第一篇：浅说区块链基础

第1讲 | 到底什么才是区块链？

自中本聪第一次发布了比特币，至今已经有 9 个年头了，那么算起来区块链也应该有 9 年的历史了吧？其实不是，“区块链”这个概念恰恰是这些年才有的，如果非要追溯，可能在 2014 年左右，才真正有了“区块链”的概念。

区块链和区块链行业

我早期写文章喜欢给区块链下定义，但是读者反响并不如意，所以今天我想“反其道而行之”，先讲一个笼统模糊的对象，再像一层层剥洋葱一样，慢慢地给你讲解区块链的来龙去脉。

首先，什么是区块链行业呢？区块链是一个崭新的行业，与社交、电影、游戏一样，具有自己独特的内涵和发展过程。

这个行业是通过比特币形成的。我们可以把比特币比作一棵树，这棵树在生长过程中不可避免地会开枝散叶，慢慢长大，而这个生长过程其实就是代码 Fork，进行再修改发布运行的过程。

比特币之后有了莱特币，莱特币之后又有了点点币，点点币之后又有了上百种币，后来的这些币仅仅在原有的比特币核心代码上做了技术上或非技术上的修改，从而形成了独有的币种。所以我们在早些时候，也将比特币之外的所有币种统称为“山寨币”。

当然，如果只有一棵树，也就不会称作一个“行业”了。一些大神，比如以太坊的创始人 V 神（Vitalik），再比如比特股、Steem 和 EOS 的创始人丹（ Dan ）等觉得比特币这棵树不够自己发挥的，于是在继承了比特币的“火之意志”之后，相继在比特币旁栽下了属于自己的“树”。

渐渐地，树变树林，几乎是以指数级增长的过程，树林又变成了森林，错综复杂，最终形成了一个崭新的行业，这个行业我们称作“区块链行业”。

我在一开始说区块链具有自己的独特内涵，那么到底是什么内涵让这么多人“趋之若鹜”呢？

第一个是具有理想主义情怀的极客所提出的“去中心化”；第二个是以赚钱为主要目标的投资者和生意人。

前者为后者提供了极佳的赚钱土壤，后者为前者注入了赖以生存的资金。听起来好像“沆瀣一气”，其实并没有，这也是区块链行业通常所说的链圈和币圈。前者组成了“链圈”，后者组成了“币圈”，以前这两个圈子“井水不犯河水”，现在却有融合的趋势，为什么？

首先是行业的需要，实在是太火热了没空吵；其次是，说到底区块链的第一大应用还是数字货币，本身就无法分割。

那么，“链圈”加“币圈”也可以是我们所说的区块链行业。

我再深入介绍一点，刚刚提到了“去中心化”，它更像是表达极客信仰的一面“旗帜”，我个人更喜欢称之为“导火索”。

它把金融领域聪明的投资者与厉害的技术人才拧在一起，点燃了无数起“回归互联网平等、自由、开放”的大讨论，任何人都可以从中构思挖掘自己熟悉领域的“区块链应用”，整个过程在技术上看就是上文提到的“开枝散叶”，这个过程你也可以看成是区块链的发展过程。

至此，你可能已经对区块链行业有了一个模糊的认知。那么，到底什么是区块链呢？

区块链究竟是什么

简单来说，区块链首先是一个分布式网络。如果你不懂“分布式”也没关系。我举个例子，假设你和朋友异地开黑打《王者荣耀》，这时候“异地开黑”就可以看成是一个小型的分布式网络。朋友语音喊你开团战上高地，那么其实这就是达成一次共识的过程，你参与了团战，就是你同意共识的过程。

区块链也是一样，它并没有超出我们的认知框架。让所有的独立节点想要达成共识去做同一件事情，是区块链在技术上首先要解决的问题，这就是我们常说的共识过程，也是“去中心化”这个概念的直接来源。

那么假如有了这样一个分布式网络，我们可以选择不同领域做产品，就像传统技术上有了迅雷、电驴等等产品一样。

区块链与之最大的不同是整个系统本身具有自己的 Token。Token 在国内有的翻译成“通证”，有的翻译成“代币”。其实最简单的理解就是“虚拟资产凭证”。它可以是我们的股权，也可以是票据，也可以是游戏积分，凡是需要资产记账的地方都可以用 Token 来做。

还是回头看上面那个例子。如果你参与了团战，你的朋友就要支付你 1 元，请问这个系统怎么做？注意，我这里说的不是银行卡转账，我就是指在游戏里面，你所在的这个分布式网络中，在你参加团战之后，对方通过这个分布式网络直接支付 1 元给你。

很多人就会说：“直接做到 App 里面呗”，可是你要知道，我并没有说支付“1 元人民币”啊，也有可能是 1 游戏积分，这个游戏积分未必是王者荣耀发行的，你有没有想过这个积分是你的朋友发行的？

你肯定会说，那我要这个积分有什么用呢？好，假设你的朋友是个超级富豪，他说你陪我玩游戏，但我不想支付你法币，我用我自己发的游戏积分给你，你看我老爸在国外开游戏积分交易所的，我的游戏积分在上面交易，你每次帮我开团，我就给你积分，你拿去自己交易换成其他资产，美元啊什么都可以。

想象一下，你的土豪朋友每次语音说“谢谢你帮我开团成功”，你就拿到 1 游戏积分，而这 1 游戏积分和腾讯没半毛钱关系，却又让这个语音与这 1 游戏积分同步生效，区块链其实就是在解决类似的事情。这里的积分可以理解为具有流动性的虚拟资产，但流动性又没有虚拟货币好，它不属于虚拟货币。

说了这么多，现在总结一下区块链是什么：

区块链是一个分布式网络；

区块链可以帮助多个节点达成共识去记录和 Token 相关的事情；

区块链可以帮助所有人无门槛地构建属于自己的小经济系统。

至于再深入的区块链内容，后续文章听我慢慢道来。

总结

今天我和你聊了下区块链及其行业的发展过程，形象化地描述了区块链是什么。

相信你对区块链行业已经有了一个基本的了解，但文章篇幅有限，希望你能够进一步发掘区块链相关的历史，甚至有趣的故事，比如说 1 万比特币购买披萨事件、真假中本聪事件、以太坊 The DAO 事件分别对应到区块链哪些发展阶段呢？ 感谢你的收听，我们下期再见。

第2讲 | 区块链到底是怎么运行的？

今天尽可能通俗地介绍一下：区块链到底是如何运行的？

这一篇文章我将以比特币区块链为例来进行讲解，理由有两个：

由于区块链发展到目前阶段，各个技术方向都有长足的发展，那么为了方便你理解，我在这里介绍最简单、最容易理解的比特币区块链；由于大部分区块链都是以比特币区块链为基础进行扩充的，所以首先了解比特币区块链有助于其他项目区块链的后续学习。

中心化记账的问题

首先，我们借鉴了一个区块链描述中的经典情景来模拟中心化记账。

假设有一个有百户居民的村子，其中有一位德高望重的村长，村长有一个儿子。村民们都把钱存到村长家，村长负责记账。比如，张三用 1000 买了李四家的牛，村长就把张三名下的存款减去 1000，李四家加上 1000。听起来是不是很像银行的操作？

对，我们就是先从中心化的银行记账开始聊起。村民都相信村长，才愿意把钱存到村长家，他们相信村长不会作恶。

可惜好景不长，老村长由于操劳过度，驾鹤西去了。新上任的村长儿子铁蛋很是聪明，但也有个毛病，就是粗心大意。他不但经常算错账，一次还被人偷改了账单。

不过，幸好村民自己都有记账，但是由于铁蛋每次错账后都要和别人核对半天，导致村民对新村长的记账能力十分不满。

时间就这么过着，然而最可怕的事情还是发生了，铁蛋的老婆竟然私下篡改账本，给铁蛋七大姑八大姨的余额全部偷偷加了好多，终于有一天事情暴露，村民们气冲冲地跑到铁蛋家里讨说法，于是一片混乱。

这时候有个叫中本聪的人站了出来，他说他设计了一套系统，可以不依赖任何人记账，于是，众人开始将目光集中到他的身上。

1. 公开记账

中本聪说他的系统稍微麻烦一点，需要干三件事儿。

每家每户都派发一只信鸽。这就是 P2P 网络，是一个点对点的分布式网络，如果不好理解，你先不用理会，我会在后面讲到。

每家每户都发一个特殊的印章和一个扫描器。这个扫描器有两个功效，一是识别他人的交易是否真实有效；二是识别这个交易是不是自己账号的，同时识别并解锁未花费的余额。这就是非对称加密。

每家每户可以参与记账，不过不再记余额，而是记交易本身的内容。这就是区块链中的交易，这个“交易”对应的英文单词是“Transaction”，这是个专有名词，专指一笔账，不同于金融交易的 Trade。

这三条总体来说其实是干一件事情，就是：

每家每户都记账，账簿上不再记载每户村民的余额，而只记载每一笔 Transaction，即记载每一笔交易的付款人、收款人和付款金额。

那么问题就来了：如果每户都记账，肯定每户的账都不统一啊，你记你的，我记我的，最后不全乱了么？

这个时候需要大家统一账本，保证大家的账本都是一致的。因为记录的交易是全村所有人有序产生的，所以这就需要有一个广播机制。这个广播机制，我先卖个关子，后面再讲。

中本聪说，其实很简单，我们现在先把全村所有人的资产都加起来。还真巧了，刚好 100 万。

中本聪接着说：“只要账簿的初始状态确定，并且每一笔交易可靠并按照物理时间自然记录，并且只加不改不删，这样，当前每户持有多少资产是可以推算出来的。”

中本聪说我现在把我的印章给你们看，这个印章很特殊，盖的章有两块标记，第一块是一个可以识别的标记，比如我往纸上一敲，可识别的标记是 1MsTg2。

这就是你们的代号，由于我们账本是公开的，使用真实姓名会很危险，所以你们记账的交易单上收款人、付款人都填这个码，不用写姓名。你的扫描器和你的印章生成的代号是关联的，有且仅有持有对应扫描器的人才能花费金额，这一步即为“解开交易”。

刚刚说印章有两块，这第二块内容配合这个扫描器才能看，肉眼看则都是乱码，扫描器一扫就知道第二块内容是否有效，这一步也就是“交易验证”。

并且所有交易大家都能接收，都能看到，但却解不开印章乱码部分的内容，仅仅收款方才能解开，因为你的扫描器和你印章生成的代号是关联的，有且仅有持有对应扫描器的人才能解开交易。

以上就是区块链中“公开记账”的过程。“公开记账”就是全网所有人都可以随时查看一套账本，然后按照规则透明公开地进行记账。

2. 创建创世区块

创世区块是我们生成全村公开账本的第一笔交易的第一个信封，好比一篇文章总得有个开头一样。

于是乎，中本聪说我先生成第一个 Transaction，这个交易单的付款人为空，收款人是村长，付款金额是 100 万，因为是创世区块，产出多少个是可以随意规定的，由于我们上面统计了全村的账目情况，所以我就写了 100 万，待会儿付款给村长以后，我们可以按照原来的账本给大家发送对应的金额过去。

好了，我们有了第一笔交易，第一个信封也已经做好了。现在让村长把信封传给张三，张三复印一份，然后传给李四，李四继续传下去，一传十，十传百，直到传给全村人，这个步骤也就是“同步区块”，也就是全网都拿到这个信封，以及信封里面的 Transaction。

3. 交易

由于上一节我们的创世区块把 100 万交给了村长，那么我们假设张三在村长那里的存款余额是 10 万，这时候村长要根据原来的旧账本，把这 10 万发送给张三，然后把旧账本上的账划掉。下面我们讨论一下如何构造这笔交易。

中本聪开始教村长写交易单，把 100 万分成两部分，第一部分 10 万，收款人是张三；第二部分是 90 万，收款人是自己；这样一个 Transaction 就做成啦。

前面我们说了，不能直接写名字，要写代号，这个代号也就是你的钱包地址，我们需要把收款人写名字的地方，让收款人拿出自己印章，把代号读出来，然后告诉村长即可。

100 万 10 万，张三

90 万，自己

村长写好 Transaction 以后，还需要拿出自己的印章，在 Transaction 上盖章，这个盖章的过程也就相当于区块链中的签名。这个章，全村人都可以拿扫描器扫一下验证是否有效，即验证付款人的章是否有效。

100 万 10 万，张三的印章（1s25vR）

90 万，村长的印章（13gYip）

就这样，村长一共写了 10 份 Transaction，分别代表了发送给不同人的交易，张三一笔 10 万，李四一笔 1 万，等等。

4. 打包 Transaction （挖矿）

现在我们有了 Transaction，但是还需要东西把 Transaction 装起来，我们用一个特殊的信封把 Transaction 装起来，这个信封就是区块链中的“区块”，这个封装过程就是“打包交易”。

为什么要封装起来呢？是为了让打包交易的人能够在信封上署名，表示这次打包是由某某某打包的，其次全村的交易可能非常多，需要装配标号，方便大家查询。

我们看到上述的 Transaction 虽然已经生成，但是有个问题，就是没有规定谁有权利把 Transaction 封装到信封里。

我们在开篇的故事中看到了中心化操作肯定是不行的，假设在全村人中，这时候如何筛选出这些打包的人呢？

中本聪这时候说了，由于我们村的人口增长，100 万未来可能不够，我们暂定 150 万，那多余的 50 万，我们就当奖励给这些装信封的人了，当然不能一次性给，谁装一次信封就领 3 个币。

这时候大家伙儿来劲了呀，只要装信封就能够领钱了，我们在这里把符合条件的人称作“矿工”。

但是中本聪又说了，要获得这个装信封的权利，是有条件的。我给大家出一个难题，谁先解出这个难题的答案，谁就有权利把 Transaction 装到一个信封中，并且要在此信封上盖上自己的章。

这个难题是这样的，它有两大特性，第一是容易验证，第二是计算过程非常复杂。

例如，有种棋牌类游戏叫作“24 点”，玩法就是给出任意 4 个整数，通过整数运算得到 24，比如现在给出 2、9、1、5 四个数，答案是（5-2）\*（9-1）= 24。当然，本处仅是举例，“24 点”游戏的答案空间非常小，是远远不够生成信封的。

答案非常好验证，但是计算过程是一个尝试的过程，需要耗费大量的精力。而在真实的比特币中，采用的是寻找符合条件的目标哈希，这也就是比特币矿工所做的事情。

好了，这时候大家开始计算给出的难题，刚好李四第一个计算出来，那么这次装信封的操作就由李四完成，李四把 10 份 Transaction 装到信封中，也就是打包 Transaction，并且要在信封背面写上一个信封的摘要信息。

比如上一个信封中的第一个交易是什么、信封封面长什么样，最后要在信封上盖上章，也就是“签名”，矿工签名的目的是为了领币，也就是 Coinbase 交易。

以上过程在区块链领域称作“打包 Transaction”，也就是大名鼎鼎的“挖矿”。

5. 广播交易

来说说上文提到的广播交易，广播是为了让全村人知道当前时刻你产生了一笔 Transaction，或者是你装好了一个信封。

广播的内容分两种，一种是广播 Transaction，一种是广播信封。第一种广播是意味着还有未被打包的 Transaction，而第二种广播信封则意味着这个 Transaction 已经被某个矿工确认。

收到了广播的通知后，大家先验证信封上难题的答案是否正确，这样便可以验证出信封是否被伪造，接着验里面的每笔交易，最后还要验证信封背面的内容，即上一个信封的摘要是否正确。因为上一个信封大家都已经确认，所以这样可以极大地规避作弊的可能。如果觉得没问题，就可以存入本地数据库中了。

至此，全村人的记账问题就差不多解决啦。

第3讲 | 浅说区块链共识机制﻿

我在第 2 讲“区块链到底是怎么运行的”一文中，提到了“打包 Transaction”和“广播交易”这两个概念，因为概述的原因，当时只带着你走了一遍过程。其实，以上谈到的两个内容正是区块链最核心的技术内容之一：共识机制。

区块链发展至今，已经形成了各种不同类型的共识机制，在今天的文章中，我们就展开聊一聊区块链共识机制到底是什么，以及区块链的共识过程到底是怎样的。

分布式系统的经典问题： 拜占庭将军问题

拜占庭将军问题其实是虚构出来的一个故事，是为了方便通俗地介绍分布式系统所面临的难题。这里我仅作一个简短的说明，你可以在中文社区找到更丰富的通俗解释材料。

为了避免重复，我们换一种表述形式，还是以上一次的村子为例，假设随着村子和人口的发展，大村子演变成了十一个小村子并分散在各地，各地的通信只能靠信鸽进行。

大家约定了每年都会举办一个相亲大会，至于谁能举办，每年轮流从两个备选村子，A 村和 B 村中选择一个，然后大家投票，票数多者可以赢得举办权。

由于地图很大，任何一个村子的投票都无法靠一只信鸽传输到每个村子，必须靠一个中继村子代为传输，这也就意味着有中继村子可以读到其他村子的投票信息。

那么，如何防止下面两个问题的出现呢？

投票者的“精分”，这里所谓的“精分”是指某个村子的投票行为不一致，发送给第一个村子的投票消息为“投票给 A”，而发送给第二个村子的投票消息却为“投票给 B”。

中继村子作弊，即篡改上一村的投票消息。

上面讨论的问题我们可以认为是简化的 “拜占庭将军问题”（完整的拜占庭将军问题还有将军 - 副官模型，如果感兴趣的话，你可以自行阅读）。

我们回头再看区块链。区块链本质上也是分布式系统的一种，其共识机制也是为了上述问题而提出的解决方案。

什么是区块链共识机制？

共识机制是区块链是核心的组成要素之一，它决定了区块链的业务吞吐量、交易速度、不可篡改性、准入门槛等等，是最为关键的技术要素之一。

要理解区块链共识机制，首先就需要理解区块链共识机制到底解决了什么问题。

共识机制主要解决了两个问题：

谁有权利；

作弊问题。

上一次我们构造了一个中心化记账的场景，在这个场景下，记账问题其实可以简化为大家信任中心记账者即可。

然而在分布式记账的场景下，问题更为复杂。首先，大家面临的最大问题是谁有权利记账，其次是如何避免记账者作弊。毕竟，谁都有权利记账，也就意味着谁都有可能作弊。

以上两部分共同构成了区块链共识机制。

另外补充一点，在比特币社区，“共识”（consensus）这个词已经跳出了技术的范畴。通常人们在表述一个比特币上的问题时，共识的内涵还包括比特币的使用者、开发者、矿工来达成社区共识的部分，所以“共识”这个词在区块链领域还有些“民主”的味道，不单单是技术领域的“共识”。

最经典的入门型共识机制：PoW 工作量证明

PoW （Proof of Work）工作量证明可以解决上述的两个问题，

在上一篇文章中，其实我们已经悄悄讲解了一点 PoW 共识机制，你还记得上文提到的“24 点”那个游戏吗？“24 点”其实是尽可能随机地选取系统中任意的节点来规避作弊者，这个方案的实践其实就是 PoW 共识机制。

产生记账者的随机性其实来自于谁最先计算出 24 点的答案，这个问题可以简化成谁拥有的计算资源更多，谁就拥有整个系统的最大概率的记账权。一旦这个概率超过一半以上，那么这个系统就有一定的中心化风险。

如何理解上面一段话呢？

举个例子，李四家发明了一种算盘，可以快速计算 24 点答案，比起其他人掰手指头，李四家总是有很大的概率拿下记账权，换句话说，也就是李四和全村其他所有人竞争，相当于算盘对全村其他人手指头的竞争。

如果算盘足够强大，就能有一半的概率获得记账权，那么李四个人的诚实性，就成为了系统的唯一破绽。

比如李四在第一次记账时篡改部分交易，第二次还是他记账，还继续篡改交易，那么两次修改如果自洽的话，是可以形成假账的，这就是所谓的中心化风险。

所以在 PoW 这种机制中，计算资源（又称算力）是决定记账权的唯一因素。与之对应的，便是计算难度。

计算难度又称作挖矿难度，计算难度是区块链为了控制产生答案的速度，比如平均 10 分钟就有一个答案产生，平均 2 分钟一个答案产生。

在上述场景中，因为李四有了算盘，强大的计算资源突然加入以后，肯定会让整个系统的产生答案的速度变快很多，作为系统本身会自适应，将难度提升，降低答案产生的速度。

上面介绍了这么多，其实是想引出另外一个问题，PoW 到底是如何避免作弊者的呢？答案就是计算资源（算力）。

设想，如果一个作弊者想篡改信封里面的交易，首先得获得记账权，也就是装信封的权利。

而影响记账权的唯一因素只有计算资源（算力）的大小，如果想篡改交易，只能投入大量的计算资源与整个系统中其他所有人进行对抗，这是十分困难的，尤其在整个系统有一定基础计算资源（算力）的情况下。

PoW 中一个有趣的设计是激励机制，在 PoW 共识机制下，我们假设所有参与者都是理性的，理性的意思就是单纯逐利，不考虑家庭、爱好等其他因素。有了理性的前提，PoW 共识机制会给每个诚实的记账者予以奖励，这个设计可以抗击作弊收益的问题。

怎么进行抗击的呢？整个过程是这样的，理性的人如果作弊、篡改账本肯定需要投入成本，也就是计算资源，收益是篡改账本获得的收益减去投入成本，这个收益往往小于诚实计算所获得的收益。所以，作弊者在作弊过程中投入的计算资源过大，反而得不偿失。

PoW 工作量证明的补充：解决双花攻击

上面给出了一个结论，我们说作弊的收益往往小于诚实计算的收益。这一点其实对应到区块链领域有个著名的问题：双花攻击（double-spending） 。

双花攻击是指一个代币被花费了两次，这在任意的区块链系统中是不被允许的。如果避免了双花问题，基本就能避免上述作弊中收益过大的问题，因为攻击者首先要窃取到你的私钥，同时又能控制了你的计算资源（算力）。

为了方便分析，我们回到上一篇中广播交易的那一节。那一节中我介绍了广播的内容分为两种，第一种是 Transaction，第二种是区块，也就是信封。

第一种又被称为未确认的 Transaction，第二种信封中所有的交易被称作已确认的 Transaction。

所有记账节点都会遵循以下两条规则：

规则一：一个代币如果已经被花费，那么会被标记成已花费，如果再次接收到这个代币被花费的请求，那么记账节点会拒绝打包这笔交易；

规则二：如果同时接收到两个信封，这两个信封中装的两笔交易出现了一个代币被花费了两次的情况，这种情况也就是我们所说的分叉（Fork），那么选择挖矿难度比较大的那个信封。

规则一避免了未确认的交易出现双花，规则二基本避免已经确认的交易中（信封中）的双花问题。

假设作弊者的计算资源（算力）占整个系统的 30%，那么连续两次获得记账权的概率是 9%，看起来作弊的可能性还是挺高的，如果是连续 6 次获得记账权呢？概率直降到万分之七。

在比特币中，这个 6 也就是 6 次确认，表示连续 6 个块过去了，如果我的交易没有被双花的话，那么它被篡改的可能性将越来越小，最后变得几乎不可能被篡改。这也是区块链不可被篡改说法的由来。

试想，如果任何作弊者花了大量的成本获取了系统 30% 的计算资源（算力），最后只有万分之七的概率获得篡改的可能性，比起作弊，还不如诚实记账的收益高。

总结

好了，今天带你了解了区块链的共识机制，也顺便浅谈了拜占庭将军问题，介绍了区块链的入门共识机制 PoW，它其实也是目前区块链领域使用最广泛，应用最成熟的共识机制。

最后，还涉及了一部分 PoW 工作量证明的补充：解决双花攻击。由于篇幅所限，我们将在技术篇详细讲解 PoW、PoS、DPoS 等共识机制。

第4讲 | 区块链的应用类型

我在前面的三篇文章中分别介绍了区块链是什么、区块链的运行原理、并且简述了区块链的共识机制，在这一篇文章中，我将为你讲解一下区块链的应用价值。

由于区块链本身发展处于早期阶段，成熟的应用并不是很多，我的主要目的是拓宽你的思路，抛砖引玉，希望你能够从中获得应用灵感，为区块链挖掘出更多有市场的应用，但需要提醒你的是，本文提到的内容不构成任何投资建议。

数字货币应用方向

数字货币是区块链的第一大应用类型，市场上目前可统计的数字货币币种有 1500 种以上，2017 年其迅速增长的市值让人措手不及。

那么说，到底如何理解数字货币这个概念呢？其实你可以简单理解为一种无主权、社区自治的货币形式，关于这部分的详细介绍我们留到下一篇。

在“区块链到底是怎么运行的”一文中，我们构建了一个中心化记账的模型，这个模型可以对应到如今央行 - 商业银行的模式上；而数字货币的运行则通常是靠社区自治的，所谓社区自治，是指用户、维护者、开发者三种角色共同决定数字货币的发展，也就对应了上一篇文章中，我们所讲到的“共识”。

我们先来看看数字货币，通常具有下面几个特点。

总量透明公开。数字货币的发行是在项目创建之初，是白皮书事先就规定好了的，白皮书通常是一个区块链项目公开发布的一种阐述性文档，其中简述了项目的宗旨和愿景以及设计蓝图。在白皮书中，这个项目总共发行多少数字货币，投资者、用户、矿工能够获得多少也都是事先分配好的。数字货币的总量也分为两种，一种是总量设上限的，另外一种是不设上限的。

数字货币缓慢释放。数字货币在分配好不同角色的额度之后，往往不是一下子就能发行完毕的，通常在矿工的那部分是需要靠“挖”才能出来的，这也就是前面我们所说的挖矿，挖矿为数字货币的缓慢释放提供了一种方法。

代码执行规则。由于我们在白皮书中规定好了总量和数字货币释放的机制，白皮书的内容会成为整个社区的基础共识，所以在项目的主网上线之后，数字货币的释放不再是人为控制，而是在代码层面体现，代码将负责控制数字货币的释放，这里去除了人为操作的因素。

基本上，所有公有区块链项目都会具备以上特性，可见数字货币和区块链的关系十分紧密。另外，在区块链领域，一个项目的开始运营，就伴随着一个新的数字货币的产生，这个数字货币会成为这个项目的基础代币，也有可能会派生出其他货币。

与区块链的其他应用类型不同的是，数字货币这种资产天然具有较好的流动性，所以在所有权上更为敏感。

比方说，如果“你的信用卡被盗了”和“你的微博账号被盗了”，正常人都会紧张第一种情况。所以说，区块链在数字货币上的应用，其“去中心化”“不可篡改”的特性相较于其他，就显得更具有划时代的意义。

数字资产方向

我们在上一节聊了数字货币，这其实可以推而广之对应到数字资产。

怎么理解呢？如果区块链可以做数字货币，那么同理，它也可以应用到其他任何资产，尤其是虚拟资产。

虚拟资产一般包括有金融资产、游戏代币、数字版权、域名、用户流量等。由于虚拟资产不需要与实体资产进行挂钩，所以在对应到区块链上更为方便。它具体的应用形式在供应链金融、票据市场都有所体现。

我们还是继续举例子。区块链圈子内有个非常有名的加拿大白胡子大叔，他基本上是逢会必现。

他要做的应用简而言之叫做“良心区块链”，不是指区块链项目的良心，是指他希望用区块链技术让所有人可以进行自我管理，自我管理的方式是对“良心”进行评价和奖励。人的良心都可以区块链化，还有什么不能尝试呢？

他的项目是这样的，比如今天我给自己设定了一个跑 10 公里的目标，如果我完成了，那么我会在系统上获得代币，如果没有完成，则有相应的惩罚机制。大叔的项目还与联合国 17 条可持续发展目标进行了关联，他的目的也很单纯，就是希望通过自己的行为让世界更好一点。

你看，在区块链上，连“良心”都可以数字化，还有什么不能数字化呢？

我们再举个例子。前些年比较火热的一个少年团体叫 TF-Boys，里面有三位成员，很多粉丝其实是与偶像割裂的，并没有一种模式叫做让粉丝与偶像共同增值。

比如我们可以让 TF-Boys 每位成员都可以发行属于自己的区块链积分，并与粉丝一起共同持有。在未来，根据偶像成长和走红的程度，偶像可以与粉丝一起分享收益。

所以说，除了数字货币，数字资产也是区块链的一个应用方向。数字资产的应用形式与资产证券化（ABS）十分类似，感兴趣的读者可以自行研究一番。

比较成熟的应用类型

那么区块链目前有哪些比较成熟的应用呢？其实我们有时候想得太远了，反而忽略了脚下。首先来说，任何的区块链创始项目如果要活下去，就要先解决钱的问题，也就是融资问题。

我们在前面说到，任何的区块链项目基本都会产生一个基础代币，那么什么样的融资模式能让投资者和项目方都满意呢？

其实，这个融资模式本身就是一个很成熟的应用。——答案是去年被七部委明令禁止的 ICO(Initial Coin Offering)。

我们在这里，简单从技术的角度介绍一下 ICO，ICO 的中文名是首次代币发行，又称为区块链众筹，这是一种新型的融资模式，投资者可以用手中的比特币或其他代币投到一些区块链创始项目。

一个区块链项目发起之后，如果选择发起 ICO，相比传统融资渠道，项目方会在很短的时间内融到资，且白皮书中规定好的代币将一次性地投放到投资者手里，并在短时间内上线数字资产交易平台。

数字资产交易平台也具有高流动性，这种高流动性为早期投资者提供了退出条件，这样投资者的投资周期大大缩短，并且可以快速抽身。

例如，马先生持有 1 个比特币，现在参加了某名为 ABC 的区块链项目 ICO，ICO 兑换比例是 1：10000，也就是说马先生投资 1 个比特币给项目方，将会拿到 1 万个 ABC 代币。

如果 ABC 代币会在一个月内上线交易平台，假设 ABC 的价格波动超过 50%，那么马先生的 1 万的 ABC 代币可以交易成 1.5 个比特币，马先生纯赚 0.5 个比特币，并且他可以抽身这个项目，再次参加新一轮的 ICO。

ICO 技术虽然为所有区块链项目提供了周期短、效率高的融资模式，但在同时，ICO 也成了传销和内幕交易的重灾区。

以上举例说明了区块链在虚拟资产下的应用模式，而另外一个高产虚拟资产的领域——游戏领域，也是区块链同化的对象。

不过，目前还没有特别成熟的案例，比较有名的是 2017 年走红的以太坊“养猫”游戏，但我并不认为这意味着区块链真正踏入了游戏圈，这仅仅只是它的小试牛刀。

试想，你在游戏里的道具，如果可以在其他任何游戏进行使用，感觉是不是很棒。虽然目前还没有现象级的游戏被区块链同化的例子，不过你也可以发散思维，构想一些新的区块链游戏模式。

当然除了虚拟资产，实体资产也可以用区块链进行应用，但是目前遇到的难题基本都是实体资产如何与链上区块链的数据进行一一映射。

这涉及了数据公证等等环节，实施起来比中心化应用困难很多，比较典型的例子是区块链与供应链结合，解决信息流、资金流、物流，“三流”合一的问题。

除了实体资产和虚拟资产，区块链最简单直接的应用还有公证公示领域，不过这里仅仅用到了区块链“不可篡改”的特性。

总结

通过本篇文章，我向你介绍了区块链的一些应用方向。包括了区块链在数字货币以及数字资产上的运用。

第5讲 | 如何理解数字货币？它与区块链又是什么样的关系？﻿

从历史进程来看，货币的形态主要经历了几次变化。从早期社会如兽皮、牲畜、陶器的物物交换，到各种贝壳类的货币，再到后面的铜币，乃至后来人们选择了黄金和白银作为流通货币。

随着消费需求不断增加，人们发现可以通过发行纸币来替代贵金属，于是，我们就一起进入了信用货币的阶段。后来，技术的发展促进了电子货币的产生。现如今区块链技术的大热，它的第一个应用就是数字货币。

数字货币的概念

数字货币通常是国内的叫法，在国外，它一般称作“加密货币”。数字货币听起来比加密货币更抽象一点，“数字”旨在表现它不同于传统货币的行为，即它可以通过“数字”表现更多自定义的行为。

那么，如何用一句话来解释什么是“数字货币”（加密货币）呢？我们可以这样形容：数字货币通常是基于区块链技术、在全球范围内公开发行的、并且没有任何国家政府背书的虚拟货币，这种虚拟货币具有“去信任”、“点对点”、“公开记账”、“不可篡改”等特征。

既然聊到了虚拟货币，我们正好可以把电子货币、虚拟货币、数字货币（加密货币）的概念捋一捋。

1. 电子货币

近年来，现金使用的频度降低，很多人首选使用电子支付。电子货币和数字货币一样都是无形的，但是电子货币其实就是将法币电子化，例如第三方支付平台，银行卡电子现金，银行大小额支付系统等等。它只是以电子的方式记录了原来法币的账目，从本质上来说，它们仍然需要在多个中心化系统中进行稽核、对账，“电子”本身并没有成为金融的一部分。

2. 虚拟货币

在 2017 年区块链投机狂热的时候，“虚拟货币”这个词基本是用来指区块链项目的基础代币，这样的叫法大多源自于圈外投机者。其实不然，虚拟货币所指代的概念远比电子货币以及数字货币都要更加广泛。

虚拟货币通常是由非金融机构发行的非实体货币，大致分为三类。

第一类比如游戏代币，通常不与实体经济发生联系。例如在《王者荣耀》这款游戏中，如果你想要得到新的道具，就必须有足够的游戏代币（钻石和点券），这种虚拟货币还有个特征就是封闭性，即只能在这款游戏中使用。

第二类是积分类，它可以与实体经济发生联系，比如常旅客积分，超市礼品卡，这种虚拟货币也有个特征叫做单向性，即只能流入，而不能流出。

第三类自然就是我们主要讲的数字货币（加密货币）了，比特币便是其中典型。

综合来看，与法币的“有形”对应，虚拟货币更多地体现在它的“虚拟无形”上，随着互联网的发展，虚拟货币本身也在逐渐发展，从而诞生了更多新的模式与机遇。

3. 数字货币

数字货币一般是指公有区块链平台底下的基础代币，该代币被记录在由密码学保证的一套公开账本上，与传统货币不同的是，由于去中心化以及可编程等特性，此种货币具有可自定义行为的属性。

在比特币中，我们可以定义多重签名交易来实现真正意义上的“由多人共同掌管的机构型账户”。

比如，在元界上，用户可以自定义交易的行为，例如在转账时可以指定代币的一个锁定期，并且指定解锁条件；而在比特股中，这种行为更被强化为具有衍生品特性的货币，这在传统货币领域是不可想象的。

与数字货币对应的，还有数字资产这个概念，不过这是另外一个话题了，后续我会有详细的讲解。

传统货币与数字货币

正因为数字货币的诸多新特性，所以金融机构和互联网公司纷纷加入研究行列，越来越多的人想要研究数字货币，这里，我想带你对比数字货币和传统货币的不同特性，以便你可以更直观地了解数字货币和传统货币的不同。

匿名性 vs 实名制

传统货币在支付过程中，除了现金，其他任何方式基本都或多或少地保留了交易者的信息，无论你是个人还是机构，运营商都可以使用这些交易数据来跟踪你的活动。

而在数字货币领域，这件事就无足轻重了，目前大部分数字货币具有假匿名性，即化名性，所以并不会被查到你自己的私人资料。

同时，由于区块链上未提供 KYC（Know Your Customer）功能，也就是充分了解你的客户，对账户持有人的强化审查，所以让监管者很难追踪到交易者的信息，也让数字货币成为了黑市交易的温床。

这样的缺点主要是因为不少公链代币设计中没有加入身份的概念，不过这在我这样的技术人的角度来看，只是算是一个需求，而不是数字货币本身存在的缺陷。

点对点 vs 中心化

数字货币的发行主体通常是项目发起方，并且会在白皮书中定义好数字货币的发行过程；在主网上线以后，所有的代币会根据一开始设计好的发行过程缓慢释放到市场，这个过程其实就是大家喜闻乐见的“挖矿”过程。

所以在主网上线以后，即使作为项目发起方，也几乎很难有权利再次修改发行机制，所有人只能以提案的形式递交到社区进行讨论，讨论的最终结果决定了能否被再次修改。

这个过程其实与民主选举的过程很相似，而在信用货币领域，发行主体通常是央行，央行可以通过货币的政策进行宏观调控，从某种意义上来说，央行模式是中心化的极致体现，而数字货币则属于点对点机制的体现。

自理型安全性 vs 托管型安全性

由于数字货币的交易过程需要网络中每个节点的认可，且每一笔交易都被记录在区块链上，所以历史交易记录永远不用担心丢失或者被篡改。

只要数字货币基础的加密算法不被攻破，并且保护好私钥，你的资产便是真正意义上、只属于你自己的资产。

传统货币的交易过程最终是落到银行的，所以银行系统的安全性决定了传统货币在使用过程中的安全阈值，这也表示你的资产是托管在银行的。

广区域流通 vs 国家内部流通

传统货币是有主权的，通常只在主权国家范围内流通；数字货币目前却没有这样的限制，只要你能连上互联网，你就可以随时随地发送交易到任意地域。

总结来看，数字货币目前也有很大风险，如今还没有比较完整规范的法律法规来约束数字货币的使用者，所以使用数字货币会有较高的法律与投资的风险。

而且普通人已经接受了信用货币这种设定，目前对数字货币的接受度在各国并不一样，例如在中国大陆接受度低，在日本接受度高。

数字货币的发行过程

数字货币在 2016 年开始加速，2017 年借助 ICO 呈井喷式发展，数字货币市场形成了一个大泡沫，这与 2000 年初的互联网泡沫十分相似，但是泡沫并不可怕，它只是一个热门新生事物的必然过程。

我们需要在这个泡沫中找到规律，那么首先就要了解数字货币的发行过程。我们可以以比特币为例子来聊聊它的发行过程。

比特币的发行过程是通过挖矿维持的，是依靠矿工挖矿产生比特币。相当于矿工自己就是一个小型的印钞机。

矿工每挖出一个区块，也就是在第二篇文章中提到的“打包一个信封”，会产生一个 Coinbase 交易，这个 Coinbase 交易相当于凭空产生了币，矿工可以从 Coinbase 获得比特币，作为维护系统的奖励。

Coinbase 的产出是每 4 年衰减一半的，第一个 4 年是挖出每个块 50 个比特币，第二个 4 年的周期就是挖出每块产出 25 个，目前比特币处于第三个 4 年，Coinbase 产出 12.5 个比特币的阶段。

以上逻辑是比特币白皮书和比特币代码规定好的，所有比特币的参与者可以进行验证。并且根据以上逻辑，我们可以画出如下的发行曲线。

我们可以看到，比特币的发行过程每隔四年发生一次改变，发行速率逐渐降低，随着时间推移趋于平缓。

同理，我们在其他数字货币项目就可以看到类似曲线，不过它们未必与比特币的发行曲线一样，有可能是离散式的，有可能是线性的，这取决于白皮书中规定的发行过程。

例如熵币 ETP 的发行过程也是一个衰减过程，不过 ETP 的衰减系数是 0.95，所以相对比特币可以说更光滑了，它随着时间收敛到挖矿总量 3000 万，那么这个曲线看起来是这样的。

所以数字货币的发行过程可以认为是一个区块链项目的核心利益分配的过程，也是一个社区激励的过程，如何把有限的代币派发给愿意为项目付出的社区人，是考量一个区块链项目运营成熟度的重要指标。

第6讲 | 理解区块链之前，先上手体验一把数字货币

﻿﻿

初次接触到区块链的你，肯定是一头雾水：“区块链是什么，这玩意到底怎么回事”。

其实对于区块链的原理，你大可不必着急，咱们可以直接上手体验一下目前区块链的第一大应用：数字货币。

本篇的内容面向所有区块链的小白，我会教你如何使用数字货币，来帮你从另外一个维度理解区块链技术。

本篇内容包括但不限于：数字货币钱包介绍、下载安装、转账、数字货币交易所充币、提币等等。

首次接触数字货币

区块链其实是从生产者的角度讨论一个抽象出来的概念。如果把区块链比作车辆设计图纸，那么数字货币就是正在跑的汽车。所以理解区块链的最直观的方式其实是从数字货币入手，而不是直接一上来就来理解原理。

数字货币作为区块链的第一大应用，拥有巨大的市场，你可以从“ coinmarketcap.com ”上了解几乎所有数字货币的概况。

如果想了解数字货币行情，可以打开 feixiaohao.com 进行查看，也可以手机下载“ MyToken ”或“ 币看”。

这两个 App 的使用方法与股票行情软件非常相似，上面几乎可以查询到所有已经“上市”的数字货币的实时价格与成交量信息。

什么是数字货币钱包

数字货币钱包是最贴近用户的区块链程序，数字货币钱包会可以帮你管理数字货币私钥，发送交易，可以显示你的交易历史记录。从用户功能的角度，数字货币钱包比较接近我们日常使用的钱包，它帮助你管理纸币、硬币、信用卡借记卡。

数字货币钱包作为数字货币的载体，从技术角度来看，数字货币钱包分为三种类型。

1、全节点钱包。全节点钱包是指官方发行的一种数字货币钱包版本，这个版本包含了完整的功能需求，挖矿、发送交易、查询交易记录、管理私钥。

2、SPV 轻钱包（Simplified Payment Verification）。轻钱包为了用户体验，牺牲了全节点的部分功能，属于全节点钱包的简化版，如挖矿功能、查询交易功能就没有。

3、中心化资产托管钱包。这种钱包其实是第三方服务商帮助你打理你的数字货币，找一个中介托管你的数字货币，比较典型的有 blockchain.info。

以上的第 1 种和第 2 种会在各个数字货币的官网出现，属于真正意义上的数字货币钱包，1 相比 2 而言，安全性要更高；所以我在这里推荐你先从全节点钱包开始尝试，毕竟全节点钱包基本囊括了该币种的所有功能实现。

而第 3 种钱包，与银行移动 App 或支付宝相比，在业务逻辑上区别不大。比如你会把钱托管到支付宝上一样，你也可以将你的数字货币放进第三类钱包中。

这种钱包往往都是多币种的，深受投资用户的喜欢，而且从方便性和用户体验来说，基本完爆 1 和 2，例如以太坊系钱包 imToken，多币种钱包 Jaxx，以及各个数字货币交易平台。

无论是什么类型的钱包，建议你在获取钱包程序的时候，一律要从官网下载，即使是移动端 App 也强烈推荐从官网的入口进入。

玩转数字货币钱包

上一节中，我们简单介绍了数字货币钱包的类型，本节内容将以全节点钱包作为例子，教你玩转数字钱包。我们这里会以某个币种的全节点钱包作为例子，穿插一些比特币 Electrum 轻钱包的例子，为你介绍数字货币钱包的上手方法。

由于我的电脑中安装了不同的数字货币钱包，它们的使用方法都是相似的。我截取的图片可能涉及了某些具体的币种，但这并不是我推荐安装建议，你可以忽略。另外在具体的操作过程中有大量图片展示，收听音频的你可以点击文稿查看。

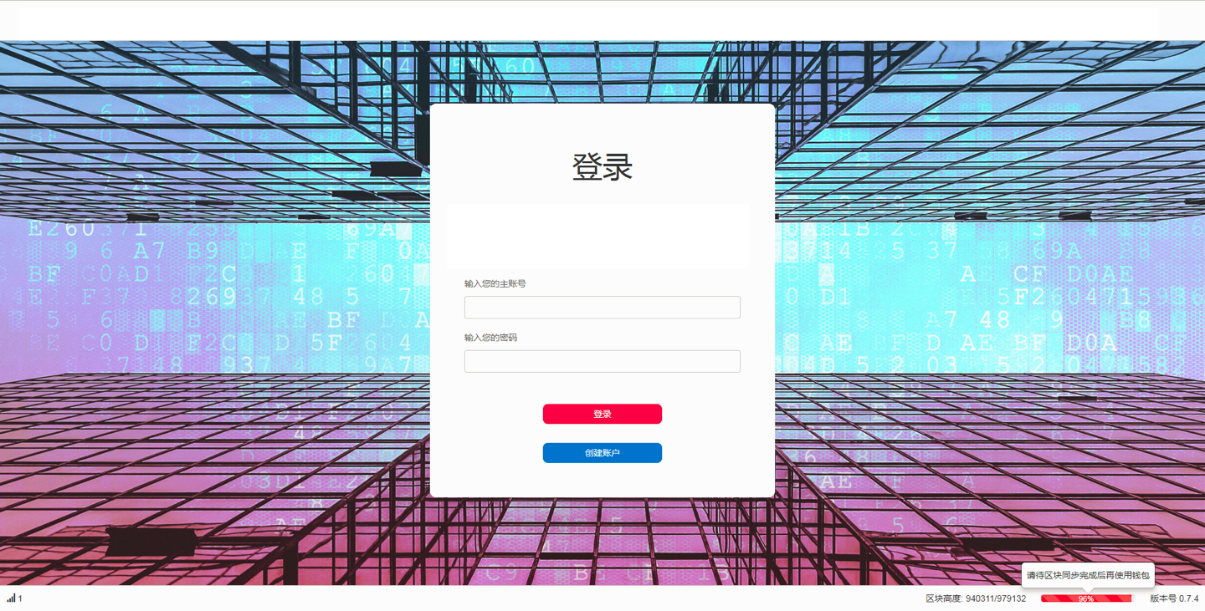
1. 获取钱包程序

全节点钱包程序是一种需要用户安装到桌面的软件，它需要互联网连接，不挖矿的话，资源消耗与其他中心化软件差不多。

与其他所有桌面客户端一样，首先用户需要获取安装包，安装包可以从官网下载，我们先到对应币种官网下载一个 Windows 版本的客户端钱包。

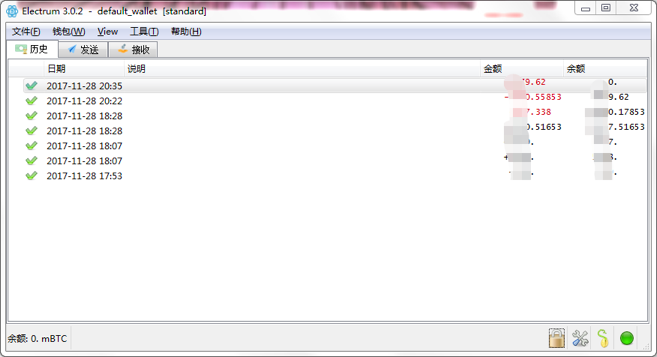
﻿﻿

一直双击安装下一步等待安装完成，安装好以后桌面出现快捷方式，咱们双击打开，通常会出现钱包的主页面。

﻿﻿

（ 某币种钱包主界面）

那我们来看看比特币，比如比特币的 Electrum 钱包长这样。

﻿﻿

（比特币钱包主界面）

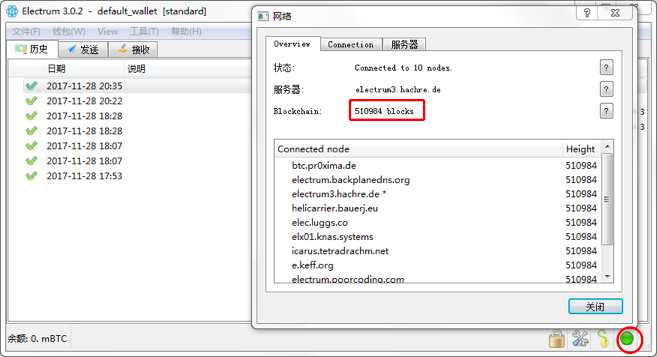
你可以搜索“Electrum”，进入官网下载。

﻿﻿

（在官网下载比特币钱包）

对于钱包程序来说，最重要信息的就是当前区块高度了，区块高度表示了当前你所在区块的序号，序号体现了你是否更新到了最新区块，而最新区块则决定了你能否查询到自己的交易。即规定了你所有交易账单的起始位置。

我们以 Electrum 钱包为例，点击圆圈中的控件，出现对话框，红框数字就代表了你本地钱包的块高。

﻿﻿

比特币钱包块高）

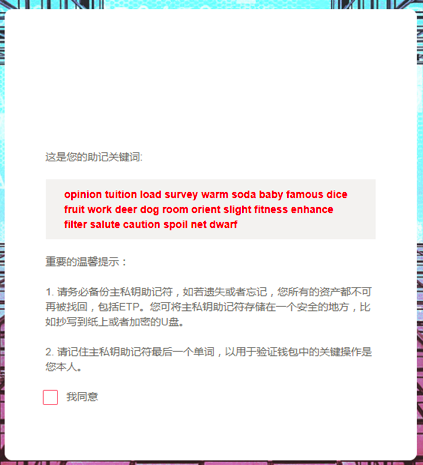
由于 Electrum 的使用教程比较丰富，我们就不赘述了。

2. 钱包文件与钱包账户

当你第一次安装好钱包以后，使用钱包的第一件事情就是创建账户（或者钱包文件）。

一般全节点钱包都支持多账户，尽管有些钱包有账户的概念，有些没有，在逻辑上也可以使用钱包文件替代账户这个概念。

例如 Electrum 轻钱包采用的是钱包文件，某些全节点钱包采用的是账户。咱们用某个币种的钱包为例子，点击创建账户以后，填好用户名密码，会得到如下信息：

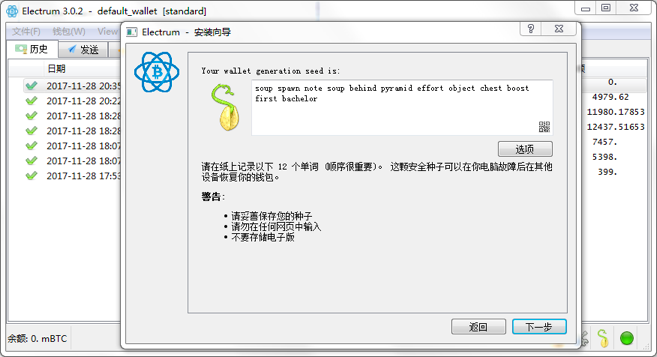
﻿﻿（某币种钱包助记词）

敲黑板划重点：红字部分又称助记词。这种助记词是为了主私钥服务的，主私钥其实是一串非常长的字母和数字组合，无论是人脑记或者笔记都是非常不容易识别的，容易弄错，助记词的有序组成与主私钥是一一对应的。

如果记录保存好了助记词（红字部分），即使钱包丢失或者被破坏也没有关系，用户可以在其他钱包中导入助记词，依然可以操作资产。

所以说在区块链的世界，主私钥和助记词是操作资产的唯一途径，如果丢失，那么资产就丢失，不存在忘记助记词还能找回资产这回事。

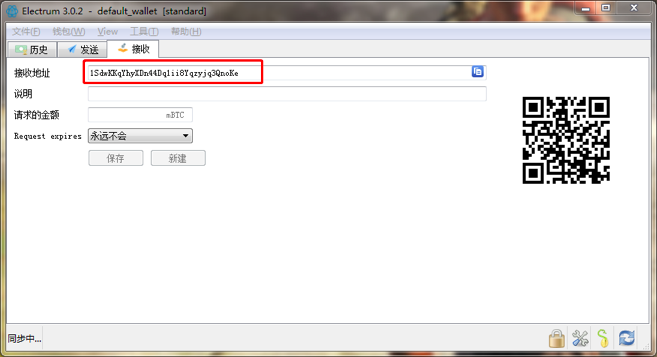
我们来看看比特币的助记词，我们点击左上角【文件】-【新建 / 恢复】，一直下一步直到出现 12 个单词（暂时不必理会每一步中的选项，不同选项代表不同格式的钱包文件），这 12 个单词也是助记词，只要保存好了助记词，你的比特币可以在任意（标准版）比特币钱包导入。

﻿﻿

3. 钱包地址

我们常听到别人说钱包地址，也就是对应到我们现在银卡的卡号。在币圈，地址其实也分很多种，我们今天只介绍最简单直观的——支付地址（Payment Address），也就是我们现在要说的钱包地址。现在咱们来看看自己的地址是什么。

在比特币中，地址是以 1 开头的一串字母和数字的组合，字母区分大小写。

﻿﻿

（比特币钱包地址）

﻿﻿4. 获取代币

好了，现在我们已经有地址了，可是地址上没有代币，钱包就是一个摆设。现在我们想办法搞点代币过来。

我们先搞点代币进来，一般有两种方式，挖矿和上数字货币交易所购买。挖矿的技术门槛虽然不高，但是过程繁杂，手续繁琐，不推荐入门尝试。

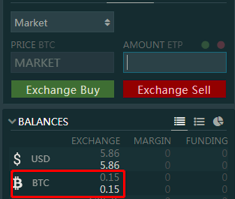
好了，现在我们就只剩下购买这一条路了。

请注意！目前不存在人民币对数字货币的场内交易平台，所以想用人民币购买数字货币的各位只能选择场外交易，比较有名的平台有 coincola.com，由于涉及投资，我们就不深入讲了。

你如果具有投资热情，可以继续挖掘“coinmarketcap”中绿框内的选项：

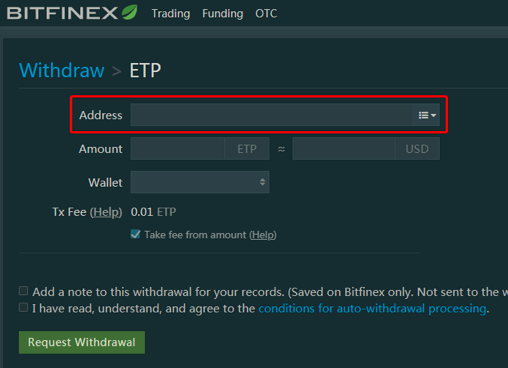
﻿﻿

假设咱们已经拥有了比特币 -BTC。

﻿﻿

这是我刚刚在 bitfinex 上购买的 0.15 个比特币，其他交易平台原理大体相同，基本上比较大的交易平台都有交易手册，你可以自行翻看教程。

咱们接下来选择 ETP/BTC 交易对，通过 BTC 购买一些 ETP，然后找到提币，选择 ETP 提币。

﻿﻿（提币地址）

这时候问题就来了，提币需要填写一个地址，这个地址就是咱们上文提到的钱包地址，你只需要把自己的钱包地址填入此处即可，填好其他项，发起提币请求即可。

这时候问题就来了，提币需要填写一个地址，这个地址就是咱们上文提到的钱包地址，你只需要把自己的钱包地址填入此处即可，填好其他项，发起提币请求即可。

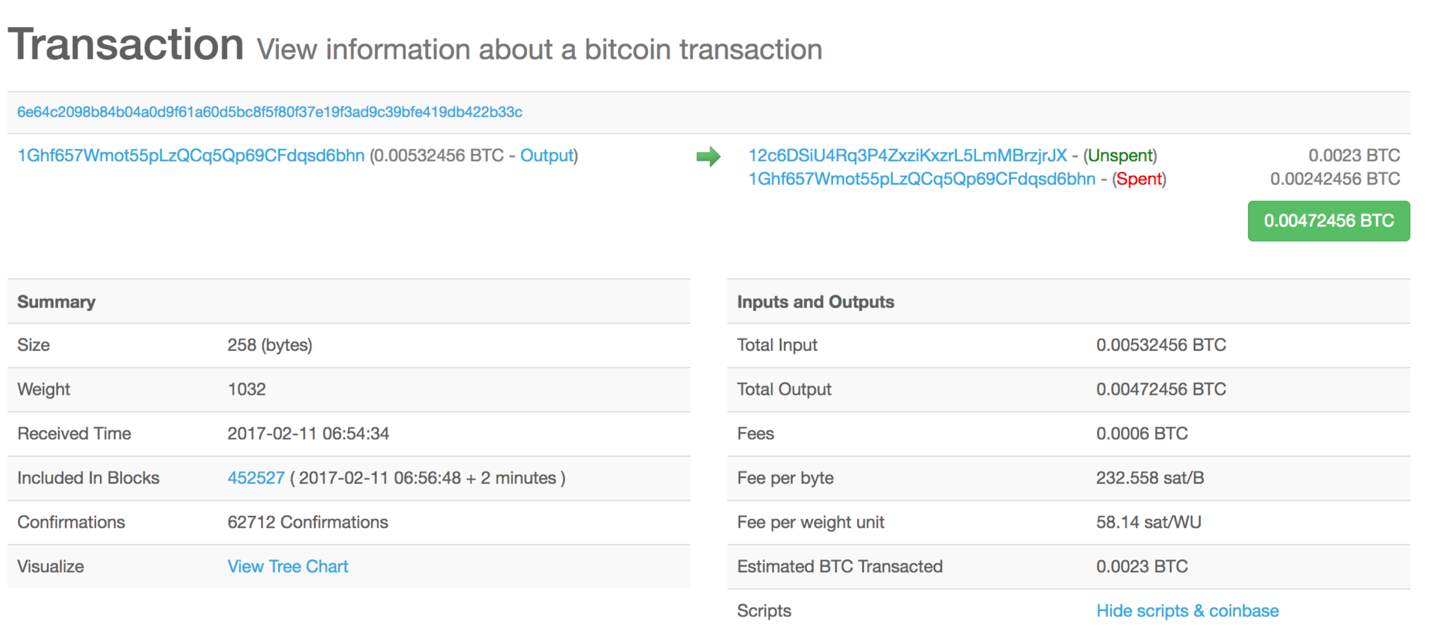
5. 区块链交易

接下来咱们只需要等待币到帐即可，到账的过程就是产生一笔区块链交易的过程，一般交易所都会提供 TXID，就是交易哈希，供用户查询，TXID 代表了这个区块链上某一个唯一的交易，也就是类似于咱们去银行转账后提供的流水单号。

我们可以根据 TXID 可以上区块浏览器（专门用于查询交易的工具链接）上查询该币交易，比如某一笔比特币交易：

[https://blockchain.info/tx/6e64c2098b84b04a0d9f61a60d5bc8f5f80f37e19f3ad9c39bfe419db422b33c](https://blockchain.info/tx/6e64c2098b84b04a0d9f61a60d5bc8f5f80f37e19f3ad9c39bfe419db422b33c" \t "_blank)

网址 [https://blockchain.info](https://blockchain.info/" \t "_blank) 后面这一长串就是 TXID，下图是这一笔比特币交易的详细信息。

﻿﻿

（比特币交易详细信息）

6. 发送代币给别人

如果要把代币发送给别人，那么需要别人提供什么呢？对，就是钱包地址，这和银行转账需要别人提供银行卡号的道理一样。

﻿﻿

（某币种钱包转账） 如上图，咱们填写好表单以后，点击“确认转移”即可：钱包程序将为你生成一笔区块链交易并广播出去，大约等待 1 分钟就会被打包进区块，这个交易在任意的区块链浏览器上可以查询得到，咱们可以使用另外一个区块浏览器进行查询：

[https://explorer.mvs.org/#!/tx/b3eb07276dbff703ecf9e4180a2bd8e58db346e55439ef831efcbbd958726a0c](https://explorer.mvs.org/" \l "!/tx/b3eb07276dbff703ecf9e4180a2bd8e58db346e55439ef831efcbbd958726a0c" \t "_blank)

这个区块链浏览器与上面一个区块浏览器不是同一个，但是都可以查询相同的交易，因为他们同属同一个主网（mainnet, 相对应的是测试网 testnet）。

各大交易所的充值功能，其实就是从自己的钱包转账到交易所的钱包地址，详细的充值和提币流程咱们会在后面的“弄懂数字货币交易平台”一文中详解。

总结

今天我带你过了一遍数字货币的参与过程，我们先介绍了钱包，接着介绍了钱包地址，以及尝试购买了一些代币，然后提币到个人钱包当中进行了测试。

为了确认交易是否达成，我们还介绍了区块浏览器，最后还教你如何将代币转移给其他人。这一篇文章虽然使用了特定的两个例子，但是在绝大多数数字货币钱包中，使用方式都是类似的。

最后，给你留下一道思考题，这一篇文章我们仅仅讨论了如何购买，那么数字货币挖矿的过程会是怎样的呢？你可以给我留言，感谢你的收听，我们下期再见。

第7讲 | 区块链的常见误区﻿

经过了我前面几篇文章的铺垫讲解，你应该已经对区块链的知识体系已经有了一个基本的了解，但是，区块链是一项新兴的事物，大多数人依然处于知识的迷雾区，对区块链的理解并不是十分透彻。

我在很多场合都做过区块链领域的分享，有趣的是，无论是线上还是线下，大家都会问我一些相似的问题，今天，我就跟你一起聊聊几类理解区块链的常见误区。观点仅代表我个人的看法，也希望你可以提出不同的见解。

1. 数字货币没有背书，我为什么要用呢？

在各种场合聊起数字货币时，我都会被问到这个问题。

其实，这个问题不是单纯一个数字货币的问题，而是货币发展的问题。

因为我们从小就被灌输了“钱可以买到东西”，所以信用货币的概念已经成了一种本能反应，这种本能反应会让我们觉得信用货币的存在是那样的理所应当，同时也自然而然地会把信用货币的概念代入到数字货币当中。

所以，这个时候，我们首先要跳出自己的视野局限。

如果你穿越成唐代人，忽然讨论起人民币这种特殊的纸可以买米买粮，其他唐代人肯定不买账。因为大家只认金子和银子。同理，当我们在讨论数字货币的时候，你完全套用信用货币的概念势必难以兼容，这与唐代人处境是不是相似呢？

并且，信用货币的体系并不是完美无缺的，首先是它在刚出现的时候不是特别的稳定，发展过程一波三折。一战和二战期间的经济问题，或多或少都与当时的货币设计缺陷有关，现代信用货币的设计都是建立在这些血的教训上的。

其次是信用货币是与国家利益息息相关的。比如国家之间的贸易战，通常会在本国货币政策上所有体现。

所以当我们在讨论数字货币的时候，先要想清楚我们到底在讨论什么，因为我们没有讨论任何基于国家的信用货币体系，我们在讨论的是一个完全崭新的虚拟货币体系。

很多人理解信用货币的方法很简单，比如我经常遇见的观点有：我相信法币是因为有政府背书。

但如果我们换个角度想，选择相信其实是个人行为。如果某种资产具有非常高度流动性，比方说美元，在东南亚或者中东地区，如果你不接受美元支付，美国政府也不会拿你怎么样，这桩生意你不做总有人做。

所以你通常会换个思路，我先接受，待会换成人民币不就好了，数字货币也是同理，充足的流动性本身就可以为资产提供良好的背书。

如果硬要说一说数字货币的背书，我认为，社区本身就是一种背书。

社区由用户、开发者、矿工三者组成的。

他们之间的利益相互绑定，用户使用数字货币决定了市场价格，开发者为数字货币开发了更多的功能来提升生产效率，矿工是系统的维护者，三者包含了数量巨大的个体，每个个体都相当于为数字货币作了背书。

2. 数字货币是不是投机炒币？

另外还有一种误解来自于行业之外的人，认为数字货币就是投机、就是炒币。其实不是这样的，数字货币出现的初衷并不是为了投机炒币，而是希望构造一个点对点的去信任系统，只是在发展过程中被投机主义者大肆利用了。

确切的说法应该是数字货币的特性刚好满足投机者的需求，即使没有数字货币，投机主义也会存在并且长期存在，而且投机在金融领域并不是一个贬义词，它也是中性词汇。

投机者为整个交易市场提供了充足的流动性，商品价格波动风险被所有投机者所稀释，这是一个健康的交易市场所必备的。所以数字货币是中立性的工具，我们应当理性看待。

3. 区块链是不是万能的？

很多人接触了区块链以后，觉得看什么都想拿区块链来做。但是，你忽略了一点，区块链本身也属于分布式系统，分布式系统有哪些局限、哪些约束，区块链一样也有。

需要指出的是，区块链领域有个说法叫做“不可能三角”，意思是说区块链的“去中心化”“安全”“环保”三个要素不可能同时全部满足。

这个说法我没有仔细论证，个人感觉这三个指标并不好量化，所以未必成立。本着学术严谨的原则，我不作过多的评价。

反而在分布式领域，有个著名的 CAP 定理。

在 CAP 中，Consistency 是一致性，表示同样数据在分布式系统中所有地方都是被复制成相同；Availability 是可用性，表示所有在分布式系统活跃的节点都能够处理操作且能响应查询；Partition tolerance 是分区容忍性，表示不同节点之间数据同步有意外情况产生时，能够容错。

一般情况下，CAP 理论认为你不能同时拥有上述三种，只能同时选择两种。所以，当我们应用到区块链上时，可以明显地发现区块链其实是一个 AP 系统，尤其在 A 这个指标上，也就是可用性做得非常好，所以相应地，C 就会降低，反映到具体系统中的交易吞吐量上，自然会也会降低。

当我们在分区容忍性和一致性中做取舍的时候，如果强调“不可篡改”“去中心化”这两个特性，就会明显感觉到区块链跟不上大吞吐量的业务。

所以理解了以上内容，我们在做技术选型时，如果去中心化不是强需求，还是建议你使用中心化的解决方案。

4. 去中心化是不是区块链唯一的评价标准？

既然谈到了中心化，我们就来看看“你是否应该去中心化”的话题，自区块链发展至今，“中心化”和“去中心化”的争论就一直存在。

支持去中心化的观点认为：区块链的初衷就是去中心化，所以也衍生出一条准则：“凡是没有做好去中心化指标的系统都不是区块链”。

持有这样观点的人通常都跟我一样是技术出身，或多或少都有些理想主义的极客情怀，这一点本来是无可厚非的，但市场是逐利的，情怀其实常常并没有办法变现。

所以，这导致的最直接结果就是：秉持这种去中心化原则会让区块链的落地过程异常缓慢。

持有“去中心化是唯一准则”这样的观点，往往也会误导刚刚入门的业务和产品相关的人员，误以为去中心化是区块链产品的一条评价标准。

其实并不是这样，去中心化只是一个公有区块链应当具备的基本特性，但是我们衍生到区块链应用层面的时候，其实去中心化往往并不能契合到一个公司的业务上，所以我在这里提倡：当我们在思考区块链的解决方案时，还是应当以需求为第一导向。

事实上，我们在讨论去中心化的时候，更多是夹杂了对强势的不满，这其实可以转化成“对服务者进行监督”的思路，一味地强调去中心化可能会陷入舍本逐末的尴尬境地，我们一定要看需求是什么，再去选择要不要。

换句话说，任何情况下，人与人之间必然存在信息不对称和认知不对称的问题，任何应用都会存在信息提供者和信息消费者这两种角色。

这是由人类社会结构决定的，妄图消除这两种角色之间的差异是非常难的。所以应用的“去中心化”要问运营者和消费者，而不是空喊口号。

有个常提及的词叫做“赋能”，被赋于能力的角色始终处于被动地位的，我们可以把区块链看做新型的赋能工具，至于是不是去中心化，设计过程中要看具体的应用场景，实施过程最终取决于消费者。

5. 联盟链为什么没有公有链普及？

我相信很多人入门区块链以后都会有个疑问，区块链这么火热，怎么都是公有链热度高，联盟链反而声响不大。

所谓联盟链，就是这个区块链具有准入许可，不像公链，任何人都可以随时进入，准入许可意味着候选节点进入区块链时，需要得到已经在网络中的节点的许可，所以联盟链也叫做许可链。联盟链的节点数通常不多，维护成本相比公链要低。

造成联盟链不普及的原因，有以下三种。

第一是观察者偏差，因为 To B 的业务往往是商务合作的形式，并不直接进入大家的视野，实际上有很多大型机构已经尝试，或者已经部分落地了的联盟链业务。

第二是联盟链往往会遇到政策和监管要求，与公链相比，实施起来条条框框太多了，发挥的空间有限。

第三是联盟链表面上是一个技术问题，本质上是一个博弈问题，这是我 2016 年在文章《论联盟链的局限性与公有链》表达过的一个观点。

你往往需要设计一个业务模型，使得所有的博弈趋于均衡稳定，但是这又非常困难，我们无法一概而论。

总不能每做一块业务还要搞个形式化验证吧，并且联盟链无论是应用生态还是技术迭代都会比公链缓慢。

所以整体上看，联盟链的应用范围仍然不及公链广泛。

6. 区块链是否会颠覆当下互联网？

很多早期的区块链文章经常说：区块链会颠覆当下的互联网什么的，关于这一点，我其实持保留意见。区块链如何打通与现有互联网的界限还是一个未知数，最大的可能性仍然是区块链成为互联网的一部分，作为底层设施改进了原来互联网的架构。

第8讲 | 最主流区块链项目有哪些？﻿

这篇文章是区块链基础部分的最后一篇，在今天的内容里，我会介绍一些主流、热门的区块链项目，同时，我也会介绍一些创新型的区块链项目，希望可以让你对区块链的行业有一个大体的认知。

由于区块链项目数量众多，我仅从市值前 100 的项目中，挑选一些我比较熟悉的区块链项目进行讲解。

区块链行业的发展非常迅速，币种市值排名的波动幅度也比较大，例如，在 2017 年 8 月以前，比特现金项目还没有上线，如今已经是常霸市值 Top5 的区块链项目之一。

现在，常霸 Top3 的区块链项目分别是比特币、以太坊、瑞波币。那么，这些币种到底是做什么的呢？为什么市值会经常波动呢？联盟链项目为什么没有出现在这里呢？今天，我就一一为你介绍这些问题。

主流区块链项目

1. 比特币

由于比特币项目已经为大家所熟知，所以在这里，我就简单介绍一下参数，不再过多介绍。总体来看，比特币的市值和交易量远远超过其他区块链项目。

比特币的发布时间为 2009 年 1 月 9 号，预计它的挖矿可以一直持续到 2140 年，发行总量收敛到 2100 万。比特币的出块时间是 10 分钟，出块时间是指全网平均产生一个区块的时间间隔。

比特币是所有数字资产的始祖，这带来的效果就是：比特币的公众认可度非常高，纵然面临着矿池中心化 （关于矿池中心化的问题会在后面的“深入区块链技术”部分内讲解）的问题，但是公众依然非常信任比特币这种资产。

比特币曾经面临过区块容量不足的问题，但随着隔离见证（关于隔离见证的问题，也会在后面“深入区块链技术”的部分进行讲解）的生效，网络拥堵的问题缓解了很多。具体细节我们留到“比特币专题”中再做详细叙述。

2. 以太坊

以太坊是一个区块链应用平台，它的极大创新在于它提供了智能合约这种可以自定义业务逻辑的工具，智能合约是一种可编程的合约，合约是由用户编写并且部署到区块链上的。

以太坊的优势是为全世界的开发者们提供了一种开发工具，这种工具让所有人都能释放出巨大的创造力，所以基本上可以看成：只要是有一定技术基础的开发者，通过智能合约可以随时为以太坊贡献内容。

这形成了一种良性循环，开发者使用智能合约的时候，发现的问题提交给以太坊开发者社区，社区改进智能合约的缺陷，新的开发者基于智能合约开发多样性的工具包，这种核心开发者与社区互动的良性循环是以太坊生态最重要的一部分。

以太坊的口号是“世界计算机”，从这句口号里，可见它野心的大小。

在 2016 年的时候，以太坊的市值大约是比特币的十分之一，在 2017 年，这个数字已经达到四分之一。

以太坊在 2014 年开始众筹，2015 年 3 月份正式运行，它采取的共识机制是 PoW，但根据核心团队公布的方案，后期会逐渐迁移到 PoS 共识算法。以太坊的总发行量是：6000 万 +1872 万 / 年，目前的区块时间是 12 秒。

同时我们从以太坊社区可以看到，以太坊绝大部分开发流程和智能合约都已经形成行业标准，比如常见的 ERC20 代币标准，ERC725 身份标准。

而 ERC20 代币标准，则为智能合约指明了主要的业务方向：数字资产，有的叫智能资产，它们的含义差不多。以太坊 2017 价格大幅上涨，最直接的原因就是：ERC20 代币成为事实意义上的区块链标准资产。

3. 瑞波币

瑞波币（Ripple）是一个比较另类的区块链项目，因为从本质上来说，它更像是一种支付结算协议，瑞波币不需要挖矿，它是通过一种叫“Open Coin”的算法，提供瑞波协议共识来达到记账的目的。

瑞波币旨在为全球跨境机构提供了高效率的支付过程，提供较好的全球支付体验。因为涉及了机构之间的资产转移，瑞波币被设计成需要准入许可才能进入瑞波的支付网络，这一点有些像我们所说的联盟链。

瑞波团队掌握了一半以上的瑞波币，所以瑞波币面临的币价被操纵的问题很严重。如果你是一个技术极客，那么你可以略过该项目。如果你想创建一个有关支付结算的区块链项目，那么一定要研究瑞波币。

4. 莱特币

如果我们仔细观察，会发现比特币的 Logo 颜色为金色，而莱特币的 Logo 的颜色为银色。一金一银，相信你应该明白莱特币的定位了。

莱特币在技术上仅仅把比特币的挖矿算法修改成了 Scrypt 算法，Scrypt 算法是一个可参数化、可配置的挖矿算法，不过它依然没有防住专业矿机的出现。它的其他核心代码几乎与比特币保持一致。

莱特币的崛起得益于良好的市场运作，从提供的功能来看，莱特币与比特币没有区别。那么说，为什么还要有莱特币呢？

是这样的，比特币扩容之争的核心焦点在是否使用“隔离见证”的方法，我们其实知道，“隔离见证”虽然在比特币社区提出，但是第一个应用的地方是莱特币，相信你能看出这里的逻辑，即：莱特币作为比特币的先行者，它会替代比特币做一些具有实验性质的试运行。

5. 比特现金

目前比特现金市值排名基本在 Top5 左右，与比特币相比，比特现金仅仅是从区块容量上高于比特币，其他技术上的区别并不是很大。

比特现金的诞生要从比特币扩容之争开始谈起，由于比特币的区块容量是 1MB，随着用户增多，交易愈发拥堵。

所以围绕着提升网络容量，社区内部发生了分歧，“支持隔离见证”与”支持直接扩大区块尺寸”分成了两派，这就是著名的扩容之争。

比特币核心开发者们支持前者，矿工们支持后者，由于比特币核心开发者掌握了代码的控制权，但是矿工掌握了记账权，所以两权发生了分离，矿工索性一拍大腿，你不改代码，我花钱找人改，这就产生了比特现金。

比特现金作为社区共识分裂的产物，体现了区块链开放共识的特点，你不支持我，我分分钟就可以独立出来。

6.Tether

Tether 也是一个特殊的区块链项目，它为所有区块链资产提供了法币（主要是美元）兑换网关。

Tether 又称 USDT，言外之意就是和美元一对一锚定，用户存入多少美元，就会产生多少 USDT 进入虚拟资产网络。USDT 可以直接在虚拟货币交易所与比特币等其他区块链资产进行交易。

Tether 可以直接在二级市场流通，是数字货币交易市场重要的交易入口。另外，Tether 可能存在被冻结和没收的风险。

7. 匿名性区块链项目

匿名性区块链项目是指：使用交易匿名技术，让公开可查询的交易内容变成私密的匿名性区块链项目。市值比较不错的有门罗币、达世币、Zcash 三种，它们分别使用了不同类型的匿名技术，为区块链技术的匿名特性发展做出了贡献。

从需求上来看，这三种都是为了解决其他所有数字货币无法匿名的问题，因为从技术上看，比特币也好，以太坊也好，交易是可以被追踪的。

所以以上三种区块链提供了不同程度的匿名，按照匿名程度分别是：达世币 < 门罗币 <Zcash。从市场认可度来看，门罗币的匿名性最为人们所认可。

国内的公有区块链项目

中国的公链项目不多，分别有 NEO、量子链、元界、公信宝、比原链。

目前市值最高的是 NEO，NEO 的前身是小蚁，在经历了 2017 年初的市值低谷之后，NEO 通过品牌重塑以及市场推广，目前已经稳居市值 Top10。

NEO 主打的也是智能合约，不过相比以太坊，NEO 更有方向性，旨在通过智能合约塑造一个基于区块链的智能经济。NEO 的创始人达鸿飞，也是一个非常 Nice 的大叔。

量子链是也是国内比较知名的区块链项目，它的市值稳居 Top20，与 NEO 不同的是，量子链完全支持以太坊智能合约，也就是说能在以太坊上运行的智能合约也能在量子链上运行。

量子链的创始人是戴旭光，人称帅初，是一个不到 30 岁就登上福布斯的技术极客。

元界在 2017 年初上线造成了一波市场轰动，元界是当时唯一一家既能提供数字货币交易平台服务，又能提供公链技术服务的技术团队，2017 上半年整个市场非常看好。

随即创始人初夏虎基于元界发了两个代币，由于这两个代币的运作没有跟上，导致市场恶评不断，再经过 9.4 的一刀切式监管，元界项目坠入低谷。

公信宝是比特股社区的开发者，将比特股的底层技术石墨烯技术改造成属于自己的公链项目，公信宝团队是一个靠谱的团队，市场价值也十分不错。

比原链是巴比特社区创始人长铗发起的，比原链目前负责人是段新星，比原链也是一个致力于打造资产数字化，提供资产流通的一个公链平台。

第二篇：深入区块链技术

第9讲 | 深入区块链技术（一）：技术基础

在“浅说区块链基础”的部分中，我概括介绍了区块链的入门知识以及区块链的应用领域，在“深入区块链技术”部分的第一篇中，我将带你一起总览下区块链的技术概要，本篇提到的所有技术内容，我们都会在后续文章中进行详细的讲解。

区块链的技术定义

简单来说，区块链是一个提供了拜占庭容错、并保证了最终一致性的分布式数据库；从数据结构上看，它是基于时间序列的链式数据块结构；从节点拓扑上看，它所有的节点互为冗余备份；从操作上看，它提供了基于密码学的公私钥管理体系来管理账户。

或许以上概念过于抽象，我来举个例子，你就好理解了。

你可以想象有 100 台计算机分布在世界各地，这 100 台机器之间的网络是广域网，并且，这 100 台机器的拥有者相不信任，那么，我们采用什么样的算法（共识机制）才能够为它提供一个可信任的环境，并且使得：

节点之间的数据交换过程不可篡改，并且已生成的历史记录不可被篡改；

每个节点的数据会同步到最新数据，并且会验证最新数据的有效性；

基于少数服从多数的原则，整体节点维护的数据本身可以客观反映交换历史。

通常我们在分布式系统领域也见到过上述的要求，比如第 2 条就阐述了分布式系统基本要求：一致性要求；基于少数服从多数原则是为了容忍网络分区；区块链就是解决上述问题的技术方案。

我们结合以往讲过的内容，和将要讲的内容，先提炼一下区块链在技术上的 7 个特征，你先记住，我们后续会慢慢道来：

区块链的存储基于分布式数据库；

数据库是区块链的数据载体，区块链是交易的业务逻辑载体；

区块链按时间序列化区块数据，整个网络有一个最终确定状态；

区块链只对添加有效，对其他操作无效；

交易基于非对称加密的公私钥验证；

区块链网络要求拜占庭将军容错；

共识算法能够“解决”双花问题。

区块链的类型

我们在讨论区块链时，通常指的是公有区块链。除此之外，还存在另外一种区块链：联盟链。

我们在前面的文章介绍过它。所谓联盟链，就是这个区块链具有准入许可，不像公链，任何人都可以随时进入。准入许可也就意味着候选节点进入区块链时需要得到已经在网络中的节点许可，所以联盟链也叫做许可链。

早期文章里可能还会涉及私有区块链的定义，其实我认为私有区块链更像是一个捏造的概念，如果是完全私有的分布式数据库，技术人员往往会有更好的选择。

如今云计算日趋成熟，大规模的分布式存储已经不是难题，不必在区块链这种低并发、低吞吐量的系统中折磨自己。

所以我们所说的区块链通常指的是公链。除了公链和联盟链的概念，还有一种区块链概念，叫作侧链。

侧链是一种双向挂钩技术，将主链中的代币锁定到侧链中使用。所以可以将主链看作主干道，侧链看作与主链相对独立的一条分支道，作为主链功能的低耦合拓展。

区块链的核心技术组成

无论是公链还是联盟链，至少需要四个模块组成：P2P 网络协议、分布式一致性算法（共识机制）、加密签名算法、账户与存储模型。

1. P2P 网络协议

P2P 网络协议是所有区块链的最底层模块，负责交易数据的网络传输和广播、节点发现和维护。

通常我们所用的都是比特币 P2P 网络协议模块，它遵循一定的交互原则。比如：初次连接到其他节点会被要求按照握手协议来确认状态，在握手之后开始请求 Peer 节点的地址数据以及区块数据。

这套 P2P 交互协议也具有自己的指令集合，指令体现在在消息头（Message Header) 的命令（command）域中，这些命令为上层提供了节点发现、节点获取、区块头获取、区块获取等功能。

这些功能都是非常底层、非常基础的功能。如果你想要深入了解，可以参考比特币开发者指南中的 Peer Discovery 的章节。

2. 分布式一致性算法

在经典分布式计算领域，我们有 Raft 和 Paxos 算法家族代表的非拜占庭容错算法，以及具有拜占庭容错特性的 PBFT 共识算法。

如果从技术演化的角度来看，我们可以得出一个图，其中，区块链技术把原来的分布式算法进行了经济学上的拓展。

在图中我们可以看到，计算机应用在最开始多为单点应用，高可用方便采用的是冷灾备，后来发展到异地多活，这些异地多活可能采用的是负载均衡和路由技术，随着分布式系统技术的发展，我们过渡到了 Paxos 和 Raft 为主的分布式系统。

而在区块链领域，多采用 PoW 工作量证明算法、PoS 权益证明算法，以及 DPoS 代理权益证明算法，以上三种是业界主流的共识算法，这些算法与经典分布式一致性算法不同的是融入了经济学博弈的概念，下面我分别简单介绍这三种共识算法。

PoW：通常是指在给定的约束下，求解一个特定难度的数学问题，谁解的速度快，谁就能获得记账权（出块）权利。这个求解过程往往会转换成计算问题，所以在比拼速度的情况下，也就变成了谁的计算方法更优，以及谁的设备性能更好。比特币本身的演化很好地诠释了这个问题，中本聪设计的思路本来是由 CPU 计算。随着市场发展，人们发现 GPU 也可以参与其中，而且效率可以达到十倍百倍，现在，这项工作基本以 ASIC 专业挖矿芯片为主。

PoS：这是一种股权证明机制，它的基本概念是产生区块的难度应该与你在网络里所占的股权（所有权占比）成比例，目前有三个版本 PoS1.0、PoS2.0、PoS3.0。它实现的核心思路是：使用你所锁定代币的币龄（CoinAge）以及一个小的工作量证明，去计算一个目标值，当满足目标值时，你将可能获取记账权。

DPoS：简单来理解就是将 PoS 共识算法中的记账者转换为指定节点数组成的小圈子，而不是所有人都可以参与记账，这个圈子可能是 21 个节点，也有可能是 101 个节点。这一点取决于设计，只有这个圈子中的节点才能获得记账权。这将极大地提高系统的吞吐量，因为更少的节点也就意味着网络和节点的可控。

3. 加密签名算法

由于我不是密码学专业出身，所以这里我将会以介绍为主。

在区块链领域，哈希算法是应用得最多的算法。哈希算法具有抗碰撞性、原像不可逆、难题友好性等特征。

其中，难题友好性正是众多 PoW 币种赖以存在的基础，在比特币中，SHA256 算法被用作工作量证明的计算方法，也就是我们所说的挖矿算法。

而在莱特币身上，我们也会看到 Scrypt 算法，该算法与 SHA256 不同的是，需要大内存支持。

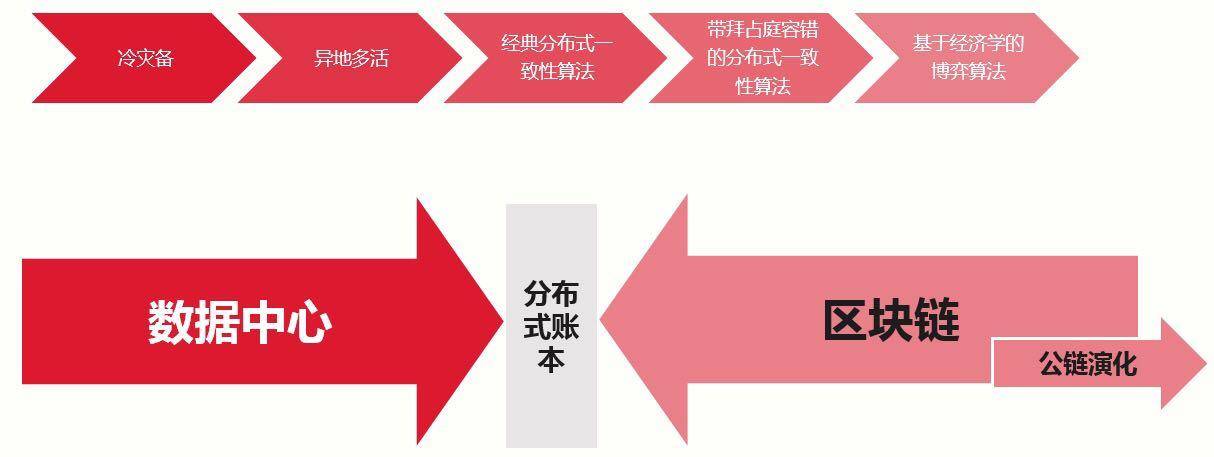
而在其他一些币种身上，我们也能看到基于 SHA3 算法的挖矿算法。以太坊使用了 Dagger-Hashimoto 算法的改良版本，并命名为 Ethash，这是一个 IO 难解性的算法。

当然，除了挖矿算法，我们还会使用到 RIPEMD160 算法，主要用于生成地址，众多的比特币衍生代码中，绝大部分都采用了比特币的地址设计。

除了地址，我们还会使用到最核心的，也是区块链 Token 系统的基石：公私钥密码算法。

在比特币大类的代码中，基本上使用的都是 ECDSA。ECDSA 是 ECC 与 DSA 的结合，整个签名过程与 DSA 类似，所不一样的是签名中采取的算法为 ECC（椭圆曲线函数）。

从技术上看，我们先从生成私钥开始，其次从私钥生成公钥，最后从公钥生成地址，以上每一步都是不可逆过程，也就是说无法从地址推导出公钥，从公钥推导到私钥。

﻿﻿

4. 账户与交易模型

从一开始的定义我们知道，仅从技术角度可以认为区块链是一种分布式数据库，那么，多数区块链到底使用了什么类型的数据库呢？

我在设计元界区块链时，参考了多种数据库，有 NoSQL 的 BerkelyDB、LevelDB，也有一些币种采用基于 SQL 的 SQLite。

这些作为底层的存储设施，多以轻量级嵌入式数据库为主，由于并不涉及区块链的账本特性，这些存储技术与其他场合下的使用并没有什么不同。

区块链的账本特性，通常分为 UTXO 结构以及基于 Accout-Balance 结构的账本结构，我们也称为账本模型。UTXO 是“unspent transaction input/output”的缩写，翻译过来就是指“未花费的交易输入输出”。

这个区块链中 Token 转移的一种记账模式，每次转移均以输入输出的形式出现。而在 Balance 结构中，是没有这个模式的。

第11讲 | 深入区块链技术（三）：共识算法与分布式一致性算法﻿

共识机制的概念，我们在前面的文章“浅说区块链共识机制”中已经讲解了一部分，但是，共识算法其实是一个非常大的话题，一篇文章肯定没有办法做到面面俱全。

那么今天的内容，我会将重点放在梳理技术的脉络上，详细分析的部分会少一点。如果你对共识算法有兴趣的话，可以自行查找相关内容，也可以和其他的资料进行相互补充的阅读。

从相亲大会说起：分布式系统的模型

由于区块链就是一种分布式系统，所以这篇文章我就从这一概念开始讲起。 为了让你更容易理解分布式系统，我们先来构建一个模型。

在“浅说区块链共识机制”那篇文章中，我举了一个村庄举办相亲大会的例子，我们来回顾一下。

大村子因为人口增长变成 11 个小村落分散在地图各地；

村落之间的通信只能依靠信鸽；

一只信鸽可能无法完全覆盖所有村落，需要有中继村落代为传输消息。

相亲大会的举办权会为村子带来巨大收益，为了产生合理的举办者，人们约定了几条规则：

大会举办权从 A 和 B 两个村子中产生，他们每一届都是候选村；

投票时所有村落仅能投 A 或 B；

用投票的方式产生举办者，少数服从多数。

所有村子会为了举办权都会使出浑身解数，比如延迟发送投票结果、篡改别人的投票结果、假装没有接收到通知等等。

其实这是一个典型的分布式系统，可以看成是我们简化版的区块链网络环境，那么这个分布式系统会遇到什么样的问题呢？

分布式系统面临的问题

分布式系统面临了几个问题：一致性问题，可终止性问题、合法性问题。

可终止性可以理解为系统必须在有限的时间内给出一致性结果，合法性是指提案必须是系统内的节点提出。当然其中面对的最重要也是最基础的问题，就是我们常说的一致性问题。

一致性是指在某个分布式系统中，任意节点的提案能够在约定的协议下被其他所有节点所认可。

需要提醒你区分的一点是：这里的“认可”表示所有节点对外呈现的信息一致，而不是对信息的内容认可。一致性也分严格一致性、最终一致性，这些我们在后文会谈到。

我们回到上面的例子，我们提到了所有的村子只能投 A 或 B，其实这个投票的动作可以理解为提案。

在“投票过程被大家所认可”这个语境下，“被大家所认可”表示某个村落投票的结果已经被记录，用于最后统计结果，而不是认可投给 A 或者投给 B，这也是我在上述强调你要注意区分的一点。

那我们这里所说的一致性到底体现在那里呢？

主要体现在下面两种类型的问题上。

非人为恶意的意外投票过程。非人为恶意篡改可归类为信鸽半路挂掉、信鸽迷路、信鸽送错目的地、信鸽送信途中下雨导致信件内容模糊、接收信件的人不在家、天气变化信鸽延迟送达等等。这些对应到分布式系统面临的问题就是：消息丢包、网络拥堵、消息延迟、消息内容校验失败、节点宕机等。

人为恶意篡改投票过程。人为恶意篡改包括“精神分裂式投票”，中继篡改上一个村落的投票信息。对应到分布式系统面临的问题就是：消息被伪造、系统安全攻击等等。发生的人为恶意篡改的过程就可以称之为系统发生了拜占庭错误（Byzantine Fault)，如果系统可以容忍拜占庭错误而不至于崩溃，也就是在发生系统被恶意篡改的情况下仍然可以达成一致，我们将这样系统称作为做拜占庭容错系统。

问题 1 我们已经有较成熟的方案了。分布式系统本质上是一种并行异步操作，如果通过中心化的手段将系统中的“并行不确定”操作变更为“同步串行”操作就能解决上述的问题。

比如让第三方机构介入托管所有人的投票；或者构造一个不可伪造令牌，大家轮流将投票统一写到令牌上。

这些也是现代分布式系统经常使用的方法。但是这些方法有个缺陷，如果在分布式系统中被过多地使用以后，系统便会越来越像单点系统。

我们设计分布式系统的初衷就是为了克服单点系统的可用性不足、扩展性不好、单点性能上限等缺陷，这种退化的方案可能不是我们想要的。

而问题 2 要求设计拜占庭容错系统，这个在 IT 行业并不常见，因为多数 IT 系统是中心化的，所以如果我们想要解决问题 2，这就引出了我们今天要介绍的共识算法与分布式一致性算法。

有关分布式系统的定理

我们在介绍具体的分布式一致性算法之前，先介绍两个定理，做一下铺垫。

第一个是 FLP 不可能性，简单来说是：即使网络通信完全可靠，只要产生了拜占庭错误，就不存在一个确定性的共识算法能够为异步分布式系统提供一致性。换句话来说就是，不存在一个通用的共识算法可以解决所有的拜占庭错误。

第二个是 CAP 定理，CAP 定理是分布式系统领域最重要的定理之一，这个我们在“理解区块链的常见误区”一文中稍微讲到过。也就是在设计分布式系统的过程中，“一致性”“可用性”“分区容忍性”三者中，我们只能选择两个作为主要强化的点，另外一个必然会被弱化。

我们由 CAP 定理可以推导出严格一致性和最终一致性。严格一致性是指在约定的时间内，通常是非常短、高精度的时间内，系统达到一致性的状态，这种系统很难实现，即使实现也很难有高的性能。

所以人们从工程的角度提出了最终一致性，最终一致性不要求严格的短时间内达到一致。为了其他两个指标，我们相当于让一致性在时间上做了妥协。区块链满足了最终一致性，而且处理过程时间比较长。

可用性其实是传统技术后端架构上非常重要的指标，从单点到主备模式、从主备模式到异地多活，再到现在的 Paxos 和 Raft 协议。

我们从软件架构上也经历了基于 ESB 的模块化 SOA 模式，到无状态的微服务架构。从工程的角度来看，根据业务需求达到 4 个 9、6 个 9 就足够了，只是肯定比不了区块链近乎 100% 的可用性。

分区容忍性在企业内部极少出现，尤其是中心化的服务性应用，所以很少考虑。然而区块链的 P2P 网络环境十分复杂，所以必须要保证很高的分区容忍性。

通过以上我们可以发现比特币、以太坊等公链是偏重高可用性、分区容忍性（AP），满足最终一致性（C）且 TPS 较低的分布式系统。

所以如果有人号称他们的区块链能够达到媲美中心化系统上万的 TPS，先别着急投资，你问问他们技术是不是知道 CAP 定理，再问问他们的去中心化程度如何。

这点我们也可以从 EOS 等高性能的区块链身上佐证，EOS 全球只有 21 个记账节点，而以太坊全球有上万个节点可以随时参与记账，所以越想去中心化，你的 TPS 就不可能高，这也就是为什么 EOS 的 TPS 高，而以太坊的 TPS 低。

接下来我来介绍一下经典的分布式一致性算法和区块链的共识算法。经典的分布式一致性算法在多数的论文中一般被叫做共识算法，在这里，我为了与区块链的共识算法做出区别，所以在命名上改成了分布式一致性算法，但是它们要解决的问题是一样的。

共识算法与分布式一致性算法

1. 经典的分布式一致性算法

经典分布式一致性算法有 Raft 协议，Raft 协议是一种强 Leader 的一致性算法，它的吞吐量基本就是 Leader 的吞吐量，它无法抵御节点恶意篡改数据的攻击。

稍微复杂一点的就是 Paxos 协议，Paxos 能提供不同场合不同种类的一致性算法，所以 Paxos 有很多变种，经典 Paxos 是 Leaderless 的，有变种是强 Leader 型的，叫做 Fast Paxos，有关 Paxos 的文献非常丰富，这里就不赘述了。

以上两种都是不提供拜占庭容错的系统，下面介绍一种具有拜占庭容错的一致性算法。

PBFT 全称实用性拜占庭容错系统（Practical Byzantine Fault Tolerance, PBFT)，PBFT 是一种状态机，要求所有节点共同维护一个状态，所有节点采取的行动一致，PBFT 非常适合联盟链等对性能具有较高要求的场合，超级账本项目中的 Fabric 框架默认采用的就是 PBFT 的修改版本。

2. 区块链共识算法

区块链的共识算法，我在某些场合直接称作基于经济学的博弈算法，以区别于经典分布式一致性算法思路，它的整体思路就是让攻击者的攻击成本远远大于收益。

区块链中的共识算法目前具有工业成熟度的是 PoW，另外两种比较成熟的是 PoS 和 DPoS，其次还有一些变种和单一币种使用的共识算法，例如 Ripple 共识、PoC 共识（概念性证明）、PoE 共识（存在性证明）。

在使用 PoW 共识算法的情况下，容错阈值是 50%，而 PBFT 及其变种的容错阈值是 33% 左右，这里的百分比是指作弊节点占全网节点的比例。

PoX 类的算法其实都延续了 PoW 的设计理念，相比较经典分布式一致性算法，PoX 类算法通过概率选择记账者降低了潜在的提案者，另外是延长了达成最终一致性的时间。

第一条降低了系统通信复杂度，每次记账系统的确定性其实是概率确定的，又由于被选中需要付出成本，此处才提高了记账成本阈值，结合区块链的基础代币设计，是一个非常天才的想法。

第12讲 | 深入区块链技术（四）：PoW共识

上一篇文章中，我们谈到了区块链其实就是一种分布式系统，它在技术上并没有跳出分布式系统的理论框架，只是给出了一种不同于计算科学领域的解决方案。今天，我们就来重点聊聊区块链的这种解决方案： PoW 共识机制。

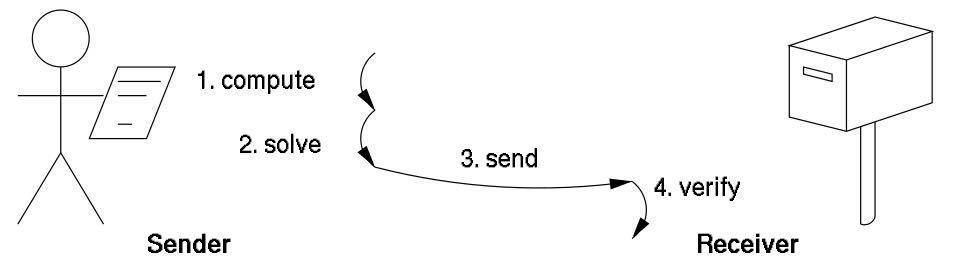
PoW 工作量证明

因为比特币采用了 PoW 共识机制，所以这个概念才得以被广泛传播。PoW 全称 Proof of Work，中文名是工作量证明，PoW 共识机制其实是一种设计思路，而不是一种具体的实现。

PoW 机制其实早在 1997 年就被提出了，它早期多被应用在抵抗滥用软件服务的场景中，例如抵抗垃圾邮件（所以 PoW在邮件服务系统会有所涉及）。

我们借用维基百科的一张图来解释一下 PoW 机制是如何用在这个场景中的。

为了防止垃圾消息泛滥，接收者并不直接接受来自任意发送者的消息，所以在一次有效的会话中，发送者需要计算一个按照规则约定难题的答案，发送给接受者的同时，需要附带验证这个答案，如果这个答案被验证有效，那么接受者才会接受这个消息。

﻿﻿

可以看出 PoW 的核心设计思路是提出一个计算难题，但是这个难题答案的验证过程是非常容易的，这种特性我们称之为计算不对称特性，我们在“浅谈区块链共识机制”中举的 24 点游戏的例子就具备了计算不对称特性。

如何理解区块链 PoW

上面介绍了一般的 PoW 是什么，那么区块链上的 PoW 又是如何设计的呢，我们还是以比特币为例子来讲一讲，这个部分会有代码演示，如果你在收听音频，可以点击文稿查看。

在分析拜占庭将军问题的时候可以看出，如果所有节点在同一时刻发起提案，那么这个系统的记账过程将会非常的复杂混乱，为了降低具有提案权的节点数量，采用工作量证明不失为一个好办法。

所以我们需要构造一个计算不对称的难题，这个难题在比特币中被选定为以 SHA256 算法计算一个目标哈希，使得这个哈希值符合前 N 位全是 0。

举个例子，假设我们给定一个字符串“geekbang”，我们提出的难题是，计算一个数字，与给定的字符串连接起来，使这个字符串的 SHA256 计算结果的前 4 位是 0，这个数字我们称作 nonce，比如字符串 "geekbang1234"，nonce 就是 1234，我们要找到符合条件的 nonce。

我们以 Python 代码作为示例。

#!/usr/bin/env python

import hashlib

def main():

  base\_string = "geekbang"

  nonce = 10000

  count = 0

  while True:

    target\_string = base\_string + str(nonce)

    pow\_hash = hashlib.sha256(target\_string).hexdigest()

    count = count + 1

    if pow\_hash.startswith("0000"):

      print pow\_hash

      print "nonce: %s scan times: %s" % (nonce, count)

      break

    nonce = nonce + 1

if \_\_name\_\_ == '\_\_main\_\_':

  main()

代码中，我规定了基础字符串是 "geekbang"，nonce 从 10000 开始自增往上搜索，直到找到符合条件的 nonce 值。

我们计算的结果放在图中，你可以点击查看。

# 前 4 位是 0

0000250248f805c558bc28864a6bb6bf0c244d836a6b1a0c5078987aa219a404

nonce: 68828 scan times: 58829

# 前 5 位是 0

0000067fc247325064f685c32f8a079584b19106c5228b533f10c775638d454c

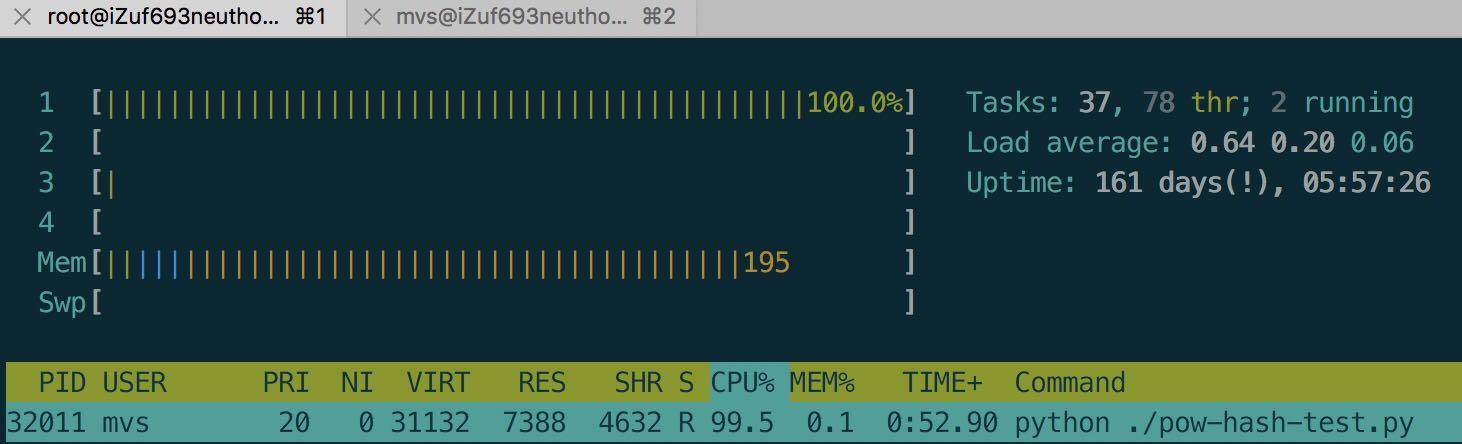
nonce: 1241205 scan times: 1231206

# 前 7 位是 0

00000003f41b126ec689b1a2da9e7d46d13d0fd1bece47983d53c5d32eb4ac90

nonce: 165744821 scan times: 165734822

可以看出，每次要求哈希结果的前 N 位多一个 0，计算次数就多了很多倍，当要求前 7 位都是 0 时，计算次数达到了 1.6 亿次。这里我同时截图了操作系统当时 CPU 的负载，可以看到单核 CPU 负载长时间达到 100%。

﻿﻿

通过上述程序，希望你对区块链 PoW 机制有个直观的了解。由于结果只能暴力搜索，而且搜索空间非常巨大，作弊几乎不可能，另外符合条件的 nonce 值也是均匀分布在整个空间中的，所以哈希是一个非常公平且粗暴的算法。

以上代码的基本逻辑就是 PoW 挖矿过程，搜索到一个目标值就会获得记账权，距离上一次打包到现在未确认的交易，矿工就可以一次性将未确认的交易打包并广播了，并从 Coinbase 获得奖励。

实际挖矿的基本步骤如下。

生成 Coinbase 交易，并与其他所有准备打包进区块的交易组成交易列表，并生成默克尔哈希；

把默克尔哈希及其他相关字段组装成区块头，将区块头（Block Header）作为工作量证明的输入，区块头中包含了前一区块的哈希，区块头一共 80 字节数据；

不停地变更区块头中的随机数即 nonce 的数值，也就是暴力搜索，并对每次变更后的的区块头做双重 SHA256 运算，即 SHA256(SHA256(Block\_Header))），将结果值与当前网络的目标值做对比，如果小于目标值，则解题成功，工作量证明完成。

如果更深程度去理解的话，PoW 机制是将现实世界的物理资源转化成区块链上虚拟资源的过程，这种转化为区块链提供了可信的前提。

PoW 挖矿的发展历程

好了，现在我们知道了，PoW 的过程其实就是计算一个难题解的过程。

在区块链的发展史上，PoW 经历了大致两个阶段。分为早期分散挖矿阶段和中心化矿池挖矿阶段。我们目前处于第二个阶段，并且将会长期处于这个阶段。

早期分散挖矿是中本聪的愿景，期望是 1CPU=1 票，所以如果 CPU 挖矿，那么将会是非常理想化的情况，而现实的情况是，SHA256 只需要非常简单的重复计算逻辑，它不需要复杂的逻辑控制。

那么 CPU这种重控制逻辑，轻重复计算的计算单元来搞这么低端的暴力计算非常吃力不讨好，大部分人的第一反应肯定是用 GPU 呀，非常正确。

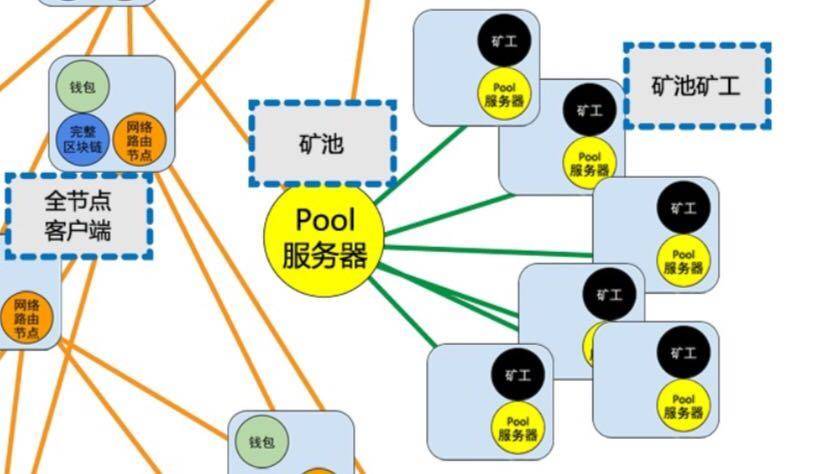
所以这个时期，出现了 GPU 挖矿，它的效率是 CPU 的十几甚至上百倍，那么 1CPU=1 票的逻辑就被打破了，挖矿工具的改变让人们意识到挖矿技术也是极大改进的。除了 GPU 挖矿，我们还有 ASIC 芯片挖矿，这部分内容我们在讨论挖矿算法分类时会详细讲解。

同期我们也慢慢进入到了中心化挖矿阶段。中心化挖矿很好理解，算力如果越分散，也就意味着竞争越激烈，如果某个节点计算出答案了，那么也意味着其他矿工这段时间的工作量几乎都白费了，投入了物理资源结果零收益，可以说是负收益。

那怎么办呢？思路就是把分散的算力汇聚到一个池子里面，这个池子我们称作矿池，就像四面八方的小溪流最终汇总成一条大江一样。

矿工参与到某个矿池，相当于矿工把算力租给矿池了，与其他矿工联合挖矿，最后看起来矿池这个节点的算力就会很大，获得记账权的概率就越大，如果这个矿池计算出了答案，将获得 Coinbase 的奖励，矿池就会按既定的分配比例打给每一位参与的矿工。

我们借用一下《精通比特币》一书中的部分图来看一下：

﻿﻿

矿池作为一个中心节点，可以被矿工连接，而在比特币全网来看，矿池节点本质上也只是一个全节点，它与其他全节点一起组成了比特币的点对点网络，特殊的地方仅仅在于它可以产生新的区块。

PoW 挖矿算法分类与简介

PoW 挖矿算法大致分为两个大类，第一类叫做计算困难，第二类叫内存困难。

这两类的区别在于对于提供工作量证明的组件要求不同。我们知道计算机的组成分为计算单元和存储单元，通过以往的编程经验我们还可以知道，一个计算机的瓶颈往往是 IO，如果要制造大量的 IO 操作，可以通过写程序撑大内存，制造大量的数据处理过程，使工作量证明从计算单元转变为存储单元。

那为什么要这么做呢？

其实在 PoW 挖矿中心化以后，又出现了一次挖矿工具改进，这次超越了 GPU，人们先是尝试在 FPGA 上尝试 SHA256 的计算过程，结果计算效率成倍于 GPU。

FPGA 出现的时间比较短暂，最终人们开发出了 ASIC 专业芯片来计算 SHA256，这就是我们常说的专业矿机。

专业矿机的出现加速了 PoW 挖矿的中心化过程，因为购买专业矿机需要额外的时间和精力，配置运行还有一定的门槛，普通人也只能从专业机构手里购买专业矿机。

所以这些专业矿机直接就是数字货币印钞机，生产专业挖矿芯片的商业公司几乎成了数字货币的货币发行司，这不得不说到市值直逼英伟达的比特大陆公司，它用的就是专业生产数字货币挖矿芯片。

新的数字货币开发者们为了防止情况重演，不断发明新的挖矿算法。有名的有 Scrypt、X11、SHA-3，不过这些依然是计算困难型的挖矿算法，依然没有逃脱出现专业矿机的命运。

这里不得不提到以太坊的 PoW 挖矿算法：ETHASH，ETHASH 是 Dagger-Hashimoto 的修改版本，它是典型的内存困难型挖矿算法。直到如今，也没有芯片厂商设计出挖矿芯片。

正如我们上文所说，因为工作量证明要求的组件从计算资源转变为内存资源，而对内存的高要求使得矿工必须加内存。

在专业矿机上加一块内存的收益与在 GPU 上加一块内存获得的收益是差不多的，所以厂商并没有研发内存困难型专业矿机的动力，没有专业矿机的出现，这从某种程度上也缓解了算力中心化的问题。

PoW 的优势和劣势

PoW 共识的内在优势在于可以稳定币价，因为在 PoW 币种下，矿工的纯收益来自 Coinbase 奖励减去设备和运营成本，成本会驱使矿工至少将币价维持在一个稳定水平，所以攻击者很难在短时间内获得大量算力来攻击主链。

PoW 共识的外在优势是目前它看起来依然是工业成熟度最高的区块共识算法，所以在用户信任度上、矿工基础上都有很好的受众。

PoW 共识最大的缺点是非常消耗计算资源，耗电耗能源，这一点也一直为人们所诟病。因为每次产生新的区块都会让相当一部分工作量证明白白浪费了，也就是将计算资源浪费了。

目前来看这个是无解的，只要是 PoW 共识，一定会遇到计算资源浪费的问题。不过人们也想了一些改进方案，早期如素数币，近期有比原币，它们都号称深度学习友好型的工作量证明方法。

从理论上来看，PoW 会一直有 51% 算力攻击的问题，即攻击者只需要购买超过全网 51% 算力设备，即可发起“双花攻击”，甚至“重放攻击”等多种高收益攻击，这个问题目前没有解决方案。

除了 51% 攻击，PoW 共识还有自私挖矿的问题，自私挖矿是一种特殊的攻击类型，不会影响区块链正常运转，但是会形成矿霸，间接造成 51% 攻击，我们就曾经遇到过这样的自私挖矿攻击。

PoW 共识机制是一种简单粗暴的共识算法，它不要求高质量的 P2P 网络资源，它可以为公链提供稳定有效的记账者筛选机制。同时它也面临了挖矿中心化严重的问题，这也促使人们研究出了新的共识机制，我们留到下一篇讲解。

第13讲 | 深入区块链技术（五）：PoS共识机制﻿

上一篇我们讲到了 PoW 共识机制，这一篇我们就来分享另外一种共识机制，PoS 共识机制。

PoS 全称是 Proof of Stake，中文翻译为权益证明。这一篇我们会将 PoS 与 PoW 对比讲解，帮助你加深理解。

PoS 的由来

PoS 最早出现在点点币的创始人 Sunny King 的白皮书中，它的目的就是为了解决使用 PoW 挖矿出现大量资源浪费的问题。PoS 共识机制一经提出就引起了广泛关注，Sunny King 也基于 PoW 的基础框架实现了第一代 PoS 区块链：点点币。

PoW 的具体实现有很多版本，但它们大多只是在挖矿算法上有所改进，主体逻辑并没有发生质的变化。PoS 包含了多个变种实现，每个变种往往会涉及区块链代币经济模型的改动，可以说是牵一发而动全身。

这些实现有点点币、黑币、未来币、瑞迪币，它们都推动了 PoS 机制的发展，PoS 研究前沿还有以太坊的 Casper ，以及 Cardano 的 Ouroboros。

那到底是什么样的机制导致 PoS 具有这样的特性呢？让我们来看一看。

什么是 PoS？

在讲 PoS 之前，我先来讲一个叫做币龄的概念，币龄这个概念其实很好理解，它的英文是 CoinAge，字面意思就是币数量乘以天数。

比如你有 100 个币，在某个地址上 9 天没有动，那么产生的币龄就是 900，如果你把这个地址上这 100 币转移到任意地址，包括你自己的地址，那么 900 个币龄就在转移过程中被花费了，你的币数量虽然还是 100 个，但是币龄变更为 0。币龄在数据链上就可以取到，任何人都可以验证。

我们回过头来看看 PoS 究竟是什么，区块链共识机制的第一步就是随机筛选一个记账者，PoW 是通过计算能力来获得记账权，计算能力越强，获得记账权的概率越大。

PoS 则将此处的计算能力更换为财产证明，就是节点所拥有的币龄越多，获得的记账的概率就越大。这有点像公司的股权结构，股权占比大的合伙人话语权越重。

以上算是简述了 PoS 的概念，实际上，PoS 的发展经历了三个版本，第一个版本是以点点币为代币的 PoS1.0 版本，这个版本中使用的是币龄；第二个版本为代表的是黑币（blackcoin），它使用的为 PoS2.0 版本，对应这个版本使用的是币数量，相当于是财产证明，后面黑币又升级到 PoS3.0，这个版本又回到了币龄。

PoW 早在比特币出现之前就已经应用了，而 PoS 是才是真正意义上为了区块链而创造出来的概念。

PoS 的实现原理

好了，现在我们开始讲解 PoS 的具体实现原理吧。这一部分公式较多，如果你在收听音频，可以点击文稿查看。

通过上一篇我们知道 PoW 挖矿的基本逻辑和步骤，我们先寻求一个 nonce小于目标值，这一步用公式可表示为：

Hash (block\_header) < Target

从公式中我们可以看到，PoW 下所有矿工的目标值是一样的，只要计算结果哈希小于目标值即可，简化来看就是前导 0 的个数。

而在 PoS 系统中，这个公式变更为：

Hash (block\_header) < Target \* CoinAge

我们可以看出多引入了一个变量叫做 CoinAge，也就是币龄，这里就有意思了。

这个变量为会造成每个矿工看到的目标值不一样，如果你的币龄越大，也就意味着你的获得答案越容易。这里的 Target 与 PoW 一致，与全网难度成反比，用来控制出块速度的。

例如当前全网的目标是 4369，A 矿工的输入的币龄是 15，那么 A 矿工的目标值为 65535，换算成十六进制就是 0xFFFF，完整的哈希长度假设是 8 位，也就是 0x0000FFFF。

而 B 矿工比较有钱，他输入的币龄是 240，那么 B 矿工的目标值就是 0x000FFFFF。你如果仔细观察肯定会发现，相比 A 矿工的目标值，B 直接少了一个零。即如下：

A 矿工 Hash( block\_header ) < 0x0000FFFF

B 矿工 Hash( block\_header ) < 0x000FFFFF

所以 B矿工获得记账权的概率肯定要比 A 高。

具体代码分析这里就不讲解了，这里需要币龄作为输入，如果我们写示例代码也只是一个简单的参数，PoS 需要放到区块链的语境中才能运作。

PoS 的相关问题

通过上述的介绍我们知道：PoS 似乎完美地解决了 PoW 挖矿资源浪费的问题，甚至还顺带解决了 51% 攻击的问题，这里可以顺便讲一下 51% 攻击是什么，它是指 PoW 矿工如果积累了超过 51% 的算力，则可以一定程度篡改账本。

这里顺便科普一下，什么是 51% 攻击呢，我们发现，矿工挖矿的成本不再是物理设备和电费，而是虚拟代币，它的边际成本几乎为零，本质上 PoS 让挖矿者和使用者合二为一了。

这也意味着如果挖矿者发起 51% 攻击，就需要拥有全网 51% 的币或币龄，这几乎不可能办到，即使你成功地实施了 51% 攻击，那么也意味着作为全网最大的持币大户的你，损失也会最大。

PoS 看起来相当完美，其实并不然，PoS 有很多缺陷。

PoS 遇到的第一个问题就是币发行的问题。一开始的时候，只有创始区块上有币，意味着只有这一个节点可以挖矿，所以让币分散出去才能让整个网络壮大，那么如何分散出去又是另外一个难题了。

所以早期 PoS 币种基本都采用了分阶段挖矿，有的叫混合挖矿，其实，我并不同意混合挖矿这个说法，混合就意味着同时。很多币种其实是分了阶段的，即第一阶段是 PoW 挖矿，到第二阶段才是 PoS 挖矿。

随着 ERC20 类型的标准合约代币的出现，这个问题被解决了，不再需要第一阶段改成 PoW，也可以将代币分散出去。

第二个问题是由于币龄是与时间挂钩的，这也意味着用户可以无限囤积一定的币，等过了很久再一次性挖矿发起攻击；所以解决方案是：PoS 机制需要引入一个时间上限来控制时间因素的自然增长。

第三个问题是虽然引入了时间上下限，用户还是倾向于囤积代币，这会造成币流通的不充分；基于此，所以瑞迪币引入了币龄按时间衰减，构造了权益速度证明，鼓励用户流动代币，而不是倾向于囤积代币。

第四个问题是离线攻击，即使引入了时间上下限，时间仍然是自然流动的，也就是可以不需要求挖矿节点长时间在线。挖矿是可以离线的，这简直是灾难，所以任意一个 PoS 机制的实践形式都必须避免这个问题，因为网络节点数量的多少直接关系到区块链网络的健壮性。

当然这些问题都不是致命问题，还记得我们一开始提到了 PoS 经历了三个版本，而第二个版本 PoS 2.0 使用的不是币龄，而直接是币的数量。

这会造成完全不同的结果，上述第二、三、四问题都不存在了，似乎看起来直接使用币的数量会更好一些，但却出现了整个 PoS 机制的致命问题。

这个问题叫做 Nothing at Stake，翻译过来叫做无成本利益问题。大体的意思在 PoS 系统中做任何事几乎没有成本，比如在 PoS 系统上挖矿几乎没有成本，这也就意味着分叉非常方便。

方便到什么程度呢，每个诚实矿工在产生孤块的时候都可以继续挖下去，反正也没什么成本，反正分叉链和主链都可以同时挖，也就是任何持币较少的用户都可以尝试分叉，并且把分叉链广播出去。

这个时候如果其他诚实矿工看到了，第一反应也是没有成本，那么咱们也来挖吧，说不定什么时候就值钱了，意思就是说任何逐利的矿工并不会使这个系统变得更强壮稳定，而是更加的混乱。

无成本利益问题无论以币龄还是币数量作为 PoS 的参数，都无法避免。

而 PoW 则没有这样的问题，我们回到 PoW 系统中来看，因为任何的分叉都会造成挖矿成本直接变成负收益，所以这会抵抗分叉的产生，矿工倾向于跟随“最长”的链。

由于以太坊部分采用了 PoS 共识，它的名字叫做 Casper，它必须解决上述无成本利益问题攻击。所以 Casper 协议要求PoS 矿工需通过抵押保证金的方法对共识结果进行下注，具体实践结果我们还需要拭目以待。

总结

最后我们来总结一下 PoS 共识机制，PoS 的区块链系统无需外部物理输入，所以它相比 PoW 更为环保不费电，并且矿工就是使用者，这会在一定程度上抵御了 51% 攻击，所以基于 PoS 机制的数字货币属于理想状态的数字货币。

PoS 的缺点是缺乏工业级的区块链应用，从逻辑上来看有点循环自证明的味道，就是用自己的币来维护系统的安全，而币的安全性是由系统保证的，所以现阶段 PoS 共识机制往往不是独立运行的，而是混合了 PoW 一起运行，这就可以弥补 PoS 的缺陷。

PoS 共识机制目前也出现了矿池，也可能会出现中心化挖矿的风险。

虽然 PoS 共识机制未来变数依然很多，但它的可塑性比 PoW 好，技术上的探索空间大，目前 PoS 币种相比较 PoW 币种风险也较高。

第14讲 | 深入区块链技术（六）：DPoS共识机制﻿

上一篇文章里，我们讲解了 PoS 共识机制，这一篇我们来分享 PoS 的一个扩展机制，这个机制在业界也非常的流行，它叫做 DPoS 共识机制。DPoS 全称是 Delegated Proof of Stake，中文翻译过来是代理权益证明。

从 BM 开始聊起的故事

我们聊 DPoS 时，为什么要从 BM 聊起呢，

其实，这和聊比特币绕不开中本聪一样，DPoS 是 BM 一手创造的。DPoS 不是独立提出的共识算法，而是直接被 BM 应用到比特股项目中，在稳定运行了 3 年多后，又接着被 BM 构造成可复用的区块链工具箱：石墨烯。

虽然应用得很早，但 DPoS 算法直到 2017 年才被 BM 单独拎出来作了一篇“DPoS 技术白皮书”，这期间伴随着比特股、Steemit、EOS 三个项目的依次发布。

那么到底 BM 是谁，市场上对这个人的评价为什么富有争议呢？或许我们从了解 BM 开始，才能体会到 DPoS 的精髓。

我们在前面的文章中曾简单提过 BM，BM 的本名是 Daniel Larimer，由于他的 GitHub 昵称是 ByteMaster，所以才被称作 BM。BM 是比特股、Steemit、EOS 项目的创始人，截止发稿时，这三个产品的市值均在区块链项目的 Top33 以内。

与年少成名 V 神的辍学经历不同，BM 2003 年毕业于弗吉尼亚理工学院，获得计算机学士学位，算是正经的科班出身。

BM 曾直言不讳地说到：“我的人生目标就是找到自由市场的方案来保护生命、自由和财产”。他认为要达成这个目标，就必须要从货币开始。

我们在数字货币一节提到过，无论是贵金属还是信用货币，都是历史的必然，所以在选择使用什么货币上，BM 认为不一定是美元，他希望的是：构造一种自由安全的数字货币。

2009 年，他怀揣梦想开始了数字货币的事业，他先发现了比特币，于是不遗余力地推广着这个项目。

然而在 2010 年，BM 指出中本聪 10 分钟一次的交易确认时间太长了，这样的话，性能会是一个瓶颈，然而这样的想法却遭到了中本聪的暴击：看不懂就算了，我没时间搭理你。

于是，BM 觉得比特币不是希望，便着手开发第一个项目——比特股，同时创造出 DPoS，把自己的高性能共识算法想法形成了实践。

在这里，我们可以看出 DPoS 与其他共识机制的第一个区别，就是交易确认时间短。

2014 年，当 V 神还在到处奔走，开始发起以太坊项目的众筹时，当很多项目还是基于比特币的微创新时，比特股就已经横空出世了。

所以比特股一跃成为了当时的明星项目，它的口号是“Beyond Bitcoin”，在这里我们可以感受到极强的攻击性和目的性，也正因为如此，日益强大的比特币社区被树在了它的对立面。

比特股一共有 2 个版本，比特股在 1.0 版本之前，某些版本甚至都没有提供向下兼容。虽然后来正式发布了 1.0 版本，似乎并没有改善多少。糟糕的使用体验，庞大的系统资源开销，还是让尝鲜的用户逐渐流失了。

这时候 BM 利用了自己手里超过 1/3 的记账节点，在没有达成社区共识的情况下，强行增发了比特股总量。这一招几乎就是比特股项目的灭顶之灾，社区人就此纷纷退出。

虽然社区萎靡，BM 还是继续了开发工作，将比特股升级到了 2.0，它的易用性和稳定性勉强可以满足正常使用。随着比特股 2.0 的发布，BM 也同时发布了石墨烯工具箱。

尽管在技术上提供了改进，但比特股社区最终选择让 BM 离开比特股项目，比特股回到了另一位币圈大佬——巨蟹的手里。随后比特股的发展陷入了长期的低迷，长期在 2 分，最多到 2 角钱左右，直到去年的牛市，比特股涨到过 2 元人民币。

虽然最终离开了比特股，但是 BM 依然会参与 BTS 紧急 Bug 修复工作。与此同时，BM 又开发了一款旨在颠覆传统互联网媒体行业的项目——Steemit，这也是开辟了基于区块链 Token 内容社区的先例。Steemit 也是基于石墨烯技术的，它非常流行。

2017 年，随着 Steemit 的成熟，BM 宣布退出了 Steemit，开展了下一个项目 EOS。EOS 的目的是要做出区块链行业的操作系统，为开发者提供底层功能，包括并行运算、数据库、账户系统等等。

EOS 一经发布，就广受关注，短短五天内，EOS 便筹集到了数亿美金，它的代币销售规模在目前为止是最大的。

现阶段的 EOS 超级节点竞选也体现出了 BM 强大的影响力。 EOS 项目影响力也越来越大，BM 因为与 V 神在区块链上的理念不合，也经常互怼，他们争论的重点是二人对于去中心化的前提假设不同，这也造就了两个不同的设计逻辑，所以，两人的争论过程可以说是非常地吸引眼球了。

我们从 BM 的个人经历、项目经验、影响力都可以看出 BM 是一个很懂金融的天才式程序员，同时也是一个有点刚愎自用导致与社区矛盾不断的意见领袖。

DPoS 详解

讲完了 BM 的故事，我们再来讲讲 DPoS。我们在前文粗略地讲过 DPoS 算法，我们先来回顾一下。

简单来理解，DPoS 共识算法就是将 PoS 共识算法中的记账者转换为指定节点数组成的小圈子，而不是所有人都可以参与记账，这个圈子可能是 21 个节点，也有可能是 101 个节点，这一点取决于设计，只有这个圈子中的节点才能获得记账权。这将极大地提高系统的吞吐量，因为更少的节点也就意味着网络和节点的可控。

1.DPoS 共识的目标

从名称上，我们也可以判断出 DPoS 与 PoS 共识是直接关联的。DPoS 算法是 BM 根据当时 PoW、PoS 的不足而改进的共识算法，它的目的就是为了提高性能，也就是交易确认时间短。

在 PoS 共识中，人们使用财产证明来“挖矿”，也就是说，这是任何人都可以参与的，只要你持有币，你就可以参与挖矿。

但是我们可以看出，PoS 并没有解决性能问题，在这里我们直接认为提高性能就是提高 TPS，我们可以构造一个等式，：

TPS = transactions / block\_time

TPS 表示区块链每秒能确认的交易数， transactions 是由区块大小 block\_size 和平均每笔交易大小决定的，而区块大小受全网网络状态 network\_bandwidth 限制，也是由记账节点之间物理带宽 witness\_performance 决定的。

记账节点的个数 witness\_count 直接决定了物理带宽的上限，因为记账节点数量越多，则对物理带宽要求越高，对网络的稳定性要求也越高。

要注意的一点是在 DPoS 中，记账节点不叫做矿工，而是改称为见证人，Witness。

所以这个公式变成了下面的样子。

TPS = (block\_size network\_bandwidth witness\_performance) /

(block\_time \* witness\_count)

我们可以看到，要提高 TPS，可以提升分子项，降低分母项，也就是增大区块大小 block\_size、提升记账节点网络带宽 network\_bandwidth、提升记账节点处理性能 witness\_performance，减小区块时间 block\_time、减小记账节点数量 witness\_count。

分子项我们可以看到，它基本受限于物理资源的上限，目前工业水平制造的物理资源的使用上限基本就是整个项的上限了，所以可操作性不大。

而分母项是由共识算法决定的，所以我们从区块时间，以及记账节点数入手，DPoS 算法便正是从这两项着手的。

首先改动的便是限制记账节点的数量，也就是见证人的数量。

我们在 PoW 和 PoS 中可以看到，成为记账节点是无需门槛的，你可以随时参与挖矿，随时退出。

那这会带来什么问题呢，首先无法确定记账节点的数量，其次无法确定记账节点之间的网络环境，记账节点数越多网络环境越复杂，这些不确定性会增大网络分区的概率，从而导致区块链分叉。

如果我们事先规定好记账节点的数量，接着让全网所有节点可以投票决定哪些节点可以成为记账节点，这样就限制并减小了分母项 witness\_count，这个过程我们也称作投票选举。

因为记账节点数量不多，那么我们可以在共识算法中可以规定出块时间为一个固定值，这个值可以很小，通过轮流出块的方式来进行记账。

以上思路基本就是 DPoS 的基本设计思路，BM 还为 DPoS 算法确立两个原则：

投票选举过程一定要保证最大权益所有者最终能控制全网，因为一旦出了问题，他们的损失最大；

与 PoW、PoS 一样，所有节点仅承认“最长”链。

这两个原则确立了 DPoS 共识的基本特性，第一条放大了 PoS 共识使用者就是记账者的优点，第二点则规定了分叉时系统应该表现的行为。

2.DPoS 共识算法分析

在 DPoS 共识算法中，区块链的正常运转依赖于见证人 (Delegates)，见证人是由全网节点投票产生的，见证人也是记账节点的实际控制人，相当于咱们选课代表，课代表帮我们整理作业。

见证人在完成打包交易的同时可以领取区块奖励和交易的手续费，并且可以执行社区投票的提案，所以 DPoS 共识算法不仅仅是算法，而是一个包含了协作治理关系的共识机制。

我们可以引用“DPoS 算法白皮书”中的内容，来看看 BM 设计 DPoS 算法是怎样的思路。

BM 认为所有区块链实际是建立交易之上的确定性状态机。共识是在确定交易顺序，过滤无效交易的一个达成一致意见的流程。

DPoS为了尽快确定交易顺序，过滤无效交易，所以规定了在正常情况下，所有记账节点轮流每 3 秒产生一个区块，轮到了某个记账节点出块时，必须在 2 秒内提交区块，否则就会错块。

假设一直没有记账节点错过自己顺序，那么他们生产的链条势必是最长的链条，如果记账节点在非指定时间生产区块被认为是无效的，每经过一轮，所有节点轮流出块的顺序就会发生重新洗牌。

下图就是一个理想的轮流记账状态。

（图来自白皮书）

DPoS 算法白皮书介绍了 7 种异常的情况会打破上面的正常情况。

例如少数记账节点发起恶意分叉或者发生故障，如下图。 （图来自白皮书）

在这种情形下，B 节点只能在 9 秒内生产 1 个块，而大多数分支，由于数量多一倍，将预期能在 9 秒内生产 2 个块，诚实的 2/3 的大多数可以比小的那一部分创建一个更长的链条，由于原则二，DPoS 可以抵御这种攻击。

在 DPoS 白皮书中介绍了少数记账节点恶意或故障造成的分叉、网络分区情况下重复出块、少数记账节点重复出块、记账节点数量不足、多数记账节点的联合腐败等各种情况。

由于篇幅有限，你如果感兴趣的话可以自行阅读。遗憾的是白皮书中的内容没有经过严格证明，以定性分析为主，所以我们无法确定 DPoS 算法是否有设计缺陷。

在实际应用中，比特股中见证人是 101 人，EOS 里是 21 人。比特股中见证人们赚取手续费，EOS 里见证人们分享 EOS 的通胀收益。他们都是通过公开选举选出来的，选票就是大家手里的比特股或 EOS。

3. 有关 DPoS 的一个争论：中心化问题。

我们之前文章中提过的 FLP 和 CAP 定理，如果为了提升性能，即一致性的效率，势必会牺牲其他两项。这也会引出有关 DPoS 的一个争论：中心化问题。

我们以比特股社区为例，每个人都可以尝试成为 101 个见证人节点中的一个，他们可以在社区里拉票，为社区做事，或者干脆用钱买很多 bts。平时大家象征性地开个会，因为是轮流记账，各个节点之间竞争不大。

但是不要忘记，区块链的发展非常依靠社区，这种方式势必会带来社区的中心化。虽然比特股中 101 个见证人负责记账，但总得有人指定发展方针，于是又设计出了 11 人理事会，这同样是通过选票选出来的。

11 人理事会有很高的权力，他们相当于 11 个超级节点，通过举手表决，甚至可以决定修改代码，而这 11 人理事会是比特股系统里的中心，也是规则的制定者。

这是 DPoS 算法的优势，也是 DPoS 算法的劣势。在 PoW 中，矿工、开发者、用户三权分立。

而 DPoS 似乎将这三权合并到了见证人和理事会手中。在 EOS 中，BM 还制定了区块链宪法，要求所有记账节点必须遵守，所以也有人抨击这是具备了 BM 特色的去中心化。

从某种角度来看，DPoS 是社区治理加上共识算法，不再是单纯的技术共识，这是与 PoW、PoS 算法最大的不同。

DPoS 的基本假设是相信节点是好的，所以尽可能快速选择记账节点，而把问题发生后的修复过程推迟到投票中，可以说 DPoS 并不考虑拜占庭容错问题，把拜占庭容错推给了社区治理，而在社区治理上可归纳为一切皆投票。

而现实生活中，很多情况下，投票并不能解决问题，比如投票人都是有惰性的，集齐所有人投票成本是很高的，如果记账节点没有上限，所有节点的投票都投给自己，DPoS 系统就会退化成 PoS 系统。

总结

我们来总结一下 DPoS 共识机制。

DPoS 共识机制本身将“矿池”纳入系统内部，并把它们统称为见证节点，虽然不会出现中心化挖矿的风险，但是 DPoS 由于节点数不多，并且见证节点权力较大，可以认为 DPoS 本身就是带中心化思路的共识机制。

第16讲 | 深入区块链技术（八）： UTXO与普通账户模型﻿

我们在第 2 讲“区块链到底是怎么运行”一文中，提到了村长给张三转账的例子，那里村长的例子就是 UTXO 模型的一个简化版本。

评论区里有不少留言在问：“为什么不直接记余额呢？”看来很多人都对这个问题很感兴趣，今天我们就来聊一聊这个话题。

区块链网络中有两种记账模式，除了 UTXO 模型还有 Account Based 结构，也就是普通账户模型，也叫账户余额模型，前者在比特币系的数字货币中被广泛使用，后者更多是用在智能合约型的区块链上。

普通账户模型

我们先从传统的账户模型出发来聊聊是如何记账的，假设我们现在有一个支付系统，在这个支付系统中有村长和张三两个账户，村长账户里有 100 万，现在要转账给张三 10 万，这其中涉及的操作是这样的：

检查村长的账户余额是否大于 10 万；

把村长的账户扣除 10 万变成 90 万，然后发送一笔转账消息给张三的账户；

张三的账户接受到转账消息，将张三的账户余额加 10 万。

我们可以发现，无论是村长还是张三，都具有一个余额作为状态，即当前余额是记录在某个地方的，只需要读出来即可，这种设计我们叫做账户余额模型。

如果以上三个步骤是在一个中心化系统中，甚至在同一个数据库中，那将非常简单，会直接退化成一个事务，我们见到的银行账户、信用卡系统、证券交易系统、各种电商类应用，理财类应用基本都是一个中心化系统中的，最多也就是跨表跨数据库。

想必这类场景下的设计，各位工程师对此应该是了如指掌的。

如果以上的步骤中，村长和张三的账户分属两个不同的系统，例如从 A 银行到 B 银行，就需要经过人民银行支付系统，即可信任的中心化第三方来做中介。

你可能发现了，在跨行转账的这种情况下，是没有办法做事务的，所以 1 和 3 是不同步的，如果 3 操作失败，还需要从 2 倒退到 1 的状态，这个情况叫做冲正交易。

普通账户模型具有自定义数据类型的优点，但是却需要自己设计事务机制，就是上述所说的冲正交易。而接下来所讲的 UTXO 模型则恰恰相反。

UTXO 模型

UTXO 全称是：“Unspent Transaction Output”，这指的是：未花费的交易输出。这里面三个单词分别表示 “未花费的”“交易”“输出”，接下来我来详细讲解一下 UTXO 的含义。

UTXO 的核心设计思路是无状态，它记录的是交易事件，而不记录最终状态，也就是说只记录变更事件，用户需要根据历史记录自行计算余额。

有点像MySQL 中的 Binlog，主从模式的情况下，按照 Binlog 来更新数据，Redis 的 AOF 模式备份模式也是如此，UTXO 也是类似的思路。

下面我们按照按照普通账户中的例子来重新讲解一遍。

如果要记录交易本身，那么我们可以构造一笔交易，这笔交易中村长转账 10 万给张三的同时，90 万转给自己。

如下所示：

村长　100 万 --> 张三　10 万

--> 村长　90 万

这里其实有三条子记录，左边一条，右边两条，左边叫做输入，右边叫做输出。

输入和输出组成了交易，输入和输入需要满足一些约束条件：

任意一个交易必须至少一个输入、一个输出；

输入必须全部移动，不能只使用部分，所以才产生了第二个输出指向村长自己；

输入金额 = 输出金额之和 + 交易手续费，这里必须是等式。

对于村长来说，首先构造交易的输入输出，满足上述条件，然后广播到全网，接收方自行判断交易是否属于自己。这里满足约束条件构成的交易模型，也就是村长记录的三条转账事件就是 UTXO 模型。

账户余额模型与 UTXO 的比较

我们可以归纳出 UTXO 与普通账户模型的一些区别。

存储空间，UTXO 占用空间比账户模型高，因为账户模型只记录最终状态。

易用性，UTXO 比较难处理，账户模型简单容易理解。例如 UTXO 在使用上，还需要配合高效的 UTXO 组装算法，这个算法要求尽可能降低输入输出的个数，还要让“零钱“归整，算法的复杂度相比账户余额无疑要高。

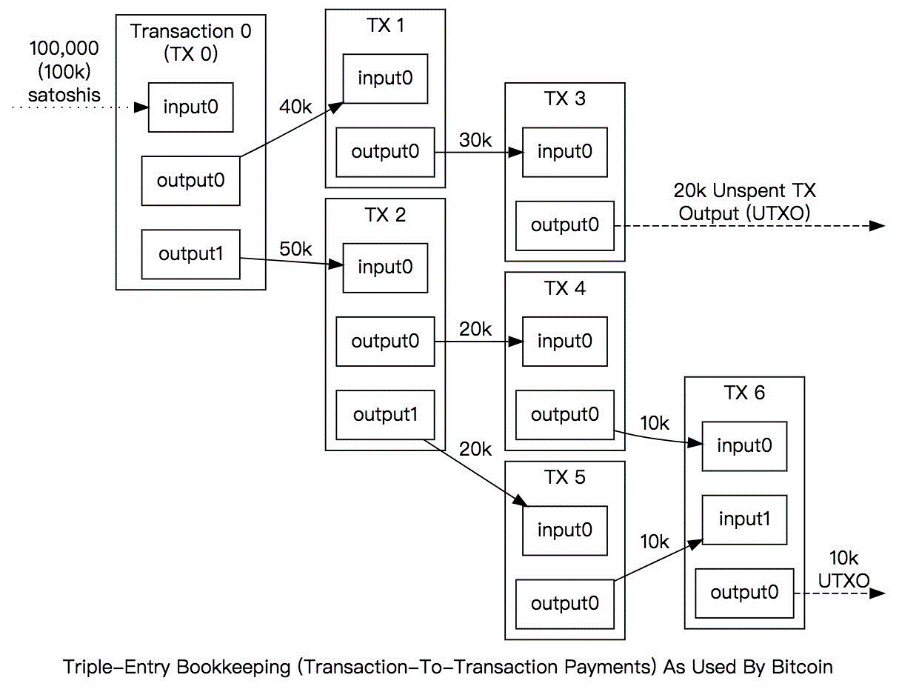
安全性，UTXO 比账户模型要高，UTXO本身具备 ACID 的记账机制，而账户模型需要自行处理，例如重放攻击。

普通账户模型具有较高的自由度，可以让智能合约有更好的发挥空间，并且它避免了 UTXO 的复杂组装逻辑，精度控制上也更为得心应手。

UTXO 似乎天然是为数字货币设计的，具有较高频次跨账户转移场景都使用 UTXO 会比较好，考虑到智能合约的普适性，UTXO 与智能合约并不能很好地兼容，但是这也对开发者的自身水平提出了更高的要求。

区块链中的 UTXO 模型

我们借用比特币开发者文档中 UTXO 模型的图示，来看看 UTXO 实际的构造形式。

﻿﻿

上图中，所有的交易都可以找到前向交易，例如 TX5 的前向交易是 TX2，TX2 中的 Output1 作为 TX5 中的 Input0。

意思就是 TX2 中的付款人使用了 Output1 中指向的比特币转移给 TX5 中的收款人，接着 TX5 中的人又把收到的比特币转移给了 TX6 中的收款人，成为了 TX6 中 Output0。

我们也可以发现，TX6 中的收款人还没有产生 TX7 交易，也就是说 Output0 还没有被花费，

这时候我们终于得到了 UTXO 的真正语义：Unspent Transaction Output，未花费的交易输出。

我们这时候可以发现 UTXO 也同样能表示余额，不过是重演计算的方式，它用不同的方式表达了余额，我们把一个地址上所有的 UTXO 全部找出来，就是这个地址总的余额了。

我们还可以发现，无论是 TX5 还是 TX2，都已经成为历史交易，它们都忠实客观地记录了两笔交易，这两笔交易代表的是事件，而不是余额状态转移，这是我们看到的最直观的区别。

我们再来看看一个真实的交易例子。

﻿﻿

这是区块链上一笔真实交易的例子，它记录了一笔 450ETP 的转账记录。

左边是输入，右边是两笔输出，其中第二个输出是给自己的账户，这和我们村长转账给张三的例子是一样的。

下图是交易解码为 JSON 格式的样子，可以看到 Previous\_output 是放到 Inputs 数组里的，意思就是前向输出作为本次的输入。

{

"hash" : "89e80e14db07c4904a57e2c1efb689bccbbf43942103c1a92166d5c0f27ea3d2",

"height" : 1093399,

"inputs" :

[

  {

    "address" : "MLWtmjwCtmK44FMwJMSfAkHaEvnnb2N6HX",

    "previous\_output" :

    {

      "hash" : "770a72f35d3e3a78bd468949bad649f03b241cf7e2a84cc2d6fdabacdcc47f06",

      "index" : 0

    },

    "script" : "[ 304402202b21d7a79276985dc99777b70fd5095796dad58f35e29a019d2cb6cca5df481802205ffab088a6047f5b6382ba02a0eed4e78ab7950fe264d3774e8b0b357a7593d101 ] [ 03ea3462dc01e7b5569e89737211887035f8f1e99e1fe4332181d83daccaa6d917 ]",

    "sequence" : 4294967295

  }

],

"lock\_time" : "0",

"outputs" :

[

  {

    "address" : "MGz9yjLLn4AqyraRjSpiP2GmTWKnT3yfiL",

    "attachment" :

    {

      "type" : "etp"

    },

    "index" : 0,

    "locked\_height\_range" : 0,

    "script" : "dup hash160 [ 63ab0013d183f2592e4b46a358df01e88a09c0b8 ] equalverify checksig",

    "value" : 45000000000

  },

  {

    "address" : "MLWtmjwCtmK44FMwJMSfAkHaEvnnb2N6HX",

    "attachment" :

    {

      "type" : "etp"

    },

    "index" : 1,

    "locked\_height\_range" : 0,

    "script" : "dup hash160 [ 8a63941b392771c40f1c15e4374808f6bb464cba ] equalverify checksig",

    "value" : 118082150283

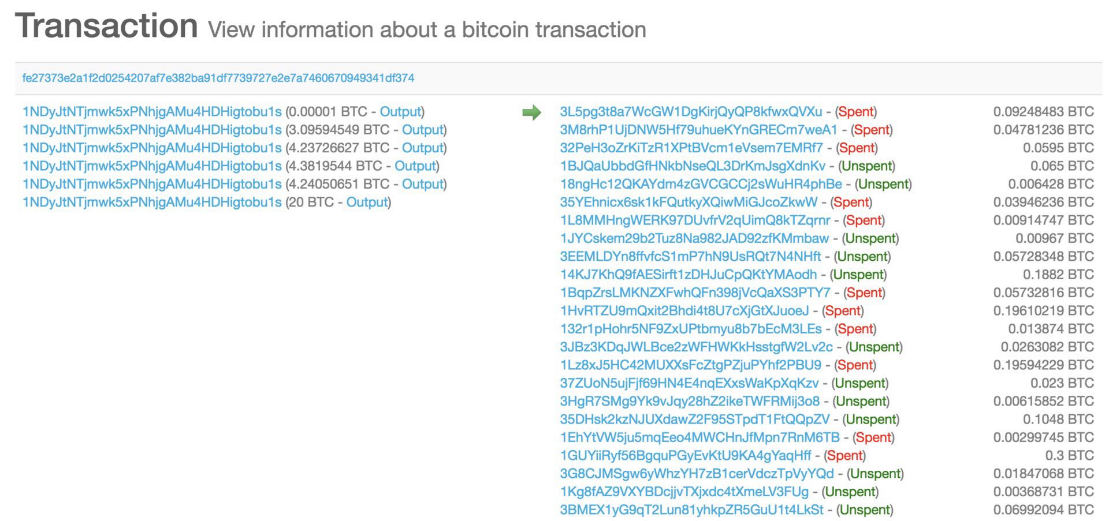
  }

],

"version" : "2"

}

我们再看看比特币上的例子：

﻿﻿

这一笔比特币交易包含 6 个输入，几十个输出，交易一共 3.5kb，交易的输入输出会影响交易大小，比特币的交易费是根据字节收费的，交易尺寸越大越贵，而交易尺寸主要和输入输出的个数有关，也就是说，算法上并不规定输入输出的个数，而只有区块尺寸限制。

在比特币中将小于 100kb 的交易称为标准交易，超过 100kb 的称为非标准交易。它的前向 input 以及生成一个 out 约占用 161~250 bytes 。所以在比特币中，大约的 inputs/ouputs 的最大数目限制为 100KB/161B ~= 600 个。

UTXO 的特性及缺点

从计算的角度来说，UTXO 具有非常好的并行支付能力，也就是我们上文中所说的如果没有尺寸限制，一笔交易可以包含任意笔输入输出，同时也没有次序要求，在一笔交易中哪一个 UTXO 在前，哪个在后面不影响最终结果。

从存储的角度来说，UTXO 具有较好的可裁剪特性，可裁剪性指的是 UTXO 类型的交易，如果从最老的那一笔 UTXO 开始截断数据库，那么之前的数据可以删除掉了。

如果想进一步压缩数据尺寸，可以在任意位置截断，记录 UTXO 对应的交易哈希即可，然后从其他节点获取并校验 UTXO，这也是 SPV 轻钱包工作的基础之一。

以太坊中并没有使用比特币的这种 UTXO 设计，这与以太坊的宗旨有关，以太坊的目标是构建通用计算，而比特币是数字货币，需求不同导致设计的不同。

V 神指出了 UTXO 的缺陷，一共有三类。

1. 可表达的状态少 。

UTXO 只能是已花费或者未花费状态，这就没有给需要任何其它内部状态的多阶段合约或者脚本留出生存空间，这也意味着 UTXO 只能用于建立简单的、一次性的合约，UTXO 更像是一种二进制控制位。

2. 区块链盲点（Blockchain-blindness）。

UTXO 的脚本只能看到自己这条历史轨迹，无法看到区块链的数据的全貌，这导致了功能性扩展受到了限制，我们在花费比特币的过程中需要小心翼翼的组合 UTXO，这也导致了系统状态逻辑复杂，不适合设计成智能合约的基础结构。

3. 价值盲点（Value-blindness）。

UTXO 脚本不能提供非常精细的金额控制，基于账户模型的余额在花费过程中，可以任意的按值存取，它仅取决于程序能表示的最小精度。

而 UTXO 要求必须全部移动，如果要满足一个目标值金额，对组合 UTXO 算法的要求会比较高，采用许多有不同面值的 UTXO，一方面要求尽可能地精确，另一方面又要求输入输出的数量尽可能的小。

UTXO 是比特币上的原生设计，在区块链以前是没有这种逻辑数据结构，UTXO 的出现给了人们看待数据转移的不同视角，但 UTXO 不是所有区块链所必需的，公链开发过程中的是否选用 UTXO 模型可以根据业务场景进行判断。

总结

好了，今天我们分别介绍了普通账户模型和 UTXO 模型，并从不同角度比较了二者的优劣。

从技术选择上来看，比特币选择 UTXO 是为了满足支付的安全性，以太坊选择普通账户模型是为了智能合约的自由度。

第18讲 | 智能合约与以太坊﻿

在前面的文章里，我们介绍了区块链的核心技术，也穿插介绍了一些项目。然而每个区块链都有自己的特色，接下来我们将针对每个项目进行详细讲解。今天我们就来讲讲智能合约和以太坊项目。

今天我们从智能合约这个概念入手，聊聊什么是以太坊项目以及它的发展历史。最后还会介绍几款钱包给你，希望通过今天文章的讲解，你也可以尝试在以太坊上编写简单的智能合约。

智能合约的概念

不同于法律意义上的合约概念，区块链领域的合约表达的是可以“自治自理”的 计算机协议，这套协议具有自我执行、自我验证的属性。

如果完全从技术角度来看，智能合约等价于一段事先就被规定好逻辑和条款的计算机代码被激活运行的状态，同时，智能合约也提供了通用的用户接口，用户可以通过接口与用户交互。

智能合约这一概念早在 20 世纪 90 年代就有人提出，这个人是从事智能合约和数字货币研究的尼克萨博（Nick Szabo）博士，尼克 1996 年在《Extopy》期刊上发表了对智能合约的描述，他认为智能合约是一个由数字表单指定的承诺，这个承诺包含关系到多方执行的一组协议。

从定义中我们可以得知，智能合约由多个协议组成，这些协议包含了用户接口，能表达用户的承诺，它可以安全有效地确定公共网络上的关系。

换句话说，智能合约是一个由计算机处理、可执行合约条款的交易协议，其总体目标是满足协议既定的条件，例如支付、抵押、保密协议。这可以降低合约欺诈造成的损失，降低仲裁和强制执行所产生的成本以及其他的交易成本。

我们举个实际的例子解释一下，今年 4 月 9 日，上海某建设银行支行开放了“无人银行”，银行中充斥了众多机器和显示屏，智慧柜员机、VTM 机、外汇兑换机、VR 设备和两台机器人代替了传统的柜台。

这里的智慧柜员机、外汇兑换机器人众多电子设备都可以认为是智能合约的一种表现形式，用户在办理银行业务时，如办理大额汇兑业务，业务流程和逻辑依据已经定在程序中，用户只需要按照操作一步一步进行，办理完成后即可获得单据。

这里“既定的业务流程、机器人模样的人机交互界面、双方同意承诺”组成了智能合约的概念，它甚至具有一定的法律效力。

萨博提出的是智能合约的概念，以及我们举的例子，都是广义的智能合约概念。智能合约具有多种实践形式，而在区块领域所说的智能合约概念，我们其实是指 Blockchain-based 这种形式。

在萨博的智能合约概念中提到了开放式网络，而我们知道开放式网络的基本要求就是拜占庭容错，通过前面文章的讲解我们知道，区块链天然具有拜占庭容错特性。所以如果在区块链上实践智能合约这个概念，两者会非常契合，天造地设。

首先实践了智能合约这一概念的是比特币，比特币脚本（bitcoin script）包含了 5 种标准交易脚本，这些脚本的功能不仅仅提供了普通单人支付的情况，它还提供了多方共同签名支付的脚本，叫做多重签名支付，多重签名支付可以看成是萨博语义下的智能合约。

除了比特币，发扬光大智能合约这个概念的区块链项目就是以太坊了，下面，我重点来介绍一下以太坊项目。

以太坊及其发展历史

以太坊 Ethereum 项目的目标是打造一个去中心化的新一代互联网应用平台，这个平台称作 Dapp 平台。

这些 Dapp 基于以太坊智能合约虚拟机开发、编译、部署，并且可以自定义业务逻辑，部署后全网可见且自动执行，理想情况下不存在宕机、审查、欺诈、第三方干预的情况。

2013 年底以太坊的创始人 Vitalik 在比特币开发者社区提出了可以运行图灵完备（Turing-complete）形式的应用，但这一思想并没有得到比特币社区的支持。

2014 年，Vitalik 带着自己的想法，宣布以太坊项目正式成立，2014 年上半年开始筹集资金，聚拢一些早期开发者，同年 7 月份进行了为期 42 天的 ICO，共筹集了超过 1800 万美元的比特币。

2015 年 7 月，第一个版本的以太坊发布，主网正式上线，这一阶段 Bug 和设计缺陷较多，多是开发者在使用。

2016 年以太坊发布第二个大版本 Homestead，用户逐渐多了起来，同期也吸纳了不少 Dapp 开发者。

2016 年 6 月，以太坊上发生了著名的黑天鹅事件——TheDAO 事件，这打开了 ICO 市场，同时也造成了以太坊社区分叉，形成了以太坊和以太坊经典两个代币。

2017 年 4 月，ICO 风靡中国，ERC20 提供了低成本方便高效的资金募集方式，为 ICO 提供了极大的便利，趁着数字货币牛市，以太坊的价格涨幅达十多倍，2018 年 1 月以太坊价格突破 1000 美元。

以太坊的核心概念

以太坊核心概念包括：智能合约虚拟机 EVM 和 Solidity 编程语言、账户模型、以太币和 Gas，交易和消息。

1. 智能合约虚拟机 EVM 和 Solidity 编程语言

以太坊的核心概念首先是智能合约。

智能合约包含两部分，一部分是开发语言，主要以 Solidity 为主，Solidity 与 Javascript 语言在使用上十分接近，这极大地降低了 Dapp 开发人员的学习成本。

Dapp 开发者编写好代码以后，使用 Solidity 编译成十六进制字节码，然后部署到 EVM 上，也就是把合约广播到全网，等矿工打包后就形成了常年运行的 Dapp 了。

另一部分就是 EVM。 EVM 是以太坊智能合约虚拟机，我们可以等价理解它为 Javascript、Python 等脚本语言的执行引擎。

它是一个轻量级的虚拟机隔离环境，它并不提供访问本地网络、进程、文件系统的功能，它更像是一个封闭的容器，这个容器里面装了一个正在运行 Dapp，可以看成是无法和外界交互的 Docker Container。

Dapp 在运行过程中，可以被请求或其他事件触发，然后执行相应的逻辑，这些请求和事件是由以太坊上的交易产生的，不是来自本地操作系统的事件。

Dapp 运行过程中，每次状态发生变化，则意味着全网同步更新，大家的计算结果都是一致的，这有两个特性：

所有 Dapp 的计算结果经过全网共识，一旦确认过几乎无法被伪造和篡改；

由于必须经过全网共识，所以这限制了整个网络的容量。

2. 账户模型

以太坊并没有采用 UTXO 模型，也不同于银行账户，它是由以太坊开发者设计了自己的账户模型。

以太坊上的账户有两种类型，第一类叫做合约账户 CA（Contracts Accounts)，第二类叫做外部账户 EOA（Externally Owned Accounts）。

简单理解就是：CA 是智能合约代码用的账户，EOA 是人用的账户；所以 CA 可以存储并执行智能合约代码，它的智能被 EOA 激活，它也不保存和存储私钥，合约账户可以调用其他合约。

EOA 则是人们直接控制的账户，可以存储以太币，可以发送交易到合约账户，触发既定的逻辑。EOA 账户由公钥标识，由对应的私钥控制。

当合约账户被调用时，存储其中的智能合约可以在矿工处的虚拟机中自动执行，并消耗 Gas，如果 Gas 不足则会触发“Out of Gas”异常，被终止执行。

无论是 CA 还是 EOA，在以太坊内部都被看做状态对象（state objects），意思就是说这些账户都有自己的状态，EOA 具有以太币余额的状态，而 CA 除了余额，还多了合约存储状态。

3. 以太币和 Gas

Gas 是执行智能合约操作的燃料，智能合约的每一个步骤都会消耗 Gas，Gas 是由以太坊的平台代币以太币转化而来，最小单位是 wei，1ETH 相当于 10 的 18 次方 wei。

以太币可以通过 PoW 挖矿而产生，目前以太坊主要通过 GPU 挖矿。挖出一个块可以换得 5 个以太币，并且还有一定的交易费、以及叔伯块的奖励。今年 4 月 6 日爆出著名矿机芯片厂商比特大陆已经开发出针对以太坊的 ASIC 专业矿机，相比 GPU 的效率提升 2.5 倍。

4. 交易和消息

以太坊上的交易与比特币中的 UTXO 交易不同，它是指 EOA 账户将一个经过签名的数据包发送到另外一个账户的过程，这个过程产生的账户状态变化将被存储到以太坊区块链上。

以太坊上除了交易还有消息这个概念，消息指一个合约账户调用其他合约账户的过程，可以类比函数调用过程。

所以以太坊上的 Dapp 如果被触发，有两种可能，第一种是交易触发，第二种是消息触发。

这两种的区别在于前者是 EOA 发起的，后者只能是其他合约账户发起的。

状态对象的状态变化被以太坊共识机制的记录下来，交易和消息驱动着状态的变化，于是，在一个开放式的网络中构建一个全球共享的 Dapp 变得十分方便。

以太坊上智能合约具有全网准实时同步、准确执行、去中心化运行、较低的人为干预风险等特性，EVM 和 Solidity 为全球开发者提供了较低的进入门槛。

与比特币的主要区别

以太坊项目又被称作区块链 2.0 项目，这里 2.0 就是指智能合约。那么以太坊与比特币相比，到底智能在那里呢？我们具体来看看。

与比特币相比，以太坊首先不是一个单纯的数字货币项目，它可以提供全世界无差别的区块链智能合约应用平台，这个平台基于我们前面文章所介绍的区块链四大核心技术要素，即 P2P 网络、共识机制、账户模型、加密模块。

除了以上的四个技术要素，以太坊还推出了 EVM——以太坊智能合约虚拟机，并且，它还推出了自己的智能合约语言 Solidity。

于是，区块链的开发者因为智能合约的出现开始分为两类。第一类是公链底层开发者，主要是以 C++ 和 Go 语言为主的全节点开发者，他们需要对区块链各个技术模块有很深的理解。

第二类是智能合约开发者，也就是应用开发者，这类开发者对区块链的运行原理不需要理解很深，只需要会编写 Solidity，了解规范即可。

除了以太坊智能合约这个概念以外，它还设计了下面的内容。

研究并实现了自己的 PoW 挖矿算法——ETHASH，这是一个内存困难型的挖矿算法。

叔伯块激励机制，降低了挖矿中心化的趋势。 取消了 UTXO 模型，采用了账户模型和世界状态，提供了数据结构的可塑性。

设计了 Gas 机制，避免程序死循环消耗全网资源的情况出现。 研究并实现了自己的 PoS 共识算法——Casper，可防止 Nothing-at-Stake 攻击。

以太坊提供了在区块链自由编程的能力，智能合约让所有人得以开发属于自己的 Dapp，这是与比特币作为单纯的数字货币所不具有的能力。

第20讲 | 区块链项目详解：比特股BTS﻿

前面两篇我们都聊了智能合约的话题，智能合约可以说是当下区块链最热的概念了，在多数人眼里，没有智能合约的区块链价值几乎就大打折扣。

那么说，实际上是不是这样呢，我们今天就来聊聊一个并没有开放式智能合约的区块链项目——比特股。

比特股发布于 2014 年，虽然没有引入智能合约的概念，但它提供了功能极为丰富的金融类工具，比特股上所有的金融合约都是事先在代码里写好的，所以说它的本身就是一个超级智能合约集合。

什么是比特股

比特股是一个公开透明的、7\*24 小时不间断运行的、基于区块链技术的去中心化交易平台。

它兼具了区块链的优点，也是第一个有关稳定数字货币的尝试，目前比特股提供了若干核心的金融服务，例如支付、撮合交易、资产存托等服务。

相较于传统的金融 IT 系统，它的服务器是由分散在世界各地的受托人（Delegated）维护的，即使其中一些人被攻击也不会导致整个系统的宕机。

比特股目前全网在线的服务器有 27 个，由于 DPoS 共识算法提供了较好的交易吞吐性能，理论上比特股的 TPS 可达 10 万，这也是比特股在技术上区别于其他区块链的最显著特征。比特股较好的 TPS 其实也是为了它的功能服务的。

在这里，我们能看出比特股平台的性质。

首先，比特股平台是一个交易平台，交易平台的显著特征是整个市场对时间敏感，大家都希望下单之后快速成交，所以高 TPS 是一个交易平台的基本需求。

其次，比特股是去中心化的交易平台。目前流行的中心化数字货币交易平台最大的问题是资金管理系统和撮合系统都由同一家控制的。

然而在传统的证券交易领域，证券登记和交易撮合是两个不同的主体，他们之间是协作关系，共同受到证券会的管辖。

所以，如果你的数字货币存在中心化交易平台，你的交易撮合也受它来控制，这里的交易撮合指的是一个交易双方通过挂出买单和卖单，系统完成撮合匹配直至最终成交的过程。

由于以上的这一切都是不透明的，这里面就有很多的不确定因素。

比如交易平台跑路风险、黑客攻击、资产莫名其妙丢失，或者撮合的过程中，交易对手方是谁，是否有内幕交易。这些情况都会带来较大的风险。

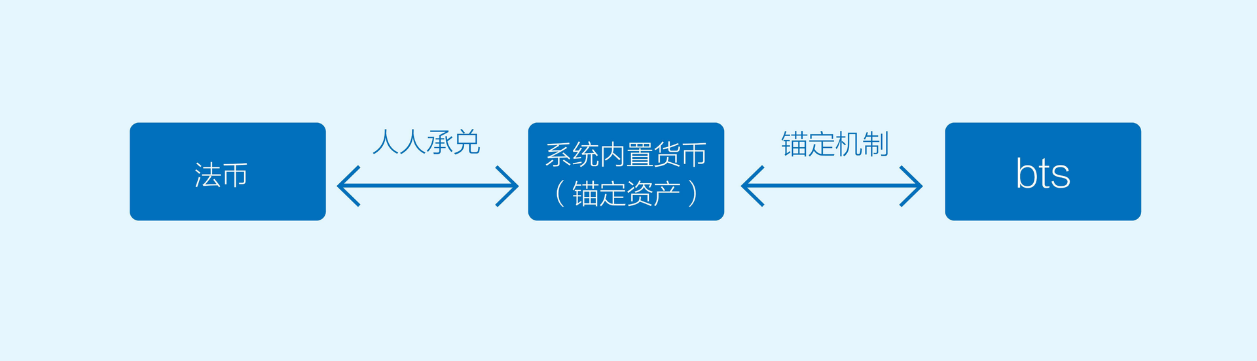
比特股的两个机制

那么比特股是如何设计中心化交易所来避免上述风险的呢？

比特股作为一个去中心化的交易所，它有两个机制可以避免上述的风险。

第一、资金出入是由承兑商来支持的，人人都可以成为承兑商，也就是人人承兑； 第二、锚定机制提供了稳定货币的出入金过程，锚定机制也保证了比特股的出入资金和交易撮合是分离的，避免了中心化交易平台的弊端。

这个过程可以简述为：法币 <—> 锚定资产（系统内置货币）<—>bts 的相互转换。从法币到系统内置货币用到了人人承兑机制，从系统内置货币到 bts 的转换用到了锚定机制。

﻿﻿

这里的 bts 是比特股上流通的平台代币，它和比特币一样有类似的总量上限设定，大约在 36 亿左右，目前流通量 26 亿左右。我们接下来就来看看这两个机制。

1. 人人承兑

人人承兑就是提供了从法币到系统内置货币的转换，比特股系统内置了多种货币，它锚定了多数法币。

例如 bitCNY、bitUSD、bitEUR 等等，这些系统内置货币是可以与 CNY、USD、EUR 按照 1：1 兑换的。而人人承兑货币其实就是提供了 bitCNY 和真正人民币之间的相互转换。

它的机制上有点类似那个比特币的场外交易。所谓场外交易，就是没有中心化撮合中介，交易双方自行议价成交。

例如，我想要买比特币，就可以找到一个专门的承兑商，直接把这个钱支付给交易商，然后承兑商再把比特币支付给我。这部分的内容，后面我们讲数字货币交易所的时候会和你详细讲解。

人人承兑在逻辑上差不多，它提供了一个 CNY 法币和 bitCNY 的兑换手段，实际上就是让法币和比特股系统内置货币的交换能够进行，而且是去信任的进行。

所以从资金托管的角度来看，比特股与中心化交易所很大的区别，比如你在一个交易所里充值，你只能信任这个交易所在保管你的钱，在你要提现的时候，你只能信任交易所愿意让你提出。

但是人人承兑的就不一样了，人人承兑是你从 A 承兑商获取 bitCNY，你可以找 B 承兑商再换成人民币，不需要只在同一个地方兑换。

因此一个人此时有充值的需求，过一段时间可能就有提现的需求，所以实际上每个人都可以成为承兑商，我可以是买家也可以是卖家，交易角色的转换可以让市场更灵活。当然市场上也有专门提供充值和提现服务的 “承兑商”，这些承兑商收取手续费来盈利。

但是，不是所有的中心化风险都可以通过技术解决，人与人的信任问题没有一劳永逸的解决办法，即使你们当面交易也有可能遇到对方欺诈的行为。

我们只能说，CNY 法币与 bitCNY 锚定之后的充值和提现相对更安全，人人承兑提供了一种有效的机制，缩短了出金入金的周期，提升了安全性，如果资金在比特股系统之内，整个使用期间也没有人能威胁到你的资产。

2. 锚定机制

锚定机制是一种去中心化的抵押机制。我们刚才提到了比特股系统内置了多种货币，它锚定了多数法币，例如 bitCNY、bitUSD、bitEUR 等等，这些系统内置货币是可以与 CNY、USD、EUR 按照 1：1 兑换的。

系统内置货币的发行商是系统自身，发行给抵押了 bts 的用户，发行的数量是由抵押的代币数量决定的。你用 bts 抵押，然后换取 bitCNY。

换句话说，任何持有 bts 的人可以用它来抵押生产系统的内置货币，例如 bitCNY，它的抵押规则要求两倍价值的 bts 进行抵押，由于有 2 倍价值的 bts 作为保障，所以定义 1 bitCNY = 1 元人民币的风险较低。

比特股系统本身提供 bts 与 bitCNY 交易对，例如现在 bts 价格是 0.5 元人民币，我就能用 4 个价值 2 元的 bts 抵押产生 1 枚 bitCNY，也就是 2 倍价格抵押。

这种抵押担保机制保障了 bitCNY 的价值，并且从技术层面来讲，比特股的共识机制保证了恶意修改 bitCNY 的数量的造假行为是不可行的。

如果 bts 价格下跌，系统就会自动把我抵押产生的 bts 卖掉，因为抵押了 2 倍价值的 bts，所以如果没有暴跌 50% 以上，系统都可以在交易市场上卖掉我抵押产生的 bts，并在市场上获得 bitCNY。

如果暴跌 50% 以上，系统会以一成的价格（强制平仓）卖出抵押的 bts，直至卖够抵押产生的 bitCNY。

从操作层面来看，支付 bitCNY 实际上消耗的还是 bts，但需要消耗多少，就以实时价格买入多少 bts。

买入操作是瞬间完成的，在比特股上有专门的代币资金池来提供，实时价格由系统为之决定的，所以使用者不用承担任何比特股代币价格波动带来的风险。

至此，稳定的 bitCNY 货币就产生了，它兼具了区块链的优点，且是一种稳定货币。

除了抵押以外，还有强制平仓、强制清算这种机制来保证价值和实际所锚定的货币等价。内容比较深，留给你自己挖掘。

比特股的技术概览

比特股的核心代码是由 Cryptonomex 公司开源的石墨烯（Graphene）框架演变而来，它的主体代码是 C++ 编写的，里面使用了大量的 boost 库组件，如果你对石墨烯技术感兴趣，并且熟悉 C++，可以仔细研究一番。

除了比特股核心，这里还有一套 Javascript 编写的 UI 产品，叫做 Bitshares-UI，Bitshares-UI 其实是一个轻量级的基于浏览器的钱包：比特股钱包，这个钱包将用户密钥存储在本地浏览器上，并且密钥是通过用户密码加密并储存在浏览器数据库。

发送交易时，先本地对交易进行签名，再传输到代理服务器上，由服务器广播至比特股全网，这个服务器你也可以自己搭建。

比特股所使用的共识算法我们已经讲过，是 DPoS，所以比特股也有见证人节点，目前有 101 个见证人节点，从 101 个节点中，社区又选出了 11 位代表，我们叫做理事会。理事会接受社区投票然后行使比特股上的治理权。

比特股使用的也是 ECC 椭圆曲线非对称加密算法，值得一提的是，比特股并没有类似比特币地址的概念，在比特股上取而代之的是可读的账号系统，这些账号与私钥一一绑定，可读账号就是比特股系统中的地址。

比如我的账号是“chenhao”，那么在比特股上，你支付给我 bitCNY 的时候，接收方一栏直接填“chenhao”即可。

总结

今天我向你详细介绍了比特股系统，比特股也是一场伟大的实验，它打破了区块链应用数字货币的局限性，让区块链技术具有丰富的金融特性。

比特股技术上的优势多体现在 DPoS 算法上，所以本篇我重点介绍了比特股的产品特性。

比特股社区也是区块链界的一股清流，因为持有比特股往往需要学习大量金融知识。

投资者想要投资比特股，光是弄清楚锚定机制足以让投机者就需要花费大量时间，所以一旦被比特股套牢，似乎只能学习比特股进行自我提升，这也让比特股社区的平均金融知识储备高于其他区块链项目。

第21讲 | 引人瞩目的区块链项目：EOS、IOTA、Cardano﻿

柚子 EOS

1. 什么是 EOS

EOS 全称 EOS.IO 软件，EOS 也是 EOS.IO 上的平台代币缩写，它暂时没有准确的中文翻译，中文社区把 EOS 叫柚子，这一点其实得益于 EOS 的发音与水果“柚子”相近。

EOS 是一个以太坊的竞争型区块链，它提供了全新的区块链架构，使得去中心化平台水平扩容和垂直扩容都成为了可能。

如果智能合约是程序，那么可以把 EOS 看成是一个超大的操作系统了，它为所有的程序，也就是智能合约提供了基本设施。例如账户、授权、数据库、异步通信等接口。

它甚至可以跨平台驱动大量的 CPU 或者集群，所以 EOS 的 TPS 肯定是远超以太坊的，这也使得构建基于区块链的应用几乎没有成本而且快速高效。

2.EOS 的瞩目之处

在说 EOS 之前，我们来回顾一下 DPoS。

DPoS 其实是 BM 参照现实世界中的议会制度而设计的共识算法。DPoS 的核心理念其实是投票，它的设计理念是延迟性惩罚，它假设参与者绝大部分都是没有恶意的。

“人性本善”的假设虽然让系统的作弊成本降低，但是随之而来的惩罚也非常严厉，就是丧失见证人的资格，但是带来的好处则是效率的提升。

我们来看看 EOS 吸引人的地方，这里一共有两点，第一是 EOS 号称可以提供百万级 TPS 交易性能，第二是 EOS 的链上治理机制：区块链宪法以及 21 个超级节点（见证人节点）。

在 EOS 中，记账节点又被称作超级节点，EOS 一共有 21 个主节点，另外还有 100 个备选超级节点，这些超级节点完全是等价的。

超级节点的基本职责包括了忠实打包交易、执行并验证智能合约、向全网广播有效区块以外，还多了一项职责：保障并促进 EOS 项目的发展。

如何促进呢？BM 在 EOS 中强化了 DPoS 算法的投票机制，并首次提出了区块链宪法的概念，我们可以直接引用 EOS 技术白皮书中的内容来一探究竟。

EOS.IO 应用使得区块链创建了一个点对点的服务条款协议或者绑定用户到一个合约，这都需要用户对其签名，简称“宪法”。

宪法的内容定义了仅仅依靠代码无法在用户间履行义务，同时通过建立管辖权和可选的法律来解决相互间的争端。

每个在网络广播的交易都必须将宪法的哈希值作为签名的一部分，从而显性地将签名者绑定在合约中。

宪法还定义了人类可读意图的源代码协议。 这个意图是用来识别错误和功能之间的差异，当错误发生时，引导社区对什么是适当或不当修复。

可以看出区块链宪法是一种非代码强制执行的规则，有点像我们安装软件时的“同意”协议，所以它更像是一种人为承诺，为了弥补 DPoS 较弱的抵抗恶意规则的缺陷。

那么什么人可以发起并修改宪法呢？就是超级节点，也就是记账节点，它规定了 17/21 以上的节点同意才能发起修改提案。

我们可以看出超级节点的权力十分巨大，这也引来了人们对此产生了争议。

3.EOS 的争议

Vitalik 针对 EOS 超级节点竞选发表过意见。他认为 21 个节点的 DPoS 虽然引入了治理结构，但也很容易受到选民和持币大户的操纵，最终导致“财阀统治型”的治理结构。

在超级节点竞选过程中，某些节点为了获得更多的选票，承诺当选后可以给投票者分红，这在西方文化中是无法接受的，这一点似乎违背了 BM 设计 DPoS 的初衷，所以 BM 以及 EOS 团队都表示坚决反对。

BM 对此也给了回应，BM 表示自己的目标是降低创建社区的准入门槛，并允许市场自由竞争来奖励最高效的社区以及惩罚最腐败的社区。

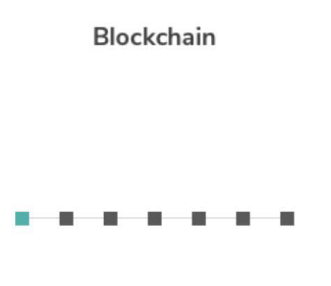
他也认为善良是主观的，而且每个社区都能定义持有什么样的价值观是好人，并积极驱逐他们所认为的坏人。

Vitalik 和 BM 都相互发文怒“怼”对方，但是总的来说，Vitalik 和 BM 这种公开讨论推进了区块链行业的发展，给人们带来了更多哲学和设计原则上的思考。我在附录中给出了社区翻译版文章，你可以进行查询。

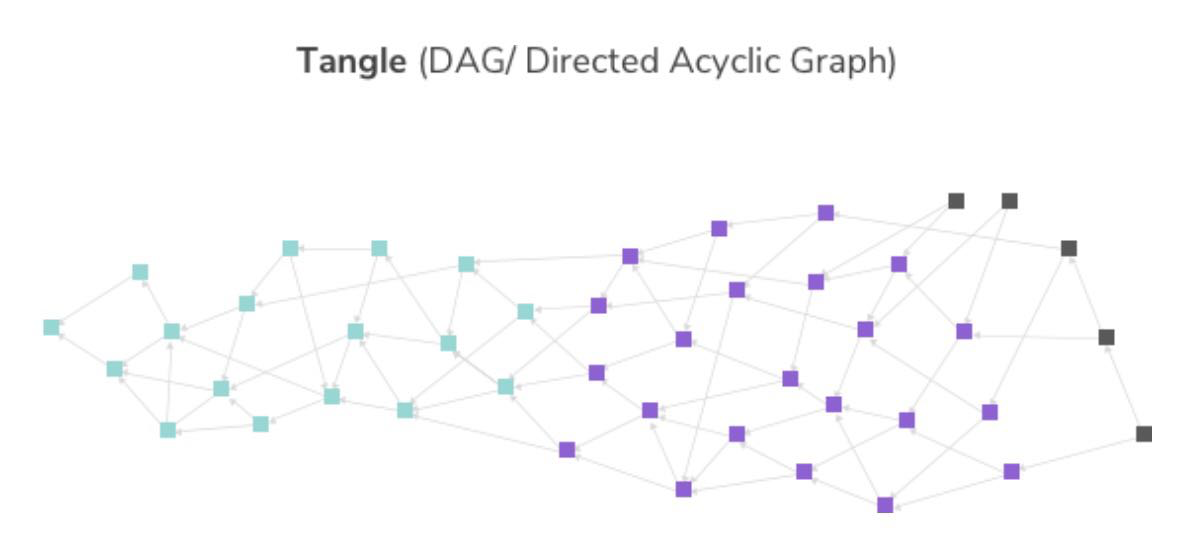
埃欧塔 IOTA

IOTA 是一个为了物联网（IoT) 而生的区块链项目。严格来说，IOTA 不是“区块链”，因为它没有区块，也不是链式结构。

IOTA 提出了一种基于有向无环图（DAG）的分布式账本结构，这种结构 IOTA 将其命名为 The Tangle，探戈。

﻿﻿

上图是常见区块链账本结构，而下图展示了 Tangle 的账本结构。

﻿﻿

我们来看看这两张图的区别，首先区块链账本结构的打包单位是区块，而 Tangle 直接就是交易，或者或“交易引用”。

任意交易 Tx-black 会引用过去的两条交易记录，这样被引用的交易 Tx-purple 相当于有了一次确认，间接地证明了合法性，随着一次又一次的被引用，Tx-purple 会转变成 Tx-green。

Tx-black 相当于图种的黑色图块，代表未确认的交易；

Tx-purple 相当于紫色图块，代表已确认但还未成熟的交易；

Tx-green 相当于是绿色图块，代表已确认已成熟的交易，是可信的。

也就是说，我们发送交易的目标是成本绿色部分的交易，成为绿色部分的交易，可信度是可以计算的，面对不同的交易场景，可信度可以设置为 51%，90% 或者百分之百。

那么说，如何计算这种可信度呢？

IOTA 上的共识算法叫做 MCMC 算法，它可以任意选择黑色部分的两笔交易，进行引用。

我们回到 DAG 的结构中，我们发现每一个绿色的交易都会有一条从黑色起始位置通往它的路径，那么你这笔交易的可信程度就可以很容易计算。

例如我们执行 MCMC 算法 N 次，这笔交易被全网接受的概率就是 M/N，其中 M 就是能从底部通往这笔交易的数量。

Tangle 结构和 MCMC 共识是非常具有吸引力的，它也带来了以下特性。

0 交易费：由于没有记账节点，目前没有考虑设置交易费。

水平扩容：由于 Tangle 的结构不涉及记账节点，交易吞吐可以随着规模大容量也跟着提升。

分区再合并：由于不是单链结构，私下记账以后也可以合并到 Tangle 账本中，不存在分叉这一说。

IOTA 的 Tangle 账本结构，为区块链技术带来了新的视角，这也是它吸引人的关键。

卡尔达诺 Cardano

卡尔达诺（Cardano）也是一个正在开发中的新一代区块链智能合约平台。

卡尔达诺项目最大的特色是由理论研究主导，严格采用数学形式化验证的来证明严谨、安全性的区块链。

卡尔达诺认为现阶段基础公链在无论在可规模化性（Scalability）、可互操作性（Interoperability）和可持续发展性（Sustainability）均存在不足，卡尔达诺希望进行概念和技术上的创新，最终解决上述三个方面问题。

卡尔达诺的团队认为目前区块链面临着两个比较突出的问题：

1. 区块链协议的升级将会导致区块链分叉； 2. 区块链的水平扩容和垂直扩容能力不足。

所以 Cardano 提出了分层架构理念，这似乎与传统 IT 架构模式：分层式架构模式有点像，卡尔达诺由两个层次组成。

Settlement Layer 清算层：卡尔达诺的代币 ADA 在该层流动，是整个系统的支付和清算的基础。

Computation Layer 计算层：卡尔达诺将在计算层提供智能合约、身份认证、消息通信等等功能。

相比于概念创新，卡尔达诺的团队研究了一种被命名为 Ouroboros 的算法，它其实也是 PoS 共识算法的变种，不同的是卡尔达诺团队为此提供了数学形式化证明，证明了它是高效、安全的共识算法。

卡尔达诺是一种理论研究驱动实践的尝试，无论是两层设计，还是 Ouroboros 算法，都为区块链技术的发展提供了值得参考的视角。

总结

今天，我们介绍了 EOS、IOTA、ADA 三个受人瞩目的区块链项目，EOS 和 ADA 都是致力于区块链去中心化的应用平台，IOTA 致力于为物联网提供分布式账本。这些项目引领了区块链的发展方向，无论是技术层面还是市场层面，他们都是非常出色的。

第22讲 | 国内区块链项目技术一览﻿

小蚁 NEO

1. 简介

我们以前讲到过，NEO 的前身是小蚁，小蚁最早在 2015 年发起，它在 2017 年中正式更名为 NEO。

NEO 项目一共经历过两次 ICO，第一次 ICO 是项目创立，第二次 ICO 是项目更名后的品牌升级。可以说通过 NEO 项目的起起落落见证了整个国内区块链项目的发展。

在重做了市值管理和社区建设后，NEO 成为了市值 TOP10 区块链项目之一。

2. 设计思路

NEO 是一个开放式智能经济平台，它提供了数字身份、数字资产、智能合约三种核心元素用来支持 NEO 智能经济生态。

数字资产：数字资产是以电子数据的形式存在的可编程控制的资产，NEO 在底层也直接支持类似 ERC20 的 Token 机制，所以用户可以在 NEO 上自行注册登记资产、交易和流转。它也通过数字身份解决与实体资产的映射关系，用户通过正规的数字身份所注册登记的资产受到法律的保护。

数字身份：数字身份是指以电子数据形式存在的个人、组织、事物的身份信息，NEO 将实现一套兼容 X.509 的数字身份标准以及支持 Web Of Trust 式的点对点的证书签发模式。

智能合约：NEO 上的智能合约与以太坊不同，叫做 NeoContract。这套智能合约体系的最大特点是直接支持 C#、Java 等主流编程语言，所以开发者可以在熟悉的 IDE 环境（Visual Studio、Eclipse 等）中进行智能合约的开发、调试、编译。

NEO 的通用轻量级虚拟机 Neo VM 具有高确定性、高并发性、高扩展性等优点。

3. 技术特点

NEO 采用了 PBFT 类的共识算法。NEO 的修改版为 dBFT 共识算法，这里 d 为 Delegated，就是代理人的意思。所有的 PBFT 类算法都有个特性，就是通信复杂度是节点数量的平方次，例如 7 个节点出一次块至少通信 72 次，对网络带宽要求很高。所以记账节点一般不会很多，它带来的优势就是 TPS 较高，并且不会分叉。

自成一派的智能合约体系。这里降低了智能合约开发者的局限性，不必使用 Solidity 语言开发。

C# 技术生态。NEO 的主要实现都是 C# 语言编写的，得益于.Net Core 的开源，NEO 的技术生态也在一直扩张。

Token 体系。提供了等价于以太坊 ERC20 的 NEP-5 Token 体系。

元界 Metaverse

1. 简介

元界是我所主导的一个开源区块链项目，项目于 2016 年 8 月发起，经过了 5 个月开发和测试，于 2017 年 2 月份上线。

元界是一个关注社会和商业需求的区块链项目，目标是构建以数字资产（Metavase Smart Token）和数字身份 (Avatar) 为基础新型区块链生态，这种生态会为人类社会带来深刻的变革。

除了数字资产和数字身份两个概念，我们还提出了 BISC 内置智能合约和 BaaS 区块链即服务的概念，并把数字身份作了延伸，提出了 Oracle 价值中介（此 Oracle 非彼 Oracle）。

总体思路是总结人与人、人与资产之间的关系，把总结后的通用需求抽象成模型，然后做到区块链底层供使用者方便使用，这种方式我们叫做 BISC（Buit-in Smart Contract）内置智能合约，它可以降低商业应用在开发和使用过程中的技术风险。

通过 BISC，元界提供了数字资产 MST、数字身份 Avatar、Oracle 以及资产交易的功能，这一切都是围绕资产和人来展开的。

数字资产 MST 可以让人们获得区块链带来的点对点操作资产的优势，数字身份 Avatar 体现了人与人、人与资产之间的关系。

它可以连接到 MST 上，通过 Avatar 任何人都可以成为 Oracle，Oracle 可以帮助人们构建不可篡改的去中心化信誉系统，资产交易可以为 MST 解决基础的流动性需求。

人们将区块链作为基础服务植入 IT 系统中的过程叫做 BaaS（Blockchain As A Service），BaaS 是一种快速、方便构建区块链应用的方式。

2. 技术特点

延续并扩展了 UTXO 模型，一切皆 UTXO 为资产和身份带来了良好的安全性。

内置 BISC，没有为用户提供自己编写智能合约的功能，提高了安全性，降低了多样性。

PoW 挖矿，与以太坊的 PoW 挖矿算法兼容。

内置了数字身份，提供了基于数字身份的域名系统，可以连接到数字资产上。

默认提供 HD 类型的主私钥账户体系。

块上限是 1MB，但出块速度是 33 秒，所以 TPS 大约是比特币的 18 倍。

提供等价于 ERC20 的 MST Token 体系。

量子链 QTUM

1. 简介

量子链致力于开发比特币和以太坊之外的新型区块链生态，它的目标是通过自行设计，让比特币和以太坊完美地融合在一起，并通过智能合约为人们提供 Dapp 平台。

除此之外，量子链还提出了移动端 Dapp 策略，通过引入身份机制和 Data-feed 链外数据达到合规性要求，最终通过推动 Dapp 的普及，让传统互联网企业可以将量子链作为一个新的应用平台进行尝试。

量子链关注利用区块链技术进行价值传输，首次提出了 VTP——Value Transfering Protocal，价值传输协议的概念。这里的价值传输协议是对标 HTTP、SMTP、POP3、SSH 等协议的。

量子链认为，在比特币之前人们一直无法在不借助第三方的情况下进行较好的点对点价值转移，比特币是运行在互联网上的一个 VTP 协议，随着区块链技术的发展，人与人、人与信息的交互更加多样化，未来会有更多的实体会被数字化（Tokenization）。

这里所说的就是资产登记，被登记完之后，肯定还会面临价值流转的问题。量子链从技术出发，提供了第一个结合比特币 UTXO 和以太坊 EVM 的区块链技术生态区来解决上述问题。

2. 技术特点

基础代币 QTM 与比特币脚本高度兼容，兼具 UTXO 和账户模型的优点。

与以太坊智能合约体系高度兼容的技术栈。

共识算法使用了 PoS3.0 算法，属于经典 PoS 算法。

提出了主控智能合约和普通智能合约的概念，通过主控合约可以引入链外数据 Data-feed。

通过主控合约可以提供合规性需求。

提供了等价于以太坊 ERC20 的 QRC20 Token 体系。

比原链 Bytom

1. 简介

比原链是一种多元的资产交互协议。简单来理解也是做数字资产的，不过换了种说法，理念稍不同。比原链认为在区块链上存在两种不同形态资产。

比特资产：是指区块链上原生的数字货币、数字资产，例如比特币、以太币；

原子资产：对应到现实世界的资产，例如权证、权益、股息、债券、情报资讯、预测信息等。

人们可以通过比原链进行对上述两种资产进行登记、交换、对赌、甚至基于合约的更具复杂性的交互操作。目的是连通原子世界与比特世界，促进资产在两个世界间的交互和流转。

比原链采用三层架构。

应用层对移动终端等多终端友好，方便开发者便捷开发出资产管理应用 ;

合约层采用创世合约和控制合约进行资产的发行和管理，在底层支持扩展的 UTXO 模型 BUTXO， 对虚拟机做了优化，采用自省机制以防止图灵完备中的死状态；

数据层使用分布式账本技术，实现资产的发行、花费、交换等操作。

2. 技术特点

共识算法是 PoW，属于忠实的比特币 PoW 党。

挖矿算法采用对人工智能 ASIC 芯片友好型算法，在哈希过程中引入矩阵和卷积计算，使得矿机在闲置或被淘汰后，可用于 AI 硬件加速服务，从而产生额外的社会效益。

兼容比特币 UTXO 模型。

默认提供了基于 HD 的主私钥账户体系。

加密模块提供了基于国密 SM2、SM3 标准算法。

植入了隔离见证设计。

本体网络 Ontology Network

1. 简介

本体网络是原 NEO 项目组成员李俊创立的，不过与 NEO 是完全独立的项目，随着技术大咖季宙栋的加入，市值跃入 TOP20。

本体网络是一个主打构建分布式信任体系的区块链项目，支持多链、多系统融合的协议网络，不同的链和不同的系统都可以通过本体的信任协议进行协作。

本体包含独立的分布式账本、P2P 网络协议、模块化的共识协议组，模块化的智能合约机制几个主要模块。

本体的产品形式是 ONTO，ONTO 是基于本体的综合客户端产品、区块链搜索引擎和区块链体系的入口。

ONTO 将帮助用户实现包括数字身份管理、数字资产管理、分布式数据交换等综合性功能，ONTO 可以将数字身份与现实身份进行映射关联，用户可以利用这款产品建立自己的数字身份和多维的身份画像，通过密码学算法实现隐私保护。

本体主要提供了以下三种协议。

提供分布式身份管理框架 （ONT ID），一个基于 W3C 的 DID 规范构建的去中心化的身份标识协议。

提供分布式数据交易协议 （ONT DATA），用于构建去中心化数据交易应用框架。

提供了信用评分协议（ONT Scores)，支持建立开发不同的声誉评价逻辑，提供评级授权与审计功能。

支撑这些协议的是 ONT 公链，以及 ONT 区块链高性能可定制化框架。

2. 技术特点

基于账户模型，并保留 UTXO 模型。

共识算法采用 VBFT，它是结合 PoS、VRF(Verifiable Random Function) 和 BFT 的全新共识算法。

模块化的智能合约，提供 WASM 和 NEO VM 两种。

通过 FPGA 加速计算密集型的业务模块。

多层跨链的结构设计。

提供链上搜索引擎。

总结

今天带你了解了一些从国内发起的比较知名的区块链项目，其实还有不少区块链项目，例如公信宝、YoYow 等，今天就介绍到这里，你可以进入这些项目的社区寻求更详细的资料。

第23讲 | 联盟链和它的困境﻿

不知不觉我已经写到了深入区块链技术部分的最后一篇，今天我们就一起来聊聊联盟链。

其实，在 2016 年的时侯，联盟链是非常火热的，当时的公链还处于探索阶段，以太坊也不够成熟，这给了很多联盟链涌现的机会。所以说，从技术上来看，联盟链其实非常强劲，毫不逊色于著名的区块链项目，下面我们就一起来看看联盟链技术。

简介

联盟链源自于 Vitalik 对区块链的概念分类，是他第一次提出了联盟链的说法，联盟链的英文是 Consortium Blockchain。

我们回顾一下联盟链。所谓联盟链，就是这个区块链具有准入许可，不像公链，任何人都可以随时进入，准入许可意味着候选节点进入区块链时需要得到已经在网络中的节点的许可。

所以联盟链也叫做许可链，也就是 Permisson Chain，这个叫法在国外比较常见。联盟链的节点数通常不多，维护成本相比公链要低。

有关联盟链与公链的概念区别，它们的区别仅仅是看新加入的节点是否要经过全网中其他节点的许可，这决定了一个区块链是否开放，开放程度决定了项目生态的大小，这也是最直观的区别。

联盟链的技术框架很多，其中又以超级账本项目下的技术框架最为知名，应用也最为广泛，它基本代表了联盟链，所以，今天我们就重点来介绍一下超级账本项目。

超级账本 HyperLedger

超级账本在 2015 年年底被发起，吸纳了众多重量级公司加入，它们包括大家耳熟能详的 IBM、Intel、Accenture、日立、JP 摩根、Digital Asset Holdings 等公司。

超级账本的代码和组织结构都结构清晰、层次分明。可以说无论从声势还是实力上来说，它都可以完胜公链。

例如，超级账本组织是会员制的，加入超级账本需要缴纳一笔入会费，入会费决定了你的会员等级。再如，超级账本 Frabric 的架构设计简直就是教科书级别的，干净利落、模块清楚，几乎挑不出毛病。

超级账本由 Linux 基金会主持，宗旨是构建一个面向企业应用场景的开源分布式账本技术平台。

因为企业应用场景的多样性，所以超级账本包含了不只一个项目，它是由多个项目组成的。一共 9 个项目，其中 5 个是主要的技术框架，其他 4 个是辅助性工具。

它的主要技术框架分别是下面的 5 种。

1.Hyperledger Fabric ：没有中文名，暂译【纺布克】，是 IBM 提供的，超级账本第一个项目。 纺布克旨在用模块化架构作为开发区块链程序或解决方案的基础，允许一些组件——例如共识算法和成员管理变成即插即用的服务。

2.Hyperledger Sawtooth：中文名【锯齿湖】，Intel 提供，是超级账本第二个项目。 锯齿湖是一个可以创建、部署和运行分布式账本的模块化平台，基于硬件依赖的 PoET 共识，可以面向大型分布式验证器群，同时也比较低功耗。

3.Hyperledger Iroha：没有中文名，暂译【伊路哈】，由 Soramitsu 提供。 伊路哈是为了将分布式账本技术简单容易地与基础架构型项目集成而设计的一个区块链框架。

4.Hyperledger Burrow：没有中文名，暂译【掘地者】，由 Monax 提供。 掘地者提供了一个模块化的区块链客户端，提供了权限管理的智能合约虚拟机，它部分建立在以太坊虚拟机（EVM）规范的基础上。

5.Hyperledger Indy：没有中文名，暂译【因迪】。 因迪是特别为去中心化的身份而建立的一种分布式账本。它提供了基于区块链或者其它分布式账本互操作来创建和使用独立数字身份的工具、代码库和可以重用的组件。

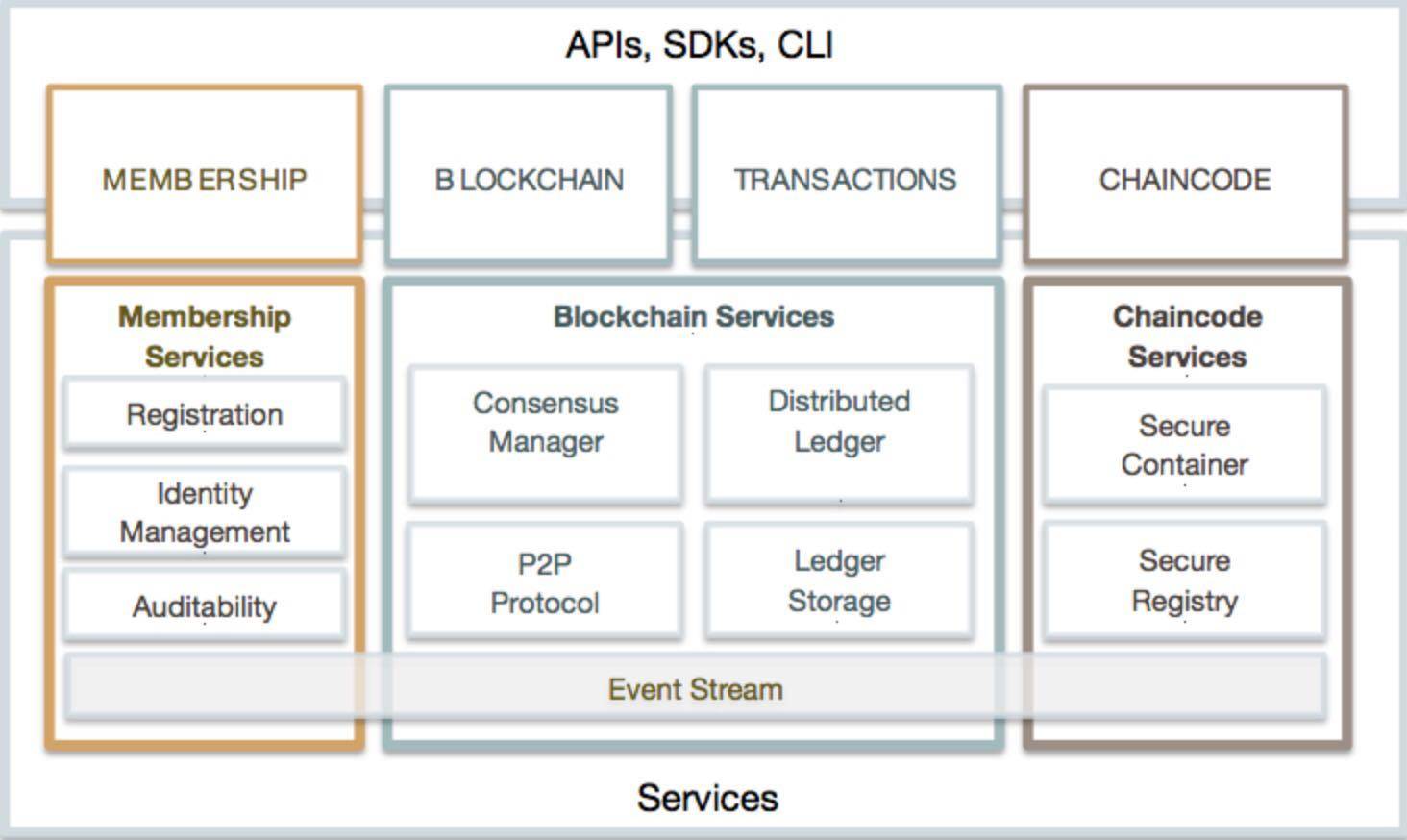
另外 4 个辅助性工具是：Cello、Composer、Explorer、Quilt，这四个辅助性工具可以对以上 5 个框架进行管理，例如 Composer 可以类比 Docker 中的 Composer，Explorer 就是区块浏览器。

我们不排除随着超级账本的发展，还有新的技术框架加入，当然，也可能存在既有的框架被市场淘汰。不过这些都不是本文的重点，所以我们不作过多介绍，你可以通过查阅超级账本官方网站获得更多内容。

1. 纺布克 Fabric

纺布克是由 IBM 提供的，它基于 Go 语言，前身是 Openchain 项目。在超级账本成立之初，Openchain 的代码量就已经达到 4 万行了，随着项目的推进，项目成员对 Openchian 进行了重构，也就是我们看到的纺布克 1.0 版本。

纺布克提供了比较完备的模块化组件，如下图所示。

﻿﻿

我们可以看到，它的架构上分成了：成员关系管理、区块链服务、Chaincode 服务三个大模块。

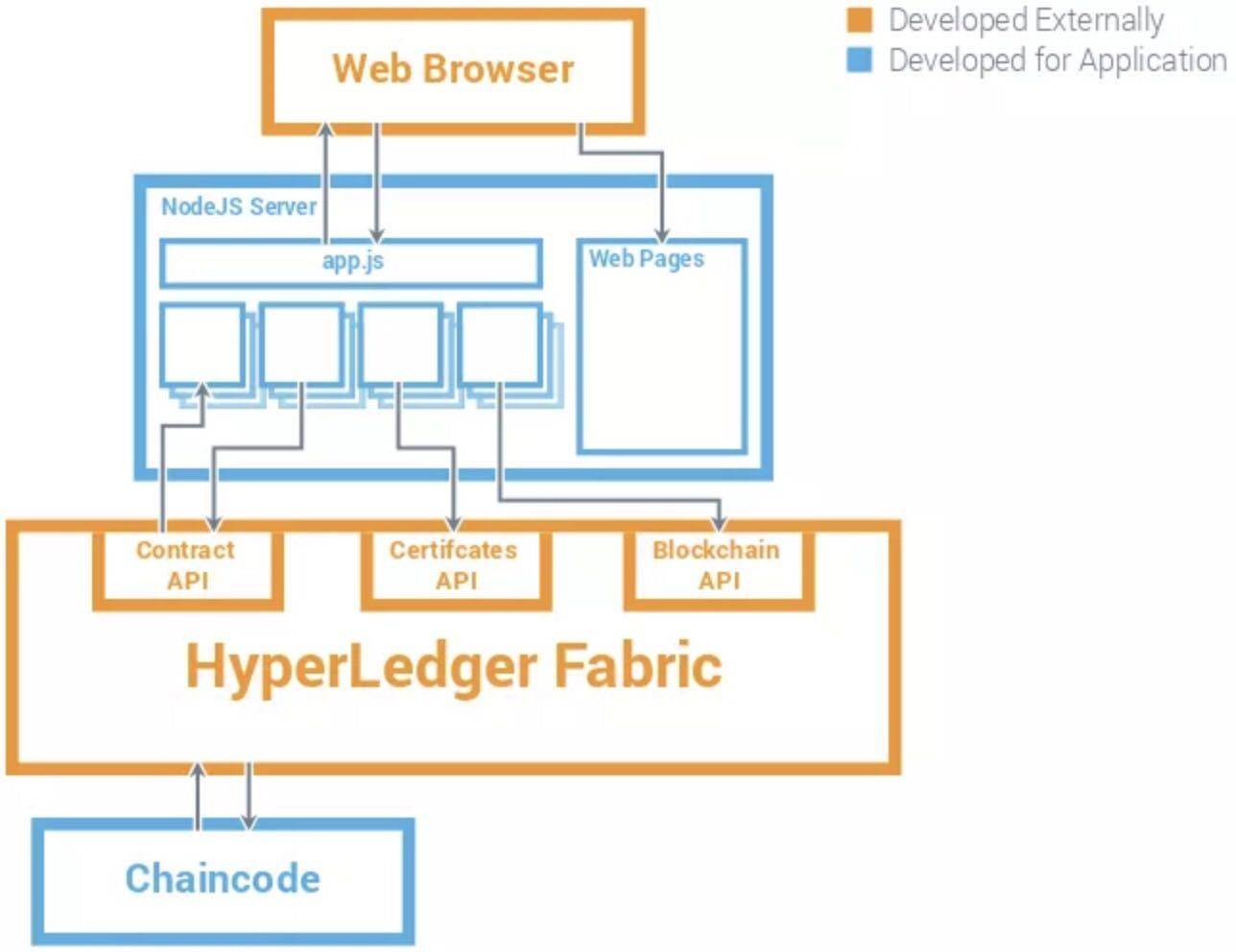
成员关系管理相当于账户和权限管理系统，区块链服务提供了区块链一样的账本结构，Chaincode 服务相当于智能合约。

成员关系管理是基于 PKI 的成员权限管理，平台可以对接入的节点和客户端的能力进行限制。

区块链服务提供一个分布式账本平台，多个交易被可以被打包进一个区块中，多个区块单向链接成一条区块链。区块链代表的是账本状态机发生变更的历史过程，这与公链区别不大。

Chaincode 包含核心的业务处理逻辑，并对外提供接口，外部通过调用 Chaincode 接口来改变账本数据，在纺布克中，Chaincode 是运行在隔离环境中的，也就是 Docker。

纺布克的一个可能的工作模式如下图。

﻿﻿

如果 Chaincode 运行在 Docker 中，我们按照经典的 IT 架构来分析，可以发现纺布克基本就是经典分布式系统的升级版，它可以提供宕机容错，可插拔的共识模块让用户自行选择是否需要拜占庭容错。

2. 锯齿湖 Sawtooth

锯齿湖也是一个高度模块化的区块链技术框架，它基于 Python 语言，1.0 版本之后和纺布克一样，作为一套稳定的框架，它已经有了实际的应用了。

它是第一真正意义上提供拜占庭容错共识选项的超级账本项目，有以下四个特点。

链上治理：利用智能合约进行投票运营成员管理彼此之间的关系。

高级交易执行引擎：可以并行处理交易的创建和验证，性能可观。

支持以太坊智能合约：兼容了以太坊智能合约技术栈。

支持主流语言编写智能合约：编写智能合约不局限 Solidity，可以是 Go、Javascript、Python 等语言。

相比以上四个特点，最引人注意的其实是锯齿湖提供了一个新的共识算法，叫做 PoET（Proof of Elapsed Time），它的中文译作：时间流逝证明。

如果你熟悉 Raft 共识算法的话，我们知道 Raft 算法是一类强 Leader 的共识算法，选举 Leader 的时候，每个节点自己倒计时（CountDown），最先数完的那个成为候选人。

这个过程叫做超时选举（Election Timeout)。每个节点每轮选举中得到的倒计时时间是不同的，它的代码实现为随机产生，通常是 150 毫秒到 300 毫秒。

PoET 与上述规则类似，只是倒计时时间的产生变更为硬件依赖的，这里的硬件目前是由英特尔提供的 SGX，Software Guard Extensions，它可以提供可信的程序执行环境。

SGX 提供了一种名为 Enclave 的机制，它支持两个函数“CreateTimer”和“CheckTimer”。CreateTimer 用于从 Enclave 中产生一个计时器。

CheckTimer 会去校验这个计时器是不是由 Enclave 产生并验证是否已经过期。如果满足这两个条件就给该节点开具一个证明，这个证明可以被其他节点验证，验证通过则表示同意该节点成为记账节点。

我们看出，PoET 共识算法的拜占庭容错是由 SGX 保证的，具有一定的硬件依赖。

锯齿湖官方提供了的四种工作模式：开发模式、PoET 模式、PoET 仿真模式以及 Raft 模式。

可以发现，锯齿湖相当于是 Raft 协议的变种版本，选择 Raft 模式使得锯齿湖可以退化成经典分布式系统。

3. 掘地者 Burrow

掘地者也是一个基于以太坊 EVM 的智能合约执行引擎的区块链技术框架，最初项目名叫 Eris，它是基于 Go 语言构造的。

掘地者主要由下述组件组成。

共识引擎：提供了基于 Tendermint PBFT 算法的高性能拜占庭容错共识算法。

应用程序区块链接口 ABCI：为共识引擎和智能合约引擎提供接口规范。

许可型以太坊虚拟机 EVM：权限许可是可以通过本地安全接口强制绑定到智能合约上，其他与以太坊智能合约一样。

API 网关：提供 REST 和 JSON-RPC 两种 API 接口。

掘地者也是模块化的分布式账本技术，提供许可型的智能合约执行环境，它也基于 EVM 规范。除了 Tendermint PBFT 共识算法，没看到与纺布克的的区别。

4. 伊路哈 Iroha

以上几个技术框架，基本都是通用技术框架，不涉及业务概念。伊路哈是第一个关注资产创建和管理的区块链平台，通过名字我们也可以发现是一个日本公司主导的项目。

伊路哈具有如下特征。

可以帮助人们创建和管理多样化的复杂资产，例如货币、不可分割的权利、产品序列号和专利等等；

提供基于域名分类的账户管理机制，类似“子账本”系统；

提供权限管理；

系统本身提供验证业务逻辑规则，以及交易查询接口。

相较于纺布克和掘地者是 Go 语言开发，伊路哈是使用 C++14 开发的。

5. 因迪 Indy

因迪也是一个从身份出发去构建一个分布式经济系统的技术框架。

因迪具有如下的特征。

基于多冗余拜占庭容错 RBFT（Redundant Byzantine Fault Tolerance）实现的共识算法，叫做 Plenum。

意图通过构建去中心化的身份来打造分布式账本。

全局唯一性的身份，无需中心化授权。

基于 W3C 标准的身份属性和格式；

提供零知识证明手段。

因迪与其他通用技术框架显得非常不同，对身份的研究或许会成为因迪的突破点，这点与元界的数字身份很像。

BaaS 与 BTaaS

超级账本很多技术框架是可以依托云计算来帮助企业进行快速搭建的，当然 IBM 和微软已经开始这么干了，他们将它称之为 BaaS（Blockchain As A Service)。

我们进一步思考，例如比特币提供了全球支付的功能，那么这种功能是否可以植入到云服务中呢？

答案是肯定的。对于诸多有支付需求的应用来说，自己搭建比特币节点，并且结构化区块到数据库中是非常痛苦的过程，毕竟比特币全节点提供的 API 有限，而我们的查询需求可能细致到交易输出和脚本签名。

所以，把比特币转化成 PaaS 服务也是另外一种 BaaS 思路。

因此，我们把原来的 BaaS 概念拆成了两种：

BaaS 是指把公链提供的服务转化成云计算中的 PaaS 服务的过程；

BTaaS 是指把区块链技术框架转化成 PaaS 服务的过程。

﻿﻿这两种概念还是有较大内涵上的差别的，我使用了上图来表达，我认为 BaaS 是未来区块链的发展方向，BTaaS 只是作为经典方案的补充。

联盟链的困境

超级账本系列技术框架很好地诠释了分布式账本技术走到极致是什么样子的。

这里也可以看出，几乎所有的超级账本项目都是技术主导，技术的强大也让他们忽视了市场的真实需求。

联盟链是少数节点之间的活动，它往往退化成微观经济中的博弈，所以利用联盟链构建少数节点之间的协作系统不是一个技术问题，而是变成了如何构造一个稳定的微观经济模型使得协作者可以达成帕累托改进，在这里，技术变成了次要的。

再好的技术工具如果不结合有效的激励和反馈机制，那么联盟链的应用落地过程似乎变得异常艰难，它很可能最后沦落为普通的分布式系统，这个分布式系统仍然是中心化的。

这里我再提出一个问题，为什么我们不用已经成熟的技术框架，非要用联盟链技术框架呢？这就是我认为联盟链最大的困境，它是一杆加农炮，但是并没有人来告诉我们这杆加农炮可以解决什么问题。

总结

今天我们重点介绍了超级账本旗下的五个联盟链技术框架，希望可以给你提供一些技术选型上的参考。随后我们又介绍了区块链即服务这一延伸概念，最后我向你分享了我对于联盟链的观点。

第24讲 | 比特币专题（一）历史与货币﻿

比特币的逆袭史

俗话说读史明智，我们就从比特币的历史开始聊起。比特币的历史总结起来大约有四个时期：创立前期、创立期、成长和稳定期。

创立前期

在比特币创立之前，世界上已有多种类似技术产品，最早的是 Ecash 协议，接着 Ecash 又有多种数字货币产品出现，其中以亚当·贝克的“Hashcash”和戴维 (Wei Dai) 的“B-money”、尼克·萨博的“Bit-gold”，以及哈尔·芬尼在“Hashcash”技术上发展出来的“RPOW”等技术产品。

创立期

2008 年 11 月，中本聪发表了比特币的白皮书《比特币：一种点对点的电子现金系统》，接下来的时间中本聪实现了他所描述的比特币系统。

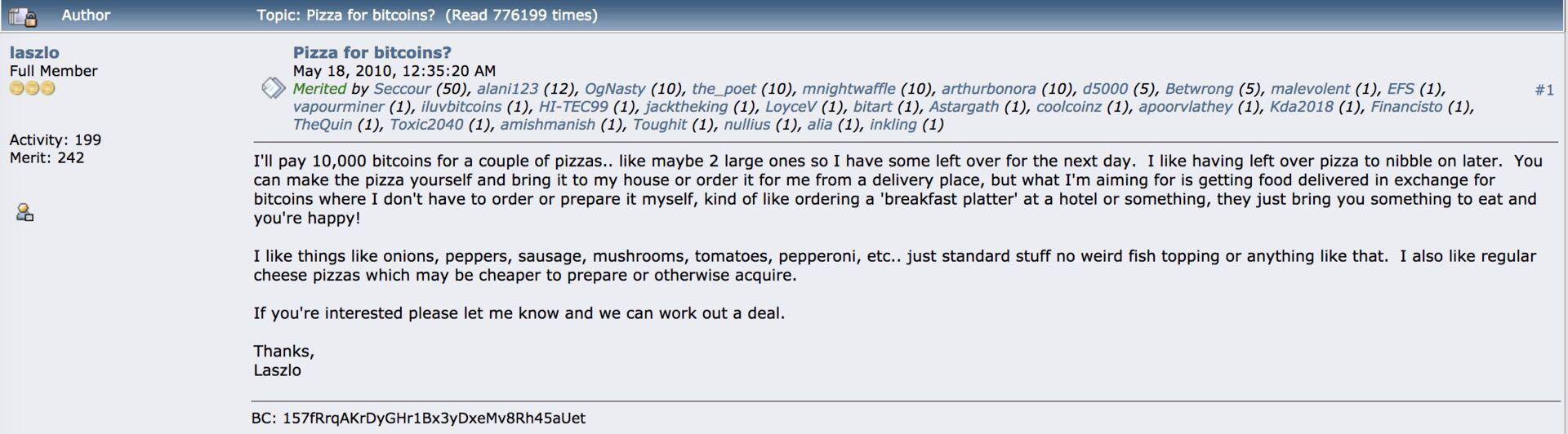
2009 年 1 月 3 日，比特币网络正式开始运行。中本聪在创始区块中写道“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”。这句话有两层意义，第一层意思是表示了中本聪没有预先挖矿，毕竟这是当天泰晤士报的新闻，中本聪显然不可能预先获知泰晤士报将要报道些什么。通常对这句话第二层意思的解读是：认为中本聪嘲讽了当下的中心化银行体系。

2009 年 1 月 9 日，Bitcoin v0.1 版本发布，12 日中本聪进行了第一次交易，这一次交易中，中本聪给海尔发送了 10 个比特币。

2009 年秋天, 一个叫“新自由标准”的用户通过 Paypal 支付了 5.02 美元，购买了 5050 个比特币，折合 0.000994 美元一个比特币，这是比特币和法币的第一次兑换。

2009 年到 2010 年初，已经有一些其他的开发者被逐渐吸引过来，大家一起开发、维护、挖矿，那时候普通电脑还可以挖到比特币。

2010 年 4 月, 一个叫拉斯诺的人发现可以使用 GPU 来挖比特币，5 月 22 日，他用挖到的比特币购买了两个比萨，共花费 10000BTC，这是比特币第一次被用于实物支付，也就是著名的比特币披萨事件。

﻿﻿

2010 年 7 月，世界上第一家比特币交易所在日本东京成立，名叫 Mt.Gox，中文“门头沟”。

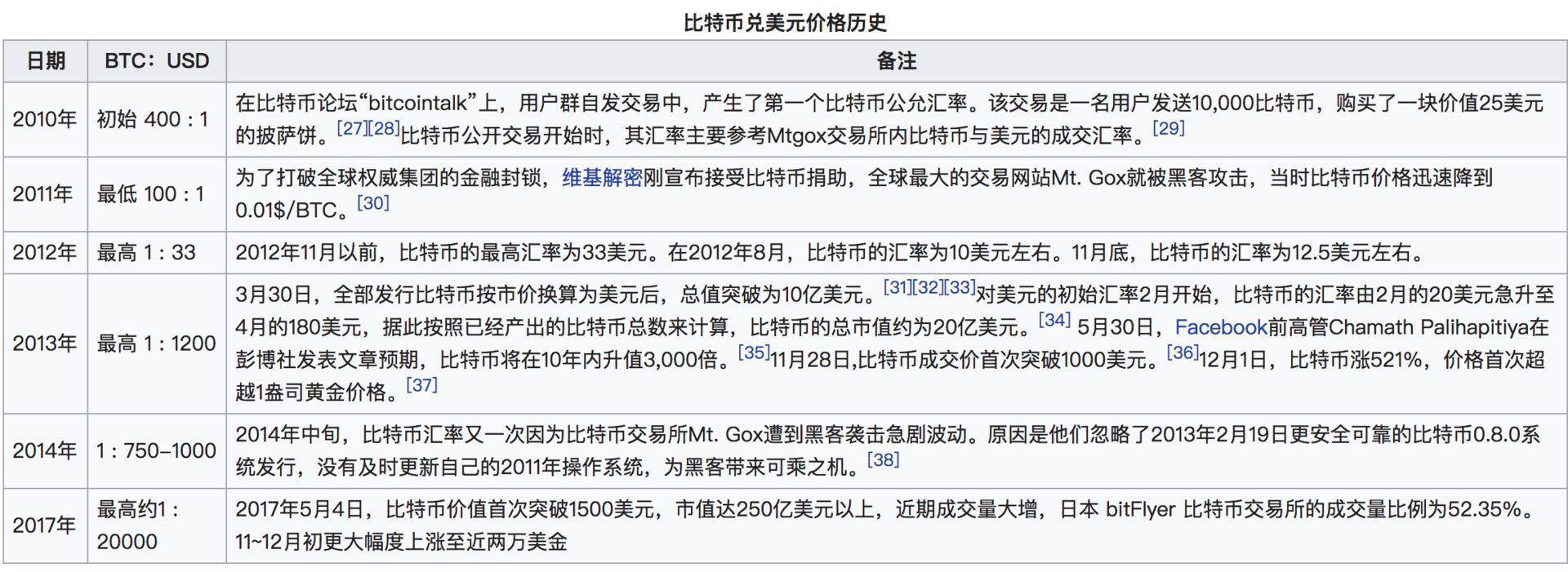
成长期和稳定期

2014 年 2 月，发生“门头沟事件”，门头沟交易所被黑一事震惊全球，比特币价格应声跳水；

2014 年 6 月，以太坊开始了为期 42 天的 ICO，众筹使用的是 BTC；

2017 年 11 月 28 日，比特币价格超过一万美元。

最后附一份由维基百科归纳的比特币价格变化以及对应的事件。

﻿﻿

从上图可以看出，比特币的成长史就是对美元的逆袭史，比特币的发展经历了很多争议和阻碍，但是依然不妨碍它成为一种世界级现象，甚至是很多人的信仰，那么比特币的意义到哪在那里呢？

比特币的意义

这个话题可能会引起一些争论，我姑且将本节的内容限定为“我”所理解的比特币，仅供你参考。

首先比特币没有通常意义上的实用价值，不单单是比特币，所有的信用货币，包括黄金白银在内都不具备实用价值。

这里的实用价值是指解决人的低层次需求，如果按照马斯洛需求层次理论来分，是指衣食住行等生存需求。

换句话说，比特币也好，黄金也好，在生活面前都是废物，而无法直接利用，毕竟黄金吃下去也不能饱还有生命危险，比特币的私钥即使看得见却也摸不到。

但是用货币就是能买东西，买来的东西可以帮你解决生存需求，换句话了吃饱了才能干其他事情。“买”这个动作就是比特币所要解决的，当然信用货币也能解决，也就是我们所说的支付功能。

所以作为信用货币的比较，比特币到底有什么不同？它的意义超过信用货币吗？我个人认为是超过的。老生常谈的去中心化、防篡改我这里就不谈了，我们接下来换几个角度来聊聊它。

1. 无国界的共识

它打破了一般信用货币的局限性，我称作无国界的共识。

比较常见的论调，比特币你信它就有价值，不信就什么用途也没有。这里隐含的语义是“承认过程”。

例如你在美国吃顿饭，使用人民币支付，美国人一定不是特别同意，毕竟在美国就必须使用美元支付。换句话来说，“承认过程”很大程度上是身不由己，你所处的国家决定了必须承认某种信用货币。

比特币奇怪就奇怪在，没有人会强迫你使用比特币，你的一念之间就可以决定比特币对于你的价值。

如果类比到黄金，比如你长这么大，一直都是别人告诉你黄金非常值钱，所以你也觉得黄金值钱，这其实就是共识灌输的过程，当然你也可以公开表示“我觉得黄金不值钱”，这当然也没什么问题。

想象一下，如果全世界都能达成比特币都可以用于支付的共识，比特币和黄金在共识的效果上也没什么不同了，那么声称“我觉得黄金不值钱”就变成了“我觉得比特币不值钱”，这里的逻辑是一样的。

2. 记账是本职

比特币的本职是记账，不要想得太复杂，它就是来帮你记账的。例如你在宜家买了一套家具，比特币可以帮你记下来，当然不是说这个事件，而是帮你记录价值转移，你动用了你曾经创造的价值的多少（BTC）来购买这套家具。

这个记账过程防篡改能力非常强，几乎没人能操控，也没有国界之分，只要你的交易方承认比特币，这笔买卖就可以达成。

3. 高效的资源调度

比特币使用的是 PoW 算法，这个需要消耗大量能源进行挖矿的算法一直被人诟病；但是结合上述记账本职，我们也换个角度来看看这件事。

目前全国的电力分配不均，中国的内蒙东北有着丰富的风力电，可惜这些富余的电力难以调度，超高压输电线路造价高昂，甚至超出了电厂本身。

而比特币挖矿恰好需要极大地耗费能源，如果在偏远的资源丰富地区进行挖矿，相当于将架设超高压输电线路蜕化为网络通信设施，地方政府可以把庞大的风电资源转化成比特币，最多只需要十分钟，就可以在资本市场变现。所以每个人每次使用比特币的过程，相当于让偏远地区获得了平等参与社会运作的过程。

4. 三权分立的社区自治形态

这里讨论的三权分立的形态，并不是指政府组织结构的形式，而是指矿工、开发者、投资者三者组成了相互制衡的数字货币的治理形态。

比特币并没有真正意义上完全地去中心化，在记账权上，它目前被 5 大矿池所把持。当人们抨击 EOS 的 21 个节点有中心化的嫌疑时，BM 总是拿出比特币矿池的例子来反击。

实际上这里偷换了概念，比特币中矿工的权力其实是有限的。

技术限制：由于 PoW 的特性，矿工无法进行长程攻击（Long Range Attack），篡改和分叉的边际成本随着篡改的区块数量线性攀升，所以看似矿工的 51% 攻击，也就改一两个块而已。

开发者制衡：扩容之争是很好的例子，我们下一篇会详细介绍，矿工是逐利的，而开发者决定了比特币的长期发展，所以从某种意义上来说，作弊不如和开发者合作。

投资者制衡：矿工是比特币的直接利益相关者，无论是社区分歧还是主链分叉，矿工首先确保的是收益稳定，黑天鹅事件造成的巨大价格波动是不利于收益预期的。

总结起来就是，虽然比特币在记账权上没有彻底去中心化，但是目前的情况也可以接受，至少矿工还受两方制约，矿工看收益，收益的价格看投资者，投资者看比特币长期发展，比特币长期发展看开发者，开发者受制于矿工，三者相互制衡。

BIP 及其发展

比特币 BIP（Bitcoin Imrpovement Proposals) 是一种设计文档，用来描述比特币新特性的提案，第一个比特币 BIP 是 2011 年 8 月 19 号一个名为 Amir Taaki 的人提交的，编号 bip001，它描述了 BIP 本身是什么。

随后几年直到现在，比特币的 BIP 编号将近 200 个，它展示了比特币强大的社区协作能力。

很多人认为某个区块链项目一旦上线这个链就稳了，实际上，做公链好比一场没有尽头的马拉松长跑，主网上线表示长跑开始，接下来才是真正拼实力的时候。

具体怎么拼？则要看 IP（Improvement Proposal）。可以说 IP 代表了一个区块链项目的生命力。例如 HD 账户是 bip32 和 bip39 提出的，最开始的比特币是没有这个功能的，隔离见证也是由一系列 bip 组成的。

我们再比如说，就算是你想修改比特币的 2100 万上限也是可以的，只要你提的 BIP 详细论证了改上限的必要性以及充分验证了达成条件，如果最终社区同意了你的提案，2100 万上限改成 3000 万个也不是梦，一切都是可以操作的。

这就回到了社区自治的特性上了，你承认并持有比特币，那么你就可以参与决策比特币的发展。

总结

好了，今天我们简要回顾了比特币的历史和货币形态，最后还介绍了 BIP，为下一篇介绍扩容之争做准备。

其实比特币作为整个数字货币的标杆和领头，对区块链生态和未来有不可忽视的力量。虽然现在号称区块链 2.0、区块链 3.0 的项目很多，但是真正意义上达到了工业级水准的，还是只有比特币。

第25讲 | 比特币专题（二）：扩容之争、IFO与链上治理﻿

扩容之争

扩容之争是比特币历史上影响较大的事件，它也是比特币社区治理的经典案例。扩容之争的背后其实是社区治理的难题：如何让社区达成一致。

扩容的需求是由于比特币的使用人数逐渐增长，于是比特币的网络也日益拥堵。关于如何解决这种网络拥堵的问题，比特币社区出现了两种不同的解决方案。

方案一：极端扩容，直接将区块的上限进行扩容，它的优点是可以快速解决问题，缺点是十分直接，只能舒缓一时的拥堵，并没有从根本上解决问题，更不能带来新的特性。

方案二：隔离见证，要求坚守 1MB 的容量上限，通过隔离见证的方法绕过 1MB 的限制。这种方式改动比特币交易的结构，它的优点是结构的改变可以带来崭新的特性，缺点也不少，不但花费的时间较长，用户的使用感知也并不算完美。

社区就上述的两种方案产生了不同的分歧（分叉），从而产生了极端扩容派和隔离见证两个派别，派别之间谁也不服谁，对峙十分激烈。

于是又出现了一些人开始试图调停双方的矛盾，希望社区不要分歧，可以达成一致。这一类人群就构成了第三个派别：调停和解派系。

至此，社区中形成了极端扩容派、调停和解派、隔离见证派三个派别，他们开启了漫长的拉锯战，中间也有达成过短暂的三次共识（92 共识、香港共识、纽约共识），调停和解也一度将极端扩容的上限从 20 降到 8M，甚至是 2M。但是，一切的努力，还是不了了之。

社区分歧仍然逐渐加大，最后比特币产生了硬分叉。一条链变成了两条。极端扩容派在比特币主链上硬分叉出一条没有隔离见证的链，分叉之后的币就是比特现金（ BitcoinCash），缩写 BCH，而隔离见证则成了现在我们看见的比特币。至此，扩容斗争进入双链对抗的时代。

关于扩容之争详细的来龙去脉。如果感兴趣的话，你可以查阅相关资料，一探究竟。

扩容之争引起的 IFO

扩容之争基本在 2017 年 11 月结束，比特币硬分叉出比特币现金已经成了定局。比特币现金的出现还带来了一件新事物，就是 IFO——Initial Fork Offering，也就是分叉比特币形成新的数字代币，这其实就是 ICO 的替代品。

这里要提一句，2017 年 9 月 4 号七部委发文明令禁止 ICO，所有和人民币挂钩的交易所都必须限期关闭。

“一刀切”政策让 ICO 在国内基本死掉了，于是国内的人坐不住了，就纷纷开始寻觅替代品。比特币的分叉带来了全新的灵感，于是 IFO 应运而生。

怎么理解呢？我们之前讲过 ICO，这里来回顾一下，ICO 的中文名是首次代币发行，又称为区块链众筹，这是一种新型的融资模式，投资者可以用手中的比特币或其他代币投到其他的区块链创始项目。

ICO 从本质上来说就是一纸白皮书，接下来全靠吹，忽悠散户投币，“我要出一个新的代币了，你们快来买吧。”

而 IFO 的集资依靠的是与比特币的关联，“我要出一个代币了，这个代币是由比特币分叉出来的哦，你们快来买吧！”靠着与比特币的连带性，IFO 打了一记集资的擦边球。

所以国内诸多项目方和经验资深的投资方一拍即合，搞 IFO 吧。但是 IFO 比 ICO 限定在只能从比特币上分叉，所以技术的发挥仍然有限。

一时间，除了比特现金，一共出现了 9 个比特币分叉项目，发行总量都是 2100 万，区别在于附加功能，例如区块时间调整、区块大小调整、是否有隔离见证、未来会加哪些功能等。

它们分别是下面这些项目，收录可能不全，你了解即可。

比特币黄金，Bitcoin Gold，简称 BTG，区块大小 1M，有隔离见证功能，区块时间 10 分钟。

比特币 2X，BitcoinX，简称 B2X，区块大小 2M，有隔离见证功能，区块时间 10 分钟。

比特币钻石，Bitcoin Diamond，简称 BTD，出块时间 60s，免手续费转账，比特币 10000:1 领取，持币有 POS 利息。

超级比特币，Super Bitcoin ，简称 SBTC，支持智能合约，闪电网络和零知识证明功能。

LBTC（闪电比特币，基于 DPoS 共识，需要重新开发，点付张银海为中国区负责人。

BTP（比特币白金）总量 2100 万，其他信息不详。

GOD（比特上帝）分叉，总量 2100 万，不挖，直接分发给用户，项目发起人郭宏才，人称宝二爷。

BUM（比特币铀）分叉，总量 2100 万，其他信息不详。

Bitcoin Silver（比特币白银），总量 2100 万，其他信息不详。

链上治理

链上治理指的是人们直接在区块链发起社区提案，并进行决策的过程。

这里首先要求的是链上支持基本治理协议，这套协议可以规定或强制执行提案，链上治理直接决定了区块链本身的发展方向。链上治理的参与方包括了投资者、使用者、开发者、矿工四类人群。

链上治理与链下治理的区别在于，区块链本身是否提供强制执行的机制让少数服从多数。

在链上治理协议中，参与者需要可以通过投票参与治理，而链下治理中，多数通过提案、社区见面开会等多种线下线上互动方式，让整个社区达成一致，扩容之争中的三次共识就是典型的链下治理。

各种类型的链上治理

1. 比特币 BIP 和区块投票

虽然比特币没有提供完整的链上治理机制，但是比特币也支持简单的投票机制，例如在区块中写入共识信息表示支持某项提案，例如矿工可以在区块中填写 NYA 表示支持纽约共识。

但这一切都是基于比特币的 BIP，首先得有 BIP，才能发起投票。BIP 的组织架构比较社区化，主要由 Github 上的一些开发者和核心社区成员组成。

矿工的所有行为也是非强制性的，当真正发生主网升级时，矿工仍可以选择不升级，这将带来分叉，也是所有人都不愿看到的。

2. 以太坊 Gas limit 投票

以太坊上提供了对 Gas 消耗的上限参数——Gas limit，矿工通过投票选择增加或减少 Gas limit，Gas limit 决定了单个区块上可以处理的智能合约数量，但这仅针对这一项细分功能，并不能决定整个区块链的发展。

实际上，以太坊的发展受 Vatalik 本身影响比较大，核心成员和早期资本的推动是以太坊治理的主要源动力。

3. 比特股 BTS 和柚子 EOS 的链上治理

我们在前面的文章介绍过 EOS 区块链链上治理结构——区块链宪法。实际上宪法也没有强制约束力，但是它成为了一种社区强制约束力，类似宣誓过程。

EOS 和比特股的治理结构来自于 DPoS 算法提供的投票过程，投票是根据币的数量作为权重的，使用者、投资者、开发者、矿工这四种角色中，其中把矿工和投资者进行了合并，受资本的要挟，风险比较大。

以上治理结构，我们把比特币和以太坊归为一类，这类倾向于链下治理，EOS 和比特股倾向于链上治理。

链上治理的几个问题

无论链上治理还是链下治理方式都存在一些问题。

升级的实际执行者矿工总是理性的，也就是追求自身利益最大化。

惰性投票，只有很少一部分人会真正地去投票。

投票权过度集中，大户持有者往往话语权更重。

链下治理相比链上治理，更接近我们现实社会的方式。链上治理不是一个设计问题，它是社区制度问题，“如何让区块链更好地发展”相比“区块链项目应当设定什么样的发展目标”，是排在第二位的。

社区在自身追求目标的过程中，会自发地找到最佳治理结构，人为设计可能会有诸多漏洞和缺陷，也限制了可开发性。

例如链上治理至少存在以下几个问题。

1. 公地悲剧

当所有人都觉得别人会投票的时候，也就没有人投票了，这个典型案例是英国脱欧公投。区块链上进行链上投票可能也会遇到类似的问题。

2.女巫攻击

目前区块链很难映射现实中人的身份，如果按照身份去投，大户是可以扮演多个伪造身份进行投票的，在产生区块链数字身份之前，链上治理只能依托于币的数量进行权重投票。这便造成一个代币一票，持币多的选民有更大的话语权。

3.贿选

这其实是女巫攻击的延伸，链上治理节点可以承诺将获得的收益与其他节点进行分享，这种拉票方式其实就是贿选，如果恶意节点可以通过贿赂成为记账节点，进而左右区块链的升级过程，后果非常可怕。

目前创始团队进行控制式治理是最常见的，在社区强大后，创始团队再退出，让社区自己运作，是比较典型的“中本聪模式”。

链上治理其实是一个很热门的话题，它关注的是区块链自身的发展，很可能会是区块链的一个重要研究方法，但是这并不是技术所能解决的，所以并不太乐观。

总结

今天带你了解了什么比特币的扩容之争，又从扩容之争谈到了区块链治理，区块链治理没有明确的最优方案，本篇更多地是带你了解了区块链行业的现状，希望能带给你一些新的思考。

第26讲 | 数字货币和数字资产﻿

据统计，截止 2018 年 3 月，全球数字货币共计 1500 多种，总市值超 3200 亿美元。然而市值分布占比不够分散，单比特币就占了一半市值，剩下以太坊、瑞波币、比特币现金等数字货币占了另外一半。

大致来分，目前区块链首先在金融领域发力，其次在信息通讯、底层基础设施、教育、能源、医疗等行业应用地比较广泛。

从占比来看，金融和信息通讯类占比最高，占所有区块链项目类型接近七成。

其中中国发起的项目偏好金融，金融类区块链项目接近一半，而从全球来看，金融类项目占比不到四成。这点也可以从我前面的文章得到佐证。区块链在各行业的快速发展，带来了全新的机遇。

从数字货币到数字资产

数字货币是数字资产的清算底层，数字资产的经济活动依赖数字货币。

数字货币一般只能是公链项目，数字资产依靠公链生态提供，这种支撑型结构决定了数字货币的种类不会很多，而数字资产会非常多。

目前数量繁多的数字货币最终会消亡一大半，只剩下几个生态丰富的数字货币，通过这几个数字货币来支持数量繁多的数字资产，而这些公链会通过一些大型的中心化交易平台完成互通互兑，小型的交易平台多为垂直类的数字资产服务。

比特币本身是最成功的数字货币项目，同时也是最成功的区块链项目。

比特币的应用生态主要集中在全球无国界支付结算上，由于比特币本身是一种原生资产，它没有与任何其他资产锚定，所以比特币的应用生态取决于人们的共识，这点比特币已经做到了。

只要比特币的社区不发生大的动乱，那么比特币的地位是很难超越的，尽管有诸多崭新的区块链技术冒出来，如提升共识效率、提升网络容量等等。

但是比特币的共识经过了近十年的历史开创，形成成熟稳定的生态结构，这一点在技术上是无法取代的。

所以比特币依然会作为互联网领域的第一支付手段，并且延伸到线下场合。

除了比特币还有 Tether 和 bitCNY 等锚定型数字货币，这些数字货币最大的特性是与法币锚定。其实也可以与实体资产锚定，只不过我们还没有走到那一步。

综上，我们可以总结出两大类数字货币：原生数字货币和锚定型数字货币。

原生型数字货币具有如下特点：

非营利性社区自治；

依赖社会共识承认；

超级结算工具；

可用于支持数字资产。

锚定型数字货币具有如下特点：

商业性自治；

依赖广泛的承兑商；

稳定的支付结算工具；

可用于支持数字资产。

那么根据数字货币的划分方法，我们也可以将数字资产划分为原生数字资产和资产数字化的资产。

数字资产的宏观分类

数字资产目前已经展现出非常强大的生命力，最终数字资产会像互联网应用一样席卷全球，数字资产交易所也会像春笋一样冒出。

借此时机，我对数字资产进行一个分类，数字资产所产生的金融我们称为数字金融，国内又称为通证和通证经济，涵义上差不多。

Token 是数字资产最直接的表现形式，Token 的生态结构具有自发和原生性，大致可以分成这几种类型。一种是基础设施型生态，一种是金融型生态，还有一种是商业垂直应用生态，这三种生态都非常有潜力。

基础设施型 Token

基础设施一般就是指公链的权益代币，很多公链都在做这个领域的研究，当然这也是最迫切需要被突破的，有了成熟的基础设施，区块链应用才得以广泛普及。

这类的 Token 的典型是以太坊上的以太币 Ether，除了以太坊，还有 EOS、NEO 等，可以说能够支持发行 Token 的公链都具有较高的潜在价值，它们目前处于军阀混战时期，后期是垂直细分还是一统江山很难判断。

另外基础设施型 Token 本身也具备数字货币的功能。

金融型 Token

这类 Token 的典型是 Tether、bitCNY 等锚定型数字货币，以及交易平台的 Token，例如火币的 HT、OKEX 的 OKB 和币安的 BNB。

这类 Token 的典型特点是在为原生数字资产创造流动性，它是数字金融发展的必然结果。

金融型 Token 有点接近证券，只能在流动性高的地方产生，例如数字资产交易所、承兑平台。

商业垂直生态型 Token

这一类 Token 具有非常大的商业潜力，释放的能量也是最大的，这里当然不是指单个 Token，而是某个商业生态形成的一类 Token。

例如游戏直播平台可以打通形成一类 Token，文化产权也可以打通形成一类 Token。这类 Token 是非常好的连接器，连接局部商业，在行业内部形成流动市场。

这类 Token 探索的人不少，例如游戏链、明星链此类，由于自己单干一个链太过垂直，会面临被以太坊收割的风险，所以在前面两个类型的 Token 成熟之前，这类 Token 并不会大规模流行。

同时，这类 Token 的设计者，也面临了两个挑战。

首先从业者需要理解区块链，理解区块链不单指理解区块链的技术原理，而是区块链本身蕴含的思维，这里的思维我归纳为两类，第一类是开放的产品形态，第二类是社区共同治理。

其次从业者容易拘泥于传统互联网时代的商业模式，例如做内容或做流量的 App，表现方式无非广告和会员，思维很难跳出来。

要知道，未来商业垂直型的 Token 几乎肯定都是原生数字资产，所以按照阿里或者腾讯的模式可能找不到区块链的方向，这类 Token 的未来一定是新的阿里和腾讯。

我预测这类 Token 会极大地改变互联网产品的运营模式，Token 模式下的产品运营会拉近用户与运营商的距离，他们不再是对立关系，而是区块链式的共生社区自治的关系，区块链的治理模式也会影响产品的运营模式。

最后我们总结一下，以上三类 Token 依赖关系是：

商业垂直生态型 Token 依赖基础设施型 Token；

金融型 Token 依赖基础设施型 Token；

商业垂直生态型 Token 可能依赖金融型 Token。

Token 的流动性大小依次是：

基础设施型 Token > 金融型 Token > 商业垂直生态型 Token

Token 的种类数量分布依次是：

商业垂直生态型 Token > 金融型 Token > 基础设施型 Token

数字资产的属性分类

上面我们从宏观角度对 Token 进行了分类，当然也可以从 Token 本身的属性进行分类。

这里可以引用我专栏第 5 讲“区块链与数字货币”那一篇，我们提到了虚拟货币的三种类型：游戏代币类、积分类、数字货币类，这里的分类方法主要是按照是否与实体经济发生联系。

那么 Token 从这个角度来看，只有两类。

普通 Token

积分型。这种 Token 可能比较常见，因为我们经常遇到，例如超市积分，产品积分等等，这种在产品运营上可能换了一种形式，相比较原来的积分体系，流动性可能有所提升。

会员型。大多数会员制的营销方式，相当于是使用权预售，例如苹果手机预售发行，不必局限在某个渠道商，可以以发行 Token 的方式进行预售。这种类型的 Token 也可以映射到当下现实场景中去。

分红型。这种类型的 Token 典型是币安的 BNB，利润回购是分红型 Token 常见的手段，但由于操作不够透明，很可能会遇到问题。

价值型 Token

很多人表示区块链是改变人类生产关系的一次革命，这点我表示认同。

例如以太坊，你拥有以太币，意味着你拥有这个系统的使用权，你需要通过以太币这个交易媒介才能跟别人进行交换目标资产。

这时以太币就有了货币属性，以太坊通过 DApp 构造了原生数字资产，例如以太猫，人们可以使用以太币购买以太猫。

原生数字资产、资产数字化的资产都可以通过以太币获得时，那么就意味着以太币改变了人类的生产关系，这当中并没有涉及任何法币兑换。

所以说，价值型的 Token，一定会触及改变了原有的生产关系。就如一个人刚接触股权概念的时候，很难解释清楚股权对应什么，Token 也是类似的处境，Token 具有可编程属性，它可以带来多种属性合一。

使用权，表示 Token 可交付产品或服务；

可交易，流动性是数字资产的基本需求；

可升值，这是由第二条带来的附加属性，也就是升值。

Token 技术栈比较

Token 的实现已经有 ERC20 为主的以太坊生态、比特股 SmartCoin 生态、NEO 的 NEP-5 生态、量子链的 QRC20 生态，还有元界的 MST 生态。

从技术上来看，Token 一定要满足高并发，快速清结算的需求，目前区块链的性能是一个问题，不少项目都在研究。

从技术发展来看，以太坊等智能合约型区块链一定会发展出类似 "Import ERC20”类似的合约机制来满足市场的需求，而由于比特股 SmartCoin 和元界的内置智能合约型的技术框架取决于市场对技术配套设施的敏感程度，安全程度的提升也带来应用的局限性。

可以看出，智能合约是 Token 的必备手段，可编程也必须降级为简单的导入合约模块的形式。

第27讲 | 弄懂数字货币交易平台（一）﻿

在前面的文章中，我向你介绍了数字货币交易平台如何操作。

可以这么说，如果没有数字货币交易所，就没有今天繁荣的数字货币市场，区块链技术也不会这样被广为人知。

交易的两种模式

先来说说交易模式，交易模式分为两种：场内交易和场外交易。

场内交易，又称成交单优先模式，指的是有交易场所将买卖双方聚集在一起，进行竞价交易的交易方式。这种交易方式中，交易场所负责用户的资产托管、交易撮合、资产结算、履约担保等功能。

场外交易，又称报价单优先模式，指的是买卖方不通过第三方而直接成为交易对手的交易方式。

本文介绍的交易所主要是第一种交易模式，即场内交易模式。

传统交易所的运作流程

区块链领域的交易所与传统金融的结构十分相似，但也存在了一些区别，为了讲清楚这种区别，我先简述一下证券交易的结构。

传统一般有四种角色，分别是投资者，在国内大部分是散户，其次是证券公司，接着是交易场所，这里的交易场所仅指场内交易场所，最后是证监会。它们的关系如下图。

通常投资者在证券公司开户，然后投资者委托证券公司下单，证券公司接受投资者下单并收取一定的佣金，然后买卖单由证券公司在交易场所进行交易，这个过程叫做委托，投资者是委托者，证券公司是受托者。

换句话说，普通投资者是无法直接接触交易所的，这是因为交易所采取会员制，只有成为交易所的会员且有交易席位，才可以接收其他投资者的委托，所以这就限定了机构投资者，也就是证券公司了。

而这里交易所是非盈利性的事业法人，它接受国家证券主管机关证券委员会及证监会的领导、管理和监督。证券交易所本身并不参与证券交易，不能决定证券价格。

所以对于投资者来说，只和证券公司有直接联系，这里的流程可以简述为：

投资者到证券公司开户，然后下单给证券公司；

证券公司再将这些订单传递到交易所，订单在交易所完成撮合成交；

接着交易所将订单和成交数据传到证券登记结算公司，结算公司据此进行资金和证券账户的结算；

结算结果再回传给证券公司，证券公司通过自己的平台显示给投资者，例如成交信息，账户余额等等。

数字资产交易平台

数字货币交易平台也叫做数字资产交易平台，主要为人们提供交易数字货币或数字资产撮合交易服务。

这种交易市场是一种典型的买单、卖单交易市场，所以这些平台以场内交易为主，通过提供买单卖单的撮合服务然后赚取手续费，这个过程中也发展出了层次丰富的金融工具，例如杠杆交易。

人们提供了买、卖交易数字资产的过程，这个过程是一种数字货币交换到另外一种数字货币的过程。

这种交易市场通常是数字货币对数字货币的，当然这显然不够，所以这就催生了法币对数字货币的交易，这也是中心化交易平台的由来，目前流行的法币与数字货币的交易有美元、欧元、日元、澳元等。

目前市场上，中心化的交易平台占据了绝大部分。从功能上来看，中心化交易所一般都会提供以下业务模块：充提数字货币、资产托管、交易撮合、资产结算、杠杆交易、KYC 等。

上面我们介绍过传统交易平台的结构，借此我们也可以归纳比较出数字货币平台的与传统交易平台的优劣势。

传统交易所依赖券商，属于金字塔型结构，用户聚集在券商处，资金托管在银行，证券登记结算在第三方机构，本质上交易场所只提供了撮合、监管辅助、信息辅助等功能。

而由于数字货币的去中心化特性，数字货币交易平台属于扁平型结构，资产管理本身就内置在交易所内部。

所以任何一个交易平台都不需要第三方机构登记结算数字货币，这带来了业务架构上的易部署特性，用户流量和资金流量最终全部汇聚在数字货币交易所。

如果我们从这些业务模块出发，结合技术架构来看，中心化的数字货币交易平台更接近互联网应用的技术架构，它本质上是金融交易系统与互联网网络服务相结合，具有以下优势特性：

能够支持海量高并发实时撮合交易 ;

用户终端全平台支持，从桌面到移动端不一而足 ;

数字资产的超高流动性；

平台可以获取超高的利润；

价值发现功能。

虽然利润和流量都超大，但中心化交易平台也面临了一些天花板，例如动不动就被爆出被黑事件，这也着实让用户提心吊胆，所以我归纳了一些如下缺点：

内幕操作，交易所相当于是一个黑盒，内部操作不透明带来了巨大风险；

监管缺失，信息披露不完善，项目方跑路风险；

持仓风险，用户的资金完全托管在交易所；

趋利优先，区块链本身的发展是在盈利之后才会被考虑的；

交易所破产倒闭风险。

总的来说，数字货币交易所目前是区块链与现实的接触面最大的接触点，也是数字金融中的最重要一环。

数字货币交易平台的三种类型

其实在数字货币交易领域，交易平台是不必局限在中心化这一种实现方案的，这由于交易所也是由很多业务模块组成的，它是把某些模块进行去中心化，而不是整体去中心化，所以实际上它可以有三种实现类型。

模式一：中心化模式，资金管理系统与区块链账本各自记账，包含充币提币的过程，需要人工干涉。模式一的代表有很多，现在市场上主流的交易所主要的有 Binance、Bittrex、Bitfinex、Gate.io、Huobi.pro、Okex、Kraken 等，它们为数字货币和数字资产的发展提供了全球化、7\*24 小时不间断的流动性，也就是上文我们介绍的数字货币交易平台。

模式二：半中心化模式，交易撮合与行情模块是中心化的，而资产是在区块链上直接结算的。代表有 0x Project、Keyber Network 这些前沿的项目。

模式三：完全去中心化模式 ，比模式二更进一步，所有模块都是去中心化的，包括交易撮合和行情部分。代表有比特股和 EtherDelta。

模式二和模式三我们统称为去中心化交易所，目前是区块链数字资产领域研究的一个前沿方向，多数方案都还不成熟，例如用户产品体验差、稳定性不足、数字货币流动性不足等等，当然更多还处于研发阶段。

虽然去中心化交易所是一个很好的方向，但可能会脱离掉用户的真实需求，正如我前面谈论“去中心化”这个概念所说，终端用户也许根本不关心平台是否是去中心化的。在这里，用户的主要诉求体现在下面几点：

用户终端产品的界面操作流畅、响应速度快、用户体验好；

资产结算速度快，如果存在充币提币的话取决于审核过程；

订单簿挂单的深度要好，可以快速成交订单；

托管的资产安全性高，如果有的话。

以上四点，目前模式一的交易平台的体验完胜模式二和模式三，这也是中心化交易平台流行的主要原因。

第28讲 | 弄懂数字货币交易平台（二）﻿

在上一篇文章中，我们介绍了数字货币交易平台的概念，那么今天我们就来重点聊聊数字货币交易平台的技术。如果你有过设计或实现传统金融交易系统的经验，那么你阅读本篇就会更加容易。

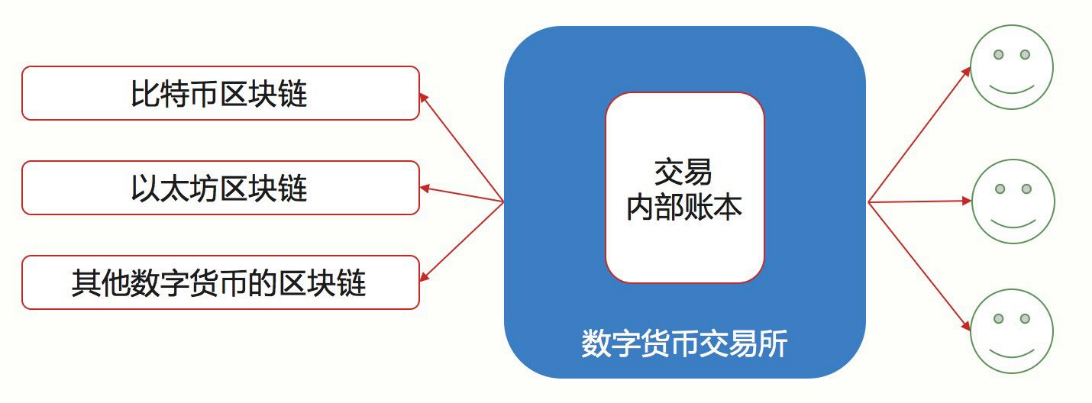
由于中心化交易所是主流应用，所以今天我主要介绍的是中心化模式下的数字货币交易平台。

两套账本

数字货币交易平台的技术基本沿用了金融交易技术中的系统架构，只是把原来针对法币和证券（或平台代币）的部分，也就是我们通常称作资金管理系统的部分，完全替换为针对数字货币的数字货币管理系统，换句话说，就是换了一套内部账本。

然而我们知道，区块链本身也是用来记账的，也算作一种金融账本，所以一套内部账本，一套区块链本身的账本，这里就出现了两套账本，如何管理这两套账本，就是资金管理系统的首要任务。

如下图所示。由于中文语境下的交易有多重含义，本篇会用英文单词标注，以示区别。

﻿﻿

(图示 数字货币交易所)

解释一下这张图，图的左边表示了多个区块链账本，右边的数字货币交易所有自己的内部账本，这两套账本是独立的。

交易所内部的账本记录的是交易 Trade，这个交易是由用户挂单，接着被撮合引擎撮合成交而产生的，而区块链账本上的交易 Transaction，是当且仅当用户发起充币提币请求并被执行时，才会产生的。

这两种交易都用了中文“交易”来表示，但是它们所属的语境不同，前者的交易表示的是金融交易语境下的资产交换，也就是 Deal；后者表示的是区块链上的技术概念，表示资产转移的一次记账过程，上述特意用英文以表区别，希望你能够区分。

数字货币交易所包含哪些系统模块

一个数字货币交易所的后端其实至少有四部分构成：Web 业务逻辑系统、交易撮合系统、运营后台管理系统、资金管理系统。资金管理系统其实就是刚才说到的内部账本。

﻿﻿

Web 业务逻辑系统：这个模块通常包含了用户账户模块、登录网关、账户安全管理、KYC 认证、行情推送等等，这个模块更偏向用户，也与通常的电商账户系统十分类似。

交易撮合系统：这个模块是一个交易所的核心模块，为所有的用户提供订单撮合。

运营后台管理：这个模块是一个交易所运营人员使用的系统，交易所内部人员才能访问。

资金管理系统：这里的资金管理其实包含了三部分，第一部分是法币的支付网关，可能需要对接银行或第三方支付机构；第二部分就是数字货币钱包管理，它提供了大部分主流数字货币的支付功能；第三部分是用户持仓信息，所谓持仓就是用户持有多少数字货币，这个是记录在数据库中的，不需要与区块链保持一致，但是要求交易所的总账是平的。

各自模块的特征

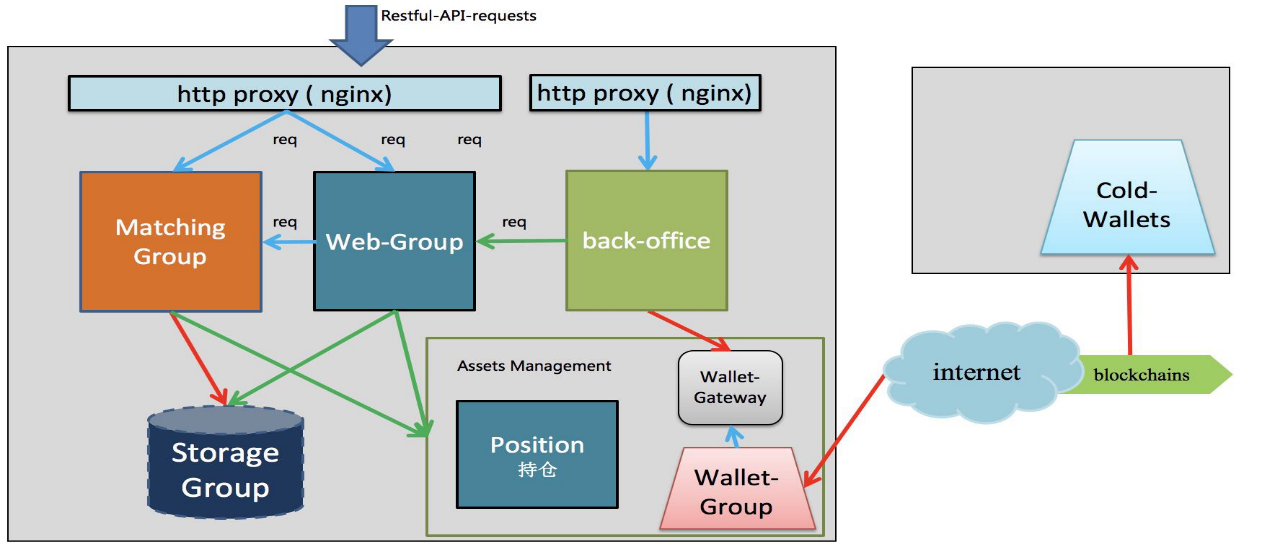
Web 业务系统与我们常见的电商系统无异，主要是用户账户以及简单的业务逻辑，重点是可扩展性，业务要求比较弹性。

交易撮合系统本质上是一个高并发的计算系统，特点是系统性能高和稳定性好，其中订单队列可以是编程语言中的数据容器，也可以是内存数据库。

运营后台系统在整个交易所生命周期的早期并不凸显重要性，但是运营后台系统恰恰是交易所中后期发展的核心系统，重点在数据准确，要求网络安全性高和可扩展性好。

资金管理系统包含用户持仓状态，以及数字货币钱包服务，它是一个交易平台中安全性要求最高的系统，资金管理系统往往要搭配一个内存数据库，其中数字货币钱包服务也可以拆出来做成独立子系统，甚至可以改造成整个公司的内部区块浏览器，因为钱包服务需要设计成多个钱包实例，并统一所有的币种钱包接口。

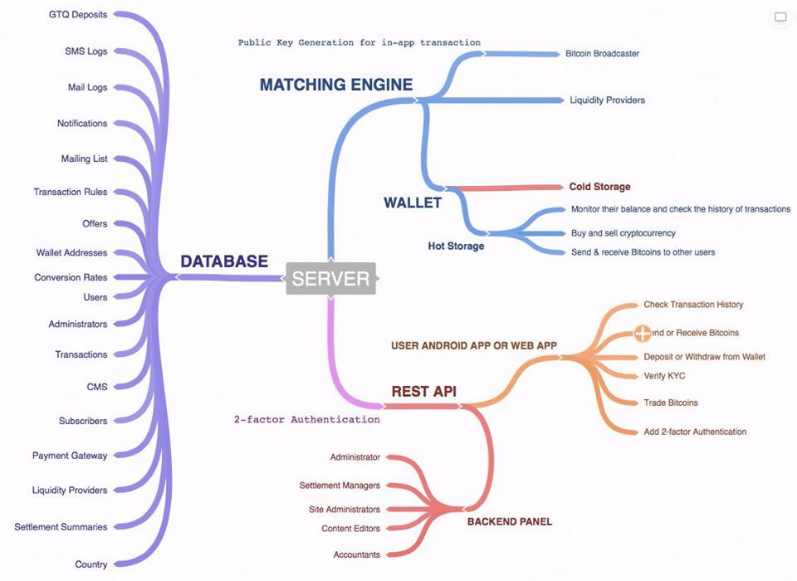
一个交易所可能的结构如下图。

﻿﻿

上图中，MatchingGroup 相当于是交易撮合系统；Web-Group 相当于 Web 业务逻辑系统；Back-office 相当于后台管理系统；AssetsManagement 相当于是资金管理系统。

涉及的技术栈

如果我们再将刚才提到的各个模块细分，会看到以下的功能。

﻿﻿

（图片来自网络）

按照上图的细分功能，我们可以得到哪些技术支持一目了然。

首先是 Server 需要数据库作为支撑，其次是 Restful API 作为基础通讯协议，并且集成钱包相关的技术，撮合引擎为 Sever 提供撮合服务。

在这里面，例如需要 SMS 系统，所以可以使用云服务中的 SMS 组件，这些都可以是成熟的通用组件技术。我们可以发现中心化交易使用的技术与互联网技术并无不同。

把这些通用组件塞到下图中各个层次和大模块当中，所以最终一个交易所的详细架构可能是下图的样子。﻿﻿

（图片来自网络，缺失了资金管理部分）

我们来解释一下这张图。

首先是存储，持久存储通常可以选择 MySQL，撮合相关的模块由于要避免接触磁盘 IO，所以需要为撮合模块提供 Redis 类型的内存存储，二者需要保证最终一致性。

撮合和行情部分，几乎与传统技术无异，行情推送可以类比到其他推送系统，只是频率更高，一般首选 Websocket 技术。

这与传统互联网应用的最大区别里主要是数字货币钱包管理，这块完全是新的内容，对安全性、易用性提出了相当高难度的挑战，这里也是交易所资金托管的根本，所以如何管理好大量数字货币，往往要结合运营、内部管理制度、冷热钱包技术一起才能做好交易所的资金管理。

那么用户是如何挂单的，又是如何产生区块链交易的呢？我们来看一看。

## 交易过程

那么说，用户 A 拿 0.01BTC 换取了 B 的 10 个 ETP 的过程究竟是什么样的呢，我来举一个例子。

用户 A 挂 10ETP 买单，出价 0.01BTC 经过 Web 业务系统进入撮合系统订单簿 ETP-BTC 买单队列，等待撮合成交，同时资金管理系统冻结 0.01BTC。

用户 B 挂 10ETP 卖单，出价 0.01BTC 经过 Web 业务系统进入撮合系统订单簿 ETP-BTC 卖单队列，与步骤 1 中 A 的订单撮合匹配成功，生成 Trade，同时资金管理系统结算对应资产，B 的资产变化为增加 0.01BTC 并减少 10ETP， A 增加 10ETP 并减少 0.01BTC。

成交 Trade 以及资产变化通过资金管理系统写 RDB 数据库，形成成交记录，同时更新行情，数据库记录可供用户和运营后台管理系统查询。 要注意的是这一步并不是登记到区块链上。

用户 B 经过 Web 业务系统发起提币请求，请求提取 10ETP 进入自己的数字货币钱包，这个请求进入资金管理系统，交易所运营人员可通过运营后台观察到这笔请求，运营人员审核用户 B 的信息，比如实名认证是否正常等。

提币请求进入运营系统后，如果通过审核，则资金管理系统会冻结用户 B 的 10ETP，同时将提币请求发起给数字货币钱包服务系统，也就是 WalletGroup，子系统发起区块链上的交易 x（Transaction）, 等待交易被打包，并根据更新提币审核状态，供用户查看。

数字货币钱包服务根据区块信息查询交易 x 是否被打包，如果已经打包，则资金管理系统将完全把用户 B 被冻结的 10ETP 直接抹成 0，更新提币状态最终为完成，提供区块交易 ID 以供用户和运营后台系统进行查询。

在步骤 3 中，我们可以看到用户所持有的资产，相当于是交易所对用户的负债，但这也只是数据库中的一个数字，并不是真正的链上资产。

在步骤 6 中，我们看到区块链上的“交易”与步骤 3 中的“交易”完全不是一个概念，同时用户的资产是否安全，完全取决于交易平台的技术是否安全，对交易所是否信任。

再来看看充值阶段。

简单来说，充值是与提币相反的过程，不同的是，充值不需要审核，一般数字货币交易所的原则都是“宽进严出”，在充值过程中，交易平台通常不直接使用数字货币钱包检测用户是否充值到账，而是使用“扫块”(block\_scan) 这一方法检测用户的充值。

总结

今天我简单介绍了数字货币交易所的业务逻辑，相信你已经对数字货币交易所有了一个初步的了解，数字货币交易所是区块链行业最重要的业务，全世界每个月都有新的数字货币交易所诞生。