区块链：定义未来金融与经济新格局, 张健

本书开篇通过简述人类社会信息转播方式和价值传递方式的演化路径，勾勒出一个从信息到信用、从互联网到区块链的发展轨迹，引出了区块链这种高效的价值传递方式出现的必然性。
张健, 区块链：定义未来金融与经济新格局, loc. 44-46. Kindle Edition

文字作为一种人际交流的手段，承载的是信息；而货币作为一种价值传输的载体，承载的是信用。
张健, 区块链：定义未来金融与经济新格局, loc. 165-166. Kindle Edition

中，香农为人类引入了一个新的单词——比特（bit）。牛顿量化了力，建立起经典物理学的大厦；香农量化了信息，打下了人类进入信息时代的基础。
张健, 区块链：定义未来金融与经济新格局, loc. 185-187. Kindle Edition

农为人类引入了一个新的单词——比特（bit）。牛顿量化了力，建立起经典物理学的大厦；香农量化了信息，打下了人类进入信息时代的基础。
张健, 区块链：定义未来金融与经济新格局, loc. 185-187. Kindle Edition

香农为人类引入了一个新的单词——比特（bit）。牛顿量化了力，建立起经典物理学的大厦；香农量化了信息，打下了人类进入信息时代的基础。
张健, 区块链：定义未来金融与经济新格局, loc. 185-187. Kindle Edition

香农为人类引入了一个新的单词——比特（bit）。牛顿量化了力，建立起经典物理学的大厦；香农量化了信息，打下了人类进入信息时代的基础。
张健, 区块链：定义未来金融与经济新格局, loc. 185-187. Kindle Edition

传统的货币理论认为货币的本质是商品或一般等价物，随着金本位制的瓦解，以20世纪70年代布雷顿森林体系的崩溃为标志，金属本位彻底退出了历史舞台。事实上，目前世界上几乎所有国家的货币都已是信用货币。信用货币是货币发展中的现代形态，不再代表任何贵金属，并且其本身价值远远低于其货币价值，已经和商品属性彻底脱钩。
张健, 区块链：定义未来金融与经济新格局, loc. 218-221. Kindle Edition

区块链是作为比特币底层技术与基础架构而诞生的。比特币是一个可以点对点进行支付、不依赖任何第三方的电子现金系统。
张健, 区块链：定义未来金融与经济新格局, loc. 227-228. Kindle Edition

这里所谓的定义信用，不是计算人或参与主体的信用，而是计算信用行为（比如交易）的可信程度，或者说计算一个信用行为在未来发生违约（欺诈）的可能性。违约的可能性越低，该行为的可信程度就越高；反之，违约的可能性越高，该行为的可信程度就越低。
张健, 区块链：定义未来金融与经济新格局, loc. 247-250. Kindle Edition

我们这里可以将信用行为的可信度简单定义为违约成本与违约收益的比值（信用行为可信度 = 违约成本/违约收益）。
张健, 区块链：定义未来金融与经济新格局, loc. 254-255. Kindle Edition

比特币从诞生到现在已经在争议中走过了7年，在这样一个去中心化的经济系统内部，在没有任何可信的第三方担保的情况下，却没有发生过严重的欺诈行为，其主要原因在于，欺诈行为的成本往往远大于预期的收益。这也符合中本聪在创造区块链时的计算及预测[11]。显然，当欺诈行为所要付出的成本远大于其所
张健, 区块链：定义未来金融与经济新格局, loc. 256-259. Kindle Edition

比特币从诞生到现在已经在争议中走过了7年，在这样一个去中心化的经济系统内部，在没有任何可信的第三方担保的情况下，却没有发生过严重的欺诈行为，其主要原因在于，欺诈行为的成本往往远大于预期的收益。这也符合中本聪在创造区块链时的计算及预测[
张健, 区块链：定义未来金融与经济新格局, loc. 256-259. Kindle Edition

信用是制造货币的真正原材料。而区块链通过构造一个可以量化信用的经济系统，使得一个点对点的电子现金系统——比特币[1]的出现成为可能。或者说，区块链创造了一个数字化的、可以点对点传输价值的信用系统。
张健, 区块链：定义未来金融与经济新格局, loc. 306-309. Kindle Edition

亚当·贝克（Adam Back）是一位英国的密码学家，1997年，他发明了哈希现金（Hashcash）[2]，其中用到了工作量证明系统（Proof Of Work）。这个机制的原型可用于解决互联网垃圾信息，比如作为垃圾邮件问题的一个解决方案[3]。它要求计算机在获得发送信息权限之前做一定的计算工作，这对正常的信息传播几乎不会造成可以察觉的影响，但是对向全网大量散布垃圾信息的计算机来说，这些计算会变得不可承受。这种工作量证明机制后来成为比特币的核心要素之一。
张健, 区块链：定义未来金融与经济新格局, loc. 344-350. Kindle Edition

哈伯和斯托尼塔（Haber and Stornetta）在1997年提出了一个用时间戳的方法保证数字文件安全的协议[4]。对它的简单解释是，用时间戳的方式表达文件创建的先后顺序，协议要求在文件创建后其时间戳不能改动，这就使文件被篡改的可能性为零。这个协议成为比特币区块链协议的原型。
张健, 区块链：定义未来金融与经济新格局, loc. 350-353. Kindle Edition

戴伟（W Dai）是一位兴趣广泛的密码学专家，他在1998年发明了B-money[5]。B-money强调点对点的交易和不可更改的交易记录，网络中的每一个交易者都保持对交易的追踪。不过在B-money中，每个节点分别记录自己的账本，这不可避免地会产生节点间的不一致。戴伟为此设计了复杂的奖惩机制以防止节点作弊，但是并没有从根本上解决问题。中本聪发明比特币的时候借鉴了很多戴伟的设计，并和戴伟有很多邮件交流。
张健, 区块链：定义未来金融与经济新格局, loc. 353-357. Kindle Edition

哈尔·芬尼（Hal Finney）是PGP公司的一位顶级开发人员，也是密码朋克运动早期和重要的成员。2004年，芬尼推出了自己的电子货币，在其中采用了可重复使用的工作量证明机制（RPOW）。哈尔·芬尼是第一笔比特币转账的接受者，在比特币发展的早期与中本聪有大量互动与交流。由于身患绝症，哈尔·芬尼已于2014年去世。
张健, 区块链：定义未来金融与经济新格局, loc. 357-360. Kindle Edition

2009年1月3日，中本聪在位于芬兰赫尔辛基的一个小型服务器上挖出了比特币的第一个区块——创世区块（Genesis Block），并获得了首批“挖矿”奖励——50个比特币。
张健, 区块链：定义未来金融与经济新格局, loc. 369-370. Kindle Edition

货币不是一种商品，而是信用与清算构成的一套体系[
张健, 区块链：定义未来金融与经济新格局, loc. 424-425. Kindle Edition

从纸质的信用货币发展到目前广泛使用的电子货币，如信用卡、网上银行、手机银行等，进一步体现了记账货币的特点——当你通过网银给其他人转账的时候，没有发生任何物理货币的转移，只是银行里记账系统的账务发生了变化而已。
张健, 区块链：定义未来金融与经济新格局, loc. 438-441. Kindle Edition

区块链[8]的本质是一种去中心化的记账系统，而比特币正是这个系统上承载的“以数字形式存在”的货币。我们可以认为区块链与比特币之间的关系就是凯恩斯所说的记账货币与货币之间的关系，也可以用菲利克斯·马丁对货币的理解[9]来说明两者的关系——比特币只是记账的表征，而区块链就是其背后的一套由信用记录以及信用记录的清算构成的体系。
张健, 区块链：定义未来金融与经济新格局, loc. 441-446. Kindle Edition

市场经济是一个典型的去中心化系统，这个系统的共识机制就是市场经济制度。参与市场经济的每个主体都在遵守商业规则的基础上，按照实现自己利益最大化的原则行事，同时在客观上推动了整个市场的繁荣。“无形的手“推动了人们争取自身利益的行为，这些行为的结果则服务于更大的社会利益。正如亚当·斯密所说：“我们的晚餐并非来自屠宰商、酿酒师和面包师的恩惠，而是来自他们对自身利益的关切。”
张健, 区块链：定义未来金融与经济新格局, loc. 537-541. Kindle Edition

经济学人》的封面文章[6]所讲的，区块链是一个制造信任的机器。在任何需要信任的领域，区块链都有用武之地。
张健, 区块链：定义未来金融与经济新格局, loc. 584-585. Kindle Edition

经济学人》的封面文章[6]所讲的，区块链是一个制造信任的机器。在任何需要信任的领域，区块链都有用武之地。
张健, 区块链：定义未来金融与经济新格局, loc. 584-585. Kindle Edition

互联网同区块链一样，也是个去中心化的网络，并没有一个“互联网中心”存在。不同的是，互联网是一个高效的信息传输网络，但并不关心信息的所有权，没有内生的、对有价值信息的保护机制；区块链作为一种可以传输所有权的协议，将会基于现有互联网协议架构构建出新的基础协议层。
张健, 区块链：定义未来金融与经济新格局, loc. 704-707. Kindle Edition

未来区块链的结构也一定是分层的，不同层级、不同类型的区块链承担着不同的作用。我们认为，未来的区块链也将会在一个统一的底层协议基础上发展出各种各样的应用层协议，从而构建出多样化生态的价值互联网。
张健, 区块链：定义未来金融与经济新格局, loc. 710-712. Kindle Edition

电子商务没有改变交易的本质，但通过打破信息不对称，提升了交易效率，降低了交易成本。
张健, 区块链：定义未来金融与经济新格局, loc. 883-883. Kindle Edition

互联网金融是新技术条件下金融手段的演化，它并不会改变金融服务的内涵。首先，金融的核心功能不变。互联网金融与传统金融一样，都是在不确定的环境中进行资源的时间和空间配置，以服务实体经济。第二，互联网金融不会改变股权、债权、保险、信托等金融契约的内涵。第三，互联网金融不会改变金融风险、外部性等概念的内涵。风险指的仍是未来遭受损失的可能性，市场风险、信用风险、流动性风险、操作风险、声誉风险和法律合规风险等概念及其分析框架依然适用[
张健, 区块链：定义未来金融与经济新格局, loc. 884-888. Kindle Edition

互联网金融最根本的意义是改善传统金融中信息不对称的问题。
张健, 区块链：定义未来金融与经济新格局, loc. 913-913. Kindle Edition

第一，互联网金融的发展速度主要取决于互联网技术的发展速度，而不是金融自身的发展速度。我们预计，20年后，互联网技术将在目前的基础上进一步大幅度降低金融活动中的交易成本，并解决信息不对称的问题。第二，20年后，伴随着互联网成长起来的这一代人将成为社会主流，他们的互联网使用习惯将极大地影响金融交易和组织形式。”
张健, 区块链：定义未来金融与经济新格局, loc. 920-923. Kindle Edition

最新崛起的以太坊是另一个典型，虽然其背后的区块链同样是公有链，但其目的并不是发行及运行一个数字货币系统，而是实现一个可编程的智能合约平台。
张健, 区块链：定义未来金融与经济新格局, loc. 1069-1070. Kindle Edition

而私有链则是最近一两年发展最为迅速及活跃的区块链类型。R3CEV是一个典型的构建私有链的公司，其发起的银行联盟的目标是制定银行间的清算标准，目前已经有40多家来自不同国家的大型银行加入。
张健, 区块链：定义未来金融与经济新格局, loc. 1071-1073. Kindle Edition

电子商务方面，最近，有一个被称为“去中心化淘宝”的开源项目OpenBazaar[8]发布了beta版本。OpenBazaar是一个去中心化商品交易市场，使用比特币进行交易，既没有费用，也不用担心受到审查。因此相对于易趣与亚马逊这些提供中心化服务的电子商务平台，通过OpenBazaar不需要支付高额费用，不需要担心平台收集个人信息致使个人信息泄露或被转卖。
张健, 区块链：定义未来金融与经济新格局, loc. 1610-1613. Kindle Edition

有两件事的发生将密码学带入了公众领域：标准加密系统——数据加密标准（Data Encryption Standard，DES）的诞生和公钥加密算法（也称为非对称加密算法）的发明[
张健, 区块链：定义未来金融与经济新格局, loc. 1686-1688. Kindle Edition

由于加密算法和解密算法都是同一模式，同时只用一把密钥保证加密数据的安全，因此这种加密算法也叫作“对称加密算法”。
张健, 区块链：定义未来金融与经济新格局, loc. 1710-1711. Kindle Edition

这个时间段是密码学开始蓬勃发展的一个开端，后期发展出来的公钥密码学、哈希算法、其实属于现代密码学的范畴。
张健, 区块链：定义未来金融与经济新格局, loc. 1712-1713. Kindle Edition

工作量证明系统的主要特征是客户端需要做一定难度的工作得出一个结果，验证方却很容易通过结果来检查客户端是不是做了相应的工作。这种方案的一个核心特征是不对称性：工作对于请求方是适中的，对于验证方则是易于验证的。它与验证码不同，验证码的设计出发点是易于被人类解决而不易被计算机解决[4]。
张健, 区块链：定义未来金融与经济新格局, loc. 1911-1914. Kindle Edition

比如企业内部可以做一个区块链，用于内部清算，那这能算是区块链吗？我个人认为这不是区块链，因为你没有连任何东西，你只是在连你自己。正如同

你不能说把自己家里的3台计算机连起来就是互联网。内部的区块链系统只能算是数据库——分布式数据库。
张健, 区块链：定义未来金融与经济新格局, loc. 2472-2474. Kindle Edition

金融是人们跨越时间、空间对价值进行交换的活动，而价值交换的前提是“信息”和“信任”。最原始的交换是以物易物，比如用一头羊换一只鸡，可是供需很难直接匹配，于是人们开始寻找贝壳、金银等作为价值交换的载体。再后来，由于金银等物质携带起来不够安全方便，纸币及银行应运而生，虽然纸币本身没有价值，但由可靠的银行为其背书，一张薄薄的纸也成了价值的载体。到了互联网时代，连纸都变得可有可无了，支付简化成单纯的“记账”行为。
张健, 区块链：定义未来金融与经济新格局, loc. 2495-2500. Kindle Edition

而互联网的本质又是什么呢？最初，它只是信息的搬运工，我们可以通过互联网迅速将信息复制到全世界，但无法解决价值转移的问题。
张健, 区块链：定义未来金融与经济新格局, loc. 2503-2505. Kindle Edition

金融民工穿西服和银行的楼盖得金碧辉煌的原理是一致的，因为需要增加客户对中心化机构的信任。如果人们不相信银行的偿付能力，可能就会发生挤兑，从而导致银行破产；如果政府没有公信力，法币便会贬值如废纸。这种基于对单点的信任而建立起来的信用共识，逼迫金融中介去维护高大上的形象。
张健, 区块链：定义未来金融与经济新格局, loc. 2508-2511. Kindle Edition

互联网企业为什么会涉足金融呢？因为线上商业场景出现，在主战场上做起金融自然得心应手。其突出优势在于可以依靠线上数据来低成本地做信用评估。阿里、京东掌握了线上商城的交易数据，可以廉价地为小商户和个人进行信用画像，降低了服务门槛，满足了中低端客户的长尾需求。这可能是互联网企业更亲民的原因所在。
张健, 区块链：定义未来金融与经济新格局, loc. 2514-2517. Kindle Edition

演变至今日，互联网必须要升级成对信息负责，给信息确权的信用互联网，而这个过程不能仅由政府、企业来完成，每个网民都应参与进来，一同决定互联网的前途。
张健, 区块链：定义未来金融与经济新格局, loc. 2532-2534. Kindle Edition

以区块链为基础，人们正在互联网上建立起一整套信用互联网治理机制，包括①工作量证明机制（如果要篡改区块链上的数据，需要拥有超过全网51%的算力，这会使得作伪的成本高于预期利益）；②互联网共识机制（无需甄别好坏，以共识来确保正确）；③智能合约机制（以可编译的程序代替合同，网络自动执行合约）；④互联网透明机制（账号全网公开而户名匿藏）；⑤密码学，非对称加密和公私钥等技术等。
张健, 区块链：定义未来金融与经济新格局, loc. 2537-2541. Kindle Edition

在传统经济学中，资源稀缺是基本假设，竞争并攫取资源所有权是主题。而如今，认知与资源盈余出现，合作并共享资源的使用权是大势所趋。而共享经济形态急需建立全球性的信用共识，因此我们寻找到人类文明最大的公约数——数学。区块链是一个对人性悲观却非常真诚的协议。既然没有办法逃避选择，不选择也是一种选择，人就必须为自己的存在和一切行为”承担责任“，与其信权威、信上帝、信他人，还不如信数学、信自己、信理性。
张健, 区块链：定义未来金融与经济新格局, loc. 2592-2596. Kindle Edition