代币。

* 1. 现有技术文档及代码评价

Mirror的技术架构满足的以下5个特点：

帖子内容不得集中。使用Arweave数据存储协议来存储用户内容。Arweave 在上传时提供一次性数据的永久存储。 发布到 Arweave 的数据包括检索出版物的所有条目（包括所做的任何更改）和验证作者身份真实性所需的所有信息。

阅读体验不需要信任Mirror。所有条目都由用户的签名密钥签名。这是一个非以太坊密钥对，不包含任何直接经济价值。然后将签名连同已签名的摘要以及进入摘要的内容一起发布到 Arweave。签名密钥本身被放入声明作者权的消息中，然后由作者的以太坊地址签名。所有这些信息与条目的内容一起存储在 Arweave 上——用于每个条目和更新。因此，任何人都可以（并且相当容易）验证条目是否由给定的以太坊帐户创作。

Mirror不得拥有作者的域名。使用 ENS 向作者提供域所有权，作者在入职期间通过销毁邀请令牌（称为 $WRITE；期待更多信息）来声明此所有权。该过程涉及与 $WRITE ERC20 代币合约进行交互，该合约授权 ENS 注册商合约在注册 ENS 标签之前销毁代币。

Mirror 不会尝试在浏览器中存储以太坊私钥。通过使用与以太坊实现不同的签名方案（使用的是 NIST 曲线P-256），因此根本不可能让密钥“保持经济价值”， 并完全回避一个主要问题。在最严重的威胁模型（例如被盗的计算机）下，最坏的情况是作者身份欺诈。通过使用不可提取属性生成密钥，并将其存储在 IndexDB 中。这意味着根本无法导出私钥——私钥只能用于在加载它的网页上 签署内容，而 IndexDB 会阻止它被加载到 mirror.xyz 之外的任何网站上。

奖励：不使用电子邮件密码注册。由于有签名密钥和基于签名的真实性模型，不需要登录会话，也没有任何东西可以通过电子邮件恢复。将来，允许电子邮件通知和电子邮件摘要可能会很有用，但现在有趣的是，使用 Mirror 不需要电子邮件确认。这是 Zerion 和 Zapper 等应用程序使用的原生加密方式，也是网络身份验证的未来。

Mirror技术架构设计如下图所示：

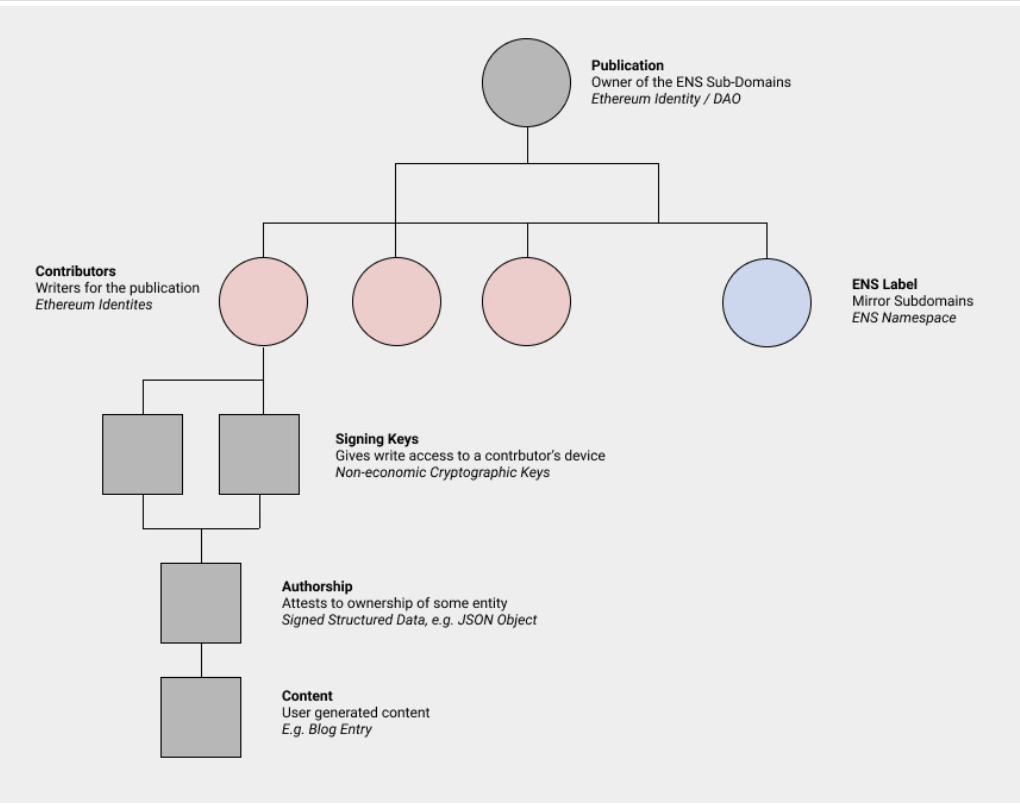


图2 Mirror目前技术架构

1. 项目未来
   1. 未来规划及激励机制

Mirror 的激励机制目前有三种：一是基于稳定币的薪资，向维护者支付约定的USTD，但支付的薪资需要经过投票决议；二是赏金，这种方式主要用于某些一次性的项目而非长期的项目，因此区别于第一种机制，项目参与者可以由于开发、运营、策展（构建创作者引流平台）、资源合作等角色的实施得到相应的报酬。三是小费制的激励，以月为单位进行预算，所有的贡献者都有额定的积分用于成员之间的互相评判，最终贡献者可依据得到他人评判的积分的百分比去分配预算。

* 1. 现有社区及应用评价

目前Mirror依据内容的不同，大致可以划分15个社区：技术、金融、商业、投资、文化、健康、音乐、宗教、科学、历史、运动、哲学、政治、教育、旅行，每个社区都有相应的DAO组织，主要做和开发者沟通、帮助内容发布者引流、不同DAO之间进行资源合作和运营等工作。

Mirror相对于传统的互联网应用有以下几个优点：首先，Mirror上发布的内容不是存储到数据库，而是采用分布式记账技术，使得平台上的信息难以被篡改和删除；其次，相对于传统互联网企业，没有订阅、阅读量和推荐系统功能，个人隐私能够得到保护；其次，创作者的收入来源于众筹，创作者不会因此有“恰饭”的内容发布，更能够激励用户的真实内容表达；最后，它的众筹功能创造了给新的组织管理方式，减少了第三方代理成本和人的主观决策因素。

但Mirror目前存在的问题主要有四点：由于没有审核的机制，关于平台是否会成为违法聚集地，隐私和权益如何保护的问题受到质疑，尽管平台只提供工具，数据内容由创作者个人承担，但目前区块链的加密性和在某些国家地区的政策法规限制，导致发布的内容难以追溯到具体的人。多媒体内容，交易的内容是存储在数据库上，和OPENSEA一样，还未上链，存储成本由MIRROR承担，但目前成本较高。鉴定身份存在假冒问题，目前是链接ENS 和TWITTER，需要技术基础设施的解决。用户将内容转换成NFT需要缴油费，但油费较贵且无创作者引流机制，创作者原始增长困难。

表2 Mirror与Web2.0平台企业对比

|  |  |
| --- | --- |
| **Mirror** | **Web2.0平台企业** |
| 提供DAO基础设施平台，可以在上面搭建任何DAO，DAO内容的管控靠社区 | 管控并审核社区发布内容 |
| 分布式记账技术使得信息难以篡改和删除，使得少数群体的声音也可以被听见 | 中心化的数据库管理下信息被企业管理，导致社区平台很可能成为资本的信息传递工具 |
| 没有订阅、阅读量、推荐系统功能 | 平台算法定制化推送 |
| 没有引流机制，创作者可能从其他社交平台引流 | 具备引流机制，创作者在平台上可积累原始粉丝 |
| 创作者的收入来源于众筹者的投资，使得创作内容与推送用户的期待不会有较大差异 | 创作者的收入来源于品牌方营销费，免不了恰饭行为，存在与粉丝期望内容差异较大的可能 |

* 1. 项目投资分析

从该项目的理念和愿景来看，Mirror是一个不错的项目，能够实现将区块链技术拓展到社交媒体上，带来全新的治理形式，能够解决现阶段中心化平台存在的某些问题。

从经济模型来看，由于该平台不存在创作者引流机制，创作者迁移成本较高，吸引更多的外部作者燃烧代币需要不断的拉新。除非该平台的去中心化机制能够吸引到足够的用户，使得本身具有足够的流量，否则大多数的创作者不会舍弃现有的互联网平台，那该项目有可能仅变成一小部分人的参与与投机，变相变成一种“庞氏骗局”。从技术模型来看，身份验证由于底层技术原因，仍存在一定的问题。此外，区块链项目下的油费过高也是通病。

综上所述,由于该项目目前仍处于发展初期，经济模型和技术模型仍待时间验证和解决，本文分析对于该项目投资持谨慎态度，暂时不建议投资。

附1：

# 1、请说明发起比特币交易到交易确认的整个过程。（说明中请包含：交易者如何产生地址、如何对交易签名、如何发出交易、矿工如何接受交易、如何选出记帐人、为何会使用矿池挖矿、矿池挖矿的过程、为何可能会有软分叉、为何限制区块大小、如何控制区块出块时间、区块中包含的内容，并讨论为什么使用UTXO设计）

1.1比特币系统产生地址大致可分为四步：首先，生成一个32字节的随机数作为私钥；其次，使用椭圆曲线算法加密，将私钥生成公钥；然后，对公钥进行一系列的哈希计算生成公钥摘要；最后，使用Base58编码对公钥摘要进行编码得到地址。以上前三步都不可逆，最后一步是可逆的。

1.2对交易签名：付款人使用特定算法生成公钥和私钥，私钥自己保留，公钥对外发布；当付款人想要发出已对某人付款的消息时，将自己的私钥进行加密，私钥加密后的密文可作为对交易签名。

1.3发出交易：付款人将交易信息，附带自己的公钥和签名发布到网络：付款人已向某人转账X BTC，请查收。我的公钥是……。签名：……。

1.4矿工接收交易：接收到信息的矿工，通过公钥解密数字签名，对交易信息进行验证，如果验证结果一致，则证明这笔交易确实由发起方地址发出，且交易信息未经修改，否则交易无效。

1.5选出记账人：比特币采用工作量证明法，记账人通过运算一道很大的数学题并能最先解出，就采用其账本，解题的过程也叫“挖矿”。

1.6矿池挖矿过程：挖矿过程分为三步：首先，构建区块，将要写入区块交易信息组成交易列表，通过梅克尔树算法把交易列表信息生成梅克尔根哈希。其次，把梅克尔根哈希、难度值等相关字段组装成区块头，把区块头80字节数据作为工作量证明的数据输入。最后，通过变更区块头的随机数，不断用SHA256运算，与目标值做对比，如果小于目标值，则解题成功，工作量证明完成。工作量证明完成后，产生新的区块，新区块在网络中传播，每个节点广播到其他节点。

1.7为何会有软分叉：比特币是由若干点对点去中心化节点共同维护，但节点操作运行还是得依靠矿工。由于矿工所处理的时间和所在地理位置存在差异，区块链使用的底层协议在同一时点上存在差异，此时会出现分叉。分叉指的是由于底层协议的不同而引发的记账差异。软分叉指的是当新的共识机制发布后，没有升级的节点会因为不知道新共识机制而生产不合法的区块，进而产生临时性分叉。但这种分叉会随着节点的升级而逐渐修复。

1.8为何限制区块大小：交易信息在被添加到新的区块之前，需要由矿工确认。而区块大小会对需要验证的交易数量产生限制。当区块较大时，需要更大的计算能力和更长的时间开采，存在交易垃圾邮件堵塞网络威胁和黑客攻击的风险，因此，需要限制区块的大小。

1.9为何限制出块时间：由于比特币采用了POW共识机制，也就是人人都可以成为矿工参与挖矿，而且可以随时退出挖矿。这样就导致了整个网络里面参与挖矿的矿工算力是动态变化的。当参与挖矿人数少的时候，算力低，挖矿难度系数根据算法相应自动降低；反之，当参与挖矿人数增多，算力增强，挖矿难度系数会根据固定算法来自动提升。通过难度系数的调整来确保相对固定的出块时间。但是由于难度系数不是在实时调整的，而是根据设计和代码实现每隔了2016块调整的，也就是差不多2周的时间（假如说绝对均匀时间出块：2\*7天\*24小时/天\*3600/小时/600秒/块 = 14\*24\*6=2016）所以调整难度系数有滞后，无法及时掌握总体算力的变化而调整，导致了每次算力调整后出块的时间有长有短，但是总体上是上下围绕10分钟波动的，而且不会有太大的偏差，也就是实现了一种统计学上的守衡。

1.10区块中包含的内容：区块是区块链的基本组成单元。每个区块由区块头和区块主体组成。区块头包括：版本号、前一区块哈希值、默克尔根、时间戳、难度值和随机数；区块主体包括挖出该区块10分钟内的所有交易信息，呈梅克尔数结构排列。

1.11为什么使用UTXO设计：UTXO设计即未花费交易输出，指的是每笔比特币交易中没支付出去的那一部分，类似于账户余额的概念。假设比特币和传统货币一样，使用账户余额系统，使用数据库来记录所有人的余额，基本上随着交易频次和交易人数的不断增加，难以有服务器可以承受。UTXO设计不再需要一个中心化的数据库来保存和验证所有的交易信息，分布式的节点就可以验证，独立的数据结构减少计算量；增强了匿名性，一个人可以生成很多账户，每交易一次就有一个新的地址，保证了账户的安全；实时对账，降低错误率，一旦发现问题可以直接找到错误。

# 2、请说明如果签名正确、余额足够的情况下，发出的交易迟迟没能出块，应该是什么原因，应该采取什么措施，分别说明不同措施的后果。

原因是手续费太低了，被排到了后面待矿工验证。

可采取措施大致有四种：一是重新发起一笔交易，提高手续费，但这样原来的那笔交易无法撤回；二是找矿工私下解决，这也涉及到找矿工成本问题；三是等，交易不会重复手续费也不会增加，但时间成本增加。

# 3、请说明以太坊项目的目标，它与比特币不同的技术设计及其原因。

3.1以太坊主要用于两个目的：与其他加密货币相同的方式在交易所上作为数字货币进行交易，并且以太坊网络上用于运行应用程序。

3.2与比特币的技术设计区别：以太坊网络上的交易可能包含可执行代码，而固定在比特币网络交易上的数据仅用于笔记。

编程语言：比特币使用的语言是“基于堆栈”的，而以太坊则是基于“完成转换”的。

区块时间：以太坊以秒为单位确认交易，而比特币以分钟为单位。

算法：以太坊使用ethash,而比特币使用SHA-256。

区块限制：比特币区块链限制为1MB，以太坊没有区块限制。

3.3主要的原因是比特币和以太坊两者的目标不同：比特币的目标是作为中心化货币的可替代物，创造一种新的货币形式；而以太坊的目标是作为一个平台，通过本国货币促进程序性合同和应用，货币化以太坊智能合约和去中心化应用程序平台。

# 4、请说明以太坊智能合约的运行原理以及合约的整个生命周期。

4.1智能合约是部署在区块链的代码，区块链本身不能执行代码，代码的执行是在本地的虚拟机EVM中，部署在区块链上的代码是能够在本地产生原智能合约代码的代码，可以理解区块链为一个数据库，而客户端从数据库中读取了存储的运行代码，并在本地运行后，将结果写入到了区块链这个数据库中。

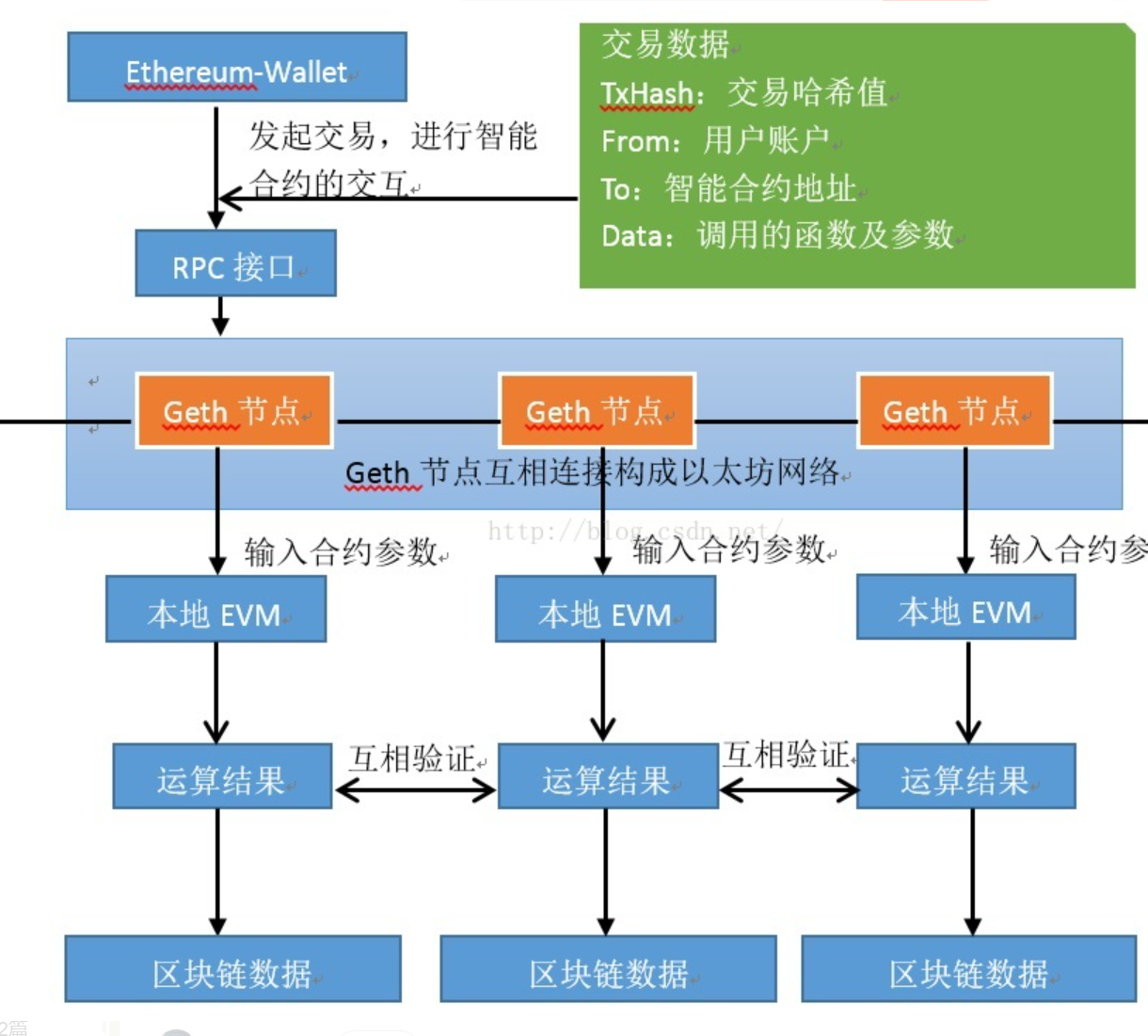


图3 以太坊智能合约运行原理

图片来源 <http://blog.csdn.net/>

4.2智能合约的整个生命周期主要包括四个部分：

4.2.1合约存储：以太坊智能合约有两种类型的账户，外部个人账户和合约账户。合约在部署时，会创建一个合约账户，合约的可执行字节码保存在合约账户中，具体是账户codehash指向的存储区域；codehash是代码的哈希值，创建后不可更改。数据主要存储在账户storageRoot指向的存储区域storageRoot 对应合约存储结构的MPT树根节点hash值，通过它能够在数据库中检索到合约的变量信息。

4.2.2合约创建：用户 A 使用 solidity 等语言创建一份合约代码，A 在 IDE/钱包/其他客户端，按一定的格式（from，data，value，Gas，GasPrice....）填写 data，然后确认（即发起一次transaction），客户端会填补 account nonce(tx计数器)、compile solidity、签名 等操作，并将 to 字段置零（代表合约创建）。该 tx 广播到网络上，B 节点收到该 tx。B 节点检查 tx 是否有效、格式是否正确，验证交易签名是否合法。如果符合要求，计算可能的最大交易费用，确定发送者的地址，并在本地的区块链上查看发送者的余额，如果账户余额不足以支付最大的交易费用，则返回错误。对于符合要求的交易请求，B 将其放在交易存储池中，并向其他节点转发（比如转发给了C）。C 收到交易请求的节点重复用户 B 的处理过程。

4.2.3合约部署：B 和 C 各自从本地的交易存储池中拿到一批 TX，然后打包进行 hash 计算（挖矿）。假设 B 挖矿成功（获得了记账权），B 会根据 A 提供的交易费用和合约代码，创建合约账户，并在账户空间中部署合约。合约账户地址在创建合约的 tx 确认后返回给 A。B 打包好的区块（包含 A 创建的智能合约）发送至对等节点，并在全网传播。C 接收到该区块，验证区块，如果区块通过验证：C 从内存池中删除 A 创建的智能合约交易请求；C 将区块链接到本地最长链上（同步区块）；C 将 A 的智能合约部署在本地区块链中。

4.2.4合约执行：用户 A 按照一定格式在网络中发起一个 tx 请求；该请求被网络中节点 B 收到: 如果符合要求，计算可能的最大交易费用，确定发送方的地址，并在本地的区块链上从发送方账户中减去相应费用。如果账户余额不足，则返回错误，这条交易被直接丢弃。B 同步到此交易，检查交易是否有效、格式是否正确。符合要求的交易请求，用户 B 将其放在交易存储池中，并向其他节点转发. 其他节点执行和B同样的操作过程。B 挖矿成功: 对于转账交易，B 将该交易和其他交易一起打包到区块。对于合约调用交易，B将该交易和其他交易一起打包到区块中，并在本地的 EVM 上运行合约代码：如果代码并未结束而 Gas 已经用完，那么因代码运行而改变的状态回滚到代码运行之前，但是已经支付的交易费用不可收回，交易费用由B获得。如果代码运行结束 Gas 还有剩余，那么B只会获得消耗的Gas×GasPrice 作为手续费，不会收取剩余 Gas 对应的手续费。 B 将包含 A 交易请求的区块传播到对等节点，在网络中广播。C 节点收到该区块后: 验证区块（用户A的交易的合法性也被再次验证） 验证通过，C 将内存池中 A 的交易请求删掉，同时将B的区块添加到本地的区块链中。验证不通过，C 丢弃该区块;执行区块中的智能合约交易 ; C 在本地的 EVM 上运行该智能合约，并与 B 的执行结果互相验证。网络上其他矿工节点重复 C 的执行过程：通过 EVM 在本地计算机上运行智能合约，作为他们参与挖矿进程的一部分，然后得出一个结果并进行验证。理论上，如果没有人恶意操作，每个计算机代码运行的结果都是相同的，因为它们运行着提供了相同信息的相同合约代码。

参考资料：

[1] 周卫华,康伟婷.基于区块链的智能治理机制研究——以 The DAO 为例[J].财会月刊,2022(04):3-5

[2]朱晓武,魏文石.区块链的共识与分叉：The DAO案例对以太坊分叉的影响分析及启示[J].管理评论，2021(33):325-326

[3][以太坊智能合约的生命周期\_跨链技术践行者的博客-CSDN博客\_智能合约生命周期](https://blog.csdn.net/shangsongwww/article/details/90199857)