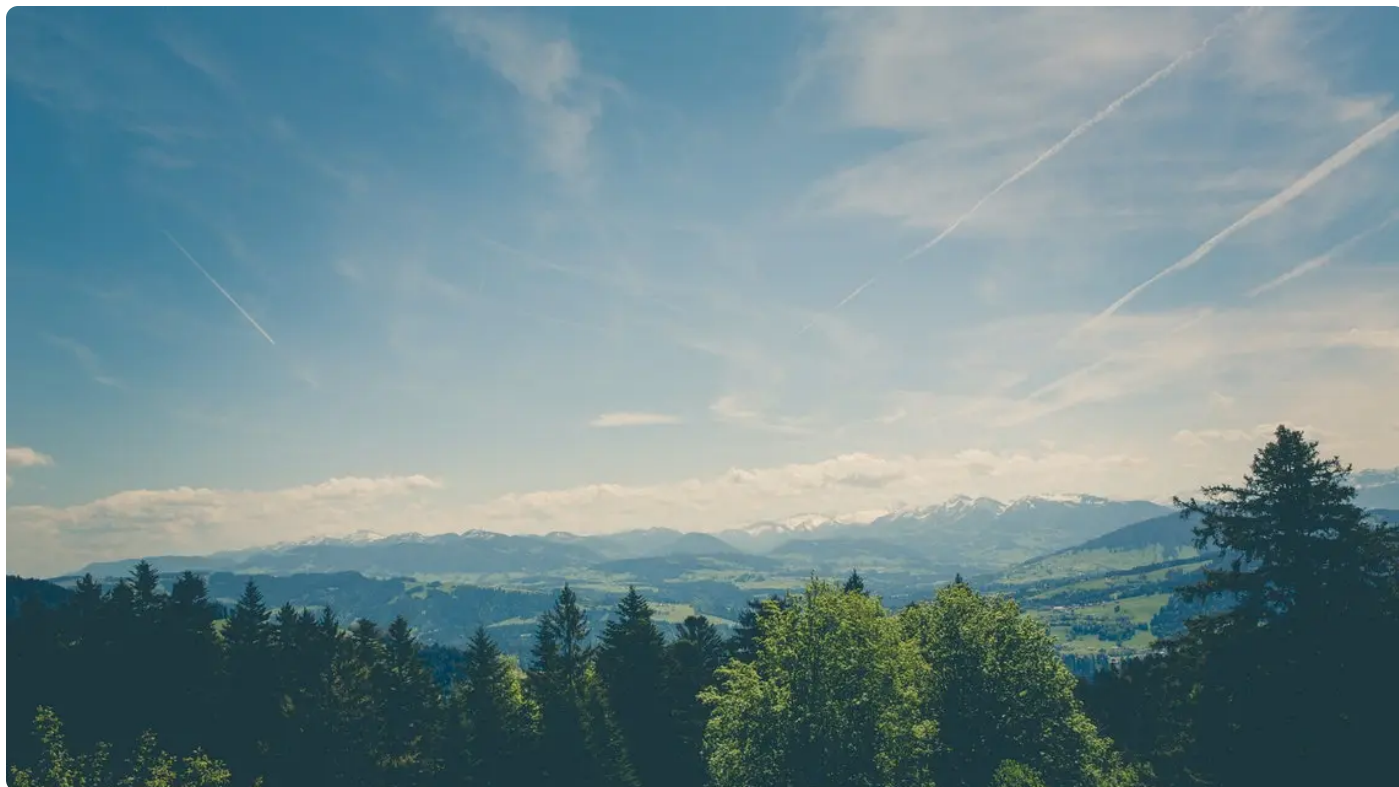


08 | 数字财产确权：用区块链建立数字所有权管理系统

2022-05-13 方军

《说透元宇宙》

课程介绍 >



讲述：山荣

时长 16:53 大小 15.47M



你好，我是方军。

我们前面说过，元宇宙 = 立体互联网 + 价值互联网。之前我们用一整个模块讨论了立体互联网，从这一讲开始，我们进入价值互联网的模块。

“价值互联网”是和“信息互联网”相对应的。信息互联网中流转的是信息，价值互联网中流转的是价值。我们现在的互联网是以信息流动为目标来设计的。在全面迎来元宇宙时代时，我们希望，在数字空间，每个人都能像在实体空间一样拥有财产所有权，而财产所有权对应的就是价值。因此，我们需要一系列与价值有关的技术基础设施，它就是基于区块链技术的价值互联网。

价值互联网：发生在协议层的变革

在 [🔗 第 4 讲](#)，我们提到过价值互联网的三个基本要素：账户、余额与转账。我们常用的支付宝就是一个典型的处在应用层的、价值流动的网络。这个网络中流转的价值是支付宝余额，它的主要功能是让我们在购物时向商家付款。

但我们期望未来的价值互联网能流转更多形式的价值。比方说个人数据、知识产权、艺术品、公司股权与期权等等。这个设想并非不能实现，我们只要将现在主要处于应用层的“中间人”去掉，在技术上实现“价值流动的去中心化”就可以了。

这样，价值互联网在基本结构上就和信息互联网一样了。以前，网络中的价值流动主要通过中间人来完成，而信息的流动却不需要中间人，任何人都可以架设一台服务器然后用网站发布信息。但是区块链技术出现之后，价值流动的去中心化成为了可能。

有人也许会说，支付宝、Paypal 等不是很方便吗，为什么要去掉它们呢？我可以给出一系列的理由。

比如，我们现在可以相信支付宝，但其他的什么宝我们可不一定能信。以同样模式运作的各种中心化服务可能存在一些安全隐患。

比如，虽然支付宝很好用，但如果你想把支付宝里的钱直接转到微信钱包，对不起，做不到，因为这是各有中心的两个封闭系统，而不是开放的系统。

再比如，我们作为工程师想要在这样的系统上开发点新应用，对不起，非常难，因为出于安全和业务的考虑，几乎每个中心化的系统都倾向于封闭，只提供极少且具有高度限制性的接口。

解决这些问题的路径，就是改造现有互联网的底层，在底层实现和价值有关的功能。也就是说，不是在支付宝所在的应用层实现账户、余额和转账功能，而是在等同于 HTTP 协议的这个层次实现这些功能，从而提高安全性、实现开放互联、创造更开放的编程接口。

其实，从 1990 年代初期互联网商业化开始，就一直有人在进行这样的技术探索，但直到 2008 年底，化名中本聪的密码学家才找到一个突破口。我们前面提过中本聪这个人，他在自己的论文中给出了用新思路来建立一个去中心的电子现金系统的技术方案，从而最终推动了区块链等一系列新技术的诞生。他的技术方案有三个要点。

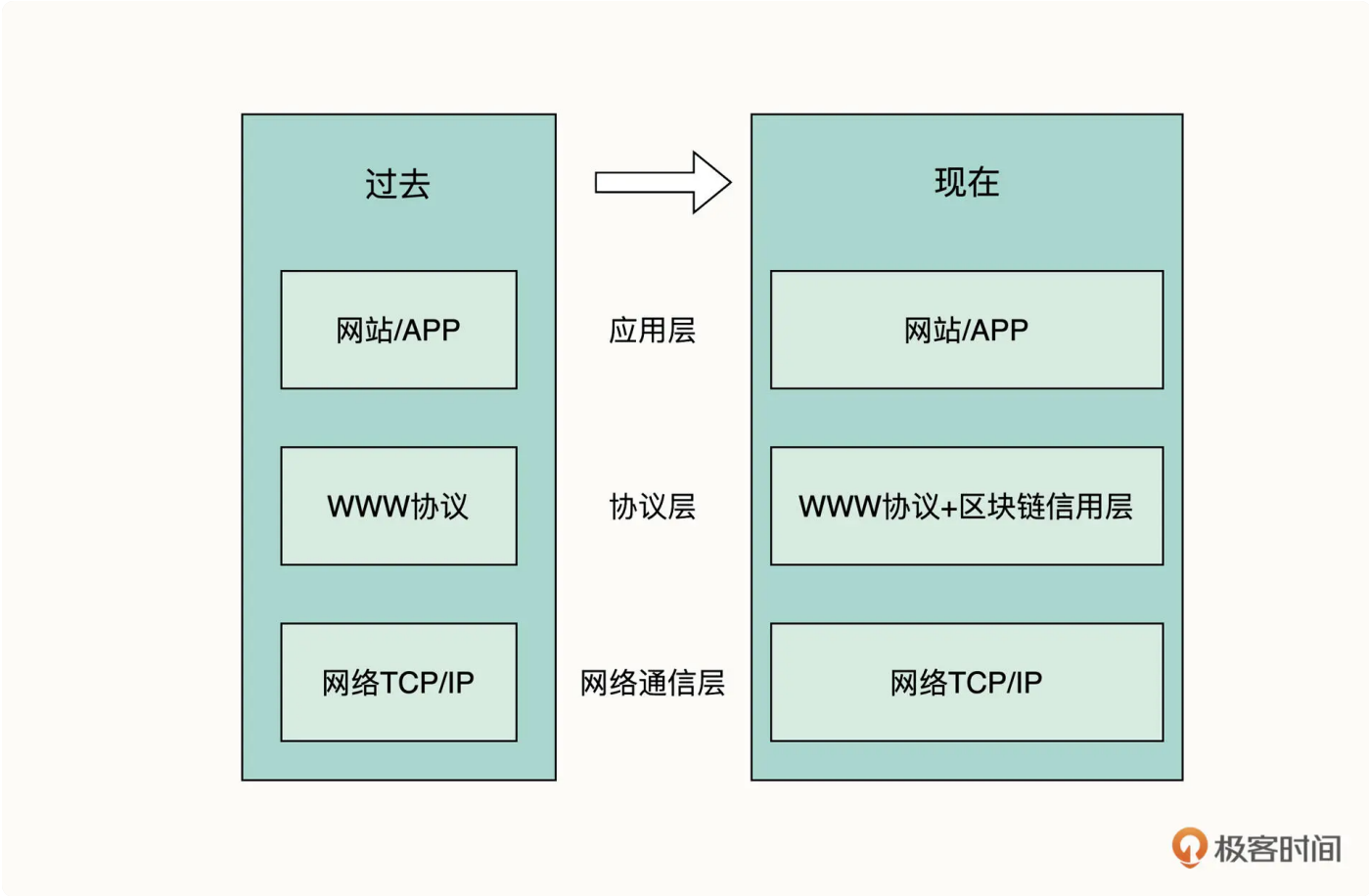
第一，它是“去中心化网络 + 分布式账本”的结构。

第二，它用“区块 + 链”来存储账本。

第三，它用工作量证明共识机制与最长链原则来达成共识。

现在，技术人员在他的最初技术方案基础上开发出了各有特色的区块链系统。这里面有大型公司和传统开源社区的努力。比如，IBM 公司推出了超级账本联盟链系统，并将这个系统捐赠、交由 Linux 基金会管理。也有新兴公有链社区的努力：其中重要的人物有提出和开发了以太坊系统的维塔利克·布特林、加文·伍德等人。

现在，价值互联网的三要素现在能够在协议层实现了。如果将互联网简单地分成三个层次：在过去，最底下是网络通信层次，中间层是 WWW 协议，上层是我们能看到的网页与 APP。现在发生的变化是，在中间层，除了处理信息的 WWW 协议，旁边还多了一个处理价值的区块链协议，区块链协议也被威廉·穆贾雅等学者称为“区块链信用层”。



对于技术创业者来说，这么大的结构性变化必然意味着创造一系列全新技术产品的机会。比如，有人开发各种公有链与联盟链，有人开发价值相关的索引服务，有人开发价值相关的数据服务，还出现了各种价值应用平台。

这些新公司融资与估值都相当惊人，这说明了风险投资人对这些技术产品前景的看好。仅以 2022 年初获得 VC 融资的一些公司为例：为程序员服务的 Alchemy 技术平台估值 102 亿美元，技术服务公司 Consensys 估值 70 亿美元，NFT 交易市场 OpenSea 估值 133 亿美元。投资它们的也是最主流的机构，比如软银愿景基金、淡马锡、A16Z 风投、红杉资本等等。

那么，区块链技术是如何实现账户、余额、转账这三要素的呢？

区块链是如何实现的？

要讲清楚这个问题，我们可以逐一讨论分布式网络、共识机制、公钥密码学、虚拟机、智能合约等一项项技术。但这里，我想换个方式带你一步步理解区块链技术的美妙之处。我们假设说，你接到一项任务，要你开发一个技术系统，这个任务是这样的：

你要实现一个包括“账户、余额、转账”三要素的财产所有权管理系统，也就是一个价值流动网络。每个人都有自己的账户、自己的余额，而且每个人都能向其他人转账。

现在各种 App 都可能会需要实现现金钱包或会员积分系统，这样的系统不难实现。你可以用一个数据表来存储用户账户，用另一个表来存储用户余额。当用户发起转账时，如果系统能确认转账是由他发起的，系统就会自动调整余额表格中的数据，把余额从一个人转给另一个人。

这些程序、数据库都是运行在一个中心化的服务器上的。假设是你管理这个服务器，那么其他人必须绝对相信你：他们确信，你不会偷偷修改数据库，把他们的财产记到别人的名下。

接下来，我们把任务的要求提高一点点。

用户不相信你，也不相信任何人。他们只相信自己，或者说只相信可以自己去验算的记录。

用技术的语言说就是：我们要实现一个“去中心化”或者说“无中心”的网络，让每个人都运行自己的服务器，让大家各自保存自己的数据库。也就是，每个人都自己记账。

这个任务初看也不难，大家都运行自己的服务器和数据库，然后时时刻刻对账呗。但细想，你会发现好像有很多可以优化的地方。

第一，除了直接把原来的服务器、数据库复制 N 份，让大家各自运行之外，有没有更好的数据结构呢？

第二，这些分布在各处的服务器如何就数据的变更达成一致呢？如果这些服务器分布式在全球互联网上，各个节点存在通信延迟，数据的一致性和变更的一致性就是个大问题。

第三，由于这个网络是公开的、允许任何人加入成为计算节点。那么，一旦网络中坏人加入的节点超过一定比例，我们就会遇到所谓的“拜占庭将军问题”，直白地说就是这个网络无法形成可信的结果。

后面两个问题是由共识机制算法来解决的，我们会放在后面说。这里，我想重点讨论第一个问题，也就是数据结构的问题：**为了实现一个有“账户、余额、转账”功能的系统，我们能不能设计出更适用于它的数据结构？**答案肯定是可以，专门为这三个功能设计的数据结构大家都已经听过无数遍了，那就是区块链中“区块 + 链”式的数据结构。

我们还是用一个小例子理解一下它的原理。假设我们有十个人，我们要实现一个供我们十个人用的财产所有权管理系统。直接用关系型数据库来实现这样一个财产所有权的账本，当然也可以做到，但是我们希望找到更好的方式。我们希望它能满足下面三个需求。

第一，在最后一刻，我们这十个人分别有多少财产。

第二，我们要有历史记录，能知道过去每一天我们这十个人分别有多少财产。

第三，我们希望这个账本告诉我们的每一个时刻的所有权状态都是确信无疑的，都是大家共同认可的。

“区块 + 链”式数据结构是专为如上需求设计的，我们来举例说明。假设我们用一个系统来管理 10 个人的账户余额。

建这个系统的第一天，我们要先确认每个人有多少余额，这是第一个状态。我们假设甲有 1000 块，乙有 500 块，丙也有 500 块。

接着，丙制作了一个东西，卖给了系统之外的其他人获得了 500 块。所有人都一致同意将这 500 块记作丙的收入。我们到了第二个状态，这时，甲还是有 1000 块，乙有 500 块，丙有了 1000 块。

又过了一段时间，一个人向系统内部的另一个人转账 1000 块，我们到了第三个状态。之后还会有第四个状态、第五个状态……第 N 个状态。

这些转账都是系统中的人共同同意的。也就是说，系统会记录每个人每一刻的财产所有权状态。转账会变更状态，转账必须经过所有人的一致同意。

区块链的整个数据结构就是用这样的方式来组织的。一个状态就是一个数据区块，新的数据区块跟在上一个数据区块之后。每个新区块里都有一个指向上一个区块的哈希指针。新区块必须由所有人按所谓共识机制同意。这就形成了一个包含所有状态的链式结构，这也是“区块链”（区块 + 链，Block+Chain）这个名字的由来。

这个设计的一大好处是防篡改，如果上一个区块的数据被人偷偷改写了，它的哈希值就会发生变化，与后一个区块中保存的哈希值就对不上了。

这个“区块 + 链”的数据结构也被称为账本（Ledger），这个名字是相当准确的，因为它的确跟我们生活中的账本很相似。一个区块就相当于现金流水账的一页，账本上记录的是每个人的余额。

总的来说，区块链网络相当于让每个人都运行了一个“区块链客户端”，这些客户端以 P2P 的方式和其他的客户端组成一个没有中心的、对等的网络，它要做两件事：第一，保存这个“区块 + 链”形式的账本；第二，在转账交易发生时，根据共识机制共同确认变更，同时保存账本的新状态。

账户与共识机制

讲到这里估计你也发现了，我们一直说价值系统有三个要素：账户、余额、转账。但上面我们主要在讲的都是余额和转账。但是，账户对于系统也相当重要，那么，区块链的账户是怎么实现的呢？我们在转账时，系统需要确认交易是由该账户的持有者发起的，在一个完全公开、开放的网络中，如何防止别人假冒你的账户与签名呢？

在技术上，区块链选择的是非对称加密密码学方法，每个人用“私钥和公钥”的组合来持有财产所有权。你拥有私钥就拥有了财产的掌控权，而密码学在技术上确保了没有你的私钥就没法伪造你的签名。

更具体地说，以主流区块链为例，如果想要创建一个账户，我们可以随机选择一个 2 的 256 次方的数字作为私钥。这是一个极大的数字，它接近于可见宇宙中的原子数量。因此，只要生成过程是绝对随机的，你生成的私钥就不会跟其他人重合。

有了私钥之后，我们可以用密码学中的椭圆曲线乘法计算出公钥，再按照规则转为适用于相应区块链的地址格式。我们可以由私钥推导出公钥，由公钥推导出地址。但要注意的是，反过来倒推都是不行的。地址和公钥略有不同，接下来，我们把用户的账户称为“私钥 + 地址”的组合。

一旦你有了私钥和地址，我们就可以用它们形成的身份机制来确保没有人能够冒充你、盗用你的财产。

我们假设你同意借给我一万块钱，那么只有你用私钥签名表示同意，这笔转账才能发生。具体来说，转账过程是这样的：这笔交易只有用你的私钥签名才会开始启动。它会在区块链网络中广播。稍后，这个交易会被按共识机制算法纳入最新的数据区块。到这时，交易就完成了，这笔钱就只有我的私钥才能动用了。也即，财产已经从你的地址转到我的地址了。

可以看出，转账功能和“区块 + 链”的结构都是耦合在这个过程之中的。账户、余额、转账三个基本要素是由一组紧密耦合的设计完成的，环环相扣。

因此，基于区块链技术，我们可以构建一个完美地适用于数字世界的管理价值的系统，它的特点有：分布式账本 + 去中心化网络、“数据区块 + 链式结构”、交易驱动的状态机、基于非对称密码学的用户身份机制。

讲到这里你可能还有一个疑问，刚才我们一直在说，账本的变更是分布式网络中的众多节点根据共识机制算法共同决定的。那什么是分布式共识机制算法呢？

简单地说，它指的是在一个分布式网络中，众多节点就数据的变更达成一致的机制。

在一个公开的、任何好人、坏人作为节点都可以加入的对等网络，众多节点怎么就数据的变更达成共识、并更新到新的数据状态呢？再具体一点说，区块链每次变更状态时，都会在链条后新增一个区块，那么这个新的区块是由谁来生成的？怎么确保这个区块是对的？

一般说来，区块链解决这个问题有三种选择。

第一种选择最简单粗暴，我们可以规定，只有经过某个核心团体认可的“好人”才能加入，这就在一开始就把坏人排除在外了。后续状态的变更也是这样，统一由这个核心团队来确定。沿着这个思路发展下去就出现了现在的各类联盟链，它的特征是有准入机制，把坏人在一开始就排除在外。

但如果还是想实现完全开放接入的目标，也就是建立无须许可的（Permissionless）分布式网络呢？根据分布式计算中的“FLP 不可能结果”，这样的分布式网络只靠技术是无解的。

区块链技术系统的做法是，引入了经济奖励与惩罚，它的共识机制算法是由技术 + 经济来完成的。具体做法又可以分成两种，也就是区块链解决这个问题的第二、第三种选择：**POW**（工作量证明）共识算法和 **POS**（权益证明）共识算法。

两种算法的思路是一致的：用户必须有一定的经济投入，以此获得网络参与权，如果成功记账，将可以获得经济奖励；如果失误或作恶，其投入会被罚没。经济上的惩罚与奖励，和技术结合在一起，确保了分布式网络中的众多节点能够就数据变更达成共识，确保分布式网络的安全性。

总结

这节课就讲到这里，我们小结一下。

这节课，我们首先讨论了价值互联网的三要素。“账户、余额、转账”这三个功能原本是在应用层实现的，现在有了区块链技术，我们可以把它移到更底层，用更开放的方式实现。这彻底改变了现有互联网的架构，推动了价值互联网的出现。

接下来，我们讨论了“区块 + 链”的数据结构、基于非对称密码学的“私钥 + 地址”账户体系，以及分布式网络就数据变更达成一致的共识机制。

总之，区块链技术的核心设计是简洁的、优美的，正是这种简洁、优美让它有了巨大的可扩展性。现在，区块链已经可以支撑起单个资金量近万亿的庞大资产系统了。它还可以拓展到艺术、数据、金融等多种应用类别。它让价值互联网的实现有了技术基础，也让元宇宙在价值方面有了技术基础。

课后题


在这一讲的最后，给你留一道思考题。

这道题有点技术性，你已经知道了区块链采用的是“区块 + 链”的数据结构，那如果你想偷偷篡改一个区块中的数据，你需要怎么做呢？请你尝试做一个思想实验。当然，最终你会发现要篡改成功根本做不到，在这个过程中，你能体会到这一设计的精妙之处。

欢迎在留言区写下你的尝试与思考。

分享给需要的人，Ta订阅超级会员，你最高得 50 元

Ta单独购买本课程，你将得 20 元

 生成海报并分享

 赞 1  提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 07 | 操控数字世界：用手与身体取代键盘

下一篇 09 | 数字交易协议：在数字空间“复制”社会经济活动

精选留言 (2)

 写留言



吃饭第一名

2022-05-17

问题：如果你想偷偷篡改一个区块中的数据，你需要怎么做呢？

思路（针对POW）：找到对应的区块的父区块，然后在此块的基础上进行分叉，并尽快出块（挖矿），然后在出块的基础上再出块，最终形成最长链。

举例：如果要篡改的是当前网络的最新的区块，那么你需要对此块的父区块进行分叉攻击，这个攻击需要的代价就是需要当前网络算力的51%+ 才有可能。如果是已经运行稳定的区块链网络，比如比特币，那么你的投入是个天文数字。如果是更早的区块，难度就会更大。



0x123.eth智能合约开...

2022-05-16

元宇宙 = 立体互联网 + 价值互联网。

