区块链：从数字货币到信用社会

作者：长铗 韩锋等

区块链

——从数字货币到信用社会

长铗 韩锋 等 著

中信出版社

目录

序一

区块链：建设互联网的价值高速公路

姚余栋[1]

区块链因比特币而生。一般民众都将比特币简单地视为一种货币，但从根本上来说，区块链更是价值传输协议。相较于通常意义上的数字货币，区块链与互联网TCP/IP（传输控制协议/网络互联协议）协议更为相似。只不过，TCP/IP协议为信息互联网而设计，区块链则为价值互联网提供了理论基础。

但在互联网上进行价值交换，需解决三个问题：一是确保价值交换的唯一性；二是如何确立价值交换双方的信任关系；三是如何确保双方的承诺能够完成依靠网络的自治机制（智能合约）而自动执行，而无需可信第三方的介入。2009年基于区块链技术的数字货币比特币的诞生，给上述三个问题找到了解决方案。

区块链是一种新型的去中心化协议，链上数据不可随意更改或伪造，因而提供了无需信任积累的信用创建范式。区块链可理解为一个账本（ledger），人们只需加入一个公开透明的数据库，通过点对点的记账、数据传输、认证或智能合约来达成信用共识，而不再借助任何中间方。这个公开透明的数据库包括了过去所有的交易记录、历史数据及其他相关信息。这些信息安全地分布式存储在一串使用密码学方法产生的数据块中，即为一个区块，从创始区块连接到当前区块，就形成了区块链。由于每个区块都包含了上一个区块的索引，即区块的哈希（hash），使得每一个区块按照时间顺序产生，若要逆转某个区块上的交易，需要重新计算该区块之后的所有区块，这在计算难度上几乎是不可能的。于是，区块链逐步成为一种可靠的审计工具，也让系统内参与者之间的信任创建得以实现。

区块链本身具有分布式（Distributed）、去中介（Disintermediation）、去信任（Trustless）、不可篡改（Immutable）、可编程（Programmable）等特征。这些特征使区块链能弥补传统金融机构的不足，提高运作效率，降低运营成本，灵活更新市场规则，防止信息篡改和伪造，同时也大大提高了稳定性，减少了宕机风险。因而区块链可应用的场景非常广泛，众多金融机构正在研究区块链技术在金融市场的应用。

区块链可直接用于银行相关业务。例如，对账户的反洗钱检查、交易后的银行结算等涉及人工审核的业务。区块链的分布式网络结构使账户资产、信用等信息可在各银行间共通，这大大简化了重复性手续，节省大量人力物力。目前，全球中央银行和商业银行都在积极寻求利用区块链技术，开发数字货币平台。R3CEV区块链项目在世界上获得多家银行支持，目前有42家银行加入该项目的研究，实现实时结算和清算功能。

各国央行还可以使用区块链技术尝试发行eSDR，来构建一套新型的超主权货币跨国支付清算体系，从而适当缓解主权货币主导下的传统货币体系缺陷，也有助于应对全球“流动性困局”。英国央行计划发布由中央机构控制的模拟特币数字货币RSCoin。这是一款完全基于央行的需求来设计的基于区块链技术的数字货币。该技术将依赖于一系列权威机构，如商业银行，防止货币重复消费。我国央行也在研讨发行数字货币方案。

由于任何人都能创造自己的区块链系统：启动条件十分简易，且不难实现。当前正迎来区块链的寒武纪大爆发，大量区块链开源或封闭试验得以实施。现有区块链林林总总，有公有链、联盟链与私有链之分。知名项目除了R3CEV，还有Linux基金会推进的超级账本（Hyperledger），以智能合约平台而著称的以太坊，以及基于比特币区块链系统的闪电网络与侧链技术……正如区块链数据的合法性是以算法来竞争最长链，这些区块链协议与技术也呈现出非常激烈的竞争局面，它们最终哪一种会胜出，联盟链与公有链哪一个笑到最后，并成为互联网通用价值传输协议，目前还是个谜。

或许，互联网的早期发展能带给我们以启示。互联网鼻祖是美国国防部的军用网，叫做“阿帕网”（ARPAnet）。在20世纪70年代，ARPAnet已经形成好几十个计算机网络，但是每个网络只能在网络内部的计算机之间互联通信，不同计算机网络是一个个信息孤岛，它们之间不能通讯。直到1974年，研

究人员设计了连接分组网络的协议，其中就包括著名的TCP/IP——网际互联协议IP和传输控制协议TCP，这才将这些孤岛连通起来，构成现在的因特网（Internet）。因而，联盟链与公有链之间，比特币与以太坊之间，以及其他区块链网络之间，也许并不是一个你死我活、赢家通吃的局面，而是会通过构建不同区块链之间的价值传输协议，而形成一个统一的区块链：互联链（Interchain）。同样，互联链也会像互联网的物理层、网络层、传输层、应用层的层级设计一样，根据功能定位的不同、应用场景的不同、共享账簿的开放权限的不同，而演化为不同层级的协议。

如果说TCP/IP协议让我们进入了信息自由传递的时代，区块链则将把我们带入价值高速公路时代。区块链协议的完善，将构成共享金融的基础设施。当今互联网正进入分布式时代，逐渐从传递信息的互联网演变为交换价值的互联链。出于价值交换的需要，人类进入数据可计算时代。数据结构也进化成为附带计算机程序的代码，数据可以自我计算，自我运行，从而成为智能数据，为整个人类社会进入智慧社会打开了大门。

[1] 作者为中国人民银行金融研究所所长。

序二

区块链：网络世界运行规则与技术的全新探索

王永利[2]

近年来，区块链成为全球互联网领域，特别是金融互联网界快速升温、越来越热的概念。在中国，区块链更是引发越来越多的人、越来越热的关注和探索。

区块链最早面世，是由于2009年初发布的比特币，区块链成为比特币产出、记录、流通的基础协议和技术应用。尽管比特币自面世以来饱受争议，甚至仍不能被政府和货币当局视同为“货币”，但比特币所应用的区块链技术却得到了包括政府和货币当局在内的广泛关注。

为什么区块链会成为快速升温的热点技术和话题？

这其中最重要的可能就是，在区块链技术基础上推出的比特币，打开了一种与传统社会（线下）没有多少关联的，完全应用于网络世界（线上）的网民身份验证、财富确认、交易记录、公证核查等全新的技术与规则体系的探索和尝试，而这给人们适应互联网社会的发展提供了可选路径和无限遐想。

从其在比特币的应用情况看，区块链直观讲，就是将加密技术与互联网技术相结合，所形成的一套全新的数据区块（Block）创建、比特币发行分配、网络身份验证，以及挖矿所形成的比特币（价值）确认、比特币交易记录，比特币的链上流动（价值转移），以及加密（加入了区块与交易时间标识等因素）登记和查验核实等在内的互联网协议规则和账本（Ledger）体系。

正因为比特币并不是线下法定货币的替代物，而是非法定货币当局发行和管理的，主要模仿黄金的模式，完全由互联网基础协议和严格的加密技术保护和支持的、全新的、去中心化的网络货币（虚拟货币），由此也形成了一套不同于、也不受制于现实社会法律的新的货币规则和体系，并且可以与法定货币进行买卖或兑换。

比特币自推出以来已超过8年时间，没有出现过资金或用户信息被盗用的记录，其安全性得到验证，而且其资金清算的效率和成本也具有明显的优势。这使得人们对比特币所应用的区块链技术的信心不断增强，而且人们也越来越清晰地认识到，区块链尽管是比特币所首创和应用的一种技术和协议，但区块链并不等同于比特币，其应用也绝不会只局限于比特币。区块链的应用，可以是去中心化的，也可以是中心化的；可以是公有链模式，也可以是私有链模式。因此，在比特币之后，区块链技术也在不断发展创新，并不断探索新的应用领域。

区块链之所以被越来越多的人高度重视，是因为互联网的发展和广泛应用，已经使得越来越多的经济交往和交易活动转到网上进行。网络世界（或线上社会）正在快速扩展、充实和活跃，而网上交易必须解决当事人的身份验证、价值核实、交易记录、查验核实等方面的效率和安全保护问题，需要严格的中介和协议（规则或宪法）。在这方面，传统思维和习惯做法就是顺应线下交易向线上转移的发展轨迹，将现实（线下）社会的通行规则和做法推到线上（网络）社会，但实践中却越来越难以适应网上交易的需求。

比如，当事人身份验证，自然的选择就是以各国法律保护的身份证件的信息为基础，再增加账户或交易密码，以及脸谱、虹膜、指纹等生物识别等，进行线上交易的身份验证。这种方法，首先就使得跨境互联互通的网络世界的公民身份信息受到现实社会行政管辖的制约。同时，非数字化的、多种身份信息的采集和验证会大大增加成本、降低效率。

再者，现实社会中各种经济活动涉及资金清算的，除直接的现金交易外，都需要当事人首先在银行等机构开立账户，并通过开户机构进行资金清算。但由于种种原因，即使一个国家内，也不可能要求所有的公民都在一个开户机构（包括其分支机构）开立账户，跨国之间就更不可能做到。这就使得在不同机构开立账户的当事人的交易，必须通过其开户机构之间的清算才能完成。将这种模式推行到网络世界，更将严重影响交易确认和资金清算的效率和成本。

还有，现实社会中，交易活动的计价和清算必然涉及货币，而货币都是以国家或地区主权保护的法定货币。在互联网跨境互联互通，互联网交易跨境发展的情况下，交易的计价和资金的清算还涉及货币的问题，多种货币的运行，也将大大增加清算的成本和风险。

因此，网络世界和网络交易的发展，亟须与之相适应的身份验证、价值核实、货币计价、交易确认与记录、账户管理与核查等方面的创新。而区块链技术为此提供了非常重要的启迪和实践。

当然，比特币的应用是一种极端的例子，最初始的比特币并不是法定货币可以直接转化出来的，而是要在网络世界通过“挖矿”才能获得的。因此，比特币可以完全撇开线下社会规则，运用区块链技术形成一套全新的游戏规则，并由线上向线下延伸。而现实社会中，无论线上还是线下交易，其主体都是人（包括法人），其财富或价值的管理不应该被完全分割，而必须连接和融合，因此，O2O是必须的。这就要求区块链的应用，不仅要研究和解决网络世界的问题，还要研究和解决网络世界与现实社会的连接与融合问题。这将带来更多的挑战和风险，也需要更多的人、更大的力量、更深入的探讨和创新。也可能未来区块链技术会被更先进更完善的技术所替代，但区块链的历史价值将是不可磨灭的！

为普及区块链的知识，引导区块链的研究，推动区块链的应用，最近我国一批对区块链理论研究和应用实践颇有造诣的专家学者，将其心得和成果精心梳理，编写出版了《区块链：从数字货币到信用社会》一书，非常值得认真阅读。当然，区块链作为一个全新的技术和概念，其研究和探索才刚刚开始，希望《区块链:从数字货币到信用社会》一书能够成为大家学习、研究区块链的“垫脚石”，也希望作者们能不断推出新的成果和作品！

[2] 作者为乐视金融CEO、中国银行原副行长。

序三

区块链——未来全球信用的基础协议

韩锋[3]

在2015年的时候，阿里巴巴研究院和中国社科院金融所举行了一个研讨会，我受邀前往。会议的主旨很宏大，提出要为互联网金融创建一个理论体系！围绕这个主题，诸多中国一流的学者提出了自己的观点。我也深受启发，尤其是随着最近几年来区块链技术的兴起，似乎给这一目标找到了答案。在探讨区块链能给互联网金融带来什么之前，让我们先看看究竟互联网会为金融带来什么。

金融的核心无疑就是“信用”的创建。最原始的商品经济是以物换物。但大家很快发现这样的交易成本很高。如果你把几车皮商品拉去，但是交易没做成，还有可能被土匪抢了，不仅交易成本高，还要面临很高的风险。所以大家考虑，要让市场经济更好地发展，首先要降低交易成本。于是很快就过渡到了利用信用创建交易的方式。信用的创建才是金融的核心。当然，我们传统的信用创建无疑是靠很多的“中心”，譬如央行、商业银行，要有法院、经济警察等。但是传统金融的问题就是成本过高。我本人很喜欢在北京周边骑车，只要骑车超过一百公里，虽然只是到了北京的郊区，但金融生态就已发生了巨大的变化！我就经常找不到ATM（自动取款机）机了，找不到银行网点了。我自己是不太爱带现金的，结果有一两次在北京郊区把我弄得既不能住店，也不能吃饭，甚至无法买水。

打个比方，这就像人的身体，只靠主动脉无法到达全身，一定要有毛细血管，才能让身体的很多地方得到营养。如果人的毛细血管出了问题，那么你这个人就会得各种病，非常严重。所以互联网金融第一步搞得风风火火的，实际上是“支付宝”们，它向前跨的一步就是依靠大数据来创建信用，这是前所未有的。在我创业的时候，我也曾经去银行贷过款。其过程非常烦琐，要调查你的资产情况，恨不得把你的家底全搞清楚，之后才决定是否给你贷款。据说当时银行里所谓的小额贷款是五百万元。为什么这么大的数额？因为成本下不来。所以光靠银行是不行的，不说我去山沟里没ATM，很多中小企业甚至都无法得到贷款服务。结果突然出现了支付宝、余额宝，“信用”是创建在互联网交易的大数据基础上，这就是一大突破！大数据金融基本上是创建互联网金融的第一步。它让信用创建的成本比传统银行吸储放贷方式的成本下降了很多。后来出现了P2P（点对点）、众筹等，都促使信用创建成本下降成为趋势。

那为什么还需要区块链？因为光靠互联网公司大数据产生“信用”是远远不够的，让我们看看传统金融出现的几个问题。

首先，互联网公司的大数据实际形成了数据孤岛。每个互联网公司都会提倡互联网的共享、公开、透明精神。但事实上，他们会将掌握的大数据与他人共享吗？目前，答案是否定的。在当前形势下，大数据必然是每一个公司的绝对内部资源，不可能进行无边界的共享，这就出现了“大数据集中”的问题。

这样一来，互联网发展到现在就出现了一个悖论，走向了初衷的反面。大数据的集中会引起富者越富的马太效应。如果形成数据孤岛，大数据资源集中到少数人手中、全社会无法形成环流，这些宝贵的数据资源只能为少数数据的掌控者所利用，用户个人作为大数据产生者完全没有获得信用资源的主动权，这非常不利于全球市场信用成本的进一步下降。

其次，数据所有权现在是错配的。海量数据是由每一个参与主体产生的，尤其是在腾讯微信这样的软件上。但大数据的所有权属于每一个参与主体吗？参与主体可以管控自己的大数据吗？答案也是否定的。尤其是2016年初发生了一件恶劣的事情——“百度卖吧”事件。在百度上形成一个“吧”产生的数据、资源的所有权应该归属于用户，这其中包括“吧主”也是由参与用户选举产生的。但是，百度却能将产生的大数据效益公开出售！

同样，在微信上我们每天能产生多少数据？我们每天产生的社交、交易数据本应该是完全属于产生者每一个人的。如果按互联网共享、平等、透明的精神，这种大数据产生的是一种“全球性的信用资源”。

所以，新的创新一定是要解决的问题是：大数据既要能够共享，又要能够清晰所有权归属。表面上看，这两点有些矛盾。众所周知，第一代互联网解决了信息的自由传递问题。“信息”本身可以复制、多次传

递并且免费，这都没有问题。但“资产”不可以。在现实中，“资产”在传递过程中所有权唯一，资产的所有权是不能随便复制的。所以，如果按第一代互联网TCP/IP协议做的话，大家似乎无法在互联网上创建所有权和信用制度。因为资产属性一定是唯一的，不能说拷贝就拷贝。如果任何一个所有权可以无限复制，就没有任何人愿意相信，也就没有任何信用可言了。

2008年比特币的诞生让以上两个问题迎刃而解。中本聪认为不能靠某个中心创建信用。因为任何过度中心化的结果都会产生信息不对称，会存在利用中心权力损害参与者的利益、损害市场上其他方利益的情况。所以，比特币白皮书开宗明义地提出：我们要开创一种不需要第三方的、不需要中介的支付系统，即电子货币的支付系统。但这首先要解决资产所有权唯一性的问题，即不能重复支付。否则，这个所谓的电子货币无外乎就是存储的数字，如果还是可以无数次拷贝是没有任何信用价值的。在此之前，很多人也尝试创建电子货币系统。类似“Q币”显然是依靠腾讯公司发行的，一旦腾讯公司垮了，Q币则一文不值。但中本聪宣称要创造的这个P2P电子货币支付系统不相信任何中心、不需要任何第三方！

比特币的解决方案就是我们现在讨论的区块链技术。第一个也是最核心的概念是“时间戳”。“时间戳”本身不是中本聪发明的，早就有国家的“时间戳”中心。比如一个合同，可以盖一个“网络时间戳”，相当于一个证明。即在这个时间点，合同的文本已经形成，当出现纠纷的时候，可以利用这个证明来打官司等。比特币系统的每笔交易，为了防止重复支付，都盖了“时间戳”。因为盖了“时间戳”以后，同一笔资产就不能支付给第二个人了。如果有人重复支付，那么时间会对不上，系统会自动识别为非法交易。唯一的合法交易只能是盖了“时间戳”的那笔，这就成功解决了重复支付的问题。这个办法听起来可以解决重复支付问题，证明了此时此刻财产转移的唯一性，但问题是：谁来盖这个“时间戳”？中本聪显然是市场的信徒，信奉亚当·斯密提出的市场都是由自利的人组成的，要有一定的利益规则。盖“时间戳”的是所谓的“矿工”。矿工每10分钟给全网的每一笔交易盖“时间戳”——记账。他们也是有利益驱动的。矿工的利益是币基所产生的新币的奖励，通过竞争到一段时间内（约10分钟）的唯一合法记账权而获得，谁竞争到了，谁就可以获得一定数量比特币的奖励，同时，全网其他矿工要同步一致它这个记账，然后竞争下一个区块记账权。最初，这个奖励是50个比特币。按照规则设定，每四年减半一次。2013年减半到25个比特币。所谓区块链，就是这样一个又一个区块账簿连接起来形成的单向记账链条。

比特币的区块链是靠消耗计算资源给全网作证，重新创建信用体系。大家经常看到网上的讨论，比如，下一代微信可能是什么，下一代淘宝可能是什么等。在我们看来，下一代最有可能的是一个真正去中心化的系统。每个人在微信上产生的大数据，对每个人自身都有很大价值。如果这些数据用类似Factom（公证通）这样的系统加密后形成一个新的数字水印（哈希）然后保存在比特币的区块链上，每个人自己产生的大数据都不可篡改，私钥掌握在每个人自己手中，也就掌握了自己大数据的所有权。当我们任何人需要向银行贷款时，只要提供自己的公钥和私钥给全球任何一家银行，根据大数据分析就可以得出贷款人的信用情况，这就可以让每个人通过大数据+区块链获得全球信用。

阿里巴巴副总裁高红冰对我说：“传统金融的信用创建在钢筋水泥的大厦上，你看银行是不是都得盖大楼？但未来的信用是创建在区块链的数据上。”所以区块链就是靠全网分布记账，自由公证，创建了一个共识数据库，这就是未来信用的数据大厦。

畅想一下未来，比如说原来你的出生证、房产证、婚姻证等，需要政府备书，好像政府才能承认。但一旦跨国，你就会遇到很多麻烦，包括合同。跨国以后合同可能就不能被承认了，或者无法执行。整个传统的信用执行系统成本非常高。这些成本都摊在了我们每个人的头上。但是，如果全网公证帮你证明，几乎无法作假。否则就像我刚才说的改时间，除非我有本事把每个人的手表都改了。将来大家公证一件事情，比如公证你们的情侣关系，一下子就会成为全网的事实，修改的话几乎是不可能的了，除非到全网的每个矿工那里去改，成本高到无法接受。现在，要想修改的话，我问过比特币的矿工，如果他们的世界想要这样篡改区块链上的数据，成本是十几亿人民币（随着时间还在迅速地增加）。成本一旦高了，大家就都不想作假了，因为付出的代价和获得不成比例。

一个新的时代，未来的信用、真假是靠全网公证某个协议，靠全网每台电脑成为记账人来实现的。这在人类历史上打开了广阔的空间。它解决了什么问题？未来信用由每个消费者自己靠大数据在区块链上产

生，就像北京市金融局霍学文书记所说的，“区块链会成为全球金融的基础架构”，这是未来的信用大厦。

[3] 作者为清华大学博士生，iCenter导师，比特币基金会终身会员，曾任清华大学十五规划重点课题“基于网络(大数据)的创新人才评价和选拔”项目负责人，美国甲骨文教育基金会中国合伙人。

第一章
区块链创世纪[4]

一、先驱篇

（一）中本聪的生日

P2P Foundation是中本聪发布比特币白皮书的网站，注册这个网站必须提供出生日期，中本聪填写的是1975年4月5日。当然，没有人会认为这些信息是真实的，但如果认为这些信息是随便填的，又似乎低估了一位密码学家的自我修养。

4月5日在货币史上是具有重要意义的一天。在1933年的这一天，美国总统富兰克林·罗斯福签署了政府法令6102，该法令规定所有美国公民持有黄金都是非法的。

罗斯福没收美国人的黄金，并以美元交换，然后让美元贬值了40%，强制推高黄金价，目的是让美国的债务贬值，从而对抗大萧条。这些措施造成的后果是美国人的财富被洗劫了40%。

有许多人认为这是美国政府所作所为中最违反宪法的行为之一。这是政府不经过民主程序对民众最直接的盗窃行为之一。

那么，在1975年又发生了什么？在1975年，福特总统签署“黄金合法化”法案，美国人可以再一次合法地拥有黄金。

这两个数字撞在一起实在太蹊跷，无法让人不怀疑这是有意为之。毕竟中本聪没有说他出生于1933年，而是说1975年。因为如果出生年份是1933，这意味着当他发明比特币时已经75岁了，显然不太可能。假如1975年出生，2008年时他33岁，这明显地更让人信服[5]。

如果仔细研究中本聪的创世论文以及比特币代码，一定对他注重细节以及对货币知识的掌握感到惊讶，显然，他的生日数字不是随机组合。没错，这是一个政治隐喻，透露给关心这些细节并能理解的特殊人群，比如那些密码朋克们。

（二）密码朋克

基于密码学技术的比特币，并非加密货币之发轫，早在20世纪80年代，密码朋克就有了加密货币的最初设想。蒂莫西·梅（Timothy May）提出了不可追踪的电子货币——加密信用（Crypto Credits），用于奖励那些致力于保护公民隐私的黑客们。

加密货币的难点在于如何创建分布式共识，也就是莱斯利·兰伯特（Leslie Lamport）等人1982年提出的拜占庭将军问题（Byzantine Generals Problem）。所谓拜占庭将军问题是指，把战争中互不信任的各城邦军队如何达成共识并决定是否出兵的决策过程，延伸至计算领域，试图创建具有容错性的分布式系统，即使部分节点失效仍可确保系统正常运行，也可让多个基于零信任基础的节点达成共识，并确保信息传递的一致性。

1990年，大卫·乔姆（David Chaum）提出注重隐私安全的密码学网络支付系统，具有不可追踪的特性，就是后来的电子货币Ecash。不过Ecash并非去中心化系统，后来大多数电子加密货币都继承了Ecash重视隐私安全的特性，以盲签名技术（Chaumian blinding）为基础，但都没有流行起来，因为它们都依赖于一个中心化的中介机构。

1993年，埃里克·休斯（Eric Hughes）和其他几个人创建了一个“密码朋克邮件名单”的加密电子邮件系统，简称“密码朋克”，对抗受到政府监控的互联网电子邮件。埃里克·休斯在《密码朋克宣言》里阐述了密码朋克的使命与目标。

> “密码朋克致力于创建匿名系统……电子时代，隐私是开放的社会不可或缺的……我们不能期望政府、企业或其他大型的匿名组织保障我们的隐私……如果

> 期望拥有隐私，那么我们必须亲自捍卫之。我们使用密码学、匿名邮件转发系统、数字签名，以及电子货币保障我们的隐私。”

密码朋克在20世纪90年代最为活跃，包括电脑黑客、密码学家和追求隐私的狂热者，他们极力主张用密码技术保护个人隐私不受其他人或者政府的侵犯，但在当时，密码技术并没有在日常生活中得到广泛应用，而是被政府垄断，主要用于情报和保密。

密码朋克们意识到密码学对社会经济的深远影响，蒂莫西·梅说：“正如印刷技术改变了中世纪的行会及社会权力结构，密码技术方法也将从根本上改变机构及政府干预经济交易的方式。”

比特币的加密理论基础来源于以下几项密码学的技术创新：1976年威特菲尔德·迪菲（Whitfield Diffie）与马蒂·赫尔曼（Marty Hellman）发明的非对称加密算法，1977年罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adelman）率先发明的第一个具备商业实用性的非对称RSA加密算法[6]，以及1985年由尼尔·科布利茨（Neal Koblit）和维科特·米勒（Victor Miller）首先提出的椭圆曲线加密算法（ECC）。这些加密算法奠定了现在非对称加密理论的基础，被广泛应用于网络通信领域。

但是，当时这些加密技术发明均在NSA（美国国家安全局）严密监视的视野之内。NSA最初认为它们对国家安全构成威胁，并将其视为军用技术。直到20世纪90年代末，NSA才放弃对这些技术的控制，RSA算法等非对称加密技术最终得以走进公众领域。

有趣的是，中本聪并不信任NSA公布的加密技术。2013年9月，斯诺登爆料NSA采用秘密方法控制加密国际标准，比特币采用的椭圆曲线函数可能留有后门，NSA能以不为人知的方法弱化这条曲线。所幸的是，中本聪使用的不是NSA的标准，而是另一条鲜为人知的曲线。全世界只有极少数程序躲过了这一漏洞，比特币便是其中之一。

1998年，另一名密码朋克戴伟（Dai Wei）提出了匿名的、分布式的电子加密货币系统——B-money。分布式思想是比特币的重要灵感来源，在比特币的官网上，B-money被认为是比特币的精神先导。

B-money的设计在很多关键的技术特质上与比特币非常相似，但是不能否认的是，B-money有些不切实际，其最大的现实困难在于货币的创造环节。

在B-money系统中，要求所有的账户持有者共同决定计算量的成本并就此达成一致意见。但计算技术发展日新月异，而且有时并不公开，计算量的成本这类信息并不准确、及时，也难以获得，因而B-money很难成为现实。

2005年，尼克·萨博（Nick Szabo）提出比特金（Bitgold）的设想：用户通过竞争解决数学难题，再将解答的结果用加密算法串联在一起公开发布，构建出一个产权认证系统。该系统已经非常类似于比特币的理念，且发布日期与比特币非常接近，所以，萨博也被视作中本聪的潜在候选人之一。除此之外，萨博还发表了许多关于《合同法》在网络中安全实现的理论文章，这些思想被视为区块链智能合约的起源。

但萨博终究不是中本聪，他擅长于理论研究而不是编程实现，他一直寻找能将比特金变为现实的开发者，但没有人响应。

从乔姆的Ecash，到戴伟的B-money，再到萨博的比特金……几代密码朋克都怀着对自由货币的向往，像堂吉诃德一般偏执而骄傲，试图征服加密货币的风车，最终都功亏一篑，这些理论探索并未真正进入应用领域，长期不为公众所知，但他们的研究成果加速了比特币面世的进程。

（三）加密货币的乔布斯

非对称加密技术的发明以及创立Napster[7]的肖恩·范宁（Shawn Fanning）与肖恩·帕克（Shawn Parker）点对点网络技术的开发，使比特币的出现成为可能。通过这两项技术，可以创建分布式交易账簿，并以呼叫问答机制向全网广播，网络节点不停地检查接收的数据，避免数据被篡改。

数字货币的诞生历程就像是一次扣人心弦的橄榄球进攻，在乔姆、戴伟、萨博等“明星球员”的冲刺下，每一次冲阵都前进了一些，但离“达阵”总还差一点距离。

最后的难点就是“双重支付”问题。“双重支付”阴云在数字货币诞生伊始，就始终盘桓不去。其实解决方法是现成的，就是亚当·拜克（Adam Back）在1997年发明的哈希现金（Hash Cash）算法机制。但起初，该设计是用于限制垃圾邮件发送与拒绝服务攻击。这就好比另一个球场正进行着田径接力赛，并没有引起橄榄球赛场的注意。2004年，哈尔·芬尼（Hal Finney）接过拜克的接力棒，将哈希现金算法改进为“可复用的工作量验证（Reusable Proofs of Work）”。他的研究又是基于达利亚·马凯（Dahlia Malkhi）与迈克尔·瑞特（Michael Reiter）的学术成果：拜占庭容错机制（Byzantine Quorum Systems）。

所有的技术都已成熟，终于由中本聪在2008年完成“达阵”。他将RPOW（可复用工作量验证）引入加密货币，就像博尔特跑入了橄榄球赛场一样，一下发挥出巨大的威力，比特币诞生了。中本聪阐述了RPOW机制如何用于解决拜占庭将军问题，RPOW消除了中枢“时间戳”服务器的需求，杜绝了那些不怀好意的人通过攻击中央服务器进行比特币无限重复消费的问题。

非对称加密、点对点技术、哈希现金这三项关键技术没有一项是中本聪发明的，但最后摘取桂冠的却是他。这与其说是运气，不如说是因为中本聪恰好具备发明比特币的全部素养：既是“橄榄球员”，又是“田径高手”，更关键的是他还是编程大师，能够把自己的想法付诸行动。中本聪就像是加密货币界的乔布斯，纵横于不同领域，采撷各家之长为我所用。

正如戴伟事后评价说：“要想开发出比特币，必须：①对货币有非常深入的思考；②要了解密码学；③认为比特币这样的系统从理论上是可行的；④要有足够的动力将这个理念开发成实际产品；⑤编程能力出色，能保证产品安全；⑥有足够的社交技巧，才能围绕这个产品创建一个成功的社区。密码学圈子能符合前三个条件的人就已是凤毛麟角。”

（四）创世区块

中本聪第一次出现是在2008年11月1日。那一天，秘密讨论群“密码学邮件组”里出现了一个新帖子：“我正在开发一种新的电子货币系统，采用完全点对点的形式，而且无须受信第三方的介入。”该帖的署名就是塞托西·中本聪（Satoshi Nakamoto）。

这样的电子货币系统是密码朋克们数十年来的梦想，有许多人进行过尝试，但都失败了。当时最积极的反应也只是持怀疑态度，因为密码组成员已经看过太多低水平的新手想出来的宏伟计划，他们的本能反应就是怀疑。当时有不少人表示，这样的系统是不可能实现的，连大卫·乔姆这样的密码学天才都失败了，更何况一个无名小辈呢。

中本聪细致入微地回答了所有疑问，最终在白皮书中提出了一个可行的方案。白皮书遵从学术习惯采用“我们”作为第一人称，行文也是标准的论文格式。

> “本文提出了一种完全通过点对点技术实现的电子现金系统。它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。”

中本聪选择在2008年全球金融危机的时候将比特币公布于世，在介绍他的创新时说道：“传统货币最根本的问题在于信任。中央银行必须让人信任它不会让货币贬值，但历史上这种可信度从来都不存在。银行必须让人信任它能管理好钱财，并让这些财富以电子货币形式流通，但银行却用货币制造信贷泡沫，使私人财富缩水。”

与密码朋克的文章相比，比特币创世论文的语言显得格外冷静和去政治化，文中没有出现政府或主权的字眼，仅将比特币描述成一个区别于传统金融的支付系统。

两个月之后，也就是2009年1月3日，中本聪发布了开源的第一版比特币客户端，宣告了比特币的诞生。他同时通过“挖矿”得到了50枚比特币，产生第一批比特币的区块就叫作“创始区块”（Genesis block）。

在全球金融危机时期，中本聪将他的怀疑和愤怒集中在了银行机构上，但与用生日密码挖苦美国政府一样，他不动声色地幽默化了英国财政大臣达林一把，在创世区块里写道："当时正是英国财政大臣第二次出手疏解银行危机之时。"

财政大臣左支右绌的窘态就这样被永久记录在区块链上。"第二次"在此与其说是一个量词，不如说是一个形容词，很形象。

9天以后，中本聪向密码学家哈尔·芬尼转账了一笔比特币。那笔转账在当时还不值一文，却在加密货币篇章里留下浓墨重彩的一笔。这是人类历史上第一次摆脱受信第三方金融机构而完成的点对点交易。

与许多患有隐私癖的黑客一样，中本聪也是独行侠。他几乎没有合作伙伴，如果非要说一个，哈尔·芬尼勉强算半个。芬尼是参与过PGP加密技术研发的一位顶级开发者，也是密码朋克的重要成员。当中本聪在加密邮件列表中宣布比特币的想法时，迎来的更多的是冷嘲热讽，但只有芬尼热情支持。芬尼很早就对加密货币计划感兴趣，早在2004年，他就推出了自己设计的加密货币，在其中采用了可重复使用的工作量证明机制，所以他明白比特币的价值。当中本聪公布第一个版本的软件时，芬尼马上下载并测试。

多年后，芬尼在社区回忆这段经历说："我想我是除了中本聪以外第一个运行比特币的。我开采了大约70个块，而且我还是第一个比特币交易的接受人，中本聪测试时转给了我10个币。在接下来的几天里，我和中本聪通过邮件谈了很多，主要是我报告一些故障然后他把它们搞定。"

社区网友亲切地把芬尼称作"中本聪的沃森"，因为当电话被发明时，第一个电话就是贝尔打给他的助手沃森："沃森，快过来，我想见你。"2014年8月，在与渐冻人症搏斗了五年之后，哈尔·芬尼在亚利桑那州去世。向"沃森"致敬！

（五）后起之秀

比特币发布后取得了空前的成功，媒体与公众纷纷把中本聪与20世纪90年代的那些密码学天才们相提并论。中本聪对此不以为然。

尽管维基解密创始人朱利安·阿桑奇（Julian Assange）[8]宣称比特币是从密码朋克中来的，中本聪却对密码朋克或者密码无政府主义只字不提。

2010年，维基解密宣布接受用比特币的捐款时，社区一片欢呼，中本聪却出人意料地提出了反对意见：

> "不，请不要揠苗助长。比特币这个项目需要平静地成长，这样软件才能够逐渐强化。我请求维基解密现在不要使用比特币。比特币还是一个非常小的测试项目，还处在婴儿期。在这个阶段，你们所带来的关注将摧毁我们。"

中本聪对20世纪90年代的失败者记忆犹新。他指出Beenz（虚拟货币）、Flooz、Ecash（电子货币）等数字货币先驱失败的根本原因就在于其中心化的架构。因为一旦为数字货币信用背书的公司倒闭，或保管总账的中央服务器被黑客攻破，该数字货币就会面临信用破产和内部崩溃的风险。

2013年，一名叫特拉梅尔的安全研究人员公布了他与中本聪的加密邮件往来。在邮件中，中本聪写道：

> '我觉得现在更多的人对90年代感兴趣，但是经过数十年，我们已经看到了基于'信任第三方'系统的失败（例如Ecash）。我希望人们能够有一种区分，即知道：我们是在尝试首次创建一个以'非信第三方'为基础的系统。"

然而，要向公众解释这两者的区分很难，有一次他在论坛抱怨："向普通读者描述比特币真是'bloody hard'（该死地困难）。"[9]

中本聪对加密货币前辈的态度难说有几分尊重，但世道轮回，没过几年他也面临后起之秀的挑战。

对比特币的共识机制来说，挖矿是必须的。正如白皮书中开门见山指出的："想要在点对点（P2P）基础

上布置一个分布式的‘时间戳’服务器，我们必须使用一种与亚当·拜克的哈希现金相似的工作证明系统。”

但很多人都认为，比特币网络消耗的庞大计算力是一场能源灾难。素数币创始人萨尼·肯（Sunny King）试图将算力应用于蛋白质折叠、寻找素数这样的科学工程。他自信地写道：“加密货币目前已分道扬镳为两条道路：一种是能源密集型，另一种是环保节能型。我相信，在未来较长一段时间（5年以上），环保节能型货币将因其成本优势而挑战能源密集型货币。素数币第一次引入非哈希现金的工作量证明机制，使算力不仅用来制造区块链，还提供额外的潜在科学价值。”

除此之外，Sunny King还发明了权益证明（PoS）。与要求矿工证明执行一定量的计算工作不同，权益证明要求用户提供证明一定数量加密货币的所有权即可。

还有一些人对比特币处理交易的效率很不满意。比特股创始人拜特·马斯特（Byte Master）在社区发帖：“互联网带宽、CPU（中央处理器）、硬盘空间等都是非常宝贵的资源，指望用户用个人时间和挖矿的方式获得财富，这对于创新而言将是不利的。此外，比特币10分钟的确认时间对于验证付款而言实在是太长了，它应该像如今刷信用卡那般迅速。”

中本聪是这样解释的：将来用户只需运行轻节点，只交易，不挖矿，处理区块的节点将是矿场部署的大型服务器。最后，他无奈地说：“如果你没有理解我的意思，我没时间说服你。”在心底，恐怕他又吐槽一遍“bloody hard”吧。

另一位技术天才维塔莱克（Vitalik）从未在社区与中本聪对过话，毕竟在2008年的时候，他才13岁。Vitalik与中本聪的交流更多的是通过代码。他指出，中本聪作为一个老派C++程序员，编程水平并不高明，但运气不错：“虽然中本聪在2008年为比特币做出的绝大多数决策我们仍坚持着，但他的选择绝对不是完美的，幸运的是他正确的次数经常比错误要多。事实上有几个实例，因为中本聪的选择我们获得了更好的结果。”

他说的是中本聪在比特币的代码中埋下的三个“彩蛋”，后来被证明都是对的。

第一个是比特币使用公钥的哈希作为地址，带来了不必要的复杂度和浪费。但事实上，这是深思远虑的未雨绸缪，因为可以让比特币完全免受量子计算机的威胁。第二个是比特币总量2100万的限制，或者说是2的50.899次方。这是一台计算机里面能以标准整数形式存放的最大整数，超过那个值的话，数值将像里程表那样归零。第三个是选择了正确的椭圆曲线，成功绕开了NSA居心叵测的陷阱。

中本聪在代码里处处留情，可惜能读懂他的人不多。很难说Vitalik能否算是一个知音，因为后者并不认为中本聪天才地设计了这一切，他说：“这些设计带来更好结果的原因可能连中本聪自己都没想到过。”他认为中本聪是蒙对的。2014年，他发起以太坊项目，试图以一套图灵完备的脚本语言，解决比特币扩展性不足的问题，提供不同智能合约，让用户搭建各种应用。有意思的是，以太坊以加密货币先驱的名字作为货币单位，戴伟、萨博、芬尼均名列其中，唯独没有中本聪。

2010年12月12日，中本聪在比特币论坛发布了他最后一个帖子，其后，他在网络上的公开活动频率也逐渐降低。直到2011年4月，他发布了最后一项公开声明，宣称自己“已经开始专注于其他事情”。他依然跟几个关键人物保持着联系，比如说比特币的首席开发者加文·安德森，并提出了一些建议。但到这一年年末，安德森公开表示，中本聪回复他电子邮件的次数越来越少，然后慢慢地就再也没了消息。

二、货币篇

（一）石币之岛

密克罗尼西亚是太平洋的三大岛群之一，其中最西边的雅浦岛上曾住着一群非常古怪的土著居民。1903年，美国的人类学家威廉·亨利·弗内斯（William Henry Furness）在雅浦岛住过几个月，并把他在当地所见的风俗记录成书，书名叫《石币之岛》，因为当地的货币体系令他印象深刻。

雅浦岛上没有金属资源，于是石器在他们的文化中扮演着重要的角色。但即使是石灰岩，也需在离雅浦岛400英里远的帕劳岛上才能找到。雅浦岛部落里的探险家们开采这些石灰岩，打制成内部中空外部呈环形的石轮，然后用木筏运回雅浦岛作为货币使用。这些石轮小的直径30多厘米，大的直径有3米多。为了便于运输，有时会往中间插一根粗壮的木柱。

雅浦石币有个很有趣的特点。交易双方在决定了使用多大的石币付费后，如果那个石头太大了，不方便运输，那么卖家只要在买家的石头上做个标记就可以了，这样就算是付费了。那个标记就说明这个石头已经属于卖家了，而石头仍然躺在买家屋里。

不只如此，还有更神奇的事情。岛上有一户大财主，所有人都承认他们家是首富，但奇怪的是，没有人见过首富家里的石币，连他的家人都没见过。他们家拥有的财产是一个巨大的石币，大小只有祖辈才知道，因为这个石币一直沉睡在海底。原来许多年以前，这户人家的祖辈和其他人外出探险，寻找和开采石灰岩，就像美国西部的淘金客一样。他们的祖辈运气不错，碰到了这个庞然大物，便将其制成石币，然后用木筏拉回家。但是归途中遭遇了强烈的暴风雨，为了逃命，探险队只好砍掉拉筏的绳子，于是那块巨大的石币沉入了大海，永远也找不回来了。回村后，探险队的成员都替他作证，那块石币尺寸巨大并且质量上乘。虽然已掉落大海，但大伙都见证了这块石头的去处，所以不会影响它的价值。它的主人仍然可以用它买东西，就跟把石币运回家存放起来的效果一样。

如果这个还不足以让你惊讶，请看下面的故事。雅浦岛岛民都不穿鞋，并且也没有发明轮子，自然也就没有车道。岛上只有一些适合原住居民裸足行走的珊瑚礁道路，但是西方殖民者却要求他们修筑能行驶汽车的公路。德国在1898年从西班牙手中买下了这座岛，要求几个部落的酋长组织修路。修路对土著居民而言完全没有意义，德国人的马克在土著居民看来跟废纸差不多，所以命令下达了几遍都无人搭理。想想也是，一伙拿枪的人登上一座自己从未踏足的岛屿便声称拥有岛屿的所有权，还强迫当地居民为自己修路，这不是流氓是什么。德国政府研究了雅浦岛的文化习俗后，突然开窍了，下令对几个违抗命令的部落征税。他们派人到这些部落的每家每户，并往他们最珍贵的石币上涂上黑十字标记，声称这些石币已经归德国政府所有了。这个解决方案既简单又“文明”——文明用在这儿真够讽刺的——但的确非常奏效，可谓是“取之于无形，使人不怒”。所有人都觉得政府抢了自己的钱，为了使钱不被抢走，只得乖乖去替政府修路。最后路修好了，德国政府就把那些标记抹去，于是岛民又幸福地过上自己富有的生活。

读到这里读者朋友也许会发出这样的感慨：天底下竟存在这样荒唐的货币！但事实上，被视为现代经济学皇冠上最璀璨宝石的信用货币，其运行原理与雅浦岛石币并无不同。

（二）法兰西银行的黄金

弗里德曼在《货币的祸害》一书里举了一个例子：1932年，法兰西银行害怕美国不再盯住金本位，不再按一盎司黄金兑换20.67美元的传统价格兑换黄金。于是，法兰西银行要求纽约联邦储备银行将它存在美国的大部分美元资产转换成黄金。为了降低将黄金装船海运的成本，法兰西银行要求联邦储备银行把黄金存到法兰西银行的会计账簿上。

于是财经报纸用头条报道了这条关于“黄金的损失”以及对美国金融体系的威胁等诸如此类的消息。美国的黄金储备开始减少，法国的黄金储备开始增加。市场认为美元走软，法郎走强。这种因法国向美国兑换黄金而造成的所谓黄金流失，甚至引发了1933年的银行业恐慌。

而事实上，黄金并没有流到法国，仍然在美联储的地下金库里，因为这只是一次会计操作而已。当时的实际情形是美国联邦储备银行在地下金库的抽屉上作了一些标记，表示这些抽屉中的金块属于法国了。

看起来雅浦岛的石币像是远古的实物货币，如法国人的兽皮，蒙古人的砖茶，印度原始居民的杏仁，中国夏代的海贝……但是，雅浦岛居民的交易并不真正需要挪动或分割那些石币，他们只需要更改石币上的标记，甚至连标记也不需要。如果大伙脑海里有关于某一石币的共同记忆，那么大伙也都承认这笔财富的存在。

对，货币只是一种记账方式。不仅雅浦岛居民这样认为，美国联邦储备银行也这样认为，比特币等区块链货币也是这样认为。当文克莱沃斯兄弟宣称他们拥有100000枚比特币，不是说在某银行的保险箱里，真的有100000枚比特币整整齐齐码在那儿，而是说比特币全网节点都承认有这些一笔比特币，且归属于文克莱沃斯兄弟的比特币地址。

（三）货币的本质

让我们回到货币的本质。假想我们处在一个没有货币的世界，比如同样也是在一个遗世独立的小岛上，与雅浦岛不同，这个小岛还没有诞生货币。岛上只有我和你，现在我们需要进行一笔交易。我想要你手里的鱼，你想要我手里的浆果。那么很简单，我们直接互相交换就可以了。但是如果我现在手里没有浆果，我的浆果得在秋天才能收获，可是我现在又很需要你手里的鱼。那么我们该怎么交易呢？好吧，鉴于岛上只有我们两个人，你决定相信我，我给你发出一个IOU（I owe you），即借据，约定到秋天浆果收获的时候我支付给你，现在我就可以获得我所想要的鱼。我们引入资产负债表的概念，让这个故事更一目了然（表1-1）。

表1-1 基于直接互换的资产负债表

在资产负债表中，我的资产由于获得鱼而增加，同时负债也增加，即对你的债务凭证。而你的资产端则是将交易给我的商品转换成了对我的债务追偿权。

现在我们来个稍微复杂的例子。假设你我素昧平生，彼此都不信任，那这个时候我们该如何进行交易？假设我们都信任一个第三方，比如银行，银行也乐意充当我们的桥梁，那么交易见表1-2。

表1-2 基于第三方的资产负债表

我把自己的IOU转换成向你所认可接受的第三方发出的IOU，在这里由银行发出的IOU即银行券（bank note）。这样如资产负债表所示，我在资产端获得所需商品，负债端为对银行的IOU；而银行的资产端则为我发出的IOU，在负债端银行以我发出的IOU转换为对你发出的银行券（钱）。你的资产就由商品转换为银行券。

所以在现代社会，货币就是一种特殊的IOU，无论把货币当作是贷款还是债务，货币的本质都是一种记账方式。

当交易的群体不只是两个人之间，而是扩大到社会中的每个成员，当我们进行这种时间上不匹配的交易时，我们每个人都发出自己的IOU，那么这个系统就会变得极为复杂（图1-1）。因为没有都认可的第三方时，我们每个人的交易都要取决于是否相信其他人，这将使我们在交易中寸步难行。于是我们不得不依赖于银行这种所谓“可信第三方”，可问题并没有解决，而是转化为另一个问题：银行真的值得信任吗？

图1-1 无“可信第三方”的交换

（四）邓巴数限制

如果雅浦岛首富登上“非诚勿扰”，骄傲地宣称自己在太平洋底拥有一块非常值钱的石头，恐怕会被女嘉宾当成疯子羞辱。这种原始的货币制度只适合自然状态下的小规模经济，也就是费孝通在《江村经济》一书所说的熟人社会。雅浦岛石币无法突破邓巴数限制。人类学家罗宾·邓巴（Robin Dunbar）发现每个人与之维持持久关系的熟人，数量通常只有150个左右，这一数量限制就称作邓巴数。狩猎采集社会的典型组织单位“游团”的规模一般不足百人，比如非洲西南部卡拉哈里沙漠的桑人，每个游团20~60人，邻近农耕区的游团100~150人；从事游耕农业的半定居社会，规模也只是略大，比如缅甸克钦邦山区的游耕群落，最大的也只有100多人。

雅浦岛之所以能孕育出如此神奇的货币现象，乃是因其处于自然经济状态，小岛居民人口不多，交易不普遍，货币的周转速度也非常慢。当地居民有的也许终其一生，也只有寥寥几次交易行为。幸亏雅浦岛上没有淘宝，没有电子商务，不然当地居民的脑子可能会“内存不足”。这也正是雅浦岛石币仅存于与世隔绝的大洋孤岛，而不见于人类主流社会的原因。

从地理上，没有比雅浦岛石币更孤独的了，它原产于西太平洋上的帕劳。但在理念上，它并不孤独，可以说它与比特币思想异曲同工。石币与比特币都具有稀缺性，前者是大自然的石灰岩矿藏分布，后者是基于数学算法；两者同样需要付出昂贵的劳力（计算力）成本才能获取，前者是冒险家的航海运输，后者是矿工的挖矿；两者交易总账均采用分布式存储，前者是大脑记忆，后者是计算机（表1-3）。幸亏有了计算机，人们终于不再需要用石头标记或集体记忆来记录交易，计算机网络可以帮助我们实现这一切。交易行为也同样打破了熟人社会的限制，在比特币交易过程中，交易双方不必彼此熟识或信任，也无须引入可信第三方，就能随时随地自由交易，也就是说，邓巴数被突破了。

表1-3 法币、石币、比特币特性对比

（五）中心化缺陷

如果雅浦岛首富为富不仁，想要私下使用这笔巨款，比如偷偷跟自己的情人说我那块大石头送给你了，那么这次交易是无效的，因为交易没有广播，并没有其他岛民在旁边作证。但如果首富临死前，当着全岛人民的面说，这块大石头就作为遗产给我的大儿子了，那么这笔交易就是有效的，因为其他岛民都做了见证，并集体更新了头脑里的“账簿”。雅浦岛石币虽已具备分布式货币的雏形，但毕竟人肉信息传递网络是脆弱的，交易在口口相传的途径中以及集体记忆中极易出现差错。

比特币全网的节点每时每刻都在向网络广播交易，每笔交易经10~60秒就能广播至全球所有节点，速度取决于节点的网络连接状况。这些广播出来的交易在经过矿工的验证后，打包到数据块中，串联起来形成环环相扣的区块链，这些交易一经六次确认便几无篡改的可能性。要修改某个区块上的数据，得从这个区块开始重新计算之后的所有区块，考虑到比特币全网1300万亿次哈希运算的算力，地球上在比特币网络之外已不存在足以逆转比特币交易的计算能力。

雅浦岛的集体记忆式账簿虽然表面上是分散的，但仍然存在一个权威的第三方，可以决定石币的归属。然而在去中心化的区块链中，并无一个高高在上的殖民政府有权宣布没收你的比特币。或许从载体来说，石币是真实存在的实体，比特币只是虚无缥缈的数字，但从实用性来说，石币只是发人深省的寓言，比特币才是实实在在的财富。

数万年以来，雅浦岛岛民将他们在遥远的岛屿上开采出来，经过打制并运回自己居住岛屿的石头，充作交换的载体，他们一直这样独特地理解着金钱与财富；数千年以来，文明社会则把金块从地底深处开采出来，花大力气进行冶炼，经过长距离的转运，再次埋进精心设计的地下金库，金块的一举一动都可能引发金融市场的离奇波动；最近几年，矿工们满世界寻找着便宜的电力，大规模部署先进的ASIC芯片，挖掘一种叫比特币的玩意，据说那是一串叫作Base58编码[10]的毫无意义的字符，居然能在全球100多家交易市场卖数百美元一个。听完上面这个故事，比特币是不是也变得不那么令人费解了呢？

三、信用篇

（一）库拉圈

社会学家马林诺夫斯基（Malinowski）考察完西太平洋上的特罗布里恩德群岛后，对古典经济学中的一个假设很生气。经济学家过去一直把人类视作“理性经济人”，假设他们在自由和竞争性的市场里同他人进行交易或交换时，总是寻求物质利益或效用的最大化。但特罗布里恩德群岛上的居民却不是这样。在他们的交易行为中，利益最大化似乎并不是他们考虑的首要前提。

在这些洋岛部落间存在着一种被称为库拉圈（Kula Ring）的封闭交换关系圈，当地居民生活的各方面都

与库拉有着紧密的联系。库拉的核心是白色贝壳雕琢的臂镯和红色贝壳打造的项圈的交换，这种交易具有方向性，人们只能逆时针方向交换臂镯，顺时针方向交换项圈（图1-2）。

图1-2 库拉圈交换

库拉贸易圈大致覆盖了整个特罗布里恩德群岛。岛上的男人长途航行，横穿公海，按顺时针方向输运项圈；另一些人则按逆时针方向输运臂镯。一个人根据地位的不同，可能有一个到数十个的库拉伙伴。库拉伙伴是具有库拉关系的不同部落的土著。这是一种相对稳定的关系，关系一旦创建就基本不会被破坏。一旦进行库拉交易，则一直进行库拉交易，交易伙伴越多，他的部落地位越高。

当一个人从南方的库拉伙伴处得到臂镯，他会再把臂镯交换给处于北方的库拉伙伴。相反，当他从北方的库拉伙伴处得到项圈，会再次把项圈交换给南方的库拉伙伴，从而形成按相反方向流动的两种库拉圈：臂镯以逆时针的方向流动，而相应地，项圈以顺时针的方向流动。处在库拉圈不同地方的土著基本按照这样的方式进行库拉。

马林诺夫斯基发现，库拉交易并不是等价交易，也不同时发生，而更像是一种礼物馈赠。一个人将臂镯交换给处于下游的库拉伙伴，上游的库拉伙伴一段时间后回赠项圈，臂镯和项圈的价值并不相等。如果臂镯的价值高，且人都是自私的话，那么他不应该将臂镯交换出去。但事实上，群岛上的每个库拉交易者都非常乐意将臂镯交换出去，而不是以占有为目的。正如马林诺夫斯基指出的：

> “在特罗布里恩德岛民的库拉交换形式中甚至没有一丝要从中获利的迹象，没有任何理由用纯功利主义的和经济的观点看待他们，因为他们没有通过交换而相互利用”。

（二）理性经济人

看到这里，读者朋友可能会觉得这群可爱的岛民都是乐施好善、淡泊名利的天使，但你要是了解他们种红薯的奇怪嗜好就不会这样认为了。特罗布里恩德人喜欢种红薯但他们并不吃红薯，因为岛上遍布野生的热带奇珍异果，既好吃又管饱，在这儿，农业更像是一种娱乐活动。他们种红薯的唯一目的就是堆在院子里炫耀，攀比谁的红薯堆大，然后储藏起来让它们烂掉。看来特罗布里恩德人同文明世界里的“土豪”一样，都喜欢炫耀自己的财富，以种红薯这样不算浪漫的方式诠释着浪费。但在库拉交易中，他们却并不以拥有臂镯和项圈多为傲，相反，他们以频繁交易为荣。这种交易要经历航海的千辛万苦，没有带来丝毫财富上的回报，这似乎很矛盾。

按照经典经济学中“理性经济人”的概念，小岛原住民的一切行为都是出于自利的理性考虑，他们过着一种“算计的、冷酷的、自我中心主义的、斤斤计较于效用的生活”。马林诺夫斯基严厉地批评了这些观点。他指出，“库拉交易绝非纯粹的商业性交易，它不是创建在对实际效用和利润得失的简单计算上”。[11]

对库拉交易行为的合理性解释很多，一种解释认为这就是礼物馈赠，因为库拉交易中隐含着一种互惠逻辑：赠予礼仪性的礼物以后，不论时间长短，总要报以差不多等值的答礼。结构主义大师列维·施特劳斯的舅舅莫斯还根据这个社会学案例写了本著名的《礼物》。另一种解释认为这是宗教仪式，因为某些库拉交易还伴随着精致的巫术仪式和公共仪礼。

但是，以上两种解释都无法回答以下几个问题：①库拉交易为何要规定方向？②为何交易对象越多，交易者的地位越高？③为何交易次数越多，交易者的地位越高？

（三）等价交易

当今电子支付是如此快捷高效，以至于人们会有这样的疑惑：既然PayPal（贝宝）、支付宝已经如此方便，我们还需要基于区块链的数字货币支付吗？

答案是肯定的。在一次支付宝处理的交易中，一个人的支出等于另一个人的收入，这是等价交易。问题

在于，如果支出与收入是同一个人的两个账户，会发生什么？由于对支付宝而言，每一笔交易的边际成本都近乎于零，所以，如果一个人同时拥有两个账户，他在两个账户里反复进行转账交易，就会以非常低的成本制造出无数被支付宝视作洪水勐兽的刷信用行为。

淘宝网非常明智地给交易引入了评价，但是无论采用多么高明的机器算法与人工干预，都无法阻止刷客与差评师这两种职业的存在。前者假扮成买家，通过虚假交易，对卖家的商品刷好评以赚取卖家支付的佣金；后者给网上卖家恶意差评，以勒索卖家提供相应的“赔偿”以获利。

淘宝网通过非常复杂的手段遏制刷信用行为：一方面使用机器算法对店铺进行排查，将出现异常情况（如交易过于频繁）的店铺进行上报；另一方面设有2000多人的团队，对涉嫌刷信用和好评的店铺进行清查，但是收效甚微。这不仅是淘宝网的难题，也是所有电子商务平台的阿喀琉斯之踵。只因它们对交易行为的处理都是一样的，即等价交易。

等价交易的观念伴随着可切割熔铸的金属货币的使用而被人们广泛接受，并随着时间的推移而根深蒂固。公元前7世纪吕底亚人使用条状的金属或者扁豆状的金属块进行支付，可以精确地衡量商品的价值。王国的统治者克里萨斯国王因发达的铸币业而富有得令人难以置信，并因此就有了“像克里萨斯一样富有”的说法。

互联网电子支付对交易的处理与吕底亚人并无不同，只不过，PayPal、支付宝不再使用粒度不同的金属，而是使用服务器里妥善存储的数据。等价交易无须精确称量，而只需进行一次数据库操作。用户用电子支付的A账户给B账户转账金额为m，反过来，再从B账户转账金额m到A账户，电子支付数据库里A账户与B账户的数值又恢复到起始，如此进行无数遍，便是典型的刷信用行为。库拉圈交易也是一次循环（库拉的含义就是循环），不同的是库拉的交易有方向性，而不能作对换交易。

试想在特罗布里恩德群岛的库拉圈贸易中，若是一个人从南方的库拉伙伴处得到臂镯，不再把臂镯交换给北方的库拉伙伴（逆时针），也不把自己的项圈回赠给南方的库拉伙伴（顺时针），而是再次把臂镯还给这位南方的库拉伙伴，将意味着什么？没错，这是一次典型的刷信用式的死循环，臂镯将永远在这两位库拉伙伴中循环，而成为两人永久占有的私藏。两人在部落中也将“刷出”非常显赫的地位。显然，如果大家都这么投机取巧，那么所有的臂镯与项圈都将退出流转，变成藏而不露的私有财产，库拉贸易圈也将不复存在，而这正是库拉贸易要规定交易的方向的缘故。交易一旦启动，库拉就会像接力游戏一样，一直按顺时针或逆时针方向流转下去。

库拉圈带给我们的启示是：如果规定交易的方向，就可以避免刷信用的行为。然而，这在真实经济中是不现实的，我们无法规定在电子商务中只允许与固定的人群交易，人们也的确有与自己交易的自由。

（四）将币天销毁引入信用评价

币天（CoinDays）销毁是区块链的一个非常重要的概念。顾名思义，币天销毁等于每笔交易的金额（币）乘以这笔交易的币在账上留存的时间（天），比如你花了一笔100天以前收到的10比特币，这笔交易的币天销毁就是1000币天。

起初，区块链研究者并没有注意到币天销毁的意义所在，因为它不像时间戳、难度、随机数等字段一样，在区块链中有明确的作用。只有少数对币价敏感的人群关注这个指标，他们认为区块链的币天销毁累积的变动，可以揭示市场走向。在市场处于下跌信道时，币天销毁的峰值意味着市场中的弱手，因为代表着大户可能要抛币。当市场处于上涨信道时，币天销毁的峰值意味着市场中的强手，表明市场可能会走强。与传统股票市场不同，在比特币等数字货币交易市场中，币天销毁比每日交易量这个指标更能准确地显示市场的资金流动。因为如果一个人开两个账户（比特币地址），用100个比特币来掉头账，这样可以把交易量做到很大，但币天销毁却几乎维持不变。

币天销毁第二次被引起重视是在权益证明（PoS）中。点点币创始人萨尼·肯为避免工作量证明机制（PoW）的算力浪费，设计了权益证明的共识方案：当创造一个权益证明的区块时，矿工需要创建一个“币权”交易，交易会按设定的比例把一些币发送给矿工本身，其原理与比特币的区块产出25个新币相

似，不同的是其难度与交易输入的“币天”成反比，而与哈希计算力无关。由于权益证明的哈希运算只是基于时间与已知数据，因此无法通过改进芯片性能来加快其运算速度。每一秒钟，每个点点币交易输出都有一定概率产生与其币天成正比的工作量[12]。显然，在权益证明中引入币天的初衷是防止矿工重复使用自己的币，因为如果挖矿难度仅与矿工的权益（拥有的币）相关，那么，每个币都可以成为“仿真矿机”，那些拥有大量币的人躺着就能挣钱（挖矿），持币较少的用户则只能喝西北风，而这正是权益证明饱受诟病的原因。但若挖矿难度是币天的函数，虽然这种“仿真矿机”的算力会随着时间累积而线性增长，但每发现一个新的区块其算力就随币天的销毁而归零，故币天可以保障权益证明机制中所有挖矿者的公平性。

以上两个应用实例虽然解决的是不同的问题，但本质上都是利用币天销毁在交易过程中不可逆的特性，使得用户不能在两个账户间反复利用同一笔钱获得某种回报。在市场中，大户不能利用同一笔比特币制造大量币天销毁虚构币的流动，在PoS挖矿中，用户不能利用同一笔点点币反复挖得区块中的新币。相应地，如果把币天销毁引入交易的信用评价呢？如果说币天销毁在市场预测与权益证明中的应用是小试牛刀的话，那么，它在信用评价中的作用则是锋芒毕露了。让我们看看为什么刷客与差评师们在区块链的信用体系中会混不下去。

如果规定把币天销毁作为信用评价因子，在一次交易中，销毁的币天越多，则信用评价的权重越高。当刷客试图给用两个账户反复交易而刷好评时，第一次交易的评价是有效的，但历史上累积的币天在交易完成之时便已销毁，当进行第二笔交易时，由于发生在第一次交易后不久，币天积累非常小。相应地，对信用评价的贡献微乎其微，其后所有交易的币天销毁之和同样也非常小，用户利用同一笔钱反复给自己刷好评，不管进行多少次，其最终效果与第一笔交易所带来的信用评价几乎一样。同样，当差评师试图通过大量小额交易给用户以恶意差评时，由于信用评价正比于币天销毁，交易的额度太小，同样也几乎不能对用户的信用产生影响。

也许在不远的将来，在淘宝、京东等电商平台泛滥成灾的刷客与差评师将会失业。需要指出的是，人们过去总是把信用当作一个道德问题，试图从道德层面约束交易行为。淘宝极其复杂的信用体系试图区分真实的交易行为与作弊交易行为，并通过大数据分析，结合用户的社会关系、职业、收入甚至公共事业缴费单，评价一个人的信用高低。然而在区块链的信用评价中，信用其实是一个数学问题。在刚才的例子中我们看到，用户的交易行为不再被区分为作弊交易与真实交易，而对所有的交易行为一视同仁，通过数学赋予交易以成本（币天销毁），便可以使信用评价结果准确地反映用户的真实信用。作弊是允许的，不存在一个中心化权威可以跳出来宣布冻结你的账户，但即使你作弊，也不会对任何人的信用产生影响。

（五）交易的热力学第二定律

目前第三方支付都把交易处理成等价交易，在一次交易中，一方的支出等于另一方的收入（式1-1）。这本身并没有错，只是还不够。在交易的过程中，还需要引入时间之矢，用于区分一笔从A账户到B账户的交易与B账户到A账户的交易，虽然金额同样为m，但两个过程中销毁的币天不一样。

等价交易是个等式，而信用评价是个不等式。在交易的过程中，既包含交易金额的转移，又包含交易双方相互的评价。如果说等价交易就像是交易的热力学第一定律（式1-2），那么基于币天销毁的信用评价就好比发现了交易的热力学第二定律（式1-3）。

热力学第二定律讲的是在孤立系统内的不可逆过程，系统的熵总是增加的，也叫作熵增加原理。这一原理的克劳修斯表述是，不可能把热量从低温物体传向高温物体而不引起其他变化。相似地，我们可以得到热力学第二定律的交易式表述：在交易过程中，系统的币天总是销毁的，不可能在一次交易中不销毁任何币天。

币天销毁的本质就是时间之矢。正如特罗布里恩德群岛的居民们规定了库拉交易的空间方向，区块链上

的交易则是用币天销毁标记了交易的时间方向。等价交易把交易理解为标量，信用评价却把交易理解为矢量，等价交易加上信用评价，这才是交易的全部。

于是，奇怪的库拉交易行为也可以进行解释了。原来，岛民们并不是在做普通的等价交易，而是在从事一个类似于信用评价的交易。一个人的交易伙伴、交易次数的多少决定了他的信用高低，这确实符合信用的逻辑。信用也不取决于交易信物的价值，占有库拉并不能提升个人财富，相反，还可能损害个人信用，交易信物的价值很小，交易行为本身才有价值，库拉只有在流动中才能展现一个人的信用。那么，岛民们不远万里地与库拉伙伴们交易，也完全合乎他们的利益。虽说在院子里晒红薯堆的行为看起来简直“蠢萌蠢萌”，但他们在交易库拉时却是不折不扣的精明人。库拉交易确实不是等价交易，在这一点上，马林诺夫斯基是对的，但在岛民是不是“理性经济人”这个问题上，他着实是错怪古典经济学家了。

最后问题来了：是谁设计了币天？如前所述，在区块链中币天并不是必须存在的字段，它可有可无。如果区块链是一部机器，那么从这部机器中去掉币天这个零件，丝毫不影响整部机器的运行。但事实上，从创世区块以来，币天就已经存在了。中本聪为什么添加币天这样一个字段，我们只能像Vitalik一样把这个归为碰巧吧。

四、区块链篇

（一）第五次计算范式创新

1970年是比特币的计时元年，比特币区块链的时间戳从1970年1月1日起开始计算秒数。

1970年，纽约清算所创建银行同业支付系统（CHIPS），以电子化的手段代替原来的纸质支付清算。当时采用的是联机作业方式，通过清算所的交换中心同9家银行的42台终端相连。

当然1970这个数字巧合并不是中本聪有意为之，区块链以1970作绝对时间的计算起点，是因为UNIX（尤尼斯）操作系统以1970年1月1日作为纪元时间，很多编程语言起源于UNIX系统，同时也在比特币代码中留下了历史的痕迹。20世纪70年代，采用UNIX操作系统的大型机大行于世，所以银行清算中心也因大型机的面世而步入电子化时代。这与其说是巧合，不如说是偶然中的必然。

分析现代社会进化过程的一种方法是观察计算范式，我们看到每隔10年就会有一次新的范式出现。20世纪70年代是大型机，20世纪80年代是个人电脑，互联网与移动互联网则是最近的两次范式创新，那么接下来10年呢？基于区块链加密协议的价值互联网很可能就是一种新的范式（图1-3）。

图1-3 五次计算范式创新

与声名大振的比特币相比，区块链技术一直默默无闻，但关于比特币的误解却一直影响着公众对区块链的认知，如与“丝绸之路”这样的网络黑市的种种关联，不免让人谈虎色变。事实上，各国政府部门、金融机构都在探索区块链技术的未来应用场景。它的以下四个特征，可能会给政府与金融服务带来跨越性创新[13]。

1.通过加密技术对账

目前，政府和商业机构会把交易的详细信息发送给对方，一旦收到信息，每个机构都会在自己的账本上更新信息。但现在还没有一种方法可以保证这些信息的准确性。区块链可以通过分布式共识机制来解决这个问题。例如，通过工作量证明、权益证明等不同共识算法解决拜占庭将军问题，或通过“证据点”检验数据，账本的参与者就可以就底层数据的状态达成共识。

2.数据复制

许多机构都有部分或全部数据的拷贝，这极大地降低了错误数据出现的可能性。对于现在的数据库技术来说，数据复制工作会增加IT（信息技术）系统的成本，并对IT系统的复杂性提出更高的要求。将数据大量复制的一个好处就是哪怕有一处数据出现错误，其他的数据还会是准确的。很多机构可以通过对账

计算，检验其数据是否准确。

3.访问控制

分布式账本使用私钥和签名管理能够访问账本的权限。这些私钥在特定情况下具有特定的功能。举例来说，一名监管人员想检查一个机构所有的交易，可能需要一把“观察钥匙”，但这样的钥匙只有被法庭授权后才能具有这样的权限。

4.透明性和私密性

因为许多机构都拥有账本的备份，同时也可能验证每份记录的真伪，所以共享账本的透明性是很高的。因此，监管者或是独立第三方（司法）可以确信数据库的内容没有被篡改。鉴于此，他们可以公开原本是私密或不可公开的文件信息。在监管报告和欺诈预防方面，共享账本可以帮助银行等商业机构，甚至可以使民众拥有监督政府履行职责的能力。通过独特的数字签名技术，可以验证正确的人已经按照正确的规则添加了正确的记录。

（二）无银行间组织的跨行结算

生活中我们经常需要跨行、异地存取款，这会给银行之间带来高昂的结算成本。在没有银行间清算组织之前，需要解决两家银行之间的通信问题。以图1-4为例，汇丰银行、花旗银行、渣打银行之间需要专门的通信接口，以满足双向通信的要求。

图1-4 无银行间清算组织的结算

下面，以银行的存付款为例，让我们设想有三个银行：汇丰银行、花旗银行、渣打银行；两个用户：用户A和用户B。每一个银行都有独立的信息系统，来核算自己的收支情况。汇丰银行的信息系统记录自己的客户的账户收支，花旗银行的信息系统记录自己的客户的账户收支，以此类推（图1-5）。

图1-5 银行各自记录账户收支的信息模型

显而易见，我们可以发现两个问题。

第一，记录的重复性。看看银行的记账方式，汇丰银行的系统记录着“花旗银行欠汇丰银行100万欧元”，而花旗银行的系统也记录这个事务。也就是说，同样的事务被两个独立研发的系统记录了两次。而在其他领域，这种重复更加庞大也更加昂贵。

第二，记录者风险。看看用户A在汇丰银行和渣打银行有存款，而他在花旗银行是处于透支状态。也就是说，汇丰银行和渣打银行欠用户A钱，那么是谁记录这个欠钱的事务呢？汇丰银行和渣打银行自身！用户A不得不相信这两家银行会妥善处理自己放在银行的钱，银行会保持所有记录的准确性。我们习惯地将这种情况视为理所当然，但总感觉哪里不对劲吧。毕竟塞浦路斯银行危机这样的事就发生在不久前，如果有一天，你拿张祖传的100万美元存单，银行说上面只有1000元……

因此我们看到了两个有趣的现象：存款方不得不相信银行会妥善保管存款，并准确记录账户信息。而银行自己也不得不花费大量的时间和金钱来创建一套系统，以相信自己可以妥善保管用户的钱并保持账户信息的准确性。然后同业银行之间会花费更多的时间和金钱，互相检查，以保证它们的系统可以达成一致。

即便是在简单的模型里面，也至少有7处需要对账（图1-6）。银行里的“事务”通常最少要由两个不同的实体记录，并且需要昂贵的重复确认过程来保证各方的记录是一致的。

图1-6 对账的简单模型

在没有清算系统之前，同业银行之间的来往增多以后，会快速增加银行之间的清算网络和成本。这还只是三家银行的简单模型，通信网络就增加到6条，当银行越来越多的时候，这种点对点的通信变得越来越复杂，每新增一家银行，要做之前银行都要做的重复性工作，成本非常高昂。

如果一家银行与业内的1000家银行之间创建清算链接，该银行需要建设1998条通信链路。类似于足球比赛中主客场之间比赛，20支球队之间的联赛，每支球队需要参加38场比赛，30支球队的联赛每支球队需要踢58场比赛。

上述例子套在保险业和金融衍生品系统也是完全合适的。事实上对后者而言，这个模型带来的问题会更加严重，因为我们不仅仅需要确认谁和谁做了什么样的交易，还要确认他们以及他们的系统都同意交易带来的结果——他们一定要在商业逻辑上达成一致。

想一想在金融领域有多少几乎一样的系统存在，每一个都几乎无差别的运行，制造更加几乎无差别的结果，这些结果不得不以昂贵的方式检查和解决，花费是十分巨大的。

（三）中心化的共享式总账

如果每一个银行都运行自己的系统，是如此昂贵和复杂，并且不可避免地带有局限性，不得不在与其他系统重叠的部分反复检查以互相匹配，那为什么不直接让大家都使用，由大家都相信的某权威运行的一份统一单独的总账（如图1-7）？

图1-7 中心化共享总账的对账模型

图1-7 左边的5张分开的表格合并后，可以完全等价地写成右边单一的表格，同样从右边的表格也很容易复原出左边的5张表格，唯一的不同是右边的表多一列。这样我们就可以用一张表记录一切，并且得到与原来的方案相同的结果。每个银行都可以毫不费力地从这个总账本中找出与自己相关的部分。

那么必须出现一个网络来保管右边这统一的表格，而且它能够接入所有的银行。新的银行只需接入这个网络，就可以和其他所有银行进行通信，清算所和银行间组织就这样应运而生。

（四）有银行间组织的跨行结算

说起美国银行业清算系统的由来，还有一段趣闻。在两百多年前，两个银行职员的偶遇擦出了债务交换的火花，成为现代银行间清算系统的雏形。那天，两个不同银行的职员在收账的路途中小憩，碰巧走进了同一家咖啡店。闲聊中，得知相互都要去对方那里取送票据，于是灵机一动，干脆在咖啡店进行交换算了，这样就可以省掉去对方营业地的旅途劳顿。从那以后，喝咖啡成了他们的正差，交换票据成了副业。如此滋润的事自然吸引了其他同行，他们纷纷加入进来，于是这家咖啡店变成了不叫清算所的清算所。

如果说咖啡店票据交换场所尚处于蹒跚学步阶段的话，那么1853年由62家银行在华尔街14号地下室共同创立的纽约清算所则标志着银行清算所已步入成年。CHIPS（纽约清算所银行同业支付系统）是全球最大的私营美元资金交换系统，平均每天清算和处理1.5万亿美元的美国境内和跨境支付业务。

美国不仅拥有全球最发达的银行清算系统，还拥有全球最发达的资本市场清算系统，也是全球最大的信用卡清算中心。VISA（维萨）和万事达两大国际信用卡组织均为位于美国纽约的摩根大通银行，同时也是自动清算所的成员，纽约也就成为全球信用卡的发源地和支付清算中心。

在VISA和万事达等这样的信用卡组织出现之前，跨行结算复杂度高，成本高，速度极慢。信用卡组织出现后，形成中心清算的模式，所有银行和该中心创建清算接口，所有跨行之间的交易都汇总到该清算中心。清算组织的出现提升了跨行清算的速度，并降低了清算的成本（图1-8）。

图1-8 有清算组织的银行间的跨行结算

但由于清算中心是中心化的架构，随着加入组织的银行成员增多，给清算中心带来收入的同时，也加大了工作量。在接入的银行超过一定程度后，再增加银行会员，就会显著增加清算中心的成本和工作量，从而降低清算速度。例如管理10人团队和管理10000人团队差别很大。目前，国际上三大信用卡上市公司VISA、万事达、美国运通2015年营业收入合计达到543亿美元。区块链技术实现分布式记账的结算之后，能为整个银行业节省一大笔费用。

清算、结算、托管和注册服务对于发行、交易和持有证券都会显著增加成本。有大量的专业代理和交易对手参与到投资者的证券和现金活动，不仅这些服务有特定的收费，还有处理各种不同系统接口的业务集成和流程的辅助成本。据估算，全球金融行业每年在交易后（post-trade）成本是650亿~800亿美元。图1-9以T+2交易机制为例，描述了主流证券交易结算的多层次的复杂交易过程[14]。

图1-9 美国证券交易的托管结算体系

同样，传统清算中心还面临中心化风险。例如“9·11”事件后，纽约联邦储备银行立刻停止靠近纽约的新泽西美元支付清算系统的运行，启动灾难备份系统，将美元支付清算系统从纽约新泽西切换到里士满和达拉斯。虽然在整个切换过程中，支付清算系统既没有中断服务，也没有丢失数据，但也惊出一身冷汗。如果袭击的不是世贸大楼，而是新泽西的美元支付清算系统，那么纽约清算中心将立即崩溃。

（五）去中心化的共享式总账

全球共享的账本可能被单一的强力实体控制，还有中心化的系统可能会有系统性的风险。因此我们可不可以对模型做两种微调？

第一，为什么不大量地复制账本，让每一个银行都保管一份拷贝？这样，单点出现故障就不会影响总体，系统也会更安全，因为要篡改其中一份拷贝很容易，但要同时改动所有人的拷贝则很难。同样，每一个银行都有一份总账本拷贝也能使现存金融机构的整合变得更容易，这也能推动共享式总账的接受度。问题是怎样保证这么多份拷贝实现同步？

第二，为什么不让这个系统的参与者——不仅仅是银行，也许还包括银行的用户——一起参与进来维持和保护这个系统呢？毕竟，银行和用户都是这个系统的直接利益攸关方，不用怀疑他们任何一方保护自己的钱与监督对方的动力。任何一方欺骗都会被及时发现并受到惩罚。因此我们将一个单一权力的实体替换为每一个人都参与系统安全的新模型。

如果以上设想成立，账本看起来应该是这样的（图1-10）。

图1-10 银行与用户共同参与的系统模型

在这个模型中，所有的参与方都有一份总账的拷贝，但是只有修改自己部分的权限，因此它既是可复制的又是分布式的。

如果一个全球化的分享式总账存在风险，那么区块链就是对各方有利的最佳选择。区块链技术以点对点的方式运行一个分布式共享账本，参与者通过非对称加密的公私钥对执行交易，这显著降低了交易结算的复杂性和交易后的服务成本。

区块链几乎不存在单点故障，数据存储在全球数以万计的节点之上，分布式网络每时每刻都有大量节点频繁地加入或退出，但丝毫不影响全局结构的稳定性。

交易数据以区块的形式被打包到数据库，每一个区块都会由节点进行审查。如果所有节点达成共识，该区块包含有效交易时就会被添加到数据库中。此外，创建和维护这些节点是完全自治的，不需要也不允许任何一个控制或监管实体的存在。

由于区块链清算和结算几乎达到同步，系统在点对点网络上运行，每一笔交易都能确保准确执行，安全透明，每笔交易都能被网络上所有节点核实，而不是依靠一个中心化机构，因此其交易几乎不能被篡改。几乎所有无形的文件或资产都能以编码的形式表达，交易历史既可以被记录且公开，也可以被自主隐藏。隐私的选择权在于私钥的拥有者用户本人，使参与者能更自主地管理自己的隐私，监管者更有效地监管资产的流动。

[4] 本章由长铗完成。长铗,巴比特（www.8btc.com）创始人，区块链研究者，科幻作家，2006~2008年连续三届中国科幻小说最高奖银河奖得主。合着有《比特币——一个真实而虚幻的金融世界》（中信出版社），合编有《2014~2015中国数字货币行业发展研究报告》（上海社科院出版社）。巴比特创立于2011年，专注于区块链信息、数据、社区与区块链众筹服务，现已发展为国内入口级区块链基础信息与数据服务平台。

[5] Dominic Frisby.搜寻中本聪.巴比特，2014.

[6] 由罗纳德·维斯特、阿迪·萨莫尔和伦纳德·阿德曼三人姓首字母为名的一种加密算法。

[7] Napster是一款可以在网络中下载自己想要的MP3文件的软件。

[8] 维基解密创始人朱利安·阿桑奇也是密码邮件组成员。

[9] 解密学家猜测中本聪可能是英国人，或受到英国文化影响，这不无道理，因为大多数人可能都会采用damn hard（非常地困难）或者更简单粗暴的语言。

[10] Base58是比特币中使用的一种独特的编码方式，主要用于产生比特币的钱包地址和私钥。

[11] 马林诺夫斯基.西太平洋的航海者.梁永佳，等，译. 北京：华夏出版社，2002.

[12] Vitalik Buterin.什么是权益证明以及为什么它重要.巴比特，2013.

[13] 英国政府首席科学顾问报告《分布式账本技术：超越区块链》。

[14] DTCC：拥抱颠覆者——探索分布式总账技术潜力，改进交易后场景。

第二章
区块链基础[15]

一、区块链的基本概念

区块链（Blockchain）技术的产生和发展离不开比特币。首先，因为随着比特币的诞生，区块链技术才得以公布于众；其次，比特币是截至目前区块链技术最成功、最成熟的应用案例。比特币的概念由中本聪在2008年发表的论文《比特币：一种点对点的电子现金系统》中首次提出。文中，中本聪将区块链技术作为构建比特币数据结构及交易体系的基础技术，将比特币打造为一种数字货币和在线支付系统，利用加密技术实现资金转移，而不再依赖于中央银行。比特币使用公钥地址发送和接收比特币，并进行交易记录，从而实现个人身份信息的匿名。交易确认的过程则需要用户贡献算力，共同对交易进行共识确认，从而将交易记录到全网公开账本中。用户可以利用电脑、手机等发送或接收比特币，并选择交易费用。现有逾百种加密数字货币（未来币、点点币、莱特币、狗狗币等），比特币约占所有加密数字货币市值的90%。

比特币的区块链毕竟是为比特币体系的设计而定制，因此比特币的区块链技术并不等于区块链技术。区块链技术应该是可以有更多种形态、更多种体系、更多种用途、更多种规格的技术，其概念为：区块链是一个去中心化的分布式数据库，该数据库由一串使用密码学方法产生的数据区块有序链接而成，区块中包含有一定时间内产生的无法被篡改的数据记录信息。

区块中包含数据记录、当前区块根哈希（Hash）、前一区块根哈希、时间戳以及其他信息（图2-1）。数据记录的类型可以根据场景决定，比如资产交易记录、资产发行记录、清算记录、智能合约记录甚至物联网数据记录等。数据记录在存储过程中，通常组织为树形式，比如默克尔树，而区块根哈希实际就是数据记录树的根节点哈希，为根据数据记录树自下而上逐步通过SHA-256等哈希算法计算得出。时间戳为区块的生成时间。其他信息包括区块签名信息、随机值等信息，也可根据具体应用场景灵活定义。

图2-1 区块链结构示意图

区块链技术不是一种单一的技术，而是多种技术整合的结果，包括密码学、数学、经济学、网络科学等。这些技术以特定方式组合在一起，形成了一种新的去中心化数据记录与存储体系，并给存储数据的区块打上时间戳使其形成一个连续的、前后关联的诚实数据记录存储结构，最终目的是创建一个保证诚实的数据系统，可将其称为能够保证系统诚实的分布式数据库。在这个系统中，只有系统本身是值得信任的，所以数据记录、存储与更新规则是为创建人们对区块链系统的信任而设计。诚实意味着系统可以被信任，正是商业活动和应用推广的前提，所以区块链技术已经被很多领域主流机构看中并非是没有理由的。因为有了区块链技术，在一个诚信的系统里，可以省去许多烦琐的审查手续，许多因数据缺乏透明度而无法开展的业务可以开展，甚至社会的自动化程度也将大幅提升。

近年来，包括高盛、摩根大通和纳斯达克等金融机构开始展开对区块链技术的重点研究。这些机构的金融业务大都具有标准化程度高、连续性强、自动化需求大、业务对信用度要求高等特点，跟区块链的优势高度契合。同时，在供应链金融中，由于物流、资金流和信息流的复杂安排会涉及众多单据，因此使用电子商务平台记账会大大节省纸质单据所需要的时间和成本，然而使用谁的电子商务平台就成为一个大问题。如果使用利益相关各方自建的电子商务平台，数据的真实性就很容易受到质疑，而自建电子商务平台往往耗资不菲；如果使用第三方的电子商务平台，第三方的经营稳定性和信息安全性又难以保证，比如因财务、政策、网络攻击等各种情况引起不稳定问题等，沟通协调成本和风险也会大幅增加。区块链技术的安全性、不可逆、不可篡改性和透明性都已经得到了证明，如果能把供应链金融业务直接创建在这样已被证明其可靠性的区块链上，将极大地降低安全和信用成本。所以，尽管目前电子商务平台的使用已经大大节约了成本，但如果能有一个具有公信力的类似区块链公共信用系统，成本仍有进一步节约的空间。从政府层面来说，这一点也很重要，因为提供值得福斯信任的系统本身就是政府职能的一部分。中国的资本运用效率远低于美国的一个非常重要的原因就是社会的信用体系不健全、信息不透明、部门协调成本过高，且利益保护现象严重。如果能从技术上应用区块链，就可以用较低的成本打破

这些阻碍，创建一个公开的社会公共信用系统，整个社会成本都将大幅降低，效率也将大幅提升，还便于监管。透明的数据不仅将大大降低监管部门的工作量（很大一部分工作量转移给了社会监督，任何异动都很难逃过众人的眼睛），而且使得监管部门的主要工作转向治理，提升治理人性化和效率。

尽管使用区块链技术所创建的系统本身是诚实可信的，但这并不意味着来自系统以外的输入信息就是诚实的，更多的时候只是意味着区块链诚实记录并储存了这些外部数据。比如认证，认证工作往往是在线下完成，即使区块链能够存储文字、图片甚至多媒体信息，也并不意味着那些信息都是真实的。这只意味着区块链真实记录并存储了这些信息，防止被篡改，如果发生业务纠纷时可以作为凭证。可能许多人没有注意到这一点，自动化是区块链技术的一个非常重要的特性，区块链网络实际上就是一个接近于自动化或存在完全自动化可能性的网络。这一点之所以重要，一方面，是因为自动化是金融机构青睐区块链技术的重要原因，金融交易需要网络能够自动记录和存储交易数据，也能够允许参与者通过设置条件在网络上自动进行和完成交易；另一方面，区块链技术在这方面提供的可能性为社会生产效率的大幅提升留下了广阔的空间，也为智能合约等一系列高级应用留下了充足的余地。在理想情况下，区块链技术最终能够同物联网结合起来。

总体而言，区块链的发展体系可以划分为四个象限（图2-2）。第一象限是比特币区块链；

第二象限是使用比特币区块链协议，但不使用比特币货币的系统，比如万事达币、彩色币、合约币，以及采用合并挖矿的域名币等；第三象限是同时使用独立货币和独立区块链的系统，比如以太坊、瑞波、莱特币和未来币等；第四象限是侧链，采用独立的网络但以比特币作为底层货币的系统，如BTC Relay等。

图2-2 区块链发展体系四象限

（一）区块链的分类

目前已知的区块链技术应用大致分为三类。

1.公共区块链（Public Blockchain）：是指全世界任何人都可读取、可发送交易进行有效性确认，任何人都能参与其共识过程的区块链（共识过程是维持区块链这种分布式数据库一致性、准确性的关键技术，将在后续章节详细介绍），如图2-3所示。区块链上的数据记录公开，所有人都可以访问，都可以发出交易请求，并通过验证被写入区块链。共识过程的参与者通过密码学技术共同维护公共区块链数据的安全、透明、不可篡改。公共区块链的典型应用包括比特币、以太坊等。

图2-3 公共区块链示意图

公共区块链是完全分布式的区块链，区块链数据公开，用户参与程度高，同时易于产生网络效应，便于应用推广。然而，系统的运行需要依赖于内建的激励机制。公共区块链上试图保存的数据越有价值，越要审视其安全性以及安全性带来的交易成本、系统可扩展性问题。

2.共同体区块链（Consortium Blockchains）：又称联盟链，是指参与区块链的节点是事先选择好的，节点间通常有良好的网络连接等合作关系，区块链上的数据可以是公开的也可以是内部的，为部分意义上的分布式，可视为“部分去中心化”。如图2-4所示为共同体区块链示意图。比如有若干家金融机构之间创建了某个共同体区块链，每个机构都运行着一个节点，而且为了使每个区块生效需要获得至少其中10个机构的确认。区块链可以允许每个机构可读取，或者只受限于共识验证参与者，或走混合型路线，例如区块的根哈希及应用程序接口对外公开，允许外界用来进行区块链数据和区块链状态信息查询等。其典型应用包括超级账本（Hyperledger）、区块链联盟R3CEV等。

图2-4 共同体区块链示意图

共同体区块链的参与节点间的连接状态较好、验证效率较高，只需较低的成本即可维持运行，提供高速交易处理的同时降低交易费用，有很好的扩展性，数据可以保持一定的隐私性。但是这也意味着在共识达成的前提下，参与节点可以一起篡改数据。

3.私有区块链（Private Blockchain）：参与的节点只有有限的范围，比如特定机构的自身用户等，数据的访问及使用有严格的权限管理，如图2-5所示为私有区块链示意图。完全私有的区块链中写入权限仅在参与者手里，读取权限可以对外开放，也可以进行任意程度的限制。相关的应用囊括数据库管理、数据库审计甚至公司管理，尽管在有些情况下希望私有区块链可以具有公共的可审计性，但在更多的情况下，没有公共的可读性。由于是私有用户说了算，里面的数据没有无法篡改的特性，对于第三方的保障力度大大降低。因此，目前很多私有区块链会通过依附在比特币等已有区块链的方式存在，定期将系统快照数据记录到比特币等系统中。其典型应用如Eris Industries。

图2-5 私有区块链示意图

私有区块链可以带来规则的改变。如果需要的话，运行着私有区块链的机构可以很容易地修改区块链的规则、回滚交易。这一点似乎略有违背区块链的本质，但是却适用于一些特殊场景需求。由于私有区块链验证者是内部公开的，所以并不存在部分验证节点共谋进行51%攻击的风险。私有区块链交易成本更低。交易只需被几个受信的高算力节点验证即可，而不是需要数万个节点的确认，因此交易成本会低。但从长远来看，随着区块链技术的进步，公共区块链的成本将可能降低1~2个数量级，大致与高效的私有区块链系统类似。私有区块链节点间连接情况好、故障可以迅速通过人工干预来修复，从而提升交易速度并可以更好地保护隐私。

公共区块链、共同体区块链和私有区块链各有优势。公共区块链很难实现得很完美，共同体区块链、私有区块链需要找到实际迫切需求的应用需求和场景。至于具体选择哪套方案取决于具体需求，有时使用公共区块链会更好，但有时又需要一定的私有控制，适用于使用共同体区块链或私有区块链。

（二）区块链的特征

1.去中心化

去中心化是区块链最基本的特征，意味着区块链不再依赖于中央处理节点，实现了数据的分布式记录、存储和更新。由于使用分布式存储和算力，不存在中心化的硬件或管理机构，全网节点的权利和义务均等，系统中的数据本质是由全网节点共同维护的。由于每个区块链节点都必须遵循同一规则，而该规则基于密码算法而非信用，同时每次数据更新需要网络内其他用户的批准，所以不需要一套第三方中介结构或信任机构背书。在传统的中心化网络中，对一个中心节点实行攻击即可破坏整个系统，而在一个去中心化的区块链网络中，攻击单个节点无法控制或破坏整个网络，掌握网内超过51%的节点只是获得控制权的开始而已。

2.透明性

区块链系统的数据记录对全网节点是透明的，数据记录的更新操作对全网节点也是透明的，这是区块链系统值得信任的基础。由于区块链系统使用开源的程序、开放的规则和高参与度，区块链数据记录和运行规则可以被全网节点审查、追溯，具有很高的透明度。

3.开放性

区块链系统是开放的，除了数据直接相关各方的私有信息被加密外，区块链的数据对所有人公开（具有特殊权限要求的区块链系统除外）。任何人或参与节点都可以通过公开的接口查询区块链数据记录或者开发相关应用，因此整个系统信息高度透明。

4.自治性

区块链采用基于协商一致的规范和协议，使整个系统中的所有节点能够在去信任的环境自由安全地交换数据、记录数据、更新数据，把对个人或机构的信任改成对体系的信任，任何人为的干预都将不起作用。

5.信息不可篡改

区块链系统的信息一旦经过验证并添加至区块链后，就会得到永久存储，无法更改（具备特殊更改需求的私有区块链等系统除外）。除非能够同时控制系统中超过51%的节点，否则单个节点上对数据库的修改是无效的，因此区块链的数据稳定性和可靠性极高。

6.匿名性

区块链技术解决了节点间信任的问题，因此数据交换甚至交易均可在匿名的情况下进行。由于节点之间的数据交换遵循固定且预知的算法，因而其数据交互是无须信任的，可以基于地址而非个人身份进行，因此交易双方无须通过公开身份的方式让对方产生信任。

二、区块链的工作原理

（一）拜占庭将军问题

拜占庭将军问题是容错计算中的一个老问题，由莱斯利·兰伯特（Leslie Lamport）等人在1982年提出。拜占庭帝国是5～15世纪的东罗马帝国，即现在的土耳其。拜占庭城邦拥有巨大的财富，使它的十个邻邦垂涎已久。但是拜占庭高墙耸立，固若金汤，没有一个单独的邻邦能够成功入侵。任何单个城邦的入侵行动都会失败，而入侵者的军队也会被歼灭，使其自身反而容易遭到其他九个城邦的入侵。这十个邻邦之间也互相觊觎对方的财富并经常爆发战争。拜占庭的防御能力如此之强，十个邻邦中的至少一半同时进攻，才能攻破。也就是说，如果六个或者更多的邻邦一起进攻，就会成功并获得拜占庭的财富。然而，如果其中有一个或者更多邻邦发生背叛，答应一起入侵但在其他人进攻的时候又不干了，会导致只有五支或者更少的军队在同时进攻，那么所有的进攻军队都会被歼灭，并随后被其他邻邦所劫掠。因此，这是一个由不互相信任的各个邻邦构成的分布式网络，每一方都小心行事，因为稍有不慎，就会给自己带来灾难。为了获取拜占庭的巨额财富，这些邻邦分散在拜占庭的周围，依靠士兵相互通信来协商进攻目标及进攻时间。这些邻邦将军想要攻克拜占庭，都面临着一个困扰，也就是拜占庭将军问题。

> 邻邦将军不确定他们中是否有叛徒，叛徒可能擅自变更进攻意向或者进攻时间。
> 在这种状态下，将军们能否找到一种分布式协议进行远程协商，进而赢取拜占庭
> 城堡攻克战役的胜利呢？这就是拜占庭将军问题。

针对拜占庭将军问题的解决方法包括：口头协议算法、书面协议算法等[16]。口头协议算法的核心思想如下：要求每个被发送的消息都能被正确投递，信息接收者知道消息的发送者身份，知道缺少的消息信息。采用口头协议算法，若叛徒数少于1/3，则拜占庭将军问题可解。也就是说，若叛徒数为m，当将军总数n至少为3m+1时，问题可解。然而，口头协议算法存在明显的缺点，那就是消息不能追根溯源。为解决该问题，提出了书面协议算法。该算法要求签名不可伪造，一旦被篡改即可发现，同时任何人都可以验证签名的可靠性。书面协议算法也不能完全解决拜占庭将军问题。因为该算法没有考虑信息传输时延、其签名体系难以实现且签名消息记录的保存难以摆脱中心化机构。

与已有方法相比，区块链技术将是更完美的解决方案。区块链是怎样来解决这个问题的呢？它为发送信息加入了成本，降低了信息传递的速率，并加入了一个随机数以保证在一段时间内只有一个矿工可以进行传播。它加入的成本就是“工作量”，区块链矿工必须完成一个随机哈希算法的计算工作量才能向各城邦传播消息。

当用户向网络输入一笔交易的时候，他们使用内嵌在客户端的标准公钥加密工具为这笔交易签名，这好比拜占庭将军问题中他们用来签名和验证消息时使用的“印章”。因此，哈希计算速率的限制，加上公钥加密，使一个不可信网络变成了一个可信的网络，使所有参与者可以在某些事情上达成一致。拜占庭将军问题的区块链解决方案可以推广到任何在分布式网络上缺乏信任的领域，比如说域名、投票选举或其

他需要分布式协议的地方[17]。

（二）区块链工作流程

区块链的工作流程主要包括如下步骤（图2-6）。

①发送节点将新的数据记录向全网进行广播。

②接收节点对收到的数据记录信息进行检验，比如记录信息是否合法，通过检验后，数据记录将被纳入一个区块中。

③ 全网所有接收节点对区块执行共识算法（工作量证明、权益证明等。

④区块通过共识算法过程后被正式纳入区块链中存储，全网节点均表示接受该区块，而表示接受的方法，就是将该区块的随机散列值视为最新的区块散列值，新区块的制造将以该区块链为基础进行延长。

图2-6 区块链的工作流程

节点始终都将最长的区块链视为正确的链，并持续以此为基础验证和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上将存在先后差别，它们将在先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成长的链条。该僵局的打破需要共识算法的进一步运行，当其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。以上就是防止区块链分叉的整个过程。

所谓“新的数据记录广播”，实际上不需要抵达全部的节点。只要数据记录信息能够抵达足够多的节点，那么将很快地被整合进一个区块中。而区块的广播对被丢弃的信息是具有容错能力的。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了某个区块，也就可以提出自己下载该区块的请求。

现在我们都知道了区块链网络里的记账者是节点，节点负责把数据记录记到数据区块里，为了鼓励节点记账，系统会按照规则随机地对记账的节点进行奖励。那么如何保证不会有人制造假数据记录或者说如何保证造假数据记录不被通过验证？这就涉及时间戳。这也正是区块链与众不同的地方。区块链不仅关注数据区块里的内容，也关注数据区块本身，把数据区块的内容与数据区块本身通过时间戳联系起来。时间戳为什么会出现？这是由区块链的性质规定的。节点把数据记入了区块，因此一个区块就相当于一页账簿，每笔数据在账簿中的记录可以自动按时间先后排列，那么账簿的页与页怎么衔接起来？也就是说，这一个区块与下一个区块的继承关系如何断定就成为问题。于是时间戳就出现了。

时间戳的重要意义在于其使数据区块形成了新的结构。这个新的结构使各个区块通过时间线有序连接起来，形成了一个区块的链条，因此才称为区块链。区块按时间的先后顺序排列使账簿的页与页的记录也具有了连续性。通过给数据记录印上时间标签，使每一条数据记录都具有唯一性，从而使数据记录本身在区块和区块上的哪个位置上发生可以被精确定位且可回溯，也给其他的校验机制协同发挥作用提供了极大的便利和确定性，使整个区块链网络能够确定性地验证某条数据记录是否真实。由于区块链网络是公开的，意味着系统知道过去发生的所有数据记录，而任何新的数据记录都继承于过去的数据记录，因为过去的数据记录是真实的，而且链条的各个区块记录由时间戳连接起来使之环环相扣，所以如果想要制造一个假的数据记录，就必须在区块链上修改过去的所有数据记录。尽管在挖矿的过程中，形成了多个链条，但因为最长的那个被诚实的节点所控制，所以想要修改过去的数据记录，首先就要从头构造出一个长度比之前最长的那个还要长的链条，在这个新的链条超过原来的那个链条后，才能制造双重支付的虚假数据。然而随着时间推移，制造新链条的难度和成本都是呈指数级上升的，而且随着链条越来越长，其难度也变得越来越大，成本也就越来越高。同时，因为去中心化的设置，区块链的各个核心客户端同时又是服务器，保存了区块链网络的完整数据，因此使对区块链网络的攻击很难像对传统的中央处理节点那样有效，一般情况下很难对区块链网络构成重大冲击。最终，区块链网络成为一个难以攻破的、公开的、不可篡改数据记录和制造虚假数据的诚实可信系统。

区块链保证数据安全、不可篡改以及透明性的关键技术包括两个方面：一是数据加密签名机制；二是共识算法。在数据加密签名机制中，首先，要有一个私钥，私钥是证明个人所有权的关键，比如证明某人有权从一个特定的钱包消费数字货币，是通过数字签名来实现的。其次，要使用哈希（Hash）算法。哈希散列是密码学里的经典技术，把任意长度的输入通过哈希算法计算，变换成固定长度的由字母和数字组成的输出，具有不可逆性。共识算法是区块链中节点保持区块数据一致、准确的基础，现有的主流共识算法包括工作量证明（PoW）、权益证明（PoS）、瑞波共识协议（RCP）等。以PoW为例，是指通过消耗节点算力形成新的区块，是节点利用自身的计算机硬件为网络做数学计算进行交易确认和提高安全性的过程。交易支持者（矿工）在电脑上运行比特币软件不断计算软件提供的复杂的密码学问题来保证交易的进行。作为对他们服务的奖励，矿工可以得到他们所确认的交易中包含的手续费，以及新产生的比特币。

三、区块链共识机制

区块链要成为一个难以攻破的、公开的、不可篡改数据记录的去中心化诚实可信系统，需要在尽可能短的时间内做到分布式数据记录的安全、明确及不可逆，提供一个最坚实且去中心化的系统。在实践中，该流程分为两个方面：一是选择一个独特的节点来产生一个区块；二是使分布式数据记录不可逆。实现上述流程的技术核心就是：共识机制。共识机制是区块链节点就区块信息达成全网一致共识的机制，可以保证最新区块被准确添加至区块链、节点存储的区块链信息一致不分叉甚至可以抵御恶意攻击。

当前主流的共识机制包括：工作量证明、权益证明、工作量证明与权益证明混合（PoS+PoW）、股份授权证明、瑞波共识协议等。

（一）工作量证明

工作量证明（Proof of Work）,顾名思义，即指工作量的证明。PoW机制的基本步骤如下：①节点监听全网数据记录，通过基本合法性验证的数据记录将进行暂存；②节点消耗自身算力尝试不同的随机数，进行指定哈希计算，并不断重复该过程直至找到合理的随机数；③找到合理的随机数后，生成区块信息，首先输入区块头信息，然后是数据记录信息；④接单对外部广播出新产生的区块，其他节点验证通过后，连接至区块链中，主链高度加一，然后所有节点切换至新区块后面继续进行工作量证明和区块生产。

PoW叫工作量证明体现在步骤②中，节点需要不断消耗算力工作，进行哈希计算，以找到期望的随机数。以比特币区块链为例，通过PoW机制维护区块链的整体运行及其安全性。验证节点通过随机的散列运算，争夺比特币区块链的记账权，防止欺诈交易，避免“双重支付”，这一过程需要消耗电力、算力来完成。因此，验证节点也成为“矿工”，随机数计算查找过程称为“挖矿”。每一个比特币区块链中的区块都包含着一个由无意义数据构成的短字符串（称为随机数），找到一个合适的随机数唯一已知的方法是不停地随机试探直到搜索到一个有效的数。比特币的PoW中，平均每10分钟有一个节点找到一个区块。如果两个节点在同一个时间找到区块，那么网络将根据后续节点和区块生成情况来确定哪个区块构建最终区块链。一般情况下，需要6个区块的生成时间进行确认，因为一般交易在6个区块（约1个小时）后被认为是安全确认且不可逆的。其工作量主要体现在：一个符合要求的区块随机数由N个前导零构成，零的个数取决于网络的难度值。要得到合理的随机数需要经过大量尝试计算，计算时间取决于机器的哈希运算速度。当某个节点提供出一个合理的随机数值，说明该节点确实经过了大量的尝试计算。当然，这并不能得出计算次数的绝对值，因为寻找合理随机数值是一个概率事件。工作量证明机制看似很神秘，其实在社会中的应用非常广泛。例如，毕业证、学位证、律师证等证书就是工作证明，拥有证书即表明在过去付出了努力。挖矿为整个系统的运转提供原动力，挖矿有三个重要功能：一是发行新的货币；二是维系系统的支付功能；三是通过算力保障系统安全。首先，挖矿消耗资源将黄金注入流通经济，比特币通过“挖矿”完成相同的事情，只不过消耗的是CPU时间与电力。其次，挖矿用于产量调节，区块的产量为大约每两周2016个，即每10分钟一块。第三，通过算力保障系统安全。算力攻击的概率难度呈指数上升（泊松分布），每个区块都必须指向前一个区块，否则无法验证通过。追根溯源便是高度为零的创世区块。PoW机制存在两方面明显的缺陷。一是算力的消耗与浪费。在PoW中，尽管区块链节

点是用来帮区块链进行分布式数据记录的，但是它们实际所做的大部分工作是寻找正确的随机数而与数据记录无关。用来寻找随机数的能量和资源将永远地消失，这显然是一种浪费。二是算力集中化凸显。PoW机制自然地导致了算力集中问题。由于作为一个普通的个体或者几十、几百台规模的矿机目前都很难挖到区块了，因此大家必须联合起来挖矿，就诞生了算力集中的地方——矿池。其中最著名的是比特币Ghash矿池，它因为数次接近甚至达到了50%比特币的算力，从而引起了比特币社区的广泛担忧。

（二）权益证明+工作量证明

2012年8月，一个化名Sunny King的极客推出了Peercoin（PPC），采用工作量证明机制PoW发行新币，采用权益证明机制PoS维护网络安全，即PoW+PoS机制。该机制中，区块被分成两种形式——PoW区块及PoS区块。在这种新型区块链体系里，区块持有人可以消耗他的币天获得利息，同时获得为网络产生一个区块和用PoS造币的优先权。PoS的第一次输入被称为权益核心，需要符合某一哈希目标协议。因此，PoS区块的产生具有随机性，其过程与PoW相似。但有一个重要的区别在于，PoS随机散列运算是在一个有限制的空间里完成的，而不是PoW那样在无限制的空间里寻找，因此无须大量的能源消耗。权益核心所要符合的随机散列目标是以在核心中消耗的币天的目标值（币×天），这与PoW是不同的，PoW的每个节点都具有相同的目标值。因此，核心消耗的币天越多，就越容易符合目标协议。PoS中还有一种新型的造币过程。PoS区块将根据所消耗的币天产生利息币，设计时设定了每币一年将产生1分利息，以避免将来的通胀。在造币初期时保留了PoW，使最初的造币更加方便。

在区块链中谁是主链的问题是解决分叉的关键。PoS判断主链的标准已经转化为对消耗币天的判断。每个区块的交易都会将其消耗的币天提交给该区块，以提高该区块的得分。获得最高消耗币天的区块将被选中为主链。此设计减少了部分对于51%攻击的忧虑，因为在PoS区块中，要进行51%攻击，首先，要控制数量众多的币天，成本可能要高于获得51%的算力，这样就提高了攻击的成本；其次，攻击者在攻击网络时，其币天也会消耗，这将使攻击者阻止交易进入主链的行为变得更加困难。

为抵御分布式拒绝服务攻击，在PoW+PoS机制中，每个区块都必须由其拥有者签名，以避免受到复制并被攻击者使用。为了抵御攻击者复制产生多个区块进行分布式拒绝服务攻击，每个节点都会收集其接触到的（核心，时间戳）配对信息。假如一个已接收到的区块包含与其他之前收到的区块中的配对信息（核心，时间戳）是重复的，会忽略此区块直到后者被孤立出去。

在PoW+POS机制下，只要持有币的人，不论持有的数量多少，都可以挖到数据块，而不用采用任何的矿池导致算力集中。同时，由于多采用币天生成区块，而不是算力，降低了资源消耗，解决了单纯PoW机制在维护网络安全方面先天不足的问题。

（三）权益证明

除了结合PoW使用外，能否单独利用PoS机制进行区块链系统设计运行呢？答案是肯定的。简单来说，PoS就是一个根据持有货币的量和时间，进行利息发放和区块产生的机制。在权益证明PoS模式下，有一个名词叫币天。例如，每个币每天产生1币天，比如持有100个币，总共持有了30天，那么此时币天就为3000。这个时候，如果发现了一个新PoS区块，币天就会被清空为0。每被清空365币天，将会从区块中获得0.05个币的利息（可理解为年利率5%）。

PoS的典型应用就是未来币。同其他加密货币一样，未来币体系的总账是创建和储存在一系列区块里的，也就是区块链中。每个区块链的备份都存放在未来币网络的每个节点里，而且在每个节点上没有加密的每个账户都能够生成区块，只要至少一个新入账户的交易已经确认了1440次。任何账户只要达到了这个标准就会被视为“激活账户”。在未来币里，每个区块都包含着255个交易，每个交易都是由包含识别参数的192字节的数据头开始的。一个区块里的每个交易量都是由128个字节所代表着。总共加在一起就意味着最大的区块大小有32K字节。每个区块都有一个“生成签名”的参数。激活账户用自己的私钥在原先的区块上签署“生成签名”。这就产生了一个64字节的签名，之后通过SHA256散列该签名。哈希产生的前八个字节给出了一个数字，作为一个“hit”。“hit”与目前的目标值相比较，如果计算出的“hit”值要比“目标值”低，那么就可以生成下一个区块了。对于每个活动账户来讲，“目标值”都是与它自身所确认

的余额成比例的。一个持有1000个币的账户得到的目标值是持有20个币账户所得到目标值的50倍。因此，拥有1000个币的持有者产生的区块数是持有20个币的人产生的50倍。同时，“目标值”并不是固定的，随着先前区块的时间戳的流逝时刻都在增长。如果在最初的一秒钟内没有哪个账户的“hit”值是低于“目标值”的，则下一秒钟“目标值”就会翻倍。“目标值”会连续地翻倍，直到一个活动账户的“hit”值有一个较低的数值。还有一个“基本目标”值，它以60秒的间隔设定为目标值。正是这个原因，一个区块平均产生的时间会在60秒。即使在网络上只有很少的激活账户，它们其中的一个最终会产生一个区块因为“目标”值会变得相当大。通过将你账户的“hit”值与目前的“目标”值相比，你就可以估算出你的“hit”值还有多久能成功。

当一个激活账户赢得产生区块的权利时，就能将任何可获得的且未确认的交易放入区块中，并用所有需要的参数来填充该区块。然后，这个区块就会被传播到网络中作为一个区块链的备选。每一个区块中的负载值、“hit”、产生的账户以及签名都能被网络上接收到它的节点所确认。每个区块参考之前的区块，区块形成的区块链可以用来追溯和查询网络中素有的交易历史，所有这些都会追溯到创世源区。上述完整地展示了利用币天进行区块产生和验证共识的过程，体现了PoS的核心思想。

（四）股份授权证明

PoS机制使用一个确定性算法以随机选择一个股东来产生下一个区块，该算法中，账户余额决定了节点被选中的可能性。然而，该系统并未使区块链变得越来越安全而不可逆，因为最终区块链的区块产生权掌握在账户余额最多的少数节点手中。同时，PoS面临的挑战是如何通过及时而高效的方法达成共识。为达到这个目标，每个持币节点可以将其投票权授予一名代表。获票数最多的前100位代表按既定时间表轮流产生区块。每名代表被分配到一个时间段生产区块。所有的代表将收到等同于一个平均水平的区块所含交易费的1%作为报酬。如果一个平均水平的区块含有100股作为交易费，一名代表将获得1股作为报酬，即可大大提高共识效率。这就是DPoS的核心思想。

网络延迟有可能使某些代表没能及时广播他们的区块，而这将导致区块链分叉。然而，这发生的概率较小，因为制造区块的代表可以与制造前后区块的代表创建直接连接。在DPoS中，第一个步骤是成为一名代表，必须在网络上注册公钥，然后分配到一个32位的特有标识符。然后该标识符会被每笔交易数据的“头部”引用。第二个步骤是授权选票。每个钱包有一个参数设置窗口，在该窗口里用户可以选择一个或更多的代表，并将其分级。一经设定，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。一般情况下，用户不会创建特别以投票为目的的交易，因为那将耗费他们一笔交易费。但在紧急情况下，某些用户可能觉得通过支付费用这一更积极的方式来改变他们的投票是值得的。每个钱包将显示一个状态指示器，让用户知道代表的表现如何。如果某代表错过了太多的区块，那么系统将会推荐用户去换一个新的代表。如果任何代表被发现签发了一个无效的区块，那么所有标准钱包将在每个钱包进行更多交易前要求选出一个新代表。与PoW系统及其他PoS系统一样，最佳区块链是最长的有效区块链。在任何时候，一名代表错过签发一个区块的机会，该区块链将比潜在竞争对手短。只要交易被写入区块后的100个区块中的51%被生产出来了，那么你就可以安全地认为在主区块链上。也许，在防止区块链分叉所导致的损失方面，最重要的事是在事发后第一时间得知消息。如果10区块中有超过5个错过生产，那么这意味着你很可能在一条支链上，因此应该停止所有交易，直到分叉得到解决。以一种及时的方式（少于5分钟）简单地发现并警示用户网络分叉，是可以最小化潜在损失的非常重要的能力。

（五）瑞波共识协议

瑞波共识协议（Ripple Consensus Protocol，RCP），使一组节点能够基于特殊节点列表达成共识。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由一定比例的该俱乐部会员投票通过。RCP机制的工作原理如下。

①验证节点接收存储待验证交易。首先，验证节点接收待验证交易，将其存储在本地；其次，本轮共识过程中新到的交易需要等待，在下次共识时再确认。

②活跃信任节点发送提议：首先，信任节点列表是验证池的一个子集，其信任节点来源于验证池；其

次，参与共识过程的信任节点须处于活跃状态，验证节点与信任节点间存在保活机制，长期不活跃节点将被从信任节点列表删除；最后，信任节点根据自身掌握的交易双方额度、交易历史等信息对交易做出判断，并加入到提议中进行发送。

③本验证节点检查收到的提议是否来自信任节点列表中的合法信任节点，如果是，则存储；如果不是，则丢弃。

④验证节点根据提议确定认可交易列表的步骤如下：首先，令信任节点列表中活跃的信任节点个数为M（比如5个），本轮中交易认可阈值为N（百分比，比如50%），则每一个超过M×N个信任节点认可的交易将被本验证节点认可；其次，本验证节点生成认可交易列表。系统为验证节点设置一个计数器，如果计数器时间已到，本信任节点需要发送自己的认可交易列表。

⑤账本共识达成的步骤如下：首先，本验证节点仍然在接收来自信任节点列表中信任节点的提议，并持续更新认可交易列表；其次，验证节点认可列表的生成并不代表最终账本的形成以及共识的达成，账本共识只有在每笔交易都获得至少超过一定阈值（比如80%）的信任节点列表认可才能达成。如果账本中每笔交易都获得至少超过一定阈值（比如80%）的信任节点列表认可，则共识达成，交易验证结束，否则继续上述过程。

⑥共识过程结束后，已经形成最新的账本，现将上轮剩余的待确认交易以及新交易纳入待确认交易列表，开始新一轮共识过程。

除上述机制外，还有恒星共识协议（Stellar Consensus Protocol，SCP）、改进型实用拜占庭容错机制（Practical Byzantine Fault Tolerance，PBFT）和Poo l验证池机制等共识机制被提出，甚至已经应用在区块链系统中，不同共识机制各有其应用场景和优势。

四、区块链面临的问题

目前，区块链技术已经受到众多领域的广泛关注并得到应用，包括托管交易、金融交易、公共交易、证件、私人记录、留存证明、实物资产、无形资产等。然而，区块链技术在面临机遇的同时，也面临着不少问题与挑战。

（一）区块链体积过大问题

随着区块链的发展，节点存储的区块链数据体积会越来越大，存储和计算负担将越来越重。以比特币区块链为例，其完整数据的大小当前已达63.61GB（千兆）（图2-7），用户如果使用比特币核心客户端进行数据同步的话，可能三天三夜都无法同步完成，并且，区块链的数据量还在不断地增加。这给比特币核心客户端的运行带来了很大的困难。

图2-7 比特币区块链体积增长趋势

数据来源：区块元blockmeta.com

（二）区块链数据确认时间的问题

目前的区块链系统，尤其是金融区块链系统中，存在数据确认时间较长的问题。以比特币区块链为例，当前比特币交易的一次确认时间大约需要10分钟（图2-8），6次确认的情况下，需要等待约1小时。当然，对于信用卡动则2~3天的确认时间来说，比特币已经有了很大的进步，但距离理想状态仍有较大距离。

图2-8 比特币区块生产间隔

数据来源：区块元blockmeta.com。

（三）处理交易频率问题

区块链系统面临交易频率过低的问题。还是以比特币区块链为例，每条交易的平均大小约为250个字节（Byte），如果区块大小限制在1MB（兆），那么可以容纳的交易数量为4000条。按照每10分钟产生一个区块的速度计算，每天可以产生144个区块，也就是能容纳576000条交易，再除以每天的秒数86400，比特币区块链最高每秒处理6.67笔交易。目前，比特币区块链上每天的实际交易量已经接近系统"瓶颈"（图2-9），如果扩容问题得不到解决，可能造成大量交易的堵塞延迟。

图2-9 比特币区块平均交易数

数据来源：区块元blockmeta.com。

相比之下，Paypal在2013年第三季度的总体交易笔数为7.29亿笔，平均每秒为93.75笔交易。全球最大的支付卡VISA的官网信息显示，VisaNet（维萨网）在2013年的测试中，实现了每秒处理47000笔交易。比特币区块链比起支付宝等几大支付网络，从交易处理频率来看，更像是一个刚出生的婴儿。当然，这也是中本聪早期故意为之的设计。比特币区块大小被限制在1MB，以此避免"流氓"矿工的恶意行为，对人们造成不良的影响。比特币区块链支付网络之所以能够成长到如今价值数十亿美元，就在于它的去中心化。

（四）区块链发展受到现行制度的制约

一方面，区块链去中心、自治化的特性淡化了国家监管的概念，对现行体制带来了冲击。比如，以比特币为代表的数字货币不但对国家货币发行权构成挑战，还影响到货币政策的传导效果，削弱央行调控经济的能力，导致货币当局对数字货币的发展保持谨慎态度。另一方面，监管部门对这项新技术也缺乏充分的认识和预期，法律和制度创建可能会滞后，导致与运用区块链相关的经济活动缺乏必要的制度规范和法律保护，无形中加大了市场主体的风险。

（五）区块链技术与现有制度的整合成本较大

对于任何创新，现有机构都要保证既能创造经济效益，又要符合监管要求，还要与传统基础设施相衔接。特别是当部署一个新型基础系统时，耗费的时间、人力、物力成本都非常大，现有传统机构内部遇到的阻力也不小。

当然，问题的存在并不能阻碍区块链的发展步伐，诸如简单支付验证、侧链、闪电网络协议等技术的提出和深入研究，已经为上述问题的解决提出了思路。

参考资料

[1]http://www.jianshu.com/p/5e06fee80460

[2]http://www.zhihu.com/question/27687960/answer/70057319

[3]http://www.8btc.com/on-public-and-private-blockchains

[4]http://www.zhuihun.com/domainnews-20983-1-1.html

[5]http://www.wanhuajing.com/d342166

[6]http://www.zhihu.com/question/22369364/answer/21169413

[7]http://8btc.com/thread-540-1-1.html

[8]http://8btc.com/article-1882-1.html

[9]http://www.8btc.com/what-proof-of-stake-is-and-why-it-matters/

[10]http://www.8btc.com/fu0powpos http://www.8btc.com/nxt-whitepaper

[11]http://coinfeed.net/cn/information/bitshares/dpos授权股权证明机制白皮书.html

[12]http://www.8btc.com/blockchain-scalability

[13]http://toutiao.com/i6243674242018181634/

[15] 本章由海滨完成。海滨,布比公司技术专家、博士，在区块链技术、网络安全、数字货币等领域有非常深厚的技术积累。布比公司专注于区块链技术和产品的创新，已经拥有多项核心技术，开发了高可扩展高性能的区块链基础服务平台，具备快速构建上层应用业务的能力，满足数千万级用户规模的场景。

[16] 范捷,易乐天,舒继武.拜占庭系统技术研究综述［J］.软件学报, 2013（6）:12.

[17] 巴比特.比特币与拜占庭将军问题，http://www.8btc.com/baizhantingjiangjun.

第三章
区块链进阶[18]

一、简单支付验证（SPV）

简单支付验证（Simplified Payment Verification，简称SPV）是一种无须维护完整的区块链信息，只需要保存所有的区块头部信息即可进行支付验证的技术。该技术可以大大节省区块链支付验证用户的存储空间，减轻用户存储负担，降低区块链未来交易量剧增而给用户带来的压力。以比特币系统为例，节点只需保存所有区块头信息，即可进行交易支付验证。节点虽然不能独立验证交易，但能够从区块链其他节点获取交易验证的必要信息，从而完成交易支付验证，同时还可以得到整个区块链网络对交易的确认数。

要理解SPV的概念，首先需要理解如下两类概念的区别。

一是SPV与轻钱包（或瘦客户端）的区别。轻钱包指的是节点本地只保存与其自身相关的交易数据（尤其是可支配交易数据），但并不保存完整区块链信息的技术。SPV的目标是验证某个支付是否真实存在，并得到了多少个确认。比如爱丽丝（Alice）收到来自鲍伯（Bob）的一个通知，鲍伯声称已经从其账户中汇款一定数额的钱给了爱丽丝。如何快速验证该支付的真实性，是SPV的工作目标。轻钱包或瘦客户端的目标不仅是支付验证，而且是用于管理节点自身的资产收入、支付等信息。比如爱丽丝使用轻钱包或瘦客户端管理自身在区块链的收入信息、支出信息，在本地只保存与爱丽丝自身相关的交易数据，尤其是可支配交易数据。轻钱包与SPV的最大区别是，轻钱包节点仍需下载每个新区块的全部数据并进行解析，获取并本地存储与自身相关的交易数据，只是无须在本地保存全部数据而已。而SPV节点不需要下载新区块的全部数据，只需要保存区块头部信息即可。虽然轻钱包或瘦客户端中部分借鉴了SPV的理念，但和SPV是完全不同的。

二是区块链支付验证与区块链交易验证的区别。SPV指的是区块链支付验证，而不是区块链交易验证。这两种验证方式存在很大的区别。区块链交易验证的过程比较复杂，包括账户余额验证、双重支付判断等，通常由保存区块链完整信息的区块链验证节点来完成。而支付验证的过程比较简单，只是判断该笔支付交易是否已经得到了区块链节点共识验证，并得到了多少的确认数即可。还是以比特币系统为例，用户爱丽丝收到来自鲍伯的通知，鲍伯声称已经从其账户中汇款一定数额的钱给爱丽丝。爱丽丝进行交易验证的过程如下：首先，爱丽丝遍历完整的区块链账本，在区块链账本的交易中保存了鲍伯的历史交易信息（包括鲍伯的汇款账户、鲍伯的签名、历史收款人的地址以及汇款金额信息等），查询鲍伯的账户，就可以判断鲍伯提供的账户是否有足够的余额，如果余额不足则交易验证失败；其次，爱丽丝要根据区块链账本判断鲍伯是否已经支出了这个账户上的钱给别人，即是否存在双重支付问题，如果存在则交易验证失败；最后，判断鲍伯是否拥有其提供账户的支配权，如果判断失败则交易验证失败。而如果爱丽丝只是进行支付验证，则过程简单得多：通过SPV，爱丽丝可以进行支付快速验证，即检查此项支付交易是否已经被收录存储于区块链中，并得到了多少个确认数，就可以判断支付验证的合法性。详细的技术原理如下。

（一）SPV的技术原理

在区块链中，区块信息主要包括区块大小、区块头、交易数量和交易信息四部分内容。其中，区块头大小为固定字节，比如比特币中区块头的大小始终为80字节。区块头中一般包括如下信息：前一区块（也称父区块）的哈希值、区块中交易默克尔树的根哈希值、时间戳等。以比特币为例，其区块头的数据结构如表3-1所示。

表3-1 区块头的数据结构

通过区块的哈希值，可以识别出区块链中的对应区块。区块前后有序链接，每一个区块都可以通过其区块头的“前一区块的哈希值”字段引用前一区块。这样把每个区块均链接到各自前一区块的哈希值序列就创建了一条一直可以追溯到第一个区块（创世区块）的链条。前一区块的哈希值，可以确保区块链所记

录的交易次序。默克尔树的根哈希值则可以确保收录到区块中的所有交易的真实性。

区块链节点利用SPV对支付进行验证的工作原理如下：

①计算待验证支付的交易哈希值；

②节点从区块链网络上获取并存储最长链的所有区块头至本地；

③节点从区块链获取待验证支付对应的默克尔树哈希认证路径；

④根据哈希认证路径，计算默克尔树的根哈希值，将计算结果与本地区块头中的默克尔树的根哈希值进行比较，定位到包含待验证支付的区块；

⑤验证该区块的区块头是否已经包含在已知最长链中，如果包含则证明支付真实有效；

⑥根据该区块头所处的位置，确定该支付已经得到的确认数量。

上述方法可以减轻用户的负担。以比特币为例，无论未来的交易量多大，区块头的大小始终只有80字节，按照每小时6个的区块生成速度，每年产出52560个区块。当只保存区块头时，每年新增存储需求约为4兆字节，100年后累计的存储需求仅为400兆字节，即使用户使用的是最低端的设备，正常情况下也完全能够负载。

SPV的工作原理中，最为关键和复杂的是步骤③，节点从区块链获取待验证支付对应的默克尔树哈希认证路径的过程。例如，一个区块链节点想要知道其钱包中某个比特币地址即将到达的某笔支付，该节点会在节点间的通信链接上创建起布鲁姆过滤器，限制只接受含有目标比特币地址的交易。当节点探测到某交易符合布鲁姆过滤器的要求时，将以默克尔区块消息的形式发送该区块。默克尔区块消息包含区块头和一条连接目标交易与默克尔树根的默克尔哈希认证路径。默克尔树哈希认证路径是验证待验证支付是否存在于默克尔树的关键条件，该认证路径由默克尔树所有路径中节点的哈希值共同构成，自下而上进行哈希计算。节点能够使用该路径找到与该交易相关的区块，进而验证对应区块中该交易的有无。如图3-1所示为根据交易A、B、C、D、E、F、G、H生成的默克尔树。这是一棵自下而上通过哈希运算生成的二叉树。叶子节点为交易信息的哈希值，叶子节点两两进行哈希运算得到其父节点，继续此过程，直至生成默克尔树根节点。需要注意的是，如果存在单个叶子节点无法匹配成对，则用复制的方法构成完整的二叉树，比如图3-2中交易H不存在，则可以将交易G的哈希值M(G)复制一份替代M(H)，从而完成二叉树的生成过程。

图3-1 交易默克尔树结构示意图

图3-2 默克尔树哈希认证路径示意图

假设待验证交易为E，则交易E的默克尔树哈希认证路径为图3-2虚线框所示的M(F)、M(GH)和M(ABCD)。通过该哈希认证路径，即可以通过哈希计算找到一条链接交易E与默克尔树根的完整路径。

（二）SPV的功能扩展

虽然SPV可以高效地进行支付验证，但对于节点当前状态（账户余额、账户信息甚至合约状态等）均无法给出证明。SPV能否扩展并更进一步呢？以太坊对SPV的功能进行了扩展：每一个区块头，并非只包含一棵默克尔树，而是包含了三棵默克尔树，分别对应了三种对象——默克尔交易树、默克尔收据树和默克尔状态树。其中默克尔收据树和默克尔状态树是比特币等现有区块链系统没有的。默克尔收据树是由展示每一笔交易影响的数据条构成的默克尔树。而在默克尔状态树中，则保存账户信息、账户余额等信息。三棵默克尔树的功能分工如下。

①默克尔交易树：保存交易信息，用于验证交易是否真实包含于区块链中。

②默克尔收据树：保存某个地址的历史事件实例，比如一个交易是否成功执行、一个众筹合约是否完成了目标等。

③默克尔状态树：保存了账户名称、账户余额等信息。

基于上述三棵树，以太坊不仅可以实现SPV的支付验证，而且可以快速验证账户是否存在、了解账户余额甚至快速判断交易是否执行成功等信息，实现了良好的SPV扩展。

（三）SPV面临的问题

SPV面临的第一个是问题是SPV节点与区块链系统去中心化程度似乎存在一定的矛盾。随着SPV节点数量的增多，那么区块链参与完整验证的节点数量就会减少。然而，SPV却不能完全独立构成区块链。由于SPV节点没有存储完整的区块链信息，SPV的实现离不开存储区块链完整信息的节点或系统的辅助。

SPV面临的第二个问题是交易可锻性攻击[19]。由于SPV实现中一个关键步骤是根据支付哈希值定位其在区块中的位置，而该过程可能遭遇交易可锻性攻击。比如比特币系统中，交易可锻性攻击体现在交易ID（账号）可被伪造，而交易ID可被伪造的原因是比特币签名算法不够完善。以比特币为例，交易可锻性攻击的过程如下：在比特币的交易中，第三方交易系统会将交易发送方、接受方、交易金额等数据作为一个交易发送到比特币网络中，发送之前会对这条交易信息进行加密和签名，接着根据生成的签名最终获得一个哈希值，这个哈希值作为交易ID返回给提现的用户。一次交易请求过后，用户接收到的仅有一个交易ID，根据这个交易ID可以查看交易是否成功。当交易发送到比特币网络中后，网络中的各个节点会根据之前生成的签名来验证交易的真实性。问题就出在签名算法上：椭圆曲线数字签名ECDSA这个算法的一个问题是，修改签名的某个字节能够使签名依然校验成功，这样伪造签名之后交易依然能够成功进行。由于交易ID是根据签名生成的，而伪造之后的签名会生成一个完全不同的交易ID，第三方判断到两个ID不同便会确定当前交易失败，而事实上交易已经成功了。这时如果用户发现交易提示失败，可以再次发起交易，第三方交易系统一看之前交易确实失败了，那就会再进行一次交易。这时用户的比特币钱包里就会多收到一份比特币，也就造成了第三方交易平台资金损失。交易的可锻性体现在虽然交易签名被“锻造过”（即修改伪造过），但最终的交易依然有效。上述攻击对于SPV是有效的，因为在交易可锻性攻击场景中，伪造的交易和正常的交易都在区块链网络中，如果伪造的交易先被处理，那么攻击就成功。从而，SPV支付在区块链中的位置定位过程可能无法完成或出现错误，最终影响支付验证的进程和准确性。

有人提出可以通过改进SPV的工作流程来提升攻击防范的有效性，比如不再仅根据哈希值来判断支付的状态，而是使用双因素或者多因素验证，包括账户余额、支付信息追踪等来综合判断支付是否真正成功，但这会增加SPV的复杂度。如何更加有效地解决SPV面临的问题还值得进一步研究。

二、侧链

（一）侧链的起源

侧链（sidechains）实质上不是特指某个区块链，而是指遵守侧链协议的所有区块链，该词是相对于比特币主链来说的。侧链协议是指可以让比特币安全地从比特币主链转移到其他区块链，又可以从其他区块链安全地返回比特币主链的一种协议。

显然，只需符合侧链协议，所有现存的区块链，如以太坊、莱特币、暗网币等竞争区块链都可以成为侧链。元素链（Elements）就是这样一种侧链。所不同的是，它是由BlockStream公司，即提出侧链协议的公司开发的一个侧链的参考实现。

侧链协议具有重大意义。它意味着比特币不仅可以在比特币区块链上流通，还可以在其他区块链上流通，其应用范围和应用前景会更加广泛；有创意的人们会研发出各种各样的应用以侧链协议与比特币主链对接，使得比特币这种基准自由货币的地位更加牢固。

侧链协议的产生有以下几个原因。

1.应对其他区块链的创新威胁

以太坊（Ethereum）区块链、比特股（Bitshares）区块链后来居上，对比特币区块链产生相当大的威胁。智能合约和各种去中心化应用在以上两个区块链上兴起，受到人们的欢迎。而基于比特币的应用则因为开发难度大，项目不多。

2.比特币核心开发组不欢迎附生链

比特币区块链也有合约币（Counterparty）、万事达币（Mastercoin）和彩色币（ColoredCoin）等附生链，但是比特币核心开发组并不欢迎它们，觉得它们降低了比特币区块链的安全性。他们曾经一度把OP_RETURN的数据区减少到40字节，逼迫合约币开发团队改用其他方式在比特币交易中附带数据。

3.BlockStream商业化考虑

2014年7月以太坊众筹时，获得了价值1.4亿元人民币的比特币，还有20%的以太币，开发团队获得了巨大的回报。但是比特币核心开发组并没有因为他们的辛勤工作获得可观回报，因而他们成立了BlockStream，拟实现商业化价值。

基于以上三个原因，提出侧链协议、把比特币转出比特币区块链、另行开发二代区块链，这样的选择既能保证比特币区块链的安全，又能应对二代币的冲击，还能针对不同应用场景实现商业化，因而成了BlockStream的必然选择。

（二）侧链协议

侧链协议的目的是实现双向锚定（Two-way Peg），使比特币可以在主链和侧链中互转（图3-3）。

图3-3 比特币主链与侧链关系图

双向锚定分为以下几个阶段（图3-4）。

1.发送锁定交易，把比特币锁定在主链上

由比特币持有者操作，发送一个特殊交易，把比特币锁定在区块链上。

图3-4 双向锚定示意图

2.等待确认期

确认期的作用是等待锁定交易被更多区块确认，可防止假冒锁定交易和拒绝服务攻击，等待时间是1~2天。

3.在侧链上赎回比特币

确认期结束后，用户在侧链上创建一个交易花掉锁定交易的输出，并且提供一个SPV工作量证明，输出到自己在侧链上的地址中。该交易称为赎回交易，SPV工作量证明是指赎回交易所在区块的工作量证明。

4.等待一个竞争期

竞争期的作用是防止双重支付。在此期间，①赎回交易不会被打包到区块；②新传输到侧链的比特币不能使用；③如果有工作量更大的工作证明出现，即该赎回交易包括了比特币主链更大难度的SPV证明，则上一个赎回交易将被替换。

竞争期结束后，该赎回交易将被打包到区块中，用户可以使用自己的比特币。

从侧链转比特币到主链的过程也是如此。这就是侧链双向锚定协议。

（三）元素链

元素链是BlockStream实现的一个参考侧链，Alpha（阿尔发）版于2015年7月推出。元素链Alpha旨在演示技术并且提供测试环境，目前还未开发完成。作为一个与比特币测试网络相对接的侧链，元素链Alpha有可能被其他技术取代。

元素链Alpha是比特币测试链的一个侧链。它依赖可审计的联合签名者来管理传输到侧链的测试币（参见确定性锚定特性），并且以此来产生签名区块（参见签名区块特性）。这样做能快速探索侧链实施的可能性，考虑如何使用不同的安全措施。在未来版本中，升级协议接口以完全支持去中心化的侧链联合挖矿，最终达到完全双向锚定的目标。

元素链所包括的技术如下。

1.私密交易

元素链中最具创新意义的特性莫过于私密交易。私密交易中的金额仅有该交易的参与者知道（或者参与者指定的人），元素链以密码学算法保证不会多花币。比特币用地址来保证隐私，同时公开交易让别人验证；元素链在保护个人隐私上更进一步，隐藏了交易金额。金额隐藏的具体技术见下文。

私密交易最明显的一点是引入了一种新地址类型，称为私密地址。私密地址含了一个盲化因子，比普通比特币地址更长，这种地址在元素链Alpha版本中是默认地址。

2.隔离见证

Alpha版的交易中，签名从交易中分离出来。此举完全消除了任何已知形式的交易可塑性的威胁，并且允许有效的区块链剪枝。

在比特币中，交易包含转账信息（未花费交易集、地址和金额）和用于证明交易合法性的签名；对于隔离见证来说，交易ID仅由转账信息生成，区块中包含签名。这样做有如下好处：

①比特币有一些“正常化交易ID”的建议，隔离见证包含了这些建议。因为正常化交易ID机制在可塑性的输入后还要重写所依赖的交易，对高层协议如闪电网络来说是必要基础。

②交易ID不覆盖签名，以比BIP62更好的方式，避免了交易可塑性的所有形式，而后可以安全地使用更大尺寸的多语句智能合同。

③具有更有效提供SPV证明（用于轻钱包）的潜力，因为签名可以从交易中被省略而不破坏默克尔树结构。节点无须存贮或验证签名，可以把签名从磁盘中删除或无须在网络上传输它，以大幅度减少区块链存储容量和宽带要求。但在Alpha版本中，证明数据比比特币签名更占空间，因为还包含了大段的输出金额证明（因为使用了私密交易，隐藏了金额，因而要使用密码学证明以防止多花）。

3.相对锁定时间

为序列号赋予了新的意义，使已签名交易被确认后，其输入在一段特定时间内保持无效，目的是支持交易替换功能。

比特币每个交易都有个序列号，初始想法是相比低序列号，最高序列号应该最占优势，矿工应该更喜欢它，但这个想法从未真正实现。在假设矿工利益最大化的前提下，为了使得交易替换机制得以加强，新增一个操作码CHECKSEQUENCEVERIFY，用于比特币脚本检查序列号限制。

相对锁定时间与常规锁定时间用途一致，如时间锁定的担保服务等。但所指的“相对”会使以区块链为媒

介的应用更有意思。例如双向锚定阶段可描述为以交易开始的一个相对锁定时间条件，该交易声明了赎回证据。

4.Schnorr签名验证

元素链未使用ECDSA签名方案，而使用了同一曲线上的Schnorr签名方案。其好处如下。

①更有效的n/n阈值签名。多个Schnorr签名可以被合成一个签名，该签名对公钥的总和来说是有效的，所以任意大的n/n多签名只需用一个合签名就可以完成，同时可以被一个CHECKSIG操作所验证。

②更小的签名容量（64字节，而非71~72字节），没有DER编码问题。潜在支持批量验证（同时验证32个签名达到最高2倍加速），这需要知道R.y坐标（ECDSA忽略这个参数）和脚本级别，确保所有签名验证错误导致脚本运行错误（比如所有CHECKSIG操作与CHECKSIGVERIFY类似），以便提供更强的安全证明。

③能证明没有固有的签名可塑性问题。ECDSA有可塑性问题，并且不知道是否存在其他形式的可塑性问题。注意，分离证据使得签名可塑性不会导致交易可塑性。

④比ECDSA的签名和验证速度更快一点。

5.新操作码

元素链Alpha版本新增几个新脚本操作码。

①被禁用的操作码。比特币以前支持许多操作码，一些操作码在2010年因为安全考虑被禁用，需要硬分叉才能重新启用。Alpha版本重新启用了一些被禁用但是安全的操作码，如字符串连接和字串操作码，整数码移码和几个位操作码。

②DETERMINISTICRANDOM操作码：根据种子在一个范围内产生一个随机数。

③CHECKSIGFROMSTACK操作码：验证堆栈中对消息的签名，而不是验证对交易本身的签名。

这些新操作码有一些使用场景，包括双花保护债券、彩票、允许1/N多签名的默克尔树结构（N可为成千上万）、概率支付等。

6.金额隐藏技术

以下工作由亚当·拜克首次在Bitcointalk上的帖子《同态值比特币》中提出。

①佩德森的承诺。CT（密码学承诺）的基础密码学工具是佩德森的承诺。

承诺场景让你把一段数据作为私密保存，但是要承诺它，使你以后不能改变该数据。一个简单的承诺场景用哈希函数构建如下：

如果你仅告诉别人承诺，别人没法确定你承诺了什么数据。但你后来揭露了盲化因子和数据，别人可以运行该哈希函数来验证是否与你之前的承诺相匹配。盲化因子必须存在，否则别人可以试图猜测数据。如果你的数据比较少而简单，猜测成功的可能性比较大。

佩德森承诺与以上场景中的承诺类似，但是附加一个特性：承诺可以相加，多个承诺的总和等于数据总和的承诺（盲化因子的集合即盲化因子总和）：

换句话说，加法律和交换律适用于承诺。

我们用椭圆曲线点来构建具体的佩德森承诺（读者无须理解椭圆曲线密码学体系，把它当成黑盒行为来了解就可以了）。通常，ECC公钥由私钥x乘基点G生成。

结果保存为33字节的数组。ECC公钥遵守以前描述过的加法同态性：

(以上特性被BIP32分层确定性钱包用来允许第三方生成新的比特币地址。)

由于佩德森承诺的额外基点（称之H点）生成方法，因而没人知道H对G的离散对数（反之亦然），即没人知道x，且xG=H。我们使用G哈希来选择H：

这里to_point把输入当成椭圆曲线上某个点的x值，并且计算出y值。给定两个基点我们能构建如下承诺场景：

这里 x 是私密盲化因子， a 是我们要承诺的金额，你可以用加法交换律验证加法同态承诺场景中的相关关系。

佩德森承诺是信息理论上的隐私，你看到的所有承诺，总能找到一些盲化因子，可以和任意金额一起匹配该承诺。如果你的盲化因子是真随机，那么拥有无穷计算力的攻击者都不能分辨你承诺的金额。这种承诺无法被假冒，没法计算出任意其他能被验证的承诺。如果你做到，这就意味着你能找到两个基点相对于彼此的离散对数，意味着承诺椭圆曲线公钥体系被破解。

②佩德森承诺应用。

利用该工具，我们替换比特币交易中的8字节金额为32字节佩德森承诺。如果一个交易的发送人认真选择他们的盲化因子，以便正确相加,然后人们还能通过承诺相加为0来验证该交易。

以上公式需要明确的交易费用，在实际交易中，这点没有问题。生成承诺和承诺验证非常简单，不幸的是，如果没有附加的措施这个场景是不安全的。

问题在于该群是循环群。加法要mod P（一个256位的质数，用于定义群的秩），结果大数的加法会“溢出”，从而像个负数金额，因而当有些输出金额为负数时，承诺加起来为0的特点依然存在，导致可凭空创造5个比特币。

以上式子可以被解释成“有人花了2个比特币，得到-5个比特币和7个比特币”。为了防止产生这种情况，交易中有多输出的时候，我们必须证明每个承诺输出金额都在允许范围（如[0，2~64]）内且没有溢出。

我们可以公开金额和盲化因子，以便其他人能检查，但是这样一来就损失了所有隐私。因而，我们要证明承诺的金额在允许范围内，除此之外不透露任何信息。我们可以使用类似于Schoenmakers二元分解的技术来解决此问题，但是在此基础上进行了许多优化（包括不使用二元）。

我们从基本的EC签名开始，如果生成了一个签名，签名的消息是公钥的哈希，该签名证明签名者知道私钥，即公钥对于某些基点的离散对数。

对于一个类似公钥的P=xG+aH，因为基点H的存在，没有人知道P对于基点G的离散对数，因为没人知道x使得xG=H，除非a为0。如果a为0，则P=xG，离散对数恰好是x，有人会为该公钥签名。

把承诺当成公钥，对承诺的哈希值签名，通过这种方法，某个佩德森承诺可以被证明是对0值的承诺。在签名中使用公钥用于防止把签名设置成任意值并且破解出承诺。签名使用的私钥正是盲化因子。

更进一步，假定我想证明C是对金额1的承诺，但不告诉你盲化因子，你能做的就是计算：

然后向我要公钥C′的签名（相对于基点G的签名），如果我能做到，则C一定是对金额1的承诺（否则我就破解了EC离散对数的安全性）。

③环签名。

为了避免给出金额，我们还需要另一个密码学技术：环签名。环签名是当存在两个（或多个）公钥的签名场景时，签名证明签名者知道至少一个公钥的离散对数。使用环签名，我们可以构建另一个场景。我证明一个承诺是对金额0或金额1的承诺，我们叫这种场景为“或证明”。

首先，我给你C，你计算C′： C′ = C - 1H

然后我提供｛C,C′｝上的环签名。

如果C是对金额1的承诺，则我不知道它的离散对数，但是C′成为金额0的承诺，我知道它的离散对数（就是盲化因子）。如果C是对金额0的承诺，我知道它的离散对数；C′是对金额1的承诺时，我不知道离散对数。如果这是一个对任意其他金额的承诺，没有一个结果为金额0，因而我没法签名。

以上机制对任何数字对有效，只需把金额进行合适的预处理再放到环中，或者超过2个数字。

假定我想证明C在范围[0,32)之中，现在我们有一个或证明，想象我发送给你一个承诺集合，每个承诺都有个或证明：

C1 is 0 or 1C2 is 0 or 2C3 is 0 or 4C4 is 0 or 8C5 is 0 or 16

我为C1—C5选择了正确的盲化因子，能使得C1 + C2 + C3 + C4 + C5=C。我创建了一些有效的二进制数，和一个只能在区间[0,32）内的5位数。

众多优化手段可以让证明过程更有效。

首先，我们提出一个新的、更有效的环签名方法——Borromean环签名，它仅要求每个公钥32字节，再加上能被其他不同环所共享的32字节。与以前提出的构建方式相比，该环签名能达到两倍效率。

CT金额并非直接表述金额，而是使用十进制浮点数来表示，每个数字要与以10为基数的指数相乘，这意味着如果在基数10之前有较少重要数字，你能用小容量证据来证明大金额。比如：11.2345和0.0112345可以有相同大小的证明，即使两个数相差一千倍。

还有一个非隐私的发送“最小金额”。如果用户愿意泄露一些最小金额信息（最小金额信息将对外公开），那么就允许更小的证据覆盖更大范围的金额，并且当使用指数时还允许最小重要数字非零。用交易中第一个金额减少最小的金额，然后证明该值非负。

其次，浮点尾数用四进制编码而不用二进制，因为可以减少要发送的承诺的数值，使得签名数据大小与二进制相当。对最后的尾数数字的承诺可以跳过，从前向后对已经证明的金额创建承诺，其他数字也一样。

最后，通过在证明中小心使用非随机化签名，对于币的接收者（由于带接收者公钥的ECDH密钥协议，他与发送者共享一个私钥）来说，“重绕”证据并且用它提取发送者发送的消息是可能的。该消息大小为证据大小的80%。我们使用该原理向接收者提供金额和盲化因子，但是也可以用来存储编号或撤款地址等信息。

三、闪电网络

闪电网络（The Lightning Network）是一个去中心化的系统。闪电网络的卓越之处在于，无须信任对方以

及第三方即可实现实时的、海量的交易。

（一）闪电网络的起源

近年来，随着比特币的蓬勃发展，比特币交易数量越来越多，而单个区块体积有1MB的最大值限制，因此区块空余空间显得越来越小。如图3-5所示，区块体积中位数在2015年里得到了翻番，从1月的292KB（千字节）快速增长至12月的749KB。

图3-5 比特币区块体积大小

数据来源：区块元blockmeta.com

扩容问题在2015年得到了充分的重视与讨论，在2015年6月左右陆续推出了诸多扩容方案，代表有BIP100、BIP101、BIP102、BIP103、BIP109、BIP248等若干方案（见表3-2）。

表3-2 区块扩容方案表

虽然提出各种方案，但基本可以划分为两类：长期规则派与短期搁置派。长期派偏理想、规则型，一口气敲定便不再折腾，典型代表是BIP101/103，设定一个增长规则，便不再调整。短期派则认为未来不可预测，固定的规则过于简单暴力，希望设置一个短期数年方案暂时先避开，搁置至未来解决，代表为BIP100，但由于投票过程复杂，后简化为BIP102/109等，而BIP248则一口推迟至2020年，近几年就简单采取翻番增长。

自2015年6月至今，经过了大半年来大范围的反复讨论，目前长期规则派基本完败。2015年12月比特币香港扩容会议由Pieter Wuille提出了隔离见证（Segregated Witness）之后，扩容问题甚至已经简化为仅升级至2MB，但陷入了关于实施时间点的争论之中。

一个看似简单的扩容技术问题，却引发比特币社区花了大半年时间，开了数次全球技术会议、私下打了无数回口水仗，却依然未有明确定论。其背后深刻的原因是，区块限制值上调是无法真正解决比特币扩容问题的。

（二）扩容问题

总的来说，根据对比特币网络的理解，有两个划分：清算系统和现金系统。

1.清算系统

比特币区块链是全球的、分布式的、有限容量的且代价昂贵的系统。每一笔交易的价值含量是不一样的，当块容量不够用时，我们应该保障高价值的交易进块。高价值的交易有意愿、有能力支付足够高的网络手续费，从而获得足够高的优先级进块。

随着比特币的繁荣，交易数量会越来越大，有限的块容量会使低价值的交易（例如发送1分钱）永远无法进块，因为低价值的交易不可能支付高网络手续费。进而，网络退化为清算系统，低价值含量交易被赶出，这些交易由第三方记账系统进行代替完成。

在闪电网络出现之前，第三方记账系统主要是链外钱包提供商。用户信任某第三方钱包平台，把比特币存入其中，同一平台用户之间转账仅带来账户余额变更，并不会产生比特币交易。

2.现金系统

现金系统意味着所有交易均应该进入区块，那么当块容量不够用时，则应该及时调整块体积限制，对系统进行扩容。短时间可能发生交易入块堵塞，但长期来看所有交易应该均可以入块，人人都享有比特币

系统带来的巨大便利和优势。

3.扩容大小的选择

我们进行一个简单的估算，假设每个交易大小为512字节，手续费单位为0.0004/KB（见表3-3）。

表3-3 区块未扩容方案表

根据VISA在2015年的记录，全年共产生92064百万笔支付交易，折合比特币网络数据（见表3-4）。

表3-4 区块扩容方案表

若提高区块体积限制至30MB，最大的问题不是CPU计算能力瓶颈，而是块的传播与存储。

30MB的块可能会导致全网孤块率和空块率大幅上升，一年产出1.5TB的区块链数据也超出大部分节点机器的硬盘容量。基于这1.5TB的数据，区块链浏览器、钱包服务商等则可能膨胀10倍达到15TB。这对于目前来说，已经远超普通机器/数据库的磁盘容量。

诚然，这些数据对于中性化的系统而言，并不具有多么大的挑战性，但对于一个全球分布式系统而言，则非常具有挑战性，会极大削弱节点数量，提高开发接入门槛，使比特币变得中心化。

扩容争论的最后，还是倾向于2MB，使升级过程更加可控一些，风险更低一些。

（三）微支付信道

闪电网络在一片扩容的吵闹声中于2015年7月发出了首篇论文。在介绍闪电之前，我们先介绍一下微支付信道（Micro-Payments Channel）。

微支付信道概念于2012年首次被提出，是解决小额度、高频次支付场景的方案，目的在于缩减支付的交易数量，使高频、小额支付成为可能。下面我们先研究一下微支付信道的原理。

假设爱丽丝为消费者，鲍伯为一家视频网站。爱丽丝非常喜欢去鲍伯网站看电影，看一部电影需要支付0.1BTC（比特币），那么爱丽丝看了10部电影就需要支付10次0.1BTC，共计1BTC并发出10笔交易。而采用微支付信道就会缩减至两笔，或者说任何多次的交易均会缩减至两笔，只要总金额不超过存入信道的额度即可。

信道（Channel）的创建以及更新过程如下。

①爱丽丝支付1BTC至一个多重签名地址，签名采用2/2方式，我们把该交易称为FTX(Fund Tx)。爱丽丝生成该交易后，并不广播。

图3-6 微支付交易结构

②爱丽丝再构造一个赎回交易，称之为RTX(Refund Tx)。其输入为交易FTX的输出，输出为爱丽丝自己。同时，该交易有Locktime锁定期，所以N天之后才会生效，才可以进块。

③爱丽丝把构造好的空RTX给鲍伯，并让鲍伯进行签名。

④爱丽丝拿到带有鲍伯签名的交易RTX后，广播出FTX。此时的交易结构如图3-6所示，图中带有尖括号的签名表示待填入。

⑤爱丽丝再看了一部电影，那么她需要再支付0.1BTC给鲍伯。于是，爱丽丝构造另一笔交易PTX2：输

入依然是交易FTX；输出为两个地址，其中爱丽丝为0.8BTC，鲍伯为0.2BTC。爱丽丝对该交易签名，并将交易和她的签名给鲍伯（图3-7）。

⑥鲍伯可以随时签名并广播交易PTX2，当然，他依然可以广播交易PTX1。作为一名理性经济人，鲍伯必然总是广播自己收益最大的那笔交易，也就是当前的PTX2。在目前总是爱丽丝付款的情况下，鲍伯总是乐于广播最后一个交易。

⑦当鲍伯广播出最后一笔交易PTXn时，则意味着信道关闭，合作结束。鲍伯需要在交易RTX锁定期结束前关闭信道，否则意味着爱丽丝可以在交易RTX解锁后拿回她所有的币。

上述，就是微支付信道创建、更新与关闭过程。在一个完整的过程中，有且仅有两笔交易广播至链上，

同时双方均无须信任对方，任何一方也无法侵害另一方的利益。在更新过程中双方只是交换交易和签名数据，并无交易广播至链上，那么意味着在存入额度范围内，

图3-7 微支付交易广播收益最大化的那笔交易

可以创造出无数笔交易。不仅信道内的更新次数不受限制，频率也可以达到非常高，只要系统允许，目前硬件条件可以轻松达到每秒数千笔。

在特定场景下，微支付信道拥有着巨大优势，让小额高频支付成为可能。但它存在一个巨大制约：币在信道中的流向是单向的。在上述例子中，币仅能从爱丽丝流至鲍伯。

（四）闪电网络交易合约

微支付信道解决了合并交易的问题，但并没有解决撤销上个交易的问题，利用“理性经济人”和单向流动来达到撤销上个交易目的，并不是真正的撤销。若交易可以撤销，则币可双向流动。

闪电网络是基于微支付信道演进而来，创造性地设计出了两种类型的交易合约：序列到期可撤销合约RSMC（Revocable Sequence Maturity Contract），哈希时间锁定合约HTLC（Hashed Timelock Contract）。

RSMC解决了信道中币单向流动问题，HTLC解决了币跨节点传递的问题。这两个类型的交易组合构成了闪电网络。

1.RSMC创建

我们先来创建一个序列到期可撤销合约（RSMC）。爱丽丝和鲍伯是合作方，经常有比特币往来，所以他们决定各拿出0.5BTC放入信道中，便于业务往来。

RSMC交易结构（图3-8）的下方，左侧为爱丽丝的视角，右侧为鲍伯的视角。中间Funding Tx为共同可见；C1a和RD1a为爱丽丝持有；C1b和RD1b为鲍伯持有。交易图中带有尖括号的签名表示待填入。

图3-8 RSMC交易的结构图

①双方各拿出0.5BTC，构建Funding Tx，输出为爱丽丝和鲍伯的2/2多重签名。此时，Funding Tx未签名，更不广播。

②爱丽丝构造Commitment Tx：C1a和RD1a，并交给鲍伯签名。C1a的第一个输出为多重签名地址，爱丽丝的另一把私钥爱丽丝2和鲍伯的2/2多重签名，第二个输出为鲍伯0.5BTC。

③RD1a为C1a第一个输出的花费交易，输出给爱丽丝0.5BTC，但此类型交易带有sequence，作用是阻止当前交易进块，只有前向交易有1000个sequence确认时才能进块。

④鲍伯构造Commitment Tx：C1b和RD1b，并交给爱丽丝签名。结构与C1a、RD1a是对称关系。

⑤鲍伯对C1a和RD1a进行签名，并将签名给爱丽丝；同理，爱丽丝对C1b和RD1b签名，完成后给鲍伯。此时，由于并未对Funding Tx进行签名，任何一方均无法作恶，任何一方也不会有任何损失。

⑥双方均完成对Commitment Tx的签名并交换后，各自再对Funding Tx进行签名，并交换。此时，Funding Tx是完整的交易，广播之。

上述过程以及结构图的描述，就是创建RSMC的全部过程。

C1a和C1b两笔交易花费的是同一个输出，故他们两个交易只有一个能进块。若爱丽丝广播C1a，则鲍伯立即拿到0.5BTC（C1a的第二个输出），而爱丽丝需要等C1a得到1000个确认，才能通过RD1a的输出拿到0.5BTC。另一方，若鲍伯广播C1b，则爱丽丝立即拿到0.5BTC，鲍伯等待C1b得到1000个确认，才能通过RD1b拿到0.5BTC。也就是说，单方广播交易终止合约的那一方会延迟拿到币，而另一放则立即拿币。

2.交易更新

爱丽丝和鲍伯各自有0.5BTC的余额，此时爱丽丝从鲍伯处购买了一件商品，价格为0.1BTC，那么余额应该变为爱丽丝0.4BTC，鲍伯0.6BTC。于是创建新的Commitment Tx，对于爱丽丝来说是C2a和RD2a，对于鲍伯来说是C2b和RD2b，过程与上面类似（图3-9）。

图3-9 交易更新时的交易结构

此时两个状态均是有效的，那么最核心的问题来了：如何才能彻底废弃C1a和C1b呢？

RSMC采用了一个非常巧妙的方法：在C1a的第一个输出中，采用了爱丽丝2和鲍伯的多重签名，爱丽丝将爱丽丝2的私钥交给鲍伯，即表示爱丽丝放弃C1a，承认C2a（图3-10）。

图3-10 交易更新时的多重签名

爱丽丝交出爱丽丝2的私钥给鲍伯，那么鲍伯就可以修改RD1a的输出给他自己，形成新的交易BR1a。若爱丽丝破坏合约，在存在C2a的情况下依然广播出C1a，那么爱丽丝受到的惩罚就是失去她全部的币。爱丽丝交出爱丽丝2的私钥，或者对交易BR1a进行签名，两者是等同的，都是对C1a的放弃。

反之亦然，鲍伯交出鲍伯2的私钥给爱丽丝即意味放弃C1b，而仅能认可C2b。

引入sequence的目的是，阻止后续交易进块（RD1a），给出一个实施惩罚窗口期，当发现对方破坏合约时，可以有1000个块确认的时间去实施惩罚交易，即广播BR1a代替RD1a。若错过1000个块时间窗口，则无法再实施惩罚了（RD1a进块了）。

3.交易关闭

关闭RSMC，直接按照最终的余额构造出一个Commitment TX即可。例如，输出为爱丽丝0.1BTC，鲍伯0.9BTC，无需再设置多重签名，构造惩罚交易等。

4.中转交易

爱丽丝想要支付0.5BTC给鲍伯，但她并没有一个渠道来和他进行交易。幸运的是，她和查理有一个交易渠道，而查理正好和鲍伯有一个交易渠道。这样爱丽丝就能借助查理的交易渠道，通过哈希时间锁定合约（HTLC）来和鲍伯进行交易了（图3-11）。

图3-11 中转交易示意图

为了完成这次交易，爱丽丝就会给鲍伯发短信说：“嘿！我要给你付笔款。”这时鲍伯将收到一个随机数字（R），接着鲍伯便会回一个被哈希的数字（H）（你可以认为被哈希的数字H是随机数字R的一种加密形式）给爱丽丝。然后爱丽丝的钱包紧接着就会联系查理说：“嘿，查理。如果你给我生成（H）的未加密值（R），那么我就同意更新我们渠道的支付分配，这样你得到的就会比0.5BTC多一点，我得的比0.5BTC少一点。”尽管查理并不知道R，但他也会同意。之后查理便会去找鲍伯说：“嘿，鲍伯。如果你给我那个能生成H的未加密的值R，我将同意更新我们渠道的支付分配，这样你得到的会比0.5BTC多一点，我得到的比0.5BTC少一点。”

因为R就是从鲍伯这里生成的，所以他肯定知道。接着他马上将R告诉查理，并更新了其渠道的支付分配。然后查理将R告诉给了爱丽丝之后也更新他们的渠道，最后交易完成，爱丽丝以脱链的形式付给鲍伯0.5BTC。

5.总结

RSMC通过巧妙地设置Commitment TX的多重签名输出，以及sequence的延迟进块形成惩罚窗口期，解决了在微支付信道中的币单向流动问题。

（五）闪电网络面临的问题

闪电网络的最初设想为一个中心辐射型网络（图3-12）。你的钱包将会连接到一个“支付中转站”，由于各种支付渠道彼此之间都保持畅通，爱丽丝有一个和中转站A相通的渠道，而鲍伯也有一个和中转站B相通的渠道，爱丽丝只需通过一两个中转站的跳跃就能直接和鲍伯交易了。

图3-12 中心辐射型网络

如果能有成百上千个中转站（小额支付中心），那么这个网络拓扑结构就能完美运行。但是，若是只有少数几个大型中转站，那么这个网络的去中心化就会受到损害，变成另一个VISA卡、万事达卡或者美国运通。

1.中转站的中心化风险

要精确地预测出存在于网络均衡中的中转站的数量是完全不可能的，但是由于众所周知的马太效应，这个数字会逐渐变小，而不是变大。然而不可否认的是，在开源项目中，任何人都可以在上面运行一个支付中转站（至少在政府部门决定监管之前），只是支付中转站运行的高成本就像是给进入者们设置了一道坚固的壁垒，从而产生了中心化压力。

为什么创建支付中转站需要高成本？让我们回到查理扮演“交易中转站”的那个例子。回想一下，爱丽丝需要通过查理把比特币付给鲍伯，所以查理不得不在更新他和爱丽丝的分配渠道之前就更新他与鲍伯的分配渠道（付给鲍伯的多，自己得到的要少）。也就是说，查理在得到鲍伯的0.5BTC之前，就得先付钱给爱丽丝。

这意味着如果查理想要成为一个支付中转站，那他自己必须在与“客户”共有的渠道里存足够多的比特币，这样才能促成这些“客户”的脱链交易。如果查理没有预存至少0.5BTC到鲍伯的渠道里，那么这笔交易就不能做成。

现在，虽然查理仍保留这些比特币百分之百的控制权，但是这笔钱至少还是需要放在那些渠道里，以便促成那些链外支付，因而资金的沉淀成本非常高昂。所以，要运行一个支付中转站还是需要真金实银的投入，最起码在刚开始之前就需要准备足够的预存款。

那么，一个支付中转站应该给每个渠道存入多少预存款呢？如果一个比特币是500美元的话，那么你想要运行一个服务100人的支付中转站，需要50000美元的资产来启动它。

因此，如果某天闪电网络最终演变为中转站辐射型拓扑网络，那么中心化就是它最大的隐患。

2.点对点的路径交易

闪电网络是否有比中转站辐射型更好的模式？目前已经有很多规避支付中转站的设想，开发者尝试创造出更多去中心化、有组织的钱包对钱包的路径。

试想一下，如果爱丽丝想要买一杯咖啡，在此之前，她的钱包会用相同的技术在网络中通过其他节点找到一个路径来支付这杯咖啡。如果钱包找不到任何一个节点，那么它将与咖啡店打开一个新的支付渠道来完成这笔交易，然后留着这个渠道以便日后再用。理论上爱丽丝的钱包能够维持数十个开放的渠道。

如果有人每次在尝试支付时都不能找到一个渠道，那么新的渠道将会被打开，长此以往，用户间的一些有组织的渠道路径就会形成（图3-13）。

图3-13 点对点的路径交易示意图

从图3-13我们可以看到，爱丽丝在离开咖啡店后仍保持其支付渠道的开放。鲍伯最近去了咖啡店后也保持其支付渠道的开放，而且他还从商店里买了一条新领带，这个支付渠道也是处于开放状态。

在这个例子中，爱丽丝不仅可以将比特币以链外的形式给鲍伯，还可以通过已形成的有组织的路径将比特币付给商店老板。这可以解决闪电网络中心化的问题。但在具体应用中，很难找到从爱丽丝到商店并通过咖啡店和鲍伯的支付路径。

图3-14 点对点交易的支付路径

爱丽丝和鲍伯都要花0.011BTC来买一杯咖啡（约5美元），这就是为什么咖啡店在爱丽丝和鲍伯的渠道中都有0.011BTC（图3-14）。对爱丽丝来说，不管她是想把钱给鲍伯还是商店老板，咖啡店老板都需要更新他和鲍伯的支付分配渠道。咖啡店老板自己得到的少（从爱丽丝想要付的钱中），鲍伯从中得到的多。但是注意一下，咖啡店老板在和鲍伯的渠道中只有0.011BTC（约5美元），也就是说爱丽丝最多只能付给鲍伯或是商店老板5美元。如果她想要付更多的钱，那她就需要重新开一个渠道。

当人们以不同金额买不同的东西时，这种类型的数值不对称性就很有可能会频繁发生。从一个节点到另一个节点的路径很容易被找到，但是每一次找到正确数值的跳跃路径则是最困难的部分。

3.路径交易造成更多的链上交易

设想一下，要是爱丽丝的钱包不能从商店那里找到一条她想要数额的路径时，她是怎样打开一条新的渠道的。据估算，在给定的时间内你钱包中的比特币有绝大部分会留在渠道中。那么爱丽丝的钱包哪里还有比特币来和商店开一个新的渠道呢？好，如果它不得不关闭现存的渠道之一，那么当你的钱包在交易时不能找到一条路径的过程将是这样：①关闭现有的一条渠道完成链上交易。②和收款人打开一条新的渠道完成链上交易。

这两笔链上交易中还只有一笔付款，要是有一笔大交易无法找到一条路径（因此不得不关闭一个旧的渠道来打开一条新的渠道），很多的预存款都将被浪费掉。如果有超过50%的交易找不到路径，闪电网络实际上会促成更多的链上交易，而不是实时的链外交易。

4.路径交易时，发送者和接收者需要同时在线

人们即便是使用桌面上的钱包，也不会让它24小时都打开。他们在不用钱包的时候就会关闭程序，盖上笔记本电脑的盖子，关掉电脑等。除此之外，很多人的手机钱包都是休眠状态，不会时刻保持上线状态。因此，99%的预期用户都不会参与路径付款。

在哈希时间锁定合约（HTLC）的例子中，爱丽丝的钱包联系鲍伯的钱包，并问他要一个哈希化的随机数字（R）。鲍伯需要在线才能将那个数字给她。而在比特币目前的使用中，发送者和接收者是不需要同时在线的。

参考资料

[1]http://8btc.com/article-2002-1.html

[2]http://www.bitabc.com/?id=169

[3]http://www.8btc.com/merkling-in-ethereum

[4]http://8btc.com/thread-23806-1-8.html

[5]http://8btc.com/article-1790-1.html

[6] http://www.8btc.com/confidential

[7] http://www.8btc.com/elements

[8] https://www.elementsproject.org/elements/deterministic-pegs/

[9] https://www.elementsproject.org/sidechains.pdf

[10] https://github.com/ElementsProject

[11]https://github.com/Blockstream/borromean_paper/raw/master/borromean_draft_0.01_34241bb.pdf

[12] https://people.xiph.org/~greg/confidential_values.txt

[13] https://bitcointalk.org/index.php?topic=305791.0

[14] https://www.elementsproject.org/elements/relative-lock-time/

[18] 本章《简单支付验证》部分由海滨完成，《侧链》部分由申屠青春完成，《闪电网络》部分由潘志彪完成。

申屠青春，深圳银链科技CEO，深圳大学ATR国防科技重点实验室博士。

潘志彪，现任比特大陆软件研发总监，BTC.COM团队负责人。前币付宝CTO、联合创始人。中国比特币行业知名技术专家，曾就职于百度，当当等互联网公司，对于大数据处理、推荐系统、模式识别等有较为深入的研究。

[19] 交易可锻性（transaction malleability）攻击，又称交易延展性攻击。攻击者侦听比特币P2P网络中的交易，利用交易签名算法的特征修改原交易中的input签名，生成拥有一样input和output的新交易，然后广播到网络中形成双重支付。这样，原来的交易将有一定的概率不能被确认，造成不可预料的后果。

第四章
智能合约[20]

一、智能合约的起源

彼特·托德（Peter Todd）是比特币核心开发者之一。他总结了智能合约（Smart contract）的现状[21]，认为“智能合约讨论的结论是：没有人理解智能合约究竟是什么。如果我们要实施智能合约，应该需要预言机（oracles）”。

确实，要想阐明智能合约的理念和本质并非易事。

我们从智能合约理念的起源开始。“智能合约”概念由计算机科学家、加密大师尼克·萨博（Nick Szabo）于1993年左右提出来。1994年他写成了《智能合约》（Smart contracts）论文，是智能合约的开山之作[22]。

尼克·萨博对智能合约的阐述以一个自动售货机的例子开始。我们可以认为智能合约的原始祖先，是不起眼的自动售货机。在经过潜在的、损失有限的评估后，自动售货机使钱箱里的钱远远少于破坏者付出的代价。售货机根据显示的商品价格收取投币，通过一个简单的机制形成了最初的计算机设计科学，并且有限自动、根据投币金额传递变化和产品。自动售货机是一种搬运合约：任何持有硬币的人都可以与供应商交易。锁定钱箱和其他安全机制保护售货机储藏的硬币和货物不被破坏，从而支撑在各种各样的区域部署自动售货机，并且产生盈利。

在自动售货机概念的基础上，尼克·萨博给出智能合约的定义如下：

> “智能合约超越了自动售货机中嵌入各种有价属性的范畴，通过数字方式控制合约。智能合约涉及具有动态性、频繁主动执行属性的财产，且提供更好的观察和验证点，其中主动积极的措施必须丝毫不差。”

尼克·萨博告诉我们的是，智能合约本质上的抽象概念是在个人、机构和财产之间形成关系的一种公认工具，是一套形成关系和达成共识的协定。智能合约的条款（如抵押品、产权划分等）可以嵌入到处理硬件和软件中，以这样的方式使违约成本非常昂贵（甚至令人望而却步）。例如，为住屋而设计出的数字保障智能合约，根据智能合约设计策略，持续完善住屋抵押品协议以便其更充分地嵌入到处理合约条款中。根据合约条款，这些协议将使加密密钥完全控制在具有操作属性的人手中，而此人也将正当地拥有该住屋财产。最简单地，为了防止偷窃，使用者需要完成正确的解锁过程，否则住屋将切换至不可使用状态，比如门禁失效和设施失效等。在传统方式中，如果住屋被用做还贷，有一个令债权人头痛的问题是很难查收赖账的住屋，需要通过频繁沟通才能收回住屋钥匙等。为了解决这一问题，我们可以创建一个智能扣押权协议：如果物主不交费，智能合约调用扣押权协议，把住屋钥匙的控制权交给银行。该协议可能会比雇佣追债人更便宜、更有效。

同时，尼克·萨博提出了智能合约的三要素：

①一把可以允许业主同时排除非法第三方的锁；

②一个允许债权人秘密接入的后门；

③后门只在违约且没有付款的一段时间被打开；最后的电子支付完成后将永久地关闭后门。

从本质上讲，这些智能合约的工作原理类似于计算机程序的if-then语句。智能合约以这种方式与真实世界的财产进行交互。当一个预先定义的条件被触发时，智能合约就执行相应的合同条款。尼克·萨博关于智能合约的工作理论迟迟没有实现，是因为缺乏天生能够支持可编程合约的数字系统。如果金融机构仍然需要手动批准资产的转移，那么智能合约的目标就没有实现。瑞波实验室的市场和交易主管菲利·拉波波特（Phil Rapoport）说[23]，“实现智能合约的一大障碍是现在计算机程序不能真正地触发支付”。区块链技术的出现和被广泛使用，正在改变阻碍智能合约实现的现状，从而使尼克·萨博的理念有了实

现的机会。智能合约技术现在正创建在区块链基础之上，因为区块链本身就是一个计算机程序，智能合约能够与它进行交互，就像它能与其他程序进行交互一样。

在已提出智能合约理念的基础上，结合近几年区块链技术的不断发展，我们将试图给出对智能合约更为具体和详细的阐述。

二、智能合约的定义

智能合约是一套以数字形式定义的承诺，承诺控制着数字资产并包含了合约参与者约定的权利和义务，由计算机系统自动执行。

承诺定义了智能合约的本质和目的。以一个销售合约为例：卖家承诺发送货物，买家承诺支付合理的货款。数字形式意味着合约需要被写入计算机可执行的代码中，只要参与者达成协定，智能合约创建的权利和义务，就由一台计算机或者计算机网络执行。

我们举个简单的例子，形象化地描述智能合约。

If Event_X_Happened:

Send(爱丽丝, 1000$)

Else:

Send(鲍伯, 1000$)

意思是：如果事件X发生，则合约给爱丽丝发送1000美元；否则，给鲍伯发送1000美元。

这就是最简单的合约。

如图4-1所示是一个智能合约模型示意，其中各组成部分的定义如下。

①合约参与者：执行智能合约的相关参与者。

②合约资源集合：智能合约执行涉及的参与者资源，比如参与各方账户、拥有的数字财产等。

③自动状态机：智能合约下一步执行的关键，包括当前资源状态判断、下一步合约事务执行选择等。

④合约事务集合：智能合约的下一步动作或行为集合，控制着合约资产并对接收到的外界信息进行回应。

图4-1 智能合约模型示意图

智能合约程序不只是一个可以自动执行的计算机程序，它本身就是一个系统参与者，对接收到的信息进行回应，可以接收和储存价值，也可以向外发送信息和价值。这个程序就像一个可以被信任的人，可以临时保管资产，总是按照事先的规则执行操作。

智能合约的实现需要底层协议支持，选择哪个协议取决于许多因素，最重要的因素是在合约履行期间被交易资产的本质。再次以销售合约为例。假设参与者同意货款以比特币支付，选择的协议很明显将会是比特币协议。在此协议上，智能合约被实施。因此，合约必须要用到的数字形式就是比特币脚本语言。比特币脚本语言是一种非图灵完备的、命令式的、基于栈的编程语言。

三、智能合约与传统合约的区别

智能合约与传统合约（如法律合约）有相似之处，比如均需要明确合约参与者的权利、义务，违约方均会受到惩罚等。但是智能合约与传统合约存在着显著的区别，表4-1为两者的对比[24]。

表4-1 智能合约与传统合约对比

①自动化维度。智能合约可以自动判断触发条件，从而选择相应的下一步事务；而传统合约需要人工判断触发条件，在条件判断准确性、及时性等方面均不如智能合约。

②主客观维度。智能合约适合客观性请求的场景，传统合约适合主观性请求的场景。智能合约中的约定、抵押及惩罚需提前明确；而主观性判断指标很难纳入合约自动机中进行判断，也就很难指导合约事务的执行。

③成本维度。智能合约的执行成本低于传统合约，合约执行权利、义务条件被写入计算机程序中自动执行，在状态判断、奖惩执行、资产处置等方面均具有低成本优势。

④执行时间维度。智能合约属于事前预定、预防执行模式；而传统合约采用的是事后执行，根据状态决定奖惩的模式。

⑤违约惩罚维度。智能合约依赖于抵押品、保证金、数字财产等具有数字化属性的抵押资产，一旦违约，参与者的资产将遭受损失；而传统合约的违约惩罚主要依赖于刑罚，一旦违约，可以采用法律手段维权。

⑥适用范围维度。智能合约技术可全球采用，适用于全球范围；而传统合约受限于具体辖区，不同国际地区的法律、人文等因素均影响着传统合约的执行过程。

四、智能合约与区块链

（一）智能合约与区块链的关系

尼克·萨博关于智能合约的工作理论迟迟没有实现，一个重要原因是因为缺乏能够支持可编程合约的数字系统和技术。区块链技术的出现解决了该问题，不仅可以支持可编程合约，而且具有去中心化、不可篡改、过程透明可追踪等优点，天然适合于智能合约。因此，也可以说，智能合约是区块链技术的特性之一。

如果说区块链1.0是以比特币为代表，解决了货币和支付手段的去中心化问题，那么区块链2.0就是更宏观地对整个市场去中心化，利用区块链技术转换许多不同的数字资产而不仅仅是比特币，通过转换创建不同资产的价值。区块链技术的去中心化账本功能可以被用来创建、确认、转移各种不同类型的资产及合约。几乎所有类型的金融交易都可以被改造成在区块链上使用，包括股票、私募股权、众筹、债券和其他类型的金融衍生品如期货、期权等。

智能合约看上去就是一段计算机执行程序，满足可准确自动执行即可，那么为什么用传统的技术很难实现，而需要区块链技术等新技术呢？传统技术即使通过软件限制、性能优化等方法，也无法同时实现区块链的特性：一是数据无法删除、修改，只能新增，保证了历史的可追溯，同时作恶的成本将很高，因为其作恶行为将被永远记录；二是去中心化，避免了中心化因素的影响。

基于区块链技术的智能合约不仅可以发挥智能合约在成本效率方面的优势，而且可以避免恶意行为对合约正常执行的干扰。将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障存储、读取、执行整个过程透明可跟踪、不可篡改。同时，由区块链自带的共识算法构建出一套状态机系统，使智能合约能够高效地运行。

（二）智能合约工作原理

基于区块链的智能合约包括事务处理和保存的机制，以及一个完备的状态机，用于接受和处理各种智能合约，而且事务的保存和状态处理都在区块链上完成。事务主要包含需要发送的数据，而事件则是对这些数据的描述信息。事务及事件信息传入智能合约后，合约资源集合中的资源状态会被更新，进而触发

智能合约进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足，则由状态机根据缺省信息选择合约动作自动执行。

智能合约系统根据事件描述信息中包含的触发条件，当满足触发条件时，从智能合约自动发出缺省的数据资源，以及包括触发条件的事件；整个智能合约系统的核心就在于智能合约以事务和事件的方式经过智能合约模块的处理，输出还是一组事务和事件；智能合约只是一个事务处理模块和状态机构成的系统，它不产生智能合约，也不会修改智能合约；它的存在只是为了让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行。

基于区块链的智能合约构建及执行分为如下几步。

①多方用户共同参与制定一份智能合约。

②合约通过P2P网络扩散并存入区块链。

③区块链构建的智能合约自动执行。

步骤①“多方用户共同参与制定一份智能合约”的过程，包括如下步骤：

A.用户必须先注册成为区块链的用户，区块链返给用户一个公钥和私钥；公钥作为用户在区块链上的账户地址，私钥作为操作该账户的唯一钥匙。

B.两个以及两个以上的用户根据需要，共同商定了一份承诺，承诺中包含了双方的权利和义务；这些权利和义务以电子化的形式，编程机器语言；参与者分别用各自私钥进行签名，以确保合约的有效性。

C.签名后的智能合约，将会根据其中的承诺内容，传入区块链网络中。

步骤②“合约通过P2P网络扩散并存入区块链”的过程，包括如下步骤：

A.合约通过P2P的方式在区块链全网中扩散，每个节点都会收到一份；区块链中的验证节点会将收到的合约先保存到内存中，等待新一轮的共识时间，触发对该份合约的共识和处理。

B.共识时间到了，验证节点会把最近一段时间内保存的所有合约，一起打包成一个合约集合（set），并算出这个合约集合的Hash值，最后将这个合约集合的Hash值组装成一个区块结构，扩散到全网；其他验证节点收到这个区块结构后，会把里面包含的合约集合的Hash取出来，与自己保存的合约集合进行比较；同时发送一份自己认可的合约集合给其他的验证节点；通过这种多轮的发送和比较，所有的验证节点最终在规定的时间内对最新的合约集合达成一致。

C.最新达成的合约集合会以区块的形式扩散到全网，如图4-2所示。每个区块包含以下信息：当前区块的Hash值、前一区块的Hash值、达成共识时的时间戳以及其他描述信息；同时区块链最重要的信息是带有一组已经达成共识的合约集；收到合约集的节点，都会对每条合约进行验证，验证通过的合约才会最终写入区块链中，验证的内容主要是合约参与者的私钥签名是否与账户匹配。

图4-2 合约区块链示意图

步骤③“区块链构建的智能合约自动执行”的过程，包括如下步骤：

A.智能合约会定期检查自动机状态，逐条遍历每个合约内包含的状态机、事务以及触发条件；将条件满足的事务推送到待验证的队列中，等待共识；未满足触发条件的事务将继续存放在区块链上。

B.进入最新轮验证的事务，会扩散到每一个验证节点，与普通区块链交易或事务一样，验证节点首先进行签名验证，确保事务的有效性；验证通过的事务会进入待共识集合，等大多数验证节点达成共识后，事务会被成功执行并通知用户。

C.事务执行成功后，智能合约自带的状态机会判断所属合约的状态，当合约包括的所有事务都顺序执行完后，状态机会将合约的状态标记为完成，并从最新的区块中移除该合约；反之将标记为进行中，继续保存在最新的区块中等待下一轮处理，直到处理完毕；整个事务和状态的处理都由区块链底层内置的智能合约系统自动完成，全程透明、不可篡改。

五、智能合约应用案例

基于区块链的智能合约应用范围很广，应用案例数不胜数，以下仅仅列出一些典型应用。

（一）住屋租赁

假设用户爱丽丝（Alice）与用户鲍伯(Bob)需要构建一个区块链智能合约，目的是爱丽丝将其住屋租赁给鲍伯，租金为1000元一个月，每月支付，租期为一年。假设爱丽丝住屋门锁可通过互联网控制，其开锁密钥为Key（每月生成一次），爱丽丝的银行账户为MA，鲍伯的银行账户为MB。智能合约的执行包括如下步骤：

①爱丽丝与鲍伯提交合约构建申请给智能合约服务器，生成合约并由服务器发布到区块链生效。

②爱丽丝将Key以及MA提供给智能合约服务器。

③鲍伯通过MB向智能合约服务器支付1000×12=12000元的资金作为抵押，或者鲍伯通过第三方机构的担保，仅向智能合约服务器支付少量资金。

④合约开始执行，智能合约服务器将Key发送到鲍伯，并从鲍伯的抵押资金中扣除1000元，发送到爱丽丝的账户，并生成参与对象记录存入区块链。

⑤每个月智能合约都会定期检查，如果合约未到期，则继续从鲍伯的抵押资金中扣除1000元发送到爱丽丝的账户并发送Key给鲍伯，并生成参与对象记录存入区块链。

⑥整个过程受到第三方机构的监控，所有参与者、第三方机构都可以通过区块链查询合约执行情况。

⑦租约期限到后，智能合约服务器生成一条合约记录，标示合约终止并发布到区块链，合约执行即终止。

（二）差价合约

金融衍生品是智能合约最普遍也最易于用代码实现的应用之一。实现金融合约的主要挑战是其中大部分需要参照一个外部的权威价值发布器。例如，一个大需求应用是用来对冲密码学货币相对美元或欧元价格波动的智能合约，但该合约需要知道密码学货币相对美元或欧元的价格。最简单的方法是通过由某特定金融机构维护的数据提供合约进行，该合约的设计使该机构能够根据需要更新合约，并提供一个接口使其他合约能够通过发送一个消息给该合约以获取包含价格信息在内的回复，从而支撑智能合约的运行。根据前文描述的智能合约和示例，可以很容易地构建出差价智能合约，在此不再赘述合约内容。

（三）代币系统

基于智能合约的代币系统非常容易实现。其中的关键点是所有的货币或者代币系统，从根本上来说是一个带有如下操作的数据库：从A中减去X单位数据并把它加到B上。其前提条件是：

① A在交易之前至少有X单位数据。

②A批准了进行该交易。

实施一个代币系统就是把这样一个逻辑应用到一个合约中去即可。区块链上的代币系统应用不少，从美元资产到公司股票等。单独的代币具有智能资产、不可伪造的优惠券、与传统价值完全没有联系的积分奖励等多种形式。

（四）储蓄钱包

假设爱丽丝想确保资金安全，但担心资金丢失或者被黑客盗走私钥。于是，她把数字货币放到和鲍伯签订的一个合约里：

①爱丽丝单独一人每天最多可提取3%的资金。

②鲍伯单独一人每天最多可提取3%的资金，但爱丽丝可以用她的私钥创建一个交易取消鲍伯的提现权限。

③爱丽丝和鲍伯一起可以提取任意数额的资金。

正常情况下，每天3%的资金对爱丽丝而言足够了。如果爱丽丝想提现更多，她可以联系鲍伯寻求帮助。如果爱丽丝的私钥不幸被盗，她可以找到鲍伯把她的资金转移到一个新合同里。此外，如果爱丽丝弄丢了她的私钥，鲍伯也可以慢慢地把钱提出给爱丽丝。但是如果鲍伯表现出了恶意，爱丽丝可以关掉鲍伯的提现权限，从而保护自己的资金不受损失。

（五）作物保险

很容易且直观的，可以用天气情况作为数据输入创建一个金融衍生品作物保险合约，该合约不是由任何价格指数决定的。如果一个浙江的农民购买了一个基于浙江省的降雨情况进行反向赔付的金融衍生品，那么如果遇到干旱，该农民将自动地收到赔付资金；而如果有足量的降雨，即使没有赔付资金，他也会很开心，因为作物收成会良好。而上述过程利用智能合约可以很方便地实现。

（六）金融借贷

想想看，许多常规的金融交易，律师和银行的工作其实就是重复性地处理一些简单的任务。但是我们还不得不向律师提供的管理工作或者银行提供的抵押贷款工作支付大量的资金作为报酬。

智能合约能够使这些处理过程自动化和非神秘化，使普通人可以节省时间和金钱，而不用担心被骗。此外，假设你购买房产，可以通过一家银行获得抵押贷款，但通常不会持有长达三十年的贷款。银行只是成为你每月还款的处理者，向投资者支付大头资金，小部分资金用于交税，更小部分资金用于房主的保险。如果贷款还款由智能合约处理，那么贷款处理费用将被取消，省下来的钱可以返还给消费者。最终的结果就是使获得住屋所有权的成本更加低，有利于消费者。

（七）设立遗嘱

虽然智能合约仍然处于初始阶段，但是其潜力显而易见。想象一下分配立遗嘱者的遗产，决定谁得到多少遗产只需简单一列就可实现。如果开发出足够简单的用户交互界面，就能够解决设立遗嘱过程的许多法律难题。一旦智能合约确认触发条件，也就是立遗嘱者已经死亡，智能合约就将开始执行，立遗嘱者的财产将被分割。

（八）证券登记清算

智能合约状态可以包含证券所有权的所有信息。如果登记的证券所有者注意到该合约中证券已经出售给了其他的参与者，其他参与者就会把密码学货币发送到担保账户，然后证券登记信息就会更新，货币就会被转发给原来的证券持有者。无论哪个信息先到达，证券或货币都会保管在一个担保账户中，以避免双重使用。当交易取消或过时后，担保也将取消。以上过程利用智能合约可以轻易实现。

（九）博彩发行

假设对手同意某个在互联网能够访问的数据源，他们就可以对数据源的价值进行衍生合约或博彩。博彩发行方创建博彩信息，如中奖方式、投注方式、投注时间、奖池钱包地址及密钥，并向该奖池地址充值作为博彩奖池底金；发行方将博彩信息、钱包地址、奖池底金等信息生成博彩智能脚本，写入区块链，

被全网用户所知；用户获取博彩信息，开始投注，确定投注目标，并按照博彩规则向博彩钱包地址充值，产生投注记录（含自身钱包地址），写入区块链；产生中奖信息；中奖信息产生后，进行奖金发放以及颁奖记录发布。

六、智能合约面临的问题

智能合约，尤其是基于区块链的智能合约，目前还处在初级阶段，尚未有任何实质性突破和应用，同时也面临着问题与挑战：一是安全性问题；二是私密性问题；三是意外情景问题。同时，人们对智能合约还存在不少的误解。

（一）安全性问题

关键问题之一是安全性及信任度的问题。这与影响区块链实施的问题类似：智能合约系统都被设计成无须信任的环境，这意味着无法改正出现的错误。这是由区块链的不可逆特性决定的。例如，在区块链中，如果你将货币发送给某个地址，这个操作是无法撤销的。因此，如果你与诈骗犯进行交易或者你已经将货币发送到错误的地址中，那么很不幸，金钱损失是无法挽回的。在现实生活中，这些事情可以通过中心化的系统来撤销，但是在智能合约中不行。同样地，在合约代码的设计过程中也有欺诈的问题：某人需要设计（编程）合约，在合约设计时就会需要确保没有欺诈的问题发生。对于去中心化的系统，用户只能自己承担相应的风险。

（二）私密性问题

有效利用区块链的一大挑战就是区块链提供彻底的透明度。例如，如果十家银行联合在一起创建一个区块链，其中有两家进行了一项双向交易，这项交易将立即在区块链上对其他八家可见。虽然也可以设计缓解这个问题的各种策略，但目前还没有一种策略可以击败简单有效的中央数据库，除非能有一个可靠的管理员完全控制参与者的权限。

智能合约尤其是基于区块链的智能合约，同样存在这样的问题。每个智能合约都包含了自己的区块链数据库，并且具有完全控制能力。由于区块链数据库中所有的读写操作都是由合约代码主导的，所以其他合约无法直接读取其数据。尽管一个智能合约不能访问其他合约的数据，即一个智能合约无法读取其他合约的数据，但是其数据仍然存储在区块链中的每一个验证节点上。对于每个区块链的参与者来说，完全可以控制一个系统的存储器或者磁盘。如果他们想要从自己的系统中阅读信息，通过计算机手段，是完全可以做到的。

那么，把智能合约隐藏到网页数据中去，就像把它隐藏在代码里一样，是否就可以保证隐私了呢？当然，一般的用户不会看到它，因为它并未显示在他们的浏览器窗口。但是，只需要一个网页浏览器的“查看源文件”功能即可使得隐藏的信息变得普遍可见。同样，对于隐藏在智能合约中的数据，所需要的只是有人修改区块链软件显示合约的代码，就可以看到隐藏的内容。这种修改只要一个水平高的程序员花很短时间就可以办到。因此，智能合约的私密性问题目前还是存在的。

（三）意外情景问题

应当承认，在某一层面上，智能合约听起来确实像一个理想化的场景。如果你不付款，你的汽车将被远程自动收回，这一过程不需要任何人为干预。但是在理论上，智能合约有利的一面是将使金融机构更加乐意接受穷人带来的风险，再也不用担心穷人还不清贷款。如果没有智能合约，穷人可能得不到金融机构的贷款。因为，遇到最坏的情况，如果借贷人不能偿还贷款，那么收回资产对银行而言，是件轻而易举的事。除了增加获得金融机构贷款的机会外，智能合约也有潜力为没有优势的人打开其他壁垒较高行业的大门。没有智能合约，这些人就没有机会也没有可能获得收益。

尽管在理论上，智能合约听起来非常好，但如何正确、合适地处理意外场景下的合约执行，是一个问题。比如需要收回的汽车正在高速公路行驶的时候，撤销汽车的使用权操作将是十分粗鲁和危险的，而如何准确判断汽车的执行状态也是存在技术难点的。

（四）对智能合约的几种误解

1. 智能合约与协议合同一样

不是这样的。这在前文智能合约与传统合约的区别中已经详细介绍过。根据尼克·萨博对智能合约的定义，智能合约能够让违反协议的一方付出昂贵代价，是通过数字形式掌控现实世界的资产。所以，智能合约能通过执行实现一种特定的需求，能够证明某些条件是否获得满足。这些实现过程都会相当的严格，例如，如果你没能按时完成对一辆汽车的付款，汽车将会被智能合约数字锁定，直到完成支付才会解除。

2.智能合约具有法律效力

不是这样的。智能合约目前并不能等同于法律，但是它可以代表法律协议的一部分。另外，智能合约合法化工作目前正在进行当中。智能合约的执行结果可以用作审计、追踪，用来证明法定协议的条款是否可以被执行。

3.智能合约包括人工智能

不是这样的。智能合约本身并不是真的非常智能，也不能等同于人工智能。智能合约实际上是运行在区块链上的软件代码，由一些外部数据来触发智能合约，外部数据的接收、判断并非人工智能可以实现。此外，对智能合约中其余数据的修改也并非是通过人工智能来实现的。

4.智能合约只能为高水平软件开发者所用

不是这样的。虽然目前的确如此，但是我们很快就会看到与用户更加友好的方法或系统出现，允许商业或个人用户通过图形界面或者简单的文本语言输入来配置智能合约。相信在未来，不需要懂得编程，也能够制定自己的智能合约并顺利执行。

5.智能合约存在应用程序限定

不是这样的。如HTML、C++一样，应用程序受到编写人的控制，智能合约可以成为现实资产、数字资产、智能财产、物联网、通信网和金融工具相互联系的理想方式。智能合约几乎可以应用到所有状态随着时间而改变的事物，并不会受应用程序的限定，参与者类型也多种多样。

七、智能合约的未来展望

智能合约是区块链最重要的特性之一，也是区块链能够被称为颠覆性技术的主要原因，更是各国央行考虑使用区块链技术发行数字货币的重要考量因素，是可编程货币、可编程金融的技术基础。智能合约在今后可能会让人类社会结构产生重大变革，尽管智能合约还有一些需要解决的问题存在。幸运的是，智能合约技术已经从理论走向实践。全球众多专业计算机科学人才、金融界人才也在共同努力完善智能合约。

毋庸置疑，智能合约已经生根发芽了。智能合约是真正的全球经济的基本构件，任何人都可以接入到这一全球经济中，不需要事前审查和高昂的预付成本。在许多经济交易中，智能合约移除了对第三方的信任，在其他情况下，将信任转移到可以信任的人或机构中。智能合约意味着区块链交易远不止买卖货币这些交易，将会有更广泛的指令代码嵌入到区块链技术中。传统合约是指双方或者多方协议做或不做某事来换取某些物品，每一方都必须信任彼此，并须履行义务。而智能合约无须彼此信任，因为智能合约不仅是由代码进行定义的，也是由代码强制执行的，完全自动且无法干预。智能合约与传统合约本质上都是解决相同问题：以一种方式形成一种合约关系，使得承诺可以执行。只不过它们采用了不同的方法。就这一点而言，智能合约似乎是更好的解决方案，因为智能合约事前执行，不像传统合约一样，事后执行。多重签名智能合约也是未来的一个趋势，比如基于多重签名的交易合约，部分参与者的私钥就可以使用合约中的资金。甚至于，合约可以更加细化。比如参与者共有6人，那么其中的6把私钥里集齐5把就可以花全部资金，如果只有4把则每天最多花20%的资金，只有3把就只能每天花1%的资金等。

在这个蓬勃发展的智能合约领域，尤其是基于区块链的智能合约领域，尽管自动化、高效率和低成本的潜力巨大，但还是有明显的不足。现有区块链技术的一个缺陷就是，智能合约的代码需要向网络内所有参与者尤其是验证者公开。对于很多金融贸易、企业交易来说，这是个巨大的缺陷。因为这就意味着资金投入之后，网络中非参与者可能会了解并积极参与贸易中并给参与者带来麻烦。这同时意味着区块链智能合约的非参与者可以囤积或出售资产，这将损害参与者的利益。此外，尽管智能合约可能给金融服务业带来最具颠覆性的改变，就如同曾经的计算机数据处理带来的变革一样。但是，在实现这个目标之前，我们首先需要清除一些障碍。幸运的是，自区块链技术出现和取得突破之后，智能合约技术已经离开学术的殿堂并走进了社会生活。全球成千上万的互联网金融人才正致力于扩大合约创新的规模，为现代金融机构提供便利。

智能合约的发展可能需要经历漫长的道路，但是更多的智能合约机制正在被设计出来，更多领域的人才正在加入。目前为止，对来自截然不同的领域，如经济学、密码学、网络科学、金融学的自动化合约执行来说，共同设计研究合约准则是必经之路。如果缺少交叉沟通，无论是对技术的缺乏还是对商业用途模式意识的缺乏，都将造成智能合约的低效。

目前Orisi、Codius、Symboint、Hedgy、BitHalo、Mirror、Hyperledger、Eris Industries、Ethereum、智能坊、小蚁、Colored Coin、IBM等已经致力于智能合约的平台开发及相关研究，相信智能合约的应用前景一片光明。

参考资料

[1]http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app

[2]https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad

[3] http://www.wtoutiao.com/p/14dyEMP.html

[4]http://www.coindesk.com/smart-contract-myths-blockchain/

[5]http://8btc.com/article-1921-1.html

[6]http://wangxiaoming.com/blog/2016/03/03/blockchain-2-0-he-yue/

[7]http://blockchain.hk/smartcontract/

[8]Vitalik在中国台湾的演讲：区块链、智能合约和以太坊

[20] 本章由海滨写作完成。

[21] https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad.

[22] http://szabo.best.vwh.net/smart_contracts_idea.html.

[23] http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app.

[24] http://8btc.com/doc-view-376.html.

第五章
区块链怎么玩[25]

[25] 本章由达鸿飞写作完成。达鸿飞,小蚁创始人，昵称“达叔”，现居上海。中国区块链社区的代表人物，上海浦东国际金融学会金融科技组委员。2013年起全职从事数字货币和区块链技术创新，联合创立了“比特创业营”，多次在北京、中国香港等地的数字货币峰会担任演讲嘉宾。

一、数字货币

（一）总量恒定型：比特币

尽管区块链的倡导者们有意把区块链技术作为一种中性的独立技术从比特币中抽离出来，但不可否认，比特币是第一个初步成功并引起广泛关注的区块链应用。它在发行机制、分配机制、币值调节机制上有不少创新。中本聪将比特币定义为一种点对点的电子现金系统，“电子现金”一词表明他想要发明的并不仅仅是一个支付系统，而是一套有着独立货币哲学的货币系统。

比特币最常被人提及的特性就是总量恒定。比特币的最高上限为2100万个。在2009年初比特币网络开始运行的最初几分钟内，比特币的数量为零。当大约10分钟过去后，第一个区块产生了，生产出这个区块的矿工也就获得了50个比特币的奖励。这50个比特币就是世界上产生的第一批比特币。通过查询历史数据，我们可以看到最早的这个区块，也就是说区块0的详细信息（见表5-1）。

表5-1 创世区块详细信息

数据来源：区块元blockmeta.com

可以发现，这个区块产生于2009年1月4日，仅包含了1笔交易，就是那笔“无中生有”新生成出来的50个比特币。在每个区块里，这些新生成的比特币被称作“区块奖励”。由于当时只有中本聪一个人在运行比特币网络，毫无疑问这个区块的产生者就是中本聪本人，这50个比特币的区块奖励也在中本聪的控制下。而迄今为止，这50个比特币都还静静地躺在这个地址里，一次也没有被花费过。

区块奖励并不是一成不变的，每隔4年，区块奖励就会减半。也就是说，2009年开始时，区块奖励是每个块50个比特币，而到2013年，区块奖励就会减半为25个；到2017年，区块链奖励就会再次减半为12.5个；以此类推，直至2100万个比特币分发完毕。这就是比特币的发行机制。图5-1描述了比特币的发行曲线。尽管2030年左右比特币就能达到2000万的发行量，但是要到2140年左右才会达到最终2100万的发行总量。

图5-1 比特币发行曲线

比特币通过将新产生的币作为区块奖励分配给矿工（区块生产者）的方式完成整个发行过程。这一过程的最主要特点有三个。

一是发行有严格的既定规则，任何人都没有权利修改这些规则，进行规则外的增发。这一约定和经济学家、诺贝尔获得者弗里德曼的观点非常接近。弗里德曼认为，根治通货膨胀的唯一出路是减少政府对经济的干预，控制货币增长。控制货币增长的方法是实行“单一规则”，即中央银行在制定和执行货币政策的时候要“公开宣布并长期采用一个固定不变的货币供应增长率”。

二是发行的主体是不特定的，任何人只要打开运算设备（不管是矿机还是普通计算机）都可以参与到挖矿也就是说货币的发行过程中。这个特点体现了“去中心化”的精神，只要拥有算力，任何人都可参与而不取决于参与者的身份、地位。

三是存在真实的发行成本，该成本主要包括购买矿机的成本和运行矿机的成本。这些成本的存在“赋予”了比特币某种价值。从经济学角度看，决定价格的并非成本，而应该是市场供需关系。你可以花费

数亿美元的成本把一块蛋糕发射到火星之上，但这块蛋糕并不会因此获得数亿美元的身价（如果没有既足够有钱又足够疯狂的疯子的话）。但是不可否认，成本的存在给了市场一个极强的心理预期信号。成本就像是一张比特币市场价格的安全网。回顾比特币的历史价格，每当触及成本时，总会快速迎来反弹。比特币的这种需要成本的发行机制是对布雷顿森林体系瓦解后世界各国无须成本就能发行所谓“信用货币”的一种反讽。

从发行需要成本，发行依照收敛性曲线这些特性来看，比特币仿真的恰好是黄金这种贵金属。和比特币类似，黄金的总量有限，开采需要一定成本。然后，比特币可以跨地域转移、几乎可无限分割、可编程、易保管等特性确实可以完胜黄金这种几千年来人类世界共通的价值存储手段。

然而正因为仿真了黄金的种种属性，比特币也就具备了黄金作为货币时体现出的种种缺点。例如在现阶段，比特币更多地被用作一种投资投机商品，而非货币，导致其价格往往大幅度波动（图5-2），暴涨暴跌阻碍了其成为一种通用的货币。即便我们假设比特币成为一种通用货币，由于总量固定，发行速率既定，比特币无法根据市场的供需而调整货币供应量，也会导致比特币成为一个糟糕的计价单位。当经济发展和财富增长时，以比特币计价的商品的比特币标价反而会持续下跌，物价越来越低。如果这也不是太大的问题的话，更糟糕的是员工的工资可能每半年就要降薪一次，用比特币计价的GDP数据可能是永远停滞不变的，国家可能要提高其他税收来弥补铸币税的消失。人类对价格数字的直觉和数千年积累的经济知识体系恐怕很难适应和跟上这样的变化。

图5-2 比特币市场汇率历史走势图

数据来源：区块元blockmeta.com

（二）锚定型：比特股

非弹性供给的货币会导致币值不稳定，而难以成为一般经济计量单位。如何创造一种能够保持币值相对稳定的货币，一直是数字货币社区的热门话题。这种稳定货币如果被发明，那么基于数字货币的支付结算将会变得非常简单易用。

比特股就是这样一个试图解决这个问题的、基于区块链技术的系统。比特股设计了一套发行“比特资产”的机制。比特资产是一个总称，具体的资产可以是比特美元、比特人民币、比特黄金等。比特股的创始人丹尼尔·拉姆（Daniel Larimer）认为通过其设计的去中心化的发行和交易，各种比特资产将能够锚定各自对应的标的物，实现币值的稳定。比如，比特美元将能够锚定美元的价值，使1比特美元总是等于1美元的购买力。那么具体机制是怎么实现的呢？我们看看比特股维基上的一段描述。

> 市场锚定指的是比特资产和真实世界中对应的资产在价值上如何保持相等或相近的一种机制。比特股通过提高预测市场的准确度和效率创建一套全新的加密资产，从而锚定如美元、黄金、石油或者任何其他的任何资产。这些资产被称为比特资产（如比特美元、比特黄金、比特石油等）。比特美元是一种在比特股块链上内建交易所交易的数字资产。比特美元跟踪的是真实美元相对于比特股的价值。这种跟踪机制是通过交易行为来确立的，市场上的交易者都预期着比特美元锚定真实美元，这种预期会使他们的交易增强预期的效果。当交易者看到比特股相对美元升值时候，他们会使用更低的以比特股计价的美元的价格来买入美元，因为他们预期着卖出者会用更低的价格抛售。

这种市场锚定基于下面的具体机制。

首先，比特股系统中内置了一种同样名为比特股（简称BTS）的数字货币。BTS的币值和其他数字货币一样是具有高度波动性的。我们可以设计一种机制，用BTS作抵押发行一种新资产，并把这种资产分为A份额和B份额，A份额保持币值的稳定，而由B份额的持有者吸收所有的波动。A份额持有人的收益是获得了稳定的币值，可以用于定价、支付、价值存储；B份额持有人的收益是获得了杠杆，因为其吸收的是A+B整体的价格波动。天底下当然没有免费的午餐。A份额获得稳定币值的交换条件是丧失了BTS币值上涨时的收益权，B份额获得杠杆的交换条件是BTS币值下跌时蒙受的加倍损失。当B份额的市值已

经临近临界点，将要不足以覆盖整体波动时，B份额将被平仓。在这里，稳定的A份额就是前文所描述的能够锚定现实资产的“比特资产”。

这样的设计非常类似中国证券市场上的分级基金。但两者的本质区别在于，比特股的设计中，包含A、B份额的类似“分级基金”的发行权是由完全去中心化的市场完成的。任何持有BTS的用户，只要能在市场上找到交易对手方，就能够抵押BTS发行出比特美元、比特人民币、比特黄金这样的比特资产。事实上，用户甚至可以自己和自己成交，发行出A和B份额，然后留下自己想持有的部分，将另一部分通过市场转让出去。在这种设计下，货币的发行权成为一种纯粹的市场行为，因此比特股创始人丹尼尔·拉姆也就把这样的机制称为“去中心化的央行”。

但是这里还存在一个问题，即A份额相对于什么而言比较稳定。通过同样的抵押机制生成的比特资产为什么有的能锚定美元，有的就能锚定石油？

比特股给出的答案很简单：“仅仅因为名字不同。”当一种比特资产被命名为比特美元时，所有发行、交易的市场参与者都会判断市场中的其他交易者对这种比特美元的价值判断，而其中最合理的假设就是市场中的其他参与者也会认为比特美元的价值应当锚定美元。因此，当比特美元币值高于美元时，会有人抛出获利，当比特美元币值低于美元时，会有人买入等待恢复1：1时获利。这一机制乍听起来似乎纯属臆想，但如果你读过经济学博弈理论就会知道，这是另一个经济学诺贝尔奖获得者托马斯·谢林于1960年在《冲突的策略》中提出的一个后来以其名字命名的著名概念——谢林点。谢林是这样阐述的：

> 假设明天你要在纽约跟一个陌生人见面，你会选择什么时间和什么地点？这是一个协调博弈问题，其中任何时间、任何地点都平等。谢林询问了一些学生，发现绝大多数的回答是“中午在纽约中央车站”。没有什么因素使“纽约中央车站”成为更好的地点（任何一个酒吧，或者图书馆阅读室都可以用于约定见面），但纽约的文化传统提高了中央车站的保险系数，从而使其成为一个自然的“谢林点”。

在比特资产的例子中，比特美元的谢林点就是美元，比特石油的谢林点就是石油。仅仅是一个名字的不同，在充分市场博弈的情况下，就真的能够各自锚定相对应的实体资产价格！

尽管在理论上，比特股的这套机制是比较合理的。但在实践中，比特资产的锚定还是碰到了不少的问题。首先，比特股的锚定机制相当复杂，用户首先需要在交易所买到BTS，然后通过比特股的客户端才能发行比特资产。发行过程相当复杂，涉及挂单、平仓、卖空、杠杆等很多复杂的类金融衍生品的概念，普通用户只能敬而远之。

其次，所有比特资产的价值都来自发行时被抵押的BTS的价值。BTS本身的流动性并不太好，因此就容易发生价格波动。而BTS一旦价格波动，就可能会影响到前文所述的高波动的B份额，引发对B份额的平仓，即将B份额所抵押的BTS卖出。这样一来又会造成BTS的价格下跌，引发更多的B份额被平仓。因此，比特股不得不设计了一种熔断机制来进行保护，但熔断也会造成比特资产的价格锚定不准确。

最后，在不同的市场环境下，用户对A、B份额的持有愿望是不同的。市场纷纷预期BTS上涨的过程中，用户倾向于持有B份额；下跌时，则更愿意持有A份额。如果不设计额外的机制来调整A、B份额的动态激励，那么就很容易导致大量比特资产被用户主动平仓，造成比特资产短缺，而不能适应市场需求。

归根结底，由于BTS只是一种虚拟财产，其市场深度和流动性明显不足。以BTS的价值抵押发行比特美元、比特人民币作为一般货币的设计在实践中碰到了较大的问题，难以实现其创始人最初“去中心化央行”的宏大愿景。

（三）政府发行型：央行数字货币

2016年1月20日，来自中国人民银行的一则新闻轰动了笔者的朋友圈，其标题看似非常普通——《中国人民银行数字货币研讨会在北京召开》，然而它的内容却是轰动性的，文中明确指出：

> 在我国当前经济新常态下，探索央行发行数字货币具有积极的现实意义和深远的历史意义。发行数字货币可以降低传统纸币发行、流通的高昂成本，提升经济交

> 易活动的便利性和透明度，减少洗钱、逃漏税等违法犯罪行为，提升央行对货币供给和货币流通的控制力，更好地支持经济和社会发展，助力普惠金融的全面实现。未来，数字货币发行、流通体系的创建还有助于我国建设全新的金融基础设施，进一步完善我国支付体系，提升支付清算效率，推动经济提质增效升级。

会议要求，人民银行数字货币研究团队要积极吸收国内外数字货币研究的重要成果和实践经验，在前期工作基础上继续推进，创建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。

关于我国央行是否会考虑将区块链技术用于央行数字货币的问题，周小川行长如是说：

> “数字货币的技术路线可分为基于账户（account-based）和基于钱包（wallet-based）两种，也可分层并用而设法共存。区块链技术是一项可选的技术，其特点是分布式簿记、不基于账户，而且无法篡改。如果数字货币重点强调保护个人隐私，可选用区块链技术。人民银行部署了重要力量研究探讨区块链应用技术，但是到目前为止区块链占用资源还是太多，不管是计算资源还是存储资源，应对不了现在的交易规模，未来能不能解决，还要看。”

周小川行长所说的基于账户和基于钱包的概念，实质系指基于服务器的电子货币和基于私钥的加密货币。前者即普通电子货币，账户所有权并不真正属于用户，而是托管于服务器之上。后者即以比特币为代表的加密货币，用户拥有账户的绝对专属权，不仅可以用自己的密钥打开，还可以通过智能合约授权别人拿密钥打开，账户的控制权归根结底在用户端，商业银行也未必有权打开。

英国央行也正在全面探索区块链技术，数字货币被纳入了英国央行在未来一年的研究重点。英国央行货币政策二把手本·布劳德本特（Ben Broadbent）曾在一次讲话中指出：比特币可能无法得到广泛应用，但由央行发行的数字货币可能对全球金融体系产生巨大影响。“去中心化的虚拟票据交易所和资产登记处”可能会是这项技术更好的探索之路。

澳大利亚央行也是探索数字货币和区块链技术的先行者。澳大利亚储备银行（Reserve Bank of Australia）支付政策部门主管托尼·理乍得（Tony Richards）就建议，在将来某个时间澳元应该转换成数字货币形式。他特别指出：“可行的方案是由中央银行发行货币，再由授权机构监管货币交易和流通，当然现有的金融机构可能会参与其中。”

各国央行发行数字货币的出发点很简单。首先，纸钞的流通成本太高。据美国零售商和银行估计，持有实物美元的年均成本在60亿美元左右，其中包括会计、储存、运输和安全成本。纸钞逐渐退出交易已经是大势所趋。一旦纸钞退出交易，那么央行就和货币的使用者切断了所有的直接联系，用户使用的不再是央行直接发行的货币，而是银行、第三方支付所发行的IOU（欠条），央行的货币政策将更难被传导至市场。其次，日本和北欧国家央行已经在实施所谓的负利率，然而负利率只能传导到金融机构而无法传导至个人。因为一旦在个人层面实施负利率，那么个人的第一反应就是从银行提取现钞，那就会造成全国范围的挤兑和银行业危机。相反，如果现钞退出市场交易，央行就可以更好地实施包括负利率在内的货币政策，从而更强地影响市场。这也是荷兰央行用DNBCoin、英国银行用RSCoin进行数字法币概念验证的出发点。

二、支付汇兑

关于货币的定义，学过政治经济学的朋友恐怕对这句话都耳熟能详，“货币具有价值尺度、流通手段、贮藏手段、支付手段和世界货币五种基本职能”。实际上后两者是前面三种手段的派生。现代经济学著作中，一般认为货币的本质只有三个，即交换媒介（medium of exchange）、价值存储（store of value）和计价单位（unit of account）。然而比特币的出现挑战了这一货币定义。即便在比特币白皮书发表七年后的今天，比特币的波动仍然较大，至少和有一定波动率的单只股票相当。而价值存储和计价单位这两个货币职能都要求货币的币值相对稳定。但是，比特币却切切实实可以被用作交换媒介来完成支付，特别是跨境的支付。

假如你想购买一个美国互联网公司的云计算服务，需要支付100美元，而你既没有信用卡也不愿去银行

办理国际电汇，要怎么办呢？你可以：

①在中国的比特币交易所花大约650元人民币买入价值100美元的比特币；

②将这些比特币立即提出，并转入美国的比特币交易所；

③将这些比特币卖出并获得100美元，将这100美元提现至上述云计算公司的收款账户。

由于比特币本身良好的全球流动性，在这里很好地起到了交换媒介的作用。由于在整个流程中，用户持有比特币的时间一般不超过1小时，也就无需承受太大的波动风险。这里的比特币已经部分起到了货币的作用，但又仅仅作为交换媒介，而非价值存储和计价单位。

在支付汇兑这一领域，目前领先的有BitPay、Circle、Coinbase这三家公司。它们都想通过比特币网络创建起一个类似VISA/万事达的全球支付网络。BitPay选择了面向商家，直接提供支付处理服务，而Circle、Coinbase选择了面向消费者提供钱包和买卖服务。

BitPay进入最早，成立于2011年。2014年5月，BitPay获得了当时数字货币领域最大的一笔投资——3000万美元的A轮融资，公司整体估值也达到了1.6亿美元。BitPay的早期投资人中还包括了香港亿万富翁李嘉诚的Horizons Ventures（维港投资）。时至今日，BitPay的客户已经包括微软、PayPal等知名公司。

BitPay为商家提供接受比特币付款的服务，并实时生成以比特币计价的价格。回到上面的100美元的收款例子，如果这家公司接入了BitPay，那么用户会发现多出一个用比特币支付的选项，并且此时的比特币计价的价格会每15分钟按照比特币的市价发生变化。用户可以直接用已有的比特币支付，没有的话就自行在交易所购买。对商家来说，可以直接把收到的比特币保存，也可以要求BitPay及时按照市价帮他卖出，而直接获得100美元。

那么为什么BitPay不提供完整的三步服务？原因在于监管。美国有严格的金融监管制度，BitPay在现有的服务模式下，其需要的金融牌照较少。如果提供完整的三步服务，那么就要面临严格的反洗钱、KYC（了解你的客户），甚至是KYCC（了解你的客户的客户）等监管挑战。由于美国是联邦制国家，在美国50个州申请一遍金融牌照可不是“好玩”的。不是财大气粗的公司，根本玩不起这个游戏。最近一轮融资额达到3000万美元的BitPay也还没有能力收集齐所需的牌照。

然而世界“土豪”总是有的。2015年，Circle获得了高盛、IDG（美国国际数据集团）等机构的5000万美元投资。Circle的商业战略就是跑马圈地拿各种牌照，处理和政府关系是它的强项。2015年9月，Circle第一个获得了美国纽约州的BitLicense。2016年4月，Circle又第一个获得了英国政府颁发的电子货币牌照。正因为各种牌照在手，Circle提供了买入、卖出、支付等全套比特币支付服务。而且用户在Circle的美元余额还能受到美国联邦存款保险制度的保障。不过，牌照是把“双刃剑”，严格的监管压力也导致Circle的用户体验下降。

说到支付汇兑不得不提的另一个项目叫作Ripple。Ripple是一个甚至比比特币还古老的项目。我们今天熟知的Ripple则是2012年由杰德·麦克莱伯（Jed McCaleb）和格瑞恩·拉森（Chris Larsen）接手后的Ripple Labs公司主导的Ripple。

Ripple的理念是SWIFT 2.0。SWIFT（Society for Worldwide Interbank Financial Telecommunication，即环球同业银行金融电讯协会）是一个国际协作组织，运营着一个全球性的金融电报网络。银行和其他金融机构通过它与同业机构交换电报，从而完成金融交易。

当用户甲通过中国的A银行向美国B银行的用户乙汇款100美元时，有如下两种情况。

1.A银行和B银行有直接合作关系

A银行首先向用户甲收取100美元和对应汇费，然后通过SWIFT网络发送一份电报给B银行，通知B银行向用户乙的账户存入100美元。尽管这100美元并没有真的从中国移到美国，但用户乙已经收到款了。由

于A、B银行有合作关系，它们彼此有一定的信任额度，可以过一段时间清算一次彼此的欠账关系，做一次结算。

2.A银行和B银行没有直接合作关系

这时就比较复杂了。A银行不能直接给B银行发电报，因为B银行并不认可A银行的指令。此时A银行就只能寻找一间和A银行、B银行都有合作关系的C银行。A银行向C银行发电报，C银行再向B银行发电报。如果找不到这么一间C银行，还可能需要经历A银行→D银行→E银行→B银行的路径。

以上的流程看起来似乎很快就能完成，但是由于SWIFT成立于1973年，是诞生于电报技术年代的产物，大量的流程设计需要人工参与。一笔SWIFT汇款，短的话也要几天时间，长的话甚至可能超过1周。同时，SWIFT网络的运行成本高昂，导致了国际汇款费用较高。以中国银行为例，每笔SWIFT汇款需要150元的电报费加上汇款金额千分之一的汇费。更糟糕的是每个中间行、收款行都会进行几美元到几十美元的扣款操作。尽管你在100美元之外，已经额外支付过了电报费、汇费，对方实际到账的却也往往只有90美元甚至更少。扣费的多少取决于中间经过多少和哪些中间行，扣费金额在用户汇款前是无法准确获知的。低速、昂贵的SWIFT系统成了国际汇款，特别是小额汇款的障碍。

Ripple便是为了解决这个问题而诞生。在Ripple协议中，各个银行可以把用户的银行余额搬到Ripple系统中来。一些做市商会在Ripple内置的交易市场里进行类似于“A银行人民币：B银行美元”这样的挂单。比如当前美元兑人民币的汇率中间价是6.5：1，那么做市商就会挂出6.51：1，卖出银行B美元同时买入银行A人民币，挂出6.49：1，买入银行B美元同时卖出银行A人民币的挂单。当银行A的用户甲想要向银行B的用户乙汇款时，神奇的事情发生了：用户甲只需要表示准备向用户乙转账100美元，此时Ripple系统会在各个内置市场里自动寻找最优的汇款路径，并自动完成兑换、汇款的全过程。一般情况下，用户甲在银行A的人民币会被直接兑换成在银行B的美元，而某些时候可能绕个圈子更便宜。比如系统会帮你发现把银行A的人民币先兑换成银行C的日元再兑换成银行B的美元更划算。

Ripple就像一个货币的同声传译，无论对方需要什么货币，你只需要提供你在Ripple里的有价值的资产，系统就能自动帮你找到最优的兑换路径，并完成汇兑的全过程。在Ripple系统里，比特币这样的交换媒介不再是必需品。银行一旦接入Ripple系统，其用户的存款余额就可以被数字化，从而拥有和比特币类似的流动性，在Ripple网络里自由流动、自由兑换。

Ripple的发展也不是一帆风顺的。其架构设计注定了其在合规性、隐私性和可扩展性上的短板，银行也对直接使用Ripple公司的服务并不感兴趣，而更愿意自建系统，自组联盟。对此最直接的印证就是包括高盛、JP摩根、巴克莱、瑞银等40多家银行加入了2014年才成立的R3联盟，而Ripple阵营的银行却屈指可数且并不知名。Ripple的商业前景还未明朗。

三、登记结算

银行间的支付汇兑只需要记录一种资产类型，即货币。而当一个系统除了货币还可以被用于其他各种类型资产的权益归属、份额转移和流转交易时，这个系统就具备了登记结算的能力。区块链的分布式账本技术备受关注，而分布式账本最适合的应用场景就是登记结算业务。

在中心化账本体系下，为了追求数据的一致性和单一真相来源（single source of truth）, A、B、C、D这些市场参与者把记账的任务托付给了中央登记结算机构，并约定大家一致认可登记结算机构处的账目为最高效力的账本。因此，这些中央登记结算机构需要非常强的公信力才能被各个市场参与者所认可，而创建和维护这样的公信力需要极为繁杂的内部规章和外部审计流程。

在分布式账本体系下，每一个市场参与者都维护一份全市场的账本，各个参与者通过区块链技术对各自的账本进行实时同步，保证账本内容的一致性。这使得分布式账本做到了在物理上的多点分布和逻辑上的数据统一。参与者当然有能力篡改自己的账本，但是区块链技术的底层密码学实现保证了这只能骗骗自己，而无法欺骗其他市场参与者。

在计算机科学中，想要在分布式系统下取得数据一致性有两种思路，分别被称为共享存储（Shared memory）和消息传递（message passing）。区块链技术兼具两种思路，通过点对点网络的共享存储和不停的消息传递，实时同步各自的账本从而实现数据一致性。

区块链技术怎样应用于登记结算业务？让我们先从登记和存管说起。在证券市场形成的早期，股票都是实体的纸质凭证。进行交易时双方就需要一手交钱，一手交票，非常烦琐。尤其当货币可以记账式支付后，股票的纸质凭证的实体转移成为制约股票交易速度的瓶颈。于是存管业务出现了，即投资者把股票的纸质凭证存放在各自的券商处，当发生股票交易时，只需要券商和券商之间在股票上做背书过户的工作就可以了，投资者不再直接持有股票。

随着上市发行的股票越来越多，股票交易越来越频繁，这种以人工操作为主的实物股票背书过户制度越来越阻碍了证券交易的发展。1968年美国出现了纸上作业危机。为了解决这一危机，美国设立了中央证券存管机构（CSD，central securities depository），即美国证券存管信托公司（DTC）。

中央证券存管机构出现后，证券交易出现了非移动交收（immobilization）和无纸化（dematerialization）的重大升级。首先是纸质凭证都被中央证券存管机构集中管理，发生流转交易时，不再需要做任何的物理上的移动工作，而仅仅是在一个账本上更新这份股票的拥有者，实现了非移动交收；然后，市场逐渐发现纸质凭证已经没有任何存在的实质意义了，只要有一份大家公认的账本，就能够完整地记录股票的归属，于是股票不再是上市公司自身发行登记的纸质凭证，而成为上市公司在中央证券存管机构电子化登记账目，实现了证券的无纸化。

对于登记和存管，可以说区块链的分布式账本是极佳的解决方案。区块链上的任何资产天然就是以无纸化和非移动形式交收的。用区块链实现的电子化登记账目可以在没有中央证券存管机构存在的情况下，由各个市场参与者分布式的分会维护更新，实现CSD所能提供的完整功能。而且区块链的智能合约还能实现证券的代码化，让证券变成可编码的智能资产。股票的分红派息、股东投票、禁售限制等可以程序化实现，将人工操作降到极低。

说完登记和存管，就要说一下结算了。结算是清算和交收的统称。清算类似于轧差，通俗地说就是如果我昨天吃饭借了你10元钱，你昨天买水又借了我3元钱，那么轧差后我就只需要还你7元钱了。可以想象如果有100个人，彼此间都相互借过钱，那么这时候需要轧差的交易对可就乱如一团麻了，而且一旦有人违约，还可能造成难以预计的风险传递。因此，在现代证券交易里，中央对手方（CCP，central counterparty）模式成为一个常用的轧差方式。有中央对手方存在的轧差就叫作清算。在中央对手方模式下，A和B之间的交易被拆分成了A和CCP，CCP和B的两笔交易。对于A、B来说，就不再需要担心对方的支付能力，CCP会保障交易的完成。

清算就是算账，账算完后，就是交收了。只有清算、交收都完成了，才是结算完成，交易成功。交收时，结算机构把A卖出的证券登记给B，“同时”把B的货币划拨给A。

上面的模式看起来很完美，但是却存在着问题。首先，中央对手方模式是一种“大而不倒”式的安全。把分散纠缠的风险都堆放在一起，并不等于风险就不再存在了。中央对手方的优点是隔离了风险传递，但代价是把风险都聚集到了中央对手方一个人的身上。最终的走向有可能就会像2008年次贷危机中的银行一样，一旦发生危险，国家就不得不动用国家财政来拯救。其次，细心的读者可能发现上一段最后一句话里的“同时”是打了引号的。是的，这里的同时只是一种希望。由于资金的划拨是通过银行体系，证券的转让是通过中央登记存管机构实现的，是没有办法做到真正的原子级的货银对付的，交钱和交货总有先后。

那么能否找到解决这些问题的终极方案呢？区块链也许是一个答案。

通过区块链的分布式账本技术，理论上可以完全消灭轧差/清算的过程。正是由于现存证券交易系统技术和流程上的低效，资金和证券登记的割裂，才导致了清算、交收环节存在的必要性。

在区块链技术下，首先资金和证券可以在同一个账本中登记，从而保证原子操作级的货银对付。所谓原

子操作，即指交钱和交货这两个动作被包含在一个不可分割的操作指令中执行，要么同时成功，要么同时失败。任何意外，无论是突然断电还是断网，都不可能导致钱付了而证券没有转移成功。

其次，中央对手方存在的必要性来自于多边轧差的混乱和可能产生的风险传递，而代价就是把风险集中到了一个中心点上，这意味着中央对手方就是一个单点故障源（Single Point Of Failure）。而区块链技术可以实现证券交易的实时全额结算（RTGS，Real-time gross settlement）模式，完全避免了轧差/清算的业务流程，让交易和结算成为一个动作，不再存在结算（清算、交收）这一过程。没有了清算、交收流程，中央对手方也就不再有存在的必要了。由于一次交易一笔结算，原来错综复杂的多边轧差关系也不复存在，世界一片清净。

当然，尽管理论上区块链可以完全消灭清算、交收流程，但由于网络宽带、存储容量、延迟性要求等技术条件的限制，在要求高频、高吞吐、低延迟的证券交易领域，基于区块链技术的实时全额结算的登记结算系统还难以胜任。基于区块链技术的登记结算目前更适合用于低频、低延迟要求的场外交易系统。

在纳斯达克上市的电商公司Overstock就以此为理念，利用区块链技术开发出了一个名为T0的证券交易平台。顾名思义，T0意味着T+0结算，是对美国现存T+3股票结算的巨大超越。T0近期收购了一间ATS（另类交易系统，有点像中国的互联网证券）公司，并已经得到了美国证券监管机构SEC的许可，将在2016年下半年发行Overstock的股票。未来，投资者既可以在既有的纳斯达克市场内，也可以通过合规的ATS交易系统在T0平台上购买到Overstock公司的股票。如果T0上的价格、流动性都不错的话，也许越来越多的公司会愿意到T0上发行股票。T0的口号是对基于区块链技术的证券登记结算系统的一个很好的诠释：The Trade Is The Settlement(交易即结算)。

纳斯达克当然也不甘示弱，通过和区块链技术公司chain.com的合作，推出了自己的非上市公私股权登记系统LINQ。有意思的是，2015年12月LINQ上第一个登记股权的公司也是其合作开发方chain.com。目前有6家和区块链技术相关的公司成为LINQ的首批内测客户。纳斯达克使用区块链技术布局非上市公司的意图有两个：一是全球资本市场越来越青睐于一级市场，大量独角兽公司迟迟不上市，越来越需要一个一级市场的登记流转服务，因此纳斯达克还收购了专注于上市前公司股权转让服务的SecondMarket（二级市场）；二是作为一个金融服务公司，纳斯达克有大量的技术输出服务，为全球几十个资本市场提供技术服务，区块链方向的技术储备会为未来几十年的技术输出业务提供基础。

同时，各国的证券交易和登记机构也没闲着。澳大利亚证券交易所ASX和美国的中央证券登记结算机构DTCC，先后宣布与区块链技术初创公司DAH（Digital Asset Holdings）合作，开发基于区块链技术的登记结算系统。东京证券交易所JPX也在和IBM以及野村综合研究所进行区块链登记结算的概念验证工作。伦敦证券交易所LSE则牵头成立了“交易后分布式账本工作小组”（Post-Trade Distributed Ledger Working Group）这一技术联盟。此外，纽交所NYSE、多伦多证券交易所TSX、芝加哥商品交易所CME、韩国证券交易所KRX等也都在区块链领域进行探索。

国内也有一个类似的项目：小蚁（AntShares）。小蚁是一个用来登记结算各种数字资产的区块链底层协议，而其中一类数字资产就是公司股权。公司可以将自己的股东名册放到小蚁区块链上进行管理，公司的投资者们用电子签名在区块链签订股权转让的电子合同，由区块链保证货银对付，实现公司股权的数字化流转。有两类公司在现阶段就非常适合使用小蚁。

第一类是进行股权众筹的公司。这些公司在股权众筹完成后面临管理大量股东的问题。股权的变更登记费时费钱费力。利用小蚁区块链，众筹投资者不仅可以在线上完成股权登记的所有电子合同，还能非常方便地进行股权的再次转让，为股权众筹提供了良好的退出机制。

第二类是进行员工持股激励方案的公司。这些公司原本的员工持股激励方案往往都是落在一份份的纸质文件上，而没有一个完整的数字化的股权激励管理系统。使用小蚁后，公司可以把股权、期权、限制性股权、虚拟股权（分红权）等各种权益在一个去中心化的区块链系统里管理起来，而员工则能够自己掌控自己的权益份额，感受到实实在在的激励。利用小蚁，公司还可以将投票权和经济权益分离，实现更好的管理架构。

在全球区块链行业会议Consensus 2016上，美国特拉华州州长宣布了一个令人震惊的消息：特拉华州将修改其公司法，允许公司用区块链技术登记股权，实现公司注册的流程简化，并更好地对股权归属进行追踪，更好地实现股权的流转交易。在特拉华州注册的美国公司超过100万家，其中包括美国一半以上的上市公司和超过65%的财富500强公司。特拉华州的举动将深刻地影响美国国家层面的公司股权登记体系。

现有证券市场的登记结算制度是历史演变的产物，其业务流程较长，参与主体复杂，导致了清算、交收的效率低下，往往要T+1甚至T+3才能真正完成交易。冗长的结算流程导致了更久的资金占用和更长的风险敞口。基于区块链技术的登记结算系统，有望实现低摩擦的登记存管流程，从中央证券存管模式转换到分布式账本存管模式；有望消灭部分低频应用场景下的清算、交收过程，从而使这类场景不再需要中央对手方这一角色，代之以实时全额结算模式。

四、数据存证

前面花了较大的篇幅介绍了区块链技术在数字货币、支付汇兑、登记结算这三大领域得以应用的内在逻辑。理解了这些内在逻辑后，就会发现，区块链在其他领域的应用往往“万变不离其宗”，总是这三种应用场景的某种变形。那么我们就先来看基于区块链的数据存证应用。

基于区块链的数据库有一个核心的特点是不可篡改。前面说过，你可以篡改你自己手里的那份账本，但那只能骗骗你自己，骗不到别人。你可以在自己的脸上写上“我是刘德华”，但全社会每个人头脑里的账本上都记录着刘德华的长相，你只能照镜子骗自己，骗不到其他人。基于不可篡改这一特点，区块链就是一个非常好的数据存证技术。

成立于2012年的存在性证明（Proof of existence）项目可能是这个领域最早的实践者。在其官网上，用户可以把一个本地的文件拖入浏览器。这个文件本身不会被上传，而是会在本地浏览器内进行一次摘要计算，计算出此文件的数据指纹——哈希值。这个哈希值会在10分钟左右被“存在性证明”网站通过一笔交易写入比特币的区块链。从而这份文件的数据指纹就永久性地被公开保存在了比特币区块链上。

值得再重复一遍的是，公开保存在比特币区块链上的仅仅是该文件的简短的数据指纹。通过数据指纹是无法反推出任何有关该文件的信息的，哪怕是文件大小也不行。文件一直留在用户本地电脑上，不会被公开或上传给“存在性证明”官网。

用户可以将“存在性证明”这样的服务用于三个目的。

①知识产权保护。用户可以把自身创作的作品、专利的数据指纹通过“存在性证明”网站记录到比特币区块链上。当未来发生版权纠纷时，用户通过展示区块链上的数据指纹，证明自己早在某某时间就已经拥有该份文件。如果对方无法提供更早的证明，再结合其他证据，就很容易推定你是该知识产权的创作者。

②给文件盖时间戳。你可以把一份合同、一份文档的数据指纹通过“存在性证明”网站记录到比特币区块链上，从而为这份合同、文档盖上一个时间戳。通过区块链向外界证明在某个时间点，这份合同、文档就已经存在了。

③完整性校验。当你把一个文件的数据指纹通过“存在性证明”网站记录到比特币区块链上后，未来你就可以校验这份文件是否被篡改过。比如微软可以把Windows的安装镜像的数据指纹上传至比特币区块链，任何用户从第三方网站下载到Windows安装镜像后，都可以通过比特币区块链比对数据指纹是否一致，从而发现该安装镜像是否遭到了恶意软件的篡改。

这个领域另一个著名的区块链项目叫作公证通（Factom）。Factom这个名字取自拉丁语Factum，意为“确定的事实”。和“存在性证明”相比，公证通的架构更为完整。公证通是这么介绍自己的：

> 公证通旨在借助区块链技术，为大型的私营或公有机构安全地存储数据。公证通将这些数据进行编码或者生成数据的独一无二的特征码（哈希），然后将其存储

> 在公证通系统内不可篡改的分布式账簿中。账簿中的这份不可篡改的数据可以被用来作为某份数据的“存在性证明”，也可以为未来的商业活动提供“事实来源”。
>
> 公证通也可以被理解为是一个不可撤销的发布系统，（公证通系统中的）数据一经发布，便不可撤销。公证通的这个特性提供了一份准确的、可验证的且无法篡改的审计跟踪记录，消除了（人类活动中的）盲目信任。

与“存在性证明”网站上传数据指纹不同，公证通还提供了一套分布式存储原始数据的存储网络。数据指纹被存储于比特币区块链，数据原文被存储在公证通自建的分布式存储网络。存储在公证通存储网络的数据将每隔十分钟被计算一次数据指纹，并将数据指纹上传到比特币区块链，从而使得公证通本身也无法修改用户的原始数据。

尽管公证通能够存储数据原文，但由于其经济模型的设计，每GB的存储成本超过1000美元。公证通并不适合当网盘来使用存储一般性数据，而更适合保存精简的需要审计的关键性数据。

与Factom、Proof of existence类似的项目还有Stampery、Bitproof等。

五、知识产权保护

把区块链技术与知识产权相结合是目前比较热门的区块链应用场景之一。一是有极高的市场需求，从每年的“3·15”维权热度可以看出，知识产权的维权存在取证难、周期长、成本高、赔偿低等一系列问题；二是区块链具有的功能恰好匹配了这种市场需求，维权难的关键原因是第三方执行效率低下，而区块链通过程序算法自动记录信息，移除了第三方，信息储存在互联互通、共享的全球网络系统中，无法被任意篡改,极大地提高了维权的效率。

知识产权保护的第一步是确认知识产权是何时生成的。具体到版权这类知识产权来说，一直以来存在两种不同的实践：一种规定必须经过登记程序的作品才享有完整的版权；另一种则规定只要作品创作问世版权就生成了。美国过去一直实行第一种实践，即经过登记的作品才享有版权，而近年来通过修改版权法，美国开始和世界其他大部分国家一样接受了创作问世即版权生成的做法。

尽管如此，当碰到侵权、诉讼、版权转让等情形时，未经登记的版权仍然面临种种不便。而在美国版权办公室每登记一件作品就要35~55美元的支出。考虑到今天大量在互联网上发表的海量文字、图片、视频，为每件这样的作品注册版权几乎是不可能的任务。基于区块链的版权登记能够很好地解决上述问题。

①区块链的开放性让任何人都可以在全球任何角落向区块链写入信息。不管是在凌晨3点的西雅图不眠之夜，还是在横跨大西洋的量子号邮轮，只要能连上互联网，版权登记就不受时间、空间的限制。

②区块链上的信息一经写入就无法篡改。无论是上传者本人，还是相关机构都无法对历史进行修改。信息一旦写入，时间戳就把这段信息永久地封存，无法篡改。

③区块链的登记将能做到几乎免费，让更多的作品有可能被登记。

④在区块链上可以很方便地实现链上版权交易。

Mediachain在区块链与分布式文件系统（IPFS)基础上推出元数据协议，允许数字创意者在他们的创作作品上附加信息，并在数据上添加时间戳传送到比特币区块链，然后存贮在IPFS。后者是一个整合了区块链技术的点对点文件系统。

Monegraph则侧重区块链的版权交易，其产品的用户体验和其他图片分享销售网站无异：创作者上传自己的作品形成作品集，Monegraph的手机App将其展现给潜在的买家，并形成交易。但在技术上，Monegraph使用区块链对每件作品进行确权登记，并在发生授权使用和权利转移时进行相应记录。

此外，从事知识产权方向的区块链项目还有Verisart、Blockai等。

六、溯源、防伪与供应链

溯源，顾名思义就是追踪记录有形商品或无形信息的流转链条。通过对每一次流转的登记，实现追溯产地、防伪鉴证、根据溯源信息优化供应链、提供供应链金融服务等目标。把区块链技术应用在溯源、防伪、优化供应链上的内在逻辑和前文所述的数据存证场景非常类似——数据不可篡改和加盖时间戳。

传统的溯源系统要么使用今天的中心化账本模式，要么由各个市场参与者分散孤立地记录和保存，是一种信息孤岛模式。

在中心化账本模式下，谁作为中心维护这个账本变成了问题的关键。无论是源头企业保存，还是渠道商保存，由于其自身都是流转链条上的利益相关方，当账本信息不利于其自身时，其很可能选择篡改账本或者谎称账本信息由于技术原因而灭失了。这样的例子在现实生活中屡见不鲜，摄像头总是在关键的时候没被打开，又或者刚好损坏。因此，利益相关方维护的中心化账本在溯源场景下是不可靠的。

信息孤岛模式下，市场的各个参与者自我维护一份账本，这样的账本俗称台账，电子化后又被冠上进销存系统的名字。不论是实体台账还是电子化的进销存系统，拥有者都可以随心所欲地进行篡改或集中事后编造。例如我国工商部门强制要求的食品台账制度，在落到小企业、个体经营者层面时，往往变成了一种为了应付检查而突击编造的形式主义。而且这些上下游链条的台账之间没有互通互联，各自是一个独立的信息孤岛，无法做到快速的追溯问责。

区块链在登记结算场景上的实时对账能力，在数据存证场景上的不可篡改和时间戳能力，为溯源、防伪、供应链场景提供了有力的工具。

位于英国伦敦的区块链初创公司运营了溯源领域的一个知名项目——Everledger。Everledger是一个用于登记钻石身份和记录钻石流转过程的区块链。Everledger的主要客户是承接钻石偷盗险的保险公司。保险欺诈是欧美保险公司最头疼的问题。美国和欧洲的保险公司因为保险欺诈每年要损失450亿英镑，经管保险公司的年度反欺诈支出高达2亿英镑，65%保险欺诈无法破案。这其中，每年约有1亿的金额被用于珠宝的失窃赔付。

Everledger正是瞄准了这样一个市场。通过和美国、安特卫普、以色列、印度等地的钻石鉴定机构合作，Everledger利用钻石的4C信息（颜色、切工、纯净度、克拉布）外加14个特征数据，为每个钻石生成一个独立编号。通过在区块链上记录这一编号的流转过程，Everledger可以转载钻石的归属和所在地。当钻石不幸失窃时，保险公司在Everledger上将该钻石标记为被盗。这个钻石无法再次投保，如果被用于抵押也很容易被接受抵押的机构在Everledger上查找到，同时还为执法机构追寻赃物提供了方便。

除了Everledger，还有侧重于药品溯源的BlockVerify，侧重于艺术品防伪的verisart，着力于奢侈品防伪的唯链（VeChain）。唯链由中国区块链初创企业BitSE开发，主要用于LV包的防伪。通过和LV集团合作，在LV包中嵌入NFC芯片，实现LV包每次流转的区块链登记，从而为防伪鉴定和二手LV包交易提供可靠的支持。

当一个溯源区块链登记的标的物是国际贸易货物时，这个溯源区块链就具备了提供供应链金融服务的能力。SKUChain通过在货物包装上装配二维码、NFC芯片或GPS定位设备，使商品的流转能够自动被记录到SKUChain上。同时，通过把银行发行的信用证数字化，使资金流和物流能够同时无缝地在SKUChain上流通。

七、身份认证与公民服务

什么是身份是一个经久不衰的哲学话题。Identity其本意乃是“同一性”，而谈到同一性，不得不提出哲学史上的“忒修斯之船”问题。

> 一艘在海上航行了几百年的船,被不间断地维修和替换部件。只要一块木板腐烂了，它就会被替换掉，以此类推，直到所有的功能部件都不是最开始的那些了。问题是，最终产生的这艘船是不是原来的那艘忒修斯之船，还是一艘完全不同的

> 船？如果不是原来的船，那么在什么时候它不再是原来的船了？哲学家托马斯·豪倍思（Thomas Hobbes）后来对此进来了延伸，如果用忒修斯之船上取下来的老部件重新建造一艘新的船，那么两艘船中哪艘才是真正的忒修斯之船？

历史上不同的哲学家给出了不同的答案。我更欣赏的一个答案是：忒修斯之船在物理上时时刻刻都不是前一刻的自己，只要时间永远单向流逝，绝对意义的“同一性”并不存在。下一秒的你已经不是绝对“同一性”的你，只是如此近似于上一秒的你，以至于我们可以认为下一秒你仍然会拥有类似的价值偏好，相近的生理反应。语言的抽象和窄域本质导致了我们只能低精度地描述世界，为每一团物质波指定一个身份。

回到现实世界的身份系统。在今天的世界，没有身份就无法拥有银行账户，无法获得社会福利，无法行使受教育的权利，更谈不上参与政治生活。同样，一个区块链上如果用户只拥有匿名的地址而无法证明自己的真实身份，那么其应用场景必然变得狭窄。

ShoCard是一个将实体身份证件的数据指纹保存在区块链上的服务。用户用手机扫描自己的身份证件，ShoCard应用会把证件信息加密后保存在用户本地，把数据指纹保存到区块链。区块链上的数据指纹受一个私钥控制，只有持有私钥的用户才有权修改，ShoCard亦无权修改。同时，为了防范用户盗用他人身份证件扫描上传，ShoCard还允许银行等机构对用户的身份进行背书，确保真实性。

OneName则提供了另一种身份服务。任何比特币的用户都可以把自己的比特币地址和自己的姓名、Twitter(推特)、Facebook（脸书）等账号绑定，相当于为每个社交账户提供了一个公开的比特币地址和进行数字签名的能力。

一个叫Bitnation的项目则更为激进。用户在其官网上通过区块链登记成为Bitnation的“公民”，并获得Bitnation“世界公民身份证”。然后凭此身份，获得Bitnation自我认可的各种公民服务。

与此相比，爱沙尼亚政府推出的“电子公民”计划可谓真正的接地气。2014年10月，其宣布向全世界开放“电子公民”身份认证服务。任何人只需要在其政府官网填写简单的信息，并用信用卡缴纳50欧元的申请费即可成为爱沙尼亚的电子公民。电子公民可以：①线上登记注册并管理一间基于欧盟商业法律体系的欧盟企业；②获得爱沙尼亚政府认可的数字签名、认证与加密文件的网络服务；③在线开立爱沙尼亚的数码银行账户；④使用全球跨境支付服务。

八、物联网

在即将到来的物联网时代，人们日常生活中的大部分设备将连接到云端网络。设备与设备可以直接通信，而无须经过主人；物联设备可以自主地决定运行的状态，自主地购买服务，自主地完成运行和维护。打印机可以自己订购所需的墨水，空调可以自动调用你的手机导航信息而提前调节温度。但是，传统的物联网模式是由一个数据中心负责收集各连接的设备信息，这种方式在生命周期成本和收入方面有着严重的缺陷。

为了解决这个问题，IBM提出的方案是让未来的每个设备实现自我管理，从而无需经常性地对它们进行维护。也就是说，这些设备的运行环境是去中心化的，它们连接在一起以形成一个持续运行的分布式云网络。只要这些设备都存在，那么整个云网络的寿命就会变得很长，并且运行的成本也将降低很多。

而解决分布式云网络的一个重要问题就是要解决各节点的信任问题。在中心化的系统中，信任是比较容易的，因为存在一个中央机构管理所有的设备以及各节点的身份，并且可以处理掉不好的节点。但是，如果这对于潜在数量几十亿的上网设备来说，几乎是一个不可能完成的任务。而IBM认为，比特币区块链技术恰恰解决了这个问题。IBM联合三星推出了一个基于区块链技术的物联网概念验证项目ADEPT。

在ADEPT的公开演示中，一台三星W9000型号的洗衣机可以自主地侦测到洗衣粉不足，然后向供应商进行自主订购。根据ADEPT项目的描述，这台洗衣机将能够自行发送更换零配件的订单，甚至能够和扫地机、洗碗机等其他家电设备进行电源竞价，最终实现用户家庭能源消耗的最小化。

同样，在物联网的世界里交易也将会和今天福斯普遍理解的交易大相径庭。今天的交易往往是人和人之间的交易，而在物联网世界，交易的参与主体将不再是人，而会是各式各样的设备；交易的金额和频次因此也会发生重大的变化，金额变得极小，频次变得极高。在这样的一个环境下，设备信任网络的创建和微支付都要求我们有一个新的基础架构，而不可能依赖于传统的面向自然人的身份认证体系和面向人际交易的支付系统。

美国一家名为21Inc的创业公司就试图将区块链技术与物联网结合起来。21Inc的愿景是制造出一种可挖比特币的芯片。这种芯片可以安装在任何物联网的设备之中，一旦设备通电，这种芯片就能开始比特币的挖矿工作，挣得比特币。当这个设备需要进行支付时，不再需要人工向此设备充值，该设备可以动用自己挖矿挣来的比特币完成整个支付过程。这个设备就像一个自主系统一样，只要提供电能，就能自我运营。尽管通过这样的芯片进行比特币挖矿的效率显著低于专业的矿机，但是这种自给自足的模式大大减低了人的认知成本。只要插上电源，就可以不用再管了。这样一个宏大的目标也帮助21Inc获得了高达1.2亿美元的风险投资。

不难发现，这样的技术还可以复制到其他设备上。比如一台饮料自动售卖机，通过卖出饮料获得用户支付的数字货币，当存货不足时，售卖机自动向供货商发出订货单。当供货商补充饮料后，售卖机自动用之前收到的数字货币支付给供货商，并留存利润备用。同样，一台无人驾驶汽车可以成为一个独立自主运营的出租车，向乘客收取数字货币，用数字货币去充电桩购买充电服务，去汽车维修处用留存的利润更换老化的零件。

当然，物联网也不全然是巨头的天下。像Filament、Tilepay，这样的小型物联网区块链初创公司也在进行着自己的探索之路。

Filament正在制造两种硬件设备：Filament Tap，一种能够让物联设备和10英里内的手机、平板或电脑进行通信的模块；Filament Patch，一种用于增强物联设备的互联能力的模块。这些模块会首先被使用在工业设备上，让各个工业设备协同工作，而无需依赖一个中心化的组织者。Filament最近也完成了500万美元的融资。

Tilepay更聚焦于传感器数据的交易上。全球的用户都可以接入Tilepay，提供自己的手机GPS（全球定位系统）、温度计、汽车传感器、可穿戴设备等实时传感数据给数据需求方。数据需求方为自己获得的实时数据支付对应的比特币。Tilepay创建了一个基于区块链的大数据交易市场。

无疑，我们正在迎来一个万物互联、价值互通的时代。

九、保险

当金融证券业在积极探索区块链应用场景的时候，保险业也在紧锣密鼓研究区块链技术，埃森哲的常务董事艾比·让拉（Abizer Rangwala）这样写道：

> 我认为，保险业正在观察区块链技术，慢慢摸清区块链技术的真正商业用途或者说在一定程度上区块链的实际应用是什么。
>
> 区块链技术对保险产品的影响还尚不清晰，相比对银行的影响，可能会需要更长的时间才能显现出来。区块链技术将提高合约执行速度，比如区块链的时间戳特征能够改善个体合同，反映实际风险，如按需车险（合约只在车辆行驶期间有效）。

这样的论述并非空中楼阁。2016年3月，一个名为SafeShares的区块链保险创业公司联合英国老牌保险公车劳合社推出了第一个为共享经济服务的区块链保险服务。这项服务是为一家名为Vrumi的创业公司而量身定制的。Vrumi是一家类似于Airbnb（空中住宿）或Uber（优步）模式的办公空间共享服务平台。每个通过Vrumi提供办公空间的房主只需要缴纳每天2英镑的保费就能成为被保险人，获得75万英镑财物险到500万英镑人身险的完整保险方案。

一般的共享经济都采用所谓“保护伞保险”模式，平台即是投保人，也是被保险人。发生赔付事件时，保

险受益人是平台，由平台再赔付给用户。在这个模式下，受损人和保险收益人不一致，而且平台的整体理赔额有上限，一旦到达上限，后续的受损人将无法得到赔付。

与其他共享经济的保险方案不同，在SafeShares这个基于区块链技术的保险方案下，办公空间的提供方是直接的被保险人，拥有直接申请理赔的权利。

区块链+保险领域另一个可能的方向是自动理赔的保险。通过区块链的智能合约技术，保险公司可以无需等待投保人申请理赔，就能主动进行赔付。例如，可以发行一种基于区块链智能合约技术的航班延误险。通过调用航空公司/机场的公共接口，智能合约得以判断某次航班是否发生了延误，延误情况的严重程度如何，从而自动触发理赔行为，而无需用户主动干预。延误理赔甚至可以是用类似出租车打表的方式完成。看着自己账户余额不停地增加，也许延误航班的常客们就不会再爆发国内机场延误时常见的打砸抢式的情绪了。

还有一个可能颠覆今天保险行业的模式是互助保险。互助保险的逻辑出发点很简单，保险本身就是一个互助行为，因此一旦技术允许，我们并不需要一个中介充当组织者，创建资金池，用用户的保费去做各种投资。用户完全可以通过点对点互助的形式，在没有资金池的情况下，通过互助达到保险的目的。2016年5月，美团早期员工创立的“水滴互助”就获得了IDG（美国国际数据集团）、腾讯、真格等机构的5000万美元投资，而其背后就使用了区块链技术。

在荷兰金融咨询机构AXVECO的区块链专家欧利文·瑞肯（Olivier Rikken）的一篇文章中，对基于区块链技术的P2P保险商业模式有过更有趣的模式设计。在Olivier设计的新模式下，保险公司的专业能力将更多体现在匹配供需、风险计算上，而不像今天的保险公司如此注重资产管理能力。

在P2P保险下，保险公司将提供一个保险交易市场，用户可以在市场内提出自己的保险需求，无论是标准化的还是非标准的，保险公司随后通过自己掌握的历史数据给这个保险需求计算出一个参考保费和响应的承保方的预期收益率。随后，想要提供承保服务的用户就可以竞标这份保单，既可以是一对一，也可以是一对多。

区块链在这个市场需要提供两个作用：①对保单交易进行登记；②利用智能合约，在满足赔付条件时，自动从承保人的账户划拨赔款给受益人，而无需银行的参与。在判断是否满足赔付条件时，保险公司可以作为提供损失鉴定报告的第三方。

在这种P2P保险模式下，用于资金端的来源是投资人用户，保险公司可以轻资本运营，甚至这个交易平台可以外包给第三方运行维护。另外，P2P保险由于没有保费资金池，可能在监管上和P2P借贷不需要银行牌照一样而不需要保险牌照，这样就减轻了合规成本。

除了初创公司，人寿保险和金融服务巨头约翰·汉克（John Hancock）也已经开始着手多个区块链概念验证的工作了，其目的在于展示分布式总账技术重塑保险行业的流程。John Hancock正在进行的概念验证项目的合作方是区块链技术公司ConsenSys和BlockApps，项目方向包括“了解你的客户”和“员工奖励计划”等。

另外，除了SafeShares、互助保险、P2P保险的模式，在溯源防伪项目中提到的Everledger也在从防伪的角度切入，和保险公司密切合作提供区块链登记溯源的珠宝盗窃险。看到这么多的保险业的创新火花，我们有理由相信埃森哲的常务董事Abizer Rangwala的看法：“我毫不怀疑，未来几年内，区块链技术将成为在保险业生态系统中的主流技术。”

十、医疗

全球医疗市场大得惊人，仅仅是制药这一个领域，市场规模就高达1.057万亿美元。美国是人均医疗开支比例最高的国家，医疗支出占整个GDP的16.8%，美国每年创造出来的财富中有1/6被花在了医疗上。医疗机构保存了大量的机密信息，例如病史记录、疾病、支付和治疗。区块链技术不仅能为这些敏感数据的安全和隐私存储提供解决方案，而且它还能帮助降低医院和医疗服务者在管理病人和其他信息时的

巨大成本。

第一个显而易见的应用场景就是电子病历。在互联网高度发达的今天，大多数的医院仍然在使用手写病历。这些病历往往如天书般难以读懂，而且一旦丢失或因故无法携带（如出国），再次就诊时就失去了历史可循，甚至可能因此耽误宝贵的有效治疗的黄金时间。中国卫生部早在2010年就签发了《电子病历系统功能规范（试行）》的通知，然而6年后的今天电子病历任然进展缓慢。这其中一个重要的问题就是电子病历的保存是在医院处，而医院却又是医患合同中的利益相关方，大量的医疗纠纷中都牵涉到了电子病历的有效性上。由于医院单方面保管电子病历，在发生医疗事故纠纷时，患者往往指责医院对电子病历进行了修改。

因区块链的不可篡改性和高强度保密性可以给这些电子病历提供一个可靠的访问环境。当电子病历被保存在一个去中心或者多中心参与的区块链上的时候，医院单方面将无法对数据进行任何篡改。而且一旦上链，就可在全球范围内访问数据，无需担心病历丢失或者携带不便的问题，一个人的终生医疗信息都可以被记录在区块链上。位于瑞士的Healthbank(健康银行)就是采用一种完全透明的方法处理医疗信息，用区块链技术为个人医疗数据安全提供保障。Healthbank的口号是“我的数据，我的选择，我的Healthbank”。Healthbank允许个人与患者自己掌握自己的信息。医生访问、睡眠模式、心率、血糖浓度和其他的物联网设备都能够被调查到，并记录到Healthbank的区块链上。

随之而来的是另一个问题：个人医疗隐私的保护。2015年初，美国第二大医疗保险公司Anthem的服务器被黑客入侵，超过8000万的医疗保险客户和员工的资料被盗取。被盗取的个人信息包括住宅地址、生日、医疗身份号码、社会安全号码、邮箱地址和收入数据。就连该公司CEO的个人信息也未能幸免。2015年7月，加州大学洛杉矶分校发现其医疗网络UCLA Health被黑客入侵，又有450万个人敏感信息被盗。究其根本，只要隐私信息依然采用中心化方式保存，就难免发生百密一疏的情况。

区块链恰恰提供了保护隐私的工具。保存在区块链上的病历虽然是可以在全球任何地方都能访问的，却是用户用密钥掌握数据的绝对专属权与访问权。同时，区块链强大的智能合约功能可以让用户自主的设置权限。比如，用户可以使用这样的智能合约——当自己发生昏迷时，只要医疗机构和自己的亲人同时使用各自的密钥，也能获得访问自己医疗记录的权限。

除了医疗记录，有些创业公司着眼于将区块链技术应用于基因检测数据的共享。成立于2014年的DNA.bits公司，致力于解决针对医疗电子交换法案（HIPAA）的共享基因识别及相关临床数据的问题。由于其产品使用了比特币区块链平台，可聚集来自多个数据源的数据，而无需将这些数据收集到一个中央数据库。

全球医疗市场的几大主要玩家包括诺华制药公司（494亿美元）、瑞辉（474亿美元）、强生（163亿美元）、复迈（118亿美元），巨头间的交叉竞争调用了海量动态医药数据和历史医疗记录，给药物发现和个性化医疗带来高昂的成本。我们可以更进一步设想，如果全世界的医疗记录都加密保存在区块链上，那么只要能设计一种机制，让用户就可以主动将自己的敏感信息清除，而把医疗方面的信息免费或收费提供给医疗研发机构使用。海量、完备的医疗大数据显然将大大加快了研发的进度，为攻克更多不治之症提供帮助。

除了医疗信息与基因检测数据，整个诊疗过程的支付也可以应用区块链技术来提升效率。前面用区块链来管理医疗记录的生命周期的方法，也可以用于管理医疗账单的生命周期。当病患的医疗记录用区块链记录后，自然的医生的处方、诊疗的账单也可以被记录在区块链上。病历、处方、账单都上链后，医院、病患、保险公司这三方也就无需再通过繁杂的申请、核验过程来完成医疗保险的赔付，大大简化了赔付流程，提升了透明度。

Gem是聚焦医疗健康领域的区块链创业公司，其在2015年获得了700万美元的风险投资。Gem使用多重、硬件安全模块等技术管控区块链上的用户身份和信息安全。2016年4月，Gem宣布与飞利浦合作，推出了Gem Health项目，构建一种能够用来开发企业级医疗应用程序的私有以太坊区块链。对于Gem在管理这种新的私有区块链系统过程中承担的角色，Gem CEO表示他们的目的并不是为了将这个网络“纳

为己有”，而是将自己定位为顾问和区块链项目研究公司之间的“红娘”。

另一个区块链医疗领域的初创公司Tierion也在与飞利浦健康开展合作。Tierion聚焦于数据保存方向，除了一般的病历外，其还开发了一种名为Chainpoint的区块链收据标准。任何行业的商家都可以通过此标准来在区块链上签发收据。

十一、博彩和预测市场

博彩与预测市场是区块链的一个重要应用方向。在区块链应用平台以太坊上，预测市场应用是出现频率最高的应用类别。

预测市场（Prediction Market）按照维基百科的定义，是以进行预测为目的而产生的一种投机市场。从发起预测的对象来说其目的是为了预测；从参与预测的用户角度，预测市场可在某种程度上理解成非标准化的博彩。预测市场和博彩的最大区别在于预测市场需要将链下信息进行记录和结果判断。

基于以太坊平台的Augur是目前融资额度最高的区块链预测市场应用，在2015年10月完成了总额520万美元的众筹。Augur目前已经进入Beta阶段，计划将于2016年底前正式运行。截至到2016年5月，Augur在进行Beta测试的阶段中共有618个预测市场项目，其中261个为开放状态，在数量上已经初具规模。Augur相比其他预测市场，其有如下优点。

①无中心化服务器，难以被关闭。传统预测市场一大问题在于扩张到一定程度后容易遭到政治等外力阻碍甚至直接闭站。利用去中心化的区块链技术可以打消该种忧虑。

②用户可以创造自己的交易市场。这意味着预测市场的项目可以是完全自定义而没有门槛。用户可以用此来预测总统大选结果或是明年玉米的收成，也可以是预测一场球赛，甚至明天是否下雨。

③低成本运营，所以低费率。低费率的原因在于运行成本通过区块链分摊，而团队成员在未来也只是通过REP代币而非工资来获取相应收入，所以后续人力成本几乎没有。

④众包型的结果判断。当某个预测项目产生结果时，Augur并不依赖于中心化的网站或个人来判断用户的输赢，即Augur不依赖中心化的信息源来获取美国大选的结果，而是用众包的方式获得大选结果。这避免了中心化信息源的单点故障问题。

⑤安全以及自动化的支付。Augur是基于以太坊的去中心化应用。参与Augur预测市场的用户无需担心对方赖账的风险，也无需担心中间平台卷款跑路。通过透明的开源代码，用户可以有充分的信心预期博弈的公平性。

Augur作为预测市场与博彩类应用的最大区别在于需要进行链下信息的链上录入以及众包式的结果判断。前者更多是利用经济激励实现，后者除了激励以外更多还需要数学模型的帮助。

Augur发行REP作为整个区块链系统的激励代币，对每笔交易收取2%手续费，相比传统预测市场收取5%的手续费更有竞争力。手续费的一半给予流动性提供方，另一半给予合格的REP代币持有者。一方面通过REP可以给予众包的结果判断者奖惩激励，[26] 另一方面REP也可以作为Augur团队成员的长期激励因为Augur团队成员持有一定数量的REP。。故REP更像是Augur这个去中心化区块链预测市场系统的股份。

从“中本聪骰子”到Augur，区块链创业者可以通过数学和博弈制度的设计让古老的博彩和对赌（预测市场）变得更公平、更透明。博彩与预测市场可能无法成为主流，但它们也许会一直存在下去，就像赌徒这个职业一样。

[26] 由于不存在一个中心化的组织，故Augur上所有预测市场结果的事后判断都由REP持有者进行，再通过相应算法确保结果和现实一致。如果没有按时完成对应的项目结果判断的话，REP持有者将失去对应分红。

第六章
从信息互联网到价值互联网[27]

一、技术创新与制度创新

（一）区块链与互联网

区块链给经济社会发展带来了一系列挑战，在明确其技术内涵、路径和应用案例的同时，我们还需要从理论层面和国家战略层面予以进一步剖析和定位，并且从历史演变的脉络中，找到区块链“应运而生”的内在支撑要素。

区块链科学研究所(Institute for Blockchain Studies)创始人梅兰妮·斯万(Melanie Swan)认为[28]，

> “我们应该把区块链当成类似互联网的事物——一种综合的信息技术，其中包含多种层面的应用，如资产登记、编写清单、价值交换，涉及金融、经济、货币的各个领域，像硬资产（有形财产、住宅、汽车）；以及无形资产（选票、创意、信誉、意向、健康数据、信息等）”，“但是，区块链的概念远不止于此：它是任何事物所有量子数据（指离散单位）呈现、评估和传递的一种新型组织范例，而且也有可能使人类活动的协同达到空前的规模。”

此外，梅兰妮·斯万把由区块链技术带来的各种已有和将有的革新分为三类，即：

①区块链1.0——货币（货币转移、汇兑和支付系统）；

②区块链2.0——合约（在经济、市场、金融全方面的应用，其可延伸内涵远比简单的现金转移要广得多，如股票、债券、期货、贷款、按揭、产权、智能资产和智能合约）；

③区块链3.0——超越货币、金融、市场之外的区块链应用，特别是在政府、健康、科学、文学、文化和艺术等领域。

我们可以看到，区块链虽然源于比特币，但是其应用层面却能够进一步拓展，究其根源，是能够促使当前的信息互联网向价值互联网（图6-1）过渡，为更多领域的金融和非金融创新奠定基础条件。正如德勤亚太区投资管理业主管合伙人秦谊认为：

> “区块链有可能颠覆金融行业，重塑如会计、审计等行业操作，并促生新的商业模式；这是一个新的、不断变化的技术，广泛应用于商业还需几年时间。尽管如此，为防错失机会和受到突如其来的科技冲击，各行业的战略家、规划者以及决策者都应该开始研究区块链的应用案例。”

图6-1 从信息互联网到价值互联网

（二）区块链兼具技术与制度创新

1.技术驱动下的金融创新

从技术视角看，我们可以用大数据、云计算、平台经济、移动支付这些通行概念来描述新技术，也可以概括称为ICT。ICT是信息、通信和技术三个英文单词的词头组合(Information Communications Technology，ICT)。它是信息技术与通信技术相融合而形成的一个新的概念和新的技术领域。21世纪初，八国集团在日本冲绳发表的《全球信息社会冲绳宪章》中认为：“信息通信技术是21世纪社会发展的最强有力动力之一，并将迅速成为世界经济增长的重要动力。”事实上，信息通信业界对ICT的理解并不统一。作为一种技术，一般对ICT的理解为不仅可提供基于宽带、高速通信网的多种业务和信息的传递和共享，而且还是一种通用的智能工具。

以ICT为代表的新技术能够改变什么？从宏观看，是经济金融活动的搜索成本、匹配效率、交易费用、外部性和网络效应。从微观看，则是影响企业内部的信息管理、激励约束机制、技术进步和治理环境

等。

当前，关于技术对金融的影响，国外最流行的概念就是Fintech（金融科技），即是指伴随着科学技术和管理技术的发展，为了降低金融交易成本、提高金融交易效率而在金融交易手段、交易方法和物质条件方面发生的变化与革新。金融技术创新既是金融效率提高的物质保证，同时还是金融创新的内在动力之一。正是由于科学技术特别是电子计算机技术在金融交易中的广泛应用，才使金融制度与金融交易工具发生了深刻的变化（图6-2）。

应该说，几个世纪以来技术对于金融的影响一直都存在，并非现在才凸显出来。例如，早在19世纪上半期，股票交易信号的传递是由经纪人信号站的工作人员通过望远镜观察信号灯，了解股票价格等重要信息，然后将信息从一个信号站传到另一个信号站，信息从费城传到纽约只需10分钟，远比马车要快，这一改变曾掀起了一轮小小的“炒股”热。直到1867年，美国电报公司将第一部股票行情自动收报机与纽约交易所连接，其便捷与连续性深刻激发了福斯对股票的兴趣。1869年，纽约证券交易所实现与伦敦证券交易所的电缆连接，使交易所行情迅速传到欧洲大陆，纽约的资本交易中心地位进一步凸显。可以说，区块链对金融带来的冲击，首先就是沿着技术演进的路径逐渐发生的，信息技术的发展同样是区块链产生的基础，而区块链技术则进一步推动了金融变革。

复合年均增长率（CAGR）

图6-2 全球Fintech的相关状况

资料来源：埃森哲报告：《全球金融科技投资飙升》全球范围（美国、欧洲、亚太）

2.制度驱动下的金融创新

从制度视角看，现代金融改革也离不开制度的优化。例如，从普惠金融到共享金融，更加强调金融发展中的伦理问题，重视制度经济学的影响。近年来，经济金融发展中由于出现了诸多矛盾，因此人们更加重视伦理学的引入，也就是从伦理方面对经济制度、经济组织和经济关系的一种系统研究。就此角度而言，市场经济和金融运行，它不仅是经济的，更是伦理的。

一方面，我国的金融创新动因，有一些全球性的制度要素，如普惠金融。技术所伴随的机制变革动力，能够对可持续协调发展与实现经济金融伦理作出贡献。例如，在2012年美联储的一份报告中指出，美国消费者中有11%享受不到银行服务（unbanked），另有11%享受的银行服务不足（underbanked）。而伴随着智能手机的普及化，这些人群更容易也愿意运用移动设备来享受电子银行或支付服务。另一方面，还有一些中国转轨期的特有因素。例如，目前很多互联网金融模式就是一种特殊的监管套利创新，是具有短期化特征的。如果利率进入完全市场化状态，金融市场充分竞争，客观地说很多模式的存在空间会进一步缩小，最典型的是货币基金消费支付，像余额宝，欧美货币市场基金的网络化发展轨迹其实已经证实了这一点，当然这只是其中一点，很多现象必须认识到它可能兼具技术和制度因素驱动的特征，所以分析新金融模式必须一分为二来看。

3.区块链兼具技术与制度驱动特征

区块链不仅是一系列新技术应用，更重要的是对制度与规则层面的创新尝试。一方面，虽然人们普遍认为我国的信息技术及其金融应用在很多方面已经居于全球前列，甚至已经开始“弯道超车”，但现实告诉我们这未免过于乐观。例如，国际电信联盟发布的2015年衡量信息社会发展的报告，陈述了2015年度全球ICT发展指数的排名，其中中国位居第82位，较2014年度上升5位。显然，我们的实际技术能力仍然距发达国家很远。就此而言，对区块链的应用，当前各国的差距并不太远。其中，由于金融天然就是基于共享模式，区块链技术则使金融共享的深度和广度空前扩大，更使这方面的应用尝试变得更加重要。因此，积极尝试并探索区块链的应用场景，有助于促使我国综合技术能力在“新平台”上的提升。

另一方面，技术变革最终还要落到制度变革之上。更具科幻视角的是，当未来技术获得极大变革和突

破，以至于从根本上改变人类社会的组织形式、管理模式、信息传递、资源配置时，甚至达到在理想模型中才存在的、稳定有序的、最优的宏观均衡之时，那么货币与金融的存在可能就没有意义了，到此，技术才在真正意义上“颠覆”了金融、“消灭”了金融。在此之前的较长时期内，还需要更多过渡性的改革尝试，目的都是解决现有经济金融运行中存在的矛盾，区块链也给这种制度变革探索提供了一条现实道路。

（三）区块链的价值内涵

在上述分析基础上，我们可以从以下几方面进一步剖析在“互联网+”时代区块链的价值内涵。

区块链是一套特定的规则，即分布式分类总账、智能数据库，或者一套基于网络难以改变的、公开透明的、超大容量的游戏规则。这套游戏规则为什么要改变金融市场中原有的一些规则？无非是因为现有的金融体系中有些规则可能存在瑕疵，即现有规则下的某些金融活动，或者有可能使金融中介部门拥有过强的话语权，或者使企业和居民等个体的影响力过于弱小，以致出现很多问题。例如金融消费者权益保护可能成为全球性的难题；金融创新可能成为少数部门的获利手段；资金配置成本较高，导致融资难、融资贵；信息不对称造成的各种金融服务缺位等问题。而类似区块链的这套新规则可能有助于缓解以上矛盾，使多数人都能够成为规则的参与者和维护者。为此，从规则层面而言，区块链具有重大意义。

首先，区块链价值的真正实现，需要面临以下三方面的挑战。

挑战一是区块链的初始规则如何确立？是依靠大多数投票的相对民主机制，还是一定程度上依靠线下的公共权威与信用的参与和支持？这是很重要的问题。虽然构建共享共赢式金融发展生态体系，区块链规则具有巨大的发展前景，但与此同时，不能够在初始规则确立时被少数人所利用，并由此非正当牟利。

挑战二是区块链新规则与既有规则的冲突和衔接问题，即如何应对新旧规则的相互适应和改良的矛盾。

挑战三是未来区块链的规则是由网络节点来维护的，但每个网络节点背后都有人的行为，因此，新规则离不开人。如何适应现代金融理论的发展，将人的非理性行为考虑进去，即结合行为经济学和金融学的视角，考虑非正式的规则对一些已有的正式规则的影响，也至关重要。

如果突破了以上三方面挑战，未来区块链这套全新的规则对传统金融市场规则而言，就是很重要的补充，甚至发挥主体的作用。

其次，我们认为，区块链将最先影响到金融基础设施建设，随后扩及一般性金融业务。金融基础设施主要包括核心金融基础设施和附属金融基础设施。按照国际主流概念，核心金融基础设施，又称金融市场基础设施，主要包括支付系统、中央证券存管、证券结算系统、中央对手方及交易数据库等。附属金融基础设施是一个相对广义的描述，主要包括信用体系、法律、会计、反洗钱、信息系统等。

为什么区块链主要影响的是金融基础设施？可以比较的是，过去基础设施都是公共产品，因其成本相对较高、收益较低，为此更多的是由政府、国企等来建设。但现在，在全球范围内，已有大量民间资本逐渐介入基础设施领域，无论是新技术还是新制度规则的演变，都使多元化资本介入基础设施建设的效率大大提高。金融基础设施也面临同样的问题，一些新机制使更多人有可能参与到金融基础设施建设中来，从而既降低成本、提高效率，又保证安全性。

一个直接的案例就是美联储。2015年初，美联储发布了一个提升美国支付体系效率的报告，报告中提及大量利用新技术改善美国支付体系效率的行为。例如，报告提出了一个未来在行业内可推动的方案，即便利金融机构间基于使用通用协议和标准发送和接收支付的公共IP网络直接清算。报告认为，与通过中心辐射状的网络结构清算交易相比，金融机构间基于公共IP网络的信息分布式架构有可能降低成本。因此，美联储欲在中央总账内创建报文标准、通信安全和记录交易的通用协议，以便利相应的银行间结算。同时，还要创建系统规则，保障参与机构能够直接进行实时授权的清算交易活动。由此可见，美联储希望促进这样一套分布式机制的发展，并使其更好地在支付清算体系中发挥作用，且美联储要在其中发挥主导作用。当然，在报告中，美联储还否定了另一方案，该方案是未来其所关注的，但是现在还没

有充分引起重视，这就是“数字价值转移工具”，美联储将其定义为银行体系外的一些利用分布式机制进行价值转换的机制。综上可见，美联储高度重视新技术，其更关注的是，在银行和金融机构体系之间如何发挥类似于区块链的这一套分布式新清算机制的作用，同时，美联储本身希望主导这一重大变革趋势。只是现在在金融体系之外，市场自发的价值转换的影响还没有足以使其必须要介入，但也已经充分关注。前者更像是在传统金融支付体系内运用类似于区块链的技术模式。

再次，区块链发展与应用的核心就是登记价值和交易。从长远来看，价值区块链的应用过程是从货币经济学到金融经济学。区块链技术最初源于比特币，是电子货币层面的规则创新。当然，类似的技术也涵盖了其他一些分布式规则的虚拟货币创新。其核心实际上是登记价值与交易价值。区块链这样一套规则有可能更好地从货币层面向金融层面转移，即未来，区块链如何更好地过渡到金融市场层面，这是一个很重要的挑战。区块链技术规则能否影响到资产定价模型？会对金融市场稳定性带来哪些冲击？如何解决金融市场中的非理性繁荣问题？即传统金融市场的短板、内在弊端能否是这样一套东西可以解决的？这些都是值得理论研究者思考的问题。

最后，我们认为，区块链可融合新金融与传统金融间的“代沟”。区块链技术已经开始影响或改变我们的现实生活。目前，有些人在关注，有些人关注还不够。究其原因，除对其内涵认识不足、理解不足之外，还有以下几方面原因。

第一，重大变革对人们脑海的冲击力在弱化。当前，技术变革层出不穷，很多技术变革都是边际上、在潜移默化中影响着人们的生活，很多人对此已习以为常。

第二，这些年来，金融本身一直在异化和扭曲，很多人对金融发展开始变得悲观。新技术能否改变金融存在的问题，从而带来美好社会？很多人对此存疑。

第三，金融的路径依赖性。整个金融（无论国内还是国外）已是“人到中年”，进入一种“亚健康”状态，通过一个“大手术”来解决矛盾是很困难的。如何不断地这个过程中改善体制，利用新技术、新机遇实现共享金融发展是一个重大的挑战。

第四，在商业经济时代，好的不一定是成功的，成功的才是好的，因为对机构和企业而言，短期利润追求才是最大的利益。为此，我们需要有一个更加长远的思路。发展区块链技术不是利用新金融来颠覆传统金融，而是要融合新金融与传统金融之间的“代沟”。

第五，区块链自身还有不成熟的地方，在具体应用模式方面还期待有更加具有突破性的进展。

总的来说，区块链技术并不是凭空出来的“造反派”，它有其历史理论的逻辑过程，核心是引领和涵盖一系列新技术支撑的新规则，使其更好地融入主流，改良现有体系和规则的不足，同时构建一个有利于监管传统金融机构、新型金融组织企业和消费者的共享共赢式金融发展生态体系。因此，需要一方面高度重视区块链技术和规则带来的巨大变革，另一方面理性看待其面临的风险和挑战。

二、中心化与去中心化

（一）金融的去中心化

1.金融去中心与去中介需区分

我们可以把金融功能和地理意义的中心看作是“大中心”，把金融中介的存在看作是“小中心”。

首先，金融中介一直伴随人类历史发展，比中心的出现要早得多。例如，“银行”（Bank)一词来源于古法语Banque和意大利语Banca，意即早期的货币兑换商借以办理业务活动的“板凳”。银行业也起源于货币经营业，早在公元前2000年巴比伦王国的寺庙、公元前500年希腊的寺庙以及公元前400年的雅典、公元前200年的罗马帝国等均有货币经营业的活动记载且十分活跃。

到了中世纪，商品流通进一步发展，欧洲各国贸易集中在地中海沿岸各国，以意大利为中心，因而银行

业首先在意大利出现并发展起来。一般认为最早的银行是意大利1407年在威尼斯成立的。其后，荷兰在阿姆斯特丹、德国在漢堡包、英国在伦敦也相继设立了银行。18世纪末至19世纪初，银行得到了普遍发展。

金融交易中的信息不对称、搜寻成本、匹配效率、交易费用、规模经济、风险控制等决定了中介存在的必要性。反过来看，金融中介能否真正消失，也要看新技术或制度能否解决这些基本问题。

其次，金融中心化可以包括（无形）权力中心化与（有形）地理中心化。据记载，17世纪时,伦敦的银行收款人,每天去别家银行收取欠它的现金。一天,两家银行的收款人偶然在一家咖啡馆相遇。他们俩决定当时就在那里核实彼此该收的款项,以节省时间和精力,不久,其他收款员得知了这个办法,均照此办理。从此,这家咖啡馆就成为第一个票据交换场所。各银行负责人发现了此事,有的下令不准这样做,但有些人认为这个方式有价值。后来他们定了一套规章制度,任命了一位经理负责此事,并发展成全世界的票据交换所——伦敦票据交换所。这就是金融基础设施的中心化尝试。

此后，中央银行最早发源于17世纪后半期，以瑞典国家银行和英格兰银行的创建为标志，而中央银行制度的形成则在19世纪初期，主要是以英格兰银行独占发行权为标志，最终创建真正意义上的中央银行制度是在20世纪初，主要是以美国的联邦储备系统的成立为标志。由此，现代意义上的金融中心化机制得以创建起来。同时，金融也在空间地理意义上进行集聚，如17世纪出现历史上第一个真正意义上的国际金融中心阿姆斯特丹。

我们看到，金融中心化的过程要晚于金融中介的出现，这就意味着在历史上曾经很长一段时间都有非中心化的状态与过程。历史的演变是逐渐波动的。这样就产生一个问题：短期和长期这种中心与中介的“去”会产生什么样的现象？

从形式上来看，去中心在短期内更容易实现，因为原有的中心在弱化。各个国家央行的控制力在迅速弱化，传统意义上的很多中心概念在新的网络时代也变得不一样了。金融的资产端、资金端、交易端都发生了一些变化。然而，这是否意味着传统的伦敦、纽约这样的国际金融中心发生了根本性的变革？从短期来看，去中心化比较容易；但从长期来看，本质上的去中心依旧是比较困难的。除非颠覆现有的社会权力架构和组织形式，否则真正的长期去中心化只能是空谈。

从长期来看，去中介似乎更容易实现。虽然短期内由于有很多伪中介，导致去中介比较难。但最终来看，金融演进的逻辑无非是利益、效率、安全的“三角制约”，主要技术的挑战都在于对这三个矛盾的权衡。

而当前，从技术视角看，我们关注的是为什么金融更可能去中心、去中介？从制度视角看，则需考虑为什么金融需要去中心、去中介？目前的中心化和去中心、中介化和去中介，不是简单快速地就从一个极端到另一个极端，历史的演变在很长一段时间对此是纠结的。

2.现实中的挑战与局限性

在现实中，中心化与去中心、中介化与去中介往往都不是单向变化的，而是充满了不确定性与多元性。我们可以从以下方面来分析其复杂性。

第一，真正的去金融中介（小中心）能否实现？

首先，以经常被看作是去中介代表的P2P网贷为例，实际上在国外，对冲基金和银行正在大张旗鼓地进入P2P领域——不仅通过证券化把P2P贷款重新包装为新的金融工具，还通过这些平台从事贷款业务。英国《金融时报》专栏作家吉莲·郎蒂撰文提出这是源于一个卑鄙的动机：监管套利。她在文中提到，纽约一名银行高管最近在一次会议上（带点不好意思地）解释称：‘我们喜欢P2P，因为我们在那里可以做一些我们在银行没法做的事。”

近年来，鉴于个人借贷或投资者发挥的作用逐渐变弱，而包括对冲基金和银行在内的大型机构则逐渐成为游戏主角。国外一些典型的大型P2P网贷平台也在考虑放弃‘PEER”的提法。例如，美国最大市场贷款

平台贷款俱乐部总裁瑞纳德·兰普（Renaud Laplanche）曾建议将行业名称改为“市场贷款”。《纽约时报》此前借用了第二大贷款平台Prosper Marketplace总裁对该行业的另一说法——“在线消费者金融”。实际上，作为P2P网贷典范的Lending Club来说，显然其典型业务模式也距离P2P甚远（图6-3）。

图6-3 Lending Club的业务流程

其次，就股权众筹来看，值得注意的是，目前众筹融资中的一个重要趋势就是采用“领投—跟投”模式，利用专业的领投人来进行项目筛选和风险控制，因此它更像是将传统金融中介的功能蕴含在新的投资者结构当中，而不是简单地“去中介化”。

最后，就银行业来看，美国的富国银行有6200家网点，这个数字在过去三年基本上没有变化。许多银行过去都讲过要进行银行业务网点调整，减少网点。但美国联邦储蓄保险公司的数据表明大银行业务网点并没有减少，相反在城市中心还有所增加[29]。一方面大家都认为互联网的兴起会减少人们对银行网点的需求，而另一方面许多大银行并没有减少网点。

第二，金融基础设施领域的中心化（大中心）表现（央行主导权）。

一方面，以支付清算基础设施为代表，在反思2008年金融危机之后，2012以来中央对手方清算机制（CCP）快速发展起来。该机制最早起源于场内衍生品交易市场。伴随着场外金融市场的发展，采用CCP可以有效降低对手方风险，促进市场交易活跃，有效管理系统性风险；从微观角度来看，净额轧差还可以显著提高资金使用效率，降低市场参与者的参与成本。金融危机以来，CCP在化解系统性风险方面的作用得到了充分发挥和高度重视。这确实是典型的中心化机制体现。另一方面，以区块链为代表的分布式支付清算机制，不仅在现实中促进了市场主体的积极参与，而且也引起了各国监管者的高度重视，这与CCP类似的中心化机制采取了截然不同的技术路径。

同时，就货币层面来看，由央行中心化的发行，也不是“与生俱来”的。在历史上的很长一段时间内，货币都是“非中心”的。20世纪中后期兴起的新货币经济学则认为，现有的货币、金融体系并非是自然演进的，而是法律限制或政府管制的必然结果。在自由放任的竞争性市场条件下，不一定存在集记账功能和交换手段两大职能于一身的货币，货币现有的两大职能将由不同的物质分别承担，市场中以货币为媒介的交换最终将被“精密的物物交换”所取代。可以看到，电子信息技术演进带来了货币新的“去中心化”的动力。

第三，如何看待地理意义上的中心化与去中心？

金融地理学(Financial Geography)作为近年来兴起的一门边缘学科，它的最大贡献是提供了研究金融问题的全新视角和方法论。进入20世纪90年代以后，很多经济学家认为由于IT技术的发展等，地理因素已经不重要，典型代表如奥·希林(O□Brien)提出的“地理已死”(end of geography)。我们需要思考的是，伴随着网络化、智能化时代的来临，传统空间地理意义上的国际金融中心会不会逐渐被弱化甚至消亡？

（二）区块链的去中心化

我们之所以进行上述讨论，并非是显示出对去中心、去中介的悲观态度，而是强调这些变化可能是多向的，在当前走向去中心的大趋势下，可能存在多向演变和阶段性波动。如果用“去中心化”来涵盖去中心和去中介两个概念，可以得出以下结论：在可预见的未来，可能不是金融完全去中心，而是多中心（小中心）与弱中心（大中心）。

区块链的探索道路也不是简单的去中心，而可能是多中心或弱中心。现在市场谈论较多的“去中心”，其最终结果更可能是多中心，从而弱化少数中心话语权过强所导致的规则失控。当万物互联使所有个体都有可能成为金融资源配置、金融产业链中重要的中心节点时，或许就实现了最理想的市场状况，使传统金融中介的中心地位发生改变。这种改变不是说传统金融完全被革命、被颠覆，而是从垄断型、资源优势型的中心和强中介转化为开放式平台，成为服务导向式的多中心当中的差异化中心，从而使传统中介

中心和新的中介中心获得共赢，在一个共享共赢的金融时代获得一种新的发展定位。

值得关注的是，2008年危机之后，早期的华盛顿共识走向了失败，出现了大量的中心化趋势。有的希望通过中心化来解决金融政策和交易效率，有的希望通过中心化机制来解决系统性金融风险。所以，当前市场面临的一个重要挑战实际上就是“中心化”与“弱中心”的挑战。

区块链带来的多中心和弱中心能否解决相应的2008年危机所昭示的效率和风险的矛盾？能否改变现代金融体系的内在脆弱性和创新失控等问题？作为研究者，目前我们非常有信心，这种信心来源于对理论内涵和逻辑线索的把握。但与此同时，这种变革并不是轻而易举的，它需要在实践层面有更深入的研究和探讨。因为当前的时代正是一个中心化与去中心都非常突出的矛盾冲突时代，现代共享金融则可以实现二者融合，也可以努力用区块链的技术来解决传统中心化难以解决的矛盾。

回顾历史，展望未来，基于中国古代的阴阳五行理论，可以看到金融发展中需避免“过犹不及”，而中心与去中心，也是“合久必分，分久必合”的关系。当前，长期中心化金融模式的弊端逐渐显现，历史“天平”开始向“去中心”一方偏离，当然这一过程可能是长期的。

区块链能够遏制传统“中心化”模式下的“短板”，也是为了达到罗伯特·希勒在《金融与美好社会》一书中所描述的目标。希勒教授是理想主义者，他相信人性的光辉。“通过技术安排为公众的利益重塑金融业，把金融业作为人类财富的管理者；通过公众的广泛参与，让金融业为人类社会的良性发展服务。全民的广泛参与也会打破金融的精英权力结构，使金融民主化，并实现财富分配的公平。”国际货币基金组织副总裁朱民这样总结《金融与美好社会》一书作者罗伯特·席勒的理想。所有这些都可以通过区块链的非中性化模式来设计，促进更多主体（节点）的参与及金融话语权提升。

如何探索出一条通往“金融与美好社会”的梦想之路？共享金融自诞生之日起就被寄予了厚望。作为共享金融重要抓手的区块链技术，实际上代表了去中心化的机制，无疑能够为人类迎接“金融与美好社会”提供最好前景。

最后，还需要注意的是，区块链带来的金融创新与去中心化不等于全民搞金融，因为当大量游离于监管之外的“灰色金融”泛滥，或者弱势群体通过“过度负债”来消费和投资，同样会带来巨大的系统性风险。

三、区块链与共享金融

（一）共享经济

2015年10月29日闭幕的中共十八届五中全会首次提出“创新、协调、绿色、开放、共享”五大发展理念。其中“共享”发展理念主要是突出人民主体地位，强调必须坚持发展为了人民、发展依靠人民、发展成果由人民共享，做出更有效的制度安排，使全体人民在共建共享发展中有更多获得感。

经济共享发展的理念一直贯穿在经济学演进与各国实践中。早期的共享经济理念主要针对市场经济国家快速发展中的收入分配矛盾，试图通过优化和完善分配结构，从根源上解决现代资本主义的某些失衡，缓解日益凸显的各阶层利益冲突。进入21世纪之后，互联网信息技术深刻改变了经济与社会组织结构，对信息采集、处理、交换产生了深远影响，对诸多行业的生产与商业模式产生了冲击。这不仅使剩余资源的使用效率、使用方式变得更丰富，抑制了资源价格的过度膨胀，同时也使消费者主权得到进一步提升，通过“使用权”而非“拥有权”的交易，就能够更好地享受经济发展的成果。

2016年政府工作报告中也指出：“支持分享经济发展，提高资源利用效率，让更多人参与进来、富裕起来；要推动新技术、新产业、新业态加快成长，以体制机制创新促进分享经济发展，建设共享平台，做大高技术产业、现代服务业等新兴产业集群，打造动力强劲的新发动机。”

从根本上看，共享经济是技术进步的结果，共享经济产权层面的特点是所有者暂时让渡使用权以获取收入的租赁经济，但是这种经济模式在互联网时代以前没有形成气候。云计算、大数据、物联网、移动互联网（云大物移）大大降低了租赁交易的信息成本，减少了信息不对称，使原本不可能达成的租赁交易成为可能。可以说，共享经济模式带来的最大好处包括更节约的时间、更优化的资源配置和更灵活的就

业。

当然，一方面，共享经济给消费者和直接从业者带来了实惠（除了收入，还有更多的从业自由），有人认为它的发展空间很大。《零成本社会》的作者里夫金(Jeremy Rifkin)指出共享经济是一个方兴未艾的新体系，并预测共享经济将颠覆许多世界大公司的运行模式。另一方面，共享经济挑战了传统商业模式以及现有制度安排，可能损害既有从业者利益，继而引起一些社会问题。

可以预期的是，共享经济将快速改变大量现有行业，例如快递业、家政服务业、教育行业、培训业、个人服务业、新闻业、租赁业、广告创意业、医疗业、个人旅游业、宠物寄养业、社区养老业等。

（二）共享金融

所谓共享金融，就是通过大数据支持下的技术手段和金融产品及服务创新，构建以资源共享、要素共享、利益共享为特征的金融模式，努力实现金融资源更加有效、公平的配置，从而在促使现代金融均衡发展和彰显金融消费者主权的同时，更好地服务于共享型经济发展道路，进而促进经济社会的创新、协调、绿色、开放型发展。

共享金融发展的基本动力，包括技术（新的信息技术+新的金融技术）与制度（新的正式规则+新的非正式规则）。这两大核心要素和基本动力，既带来了全新的金融创新模式（自金融模式），也引起了对传统金融的改革与完善，更有二者的融合式创新。

值得注意的是，无论从技术还是制度来看，互联网金融体现出的都是共享金融的核心理念。时光向前追溯，早期促使金融得以变革的技术与互联网无关，可能是电报、电话等，而源自草根的金融萌芽却一直带有互助共享的色彩，直到被大资本的贪婪所淹没。未来的物联网可能替代当前的互联网形态，主流的信息技术也可能发生难以想象的演变，但是金融发展目标，仍然是如何进一步在金融运行中体现出个性与民主，遏制金融巨鳄的“丑恶”与金融面纱的“虚妄”，在决策共举、各方共赢、利益共分、机制共建、风险共担、事业共助的基础之上，构建真正有利于美好社会的“好金融”。由此来看，即便互联网金融一词终将消逝在历史长河之中，共享金融的生命力也能够伴随金融理性、道德、自律的成长而延续下去。

（三）区块链助力共享金融

作为一种去中心化的机制和信用共识机制，区块链有助于推动共享金融的模式不断扩展和演变，从而推动整个现有金融产业链的不同层面都能够进一步实现资源的共享、共赢发展。

展望未来，区块链技术所助推的共享金融应该呈现如下发展路径。

第一，金融终端的资源与功能共享。从国家资金流量表（金融交易）来看，在非金融企业、金融机构、政府、住户这四大部门中，其中住户部门是典型资金净流出，也是金融资源交易链条的起点。在主流金融运行模式下，住户资金只能通过间接融资市场（银行为主）、直接融资市场（股票和债券市场为主）、结构性融资（复合型的证券化产品）等，进入到一国的“金融血管”之中。在此过程中，住户部门往往缺乏有效的话语权，只能作为金融机构“厂商”的“原材料”提供者。在区块链推动的共享金融发展模式下，首先意味著作为金融产业链上游的住户部门，应该在金融产品和服务的提供中发挥更大的作用、拥有更高的地位。因为住户部门可以借助于互联网技术、开放的平台、众律性的规则，低门槛地直接成为金融资源的供给者，使金融产业链进一步“前移”，从而对主流金融部门的“谈判权”形成制约。对住户部门来说，这实现了与金融部门的责权“共享”。

第二，金融媒介与渠道的共享。互联网的发展带来了一个全新的大平台经济时代，平台的参与主体越多，对供给、需求、中介各方的利益和价值就越大。平台经济的开放特征与传统金融部门的封闭式发展，本来就形成了鲜明的对比。平台经济与金融的发展恰恰反映了共享金融的核心思想。一方面，传统的金融与非金融部门的边界进一步模糊，主流金融机构面临更加明显的“脱媒”，越来越多的主体参与到金融产品与服务的提供中，成为重要的金融资源流转中介。另一方面，越来越多的“金融厂商”转换成为“金融平台服务商”，平台经济效应使“自金融”模式在效率和风控上成为可能。所有这些变化虽然仍处

于萌芽阶段，但是对于传统金融中介与新兴金融中介围绕渠道的共享，对于金融供给者、需求者、中介依托合作平台的共享，都提供了令人振奋的发展基础。

第三，金融消费与需求的共享。对于金融消费和需求来说，面临的是日益复杂多样的金融产业链，而新技术和制度变化将有助于其“拨云见日”，更充分地参与到金融运作之中。一是对于需要金融资源流入来维持的企业部门来说，其中的小微企业是最为“饥渴”的需求者，有限的金融资源支撑着其在就业方面的巨大贡献。共享金融的理念和模式必须着眼于为其创造可持续的金融“输血”模式。二是金融资源的流动并非单向，而是双向甚至多向，在众多维度上同时交织在一起。例如，居民也是消费金融的资金需求者，企业可能是资产管理的资金供给者，在此过程中，既需要着力实现不同角色功能的共享与转移，也应促进以共享理念来提高不同定位中的企业和居民对于金融中介的“谈判权”。三是推动金融创新更加重视需求导向，在技术可行的支持下，实现“流水线”式的标准化“金融快餐”与“口味各异”的“金融风味小吃与大餐”并行发展。

第四，金融风险与监管的共享。一方面，现代金融体系之所以存在许多功能缺失，原因之一就是风险的不可控或弥补的高成本。例如，在小微金融和普惠金融领域，信息的不确定、信用基础的缺乏等加重了金融服务困难，而如果实现不同组织与主体的信息系统交互、风险合理共担，则有助于介入那些传统的金融“空白区”。再如，系统性风险与非系统性风险的边界，其实并没有教科书中那样分明，在“动物精神”与“冰冷技术”共存的现代金融市场上，风险预期提升、普遍恐慌、羊群效应、以邻为壑等现象的存在，都容易助推风险的积累。由此，随着新技术使得微观金融行为的甄别能力上升及不确定性分析的越加准确，通过某种技术与制度安排对风险进行合理分担和分散，而非“游牧民族”式的驱离或被投机利用，则成为区块链式共享金融有助于金融稳定的重要尝试。另一方面，区块链技术与规则的探索可以推动社会信用体系的完善，尤其是对于难以进入到传统金融体系来积累信用的主体来说，介入共享金融实践可以为其创建金融信用基础。同时在“人人参与”的新模式中，自律与他律成为能否继续参与的前提，这也使传统金融监管难以覆盖的“盲区”受到公共金融规则的约束，从而实现新旧监管模式的共存。

第五，金融与实体的共享式发展。无论在经济上还是统计意义上，金融与非金融部门在本质上就是相依相存的，金融部门的利润很大程度上是与实体部门交易完成的，只是随着金融部门权力的扩张和衍生金融产品创新失控，才出现了某些“自我游戏”式的交易。区块链助推的共享金融模式，强调的是与实体部门的共赢发展，包括使多数微观主体充分享受经济增长与金融发展的成果；有利于实体部门规模和结构的完善，而非强化已有的矛盾；避免内部结构失衡和金融创新的失控；解决好金融部门与实体部门之间的分配问题；减少行政性干预，强调市场化运行机制和自律环境优化。综上所述，在全新的共享金融理念的引导下，现代金融发展将从“脱实向虚”转向“以实为主、以虚为辅”。

四、区块链与货币创新

（一）无现金社会

当前，随着互联网时代的技术进步不断推进，作为金融基础设施重要组成部分的支付体系正在发生着根本性变革。

在世界各国，当前现金使用比率的下降，确是不争的事实。其根源还是电子支付、电子货币带来了更高的效率和更低的成本，当然也有助于“魔高一尺、道高一丈”的违法追踪与风险控制。根据可得到的最新数据，凯捷(Capgemini)与苏格兰皇家银行集团（RBS）联合发布的《2015年全球支付报告》显示，2014年非现金支付交易量增速预计达到8.9%，高于2013年的7.6%，创下3897亿美元的交易量新高。另据国际清算银行(BIS)统计，2014年19个最大经济体的流通中现金余额为国内生产总值(GDP)的7.9%，2010年则为8.4%。

目前，我国的非现金支付增速业已居全球前列，近年来银行和非银行支付机构的电子支付业务较快增长，其中，由于网络经济的快速增长、智能手机用户数量的大幅提升，使我国成为全球范围的移动支付高增长区域，也是新支付技术的实践“热土”。例如，2016年2月18日苹果公司Apple Pay移动支付服务正式登陆国内市场，引起了业界、媒体和“果粉”们的热议。

对此，一方面，从需求角度看，老百姓更加适应非现金的电子化支付模式的运用，因为网络购物、线下电子支付场景正日益完善。另一方面，从供给角度看，新兴电子支付技术已经更加成熟，各类机构不断推出效率与安排相协调的支付工具与方式。

根据央行统计，2015年，全国共办理非现金支付业务943.22亿笔，同比增长50.4%，增速较2014年提升25.29%；共处理金额3448.85万亿元，同比增长89.76%，增速较2014年提升76.71%。在非现金支付中，电子支付尤其是移动支付业务保持快速增长，非银行支付机构发展势头迅勐。2015年，银行业金融机构共发生电子支付业务1052.34亿笔，金额2506.23万亿元。其中，移动支付业务尽管总体占比较小，但发展速度较快，2015年全年发生业务138.37亿笔，金额108.22万亿元，同比分别增长205.86%和379.06%。2015年，非银行支付机构累计发生网络支付业务821.45亿笔，金额49.48万亿元，同比分别增长119.51%和100.16%。

无论在发展中国家还是发达国家，新兴电子支付不仅能够替代纸币的支付功能，而且能够依托支付渠道解决弱势人群的金融需求。例如，肯尼亚M—Pesa手机银行的出现，使移动业务与家庭汇款等基本金融需求密切结合起来，充分体现了移动支付的高效率和低成本，较好地满足了落后地区的支付需求。再比如，美联储在2012年发布的报告就表明，在美国的消费者中还有大约11%的人无法享受到银行服务，另有11%的人只享受到较低水平的银行服务，而与充分享有银行服务的人相比，这些人往往属于弱势群体，但他们却多数都拥有智能手机，并且也愿意使用移动银行和移动支付。由此来看，在我国，除了城市的中低收入人群，广大农村领域也应是以新兴电子支付来践行普惠金融的重要试验田。

在政策支持和科技进步驱动下，似乎全球都不可避免地从现金走向电子支付。2013年挪威学者纯德·艾德森（Trond Andresen）就在一篇工作报告中指出，“实物货币的必然消亡只是个时间问题”。当然，这一过程可能是漫长的，因为纸币仍然有其需求空间。例如据统计在美国，50~100美元的交易只有16%用现金，而1美元以下的交易则有66%以现金完成。由此来看，无现金社会也需要支付习惯的转变，以及电子支付真正在低成本、便利与安全之间做到极致。

（二）数字货币支付

电子支付的变革与货币形态的变化也是密不可分的。此前，央行召开数字货币研讨会，周小川行长也就此接受了采访。数字货币这一公众相对还较陌生的概念，迅速引起了各界的关注和热议。实际上，虽然近年来数字货币已经成为业内流行的全新概念，但迄今为止还没有统一的内涵边界。

如果要追根溯源，则需从电子货币的概念着手讨论。根据巴塞尔银行监管委员会（BCBS）的定义，电子货币是指通过销售终端、设备直接转账或电脑网络来完成支付的储存价值或预先支付机制。国际清算银行（BIS）早在1996年就开展了一系列研究，并认为电子货币可能会影响到中央银行的货币政策，如影响央行控制的利率和主要市场利率的联系。

客观来说，一方面，长期以来央行依然具有垄断性的货币发行权，同时也基本掌控着主要电子货币的发行权；另一方面，电子货币也给货币政策理论框架带来了很大冲击，因为“货币”的可控性、可测性、相关性都在发生变化。当然，随着新技术日新月异的变化，逐渐出现了可能脱离央行控制的新兴网络电子货币形态。在新技术的冲击下，究竟什么是“货币”可能越来越说不清楚了，其概念、范畴、转移机制都在发生变化。其中，大额与小额、银行与非银行、中心与去中心产生了不同形态的货币及货币转移带来的深刻影响，这体现为对货币数量、价格、货币流通速度、货币乘数，以及存款准备金等制度的冲击。

进一步梳理电子货币的发展脉络，需要从货币背后的信用最终支撑入手。

第一，最为典型的法定电子货币的信用支撑，或者直接来源于各国央行，或者是由银行业机构提供直接支持，央行依托委托—代理关系给予间接信用支撑。以信用卡为代表的传统电子支付创新，以及金融机构电子钱包的出现，实际上都属于货币的形态和体现发生了变化，但没有跳出央行信用直接或间接的覆盖范畴。

第二，伴随着电子商务的发展，越来越多的非银行机构介入电子支付工具中，也对货币结构和范畴带来

了新的影响，其信用最终性支撑与央行的联系变得更弱一些，因此成为各国监管的重点。如欧盟专门制定规则，用以规范在信用机构之外发行以电子货币为支付方式的企业或任何法人。

第三，在多元化的网络经济时代也出现了由某些“网络货币发行主体”提供信用支持的虚拟货币。如果这些虚拟货币最终用于购买程序开发商所提供的电子产品，则交易中真正发挥媒介作用的是现实中的货币，虚拟货币并未形成独立的电子货币。如果虚拟货币不是从程序开发商中兑换获得、且交易对手不是货币发行方（程序开发商），那么这种虚拟货币就可能独立地在虚拟世界里执行其商品媒介的功能，如游戏玩家间在淘宝网上用人民币交易某种游戏币。当然由于规模通常较小，其对现实经济的影响并不显著。

第四，20世纪80年代，一批国外专家开始研究基于特定密码学的网络支付体系，并且探讨了匿名加密货币，由此出现了作为电子货币高级阶段的、新型数字货币的萌芽。到2008年中本聪发表论文描述比特币电子现金系统，2009年比特币诞生，使我们对数字货币探索到了新阶段。当然，目前数字货币多少都存在各种缺陷，比特币的资本属性也似乎多于货币属性，并且常常陷入炒作带来的价格波动中。

总的来看，严格意义上的数字货币属于最后一种，更多开始依托以区块链为代表的分布式规则、智能代码来发行和运行，其信用支撑距离央行的中心化机制越来越远，虽现在规模尚小且技术还需成熟，但未来对现有货币机制可能带来重大影响。对于数字货币与区块链的关系，需要从不同角度来看，例如当我们谈到比特币时，它实际由区块链底层技术（协议与客户端）和现实存在的加密数字货币组成。依托于区块链或其改良技术，也出现了其他一些类似比特币的虚拟货币。此外，虽然是当前最典型的技术，但数字货币的底层支撑不一定限于区块链，同时区块链也可以进一步拓展到货币之外的各类去中心化价值交换活动。

因此，当我们谈到数字货币的时候，一种强调的是新型的电子货币，可以利用加密技术实现独立于中央银行之外，按照特定协议发行和验证支付有效性；另一种则是对现有电子货币典型模式的进一步优化，从而既引入包括赋予货币智能合约之类的新技术支持，又保持央行对货币运行的适度控制力。就我国央行来看，短期内应该更为关注的是后者。

从现金到非现金支付、从传统卡基电子支付到网基电子支付、从简单电子形态支付到智能代码支付、从支付工具层面到货币层面，应该说新技术在不断改变着货币金融体系。最终有可能带来更高的交易效率、更低的成本、更精准的政策执行、更有效的反洗钱等风险控制，从而深刻改变着老百姓的生活，并使我们有可能在全球货币体系变革中争取更多话语权。当然，这些目标并非轻易能实现，夸大或低估其影响都是不理性的，还需大量的研究探索，专业的普及与公众教育，从而“挤出”数字货币领域的违法者、投机者与行业“劣币”。

五、区块链与金融创新

除了数字货币之外，区块链的其他金融应用也有广泛的前景。例如在支付清算基础设施领域，SWIFT作为一个链接了数万家银行的通信平台，已经被新兴崛起的区块链技术所威胁，一些区块链初创企业和合作机构开始提出一些全新的结算标准，如R3区块链联盟已经制定了可交互结算的标准，截至目前，全球已有近50家大型银行和金融集团加入了R3。

（一）金融应用领域

如在资本市场方面，据华尔街日报于2015年11月报道，世界上一些最大的交易所、银行和交易服务公司已联合成立了一个跨行业集团，命名为“交易后分布式总账工作组”，探索区块链将如何改变证券交易结算方式。参与机构包括伦敦证券交易所、伦敦清算所、芝加哥商品交易所、瑞银集团以及欧洲清算中心。区块链可以创建一个开放式、防篡改的交易总账，它可能取代并简化证券交易中许多复杂的系统。任何类型的金融资产，比如债券或者股票，都可以转变成编码，通过区块链来完成传输交易，而无须到清算所。这意味着股票交易结算过程可能在几分钟内能完成，而不需要耗费两三天的时间。此外，纳斯达克（Nasdaq）总裁兼首席运营官弗里德曼在2016年4月表示，区块链技术可以让金融机构例如纳斯达克追踪到任何资产类别的最终所有者。纳斯达克在世界范围内向超过100个地区的交易所和清算机构提

供技术支持，公司正在与客户讨论区块链技术以及它的潜在用途。她认为，在纳斯达克的技术空间里，区块链可以缩短结算时间以及释放银行中的资本，区块链技术有发展的潜力，但是需要一点时间。

区块链还可以应用到票据领域。票据是一种有价凭证，其在传递中一直需要隐藏的“第三方”角色来确保交易双方的安全可靠。比如在电子票据交易中，交易双方其实是通过了人行ECDS系统的信息交互和认证；纸质票据交易中，交易双方信任的第三方是票据实物的真伪性。但借助区块链，既不需要第三方对交易双方价值传递的信息做监督和验证，也不需要特定的实物作为连接双方取得信任的证明，实现了价值在点对点之间的“无形”传递。另外，在实际的票据交易中，经常会有票据中介这一角色利用信息差撮合，借助区块链实现点对点交易后，票据中介的现有职能将被消除，并以参与者的身份重新定位。[30]

再者，区块链有助于金融信用体系建设。目前，商业银行信贷业务的开展，无论是针对企业还是个人，最基础的考量是借款主体本身所具备的金融信用。各家银行将每个借款主体的还款情况上传至央行的征信中心，需要查询时，在客户授权的前提下，再从央行征信中心下载参考。这其中存在信息不完整、数据不准确、使用效率低、使用成本高等问题。在这一领域，区块链的优势在于依靠程序算法自动记录海量信息，并存储在区块链网络的每一台计算机上，信息透明、篡改难度高、使用成本低。各商业银行以加密的形式存储并共享客户在本机构的信用状况，客户申请贷款时不必再到央行申请查询征信，即去中心化，贷款机构通过调取区块链的相应信息数据即可完成全部征信工作。[31]

最后就保险方面来看，基于区块链的风险管理模型，可能包括自管理或风险管理协议，点对点保险平台，以及充分的资金解决方案。应该说，近年来国内大力推动的相互保险，实际上就与区块链技术有天然的联系，因为其具有安全性、信任、交易更直接、效率等保险业需要的基本特质。2015年底，劳合社（Lloyd□s）在伦敦举行研讨会，强调将区块链及其他技术应用到保险市场，并将其作为现代化计划—目标运营模式（Target Operating Model，TOM）的一部分。劳合社运营总监思瑞·坎瑞（Shirine Khoury-Haq）在一份声明中提道，区块链技术有望增加保险市场的风险记录能力、透明度、准确度以及速度。埃森哲的常务董事艾比译·让拉（Abizer Rangwala）指出：“保险业正在观察区块链技术，慢慢摸清区块链技术的真正商业用途或者说在一定程度上区块链的实际用例是什么。毫无疑问，未来几年内，区块链技术将成为在保险业生态系统中的主流技术。”

（二）应用前景分析

当前，IBM、摩根大通和其他一些大机构以及美联储为什么要重视区块链这套分布式的去中心机制？它们不是要为自己培养一个完全的颠覆者，而是希望把握未来的不确定性，在这个新的机制中掌握一定的话语权。

如果传统（金融）机构做的是规则1.0，互联网（金融）企业是2.0，那么区块链就是3.0，2.0的互联网（金融）企业对于区块链不积极，因为它们正处于赚钱比较容易的黄金时期，并且本质上还是一种中介化的替代机制，对于大数据的集中掌控；1.0的传统金融机构更积极，因为它们的竞争压力更大，在2.0的竞争中已经落后，还不如直接跳到3.0的竞争。但是，历史上的转换值得我们思考。技术的快速变革令人惊讶，从一代到下一代的迭代似乎瞬间就可以完成。正如过去人们不相信人工智能可以打败世界顶尖围棋手，但当“阿尔法”赢了李世石，人们仿佛突然发现一列技术革命的“火车”扑面而来。而当你认识到技术来到眼前的时候，它其实已经离你远去了。这就是新技术的挑战值得我们敬畏、探讨的原因。

总而言之，我们需重视区块链和数字货币的巨大挑战，但不应神化！区块链的生命力在于打开了冲击既有僵化体系的“潘多拉之盒”。但在初始阶段，除了理念转变与宏观把握，最需要的是专业技术人才的培育、应用技术的拓展与实践项目的落地。

此外，由于这个领域是跨界的，只了解程序而不了解技术是行不通的，只了解金融不了解技术也会面临挑战。但是也不要把什么东西都装进去。无论中心化还是去中心，背后都是规则（技术规则+ 制度规则）之争；衡量其成功与否的标准，则是能否真正有益于“实现好的社会”。

参考资料

姚余栋，杨涛.共享金融：金融新业态［M］.中信出版社，2016

罗伯特·席勒.金融与好的社会［M］.中信出版社，2012

杨涛.区块链——构建共享共赢式金融发展生态体系［J］.当代金融家，2016（2）

杨涛.区块链与金融中心化挑战［J］.当代金融家，2016（4）

杨涛.新技术引领数字货币演变［N］.人民日报，2016-05-03

中国人民银行支付结算司.2015年支付体系运行总体情况.中国人民银行，2015

美联储.Strategies for Improving the U.S. Payment System，美联储网站

美联储.Use of Financial Services by the Unbanked and Underbanked and the Potential for Mobile Financial Services Adoption

[27] 本章由杨涛写作完成。杨涛，研究员，博士生导师。中国社会科学院金融研究所所长助理，中国社科院金融所支付清算研究中心主任、中国区块链研究联盟主任。研究方向：货币与财政政策、金融市场、产业金融、政策性金融、支付清算。

[28] [美]梅兰妮·斯万.区块链：新经济蓝图及导读［M］.北京：新星出版社，2015.

[29] 王强.银行网点过时了吗［N］.财新网，2015-03-26.

[30] 上海金融学会票据专业委员会课题组.区块链技术如何运用在票据领域［N］.上海证券报，2016-04-23.

[31] 蔡钊.区块链技术及其在金融行业的应用初探［J］.中国金融电脑，2016（2）.

第七章
区块链政策与法规[32]

一、各国政府的监管态度

（一）对加密货币的态度

比特币作为区块链技术运用的典型代表，已存在了数年之久，比特币的广泛使用与随之而来产生的影响力已经让各国的立法者无法忽视。各国针对比特币制定了相应的监管政策。尽管像比特币这样的加密货币因为“货币属性”而具有一定的特殊性，但仍可以帮助我们来推测各国政府对区块链技术可能采取的态度。

1.美国

美国意识到数字货币如比特币可用来支付商品、服务或持有用作投资。2014年3月，美国关于数字货币的指引，认为数字货币不是货币，而是一种商品，对比特币交易应当征税。[33]这意味着在美国对于诸如比特币、莱特币或其他加密货币的使用将会支付更高昂的成本。

2014年6月，美国加利福尼亚州州长签署了一项编号为AB129的法律，保障加州比特币以及其他数字货币交易的合法化。该法律规定，在确认不违法的前提下，法案将保障包括数字货币的替代货币在购买商品、服务以及货币传播中的使用。美国纽约州在2014年7月公布了监管比特币和其他数字货币的提案。提案提出要在纽约州开展经营活动，从事数字货币的买卖、存储或者兑换的公司必须要申请许可证。依照提案，比特币公司不仅仅需要追踪其客户的物理地址，还需要追踪利用比特币网络向其客户转账的人的物理地址。这会降低比特币的基本价值。最大的比特币交易平台之一的Coinbase于2015年1月在美国得到了包括纽约州、加州在内的25个州的认可，未来有望获得更多州政府的认可。

美国商品期货交易委员会（U.S. Commodity Futures Trading Commission）在2015年9月正式将比特币和其他数字货币定义为商品。该委员会将监管比特币相关的交易活动。在美国如果一家企业想要经营一个比特币衍生品或期货的交易平台，将需要申请成为掉期合约执行机构或指定合同市场。

2.欧盟

德国联邦金融监管局在2011年11月制定了一份“金融工具”备忘录，赋予“比特币”与外汇同等的地位，并规定比特币为一种“记账单位”（Unit of Account），而非法定支付手段。2013年8月，德国财政部宣布，德国或将认可比特币是一种记账单位，但不具备充当法定支付手段的功能。比特币的持有者将可以使用比特币缴纳税金或用作其他用途，德国也将成为全球首个认可比特币的国家。

2015年的“巴黎暴恐事件”发生后，匿名者黑客组织附属组织“幽灵安全”（GhostSec）称，他们相信比特币是极端组织“伊斯兰国”加密货币的首要形式，并且已经在“深网（Deep Web）”上定位到几个“伊斯兰国”用来接受捐赠的网站。为应对恐怖主义使用加密货币所带来的威胁，欧盟委员会计划强化对“非银行支付方式”的控制，如电子支付、匿名支付、数字货币支付以及黄金和其他贵金属的转移。法国的中央银行法兰西银行在2016年发布了一份题为《数字时代的金融稳定性》的新报告，在报告中提到法兰西银行正在考虑跟随区块链技术的发展计划，既包括区块链可能的应用，还包括区块链存在的问题，特别是安全性。

2015年10月，英国财政部的经济秘书哈里特·鲍德温在一次演讲上表示，英国正致力于将数字货币交易所引入监管体系，并努力为加密货币企业创立合适的制度以吸引海外投资者到英国投资，且英国财政部先后设立了1000万英镑的加密货币研究资金。

2015年10月，为了澄清了欧盟内部对于比特币属性的争议，欧盟法院（Court of Justice of the European Union）做出裁决，认为比特币应该被视为一种支付手段，根据欧盟的相关法律，这种交易应免征增值税。该裁决免除了比特币的税收威胁，否则将增加购买或使用比特币等数字货币的成本。该裁决向比特

币合法化迈出坚实一步，加快了比特币在欧盟的市场的进一步发展。这项新规源于2014年6月发生在瑞典的一场争论。当时，瑞典税务局与比特币论坛运营人丹尼尔·海德奎斯特（Daniel Hedqvist）就比特币交易是否需要缴税这一问题展开了争论。

3.中国

2013年12月，为了应对比特币交易在市场上的日益流行，中国人民银行、工业和信息化部、中国银行业监督管理委员会、中国证券监督管理委员会以及中国保险监督管理委员会五个行政部门联合发布了《关于防范比特币风险的通知》。在通知中明确："虽然比特币被称为'货币'，但由于其不是由货币当局发行，不具有法偿性与强制性等货币属性，并不是真正意义的货币。从性质上看，比特币应当是一种特定的虚拟商品，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。"消息发布后，在全球范围内比特币的价格急转直下，当时全球最大比特币交易市场Mt.Gox在一天之内的跌幅就达到了29.44%。该《通知》同时要求"各金融机构和支付机构不得以比特币为产品或服务定价，不得买卖或作为中央对手买卖比特币，不得承保与比特币相关的保险业务或将比特币纳入保险责任范围，不得直接或间接为客户提供其他与比特币相关的服务"。通知的出台基本划定了金融与比特币之间的红线。自此以后，中国监管层面后续再没有就比特币出台其他相关规定，但银行根据上级部门的约谈或电话的要求开始对比特币交易关闭充值接口，看似给以比特币为代表的加密货币判了"无期徒刑"。

但在2016年1月20日举行的央行数字货币研讨会上，传递了一个明确信号：央行将争取早日推出数字货币，并早在2014年就成立了专门的研究团队。只是加密的算法、防伪技术因为涉及国家金融安全，肯定会不同于比特币。至于央行后续是否会选择基于区块链技术的数字货币，需要看进一步的研究结果，但数字货币的发展已势不可当。

（二）对区块链的态度

区块链技术方兴未艾，目前各个领域的运用还算不上随处可见，更多的是开展可行性研究。但区块链技术所具有的潜力依然获得了政府，尤其是金融监管机构的高度重视，考虑将区块链技术投入政府服务中去。

2015年5月，洪都拉斯政府与美国区块链企业公证通（Factom）合作，以创建一套基于区块链技术的土地登记系统。[34] 不过该项目在实施过程中遭遇了挫折，据公证通发布的新的进展公告，称其先前宣布的概念证明项目已经"停滞"。

据韩国央行在2016年1月发布的一份最新研究报告显示，韩国央行正在密切关注区块链技术的发展，甚至在自己研究区块链技术。这份报告由韩国央行的支付系统研究小组撰写，介绍了数字货币和分布式总账技术，并对该技术在未来的发展状况做出了预测。报告认为数字货币还不太可能成为主流应用，因为价格波动过大、技术操作复杂、面临被黑客攻击以及终端用户丢失私钥的风险。[35] 突尼斯政府则计划通过Monetas所提供的区块链技术发行本国货币。Monetas在突尼斯首次实现了完整的数字支付生态系统中的应用。随着Monetas驱动的法国邮政突尼斯安卓应用程序的推出，突尼斯人将可以使用他们的智能手机，实现瞬间移动汇款、在线支付商品和服务、支付工资和账单、管理政府官方身份证明文件。2016年2月，中国人民银行行长周小川接受媒体采访时，也表示央行在发行数字货币时会考虑使用区块链技术，对区块链技术的优缺点进行进一步的研究。

英国政府科学办公室在2016年1月发布了名为《分布式账本技术：超越区块链》的报告，报告中强调分布式账本技术可以实现完全透明的信息更新与共享，减少欺诈、腐败，降低错误率和用纸成本，提高行政效率，并重新定义政府与公民在数据共享、透明性和信任方面的关系。2016年4月，英国内阁办公室部长马特·汉考克表示，区块链技术能为政府提供一个以公开可验证的方式来监控资金的移动，可以利用区块链的透明性对资金支付到研究中心发挥更好的控制，以帮助学生组织或个人。英国政府目前正在探索使用区块链技术提高纳税人税款的分配效率，例如补助金。英国政府正在查看如何使用区块链技术来管理和跟踪公共资金的分配，例如补助金和学生贷款，马特·汉考克认为区块链技术可能会"推动产生一种新的信任文化"。

澳大利亚标准机构标准澳大利亚（Standards Australia）在2016年4月已经要求国际标准化组织（ISO）为区块链技术设定全球标准。Standards Australia的行政长官艾德里安·奥康奈尔表示：“在全球不同区块链交易商之间实现区块链的互操作性是释放区块链潜力的关键。这就需要有全球标准来释放区块链潜力，而最好的方式就是通过ISO来实现。”

二、区块链资产的合法性问题

在互联网领域，各种新技术高速发展、层出不穷，各种新型权利也不断涌现。法律法规对新型权利的认可难免滞后，很多新型权利无法及时得到法律法规的认可，因此应谨慎判断互联网领域的合法性。

区块链技术正是互联网领域最新的发展成果之一，讨论区块链资产的合法性问题，应综合考虑区块链资产是否具有强大公众需求和商业应用前景，是否损害公众利益，是否影响网络安全。并需要从现行的法律制度、司法实践或行政机关的态度中查找区块链资产的法律依据。

区块链技术拥有巨大的商业潜力，各种基于区块链技术的产品不断涌现。包括中国在内的各国政府也都对区块链技术持开放态度。对于区块链资产，只要不违反法律法规，不损害社会公共利益，其合法性就可以得到保障。

（一）法律

《宪法》是国家的根本大法，也是拥有最高的效力的法律。《宪法》第十三条对财产保护进行了规定：“公民的合法的私有财产不受侵犯。国家依照法律规定保护公民的私有财产权和继承权……”根据《宪法》的规定，区块链资产只要是合法取得的，就应是受到法律保护的财产，并且可以享有私有财产权和继承权。

在我国的民法体系中也有着类似的规定，《民法通则》第七十二条规定：“财产所有权的取得，不得违反法律规定。”同时，《民法通则》对公民个人财产的类型进行了开放式的列举，以备新的财产类型出现，《民法通则》第七十五条第一款规定：“公民的个人财产，包括公民的合法收入、住屋、储蓄、生活用品、文物、图书资料、林木、牲畜和法律允许公民所有的生产资料以及其他合法财产。”该条文列明了财产的范围，并且明确了取得财产权的条件。尽管在《民法通则》中没有明确规定区块链资产或者网络资产，但区块链资产毫无疑问属于“其他合法财产”的范畴。只要是通过合法方式取得的区块链技术资产，如通过交易、继承、生产的途径取得区块链资产的所有权，就没有理由不受到法律的保护。

对于针对区块链资产的刑事犯罪行为，可以依据《刑法》进行打击。在《刑法》中所列明的财产犯罪中，相关罪名都明确规定了犯罪行为的对象是财物，也就是以财物为目标的犯罪。区块链资产可以作为一种新型的财产，受到刑法的保护。对针对区块链资产的犯罪，有关部门有责任维护公民对区块链资产所享有的合法权益。

简而言之，尽管在现行法律中没有对区块链资产是否合法进行明确的规定，未来的立法（如《民法典》的制定）过程中也不会有专门提到区块链类型的资产，但我国在立法上对财产的范围采取了开放的态度，区块链资产并没有被排除在合法财产的范围之外，因此受到我国法律的保护。

（二）监管态度

尽管我国的行政机关对比特币的使用持谨慎态度，但对区块链资产却持开放态度，在五部委发布的《关于防范比特币风险的通知》中，在否定比特币的货币属性的同时，认同了比特币作为一种可以交易的虚拟商品的存在。在2014年的博鳌亚洲论坛上，中国人民银行行长周小川也表示：“……比特币像是一种能够交易的资产，不太像支付货币，……（比特币）作为资产进行为交易，并不是支付性的货币，所以应该说不属于我们有没有一个什么取缔的问题。”[36] 可见，即使对于比特币而言，在有关部门的文件以及金融领导表态中也未曾否认比特币的合法性，只是对于比特币作为货币可能扰乱金融秩序保持了高度的警惕。

因此，对于区块链资产的商品属性，在不会扰乱金融秩序或违反其他法律法规（如危害网络安全或其他财产安全）的情况下，有关部门也没有否定其存在的必要和理由。在“万众创新，福斯创业”的大背景下，有理由相信有关部门对区块链这样的新技术本身更多的会持中立，甚至是持欢迎的态度。

（三）司法案例

在立法尚未完善时，法院对新型技术所涉案件的裁判员结果是判断新型技术是否具有合法性的风向标。如果法院不支持保护某新型财产的权利，那么就很难认为该财产具有合法性，反之亦然。近年来，各种新型资产不断涌现，其中最为典型的就是虚拟财产的广泛使用，而法院对于虚拟财产的态度或可以为日后对待区块链技术的纠纷所借鉴。

在李宏晨诉北京北极冰科技发展有限公司娱乐服务合同纠纷案[37]中（该案件是我国第一例关于网络游戏虚拟财产的案件，也被称为“红月案”），法院在法律法规没有明确规定虚拟财产属性的情况下，对网络游戏道具进行了处理。在红月案中，一个重要的争议焦点是案件所涉的虚拟装备的价值及李宏晨损失的证据证明情况，法院就此焦点认为“玩家参与游戏需支付费用，可获得游戏时间和装备的游戏卡均须以货币购买，这些事实均反映出作为游戏主要产品之一的虚拟装备具有价值含量。”所以法院最终支持了李宏晨要求北极冰公司赔偿虚拟道具的诉讼请求。在“红月案”后，有关虚拟财产的案件有增无减，涉及盗窃、权属、继承等问题的纠纷层出不穷，法院也都一一进行了裁判员。

在法律对虚拟财产没有明确进行规定的情况下，法院依然根据法律原则及法学理论承认了用户对网络游戏中虚拟的道具所享有的权利，并且判决游戏运营公司进行赔偿。可见，法院对于法律尚未明确规定的新型网络财产不会拒绝承认其合法性，更不会拒绝裁判员。因此，法院在审理基于区块链技术资产的有关案件时，因为区块链资产本身具有使用价值与交易价值，所以可以得到法律的保护。

三、区块链与法律的重构

（一）代码即法律

长期以来，代码都是规制网络空间中行为的一股重要力量。劳伦斯·莱斯格（Lessig）教授对此进行了经典对论述：代码与法律、市场、准则共同对网络空间中的各种行为进行调整，基于代码的软件或与协议会决定人们利用互联网的方式。[38]

现行的与互联网相关的法律法规需要以如TCP/IP协议、防火墙技术、域名解析技术、超链接技术、数字签名技术等网络协议为基础的，更高级一些如微信平台、微博平台、淘宝平台的技术也是各种网络规范的基础。与TCP/IP协议、微信平台或其他网络上的代码一样，区块链技术同样会对各种网络行为产生深远的影响，并且直接影响到相关的法律关系、涉及的法律主体，以及崭新的法律客体，从而促使现行的互联网法律制度相应地进行调整。即使目前在行业中区块链应用程序非常的少，但仍有许多人都相信区块链技术具有巨大的发展前景。目前，越来越多国家正在达成一个共识——在政府出台有关规定之前，应该对区块链的好处和成本进行精确的分析。

一般认为，区块链技术具有以下技术特征：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively maintain）、可靠数据库（Reliable Database）、时间戳（Time stamp）、非对称加密（Asymmetric Cryptography）等。正是这些技术特征的存在，使区块链技术的应用特点十分显著：去中心化的分布式结构应用于现实中可节省大量的中介成本；不可篡改的时间戳可解决数据追踪与信息防伪问题；安全的信任机制可解决物联网技术的核心缺陷。[39]也正是因为区块链的优点，让基于区块链系统的网络资产与以往任何的网络的财产（如域名、账号、网络游戏道具等）都不相同，主要表现在：

①区块链资产并不存在一个中央节点；

②每一个节点都会存储全部网络的系统信息；

③在区块链系统中资产的变动可以被跟踪；

④区块链系统的资产具有更高的安全性。

最近麦肯锡公司发表了一份针对“区块链技术”的研究报告，该报告预测区块链技术将极大地重塑资本市场、影响商业模式并节约成本。根据区块链技术所具有的特点，《经济学人》将区块链技术描述为“一台创造信任的机器。”区块链技术改变了关于互联网上一切与信任有关的经济模式，让可信第三方变得不再必要。在传统网络交易的模式里，需要可信第三方提供担保，可信第三方可以至少具有以下三个方面的功能：

①证明交易的物品实际存在；

②避免多重交易；

③预防交易纠纷，记录交易历史。

传统互联网上信任的创建有赖于可信第三方的存在，比如在淘宝网上购买商品，需要使用支付宝作为可信的第三方负责担保并中转资金，在买家收到货物后再将款项从支付宝转移到卖家。尽管被称为“可信”第三方，但是作为交易的局外人，始终要面临谁来监督可信第三方的问题。而区块链技术的意义在于区块链资产的网络交易无须支付宝这样的第三方提供信用保证，就可以提供可被信任的交易模式，不会涉及谁来监督可信第三方这样的问题。中国信息化百人会成员、中国农业银行副行长林晓轩认为：“区块链技术从根本上改变了中心化的信用创建方式，它运用一套基于共识的数学算法，在机器之间创建信任网络，从而通过技术背书而非中心化信用机构来创建信用。通过这种机制，参与方不必知道交易的对手是谁，更不需要借助第三方机构来进行交易背书或者担保验证，而只需要信任共同的算法就可以创建互信，通过算法为参与者创造信用、产生信任和达成共识。”[40] 通过区块链技术，交易的合同可以直接嵌入到被交易过程中，在一定条件下合同条款被触发而自动履行。进一步来说，如果区块链技术与物联网技术结合，甚至可以让这些变革延伸到线下的现实生活中。

借助区块链技术所特有的信任机制，可以让交易的过程变得更加简洁。比如唯链就致力于提供一个基于区块链技术的真假校验云平台，贯彻区块链即服务（BaaS：Blockchain as a Service）的理念，把区块链当作一个基础设施，并在上面搭建各种满足普通用户需求的应用。随着对区块链技术应用水平的不断提高，会有越来越多的领域受益于此。

（二）知识产权

1.知识产权登记

近年来知识产权（Intellectual Property，IP）的概念日益得到重视，各行业的知识产权意识也显著增强。知识产权包括版权（著作权）、商标、专利、商业秘密等。

在这些不同类型的知识产权中，商标与专利的获得均需要向有关负责机关进行申请登记后方可获得权利。版权虽然在作品创作完成时就可以获得，但为了证明版权的获得时间，也可以向有关机关进行登记以获取著作权登记证明。因此，知识产权的效力严重依赖于登记机关对于知识产权信息的记录情况。而一旦知识产权登记机关的登记系统出现故障，如不能正常进行登记或登记信息有误，将会给知识产权权利归属的判断带来不便。国家商标局在2014年年中就曾因为系统升级中出现较大技术故障，导致商标审查工作停滞近四个月，致使216万商标申请“暂时性积压”。[41] 无独有偶，美国专利与商标局（United States Patent and Trademark Office）在2015年12月也出现技术故障，导致专利与商标的申请、查询、付费等功能无法正常使用。[42] 类似的故障不仅会造成知识产权申请的积压，更会影响到知识产权的日常运作与管理，导致整个知识产权体系无法正常运行。这样的故障哪怕只发生一天，也会给知识产权行业造成不小的影响。因此，一套安全、可靠的知识产权登记系统是必不可少的。

现行知识产权体系严重依赖于中央登记制度。而在信息登记方面，区块链技术具有先天的优势，时间戳功能可以提供可信的知识产权登记记录，证明知识产权的登记时间。另外，区块链技术所具有的分布式存储结构能够有效避免因为中央节点系统故障而导致整个登记系统瘫痪的情况发生。因此，对知识产权

的登记制度来说，区块链技术有能力提供更加可靠的技术保障。

作为一种所有权账本，基于区块链的注册与传统的数据登记相比，有着独一无二的优势：区块链数据库的去中心化且加密安全性质使它不太可能会遭受灾难性损失或失败，又或者遭受黑客攻击。而且，区块链注册过程几乎是瞬时的，并且可以降低注册成本。除此以外，作品的后续交易也会被实时记录，并且在交易网上可以被追踪到。同时，鉴于区块链的公开性，区块链注册可以使更多的人知道作者对作品拥有所有权，有利于宣示权利归属。但除非官方登记机构使用区块链技术进行登记，其他非官方的登记均需要解决证明效力的问题，即在出现争议时有效证明知识产权的登记时间。

2.作品发行

作品的发行、传播是一项重要的知识产权权利，而在作品发布以后的传播过程中，版权人往往是对整个过程缺乏控制的。尤其是在互联网时代，作品的复制与传播近乎没有成本，也导致了盗版的盛行，未经授权使用他人的文字或美术作品屡见不鲜，这让许多产业深受其害，唱片产业甚至一蹶不振，游戏、电影产业投入了大量资源以求遏制盗版，但效果始终有限。而将区块链技术的引入作品的发行有望改变盗版泛滥的窘况。

区块链技术也有望对网络上普遍存在的版权侵权行为进行遏制。传统上，因为网络上的各类知识产权因为计算机网络可以实现对信息的无损复制与低成本传播，导致权利人难以对版权进行有效控制，像盗版、“私服”“外挂”这样的侵权屡见不鲜。利用区块链技术，有望让网络上各类作品本身成为可信登记的证明。版权人借助区块链技术有能力控制、追踪网络上自己的各类知识产权的实时情况，避免像在传统网络环境下一样，作品一经发布就失去控制。作品在区块链系统下进行发布时就可以对使用作品的条件进行约定、限制，以加强权利人对自己的知识产权的掌控力度，形成一种崭新的商业模式。

以软件为例，软件的著作权登记证书记载了软件的作者、创作时间、权利归属等事项。如果软件基于区块链技术来进行发行，在软件的每份拷贝中都记载了软件的基本信息，如权利人的信息、使用软件的范围、使用期限，并且通过区块链技术可以轻易识别未经授权的拷贝，并拒绝盗版拷贝的使用，以给予版权人对软件作品更强大的控制力度。因此，区块链技术可能会成为更加有效的软件数字版权管理（DRM）技术，通过基于区块链技术的播放器、浏览器、阅读器或其他软件，影音、美术、文字等类型作品的网络传播都可以加强对作者权利的控制，更好地维护作者的权益。

正是因为区块链技术对于知识产权作品发行的天然优势，基于区块链的知识产权众筹模式也被提出。而位于德国柏林的Ascribe公司就通过使用基于区块链技术的记账系统，让作者可以固定作品的权利属性，安全进行分享并追踪作品的传播。并且可以通过区块链系统对作品的真实性进行真名，在发行时也可以限制发行的数量。音乐人伊门·哈普（Imogen Heap）也提出希望能够创建一套基于区块链技术的简单直接的交易模式，音乐人的作品直接面向听众销售。据使用过该平台的用户介绍，使用该平台的流程是：①登录歌曲“发行”页面；②启动Prototype（使用“数据区块链”所需的前端框架）；③点击歌曲的“下载”；④创建以太账本钱包；⑤用比特币给第④步创建的钱包充值；⑥钱包到账的时候，正式的下载链接出现。

利用区块链技术来进行作品发行，有利于让版权人获得对作品传播过程更完整的控制，这将导致利益的天平可能会向版权人一方倾斜。

（三）登记制度

登记制度在法律领域内被广泛运用，除了知识产权登记制度以外，还有不动产登记、机动车登记、企业工商登记、部分财物的交易登记、股权登记、诉讼立案登记等。在这些登记制度中，有些不经登记会导致法律行为无效，这通常是一些特殊权利变更的登记，比如《专利法》规定：转让专利权的，当事人应当订立书面合同，并向国务院专利行政部门登记，并由国务院专利行政部门予以公告，专利权的转让从登记之日起生效。还有一些是不经登记就无法继续推进流程，比如进行立案登记是法院受理、审理与执行案件的前提条件。

传统上对于权利的记录依赖于纸质凭证，近些年随着电子政务的推进，开始越来越多地使用中央数据库对权利凭证进行登记、管理。以股权为例，《公司法》第三十二条第二款、第三款规定：“记载于股东名册的股东，可以依股东名册主张行使股东权利。公司应当将股东的姓名或者名称向公司登记机关登记；登记事项发生变更的，应当办理变更登记。未经登记或者变更登记的，不得对抗第三人。”股权虽然不是强制要求登记，但如果不在管理部门进行登记，会面对无法对抗第三人的后果。区块链技术无疑可以帮助有关管理部门进行登记。在权利变更的过程中，登记是权利变更流程的一部分，但变更程序是复杂、缓慢且昂贵的，由于变更登记往往会涉及大量的资金，每个人都需要进行足够的尽职调查。因此，区块链成为保证这些调查的候选者。以不动产交易为例，买家和贷款人都需要对不动产的价值进行评估，买家和贷款人要求土地登记，对周边环境、住屋内的户口情况、学区等问题进行和调查，有时还需要了解借款人信用检查，这无一不是交易中可能的障碍，而所有这些调查依赖于开放和信任的数据源。国内创业团队小蚁（AntShares）做的就是将实体世界的资产和权益进行数字化，用区块链技术解决资产的登记发行、转让交易、清算交割等业务。

目前，Bitland(宝龙达)提出了一种新的区块链技术项目，目标是提供允许个人和团体在Bitland区块链上进行土地调查和土地所有权记录的服务，提供永久性的、可审计的记录，并作为一个联络机构帮助解决纠纷。该项目旨在消除腐败，并且声称能够释放价值数万亿美元的基础设施建设产业。项目首先在加纳最大城市之一库马西（200万人口）的28个社区进行试点，长远目标是将这个服务推广到整个非洲大陆。

（四）网络财产

网络早已成为人们社会生活中不可或缺的一部分，越来越多的财产也从线下转移到了线上。我们的电子邮箱、域名、各种网络服务的账号等具有经济性的财产都成为我们日常生活中不可抛弃的部分。因为网络上的各种安全风险，导致这些财产不时面临黑客入侵窃取、篡改、删除数据的隐患。而关于这些财产的归属权问题，尽管普通用户可能未曾留意过，但绝大多数的网络财产的所有权都归于网络服务的提供商所有，用户只是享有使用权。网络服务提供商与用户之间通过用户协议约定了虚拟财产的所有权归属。

传统上，因为网络财产大多存储于网络服务提供商的服务器中，网络服务提供方可以随时进行修改、删除等操作，因此提供网络服务的一方对网络财产具有绝对的掌控，用户的处置权利有限。而基于区块链技术的网络财产，尽管可以通过应用软件设置各种权限，但还是会被储存在每一个节点中，而这样的存储方式无疑会削弱网络服务提供方对财产的掌控力度，用户对网络财产的掌控会在一定程度上得到加强。而这样的改变会影响到网络财产的归属等一系列问题，网络财产归属的平衡可能会被打破，用户会对网络财产享有更多的权利。

借助区块链技术，可以开发出基于区块链技术的网络财产管理系统。网络服务的提供商通过区块链账号管理系统有能力加强对各类型财产的控制，降低中央服务器被攻击、拖库而导致的服务瘫痪、隐私泄露的风险。对于用户来说，区块链技术有能力带来更高的安全性，以有效降低网络财产所面临的安全风险，并且可以提供一种更加便利的使用权证明，方便各方确定网络财产的权利与义务，避免因为服务协议或内容的变更导致的用户权益受损。

（五）从电子合同到智能合同

随着互联网经济的日益活跃，电子合同因为具有便捷、高效的特点开始被广泛利用，如用户在注册网站时所点击同意的“用户协议”、电子商务平台为了交易方便而与供货商利用网络所签订的“供货合同”、互联网金融的有关交易等，都依赖于有效力的电子合同。电子合同甚至可以说是大多数互联网交易活动的法律基础。国务院在2015年5月制定的《关于大力发展电子商务加快培育经济新动力的意见》第一次明确提出了“创建电子合同等电子交易凭证的规范管理机制，确保网络交易各方的合法权益”。电子合同因为完全是在网上进行操作，所以保证电子合同的真实性是重中之重，目前主要是以电子签名的形式进行保证。在常规集中的数据库，这些交易是由一个单一可信权威管理机构创建的。相比之下，由区块链驱动的共享数据库，交易可以由任何一个区块链的用户创建。而且，由于这些用户不完全信任对方，数据库必须含有限制进行交易的规则。例如，在一个点对点网络的财务分类账，每一笔交易必须保持资金的

总量不变；否则，用户可以随意给自己取尽可能多的钱，因为他们都很喜欢。

甲骨文公司洞察与客户战略部门副主管萨波拉曼尼亚·艾耶（Subramanian Iyer）认为，区块链可以容纳大量的数据，包括完整的合同。智能合同会消除如法律公司这样中间人的存在，当特定的一些条件获得满足的时候，支付将会自动进行。就其本质而言，智能合约以电子的方式很容易执行，它通过脱离单一机构的掌控创建了一种强大的第三方机构。借助区块链技术，电子合同可以具备相较于传统电子签名更高的安全性。更重要的是区块链技术可以让合同文本与合同内容紧密地结合在一起，像网络财产、网络版权作品都可以将合同文本嵌入其中，让合同内容根据约定的情况自主去履行权利与义务。例如在线影音作品的租赁。如果借助于区块链技术，在影视作品的拷贝中嵌入合同的内容，在视频中嵌入著作权人的信息以及授权用户观看的时间、范围，以减少抄袭或其他侵权行为的可能，甚至可以设置按照观看的进度来进行自动付费。因此，简而言之，智能合同其实是一段被存储在一个区块链上的代码，由区块链交易触发。[43]

而随着网络环境的变化，面对可以自动履行的合同，传统合同法中的部分规定可能将不再适用。在中国现行的《合同法》中，第四章专门规定了“合同的履行”，而随着基于区块链技术的智能合同广泛运用，合同履行或许会与合同文本的制定融为一体。在智能合同时代，如果智能合同在履行时出现瑕疵，可能并非是因为合同履行方没有去履行合同，而是智能合同在研发时存在隐患，导致具有履行合同义务的一方无法履行。这时，可能就会需要智能合同的提供方或开发方就合同不能履行承担相应的法律责任。简而言之，智能合同的运用会让合同的权利、义务重新划分，以适应智能合同所带来的变革，而这需要对现行的《合同法》根据区块链技术的特点进行修订。

信达证券首席区块链专家曹寅认为：“在区块链时代，传统的社会契约形式，将被对于基于区块链的智能合同的运用前景。”汤森路透的副总裁兼产品管理负责人斯科特·曼纽尔表示，他们的许多法律客户对智能合约的潜力，智能合约能够做些什么，以及它们在区块链世界中允许什么很有兴趣。区块链以点对点信任直接传递和强制信任化的功能，实现了生产关系的解构，其解构原理非常类似“物理第一性原理”对于宏观物理现象的解构，任何尺度的宏观物理现象，不管是山崩地裂，还是日月运行，都可以用最基本的质子和电子间的关系来解释。在区块链时代，任何经济行为，不管是股票发行还是破产清算；任何组织形式，不管是创业合伙还是跨国企业，都将被区块链解构，解构为最基本的人和人之间的经济行为。

以太坊（Ethereum）项目正是一个提供智能合同的去中心化平台。平台上的应用在运行时可以被设计，允许用户编写复杂的智能合同，担保和交易任何事物：投票、域名、金融交易所、众筹、公司管理、合同、知识产权等。比如在接收货物时能创建电子发票，或者在利润达到一定金额时自动向股票持有者发送分红。还可以设置以太坊区块链内置的汽车钥匙，遵循相应规则进行出售或出租，产生新型的P2P汽车租赁或共享。2016年4月，区块链技术专业公司Gem(宝石)官方正式宣布推出Gem Health（宝石健康）项目，以推动医疗领域的新兴技术的合作和发展。Gem在公告中表示，飞利浦公司将会成为他们的第一个合作伙伴，飞利浦将会帮助Gem以构建一种能够用来开发企业级医疗应用程序的私有以太坊区块链。

（六）物联网与区块链

物联网是一种基于互联网、传统电信网等信息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络。统计显示，在2015年通过无线网络进行连接的物联网设备就已经达到134亿台，预计到2020年将会有超过280亿台物联网设备。万物互联的景象似乎已经近在咫尺。

区块链技术有望协助解决物联网发展所面临的一些技术性问题，比如成本、诚信以及防护。对物联网设备进行中心化的追踪和管理不仅在技术上难以实现，这样的尝试也不明智，而在去中心化物联网中，区块链可以被用于促进交易的处理和交互设备间的协调，每一个物联网设备都会管理自己在交互作用中的角色、行为和规则。与物联网设备结合，基于区块链技术的智能合同可以将网络上所能利用到各种便利服务扩展到实体物中。区块链技术可以在无须信任单个节点的同时创建整个网络的信任共识，从而很好地解决物联网的一些核心缺陷，让物与物之间不仅连接起来，而且能够自发地活动起来，互相进行认证，让我们更好地利用物联网所带来的便利。[44]

在纽约布鲁克林区，区块链正在使新型的微智能电网，最终能够允许点对点技术，超本地绿色电网从传统电网中独立运行。分布式能源将彻底改变能源市场如何运作。埃森哲咨询公司也正在验证使用区块链技术打击假冒药品的项目的可能性。而创业公司Hellosent认为智能合同和物联网设备可以用于监测红酒的交付，Hellosent将基于区块链技术传感器用于运输中连续测量红酒的温度和湿度，如果任意一项低于智能合约中记录的约定水平，那么购买订单将会自动取消，以此来保证所销售葡萄酒的品质。这种应用模式完全可以用于疫苗、食品、危险品的运输存储过程中，区块链技术有助于监控这类需要冷链或专门保存条件的运输过程。

除此以外，区块链技术还可以帮助物联网设备的所有人实时跟踪自己财产的真实状态，包括财产的地理位置、完好程度、使用人资质、过往交易记录、担保情况等信息。这可以让实体物的交易、使用可以像在网络上一样得到有效监控。线下的房产交易租赁、汽车的销售租赁、物联网所收集个人信息的安全，都有望借助于物联网技术与区块链技术得到更好的解决方案，以减少各类因为登记信息被篡改或伪造产权证明所产生的争端。另外，区块链技术也能够让对于财产的执法行为变得更为容易，有效避免为了躲避对财产执行而对财产进行的转移。像空中住宿（Airbnb）这样的住屋短租公司也开始关注区块链技术，在2016年雇佣大量ChangeTip员工，以对区块链技术在短租领域的商业运用进行研发。Airbnb的用户能找到心仪的短期住所，一个重要的原因是Airbnb拥有一个相对完整的评分和评论数据库，以存储住屋主人和房客的评价交易信息。而像记账本一般的“数据区块链”能够储存几乎所有交易、评分和评论明细，从而将数据变得更加可读。另外，以“区块链”的方式安全、谨慎地将数据“出口”到其他平台，或者共享数据。

但是，在看到区块链技术与物联网结合的潜力的同时，也不应忽视其潜在的法律风险。伴随着物联网数据存储而来的信任问题和身份问题，隐私和个人数据的保密将是物联网市场发展不得不跨越的障碍。换句话说，区块链技术或将成为全球连通数字与物理世界的基础设置，包括可穿戴计算、物联网、传感器、智能手机、笔记本电脑和照相机、智能家居、智能汽车，甚至智能城市可能都会基于区块链技术，区块链上每一个节点都会记录全部数据库的数据，这也会导致用户的隐私问题随之而来，毕竟没有人希望在使用自己财产时处于时刻被他人监视的状态，或者是存在被监控的可能。需要技术开发者在提升区块链与物联网技术用户体验的同时，做好用户隐私的保护工作。

（七）区块链鉴证

1.证据的真实性

无论是解决哪一类型法律纠纷，对证据真实性的确认总是重点。如果无法保证证据的真实性，那么无论证据看上去是多么有说服力都无济于事。但因为现实纠纷的复杂性、专业性与日俱增，法官单纯凭借自己的法律专业知识无从判断一些新型证据的真实性，所以需要借助第三方的专业意见来就证据是否真实进行判断，比如对于借条上签名的真实性需要通过笔迹鉴定来判断，对血缘关系是否真实通过DNA（脱氧核糖核酸）鉴定来判断，对于死者的死因则需要通过法医鉴定来判断，不一而足。

在进入计算机互联网时代后，对电子证据真实性判断的需求更加迫切。在计算机互联网环境下，编辑、复制、传输文件信息不仅简单，成本更是低廉。而随着人们越来越多的商务往来、信息交易、休闲娱乐全部过程都发生在互联网上，在遇到纠纷时或者为了避免纠纷，对电子数据证据真实性的证明需求也越来越高。

但是，电子数据因为具有无形性、隐蔽性强、易被破坏的特点，给证据真实性的认定带来较多困难。[45] 根据证据规则，无法与原件、原物核对的复印件、复制品是不能单独作为认定的依据，原始文件的证明力也是大于经过复制的文件。因此对电子数据真实性认定是以电子数据证据原件为前提。但计算机等输出的书面材料很难说是原件，且电子数据依附于存储介质而存在。在物理意义上，电子数据是信息附着于存储介质后才生成的，其原件应当指最初生成的及首先固定所在的各种存储介质上的信息，随后无论采取何种方法取得的信息都是该电子数据的复本。因而，何为电子数据的原件在司法认定上难以确定。

传统上，司法实践中对电子数据证据真实性的证明主要通过公证机构进行公证的方法，如证明电子邮件真实性可以通过在公证处登录电子邮箱查看邮件并将整个过程以录像或截屏的方式进行。除了公证以外，还可以使用可信时间戳认证的方式，即通过我国法定时间源和现代密码技术相结合而提供的一种第三方服务，通过可信时间戳证明数据电文（电子文件）产生的时间及内容完整性。无论是通过公证还是时间戳认证，都是借助第三方机构的权威性来证明证据的真实性，而第三方机构的权威性要么是来源于特殊的法律地位，要么是来源于技术上的可靠性。借助第三方机构可以在一定程度上解决电子数据证据真实性的问题，但不可避免地会遇到成本高昂、手续烦琐的问题。而真正造成“麻烦”的是对电子证据真实性的确认无法离开第三方。

2.区块链技术与证据的真实性

在区块链技术的结构中，每一个节点都记录了数据库的完整历史。区块链上的每一条数据都可以通过“区块链”的结构追本溯源进行验证。[46] 区块链技术也因此被誉为“创造信任的工具”，并且自带有时间戳认证以及加密的功能。在有能力不借助第三方的情况下，提供足以保证证据真实性的证明。以基于区块链技术的比特币为例，根据中本聪的论文《比特币：一种点对点的电子现金系统》中的描述：比特币的“时间戳服务器通过对以区块形式存在的一组数据实施随机散列而加上时间戳，并将该随机散列进行广播，就像在新闻或世界性新闻组网络的发帖一样”。且“该时间戳能够……的确存在的，因为只有在该时刻存在才能获取相应的随机数列。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前一个时间戳进行增强，形成一个链条”。因为自带时间认证功能，在网上甚至可以找到用比特币来证明截图的时间的教程，其原理就是基于区块链技术的时间戳不可被篡改性。[47] 可见区块链技术在时间认证方面的可靠性。

实际上，已经有区块链技术试图取代公证机构的存在，Stampery公司就试图利用区块链技术所具有的时间戳属性来代替传统公证的效力。将区块链技术引入公证，在无须公证机关介入的情况下，降低用户对证明与时间有关事项的时间成本与经济成本。不过目前Stampery的法律效力还没有得到法院的认可，但创始人对此颇为自信，认为法官会接受Stampery公证的效力，因为Stampery提供的不是观点，而是数学。另外，公证通（Factom）也在利用比特币的区块链技术来革新商业社会和政府部门的数据管理和数据记录方式。公证通维护了一个永久不可更改的、基于时间戳记录的区块链数据网络。减少进行独立审计、管理真实记录、遵守政府监管条例的成本和难度。公证通的应用远远超出记录保存和资产管理的范畴，它还可被应用在版权、教育和契约法的制定。政府已经找到这项技术的用途，并会继续发掘它的可能。拥有庞大人口的国家可在税收、普查中使用公证通，会大大削减成本。

3.作为证据的区块链技术

区块链作为证据的前提是利用区块链技术进行证明的事项在法庭上站得住脚。从证据的角度需要确保区块链资产在作为证据时的真实性、合法性与关联性，即证据的“三性”。

证据的真实性指服务的内容作为证据事实，需要不以任何人的主观意志为转移，它以真实而非虚无的、客观而非想象的面目出现于客观世界，且能够为人所认识和理解。证据的合法性是指作为民事案件定案依据的事实材料必须符合法定的存在形式，并且其获得、提供、审查、保全、认证、质证等证据的适用过程和程序也必须是合乎法律规定的。证据的关联性指民事证据必须与案件的待证明的事实之间有内在的联系。与区块链技术本身相关的主要是真实性与合法性的要求，关联性通常需要结合具体案件的情况进行判断。

从真实性的角度来讲，区块链本身就具备了时间戳的属性。即对数据库中的信息形成时间提供可信的证明，并且在整个过程中排除人为干涉的可能，天然具有证明时间的属性。虽然在普通电脑上也可以通过查看文件属性来确认文件的“创建时间”“修改时间”或“访问时间”“作者”“单位”等信息。但是这样的信息并不难被篡改，即没有密码学上的科学保证。在法庭上，只需要演示一下这些文件的属性信息是可以被修改，或是存在被修改的可能性就足以让这些文件的效力大打折扣。与此不同，区块链技术对于时间的证明在现有科技的条件下无法修改，只要在庭审时能够证明基于区块链技术的电子数据证据的效力就不难得到法官的认可。

从合法性的角度来讲，基于区块链技术所提供服务的内容需要是符合法律规定的。如果利用区块链技术进行窃听、偷拍或胁迫抑或其他违法方式取得，那么该项证据则不具有合法性，不可能在法庭上得到认可。

从举证的角度来说，基于区块链技术所提供的网络服务，无须对提供服务的过程进行逐一的证据保全，只需要在出现纠纷时向法庭展示文件内容，说明系统的原理即可保证证据的真实性。这节省了将大量文件进行公证或时间戳认证所产生经济成本与时间成本，减少了工作流程。区块链系统是一种“天然”的证据保全工具，证据保全伴随着网络服务的过程同步进行，无须专门的流程就可完成证据保全工作，可以为健全网络交易规范、规范网络环境、追究侵权责任方、查处违法违规行为提供助力，让证据的真实性不再是一个问题，更无须专门为此费心进行证明。不过需要注意的是，为了应对与区块链技术有关的诉讼，需要了解区块链技术原理的律师、技术专家密切配合，清楚、无误地向法庭解释区块链技术，帮助法官了解区块链技术为何能够保证文件的真实性，减少因为解释不清而导致无法认定证据效力的情况。

（八）隐私保护

根据工业和信息化部在2013年制定的《电信和互联网用户个人信息保护规定》，网络个人信息是指用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等数据，并且具备能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。在传统互联网环境下，个人信息主要包括用户上网所产生的信息，如用户在网络上的言论、Cookie中的信息、网络账户的账号及密码、实名登记的身份信息等。在使用互联网时，个人数据不可避免会在网络上传输，而在传输的过程中个人信息就存在被盗用、传播的可能性，这也让每一个网络用户都成为潜在的受害者。个人信息泄露会给信息相关人造成巨大的伤害，使其饱受骚扰之苦。更可怕的是个人信息的泄露往往并不是单一的个案，而是大范围的个人信息泄露，通常会伴随着数以万计的个人信息被窃取、非法贩卖，甚至会利用正规的数据交易机构交易窃取到的数据。

区块链技术所具有的加密性可以为个人信息的保护提供解决方案。区块链技术可以对个人信息进行分布式保存，避免单一服务器所面临的安全风险。

用户还可以借助区块链技术加强对自己个人信息的控制。传统上，用户的个人信息的收集、挖掘、交易等过程被网络服务提供商牢牢控制，用户难以了解到自己的个人数据如何被利用，更难以了解网络服务提供商在利用自己信息时是否存在违规甚至是违法行为，而约束这些网络服务提供商的，只有与用户之间的用户协议而已。基于区块链技术，可以帮助用户加强对自己个人信息的控制力度。区块链所有的交易信息对于用户可以是公开透明的，让用户有办法跟踪自己个人信息的使用情况，有效避免用户在自己的信息被收集后就完全被抛在一边的窘境。

Enigma是麻省理工学院媒体实验室旗下的项目。Enigma是一个基于区块链技术的去中心化的云平台，可以保护隐私安全的去中心化的云平台项目。私人数据在Enigma的存储、分享和分析，完全不会透露给第三方，Enigma取消了对可信任第三方的需要。在Enigma平台上，私人信息可以在不完全泄露给任何一方的情况下进行存储和分析。Enigma平台是基于高度优化的区块链技术的多方安全计算（Secure Multi-party Computation）技术。据Enigma项目创始人光·祖卡德（Guy Zyskind）介绍，整个平台就像是一个“黑箱”，人们可以随意上传任何类型的数据，这些数据在黑箱中被进行处理并返回结果，真实的数据从未被泄露给外部或处理数据的计算机。据《连线》网站的报道[48]，Enigma项目的安全性与节点的数量息息相关，越多的计算机参与其中，用户的数据就越安全，但是处理的速度也会越慢。而当每次有人从Enigma系统中进行计算请求时，需要以比特币支付费用。这笔钱的少部分会支付给区块链系统中一台记录Enigma元数据的计算机。大部分费用会支付给Enigma网络中的节点，以作为存储、处理用户加密数据的奖励。Enigma软件同样可以设置奖励数据的所有者。因此，Enigma的用户，例如广告商可以在不将个人数据破解的情况下向用户支付数据挖掘的费用，让各方都有利可图。

（九）规制区块链

区块链是一项新兴技术，对区块链的规制离不开法律、代码、市场、准则四个方面，区块链技术的应用

与发展同样不可能不受这四个方面的影响。

法律规制着使用区块链技术的各种行为。著作权法、侵权责任法、合同法直接对各种利用区块链的侵权行为进行处罚，划定了法律上的红线。比如行政机构对比特币使用的限制就直接影响了比特币的发展。

代码也规制着网络空间的行为。区块链代码本身所具有的特点决定了基于区块链技术各种应用的使用方式。像开放源代码这样的运动可以提高区块链技术的安全性与稳定性，让用户的使用可以更加放心。

市场也是规制区块链技术的重要力量。市场的好恶直接决定了区块链技术的发展前景。另外，如果区块链技术的使用成本过高，那么区块链的应用难免会被局限。也就是说，即使区块链在技术上再领先，如果缺少商业上的成功，那么利益所涉及的各方也不会有太多心思去对区块链进行规制。

准则与法律类似，但在法律尚未健全之时可以起到关键的作用。因此，创建一套区块链技术的使用准则也显得尤为必要。像澳大利亚标准机构(Standards Australia)已经要求国际标准化组织为区块链技术设定全球标准。标准一旦设定，将会对区块链技术的使用起到重要的指引作用，甚至是树立基本的使用规范。

因此，在考虑对区块链进行规制时，需要将目光放的更加长远，思考的角度也需要更加全面，综合考虑法律、代码、市场、准则四个方面，以对区块链技术所面临的潜在问题进行规制。

四、区块链的法律前景

在社会经济发展过程中，技术因素一直都起着重要的作用。社会关系因为技术的发展不断发生着变化，社会关系的变化也让法律的调整成为了必然。与此同时，法律也直接影响着技术的发展，像《促进科技成果转化法》这样的法律法规会直接影响到科技的进步。技术对于法律的影响永远都是一个复杂的话题，法律制度变迁的背后从来都少不了技术的影子。区块链技术有能力彻底改变互联网上的信任关系，而这对现行互联网法律体系的影响难以估量。区块链技术让网络更像现实，让网络规则更像物理规则。区块链让现实中的物理学定理变成了加密的算法，来保证数据的唯一性。

近年来，无论是在法律圈还是在科技圈讨论“互联网+法律”的人都不在少数，法律人担心互联网会改变现行法律行业的经营方式，而互联网行业从业者们则在试图通过互联网渗透法律这一古老的行业。因此，法律人有必要对互联网技术进行更广泛的了解，互联网行业从业者也有必要了解现行的法律制度。区块链技术为法律制度与互联网的结合与发展提供一种完全不同的可能性，或许未来真的会走上这条路，或许会由于各种原因另辟蹊径。无论是哪种情况，大家都没有理由去忽视区块链技术可能对法律的影响，更不能无视法律对区块链技术的规制。

[32] 本章由史宇航写作完成。史宇航，上海交通大学凯原法学院博士研究生，主要研究领域为知识产权法，对区块链的法律重构有深入的研究。

[33] IRS Virtual Currency，Guidance http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance。

[34] Honduras to build land title registry using bitcoin technology http://in.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515。

[35] http://bok.or.kr/contents/total/ko/boardView.action?boardBean.brdid=123570&boardBean.menuid=110&boardBean.rnum=2&menuNaviId=2123&boardBean.cPage=1&boardBean.categorycd=0。

[36] 周小川.比特币不像支付货币 谈不上取缔，http://tech.qq.com/a/20140411/015521.htm。

[37] 参见李宏晨诉北京北极冰科技发展有限公司娱乐服务合同纠纷案一审：北京市朝阳区人民法院，（2003）朝民初字第17848号；二审：北京市第二中级人民法院，（2004）二中民终字第02877号。

[38] 劳伦斯·莱斯格.代码2.0：网络空间中的法律［M］.北京：清华大学出版社，2009：140.

[39] 区块链：星星之火，可以燎原，http://www.8btc.com/blockchain-revolution。

[40] 林晓轩.区块链技术或将根本改变金融机构间的交易规则［J］.中国金融，2016：8.

[41] 216万商标申请“暂时性积压”，http://www.infzm.com/content/104797/。

[42] USPTO Systems Status and Availability，http://www.uspto.gov/blog/ebiz/entry/uspto_power_outage_update。

[43] 智能合约中存在的3种最常见的误解，http://www.8btc.com/beware-the-impossible-smart-contract。

[44] 区块链：星星之火，可以燎原，http://www.8btc.com/blockchain-revolution。

[45] 电子数据真实性如何认定，http://www.chinacourt.org/article/detail/2014/07/id/1329854.shtml。

[46] 区块链：星星之火，可以燎原，http://www.8btc.com/blockchain-revolution。

[47] 怎样用比特币来证明截图的时间，http://btc.cnfol.com/bitebixueyuan/20131220/16523255.shtml。

[48] MIT□s Bitcoin-Inspired ‘Enigma□ Lets Computers Mine Encrypted Data http://www. wired.com/2015/06/mits-bitcoin-inspired-enigma-lets-computers-mine-encrypted-data/.

第八章
区块链经济学的范式革命[49]

一、自由与演化：发自社区，来自市场

从经济学角度观察区块链的发展，首先会发现它的诞生并非来自政府，也不是出自金融巨头，而是肇始于互联网的社区之中。

区块链来自比特币等数字货币，数字货币的出现是社区形式的，这一点是比特币等数字货币得以在全世界范围发展的重要原因。现在看来，区块链发自社区正是一把“双刃剑”。社区形式的数字货币自从诞生伊始便是市场化的。这句话怎么理解呢？如果我们把整个世界上的各种货币之间看成是一个竞争的市场，那么数字货币一方面可以低门槛地参与到这个全球性的市场里，另一方面其一旦跨出这一步，也就等于面临着全球其他所有货币之间的竞争。低门槛表现在数字货币的交易流通相比现有货币市场（外汇市场）更方便。理论上只要世界各地有任何一个民间的多币种数字货币交易所接受了某个数字货币，那么也就等于其已经进入了全球的交易市场之中[50]。当然进入全球的交易市场并不完全是好事，因为这么做意味着该种数字货币的竞争对象起码也已经是包括比特币在内的其他数百种数字货币，如果自身没有足够的特色和生命力，资本很快就会转移。

读者看到这里可能会提出质疑：数字货币名不正言不顺，所谓的全球交易市场不过是民间的多币种交易所而已，相比外汇市场而言体量微乎其微，凭什么相提并论？

确实，从交易体量上看，即使把现存的所有数字货币以及各种区块链应用代币全都算上去，也就只有比特币能够称得上是“外汇交易品种”。其余各种品类各异千奇百怪的数字货币、区块链应用代币乃至数字资产都和“外汇”一词体现出的世界级别影响力相差甚远，可是，他们却拥有着对于演化而言最重要的条件：自由竞争。

让我们分别从数字货币代表比特币和区块链的发展来观察竞争和演化带来了什么。先看比特币。比特币的发展之路，一是不停地面临着后续其他新生数字货币的竞争和挑战；二是自身的升级和优化方面遇到多种力量的博弈和制衡；三是其在慢慢为世界所接受成为一种新生的外汇品类之时也面临着世界上其他主流货币的竞争和挑战。就第一点来说，其他数字货币往往在基于比特币的基础上提出自身的改良，进而具备更多的特征。这种技术上的改良与挑战对于比特币来说始终是一种压力，也是其不断改进的动力和参考。就第二点来说，从近期比特币的扩容升级问题可以看到，从各种BIP[51]到Core和Classic的派别之分的涌现，正是内生演化的具体表现。就第三点来说，比特币从一个备受争议的虚拟代币，经过数年的发展逐渐从极客的小圈子，从世界范围内的抵触、怀疑到被初步接受、认可的过程，也正是比特币作为一种新生的外汇品种的演化之路。

从以上三点可以看出，比特币内生和外部相关联的演化道路之所以曲折复杂，从表面看得益于开源和去中心化理念积累数十载后于区块链上的突然爆发，而深究其背后的原因便可得知，动力来自于自由竞争和市场。比特币的社区文化可以说便是开源、自由、无国界的互联网文化缩影；比特币内在价值也体现在互联网无国界低租值的货币需要构成上；最后，通过市场的充分竞争，比特币得以在演化的过程中不断历练、充实并完善、提升。演化说里关于生命的诞生有一种观点认为，最初的有机物是从无机物诞生的，而无机物到有机物的跳跃最关键要素之一便是一个良好的“原汤”环境。由此观之，在自由竞争和市场的“原汤”环境下，比特币的出现和成长是一种偶然，也可以说是一种必然。偶然之处在于比特币竟然活到了现在而没有被无数次危机淹没，必然之处在于就像无机物到有机物的进化一般，货币总会向着数字货币这种更经济的方向进化。

区块链经过近8年的发展，其概念覆盖了账簿、货币、数字资产到智能合约等多个方面。这种不断开花——结果——进化的循环过程正是上述比特币发展路程的全景和衍生。

二、组织与激励：各花入各眼

在区块链发展的过程里，我们经常看到的是其应用如何多姿多彩。有趣的是除了应用和功能以外其发展

的土壤——其内部组织架构也在发生着变化。接下来让我们去一探究竟。

①社区型：比特币（Bitcoin），数字货币，2009年至今[52]。

②社区+基金会：以太坊（Ethereum），智能合约，2014年至今。

③基金会+公司型：公证通（Factom），防伪证明，2015年至今。

④公司制：各种联盟链、私链，2015年至今。

从以上四种形式分别看，基于社区形式的组织数量伴随着比特币2014~2015年的价格低谷逐渐减少。但社区形式因其低成本、低门槛，始终维持相当的生命力，并且在2016年通过TheDAO巨额众筹的成功得以另一种形式的发展。作为当前区块链领域的知名项目以太坊，其基金会可谓是毁誉参半。赞同者认为其让以太坊更纯粹和非商业化，质疑者认为其财务管理不善，若非以太（以太坊区块链的代币）暴涨，项目甚至可能中途"夭折"。基金会+公司形式的优点在于运营团队的稳定，但同时也有团队以及资金的归属疑问。

最后一种完全的公司制一般对应的是联盟链和私有链，鲜有公开链的项目。其原因可能在于公开链的共识机制对于独立第三方的经济激励导致其代币（Token）的不可或缺，而代币的扩散与注资往往与挖矿（PoW）和众筹（PoS）等社区行为相关联。加上开源的默认特点，社区行为以及代币更流行的组织架构是基金会而非公司。公司制的区块链组织稳定，但不够开放。稳定的原因在于其团队激励更多来源于传统的工资以及股权，团队更多体现的是经济人假设的特点——逐利；不够开放其实是指激励的单样性——想象某人为了世界公平，更可能加入某公司制区块链团队还是社区形式？一般理解便是后者。所以在我看来，公司制与社区型的区块链区别更多体现在激励的不同上。

以上四种形式按照其典型案例的出现时间先后排列。可以发现社区型区块链应用出现最早，其后逐渐向公司形式转变。有的读者现在可能在想这样一个问题：上一节不是说到区块链发自社区来自市场吗，怎么看上去随着时间的推移区块链离社区越来越远了呢？

一般认为社区形式是最为自由也是组织架构最为松散的一种形式；公司形式则是这四种组织形式之中最为规范，目标也最为明确（即盈利）的一种；基金会则介于两者之间。可以这样去理解以上信息：为了更好地适应外部环境，区块链的参与人员由一开始的弱组织形式慢慢向强组织靠拢；同时也越来越偏向于找到一种稳定的、可以长期盈利的模式。从理性人角度出发很容易可以理解这种转变，即任何新技术的诞生可以是偶然的，但其发展和扩张一定满足的是：为自己同时也为社会整体运行带来更低成本、更高效用，实现帕累托优化。

那么是不是说将来的结果就一定是社区形式区块链组织式微，而公司形式的区块链组织越来越多呢？不尽然。帕累托优化的意思是在没有使任何人境况变坏的前提下，使至少一个人变得更好。需要注意，对于每个人来说，更好的含义是不同的。可能出现这种情况：对于甲来说获取更多工资是更好的；而对于乙来说世界公平是更好的。对于甲来说加入公司制的组织可能是更好的，而对于乙来说加入社区制的组织可能是更好的。由此可以推测，同时存在公司制和社区制的两种组织相比单纯的一种组织，对于甲乙两人来说是一种帕累托优化。

再深究下去，我们会发现这涉及经济学的基础问题：是经济人假设，还是社会人假设？人是经济理性的，还是社会理性的？人是自私的，还是利他的？To be or not to be(是，还是不是)？永恒的问题。[53]

个人认为未来会是越来越偏社区化的，因为我相信随着技术生产力持续不断的指数级别提升，经济激励的效用相对而言会越来越低。

三、纳什均衡：公有链的永动机之谜

经常会看到人们讨论区块链（本节"区块链"等于"区块链公链"）的成本，奇怪的是往往会出现以下两种相反的论述：

①区块链是免费的，低成本的；②区块链很贵很浪费。

到底谁对谁错？都答对了一半。

先看看第一种：“区块链是免费的，低成本的。”这种说法是从用户角度出发而言的。对于用户来说，使用某个区块链应用（例如比特币）进行转账的时候，并不需要考虑比特币的运营和维护费用。用户根据比特币协议理论上只需要付出极少部分的转账手续费即可实现付款。从这角度来看此论述正确。

再看看第二种：“区块链很贵很浪费。”这种说法是从区块链的设计者或是投资者角度出发的。对于设计者而言心里很清楚“天下没有免费的午餐”这一道理。区块链的设计里不论是PoW（Proof of Work，工作量证明机制）还是PoS（Proof of Stake，股权证明机制），都需要有对应的资源付出以换取整个系统的共识和平稳运行。在PoW里，资源是矿工挖矿的工作量；在PoS里，资源是购买股权付出的金钱。

图8-1 是比特币PoW机制下的区块链运作机制。作为分布式账簿来说，左边条线是系统运维得以实现的基础，即分布式账簿通过挖矿机制激励矿工维护系统运行。右边条线是系统得以不断扩大的条件，即分布式账簿确实满足了需要进行价值交换用户的需要，在某个时点有人会去使用。下方的价格投机则是连接矿工和用户的桥梁，即账簿的代币因为右方用户需要产生了价格，而左方矿工通过有价代币将代币激励落到实处，价格投机者则为双方将价格流动性坐实。

图8-1 PoW机制下的区块链运作机制

在以上运行机制里任一环节都必不可少。缺少了挖矿，系统没有了记账人无法运作；缺少了用户，系统代币无法产生价格；缺少了价格投机者，代币价格缺少流动性矿工激励不足。反之每个环节都各司其职的话，理论上来说图8-1可以形成一个闭环，也就是形成了一个纳什均衡。[54]

纳什均衡有一个很重要的特点，即信念和选择之间的一致性。也就是说，基于信念的选择是合理的，同时支持这个选择的信念也是正确的。所以，纳什均衡具有预测的自我实现（self-enforcement）特征：如果所有人都认为这个结果会出现，这个结果就真的就会出现[55]。中本聪有类似的观点，他说比特币就是一个自我实现的预言。

理论上，信念和选择之间的一致性自我实现特征，使区块链可以像永动机一样稳定运行。然而永动机真的永动吗？仔细观察图8-1便会发现该永动机始终还需要燃料，燃料首先便是用户对于账簿的持续性使用的需求，其次是价格投机的需求。

实际上情况是，由于区块链代币的强交易品特性，使图8-1下方的价格投机和真正的用户需要往往混在一起，难以分辨（更不用说矿工本身也是价格投机的常客）。先把比特币放一边，可以发现近年来诞生的大部分区块链代币存活过两年的比例很低。这个事实可以说明想要单纯依靠价格投机的需求实现区块链运行的纳什均衡几乎是不可能的。区块链的运行始终还是需要能够满足真正的用户需要，提升用户使用需要的效用。

回到本节开篇的问题：区块链到底是贵还是便宜呢？我的答案有些取巧：只要能够真正提升用户的边际效用，那么不管多贵的区块链都是便宜的。

四、比特币的内在价值：当它成为一种刚性需求

自从比特币出现价格后，质疑之声就不绝于耳。好听一些的有格林斯潘和诺奖得主罗伯特·席勒说比特币没有内在价值，是泡沫。难听一些的就直接说它是庞氏骗局，是传销。果真如此吗？下面将对比特币的价格构成进行拆解分析，看看它的内里到底有没有什么价值。

比特币诞生至今也不算长远，不到8年的时间。让我感到不可理解的是，当质疑者们讨论比特币有没有价值的时候，仿佛都在讨论一个形而上的东西，例如法币、内在价值等，却很少有人愿意看一看这几年间除了价格图表和舆论口水实实在在的发展历程。

第一个例子：2011年开始伴随着网络黑市“丝绸之路”的快速发展，比特币作为其唯一的支付手段价格开始水涨船高。价格上涨的原因很简单：

①互联网上有人需要买丝绸之路上的东西，例如毒品、枪支；

②有人也想卖；

③没有一种互联网上的跨国支付手段（例如VISA）可以，或者说愿意接入丝绸之路，因为它是黑市；

④比特币是跨国的，同时不需要有机构“许可”即可接入；

⑤比特币因此被买卖双方需要了，而且还是客观上的垄断性需要。

第二个例子：维基解密。VISA和MasterCard于2010年12月停止维基解密的捐款支付信道，此后Paypal和西联汇款也加入该行列。迫于财务压力，维基解密于2011年开始支持比特币捐款。那么对于想要支持维基解密的互联网公民来说，比特币成为一种刚性需要。

第三个例子：越来越多的劫匪开始拥抱比特币。迫于劫匪的压力，纽约警方都曾在市场上大量购入比特币交赎金。此外，也有越来越多的木马程序开始加入比特币元素：“往×××地址打入一个比特币，否则你电脑里的文件将被删除。”此时比特币对于警察和受害者也是一种刚性需要，而他们既不是自由主义者也不是极客，对于改变世界的金融秩序更是毫无兴趣。

看，这不就是比特币的内在价值吗？

黄金有内在价值，因为它在某些工业上的消耗需要是不可替代的。同时其作为饰品的需要虽然糅杂了投资和消费，其内在价值却是消费的需要——如果买入某一件物品是为了卖出获利的话，这就不是内在价值。大豆的内在价值是粮食裹腹，咖啡的内在价值是提神醒脑，汽车的内在价值是高效的移动，这些最后都会落到人的非投资需要上。和以上物品一样，比特币的内在价值也不是交易市场里的投资或投机，而是来自于刚才说的那些需要。

就像所有大宗商品一样，我以为比特币的价格构成就像一个鸡蛋，蛋黄是其内在价值，蛋清则是价格投机（图8-2）。

图8-2 比特币价格构成

单纯依靠内在价值也能产生价格，只是比特币作为商品来说天生又是一个交易品（对于买方来说只是购入了比特币，但是对于丝绸之路卖家、阿桑奇、劫匪这一方来说迟早也会卖出，而窍门正是在于“迟早”两字），所以其价格自诞生之日起就包含着内在的消费性需要和外在的价格投机，无法分开。由于作为其价格蛋清组成部分的投机资金占据了更大的比例，这种构成导致了比特币价格长久来看都会是巨幅波动的。

另外要提一句，庞式结构不等于庞氏骗局。庞式结构出现在所有交易品上，股票、大宗商品、黄金、外汇，甚至房产的价格里都有庞式结构存在[56]。交易品的价格就像行驶在大海中的帆船，船上的人们时不时都会被大大小小的旋涡——庞式结构——所影响甚至是卷入。

五、博弈与合作：区块链——信任的机器

2015年11月，《经济学人》刊登了区块链主题的封面文章：信任的机器。信任是什么？信任是一座被云雾覆盖看不到桥面的桥，连接着合作双方。想要合作吗？行，走过桥来。看不到桥面怎么办？不知道对方怎么想的怎么办？选择吧，相信或者不相信。人们为了此次的合作和将来的合作，在选择之前和选择之中和选择之后不断进行着信息的交换和反复的博弈。

信任是什么？信任是一种预期和期望。人们通过信息的收集和自主的判断，对于某项事件的发生（尤指

合作）进行概率的判断。是100%，50%，还是10%？[57]刚才的那座桥就是博弈中的不完全信息，而对于桥对面的人内心想法的猜不透便是博弈中的不完美信息。但是人们始终还是要判断，要去信任，否则人类社会就没有合作，就没有发展。

区块链这个机器通过数学、代码和经济使一些过去发生的记录不可更改甚至牢不可破，这是其一。它还通过智能合约将合作的约定写在区块链上一方面无法更改，另一方面区块链在将来条件触发之时也会自动执行，这是其二。

可以这样去理解区块链的第一个特点“不可更改”。不可更改意味着信息的可信，如果乙方主动提出将区块链上的数据给予甲方，那么其他条件不变至少甲方会更信任乙方和乙方的数据一些。可能甲方本来对于乙方非区块链数据的信任是50%。那么当甲方看到乙方愿意给出区块链数据之后，甲方可以认为由于这些数据造假的难度更高，也就是说虽然仍有造假的可能但是由于区块链提升了乙方造假的机会成本，甲方可能会对乙方数据的信任提升到60%。区块链的数据还有一个特点，即历史越长，造假成本越高。这是因为区块链的数据可以很方便的回溯到此前任一时点。另一方面和一般数据一样的，数据产生的历史交互越多，该数据造假的成本也就越高。所以这时候甲方如果看到乙方给出的区块链数据有10年的历史，而且经过多方使用留下数字签名，那么甲方可能就会对乙方的数据信任提升到80%。这便是第一个特点“不可更改”。

要理解区块链的第二个特点“智能合约”，就要先了解一下博弈论中最基础也是最耐人寻味的“囚徒困境”。囚徒困境讲的是人类在某些合作情况下个人理性与集体理性产生背离。这被认为是人类合作发展的悖论：既然从个人理性和天性出发最优选择总是不合作，那么人类又为何总想着去合作呢？囚徒们彼此合作，可为全体带来最佳利益（无罪开释），但在无法沟通的情况下，因为出卖同伙可为自己带来利益（缩短刑期），也因为同伙把自己招出来可为他带来利益，因此彼此出卖虽违反最佳共同利益，但却是自己最大利益所在。但实际上，执法机构不可能设立如此情境来诱使所有囚徒招供，因为囚徒们必须考虑刑期以外的因素（出卖同伙会受到报复等），而无法完全以执法者所设立之利益（刑期）作考量。解决囚徒困境一般理解有三种方式：第一，订立具有强制力的契约、合同等；第二，重复博弈；第三，教育。[58]智能合约想要实现的便是通过订立具有强制力的契约、合同，解决囚徒困境。

智能合约初看似乎很好，没有问题，细细想来却有很多疑问。一方面具有强制力的契约与合同，似乎已经在社会上普遍存在；另一方面脱离了现有的国家机器，智能合约真的能够实现强制执行吗？

要回答这两个问题，就需要先退回来看一看现行的信任体系是怎么样的。一般认为现行的信任体系来自于两个方面：国家机器和文化传统。

国家机器是对国家层面进行公信力和公权力的背书，在国家的法律法规以外，民间签订的合同也都有对应的法律条款进行约束。相比国家机器的直接明确，文化传统则更软性，主要体现在一些隐形的规则之上。例如，证券公司需要根据法律法规对投资者进行T+1的结算，如果证券公司违规没有按时结算，那么国家机器就会采取行动强制其执行结算。而对于温州人来说各种民间小会的投入和结算则由当地的文化习俗所致。文化习俗的信任体系形成相对较慢，相比国家机器而言成本低很多。2016年春晚宣贯的诚信社会就是希望民间的文化习俗向着互信发展，因为单单依靠国家机器的成本太高了，很多地方管不到也管不好。从刚才三种解决囚徒困境的方式看，可以认为国家机器是订立具有强制力的契约、合同；文化习俗则是重复博弈和教育。

但国家机器不是万能的，订立具有强制力的契约也不是万能的。原因很简单：社会很复杂，事事都要签订契约太麻烦，国家机器在强制执行层面的成本也太高。成本达到一定程度后的结果就是管不了。那么智能合约在这里是不是刚好可以帮助国家机器节约成本呢？如果说要用来填补国家机器空白的话，又如何实现智能合约的强制执行呢？

如前所述，区块链机器具有不可修改和不可逆的特性，以工作量证明机制为例，计算力决定了它数学上的合法性。在国家机器触手无法触及的领域，可以依靠智能合约和数字货币实现自动化执行。此处货币为广义上的货币，即一种价值共识，可以是货币，也可以是信用甚至可以是双方之间独有的价值共识。

当智能合约将甲乙双方的价值共识（当然也包含狭义上的金钱财货）内置其中，并约定通过区块链进行条件设立以及触发后的执行，就等于是甲乙双方在订立合约时进行了相关的承诺。只要价值共识存在，违约成本就存在，双方理性的情况下，承诺的效果就不会变。

那么，区块链消除了“可信第三方”又是指什么？现在的主流说法是区块链实现了“去信任化”，通过区块链使人们不必需要信任对方或是可信第三方机构。区块链实现的是一种信任的转移，使人们在合作过程中的信任对象由人和机构转移到区块链这个共识机器上。

区块链没有消除信任，在合作的过程中人们仍然需要去“信任”一些东西。只不过信任的对象由此前的人和由人组成的机构，转变为共识机制构成的区块链。而共识机制并没有把人性剥离。恰恰相反，共识机制的基础正是人类最为理性纯粹的经济人假设中的逐利特性，辅以密码学以及代码作为封装，再通过互联网和参与者的共同偏好将传播的成本尽量最低。可以认为区块链所做的事情是，先找到人类共有的共识：逐利并通过共识机制收拢，然后告诉具体的博弈双方：别猜了，相信其他人的共识吧，最后具体博弈双方完成博弈合作。当所有使用区块链完成合作的人所获得的集体效应超过维系区块链所需要的成本之时，其应用就会不断发展壮大，也会通过更多的合作增加人类社会的福祉。

[49] 本章由陶荣祺写作完成。陶荣祺，小蚁Onchain VP，上海国际金融研究中心特约研究员，巴比特专栏作家；多年银行、银联、第三方支付及数字货币行业从业背景；《区块链新经济蓝图及导读》译者之一。

[50] 世界上的各类数字货币交易所交易量虽然不断呈上升趋势，可在世界范围被认可的多币种交易所。多币种交易所也被称作“山寨币交易所”或“数字资产交易所”。典型的多币种交易所如Poloniex.com，其以比特币作为基准交易货币，拥有百余个交易品种。同时近年其门槛也有了相对的提高，也就是说某种数字货币要想进入全球交易市场也并不是随心所欲就可以实现的。

[51] Bitcoin Improvement Proposals，基于社区的比特币改良建议。

[52] 比特币虽然有基金会但其口碑与影响力一般，故定其为社区主导。

[53] 或许最近结合量子理论的脑科学告诉了我们答案：人的行为是随机的。

[54] 区块链运行的纳什均衡的定义是：当所有其他人都不改变策略时，没有人会改变自己的策略，则该策略组合就是一个纳什均衡。

[55] 张维迎.博弈与社会［M］.北京：北京大学出版社，2014.

[56] 关于庞式结构的定义和介绍见乐平：《信用、支付和流动性——金融危机结构观察》。

[57] 该定义取来以太坊创始人Vitalik Buterin的Blog“Visions, Part 2: The Problem of Trust”。

[58] 来自耶鲁大学本·波拉克（Ben Polak）教授的公开课。

后记

长铗

如果用一件事物的发明来模拟区块链的诞生，我会选择印刷机。印刷机影响了历史的进程，进而影响人们对资源与交易的认知。

在印刷机诞生之前，人们处理知识的方式就是处理竞争性资源的方式，比如某本手抄本圣经、兵书或制造工艺手册。印刷机、计算机发明以后，知识不再是竞争性资源，而变成了一种可规模化生产的商品，“所有东西都在变成软件。印刷机诞生后，人类写过多少个字，未来就有多少家软件公司……”[59]但与之带来的问题是，在数字世界，我们很难防止资源被复制。我们无法像销售土豆一样销售音乐、软件与其他电子资源，除非我们引入可信第三方，寻求他们来管理我们的财富，证明我们的身份，保护我们知识产权，评估我们的信用。然而，区块链的面世有可能终结这一局面。

如果说印刷机的意义就在于将信息资源抽离物理世界的束缚，变为一种非竞争性资源，区块链则是起着与印刷机截然相反的作用，它以处理竞争性资源的方式来处理信息资源（非竞争性），人们可以摆脱对可信第三方的依赖，在数字世界中自由地交换数字货币、知识产权、股权甚至不动产所有权。虽然两者处理资源的方式是相反的，但两者对话语结构的改变是一致的。

在中世纪，教会垄断着知识与教育，普通人没有直接阅读和解释《圣经》的权利，教会能随心所欲地释读《圣经》。同样，行业工会为了垄断商品制造工艺，排斥外来竞争，对制造工艺知识的出版印刷进行严格的控制。那个时候欧洲大多数国家都通过许可制度，对印刷出版进行严格的管控，而权力则掌握在天主教堂和政府的手中。行业工会则与天主教和政府进行合谋，对工艺知识的出版和流通进行审查。

也许，今天的我们难以理解私自印刷一本《几何原本》怎么会是犯罪行为。可是仔细想一下，中心化的信用管理机构，不正像是中世纪的行会吗？如果区块链技术能够代替第三方完成对信用的管理，甚至管理的更高效、更安全，我们为什么不投身于其中，去探讨另一种可能？

三年前，我与志趣相投的朋友们一道写了国内第一本比特币专着《比特币——一个真实而虚幻的金融世界》。三年后，比特币归于沉寂，一些曾经热血沸腾的朋友也杳如黄鹤渐无音信，所幸，更多的人坚持了下来，从比特币底层技术里窥见了区块链的潜力。于是，这本书有了更多远见卓识的同人加入，他们有学者、研究员、程序员，还有创业者，在各自擅长的领域，如经济、管理、金融、法律、创业实践等，贡献自己的思想与热情……

在组稿过程中，我们并不盲求认识统一，而是主张各自在专业领域自由发挥所长。区块链思想就好比一个多面体骰子，目前有一面已经揭晓，即数字货币，我们都承认比特币是第一个成功的区块链应用，但接下来，掷下的骰子会是哪面？却是个未知数。每个人心中都有一个自己理解的区块链，很难说哪种理解更高明、更深远。正如本书的副标题，一波三折。起初，达鸿飞主张叫“从数字货币到可编程社会”；后来韩锋老师提议叫“从数字货币到信用协议基础”，还有杨涛老师、蒋海提议“从数字货币到价值互联”……

可编程社会侧重的是区块链强大的脚本功能与可扩展性，区块链通过特定的算法来计算出权益、信用与身份的真伪，这些算法以强大的加密技术为支撑，可以根据不同应用场景，灵活编写不同的智能合约。

信用协议基础侧重的是区块链交易不可逆、数据不可篡改的一面。需要指出的是信用在此有两种蕴含，第一层是信任，解决的是交易行为的诚实问题。工作量证明等共识机制的发明消除了对可信第三方的依赖，通过分布式网络来保障交易的真实可靠，杜绝了双重支付、交易回滚的可能。第二层是信用，解决的是交易对象的诚实问题。区块链信用的真实可靠，可以让两个素昧平生的人彼此交易，或者完成借贷、担保交易等复杂智能合约行为，本质上利用的是区块链时间戳使真实交易行为与刷信用交易行为在概率分布上可区分的特性。

价值互联网侧重的是区块链以处理竞争性资源的方式来处理非竞争性资源的一面，有人说区块链是互联

网世界继万维网以来的的第二个伟大纪元。如果说万维网实现了信息互联网，把竞争性资源搬到了数字世界，使复制的边际成本无限等于零，那么区块链则实现了价值互联网，可以在数字世界中处理竞争性资源，使攻击者难以承受51%攻击、篡改交易记录的成本。

还有人把区块链理解为共享账簿，欧洲央行和英国政府都发布了关于共享账簿的报告，侧重的是区块链作为分布式记账的一面，旨在从政府职能与不同利益集团的角度，改善自身业务流程与服务公民、用户的质量，提高金融市场、供应链、电子商务以及上市公司注册等领域的效率。但将区块链仅仅视为一个分布式的记账系统，是一种买椟还珠式的误解。分布式的记账功能，不过是区块链众多特性中的一个。共享账簿只是看到了区块链在数据库层面的创新，而忽视了区块链在创建信用的互联网协议层面的创新。

《经济学人》则把区块链喻为“信任的机器”，机器是智能合约的形象化，每一个智能合约就像是一个原胞自动机，通过简单的规则，构造各种不同的交易行为，整体上大大优化社会资源的流转效率。区块链将过去我们对权威第三方的信任转化为对算法对数学的信任。但信任仅是信用的第一层蕴含，针对的是交易行为本身，信用机器一词的蕴含更饱满，因为区块链同样可以创建交易对象的信用，一个人的区块链交易历史足以证明他的诚信记录，且这种记录具有专属性与跨平台性。然而即使是信用机器的说法，也是不够全面。如潘志彪所指出的，区块链不是一般的机器，大部分机器可以被关掉，区块链却是一个分布式系统，一旦被启动，便无法停机。最终，我们选择“从数字货币到信用社会”这一副标题，因为我们相信随着信息互联网向价值互联网的过渡，区块链终将润物细无声，深入到社会的方方面面。

区块链是一种思想，是许多个开源项目的集合，也是无数头脑风暴的“总账”，技术会被淘汰，发明会过时，公司会倒闭，但分布式思想不会。正如印刷机的诞生一举瓦解了中世纪行会、教会对知识的垄断，重塑了社会权力结构，区块链技术也将从根本上改变今天我们对资源与交易的理解，改变政府、公司与个体参与经济行为的方式。托克维尔在《美国的民主》中说：“枪炮的发明使奴隶和贵族在战场上平等对峙；印刷术为各阶层的人们打开了信息之门，邮差把知识一视同仁地送到茅屋和宫殿前。”那么现在，时代可以为这段话添加新的注脚：区块链为我们启动了信用机器，让政府、公司、机构与个体作为平等的节点呈现在分布式网络上，各自管理自己的身份与信用，共享一部不可修改的交易总账。

虽然区块链技术自身还不完善，就像是一个粗陋的玩具，但不要忘了1876年电话发明时，人们是怎样评价的。在当年西联电报公司备忘录里还写着：“电话这个东西毛病太多，并不是一个值得考虑的通信方式，基本上对我们没有什么价值。”

[59] 阮一峰在《黑客与画家》中介绍保罗·格雷厄姆（Paul Graham）时引用的一句话。

附录

附录1 国内区块链项目一览表

附录2 国外区块链项目一览表

附录3 区块链专业名词中英文对照表 [60]

A

51% attacks51% 攻击

account level(multiaccountstructure) 账户等级（多账户结构）

accounts 账户

addition operator 加法操作符

addr message 地址消息

Advanced Encryption Standard(AES) 高级加密标准(AES)

altchains 竞争币区块链

altcoins 竞争币

anonymity 匿名

assembling blocks into 将区块集合至

Asymmetric Cryptography 非对称加密

attacks 攻击

authentication path 认证路径

B

backing up 备份

balanced trees 平衡树

balances 余额

Base58 encodingBase58 编码

Base—64 representation Base—64表示

binary hash tree 二叉哈希树

BIP0038 encryption BIP0038 加密标准

Bitcoin 比特币

bitcoin addresses 比特币地址

bitcoin ledger 比特币账目

bitcoin network 比特币网络

Bitshares 比特股

Blake algorithmBlake 算法

Blockchain 区块链

block chain apps 区块链应用

block generation rate 出块速度

block hash 区块散列值

block header hash 区块头散列值

block headers 区块头

block height 区块高度

block templates 区块模板

blockchains 区块链

bloom filtersand 布鲁姆过滤器

BOINC open grid computingBOINC 开放式网格计算

broad casting to network 全网广播

broad casting transactions to 广播交易到

Byzantine Generals Problem 拜占庭将军问题

Byzantine Quorum Systems 拜占庭容错机制

C

centralized control 中心化控制

chaining transactions 交易链条

Chaumian blinding 盲签名技术

check Block function(Bitcoin Core Client）区块检查功能（Bitcoin Core 客户端）

checksum 校验和

child key derivation(CKD) function 子密钥导出(CKD)函数

child private keys 子私钥

coinbase 币基

coinbase rewards 币基奖励

coinbase transaction 币基交易

CoinDays 币天（币龄）

cold-storage wallets 冷钱包

ColoredCoin 彩色币

Collectively maintain 集体维护

compressed keys 压缩钥

compressed private keys 压缩格式私钥

compressed public keys 压缩格式公钥

computing power 算力

connections 连接

Consortium Blockchains 共同体区块链（联盟链）

Consensus 共识

constant 常数

constructing block headers 构造区块头部

converting compressed keys to 将压缩地址转换为

converting to bitcoin addresses 转换为比特币地址

counterparty protocol 合约方协议

Counterparty 合约币

CryptoCurrency 加密货币

CryptoCredits 加密信用

Cunning hamprime chains 坎宁安素数链

currency creation 货币创造

D

data structure 数据结构

decentralized 去中心化

decentralized consensus 去中心化共识

decoding Base58Check to/from hexBase58Check 编码与16进制的相互转换

decoding to hex 解码为16进制

deflationary money 通缩货币

delegated proof of stake 股份授权证明

demurrage currency 滞期费

denial of service attack 拒绝服务攻击

deterministic wallets 确定性钱包

difficulty bits 难度位

difficulty retargeting 难度调整

difficulty targets 难度目标

digital signature 数字签名

digitalnotary services 数字公证服务

Distributed Ledger 分布式账本

domain name service(DNS) 域名服务(DNS)

double-spend attack 双重支付攻击

dual-purpose 双重目标

dual-purposemining 双重目的挖矿

dust rule 尘额规则

E

electricity cost 电力成本

electricity cost and target difficulty 电力消耗与目标难度

Electrum wallet Electrum 钱包

Elements 元素链

Ethereum 以太坊

ellipticcurve multiplication 椭圆曲线乘法

encoding/decoding from Base58Check 依据Base58Check 编码/解码

encrypted 加密

encryption algorithm 加密算法

encrypted private keys 加密私钥

extended key 扩展密钥

extra nonce solutions 添加额外随机数的方式

F

fees 手续费

field programma blegatearray(FPGA) 现场可编程门阵列(FPGA)

fork attack 分叉攻击

forks 分叉

full nodes 完整节点

G

generating 生成

generation transactions 生成交易

generator point 生成点

genesis block 创世块

genesis block 创世区块

GetBlock Template(GBT)mining protocolGBT 挖矿协议

GetWork(GWK) mining protocol GWK 挖矿协议

graphical processing units(GPUs) 图形处理单元(GPUs)

H

hackers 黑客

hardware wallets 硬件钱包

Hash 哈希，又称散列

HashCash 哈希现金

Hashed Timelock Contract 哈希时间锁定合约HTLC

hashing powerand 哈希算力

HD walletHD 钱包

header hash 头部散列值

Hierarchy deterministic 分层确定的

Hyperledger 超级账本

I

identifiers 标识符

immutability of blockchai 区块链不可更改性

in block header 在区块的头部

independent verificatio 独立验证

I owe you 借据（IOU）

K

key formats 密钥格式

L

Level DB database(Google)LevelDB 数据库(Google)

light weight 轻量级

Lightning Network 闪电网络

lock time 锁定时间

lock time 锁定时间

locking scripts 锁定脚本

M

managed pools 托管池

Mastercoin 万事达币

memorypool 内存池

merkle tree 默克尔树

merged mining 合并挖矿

metachains 附生区块链

Micro-Payments Channel 微支付信道

mining 挖矿

mining blocks successfully 成功挖出区块

mining pools 矿池

mining rigs 矿机

modifying private key formats 修改密钥格式

monetary parameter alternatives 货币参数替代物

Moore□sLaw 摩尔定律

multi account structure 多重账户结构

multi-signature addresse 多重签名地址

multi-signature addresses 多重签名地址

multi-signature scripts 多重签名脚本

multi-signature account 多重签名账户

N

Namecoin 域名币

nodes 节点

nonce 随机数

noncurrency 非货币

nondeterministic wallets 非确定性的

O

on full nodes 在全节点上

on new nodes 在新节点上

on SPV nodes 在SPV 节点

on the bitcoin network 在比特币网络中

OP_RETURN operatorOP_RETURN 操作符

OpenSSL cryptographiclibraryOpenSSL 密码库

orphan block 孤块

outputs 输出

P

P2P Pool 点对点挖矿的矿池

parent blocks 父区块

peer-to-peer networksP2P 网络

physical bitcoin storage 比特币物理存储

Practical Byzantine Fault Tolerance 改进型实用拜占庭容错机制（简称PBFT）

Premine 预挖

priority of transactions 交易优先级

Private Blockchain 私有区块链

Proof of existence 存在性证明

proof of stake 权益证明

proof of work 工作量证明

propagating transactions on 交易广播

protein folding algorithms 蛋白质折叠算法

Public Blockchain 公共区块链（公有链）

public child key derivation 公钥子钥派生

public child key derivation 导出公有子密钥

publickeys 公钥

public key derivation 公钥推导

purpose level(multiaccount structure)目标层（多帐户结构）

Python ECDSA library PythonECDSA 库

R

random 随机

retargeting 切换目标

Reliable Database 可靠数据库

Reusable Proofs of Work 可复用的工作量验证

Revocable Sequence Maturity Contract 序列到期可撤销合约RSMC

RIPEMD160RIPEMD160算法

Ripple Consensus Protocol 瑞波共识协议

risk balancing 适度安保

risk diversifying 分散风险

root of trust 可信根

root seeds 根种子

S

satoshis 聪

scriptcons truction 脚本构建

script language for 脚本语言

Script Language 脚本语言

scripts 脚本

scrypt algorithmscrypt 算法

scrypt-N algorithmscrypt-N 算法

Secure Hash Algorithm(SHA)SHA 哈希算法

Secure Multi-party Computation 多方安全计算

seed nodes 种子节点

seeded 种子

seeded wallets 种子钱包

Segregated Witness 隔离见证

shopping carts public keys 购物车公钥

simplified payment verification (SPV)简易支付验证（SPV）

sidechains 侧链

Skein algorithmSkein 算法

smart contracts 智能合约

smart pool 机枪池

solo miners 独立矿工

solo mining 单机挖矿

stateless verification of transactions 交易状态验证

statelessness 无状态

Stellar Consensus Protocol(SCP)恒星共识（SCP）

storage 存储

Stratum(STM)mining protocolStratum 挖矿协议

syncing the blockchain 同步区块链

system security 系统安全

T

taking off blockchain 从区块链中删除

testnet 比特币测试网络

timeline 时间轴

timestamp 时间戳

token system 代币系统

transaction fees 矿工费

transaction fees 交易费

transaction pools 交易池

transaction validation 交易验证

transactions independent verification 独立验证交易

tree structure 树结构

Trezor walletTrezor 钱包

Turing Complete 图灵完备

trust in a third party 可信第三方

tx messagestx 消息

Type-0 nondeterministic wallet 原始随机钱包

U

uncompressed keys 解密钥

unconfirmed transactions 未确认交易

user security 用户安全性

UTXO 未花费的输出

UTXO poolUTXO 池

UTXO setUTXO 集合

V

validating new blocks 验证新区块

validation 验证条件

validation(transaction) 校验(交易)

vanity addresses 个性地址

vanity-miners 个性地址挖掘程序

verification 验证

verification criteria 验证条件

version message 版本信息

W

Wallet Import Format(WIF)钱包导入格式

wallets 钱包

[60] 巴比特翻译小组整理。

图书在版编目（CIP）数据

区块链:从数字货币到信用社会 / 长铗等着.—北京：中信出版社，2016.7

ISBN 978-7-5086-6344-9

I.①区… II.①长… III.①电子商务—支付方式—研究 IV.①F713.36

中国版本图书馆CIP数据核字（2016）第126195号

区块链:从数字货币到信用社会

著者：长铗 韩锋 等

策划推广：中信出版社（China CITIC Press）

出版发行：中信出版集团股份有限公司

（北京市朝阳区惠新东街甲4号富盛大厦2座 邮编100029）

（CITIC Publishing Group）

电子书排版：张明霞

中信出版社官网：http://www.citicpub.com/

官方微博：http://weibo.com/citicpub

更多好书，尽在大布阅读；

大布阅读：App下载地址（中信电子书直销平台）

微信号：大布阅读

Table of Contents