

# 区块链经济学：制度密码经济学入门指南

---

区块链是一种数字化的、去中心化的、分布式的**账本**。

人们对区块链技术的解释大多始于比特币，以及货币的发展历史。然而，货币仅仅是区块链的首个使用案例，且未必是最重要的应用。

这或许看着有些奇怪，账本，这种主要和记账相关的枯燥且实用的记录证明，竟然会被大家描述为一项具有革命性的技术。然而，区块链之所以重要，正是因为账本很重要。

## 账本溯源

---

账本无处不在，其功能并不局限于记录会计交易。一个账本是由按照规则排列的数据结构所组成的。每当我们需要对一些**事实**达成某种**共识**时，我们就会使用账本。账本里记录的事实支撑着我们现代经济学的基石。

**账本确认所有权。**财产契据登记好比一张地图，它显示出谁拥有什么，以及他们的土地是否受到过警告或者破坏。Hernando de Soto 就曾经证明过，当穷人的自有财产没有在账本中得到确认时，会遭受到何等的痛苦。公司是一个账本，就像是由所有权关系、雇佣关系和生产关系构成的为服务某单一目的的网络。社团也是一个账本，制定着谁将受益或者无法受益。

**账本确认身份。**商业主体只有在政府账本上登记身份后，其在纳税法下的存续状态才得以被记录。出生证明、死亡证明和结婚证明都是用来记录个体存在着的关键时刻，而当这些个体和世界产生互动的时候，这些信息可以用来确认个体身份。

**账本确认状态。**公民身份是一个账本，记着哪些人作为国家公民应当享有权利和义务。选民名册是一个账本，允许登记在该名册上的选民进行投票（澳大利亚是普遍选举制）。雇佣是一个账本，让雇员可以按照合约索偿来获取工作报酬。

**账本确认权威。**账本可证明谁能够合法地在国会中占据席位、谁能接入相关的银行账户、谁能与儿童一起工作，以及谁能进入禁地。

**从根本上来看，账本描绘了经济和社会关系。**

人们对事实及其变化达成一致（即对账本内容达成共识，以及对账本的精确性充分信任）是市场资本主义的基石。

## 所有权，占有权和账本

---

让我们在这里对**所有权**和**占有权**的概念做一个区分。这很重要，但却容易被忽视。

以护照为例。每个国家都维护着其控制谁能出入境的权利，此外，每个国家都维护着一本账本，其中记录着哪些公民可以旅行。护照是一种实物，也可以称其为一种**代币**，用以查阅这个账本。

在数字时代到来之前，占有权指对那种权利的所有权。澳大利亚的护照账本由各州政府持有的索引卡组成。当边境的工作人员拿到递交的护照时，他们可以做出如下推测：这位旅行者被记录在一个远程账本上，并被获准旅行。当然，这种激进的边境管制很容易遭受诈骗风险。



—一张收藏在澳大利亚国家档案馆的比利时护照，A435 1944 / 4 / 2579—

占有权隐含着所有权，但是所有权不是占有权。当下，现代的护照可以使得当局直接确认所有权。其数字化的特征使航空公司和移民局可以通过访问国家护照数据中心来决定是否让这位旅客自由通行。

护照是一种相对直接的例子用来证明两者间的区别。然而，比特币已经向我们展示了：**货币也是一种记账**。

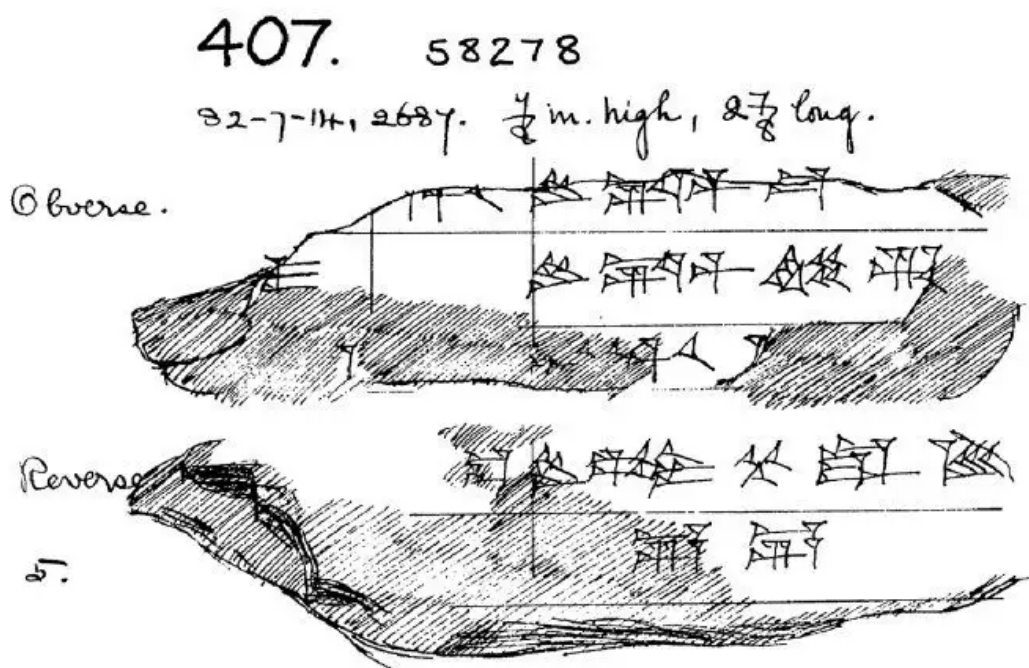
银行票据凭证的占有权象征着所有权。在十九世纪，银行票据的持有者，即“持票人”，有权动用这些票据在发行银行对应的价值。这些银行票据作为发行银行的直接负债记录在银行的账本上。占有权这种制度指出：所有权意味着银行票据易受偷窃和伪造的影响。

在我们这个法币流通的时代，一张五美元的钞票是无法退还给银行以换取黄金的。但其中的关系依旧存在——钞票的价值取决于社会对货币及作为其发行主体的政府的共识。但不幸的是，正如津巴布韦、南斯拉夫和德国魏玛共和国意识到的那样，银行票据并不是财富。一张钞票是对（人工合成的）记录在账本里的某种关系的访问，但如果那种关系瓦解了，那么这张钞票的价值也随之崩溃。

## 账本的演变

虽然账本非常重要，但这门技术几乎一直没有太大的变化.....直到现在。

账本出现在书面交流的初期。在古代近东地区，**账本和书写同时发展起来**以记录生产、交易和债务。通过在泥板上刻下楔形文字，来详细记录口粮、税收、工人等的数量，然后将其烧制保存。首个国际“社区”是以结构化的网络联盟形式组建的，其运作方式和分布式账本非常相像。



-一张由大英博物馆收藏的巴比伦尼亚楔形文字账本残片，58278-

账本的第一次重大变化出现在十四世纪，那时，人们发明了**复式记账法**。复式记账法需要在多个（分布式）账本里同时登记等额的借贷数据，以使各账本之间的信息守恒。

到了十九世纪，随着大型公司和大型官僚组织的兴起，账本技术有了下一个发展。这些**中心化账本**使得组织的规模和范围都急剧增加，但完全基于对中心化机构的信任之上。

到了二十世纪后期，模拟化账本向**数字化账本**转变。例如，在十九世纪七十年代，澳大利亚的护照账本就进行了数字化和中心化处理。数据库可以实现更加复杂的分配、计算、分析和跟踪。一个数据库是可计算且可搜索的。

但是，数据库依然是基于信任的。一个数字化账本的可靠性依赖于维护其账本的组织及该组织雇佣的员工。区块链解决的正是这个问题。区块链是一个分布式账本，它无需依赖可信任的中心机构去维护和验证账本。

## 区块链和资本主义经济制度

现代资本主义的经济结构逐步演变为用来服务这些账本。

2009年诺贝尔经济学奖获得者 Oliver Williamson 提出：人们在市场、公司或者政府之间的生产和交换行为，取决于这些机构间交易成本的差异。Williamson的交易成本法指出了“何种机构管理账本？”及“机构为什么管理账本？”的关键所在。

政府维护着账本的权利、特权、责任和准入。政府是可被信赖的主体，他们保管着存有公民身份及其旅行权、纳税义务、社会保障权和财产所有权的数据库。当账本需要被强制执行的时候，我们就会需要政府的帮助。

公司也同样需要维护账本。公司的专有账本涵盖了员工的职务和义务、所有权分配、人力及实物调度、供应商和客户以及知识产权和公司特权的管理。公司也经常被描述为是“一系列合约的联结”。企业的价值正是来自于这组联结的方式及结构。因此，公司实际上是一本记载着合约和资本的账本。

**公司和政府能够利用区块链技术来提高他们的工作效率及可信度。**跨国公司及其公司网络需要对其全球范围内的交易进行核对，而区块链就可以近乎即时地完成以上工作。政府可以利用区块链不可更改的技术来保证财产契据和身份记录是精确且未经篡改过的。区块链的应用在经过了巧妙的许可规则设计后，可以让公民和消费者更好地掌控他们自己的数据。

**但同时，区块链与公司及政府也有竞争关系。**区块链是一种制度技术。和政府及公司不同的是，区块链是一种维护账本的新型方式，即协作性经济活动。

Before 2009				
Hierarchy				
Government		Firms	Market	
After 2009				
Government	Blockchain	Firms	Blockchain	Markets

-新资本主义经济制度-

公司可以使用区块链技术，但是，也可以被这门技术所取代。现在，一个记录着合约和资本的账本能够以去中心化和分布式的方式存在，而这是前所未有的。记载着身份、许可、特权以及授权的账本无需在政府的支持下维护和执行。

## 制度加密经济学

制度加密经济学的研究对象是：在密码安全且无需信任的账本中，制度的重要性。古典主义和新古典主义经济学家将稀有资源的生产和分配，以及支撑生产和分配的要素作为研究对象。

制度经济学是把规则作为研究对象的一门经济学。规则（如法律、语言、产权、规定、社会准则和意识形态）使得分散的和投机的人们之间的活动得以相互协作。规则可以促进交换——不仅是经济交换，还有社会和政治交换。

所谓加密经济学正是聚焦在支撑区块链及其衍生应用上的经济学原理和理论。它着眼于区块链机制设计中主要使用到的博弈论和激励设计。

相反地，制度加密经济学着眼于区块链和加密经济学中的制度经济学。经济和作为其分支的制度经济学一样，都是一个协调交换的系统。但制度经济学并非着眼于规则，而是聚焦在账本上：由规则构成的数据。

制度加密经济学对如下内容感兴趣：账本的治理规则；服务于这些账本的社会、政治和经济机构的发展；以及区块链的发明是如何在全社会范围内改变账本模式的。

## 经济学在区块链中的重要地位

制度加密经济学给了我们一种工具用来理解区块链革命正在发生什么，以及我们无法预测的事情。

区块链是一项实验性的技术。它到底该用在哪里？这是大多数企业家的疑问。有些账本会被转移到区块链上，而有些企业家虽然试图将账本也转移到区块链上，但却不会成功。区块链不是万能的。我们至今还未看到区块链杀手级的应用。我们现在无法估计账本、密码学、点对点网络的组合在未来究竟会带来什么样的结果。

**这一过程将会极为混乱。**我们预计，全球经济将长期面临不确定性，而这种不确定性来自于其背后的事实论据将有可能被调整、废除和重构。

区块链的最佳使用方式还有待“发现”。之后，必然会将其引入现实世界的政治和经济系统里，而这些系统里已经拥有一批为账本服务的资深且成熟的机构，因此，其代价必然存在。

账本的使用极其普遍，一些治理社会的基本原则唾手可得。因此，区块链的应用可谓是包罗万象的。



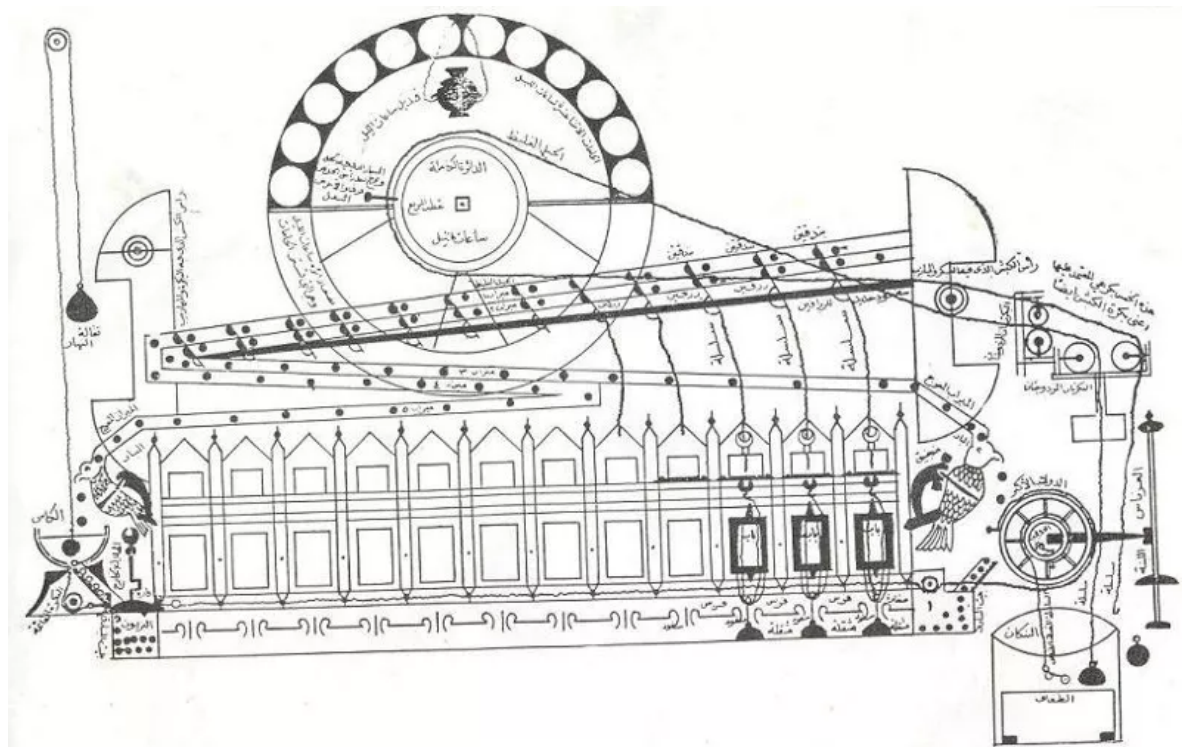
# 制度的创造性破坏

我们曾经也经历过这样的革命。

人们很容易将比特币和区块链的发明与互联网相提并论。区块链是互联网2.0，亦或者是互联网4.0。互联网是一个强大的工具，它颠覆了我们互动和经商的方式。但任何这些比较都低估了区块链的价值。互联网可以让我们更加流畅、快速、有效地交流和交换。

然而，区块链让我们以不同的方式进行交换。**对区块链技术的一个更好的比喻是机械时间的发明。**

在机械时间出现以前，人类活动受制于大自然的临时调控：公鸡黎明报晓，夜晚逐渐黑暗。正如经济史学家 Douglas W. Allen 提出的，问题在于可变因素：“测量时间的变量太过繁多.....以至于无法在许多日常活动中找到借鉴意义。”



-十二世纪的 Jayrun 水钟-

“在任何地方都能感受到因减少度量时间的可变因素所带来的影响”，Allen如此写道。**机械时间开启了一个让人难以置信且几乎不可能出现的经济组织的全新分类。**机械时间使贸易和交换得以同步，超越了地域的限制。它让生产和运输可以相互协调，让一天的安排得以实现，让劳动按照工时得到相应的报酬（让劳动者知道他们是否得到了合理的报酬）。雇主和雇员都能根据一种标准化的，独立的工具来验证契约被履行了。

## 完全和不完整的智能合约

Oliver Williamson 和 Ronald Coase（1991年诺贝尔经济学奖获得者）将合约视为经济和商业组织的核心。合约也是制度加密经济学的核心。这正是区块链最具革命性意义的地方。

区块链上的智能合约可以使合约协议被自动、匿名和安全的执行。智能合约能消除一系列当下用以维护、实施和确认合同被执行的工作——会计师、审计师、律师，以及法律系统的大部分工作。

但是，智能合约受到算法编译的限制。经济学家聚焦在完全合同和不完全合同的区别中。

完全合同特指在任意一种可能性下都将执行的条款。而不完全合同则允许在发生意外情况下，合同条款可以重新商榷。不完全合同对以下问题做了解释：为什么公司会进行交换？为什么市场上会出现交换？同时，它也为一系列关于公司的垂直整合和规模的问题提供了进一步指引。

完全合约是无法被执行的，而不完全合约比较昂贵。但通过智能合约，区块链可以降低与许多不完全合约相关的信息及交易成本，并且以此扩大可进行的经济活动的规模和范围。如此，市场得以在以前只有大公司才可以经营的地方运营，同时，商业和市场也得以在以前只有政府可以经营的地方运营。

具体在何时以何种方式实现上述情况，是企业家所面临的问题和挑战。当下，**预言机**将区块链算法世界和真实世界连接起来，让信任主体能够将信息转化为可以让智能合约处理的数据。

我们认为，区块链革命的真实收益应当来自于开发更加完善和更加强大的预言机——将不完全合约转化为可以在区块链上用算法编译及执行的充分完全的合约。

商业法庭的发展让中世纪的商业革命得以实现。可信任的高效预言机让贸易商可以私下执行协议。但对区块链而言，这场革命似乎还未到来。

### 政府将去向何方？

区块链经济给政务流程带来了全方位的压力，从税收、监管、到提供服务。我们当下的研究项目就是对这一系列的变化进行调查。我们可以思考一下，例如，如何监管银行？

我们采用审慎监管制度来确保金融机构和公众的互动是安全和稳固的。然而，我们常见的情况却是，这些监管（例如流动性和资本金要求）未能让储户和股东们观察到银行的账本。储户和股东们也无法惩罚公司和其管理层。

当储户们发现（或者只是单纯的想象）他们储蓄的银行可能无法支付他们的存款，人们将争先恐后地取钱，此时，银行就会发生挤兑。



- 电影《欢乐满人间》中的银行挤兑的场景（1964年） -

区块链可能存在的一种应用方式是，让储户和股东们持续监控银行的储备金和贷款，以充分消除他们和银行管理层之间的信息不对称。

在这个世界上，市场自律是有可能实现的。公众对区块链不可更改性的信任将确保不会出现错误的银行挤兑。而监管机构的角色将受到限制，他们仅需保证区块链被正确及安全地构建。

一个更为深远的意义将会是加密银行——一个自治的区块链应用，可实现借短贷长，从而直接将借款人和贷款人进行匹配。一个由智能合约算法实现的加密银行拥有和其他银行同等的透明性特征，而一个拥有公众区块链账本和其他一些特征的银行，也可能完全忽略对监管的需求。例如，**加密银行拥有自行清偿的能力**。当加密银行在破产时需要进行交易，其相关资产将会被自动支付给股东和储户们。

在上述这样的世界里，政府应当承担何种监管角色尚不清晰。

Tyler Cowen 和 Alex Tabarrok 提出：似乎大多数政府设计的监管都是用来解决信息不对称问题的，然而，在一个信息无处不在的世界里，并不经常存在这样的问题。区块链应用大幅增加了信息的扩散，使其变得更为透明、永久和易获取。

区块链将其用户置于所谓的“**监管技术**”里——将技术应用于审计、合规和市场监管等传统的监管职能。但我们不可以忽略的是，在区块链的世界里会出现一些新的经济学问题，它将要求我们制定出新的消费者保护措施和市场管理措施。

无论如何，针对类似银行这种基础经济形式的重建和重构，将不仅对如何实施监管带来压力，而且还将对监管应该做什么带来压力。

## 大企业将去向何方？

对大企业的影响可能会是非常深远的。经营规模从通常是由覆盖其业务层次的成本驱动，转而由大规模金融投资下不完全合同和技术必要性驱动。这个商业模式意味着，股东资本主义是商业组织的主要形态。如果能够在区块链上开发更多的完全合约，则意味着企业家和创新者们能够同时维持他们所有权、人力资源控制权和利润。运作一个成功的商业和获得金融资本的关系长期以来不断被削弱，但现在这种关系可能会破裂。**人力资本主义正迎来一个黎明破晓的崭新时代。**

企业家将会开发一个有价值的应用，并将其发布到在“野外”的，任何一个准备好受雇或者需要这个应用功能的人手里。而企业家只需观察他们钱包里累计的微支付即可。一个设计师可以将他的作品发布到“野外”，然后，终端消费者可以下载这个设计到3D打印机，从而马上获得相关产品。这种商业模式使得澳大利亚拥有比目前更多的（本土化的）制造业。

这种让消费者直接与制造商或者设计师沟通的能力，将会限制中间人在经济中的作用。虽然物流公司会继续蓬勃发展，但是，无人驾驶运输的出现也将颠覆此行业。

这里需要记住的是，任何商业模式的颠覆都会破坏公司的税基。或许政府将很难对商业活动收税，因此，我们可能会看到销售（消费）税和人头税将面临巨大压力。

## 结论

区块链和其相关技术的变化将会对当代经济状况产生巨大的颠覆作用。工业革命出现在一个商业模式以等级制度和金融资本主义为根据的世界里。区块链革命将会见证一个由人力资本主义和高度自治为主导的经济体制。

这一切最终将如何呈现，目前尚不清晰。企业家和创新者将会一如既往的通过不断试错去解决我们的不确定性。毋庸置疑的是，在我们确切知道这种颠覆将如何呈现之前，大量的财富将被创造和毁灭。

而我们的贡献在于，当这场颠覆出现时，我们可以提供一个模型，让人们清晰的认识到这场颠覆的含义。

---

**原文链接:** <https://medium.com/@cryptoeconomics/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4> **作者:** Chris Berg, Sinclair Davidson and Jason Potts  
**翻译:** Nicole Yao

Chris Berg, Sinclair Davidson和Jason Potts来自RMIT区块链创新中心——世界上第一个以区块链技术中的经济学、政治学、社会学和法律为研究方向的社科院中心。

三位作者的Twitter: Chris Berg Sinclair Davidson Jason Potts 他们的网站: <http://cryptoeconomics.com.au/>