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

BLOCKCHAIN IN CHINA

它将如何颠覆未来

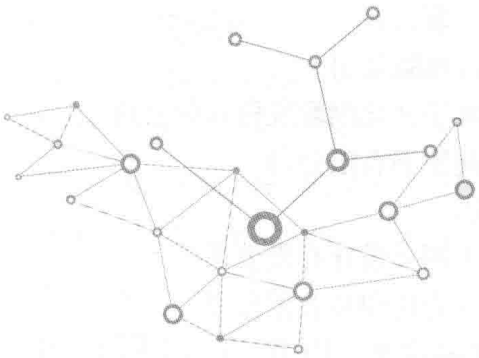
刘兴亮◎著

中国友谊出版公司

区块链在中国

它将如何颠覆未来

刘兴亮◎著



中国友谊出版公司

图书在版编目（CIP）数据

区块链在中国 ：它将如何颠覆未来 / 刘兴亮著 . -- 北京 ：中国友谊出版公司，2019.3
ISBN 978-7-5057-4312-0

Ⅰ . ①区… Ⅱ . ①刘… Ⅲ . ①电子商务－支付方式－研究 Ⅳ . ① F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 288554 号

书名 区块链在中国
作者 刘兴亮 著
出版 中国友谊出版公司
策划 杭州蓝狮子文化创意股份有限公司
发行 杭州飞阅图书有限公司
经销 新华书店
制版 杭州中大图文设计有限公司
印刷 杭州钱江彩色印务有限公司
规格 710×1000 毫米 16 开
15.5 印张 210 千字
版次 2019 年 3 月第 1 版
印次 2019 年 3 月第 1 次印刷
书号 ISBN 978-7-5057-4312-0
定价 49.00 元
地址 北京市朝阳区西坝河南里 17 号楼
邮编 100028
电话 （010）64678009

安徽大学图书馆 藏书 www.lib.ahu.edu.cn

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了，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

此为试读，需要完整PDF请访问：www.ertongbook.com

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）×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，因此也就不用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

---

❶ 《“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

此为试读，需要完整PDF请访问：www.ertongbook.com

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。[1]

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

---

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

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，也可能会导致交易不顺利；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。你如果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。[1]

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

---

1 《区块链：既是技术方案，也是制度机制》，https://www.sohu.com/a/228103176_355061

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

关系（定向）	活动	目的
政府—区块链	政府可以在区块链上发布其最新政策，由区块链来执行和监控。	确保政府制定的政策对所有官员均可见。
政府—大众	政府可以给大众制定政策，例如一夫一妻制。而且政府可以监控大众的行为，例如监督是否有人同时与两个人结为夫妻。	确保大众能够遵从政府政策。
政府—政府	政府可以验证其政策是否妥善地储存在区块链上，上级可以监督其他政府工作人员的行为。	确保政策有效地被下级贯彻和实施。
大众—区块链	大众可以在区块链中跟踪并监督自己的个人数据，以确保数据储存正确，并可以使用区块链中的个人数据，作为银行、产权交易等个人事务的凭证。	确保大众可以验证其储存在有关部门的数据是否正确，存储本身是否妥当。
大众—政府	大众可以确保政府“内鬼”无法在区块链上更改他们的个人数据。	确保政府官员不能更改数据，防止其用“更改数据”的手段钳制大众。
大众—大众	在任何财产或法律事务中，人们可以通过区块链验证其他人的身份。例如，一个女性可以验证，她未来的丈夫在此时没有与另一个女性结婚。	防止许多欺诈案件的发生。
区块链—区块链	由多个节点参与的区块链能够确保数据不被更改，任何人试图改变数据的行为都会被发现并追责。	确保所有节点都参与到区块链中，并互相监督。

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

此为试读，需要完整PDF请访问：www.ertongbook.com