

匿名性×自治性×开放性×去中心化

信息安全、身份认定、数字货币交易、共享经济

.....

都能大展拳脚

# 区块链在中国

收录国内区块链技术最新实践案例 全面聚焦新一轮数字技术发展趋势

B L O C K C H A I N I N C H I N A

## 它将如何颠覆未来

刘兴亮◎著

中国友谊出版公司

商业思维 | 投资理财  
职场生活 | 知识社群



扫一扫，加入吴晓波频道会员

开启商业世界的从0到1



吴晓波





# 目 录

---

## [导言 从区块链谈起](#)

### [01 区块链发展的全球趋势](#)

#### [第一节 “币圈”热潮背后的信任危机](#)

#### [第二节 主流区块链“货币”生存战](#)

#### [第三节 加密数字货币监管风暴](#)

#### [第四节 法定数字货币“破冰”](#)

#### [第五节 戴上镣铐跳舞：新的探索](#)

#### [第六节 区块链应用的正确“解题思路”](#)

### [02 中国错过了芯片，还会错过区块链吗](#)

#### [第一节 比云计算革命更猛烈的冲击](#)

#### [第二节 巨额投资下的中国区块链技术](#)

#### [第三节 区块链未来中国的蓝图](#)

#### [第四节 中国“区块链+”的应用趋势](#)

#### [第五节 区块链+物联网的无限可能](#)

#### [第六节 哪种区块链技术更具人气](#)

#### [第七节 “空气币”对区块链信任层的侵蚀](#)

### [03 区块链+金融：重构传统金融业的“戏法”](#)

#### [第一节 中国金融业将首先拥抱 区块链](#)

#### [第二节 解决安全与效率的平衡问题](#)

#### [第三节 “无须可信第三方”的世界](#)

#### [第四节 保险行业的区块链试水](#)

#### [第五节 点对点形式的区块链](#)

#### [第六节 支付行业的飞跃](#)

#### [第七节 银行业的再次升级](#)

### [04 区块链+商业：开启全新商业时代](#)

[第一节 可追溯的农产品](#)

[第二节 物联网的“正确打开方式”](#)

[第三节 电商的新生](#)

[第四节 能源区块链的崛起](#)

[第五节 商业领域所期待的区块链](#)

[第六节 权属确定不再是麻烦](#)

## [05 区块链+生活：与更好的生活相关](#)

[第一节 房产证明可以很简单：分布式数据 存储模式下的政府信息安全](#)

[第二节 证明“你是你”：分布式智能 身份认证系统](#)

[第三节 打破医疗困局：区块链视角下的健康联合体](#)

[第四节 消灭贫困的区块链](#)

[第五节 让艺术家们掌控自己的作品](#)

[第六节 农业迎来区块链的春天](#)

[第七节 搭建“公益寻人链”](#)

## [06 新的愿景：区块链应用时代](#)

[第一节 区块链3.0不同在哪儿](#)

[第二节 基础设施建设的效率密码](#)

[第三节 区块链的一小步，有价证券的一大步](#)

[第四节 区块链“提速”公证业务](#)

[第五节 市场预测的“天敌”](#)

[第六节 改造注意力经济](#)

[第七节 让共享成为常态](#)

[第八节 游戏业的破局新方向](#)

# 导言 从区块链谈起

## 区块链到底是什么

随着手机银行、支付宝、微信支付等移动支付手段的普及，我们的线上消费变得越来越简单，但是同时，各种可能的风险也伴随其中。回忆一下我们使用支付宝消费的流程：

第一步，你需要开通支付宝，进行各种实名认证，将手机号、银行卡信息与支付宝绑定；

第二步，将银行卡的支付信息与支付宝绑定，并且确认可以通过支付宝消费；

第三步，开始我们愉快的购物之旅，需要消费的时候拿出支付宝；

第四步，这是一个关键的步骤，也就是你其实并没有与商家直接交易，而是通过支付宝这个中介，将银行卡中的钱转给了商家；

第五步，商家收到你支付的费用，支付宝返回支付信息，整个交易流程结束。

在这个过程中，支付宝起到了一个非常重要的作用。虽然消费者购买的是卖家的商品，卖家也将商品提供给消费者，但是这中间却没有消费者和商家的直接交易，取而代之的是消费者与支付宝、支付宝与商家之间的联系。这种设计的好处在于互不信任的消费者和商家之

间有了一个信任保障机制——支付宝，通过这种机制，解决了交易双方不信任的问题。

这种模式基于一种对权威背书的信任。支付宝首先确立了自身在消费者和商家心中的地位，让“消费者—支付宝”的交易与“支付宝—商家”的交易获得信任，然后以支付宝本身作为信用中介，打通双方的信任。

但是这就带来另一个问题：这种交易真的可信吗？消费者与商家的信任都交给了支付宝，但是支付宝并不直接承担交易。假如我们信赖的这个中介出现问题，是不是整个交易体系都会出现问题？

这种交易具有一定的风险。即使不考虑支付宝本身的信用问题，我们也需要担心，我们全部信任建立的基础都依赖于支付宝这个中介，而它是依托自身的信息中心来实现的。如果这个信息中心出现漏洞或遭到黑客攻击，甚至在物理上受到灾害的影响，那么整个交易的信任机制将不复存在。

如果这些假设成真，那刚刚转出去的钱不知去向，你找谁说理去？就算支付宝是一家有良心的企业，它有什么办法确认这笔转账就是真实发生的？你百口莫辩。

这种危机的本质就是集中式存储带来的问题。消费者本身对交易的不信任，借助一个第三方的权威中心来化解，这本质上放大了权威中心的价值和地位，事实上也就意味着中心的高度价值，而价值的另一面是风险。

那么，有没有一种方式可以解决这个问题呢？假如消费中不再存在集中式交易场景，而是变成一个非中心化的体系，我们会不会获得一种不同的交易体验呢？

让我们来重新构建一个交易流程。如果要购买一件商品，假设这件商品是一个杯子，我们也许可以用这样的方法：

第一步，消费者挑选到了喜欢的杯子，于是在网上联系商家，并且双方同意进行交易；

第二步，消费者和商家都确定了一个记账的区域和范围。假设我们将这个范围称为“公共账本A”，消费者将自己的交易需求写入“公共账本A”；

第三步，为了保证交易可靠，消费者将交易信息广播出去，向所有人说明，自己已经确认了一笔交易，虽然这笔交易还没有支付，但是用于支付的“金钱”已经被预定了。除非重新写入一条交易撤销的信息，否则这些“金钱”已经不能用于其他交易了；

第四步，卖家查阅“公共账本A”，确认交易信息，同时在自己手中的“公共账本B”上写明自己的商品已经被人购买；

第五步，卖家把这条消息广播出去；

第六步，交易双方确认交易成立，并且在公共账本A和公共账本B上记录信息；

第七步，卖家发货，消费者收到杯子。

在这样一种模式下，原本处于交易中心的“权威”就不再具有意义了，原来对集中式框架的“权威中心”的威胁，也就不存在了。所有的信息都存在于一个公共的广播体系之中，很难找到一种方法可以将这么多中心里的内容一并改变。所以这笔交易一旦发生，就再也抹不去痕迹。



我们也许会发现，现阶段很多社会机制都是“集中”的机制，包括政府、银行、评级机构、交易中心甚至我们最熟悉的公司。这些组织围绕权力、权威的分配形成一系列的集中式组织，这种“集中”的背后，其实都是为了解决人与人之间的“信任中介”问题。

最典型的是政府机构出具的各种“证明文件”，比如我们熟悉的身份证，其实就是为了在完全陌生的人群之间或交易之中，确认个人的身份。

在现阶段，“集中”是社会运行过程中效率最高、成本最低的方法。但是不可否认，集中式的权威背书会产生很多问题。各种各样的专家丑闻、政策丑闻，就是这种集中制度带来的副作用。面对这些副作用，采用一种新的、去中心化的模式，可能是一种有效的方法，而实现这种模式的技术基础就是区块链。

## **区块链的颠覆力量：底层技术**

从根本上来讲，区块链是一种数据存储技术，只是这种技术与曾经的存储模式有非常大的区别。

在人类社会发展过程中，有很多种不同类型的信息存储方式。虽然随着社会的发展，我们越来越倾向于将信息存储与U盘、硬盘、云盘这类存储技术相关联，但是事实上，信息的存储从人类进入文明就开始了。

有据可查的人类记录行为是结绳记事。为了记录部落的打猎收获和分配情况，人类祖先采用给绳子打结的方式来记录。

这些记录行为贯穿人类社会的始终。后来的U盘、硬盘、云盘这类有形的存储模式，只是信息的一种载体，它们从本质上讲，与人类

社会最早期记事的绳子、画壁画的岩石和后来改变世界面貌的纸张是一样的。

在过去，人类记录水平的高低，很大程度上是由存储介质的能力决定的。比如我们采用纸张记录的时候，就很难记录数字化信息，直到磁盘介质开始进入存储领域的时候，人们才真正地获得数字信息存储和处理的能力。这也是大部分人对于信息存储的认识都会不自觉地向存储介质方面倾斜的原因。

但是区块链的出现则打破了以往的规则。区块链从本质上讲，并没有改变我们信息存储的介质。就信息存储的载体而言，区块链使用的依然是数字时代的存储介质。但我们依然把区块链技术看作是信息时代的一种技术革新，而这种革新，最主要是体现在信息存储模式上。

区块链的本质是用一种链式结构连接多个数据区块。

数据区块本身可以理解为一种信息的集合。区块可能是几个数字，也可能是几个文字，这些数据区块是最重要的，因为它们可能代表不同的意义。比如，这几个数字可能是你的银行卡密码，那几个文字可能是某个重要岗位即将任命的人员名单。

当然，如果这些信息区块失去了特定的作用环境，也就不存在意义了。而这些作用环境信息又被拆解为无数个不同的数据区块。就像银行卡的密码，如果不是与某个人的银行卡相联系，这些数字就没有意义了。而银行卡的账户信息又是一串数据区块，账户信息内的货币又是一堆的区块信息。

每一个区块信息单独拿出来可能都没有意义，但是如果用一种方式把这些数据区块组合起来，就有了意义。

那么，这种把一个完整的信息切分成多个数据区块、并形成这样一种组合起来才存在意义的方式，就是链式的区块信息保存技术。

这种信息保存方式本身并不新鲜，比如我们最熟悉的电脑硬盘，其实就是用这种块状的模式来存储信息的。

区块链到底有什么不同呢？其本质是存储的模式不同。

传统的信息存储方式是中心节点的方式。也就是说，关键的、核心的信息是存储在某一台电脑主机上的，信息的所有区块组合都放在一起，而把它们串起来的数据链条也存在于这台电脑中。一旦这台电脑被人窃取，所有的数据也就丢失了。

而区块链用了一个不一样的逻辑来解决这个问题。区块链的底层其实是一个拥有数量巨大但有限个解的数学公式。例如，我们可以把区块链理解为这样一个公式：

$$(X+Y) \times 3 = 123$$

为了让这个逻辑简单一点，我们假设X与Y都是正整数，那么我们知道，会有有限组的数字组合能够让这个公式成立。那么我们认为其中每一组X与Y的解，就是一组存储密码。

这个数学公式拆分成几个数据区块，可能包括一个解答的区块123，一个计算规则的区块乘号，一个乘数3，以及有限个解。

这样，计算规则是不确定的，数据也是不确定的，将这些数据分散放到不同的电脑中，即所有的“X”“Y”“123”“3”分布在不同的电脑中。

我们需要一个公共的计算共识，假设定义一个公共共识是“=”。如果我们将“X”作为我们想要储存的信息，那么对于“X”就可能有很多种不同的“Y”对应。如果我们不知道某个特定的Y，就无法知道对应的X。

而知道某个特定的Y的时候，掌握这个信息的人就能得到X。假如我们的X与Y接近无限个，那么没有得到Y的人永远无法知道X是什么，这种模式保证了数据X的安全。

这是一种相对好理解的方式，而真正的区块链中则是针对乘号来运算的。也就是我们将数字组合X和Y作为数据区块存储起来，但是运算规则是我们的解密条件，这种情况下，每一种运算模式就代表了一种数据含义。

这就让我们摆脱了集中式数据存储的风险，让我们能够随意地把数据区块存储在不同的位置上，而我们自己掌握运算规则。结合具体的应用模式，就可以获得各种各样的区块链应用场景。

基于这样的结果，我们就得到了区块链匿名性、自治性、开放性、去中心化的特点。

匿名性最好理解。因为我们看到信息区块的时候，只能看到信息，并不知道信息的储存者。同样，由于存储的分布性，当信息被提取的时候，别人也不知道信息被什么人提取。这保证了信息基本的匿名特征。

自治性与匿名性一脉相承。由于信息的存储与提取都是绝对自由的，人们相互之间也就不存在管理关系，信息与人的关系简化为人与存储信息的机器的关系。人们不需要考虑各种限制条件或复杂的保密协议，只要把自己的秘钥输入机器，就可以得到结果。

开放性则是前面两个特点带来的应用结果。因为人们不用再担心数据的管理责任与安全的问题，因此也就不再担心存储的客观性，只需要担心存储的正确性，因此就可以更加简单地存放信息。

去中心化是区块链的基础特征，所有的其他特性都是基于这个特点形成的，而这带来了极大的信息安全性。如果一个人想要篡改某个数据，就需要找到分布在所有存储介质中的可能相关的信息，同时再修改运算规则，而这几乎就是对全世界所有数据进行一次筛选，不可能完成。

正是这样的技术特点，让区块链为我们的信息存储带来了新的模式。这也正是区块链可能带给各个行业的最有价值的应用。

## 比特币的“前世今生”

比特币最初的发明可能是一种偶然，也可能是一种有意而为之的创举。今天来看，已经很难确定中本聪最早设计比特币的缘由，但是比特币的发明最终让人们看到了一种打破现有银行体系甚至所有金融体系的、新的支付方式的可能。随着比特币的日渐风靡，人们对于比特币底层的区块链技术也越发熟悉，应用越来越广泛，其光芒甚至已经掩盖了比特币本身。

那么追本溯源，比特币是如何实现替代银行的呢？首先要知道银行是怎么在两个账户间进行交易的：

A账户有2000元，B账户有1000元，A支付了100元给B，银行就在A的账户上标记一笔“A付了100元给B，余额1900元”，在B的账户上标记“收到A的100元，余额1100元”。

简单讲，货币交易的过程，就是一个记账的过程。之所以通过银行，是因为它权威、可信，不会作弊。但是，银行的记账之所以能不



出错，也是借助了一些外力的。比如，当你通过网银付款时，银行怎么确信就是你付的呢？还是得借助密码、验证码等计算机、互联网方面的技术。 [1]

这种通过银行的交易过程在过去很长一段时间里，都是一种高效的方式，甚至可以说，从银行业开始出现并发展至今的几百年时间里，这是银行业找到的最高效的一种支付方式。随着计算机技术的进步，这种以记账、密码为基本元素的交易方式为银行业带来了快速发展。但是中本聪却并不认为这是在现今的技术条件下解决银行交易效率问题的最佳方式，于是他用一种去中心化的方式重新设计了交易逻辑。

银行的根本是解决信任问题，也就是说，如果中本聪以一种可靠的方式来解决信任问题，他就能找到一种全新的交易方式。于是，他找到了一种新的解决方案：

计算机“群狼”中的某一台，收到A发来“付100元给B”的请求后，需要先确认两个问题，然后才能决定是否执行请求，帮A记账——

一、这个请求是否真是由A发出？这个简单，计算机领域已经有一种叫作“数字签名”的技术，只要A能提供某个只有他自己知道的私钥，计算机就能够确定这个请求确实是A发出的。

二、A的请求与目前整个记账系统中的所有既存信息是否矛盾？比如，系统显示A的余额只有99元，A却请求支付100元，这肯定不行。

问题二解决起来相对麻烦一点，因为每台计算机都属于整个系统的一部分，一旦出现矛盾，谁都认为自己是“目前整个记账系统中的所有既存信息”之一，要求别人“不许和我矛盾”。那究竟该以谁为准？

比如，A在余额还有100元钱时，请求支付100元钱买某个东西；紧接着，他又请求再支付100元钱，还要买另外一件东西。由于存在网络延迟之类的问题，计算机们难以确定这两条请求究竟哪条在前。但可以肯定的是，其中一条是无效的。

“区块链”技术怎么解决这个问题？那就是“做题定胜负”——先将两条请求都记录在案，不忙于确认，然后系统会出一些公费雇甲乙两人对赌，分别押注那两条矛盾的请求，然后让两人分别运用自己计算机的算力，比赛做题。谁的计算机算力强而且运气好（解题成败具有一定的随机性），先把题解出来，这笔公费就归他了。同时，他押注的那条请求也就被系统正式确认，而另外一条请求则自然作废。

如果甲乙两人旗鼓相当，不分高下，怎么办？那就再雇丙丁两人接着比。丙跟在甲后面，丁跟在乙后面，如果丙赢了，丙和他前面的甲就都赢了，如果丁赢了，丁和他前面的乙就都赢了。

如果丙丁又打平了呢？那就再雇戊己，重复上述过程，一直到分出胜负为止。 [\[2\]](#)

这种模式从根本上消除了银行核对密码与交易信息的过程，把所有交易过程中可能需要集中核对的内容分散到了不同的计算步骤中。这样的好处是可以最大限度地使用机器去承担过去需要人来进行分析的工作。

如果再向底层分析，那就需要进一步地深入到人们交易的信任底层。而打通信任底层，可以省去银行的中间环节，极大地提高交易效率，降低交易的成本。这种成本不仅仅是全社会为了实现可信交易而进行的银行间交易成本，更重要的是降低了时间成本。

人们通过银行进行交易，其实是因为它可以在方便与安全之间找到一个平衡。银行交易过程中，银行承担了“责任承担者”的职责，这种职责以保证交易可靠为基础。当遇到违规交易行为，银行将会分担相应责任。

在过去，这种职责的承担是通过核验、监察和安全的印鉴体系来实现的，而比特币的逻辑则是以算法为基础、形成“绝对不可篡改的数据”来实现。这种数据实现的模式也就是最终交易的信息保障。

从本质上来说，货币就是信息综合载体的集合。因此，如果能找到某种模式也提供类似货币的信息保障，就可能找到另一种货币的表现形式。

比特币就找到了这样一种形式。

解决这种需求的方式就是将交易信息拆分，同时多段备份，而且寻找一个算法作为提取这些信息的**钥匙**，让这些信息不可能同时被篡改，以此来保证信息的准确安全。

而将信息拆分、备份的过程中，就形成了多个信息区块，将他们提取串联起来的算法就是链条，这就形成了区块链。信息区块的生产，是使用过程，而链条的生产则是信息使用的前提。

其实比特币的核心就是这些链条，也就是某种算法的有限个解。所谓的“挖矿”，就是不断地计算出这些解的过程。

这样，我们就能看到比特币完整的发展进化过程和解决问题的逻辑：代替货币——寻找信任机制的载体——找到区块链技术。

但是没有想到的是，区块链技术的发展最终突破了比特币的原始设计目标，反而为后续的区块链应用打开了新的可能性。而这种可能

性也最终让比特币从一个可能带来金融体系崩溃的潜在货币，变成了可能推动生产发展的新型技术。这也是一种技术发展过程中带来的进化的可能性。

# 区块链掀起的公信力革命

区块链技术本身所希望解决的，是人们日常生活中的信任问题。而且我们看到，随着各种各样的信任问题的出现，人们对于区块链方面的需求正变得越来越旺盛。尤其随着P2P（点对点网络借款）产品“爆雷”，我们发现新型金融模式的安全是一个大问题，而区块链很有可能解决这个问题。

区块链的底层是去中心化，但是它在去中心化的基础上，可以实现陌生人之间的信任。

在现行的社会机制之下，社会用巨大的成本承载了信任机制的建设。从政府到银行，从司法到货币，甚至教育、医疗，在信任上都花费巨大。其实日常生活中我们最头疼的各种证明，本质上就是信任问题外显的结果。

社会解决信任问题的直接成本巨大，间接成本更大，其中的核心成本是不信任带来的机会成本和轻信带来的风险成本。因为不信任，可能会延长事情的处理时间，也可能导致交易不顺利；而轻信带来的风险可能是更加直接和致命的。那么区块链是如何解决这些风险的呢？

区块链解决信任问题的方法，是要求每个联结点在共同的账本上，对每一笔交易进行分布式记账。每当交易发生，信息会传达到所有的“点”，各个“点”（即人）按照预设的规则，独立地对交易进行确认。整个过程中，信息透明、统一，参与者资格和权限完全对等。

多数“点”确认的结果，就是最终的结论，系统会自动将其他“点”的数据修正为大家认可的结果。如果你想作弊或者坚持不同的



观点，除非能让超过50%的“点”同时认可你的结论。但是当参与的“点”多到一定程度时，这事实上是不可能的。一次交易得到确认之后，交易的记录和各种数据被打包成块，加上时间戳编入链中，然后启动下一轮交易（块）。新旧区块前后相继，形成“链”。各个区块所储存的交易记录可以无限追溯，随时备查，且无法更改，想要作假、撒谎、隐瞒真相，根本无机可乘。人与人之间的信任由此得以确立。

这种信任不依赖于某个权威，而是建立在“共识”之上——一种由所有参与者在完全平等和信息充分透明的基础之上达成的“共识”，并且所有人共同维护和传承已经形成的“共识”，是真正的“多数人对少数人的暴政”。

第二代区块链还引入“智能合约”机制，在程序中加入了能够自动履行的合约。一旦约定的条件得到满足，系统将自动实施强制交付，所有的联结点也会见证和确认这一过程，容不得背信弃义行为的发生。<sup>[3]</sup>

传统的社会公信力以实体凭证为主体，实现了人与实物之间的切割，但是进入数字化时代之后，虚拟物质的大量产生尤其是过去的实体凭证逐渐虚拟化，对人们的信任机制提出了更多的要求。身份信息、财产信息等，都成为重要的虚拟证明系统。

这也让很多人开始钻营，如何通过假造电子凭证来非法获利。

在以往的社会治理过程中，制贩假证会面临各种责罚，但是在网络世界中，在一些灰色地带制造非法的电子凭证，一方面很难查证，另一方面也存在管理空白。

比如我们比较容易接触到的钓鱼网站，在过去网络治理水平还不如今天的时候，这些网站总能以假乱真，诱骗人们上当。甚至直到今

天，这种事情还是会不时地发生。

这类事情多发生在网络购物的过程中。通过一些搜索引擎或一些购物链接的跳转，都可能遇到虚假的链接。

而要避免这种虚假链接，可以用到区块链技术。工程师创建一个固定的信息区块链来完成信息的录入，这个过程可以同时储存在多个信息区块中，以确保网站信息的唯一性，而真实的网站通过公布自身的验证区块，供公众进行检验。而这个过程，又可以通过计算机协议进行，事实上对于人们的购物过程没有任何影响。

这还仅仅是一种区块链的使用模式。在实际应用当中，区块链还可以有很多种不同的应用场景：

**表1-1 公信力当事人之间的关系**



正如表格1中所看到的，公信力现在可以被多方交叉验证与监督。重要的是，数据一旦进入区块链，是无法被改变的，各方公信力可得到认可和增强。

在这种模式下，一方面是社会各方都可以留存信息，另一方面，政策的出台仍然是一个集中的权力模式，但是在信息的使用和存储方面却有很多不同。在这种体系中，所有信息都存储于不同的信息节点中，公信力的实施不再需要复杂的证明过程，只需要通过区块链来行使权利，另外添加了独立而重复的计算，使得公信力可以被多方（大众、公司、政府）检验，甚至政府的失职行为（例如政府官员更改数据、数据保护不当）都可以被发现。

区块链不制定政策，只有政府才能建立和执行政策。区块链只是有助于政策被其他方所知，并为执行这些政策提供一个不变的且可被复制的数据库。这类数据库有助于保证每个人都成为诚实守信的公民。<sup>[4]</sup>

## “挖矿机”进化史

上文中我们提到了“挖矿”，这也是获得比特币最原始的方式。那么“挖矿”是怎样运作的呢？实际上，“挖矿”就是在用户相互验证并实现比特币交易去中心化过程中，通过计算机对各种复杂密码问题进行解析，最终实现包括交易金额、交易时间、交易钱包地址等信息，并被“区块”采纳整合。当然，这个简单的定义很难完全解释清楚“挖矿”的原理，我们需要结合区块链的核心特点来阐述。

前文曾叙述了区块链具有不可篡改的特点，这源于区块链只有append（追加、添加）程序，而没有update（更新、最新）程序，所以新成立的区块只能被放置在区块链尾端。这意味着，每次想要增加新的区块到区块链上时，当前区块的操作就必须结束，将最新的区块数据传输至本地，才能继续开始创建新区块的工作。

同时，创建新区块需要一系列复杂的操作，通过特定的计算规则来满足一个特定的值。因此“挖矿”过程就是运行特定计算公式，试图计算出符合规则的哈希值（HashFunction，散列函数，是一种从任何一种数据中创建小的数字“指纹”的方法）。当我们通过种种手段实现了这个过程，就相当于生成了一个最新的区块，可以放在区块链的尾端，而生成新区块的操作，会产生大量的可以超越成本的奖励。

奖励包含两部分：一部分是创建新区块的奖励金，这部分占奖励的绝大比例。给“矿工”奖励金是为了激发“矿工挖矿”的热情，因为“挖矿”能够维护比特币的稳定和安全，它可以确认比特币交易，从而防止

欺诈交易，避免“双重支付”的情况发生。这部分奖励又被称为“Coinbase（一家比特币交易所）交易金”；奖励的另一部分是新生成区块打包全部交易的佣金，这部分奖励占比较低。

比特币创始人中本聪做了这样一个设定：新区块产生的速度在每10分钟一个左右，新区块的诞生代表着一定数量比特币的发行，但新币发行速度是减慢的，每隔4年就降低50%。这意味着“挖矿”有一个特点，就是密码问题会随着挖矿人数的增多而不断提升难度，这也意味着需要越来越强大的运算能力和越来越昂贵的软硬件条件。但实际情况是：有时网络中算力比较强，那么开发一个新区块或计算出一个符合的哈希值用不了10分钟；而有时算力比较弱，开发时间又被大大拉长。交易时间太短，会对比特币系统带来一系列危害：一方面，“矿工”在挖掘出新区块后，需要借助网络进行交流，以判断这个新的区块是否在主链上，如果不在，则只能丢弃这个区块，因此间隔时间较短，就会出现很多不安全的“孤块”，造成极大的浪费；另一方面，速度快说明计算难度低。出块速度增快的时候，块与块之间的碰撞也会急速增加，使得主链的分叉增大，系统需要花更多的时间在众多分叉中识别主叉及分叉，这会大大影响系统的正常运行。

为了解决这个问题，中本聪设计出一个参数difficulty值，在每2016个区块产生后，系统将会自动调节difficulty值大小，调整公式为：

新difficulty值 =  $\text{difficulty值} \times (20160 \text{分钟} / \text{过去最新2016个区块的生成时间})$

为什么是2016这个数字呢？因为 $2016 = 14 \text{天} \times 24 \text{小时} \times 60 \text{分钟} / 10 \text{分钟}$ 。当生成时间缩小时，difficulty值自动调节。比如说，原来哈希值为15个0开头的16进制数字，为了加强难度，系统可以将哈希值改为20个0开头的16进制数字，相当于原来需要连续15次从一张标记为1、另

一张标记为0的纸条中，精确抽中0；经过调整变为要连续20次抽中0，难度当然大大提升了，所花费的计算时间也相应增加了。

通过上面对“挖矿”原理的阐述，想必大家也知道了，如果想要通过“挖矿”得到更多的奖励，那么“矿机”的算力是一个非常重要的条件。在实际“挖矿”过程中，对“矿机”的选择上，人们不仅会考虑算力，还会考虑质量、功耗、电量等种种因素。2009年～2013年，比特币从诞生至炙手可热的短短5年时间里，“挖矿”硬件（也就是我们所说的“矿机”）已历经了四代发展——

第一代为“CPU（中央处理器）挖矿机”，是比特币在2009年出现以后被最先用于“挖矿”的矿机。它的特点在于性能强大且难度极低，可以简单地使用处理器进行挖矿。然而由于其逻辑十分复杂，计算能力较低，随着区块难度的不断增大，已经不再适用于现在的“挖矿”；

第二代为“GPU（图形处理器）挖矿机”，2010年9月出现，逐渐取代了常规的CPU挖矿机。GPU挖矿的工作原理，主要是依赖于显卡中的SP（流处理器）单元，运算能力大小取决于SP单元的数量；

第三代为“FPGA挖矿机”，即现场可编程门阵列，可以理解为简易版的ASIC（专用集成电路）芯片。2011年1月开始应用，在2014年达到50亿美元的市场份额，但现在已经逐渐被ASIC所取代。目前除了一些小额币种，已经很少使用。

第四代挖矿机，也是目前市场上应用最为广泛的矿机，被称为“ASIC挖矿机”。它是2013年1月由嘉楠耘智研制的商用挖矿机，能够迎合特定的需求，具备更低的功耗、更高的可靠性和保密性、更小的体积及更低的成本等多项优点，从而使它成为主流矿机。



将“矿机聚集在一起，就形成了“矿场”。目前全球“矿场”占有量居世界第一的国家为中国，占有全球58%的“矿机”，与之相比，第二位的美国仅占有16%。

经营一家“矿场”不得不考虑的事情，就是耗电量及电费，这也是比特币隐形的软件需求。局限于计算机硬件设备和技术，“挖矿”的耗电量正处于日益增高的态势。据统计，目前比特币年耗电量为68.08万亿瓦小时，占全球总电量的0.3%；比特币已用电量相当于600多万个美国家庭的用电量，甚至可以供应1/4的意大利和英国用电。耗电量的增加，也使得“挖矿”成本不断上升。目前比特币的“挖矿”成本已占收入的一半。可以预见，当耗电成本与收入接近时，比特币的开采将陷入停滞。

不同国家的电力成本差距，也成为这个国家“挖矿”的优势之一。如中国挖一个比特币的电力成本约为3172美元，远低于大部分欧洲国家，这也解释了为什么中国成为拥有最多“矿场”的国家。

比特币最初设计的上限为2100万枚，每过4年其增速就会降低一半，预计至2030年，潜在的比特币将被挖掘殆尽，比特币所有存量将不再有任何变动。

综合考虑“挖矿”所需的软硬件条件，我们会发现，对比收益来说，投资几百万元建立“矿场”，也只能被称为“小试牛刀”而已，特别是在比特币价格不断起伏的情况下，投资“矿场”成了一场比拼财力雄厚的比赛，没有足够的资金支持是很难长期运行的。对于很多小“矿场”而言，他们会逐渐发现“挖矿”并没有想象中那么容易，成本收益比在持续下滑。

An abstract graphic on the left side of the page, featuring a complex network of interconnected circles and lines. The circles vary in size and are shaded in different tones of gray, creating a sense of depth and movement. The lines connecting them form a web-like structure, reminiscent of a molecular model or a network diagram. The overall effect is a dynamic and intricate visual element that complements the technological theme of the text.

01

## 区块链发展的 全球趋势

## 第一节 “币圈”热潮背后的信任危机

比特币的匿名性及去中心化，在赋予其自由交易、保护隐私等种种优势的同时，也为其发展设置了障碍——成为洗钱的工具、遭受暴力盗取的风险。

我们来看一起审判案例：

绥化市华辰商贸有限公司遭受网络诈骗，财务部经理董某收到诈骗信息，误认为单位同事要求汇款，不慎将1200万元公司公款打至诈骗犯罪嫌疑人肖某某从网上购买来的银行账户中。同时犯罪同伙黄某某，提前用网上购买得来的身份证、银行卡等信息，在北京乐酷达网络科技有限公司旗下的比特币交易平台“OKCoin”注册了账户。

在取得诈骗款后，犯罪嫌疑人肖某某将其中500万转至黄某某买来的账户中，另一名犯罪同伙许某即以“wuge”的名义通过QQ与乐酷达公司客服联系，充值200万元，并通过QQ要求客服将款充入另一个账号。

客服发现充值方和被充值方非同一人，且数额较大，遂要求“wuge”发送身份证正反面照片。许某以照片的形式发给客服一张网上买来的身份证复印件，客服只核对了身份证复印件与注册时信息相符，没有坚持要求“wuge”发送身份证正反面照片及手持身份证的照片。在没有进一步确认此笔业务的操作人与注册客户是否为同一人的前提下，客服即同意许某在账户充值200万元。

许某以他人名义获得充值后，利用乐酷达公司网站“OKCoin”交易平台，分34笔购买价值约200万元的比特币553.0346个。在进行比特币买入的同时，他又操作该账户同时进行提币业务，先后分4笔将购买的

553.0346个比特币全部提出平台，转移到他在另一个网站注册的比特币钱包。之后，他伙同黄某某在澳门地下钱庄将比特币卖出，所获取的现金被两人挥霍、还债，已无法全部追回。

华辰公司于2015年2月诉至绥化市中级人民法院，要求乐酷达公司及相关责任人赔偿公司财产损失177万元。对此，法院判定乐酷达公司存在过错，判决其对华辰公司不能追回的损失应承担40%的赔偿责任。<sup>[5]</sup>

这样一个案例可以视作国家管理比特币交易的风向标，即比特币交易平台需要承担与金融机构或支付机构相类似的反洗钱职能。另一方面，比特币的交易特性及金融属性，也促使国家希望将比特币纳入监管系统，从而避免它为洗钱等不法交易提供渠道。

另一方面，网络平台的数字化，也使得比特币可能成为犯罪的温床。世界五大比特币交易所之一的Bithumb，在2018年6月就因黑客攻击被盗取了价值3000万美元的数字货币。受此消息影响，各种数字货币市值均出现一定程度的下跌。

比特币交易中心被盗与普通的银行账号被盗不同，之前说过，交易中心是将所有信息记录在区块链上的，资产仍然保存在个人账户中，那黑客是如何盗取数字货币的呢？

我们可以拿淘宝购物做一个类比：当我们在淘宝挑选好商品，最终结账时，淘宝相当于在卖家与买家之间建立起一个交易联系，形成一个虚拟的交易账号链接。通过这个链接，买家把钱从银行账户转移给卖家。而黑客攻击的就是这虚拟链接——通过一系列操作，将交易链接篡改为自己的账户，从而使得交易过程中买家向卖家支付的钱被转移到黑客的账户中。黑客盗取的主要是信息流，这就是通常所说的去中心交易平台的“智能合约漏洞”。

不仅如此，黑客还创造性地开发出一种“赎金”形式。2014年开始，陆续有人在打开电脑或手机时发现所有文档被人加密，难以自行破解，加密者同时留下了一段文字：如果想要取回文件，请支付“赎金”。而“赎金”的支付方式正是通过比特币——将“赎金”以比特币的形式支付给某个匿名账户，对方将在获得“赎金”后将文档的密码发送给支付者。一旦有所迟疑，超过了黑客所要求的时间，黑客将关闭交易渠道，且不再有任何答复或处理，电脑或手机直接变成一块价值高昂的“砖头”。毕竟，黑客可以通过高超的技术入侵多个电脑或手机，不必局限于一个“受绑者”。

美国的一些连锁快餐店则受到了另一种威胁。这些店收到黑客的通知，要求在一定时间内向某个账户支付比特币，否则就在网上对餐厅恶意差评，或是拨打投诉热线投诉餐厅乱收费、食物卫生不健康，还用假订单骚扰客服，让外卖员无暇他顾……诸如此类恶劣手段，让餐厅不堪其扰，不得不向对方支付敲诈勒索的金额。

比特币的种种特性，一方面使它风靡于世，另一方面，也使它在监管领域形成空白。所以，很多国家或是对比特币设置各种限制或监管要求，或是直接限制比特币的交易。这一点我们在本章第五节再进行详细的介绍。



## 第二节 主流区块链“货币”生存战

比特币的暴涨、区块链理念的传播，在造就亿万富翁的同时，也让闻风而动的投资人看到了未来的趋势和更多的可能，越来越多的数字货币开始涌现。打开一个交易所的页面，可以看到眼花缭乱的数字货币，让投资者感到无从下手。据统计，现在已经有3000多种数字货币，每天都有新币上交易所，同样也有不幸清零者。仅仅在2018年8月之前的18个月里，已有近千种数字货币宣告“死亡”。

目前世界主要的数字货币大约有60余种，这些数字货币也是拥有完整交易链条的货币种类。第一名是引领数字潮流的比特币，在前文中我们已经围绕它进行了详细的介绍，此处无须赘述。需要注意的是，比特币目前仍是各类虚拟数字货币的老大，在各个交易所名列首位，也是初次进入数字货币投资领域的投资者最爱选择的币种。作为全球第一的区块链项目，比特币是当之无愧的No.1。未来会不会有其他虚拟货币超过它呢？至少目前看似还没有。

排名第二位的是以太币，是区块链2.0时代的开创者和引导者，以太币开发的imToken数字货币钱包目前被百万币圈人士使用，受到广大投资者的欢迎。作为各个交易所中比特币之下公认的第二名，它是最有可能超越比特币的数字货币。

排名第三的瑞波币，是Ripple网络的基础货币，它可以在整个Ripple网络中流通，总数量为1000亿个，并且随着交易的增多而逐渐减少，瑞波币的运营公司为Ripple Labs（其前身为OpenCoin）。同比特币一样，Ripple也是一种可共享的公共数据库；但不同的是，比特币是一种虚拟货币，而Ripple是一种互联网交易协议，它允许人们用任意一种货币支付。

其余更多币种，就不一一介绍了。

为筹集资金，目前世界各地区块链企业采取将代币直接向投资者出售的形式，这被称为首次代币发行，即ICO。投资者购买ICO，主要因为一旦该虚拟数字货币发行成功，币值上涨，将为自己带来巨大的经济利益。然而随着比特币币值的下跌，人们对ICO越来越慎重，投资意愿也有所降低。据2018年6月普华永道咨询公司和瑞士加密谷协会的一份联合报告显示：2018年1月至5月间，共有537家公司注册发行了ICO项目，并筹集了137亿美元，规模几乎是整个2017年的2倍（2017年总共有552家公司ICO，筹集总额仅超过70亿美元）。

同时，该报告还指出，自2013年第一个以筹资为目的的代币产品发布以来，至今已累计有3470个公司宣布推出ICO，但其中只有30%的ICO最后圆满完成筹资。其他许多公司或是由于各种原因推迟产品推出，或是在ICO的过程中逐渐失去动力，消失不见。

商业诈骗、币值炒作、融资风险……一系列问题的出现，为数字货币的发展蒙上了一层阴影，但这并不意味着数字货币将被时代抛弃。事实证明，加强监管、增强透明化，反而会让ICO得到进一步的发展。例如，美国、新加坡和瑞士是国家监管力度较强、监管进步较大的3个国家，也建立了全球3个最重要的ICO中心。

普华永道恩略特的区块链EMEA（欧洲、非洲、中东地区）负责人戴默斯（Diemers）在报告中表示，在2017年区块链炒作泛滥之后，ICO行业已经发展成熟。他强调，随着ICO的法律和投资者关系方面在未来有所改善，ICO的失败率将下降，更多项目将在合适的合作伙伴和投资者的帮助下取得成功。

### 第三节 加密数字货币监管风暴

信用诈骗、偷税洗钱、转移外汇……区块链货币带来的风险，使很多国家对其望而却步。如中国货币主管机构曾几次发文，对区块链货币做出限制。其他国家政府也意识到了这种风险，它们或是采取限制措施，或是彻底禁止区块链货币化。

2018年4月，印度储备银行宣布停止商业银行、金融机构与加密货币相关的各类服务。该银行明确指出，货币应由金属或实物制造而成，并需要经过中央主管机构的审批，比特币等加密货币不得被视为货币。同时，印度储备银行警告说，任何持有加密货币的组织或个人将自行承担加密货币所带来的风险。受此影响，印度最大的数字货币运营商Zebpay要求投资者在限制时间内提取资金。对此，印度互联网和移动协会（IAMAI）向印度最高法院请愿，详细解释了加密货币的原理、运行机制及区块链技术，企图迫使银行主管机构暂停此禁令。令他们失望的是，最终最高法院认定不接受此项请愿，寻求银行替代品成了唯一可行的方案。

紧接着在2018年5月，受到波兰政府新的监管方案的影响，波兰境内的银行开始逐步宣布暂停与波兰的加密货币交易中心Bitbay合作。6月1日，随着最后一家波兰银行宣布暂停服务，Bitbay也暂停了在波兰的服务并转移至不受限制的马耳他。Bitbay是东欧和中欧最大的交易所，拥有80万以上用户，其24小时交易量可达835万美元，占全球比特币市场交易总额的0.26%，居世界数字货币交易中心第10位。令人惊奇的是，马耳他政府的表现恰恰与波兰相反，马耳他怀着成为加密货币新交易中心的野心，连其总理也亲自通过Twitter向Bitbay示好。在政府的积极推动下，已有超过20个大型加密货币项目即将在马耳他落地。两个政府截然不同的态度，令人玩味。

除此之外，2018年6月日本金融监管机构——金融服务局（FSA）发布命令，要求数家加密货币交易所出台反洗钱措施，这意味着日本监管机构对现行加密货币交易中心制度存在担忧，认为加密货币有参与洗钱甚至是参与恐怖组织洗钱活动的风险。此命令发布后，各大加密货币项目及交易中心备受打击，虽然美国资金管理公司BKCM创始人兼CEO提出，从长远来看，这项举措可以加强加密货币的合法化，为区块链建立良好生态系统奠定了基础，但仍无法改变这次政令导致比特币价格下跌11%。毕竟，日元兑换比特币占有所有加密货币日交易量的60%以上。可以预见，短期内数字货币的新流入资金将大大减少。

我们还能列举更多出台限制措施的国家，如哥伦比亚、纳米比亚等等。

可以看到，进入2018年以来，很多国家开始出台限制措施，使得各种加密货币的新买家来源不断受限，引发一系列连锁反应。首先是币值不稳，价格下降。2017年12月比特币上涨至2万美元，而2018年仅仅半年已下跌了一半以上。据统计，全部加密货币2018年以来跌幅已高至50%。另一方面，监管严格、新用户减少、持续亏损，也造成部分加密货币交易中心倒闭。如86bex于2018年6月宣布关闭货币提取通道，与此同时CATTLEEX交易所也宣布无法正常运营，这更加剧了加密货币的币值下跌，形成一个似乎愈演愈烈的恶性循环。

也有很多国家对加密数字货币持观望态度，典型者如澳大利亚。澳大利亚储备银行支付政策主管、经济学家托尼·理查德（Tony Richards）表示，因澳元兑美元长期以来有着稳定的汇率，长远来看加密货币在澳大利亚并没有更大的实际用途，前景发展有限。他很自信地指出，澳元已经持续了25年较低的通货膨胀率，转而采用加密货币的可能性很低，主管机构也认为加密货币不会对澳大利亚的金融体

系造成很大的影响。他同时认为，币值不稳是影响加密货币成为政府选择的除安全问题以外的另一个致命因素，这将导致政府机构怀疑其是否具备成为价值储备手段的特性。

与托尼·理查德观念类似，在比邻而居的新西兰，其储备银行副行长杰夫·巴斯坎德（Geoff Bascand）也表示，尚不能判定政府出台加密货币政策是一件有利还是有弊的事情。看来加密货币的应用前景还待考验，需要进一步向各个怀迟疑态度的国家证明，这项伟大的发明将在人类未来经济活动中占据无可比拟的重要地位。

当然，那些相信加密货币广阔前景的投资者们，也不会坐以待毙。如爱尔兰比特币经纪商Eircoin的联合创始人戴夫·弗莱明（Dave Fleming），就公开对爱尔兰银行与支付联合会（BPFI）提出指责及质疑。弗莱明表示，因为爱尔兰银行拒绝为Eircoin新的二级咨询业务提供服务，导致公司以破产告终。他认为这是一种歧视行为，银行及金融机构无权拒绝为加密货币提供服务；如果加密货币交易存在非法问题，这也是国家法律应该涉及的领域，而非银行和金融机构主导；这项举措与爱尔兰投资发展局（IDA Ireland）所提倡的“拥抱加密货币”态度完全相反，令其十分失望。对于此项控诉，爱尔兰银行及金融机构纷纷否认，表示并没有针对加密货币的歧视性行为，而是部分交易公司自己无法落实反洗钱的监管要求。双方对谁来承担责任莫衷一是，但可以肯定的是，爱尔兰监管机构秉承“积极监管”的态度，既欢迎加密货币的到来及发展，也不愿其造成的弊端影响金融行业正常运转。

不同国家针对加密货币的态度，与其经济政策、金融发展水平、经济理念有着密切的关系。总体来说，我们可以把国家监管分为几种类型。

第一种是完全禁止型，代表国家有孟加拉国、玻利维亚、厄瓜多尔、吉尔吉斯斯坦等。这些国家禁止个人及机构购买、交易、持有加

密货币，也不将加密货币看作真正的货币。

第二种是限制型，也是本节提到的多数国家，如中国、日本等。值得一提的是，日本监管机构对待比特币的态度，前后经历了多次的转变：2014年日本政府决议不将比特币看作正常货币，禁止银行及金融机构涉足，但允许个人持有；2016年对加密货币的支付方式进行监管；2017年官方认可比特币可作为法定支付方式，并取消其8%的消费税；但在2018年又进一步加强了对加密货币交易中心的限制监管。当然，这与加密货币及区块链的发展形势息息相关。

第三种是积极监管型。比如德国，认可比特币用于交易和纳税，定义其为可以用于结算的“私人货币”。

第四种则是不干预型。这类国家一般不限制加密货币的发展，不认为加密货币非法，但也对加密货币的发展进行观察和监控。随着加密货币及区块链的发展，很有可能会转变为以上三种类型。

我们无法对各个国家的监管措施及态度进行评判。必须注意到，加密货币及区块链技术是未来经济发展的一种趋势及可能性，但我们也绝不能忽视其本身固有的弊端，并对其带来的风险及隐患放任自流。

## 第四节 法定数字货币“破冰”

上一节我们介绍了区块链货币化国家监管的四种类型，其中第四种是持最开放态度的不干预型，他们认同区块链货币，较少出台监管措施，部分国家监管机构支持区块链货币化的发展，甚至亲自下场积极参与到这项新技术中。

2018年1月5日，委内瑞拉总统马杜罗（Nicolás Maduro）宣布将发行“石油币”，这是委内瑞拉的官方加密货币，也是全球第一例由国家发行、以国家信用为背书的加密货币。基于此，不少投资者对“石油币”跃跃欲试。委内瑞拉总统马杜罗宣称，“石油币”是一个有效的金融工具，能够实现更自由、更开放、更公平的国际金融体系。事实如他所述吗？我们要从“石油币”发布的经济政治背景谈起。

委内瑞拉是世界重要的产油国之一，其石油潜在储量为2210亿桶，世界排名第五，西半球排名第一，相当于中东地区石油储量的一半。它是石油输出国组织（OPEC）的创始国家之一，目前原油产量占OPEC的10%左右。作为一个石油储量充沛的资源“大国”，委内瑞拉原本可以“躺”在上天赋予的礼物上，轻轻松松过日子——实际上它也是这样做的。据统计，委内瑞拉出口总收入的95%以上来自石油，政府收入的50%以上来自石油，政府判断石油价格只升不降，将国家全部经济重心押在石油产业上。然而2014年突然爆发的国际石油价格暴跌，给了委内瑞拉猝不及防的打击，加上政府前期设计众多大型项目、外汇储备不足等种种原因，委内瑞拉出现了严重的财务危机。政府采取大量印刷货币的方式来弥补赤字，继而引发严重的通货膨胀。截至2017年12月，委内瑞拉累计通货膨胀率高达1300%，而根据国际货币基金组织预估，委内瑞拉2018年通货膨胀率将飙升至13000%。

持续的恶性通货膨胀，使得委内瑞拉人民丧失了对国家法定货币的信任，而委内瑞拉实施的外汇管制又限制居民持有美元等外币，区块链加密货币便成为众多民众的选择。根据委内瑞拉比特币交易平台 Surbitcoin 的统计，从2014年8月到2016年11月，委内瑞拉比特币用户数量从450人上涨到8.5万人。比特币甚至已成为很多民众的日常交易货币——他们使用比特币购买食品、药物等各类生活必需品，用比特币支付薪水。在很多委内瑞拉人眼中，比特币等加密货币是他们的救星，可以使他们的储蓄保值，维持相对较好的生活。对他们而言，选择加密货币不是投资手段，不是政治选择，而是为了生存。委内瑞拉较为低廉且易获取的电力、比特币等加密货币在当地的发展空间，也让许多企业家看到了商机，不少人开始涉足“挖矿”产业。

人们对比特币的青睐，让委内瑞拉政府感受到进一步的危机，他们首先选择的是限制政策，对“挖矿”采取罚款和拘留等措施。2017年11月，当地警方搜查了加拉加斯一对兄弟的住所，查处了超过90个“挖矿”终端。2018年5月，委内瑞拉政府出台了禁止进口加密货币“采矿”设备的禁令，同时限制民众购买涉及“挖矿”业务的电子设备。虽然当地政府允许民众使用比特币等加密货币进行交易，但2018年2月，委内瑞拉 Surbitcoin 交易中心曾因合作银行计划撤销其账户而关闭两周——Surbitcoin 是受当地民众欢迎的加密货币交易中心。种种情况表明，委内瑞拉政府十分担心比特币等加密货币对国家法定货币地位造成威胁甚至是取代法定货币。雪上加霜的是，2018年5月底，美国指责委内瑞拉操纵制宪委员会选举，不断扩大总统权力，正在迈向独裁，因而加大了对其经济制裁的力度，包括禁止美国公民进行与委内瑞拉政府债务相关的任何交易，禁止美国金融机构参与委内瑞拉相关的债券和股权交易等。对于政府正陷入财政危机的委内瑞拉来说，这无疑又是一个重大打击。



正是在法定货币丧失信任、加密货币不断发展、政府财政入不敷出的背景下，委内瑞拉政府提出了这项决议：由政府来发行委内瑞拉自己的加密货币——“石油币”。首批“石油币”将发行一亿个代币，每个代币均以委内瑞拉的一桶原油作为抵押物，由阿亚库乔区1号油田全部储量作为支持，总价值超过60亿美元。但是，“石油币”虽然与原油挂钩，却不能用来兑换石油。“石油币”折算价=石油价格×“石油币”交易所价格×（1贴 现率）。据了解，发行首日“石油币”就实现了7.35亿美元的融资，总统马杜罗还透露，将在委内瑞拉设置挖掘加密货币的“矿场”。

委内瑞拉政府希望通过发行“石油币”来缓解日益严峻的经济危机，并规避美国对其的经济制裁。可惜的是，伴随而来的并不仅是好消息，委内瑞拉政府的部分设想没有实现，美国总统特朗普已签署行政令，下令美国境内禁止购买、交易、使用委内瑞拉发行的“石油币”。同时有人质疑“石油币”销售数据是否真实。鉴于委内瑞拉政府拖欠外债、滥发货币，其信用已经透支，“石油币”是否真的值得信任，政府是否存在欺瞒情况，是否会操纵交易价格？而官方发布的“石油币”白皮书对加密货币所述甚少，对购买途径及方式却言无不尽，也透露出委内瑞拉发行“石油币”醉翁之意不在酒，恐怕不单单是看好加密货币的前景，更重要在于融资。在这样的意图支配下，“石油币”又能走向何方呢？

除了委内瑞拉，还有其他一些国家政府提出了发行加密货币的设想。如以色列政府曾计划发布“数字谢克尔（digital shekel）”，类似的，迪拜政府也设想过加快推进国家主导的区块链加密货币，甚至俄罗斯政府也公开宣布过发行加密货币“加密卢布（CryptoRuble）”。虽然现在只有委内瑞拉政府正式发行加密货币，但各个国家主导加密货币发展的这一天也许并不遥远。

有些同样看好加密货币前景的国家或地区，目前可能没有采取直接主导发行这样看起来似乎较为激进的政策，但也在最大范围内为加密货币的发展开了绿灯。美国亚利桑那州目前就在推进一项法案：允许该州公民使用比特币来缴纳税款。在允许公民使用比特币的基础上可以说是迈出了更大一步，体现了州政府对比特币等加密货币的认可。该法案已于2018年2月在该州参议院获得通过，并被众议院的一个委员会建议通过，一旦最终审核通过，亚利桑那州公民将可以直接用比特币缴纳税费。收到税款后，国税局会按照24小时内比特币兑换美元的汇率，将其换算为美元并计入纳税人账户中。

“这项法案源自选民的呼声。”州参议员、法案起草人沃伦·彼得森（Warren Petersen）表示，加密货币持有人比想象中多得多，其数量足以让人惊讶。这样循序渐进的尝试不失为一个好的方法。毕竟我们不能否认，区块链货币化不仅仅是赶时髦，也不仅仅是一种潮流，它代表的可能是更加透明有序的未来经济世界。

## 第五节 戴上镣铐跳舞：新的探索

2017年9月4日，央行等七部委联合发布了《关于防范代币发行融资风险的公告》，公告明确指出：“ICO本质上是一种未经批准非法公开融资的行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动。”同时公告要求即日起停止代币发行融资活动，已完成代币发行融资的组织及个人应当合理安排进行清退，妥善保护投资者权益，妥善处置风险，等等。

公告发出后，一时之间人人自危，国内多家代币发行项目暂停了相关业务，将视线转向海外，部分代币发行项目及投资者开始在海外挖掘新的机会。这样的事态的产生，主要源于一个信号——相关监管部门将全方位对代币发行加强监管，避免代币发行引发的市场乱象和金融风险。这次公告主要从六个方面入手，从根本上动摇了代币发行的合法性。

一是对代币发行进行了定位，即属于非法公开融资行为。同时明确，对于存在侥幸心理的人，有关部门将依据相关法律法规严肃查处。

二是对加密货币进行了官方定位。公告指出，加密货币不是货币当局发行的，不具有货币属性，也就不享有与货币等同的法律地位，不能作为货币在市场上流通使用。实际上，在2013年12月5日央行等五部委联合发布的《关于防范比特币风险的通知》中，就已经明确了比特币不具有与货币同等的法律地位，这一点只是在此基础上对加密货币定位的范畴进行了扩大，对很多投资者而言并不意外。

但让人意外的是第三点：公告要求代币融资平台不能从事加密货币或者法币与代币之间的兑换业务，不得买卖或者作为中央对手方买卖代币或“虚拟货币”，不得为代币或“虚拟货币”提供定价、信息中介等服务。这是导致众多交易中心纷纷关闭在华业务的关键。

在2013年五部委通知中，还提出作为比特币交易平台的网站需要根据《中华人民共和国电信条例》和《互联网信息服务管理办法》的规定，依法在电信管理机构备案，加强反洗钱义务，防范洗钱风险；同时指出比特币交易作为一种互联网上的商品买卖行为，普通民众在自担风险的前提下拥有参与的自由。

但在2017年七部委公告中，交易中心的合法性已经受到了根本性的动摇，有关部门根据公告要求对相关交易中心进行清理，并要求电信主管部门关闭相关网络平台及移动App，网信主管部门对相关App下架，工商主管部门吊销营业执照，彻底杜绝了部分交易中心违规操作、谋取不当利益的行为。

第四点，也是此次公告中最为关键、最吸引人们注意的一点：明确各金融机构和非银行支付机构不得开展与代币发行融资交易相关的业务。我们知道，代币发行如果想要真正实现金融化并取得公信力，就离不开金融机构的参与。公告要求各金融机构及非银行支付机构不得直接或间接为代币发行融资和“虚拟货币”提供账户开立、登记、交易、清算、结算等产品或服务，不得承保与代币和“虚拟货币”相关的保险业务或将代币和“虚拟货币”纳入保险责任范围，这就将银行、证券、保险全部囊括在内了，可以说完全杜绝了代币交易及加密货币的最大风险。

第五点是向社会提示，要注意防范代币发行融资与交易的风险隐患，避免上当受骗。

第六点则要求金融行业组织加强对会员单位的管理和监督，发挥行业自律作用，加强投资风险教育。

可以说，七部委公告有针对性地抑制和防范了ICO可能引发的投资金融风险，对防止投资者盲目跟风陷入困境起到了积极作用，进一步规范了加密货币市场。

随着公告的发布，各单位也积极行动。先是2018年初中国互联网金融协会发布《关于防范变相ICO活动的风险提示》。提示中指出，虽然各地ICO项目在逐步完成清退，但一种名为“以矿机为核心发行虚拟数字资产（IMO）”的模式又涌现出来，协会认为其存在较大风险，值得投资者警惕，其中典型代表为迅雷“链克”（原名“玩客币”）。同时协会呼吁，对于IMO模式及各类通过部署境外服务器继续面向境内居民开办ICO服务的，广大民众可向有关监管机关或中国互联网金融协会举报，对其中涉嫌违法犯罪的，可向公安机关报案。

什么是IMO呢？拿提示中明确提到的“链克”为例，据玩客云官网所述，链克是玩客云共享计算生态下的基于区块链技术的原生数字资产，用户通过官方平台指定规则获取，并在其创造的特定场景下使用，同时可以在二级市场流通，并在交易过程中获得增值，与加密货币的流通、发售、交易过程极其类似。

2018年1月16日，深交所及上交所也分别发布了公告。深交所称，近期一些上市公司通过公告和互动易App发布了涉及区块链概念的信息，部分公司股票价格涨幅较大，深交所已对17家相关公司采取了问询、关注和要求停牌核查等监管措施，将继续关注利用区块链概念进行炒作和误导投资者的违规行为。上交所也表示将对四类情况采取停牌问询、停牌冷却、澄清说明等监管措施，包括：公司公开披露区块链业务，股价出现连续上涨的；自行发布公司业务涉及区块链，涉嫌“蹭热点”的；业务与区块链有联系，被市场归为区块链概念股，近

期有一定涨幅的；涉及区块链边缘概念股，主营业务为互联网、计算机方向，股价出现一定涨幅的。

一系列的公告、通知、提示，表明了中国对代币发行及加密货币进行监管的方向和尝试。当时人民银行行长周小川在回答关于比特币、ICO相关问题时就指出，央行早就对互联网金融创新进行密切关注，研究新东西是好的，但除了市场的动力，还要顾全全局，比特币等分叉产品出台太快，不够慎重，可能对金融稳定和货币政策传导产生不可预测的作用，在测试不太充分和未获得广泛认同的情况下，可能会出现一些问题。因此政策的方向是不慎重的产品就先停一停，有前途的产品也需要先经过测试再推广。

## 第六节 区块链应用的正确“解题思路”

前文我们分析了以比特币为首的加密货币及区块链技术的前世今生，并重点阐述了各国对加密货币及区块链技术的态度及监管模式，那么对于加密货币及相关区块链应用，政府怎样开展监管才是正确的解题思路呢？这一节我们主要对未来可能会有的区块链应用的监管模式进行探讨。

2018年2月，基于加密货币、区块链技术及应用趋于白炽化，美国国会专门邀请了政府专员、技术专家及区块链应用公司，连续展开四场针对区块链发展及监管的听证会，对加密货币的性质进行探讨，对ICO融资监管进行研究，对区块链技术在政府服务等领域的发展进行展望。

在加密货币的定性上，不同立场的专业人士提出了截然不同的观点。美国证券交易委员会（SEC）主席杰伊·克莱顿（Jay Clayton）认为，加密货币是一种“证券”。的确，加密货币用于筹集资金，具有影响人们投资及做出金融决策、管理金融风险的因素。在这方面，加密货币是在走向证券化。同时他强调，对于任何持有加密货币或与加密货币有关资产的交易中心产品，证券交易委员会均没有批准上市或交易，也没有批准任何代币发行的注册。

美国商品期货交易委员会（CFTC）主席J.克里斯托弗·吉安卡罗（J.Christopher Giancarlo）则认为比特币是一种“商品”，这是依据美国《商品交易法》“商品”的定义。美国众议院听证会主席比尔·惠曾加（Bill Huizenga）持反对意见，他表示数字货币不是黄金，也不是商品。众议员布拉德·谢尔曼（Brad Sherman）的观点更为激进，他认为数字货币就是一场不折不扣的骗局。

直至完成四场听证会，专家学者们对比特币等加密货币的定位也没有达成共识，但即使是最开明的专家，也没有认可加密货币的法定地位，他们还是倾向于认为加密货币与法定货币是不同的。

ICO在日益受到投资者追捧的当下，也成为本次听证会不可避免的话题，特别是虚假或带有欺诈性的代币发行引发的市场混乱和投资失效。对代币发行的融资及监管，各位专家也发表了自己的看法。Coinbase加密货币交易中心的首席法律与风险官迈克·伦普雷斯（Mike Lempres）当然是非常支持和认可代币发行的，他指出，ICO在融资方面有着巨大潜力和作用，目前在Coinbase有近1400种代币项目，但交易主要以比特币（BTC）、以太坊（ETH）、莱特币（LTC）和比特币现金（BCH）这四种数字货币为准。在SEC和CFTC达成协议前，Coinbase是不会支持其他ICO资产交易的。

而针对当前代币发行的乱象，伦普雷斯认为恰恰是由于各个机构对代币权属的定性都比较狭隘，从而导致各联邦监管机构对代币发行监管的协调性不足。现在，国会与其建立新的监管机构和机制，倒不如通过立法界定代币的权属。现有的联邦监管机构的权限及能力就足以实现对代币发行的有效监管。

SEC对此持有反对意见。与对加密货币的看法类似，克莱顿认为当前的ICO和交易平台绝大多数都是违法的，也没有ICO曾在SEC注册过；而CFTC则相对更为开明，吉安卡洛指出代币发行的确促进了区块链技术的快速发展，这与投资者对ICO的支持和追逐是分不开的，在监管方面，政府应对加密货币和ICO秉持“不伤害（No harm）”的监管原则。

乔治城大学法律中心教授克里斯·布鲁默（Chris Brummer）观点与伦普雷斯类似，他指出目前最紧迫的是解决SEC和CFTC之间监管权的分配问题，以及它们的权力是否应深入到加密货币的生态系统中心。



他认为就如证券一样，代币发行机构需要对公众进行充分的信息披露，从而保护投资者的合法权益，避免虚假ICO，信息披露应该在美国《证券法》下开展，并由SEC进行持续的监控。

威尔逊律师事务所合伙人罗伯特·罗森布鲁姆（Robert Rosenblum）从法律法规角度出发，认为在已经运行众多ICO项目的情况下，国会应该尽快考虑修改加密货币相关的法律，以保护投资者的合法权益。立法的目标包括：确定合法单一的监管机构，指导监管机构修改关于代币发行或加密货币的法规文件，建立对加密货币及ICO的全面监管体系。

货币中心研究总监彼得·范·凡尔肯堡（Peter Van Valken-burgh）也认为目前美国各州对加密货币及ICO的分散管理，非常不利于对投资者及市场的保护，建立统一的监管才能减少各州之间的贸易壁垒。同时他认为比特币和以太币是虚拟商品，而其他区块链资产是证券，在监管时应做区分。

通过各位专家学者的阐述，我们可以看到，目前基本上所有专家都认为加强监管并建立统一监管机构和监管模式是非常必要的，现阶段分散管理的情况导致管理权限划分不清，反而容易造成无人监管。另外对加密货币的性质应该尽快立法明确，建立起完善的监管机制。

针对区块链技术的发展及应用，听证会主要倾听了沃尔玛食品安全与健康副总裁弗兰克·扬纳斯（Frank Yiannas）对应用区块链技术实现食品可追溯化的介绍，他也对区块链技术立法监管领域提出了种种建议。扬纳斯说明，现在沃尔玛已经开始应用区块链技术对供应链进行管理，能够对食品从原产地到出售的全供应链进行追踪，消费者可通过区块链技术获取食品的相关信息，增加食品从生产到售出全过程的透明性，使企业能更好地获取消费者信任并确保全供应链的安全，从而帮助沃尔玛建立一个透明、高效、安全的食品供应体系。

IBM公司区块链技术副总裁柁纳罗·杰里·科莫（Gennaro Jerry Cuomo）也认可区块链技术是一项颠覆性、变革性的创新技术，IBM目前也在考虑区块链技术的合作，并与多方洽谈。他希望在立法的时候，政府能够将区块链技术与加密货币、ICO进行区分，对区块链技术在其他领域的应用加以鼓励。

马士基集团全球贸易数字化部门负责人迈克·怀特（Mike White）更加认可区块链在安全方面的作用，他认为区块链技术可以提高供应链系统的信息安全，提升信息的可获得性，从而使各个行业在信息数字化中发挥更大的潜力。

美国国会研究服务部政府和财务部网络安全政策分析师克里斯·A·凯卡兰（Chris A.Jaikaran）指出，区块链技术不仅可以应用在商业领域，也可以应用于公共服务领域，促进政府效率的提升。在此基础上，政府可以加深区块链技术的理解，并将其应用于对其他领域的规范和指导。

美国国土安全部科学技术理事会网络安全事业部主任道格拉斯·莫恩（Douglas Maughan）同样认可区块链技术对公共服务领域的改造，认为其可以进一步提升公共服务活动的透明度。

UPS全球海关经纪副总裁克里斯托弗·卢比奥（Christopher Rubio）进一步指出区块链技术对跨国公司管理的推动，通过区块链技术可以提升管理效率，并有效保护知识产权。他希望政府能够尽快出台区块链技术标准，同时与其他国家进行标准的统一互换。

本杰明·卡多佐法学院副教授、区块链项目主任亚伦·赖特（Aaron Wrigh）指出，基于区块链技术正在广泛领域进行应用的事实，法律法规监管已经迫在眉睫，政府可以建立全面的监管框架来对区块链技术

进行指导和限制。鉴于区块链技术对各行业的革新，赖特希望政府和技术上持中立的态度，着重于建立良好的法律环境来保护消费者。

对区块链技术，与会专家的观点方向基本是一致的，即认可区块链在供应链管理、公共服务等方面的积极作用，同时希望政府能够出台统一标准和法律框架，在对区块链技术进行管控的同时，指导和支持相关企业在区块链技术的帮助下，提升生产运行效率，促进社会管理革新。

作为区块链技术全球领先的国家，美国此次听证会的研讨，可以说代表着区块链技术、ICO、加密货币在未来监管及应用方面的前进方向。在谁来监管、监管什么、怎么监管成为许多国家对区块链及相关技术的疑虑时，此次听证会也提供了一部分解题思路。正如中国人大金融科技中心主任杨东教授指出，不能简单认为加强区块链监管就是利空，厘清区块链与监管之间的关系，从长远来看反而是一种利好。

监管绝不是一蹴而就的，而是要不断随着区块链技术及应用的发展进行调整，以“技术驱动型”监管来应对区块链应用中可能产生的各类问题。

An abstract graphic on the left side of the page, featuring a complex network of interconnected circles and lines, resembling a molecular structure or a network diagram. The circles vary in size and are shaded in different tones of gray, creating a sense of depth and complexity. The lines connecting them are thin and dark, forming a web-like pattern that extends across the left half of the page.

02

中国错过了芯  
片，还会错过  
区块链吗

## 第一节 比云计算革命更猛烈的冲击

在互联网高速发展近20年的今天，人们对互联网不断涌现新兴技术不再感到陌生，从社交网络、移动App、O2O（将线下商务机会与互联网结合的一种商业模式）到大数据、物联网、云计算……不断有新的互联网技术及发展模式横空出世，为互联网行业的发展带来巨大的飞跃和革新。同时，每一项技术都不是孤立的，都站在“巨人的肩膀”上——依靠前一阶段互联网技术及理念的发展；这些技术彼此之间还能够相互协作，持续深入进化。区块链是近几年才广为流传、被人们追捧的互联网技术，而上一个受到此待遇的是云计算。因此，在了解区块链之前，我们也要对云计算进行剖析，从而明确区块链技术在云计算的基础上又将为人类社会的变迁带来怎样的影响。

什么是云计算？通俗来讲，它提供了一种可以替代用户在本地自建服务的虚拟化网络服务。具体来说，云计算相当于在网络上建立一个信息中心，当人们使用这项服务时，可以直接通过网络从信息中心调取、存储自己所需要的资源，而不必在自己的设备上开展相关工作，从而节省了资源，提高了效率。

我们可以举一个简单的例子：当一个人处理自己的视频和照片资料时，按照传统的方法，他需要先将视频照片等资料上传至本地电脑，在本地电脑中安装视频照片处理软件，然后利用软件开始各项操作。使用云计算服务后，视频照片资料将在网络中存储——而非电脑硬盘，他可以使用手机轻松调取各种资料；同时，他处理这些照片和视频时可以直接运用网上的视频照片处理技术，不需要再在本地电脑上下载软件。这就是云计算的本质。

故此我们可以说，云计算实质上是将互联网技术从以设备为核心，转变为以信息为核心的过程。这样带来的好处是：对个体来说，大大方便了用户的网络体验，仅用一台设备，就可以享用不同类型的应用，降低了个体用户的互联网成本。以前，上网是少数人的专利，毕竟要购买一台电脑，需要有足够的金钱，也需要有足够的空间。而移动网络+云计算技术，让个体用户只用一台手机就能实现自己的需求。对企业用户而言，有了云计算技术，可以不用再购买实体计算机或配置庞大的机房，甚至不用再聘任运维人员以维持设备的有效运转。这一切均可以用云服务的租赁费用来代替，可以说大大解决了企业运维的资金问题，有助于中小企业的成立和发展。成百上千个企业汇总在一起，对社会资源的节约来说也是一笔不小的数目。我们在看电影《钢铁侠》时，总是羡慕钢铁侠有极其强大的计算机分析支持，有随时可放大缩小的虚拟电子屏幕，而这一切都依赖于云计算技术。

除此之外，云计算还具备存储空间不受限制、促进用户相互分享协作、提升计算机运行效能等众多优势。

因此，云计算领域也成为互联网巨头们的“兵家必争之地”，毕竟它代表着互联网的明天，抢占成功就意味着未来将财源滚滚。云计算行业的正式兴起，可以追溯到2006年AWS（亚马逊旗下云计算服务平台）的发布，10余年的发展，使得云计算行业已成为一个较为成熟的互联网领域，众多企业通过云计算技术，获取了长远的发展和丰厚的回报。微软财报显示，微软智能云（Intelligent Cloud）2018年第二季度业务营收77.95亿美元，较去年同期的67.58亿美元增长了15.3%；其中旗舰产品Azure取得了98%的增长，而云服务平台的利润更是接近30亿美元，接近70亿美元利润的一半。这也证明了微软将重心转向云计算和物联网来代替曾占据这个位置近30年的Windows的举措非常正确，更可见云计算的前景之广阔。而亚马逊目前主要的营收来源，早

已被AWS以73%的比例牢牢占据，不得不让人感慨亚马逊转型之准，云计算全球排名第一的服务商果然名不虚传。

云计算虽然有以上种种好处，但其弊端也十分明显：第一就是安全问题，云计算建立了一个共享的环境，所有服务器都联入互联网，带来的弊端就是一旦遭遇黑客袭击或存在安全漏洞，就有可能导致数据损失和泄露。这也是云计算最核心的问题，如果不能够妥善地予以解决，就无法获得用户的信任，也难以进行更深层次的推广和应用。第二就是性能问题，云计算的实现依赖于用户接入网络设备的稳定性，同时云计算有大量用户的连入，意味着需要高效的信息处理技术，而作为一个中心式的集群服务模式，一旦中心服务器出现状况，将使云计算提供的服务大打折扣。另外还有相互协作的问题，现在市面上的云计算服务平台有很多，如何实现平台之间数据的相互协作？这需要平台之间有智能化的协议，对信息数据的提供做出定义，才能更好地为用户服务，实现畅通无障碍的计算机虚拟化。

而针对以上问题，区块链提供了解决的思路。

从安全性上来讲，云计算的安全仍然属于传统网络安全的范畴，更多考虑的是运行的稳定、可靠；而区块链的安全性，我们在之前的文章中已经探讨过，在没有密钥的情况下无法破解信息使得信息和数据的安全得到了极大的保障。因此区块链技术 with 云计算技术相结合，可以推动其安全性能方面的大幅提升。另外，区块链录入的数据是无法擅自篡改的，这也可以为云计算所用，对每一个记录的数据信息设置哈希值，将哈希值记录在区块链上来对应云计算平台上的实际数据信息。当有人想要篡改记录时，就会导致其对应的哈希值发生变化，无法匹配区块链上的哈希值，从而被管理器禁止，避免数据被篡改。这样可以大大拓展云计算的服务领域，一些涉及隐私的法律、协议、

合同等，以及一些需要确保完整性的数据内容，也可以被安全地储存在云计算平台上。

在信息和数据的管理模式上，两者也有很大的区别。云计算是中心式管理，依靠集群服务器的集中管理；但区块链的特点就在于去中心化，每一个节点都是独立的，通过底层的自发驱动来进行数据传输、存储和计算，从而也不需要一个集中式的服务器来进行统一的计算、调度。所以当云计算服务将区块链技术纳入其中时，可以有效解决性能上的困境，也更有利于云计算服务的稳定性。

另外，区块链特有的智能合约模式，可以帮助不同云计算平台之间进行信息共享与相互协作，在此就不做更多阐述了。

当然反过来说，云计算也对区块链技术的发展及完善做出了贡献。从成本上来看，云计算有着低成本、高可靠性、易调整的特点，有助于一些中小企业快速、低成本地应用区块链技术。通过云计算与区块链的技术结合，区块链可以借助云计算在众多领域发展的经验，在其驱动下进一步拓展应用领域，加速自身的发展。

与大数据、物联网等技术一样，云计算与区块链都是互联网技术发展的更新阶段，区块链技术的发展与成熟离不开以上新一代互联网技术的基础和铺垫。区块链不单单是一种技术，更提供了一种服务模式和解决方案，为互联网产业的进一步发展起到了极其重要的推动作用。



## 第二节 巨额投资下的中国区块链技术

互联网时代有一个著名的“飞猪理论”：“如果站在风口，一头猪也能飞上天。”这是互联网创业者兼投资人雷军2014年底在微博上提出的概念，这一理论迅速引爆互联网，成为人们推崇备至的“名言”。可以说，这些年互联网行业的发展，使得很多人一直在追寻风口，试图成为一头赶上潮流甚至超越潮流的“猪”。当然，软硬件技术的发展也是互联网技术日益进步的一大助力。确实，有很多人凭借敏锐的洞察力和大胆的行动力，成为互联网行业的新贵。从商务到社交，从消费到金融，“互联网+”改变了一个个行业领域。那么到了2018年，互联网的“风口”又在哪里呢？答案自然是区块链。

随着共享经济和云技术的发展，人们逐渐发现，人类社会迫切需要一种去中心化、分账式的数据管控模式，使得它成为一个可信任、高度透明的公众账本，并因其不可随意篡改、不能轻易抵赖，形成多边互信的机制，从而解决“互联网+”最大的风险——信任问题。

这个“风口”现在有多火？一组数据来告诉大家答案：截至2018年4月，国内经营区块链的企业超过320家，累计融资高达89亿元，仅仅在2018年第一季度就完成了63亿元融资，融资次数达106次，远超过2017年水平。将国内“20强”投资机构的投资项目按行业分类，其中区块链平台类项目占了44%，大部分投资在私募甚至是更早阶段，区块链项目为投资人带来了超百倍的回报。2018年中国区块链最大的一笔融资来自中国平安旗下的“金融壹账通”，它获得了思佰益（SBI）和IDG资本高达6.5亿美元的投资。连美国加州大学伯克利分校计算机系的教授宋晓冬，也对区块链的火热程度不无感慨：“几年前我曾在学校开设过区块链的课程，听者寥寥无几，影响不大，大家并没有显露出对这门学科的兴趣；而2018年当我再次开设这门课程时，大家热情高涨，

课上座无虚席，每4名申请这门课程的同学中，只有一个人能被选上。”可见如今区块链正经历热潮，备受资本及从业者的青睐。

这得益于区块链技术广阔的应用场景。对普通人而言，区块链似乎仍仅仅与加密货币联系在一起，是加密货币的衍生概念。经历了2017年七部委联合叫停ICO融资，加密货币行情大受打击，区块链也随之遭受牵连，饱受争议。实际上，这是对区块链技术的误解。区块链并不是仅仅应用于加密货币，而是可以应用在支付场景、金融交易、物联网通信、信息安全甚至公共服务等众多领域，因其能够解决不同个体组织间的信任危机问题，有着广阔的发展前景和空间。因为“币圈”与区块链在概念上被许多人捆绑在一起，随着加密货币概念大热，部分不法分子趁机炒作、恶意募集ICO，才使得区块链与非法投机被联系在了一起。而国家实施的加密货币“降温”政策，有助于将加密货币和区块链这两个概念区分开来，让人们意识到区块链在“互联网+”时代的重要意义。

区块链可以为实体经济提供服务，比如它可以协助溯源。众安保险的养鸡场应用区块链技术，在400只鸡的脚上安装识别器，对鸡的生长情况进行实时监控和溯源。消费者可以通过此项技术，追溯这只鸡吃了哪些饲料、做了哪些运动、走了多少路、活了多少天。这些信息是完全公开透明的，因为区块链技术决定了其不能被篡改。浪潮集团也在应用区块链技术为茅台酒提供溯源服务，实现对茅台酒全生命周期的跟踪，追溯每一瓶酒的生产过程、供应过程和销售过程，从而有效地帮助消费者鉴真。

区块链有效实现了现实生活的数字化，可以作为一项生产资料。正在建设中的雄安新区，就有这样一个设想——将全部的租赁产业搬到虚拟数字世界中。房东的房屋信息经房产局公证后纳入区块链平台中，租客中介的合同信息也分享到区块链平台上，通过房东、中介、

租客的三方信息数据协同，打造有效的数据共享机制，避免黑中介、虚假房源、二手房东和违规租赁的存在，为政府对房屋租赁市场的高效管理提供了基础和保障。

区块链可以升级生产关系。比如将商家的会员积分以数字形式保存在区块链上，从而实现线上线下交易的无缝隙链接，实现多场景的交易和兑换。三星也在考虑打造货运区块链技术，通过区块链监控全部产品的运输。这一系统将把三星全球范围内每年价值几百亿美元的产品全部囊括在内，预计每年将节省20%的运费。

区块链甚至可以推动公共服务领域的发展和进步。一方面，由于具备不可篡改、透明和公开等特点，区块链技术非常适合公益募捐，人们可以在网上监控募捐资金的全部动态及去向，有助于募捐资金在全社会范围内得到有效监督，避免其中可能产生的贪腐行为及信用危机；另一方面，它也可以提高公共服务效率。2017年贵阳市政府就已经在政府信息公开、互联网金融监管、小微企业认证、精准扶贫等领域运用区块链技术，以提高办事效率，并实施有效监督。

前景是光明的，但道路是曲折的。虽然拥有众多应用场景，但区块链目前仍在发展的初级阶段，远未成熟，这体现在被投资项目多处于发展初期。据链塔智库统计，2018年3月底，被投资的区块链项目中占比最多的是天使轮（64%）和A轮（25%），两者之和高达总量的90%，其他阶段的投资仅占10%。这也显示出了区块链投资领域的隐忧——高质量的、值得多轮次投资的项目不多。

底层技术是限制区块链发展的一大难题。将现实世界搬移至网上，看起来容易，实际操作并不简单，需要具备极强的数据计算能力，才能实现服务的稳定。提升每秒同时交易次数，是区块链技术目前的最大障碍。毕竟，最热门的比特币，每秒交易仅能达到7笔，距离现实交易数量还是太远了。当然，此项技术障碍已经在攻克中，据韩

国三星公司透露，其区块链技术已达到TPS（每秒系统处理次数）2000次；而VISA更是称其TPS达到5000～8000次；迅雷正在研发超级区块链，交易速度可达百万级TPS。依据摩尔定律，大规模工业化区块链技术的应用，已然离我们不远了。

同时，区块链技术也面临着跨链技术和隐私保护的问题。不同区块链之间是需要交互沟通协作的，特别是交易方众多、交易内容复杂的情况下，如何实现多维度、跨链甚至是多链的无缝交互，是一个难题。好在2017年建立的多维度直接交互架构，解决了这个问题的基本框架。区块链是信息透明化、去中心化的，在此条件下，如何保护隐私数据，也是人们很关注的一点。让人欣喜的是，这点可以在技术上得到解决——通过设置一个条件，将涉密数据和非涉密数据区分开来，将涉密数据放到特殊空间进行加密，然后运用加密合同实施有条件的访问，从而避免隐私的外泄。

除了底层技术，顶层设计也是限制区块链技术发展的另一个因素，即缺少必要的技术标准体系。区块链专家、威睿（VMwave）首席架构师张海宁表示，没有技术标准，区块链的应用和推广就会受到限制，缺少驱动力。数据安全标准、数据存储标准、客户身份识别，这些必要的限制标准在区块链发展中起着重中之重的作用。在没有第三方权威公正的监管时，只能靠行业自律，各利益相关方共同努力约束。这样，不仅标准的范围广度会受到限制，不利于区块链的交流整合，而且由于出台过程中缺少权威机构，效率也会大打折扣。政府监管也是相关专家的共同呼声。虽然中国几部委曾两次联合发布政令加强对区块链货币化的监管，但在区块链的综合法律监管上，与其他国家相比仍较为落后。幸运的是，中国互联网金融协会2018年的一项重要工作就是推进区块链技术的标准化体系建设，相信能够一解区块链标准体系落后的燃眉之急。区块链的大规模应用虽然为时尚早，但已

在征程，相信在不久的将来，我们可以享受到区块链技术带给我们的革新与便利。

### 第三节 区块链未来中国的蓝图

基于区块链的众多应用领域及被世人看好的发展前景，无论是企业、投资者还是政府，都投入极大的热情积极参与到这个“风口”中，以避免在区块链技术上有所落后而痛失发展空间。

据统计，截至2018年3月底，中国区块链公司已达到456家，正处于高速增长阶段，其规模效应已初步显现。对排名靠前的20家区块链公司进行分类可发现，其中13家专注区块链技术发展，致力于区块链底层技术及基础设施、软硬件环境和平台的构建，占比高达65%，为区块链产业高速发展奠定了技术基础；另外7家则专注应用层面，包括阿里巴巴、腾讯、京东等几家互联网巨头，主要将其应用于商品溯源；也有不少金融服务业的企业，如中国平安、中国银行、招商银行，主要将其应用于金融创新……区块链的应用场景正不断实现丰富化和立体化。

具体来看，各公司对区块链的应用都与本公司业务特点紧密结合——金融公司主要将区块链技术与金融业务深度融合，如中国银行和招商银行将区块链应用于票据和清算这种传统金融领域，中国平安则主要应用于黑名单及供应链领域。

从地域来看，我国的区块链企业主要集中于北上广等一线城市。根据工商注册信息，约有42%的区块链企业在北京注册，数量处于遥遥领先的地位；约22%在上海注册，也符合上海金融中心的地位特征；约有16%的企业在广州及深圳地区，约9%在浙江地区，这与长三角、珠三角发达的商品经济有一定相关性；另11%分布于全国其他多个二三线城市。可见，区块链企业目前较多地出现在经济发展活跃的地区。

其中，上海具备先发优势，是最先引入区块链概念和应用的地区。而浙江省政府已经将区块链的发展纳入政府工作报告中，杭州市政府更明确提出要打造区块链第一城，出台了各项优惠政策，为区块链在杭州的落地提供了巨大的政策扶持。目前杭州已有60余家区块链企业，包括较早成立的区块链媒体巴比特、数据交易所公信宝、底层区块链技术供应商趣链等，创造了良好的区块链创业氛围，企业质量较高，发展蒸蒸日上。

从行业来看，中国区块链企业主要集中于金融及企业服务行业。金融相关企业占比高达80%以上，重点包括加密货币业务、供应链金融业务、清算支付业务。企业服务则主要关注为企业提供数据支持，如溯源系统、电子存证服务等。从行业跨度来看，覆盖的领域还比较狭窄，发展处于初期阶段。当然，也出现了数据交换服务等利用区块链发展的新兴模式，但仍在探索阶段。

从融资角度来看，区块链企业融资进入高速发展期，投资人对区块链的兴趣较为浓厚。据统计，2017年区块链企业融资金额是2016年融资额的两倍，2018年仅第一季度融资额已接近2017年半年的融资额，且出现众多A轮单次融资超过1亿元的“独角兽”公司。融资的重点领域仍是金融业，2016年开始，区块链融资已超过移动支付、P2P等“明日黄花”，成为当之无愧的“当红炸子鸡”。不过正如前文所述，目前融资仍较大比例集中在种子轮和A轮。

从技术上来看，目前我国区块链专利技术拥有量及专利增速均为世界第一。2015年开始，我国区块链专利技术增速达到200%，领先于全球，是我国目前增速最快的专利领域。不仅如此，全球前100名区块链技术企业中，中国企业占比为49%，比美国高了16个百分点，阿里巴巴更是名列第一。但中国区块链技术企业主要集中于央企，其中典型代表为中国人民银行数字货币研究所，在全球排名第三。

虽然没有形成巨头企业，但不少区块链企业专注技术，发展势头较猛，典型如众链，是一条致力于解决大规模电子化存证的区块链存证联盟链。电子化存证，是对数据的主体信息、环境信息、过程信息进行搜集、厘清、存档和调用的过程。其中存在两个“痛点”：一是我国法院对电子数据的采信标准和认证手段没有明确规定；二是电子数据有后期改写的可能性，无法作为有效凭证，形成完整严实的证据链。众所周知，区块链的一大特点即不可篡改性，故通过区块链技术的有效应用，能够解决数字凭证先天不足的问题。针对司法鉴定，清华大学电子商务交易技术国家工程实验室、北京众签、广州仲裁委员会、中国物品编码中心、普华永道等多家机构建立了中国区块链基础保障联盟，共同搭建了众链，致力于一站式解决数字凭证司法落地的问题，对仲裁、司法鉴定、审计机构等相关单位进行整合，实现了数字凭证到司法鉴定的直接转换，有效解决了数字凭证司法鉴定的“痛点”。

我们可以通过电子合同的存证来看看众链是如何解决这一难题的：

当双方需要签订电子合同时，首先由北京众签（第三方电子合同、电子签名服务平台）提供符合国家规定的身份认证，然后由证书授权中心提供数字证书，接着客户可以基于自身需要，选择共有云、私有云等多种电子证书签订方式，北京众签再利用加密算法提取双方数字指纹，将其以哈希值的形式存储在众链上。需要注意的是，每一个数字指纹都有唯一的哈希值，从而避免了混淆。众链将通过7个权威节点储存这些信息，并向双方出具查询接口，一旦出现有人篡改电子合同的情况，将无法通过原有的哈希值，也无法保存在众链系统里，从而从根源上确保无法对电子合同进行改写。众链对电子合同进行存证保管，设定访问查看的权限，并引入第三方监控，审计机构、仲裁机构、司法机关、鉴定中心则可以通过其进行取证。



使用众链存证区块链至今，众签区块链电子合同已为近千家企业、1000多万人提供电子合同业务，日签署量峰值达到100多万份，签署总量突破1亿，为用户节省管理成本超过40亿元。

区块链技术还在大数据、供应链金融系统等领域落地开花，本节就不一一介绍了。可以预见的是，区块链技术在未来将和每个人的日常生活息息相关，这一领域出现“独角兽”或巨头企业也是未来发展的必然。因此阿里巴巴、腾讯等众多互联网巨头纷纷布局区块链，将其作为一项长远战略，不断深挖其潜力。

不仅在企业领域，在社会公共服务领域，区块链技术也能起到十分重要的作用。例如佛山禅城区从2017年6月起就运用区块链技术为居民提供各种公共服务。我们知道，个人身份信息在网上泄露，是当前社会的一个“痛点”。互联网在为人们的生活提供便利的同时，也潜伏着一个隐藏的“杀手”，觊觎着人们口袋里的金钱，如层出不穷的诈骗行为、非法盗用身份开展违法行为等。这也让人从侧面可以理解，为什么一些保守的中老年人不愿意使用网络，毕竟无论是上网购物、社交媒体还是咨询缴费，提供个人身份信息都成了一种必要。怎么避免我们的个人身份、银行账户、联系方式等敏感信息泄露或被盗取，成为对企业及政府的一项重要考验。而区块链技术提供了一种与传统网络安全技术大相径庭的手段。

佛山禅城区使用的是IDHub区块链数字身份技术，其工作原理为设置身份自主权、数据安全、个人隐私、资产性四个维度。身份自主权是保证个人对数据修改、删除、恢复、授权的自主权利，用户可以自行选择授予机构个人身份的权限。个人隐私维度是将隐私区分为较低和较高级别的不同层级，级别较低的身份信息可以留存在公共网络上，级别较高的隐私信息则只留存在用户个人设备上，实现了公开和隐私的双重身份体系，建立了链上加链下的管理模式。

禅城区目前有约130万名用户使用此系统，利用IMI（中国人民大学国际货币研究所）身份认证系统，将居民身份信息与各项社会公共服务相连，用户扫码登录即可取得权限，在线上完成费用缴纳、社保查询、交通信息查询、预约挂号等多项行政业务，大大提高了办事效率；同时各部门可以通过公证书轻松提取居民储存的个人信息，快速完成核查认证，减少了沟通取证难的问题。居民在线办理无犯罪记录、社保记录、出生证明等，仅需一个小时，加速了“可信化数字”进程。

从中可以看出，政府角度加大对区块链的扶持力度也是十分必要的。2018年5月工信部出台《2018年中国区块链产业白皮书》，可以看出政府对区块链技术发展的重视。工信部也明确提出要进一步加大对区块链产业的扶持力度，完善区块链标准体系。这标志着中国政府正从国家和政策层面督促区块链技术落地开花、创新升级。

中国的区块链技术发展还存在基础技术有难点、应用场景不多、发展较为初级等一些问题。在这个新兴领域中，我们还在路上。2018年6月30日，“2018年首届中国区块链应用场景峰会”在北京召开，这次峰会由近百名区块链技术专家、行业精英、资深投资者参加，深入讨论区块链在公共服务、物联网、供应链金融等众多领域的应用及发展。我们有理由相信，中国信息技术的5.0时代，在以区块链为核心的技术升级背景下，将很快到来。

## 第四节 中国“区块链+”的应用趋势

区块链技术诞生于比特币，然而区块链却不是单单为比特币或者说加密货币服务的，它有着广阔的应用范围和发展前景。这一点我们已经从区块链的技术、特征、作用乃至应用案例等多个维度做了解释，以改变人们长久以来“区块链=加密货币”的刻板印象。区块链作为第四次科技革命的核心技术，被众多国家和企业所重视，并投入大量资源进行布局以占据先机。那么区块链技术将结合什么样的场景，应怎样进行布局，未来趋势如何？我们就通过2016年的《中国区块链技术和应用发展白皮书》，对中国“区块链+”应用发展趋势做一个展望吧。

近年来，无论是联合国、国际货币基金组织还是各个有条件的国家，纷纷发布关于区块链发展的报告，对区块链技术研发及应用进行系统的剖析与解读。2016年，根据工信部的委托，中国电子技术标准化研究院联合万向控股、蚂蚁金服、微众银行、平安科技等互联网金融企业，先后收集了20多项国外文献资料，研究了200多个相关案例，完成了《中国区块链技术和应用发展白皮书（2016）》的编纂制定，完成了对区块链技术及应用的系统化研究。其中指出了6种典型区块链应用领域及场景，并明确规划了我国区块链发展的标准化路线图。

白皮书指出，区块链将主要应用于6个场景：金融服务、供应链管理、智能制造、公共服务、教育就业、文化娱乐。

区块链的可追溯性及不可篡改性，与金融行业的天生本质及需求恰好完美地结合到一起，这使得区块链在金融服务领域的应用是目前为止最为深入、相对成熟的。在支付领域，区块链技术可以有效解决不同金融主体之间的对账问题，从而起到降低成本、提升效率的作

用；对于跨境支付而言，区块链可以通过去中心化技术，实现点对点的交易记录，从而解决现有第三方支付介入的情况下，跨境支付链条多、成本高、效率低、耗时长现状，助力普惠金融的实现。在票据及结算清算方面，区块链的去中心化技术避免了中心服务器瘫痪导致整个交易市场无法使用的风险；通过区块链加密货币实现点对点的实时对接清算，从而降低成本，缩小结算清算的周期；其透明性也解决了目前存在的票据造假及“一票多卖”现象。

在资产数字化方面，区块链技术可以实现线下资产向线上资产的转移，所有交易行为均在线上发生、记录，从而避免了线上线下两个途径无法验证的问题；另外各类资产全部整合至区块链中，确保了资产数据的真实化和规范性，各方可以不再借助中介，直接发起交易，解决交易主体多、环节多、交易不透明、信息不对称的问题，化解了各方对资产数据准确性的信用危机。

区块链还可以应用于证券领域，实现证券交易的智能化。证券交易基于一系列相互达成的规则和协议，区块链以代码形式对这些规则和协议进行保存，推动协议的自动履行，并通过逻辑确保其符合法律规范的要求。同时我们还可以对数据进行设置，确保交易行为只有双方可见，避免向第三方泄露。

在金融领域最重要的客户身份识别方面，区块链可以快速高效地对客户身份进行甄别验证；同时，运用数字化的身份管理，可以有效地对客户金融交易进行跟踪，也可以解决不同金融主体之间身份信息和交易信息难以有效对接的问题。

供应链管理上现在面临的主要“痛点”有两个：一是供应链主体较多，不同主体之间交互的行为和信息很难有效整合在一起，信息不透明、分散化，导致一旦发生风险，各环节难以把握事情的全局及存在的问题，对供应链系统的效率产生较大影响；二是主体多、信息分

散，使得各环节的可追溯性差，在主体之间出现纠纷时，追责变得愈加困难。区块链技术则可以协助将供应链整合成一条完整的信息流，不同主体可以全面地探测各个环节中存在的问题，数据的不可篡改性、时间性也能够为主体之间发生纠纷时提供可靠的证据链。

区块链对供应链管理的促进，可以广泛应用于各实体行业中，如前文中提到的养鸡场。养鸡场建立的可追溯记录确保消费者能对鸡的每一个生产环节进行检验。我们还可以不断发散思维，任何需要追溯时间线的商品，都能够采取区块链技术，解决生产者相对于消费者的信息不对称问题。比如我们十分关注的药品生产，通过区块链技术建立药品的身份记录，药品生产的全周期就能够时刻处于监控之下，一方面节省监督成本，另一方面提高效率，减少生产过程中的人为事故。

公共服务领域的区块链应用，我们在介绍佛山禅城区居民服务时已经做了详细的阐述。除此之外，区块链还可以完美解决公共服务领域的信任危机问题。我们都知道，慈善事业的长期发展与人们的信任支持是分不开的，一旦人们对某个慈善项目有所怀疑，投了反对票，慈善事业就无法取得社会资金，实现预定的成效。人们迫切地希望知道，自己捐赠的金钱、物品流到了哪里，是否满足对方所需，是否达到了应有的效果。同时人们也好奇，慈善组织在其中起到多大的作用，是否履行了诚信职责。而区块链可以将捐赠明细、机构成本、受益对象、资金流向等信息，在保护隐私的情况下进行公示，提升了公益的透明度。更进一步升级的话，区块链还能有效地将被捐助人群的需求与捐助者进行高效对接，从而提升慈善事业的针对性和专业性。

在传统的生产过程中，区块链可以有效采集分散在各个环节的数据，通过数据分析将孤立的生产环节有机结合在一起，帮助简化流程、评估预期、降低成本、安全运营。区块链在智能制造方面的一大

应用就是与物联网结合，这一点我们将在本章第五节中进行详细的阐述。

教育和就业对区块链技术的利用，则主要体现在学生信用体系的建立和知识产权保护方面。企业在聘选人才时有一个难以跨越的难关，就是如何判定这个人是否符合企业特质的、企业需要的人才。短短的几次面试，很难对个人的能力水平有一个全面的把握。实际上，企业招聘往往靠“猜”，设立几个指标，对方表现出类似的特征，便选拔录用。这样的后果是企业很有可能选错人才，把不适合的人放在岗位上，这也是对人力资源的一大浪费。学生信用体系就是一个解决办法，可以实现学生、教育机构和企业无缝对接，使企业获得学生就学阶段完整有效的信息，从各个维度判断对方是否合适。对此系统进行进一步的升级，可以建立产学结合的系统，使学生在学校获得的技能便能满足企业的需求，增强教学的实操性和针对性，避免封闭办学、闭门造车。

知识产权方面，则可以借助区块链的共享性和不可更改性。对每篇论文建立以哈希值为基础的数字凭证，确保用户信息和论文的一致性，将论文信息上传至区块链中。每一次查询时，都智能触发校验机制，并留存可追溯记录，从而避免恶意侵犯知识产权。

对于文化娱乐，区块链也能解决电影、音乐等具备知识产权的作品频频遭遇侵权的问题。与文字化的文献相比，可视化的娱乐产业知识产权，更存在举证难、维权成本高的难题。利用区块链的哈希值确保每个视频、音频的唯一性、真实性，后续一旦有任何交易、转移等行为，都能被区块链实时记录，为后续的司法验证提供基础。比如在音乐产业，创作者可以对作品的传播过程进行监控，从而获得版权报酬，甚至可以绕过发行商，直接在区块链上发布音乐，避免侵权现

象。区块链也可以将文化产业链上的各个环节进行有机整合，拓展文化项目生命长度，缩短价值创造周期。

以上就是白皮书中对区块链未来应用6个场景的设想，也是我国未来区块链应用的发展方向。在加密货币领域的规模化应用以外，其他领域的应用也正处于探索甚至是快速发展阶段。腾讯发布的《腾讯区块链方案白皮书》就认为未来区块链将在金融、物联网、公共服务、供应链、公益慈善这5个方面迎来发展。据2018年麦肯锡官网消息，世界经济论坛大胆预测，到2027年，世界10%的GDP将存储于区块链上。

## 第五节 区块链+物联网的无限可能

物联网这个词你一定不陌生，它被称为“世界信息技术第三次浪潮”，其发展前景及空间被人们津津乐道。物联网，顾名思义是指实现物物连接的互联网技术，是运用互联网技术将信息交换及流通拓展到物品与物品之间的过程与系统。物联网的实现最早可追溯到1990年施乐公司的网络可乐售卖机。1999年，美国麻省理工学院的凯文·阿什顿（Kevin Ashton）首先提出物联网概念。

具体来说，物联网是指利用信息传感设备，实时收集各类需要监控、管理、连接、交互的物品过程性信息，从而实现物品与物品、物品与人的网络化信息连接。目前其应用模式主要有两种：一是通过智能标签来识别对象，这是基于NFC（近距离无线通信技术）、二维码等技术实现的；二是基于云计算和智能网络，加强对物品的智能控制，如根据车流量调整红绿灯时间间隔、根据温度调整室内大棚供水量，等等。

物联网用途广泛，涉及公共交通、公共安全、环境监测等各个领域。专家预计，物联网将是下一个推动世界经济发展的引擎，能够提供一个万亿级的巨大市场。然而，物联网的发展目前还面临着众多难题：一是中心控制需要巨大的成本，物联网将所有信息数据汇总到统一的中心枢纽，中心枢纽需布置大型服务器，承担巨大的成本压力；二是隐私保护的问题，近几年摄像头被网络直播的事件屡见不鲜，数据汇集到中心枢纽的过程中，很容易出现隐私泄露的问题；三是网络暴力攻击，美国曾发生僵尸物联网入侵摄像头，感染超过200万个摄像头的事件，设备入网后很可能成为系统暴力攻击的对象；四是通信兼容层面上，全球并没有统一的物联网标准及平台，而是存在多个竞争性的系统标准及平台，物联网之间的通信存在障碍；五是协同成本



高，物联网参与者可能包括个体、企业、机构等多方主体，如何低成本实现多方协作，是一个现实的问题。

而区块链的介入，为物联网以上问题的解决提供了一个渠道。首先，区块链+物联网，能够实现成本的降低。运用区块链技术后，无须再布置信息中心枢纽，节约了巨大的设备成本，也避免了后续昂贵的运营维护费用。其次，加强隐私保护。区块链所有传输的数据都经过系统加密处理，可以确保用户的个人信息更加安全。第三，能提供身份鉴别的权限。区块链的验证和鉴别机制，可以避免非法入侵等网络暴力行为，为设备的安全提供保障。第四，可证明性及可追溯性。数据被纳入区块链后无法更改，同时可以对数据实施有效追溯。第五，可以实现跨主体的协作。区块链可以低成本地建立互信机制，打破不同主体间信息的屏障，促进多方之间信息无障碍地流动。

另外从商业角度来看，区块链与物联网的结合极大拓展了双方的发展空间和商业价值。区块链带来的信用保证，使人们可从物联网采集到最真实、也最有价值的数据，并对数据综合利用，推动各行业算法及商业模式的发展。其次，实现进一步的经济共享，让终端设备不再是简单的设备，而是能够提供数据、参与互动的主体。在区块链参与下，可以打通不同设备主体之间的信息沟通屏障，促进闲置资源的共用，从而获得共享经济利益。

举例来讲，区块链可以建立智能化合约，租赁双方通过智能化合约实现交易，出租者可以获得租金，租赁者可以获得设备的使用权限。

2018年10月26日，由平安城科与乐山市住房保障和房地产管理局合作研发的“乐山市房屋租赁平台”在四川省内率先上线运行。该平台借助人脸识别、大数据、区块链等前沿科技，打通了城市房屋楼盘数

据，通过房源核验码机制、电子合约、中介信用管理等技术手段，可以高效实现房源验真并支持抽查复审，三重保障确保房源真实性。<sup>[6]</sup>

各物联网巨头纷纷开始布局区块链产业。2016年8月微软区块链服务正式面世，向Azure云平台用户开放；2016年10月，IBM推出了Bluemix云平台的区块链服务；同年，GE（通用电气）和爱立信合作，在GE Predix云平台上提供以区块链技术为基础的数字指纹认证服务；2017年4月，思科（Cisco）开始研究用区块链对设备标识进行登记处理……根据物联网软件平台数据显示，IBM、GE、微软等占据物联网主导地位的企业，均加强了对区块链领域的研究及应用。

除了物联网企业，初创公司及传统企业也加强了区块链+物联网的布局。初创公司主要涉及分布式能源系统、新型交易模式、新型交易市场等区块链领域，扩展了物联网硬件产业形态，如区块链平台Solar Change出台了太阳币（SolarCoin）<sup>[7]</sup>，太阳币代表太阳能发电量，通过太阳币交易实现能源的线上交易。传统企业则主要加强与初创公司的协作，通过买下初创公司技术、成立子公司等方式，使其为自身提供能源系统和交易平台，例如建立可再生能源的区块链交易试点。初创公司与传统企业的协作，不断推动区块链与物联网的双向驱动。

从整个行业领域看，区块链和物联网结合，可以打造多种垂直行业的生态格局。拿电力行业来举例：首先，运用加密货币装备支付终端，加密货币代表电力供应资源；在此基础上建立能源的交易市场，通过加密货币的自由流动和交易，实现能源在不同个体组织间的高效转换；接着，智能家居点对点交易，实现资源从货币形式到家具用电的自动化供应；最终，技术支撑加上行业支持，实现智慧城市。

另外，区块链+物联网的国际标准，也处于不断的探索之中。2017年3月，中国联通就联合众多公司及研究机构，建立了物联网区块

链项目标准。这是全球首次提出标准化的双网联合机制，为去中心化的物联网平台框架奠定了体系基础。

综上所述，我们看到区块链可以被称为物联网的主干基础。据估计，到2020年，每个人身上的联网装置平均将在6.58个以上，这使得区块链的介入成为必然，实体世界将进一步与数字世界同步。再举一个例子，电动汽车处于高速发展阶段，但人们发现充电成了老大难问题。不同公司充电桩接口不同，交易方式不同，好不容易找到一个充电桩，却可能存在无法接入或难以支付的问题。为了解决这个难题，德国莱茵集团（RWE）与德国区块链初创公司Slock.it合作，创造性地将区块链和物联网技术结合起来。他们在每个充电桩上安装了Linux系统，把不同公司或个人的充电桩通过区块链连起来，当有人需要为电动车充电时，可以使用适配各家充电桩接口的设备。在区块链平台上充值缴费后，费用会被划转到相应的电力公司账户中，从而实现了物联网平台的有效搭建。 [8]

未来，基于区块链及物联网技术的共享制度会越来越多，区块链+物联网无疑将是下一个“风口”。

## 第六节 哪种区块链技术更具人气

区块链技术引发了新一轮的互联网热潮，前文我们已经介绍了很多区块链技术的应用，那么迄今为止，哪种区块链技术更具人气呢？

答案可能让人意想不到。DappRadar是一款显示区块链交易情况的网站，它会实时更新区块链应用的线上交易数量、总额及活跃人数，其排名在一定意义上显示了各区块链应用的人气。在DappRadar2017年的排名中，排名第一的是IDEX。IDEX是以以太坊加密货币为基础的加密货币交易中心。它使用以太坊去中心化交易，建立了一个智能交易平台，支持实时交易及一次多笔交易。作为一个智能合约系统，IDEX可以存储所有线上资产并记录交易情况、执行交易结算。目前IDEX加密货币交易中心货币种类不断增多，交易量已超过一些著名的交易中心。

第二名是ForkDelta去中心化数字资产交易所。ForkDelta日前发展迅猛，大有赶超第一名的趋势。这要归功于DAGT（Digital Assets Guarantee Token，基于以太坊公有区块链技术和智能合约技术实现去中心化的数字资产质押授信平台）的成功登陆。DAGT是全球首家区块链数字资产质押授信平台，其强大的技术优势、利润共享的理念、独特的运营模式，使它成为受到投资者追捧的冉冉新星。与其他区块链加密货币不同的是，DAGT追求的是区块链技术开发。它以解决用户在区块链中遇到的金融服务问题为导向，致力于用区块链重新定义数字资产贷款领域，获得了多家业务机构和专业人士的认可。DAGT在追捧下价值不断提升，仅在交易所上线首日就暴涨了60%，交易量也随之持续上升。它的独领风骚，为ForkDelta用户活跃量带来了十分重要的影响。

CryptoKitties 紧随其后，排名第三。让人大跌眼镜的是，CryptoKitties不是加密货币，也不是交易中心，而是一款所谓的“云吸猫”游戏——人们可以在游戏中养殖、繁育及交易电子宠物猫。这款游戏基于以太坊平台运行，以太币是唯一交易货币。特点在于每一只电子猫都是独一无二的，可以通过外观、特性、特征等来区分。两只电子猫交配生育的小猫基因，均由电子猫各自的256个元基因组遗传而来，理论上有40亿种可能性。CryptoKitties上的电子猫价格，均由卖家自己决定，但CryptoKitties团队称，他们将每15分钟制造一个新品种的电子猫，其价格是最后5只电子猫平均价格的150%。

为什么CryptoKitties团队会想出这样一个创意呢？让我们来看看它带来的影响。CryptoKitties一经上市，便成为推动以太币交易的幕后推手，仅仅在2017年11月200名玩家的封闭测试阶段，CryptoKitties就上榜成为以太坊网络上排名第三的智能合约，其产生的交易链占以太币交易量的2%。据统计，CryptoKitties上线以前，以太坊排队交易量几乎从未超过5000笔，自CryptoKitties于2017年12月3日上线后不到一个月的时间内，待交易量急速上升，12月4日升至1万笔，到12月5日便突破了2万大关。截至2018年8月，CryptoKitties游戏平台已成交了200多万只电子猫，交易额高达330万美元。可以说，以太坊近期的异军突起，这款“云吸猫”游戏功不可没。

然而，CryptoKitties的出台并不仅仅是为了促进以太币的交易和推动以太坊的壮大，而是为了在结合爱“吸猫”人士喜好的基础上，向普通人推广区块链技术。前文我们曾经提到，对于普通人来说，一提到区块链，脑海中浮现的就是加密货币，区块链和加密货币在概念上紧紧结合在一起。这带来一个弊端，就是大众对区块链技术的认识不足，对区块链技术的推广和普及造成了一定的负面影响。在这种情况下，CryptoKitties以游戏的形式让普通人能够在无形中接触到区块链技术，这源于它虽然没有设置加密货币，但电子猫是由区块链技术来决

定所有权的。这款游戏的火爆，使它吸引了更多的目光。2018年初，CryptoKitties被拆分为独立公司，安德森·霍洛维茨（Andreessen Horowitz，一家位于硅谷的风投公司）和合广风投（Union Square Ventures）领头对其进行了约1200万美元的融资，它可以被称为区块链游戏当之无愧的No.1。

排名第四和第五位的分别是EtherCraft及EtherBots。它们同样是区块链游戏。是的，你没有看错，目前最火爆的5个区块链项目中，区块链游戏占比高达60%，看来纯粹投资带来的乐趣，还是无法企及“娱乐+投资”带来的乐趣，也许成人就是在玩着看起来更高端游戏的“孩子”罢了。EtherCraft同样在以太坊上运行，是一款典型的RPG（角色扮演游戏），其目前的乐趣主要在于购买、收集区块链游戏上的武器、装备和道具。虽说是购买，但玩家无须支付任何费用，而是以游戏内货币XGP交易，收集主要是通过打开战利品箱子获取。另外，游戏中还有第三个获得手段，即通过特定配方制作物品——玩家可以用分解物品、获得原料、再合并物品等形式，得到属于自己的新装备。同时为了奖励早期玩家，EtherCraft开发团队设置了一个规则：如果新玩家购买相同的道具，前期购买的玩家可以获得一定比例的分红。EtherCraft是一款可以通过浏览器访问的视频类游戏，其中包含了大量的视频因素。开发团队表示，未来将继续开发使用这些装备、道具来进行探险的活动，同时他们制作并展示了探索和战斗的画面，并预告将以iOS和Android两种形式发布，以满足不同玩家的需求。目前在DappRadar上，EtherCraft成交量为180万笔左右，如果开发团队能够尽快上线新的功能，谁能说一场新的EtherCraft热潮不会席卷而来呢？

EtherBots则是由澳大利亚弗格森（Ferguson）兄弟团队开发的机器人区块链小游戏。它以组装机器人战斗为主题，玩家购买机器人配件，对配件加以整合组装，就可以得到属于自己的机器人了。玩家可以升级机器人，也可以选择参加比赛进行战斗，有点类似现在大热的

《铁甲机器人》节目的网上游戏版本。同时玩家还可以对机器人进行交易，交易及购买方式仍然是以太币。这款游戏因其新颖性也是万众瞩目，仅仅在预售阶段就成交了3900多个机器人，合计约500万元人民币；如今在DappRadar上的交易量更是达到1135万元人民币。

这就是当前国际上最受欢迎的5个区块链技术。我们可以看到，区块链游戏的行情日益火爆。那么就国内而言，最热门的区块链项目又是什么呢？

排名第一的是量子链，是实现比特币和以太坊两大生态“币圈”兼容的智能合约平台，旨在通过与合作伙伴和第三方，共同形成一个智能合约枢纽系统，为供应链、物联网等行业提供智能合约服务。排名第二的是HSP（Hash Planet Chain，哈希网络自由价值流通系统），即超级现金Hcash的代币发行。根据Hcash白皮书的介绍，“Hcash是分布式去中心化账本系统，运用零知识证明、双向加密、即时通信等技术，整合各独立区块链”。项目代币发行8400万人民币，代币流通量为4200万。排名第三的是共享链加密货币（ShareChain），第四名是公信宝加密货币交易中心，第五名是NEO智能经济区块链。

通过对比可以发现，中国较为热门的区块链技术主要还是加密货币和交易中心，区块链技术的整体发展与部分优势国家相比，还有一定的距离。

## 第七节 “空气币”对区块链信任层的侵蚀

什么是“空气币”？这源于2017年各类加密货币价格大涨。在利益的驱使下，国内投机者出台了这样一些加密货币——货币背后没有任何实体项目，也没有任何资源作为支撑，且不会在GitHub上发布项目代码开发的进度，甚至部分加密货币的背后没有任何公司支撑，发行者全靠欺骗设立一个虚无缥缈却“高大上”的前景，来吸引投资者投资此类货币。在积累一定的投资客户后，便溜之大吉或人为操纵价格，从而谋取不当利益。这就是所谓的“空气币”。

“空气币”实际上就是借区块链概念来实施的经济诈骗。它一般具备以下几个特点：主要运用发行者的名声、资源或者背景来进行宣传，而不传播其实际技术情况，没有任何的技术路线图；十分重视营销，过分看重币值的涨幅，对一夜暴富大书特书；流通主要靠拉人头、发展下级的形式，或者以充值会员、购买挖矿权益的形式，不会提供实际“挖矿”的渠道和途径；加密货币不能在交易中心进行交易，只能在特定平台，同时不能自由提取；宣传只涨不跌，其涨幅与技术进步、项目开发没有任何关系。在这样的情况下，基本可以断定它是“空气币”。

举个例子来说明：

某个购物平台出台了一种购物币，投资者可以通过购买一定数量的网上物品，或者发展其他消费者投资购物币获得；同时此购物平台宣称公司网上销售情况良好，利润不断增加，公司即将上市，购物币届时就可以变现，并使投资者获得巨额利润。其实这就是传销组织利用区块链的“外衣”，在开展传销欺诈活动。



随着区块链货币化的发展热潮，想搭上这班车的人越来越多，使用歪门邪道手段的也不少。被人们称为“中国比特币首富”的李笑来，曾直言币安等虚拟货币交易所是“骗子”。他指出，只要有流量和技术，谁都能开虚拟货币交易所，好像开博客一样，找个域名就可以了。区块链技术的共识价值，在很多地方变成了炒作。当然，币安也很快进行了回击，其创始人何一在微博上直言：“骗子看谁都像骗子。”

这样一场“币圈”里的相互攻讦，看起来像是一场无头无尾的闹剧，但它也的确揭露了“空气币”的存在，将此种行为暴露在蓝天下。不仅仅是“空气币”在“割韭菜”，个别加密货币交易中心也开始“变质”。大量加密货币上市，使得交易中心越发强势起来，向发行商加收“上市费”的情况屡屡得见。见此情景，不少投资机构不再投资加密货币，反而转型成为加密货币交易中心。

2018年1月，博彩游戏平台“英雄链”发行了号称全球首个支持博彩游戏的加密货币，发行后即刻跌破发行价，由0.6元跌至0.05元。2018年2月，“艺术链”因虚假宣传，发行人不得不进行代币回购，以1：1的比例开展退市，网站下线关闭。2018年3月，“太空币”涉嫌投资欺诈，被公安机关立案侦查，其曾经仅用1天就私募到了10亿元……一个个“空气币”倒塌的背后，是一批批被割得体无完肤的“韭菜”。

为什么人们会相信“空气币”？主要是因为人们对区块链货币化的了解并不全面，很多普通投资者根本不理解区块链技术及发展，只能通过加密货币的宣传包装甚至是站台人来判断投资方向；另一方面，国家也缺乏行之有效的监管，加密货币的涨幅不仅可以依靠技术、前景，资本鼓动也能够实现货币价值大增。特别是对发行量较小、总额度较低的加密货币，资本所需操作资金更少，操作的空间也就更大，这也引发了资本制造“空气币”的可能。

另外有一些人，明明知道投资的是“空气币”，却怀有极大自信认为自己不会成为最后一波“韭菜”，反而积极投资，成了发行者的“帮凶”，只求在涨到高点时能够卖给其他“接盘者”。

2017年2月，新加坡共享单车品牌oBike成立，仅仅半年后就获得了4500万美元的B轮融资。然而共享单车融资风向在2017年底骤转，很快资金就被共享单车项目烧完了，又没有新的投资进入，于是项目创始人石一将目光转向了当时大热的加密货币。2018年1月，由Odyssey项目发行的OCN加密货币在6家交易所陆续上市，Odyssey对外号称是由oBike共享单车团队创立的区块链项目，将发行40亿枚代币，自发售之日起6天内就被超额认购，累计募集金额达到4亿元人民币。而这些资金并没有流转 to oBike开展业务运营。OCN的成功发行让石一尝到了甜头，他自己也称，“2017年最伟大的事情就是发现了ICO（首次币发行）这台印钞机，一个项目赚几亿，还不用纳税”。在OCN之后，石一又先后“发行”了CNN、DATx、SAY，3个月内连续以相同的方法发行3种加密货币，涉及资金高达7.28亿元人民币。针对外界的“割韭菜”“跑路”言论，石一表示自己并非货币直接发行方，而是股权投资者或战略投资方，没有直接参与到货币发行之中。然而经过部分人的梳理发现，石一与此4种加密货币的发行方有着千丝万缕的联系。这些加密货币是怎样躲避投资者的“火眼金睛”的呢？主要操作流程包括如下几步：

首先要打造一份具备吸引力的白皮书，有传统股权投资机构或新兴区块链投资机构的背书，当然如果能两者兼具是最好的。投资者在选择时往往会有趋同性和盲目崇拜，他们更认可有大机构背书的加密货币，却忽视了这些机构背书的根本原因，或者忽视这些背书是否是真实的。拿DATx来举例，白皮书中的投资机构显示有晨兴资本、创世资本等传统股权投资公司，然而这两家公司实际上并没有投资DATx加密货币，而是投资了石一的另一个股权项目DotC，也就是说DATx加

密货币白皮书存在错误的信息，刻意打造众多投资机构青睐的表象，诱导投资者。在不知情的情况下，晨兴资本、创世资本等投资公司为其作了背书。同时项目其他环节也要看起来“高大上”，比如项目顾问选择外国人，看起来要十分专业；项目官方网站要用全英文，再标明无第三方销售，投资者须通过官方加密货币交易中心购买，以显示其正规性及规范性。

其次，发行私募，确保上市。在加密货币交易中心上市有个前提条件，就是要满足交易中心的上市费用。据统计，想要上市至少要准备3000万元以上的资金，而这意味着加密货币的上市极其依赖私募筹集情况，私募完成越快，筹集资金越多，越有利于加密货币在交易中心的发行。这也很好理解，对于“空气币”来说，发行加密货币就是“割韭菜”，“韭菜”越割越少，因此越快上市越好。另外要发动媒体进行造势，10万元一篇“软文”已然成为“币圈”公开的秘密。

最后，就是开始“割韭菜”行动。庄家下场进行币值控制，先将币值拉高，再缓慢砸盘，逐步收割韭菜；然后在币值到达一个低点后，发动媒体造势宣称币值被低估；接着迅速拉高币值，让投资者看到币值的急速提升，继而新一波韭菜再次涌入市场。这时庄家就可以再进行一场大收割了。

“空气币”严重扰乱了加密货币市场的交易秩序，操纵者将加密货币看作一种新型的传销手段，对区块链的发展造成了极大的负面影响。采取政策介入、第三方监管、行业自律等种种手段已势在必行。

An abstract graphic on the left side of the page, featuring a complex network of interconnected circles and lines, resembling a molecular structure or a network diagram. The circles vary in size and are shaded in different tones of gray, creating a sense of depth and complexity. The lines connecting them are thin and gray, forming a web-like pattern that extends across the left half of the page.

03

**区块链 + 金融：  
重构传统金融  
业的“戏法”**

## 第一节 中国金融业将首先拥抱区块链

2018年6月27日，第十二届上海金融服务实体经济洽谈会暨论坛在上海世博展览馆正式拉开帷幕。本次金洽会由上海金融业联合会和上海各金融行业协会、各区金融办共同举办，旨在促进互联网技术与金融业的进一步交流协作，助力金融业的深化改革和发展创新。引人注意的是，本次金洽会特别设置了区块链主题，并邀请众多区块链企业及服务组织参会，如北京天德科技有限公司、Alphacat等。我们可以看到，金融业拥抱区块链的趋势已经成为业内的共识。

这种趋势已经不是第一次显露了。众所周知，区块链技术被视为是继蒸汽机、电力、互联网三大技术发明后的下一个颠覆性技术，将引领第四次科技革命的浪潮。近年来，传统银行因为互联网金融的强势碾压、人们支付习惯的改变，已经承受着巨大的压力，在此情况下，传统银行业迫切希望革新，以打破自身局限性带来的枷锁，突破互联网金融建立的壁垒。区块链技术随之进入银行的视线。

在前一章我们已经阐述过，金融行业是最先应用区块链技术的领域，同时也是目前区块链技术发展最迅猛和成熟的领域，加密货币和代币发行就是典型的例子。为什么区块链技术会最先获得金融业的拥抱？这与区块链技术对传统金融业的积极改造有关。它能够改变传统金融业中存在的不足，尤其是解决效率与安全之间的平衡问题。这一部分我们将在下一节里进行详细的叙述。

总之，对于传统金融业而言，区块链技术就像给了它一个弯道超车的机会，让它与互联网金融能够站在同一起跑线上。传统金融业在连续几年的行业阵痛后，终于迎来了一个赶超的机会，这让我们可以理解为什么金融业对区块链技术如此寄予厚望。

据统计数据显示，2017年全球范围内有14%的金融机构进入区块链市场，虽然随后出现了一些地区金融机构退出的情况，但是这种趋势并没有逆转。这对金融业结合自身业务特点应用区块链技术和直接投资区块链服务行业起到了推动作用。而到了2018年，这个数字有增无减，据估算将有91%的银行投资区块链行业。

我国银行业也在2016年就开始了对区块链技术的尝试，并且取得了良好的效果。2016年1月20日，中国人民银行数字货币研讨会宣布数字货币研究取得阶段性成果。中国人民银行行长周小川出席会议，副行长范一飞主持会议。会议肯定了数字货币在降低传统纸币发行、流通的高昂成本等方面的价值，要求中国人民银行数字货币研究团队积极吸收国内外数字货币研究的重要成果和实践经验，在前期工作的基础上继续推进发展，建立更为有效的组织保障机制，进一步明确央行发行数字货币的战略目标，做好关键技术攻关，研究数字货币的多场景应用，争取早日推出央行发行的数字货币。<sup>[9]</sup>

据“2017全球区块链企业专利排行榜”显示，中国央行数字货币研究所等我国3家银行相关机构2017年区块链专利技术申请量为66件，区块链在货币方面应用的专利技术居2017年全世界银体系第一。这些尝试涵盖了票据、支付、资产托管、数据安全等众多领域，覆盖了从央行到五大国有银行，从股份制银行到互联网银行等众多机构。其中较为突出的仍是部分大中型银行，如中国工商银行建立了区块链与生物识别创新实验室，将区块链的应用主要放在“智能合约+共享账本”一体化机制上。实验室通过不懈努力，于2017年12月上线了面向金融应用的区块链基础技术平台和生物识别平台，从而实现了对客户身份快速精准鉴别，并申请了8项专利。此技术成功应用于工商银行与贵州省政府合作搭建的脱贫攻坚基金区块链管理系统，成为首个服务于精准扶贫的区块链平台。其他银行还有许多令人耳目一新的创新，我们将在本章第七节进行详细的阐述。

除了银行业，保险公司也纷纷开始对区块链技术布局。2016年3月阳光保险率先推出的“阳光贝”积分，就是采用区块链作为底层技术架构；2016年7月，易安保险协同慕尼黑保险建立了“区块链保险实验室”，以期对区块链技术在保险行业的应用进行探索；2017年3月，泰康保险与人保财险分别推出了基于区块链技术的积分管理平台及养牛保险项目；2017年9月，上海保交所正式发布区块链底层技术平台保交链.....越来越多的保险企业将目光聚焦至区块链应用上。

“10年前，谁也无法预料到互联网与移动互联网对今天的影响。同样，10年后区块链对我们生活的改变也一定将远超此刻的预想。”正如众鼎集团董事长张哲仁在2018年金洽会上的致辞，区块链技术在金融业领域的应用还不够深入，还面临着技术成熟度不足、合规标准不统一等众多问题，金融领域的区块链应用还有更长的路要走。但毫无疑问，区块链技术在金融领域的成功已令人看到它的潜力，更多创新型企业将涌入这一领域，挖掘更多的可能性。

## 第二节 解决安全与效率的平衡问题

对金融业来说，引入区块链技术将带来很多益处。金融的本质是融通资金，传统金融机构更像一个金融中介，为资金需求方与供给方建立起一个互通有无的桥梁，促进资金的有效流动，实现价值最大化。然而传统金融存在一定的弊端：信息的不对称性，造成传统金融业效率较低、成本较高，资金流动贵、慢、难；其提供的标准化金融产品无法根据企业生产经营规律研究企业的资金需求，从而无法提供个性化的金融服务。

区块链技术的加入可以有效解决以上问题。一方面区块链具有去中心化、去中介化的特点，能够打通信息壁垒，畅通资金供求双方的沟通渠道；另一方面区块链特有的智能合约系统，可以建立资金双方的信任，精简金融活动的步骤，从而起到提高效率、降低成本、减少风险的作用。它类似于一个交通枢纽，当我们建成一个十字路口时，一个时间内只有两个方向可以通车；但一旦建成一个上下纵横的立体交通体系，可以通车的通道就变得四通八达，也就不会再出现资金累积、效率低下的情况，使资金能找到最高效的应用方向。

区块链对金融业的改造，主要体现在四个方面，分别是：验证客户身份、资产数字化、支付清算一体化和法规重构。

首先，验证客户身份是出于金融安全、反洗钱的需要。传统金融业需要对客户身份、资金来源、资金流向、客户业务及风险等多个方面进行审核，同时对客户资金使用情况进行跟踪，导致审核时间长、审批速度慢、耗费精力多等弊端。而我们知道区块链技术具备数据信息不可篡改、透明的特点，这就确保了信息的共享与安全，从而减少客户身份核验的环节。



其次，资产数字化是在信息时代逐渐普及的，它有效提升了社会效率，但在目前的运行模式下存在的问题是：一方面客户对机构存在信任疑虑，不愿意将全部资产信息暴露给相关机构；另一方面，资产数字化是有边界的，脱离了边界范围，机构之间就会形成信息壁垒，像一座座孤岛，很难实现交流互动。而我们知道区块链的特点就在于去中心化，通过智能合约系统将不同金融机构纳入统一的数字平台，可以消除边界，实现资产信息的自由流动。

再次，就支付清算来说，中国的支付清算体系主要是由央行来主导的。虽然微信、支付宝促进了移动支付系统的欣欣向荣，实现了全球第一的移动支付普及率，但移动支付背后的清算系统并没有太大的改变，是一种资金在各支付机构内滞后流转的模式，实时交易系统与对账系统在短期内是分离的，很容易造成效率低下。举个例子来说，小明购买了淘宝某商家的商品，在使用支付宝系统结账时，资金流动方向为“买家银行—买家支付宝—线上支付—卖家支付宝—卖家银行”。在账面上，双方能够看到资金已经流传，但实际上，背后却要在央行清算系统的指导下完成各个银行之间的清算，才算是真正实现了资金的流动，而这一环节是落后于账面的。

区块链解决了这一难题，人们每次交易后，就利用加密货币来代表实际发生的金额，智能合约系统可以实时转变加密货币的所有权，从而实现清算支付的一体化。在这种情况下，清算系统可以不再依赖央行，避免了滞后的清算过程，使交易环节的风险更加可控，也提升了支付效率，更避免了跨行、跨境之间高昂的手续费，可谓一举多得。

最后，在使用区块链进行金融交易后，金融运行的模式将发生极大的变化。这意味着现行的金融运行规则、法律标准、监管方式都不再适用。在这种情况下，区块链技术的引入起到了“倒逼”的作用，推

动国家及相关机构出台适合区块链技术应用的金融业标准体系，持续建立完善的相关法律法规体系，从根本上杜绝现在的乱象，使监管体制跟得上技术发展。

从业务类型上来看，区块链技术对银行、证券、保险、基金都能够产生巨大的价值，推动其产业升级。作为最大、最传统的金融行业，银行的业务可以分为资产、负债和中间业务三个类别。负债是指银行的资金来源，包括存款、借款业务等；资产是指贷款、投资等管理运行资金的业务；中间业务是指结算、清算、托管、担保等在资产和负债之外的业务，涉及范围比较广。银行主要承担着金融中介和资金来源的角色，这就意味着其核心在于解决信用问题，银行要确保客户身份的规范性和真实性，从而防范风险。大银行背后有国家信誉或政府背书，辐射范围较广，故大银行的客户较多且较为复杂，这导致客户身份认证核验更为繁杂；而中小银行个性化及针对性较强，却缺少强有力的背书及较大规模的客户，面临着融资难及信用评级标准不完善的问题。区块链可以建立起一套可共享、效力高的客户身份核验体系，对大银行来说能够大大简化审核步骤，提高审核效率；对小银行而言建立了统一的信用评级标准，同时也解决了融资难的问题。另外，银行也可以通过区块链实现清算支付一体化，将清算业务变为实时开展，不必再花费大量精力投入到清算业务中，转为对各种加密货币的管理和交易。

证券公司的业务包括以下几种：以中介代理的形式，帮助投资者买卖证券，从中赚取一定的佣金；通过承揽、承做、承销等模式，为客户开展直接融资业务，帮助客户筹集资金，实现企业的IPO（首次公开募股）；接受客户的资金委托，帮助客户进行投资，承接资产证券化方向的金融业务；另外还有利用自有资金进行证券买卖、接受投资咨询业务、为买方机构提供研究报告等其他业务。

区块链技术可能会改变证券的发行方式。根据国家证券管理相关要求，如果一个公司想要发行证券，必须先通过证监会审核，然后在二级市场发行，最后才能够进行公开的股权交易。代币发行可能改变这一流程，因为它实施的是先发行后审核流程，能使市场上的融资形式产生很大的变化。当然这一条只是为证券发行提供了一个未来蓝图和思路。随着七部委共同文件的下发，国家对代币发行的严格管控，这一流程可能会有所变化，但流程的简化效果是有目共睹的，证券业务也可能随之转型。

另外就是前文提到的资产证券化。区块链可以实现信息数据的共享，使得融资方对一套账本数据进行统一维护，节约了各方进行信息交流和清算结算的时间。另外如股票、债券的买卖都是在证券交易所进行，期权、期货这些较为复杂的证券则有专门的交易所开展交易买卖，区块链技术可以利用加密货币及智能合约，实现证券的自动交割，支付清算一体化，也能实现简化交易清算流程、提升交易效率的效果。同时对一些非传统型的、比较复杂的证券交易来说，区块链技术可以替代律师或者交易所的介入，使得交易更加智能化。如美国Overstock公司的目标，就是希望用去中心化的区块链技术来取代华尔街对美国金融行业的垄断。让人震惊的是，SEC对Overstock在自己创建的市场上进行证券发行、交易，采取了认可的态度，这可以看作是SEC对未来证券交易的一个设想和一种尝试。而中国也于2016年成立了中国账本计划联盟，其成员包括省级的股权交易所、大型的商品交易所等。

保险，我们每个人都耳熟能详，对其业务也十分了解，就是在发生意外时，人们能够根据之前与保险公司签订的协议得到及时有效的帮助。其核心业务包括产品、服务和资产的管理。虽然近几年互联网保险开始兴起，但经营模式并没有任何变化，只是将线下业务转换形式放到了线上。而区块链技术在保险领域的应用则不同——保险行业

同样可以应用于对客户身份的核验，各公司共享并维护同一用户身份账本，可以减少投保人身份验证的时间和环节，从而也提高了保险业务的办理效率。基于区块链的不可篡改性，投保会有明确的记录，从而避免了骗保或欺诈行为。同时保险契约也可以应用智能化合约体系，从而对保险产品实现个性化的设置，保障投保者权益，提升服务体验。

另外，区块链在保险行业中有一个特殊的应用——相互保险。它指的是当单位或者个人有类似的保障需求时，可以签订合同成为相互保险的会员，缴纳一定数额的保费形成互助基金后，利用互助基金对合同约定发生的情况进行赔偿和保障。与传统的保险形式相比，互助保险有以下几个优点：它是投保人有着类似保障需求的情况下形成的，因此各方的利益一致，是由全部投保人共有的；因为是共有的，没有其他外部股东，也就没有盈利的压力，相应经营成本低、费用低，可以为投保人提供更加优质低廉的保险服务，也会将组织全部的资金和精力放在投保人的利益上。相互保险在国际上应用较广，2014年全球相互保险业务收入高达1.3万亿美元，在全球保险市场的份额中占27.1%。但在中国因为政策的限制，相互保险基本没有开展起来。2016年，一些保险公司在保监会的许可下筹建了首批试点单位，处于发展的初级阶段。

对相互保险的性质进行剖析，我们会发现它与区块链技术有着许多相似之处——都是去中心化的形式，都是先履行合约后开展业务的形式。但恰恰因为这一点，相互保险面临着基因上带来的漏洞——信任问题。没有有效的手段对契约履行进行约束，就无法实现真正意义上的相互保险。区块链技术的智能合约体系及数据不可篡改性，可以帮助相互保险解决这一个问题，建立起相互保险的信用机制，使其回归保险业互助的本质。

最后我们再来看一下区块链技术在基金行业的应用。通常，我们将基金划分为公募基金和私募基金，主要涉及非上市企业的投资业务。简单来讲就是通过收购股份、参与公司决策、开展风险运作抑或直接开展企业管理，使企业增值的过程。

但在传统的基金投资过程中，投资者、基金运营人及被投资企业之间存在严重的信息不对称情况，投资者本身对企业经营状况不了解，信心不足，会影响被投资企业的融资进程，也使得交易的流程复杂、步骤较多，大大降低了基金投资的效率。区块链技术则可以帮助在三者之间建立一个有效的信息沟通平台，同样是利用区块链技术的透明性和数据不可篡改性，帮助投资者深入了解企业，树立投资者对企业经营的信心，确保投资的高效运行。另外，智能合约体系可以帮助募集资金、签订协议、自动履行退出机制，提高基金投资的效率。同时，代币发行也为基金投资提供了一个发展思路，有可能改变传统的私募投资体系。

### 第三节 “无须可信第三方”的世界

前文我们已经阐述过，区块链技术建立了“分布式账本”，避免对信息和数据的篡改，同时也保障了信息的可追溯性，任何特定交易都有据可查，确保了公正性及透明性。另外，区块链还具备共享及自动化的机制。以上几点结合在一起，我们可以说区块链建立起了点对点的互信机制，相当于“干掉了”第三方，实现了去中介化，打造了一个“无须可信第三方”的世界。而这一点对金融行业的冲击及革新最为关键。这也让我们理解了为什么今天金融圈内人人都在谈论区块链。

传统账本主要是以集中的形式出现的，有一个可信的第三方机构充当集中清算和担保的角色，账本的可靠性主要依赖第三方可信机构的信用和技术，一旦第三方中心机构出现数据被篡改、损坏等无法修复的问题，金融系统将遭受巨大的危机。而区块链技术恰恰符合去中心化这一要求。

全球银行业是一个价值134万亿美元的巨大产业。它帮助实现信用贷款、中介支付、募资清算等金融服务，而区块链技术的去中介化特质，能够完全颠覆银行业的各个领域，在不可信情况下省却中介环节，推动新的商业模式的建立。如支付领域，我们都知道，很多第三世界国家金融服务业不发达，特别是可信第三方的建立较为困难。BitPesa公司看到了这一“痛点”，利用区块链技术在肯尼亚、尼日利亚、乌干达等发展中国家提供企业间汇款结算业务，让发展中国家能够享受到无可信第三方的金融服务。肯尼亚传统跨境支付的平均费率约为9.2%，而BitPesa公司能够将费率降低至3%，大大降低了中小企业的压力。目前BitPesa公司的月均处理量已达到1000亿美元。

区块链技术创造的信任机制，还可以改善供应链金融管理水平。传统供应链金融的流程主要包含以下几个特质：一是核心企业和一级供应商、一级供应商和二级供应商之间产生应收账款；二是银行主要对核心企业进行授信，对一级供应商谨慎授信，基本不对二级供应商和三级供应商授信。因此一级供应商融资时，主要采取几个方式，包括向核心企业寻求融资，或以应收账款质押的方式向银行融资，或是对应收账款进行保理。对于二级及三级供应商来说，以上三个方法都比较困难，一方面不能向核心企业融资，也不能通过应收账款向银行融资；另一方面也无法进行应收账款保理，只能自求多福了。

供应链金融存在的主要限制在于：应收账款流通困难，一级企业还能够通过与核心企业的资质承诺来融资，二三级则很难进行有效的融资；融资成本较高，主要是以应收账款获得短期融资；第三方介入困难，一级以下的企业因为缺乏相关资质，在供应链金融体系中生存困难，不具备资金及上下游产业链优势；最后则是信用危机，供应链金融各环节，特别是一级以下企业融资的真实性容易受到怀疑，因信用危机导致的骗贷事件频频爆发。实际上，以上几条归结起来，其根源都在于信用问题，因为一级、二级、三级企业无法获得可靠的信用背书，因此难以获得融资，融资成本也极高，从而使供应链金融的流畅性及完整性受到了极大的影响。

而区块链技术有效解决了这一问题，企业可以将应收账款以数字资产的形式放在链上，这种数字资产具备可追溯性、可拆分性和可转让性，一级企业可以以拆分支付的形式，融资给二三级企业，使得资产的传递有了核心企业的背书。另外一方面，区块链数据的不可篡改性，为供应链金融提供了银行及核心企业之外的第三方运营的能力。

当然对于区块链技术在金融领域的应用，也有很多人表示了怀疑和担忧。如金融服务公司True Link Financial的创始人兼执行总裁凯·斯

廷 奇康姆（ Kai Stinchcombe ）认为，建立在信任、规范基础上的机构及金融系统，比建立在区块链技术基础上的“无需可信第三方”系统要可靠得更多。他认为，传统支付世界是不可放弃的，买家实际选择了信任第三方中介，而非自身对软件数据进行区分和审核的能力。信任在金融领域极其重要，基于消除信任的项目并没能抓住客户最核心的需求。



## 第四节 保险行业的区块链试水

前文我们已经阐述过，区块链技术可以在保险行业领域起到十分重要的作用，而国内也有众多保险公司开始应用区块链技术。两者的强强联合，将会碰撞出怎样的火花？下面我们具体来看近年来保险行业对区块链技术的典型应用。

首先我们将目光对准国外。早在几年前，国外保险巨头们就已开始了对区块链+保险行业的尝试。2016年，欧洲保险行业五大巨头——安联保险（Allianz）、荷兰全球保险（Aegon）、慕尼黑再保险（Munich Re）、瑞士再保险（Swiss Re）和苏黎世保险（Zurich Insurance Group）——就组建了区块链研究组织联盟，旨在为区块链在保险业的应用提供意见交流的平台，评估区块链是否能够切实应用于保险行业，以及如何提高保险行业的效能。当时区块链技术在银行业已经大显身手，但在保险行业进展缓慢，这迫使五大保险公司联合出手，此次行动也是为了通过区块链在保险行业占领先机。苏黎世保险该项目的负责人亚历山德罗·斯帕多尼（Alessandro Spadoni）认为，区块链技术可以通过智能合约体系简化保险销售和理赔的处理流程，从而为保险客户提供更加高效和流畅的服务。

除此之外，2016年10月区块链保险联盟B3i正式宣告成立。它同样是多家保险公司的联盟，但与五大巨头的区块链研究组织联盟相比，参与公司更多，辐射范围也更广，目前已有美国再保险公司、利保互助（Liberty Mutual）保险公司、汉诺威保险公司、SCOR、杰勒拉利保险集团、瑞士苏黎世保险集团、瑞士再保险集团、慕尼黑保险集团、安联保险集团等15家保险或再保险公司成为B3i联盟的成员。这个联盟同样聚焦于联合承保和精准理赔，希望通过区块链技术提高对保险资金的管理能力。2017年8月，B3i联盟发布了利用区块链技术的核

心组件Codex 1 [\[10\]](#)，它是一个提高再保险自动化程度的智能合约技术。所谓再保险，是保险人在原保险合同的基础上，与他人签订分保合同，将其承担的责任和风险向他人进行保险的过程。再保险的目的在于分散风险，一份再保险合约会涉及原保险人和再保险人两个角色，其保险关系根据双方身份的不同，可以分为6种情况，整体操作较为复杂。而Codex 1可以帮助再保险经纪人优化工作流程，具体方式如下：再保险的保险关系人包括被保险人、保险受益人、保险公估公司、保险经纪公司和保险代理公司，再保险经纪人需要收集各方意见，并在其中起到信息传递的作用。一旦各方被放置到区块链上，就不再需要再保险经纪人在不同关系人之间“传话”，减少了各方对中介的依赖度，从而大大提升了效率。同时投保人可以自己建模，结合投保人及保险标的情况，预估未来可能发生的损失，从而计算出合理的风险等级，并相应给出不同的保险费率和理赔率。

据计算，再保险业务一般需要10天以上的时间进行财务核算，而B3i联盟的区块链平台将这个时间缩短到仅仅5~10分钟的时间。同时，多家保险公司测试确定，该项技术能够提供更加快捷、有效、安全的交易模式，其系统的稳定性也不遑多让。2018年B3i联盟除了已开始在区块链平台上开展保险业务，同时也在探索其他商业保险中区块链的应用，计划将应用场景从客户终端推广到整个保险及资产管理平台。

在其他保险行业细分领域，相关公司也在进行着实验，甚至还有非保险公司也积极参与，想要“分一杯羹”。2017年“四大”会计师事务所之一的安永、互联网公司微软和世界上最大的航运公司马士基联合推出了海运保险区块链平台，这也是世界海运保险行业的首次区块链应用。海运保险行业是世界上历史最悠久的保险领域之一，然而也是效率最低的保险领域，存在的问题主要在于交易繁琐和计算复杂。海运保险区块链平台基于微软的Azure云服务技术，将客户、经纪人、保

险公司或第三方放置于共同的链上，实现货物、物流、风险数据的自动收集，并确保各方实时共享，建立起一个国际海运保险生态系统。目前该区块链平台已通过为期20周的理论证明，将在Azure云计算平台上做进一步的测试。

除了国际保险巨头，一些新兴公司也在不同的保险领域大胆开展了相关应用。典型如InsurChain——它是由新加坡XLab基金会建立的区块链保险平台，主要提供保险行业区块链的基础技术服务，帮助企业打造区块链基础平台，并在此基础上构建应用业务系统。其特点在于利用智能合约系统，实现数据与企业的分离，可以快速进行投保人身份信息的校对，授权第三方进行数据信息的分析和统计，确保保险合约公正公平地执行。任何一家公司或个人都能设计提供保险产品上传至区块链上，由客户购买，并在出现协议设定的情况下自动理赔。InsurChain目前已在以太坊上线，全球用户都可以在链上设计产品或者购买，当然交易方式采用的是加密货币。

另外还有Dynamis——一个互助失业保险平台，同样已在以太坊上线。它生成了一个智能合约，企业可以将失业保险金放在合约中，雇员通过身份及就业情况验证就能进行失业保险的自动理赔，从而避免了企业拖欠失业保险的行为；Z/Yen集团——业务为共享经济实时保险——开创了保险的新领域，用途在于用户使用共享经济产品时，可以签订智能合约系统，对意外情况以比特币进行赔付。此外，还有Everledger（防伪验真保险）、InsurETH（飞行延误险）等利用区块链技术的保险业务。

国内对保险行业区块链的应用也进行了不少有益的探索。2016年成立的“水滴互助”项目，以区块链技术来应对看病难、看病贵的问题。“水滴互助”是一个互助式保险项目，保险标的是那些患有重大疾病的贫困人群，采取“保险+股份”的形式，保险金类似于参股的股份，

用来进行赔付。2017年8月，信美人寿也推出了建立在蚂蚁金服区块链技术基础上的爱心救助保险项目，是国内第一个用区块链技术记账的相互保险项目。其承诺一旦客户发生意外情况，不仅能获得理赔金，在家庭困顿的情况下还可以申请账户上的额外资金救助。区块链技术的引入，在解决身份验证的同时也保障了救助资金的公平性和透明性。

中国商业保险巨头中国平安，也依托“平安金融云”于2017年公布了自己的区块链保险平台；2018年更是与麦粒资本合作，主要关注知识产权的商业保险领域的区块链应用，也创造了国内首次保险行业应用区块链的历史纪录。

保监会数据显示，早在2016年末，我国保费收入就已高达3.1万亿元，跃居世界第二位。而保险行业的信用危机、理赔困难、效率低下等问题，仍在困扰着中国保险业，其发展速度与质量有较大的差距。可以预见，在未来我国的保险行业将继续高速发展，引入区块链技术对于有效解决传统保险行业的各种“痛点”，有着十分积极的作用。

## 第五节 点对点形式的区块链

之前我们已经提到，根据国家七部委下发的通知，ICO（首次币发行）已被取缔，交易中心也随之宣告关闭。但对于一些大型的交易中心来说，发展到这么大的规模已无法轻言结束，又该何去何从呢？答案是海外市场的点对点场外交易。海外市场很好理解，就是将交易中心转移至对ICO不做严格限制的国家和地区。那什么是点对点场外交易呢，它对区块链技术发展又有哪些意义？本节我们就来探讨一下点对点形式的区块链技术应用。

点对点技术又被称为对称互联网技术，其特性在于在多节点上分布数据，而不是聚集于少数服务器上。加密货币的点对点交易是指个人对个人的交易模式，区别于交易中心的个人对机构。这种新型交易模式没有固定的成员资质，没有规定的规则制度，交易平台只提供交接和托管服务而不接触资金，也不提供身份验证和居中协调作用。交易过程依靠各自独立的经营机构进行，买卖双方根据需求自主选择交易途径和方式。当然，为了确保交易的切实可行，一般会设置一名交易员（在加密货币领域具有担保资格的人员）来负责收币和出币，买卖双方根据前期沟通协调，对交易员支付一定的中介费用。

点对点场外交易的优点主要在于：首先，使用双重身份验证来确保安全性。虽然是个人对个人的交易模式，但它并不等同于就没有了信任机制。点对点交易平台使用双重身份认证系统，需要通过手机和口令进行二次认证，从而使得黑客无法攻击个人账户，避免了账户信息被盗取的风险，为账户提供更安全的资金保障。其次，点对点交易可以实现自动化。其流程类似于淘宝上的商品交易，卖方与买方商定交易的方式、时间和价格，买方先发出交易申请，钱就会自动从其账户中扣除，转入托管中心，卖方收到钱后，加密货币才真正属于对

方，避免了买卖双方存在欺诈行为。第三个优势在于交易的速度和便捷性大大增强。只要知道对方的地址，便可以直接进行交易和支付，双方直接建立起信任，而无须通过第三方的层层审核。这使得加密货币完全属于个人，不再依靠中间机构或者权威组织，有利于加密货币流通顺畅，为其提供了更顽强的生命力。可以说，这是一个自由的加密货币市场，双方交易依据为协商价格，不再依赖于交易中心的实时定价。

区块链的点对点技术不仅会在加密货币交易中应用，在其他领域也有着广泛的应用空间，目前最令人瞩目的是在电力资源领域。早在2017年，Drift能源区块链公司、Power Ledger等公司项目就在试图建立点对点的区块链电力交易平台，率先进行市场布局。

一直以来，庞大的输配电力资源费用计算、复杂的电力系统数据共享、细化的信息采集及要在此基础上实现的动力平衡，都给电力资源交易机制带来了极大的压力。点对点的区块链交易模式，是建立起一整套的电力资源交易及供给系统。在这个系统中将电力生产厂家、输电和配电运营商、电力零售服务商及消费者，共同纳入到链上，消费者可以直接与各个电力供应商交易，去除了电力交易的中间环节，减少了交易的复杂层级，实现了电力资源交易的扁平化。

另一方面，点对点的电力资源交易，也使得消费者获得了更大的选择权，可以随时自由切换电力供应商。辅助识别清洁能源、可再生能源的电力认证系统以及区块链技术中的数据信息不可篡改性，也为可再生能源的记录和交易提供了便利的基础。

纽约布鲁克林的能源微电系统实际上就是点对点区块链技术的应用。该项目的团队主要在进行一个实验式的应用：将10个家庭的电力系统纳入区块链，其中5家利用太阳能电热板发电，另外5家则可以购买前者富余的能源。购买方式建立在以太坊的区块链智能合约基础

上，各家的电力仪表都能自动连接该区块链平台，一旦产生交易行为，将自动在链上进行记录和保存，且此记录不可篡改，能够确保每家每户随时在链上追溯交易历史。

这相当于建立了一个再生电力能源市场，用户之间的交易比自上至下配置电力更有效率，可避免电力资源在运输中的损耗，也能够使富余的资源被有效地利用起来。一旦这个系统被广泛应用，可以预见，它将在整个社会范围内节约大量的资源，在电力资源愈发紧张的今天有着重要的意义。

同时，这项技术也是电力生产交易模式的一个重大转变，家庭从单纯的“消费者”转变为“生产消费者”。区别在于，“生产消费者”可以自己生产并控制能源，同时也可以将多余的能源转卖给邻居或是交易给社区保存，提高微观电力资源的利用效率，从而使原本自上而下的大型电力能源系统转变为可以自动执行、自由交易的双向选择系统。

在其他领域，点对点区块链技术更为擅长的是与“共享经济”相结合。比如打车，可以由所有乘客及司机共同组成协作性的区块链平台。当顾客需要用车时，区块链根据顾客需求对司机进行快速过滤，及时快速地将与之相配的司机筛选出来供顾客选择，实现司机与乘客的点对点交易。届时，网约车平台将更像是一个系统建设公司、技术支持公司和服务平台，而不再发挥其第三方中介的作用。区块链技术因其数据信息不可篡改性，更能真实有效地显示司机和乘客过去的全部交易情况及评价，从而为运行提供安全保障，也解决了目前网约车平台面临的安全保障难题。

可以说，这种点对点的区块链技术将极大地改变交易模式，甚至是人们的思维模式。它使每个人都成为交易的直接参与者，减少了第三方中介的介入，改造了我们的交易流程，未来将在更广阔的领域带给我们惊喜。

## 第六节 支付行业的飞跃

支付系统是国家金融体系的重要基础组成部分。随着我国金融行业的不断发展及开放，以现金、票据、卡类为工具，以汇兑、委托收款、定期借记、托收承付、直接贷记等为手段的支付系统持续完善。近些年随着互联网技术的发展，更增添了电子票据等其他以计算机技术为基础的新型支付手段。

然而自16世纪以来，现代支付系统并没有根本意义上的革新，本质上都是由中央权威机构担当清算中心，对支付记录进行保存和结算；大型金融机构在中央权威机构中开辟账户，实现相互之间支付情况的记录和结算；小型金融机构或者个人消费者在大型金融机构中持有账户，他们之间的交易则由大型金融机构进行统计和结算。这样就形成了一个多层的交易结算体系，当消费者完成一项交易时，不同账户之间进行记录，最终统一汇总至中央权威机构结算，从而实现金钱从一个账户到另一个账户的转移支付。几百年来，支付的革新主要集中在记录方式和转账技术上，其根源没有丝毫的动摇。

区块链技术对金融支付行业的革新，主要在于对底层支付流程和理念的动摇。它使支付体系改变了对中央权威机构的依赖：点对点交易、分布式记账方式，使交易支付不再需要由第三方机构来记录，达到“去中心化”的作用，从而实现实时的结算，从根本上改变了集中式存储的流程要求。这有助于改善现在复杂冗余的支付体系，各个机构也不再需要建立专门的支付账户系统，对每一笔交易进行跟踪、记录、清算和对账，减少了对系统的要求及人员配置，从而大大节约了成本，提高了支付体系的整体效率，解决了现有支付系统的“痛点”。



举个例子来说，当我们使用支付宝购买一件商品时，传统的支付流程是：消费者的支付宝账户提出一个消费请求，这个信息被传递到卖方的银行账户，卖方银行通过银联系统将交易信息转达至消费者银行账户，消费者银行账户扣款，再通过银联系统将交易金额结算给卖方的银行，卖方银行将资金记录在卖方账户上。央行通过银联系统对全部的交易进行管理和控制，资金的结算是落后于交易和支付行为的。而区块链技术下的支付，其信息流和资金流可以实现有效的统一，在消费者确认信息时，实际的资金结算和清算也就完成了，不再需要后续清算的时间。

当我们用支付宝购买一件商品时，区块链技术会实时在链上记录和传递交易信息。区块链上没有账户体系，而是设立了两个密码匙——一个私钥、一个公钥，代表着身份和资产所有权。账户之间直接进行点对点的信息处理，双方账户之间直接进行结算和清算，而记录会被保存在链上，也就简化了支付的流程。

除此之外，我们在前文中还说过，利用区块链技术的去中心化和数据不可篡改性，还能为支付交易的隐私和安全提供保证，简化身份认证的流程，这也是区块链技术最基础的特性，在多个领域都有着类似的应用。

我们重点来说一说区块链技术在跨境支付领域的应用。这是近年来部分大型银行比较关注的业务。随着经济全球化的步伐加快，各个国家之间的经济往来日益密切，随之而来的跨国交易数量也在持续上升，2016年我国的货物进出口总值就超过了3.68万亿美元<sup>[11]</sup>，相当于当年德国GDP总量（3.36万亿美元）。而在不断增加的交易量、持续加大的支付压力下，跨国支付却面临着效率低、速度慢甚至是坏账等问题，区块链技术为以上问题的解决提供了一个新的渠道。

具体来讲，就是建立一个基于区块链技术的跨境支付体系，其中包含两大角色和四大模块：两大角色指的是参与跨境支付的机构和客户，前者包括银行、流动性提供商等机构，其作用在于让现实中的法定货币进入区块链，因此我们也称之为“网关”，后者是指实际参与国际贸易的客户；四大模块则分别是网络连接模块、支付账本、做市商交易端和客户交易端，网络连接模块帮助作为“网关”的机构接入区块链，支付账本则将银行和做市商作为节点接入区块链账本，做市商交易端向区块链支付系统提交外汇实时价格，客户交易端则是客户的直接操作系统，客户可以通过交易端发起支付。

具体举一个例子：

中国某公司（我们称为甲公司）要给美国的某公司（我们称为乙公司）支付10万美元货款，甲公司通过本地银行发起向乙公司在当地账户的汇款请求，甲公司本地银行收到请求后，使用网络连接模块连接到乙公司当地银行，提交相关的汇款信息和账户信息，乙公司当地银行对提交的信息进行审核，审核其是否符合当地监管要求。如审核通过，则乙公司当地银行向甲公司本地银行反馈收款人信息和相关费用信息。甲公司当地银行收到反馈后，通过网络连接模块查找到适合的做市商，由做市商提供实时美元对人民币汇率，甲公司本地银行再在做市商及乙公司所在银行费用基础上，加入自己的相关费用，形成最终明细，提供给甲公司。

如甲公司认同其间发生的支付费用，则乙公司在发货后，向当地银行提供已发货的信息，乙公司当地银行再次通过网络连接模块，向做市商及甲公司本地银行通知已发货，多方进行信息的再次核对，确保信息的真实性和一致性，对此笔交易达成共识。甲公司当地银行在系统中记账“借给甲公司XX元，交易费用XX元”，并发出记账完成的信息；做市商收到此条信息后，也在区块链系统中记账“借甲公司本地

银行XX元，贷记做市商账户XX元，借记做市商账户XX美元，乙公司当地银行XX美元”，并通过区块链连接模块，通知双方银行已完成账本记账；乙公司当地银行接到信息后，将在系统内记账“贷记乙公司XX美元，费用XX美元”，同时也发出记账完成的信息。

以上就是区块链在跨境支付系统中的应用流程。虽然看起来十分复杂，但通过区块链技术进行电子化实时操作，实际所需的时间和过程都十分简便，成本也低于现行的跨境支付系统。基于此，各国金融机构都在积极部署跨境区块链支付技术，以提前抢占市场。如外汇交易结算巨头CLS集团已在开展对银行区块链支付服务的测试，它主要与IBM合作，为旗下的银行合作伙伴提供一个连接新系统CLSNet [\[12\]](#) 服务的选项，已有7家银行做好加入此项目的准备，但也存在部分银行对其在证券结算和安全保管方面的疑虑。Ripple公司则建立了一个跨境账本协议，它基于分布式互联网协议、共识总账和加密货币瑞波币，形成了一个实时结算系统和汇款网络。据其测试估计，使用瑞波区块链平台进行跨境支付，银行方面可以节约高达42%的交易费用、65%的流动性成本和48%的运营成本。Circle International Financial [\[13\]](#) 则在150多个国家开展了资金转账服务，通过区块链技术实现低成本的货币跨国兑换，使用者可以通过手机App，在没有手续费的情况下进行美元、英镑与比特币之间的互换转账。中国金融机构也持续在支付领域发力。2017年3月，招商银行发布了区块链直联跨境支付应用技术，实现了国内首个区块链跨境项目的落地。

当然，区块链技术在金融支付领域的应用尚不成熟，面临着种种挑战。问题主要在于信息的安全性：虽然区块链技术能够通过密钥避免信息被盗，但密钥的生成与保管全部依赖于个体，一旦不慎将密钥遗失，用户的账户就丢失了，任何机构和个人都没有办法帮助找回，这种安全性在银行支付账户领域反而会起到反作用；另一方面，区块

链技术的成熟性还有待提高，无论是加密算法还是共识算法，都需要持续优化。

## 第七节 银行业的再次升级

正如前文所述，传统银行业正积极运用互联网技术开展转型升级，区块链技术是其重要的选择之一，在应用场景中已经开始生根发芽。2018年各大银行年报已经开始体现对区块链技术的展望及应用，特别是五大行已经计划将区块链技术落实到国际贸易、住房租赁、精准扶贫、供应链管理等过程中。

首先是工商银行。它建立了基于区块链技术的金融产品交易平台，在传统交易平台的基础上增加了点对点技术，可以为客户更加便捷、迅速地提供金融资产交易和转移服务。此外，为了解决个人身份认证——提供各种如结婚证、出生证等证明文件的问题，工商银行研发了可以鉴定数字证明及存储区域的可共享区块链技术，从而避免用户多次重复提交同一证明材料。此项目已于2018年4月正式宣布实施。该项技术改变了过去向权威机构获取证书，再向其他提出要求单位出示证书这一重复性过程。它转变为用户对电子证书授权，通过授权将电子证书的数据存储到区块链上，有关机构得到用户的证明后可以随时调取或更新相关证书数据，从而大大提升了效率，降低了提供证明文件的社会成本。

除了成立研究院、自主开展研发工作，工商银行还通过招标，与新兴区块链企业开展深度合作，发掘区块链技术的深度应用场景。2018年1月，工商银行正式发布文件，称杭州趣链科技有限公司中标其区块链项目。前文中我们曾经提到过，趣链科技有限公司是区块链底层技术的开发商，它建立的区块链底层平台Hyperchain已与中国农业银行、中国光大银行、浙商银行、北京银行等众多传统银行合作，并曾为中国银联、上海证券交易所、德邦证券等大型金融机构提供基础

区块链技术服务。趣链主要可以为工商银行提供区块链技术培训和区块链技术支持，帮助工商银行完善其区块链底层建设。

在精准扶贫领域，工商银行与贵州省政府合作，对银行金融服务链及政府扶贫审批程序链进行整合，建立跨链互信的机制，并利用区块链的公开透明机制，帮助扶贫资金的使用实现公正、高效、透明及可追溯。

综上所述，工商银行可以说是在中国所有银行中，对区块链技术应用范围最广阔、应用场景最多样、应用技术最先进、应用理念最领先的传统商业银行。

中国银行在区块链技术的应用方面不遑多让。中国银行的应用方向主要在于反金融诈骗。2017年1月，中国银行上线了基于区块链技术的电子钱包App，该App可以与中国银行的借记卡绑定，以32位数字+字母组成有效地址。其功能在于登录App后可以查看银行卡余额及转账记录、发送和接收红包、以二维码收款等等。2017年6月，中国银行宣布与腾讯合作，重点在云计算、大数据等方向测试区块链技术。2017年9月，中国银行提交了“区块链数据压缩方法及系统”的专利技术申请，提出以压缩数据的方式来应对区块链技术发展、数据量不断增多而引发的存储空间不足问题。在公共服务领域，中国银行也在积极探索，参与雄安新区的土地赔偿及“智慧森林”供应链融资区块链业务，还与汇丰银行强强联合，推出指纹等生物认证系统及其他区块链应用场景。可以说，中国银行的区块链技术开发虽然略晚一些，但进步神速，一直处于不断前进的过程中。

建设银行则推出了区块链保险业务平台，其与IBM合作在2018年1月完成了国际保理区块链交易，成为国内首家将区块链技术应用于国际保理领域的商业银行。在公共服务领域，其主要建立了雄安新区的

房屋租赁区块链服务平台，协助雄安新区管委会做好住房租赁平台的建立和监测。

中国农业银行主要专注农业领域。它在电商供应链金融领域，基于区块链技术和理念，上线了农产品互联网金融融资产品“e链贷”，主要向客户提供订单采购、灵活定价、批量授信、自动审批等服务在内的金融服务，提升为三农服务的效率，拓展农业商业发展机遇。

五大行之外，其他商业银行也在进行区块链技术+金融业的探索。在票据领域，中小银行大胆利用区块链技术，对小微企业票据融资的细分市场发起“猛攻”。赣州银行联合贵阳银行、廊坊银行等13家城商行，建立了国内首家区块链技术银行合作联盟，于2017年3月公布了第一款产品“票链”。“票链”主要面向小微企业，解决其融资难、融资贵的难题，利用区块链技术不可篡改、透明化程度高等特点，处理小微企业的小额支取贴现融资，提供不限金额、不限时间的高效服务，简化审批流程，降低服务成本。截至2018年1月，短短10个月内它已为198家小微企业提供了价值超过4.76亿元的票据融资服务，完成了1500余起票链业务，近80%为30万元以下的融资服务，为小微企业和实体经济的发展起到了重要的促进作用。截至2018年3月15日，这个服务的企业个数进一步增加为227家，业务数量达到1975笔，提供融资6.38亿元。

在资产托管领域，邮政储蓄银行和浙商银行也进行了有益的尝试。资产托管主要难题在于涉及金额大、牵涉机构多，需要反复进行信用验证，消耗大量的人力及时间资源，而信用验证正是区块链技术的特点之一。浙商银行建立了“应收款链平台”，企业应收款项可以通过区块链技术转化为电子支付结算和融资工具，从而为企业盘活应收款项。邮政储蓄银行则携手IBM，推出了区块链资产托管服务平台，这也是国内首个资产托管区块链系统。

招商银行侧重于清算结算业务的区块链技术应用。在内部，招商银行建立了直连清算系统，通过运用私有链技术，将原本只限于总行与分行之间的清算结算，拓展到各分行之间。同时也使得原来分钟级别的报文传递速度，加快到秒级别。2016年6月，招商银行与香港永隆银行、永隆深圳分行三方合作，建立了“招行直联支付区块链平台”，运用区块链技术“分布式记账”的特点，在链上同步更新并共享资金清算信息，从而大大提升了资金清算结算效率。

除了传统商业银行，互联网银行更是基于自身技术优势，将金融业务与区块链技术紧密结合起来。由腾讯主导的微众银行，与上海华瑞银行联合开发了针对联合贷款的清算、结算业务区块链服务平台，为微众银行的“微粒贷”业务提供技术支持。同时微众银行还与平安银行、京东金融、华为、前海人寿等25家互联网和金融公司，在深圳建立了区块链技术联盟“金链盟”，旨在整合协调区块链技术研究资源，实现适用于金融机构的金融联盟区块链及其之上的场景应用。2017年12月，“金链盟”推出了基于BCOS（BlockChain OpenSource，区块链底层技术开源平台）平台的金融区块链底层平台FISCO BCOS。

通过观察以上银行系统对区块链技术在各领域的应用，我们可以看到区块链技术基于其信用机制和去中心化等特点，对商业银行业务的革新和升级有着无可比拟的作用。未来商业银行将继续从四个方面深入对区块链技术的探索。

一是组建区块链技术联盟，如“金链盟”的模式，不仅是在技术和应用层面上进行合作尝试，更是在标准制定和行业监管方面谋求一致，推动区块链技术在银行业的落地生根。

二是加强对加密货币的研究。加密货币是未来的大势所趋，货币数字化后续可能带来新的商业变革、金融变革，甚至是更广泛的社会变革，有能力抓住这一机遇的商业银行，其发展也无可限量。



三是在清算结算、跨境支付、供应链金融、公共服务等多个领域，细化对区块链技术的探索应用，持续开展区块链技术应用研究，拓展区块链应用的场景和领域。

四是内外并举，大力打造区块链技术平台。对外可以加强与相关区块链技术企业的合作，或是对区块链技术企业进行资本运作，从而加强对自身区块链技术的支撑；对内则培养区块链技术人才，设立区块链技术研究院，积极引导、积累经验，将银行业务与区块链技术有机地结合起来。

An abstract graphic on the left side of the page, featuring a complex network of interconnected circles and lines, resembling a molecular structure or a network diagram. The circles vary in size and are shaded in different tones of gray, creating a sense of depth and complexity. The lines connecting them are thin and dark, forming a web-like pattern that extends across the left half of the page.

04

**区块链 + 商业：  
开启全新商业  
时代**

## 第一节 可追溯的农产品

农产品，是一个我们既熟悉而又陌生的词。在整个社会发展过程中，农产品都是经济发展的基础。因为它的发展水平决定了我们的食物生产，而食物的使用价值远超任何一种商品。

而这样一种重要的商品，我们却对它既熟悉又陌生。虽然每天的餐桌上都少不了，但是我们却很少探究这些农产品的生产与流通过程。这样的结果是，我们每天都要接触和消费农产品，但对它们的熟悉程度还不如电视、汽车等大宗商品。

事实上，农产品的交易过程非常复杂，从农产品的生产地一直到最终的消费地，其间的运输过程非常复杂，科技要求很高。今天，我们可能已经熟悉了各种利乐包装里的牛奶、打包装好的牛肉与鸡肉，这些事物都如此自然，已经很少有人感叹这些技术的伟大了。

实际上，这些包装与冷冻技术对农业的发展起到了非常巨大的作用。早在几十年前，冷冻冷藏技术还没有出现和普及时，远距离运输蔬菜与豆类制品曾面临许多困难。

农产品运输难题的解决，不仅让我们能够吃到新鲜的蔬菜，甚至影响了国家的发展。南美洲的阿根廷以盛产牛肉和足球明星著称。但在冷冻技术发明以前，阿根廷的牛肉却根本无法运往主要的消费市场——欧洲。为了解决这个问题，阿根廷不得不把一船一船的活牛运往消费地，这其中的困难可想而知。旅途中的饲养照料、疾病、上岸后的处理，都是复杂的问题。而真正从阿根廷运往欧洲的牛肉数量和质量，也远不及今天。

小规模的市场限制了阿根廷的发展，广袤的草原资源无法得到充分开发。牛肉产业变成了饲料产业，牧场主变成了农场主。而冷冻船的出现，改变了阿根廷的国家命运。正因为冷冻船的出现，让阿根廷的各种畜牧产品行销世界，不仅解决了牛肉问题，甚至奶制品也走出了潘帕斯草原。

一艘小小的冷冻船，为阿根廷打开了畜牧产品外送的窗口，带来了丰富的外汇储备，也让阿根廷成为一个国力相对强盛的国家。从某种意义上说，农产品运输技术的变化对于阿根廷来说不亚于一场工业革命，但是由于人们的忽视，农业的发展与工业革命似乎并不能画上等号。

在我们的意识深处，依然认为农产品与几千年前的基本种植业产品没有太大的差别。而从另一个角度，这也是因为农产品本身并没有发生根本性的变化。

这也就决定了农产品的变化必须来源于市场而不是产品。而每一次农产品市场的变化，实际上都是由新技术的引入带来流通环节的变化而产生的。这样一来，我们也就能够理解区块链技术对于农产品，可能会产生什么样的影响。

传统的农产品运输是不可控的，甚至是一个销售的黑箱环节。农产品的生产端和销售端之间，隔着一个永远也无法厘清的运输网络。终端的消费者只能从直接面对的摊贩那里了解商品的信息。

而摊贩实际上也并不见得真的了解这些农产品的来源，只是从上一级的经销商那里获得信息。这就造成消费者对农产品的了解仅限于价格，至于对农产品生产运输过程的跟踪，则根本无从谈起。

我们不能确定，某一个贴着地理保护标志的产品是不是真的来源于那个地方，也无法判断某一个农产品是否真的与它所标称的一样，属于某个地区的特产。

并不是消费者不希望得到这些信息，也并不是商贩不愿意提供这些信息，而是想要了解这些信息需要付出非常巨大的代价。

阿根廷的牛肉因为冷冻技术的发明而能够运往世界各地，但是在这个运输过程中，还有无数的公司与个人为这些牛肉的流通服务，他们遍布世界的各个地方。阿根廷牧场饲养的肉牛从草原上运到屠宰场，进行分割；随后，牛肉通过地面的运输网络被送上远洋的货轮；其间可能又经历了中型货轮、大型货轮，直到运到消费国的边境；这时这些牛肉可能还需要换成小型的轮渡，或者通过港口设施，通过公路网络，真正运送到消费地。

在这个过程中，经手的供销商数量之繁杂，让人无法想象。在这种情况下，我们很难说这些牛肉来自阿根廷、巴西或是美国，只知道这些牛肉经过了基本的安全检验，从一个遥远的地方运到了我们的餐桌。

今天，随着对食品的要求越来越高，我们希望得到的食品信息也越来越多，而传统的技术很难突破这样的运输屏障。

商品本身很难告诉我们真正的信息，为了解决这个问题，区块链可以发挥巨大的作用。它可以像普通的二维码一样贴在产品上，但是与二维码不同的是，区块链具有唯一性和不可复制性。人们可以为一段条码，但是却没法为区块链。

使用二维码，扫码枪扫出来的信息也许是我们想要的，但是我们并不能确认这些信息的真伪，无法判断这些信息是否真的属于手中的

这个商品，而区块链却解决了这个问题。

实际上，农产品很难从生产端发生革命，虽然改进一直在发生，但是彻底地改变农业生产的模式却非常困难。不过流通领域却发生了翻天覆地的变化，从传统的农产品运输不能超过一定范围，到今天几乎可以行销全球，这实际上可以被称为一场彻底的变革。

而区块链所带来的潜在变化，可能也会造成这样的效果——通过区块链，我们可以让所有在农产品的增值流通过程中产生利益关系的人，都紧密地围绕同一个区块链进行操作。这些人可以把自己的商品信息甚至工作信息都融入其中，让人们在使用商品的时候真正知道它来源于哪里。

通过这样的区块链模式，人们能够了解到一个农产品在运输环节都经历了什么，它在哪一个环节最容易受到伤害。如此一来，我们的运输效率和质量都会得到极大的提高，这也保证了我们未来吃的食品会越来越新鲜、越来越安全。

## 第二节 物联网的“正确打开方式”

物联网一直是互联网经济发展的重要方向，也是很多人认为的未来互联网技术发展的高地。物联网的建成将会带来巨大的变革，用传感器、控制器等设备把各种没有思想和生命的物连接成一个网络，让它们更好地服务人类。

从应用场景来说，物的连接是进一步改变流通行为的方式。通过连接各种设备，可以记录所有的决策、行为、运动，最终形成一个完善的、可追溯的网络。通过这个网络，可以实现控制产品质量、提高流通效率等功能，最终实现全社会物流效率和生产效率的提高。

物联网从本质上说，是通过物物相连实现机器设备智能化管理和控制的目的。然而，物联网技术也面临着许多问题和挑战，这些问题有可能成为物联网未来发展和应用的巨大障碍，而区块链技术为解决这些问题提供了可能性。

物联网在长期发展演进的过程中，遇到了以下几个行业“痛点”：

首先是设备安全问题。物联网连接所有我们能够想到的设备，这带来了极大的安全挑战。我们不知道自己的设备可能被什么人攻击、什么信息可能流失。因为所有节点都在网络上连接，理论上都存在被攻击的可能。

2017年，《麻省理工科技评论》将Mirai创造的僵尸物联网（Botnets of Things）评为2017年的10大突破性技术之一。通过这个网络，Mirai成功地实现了多重攻击，这也证明了物联网设想在安全方面存在巨大风险。

据统计，Mirai僵尸网络在2017年5月就已经感染超过200万台摄像机等IoT设备，由其发起的DDoS攻击，让美国域名解析服务提供商Dyn瘫痪，Twitter、Paypal等多个人气网站一时间无法访问。接着，又出现了奴役物联网设备为其“挖矿”比特币的僵尸网络、规模更大更活跃的http81僵尸网络等。

在架构僵化方面，目前的物联网数据流都汇总到单一的中心控制系统。随着低功耗广域技术（LPWA）的持续演进，可以预见，未来物联网设备将呈几何级数增长，集中服务成本难以负担。据IBM预测，2020年万物互联的设备将超过250亿个。如何解决物联网的设备安全问题，是物联网走向实用的过程中必须解决的问题。

其次是个人隐私。在个人隐私方面，物联网也存在很多风险。一个典型的风险是集中式的架构带来风险，且这种风险以几何倍数增加。

从目前的情况来看，物联网通过连接无数个网络设备来实现数据的海量采集，但是这些数据全部被储存在集中的存储设备中。

这种管理架构无法自证清白，每一次调取、复制都处于不可控的情况下，这样就造成了个人隐私数据泄露的事件时有发生。这类事件也时常见之于新闻媒体，《成都商报》就曾报道过成都266个摄像头被控制的事件（2017年5月3日）；而央视也对各种摄像头设备进行了质量调查，发现能够有效抵御风险的摄像头并不多见，大部分摄像头存在一些缺陷。 [\[14\]](#)

最后是通信兼容的问题。在通信兼容方面，全球物联网平台缺少统一的语言，这很容易造成多个物联网设备之间的通信受到阻碍，并产生多个竞争性的标准和平台。



在多主体协同方面，目前很多物联网都是运营商或企业内部的自组织网络。在涉及跨多个运营商、多个对等主体之间的协作时，建立信用的成本很高。

### 第三节 电商的新生

今天，当我们打开淘宝、京东、苏宁易购这些电商平台时，都不会觉得陌生，因为它们已经进入了我们生活的方方面面，帮助我们更好地生活和消费。但是回想一下，在十几年前电商刚刚出现时，人们对它又是什么样的态度呢？

那个时代是电视购物和邮寄购物的时代。邮局一项重要的业务就是把各种免费寄送到各个家庭的商品目录，送到指定的地址。拿到这些商品目录的家庭，浏览相关商品后可能会选择某些自己喜欢的商品购买，这在当时是一件非常顺理成章的事情。人们不会顾虑商品目录背后的生产商是否真的像他们所说的那样符合要求，因为邮局投递的产品具有一定的可信度；而且没有人认为，商家会为了一件并不太贵的商品花这么大的力气投放广告。

电视购物同样有类似的魔力。人们不太会质疑电视的权威，只会在拿到商品之后觉得：嗯，这是电视上推荐的，我用起来效果一定很好。

但是今天，邮政购物已经成了历史，电视购物也不再火爆，电商却因为它的灵活性进入了我们的日常生活。

可是在不久之前，电商是被看作骗子的。从网上买的东西拿到手里，人们往往会反复掂量；在电商平台上出售商品的商家，也因为担心收不到钱而提心吊胆。但是随着电商平台的发展，我们发现，这些场景都不再发生了。

那么电商究竟解决了什么问题，让人们变得如此信任它，让交易变得如此顺畅？不难发现，拥有这个魔力的，其实就是第三方支付平

台。

消费者出于担忧，不敢把钱直接交给商家；而商家出于担忧，也不敢把商品直接交给消费者。在这之间就需要一个第三方的协调者代为收钱，同时代为邮寄货物。这样交易对双方来说都是公平的。

买家拿不到商品，卖家就不可能从平台上支取费用。如此，买家也就不再担心卖家会随便地提供残次商品。这其实正是一个信任建立和深化的过程。

我们也可以说，电商的真正成功，其实是在解决了信任危机之后。如果没有解决这个问题，电商可能就会像昨日的电视购物和邮政购物一样走向末路。

时代在不断向前发展，电商平台也在不断向前发展。接下来电商又会走向何处，它面临的问题又是什么呢？

今天，制约电商平台发展的核心问题有两大类：第一类还是我们之前所说的信任问题，人们依然会在各种电商平台上发现真假难辨的商品，对这些平台上销售的物品投去不信任的目光。电商平台也做出了很多的努力——尝试建立更有信用的店铺体系，使用更加有效的假货识别方式。但是这些似乎都不能推动电商向前更进一步。

第二类是物流的效率问题。通过这几年的“双十一”购物节我们发现，电商其实并不担心找不到爆发的销售机会，他们更担心的是如何将商品高效地运送到每一个消费者手中。这确实是一个难题。当面对海量的包裹时，传统的寄递服务网络可能已经无法有效支持了，这个时候就需要一种新技术来解决这个问题。

上面提到的这两个问题，都是区块链能够大显身手的地方。通过应用区块链，很可能会给电商带来一次新的生命。通过区块链开店模

式，我们可以轻易地识别一件商品是否真实，在这件商品背后是否存在某些难以解决的质量问题。这样，我们就通过区块链技术打消人们对电商平台的最后一层顾虑。打破信任危机，对于电商平台来说有可能会是一个爆发式的增长点。

这种变化还有可能将更多的线下购物机会吸引到电商平台上，一些人甚至可能会彻底地将网上购物作为自己的唯一消费模式。

虽然在今天，人们的网购习惯已经足够成熟，但是如果区块链技术进一步成熟，我们所面临的，可能将是一个全新的商业。

针对物流领域，我们在前两节中已经比较系统地进行了说明，在这里也就不再赘述。通过上面提到的问题我们可以看到，区块链的应用对在线商场能产生巨大作用和影响。

事实上，对区块链应用的研究，已经成为一些电商平台的必备课题。通过区块链来解决假货的危机和物流的难题，是未来电商的发展方向。相信电商与区块链的组合，最终不会让我们失望。

## 第四节 能源区块链的崛起

能源消费与其他消费相比，具有比较典型的区别——能源消费具有鲜明的资源限制属性。因此它并不是完全的市场行为，而是一个更为复杂的资源管控行为。

在任何一个国家，能源领域的消费行为都一直被列为一个独立的研究领域。它与一般的大众消费无论是消费的形式、内容还是监管方式上，都有很大的不同。

简单来说，能源主要包括电力、天然气、石油、煤炭。

这些是我们能够接触到或者日常中能够了解的能源。事实上，能源消费的真正主体并不是老百姓，而是企业与社会组织。比如我们每天工作的办公场所消耗的能源，其实比我们自己家消耗的多得多。而这些能源消耗的主体，往往面临着能源限制开发、能源使用的非精准化提供等方方面面的问题。

对于监管方来说，能源消费是一个复杂的消费过程。这一过程中，必须要考虑各种不同的利益关系。

比如在面对有限的资源储量和不断增长的市场需求时，就要进行有效的调控，防止资源被过快地消耗掉。也正因为此，能源领域的消费呈现出更多的矛盾性。一方面是能源企业希望有更多能源销售；另一方面对于监管方来说，却希望限制能源消费，让能源的供需达到均衡稳定的状态。这种矛盾其实很难破解。

世界上任何一个国家都将能源的控制作为国家发展的重要动力，尤其是那些资源出口型国家。而对于更多的国家而言，能源政策的好

坏则关系到国民经济的稳定运行。能源的生产与消费同样也受到了严格的限制，这事实上也在反映能源消费与政策监管之间的不平衡性。

能源政策这种矛盾的本质，其实是有限的能源和人类无限的发展需求之间的矛盾。因此，单纯的监管其实并不能解决所有的问题。即使在今天，政府仍在不断地下大力气进行新能源的开发。但这不是一朝一夕的事，在未来很长一段时间里，我们依然要在现有的能源结构中谋求发展。即使是找到了新能源，我们依然不能从根本上解决能源精准投放的问题。

区块链的出现让人类社会获得了更早进入能源消费配置时代的机会。

通过区块链的模式，我们可以将人类社会所有已经发现和可能发现的资源进行编码，然后在相对开放的网络上对资源的分配进行全面表决，让所有利益相关方共同决定这些能源的归属。这样，能源消费就突破传统市场经济条件下的资源配置，变成了一种真正的资源配置型消费模式。

在中国，这样的尝试已经开始了一段时间，并在现实中运行了很久。

结合前面的经验加上区块链的新技术，就可能为解决能源消耗、环境保护和经济发展三方之间的矛盾开辟一条新道路。

过去，能源消费领域往往被一些企业控制。这些企业本身就有盈利属性，因此在这种情况下，企业的选择自然就是尽可能多地销售资源。

但是这带来了自然资源加速消耗的问题。虽然在解决能源危机方面，政府做了很多的尝试——比如开发风电、水电、核能等新的能源

技术方式，来解决能源相对不足的问题，但是由于这些能源价格过高，人们还是倾向于消费传统化石能源。

另一方面，中国的污染情况已经非常严重。要解决这种问题，单纯地依靠现有的管控模式，不能解决根本问题。

在能源领域，现在的中国需要的是一个通盘考虑的方案，从能源的生产端到消费端，再到最终的污染治理段，形成一个完整的循环管理。在这点上，区块链就有了用武之地。

我们可以这样设想：假如我们并不依据能源的生产价格加上利润的传统模式对资源进行评价，而是依据单位资源所产出的价值来进行评价，那么所有的能源价格都将失去利益属性，而只具备单纯的资源属性。以电力消费为例，不考虑电能的生产端，不论是风电、核电还是火电，对于消费来说都是同样的，这些电力生产者依据不同的产品价值确定价格。

通过区块链，从电力生产到商品生产的全流程成为一个共同的价值链条。通过这种模式，可以保证所有的能源都实现有效利用和价值最大化，避免能源浪费。

区块链的模式甚至可以延伸到后端，直接将价值创造的链条连接污染治理方面。通过这种形式，使能源消费与环境治理达成统一，解决过往的生产、消费、治理分散的问题。

这个过程现在也在缓慢地进行，只是使用的是市场方式，本质上也就是以金钱作为中介——在末端的治理中，让污染企业出资治理，通过增加污染企业的成本来影响他们的消费选择，最终实现消费行为的改变。

但是这种转化过程没有区块链模式带来的变化那么直接。这也是为什么当前污染治理成为国际热门话题。人们发现，那些想方设法鼓励大家消费能源的能源公司，在污染治理方面几乎没有什么投入，而在这些能源公司变得越来越有钱的同时，世界环境却变得越来越差。

通过区块链，可以平衡现在的能源生产的先消费后治理模式带来的环境破坏的影响，而在生产端，这种变化也已显露。

资源的开发和生产最大的危机就是：开发的时候永远不知道是否真的能够产出资源。所以开发前要勘探，前期的风险都由勘探公司承担，而一旦能源储量确定，勘探公司退出，风险又转移给了能源公司。

如果我们用区块链的方式把整个能源的勘探与生产相连接，就可以最大限度地分散勘探失败的风险，同时也能有效地分享能源的产出。

一个链式技术的本质，是信息沟通和交流的通道，而通过将这种链式技术不断地应用到不同的领域，我们能得到的就是一个又一个新的商业模式。



## 第五节 商业领域所期待的区块链

商业的本质是交换的艺术。通过对资源、资金、信息、人才等各种要素进行有效的交换和配置，创造新的价值。要实现这些，商业需要不断创新自身的信息载体，让信息流动更加顺畅，资源配置更加简洁。而这也是信息革命主要希望破解的问题。

在新一轮的信息革命中，各种技术以信息的存储、传输和读取为核心，希望把所有的信息公平、公开地呈现在所有人的面前，让经济学完全信息市场的假设成为现实。理论上，这种市场一旦形成，所有资源都将按照最合理的方式进行配置。

事实上，能够解决信息流通的问题就可以获得更多的价值，这已经被现在各种各样的互联网企业所证明。淘宝、阿里巴巴让世界上的所有供应商和采购商都能在同一个平台上交易，打破了贸易间的第一重基本壁垒；58同城这样的区域信息网络，链家、贝壳等各种各样的专业分类资讯网站，事实上都是在解决信息传输的问题。解决了信息传输的问题，又能带来生产模式的变化，比如建立线上和线下互动的美团、滴滴等。

从本质上来说，这些企业都在改变信息和人们之间的关系。也就是说在商业领域，谁能解决让信息跑得更快、投放更精准的问题，谁就能成为新时代商业信息的核心价值获得者。而一旦获得这样的力量，盈利就变成了一个非常简单的问题。

也正因为如此，商业领域对区块链充满了期待。

今天阻碍商业信息流通的几个基本因素中，居首位的难题是我们无法辨别信息的真假。从古至今，假货、假消息、假情报，都是阻碍

国家正常发展的因素。尽管今天通过不断发展和健全的市场机制，我们已经可以逐渐杜绝这些虚假信息，但是不可否认，在某些平台上难免还是会出现此类虚假信息。那么，如何解决这些顽疾呢？其中一个很重要的方法就是让信息变得真实可查，而这也是区块链最擅长的领域——可以让各种各样的商业信息进行一对一的真实绑定，以确认信息的准确度。

另一方面，市场上的价值变化从根本上来说也取决于信息传递的快速与准确。能否让一条信息在最短的时间内投递到最需要它的人手中，这是商业附加值最大的意义。

路透社有这样一门生意：它通过对全球股市的精准预测和对现金流量的监控，实现了对未来股价的一个预报盘。这个预报盘在大部分人看来是一个公共信息，所有的投资者都可以在世界各大交易所中看到。但路透社还有一项业务——这也是他们最重要的盈利模式，就是会在这些信息正式公布在大屏幕上的几毫秒之前，把它们公布给购买的机构与个人，而这些机构与个人会把这些信息交给自己的操盘手，让他们在市场中进行博弈时，获得几毫秒的优势。<sup>[15]</sup>

这个提前量虽然只有几毫秒，但是对于现今的博弈来说已经足够长了，购买这些信息的企业往往可以通过这个优势获利颇丰。

事实上，这种现象一方面是市场经济发展的必然，另一方面也是我们所不希望看到的通过信息时间差来获利的行为。从根本上来说，这种行为并不见得有利于市场的发展。与这种现象正相反，我们需要的是一个更有效的信息传递手段，让信息对每一个人都公开透明。

但是在现阶段，这一点很难做到。所以我们寄希望于新的技术，比如区块链的诞生，能够帮助我们解决这样的问题。通过使用区块链，可以更好地储存信息；同时在读取的过程中，信息的获取还具有

相对的唯一性。因此，当所有人都需要一段信息的时候，这些人就有可能站在同一个价值链的链条中。以此为基础，再利用区块链的模式，就能把大家的利益系在一起。

这个过程不再像过去一样，要通过购买等非公平的竞争手段来获取。未来，也许几毫秒就不存在了，但是所有人的交易结果将反馈到一个公共账户上，所有人的盈利都将从这个公共账户上按照比例分配。即使你只是进行了一次试错，但是你的行为也是有价值的，那么在区块链的世界中，这些行为都将被认可。

也许这样的世界到来会让一些商业企业的利益受到损害，那些建立在信息不对称基础上的公司将变得一文不值——但是这难道不是商业的本质吗？

商业的本质就是希望能够对资源进行更有效的配置。我们所有人都生活在一个信息共享、信息公开透明的世界中，这不是很好吗？

## 第六节 权属确定不再是麻烦

权属的确定很有可能比我们想象的更为复杂。所谓的权属其实很好理解，就是一件事物或者一种权利到底归属于谁。但是在现实生活中，这个看似简单的事情往往变得很复杂，确认一件商品的所属或确定一个价值所有权，是一个非常困难的问题。

也正因为这样的原因，我们才会有各种各样的公证处以及法院等确认权属的机构。这些机构共同服务，让我们生活在一个可以有效确认权属的法律体系中。但是无疑，通过这样的体系进行法权属确认，不仅要耗费巨大的资金，还要耗费大量的时间。

因此，在日常生活中，权属的确认变成了一件可有可无的事情，只有当极端情况发生——比如要确认一笔大额资金交易或者复杂环境中的真实交易过程以及其他的重要事项时，我们才会想起来进行这种正式的权属确认。

而这又进一步加剧了对权属确认的难度。毕竟，当时看起来并不重要的信息，到最后可能会产生重要的影响。而这些信息被当作无用信息处理之后，人们往往很难找回，这也就意味着确认最终权属之难。

我们也许能发现一个有效解决权属的方案，那就是区块链。权属确认的核心难点在于，我们没有办法掌握一条真正的、有效的价值链条。如果能够完全构建某一种商品的价值链条，那么就可以确认它的最终权属。但是往往这种理想的条件并不存在，我们必须面对的往往是一个杂乱无章的环境。而区块链有可能拯救我们。

在使用区块链进行信息记录和确认的过程中，区块链会自动对所有的信息进行分布式存储。我们也就不用再为那些凭据丢失或者是交易过程消失而烦恼，可以更加自由和洒脱地解决这些问题。

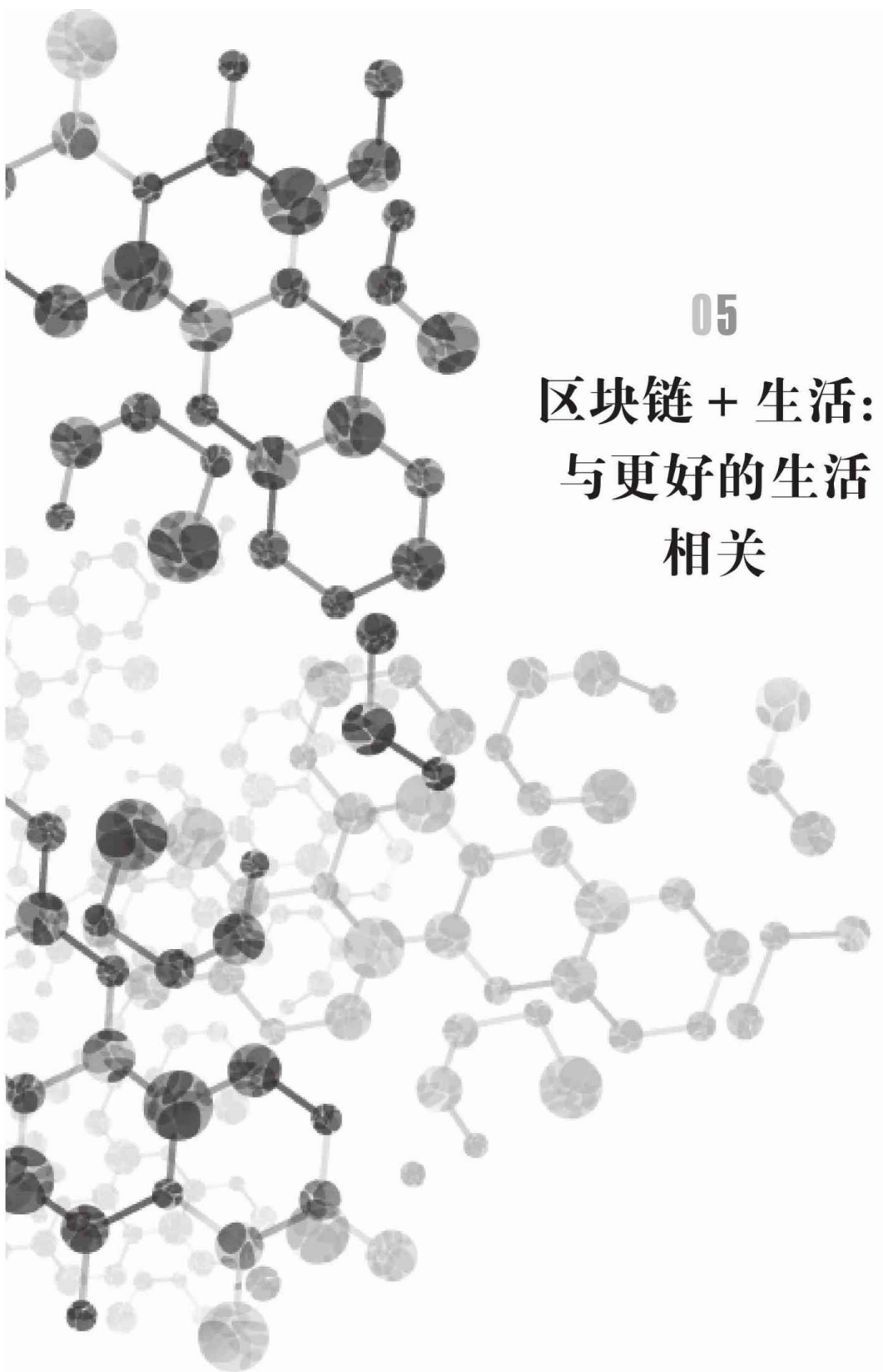
通过区块链的分布式存储和可追溯的模式，我们可以清晰地看到一事物发生发展的全过程，而且分布式存储也解决了过去中心节点存储的巨额费用问题。

试想一下这个场景：面对一个复杂的合同纠纷，我们只要核对各自区块链条码就能知道，产生争议的标的物究竟在它过往的整个价值周期过程中经历了什么。也许我们能看到，原告通过网上交易的形式获取了这个物品的最终价值属性，但是被告却没有完成自己的手续，当物品价格增长的时候，被告突然反悔，不愿意出售了。

类似这种问题在现实的经济纠纷中并不少见，证明这件事是一个复杂而繁琐的过程。但是区块链可以帮我们找到最终的答案，真正高效地解决这些争议。

这可以让我们在权属确认过程中省去很多麻烦。只需要简单地对手中的区块链，核对一下记录信息的种类和大小，就可以判断权属的最终归属。而这一切并不是空中楼阁，它事实上已经在世界各地陆续发生了。一些国家已经开始尝试用全记录的模式记录各种财产信息，一座大楼在建造的时候，人们就将与它相关的所有交易记录储存起来以方便后续查找。通过这种模式，我们可以更有效、更轻松地面对未来，这提高了社会效率，减少了合作伙伴之间的矛盾。

通过发挥自身优势并结合权属确认的需求，区块链可以有效地帮助我们提升工作效率，也可以帮我们节省资源，让我们更好地将手中的资源用在那些更能创造直接价值的领域，而不再为了争论这一笔价值究竟属于谁而影响效率。



05

**区块链 + 生活：  
与更好的生活  
相关**

## 第一节 房产证明可以很简单：分布式数据存储模式下的政府信息安全

说到政府组织运行的效率，很多人都想吐槽，但是从某种意义上来说，政府也很委屈。因为政府面对的数据是海量的，而政府每次做出决定所影响的数据也是海量的，所以它必须严肃谨慎地面对自己所有的决定。更重要的是，政府的数据有更高的安全性要求，大数据的正确与否，可能带来深刻而广泛的社会影响。

《区块链：重塑经济与世界》一书里提到过这样一个案例：

一位居住在洪都拉斯的老太太，住在自己家的房子里30多年，某天忽然两个警察要将她赶走，因为国家财产局的记录显示，该房子为另一人所有。

住了30多年的房子，忽然属于另一个人！如何证明我的房子就是我的呢？老太太出具的土地凭证，在法院也未予采信，并依据国家财产局的记录为准，将房屋判归给另一人。

老太太很无奈，眼睁睁看着自己住了几十年的房屋被拆毁。直到被拆除以后，有人才发现财产局的记录有误，房子确实是老太太的。

[\[16\]](#)

类似这样因为有意无意的记录错误而导致的不公正与财产损失，在世界各地时有发生，但普通人对此无可奈何，因为最终判断的标准掌握在少数人手上。而掌握这些标准的人，就是政府相关部门及其办事员。正因为如此，为了避免这样的事情发生，政府必须严格管理数据，防止数据错误；也因为同样的原因，政府在查询数据的过程中必

须进行反复验证，通过不同部门的数据交叉验证来确保其正确性和真实性。

有过买房经历的人可能知道，想要买到一套房，不仅是一次对金钱的考验，还是一次对体力付出的考验。我们需要在不同的部门之间奔走，寻找相关证明来支持自己的诉求。

从基本的房屋产权证明到个人身份证明，再到相关银行资产的证明，其实核心目的只为一件，就是证明你拥有相关房屋的交易资格。

然而，所有这些证明，并不是由某个政府部门统一管理，而是由多个部门甚至一些社会机构分散管理的。因此对于有这些信息需求的人来说，就必须前往不同部门想办法获得这些证明，最终拼凑出自己要的材料。

这一方面是政府工作低效的表现，但另一方面也显示了政府的无奈。

政府的信息存储必须得是多部门的，因为这涉及政府的权力和管理的基本逻辑。信息的本质就是权力，权力是通过掌握信息的多少来实现的。因此，如果所有的信息都归口于一个部门，那么这个部门的权力将无比巨大。

在我们现行的社会组织中，任何一个政府机构权力过大，都会带来各种各样的问题。所以这些信息必须采用分布式存储，由多个部门共享。这样，权力才能得到有效的制约。

这就意味着政府在存储信息时有一个大麻烦——不能将所有的信息归口于一个中心。我们需要打通不同政府部门之间的接口，才能实现这些信息的互通。



但是打通接口也面临另一个风险——我们不得不为信息安全问题做好防范。任何集中存储模式都有可能被打破。责任的可追溯性，带来的是管理动力的提升，通过这些可追溯的结果，政府部门才能进一步推动信息安全的建立。这样的模式，让各个政府部门不断提高自己的管理水平，把信息存储变得安全可靠，防止被篡改。从这个角度去看，也许我们就能够理解政府为什么采取如此低效的方式去处理和存储信息。权力的分布要求和信息安全的要求，让政府不可能把所有的信息都放到一个“篮子”里。因为那样做，会造成一个权力巨大的机构，同时造成一个巨大的中心信息库的风险。

权力的分布，也许不能通过一项技术来解决。但是一个巨大的信息中心库的安全问题，却是一个复杂的技术问题。理论上我们需要通过不断增设安全网络和安全技术手段，来实现保护功能。

这就导致政府必须不断增加信息安全保护的投入，才能够保证自己的信息安全，不被篡改和利用。在这个基础上，政府才能进一步保证使用的信息是安全、正确和可靠的。

这种做法其实严重阻碍了效率提升。为了解决这个问题，我们可以通过区块链的分布式存储模式来让一段有用的信息变得牢不可破。很明显，如果通过区块连来管理政府的信息数据，就可以极大地提高信息存储的安全性。更为重要的是，可以极大地提高信息的使用效率。

想象一下，假如用这种模式储存政府的各种信息，并用这种区块链储存的信息去解决上文提到的洪都拉斯房产纠纷案件，就可能得到新的解决方式。

政府在调阅各种信息的时候，不再单纯依靠记录文件，也不依靠房主提供的财产文件，因为这两种文件都可能并非原始文件，而是为

造的。

如果使用区块链技术，在最初对这个房子的产权进行确认的时候，就会把相关信息生成一个单一的文件，以区块链的模式分布储存在网络中。当政府与房主起纠纷的时候，只要任何一方能够提供相应区块链的解码方式，找到网络上储存的最初的原始财产证明，就能确认这段信息是真实和准确的。接下来，解决这类纠纷的思路就变得非常简单和清晰。双方不断提供相关的证据链，从区块链的分布式存储模式中挖掘各种各样能够支持己方的信息，找到当时的交易记录。如此一来，只要按时间顺序理顺记录，就能知道这座房子最终的财产所有者究竟是谁。

这样的模式解决了政府单一部门管理造成的公信危机。因为我们并不知道财产相关的数据错误究竟是有人有意为之，还是一个简单的低级错误。这样，政府的效率提高了，使用这些信息的普通百姓更方便了，信息的准确性和安全性也提高了，政府所面对的压力和质疑也会减少很多。

试想一下，如果海量的政府文件全部都通过这种模式储存在网络上，那么我们的诉求就会得到更快速的响应，政府也将因此变得更加亲民、更加可信。

## 第二节 证明“你是你”：分布式智能 身份认证系统

上一节中我们说了关于房产的例子。通过这个例子，我们要说明：政府信息管理中如果引入区块链的方式，可以更加快速准确和直接地解决各种问题，减少矛盾，提高政府和社会的运营效率。

但在日常生活中，我们最难处理的可能并不是这种复杂的事件，而是最基础的个人身份确认问题。

政府管理的基础其实就是确认每一个人是其本人，这听起来可能非常的荒诞。例如我们偶尔会需要开一个证明，证明“我爸是我爸”“我妈是我妈”。但事实上，在政府治理方面，这是一个非常严肃的话题。政府要对自己的结论负责，因此必须有一个有效的方式，通过一种证明文件，证明某个人的身份符合其自称。

在古代中国，政府就曾试图通过“人盯户”的模式来确认每个人的身份。现有的技术是通过身份证的方式，其中包含一些个人生物信息的采集，比如照片。进一步的技术已经可以给予更多的支持，在身份证制作的过程中，已经开始登记指纹来帮助身份验证，这些都是底层的技术突破。

在这个基础上，才能附加财产的认证、权利的认证。因此我们能够从政府的管理逻辑中看到，一个社会运行的根本，在于对个人身份的确认。

这件事情其实非常的复杂和困难。政府投入巨大的财力建立了一个复杂庞大的政府管理体系，来确保自己获得的信息是相对真实有效的。

在这里面特别要说明，这只是“相对”真实有效，而并不能保证“绝对”。因为存储和使用这些信息确实非常困难。

政府在这方面毕竟做了很多有效的工作，因而在各种各样的应用中，很多人或机构会将政府的这种信任机制、身份证明机制作为一个已知条件，通过认证相关的身份证明文件——比如身份证、驾驶证或结婚证及其他身份证明文件，来认定个人身份。现代商业社会在运行中，又在这个基础上嫁接了很多商业的应用与权利的确认。

举一个最简单的例子，假如你要购买某个视频网站的账号，那么网站可能会要你通过手机认证自己的身份。这种认证的有效性究竟有多少？这是一个非常值得探讨的问题。

因此，在其他一些对身份要求更加严格的领域里，就会需要各种附加的条件。比如说，在购买手机卡的时候，我们要提供身份证来证明身份信息。而这种逻辑的前提是，我们默认身份证是一种有效的信息证明文件，它能够证明“我是我”。通过这样的逻辑，导出能提供身份证的人就是这个身份证的所有者。但这样的逻辑通过反复的嫁接被应用于不同的场景中时，就会出现很多问题。

比如，有些人在交友网站中提供的注册信息并不能保证真实和准确，而商业网站也没有能力像政府一样建立一套完整的体系，保证它收集的信息是真实的。这进一步带来了社会风险，比如诈骗甚至其他犯罪行为。

另一方面，在现实商业社会的运行中，个人信息泄露成了一个大默认的规则。不论我们做什么事情，即使仅仅是想要办理一张蛋糕店的打折会员卡，也需要“出卖”我们的个人信息。这带来了很大的风险。

那么有没有一种简单、高效、低成本的方式，让我们能够更加有效地进行身份认证，在各种商业领域使用自己的身份呢？区块链为我们提供了这样一种解决方案。

假如我们有一个安全准确的信息存储模式，让所有的信息可以公开地流动，当验证这些信息的时候，我们只需要证明自己是这个信息的所有者就可以了。这种时候，我们就不再需要复杂的社会认证体系了。

而且，我们将可以建立一套全社会的分布式信息证明体系。在这个体系中，我们真实的信息、底层的数据和基于政府的复杂管理系统的各种有效文件，都可以保存在一个区块链中，且这个区块链中的信息是不对外公开的，采取保密的存储模式。当我们需要使用这些身份信息的时候，只需要输入对应的提取编码，就可以提取它们，然后通过证明这些信息的真实有效，就可以确定身份。

这样，相关的商业系统所获得的仅仅是我们不完整的信息区块，而不能获取我们全部的、本质上的信息。这样的商业模式和逻辑，带来的就是个人身份信息更广泛和安全的应用。

这样的模式可以有效帮助我们实现信息的整合。比如一个区块里可能储存了身份证信息、婚姻状况和财产信息，但这些信息都不是完整的，只是其中的一部分。

于是，我们就能够利用这些信息形成一个包含了所有信息的区块组合，来证明我们是谁。而这些信息储存在分布式的各个政府部门网站中，在使用的时候，就不用在各个政府部门之间经历证明自己身份的过程了。

当然，将一套社会身份信息认证系统研制出来，让人们能够应用这套系统验证人员的身份，但是却不能提取和存储信息，这是区块链3.0在探索的问题。

通过什么有效的方式和载体，能够真正地实现个人信息的传输和使用？如果能够突破这一点，那么区块链就真正完成了从一般的电子代币再到分散式的研发、进一步实现全社会信息流动的使命，也就真正能够完成进化了。

但是如果在不能实现这一点的情况下贸然采用区块链储存身份信息，就不能实现我们的目标。要实现区块链对个人身份信息的安全传输，必须要建立一套验证区块链而不是提取区块链的信息认证系统。而这种信息认证系统的建立，必须由政府去推动和实施。

相信随着信息存储技术的快速发展，我们使用区块链技术进行安全的信息传递的日子将会很快到来。

### 第三节 打破医疗困局：区块链视角下的 健康联合体

医疗改革不仅在中国是一个非常热门的公共话题，在全世界也是一个难题。从美国前总统奥巴马的医疗改革计划到以色列的全民医疗，几乎所有国家都在想尽办法提供更好的医疗服务。当然，这也是有代价的，各国的财政都在医疗改革方面投入了巨大的资源。而区块链，可能给我们提供一个解决这个问题新视角。

医疗改革的本质是三个问题：第一个是医疗技术水平不能解决所有医疗需求的问题，第二个是医疗资源分布不均衡的问题，第三个是医疗信息不流通的问题。

医疗技术水平的问题有两个方面的表现：一个方面是以医学研究的绝对技术水平还无法治好人们所有的疾病，另一个方面则是新发明的医疗技术价格过于高昂。

医疗资源分布的问题则体现在有效的优质资源不能被最需要的人享有。所有国家和地区都必须面对这个问题。

最重要又容易被人们忽视的一个问题则是医疗信息的流动。按照我国现行的医疗改革方向，以社区医疗为基础、核心医院为支撑的医疗体系 [\[17\]](#) 的搭建过程中，最核心的就是医疗信息的流通问题。

区块链对解决这几个问题都有着得天独厚的优势。

首先，在解决医疗技术水平的问题方面，区块链可以真正地加速医疗技术的发展和普及。

医疗技术的研究需要耗费大量的资金和时间，例如今天我们熟悉的阿司匹林，曾经耗费了拜耳实验室几十年的时间来研发。如果这些投入全都由一家商业企业来承担，那么要收回成本的唯一方法就是提升终端的药品价格。这也是当今很多抗癌药物研发成功，但是大众却无法得到普遍治疗的原因。

区块链可以解决这个问题。通过去中心化的融资模式，区块链可以鼓励社会以最大的力量创新，在解决单一投入的问题的同时，又可以减少每个研究节点的研发投入。

拜耳实验室的阿司匹林研发经历了近200次失败，仅拜耳实验室的研究团队就耗费了将近40年的时间。但是我们如果用区块链模式帮助研发，就可能改变这一点。在尝试阶段，研究组就可以把要尝试的方向和项目发送到以区块链为媒介的研发网络上，由分布在世界各地的人组成项目研究组。

由于传统的研发模式属于“专利专属”，也就是研究者一旦成功，就可以获得全部的权益，因此时间竞争压力很大，一旦比其他项目组晚，就意味着彻底的失败。而区块链重新定义了这个逻辑，让所有的参与者共享最终的研究结果。这样一来，就在客观上让更多人能参与到研发中，提高了药品研发的效率；而分散式的研发，也降低了单次投入。

这样的结果就是医疗技术研究效率快速提升，而终端的消费价格则快速下降。

当然，区块链技术在医疗技术研究领域的应用才刚刚启动，由于医疗实验的伦理性和医患数据的敏感性等原因，这方面的应用还不是区块链解决医疗问题的主要发力点。在医疗资源的平衡和数据的流通方面，区块链更加游刃有余。



传统医疗中一个难以解决的问题是医院之间的信息不互通，一个患者的信息只能在一家医院的中心数据库里留存，这带来了很多的不便。

我们可以回忆一个过去常见的场景：医生的处方一直是一个让人觉得有些“抓狂”的存在。我们在一家医院诊断的结果、开具的手写处方，拿到其他医院就没有人能认识，最后患者还是要回到最初就诊的医院才行。

今天，医院的数据化已经大大地缓解了这个问题，医生的诊断和处方通过电脑记录，统一存在医院的数据中心。

这样做虽然解决了医生手写处方读不懂的问题，但是并没有解决医院之间数据的互通问题。既然已经实现数字化存储了，为什么不让数据库连接互通呢？

事情没有这么简单。我们知道，医疗信息是高度敏感的个人信息，因此各家医院都将患者信息作为高度保密的信息来管理。对于单个医院主体来说，信息外传的风险一般以管理手段来防止，比如建立自己的保密制度，设定专门的权限控制复制和传播，选择恰当的保存介质如光盘、受限制的硬盘等。一旦发生泄密事件，医院就可以依托自身的管理体系进行责任追究和制度完善。

如果医院之间互联互通，那么情况就变得非常复杂了。一旦有患者的医疗信息被泄露了，就会演变成一场查实过程的灾难，各家医院会为了“谁担责任”而争吵不休。这也是医疗信息最终变成信息“孤岛”的根本原因。

如果使用区块链来解决这个问题，就变得相对简单了。区块链最大的特征之一就是去中心化，那么按照区块链的逻辑，医院之间的信

息互通就不是现在这个模式了。

所有的医疗信息不再存在于特定医院的特定中心，而是随机地存储在不同的设备中。比如，A医院的病例信息可能存储在B医院的C电脑当中，但是这些数据是相对无意义的。对于任何一个看到的人来说，它们也许只是一些随机的代号和数字，只有拿着秘钥，才能找到这些信息真正的含义。而拿着秘钥的人就是患者自己。只有当他需要提取自己的病例信息或者将自己的病例信息授权给特定的人看的时候，这些无意义的信息才会变成有意义的疾病信息。

这样做的好处是，不再有集中存储的信息中心，也不再有一家对这些信息负责的医院。医院不用担心信息被窃取和滥用，而疾病信息回归到了真正的拥有者手里。

在这个基础上，医疗信息不再与医疗方案绑定在一起，病人可以带着自己的信息在医院之间选择，而不用担心自己的医疗档案信息。这其实也在某种程度上解决了病人的自由流动问题，可以缓解大医院的就诊压力。

这一切已经有了一些实践性的尝试，比如阿里健康。随着区块链技术的发展，它找到了一个提升医疗服务的方法。

2017年8月17日，阿里健康宣布与常州医联体合作，用区块链的方式打通常州医联体范围内的医院之间的信息关联，提高信息的流转效率。

具体来说，它通过三个层面来解决常州医院之间的信息连通问题：首先，区块链内的数据存储、流转环节都是密文存储和密文传输，即便被截取或者盗取也无法解密；其次，为常州医联体设计的数字资产协议和数据分级体系，通过协议和证书约定上下级医院和政府

管理部门的访问和操作权限；最后，审计单位利用区块链防篡改、可追溯的技术特性，定位医疗敏感数据的流转全过程。

常州模式的主要目标是打通常州地区村镇一级卫生院、综合医院和三甲医院之间的关系，提高医疗体系的诊疗能力。<sup>[18]</sup>阿里健康利用自身熟悉的互联网技术，应用区块链模式做了一次尝试。

虽然这种尝试目前还在有限的范围内，但是未来的应用前景却非常光明。如果常州模式成功，很有可能彻底改变中国的医疗现状，推动我们的生活发生变化。

## 第四节 消灭贫困的区块链

贫富差距是一个世界性的重大问题，很多国家为这个问题所困扰。世界上出产顶级富人最多的国家，往往都存在贫富差距非常严重的问题，比如印度、俄罗斯、墨西哥。这些国家都有富甲一方的富豪，但是同时还有大量赤贫群体。

如何才能消除贫困，成为人类一直在思考的问题。早期联合国有专门的扶贫部门<sup>[19]</sup>，而随着整个世界的发展，联合国千年计划也进入了新的阶段，这一阶段的目标就是尽可能地消灭世界上的贫困。

如何解决贫困问题？各国政府采取了各种各样的措施，而中国在这方面无疑是非常成功的。很多国家专门向中国寻求消灭贫困的方法，联合国甚至成立了提取中国经验的机构，把中国各种各样的扶贫方式向世界推广。比如中国南方的梯田就被作为一种非常好的方法，向世界上那些土地贫瘠、粮食生产能力有限的国家推广。

随着中国经济的发展，有越来越多的中国扶贫方式被作为成功经验对外输出。最典型的就中国的基础建设。

“要想富，先修路”，这是人们耳熟能详的一句话。中国贫困地区快速减少的一个重要原因就是基础设施的建设。

道路的通畅能够带来三个方面的变化：第一个也是最直接的一个方面就是物流的变化。通过道路可以把贫困地区生产的各种物资、土特产向外运出，增加当地居民的收入；第二个方面的变化是人流的变化。通过道路的修建，让更多的人来到这些地区。人流可以狭隘地理解为本身的人的流动，他们可能是商人，也可能是游客，可能过来推销商品，也有可能过来采购商品，还有可能留下大笔的消费，这些都可

以推动当地经济的发展，让当地人变得更加富有；第三个方面的变化是信息流的变化，在某种意义上，这种变化甚至更为重要。在互联网还没有这么发达的时候，信息往往需要通过口口相传的模式来传递。道路修通了，贫困地区的人就能看到外面的人，就会有新的想法、新的变化，这会从根本上推动当地的经济发展。

以印度的很多贫困地区为例。当地政府采取了很多方式希望这些地方能够发展。但是由于传统观念的束缚，当地人甚至完全不了解外界。这导致印度政府很多扶贫举措没办法真正沉淀到乡村的基层中。

大量的基础建设可以让贫困地区的人们看到与外界的差距，看到自己追求和努力的方向，这能产生持久和有效的动力。这是基础建设能带来的最根本的变化。

一方面，基础设施的发展已经越来越完善，投入也越来越高；另一方面，我们不可能要求所有的贫困地区都能像那些快速发展的地区一样，拥有大量的人流和物流。

通过区块链的模式，就可能改变这种信息使用方式。我们可以通过分布式存储，有效地识别和验证一个地区真正的贫困原因。

传统的信息技术扶贫模式，其实并没有做到对贫困人口和贫困地区的精准识别。因为与相对复杂的经济信息变化相比，政府依据的往往是某些固定时间节点的信息，如一年或者两年进行一次的经济普查、人口普查等。

更重要的是，录入这些重要信息的人往往是基层的公务人员。他们采用电子表格的形式，把需要的信息录入。而这一过程中，可能存在大量的人为失误甚至是故意为之的错误——在某些情况下，由于基

层人员急于实现自己的工作目标，他们甚至会伪造数据。这些数据汇总起来，最终可能让政府的决策有失偏颇。

区块链技术改变了这样的存储模式。所有信息不再由个别基层公务人员汇总和统计，而是可以由相关人员自己维护。信息被输入到一个固定的模板里，同时进行分布式的存储，并且在所有有关部门中流转。任何一个部门使用的时候都可以随意地点开，看到想要的信息。

这件事情的重大意义已经远远超出了信息本身。我们可以想象这样一个场景：过去政府的运行模式中，不同部门往往有不同的考核指标，例如医疗部门可能关心居民的健康状况，财政部门需要了解当地税收和企业发展情况，环保部门要了解当地的环境是否达标、工矿企业污染是否超标等问题.....

面对这些不同的检查时，个别基层公务人员为了完成自己的业绩，往往会根据不同的需求来提供不同的统计数据，而这些数据甚至可能是相互矛盾的。

然而，由于数据的海量性，任何一个部门都没有办法去验证它。而在区块链模式下，不再需要工作人员提供相关的数据，而是会更加全面系统地将数据以结构化的模式存储在分布式网络中。

这样，任何部门都可以直接获取这些底层数据来支持他们的政策，制订相关的扶贫计划。这样无疑可以带来更有效的扶贫结果。

在这方面，中国已经有了很多具体的实践。中国扶贫难度最大的贵州地区，已经率先成立了以区块链为底层技术的大数据分析中心，尝试用大数据的方式解决扶贫的精准性问题。

贵州地处我国西南地区，至2017年年中依然有50个以上的国家级贫困县，其中多数分布在黔东南苗族侗族自治州、黔西南布依族苗族

自治州、铜仁市这几个区市。贵州这几年在新技术成果试验上走在了国家的前列，是国内首个建立大数据国家综合试验区的省份。据了解，国家批复贵州成立该试验区的时间是2016年2月，目标之一就是建立“大扶贫”战略方向。2016年年底，贵阳市发布了《贵阳区块链发展和应用白皮书》，宣布搭建区块链扶贫和电子政务的“沙盒测试”环境。从近些年“区块链+”的落地情况来看，贵州省贵阳市是我国率先将区块链技术应用到电子政务中的地方之一。 [\[20\]](#)

2017年5月，在大数据实验中心，贵阳首个“区块链+扶贫”项目开始运作，针对的扶贫对象是贵阳市白云区红云社区城镇的低收入人群和残障人群。目标是搭建红云社区区块链助困系统，通过区块链平台记录贫困、残障人员的身份信息和扶贫助残的服务信息、资金流向信息。

## 第五节 让艺术家们掌控自己的作品

如果要问区块链至今为止最成功的应用是什么，那么除了各种各样的虚拟货币，就是数字娱乐领域了。

几年前，线上音乐的快速发展带来了一个非常麻烦的问题——音乐版权的确认。在此之前，歌手演唱的歌曲的相关版权都会交给所属唱片公司，唱片公司为了宣传，又会制作各种各样的版本，有些提供给电台、电视台，有些提供给演出机构，所有版权的获取都要通过同一个唱片公司。

数字化娱乐的出现严重冲击了这种出版发行模式。在原有的法律体系中，唱片的出版——包括录音带、光盘——都有介质，而互联网上的音乐往往是开放、分散的，大家免费享有这些音乐，不支付任何版权费用。

传统意义上，音乐出版方的盈利模式是向那些有偿使用音乐的使用方收取费用，但是在实际的推广传播中，出版方往往很少收费。比如电台使用的各种音乐版权并不一定是有偿购买的，因为音乐想要实现盈利，必须要进行推广，而在传统的音乐推广过程中，传播往往是可控的。

互联网的音乐使用形式，让用户有了选择权。他们可以选择在什么时间点开这些音乐网站听这些歌，甚至可以选择循环播放这首歌。听音乐的人有了筛选的自主权，也就对唱片公司的各种出版物失去了兴趣。

这带来严重的问题——唱片公司的利益受损，但这些音乐网站又不向任何用户收费，因此，唱片公司也很难向网站收费，但是传统音



乐出版物销量的减少却是实实在在的。由此，唱片公司和音乐网站之间，产生了一场旷日持久而规模浩大的诉讼。

被卷入这场诉讼的，包括当时的音乐巨头索尼、滚石等，同时包括一批知名音乐网站。大家也都意识到：如果不通过付费模式有效地保障歌手和制作人的利益，音乐的创造和制作将会受到极大的影响，音乐的消费者自然也就享受不到优质的音乐了。最终结果是，音乐网站开始尝试以付费模式向客户提供音乐下载服务，同时将原来无限制的播放模式改为有限的试听模式，并向唱片公司支付一些费用。这样一来，解决了数字娱乐中的大问题。

此事有没有更好的解决途径呢？区块链提供了这种可能。假设一名创作人创作了一首歌，并将这个创意作为区块链上的一个节点进行发布；一名音乐制作人看到这首歌，认为它很有可能变成一首流行歌曲，于是把这首歌制成了demo（样本唱片），并将这个demo交给了一名知名歌手；这位歌手也认可这首歌，于是进行了深情演绎；正式录制的歌曲上传到网站上传播，所有传播的节点和创造的价值都可计量。当这首歌被一些商业机构用于商业演出或者其他的营利活动时，所有的收入都被记录在这首歌的价值链条上。这样，所有人都能从中获益。而承担这些成本的，也是价值链上的所有人。

通过这样的模式，我们就可以完成一首歌积沙成塔的过程，无数用户和无数分散的制作点，都是这首歌成功的保障和价值的产出。

想象一下，如果这种模式全面地应用到我们的商业活动当中，会带来什么样的变化？

今天困扰很多数字娱乐公司的一个重要问题是，在早期的商业竞争环境中，数字娱乐公司为了培养用户习惯，把他们从传统的电视广

播吸引过来加入线上电子娱乐，必须采取免费的方式。但随着整个市场的快速发展和成熟，这种免费模式终究不能持续。

为了盈利，很多线上平台转为付费制，而这样的措施却造成了客户流失。这成了一个难解的悖论，因为没有人愿意改变自己的免费习惯，虽然他们可能愿意为自己喜欢的内容付费，却并不喜欢将这些费用付给网站。其中一部分人会觉得，自己应该把钱支付给内容的提供者，而不是传播者。

区块链的模式可以解决这个问题——让所有人为某个内容付费，而关于这个内容的所有收益，将会被公平有效地分配给整个利益链条上的所有产出者。通过这样的模式，就可以对优质的内容付费了。

这就打破了传统娱乐出版发行的流程。消费端可以为喜欢的节目买单，而不再需要接受那些强制的营销手段和捆绑式消费；真正的内容产出者也因为这样的变化可以获得更好的收益。

当然，那些传播平台也会从中分得利润。事实上，我们“挤压”掉的是原来产业链条上并没有给我们带来实际价值、却控制着核心渠道的分销商的利益。这些利益将会被有效地回报给消费者和内容产出者，让我们的消费更加精准和直接，让数字娱乐业实现真正的价值增值而非各种各样的炒作和操作增值。

## 第六节 农业迎来区块链的春天

农业是人类社会发展的第一个产业，是人类最古老的生产方式。它在漫长的发展历程中不断地进化。今天我们所看到的农业已经与几千年前的农业大相径庭了。然而，来到互联网时代，农业发展和进化速度却开始相对变慢。我们使用的手机、电脑、汽车等产品每年都会涌现出更新换代的产品，而农产品却似乎一成不变。

不管是蔬菜水果还是粮食，好像都难有根本性的突破。从某种角度来说，今天的食品安全问题，主要是由农业生产端到流通端的整个链条管理的不规范所造成的。

信奉“民以食为天”的中国人，在现代社会却常常遭遇一些难以想象的食品安全事件。比如某些区域的土壤、水源遭到严重的污染，当地生产的粮食已经含有一定的毒素，给我们的身体健康带来巨大的隐患。而我们又很难界定这些商品到底来源于哪里，哪些可能给我们带来危害。举一个典型的例子：超市里售卖的各种包装高端的蔬菜，以绿色、环保、高品质等作为卖点，价格昂贵。但这背后其实存在两方面的问题：一方面是产品本身的追踪是很难做到的，可能需要通过大规模的物联网技术和可追溯的产品流通和生产环节来实现这一点；另一方面，我们对这些商品的信任很难建立起来。

而对于信任问题，区块链是一个非常好的解决方案。试想一下：假如我们在面对一个商品的时候，可以完整地看到它的整个生产和运输的流程，一目了然地看到各种相关信息，并确保这个商品准确的来源和属性，那是不是就可以放心地消费了呢？

在目前的农产品安全领域，质量控制是通过节点倒查的方式实现的——用下一节点去验证上一节点的农产品是否来源于正规渠道。如果来源于正规渠道，就默认这个商品是正确的，然后再进入下一个流通环节。

这种方式一方面从实际操作性来说，越往后的节点越不可能管控整个流通流程。因为想管控全部的流程，需要进行复杂的监控，这就需要大量的人力和资源的投入，这显然是不现实的。

而另一方面，消费者最终拿到商品的时候，也很难通过商品的这些记录明确认识到，这件商品到底是不是他们希望的绝对安全的商品。

要想解决这两方面问题，一个很简单的模式是：使商品可以在终端消费的时候追溯全部过程。

区块链可以帮我们实现这一点。通过一个特定的区块链数据提取，消费者就可以看到农产品流通的全部流程，同时也能看到各种各样的生产信息记录在这个数据块里。

假如我们在超市买了一个西红柿，但是觉得口感并不像宣传的那样好吃，那么我们就可以回溯查看。对农产品生产企业来说，可以看到整个生产、采摘和流通环节是否有问题。比如运输过程中是否过多地使用了辅助成熟的药品、保鲜条件是否达到等等。这有利于促进整个农业生产和流通水平的提高。

而这种模式的建立也能进一步推动整个农业附加产值的快速提升，甚至可能催生出新的农业生产模式。正在逐步推广的订单式农产品生产模式可能就是受益者之一。

订单式农产品生产指的是，消费者可以根据自己的需要，从农场直接订购想要的蔬菜。这个时候就产生了一个问题：我们可以通过各种各样的方式选择我们要种什么样的蔬菜，比如选择什么种子、采取什么样的种植管理、采取什么模式除虫等等，但是这里有一个核心的信任问题，就是消费者其实并不知道在严密监控的过程中生产出来的商品与拿到手中的商品是否是同一个。

用区块链模式，消费者就可以查询所有的信息来实现对商品的真正身份的验证。我们可以查看它的品种与整个生产过程等所有的相关记录，而这些都整合在我们手中的区块链中。

这种情况下，任何人都不可能篡改这些数据，因为所有的记录都被分布式存储在不同的信息节点中。任何一个企业或者组织都不可能找到所有相关信息并把它们整合成一个新的数据模块，因此能够保证我们拿到的这个产品就是我们最初选择的。

试想一下，如果这种模式得到全面推广，每个人都可以定制属于自己的农产品，农业生产就可以从固有的生产模式转化为我们所期待的根据不同人的需求定制化生产的过程。

但是，农业的改造在整个信息改造中是最复杂的，这主要体现在基础数据的庞大，现有的技术很难保证对每一件农产品都进行追踪。

## 第七节 搭建“公益寻人链”

儿童走失一直是一个非常严重的社会问题，一个家庭如果发生这样的事，将是非常大的打击。

儿童走失主要有两种可能：一种是人为的拐骗，另一种则是儿童无意间走失。这两种形式的儿童失踪给家庭带来的伤害是一样的。

在国外，人们越来越关注儿童走失事件，并且开发出了针对性的安伯（AMBER）警报系统。这个系统强调，只要是儿童走失案件，警方会立即立案并开展搜寻工作。在一定时间内，就会将失踪儿童的相关信息向全国所有的警察局等相关执法机构发布，并且通过公共电视与广播频道，不断播放相关信息，以求尽可能快速地找到失踪儿童。

寻找失踪儿童的黄金时间，大约只有短短的几个小时。而随后的72个小时，则是最后的可能找到的时间。一旦失踪超过了78个小时，儿童被找到的可能性就将低于30%。因此，为了快速传播儿童走失的信息，就需要尽可能快速地调动尽可能多的社会资源。

中国公安大学的一位教授曾经开发出一套寻找走失儿童的8点循环法则。这种寻人的方式是：一旦发生儿童走失，迅速安排8名成年人，其中4名沿着东西南北4个不同的方向寻找，另外4名则快速地前往在周边两公里范围内的主要长途车站、火车站、港口等交通枢纽。通过这种模式可以比较有效地找到那些被恶意拐骗的儿童。

所有这些方式依然不能达到我们所希望的结果。从2012年开始，腾讯尝试利用各种404页面——也就是无法打开而报警的页面——来发布儿童走失信息，通过这种方式，尽可能快速、广泛地传播走失儿童

的信息，来提高儿童被寻获的可能性。这种尝试也被称为是中国民间的安伯警报的建立。

但是这个404系统存在的问题，是不能真正有效地对儿童走失的信息进行大规模的传递。因为404页面是人们在浏览网页的过程中产生的，不能保证看到相关页面的人能够提供有效信息。

而随着区块链的发展，尤其是在腾讯开始系统地研究如何建立中国信息社会的信任底层基石的问题后，腾讯开始使用一种新的形式来发布儿童走失信息，即通过微信、QQ等终端。这种模式可以快速地将儿童走失的信息传递到人们使用的各种信息终端中，让人们及时关注相关资讯，迅速地调动更多人参与到寻找失踪儿童的行列中，增加寻获可能。

随后，腾讯又将其在区块链方面的丰富经验移植到公益慈善领域，连接起各大公益平台的数据。腾讯可信区块链写入全球PFIF（设计用来在不同政府、信仰组织或其他的一些灾难中生存者与亲人联系的网站间进行数据交换的协议）寻人协议，从我国的实际情况出发，凭借成熟的区块链“分布式账本”，搭建起“公益寻人链”。

使用“公益寻人链”的公益慈善机构可以进行数据的分享；另一方面，它们依然能够保持各自独立的筛选机制和自主性。区块链技术的引入，使各个机构能更高效地合作。

传统意义上的寻人启事需要逐个发布在多家平台，而腾讯“公益寻人链”推出后，只需一个平台就能完成多平台同步发布、多平台同步实时更新。区块链技术将多种寻人信息发布渠道有效地联合起来，将原本的各平台独立运营变为多点联动，实现1+1>2的效果，帮助失联人员尽快与家人团聚。

从某种意义上来说，公益区块链的开发，代表的是整个公益事业发展的趋势。通过与区块链技术的快速连接，公益可能可以变得更加有效、有针对性。

各种类型的骗捐、挥霍善款等慈善领域的负面事件，曾经让中国慈善公益体系的社会认同度降到最低点。随着近年来中国各种大型企业对社会公益的广泛关注，情况又有所好转。越来越多的企业投身到社会公益事业中，并不断探索新型的公益服务模式。

而未来随着区块链技术的广泛应用，我们就可以真正地追踪每一笔善款最终的消费节点和使用节点。这样，所有的社会捐赠体系和捐赠人就可以准确地了解每一笔捐赠、每一个慈善活动的实际效果和这些爱心所帮助的真正人群。这可以极大地提升公众对于参与慈善活动的兴趣与信心，让人们更加安心地奉献爱心。

从这个角度来看，区块链与公益之间的结合，其影响可能已经远远超过了公益本身，这种结合可能会带来整个社会信任机制的重新构建。这也许正是区块链与慈善相结合的真正意义。



An abstract graphic on the left side of the page, featuring a complex network of interconnected circles and lines. The circles vary in size and are shaded in different tones of gray, creating a sense of depth and movement. The lines connecting them form a web-like structure, reminiscent of a molecular model or a network diagram. The overall effect is a dynamic and intricate visual element that complements the technological theme of the text.

06

## 新的愿景：区块链应用时代

## 第一节 区块链3.0不同在哪儿

区块链3.0的时代，到来得比我们想象的要快很多。

与其他产业相比，区块链的进化速度确实异乎寻常。虽然从本质上来说，区块链的底层技术并没有什么根本上的创新——从技术上说，区块链依然是以分布式账本、多维度存储技术和新的密码技术为基础。但因其应用范围的大规模扩大，我们把即将到来的区块链应用的时期称为区块链3.0时代。

区块链1.0时代主要探索的是区块链本身的技术应用，研究的重点是其作为安全货币和分布式账本的作用，主要功能还是围绕支付、信任而开发的；到了2.0阶段，区块链的发展趋势与重点变为如何更好地与日常生活相结合，实实在在地解决一些日常生活中的需求，其中包括我们熟悉的物流网络、物联网、万物互联等这些相互关联、形成一个综合网络的互联互通技术。

而到了3.0阶段，区块链与大数据、人工智能技术彻底融合，通过新的区块链技术，实现新的存储模式的创新。这实际上也是区块链3.0的根本特征之一。

区块链3.0与区块链1.0、区块链2.0最重要的一个区别，就是这种技术的使用方式与领域，而非其底层技术的变化。主要表现在通过区块链技术实现个人全部信息的综合传递和安全存储。如果实现这一点，带来的变化将是巨大的。

通过全面与政府公共部门展开合作，区块链可以更好地储存个人全部信息，将我们的个人身份信息、证件信息与公共信息，甚至财产、健康信息等数据全部进行分布式的存储和连接，通过这种安全的

存储模式，实现真正的大数据化。这将是区块链3.0应用的一个非常重要的方向。通过这样的模式，区块链3.0可以有效促进整个社会信息的传播和流动。

首先，安全地传递个人信息，可以提高社会的运转效率。如果仔细思索就可以发现，实际上我们身边的许多设计都是为了能够安全有效地传递信息。

比如，我们最常用的密码系统其实就是通过无数个配对的密钥，实现信息的提取和使用，这样一来我们就能在各种各样的环境中验证身份。

虽然很多人希望能够将所有的密码与个人挂钩，实现使用上的方便，但是这却并不容易。其中很重要的一个原因就是我们的个人信息安全难以保证。

如果将一个人所有的密码统一设置在同一个存储空间中，就会让这个空间变成传统意义上的数据中心，这将是非常危险的一件事情。

一旦这个数据中心被攻破，那么我们所有的个人信息都将会泄露，因此我们无法对密码进行统一存储。前面已经说过，区块链技术的本质是一种可信任的密码存储和分布式存储的模式，所以在这种模式下我们就可以毫无顾忌地把个人的全部密码和相关的身份识别信息存储在同一个逻辑存储空间中。这样，我们就可以最大限度地实现人与人之间、人与信息之间、人与物品之间的交流，最终达到人与一切的交流。

比如我们出行时，往往需要打开一个又一个不同功能的App，为我们提供机票、酒店、租车等各种服务，以及当地游玩美食的建议。如果能实现这些App的底层互通，我们就可以在一次登录后便捷地获

得不同的服务。但其风险也显而易见——我们将各种各样的个人信息和消费偏好全部授予这些互联网公司浏览，能否保证我们的信息安全、保障提供的服务十分精准？

未来的区块链3.0技术将有可能彻底解决这类问题。我们可以使用无数个App，把我们的消费习惯充分个性化，在不同的App的帮助下消费，而现在阻挡我们的密码存储问题将通过区块链获得完美的解决方案。

## 第二节 基础设施建设的效率密码

基础设施建设一直都是一件耗资巨大、涉及国计民生的事情。要提高基础设施的建设质量，就有了区块链的用武之地。基础设施建设中最重要的是进行资源的有效配置，保证基本的建设质量，更重要的是确保不会出现方向重叠和浪费。

区块链3.0的核心是在于对各种信息进行有效编码。在基础设施领域，我们也可以广泛地应用这种编码体系。在基础设施建设过程中，相关人员可以通过广泛的数据分析得出最优的配置方式。

基础设施建设包括两个部分：一个是我们熟知的公路、铁路、楼宇建筑等方面的建设；另一个则包括了更广泛的设施，包括水电、能源、通信等我们虽然看不到但是却要维持社会正常运转的各种供应体系。区块链在这两个方面都有着无与伦比的优势，可以快速提升建设效率。

首先，从基础的城市设施建设来说，由于现在的设计及建造技术越来越发达，很多建筑也变得越来越智能化、体系化，可以通过遍布整个设施的传感系统收集各种各样的数据。在传统的应用中，这些数据会被存储到设施所在的固定服务器中，但这个服务器本身的存储能力是有限的，而且因为没有在很短的时间内被分析和应用，数据很快会变得无用。

而长期存储的数据和快速使用的数据，对于计算的要求都非常高。长期存储的数据需要大量昂贵的设备才能保证存储的可靠性，快速的数据处理则需要强大的运算处理系统的支持。在现有的环境中，如果我们想实现这两点，都需要投入巨资引进与购买相关电子信息设

备，但建筑商们显然没有这样的动力。这样一来，我们宝贵的建筑数据就白白浪费了。

类似的事情可能也会发生在道路上。比如，道路养护部门会定期抽查道路的各种安全数据，包括路面硬化程度、沥青的损耗程度等等，但是这些数据往往是一次性使用，不能长期地存储，更不可能形成系统、完善的数据分析应用。而且，不同的记录信息可能在不同的存储环境中会有不同的应用场景，有的会被放弃或者处理掉，有的则在提取阶段就并不完整，无法得到我们需要的应用信息。我们拿到的可能只是一个小范围内的区域性信息，并不能体现真正全面的信息。这其实在一定程度上阻碍了整个社会基础设施的建设。

更根本的问题是，我们目前对于基础设施的规划，更多地还是依靠专家经验和过往数据的积累，并没有真正达到精细化测量和分析应用的程度，但这个难题通过区块链就可以解决。

区块链可以帮助我们信息存入各种空闲的存储设备中，同时又可以利用相对空闲的设备的运算能力，进行大规模的数据分析，就如同今天的数据“挖矿”，实际上使用了大量的社会富余计算能力。

而对于整个基础设施需求的测算，则可以通过分布式的数据存储来实现真正的大数据应用。同时，区块链在水电与能源供应方面，有着更广泛的应用前景。

这种应用前景主要体现在对既有能源消耗模式的改变。能源供应商主要考虑的是如何开采能源并把能源输送到终端的消费者手中。在这过程中，供应商主要的价值贡献和利益增加点，主要是开采和输送能源的模式，但这一模式却忽略了非常关键的一点，那就是资源的使用效率。

在整个能源供应链中，往往由终端的消费者来决定能源消费的最终数据形态，这事实上造成一种相对的资源浪费。也就是说，能源公司根据他们认为的客户核心数据进行能源匹配，但是却并不了解每个用户到底有什么样的需求，这样必然会带来一些资源的浪费。

最典型的是电力消费领域，因为电力往往处于生产与消费瞬时同步的状态。因此，电力的消耗是一个非常复杂的运算过程。电力的实际研究中，有一门专门的学科叫作电力负荷运算，其中的重点内容就是预测下一个时间点上的发电量。那么，这就又带来了一个问题，一个时间点内发出的电能可能没有办法完全被消耗，其中一部分就被浪费了。

为了解决这种问题，利用区块链的技术可以形成新的电能消耗模式——电力并不直接输送到终端消费者处，而是模仿区块链的分布式账本模式，被同时存储到可能使用电能的几个分站站点中。在这个过程中，通过使用电能的智能化分配来实现最大化利用。

除了这些区块链在实际应用场景中解决基础设施建设、能源消耗等基础性资源匹配的案例，还有一些我们不太熟悉的应用场景，如在公共平台方面。

2018年1月，IBM和Maersk联合宣布将成立一家合资企业，以创建一个数字化全球贸易的单一平台。UPS和FedEx等运输巨头也与区块链运输联盟合作设定行业标准，探索利用区块链技术跟踪货运、管理物流和取代货运经纪商的方式。据摩根士丹利（Morgan Stanley）透露，这将是一个市场价值超过5000亿美元的机会。

通过使用具体的区块链技术或者区块链的逻辑模式，基础设施建设领域可以实现更高的建设和使用效率，进一步降低基础设施建设和

能源的费用，提高整个社会的基础设施建设效率，降低综合建设成本。



### 第三节 区块链的一小步，有价证券的一大步

区块链技术有一种与生俱来的应用在货币领域的可能性，将这种技术应用在有价证券上似乎顺理成章。但是与其他类似技术相比，区块链并不是作为一般等价物应用在有价证券领域中，而是更多应用在结算方面。

有价证券的交易其实是一个比较复杂的过程。由于有价证券本身就具有资金属性，因此是一种具有一定流动性的物品。凡是具有流动性的物品，在交易过程中都需要格外细致，因此任何证券交易所或者证券交易的承接商，都会在交易过程中反复验证，然后才会继续进行清算和结算。

证券交易商这样做，其实有两方面的原因：第一是有价证券的价值很高，但缺乏国家的背书和系统化管理，不能像印刷钱币一样进行规范的管理，因此相比为造货币而言，有价证券的伪造难度小得多，在交易过程中遭遇虚假有价证券的风险相对更大；同时，在有价证券交易过程中不能实时结算。由于有些证券的交易比较复杂繁琐，需要不断核对价格与交易量，因此一般有价证券交易采取三天交割、两天交割等不同的交割形式，进行实时结算的有价证券交易并不多。

回忆一下股票买卖过程：买卖股票的时候，我们事实上并不是直接把股票卖给某个人，而是先把它委托给中介机构，由中介机构在电子报价牌上挂出。我们所期待的价格，最终形成了整个股票交易过程中的价格。在这个过程中，股票价格的实时变动，本质上是无数个出价人的出价结果所导致的。这种计算往往有一定的顺序，而我们为了保证交易的顺畅，又不能将相关交易停下来进行个别有价证券的结算和交割，这样就出现了一个时间差。有些人正是利用其不能实时结算

的特点，制造出各种各样的骗局。另一种我们熟悉的有价证券——债券的交易，有些便采取三天后交割的模式，理论上在这三天里，卖方其实并没有丧失债券的所有权，因此他继续交易，这就导致了“一债多卖”的情况，也带来了交易的衍生风险。

人们在进行各种有价证券的交易时，往往不能识别这些风险。甚至一些有价证券的交易过程中还存在恶意拖欠或是刻意曲解相关交易规则的行为，造成了交易某一方的损失。

因此，区块链与有价证券之间的有效结合，最主要体现在它能够更好地帮助有价证券满足发行交易等过程中的各种需求。

在验明真伪的方面，区块链具有得天独厚的优势。在传统的有价证券骗局中，很重要的一点就是各种有价证券的信息全部储存在一个中心节点，因此不管是纸质的交易数据还是电子化的交易数据，造假人都可以通过更改这些储存在一起的数据来实施自己的欺诈行为。区块链将数据进行分散存储，没有人能够拿到完整的数据，也就杜绝了相关骗局的产生。

同时，由于区块链要求数据信息的实时收集和处理，通过区块链的分布式计算模式，也可以有效地提升整体的运算速度，因此在以区块链为中介的有价证券交易过程中，可以将有价证券的实时价格直接输入相关的采样系统中，实现更有效的报价。在这个输入过程中，也必须明确相关的交易条件，这样我们就构建了一个不可篡改、信息准确同时兼具即时性的数据网络，这对于有价证券的交易来说是非常有帮助的。

在基础应用层面，区块链的分布式计算模式大大提高了各种存储设备的计算能力。因此，通过区块链的大量使用，我们的证券交易尤

其是有价证券的交易可以实现更全面的更新和更快速的结算，这将带来巨大的成本削减和商业价值的提升。

与以往交易确认需要T+3个工作日不同，在区块链上结算和清算的完成时间仅以分钟为单位（即在区块链上确认完成一笔交易的时间），且可以节省大量的费用支出。据估算，美国两大证券交易所每年清算和结算的费用高达650亿美元至850亿美元。如果将T+3天缩短为T+2天，则每年费用将减少27亿美元。如果降低为10分钟，那么节约的费用及提升的效率无疑更大。

通过这个事例我们也能够发现，如果用区块链技术推动整个有价证券的交易过程发生变革，带来的现实收益将会是非常巨大的。

## 第四节 区块链“提速”公证业务

现代商业社会最难突破的一个点就是社会信用体系的搭建，而区块链正是目前人类所能找到的、解决信任问题的最有效的工具。

因此，区块链被寄予厚望，被认为可能替代各种数据收集和分析，帮助政府实现有效的基础信息管理，成为信息化时代构建社会信用体系有效技术方法和手段。

目前，区块链技术已经广泛应用于各种需要搭建信用体系的行业中。除了上一节中提到的有价证券交易，它还在众多的交易领域中被作为构建信用关系的重要手段。在公证领域，区块链技术也是当仁不让。

公证行业本身就属于社会信用体系构建过程中的一个“副产品”——之所以产生公证行业，主要的原因就在于我们很难区分各种各样的证件的有效性，很多身份信息在市场交易过程中难以被认可。公证行业中的一项重要技术是基于印鉴来判断真伪，根据丰富的鉴定知识，公证员可以判别眼前的法律文书是否真实有效。

这样一个机构在社会运行中有非常重要的作用，人们在决策或交易过程中的不信任感，可以借助公证的力量消弭。

如果使用区块链技术，这一切会有巨大改变——区块链可以从证明的最初环节就设置单一的、不可篡改的信息底层逻辑，让所有文件统一储存在一个数据模块上，以后的鉴别就变得非常简单。只要输入一个验证代码，就可以知道眼前的文件是否真实。因为所有这些文件的唯一真实样本都在最初录入了系统。

因此，随着区块链技术的发展，公证行业可能不再依托公证人员的技能，而是偏向于技术解决鉴别问题，比如如何对法律文件进行编码，并且将它们匹配到一个固定的区块链数据块中。在这种存储系统中，人们能够通过某种单一、可信的形式，进行相关的验证。

鉴证行业本身是用于判断证明物品真为 的一个行业。假如某一件物品从它被发现开始，就已经有了唯一准确的数字编码，那么这件物品的真实性本身可能就不再是我们需要关注的重点了。在这方面已经有了一些尝试，例如美国的一些拍卖公司已经开始在一些近现代拍卖品中应用区块链的标准技术。

另外，一些具有市场影响力、品牌力并具有一定收藏价值的商品，也开始引入区块链技术。如一些知名球鞋生产商在生产过程中引入区块链技术，让鞋子拥有唯一的、可信的编码。当拍卖举行的时候，只要进行相关区块链的验证，人们就可以了解到现在所购买的是否是真的产品。

随着整个行业的发展，未来区块链可能还会在各种各样的产品鉴定和法律文件的公证中，产生巨大作用和影响。但在今天，区块链更多的还是应用在我们可控的近现代人工制成品方面。久远的文物、古物等涉及复杂的专业知识的物品的鉴定，可能在现阶段还没有办法得到有效解决，但是随着区块链技术的广泛应用，这一天很可能会到来。

## 第五节 市场预测的“天敌”

市场预测一直是一个非常复杂的领域，需要分析师凭借专业知识和在市场中积攒的丰富经验后才能做出判断，这些判断很可能成为后续市场投资的重要建议。

虽然人们希望从各种各样的市场分析报告看到未来的行情走势，以此来指导自己的投资交易。但事实上，能够获得有价值的报告的人少之又少。在实际投资交易过程中，一些人正是利用这样的信息不对称牟取暴利的。

这是一个典型的非信任市场环境，也许就是因为人们相互的不信任而催生了市场预测这样一个行当。市场预测本质上是一个信息非对称的产业，在这方面，区块链可能会成为它的“天敌”，因为区块链的核心就是希望能够建立人与人之间的信任关系。

市场预测不仅仅具有预测未来价格走向这样一种单一的功能，还有很多复杂的功能，例如分析未来销量、预测总统大选的结果、预测球队比赛的结果甚至分析区块链技术的未来价值。这些都是市场预测的一部分。

如果能让市场预测变得尽可能可信和一致，就必须解决两个问题：第一个是如何预测市场走向，第二个则是预测结果带来的利益分配问题。

第一个问题，其实应用区块链技术可以相对比较简单直接地解决。比如现在的一些区块链应用中，已经出现了开放式的预测服务，只要把自己感兴趣的话题发布到网站上，就会获得相关的分析数据，

其他人可以看到你提出的问题，并做出他们的预测。所有这些预测将会根据一定的算法转化成最终的预测结果，指导行为人的选择。

通过这种开放式的区块链平台，人们可以把自己所关心的问题都提交上去。至于传统的围绕有价值或者重大价值的商品进行的市场预测，则与其有一定的差异。

现在人们可以完全根据自己的兴趣选择要不要向区块链公司提出问题、要不要邀请其他人协助解决。这是整个预测行为的基础，而这种基础在未来会变得更加的宽泛。

这在过去是不可想象的，没有任何一家市场预测公司敢说它的客户可以随意提出任何问题。一般来说，市场预测公司必须依据自身积累的专业经验来选择预测的领域，甚至在某种程度上，这些公司预测的内容并不是市场真实的需求，而是取决于它们能够做些什么样的预测。

但区块链完全打破了这种状态，让我们有机会提出自己真正感兴趣的问题。这是一个非常巨大的变化。

如何保证预测人的收益，是第二个重大问题。因为如果无法保证预测者的收益，这一行业就将不复存在。

在现今的区块链应用领域，解决报酬问题的一个有效方法是所有希望获得预测结果的人都提供一份报酬。这有些类似现在的赌球，所有的人都可以购买输赢结果，而最终将依据比赛的结果来分配报酬。

举一个例子。在美国总统大选期间，人们可以抛出一个话题：是否选择特朗普作为总统？这时会有一些人希望特朗普当选总统，而另一些人则不喜欢他，每一个预测的人将会获得一个区块链编码。最终，预测特朗普当选总统的人凭自己的编码就可以换取奖励。

这就是区块链在市场预测方面的一个应用场景。未来，随着我们的话题越来越多，在区块链平台上的各种预测的商品和结果也会越来越多。当数据达到一个理论上足够大的数量时，我们可以认为，这个预测无限趋近于真实。或许随着技术的发展，整个区块链的市场预测技术也将会越来越精准。



## 第六节 改造注意力经济

注意力经济是一种既陌生又熟悉的经济模式。在浮躁的投资领域，注意力经济在某种程度上正在蜕变成一个贬义词。随着真实应用场景越来越多，它似乎在等待彻底爆发的那个时刻的到来。

注意力经济最早被人们所诟病，是在泡沫经济时代。但随着互联网泡沫的破灭和世界经济的发展，加上信息技术的不断进步，人们对注意力经济渐渐也有了新的认识。

在过去的经济模式中，信息是整个交易的核心环节。人们获取信息的能力是有限的，读取到的信息也是有限的。因此，信息在过去的交易过程中是绝对的稀缺资源，是相对核心的交易对象。

随着信息技术的发展，人们传递信息的能力变得空前强大，因此信息本身不再具有原来的稀缺属性。相反，谁会阅读信息或者有没有人愿意阅读它，变成了一个非常重要的问题。因此一些经济学家提出，注意力经济是信息化时代到来之后一个非常重要的经济类型。

从当今的注意力经济的发展情况来看，其核心内容是如何产出有价值的信息以不断吸引对其有兴趣的人，通过培育这些潜在的兴趣，最终实现消费。

我们能够看到，注意力经济的本质，实际上是如何产出高质量的内容及如何精准地投放信息。这类似于今天我们熟悉的“头条”模式——不断地把读者感兴趣的内容推送到读者眼前，进而不断强化读者的消费习惯，最终让其成为一个有价值的“套现”对象。

这带来两个问题，第一个是信息道德的问题，第二个是信息接收者如何变被动为主动的问题。

信息道德比较好理解。生产信息的人为了博得眼球，可能会放弃真实性与全面性，将信息的某个侧面夸张放大，因为这样才有可能吸引对它感兴趣的用户。

但信息应该是相对客观的，不应该存在主观需求。因此，一些地方存在反新闻定制化的浪潮，也就是认为，新闻和信息应该处于一个完全自由流动的状态，不能人为地进行筛选，而让接受者被动接受，影响信息接受者的价值判断和行为。

信息筛选的危害实际上有非常多的案例，最典型的的就是剑桥分析对各国政治的影响。

剑桥分析是一家英国咨询公司，它帮助全世界很多政治家分析获取选票的最佳途径。在传统意义上，这类公司是可以正常开展经营的，因为它们的服务逻辑是以自己的专业技术提供一些专业的咨询建议，帮助候选人获取更多选票。在知识经济时代，这是一种大家都能广泛接受和认可的行为。

但剑桥分析的所作所为不能让人接受。因为它通过分析Facebook（脸书）上人们点赞的行为，预测其潜在的投票可能性，在这个基础上给候选人意见和建议，制定迎合投票人的政策。同时，剑桥分析还定点投放这方面的新闻，这些投放并不以候选人真正的价值观为基础，而是完全以受众的兴趣爱好为基础。这事实上在某个层面影响了对象国的国内政治环境。这种行为显然是不被接受的。因此这家公司在很多国家都被严厉禁止了。

这样的行为其实就与刚刚所说的注意力经济的第一个层面非常相似——如果我们是通过精准投放的、筛选之后的新闻来获取信息，那我们的信息渠道会越来越窄。依据爱好所构建的世界，将成为我们自认为的世界的真实景象，对世界的判断失去客观性。更严重的是，这种筛选技术通过对你注意力的反向应用，甚至可能影响你的选择和行为。说得严重一点，这可能成为一个控制你的利器。

另一方面，我们也很难打破这种现状。这也是注意力经济应用中的第二个难题——人们是如何找到自己真正的兴趣爱好的。

事实上，我们所有的新闻都由人采编和写作，这本身就含有一定的主观性。而编辑的过程同样又是一个信息筛选的过程，所以我们拿到的信息其实永远都是被筛选过的结果，它并不代表真实客观的信息。但在传统传媒行业，我们毕竟还是可以选择要关注或看哪些新闻，相对全面的信息还是会被呈现出来；而在注意力经济时代，如果稍不注意，这种行为就演变成了精神的投放和影响。

区块链模式可以在一定程度上改变这样的状况，将信息的生产端与实际使用端完美隔离——信息的发布者并不清楚他写作的内容会被谁看到，因此也不存在主观的定点投放问题；而阅读这些材料的人也不一定会受到这些材料的影响，因为他们所能看到的是整个信息丛林。

做到这一点的基本前提，是所有的信息都会被记录，而且同时又被分散储存。当我们使用这些信息的时候，可以用自己的算法提炼出需要什么。人们阅读的数据会存储在一个相对独立的第三方空间中，而信息的制造者并不知道最终信息传播的情况，只会知道自己的信息是否被人们看到，并不清楚具体会影响哪类人群，从而避免信息制造者为了迎合这个人群的特点而不断创作符合他们价值观的新闻报道。

通过提供相对客观的获取信息的手段，区块链可以很好地让我们发挥注意力经济的根本价值，也就是让我们的内容产出更加精彩和高效。

## 第七节 让共享成为常态

共享经济与区块链，本身就是一对“好兄弟”——一方面他们产生的背景和环境有一些相似；另一方面，这两种类型的技术在很大程度上可以取长补短。

共享经济的底层逻辑是打破所有权和产权的隔离。它对于价值释放的影响非常显著，能够充分发挥物品的价值，消灭销售和流通之间的利益增加，完全专注于生产与消费两端，尽可能压缩中间的流通环节，提高资源的运转效率，同时提高资源在闲置状态的使用效率。

共享经济在很多领域都有了非常好的实践，最典型的是共享单车。企业投放单车解决人们用车的需求，同时人们又完全避免了购买自行车之后所需要的保养保管，只需享受自行车这个物品的使用权。

在共享单车之后，还有很多共享经济的尝试，比如共享汽车、共享住宅等。这些探索不见得全部成功，甚至有一些并不能称为真正的共享经济。在后来的发展过程中，共享经济逐渐被市场所认可，经过反复调整，最终正式名称定为分时租赁业务。

在现行阶段，共享经济还无法突破分时租赁的业务特点。虽然在某种程度上，它解除了产权对物品使用价值的限制，但是由于大部分的工厂和企业没有能力全面掌控人们希望共享的物品的信息，因而无法掌握产权所有者和产权使用者的需求信息，也很难在现有的共享经济模式下有所突破。

事实上，分时租赁行业并不是一个新鲜产物，而是传统金融行业的衍生。如果想要实现更有价值的共享经济模式，就必须突破现有的阻碍，也就是解决产权的信息归属问题。

共享经济本质上是在产权基础上进行的使用价值的让渡。在现有模式下，这种让渡其实并不完全。事实上，这种模式并没有真正让所有的资产都实现共享，也没有达到最大的社会效益。

通过区块链的模式，我们可能形成一种新的共享经济的概念。最简单的是把一些传统的、不太容易共享的东西实现共享，而根本性的改变，是共享的内容出现了变化。

现在共享经济最成功的领域无疑是出行方式。当然，这些模式也被证实存在缺陷，比如共享单车大量出现押金和盈利模式的问题，网约车出现“黑车”和安全监控问题。这些都说明，现有的共享经济模式实际上只是分时租赁的一种形式。但区块链技术可以实现更广泛或者更具深度的共享模式，也就是多余算力能力应用模式。区块链的生产模式决定了，如果想要使用这种技术，就需要不断“挖矿”，通过不断地运算寻找这个区块链模式中的有限多个解，这就需要大量的运算和支持其运算的计算工具。如此大量的计算，如果专门使用某些设备进行，生产成本将会非常高。就像现在的比特币“矿场”，从硬件的购买到电能的损耗，都是一笔不小的支出。

引入共享经济模式之后，我们就可以把多余的计算能力全部利用起来，比如冰箱、电视、路由器，运用它们所具有的计算能力协助运算，寻找区块链中的有效解。

同样，现有的一些共享经济企业，比如共享单车企业，也正在考虑在单车闲暇时间利用其身上自带的芯片协助“挖矿”，这些事实上都拓展了我们对共享概念的理解。和我们传统使用物品不同，共享经济不再要求被使用的物品与使用的人存在于同一个时空，只要物品的使用价值可以实现，就达成了目标。

在这种情况下，我们就可以实现更广泛和有价值的共享了。进一步而言，区块链技术与共享经济结合在一起的时候，我们就会发现，原来那些不可逾越的信息孤岛都不存在了。人们可以通过相对安全和可信赖的方式，将自己的私人物品交由他人使用，而使用结束之后，又可以有效地规划这些物品，实现物品价值最大化。

虽然目前共享经济与区块链的结合还处于想象阶段，但是随着技术发展，我们有理由相信，使用共享化的区块链技术的日子已经不遥远了。

## 第八节 游戏业的破局新方向

要说游戏行业很赚钱，相信没有人会反对这样的结论。企业对游戏的研发投入可能很大，但是只要游戏上线并被人们认可和接受，就会变成一棵摇钱树，持续地创造利润。

但是，赚钱的游戏行业存在很多挑战。比如安全管理问题就一直是游戏开发者非常头疼的问题之一。通过游戏的漏洞来实施诈骗几乎成了骗子的惯用伎俩；人们经常会通过改写游戏数据、增加外挂来改变游戏的平衡性，这种行为屡禁不止。游戏开发者有没有可能用一种方式一劳永逸地解决这些问题？区块链可能给我们提供了一个方向。

区块链的底层技术是分布式存储各种信息。假如把它应用在游戏里面，可能就会看到这样的场景：玩家虽然是在某个共有的地址中玩游戏，但游戏所有相关运算和数据，是由分布在世界各地的不同计算机同时支持进行的。如果这样的模式能够实现，也就意味着玩家想修改游戏中的某个数据会变得非常困难。因为人们并不清楚这个数据在当前时间点上究竟是由哪一台机器运算和储存的。人们很难通过伪装成服务器或客户端等方式，来实现外挂的各种功能。

同样的，对游戏账号的安全保护也适用类似模式。游戏公司可以将用户账号信息与直接交易的信息全部分散储存在不同的服务器中，当需要使用时才从服务器中调取出来，提供给相关使用者。这种情况下，任何黑客想攻破游戏的安全屏障都会非常困难。就如同前面所说，要修改游戏参数需要找到相应的服务器，但是攻击者根本不可能知道这个数据究竟存放在哪里。既然不能找到数据存放的位置，修改也自然无从谈起了。



这是区块链在游戏安全性方面的应用。而另一方面，利用区块链对游戏进行法律法规方面的限制，也可以帮游戏实现更大的成功。

游戏的非分级模式是今天游戏市场被人们诟病的问题之一。这就意味着一个很小的孩子也可能有机会接触不合适的游戏。不同年龄的孩子在玩游戏的时候按法律法规应受到不同的限制，但这种限制目前仅能通过在游戏注册时进行身份认证来实现，而这一点在很多时候并不是难以突破的。

怎样才能让游戏制造商识别每一个玩家的真实身份呢？假如我们通过区块链技术，把所有人的信息分布式存储到整个网络中，那么游戏制造商就可以很轻松地在玩家玩游戏的过程中对他的身份信息进行比对。这个过程在传统模式下非常困难，而使用区块链模式，就可以相对轻松地做到。

在传统模式下，人们可能会担心数据外泄或是信息安全受到挑战，会把相关身份信息保存得很好。但对于游戏玩家来说，他们在注册游戏的时候往往需要上传身份信息，这事实上也成为信息泄露的一个重要缺口。那么在这种背景下，我们想要让所有的游戏玩家提供自己最准确真实的身份信息，很有可能是做不到的。

如果玩家所有的身份信息都分布式地储存在整个网络中，那么游戏制造者就可以直接提取这些信息，通过比对年龄、地点甚至游戏操作的特征，确定信息是否真实。同时游戏制造商还可以通过各种各样的回访制度来实现对游戏信息的控制，了解到真实的玩游戏的人是否符合国家的相关的法律法规。

另外，通过区块链技术游戏服务提供商还可以及时地获取每一名玩家在玩游戏时的真实状态。比如说，根据监管者的要求，游戏制造商在很多的游戏里设置了防沉迷系统，告诫到一定的时间就必须退出

游戏。但事实上，很多人在玩游戏的过程中可以通过用不同的游戏号码反复登录来规避这个问题。如果在整个游戏系统中也用区块链的思维，所有的相关账号都在同一时间点内不断地检验自己的IP和所处的地理位置，同时检验使用账号的人，那这样的话，游戏服务提供者就可以轻易地识别到底哪些人是真正遵守规则的，又有哪些人是在破坏规则。

这一点其实通过现有的技术也很容易实现，但为什么没有人愿意这样做呢？这是因为游戏制造商需要玩家更多地沉迷其中，这样商家才能获利更多。只有通过区块链的体系记录所有真实的游戏数据，才能帮助监管部门更有效地监控游戏实际使用者的情况。而且采用现有技术还会涉及庞大的数据库和防止信息泄露的问题，而通过区块链的模式将所有的游戏记录上传到一个公共平台中，有相关监管能力的人才有权查阅这些信息，游戏制造商的造假空间会被压缩。同时监管部门也可以让这些信息更有效地流动起来。

因此从游戏自身的安全需求角度来说，区块链可以给玩家带来一个解决问题的方式；而从游戏监管的角度来说，也可以给监管者提供一种有效的手段，这可以帮助游戏业更加持续地发展。

An abstract graphic of a molecular structure, possibly representing a crystal lattice or a complex molecule, rendered in grayscale. The structure consists of numerous spheres (atoms) connected by lines (bonds), forming a complex, interconnected network. The spheres vary in size and are shaded to create a three-dimensional effect. The overall shape is irregular and extends across the left and bottom portions of the page.

07

## 未来已来：迈向第四次工业革命

## 第一节 区块链布道工业4.0

如果100年后人类组织一次关于“21世纪初的伟大变革”的评选，那么工业4.0时代的到来一定会入选。在信息产业革命之后，人类社会经过了漫长的等待，又迎来新一次的工业和生产技术的跨越式发展，一场新的生产力革命呼之欲出。

人类历史上的每一次工业革命，都是一场生产力的跨越式发展。而每一次工业革命，最终都会使人类改造自然的能力得到极大的提升。

第一次工业革命通过引进蒸汽动力实现了产能的提升；第二次工业革命通过电力的普及实现了对不同能源的充分利用；信息技术革命带来了信息传播方式的改变，最终作用在了生产组织方面，进一步提高了工厂的规模化生产能力。虽然三次工业革命的核心内容不同，但本质上，都解决了生产力提升的问题。与前三次工业革命不同，工业4.0需要解决产能精准化投放的问题。

按照工业革命的基本特征，我们可以把蒸汽时代称为工业1.0时代。这个时代主要解决的是如何用另一种动力替代人的劳动。在工业1.0阶段，通过蒸汽机械的大量运用，人类实现了批量化复制的生产模式，不再受限于人力，可以用机器替代人工。

随后，人类世界进入第二次工业革命阶段。随着电力的发现，动力的组成形式变得更加丰富多样，人类有了能量转化的概念。能源的使用模式不再仅仅是用煤把一锅水烧开来提供蒸汽动能，而是采取发电的方式让能源生产和消费突破了时空的限制。人们可以在几百甚至上千公里之外生产电能，然后通过电路将其输送到用电区域。工业2.0

时代，我们面对的是一个加速发展的时代。电力的广泛应用带动人们对世界的探索进入一个新的阶段，技术的发展甚至突破了人的想象力，新的技术与产品层出不穷。电视广播的发展带来了信息与知识的加速普及，无线电的应用带动了信息传播手段的革命性更新。但是这些产品的创造，都是基于没有具体形态的能量形式，人类捕捉到了肉眼看不到的物理定律。而这一切，也带来了第三次工业革命——信息革命的曙光。

随着电子计算机的广泛应用，人类社会由第二次工业革命进化到工业3.0阶段。这个阶段的到来，让人们更加深入地触及社会生产力进步的底层逻辑，这就是信息在生产力提升中的作用。

随着电子技术的发展，信息的重要性在生产过程中也逐渐凸显出来。同时，信息技术发展也造成人们对信息处理能力的加强，进一步缩小了不同人群获取信息能力的差异，并提升了人们利用信息获利的能力。从某种意义上来说，这是以电子信息技术为代表的第三次工业革命所带来的本质变化。

如果从看得见摸得着的角度来看第三次工业革命的成果，对于大部分人来说，它带来的是商业的便利——流通的便利和生产的便利。信息技术通过把各种各样的数据进行有效的整合，实现我们对信息的应用，加速整个社会的发展。这就是第三次工业革命，也是工业3.0时代带给人类社会的启发。

如果说第一次工业革命启发了人类规模化应用非生物动力，第二次工业革命启发了人类社会应用看不见的能量形式，那么第三次工业革命带来的启示则是不直接变成产品的非物化的信息在生产中的作用。沿着工业3.0的方向继续发展，人类社会迎来的就是工业4.0时代。

关于工业4.0的讨论，其实早在2012年就已经开始。当时法国提出了自己的新工业计划，德国甚至明确提出了“工业4.0”这个名称，美国也提出了工业振兴计划。而中国也几乎在同一时间开始讨论智能制造优势产业的打造。

当然，这些都是官方发布的、在正式、严肃的语境中讨论的工业升级蓝图。而民间智库对工业升级的讨论甚至更早。早在信息技术泡沫破裂的20世纪90年代，就已经有人开始考虑工业4.0的面貌。有的人认为工业4.0将是全面信息化和无人化生产到来的时代，有的人认为工业4.0是大型企业彻底垄断经济的时代，有的人则认为工业4.0将成为国家之间竞争的惨烈战场……这些观点从不同的角度探讨工业4.0的本质，但不难发现，不论是政府还是民间，对于工业4.0的面貌还没有一个统一的认识。

什么是真正的工业4.0？它究竟要解决什么样的问题？与前三次工业革命相比，工业4.0有什么鲜明的特点，它会给我们的生活和经济发展模式带来什么样的改变？这些基本问题还没有答案。

但是随着世界各国的“国家队”入场探索工业4.0，尤其是随着信息技术——云技术、大数据、区块链这些新兴技术的发展，工业4.0的脉络框架也变得越来越清晰。

最早提出工业4.0的一批国家，已经开始了系统的研发甚至使用人工智能，用越来越多的机器人来替代人工。在某种意义上，一些国家已经将无人化的工厂甚至无人化的生产作为工业4.0的一个核心指标。但是这似乎只解决了一个问题，就是工业4.0如何改变工业的现状，并没有解决其根本定义问题。尤其是从工业1.0到工业3.0的进化过程来看，工业进化是一个越来越脱离现实生产的过程，仅仅回答工业4.0是实现生产的无人化，显然是无法充分定义它。

从根本的角度来看，工业革命的每一次重新定义都带来了与过去完全不一样的工业生产方式。事实上，我们在工业3.0时代就已经把信息整合到了生产之中，在工业2.0时代我们就已经有了使用机器替代人工的工作模式。工业4.0与前面几个阶段之间的差别究竟在哪里？

通过不断摸索，德国人率先回答了这个问题。德国人认为，在工业4.0时代，工厂的生产应该由原来的规模化和统一化变为个性化和定制化。也就是说，过去我们已经熟悉并成功运用的生产线生产的模型化生产方式到了需要改变的时候，而这种改变的核心特征就是个性化的生产。

换句话说，我们可能会面临一种新的购买场景：在网上浏览的过程中发现了一款新产品，我想购买这个产品。在现在的商业模式中，这个流程是消费者购买这个产品，后台就有人去寻找库存。当有库存的时候，消费者就能够买到。

但是在工业4.0时代，库存的概念已经不存在了。从买家下订单的时间开始，工厂组合原料，然后完全按照买家的要求生产出一款产品，再通过高效的物流方式送到买家的手中。

在这种模式中，每个人购买的商品都是不同的，每个人拿到的商品也是不同的。每个人都有自己的设计要求和功能要求，而工厂最大限度地满足这些要求。在某种程度上，这彻底改变了工业生产的面貌，工厂从规模化的生产变为了资源的精准投放。这对于曾经的工业生产来说是完全不可想象的事情。

工业的一个本质就是我们可以用规模化来实现快速生产，通过工厂模具的开发，不断实现标准化生产，让生产能力快速提升。工厂最重要的就是标准化和去个性化。

但是，为了提升效率所付出的代价是否值得？这在工业化时代是没有讨论基础的。在规模化生产的阶段，生产者提供给市场的往往是有限制的可选择范本。虽然我们也将这些不同种类的商品称为“丰富多彩”，但是实际上，这是统一化基础上的丰富多彩。

随着工业4.0的发生，我们发现过去集中设计的模式已经不能再满足需求，甚至不支持有效的生产。在这种状况下，我们就需要新的设计模式。

要实现这一点，我们需要依赖全新的创新模式，最大限度地激发出全社会的创新热情，让所有人都能拥有设计的自由，而生产则蜕变为大量节点性工厂的联合。这种创造需要通过大量使用区块链来实现。

随着人工智能的普及，越来越多的工作被机器取代，但是机器并不能包办一切。工厂只能根据得到的创意来生产。机器人的普及让我们的生产能力快速提升，但是创意却不能通过机器人来产生。

要解决这个问题，需要全面开发和应用创新成果——最大限度地增加从事创新的人员，应用创新成果。而结合区块链技术，我们可以将一个产品设计变成一个区块链需求进行发布。所有人都在这个创意的增值链条中——有的人提供创意，有的人提供生产，有的人提供物流支持——这些专业化的领域都被统一在共同的利益链条中，同时还共同承担着风险，一起来创造最佳的产品结果。做好这一点，才能实现工业4.0的创新基础和根本意义，真正为所有人提供个性化的生产与商品。



## 第二节 人工智能与区块链：1+1 > 2

人工智能是人们非常期待的应用技术。在众多领域，人们都期望能够在下一个10年里人工智能的实际应用。

随着对人工智能的研究和相关技术的发展，人们对人工智能的认识也越来越清晰。今天，人们已经经历了从将人工智能看作洪水猛兽到逐渐接受的过程。通过实践，人们越来越清楚人工智能的本质。今天，它已经被定义为“可以帮助人们更好地实现现有工作的一种有效的信息技术支持手段”。

这个定义体现了人们对人工智能与人类本身之间的关系认识，也反映了历次工业革命都无法绕过的问题——机器和人之间的竞争问题。

任何一次工业革命，事实上都消灭了一批人的岗位，而人工智能给人带来的恐慌更甚于前几次。一台有智慧的机器与人类竞争，而且这些机器更加聪明、更少犯错，这似乎带来了更让人绝望的体验。

人工智能的定义和发展走向，其实在某种程度上回应了这种焦虑。人工智能其实只是辅助人们工作，而非取代。这就强调了人工智能与人之间的关系并不是替代的关系，它的出现只是为了辅助人们做一些过去做不到或者很难做到的事情。这事实上解决了人与人工智能究竟应该如何相处的问题——在重大责任与决策方面，人工智能能帮助我们，而非替代我们。

就如在自动驾驶领域，虽然在飞机航行过程中，人工智能或者自动驾驶技术已经非常成熟，但是在关键阶段，我们依然需要人来做最终的判断。这也是未来人工智能与人之间的关系。

但是如何让人工智能既能帮助我们，又能充分地学习，同时还不会随意地替代人来做决策呢？这之中最困难的就是人工智能的算法优化问题。

机器学习可以让人工智能不断学习和掌握新的情况，也就是说，人工智能可以在脱离人的决策的基础上，实现对各种知识的不断学习和应用。这也是人工智能最早被开发出来时被寄予的期待。

在这里，我们不探讨人工智能的道德和社会问题，只考虑它的实际应用。

想象一下：如果你的电脑可以在不经同意的情况下，提前预判你是否需要一顿丰盛的早餐，或者是否需要打开空调，你是不是会觉得它对你的帮助非常有效？

假如把这种场景变得更大规模、更复杂，我们就可能看到更加宏大的画面。在这些场景中，人工智能可能帮助我们做更多的事情。

比如，在战斗机的开发过程中，驾驶员由于需要同时控制多种部件，往往会感到操作困难。在传统意义上，战争中的强对抗要求人必须瞬间做出各种各样的判断而不能依靠机器。但今天随着技术发展，人工智能也可以在空中战斗机的管理方面为我们提供支持。比如它可以决定是否向对方发射弹药，或者决定是否应该加速离开。这种活动原本其实都应该是由人来决定的，但是由于人工智能拥有强大的信息处理能力，所以它可以帮助我们更好地做出这些决策。

当军方使用非人工智能的方法来解决战斗机的作战问题的时候，必须给战斗机的控制系统提供各种各样的决策依据。飞行员需要告诉它在什么情境下应该采取什么样的措施。但是我们都知道，在任何情

况下要想穷尽所有情境都是非常困难的事。因此，要解决这个问题，只能让人工智能在面对各种各样不同的环境时自己做出决策。

实现了这一点，人工智能才会变得真正可用。现在的战斗机驾驶中，虽然自动控制的一些动作已经可以实现计算机辅助，但是在真正的决策还没能够实现人工智能的完全操作。

不过，如果人工智能真的能够根据不同情境做出行为选择，就意味着它真正成为“智能”。假如你的家里有这样一个智能助手，即使你并没有让它帮你泡一壶咖啡，它也能够判断你现在已经非常疲惫了，非常需要一杯热咖啡来提神，在能实现类似这样的判断之后，人工智能就真的变成了智能。因为它不需要我们思考和决策，就会帮我们做好各种各样的判断。

而上面这个过程其实都必须通过机器学习实现。一开始，人工智能可能只是知道在某些固定时间点冲泡咖啡；随后，机器学会了“思考”，能够判断这些固定时间点的特征是什么；然后再实现不需要“询问”意见就能自己行动。

最终，人工智能甚至还可以打通知识之间的隔阂，思考除了咖啡你还需要什么一类的问题。而这些的基础都源于机器学习。实现这种机器学习的其实是一套算法，它能教会机器如何提取和识别需要的信息。

应用机器学习之后，人工智能面对的另一个挑战就是海量信息的获取。掌握了学习方法还不能生产出一台聪明的机器。除了方法，还需要海量的可学习的对象，这就是机器学习中对学习数据库的需求。

人工智能有了机器学习程序之后，还必须有可学习的对象。因此，如何给人工智能提供海量的学习内容和仿真模式就变得非常重

要。这个数据库一般有两个来源：一个是利用已有的数据积累，另一个是通过人工题库整理。

在机器学习方面，有一个非常有意思的故事是关于围棋 人工智能项目AlphaGo的进化的。最初，人工智能无论如何都无法击败人类棋手，这也让围棋 领域成为主流棋 类中人类最后一块没有被人工智能攻陷的地方。但经过一段时间的学习之后，AlphaGo居然击败了当时人类最优秀的棋 手。这种变化很重要的一个原因就是AlphaGo有了学习数据库。

在第一阶段，AlphaGo的训练模式是学习人类的各种棋 谱，模拟人类所有的棋 局棋 谱，同时进行数据推导以掌握围棋 的套路方法。但是即使掌握了能够搜集到的人类所有围棋棋 谱，AlphaGo依然无法战胜优秀棋 手。

后来AlphaGo采取了另外一种学习 模式：它不再向人类的棋 谱学习，而是自己与自己对弈，通过不断推导每一个步骤，最终实现棋 技的提升。这样的训练让AlphaGo最终战胜了人类棋 手。

这件事引起了人类社会的恐慌，因为这件事从一个侧面证明了人类的智慧并不是最优的解决方案。相反，人工智能抛弃向人类学习的方案反而获得了更佳 的实践。这也说明了一种可能性，那也就是人工智能通过自我学习，很有可能超越人类。

联想那些红极一时的科幻电影，如《黑客帝国》《机械公敌》等，也许我们就会觉得，这些电影中描绘的人工智能对人类的控制和屠杀可能真的会发生。当然，这只是一种可能性。毕竟在目前阶段，人工智能还没有能力与动机来这样做。在今天，我们依然认为人工智能将会是实现人类社会快速进步的一个重要支持力量，不会把它看成是敌人。

当然，这种风险并不是完全没有可能。这就要求我们在编写每一段程序、设计每一种算法的时候都非常小心，投入大量的人工团队。

在这方面，区块链也可以提供非常大的支持。一方面，在人工智能开发过程中，机器学习要依赖算法的不断改进来进化，而这个过程需要不断试错。这些也是区块链擅长的。它可以快速地让一个人工智能小组实现有效分工，更大可能地获取人工智能开发方面的资源。通过散布在各地的终端，把人们都拉进人工智能的开发小组中，实现人工智能的快速迭代。这样的模式不仅更有利于人工智能的技术开发，同时也可能在某种程度上解决人工智能潜在的道德问题。因为毕竟所有的开发者分布在不同的文化领域、不同的国度，拥有不同的政治目标，因此人工智能的学习最终可能会涵盖各种各样不同的价值观，而这带来的可能是远超人类想象的成功。

另外，人工智能学习所需的大量数据库，也不可能是由一两个人完成的。它必须不断提取社会大数据并应用。而在这一点上，区块链可以帮我们突破很多现有的限制。

比如说，现在很多人认为隐私不安全、个人行为不受控，甚至对整个人类社会信用体系不信任，这些都可能通过区块链技术来解决。因为对个人来说最有用的那些信息，永远只能通过本人才能读取，人工智能开发者所需要的是个人数据组合在一起的大数据应用方面的一些变化。

人工智能与区块链结合在一起，很有可能会带来人工智能的加速发展。人们会发现，人工智能的发展速度并不像原来想象的那样呈线性增长模式，而是一个指数型的快速爆炸增长的变化过程。也许在不久的将来，我们就能看到应用人工智能的设备走入我们的生活中。而保证这些设备互联互通、并保证它们在共有的学习机制之下实现成功应用的，事实上就是区块链技术。

试想，如果为了让人工智能更好地学习而把所有的数据汇总到某一台主机中，那么这台主机就将变成世界上最危险的“万恶之源”。

只要有人控制了它，那么所有的大数据信息都将被这个人利用，这将是一件非常可怕的事情。区块链的分布式存储模式解决了这个问题，具体原因我们已经反复强调。我们能够看到，区块链在未来人工智能应用领域一方面可以帮助我们解决算法的开发难题，另一方面也可以解决数据应用的安全性问题。因此数据区块链与人工智能的合并，将成为一种必然的趋势。

### 第三节 优化法律体系

曾经流行过这样一种观点：人类在过去几千年的发展变化之中，其实只做了一件事情，那就是把权力关进笼子里。

在过去的几千年中，人类社会的发展和进步其实并不仅仅依赖于技术手段的进步。可以说，人类社会的变化发展，其实核心是社会运行机制和组织形式的变迁。

人类社会找到了一种有效的权利运行模式，让我们通过分工协作，实现了今天所有的科技成就。而这种权利的运行和约束机制的最典型的代表，就是法律。

法律对于人类社会来说非常重要。通过法律的约束，人才能更好地合作，更好地建立企业、发明产品。虽然法律并不是具有实体的物质，但是却让我们生活在秩序和规范之中，让人类社会有持续的向心力。

如果一个国家的基本法律构建不完整，那么这个国家一定会出现极度混乱和不稳定。从历史的维度来看，法律制度甚至决定了国家国力的强盛程度。比如鸦片战争之前的中国，拥有规模在世界上数一数二的军队。虽然武器称不上先进，但是也绝对不是毫无用处。在经济领域，中国更是一家独大，长期处于入超状态。西方世界必须依赖中国的很多商品才能正常地运转下去，如英国人的下午茶、法国人的刺绣时装，这些都要依赖中国的商品。

而当时的中国却不依赖世界任何国家，这造成了整个世界贸易向中国的倾斜。为了打破这一点，英国发动了鸦片贸易战，企图通过大量出口鸦片来赚取中国的现银，进而实现贸易的平衡。

事实上，在第一次鸦片战争开始时，英国原本首选的进攻地点是广州，但是他们看到林则徐广泛修筑工事、整军备战，于是没有贸然在广州登陆，而是一路向北，通过天津攻入中国。这也说明当时的中国并不是没有能力抵抗英国，我们的军事能力与装备水平在当时并没有与世界强国之间存在根本性的差距。相比能够看到的技术层面的问题，中国军队在军队组织方面的差距更为巨大。

鸦片战争期间，八旗制度依然是清政府的基本军队组织形式。虽然八旗兵的训练水平、作战能力已经远不如当年，但是八旗军队却依然是当时军队中最大的组成部分。而为了稳固统治，清政府又不允许招募过多的汉人，这事实上影响了军队的战斗力。

从鸦片战争这段历史，我们能看到，依靠当地群众和汉人、满人共同组成的军队，林则徐在广州吓退了英国军队，但是依靠八旗军队的天津则没能抵抗住英国军队。这也从一个方面证明了军队制度对于军队战斗力的影响。

而今天，中国又到了科学技术快速发展的十字路口。中国在技术方面一直投入很多，也有颇多建树；与此同时，社会组织形式也在不断进化完善，其中典型的代表之一就是法制建设。

法律在人类社会中所起的作用其实并不亚于科学技术的作用，甚至在某种程度上，法律也是一种自然科学的变种形式与载体。

那么人类的法律与区块链有什么关系呢？法律非常的严肃和严苛，涉及证据的存取使用，这甚至可能会影响法官的判断。通过区块链，我们可以把这些具体的问题变得更加顺畅和直接。



## 第四节 加速智能交通“上路”

智能交通，看起来好像是一个具体的技术发展领域，与我们前面所说的工业、人工智能或法律似乎并不处于同一个层面。但是对于区块链来说，这却是最有可能成为第一个具有广泛社会影响的具体应用领域。

智能交通一直被作为人工智能发展的一个重要领域，也是程序员们乐此不疲的重要竞技场。

相比其他领域而言，智能交通目前的具体应用方式和技术实现脉络都比较清晰。它主要包括了几个层面，第一是所有交通参与者层面，也就是驾驶员、行人和各种车辆。

第二是基础交通网络的建设。这就超出了原有的道路层面的概念，还包括各种信号传输、安全管理、信息管理等等。这些方面都属于智慧交通的范围。

第三是与交通相关的各种法律、制度建设和各种社会规则。这些曾经可能并不属于智慧交通的研究范围，但是随着智能化的进一步发展，人们越来越深刻地认识到，如果不讲社会的基本运营规则，这个智能应用可能就难以发挥其应有的作用。因此在整个智能交通发展的过程中，制定和完善交通运行的各种规定、规则、法律，是一个非常有效的方法。

这三个层面是未来智能交通重要的发展方向。

在具体的交通参与者层面，很多具体的应用正在逐渐被突破。最典型的如无人驾驶技术，现在就正获得越来越广泛的应用。

如果半夜在北京驾车回家，那么你很有可能在北京的环线上，看到正处于试验状态的各种无人驾驶车辆在路上飞驰。同样，我们也能看到各种新闻里国内外的自动驾驶创新层出不穷，以优步、谷歌为代表的自动驾驶技术正在逐渐成熟；以亚马逊、京东为代表的自动货运网络体系也在搭建和逐渐完善。智能交通正在快速向我们走近。

这种交通方式事实上带来了驾驶者和车辆之间的互动，但对于行人，目前的影响还没有那么大。未来，行人很有可能通过佩戴便携式智能装备，实现人与其他交通参与者之间的互动互联，以实现更安全的交通，充分防止交通意外的发生。

试想这样一个场景：在一个繁忙的路口，信号灯已经不复存在。一个行人准备横穿马路，而装备了自动驾驶技术的车辆正在飞驰。那么行人要如何穿过这个路口呢？

他可能会扬扬手，通过自己的手环告诉周围所有的车辆，自己即将通过。所有的车辆都停了下来，等这个人走过之后再继续行动。而这个过程事实上就是应用了人工智能和智能交通技术。这是未来我们最希望看到的一个有秩序、高效、安全、快捷的交通网络。

但是这里面临的一个重要问题是，要实现这种互动和交流，事实上需要通过设备获取和发送多种信息，而这很有可能会带来危险。

任何关于个人位置的信息都可能被别有用心的人利用，那么如何更好地保护这些信息，就变成一个非常重要的问题。这样，我们就又回到了区块链技术。

通过区块链技术，我们可以有效地打通人与车辆之间的关系。即使在某一个路口，我们发布了自己的位置信息，这些信息也不会被其

他无关的人获取。这就解决了我们现在所面临的一个非常重要的行动轨迹记录安全性问题。

2018年，国际恐怖组织通过几个智能运动手环的信息，模拟出了美军在某些区域的秘密军事基地的布局。方法非常简单，就是通过手环的密集运动轨迹，找到这个区域里大运动量的人群，而这些人群的运动特点又与军队军人很像，因此可以推测这些人属于军事基地。

智能设备已经带来了很多军事上的风险。比如在战争和反恐前线，很多美军基地曾因为这样的方式暴露，不得不转移基地，更换防御模式，以应对即将到来的危机。为了彻底杜绝这种危险，美军甚至修改了部分条例，限制军队使用运动手环。

假如我们把这些设备应用到智能交通中，那么我们的位置信息也就暴露了。而区块链可以帮我们避免这种尴尬。所有的位置信息，仅仅在我们需要使用的时候透露；在要保密的时候，这些信息不能被任何人获取。这样，区块链又帮我们解决了智能交通应用方面的一个重要问题——不能通过实时位置互换来实现智能交通的全流程联通。

在具体的路网建设和制度建设方面，区块链也有很重要的应用。前面我们已经说过了区块链在法律方面的应用，而在具体的制度方面，区块链的应用与这也有异曲同工之妙。更重要的是，我们在智能交通的发展过程中往往更偏重于技术的应用而忽略社会制度的影响；而在用区块链建设智能交通的过程中，可能会采取分包制度，让不同的人共同完成，关注不同的重点，而这些最终都将体现在程序中，而不像过往需要先开会讨论制度如何制定，然后再通过技术去实现。这样就可以最大限度地提高发展效率。

在路网建设方面，区块链更多的是提供快速的建设模式。路网建设最大的难题是资金投入。随着人类社会的进步、技术的发展，我们

的工程规模越来越大，而且拥有大型建筑设计能力的中国，对建设公路的各种方式方法都已经有了非常丰富的经验。更重要的是如何找到足够巨量的资金，支持各种路网建设。区块链可以更好地帮助我们融合这些资金，带来各种各样的投资，帮助我们实现发展目标。

可以看到，区块链最有可能率先落地的就是在智能交通领域。它可以快速地找到这一领域的突破口。如果条件允许，拿出一个路网规划，相关人员可以马上用区块链的思维和模式解决。其实在中国，已经有一些公司在探索通过区块链模式实现公路建设的投融资，融合各种技术，提高汽车的使用效率，实现智慧路网的部分功能。

## 第五节 大数据与区块链的碰撞

大数据与区块链是当今最热门的两个话题，带动了一系列的投资热潮。不论是风投领域，还是传统的金融领域，只要有这两个关键词出现，往往能让企业获得特别的关注。这也说明了这两个词在当今社会的火爆程度。

我们在前文中已经从各个维度对区块链进行了详细阐述，那么大数据又是什么呢？

现在很多人都认为，大数据的本质是“大”。也就是说，它的数据量必须非常的广泛和巨大，可能是海量级的。其实这并不准确。

大数据所指的“大”其实更偏向于全，也就是尽可能地接近某个统计范畴内最全面的数据，甚至达到全数据的统计结果。只有这样才能真正实现大数据的基本目标。

大数据引起人们的关注，事实上是因为可以通过它对未来做出预测，获取详细分析，对未来进行有针对性的指导。想要实现这些，最重要的就是数据的提取和分析。

事实上，大数据目前最成功的领域是在历史学。这可能是一个平时不太引人注目的范畴。但事实上，正是在因为在历史数据的分析方面发挥了巨大作用，人们才会对大数据有了更大的兴趣。

最早进行这种分析的是一位英国的历史学家。他把所有历史数据进行了一次编码——当然这里的历史数据指的是关于重大事件与经济、政治等方面的数据。之后，他把这些编码以一个自有的逻辑对其进行了分析。

例如，在一个重大的政治事件发生之前多少年，会发生一次旱灾，或者一次重大疾病的流行对宗教的传播有什么影响。以这样的模式，这位历史学家对过去几千年的人类历史进行了一次梳理和分析。结果他发现了一个预测模式，通过这个模式，他甚至可以预测未来的某一年，在世界上的某个国家会发生什么样的重大历史事件，而这种预测的准确率达到了一个很高的水平。虽然这些所谓的预测最终可以被改变，因为人们已经掌握了规律，可能采取一些措施，但是这样的尝试给了人们一种可能：也就是通过对过去的历史数据进行分析，可以得到对未来发展变化的预测。这当然也符合我们现在所有的预测模式。比如在灰色预测过程中，事实上就是通过将过去的数据放入方程，去预测未来的发展模式，而这一切都与数据相关。

因此我们可以认为，假如有足够多的数据量，就可能对世界上所有即将发生的事情进行预测。如果能够做到这一点，那么无疑我们将控制整个世界的变迁。

这要怎么做到呢？要实现这一点需要不断提取尽可能多的数据。

但是，现实和理想总是有区别的。在整个大数据分析过程中，有一种观点是：世界上只有5%的数据是结构化数据，也就是人们常规认为的数字信息；剩下95%的数据都是不可量化的。这意味着，不可能有绝对正确、绝对全面的数据。

通过区块链模式，可以尽可能地将那些非结构化的数据进行结构化处理。通过将现有各种数据拆解并存储于各个存储单元，我们能对整个世界的模式有更加清晰的认知。

既然说到区块链，那么要解决的一个问题必然是信息的安全性问题。区块链在这方面所能起到的作用是不可替代的。通过将区块链应用到各种数据的提取过程中，就可以实现我们对各种研究所需的非结

构化数据的集中使用，而不用担心这些数据被肆意传播和滥用。这也就预防了可能出现的数据风险。

从更深远的意义来说，我们对数字的应用模式从根本上发生了变化。也就是说，我们过往的研究所需要使用的数据，往往都是某个机构积累的，或者某些企业出钱购买的数据。但是当我们通过区块链模式链接各种各样的数据之后，就会发现数据之间的壁垒被打通了，研究也会变得更加顺畅，大数据分析也就变得更加有效。

当然，区块链也可能带来另外的问题。

在大数据研究中，有的时候我们需要对某一群体的特征进行精确的分析和描绘。但是大数据要求的这种数据模式，在区块链中却很难实现。比如说，我们要确认一组人群——80后或者90后——他们在职场中真正面临的困境是些什么。通过对这个问题的进一步细致和深化，我们就可以把分布式存储在各个领域里的、关于各种各样情境的困惑集中起来，形成我们的结论。但如果再进一步，想了解某一家企业、一个群体或者某一个具体区域的人群的特点，我们就无法得到有效的数据标签来实现分析了。

换句话说，区块链通过牺牲数据的个性化标签来实现我们对某一类问题进行系统研究的可能性，但是同时也让我们在进一步的分析过程中，遭遇数据提取的困难。

总体来说，区块链还是为大数据研究提供了一种非常有效的支撑。它可以帮助我们更好地实现大数据的应用，也解决了各种数据之间横向迁移时的壁垒。

而另一方面，大数据也为区块链的应用提供了更好的支撑。

从目前的情况来看，区块链的应用范围依然比较狭窄。虽然它在很多领域中都有非常好的前景和解决具体问题的能力，但是具体到某个领域的时候，区块链却总是很难实现目标。

在这种情况下，如何能够取得突破，快速找到一个能够让区块链落地并且被大家使用的方式，就非常重要了。

与之相反，大数据的应用事实上已经被很多人所接受。尤其在商业领域，通过大数据分析实现商业竞争的目标，也成为很多企业的首选做法。在这种环境下，如果区块链能够给大数据的研究提供更好的支撑，可能就会带来对区块链应用需求的上升，这事实上可以为区块链的应用和推广带来非常好的推动作用。

区块链与大数据的整合，在未来将是一个必然的趋势，大数据的研究将越来越深入地触及人类社会的底线。我们的隐私、数据权利和思想权，都将成为讨论的范畴。而区块链则可以让大数据的研究跨越这些壁垒，形成无标签化的数据结构，让大数据研究者仅从数据看数据，而不考虑伦理的种种限制，这事实上也为未来的技术研发带来更广阔的可能性。同样，借助大数据的东风，区块链也有可能很快找到自己在现实中的落脚点，获得更好的发展。



[1] 《“区块链技术”究竟是什么？通俗版解读来了！》, <https://baijiahao.baidu.com/s?id=1591182779653995536&wfr=spider&for=pc>

[2] 《“区块链技术”究竟是什么？通俗版解读来了！》, <https://baijiahao.baidu.com/s?id=1591182779653995536&wfr=spider&for=pc>

[3] 《区块链：既是技术方案，也是制度机制》，[https://www.sohu.com/a/228103176\\_355061](https://www.sohu.com/a/228103176_355061)

[4] 《区块链所带来的公信力革命》，<http://www.civillaw.com.cn/zt/t?id=29937>

[5] 《北京乐酷达网络科技有限公司与绥化市华辰商贸有限公司彭泉泉侵权责任纠纷一案二审民事判决书》（有删减），<http://wenshu.court.gov.cn/content/content?DocID=ce26a599-64e9-44ab-96fd-b04617d482b4>

[6] 《四川省内上线用区块链等技术打造的房屋租赁平台》，原载《乐山日报》2018年10月29日。

[7] 《光伏区块链企业SolarCoin生成记》，[http://www.sohu.com/a/228245235\\_257724](http://www.sohu.com/a/228245235_257724)

[8] 《扒一扒物联网与区块链的关系》，[https://www.sohu.com/a/209940299\\_828257](https://www.sohu.com/a/209940299_828257)

[9] 《中国人民银行数字货币研讨会在京召开》，<http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3008070/index.html>

[10] 《保险业联盟将发布 Codex 1 区块链原型经纪人饭碗可能不保》，<https://www.jinse.com/news/blockchain/61620.html>

[11] 《WTO 发布 2016 年全球贸易统计报告，商务部重申不追求贸易顺差》，[http://www.sohu.com/a/134030039\\_611309](http://www.sohu.com/a/134030039_611309)

[12] 据英国《金融时报》2018年7月27日报道，CLS与科技公司IBM合作推出的CLNet，是一种基于区块链技术的支付网络服务，能够整合到银行IT系统，以提升全球外汇市场的标准化交易水平，同时降低流程处理成本。

[13] Circle International Financial是数字资产领域著名企业家杰里米·阿莱尔（Jeremy Allaire）在2013年10月推出的产品。2015年5月，Circle开启美元存储与转账业务，允许用户只使用美元进行交易，用户可持有、转出并即时接收美元，无须额外收费，同时还受到联邦储蓄保险公司和美元稳定价值保护。这让它从一个简单的比特币公司变身为类似PayPal和传统银行的机构。

[14] 泄密的“看家神器”，<http://tv.cctv.com/2017/06/18/VIDExc32bHCyKW74Eml7GTNd170618.shtml>

[15] <https://www.thomsonreuters.cn/zh/products-services/financial/quantitative-research-trading.html>

[16] 《区块链：重塑经济与世界》，徐明星、刘勇、段新星等著，中信出版集团，2016年。

[17] 参见《关于深化医药卫生体制改革的意见（征求意见稿）》第三条第五款。

[18] 《国内首个医疗场景“区块链”落地常州》，[http://www.sohu.com/a/166552738\\_128505](http://www.sohu.com/a/166552738_128505)

[19] 联合国开发计划署前身是1949年成立的“技术援助扩大方案”和1958年设立的旨在向较大规模发展项目提供投资前援助的“联合国特别基金”。根据联合国大会决议，这两个组织于1965合并成立了今天的开发署。在早期，由于特别基金主要面向不发达地区且提供发展专项基金，因此一些机构和个人将特别基金称为“扶贫署”。随着联合国机构合并，相关的扶贫工作也转移至开发署。

[20] 根据2018年9月18日国务院扶贫开发领导小组办公室文件《国务院扶贫办关于反馈 贵州省2017年贫困县退出专项评估检查结果的函》，截至2018年9月，贵州贫困县数量已经下降至47个。