# 区块链到底怎么用？比如GitChat会用到吗？

## 一、区块链技术简介

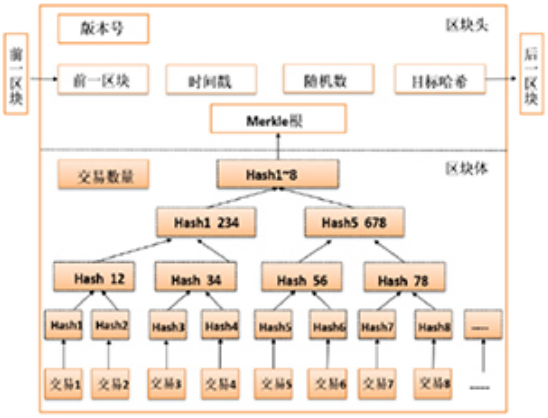
在探讨区块链（Blockchain）到底怎么用之前，有必要简单的介绍一下区块链技术本身。区块链成名于比特币，人类历史上第一次去中心化的实现了电子货币的发行。理解区块链的技术和应用方向，从比特币开始，比特币也被称为区块链1.0：

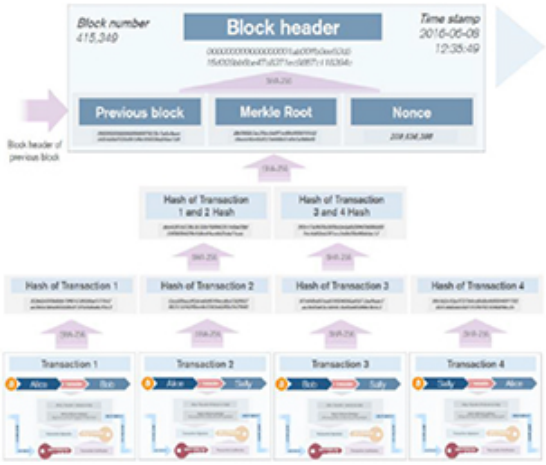
首先上图一张，先大致理解区块链的工作流程。




1. 数据区块（链）：比特币的交易记录会保存在数据区块之中，大约每10分钟产生一个区块，包括了10分钟内的所有交易打包生成一个区块，每个数据区块包括区块头和区块体。区块体包含了交易计数和交易内容清单的列表，从而像记账本一样永久记录了每一笔交易的详情。区块体中每笔交易清单都会生成一个哈希（HASH)值-256位的字符串，构成叶子节点，然后递归的向上产生新的哈希值，直到生成根节点哈希值。哈希（HASH）算法将任意数据换算成唯一对应的256位字符串哈希

值，而且过程是单向不可逆的，原始数据稍有改动，哈希值也会相应的改变。这样无论数据多大，都可以产生一个256位的唯一标识。从而为验证数据完整性（不可篡改）提供了便利；还有一个好处是可以只对数据对应的哈希值做数据签名（私钥加密）来实现用户拥有确认和数据未经第三方篡改，从而大大降低运算量。区块头包括了 版本号，前一区块的地址（构成区块链），时间戳（格林威治时间起到产生区块时的间隔时长），随机数（和挖矿有关），当前区块的目标哈希值（POW工作量证明），Merkle树的根值（保证区块数据的不可篡改）。如下图所示：




2. 密码学原理和UTXO交易模式：比特币实际上没有账户的概念，记录的是一张一张的“银票”的“生死”。每一张银票都有对应的公钥和私钥和相应的金额，银票的地址就是公钥按照标准哈希算法变换后的值，区块里记录的转账交易就是把原来的银票撕掉，把银票里的“钱”转到新的银票上，如果有余额也会产生一张新的银票。私钥用来签名，公钥放在交易清单的验证脚本里，用来验证私钥的签名。

3. 去中心化的分布式网络：用户不用注册就能匿名参加，无需授权即可加入或者退出网络。采用P2P协议同步数据，每个节点都可以保留所有的原始数据清单区块链，有点像git可以拿到所有的代码库(分支和入库/出库细节）于本地。

4. 共识机制（挖矿和分叉）：区块在挖矿过程中产生（也称之为POW）。所谓挖矿就是穷举随机数算法，把上个区块的哈希值加上10分钟内的尚未记账的现有交易单打包，加上不断遍历来寻找的一个随机数，使得最终算出的一个256位的字符串哈希值，满足一定的难度条件，比如前面10位都是零。找到这个随机数就可以获得记账权，然后将新的区块发布到网上，被大家验证。有可能短期内，造成分叉，但是规则是工作量最大的最长的链最终被网络各节点接受，从而抛弃短的链条。一般等6个新的块产生后，交易才可以被最终确认被计入区块链。2009年到2013年，每10分钟产生一个区块奖励比特币50个，2014年至今每个区块减半为25个。

5. 比特币实际是一种股份: 比特币的总额是2000万，发明的本意就是对抗通货膨胀的电子货币。获得比特币3种途径：一是获得记账权的矿工（挖矿成功）获得；二是交易中心购买；三是商家收取比特币。

## 以太坊：区块链2.0

随着比特币的成功，很多类似的代币发行，利用了比特币的基础技术，但是修改了代币的发行原则。到2016年，已经有超过600多种代币发布。这样为了不同的代币管理规则，去重复的创建类似比特币的网络，成本是很高的，也发展不起来（势必一盘散沙）。能不能在一个区块链上，提供应用开发的能力，从而满足不同应用需求共生于一个底层平台之上？以太坊就是为了解决区块链技术通用性问题，应运而生，通过虚拟机EVM运行以太坊脚本（智能合约），在以太币的基础上，用户可以登记和发行各种资产和代币。在智能合约的基础上，形成了DAPP（去中心化应用）和DAO（去中心化自治组织）。DAPP是指由智能合约和客户端代码组成，智能合约运行在区块链上，客户端代码运行在特殊浏览器Mist里。

1. 应用举例：Augur（www.augur.net）

   一个去中心化的预测系统。用户可以在这个应用上对各种时间打赌和下注，用户个人赌赢则获得代币；巧妙之处在于对于整体参与应用平台而言，成了一个群体智慧的收集器。某件事件，搜索完全可以得到“Augur： 该事件发生的可能性为xx.x%”。脑洞一下：如果这个有意思的网站带来的广告收入，是否可以按照代币（股份）分给所有参与打赌和下注的用户呢？

2. 应用举例：Maker（www.makerdao.com）

   一个金融类去中心化组织，当用户在区块链上登记了众多资产时，在不出售资产的情况下通过抵押借款获得资金；资产的验证通过线下的律师和事务所参与，形成一个自动管理的市场。大家有兴趣可以直接点开看细节。



打开脑洞（其实已经存在了）：众筹平台DAO，投票决策平台DAO，类似微信通信交友平台DAO，等等。几乎凡是现有的组织形式，都存在被DAO改造或者结合的机会，这个后面再详细讨论。

小蚁是国内本土研发的的类似以太坊的公有链，业余时间在看代码，最近比较忙，看的比较慢。个人还是很欣赏小蚁针对以太坊的不足，而做的一些革新。特别是他们想做的跨链操作，还是比较有意思的。（跑题了，就此打住）

**值得注意的特点：**

1. 比特币和以太坊都提供了REST API，用来和平台进行交互，包括保存（产生）私钥的 钱包，一些基础的账户管理（以太坊），智能合约的部署和调用等，处于比较初级的阶段。个人认为，基于公链的比特币和以太坊本身，去完善服务能力是很好的创新方向。闪电网络，就是用离线支付比特币的方式，去解决比特币交易吞吐慢的问题。DAPP 和 DAO是很好的创业方式。

2. 在比特币区块链中有加入定制数据的机会，理论上可以写小说。这是一个通过比特币或者以太坊，实现某种信息存证的机会。原理，这里就不赘述了，可以讨论时再详细解释。

3. 比特币网络的吞吐严重受限（每10分钟产生一个区块，大约每秒7笔交易），以太坊虽有提高，但是因为智能合约的支持也没高到哪里去（每15秒产生一个区块，每秒交易提高到百笔左右），所以在提高交易频次方面，私链和联盟链纷纷用PBFT

共识机制取代了POW，提高每秒吞吐量，但是个人并不认同这个方向。结合云计算完全有更好的方法来获得更好的性能。因为目前私链/联盟链的多中心的模式，很可能只是一个过渡，会被单中心但是共享的模式取代。好比GitHub促进了Git的发展，但是又回到了中心服务的模式。细节就不在这篇文章里详述了，可以再写一篇gitchat文章，详细论述。

# 二、对区块链技术演进的反思

**去中心化不是区块链的本质。DAO本质是“用户”的共享和自治。**

Git相对于Subversion的中心化，迈出了一大步，形成去中心化的代码库的使用，但是GitHub还是以中心化的方式，成为真正的杀手级应用。P2P的网络比如一开始用来下载电影，但是目前的主流则是中心化的互联网视频网站服务。滴滴和共享单车，都是共享经济，但是通过中心化的方式来运营的。所以说如果有中心能提供更好的区块链设施和服务，就会推动它的发展，是矛盾统一的辩证法。关键还是分布式的机制，自动运行的智能合约，通过机器来执行组织的既定规则（智能合约），通过密码学保证了不可篡改的分布式记账方式，因为无需信任，所以产生了信任。

比特币网络可以看成是超越了国家的，不同于跨国企业的一种新型组织：开源社区，开源代码，一个由分布式网络的大量节点，将规则自动执行的“股份公司”，虽然比特币的规则只是电子货币，而以太坊发明了智能合约，将区块链技术发展成为一个支持应用（智能合约）开发的基础平台：支持虚拟机图灵完备的执行智能合约指令，基于共识、可扩展，标准化的易于开发和协同的应用。



**比特币只有一个，而不应该是一群。**

如果说比特币成为了事实上黄金储备，那模仿它的代币就不会有太大的机会，号称区块链2.0的以太坊本身就是基于比特币成功募集的ICO。创造性提出了智能合约，但是以太坊的市值不到比特币的十分之一。坦率说，目前看到凡是涉及探讨区块链应用的，都比较玄妙，或者说太跳跃，或者是把金融、存证、身份管理、供应链管理等一堆垂直领域拿出来，拿着锤子找钉子，哪里都想敲一下的感觉。所以我想从一个不同的角度去探讨区块链的应用方向：**如果说人工智能的发展方向是机器帮助人，那么区块链技术的方向就是机器帮助组织。**DAO才是正途，而且一切刚刚开始。

# 三、区块链到底怎么用

围绕在比特币和以太坊上的公链的应用，具备很多机会，比如以太坊上著名的打赌项目 Augur 和 预测项目 Gnosis。在金融领域里的应用，也是大家研究的重点方向，所谓“离钱近的地方好赚钱”。

但是，个人在学习了区块链技术后，感觉区块链还有更加普世的价值，那就是通过DAO**构建新型社会组织关系。**如果从DAO（DAPP）角度看，那区块链本省就会成为一个基础性的，类似数据库一样的平台性服务，从而有更加广阔的应用空间。区块链的本质是分

布式的账本，怎么用？实质上是通过智能合约，对新型组织关系进行设计，并通过机器去执行这个规则，并通过分享的方式和密码学技术，确保数据可追朔和不可篡改。

规则的设计，本质上要想好两个问题：一、什么要记到共享账本里（解决什么问题），二、记账了有什么好处（分配和激励机制）。

下面我举几个例子，以假想的方式，探讨如何通过区块链去构建（DAO）新型社会关系。

## 开源项目DevOps DAO

最近基于云的CI工具，Travis (https://www.oschina.net/p/travis-ci)挺火，和GitHub紧密集成，提供云端的CI服务（build）。我们是否可以创建一个DAO，提供SaaS服务，让开源项目在云端不仅可以CI，还可以CD（部署）。发行代币（股份）让投资者购买，然后团购云资源，在云端搭建CI/CD的系统，为开源项目服务。区块链上保存什么（价值设计）？开源项目作者免费创建用于CI/CD的配置文件和部署后成功的配置，者相当于创建了“资产”，它的价值是如果有用户（包括开发者自己）想运行一下看看，甚至是改动代码后的验证，这个预定义（配置）的资产，可以方便用户一键部署。那么用户对项目的使用（CI/CD，修改、展示等）情况，就可以记录到区块链中。占用云资源超过一定的时间，就需要付费。根据情况也可以对资源消耗严重的大项目，预先收费才能使用。付费方式就是购买代币，当然很多时候简单看看，是免费的。



可以想象，这个区块链将记录所有的用户使用参与的项目的情况，包括使用时长，是否修改，需求或者问题的提出，以及是否解决等一系列的使用情况。稍加积累，这条链就可以反映出开发者对所有参与项目的喜好和需求，对这条链保存的各种维度数据的挖掘，就会带来商业的价值。每个区块的产生会有一些代币，奖励开源项目CI/CD环境（资产）的创建者（可以制定的更加复杂，群里私聊吧）。而对链的分析和访问，可以收费（卖商业报告，广告等）。还有一个收费的场景是云资源的占用。所有的代币持有者，拥有这条区块链上的数据的商业价值。

## 共享单车（摩拜单车）的粉丝DAO

北京春天阳光明媚，开始骑摩拜单车一周左右，感觉不错。经常看见人力车把散落的单车运到不同的地方投放，摩拜单车还提供了红包车的功能，把停的比较不方便（位置不佳）的单车，奖励用户红包的方式，去“舍近求远”。所以我想是否可以通过建立一个粉丝DAO，共享出来单车位置数据的方法，并把停的不好的车的期望位置标出来，发动群众去骑（搬）车（运），所有的搬运被记录到区块链中，每个区块产生的代币被分给做好事的用户。区块的价值，提供了单车被谁（匿名）搬运的路径和时间，频次等信息，相当于人工标注了大数据。扩大一下，在上面叠加的事情，可以很多。基本原则不是用一个红包来激励用户，而是让用户能共享整个大数据链的价值。

本来要写 GitChatXXXDAO的，突然想到，不能在别人家里反客为主，所以还是私下沟通吧。通过上面两个例子，原则是清楚的，可以举一反三。而且作为GitChat这样本身就极具创新特色的社会化内容产生和分享的平台，DAO的模式一定可以为平台的发展助力！

写了两个，已经精疲力尽。最后希望开源社能够成为DAO项目的专业设计组织，为广大的开源项目商业化出谋划策！并通过参与其中，每个项目都可以获得一定的代币，然后组织自身也能够随着各种DAO项目一起发展。