第五章　加密货币：炒作之外

在出现不到 10 年的时间里，加密货币[①]从默默无闻到引起企业和消费者以及中央银行和其他当局的强烈兴趣。加密货币获得关注的原因在于提供了新的信用机制，即采用全新的基于区块链和分布式账本技术的完全去中心化系统的信用，替代商业银行、中央银行这些历史悠久的机构的信用。

本章将评估加密货币是否能扮演货币的角色：抛开炒作，加密货币能否解决具体的经济问题？本章首先回顾了历史背景。许多货币不稳定和货币崩溃的例子表明，货币供应的制度安排十分重要。我们的回顾表明，好的货币的本质一直是对其币值稳定的信任。而货币若要拥有其标志性属性，即作为促进交易的协调手段，需要有效地与经济规模相匹配，并通过有弹性的供给来应对需求的波动。这些性质需要特定的制度安排，这也是如今独立、可靠的中央银行出现的原因。

本章接下来对加密货币进行了介绍，并探讨去中心化创造信用所固有的经济局限性。为了维持信用，诚实的网络参与者需要控制绝大多数计算能力，每个用户需要验证交易历史，加密货币的供应也需要通过其协议预先确定。由于记录交易的去中心化共识具有脆弱性，信任随时会消失。

这不仅会影响个人支付的最终性，还意味着加密货币可能会直接停止运作，导致价值的完全丧失。而且，即使信用可以维持，加密货币技术也带来了效率的低下和能源的耗费。

加密货币不能随着交易需求而扩大规模，容易出现拥堵并且币值波动大。总的来看，加密货币的去中心化技术无论多么复杂，对于有坚实制度依托的货币来说都是糟糕的替代品。

尽管如此，其底层技术仍可能在其他程序中有所应用，例如简化金融交易结算的行政流程。不过，这仍有待测试。由于加密货币引发了许多问题，本章最后讨论了政策应对，包括对私人使用技术的监管，防止滥用加密货币的措施以及中央银行发行数字货币所引发的微妙问题。

审视加密货币的崛起

检验一项新技术能否对现有货币格局形成有益补充的一个好方法是退后一步，回顾货币在经济中的基本作用，以及创造新私人货币的失败尝试告诉我们的历史经验。之后我们才能探究，基于这种新技术的货币能否以任何方式改善现有货币格局[②]。

货币简史

货币在便利经济交换中扮演着关键角色。在它问世的几千年前，商品主要是通过未来的利益回报承诺（即交易欠条）[3]来交易的。然而，随着社会规模增长，经济活动扩张，记录日益复杂的欠条变得越来越困难，违约和结算风险成为隐忧。为了解决与日俱增的复杂性和与之相关的信任难题，货币和货币发行机构应运而生。

货币有三个基础且互补的作用，它是：（1）记账单位：这是一个衡量我们购买物品的价格以及我们所做承诺的价值的标准；（2）交易媒介：卖方接受它作为支付手段，且期望别人也接受它；（3）价值储藏：使用户能够随时间而转移购买力[4]。

为了完成这些功能，货币需要在不同地方有相同的价值，并保持价值稳定。如果人们能确信收到的货币在当下和未来都有稳定的购买力，评估是否要卖某种商品或服务就会简单得多。实现这个目标的一种方法是使用具有内在价值的纯商品货币，例如盐或谷物。但商品货币本身不能有效地支持交易：它不总是易得，生产成本昂贵，交易繁琐，还可能易腐坏[5]。

经济活动的扩张需要更多便利的货币来应对不断增长的需求，有效地用于贸易并具有稳定的价值。然而，维持对货币供应制度安排的信任一直是最大的挑战。在世界各地，不同背景和年代，货币开始依赖中心化当局的发行。在古代，主权印章证明了硬币在交易中的价值，随后，由银行作为中介的汇票交易成为商人节省携带大量货币旅行的成本和风险的一种方式[6]。

然而，历史经验也表明，供给具有弹性的货币很容易贬值，两者存在权衡取舍[7]。长期稳定的货币在历史上其实是特例而不是常态。事实上，信任的崩溃相当频繁，历史就是货币的坟墓。世界各地的博物馆用整片的区域展示死去的货币——比如大英博物馆 68 号房间展示了石头、贝壳、烟草、无数的硬币和纸币以及其他很多物品，人们不再接受它们作为交换媒介。有些货币成为商业和经济活动扩张的牺牲品，被认为不便于大规模使用。有些货币被抛弃是因为曾经支持它们的政治秩序弱化或崩溃。还有很多货币被弃用是因为对其价值稳定性的信任被侵蚀。

历史证明，无论货币供应者是竞争性的私人还是垄断性的主权国家，货币都可能是脆弱的。银行发行的货币质量取决于支撑它的资产质量。银行希望转换风险，因此在极端情况下，对私人发行的货币的信心可能在一夜之间消失。对政府支持的货币安排来说，维持对货币的信任是一项集中的任务，但也并不总是奏效。历史还远非如此，一个众所周知的例子是 17 世纪早期德国王子们发行的硬币出现了竞争性贬值，史称“Kipper – und Wipperzeit”[8]。还有很多其他例子，比如当今委内瑞拉和津巴布韦的案例。因此，避免主权国家的滥用是货币安排设计中的关键考量因素。

追求货币信用的坚实制度基础最终导致了当今的中央银行的出现。早期的例子是 1400—1600 年期间在欧洲城邦建立的特许公共银行，通过提供高质量、高效的支付方式和集中处理一系列清算结算业务来改进交易。这些银行设立在阿姆

斯特丹、巴塞罗那、热那亚、汉堡、威尼斯等贸易中心，在促进国际贸易和更广泛的经济活动方面发挥了重要作用。[9]随着时间推移，特许银行的运作方式与目前的中央银行类似。我们今天所知道的正式的中央银行，其诞生通常也是为了应对表现不佳的非中心货币。例如，美国的“野猫银行”（在联邦政府的监管之外开设的银行）的失败最终导致了联邦储备系统的诞生。

当前货币和支付体系

独立的中央银行是现代社会提供货币信心的可靠、值得信赖且稳健的方式。这意味着商定的目标：清晰的货币政策和金融稳定目标；操作上、工具上和行政上的独立性；承担民主责任，确保广泛的政治支持和合法性。独立央行很大程度上实现了用稳定货币保护社会经济和政治利益的目标。[10]在这种设定下，货币可以被精确地定义为“在享有公共信任的国家内由负责任的机构支持的不可或缺的社会惯例”。[11]

几乎在所有现代经济体中，货币都由中央银行和私人银行共同提供，中央银行则是这一体系的核心。电子银行存款是最终用户之间支付的主要手段，而中央银行的存款则是银行之间的支付手段。在这个双层体系中，信任由独立而可靠的中央银行产生，中央银行通过资产持有和操作规则支持准备金。反过来，对银行存款的信任是通过各种手段产生的，包括监管、监督和储蓄保险制度，其中许多途径最终归结于国家。

作为履行其维持稳定记账单位和支付手段职责的一部分，中央银行在监督和监管并在某些情况下为其货币提供支付基础设施方面发挥着积极作用。中央银行的角色包括确保支付系统平稳运行，确保准备金的供应能够妥善应对不断变化的需求（包括日内变动），即确保弹性的货币供应。[12]

得益于中央银行的积极参与，当今多元化的支付系统已经实现了安全性、成本效益、可扩展性和对支付最终性的信任。

支付系统既安全又具成本效益，可以在几乎没有任何滥用和低成本的条件下，处理大量支付，并适应快速增长。安全性和成本效益的一个重要贡献因素是可扩展性。在当今复杂经济中，支付量非常巨大，是 GDP 的数倍。尽管如此，工具的大规模使用并不会带来成本的等比例增加。这一点很重要，因为任何成功的货币和支付系统的基本特征是买卖双方的广泛使用情况：当使用特定支付系统的其他人越多，一个人使用该系统的自身动机就越强。

使用者不仅要对货币本身有信心，还需要相信支付能快速且顺利地进行。因此理想的操作属性是支付的确定性（“最终性”），以及判定交易可能被错误执行的相关能力。“最终性”意味着系统在个别交易和系统整体层面都基本没有欺骗和操作风险。强大的监管和央行负责制都有助于支持最终性，进而增进信任。

尽管现代大多数交易手段最终都由央行支持，但随着时间的推移，各种公共和私人支付手段层出不穷。我们可以用一种称为“货币之花”的分类体系来很好地归纳它们（图 5. 1）。[13]

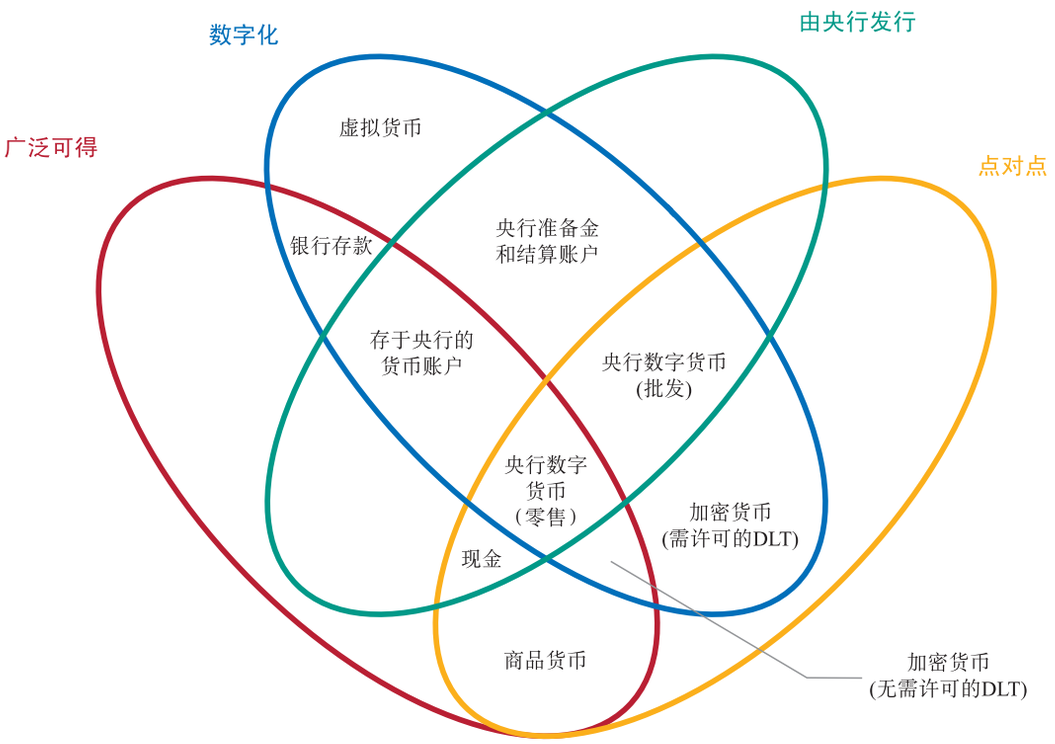

图 5.1　货币之花：对货币的分类

资料来源：改编自 M Bech and R Garratt，《央行数字货币》，BIS 季报，2017 年 9 月，第 55—70 页。

货币之花区分了货币的四个关键属性：发行者、形式、可得性和支付转移机制。发行人可以是中央银行、银行或无人发行，就像货币采取商品形式的情况一样。其形式可以是实体的，例如金属硬币和纸币，也可以是数字的。它可以像商业银行存款那样广泛可得，也可以像中央银行准备金那样只在小范围内可得。最后一个属性关于转移机制，可以是点对点的，也可以是经由中央中介机构，比如存款。货币通常基于两种基本技术之一：所谓的“代币”或账户。基于“代币”的货币，例如纸币和硬币，可以点对点地交换，但这种交换依赖于收币方验证支付物的真实性的能力——对现金来说就是假币的问题。相比之下，基于账户资金的系统从根本上取决于验证账户持有人身份的能力。

加密货币：去中心化信用的不明朗的未来

加密货币能实现它们所承诺的吗？或者最终只是昙花一现？为回答这些问题，我们需要更精确地定义加密货币，了解支持它们的技术，同时审视相关的经济局限性。

货币之花的新花瓣？

加密货币渴望成为一种新的货币形式，并承诺通过技术手段维持对其币值稳

定的信任。它们由三个要素构成：第一，一组规则（“协议”），指明参与者如何交易的计算机代码；第二，存储交易历史的账本；第三，去中心化的参与者网络，他们依据协议中的规则更新、存储、读取交易账簿。有了这些要素，加密货币的倡导者声称，加密货币不会受害于银行和主权国家的潜在不良意图。

就货币之花的分类而言，加密货币结合了三个关键要素：第一，它们是数字化的，致力于成为一种便利的支付手段，并依靠加密技术来防止伪造和欺诈性交易；第二，尽管是私人创设的，它们不是任何人的负债，即它们不能被赎买，它们的价值只来自于对它们会继续被其他人所接受的预期。这使它们有点类似商品货币（尽管没有任何内在使用价值）；第三，它们允许数字化点对点交易。

和其他的私人数字货币（如银行储蓄）相比，加密货币的突出特点是数字化点对点交易。数字银行账户数十年前就出现了，私人发行的“虚拟货币”（例如在魔兽世界这种大型多玩家在线游戏中使用的货币）也比加密货币早出现十年，与之不同的是，加密货币的交易原则上可以在去中心化场景下发生，不需要一个中央对手方来执行交易。

加密货币的分布式账本技术

数字化点对点交易的技术挑战是所谓的“双重花费问题”。任何数字形式的货币都很容易复制，因此可能会被欺诈地花费不止一次。数字信息比纸币更容易被复制。对数字货币来说，解决双重花费问题至少需要有人记录所有交易。在加密货币之前，唯一的解决方案是设立一个中央代理人来执行此操作并验证所有交易。

加密货币通过利用分布式账本（DLT）来去中心化地记录交易，以此解决双重花费问题。账本可以被看成是一个文件（就像一个 Excel 工作簿），以加密货币的最初发布开始，记录了此后的所有交易历史。整个账本的最新副本由每个用户存储（即所谓“分布式”）。有了分布式账本，数字货币就可以进行点对点交易了，每个用户可以直接在自己的账本副本中验证是否发生了转账，以及是否存在双重花费问题。[14]

所有加密货币都依赖于分布式账本，但它们在账本更新方式方面存在差异。人们可以将之区分为两大类，它们的操作设置有显著的差异（图 5. 2 和表 5. 1）。

第一类是基于“需许可”的分布式账本技术。这类加密货币类似于传统的支付机制，为了防止滥用，账本只能由加密货币中的可信参与者（被称为“受信节点”）更新。这些节点由中央当局选定并受其监督，例如开发加密货币的公司。因此，虽然基于授权系统的加密货币在交易记录存储方式（去中心化和中心化）方面与传统货币不同，但它们与传统货币相同，都依赖于特定机构作为最终的信任来源。[15]

第二类加密货币和当前基于机构的货币设置相比则彻底不同，它们采用“无需许可”的分布式账本技术，在完全去中心化的场景下创造信用。记录交易的账本只能被货币参与者的共识所修改：人人都能参与，但没有人有修改账本的特殊钥匙。

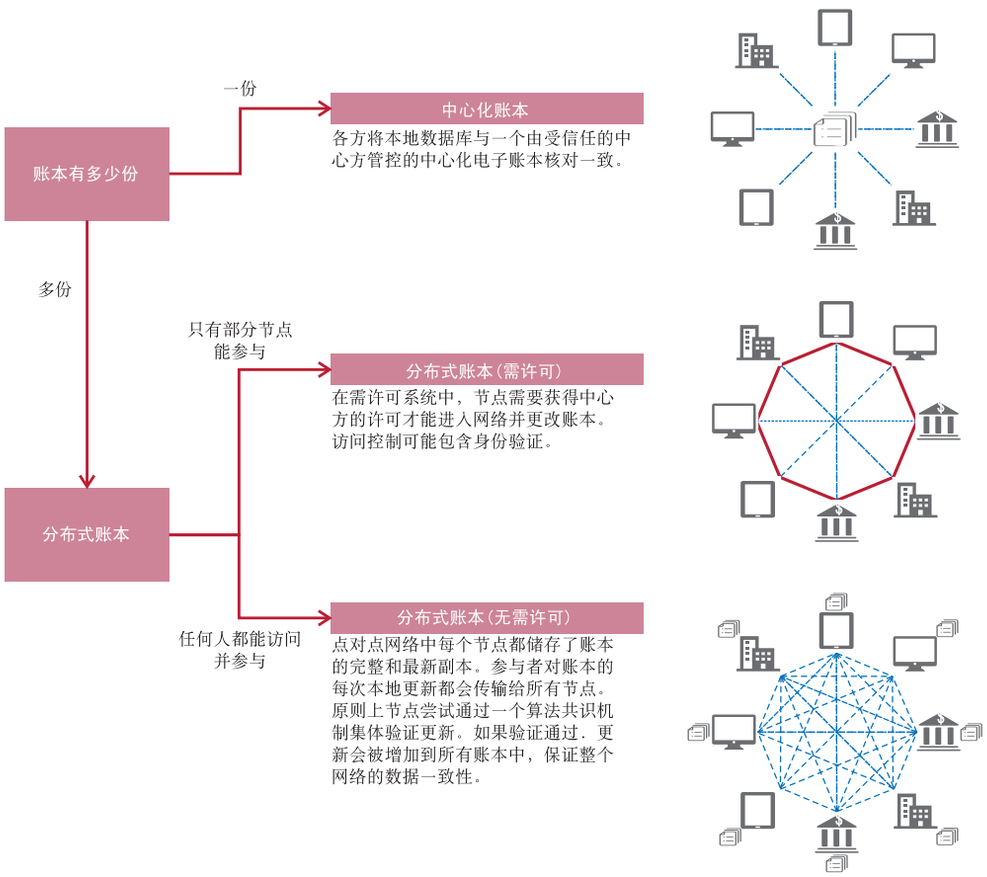

图 5.2　中心化账本和需许可/无需许可的去中心化账本

表 5.1　　中心化账本和需许可/无需许可的去中心化账本

	基于法币系统的私人电子货币	私人发行的加密货币	
		需许可	无需许可
1. 余额/持有量的储存	账本（账户）由银行或其他金融机构中心化储存	账本去中心化储存	
2. 防止双重花费的验证措施	基于身份的概念	点对点的概念：可以检查分布式账本来核对某一单位的货币是否已经被支出	
3. 处理交易	银行更新账户	受信任节点更新账本	通过工作证明更新账本；遵从最长链条的规则
4. 最终性/清算的概念	最终通过央行清算	加密货币自身清算	由于存在遵从最长链条的规则，最终性概念是概率性的
5. 供给弹性	中央银行政策，例如关于日内信贷活动的政策	基于协议，受信任节点可以更改	基于预先确定的协议
6. 信任创造机制	银行和央行的声誉，银行监管，最后借款人机制，法币相关的法律，央行独立性和可靠性，反洗钱反恐融资检查，网络安全	发行公司和节点的声誉；受信任节点，其中有些可能受到监督	工作证明需要诚实的多数算力

资料来源：改编自 H Natarajan，S Krause and H Gradstein，“Distributed ledger technology（DLT）and blockchain”，World Bank Group，FinTech Note，no 1，2017；BIS.

无许可加密货币的概念是由一位（或一组）匿名程序员以假名 Satoshi Nakamoto 在白皮书中为比特币[16]的案例提出的，他提出一种基于特定种类的分布式账本——即“区块链”——的货币。区块链是一个分布式账本，它在被称为区块的交易组中进行更新。然后通过使用加密技术将每块连接形成区块链。这个概念已经适用于无数其他加密货币。[17]

基于区块链的无需许可的加密货币有两类参与者：充当记账员的“矿工”和想要交易加密货币的“用户”。从表面上来看，这些加密货币的基本思路很简单：与银行集中记录交易（图 5.3 左）不同，矿工更新账本，随后更新后的账本由所有用户和矿工存储（图 5.3 右）[18]。

在这个设置之下，这些加密货币的关键特征是实施一组规则（协议）来统一所有参与者的动机，以便在没有中央信任代理人的情况下创建可靠的支付技术。协议确定资产的供应以抵御贬值，例如在比特币的例子下，该协议规定比特币数量的上限是 2100 万。此外，协议还需确保所有参与者都出于自身利益维持规则，即他们形成了可自我保持的均衡。这里有三个关键点：

首先，这些规则带来了更新账本的成本。在大多数情况下，这种成本是因为更新需要“工作证明”，即通过数学证据表明已经完成了一定量的计算工作，反过来又要求昂贵的设备和电力使用，由于工作证明过程可以类比为通过费力的计算挖掘罕见数字，因此通常称为采矿，[19]作为对他们努力的回报，矿工从用户处收取费用，如果协议规定的话，就是新铸的加密货币。

其次，加密货币的所有矿工和用户会验证所有的账本更新，这会引导矿工只

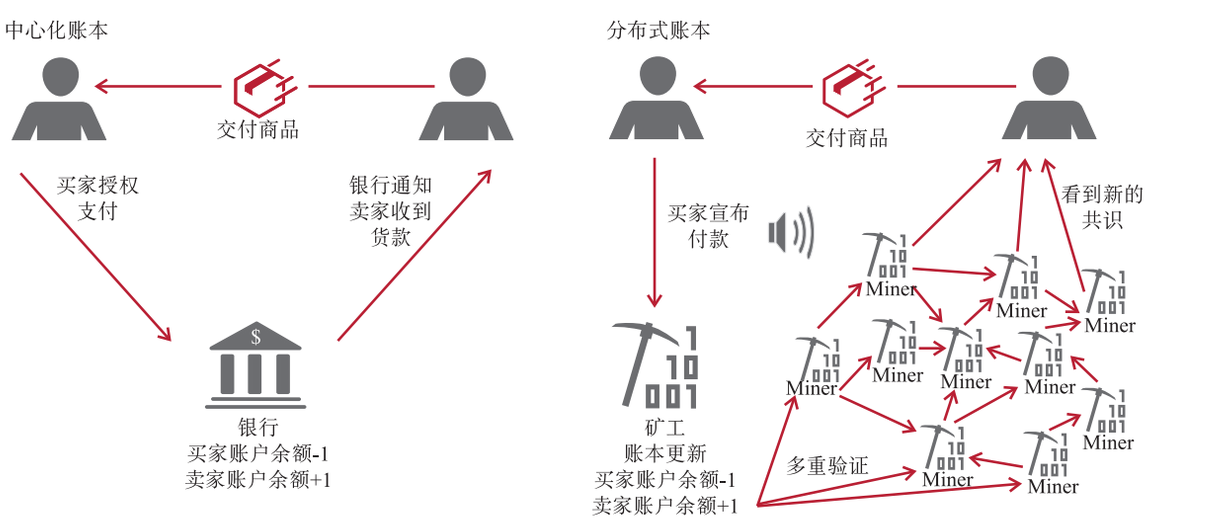

图 5.3　中心化账本/银行账户和无需许可加密货币中的交易验证

买家从卖家手中购买商品，卖家受到支付确认后即交付商品。如果支付通过银行账户完成，即通过中心化账本（如图左侧）完成，则买家向银行发送付款指令，银行调整余额，从买家账户扣减相应金额并增加至卖家账户。银行随后向卖家确认付款。与之不同，如果支付通过无需许可的加密货币（如图右侧），买家首先公开宣布支付指令，宣称买家持有量减一，同时卖家持有量加一。一段时间的延迟后，一个矿工在账本更新中包含了这个支付信息。更新后的账本被其他矿工和用户接受，每个人都验证新增的这个交易指令不涉及双重花费，并已经买家授权。随后，卖家才观察到包含了此次支付的账本被矿工和用户网络广泛接受。

资料来源：改编自 R Auer. “The mechanics of decentralised trust in Bitcoin and the blockchain”，BIS 工作报告，即将发表。

把有效的交易涵盖进去。有效的交易需要由资金所有者发起，且不能尝试双重花费。如果账本更新包含了无效交易，它会被网络拒绝，矿工奖励也会被取消。矿工和用户网络对所有账本更新的核查对于激励矿工只增加有效交易至关重要。[20]

最后，协议规定了规则，以对账本更新的顺序达成共识。这通常是通过创建激励措施，使个人矿工实施更新时跟随其他所有矿工的多数算力。这种协调是必需的，例如，通信迟滞导致不同矿工增加了互相冲突的更新条目，即包含不同交易集的更新，这样的问题需得到解决。

有了这些关键要素，任何人伪造加密货币的成本都会非常高昂，尽管不是不可能。要成功实现双重花费，伪造者需要把加密货币花给一个商家，同时秘密伪造一个未记录此次交易的区块链。收到商品后，伪造者发布伪造的区块链，即逆转付款。只有这段伪造的区块链比其他网络矿工在此期间制作的区块链更长的前提下，这种伪造的区块链才可能成为普遍接受的链。因此一次成功的双重花费攻击需要拥有大量的算力。反过来说，用比特币白皮书的话说，只有“诚实的节点控制了大部分（计算）能力”，加密货币才能以去中心化的方式克服双重花费问题。[21]

评估无需许可加密货币的经济局限性

比特币等加密货币承诺带来的不只是基于数字技术的支付方式，还是一种新的信任模式。但实现这一承诺取决于一系列假设：诚实的矿工控制绝大多数计算能力，用户核查所有交易历史，协议预先设定货币供给。理解这些假设很重要，因为它们对加密货币的实用性提出了两个问题：第一，这种试图实现信任的繁琐方法是否以牺牲效率为代价？第二，信任是否真正得以实现并永续？

正如第一个问题所暗示的，效率方面一个关键的潜在限制是获取去中心化信任所带来的巨大成本。人们预计矿工会持续通过工作证明竞争为账本增加新区块，直到他们的期望利润降至零。[22]由矿工运营的个人设施可以拥有与数百万台个人电脑相当的计算能力。在本书写作之时，比特币挖矿总耗电量与瑞士这样的中型经济体耗电量相当，其他加密货币也使用了相当多的电力（图 5.4 左）。简而言之，对去中心化信任的追求很快就会变成一场环境灾难。[23]

但潜在的经济问题远远超出能源问题。这涉及货币的标志性属性：促进使用者之间的“网络外部性”，从而成为经济活动的协调工具。加密货币在这方面的缺点体现在三个方面：可扩张性、币值稳定、对支付最终性的信任。

首先，加密货币根本不能像主权货币那样大规模扩张。在最基本的层面上说，为了达到它们所宣扬的去中心化信任，加密货币需要每个使用者下载并验证所有历史交易，包括支付金额、支付者、接收者和其他细节信息。随着每次交易增加几百字节，账本“篇幅”会随着时间的推移大幅增长。比如，在撰写本书时，比特币区块链每年增长约 50GB，目前大约 170GB。因此，为了使账本规模和核对所有交易的时间（这个时间也随着账本增大而变长）可控，加密货币对交易流量有硬性限制（图 5.4 中）。

一个思想实验可以表明加密货币作为日常支付手段的不足之处（图 5.4 右）。我们选取了若干个全国零售支付系统，为了处理目前这些系统的数字零售交易量，即使在乐观假设下，账本的规模也将在几天时间内迅速超过一个智能手机的存储容量，在几星期内超过个人电脑的存储容量，在几个月内超过服务器的存储容量。但问题不仅仅在于存储容量，更在于处理能力：只有超级计算机才能跟上新交易的验证，而与之相关的通信量会让互联网瘫痪停止，因为数百万用户以 TB 级的数量级交换文件。

可扩展性问题的另一个方面是更新账本会遇到网络堵塞问题。比如，对于基于区块链的加密货币，为限制在任何给定时间点添加到账本的交易数量，只能按照预先指定的时间间隔添加新的区块。一旦交易量大到新加区块触及协议允许数量的，系统就会拥堵，许多交易将进入队列。由于处理能力有上限，每当交易需求达到上限，交易费用会猛增（图 5.5）。有时交易会排队数小时之久，从而中断支付流程。这限制了加密货币在日常交易中的实用性，例如支付咖啡或会议费用，更不用说批发性的支付。[24]因此，使用加密货币的人越多，付款越麻烦。这违背了当今货币的关键属性：人们使用它越多，使用它的动机就越强。[25]

其次，加密货币的第二个关键问题是币值不稳定。这是由于缺乏一个中央发行人来负责维持币值稳定。运行良好的中央银行根据交易需求调节货币发行量，成功地稳定了主权货币的本土价值。央行进行此类操作的频率很高，尤其是在市场紧张时期，在正常时期也会高频操作。

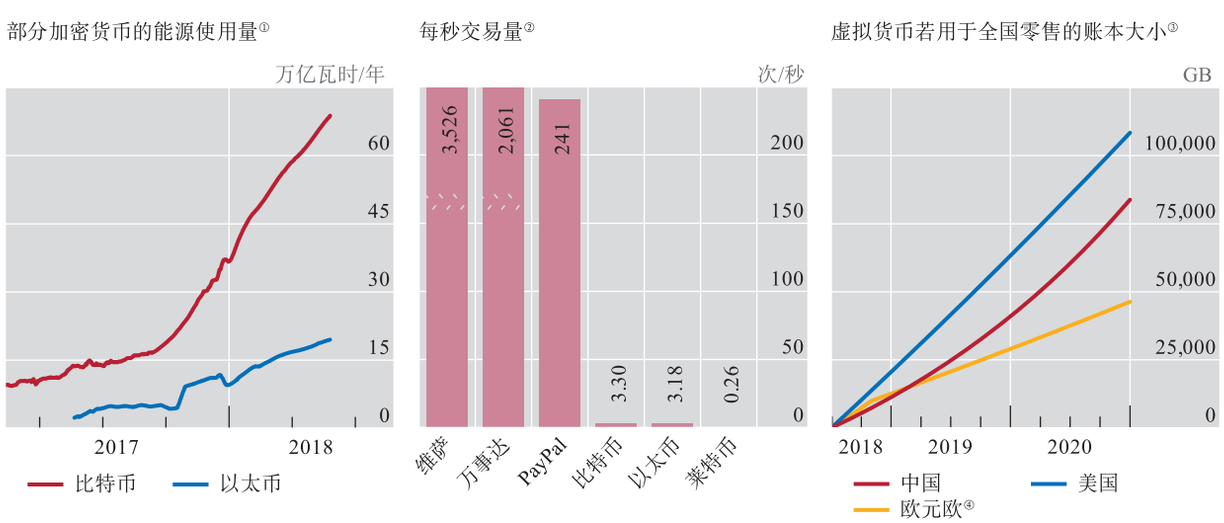

图 5.4　能源消耗和可扩张性问题

①估计值。②2017 年数据。③图中所示的假设的区块链/账本大小计算中，假设从 2018 年 7 月 1 日开始，中国、美国或欧元区的所有非现金零售交易都通过加密货币处理。计算基于 CPMI（2017）中的非现金交易数据，并假设每次交易向账本增加 250 字节。④比利时、法国、德国、意大利和荷兰。

资料来源：Committee on Payments and Market Infrastructures, Statistics on payment, clearing and settlement systems in the CPMI countries, December 2017; www. bitinfocharts. com; Digiconomist; Mastercard; PayPal; Visa; BIS calculations.

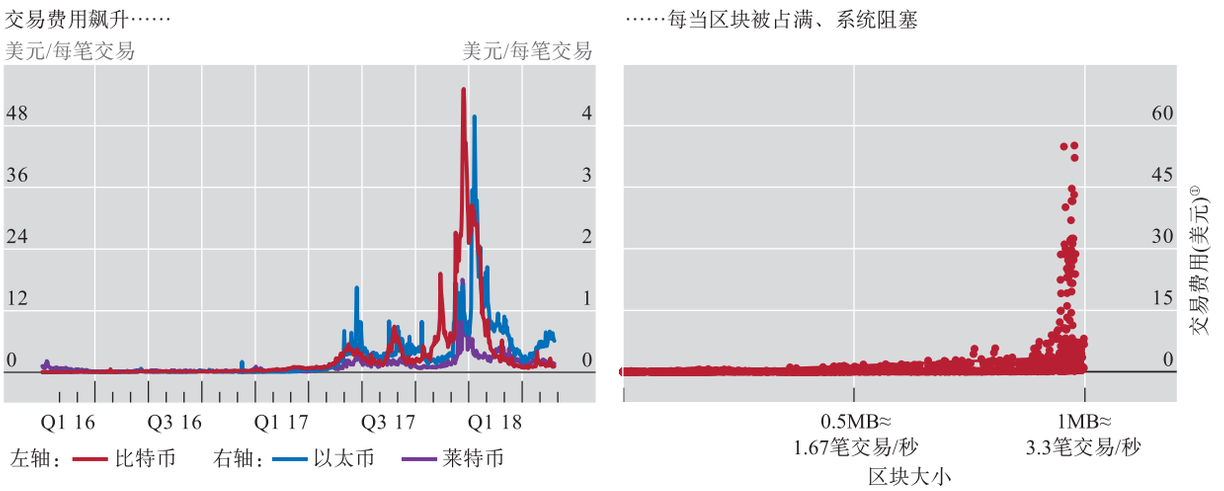

图 5.5　历史交易费用及其与交易量的关系

①2010 年 8 月 1 日至 2018 年 5 月 25 日，日均支付给矿工的交易费用。

资料来源：www. bitinfocharts. com；BIS 计算 .

这与加密货币形成了鲜明对比，对加密货币价值产生一定的信心需要协议预先确定供应量，但这阻碍了弹性供应。因此，需求端的任何波动都会传导到币值上。这意味着加密货币的币值极不稳定（图 5.6 左侧）。这一内在不稳定性很难被更好的协议或者金融工程所克服，如 Dai 加密货币的例子所示，它被设计为 1:1 锚定美元，但在 2017 年末发行仅数周后就跌到了 0.72 美元的低点。其他被设计为稳定币值的加密货币也都波动剧烈（图 5.6 中心）。

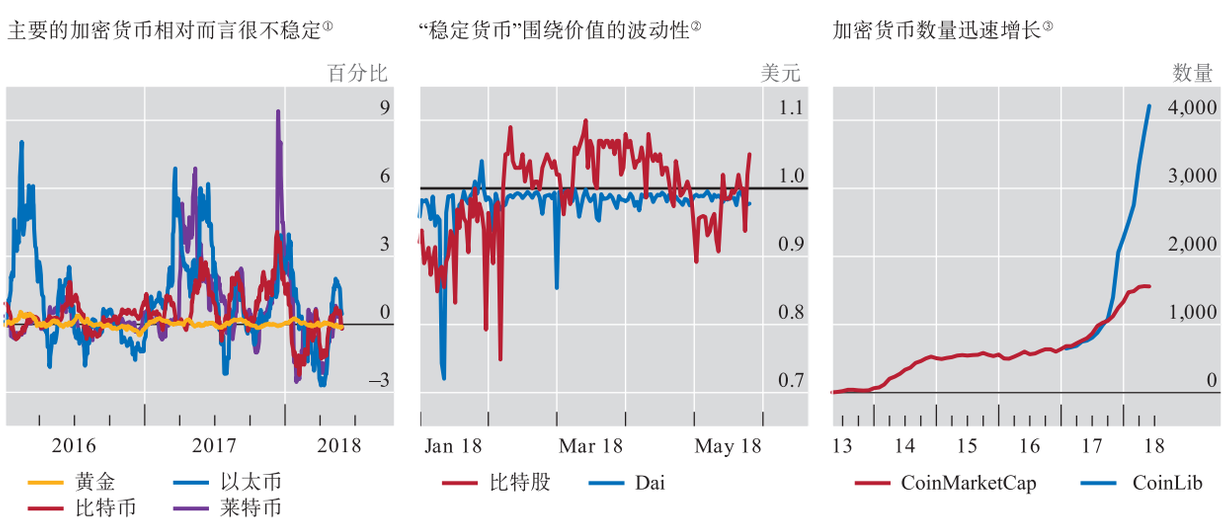

图 5.6　选取的加密货币的波动性，以及加密货币的数量

①每日收益的 30 天移动平均值。②每日价格最小值。③基于两个不同提供者的月度快照。CoinMarketCap 仅包括 24 小时交易量在 10 万美元以上的加密货币；CoinLib 并不对此分类。

资料来源：www. bitinfocharts. com；www. coinlib. io；www. coinmarketcap. com；Datastream.

这个结果并不是巧合。为保持支付手段的供应符合交易需求，需要一个中心化的机构——通常是可以扩大或缩小资产负债表的中央银行。当局有时需要愿意与市场进行交易，即使这意味着将风险纳入其资产负债表并吸收损失。在一个去中心化的加密货币用户网络中，没有中央代理人承担稳定货币价值的义务或动力：每当对加密货币的需求下降时，其价格也会下降。

另一个影响估值不稳定的因素来自于新加密货币的发行速度——所有这些加密货币都非常类似且相互可替代。在撰写本书时，已有数千种加密货币存在，这种扩增速度使我们难以估算（图 5.6 右）。回顾过去的私人银行业务的经验，这种自由发行新货币的结果很难带来稳定性。

最后一个问题涉及加密货币信任的基础脆弱。这涉及个人支付的完结性存在不确定性，以及涉及对单个加密货币价值的信任。

在主流支付系统中，一旦个人支付经由国家支付系统并最终通过中央银行账本进行支付，它就不能撤销。相比之下，无许可的加密货币不能保证个人支付的完结性。其中一个原因是，虽然用户可以验证账本中是否包含特定交易，但不知道他们可能存在竞争对手的账本版本。这可能导致交易反转，比如当两名矿工几乎同时更新账本时。由于两种更新只有一种可以最终生存，因此在哪个账本版本中支付得以完结则是个概率性事件。

由于加密货币可以被控制大量计算能力的矿工操纵，许多加密货币的采矿活动高度集中，所以加剧了付款完结性的缺失（图 5.7 左）。人们不能分辨是否正在进行战略攻击，因为攻击者只有在确定成功后才会显示（伪造的）账本。这意味着完结性将永远不确定。对于加密货币，账本的每次更新都会附带一份攻击者必须复制的额外工作量证明。即使支付完结的可能性随着后续账本更新的数量而增加，但从未达到 100%。[29]

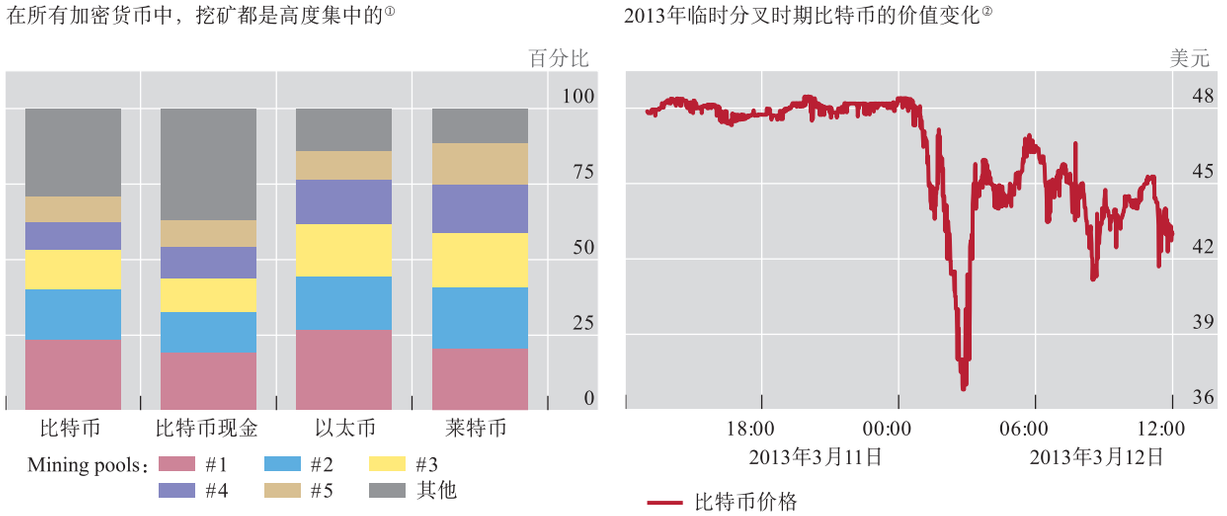

图 5.7　挖矿集中度以及在临时分叉时期比特币的价值变化

①截至 2018 年 5 月 28 日，最大挖矿池的数据。②在 2013 年 3 月 11 – 12 日比特币分叉期间，比特币价格的动态变化。

资料来源：www. btc. com；www. cash. coin. dance；CoinDesk；www. etherchain. org；www. litecoinpool. org.

不仅个人支付的信任不确定，由于存在“分叉”，每种加密货币的信任基础也很脆弱。“分叉”的过程，就是加密货币持有者的一个子集协调使用新版本的账本和协议，而另一些则坚持原来的账本和协议的过程。这样一来，一个加密货币可以分成两个用户子网。虽然最近有许多例子，但 2013 年 3 月 11 日发生的一件事值得注意，因为这与通过去中心化的手段实现信任的想法相违背，这个“分叉”是通过矿工的中心化协调而取消的。在那一天，错误的软件更新导致传统协议的比特币网络挖矿的一部分与使用更新的协议的另一部分挖矿之间不兼容。几个小时后，两个独立的区块链逐渐壮大；当这个分叉的消息传播开来，比特币的价格几乎下跌了 1/3（图 5. 7 右）。最终通过协调一致的努力使分叉得以反转，矿工们暂时脱离协议，无视最长的链条。但是许多交易在用户认为他们完结的几个小时后就消失了。这一事件显示了加密货币可以轻易分裂，并导致重大的估值损失。

这种情节背后的一个更令人担忧的方面是分叉可能仅仅是症状之一，症状背后反映的是加密货币的基本缺陷：更新账本所涉及的去中心化共识的脆弱性，并且与之相关的加密货币的基础信任。理论分析表明（专栏 5. A），关于如何更新账本的协调可能会随时崩溃，进而导致价值的完全丧失。

总体而言，去中心化的加密货币存在一系列缺点。主要的低效率来自于极端的去中心化程度：在这种背景下创造所需的信任浪费了大量的计算能力，交易账本的分散存储效率低下，去中心化共识脆弱。其中一些问题可能由新协议和其他进展[27]来解决，但另一些问题似乎与这种去中心化系统的脆弱性和有限的可扩展性有内在联系。最终，这表明在国家层面缺乏适当的体制安排是其根本缺陷。

超越泡沫：利用分布式账本技术（DLT）

虽然加密货币并不发挥货币功能，但其他领域的潜在技术可能会有所应用。一个值得注意的例子是小额跨境支付服务。更笼统地说，在一些去中心化的好处超过维护多份账本的较高运营成本的情况下，DLT 技术比主流的中心化技术解决方案更有效。

可以肯定的是，这种支付解决方案与加密货币在本质上存在差异。最近一个非营利性的例子是世界粮食计划署基于区块链的 Building Blocks 系统，该系统为在约旦的叙利亚难民的粮食援助付款提供支付支持。Building Block 中的账户单位和最终支付方式是主权货币，因此它是一个“密码支付”系统，但不是加密货币。它也受到世界粮食计划署的中央控制，其理由比较充分，即基于无需许可以太坊协议的初步实验会导致交易缓慢且成本高昂。随后系统重新设计为在以太坊协议的有许可版本上运行。随着这一变化，与银行的替代方案相比，交易成本降低了约 98%。[28]

对于小额跨境支付来说，有许可的加密支付系统也很有用，这对那些居住在海外的劳动力比例较大的国家尤为重要。全球汇款流量总计每年逾 5400 亿美元（图 5. 8 左图和中图）。目前，国际支付形式涉及多个中介机构，导致成本高昂

专栏 5. A　分叉以及区块链去中心化共识的不稳定性

分叉导致了加密货币数量的爆炸性增长（图 5. 6 右）。例如，仅 2018 年 1 月份，就有 Bitcoin ALL、Bitcoin Cash Plus、Bitcoin Smart、Bitcoin Interest、Quantum Bitcoin、BitcoinLite、Bitcoin Ore、Bitcoin Private、Bitcoin Atom 和 Bitcoin Pizza 经历了分叉。有多种不同的方式可以产生这种分叉，有些是永久性的，有些是暂时性的。一个例子被称为“硬分叉”（图 5. A）。如果加密货币的某些矿工协调将协议更改为与旧协议不兼容的一组新规则，就会出现这种情况。这种变化可能涉及协议的许多方面，例如允许的最大块大小、块可以添加到区块链的频率或更新区块链所需的工作量证明的更改。升级到新规则的矿工从旧区块链开始，但随后添加的区块无法被未升级的矿工所识别。未升级的矿工继续按照旧规则建立在现有区块链上。这样，两个独立的区块链就会各自增长，每个区块链都有自己的交易历史。

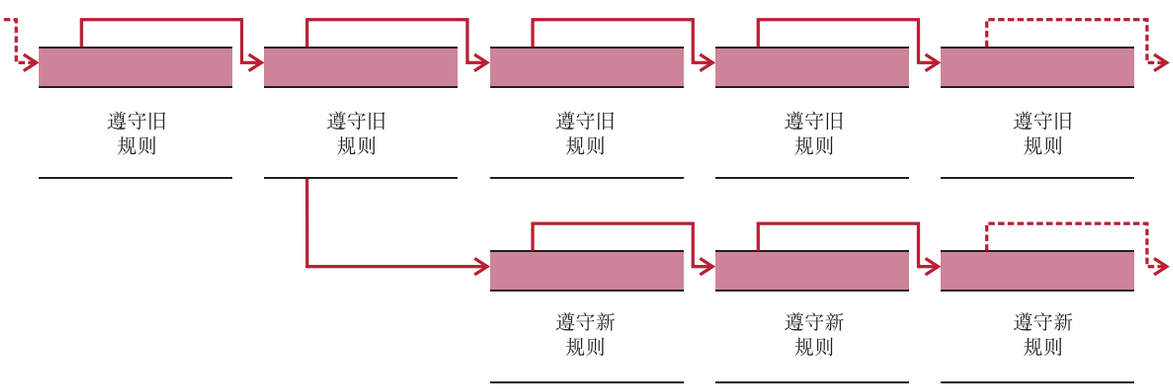

图 5. A　硬分叉

资料来源：BIS。

经常发生的分叉事件可能是一个固有问题的征兆，它与加密货币分散的矿工网络形成共识的方式有关。潜在的经济问题是这种去中心化的共识并不是唯一的。遵循最长链条的规则激励矿工遵循大多数算例，但它并不能唯一地确定多数人自己的路径。例如，如果矿工认为账本的最后一次更新将被矿工网络的其余部分忽略，那么对矿工而言，最好也忽略最后一次更新。而如果大多数矿工协调忽略更新，这确实成为了一种新的均衡。通过这种方式，就可以产生随机均衡——事实上经常出现这种情况，正如分叉以及比特币中的“侄子区块”、以太坊中的“叔叔区块”那样。关于去中心化更新区块链稳健性的其他问题涉及矿工的战略性分叉动机，只要不同矿工最后添加的区块包含高交易费用，可通过分叉排除有问题的区块[①]

①关于对更新区块链独特性的分析，参见 B Biais, C Bisieère, M Bouvard and C Casamatta, “The blockchain folk theorem”, TSE Working Papers, no 17—817, 2017。关于对创造分叉的战略性动机，参见 M Carlsten, H Kalodner, S M Weinberg and A Narayanan, “On the instability of Bitcoin without the block reward”, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security。

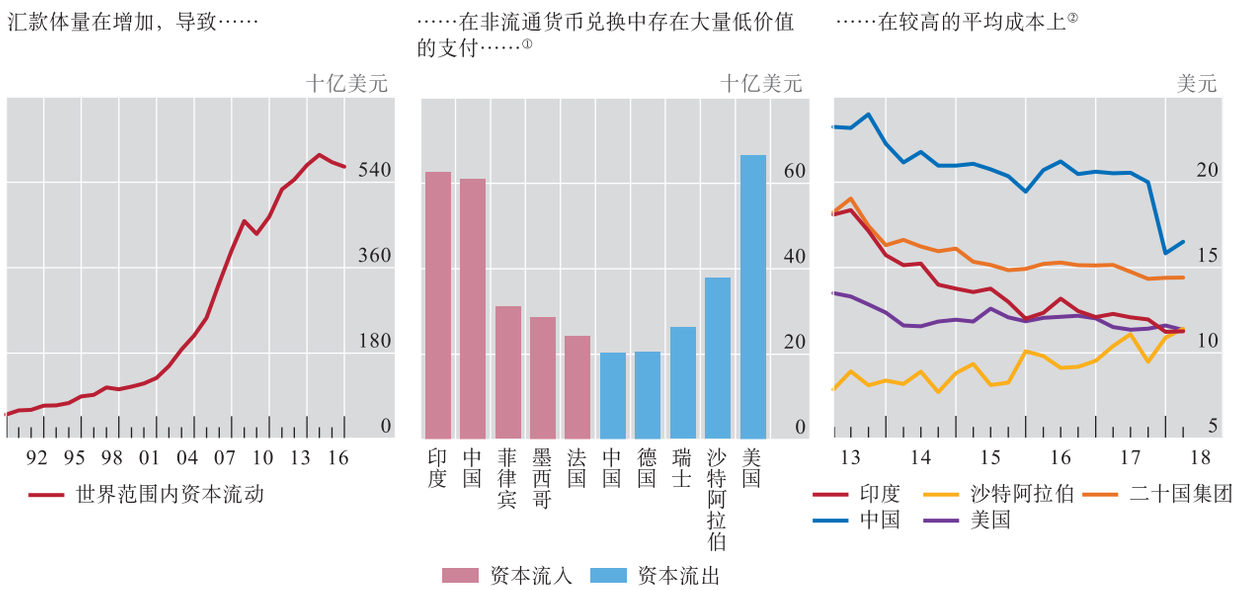

图 5.8　汇款体量和成本的一些指标

①2016 年数据。②世界范围内所有汇款服务提供商发送 200 美元汇款的平均总成本。对中国和印度，数据为接收国家的平均总成本；对二十国集团、沙特阿拉伯及美国，为发送国家的平均总成本。

资料来源：世界银行，*Remittance Prices Worldwide*，remittanceprices. worldbank. org；世界银行；国际清算银行计算。

（图 5. 8 右）。尽管如此，虽然加密支付系统是解决这些需求的一种选择，但其他技术也正在考虑之中，哪一个最有效仍待考察。

更重要的应用可能会将加密支付与复杂的自执行代码和数据许可系统结合起来。一些去中心化的加密货币协议（如以太坊）已经允许智能合约自动执行衍生工具的支付流程。目前，这些产品的功效受限于流动性低和无需许可加密货币的内在低效率。但基础技术可以通过以主权货币为后盾的有许可协议的注册交易所来采用，从而简化结算执行。该技术的附加价值可能来源于简化与复杂金融交易有关的行政流程，如贸易融资（专栏 5. B）。然而，至关重要的是，这些应用程序都不需要使用或产生加密货币。

政策影响

加密货币和相关技术的兴起带来了一些政策问题。当局正在寻找方法来确保市场和支付系统的完整性，以保护消费者和投资者，并维护整体金融稳定。打击非法使用资金是一个重要挑战。同时，当局希望保留长期的创新激励措施，特别是保持“相同风险，相同法规”的原则。[29]这些实质上是常规目标，但加密货币带来了新挑战并可能要求使用新工具和方法。一个相关问题是央行是否应该发行自己的央行数字货币（CBDC）。

专栏 5. B　贸易融资中的分布式账本技术

世界贸易组织估计，全球贸易的 80%—90% 依赖贸易融资。当出口商和进口商同意进行交易时，由于进口商有收到货物后不付款的风险，出口商通常更倾向于进口商先付款，而进口商更愿意通过在开始付款之前要求提供货物已经装运的文件来降低自己的风险。

银行和其他金融机构提供的贸易融资旨在弥补这一缺口。最常见的情况是，进口国本国的一家银行在收到货物文件（如提单）后向出口商发出保证付款的信用证。反过来，出口国的银行可能会根据这一抵押向出口商提供信贷，并从进口商的银行收取付款以完成交易。

在目前的形式下（图 5. B 左），贸易融资繁琐、复杂且成本高昂。它涉及出口商，进口商，各自的银行、在每个检查点对货物进行实物检查的代理商、海关机构、公共出口信贷机构以及货运保险公司之间的多次文件交换。该过程通常涉及基于文本文件的管理。DLT 可以简化潜在合同的执行（图 5. B 右图）。例如，智能合约可能会在账本中添加有效提货单时自动向出口商发放付款。而更好地获得有关哪批货物已经获得融资的信息还可以降低出口商多次从同一批货物中获得不同银行款项的风险。

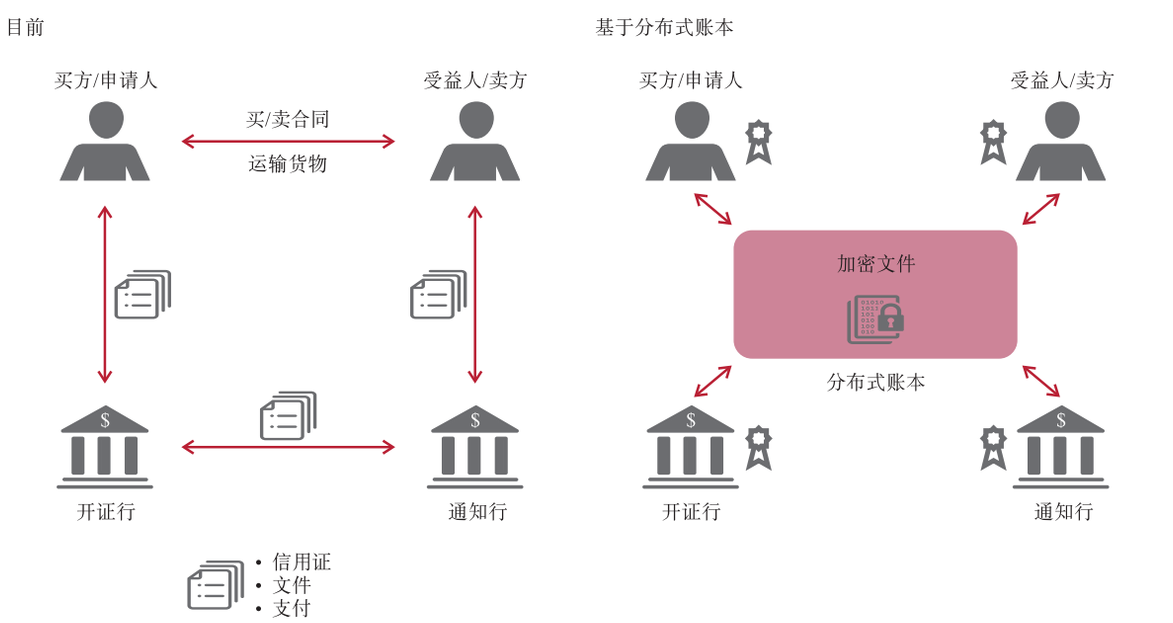

图 5. B　贸易融资如何在分布式账本中进行

资料来源：采用 www. virtusapolaris. com。

加密货币带来的监管挑战

第一个关键的监管挑战是反洗钱（AML）和反恐融资（CFT）。问题在于加密货币的崛起是否以及在多大程度上允许回避一些反洗钱/反恐融资措施（如“知道你的顾客”标准）。由于加密货币是匿名的，因此很难量化它们在多大程度上会被用于逃避资本控制或税收，或者更普遍地参与非法交易。但比特币对关闭丝绸之路——一个主要的毒品市场——的强烈市场反应表明，加密货币需求的不

可忽视的一部分来自非法活动（图 5.9 左）。[30]

第二个挑战包括证券规则和其他确保消费者和投资者保护的条例。数字盗窃是一个常见的问题。考虑到分布式账本的大小、不便以及高交易成本，大多数用户通过诸如“加密钱包”提供商或“加密交易所”之类的第三方访问他们的加密货币。具有讽刺意味的是，与比特币和其他加密货币的最初承诺形成鲜明对比，许多因不信任银行和政府而使用加密货币的用户却依靠着不受监管的中介机构。其中一些（如 MtGox 或 Bitfinex）被证明存在欺诈行为或遭受过黑客攻击。[31]

欺诈问题也困扰着首次代币发行（ICO）。ICO 涉及向公众出售一系列初始的加密货币代币，而收益有时会授予创业公司的参与权。尽管当局发出警告，投资者仍纷纷涌向 ICO，即使它们经常与提供最少且未经审计的信息的不透明商业项目相关联。这些项目中有很多都是欺诈性的庞氏骗局（图 5.9 右）。

第三个更长期的挑战涉及金融体系的稳定性。关于加密货币和相关自行执行的金融产品的广泛使用是否会导致新的金融脆弱性和系统性风险，依然有待观察。对发展情况进行密切监测依然很有必要。而且，鉴于其新颖的风险特征，这些技术要求提高监管当局的能力。在某些情况下，例如执行大额高量的付款，可能需要扩大监管边界来包括使用新技术的实体，从而避免系统性风险的积聚。

全球监管当局已达成广泛共识，认为有必要加强或通过制定新的监管措施，对加密货币和相关加密资产进行监管与监测。特别是二十国集团财长和央行行长最近的公报强调了消费者和投资者保护、市场完整性、逃税和反洗钱/反恐融资等问题，并呼吁国际标准制定机构持续监督。公报还呼吁金融行动特别工作组推动适用全球的实施标准。[32]

但是，加强标准的设计和有效实施具有挑战性。法律和监管的定义并不总是

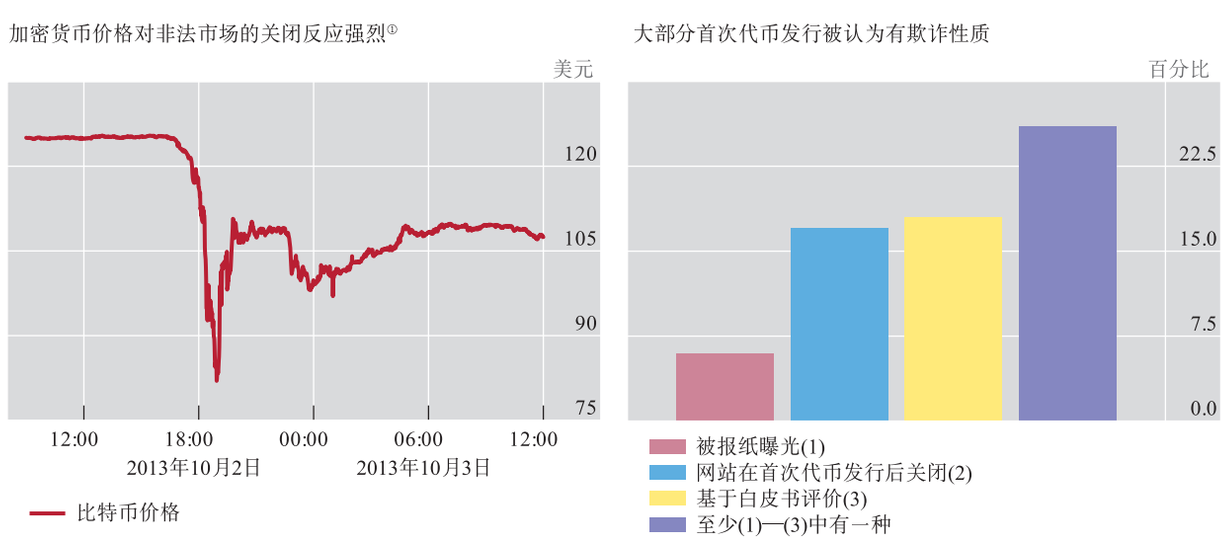

图 5.9　非法市场的关闭以及首次代币发行的合法性

①2013 年丝路市场关闭前后的比特币价格。

资料来源：C Catalini，J Boslego and K Zhang，“Technological opportunity，bubbles and innovation：the dynamics of initial coin offerings”，*MIT* 工作论文，即将发表；CoinDesk.

与新的现实相一致。这些技术用于多种经济活动，在许多情况下，这些活动受不同的监督机构监管。例如，科技公司目前正在使用 ICO 为与加密货币无关的项目筹集资金。除了语义上的差别——拍卖数字货币而不是股票——这类 ICO 与既定交易所上市首次公开募股（IPO）没有区别，因此证券监管当局对其采用类似的监管政策是很自然的。但是一些 ICO 还有“效用代币”的功能，它们保证未来能够访问游戏和其他软件。这一特征不构成投资活动，而是要求有关机构适用消费者保护法。[33]

在操作上，主要的复杂因素是无需许可的加密货币不适合现有的框架。尤其是它们缺乏可以纳入监管边界的法律实体或人员。加密货币生存在他们自己的数字化、无国籍的领域，可以在很大程度上独立于现有的制度环境或其他基础设施。他们的合法居所——如果他们有一个——可能是离岸的，或无法清楚地确定。因此，它们只能被间接监管。

当局如何实施监管方法？有三个相关的考虑：

第一，加密货币和加密资产的兴起要求重新确定监管边界。监管边界需要适应一种新的情况，即划定跨境和跨监管当局的责任界限越来越模糊。[34]由于加密货币本质上是全球性的，因此只有在全球层面进行了协调的监管才有可能发挥效用。[35]

第二，可以解决加密货币与受监管金融实体的协同能力。只有受监管的交易所才能为基于 DLT 的金融产品提供必要的流动性，使之成为利基市场，而结算流最终需要转换为主权货币。因此，针对那些希望处理加密货币相关资产的受监管机构，可以调整它们的税收和资本处理原则。监管当局可以监控银行是否以及如何交付、接收加密货币作为抵押品。

第三，可以针对提供加密货币服务的机构进行监管。例如，为确保有效的反洗钱/反恐融资，监管可侧重于在何种情况下加密货币可兑换为主权货币。其他与支付服务有关的现行法律法规侧重于安全性、效率和使用合法性。这些原则也可以应用于加密货币基础设施提供商，如“加密钱包”。[36]为避免监管效果出现漏损，理想情况下，各国家或地区的监管应大体类似且应在落实监管措施时保持一致性。

央行是否应该发行数字货币（CBDC）？

一个涉及 CBDC 发行的中期政策问题是谁可以获得 CBDC。CBDC 的功能与现金非常相似：央行将在一开始发行 CBDC，但一旦发行，它将在银行，非金融公司和消费者之间流通，而无需中央银行的进一步参与。[37]这种 CBDC 可能会在私人部门参与者之间进行交换，双边使用分布式账本而不要求中央银行跟踪和调整余额。它将基于一个经过许可的分布式分类账（图 5. 2），由中央银行决定谁作为一个可信节点。

虽然通用 CBDC 与现有数字中央银行负债（商业银行准备金余额）之间的区别可能看起来是技术性的，但它对于金融体系的影响实际上是根本的。发给消费者和企业的通用 CBDC 可能会深刻影响三个核心中央银行业务领域：支付、金融稳定和货币政策。支付与市场基础设施委员会和市场委员会最近的一份联合报告

强调了潜在的考虑因素。[38]这篇报告指出，通用 CBDC 的优势和劣势取决于具体的设计特征。报告进一步指出，虽然尚未出现领先的竞争者，但这样的工具将带来巨大的金融脆弱性，且效益不太明显。

目前，央行正在密切关注技术，同时谨慎执行。一些人正在评估发行狭义的 CBDC 的利弊，这种 CBDC 限于金融机构之间的批发交易。这些不会对目前的双层货币体系提出挑战，而是打算提高现有安排的运作效率。然而，迄今为止，对这种批发 CBDC 进行的实验并未提供可立即发行的强有力的证据（专栏 5. C）。

专栏 5. C　批发性的央行数字货币

近几十年来，中央银行利用数字技术来提高支付以及更广泛的金融体系的效率和稳健性。数字技术使中央银行能够为实时全额结算（RTGS）系统节省流动资金。通过连续链接结算（CLS）将这些系统连接起来，全世界的商业银行每天都可以全天候结算数万亿美元的外汇。CLS 有助于消除赫斯特风险，即外汇交易中代理银行在向指定收款人支付等值外币之前发生财务问题的风险。之前这种风险已经构成重大的金融稳定风险。最近，更快的零售支付已遍布全球，各国央行正在积极推动促进这一趋势。

作为对新支付技术更广泛投资的一部分，央行也在试验批发性的 CBDC。CBDC 是传统准备金和结算账户的基于代币的版本。大额资金流转基于 DLT 的 CBDC 的情况取决于这些技术提高效率和降低运营和结算成本的潜力。收益可能很大，因为目前许多中央银行运营的批发支付系统都依赖过时和昂贵的维护技术。

实施批发 CBDC 面临两大挑战。首先，无需许可 DLT 的缺陷也适用于 CBDC，这意味着它们需要根据有许可的协议进行建模。其次，中央银行准备金的可兑换性进出分布式账本的设计选择需要谨慎实施，以维持日内流动性，同时尽量减少结算风险。

包括加拿大银行（Jasper 项目），欧洲中央银行，日本银行（Stella 项目）和新加坡金融管理局（Ubin 项目）在内的一些中央银行已经开展了基于 DLT 的 CBDC 批发 RTGS 系统的实验。在大多数情况下，中央银行选择了数字存款收据（DDR）方式，即央行在分布式账本上发行数字代币，由分离账户持有并可兑换为中央银行准备金。代币可以用于在分布式账本上进行银行间转账。

中央银行现在正在公布结果。在初始阶段，每项实验都大大成功地复制了现有的高价值支付系统。但是，结果并不明显优于现有的基础设施。[①]

①参见 M Bech and R Garratt，“Central bank cryptocurrencies”，BIS 季报，2019 年 9 月，第 55 – 70 页；and Committee on Payments and Market Infrastructures and Markets Committee，Central bank digital currencies，2018 年 3 月。

本章注释

①该主题下的术语尚处于演变中，含义并不固定，在法律和监管上存在模糊之处。本章使用的术语“虚拟货币”并不代表对基于协议的底层系统的任何特定观点。虚拟货币通常具有主权货币的部分特征，但在不同的法律体系里，其法律地位亦有不同。本文以特定的虚拟货币

或虚拟资产为例，这些例子并未涵盖所有情况，亦不构成 BIS 及股东对任何虚拟货币及关联的公司、产品或服务的认可。

②该问题可参考 Carstens（2018a，c）。

③Graeber（2011）认为货币只是随着造币术的发明而普及，在公元前 600—500 年左右，货币在中国、印度和吕底亚几乎同时出现。与普遍观点相左的是，他还认为在使用货币之前，交易主要通过交易欠条方式，而不是以货易货。

④货币的这些功能在以往文献中已被广泛研究。一些重要的文献包括：Kiyotaki 和 Wright（1989）展示了货币作为交易媒介如何改善以物易物的交易方式。Kocherlakota（1996）认为，当完美的簿记和承诺兑现难以实现时，货币可以作为一种“记忆”方式改善上述情况。Samuelson（1958）采用世代交替模型研究，认为货币作为价值储存工具可以提高效率。Doepke 和 Schneider（2017）阐释了为何使用相同的记账单位可以改善结果，为什么政府发行的货币既是记账单位又是交易媒介。

⑤作为商品货币的物品包括非洲的贝壳、阿兹特克文明中的可可豆和北美殖民地的贝壳念珠。即使在这些情况下，信用关系与货币制度也是共存的。更详细的讨论可参见 Melitz（1974）。

⑥关于信用证的演变和它们在整个货币体系发展中所起的关键作用，特别是在贸易融资中起到的作用，可参见 De Roover（1948、1953）。了解具体分析和历史回顾可参见 Kindleberger（1984），了解引入共同责任的重要性可参见 Santarosa（2015）。

⑦ 以商品为支撑的法币，如金本位货币，它是另一种寻求平衡的尝试。此类货币在正常时期可以保持稳定性，同时在金融经济紧缩情况下限制了中央银行供应货币的弹性。极端情形下，此类特性往往被简单废弃，从而转向不可兑换。例如，在金本位制度下，人们将货币与黄金的可兑换性视为限制主权国家过度发行货币或贬值货币的能力。这种约束力之所以具有精确的可信度，正是因为商品在非货币用途领域仍具有市场价值，避免了主权国家过度使用其货币发行的垄断力量。进一步的讨论见 Giannini（2011）。

⑧关于近期的讨论，包括对货币贬值动机的分析，可参见 Schnabel 和 Shin（2018）。

⑨可参见 Van Dillen（1964）、Roberds 和 Velde（2014）和 Bindseil（2018）。有关与央行关系的讨论可参见 Ugolini（2017）、Bindseil（2018）、Schnabel 和 Shin（2018）。

⑩进一步地，中央银行通常有充当最后贷款人的灵活性。最近的 2008 年金融危机再次提醒人们，即便是在最发达的经济体中，当前货币安排的脆弱性和适应性是并存的。尽管此次危机暴露了现行监管框架的缺陷，但危机后对银行监管的重视程度增加，突显出机构安排可以不断演进以在两级体系框架下维持对货币的信任。

⑪参见 Carstens（2018a）。Giannini（2011）也强调了建立货币供应制度的重要性：“货币制度的演变似乎是经济和政治两个领域之间持续对话的结果，两者轮流创造货币创新……维护共同利益，防止派系为了自身利益滥用权力。”

⑫事实上，中央银行目前也监管支付系统并提供大量日内信贷，以确保系统，尤其是批发型支付系统运行准确无误。根据这些制度安排的具体情况，此类信贷也可延伸至隔夜或者更长期限。关于制度安排、业务程序和其他问题的进一步说明，可参见 BIS（1994）和 Borio（1997）。

⑬详细讨论参见 Bech 和 Garratt（2017）和 CPMI – MC（2018）。

⑭与纸币和其他实物货币很相似，每笔交易都基于支付对象（如相应的账本分录）来核实，这与其他基于账户持有人身份来核实的电子货币不同。因此加密货币是基于代币的数字货币。

⑮正在使用指定可信节点或预计使用该模式的“需许可”加密货币包括由 SAGA 基金会、Ripple 和 Utility Settlement 发行的货币。

⑯我们使用“Bitcoin”来表示加密货币用户及矿工的协议和网络，使用“bitcoin”来表示货币单位。

⑰例如以太坊、莱特币和域名币。

⑱Auer（2018）详细描述了比特币和其他基于区块链的加密货币的技术要素，例如数字签名、散列和块的加密链接。另见 Berentsen 和 Schär（2018）。

⑲从技术上讲，这是通过使用加密散列函数（如比特币中的 SHA－256）实现的。它们的结果不可预测，一个特定的结果因此只能通过试错生成。

⑳要使无许可加密货币在完全无信任的环境中运行，所有矿工和用户都需要存储整个账本的最新副本。但是，实际上许多用户信任他人提供的信息。有些用户只通过简化付款验证流程验证账本的摘要信息。而且，与比特币的基本理念向左的是，更多的用户只能通过第三方网站渠道连接他们的资金。在这种情况下，第三方主体自身就可控制其客户持有的加密货币。

㉑Nakamoto（2009），第 8 页。

㉒这是通过工作量证明的自我校准来实现的，这个过程不断提高运行所需的数学难度，直到所有矿工加总后的计算能力刚好达到以协议预设速度更新账本的状态。

㉓参见 Carstens（2018a）。

㉔虽然可以通过允许更大的区块来消除网络堵塞，但实际上这可能更具破坏性。一定程度的网络堵塞对于推动用户为交易付费至关重要，如果系统在低于上限的状态下运行，所有交易都会被处理，理性的用户将不会支付任何的交易费用，因此区块也是一种奖励。如果矿工无法通过更新交易来获得任何好处，虚拟货币的均衡将很可能会崩溃。参见 Hubermann et al（2017）和 Easley et al（2017），以及 Abadi 和 Brunnermeier（2018）。

㉕从技术角度来看，用户之间的交互是替代关系，而非互补关系。由此，加密货币是一种网络堵塞式而非协调式的博弈。

㉖如果在批发环境中使用加密货币，那么最终的概率本质可能会产生总体风险，其中资金往往会毫不拖延地进行再投资。事实上，这将创造一个全新的总体风险维度，因为风险将通过整个交易历史的非终结概率相互关联。

㉗提出的解决方案并不缺乏，但大多数尚未在实践中得到证明。一方面，未来的加密货币协议可以通过将其替换为“利益证明”来消除昂贵的工作量证明，其基本思想是通过持有加密货币而不是进行昂贵的计算工作来实现可信度。针对扩展问题的拟议解决方案包括 Lightning Network，它实质上将小型交易从主要区块链转移到单独的预先筹资的环境中。还有一些新的加密货币，例如 IOTA，旨在用更复杂的分类账和验证结构取代区块链。

㉘参见 Juskalian（2018）。

㉙参见 Carstens（2018a，b）。

㉚政府官员也不能免受加密货币的诱惑：两名美国政府特工被控盗窃在丝绸之路关闭期间被没收的比特币。

㉛例如，通过智能手机进行的大多数比特币支付很可能是通过第三方间接进行的，因为当前的区块链大小超过了大多数智能手机的存储容量。Reuters（2017）和 Moore and Christin（2013）列举了一些案件，其中第三方被证明是欺诈性的，或者已经成为黑客攻击的受害者。关于分析加密货币的非法使用，可参见 Fanusie and Robinson（2018）和 Foley et al（2018）。

㉜参见二十国集团财长和央行行长会议（2018）。

㉝Clayton（2017）从美国角度讨论 ICO 监管而不是 IPO，并指出“证券发行结构的变化并未改变提供证券时的基本要点，必须要遵从我们的证券法”。FINMA（2018）在瑞士制定了一个监管框架，根据所发行代币的最终使用情况对 ICO 进行分类：支付，资产或公用事业代币。

㉞从技术上讲，基于协议的加密货币运作所需要的只是至少一个国家允许进行加速。当局难以关闭 Napster 或 The Pirate Bay 等非法下载网站以及 BitTorrent 等下载协议，这突出了相关的

执法问题。

㉟金融行动特别工作组（2015）认为，根据各司法管辖区的职能和风险状况始终如一地处理类似产品和服务对于提高国际反洗钱标准的有效性至关重要。

㊱复杂之处是支付受到一系列具有不同目标的权威机构和法律的监管，例如支付系统监督，审慎监管，消费者保护和反洗钱/反恐融资。例如，美国的机构必须遵守“银行保密法”，“美国爱国者法案”和“外国资产管制办公室”等法规。另一个复杂因素与现有立法对新文书的适用性有关。例如，在欧盟，电子货币的法律定义包括要求余额应代表对发行人的索赔。由于加密货币不代表任何索赔，不能将其视为电子货币，因此默认情况下不受相关法律的约束。

㊲基于代币的 CBDC 有许多潜在的技术实现。它们可以基于分布式账本，具有与加密货币类似的特征，不同之处在于中央银行而不是协议本身可以控制已发行的金额并保证代币的价值。

㊳CPMI – MC（2018）。

参考文献

Abadi, J and M Brunnermeier (2018): "Blockchain economics", Princeton University, mimeo, May.

Auer, R (2018): "The mechanics of decentralised trust in Bitcoin and the blockchain", BIS Working Papers, forthcoming.

Bank for International Settlements (1994): 64th Annual Report, June.

Bech, M and R Garratt (2017): "Central bank cryptocurrencies", BIS Quarterly Review, September 2017, pp 55 – 70.

Berentsen, A and F Schär (2018): "A short introduction to the world of cryptocurrencies", Federal Reserve Bank of St Louis, Review, vol 100, no 1.

Bindseil, U (2018): "Pre – 1800 central bank operations and the origins of central banking", Mannheim University, mimeo.

Borio, C (1997): "The implementation of monetary policy in industrial countries: a survey", BIS Economic Papers, no 47, July.

Carstens, A (2018a): "Money in the digital age: what role for central banks?", lecture at the House of Finance, Goethe University, Frankfurt, 6 February.

——— (2018b): "Central banks and cryptocurrencies: guarding trust in a digital age", remarks at Brookings Institution, Washington DC, 17 April.

——— (2018c): "Technology is no substitute for trust", Börsen – Zeitung, 23 May.

Catalini, C, J Boslego and K Zhang (2018): "Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings", MIT Working Papers, forthcoming.

Clayton, J (2017): "Statement on cryptocurrencies and initial coin offerings", www. sec. gov/news/public – statement/statement – clayton – 2017 – 12 – 11, 11 December.

Committee on Payments and Market Infrastructures and Markets Committee (2018): Central bank digital currencies, March.

De Roover, R (1948): Money, banking and credit in mediaeval Bruges: Italian merchant – bankers, Lombards and money changers – a study in the origins of banking, Mediaeval Academy of America.

——— (1953): L'évolution de la lettre de change: XIVe – XVIIIe siècle, Armand Colin.

Doepke, M and M Schneider (2017): "Money as a unit of account", Econometrica, vol 85, no 5, pp 1537 – 74.

Easley, D, M O'Hara and S Basu (2017): "From mining to markets: The evolution of Bitcoin transaction fees", papers. ssrn. com/sol3/papers. cfm? abstract_id = 3055380.

Fanusie, Y and T Robinson (2018): "Bitcoin laundering: an analysis of illicit flows into digital currency services", Center on Sanctions & Illicit Finance memorandum, January.

Financial Action Task Force (2015): Guidance for a risk – based approach to virtual currencies, June.

Financial Market Supervisory Authority (FINMA) (2018): Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), 16 February.

Foley, S, J Karlsen and T Putniņš (2018): "Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?", dx. doi. org/10. 2139/ssrn. 3102645.

G20 Finance Ministers and Central Bank Governors (2018): Buenos Aires Summit communiqué, 19–20 March.

Giannini, C (2011): The age of central banks, Edward Elgar.

Graeber, D (2011): Debt: the frst 5,000 years, Melville House.

Huberman, G, J Leshno and C Moellemi (2017): "Monopoly without a monopolist: an economic analysis of the Bitcoin payment system", Columbia Business School Research Papers, no 17–92.

Juskalian, R (2018): "Inside the Jordan refugee camp that runs on blockchain", MIT Technology Review, online edition, 12 April.

Kindleberger, C (1984): A fnancial history of western Europe, Allen & Unwin.

Kiyotaki, N and R Wright (1989): "On money as a medium of exchange", Journal of Political Economy, vol 97, no 4, pp 927–54.

Kocherlakota, N (1996): "Money is memory", Journal of Economic Theory, vol 81, issue 2, pp 232–51.

Melitz, J (1974): Primitive and modern money: an interdisciplinary approach, Addison–Wesley.

Moore, T and N Christin (2013): "Beware the middleman: empirical analysis of Bitcoin–exchange risk", in A–R Sadeghi (ed), Lecture Notes in Computer Science, vol 7859.

Nakamoto, S (2009): "Bitcoin: a peer–to–peer electronic cash system", white paper.

Reuters (2017): "Cryptocurrency exchanges are increasingly roiled by hackings and chaos", 29 September.

Roberds, W and F Velde (2014): "Early public banks", Federal Reserve Bank of Chicago Working Papers, no 2014–03.

Samuelson, P (1958): "An exact consumption–loan model of interest with or without the social contrivance of money", Journal of Political Economy, vol 66, no 6, pp 467–82.

Santarosa, V (2015): "Financing long–distance trade: the joint liability rule and bills of exchange in eighteenth–century France", The Journal of Economic History, vol 75, no 3, pp 690–719.

Schnabel, I and H S Shin (2018): "Money and trust: lessons from the 1620s for money in the digital age", BIS Working Papers, no 698, February.

Ugolini, S (2017): The evolution of central banking: theory and history, Palgrave–Macmillan.

Van Dillen, J G (1964): History of the principal public banks, Frank Cass & Co.