免责声明：本文旨在传递更多市场信息，不构成任何投资建议。文章仅代表作者观点，不代表火星财经官方立场。

小编：记得关注哦

来源：国家金融与发展实验室

原文标题：| 数字货币：从经济到社会

文 | 程 炼 国家金融与发展实验室 学术委员会秘书长

数字货币在获得社会广泛关注的同时，也引发了大众媒体与主流学界的观点分歧。本文试图通过对于数字货币特征、运行逻辑和文化象征意义的概念性探讨来弥合不同视角之间的鸿沟。我们的基本观点是，数字货币的出现并没有构成对于现有主流货币理论“新”的实质性挑战，但它确实揭示了对于传统概念框架进行反思并拓展分析视角的必要性。我们应该将数字货币所折射出的各种冲突作为一条线索，来探索现代经济与社会运行的观念基础。

自2009年比特币创立以来，数字货币获得了IT与金融行业乃至社会的广泛关注，最近Facebook公布Libra加密货币计划以及一些中央银行正在考虑发行数字货币的传闻，更使得数字货币再次成为热点。数字货币的特殊性激起了社会各界的巨大争议与期待，许多人认为这种既没有政府信用也缺乏“内在价值”的货币能够得以产生，颠覆了传统货币观念和经济理论，还有人认为虚拟货币不仅仅是货币，更提供了一种可能改变社会治理形态的技术。

数字货币的兴起同样也引起主流经济学界的兴趣，催生了大量的学术研究，包括数字货币的技术原理、数字货币对于货币政策的影响、数字货币的金融与经济效应、数字货币对于法定货币的替代、数字货币的汇率动态与交易模式、数字货币的监管等等。不过值得注意的是，主流经济学界与大众媒体的关注点存在着明显的差异。例如，尽管在主流经济学期刊上有不少讨论“比特币是否是货币”的文献，但这些分析基本都没有脱离传统的货币理论范式，并且更关注数字货币相关属性的实证检验。

与大众媒体相比，主流经济学文献在数字货币的功能与影响方面似乎显得缺乏想象力，不过考虑到学术研究的严谨性，这应该是可以理解的。但学术界一直未就数字货币

对于现有
经济理论的冲击作
出正式的回应，仍然很容易引起大众
的疑惑。这其中有着两方面的原因
：一是主流货币理论范式确实具有很强的弹性与稳健性，许多对于其现实解释力的质疑是来自于对相关理论的无知或误解；二是尽管“经济学帝国主义”带来了经济研究领域的扩张，但是在主流经济学期刊，尤其是金融学期刊上，关于什么是“严肃”的研究课题仍然有着相对保守的默契，这也使得关于数字货币的许多争议落在学界的视野之外。

本文试图通过对于数字货币的概念性探讨来弥合主流经济学界与大众媒体观点之间的鸿沟。在这里我们将基于现代货币理论来解释数字货币的运行逻辑和经济效应，

我们的基本观点是，数字货币的出现并没有构成对于现有主流货币理论“新”的实质性挑战，但它确实揭示了对于传统概念框架进行反思并拓展分析视角的必要性。我们应该将数字货币所折射出的各种冲突作为一条线索，来探索现代经济与社会运行的观念基础。

—

货币的历史源流

在数字货币的支持者与
批评者之间争论的一个终极问题是：
“数字货币是不是货币？”
对于这一问题的解答，学术界有两条常见的路径：一条路径是首先确定作为货币内涵的一系列特征（“什么是货币？”），然后与此为标准将数字货币加以对照；另一条路径则更关注具体的货币职能而不是抽象的货币概念，于是相应的问题也就转换为了“在何种情境下，数字货币可以被看作（适用某种模型的）货币？”。显然，后一条路径的实践者对于数字货币要更为宽容，在他们的视角下，比特币等数字货币就类似于一条会跳舞的小狗：重要的并不是它跳得有多好，而是它居然能够跳起舞来。许多研究者也因此选择了这种实用主义的策略以回避恼人的概念之争。然而在本质上，这两条路径是一致的，第二条路径仅仅是通过对于货币属性的分割而暂时逃避了终极问题，一旦遇到现实中的复杂情况，它又会以“模型或方法适用性”的形式重新出现。

在遵循上述第一条路径的文献中，一种非常普遍的做法是回溯货币的历史起源，从

它的发端去寻找货币的本质属性。但是这种作法的困难在于，基于现有的人类学证据，关于货币的起源存在着相当多的争论，其中不乏极为激进的观点。与此同时，这种做法的一个逻辑陷阱在于，货币的初始形态并不一定代表着它的“本质”。我们可以用一个生物进化上的类比来说明这一点。现代生物的一些组织器官最初是由执行完全不同功能的组织演化而来的，例如鸟类的羽毛最初的功能是为了调节体温，后来才进化为飞行功能的承担者，但我们显然不能由此宣称，羽毛的“本质”职能是体温调节，或者说鸟类的飞行能力是体温调节功能的衍生品。

尽管存在着上面的困难，回顾历史仍然可以使我们通过检视那些不随着货币形式而改变的特征来确认支持其履行货币职能的核心要素。图1中高度简化的货币演化路径应该是当前货币史的共识。在货币出现之后，第一步的飞跃是从商品货币（Commodity Money）向符号货币（Token Money）的演化：一袋盐变成了邻居签写的一袋盐的借据，或者一两白银变成了钱庄发行的一两银票。最初的符号货币是有形的，多数情况下以纸张和贱金属的形式存在，并且可以向最初的发行者兑换为它们所代表的物资。此后，符号货币则沿着两条路径演化。一条路径是符号的抽象化，如持有的现金变成了银行账户上的数字；另一条路径是符号与其所代表的债权债务关系的脱钩，即货币不再能够兑现为信用抵押品，这也是大多数政府所走的道路。两条路径在不可兑现的无形符号货币处会合，成为了现代货币的长期形态。

最下方的两个模块则是互联网与IT技术为货币带来的改变。在账户和支付过程完全电子化之后，某些非银行运营的商业平台账户中的储值形式具有了超出这一平台商品范围的购买力，成为更一般意义上的交易媒介，这其中最为典型的例子就是M-Pesa和瑞波币（XRP）。这类非银行账户系统中的储值形式可以看作基于互联网的“传统”数字货币：它们由法定货币当局之外的机构发行，但是仍然基于中心化的发行方式，以传统银行或持照交易所为合作对象，并且通常具有保值机制。这类“传统”数字货币经常被作为非金融机构获得金融权力的重要渠道，但它们的运行仍然需要依托于现有的货币与金融体系。这种中心化体系内部的竞争看起来非常适用哈耶克的私人货币理论。

与这类“传统”数字货币相比，
比特币、莱特币（Litecoin）等“狭义”的数字货币或“虚拟货币”则是货币演进过程中更大的跳跃。
后者的特殊性并不仅仅体现在非中心化的发行方式或者匿名性方面，更为重要的是它们相对于既有金融体系（至少在理论上的）独立性。在理想状态下，即便所有的银行、金融机构乃至政府都完全消失，只要互联网还能够正常运作，比特币的拥有者就仍然可以使用它进行交易。这似乎是法定货币主导经济以来从未出现过的局面，比特币的出现对于现有金融秩序或观念的冲击也因此远远大于“传统”的数字货币。

图1 货币的历史演化路径

二

主流货币理论所能解释的和不能解释的

现在回到我们前面提出的问题：在货币历史演化过程中是哪些因素支持着不同形式的货币履行其职能，尤其是交换媒介职能。商品货币具有使用价值，即使它的使用价值对于每个人并不相等，但只要人们相信它对于大部分人，甚至只是某些人有足够的使用价值（或者用博弈论的术语更为严格地表述：“商品货币对于某些人具有使用价值”是公共知识），它作为交易媒介的可接受性就能得到支持。对于可兑换的符号货币而言，仅仅依托抵押品的使用价值是不够的，还需要信任。以一袋盐的借据为例，要愿意接受它作为交易媒介，你不仅需要知道盐对于人们生活的重要性，还需要相信写借据的人具备归还这袋盐的能力和意愿，以及相信这张借据是真实的。回溯历史，为了克服关于兑现能力和意愿的信任障碍，诞生了复杂的货币发行准备制度，而围绕着凭证真实性的信任问题则是货币防伪技术与伪造技术之间“道高一尺，魔高一丈”的博弈。到目前为止，一切都还符合米塞斯的“回溯定理”（Regression Theorem）：货币的可接受性可以追溯到其最初得以衍生出来的物品的价值，然而一旦货币形式进入了不可兑现的法定货币（Fiat Money）阶段，这条追溯的链条忽然中断了，被代之以模糊的“国家信用”。

考虑到法定非兑现货币的历史，比特币对于大众货币观念最大的冲击不应该来自于它缺乏“内在价值”（毕竟当今世界绝大多数法定非兑现货币都没有任何“内在价值”），而更应该来自于它缺乏公共权威的信用支持。不过，在人们惊讶于这一点之时，却常常忽略了一个同样重要的问题：为什么人们会愿意接受缺乏“内在价值”的法定非兑现货币。简单地强调“主权货币有国家信用作为支持”并不能作为满意的回答，它很容易遭受后续一系列的追问：什么是国家信用？如果政府根本不兑现货币，那么国家信用体现在哪里？对此，货币国定论（Chartalism）给出的一种解释是法定货币的纳税功能。这种税收驱动货币的观点使得米塞斯的回溯链条得以继续（尽管货币国定论者显然不会对印证奥地利学派的理论感兴趣）：纳税的能力赋予了法定货币最初的“使用价值”。然而，这种直截了当的逻辑会面临另一个问题：税收价值只占经济体中流通货币总量的很小一部分，这就意味着大部分的货币价值得不到前面回溯链条的支持。除了税收驱动货币论之外，那些诉诸政府权威或强制力的解释则更缺乏说服力。除了缺乏微观行为基础之外，在历史上有过太多政府强之而民不为的例子，即使在目前的现实生活中，消费者抱怨某些商家不接受纸钞现金的新闻屡见不鲜，这也从侧面反映了政府在货币方面强制力的有限性。

与许多人的印象不同，在主流货币理论中，缺乏“内在价值”的货币的可接受性并不是一个问题。

Tirole等人的“理性泡沫”模型证明，即使所有的行为人都是完全理性的，在无限期界的代际交叠模型中，没有任何“内在价值”的金融资产也可能成为价值储存的手段，而非兑现货币就是一个典型的例子。类似地，在Kiyotaki和Wright基于搜寻-匹配框架的货币模型中，均衡状态下用作交易媒介的货币也可以没有“内在价值”。虽然这些看似反直觉的模型对于大众而言有点难以理解，但是它们背后的逻辑则不难用浅显的语言阐述清楚。设想投资者购买某种无“内在价值”金融产品然后在下一期卖给他人的资产交易，其中每次交易都会给买卖双方带来一定收益，但是其数量远远低于金融产品的面值。如果这一交易的期限是给定的，也即会在未来的确定时刻让所有投资者都清仓离场，那么对于理性的投资者，没有人会参与这种“击鼓传花”的游戏。因为人们知道，在游戏结束时金融产品的价值为零，因此那时没有人会愿意持有它。考虑到没人接最后一棒，在游戏结束的前一期人们就不会愿意持有这种产品，以此类推，在游戏一开始就不会有任何人进场，即使这种金融产品的存在是对大家有益的。实际上，这也是博弈论基本定理——“有限次重复博弈的均衡是单次博弈均衡的有限次重复”——的一个具体情境，即“囚徒困境”下的合作无法在时间有限的博弈中实现。

继续考虑上面的例子，只是这时我们假定不存在强制清仓离场的时间。游戏规则的这一改变取消了人们对于最后一位接棒者是否存在的顾虑，于是只要相信有很多人愿意参与这个游戏，大家就会放心地以远高于“内在价值”的价格购买金融产品，无限期地将游戏进行下去，并使得所有参与者都因此受益。在数学上，这一局面的神奇反转来自于“无限”概念的特殊属性，它使类似于“希尔伯特旅馆悖论（The Hotel Hilbert Paradox）”这样的佯谬得以存在，也为人类的经济合作提供了更大的空间。在无限期界的情境下，金融产品能够被潜在的买家接受并不是由于它的“内在价值”，而仅仅是由于买家对于未来其他潜在买家同样会接受这种金融产品的预期，也就是货币可接受性上的“网络效应（Network Effect）”。当然，为了让这个故事贴合于现实，我们还需要在正式的模型中加入更多的条件，如金融资产面值的上涨速率、人们的耐心程度（贴现率）、潜在交易者相遇的概率等等，但这些并不会影响模型的基本结论：
用于价值储存与交易媒介功能的货币不需要具有“内在价值”。

然而到目前为止，故事还没有结束。仔细审视上面例子的第二部分就会发现，它只描述了一个美好的结局，即货币被所有人接受，但是即使在无限期界情境中，也依然可能复制有限期界情境中的局面，就是所有人都不愿意持有金融资产，也不相信其他人会接受它。无论哪种局面出现，都会被网络效应锁定在当时的状态下。换句话说，对于任何局面的预期都是自我实现（Self-fulfilling）的：当所有人都不相信所有人的时候，他们的判断无疑是正确的，反之亦然。这也是绝大部分类似结构的货币模型所面临的困境，这类模型中通常存在着福利状态不同的多种均衡（不仅是有无货币的状况，还包括多种货币之间的选择），但是没有人能够预测哪一种均衡能够最终得以实现，因而它们最多只是给出了数字货币存在的可能性，却并没有说

明为什么数字货币会在一个已经被法定货币主导的世界里出现。

虽然专门针对上述货币跃迁问题的主流货币模型尚不多见，走出被网络效应锁定困境的机制却已经在经济学理
论中得到了相当多的讨论。
其中之一是引入外部的协调
者，最为典型的就是政府。
需要注意的是，虽然这种解决思路看起来和货币国定论有些相似，两者却存在本质的不同。在协调者框架下，政府的作用仅仅是在选择不同货币时预期的统一，它并不持续干预人们的行为，也不是货币信用的来源。但尽管如此，考虑到世界各国政府对于比特币等不算太友好的态度，这类外部协调机制显然很难解释现实。另一种不依赖于外部力量的均衡跃迁机制则诉诸理性和时间：当选择不同福利水平体系的决定并非由所有人同时做出，而是以序贯决策的方式进行，那么理性行为人会自发地逐个进入社会福利更高的体系。这一机制的关键仍然在于对序贯理性行为的逆向推演：可以想见，当经济中几乎所有人都已经处于高福利体系中，只剩最后一个人面临选择时，他会毫不犹豫地跟随前人的选择；基于这样的考虑，倒数第二个人也会跟随前人；由此递推，只要第一个人选择了高福利体系，之后的所有人都会跟随他做出这一明智的决定，网络效应锁定的困境因此不攻自破。但这种巧妙的机制也有它的问题，就是当每个人的行动次序并非事先决定而需要自己来选择时，谁来走出第一步又构成了新的囚徒困境，需要依靠引入行为人的异质性等新的假设来加以解决。

在极其粗略地回顾了相关领域的研究之
后，
我
们的
总体印象
是数字货币存在的
合理性并没有对主流货币理论构成特
殊的挑战
，虽然这些理论机制的实际效果颇为可疑，而在诸如存在多种货币的情境下货币竞争结果尤其是动态分析上的力不从心，则是主流货币理论在数字货币出现许久之前一直存在的困扰。不过在一切似乎即将盖棺定论的时候，细心的读者可能会发现一个问题：我们前面的讨论里自始至终将数字货币总结为一种非政府发行的无“内在价值”货币，以使得它能够适用现有的分析框架（这种典型的主流经济学抽象方式也是它最受诟病的一点，即通过巧妙的假设和严格的数学结构回避了真正的问题）。但是这一简化能否概括数字货币的“本质”，如果不能，那么数字货币的特殊性到底是什么？

三

基于互联网的“复古”货币

为了
回答上面
的问题，我们需要
回顾一下符号货币出现之后面对的两
个困扰：
票据发行者的偿付意愿和票据本身的
真实性。
在基于电子支付系统的法定货币时代，这两个困扰则分别转化为对政府（中央银行）和那些持有储蓄者和投资者账户的金融机构的信任问题。一旦类似于全球金融危机这样的冲击使得这种信任岌岌可危时，就会有人给出替代方案，例如回到金本位、发行世界货币等等。数字货币无疑是这些替代方案中最为激进的，因为它完全地另起炉灶，没有给政府和金融机构留任何位置。

虽然比特币等数字货币的技术看起来极为深奥，但其实它的经济机理并不复杂，而且早已经在人类社会出现过。有人注意到，非中心化数字货币的运行机制与雅浦岛（Yap island）的石头货币（Rai Stones）极为相似。这些磨盘状石头货币通常放置在公屋或者道路的旁边，作为其主人财富的象征。在石头货币的使用上极为特殊的一点是，即使这些石头已经由于某笔交易而转换了所有权，它的位置经常也不会变动，而是依靠大家的认可来确定新主人的所有权，这和现代主流货币制度截然不同。虽然在日常生活中，我们经常依靠“公众见证”的方式来确定我们对于放置在公共场所物品的所有权，但是对于货币而言，这种做法却非常罕见，原因至少有三个：第一，货币交易涉及琐碎的数目且极为频繁，要求旁观者精确地记录这些数字会构成巨大的负担；第二，货币交易的场景非常多样化，很难为每次交易找到一批可以事后召集作证的旁观者；第三，很多交易涉及隐私，当事人不愿意将其暴露在外人面前。因此，类似石头货币那样的制度只有在人口规模小且经济结构非常简单的熟人社会才有可能行得通。

仔细观察比特币的运行机制，很容易看到两者的相似之处。比特币交易实际上是对于作为资产标志的比特币的所有权加密标签的转换，它并不涉及对于比特币自身其他属性的操作。因此，
比特币既不同于商品货币或有形符号货币
（交易不涉及货币物理形态的交接），
也不同于银行账户系统
（账户上数字是抽象的财富标记，会随着会计操作增减甚至消失，而比特币一旦被创造出来之后就会在系统中永远存在）。因此从某种角度来看，比特币等数字货币

更倾向于是建立在互联网上的一个“复古”货币系统，用现代技术重现了“原始”的交易制度。与此同时，为了克服前面提及的“公众见证”障碍，比特币引入区块链对每笔交易做精确的记录，通过采矿收益和交易费为鉴证者提供激励，通过交易者身份的匿名化来保护其隐私，让这套系统得以流畅运转。

通过将账簿复制保存在每一个参与者的计算机里，比特币等数字货币在绕开传统金融体系的同时实现了流动性创造与转移的去中心化，这是数字货币的支持者最为推崇的一个特性。但“非中心化”本身在货币史中并不是一个新概念，尤其在将货币创造与支付分开讨论时则更是如此。在商品货币时代，无论货币创造或支付都是非中心化的：
货币可以由任
何人创造，交易也可以在任
何地方仅由买卖双方完成。
进入到最初的法定货币时代，货币创造变得中心化，而支付仍然是非中心化的。支付过程的中心化是随着银行结算体系的建立而逐渐扩张的，电子支付的兴起则更加速了这一趋势，其中的部分原因来自防范分散化电子支付中的伪造和“双重支付”问题极为困难，只能通过第三方鉴证来加以控制。但即便如此，现钞的存在依然为非中心化的支付提供了相当大的空间。具有讽刺意味的是，为货币支付中心化送去“临门一脚”的恰恰是以“非中心化”为标榜的互联网：随着“互联网金融”大潮而来的第三方支付和银行零售支付系统几乎彻底扫荡了现钞的生存空间，从而将所有交易都纳入到了某个账户的变动之中。沿着这条线路，比特币等数字货币对于去中心化的追求更显现了它在现代技术包装下的“复古”内核。

然而即使同为去中心化的支付系统，数字货币与贵金属货币或纸钞的运行机制仍然有很大差别。贵金属货币或纸钞不仅支付是分散化的，而且信息的处理也是局部性的，交易只需要买卖双方就可以完成，并不需要了解其他交易者的信息，更不用向他们通报自己的交易情况。而在基于区块链的数字货币支付过程中，交易信息的流动和储存则是全局性的，货币系统的每个使用者都需要备份系统中所有交易的资料。正因为此，Luther和Smith认为比特币并非去中心化的支付系统，而是一个分布式（Distributed）支付系统。

更重要的是，对于数字货币去中心化特性的推崇有意无意地忽略了一个事实，即比特币和其他类似数字货币的系统和程序设计是中心化的，由它们的创始者编写和发布，其他绝大部分的货币用户只是这个系统的接受者。当然，理论上这个系统是完全透明的，如果你有足够的知识，可以去检查程序的源代码来确认它的合理性和安

数字货币仍然是一个中心化的系统，只不过它的“中心化”体现在更为底层的位置

，从而也更为隐蔽。
类似地，信任对于数字货币的运行也依然至关重要，只不过所需的这种信任由政府和金融机构转移到了数字货币的创立者和能够理解这一系统运作细节的技术精英身上。于是，如果我们相信克莱蒙梭的那句名言，“货币重要到如此的程度，以致于不能让它为中央银行所管理”，那么为什么将它交给“极客（Geek）”就会更令人放心一些呢？

数字货币经常被宣传的另一个重要优点是交易的匿名性。如果排除那些非法活动的企图，对于这一特性的重视应该源于对隐私泄漏的恐惧。然而，至少对于比特币而言，这一特性相当地名不副实。比特币的匿名性来自于它的交易无需任何传统金融机构的账户，因而不会暴露交易者在现实世界里的真实身份。但这一防线是非常脆弱的，一旦某个人的公钥地址和他的真实身份对应上，那么由于区块链记录的全面性，追踪他的所有交易甚至比在传统金融系统中更为简单。考虑到比特币交易和使用者实际生活的关联（例如收货地址或者更为广泛的网络足迹），对于金融监管当局或者刑侦系统，确认某个公钥地址的真实身份并不那么困难。当然，数字货币的用户也意识到了这个问题，并且在比特币和新一代数字货币中启用了更为复杂的防追踪机制，最为典型的就是混淆（Mixing），即将多笔交易混合在一起以隐蔽真正的支付者，然后采用多重公钥来保护接受者的地址。但是这类加密措施仍然可能被流量分析或其他的社会工程学手段突破。看起来，数字货币在匿名性问题上又陷入了传统货币防伪技
术那样的猫鼠缠斗，但它的影响并不
止于此。
随着数字货币引入越来越复杂的加密机制，像比特币那样直观地确认某笔交易的真实性也变得越来越不可能，最终人们只能指望正确的程序设计和运行来确保这一货币体系的可靠性。
而一旦系统中存在着潜在的漏洞或者遭受攻击，要查明问题的原因和全部影响也将极为困难。在这里，数字货币重现了现实世界中的治理难题。

从互联网上的“复古”货币这一视角出发，我们可以更为清晰地理解数字货币的其他一些特征，如货币供给的总量控制。比特币将其货币总量限制为2100万枚，一旦达到这一上限，矿工创建新的区块将不再获得比特币奖励，而是依靠交易费获得激励。这种严格的总量限制显然是为了与滥用货币发行权的法定货币当局划清界限，同时也给比特币以更为稳固的价值基础。但是正如贵金属货币体制经常受制于通货紧缩，如果比特币成为主导货币，也肯定会面对如何满足经济交易不断增长的流动性需求的问题。对此相当多的比特币倡导者似乎并不以为然，认为数字货币单位的可分割性自然化解了上面的疑问。但是这一自信的思路显然低估了价格粘性，尤其是工资刚性的威力。事实上，
目前比特币价格的高度弹性是由于它本身并非经济体的主要定价货币，而是依托于

除此之外，比特币的总量限制还带来了一个贵金属货币体系不曾有过的风险：随着挖矿获得的收益越来越低，要保持矿工们创造区块以验证交易的激励，交易费就需要大幅上涨，大容量矿池拥有者将其算力转而用于攻击主链的危险也会随之上升。

和货币供给上限密切相关的一个问题是数字货币在信用扩张上的困难，这也是贵金属货币体制的一个典型特征。
在一个纯粹的贵金属货币体系中（这里需要注意它与“贵金属本位货币体系”的区别），流动性完全由贵金属的总量决定，而不存在由于信贷而衍生的货币乘数，这也排除了任何货币政策的可能性。因为对于有形货币，当你将它借出的同时，也就丧失了运用它进行支付的能力。正因为此，在一个纯正的比特币体系中，不可能存在银行这样的金融机构，因为在这个数字货币世界里“存款凭证”不是可接受的支付工具。而那些在现实中确实存在的“比特币银行”或类似的比特币储蓄机构，则是比特币的衍生物而非体系本身的一部分，并且很有可能是比特币创立者极不愿意看到的衍生物。这也折射出了
数字货币的一个窘境：
如果它们真的希望成为现代经济体中的主流货币而不是某个小圈子里的交换媒介，那么就必须抛弃最初的理念，重新拥抱在其创立时被扫地出门的传统金融机构，从比特币体系变为“比特币本位”体系，进而逐步放弃去中心化、匿名性、总量上限等当初精心设计的一系列特性。回顾货币演进的历史，这是一条似曾相识的道路。

四

投机驱动的竞争与进化

如果数字货币退而求其次，安心于某种小众货币的地位，那又如何？就如同数字货币体系“竞争论”所强调的，尽管比特币或者具体的某种数字货币可能不完美，但是数字货币打破了法定货币的垄断，从而可以通过货币竞争来促进优胜劣汰，最终实现货币体系的有效性。这一观点经常引用奥地利学派的货币观念，尤其是哈耶克的私人货币学说作为自己的理论基础。然而这一理论基础的稳固性是极富争议的。
首先，相对于已经被主流学家接受并给出形式化证明的商品市场自由竞争理论（尽管哈耶克显然对这种数学论证不以为然，并且认为将其观念概括为瓦尔拉斯均衡的存在性与有效性完全扭曲了他的原意），更进一步的自由货币竞争理论则还停留在“理念”阶段。事实上，无论在理论还是政策实践层面，货币体系中自由竞争的效果都有不少反例。即便我们略去这一层的争议，数字货币能否担当哈耶克理论中私人货币竞争者的角色也很成问题。虽然哈耶克对于快捷的电子货币交易系统颇有好感，但是考虑到他对于市场竞争过程（私人货币发行者根据市场状况对于货币供给进行调整）的重视和奥地利学派基于“回溯定理”的货币价值观，很难想象他会接

受一个由自动化运行的数字货币构成的世界。

即便竞争性货币体系的理论基础不是那么可靠，或者实践当中的种种约束让我们不得不接受法定货币的主导地位，也许有一种潜在的竞争货币也可以给中央银行以一定压力，使得它不至于在货币政策上过于放任。这个看起来颇为合理的想法早在比特币诞生之前就不断被人提及。不过当前的数字货币能否承担这种设想中潜在竞争者的角色，履行“真正的”货币职能却没有定论。在此方面的实证研究集中于数字货币的价格动态和与其他金融指标的相关性，试图籍此判断交易者持有货币的真实动机，并且不少文献给出了不利的结论，认为数字货币更类似于投机资产而非交易媒介。但也有人给出了不同意见，认为对于比特币的大规模需求本身就说明了它或者已经获得了广泛使用的交易媒介的地位，或者由于有着成为广泛使用的交易媒介的预期而成为有利的投机资产。虽然这一逻辑看上去并不是非常有说服力（即使所有交易者都是理性的，只要市场存在一定程度的信息不确定性，就可能出现不可持续的投机性泡沫），但是它却引出了一个重要的问题，即投机交易在数字货币存在与发展中的角色。

毫无疑问，数字货币的交易性需求（通过持有数字货币作为中介来交换其他物品）和投机需求（通过持有数字货币待其升值后卖出获得收益）不仅在动机上，而且在对于数字货币市场特征的关注点上都存在巨大的差异（图2）。某种角度上看，这种市场特征的差异非常符合布罗代尔对于贸易类型的概括：“有两种类型的交换，一种是普通的、竞争性的、几乎是透明的；另一种是高级的、复杂周密的、具有支配性的”。这种差异性使得数字货币市场中投机者的大量涌入很容易“挤出”真正对数字货币有交易性需求者。但是另一方面，在一种货币被广泛接受的过程中，尤其是在起步阶段，交易性需求也许是有益甚至必不可少的，因为它不仅能够扩大公众对于这种货币的认知，而且可以为其带来市场流动性和配套设施。而对于数字货币圈之外的交易者，这两点在其决定是否接受对方用数字货币支付时，可能成为至关重要的决定因素。

图2 数字货币交易需求和投机需求的差异

我们已经习惯于法定货币的日常使用，因此很容易忽视它所依托的基础设施，如支付清算体系、法律法规等等，以及相应的金融认知，如假钞的识别、银行账户操作、不同场合对于货币类型的要求（信用卡或现金、纸钞或硬币）等等。然而在面对一种新的货币或支付方式时，基础设施和金融认知的重要性就会凸显出来，并且直接影响着它的用户门槛和使用效
率。与此类似的是货币使用的安全性
，即在交易过程中损失资金的可能性，包括支付过程中由于操作失误或者系统故障导致资金被错误发送甚至直接消失，交易发生争执时撤回支付的可能，账户中的资金被窃取或者被用于违背自身意愿的交易等等。显然，它同时取决于与特定货币相

关的技术和法律因素。货币的使用效率和安全性决定了它的用户数量，而后者又通过网络效应影响着它的可接受性，也就是这种货币可以购买的商品或金融资产的丰富性。反过来，货币的可接受性和用户数量又会诱导政府、商家和用户在货币基础设施、应用设备和软件以及认知方面的投资，进而影响其使用效率和安全性，构成一个内生的循环。

如果从上面的视角来审视数字货币的发展，我们可能会对它们的前景极为悲观。就用户体验而言，大部分的数字货币都更类似于还在内部测试阶段的半成品，几乎没有界面友好的概念。以比特币为例，除了要了解挖矿相关的技术知识，用户还必须依靠由无规律字符组成的私钥来进行操作，钱包地址也同样是一串字符，稍有不慎，就会由于误操作而导致资金汇到错误的地址，由于忘记私钥或私钥文件损坏而导致比特币丢失的情况更是屡见不鲜。程序操作的复杂性还使得用户常常为了效率而忽视安全，例如将私钥保存在非加密的硬盘中，或者钱包长期保持在线状态，导致被黑客攻击遭受损失的风险大大增加。雪上加霜的是，由于许多国家的政府对于数字货币的态度并不友好，一旦数字货币由于交易纠纷或黑客攻击而遭受损失，很难得到法律的保护。在这些界面设计和制度层面的问题之外，基于区块链的数字货币在使用效率上还受制于一个底层的技术约束：由于“公众见证”的机制，在交易量随用户增加的情况下，交易获得确认的时间也会急剧上升。网速的提高和区块扩容可以部分缓解这个问题，但仍然不可能跟上交易量随用户数的级数增长，以致于有人认为交易记录系统的精确性、去中心化和高效费比是不可能同时成立的三角。

鉴于以上的种种问题，数字货币能够获得今天的成绩几乎是一个奇迹，那么它背后的动力是什么？正如Gandal等人所观察到的，在比特币市场存在大量的价格操纵行为，相当比例的价格上涨是由可疑的交易所推动的，这显然不是一种交易媒介应有的状态。因此，
除了一小部分比特币理念的坚持者和由于种种原因（如匿名性）对于数字货币有着特殊需求者外，
数字货币的大部分交易者更多地
是出于投机动机。
这也解释了为什么比特币的剧烈价格波动和高度分割的市场结构（这些都是交易媒介的致命缺陷）并没有吓退大批涌入的交易者，因为价格波动、市场扭曲和信息不透明正是投机交易的利润来源，而一旦市场透明化之后，这些套利空间也就消失了。不过，尽管可能有违比特币创立的初衷，数字货币投机者确实带来了数字货币知识的普及、市场流动性、交易配套设施和更好的用户体验，一旦将来遇到合适的时机，它们将会是数字货币真正参与经济生活和货币竞争的基础。但另一方面，我们也需要清楚地看到投机的危险性：除了可能损害数字货币的声誉和信用之外，投机力量还可能合谋固化扭曲的市场结构以持续牟利。投机者会冒险开辟新航线，但也会不顾一切地垄断它，我们需要记住布罗代尔的告诫。

五

文化意象与货币职能的纠葛

对于数字货币有更多了解之后，我们发现，至少就比特币而言，它并不一定是具有多重均衡的主流货币模型中那个福利水平更高的均衡点。于是重新回到最初的问题上，为什么比特币仍然能够在一定范围内成为交易媒介？在模型中加入“黑市”（如Silk Road平台）的特殊货币需求或者类似MIU（Money in Utility）模型那样直接引入“极客”对于比特币的热爱可以部分地解决上述疑问，但仍然是不够的。我们看到，许多数字货币的倡导者都坚信数字货币能够成为未来世界的通行货币（虽然其中肯定不乏只是想炒作概念的投机者），那么这种信心又从何而来？

在《比特币白皮书》中，“信任（Trust）”是一个关键词。尽管中本聪没有在文中做过多的渲染，人们还是可以从中嗅到对于高度复杂化的金融体系顶层操纵者的质疑与不满。但是不同于许多当前金融制度的批判者，中本聪并没有选择回到熟人社会以恢复平等和信任的路径（例如社区货币），而是基于互联网建立了一个至少在理论上不需要对于任何特定个人的信任的去中心化交易体制。虽然在技术上颇为不同，但这一模式对于经济学家来说其实并不陌生，那就是完全竞争市场。在完全竞争市场中，任何特定参与者对于价格的影响都趋近于零，可以被无成本地替代（因而没有能力和动机去做恶），因此市场履行其职能并不需要依靠任何特定的个人。从这一角度出发，颇为有趣的是，看上去离经叛道的数字货币其实却有着和主流经济学一脉相承的理念：任何个人都是不可信任的，可以相信的是制度约束下的群体。不过，正如制度经济学所一再强调的，竞争性市场正常运转的基础是人们对于自由市场制度的信任。同样，正如前文所分析的，对于比特币，信任问题并没有消失，只是从传统金融机构转移到了这套体系（以及它的创立者和了解系统运作细节的技术精英）身上。在这里，“信任”的含义远远超出了前面多重均衡博弈中对于大多数人行为的预期问题，因为不仅每个均衡里的收益是不确定的，甚至博弈的结构本身都是不确定的。

对于某种史无前例的数字货币最终是否能够被世界所接受这样的问题，其判断不仅取决于个人所获得的信息，而且还依赖于他的世界观，或者用博弈论的术语来说，他关于这一博弈的结构的“信念”（Belief）。当然，如果这个人足够理性，他会随着博弈的进行更新他的“信念”（并且博弈结构本身也会随着参与者的变化和时间推演而改变）。想要引导这一博弈向着自己希望的方向演化，对于当前和潜在参与者的“信念”塑造就极为重要。数字货币的创设者显然也意识到了这一点。在中本聪与比特币早期核心圈成员的交流中明确地提及了比特币可接受性预期的自我实现效应，而为了尽快将比特币的使用者规模提升到可维持的网络效应门槛之上，他们设计了针对不同需求群体逐步扩张用户群的策略，并且将最初的用户类型锁定在与互联网相关的亚文化群体。而比特币的文化象征意义也在起步过程中发挥了巨大

作用，很多早期的比特币持有者更多地是用这一行动来宣示他们“反建制”的政治态度或者特有的“极客”文化，这一人群在比特币的用户中占有重要的位置。

虽然在其起步阶段提供了重要的助力，比特币的文化象征意义对于其成为主流货币

我们已经看到，在理论上匿名的比特币用户，其活动却是可以追踪的。正如Meiklejohn等所展示的，只要有足够耐心对区块链中的地址进行分析，就能够掌握资金流动的情况，甚至包括那些用于非法活动和被盗资金的动向。因此，比特币用户就像假面舞会的参加者，尽管我们暂时不知道面具后人们的真实身份，但是每一个客人仍然有其独特的个性，其活动也都在大家的眼底。这种不彻底的匿名性固然有初始技术限制的原因，但也在一定程度上反映了“极客”文化的本质：“极客”希望保持匿名并不是为了混同于众人，而是为了以新的身份生活在虚拟空间里；在其中他们建立自己的声誉，有着各自的社会交往，比特币则是这种另类生活的一种媒介。但这种颇具浪漫色彩的风格显然与现代商业“朋友归朋友，生意归生意”的信条格格不入。

与此同时，
比特
币流动轨
迹的可追踪性还带
来了另一个问题，就是每枚比特币的
特异性。
比特币很容易被其使用者所“污染”：如果某个比特币曾涉及非法活动或者被公众憎恶的人物使用过，就会永远存留在其交易记录中，导致人们对它的规避；反过来，如果某个比特币曾经过社会名人之手，很可能在其崇拜者眼中价值倍增。然而对于货币，匿名性（相同面值的货币之间不可区分）是其履行价值尺度和交易媒介职能的基础，一旦每枚比特币都具有自己的“个性”从而价值各异，也就失去了作为计价单位的能力。在这里我们同样看到了比特币的文化含义与其货币属性之间的潜在冲突。

比特币的上述特征，再加上由于区块链容量和交易确定速度限制对于用户规模的制约，很容易给人造成一种印象，
即无论其创立者的真正意图如何，比特币实际上仍然是一种特定社会圈层内的小众货币。
比特币早期的支持者愿意接受和使用它，更多地是表达“有了区块链，我们不再需要政府和银行家”的理念，而未必相信比特币这一具体货币形式能够承载这一梦想。对于公众，“极客和黑客使用的货币”是他们对比特币的最初印象（不幸的是，

这一印象随后又被“投机商炒作的货币”所取代）。在这一点上，比特币不信任任何个体（以及抽象的“人性”）的技术理念和它在现实世界中对于支持者社会理想的依赖构成了微妙的反差，让我们不由得联想到影视作品中经常出现的那种表面上愤世嫉俗，内心却激情燃烧的角色。

不过比特币文化象征与货币职能的种种冲突在随后出现的数字货币上则大大弱化了。这些后来者在货币职能上显得更为“专业”，对于用户更为友好，不拒绝与传统的金融机构甚至政府合作，发行机制上也向传统货币观念做了妥协（例如重新引入中心化的发行机制），这有效地抵销了比特币的先发优势，使得它们得以迅速后来居上。尽管比特币仍然在数字资产存量中占据着绝对主导地位，但在日常交易量上已经被泰达币（Tether）等更为商业化的数字货币所超越。就比特币自身发展而言，除了技术上的限制，其创立之初的一些理念能否得以持续也变成了疑问。例如用于遏制资本垄断力量的算力原则在大型矿池出现后反而变为了资本博弈的工具，看似人人平等的治理架构在“扩容”方案的激烈争斗中被撕得粉碎，比特币现金（Bitcoin Cash）的出现更让人们对其未来充满疑惑。在历史中，我们见过了太多挑战者最终皈依传统的例子，因此数字货币的上述变化也许并不令人惊讶。但是数字货币演化过程中文化象征意义与货币职能之间的纠缠，却仍然能够为我们理解经济与社会之间的复杂关系提供许多线索。

六

结语

比特币诞生时，“金融科技”和“人工智能”还没有成为热门词汇。但是在“互联网金融元年”到来之后，数字货币被许多人划归到这次金融科技浪潮之中，成为未来数字金融体系“美丽新世界”的一部分，基于区块链的分布式信息处理技术也在经济发展和社会治理中被寄予厚望。现在我们很难猜测中本聪创立比特币时的真实想法，不过从当时的讨论记录来看，数字货币目前的发展路径应该多少有些出乎他的意料。比特币成为主流货币的前景依然不明，但它的理念和技术已经产生了巨大的带动效应，而其经济和社会影响则是高度不确定的，这也给不同视角的观点提供了想象空间。

主流经济学擅长于均衡分析，但在很
多时候，
类似数字货币这样尘埃未定的事物更能够反衬出那些对于支持均衡至关重要却经常被我们忽略的因素
（这也是中国经济学家拥有却尚未充分利用的一个优势）。意识到我们一直认为理所当然的观念可能是错误的，很可能导致类似大众媒体宣称比特币颠覆货币理论那样的“过度反应”；与此同时，主流经济学界虽然惯于自嘲，对于“外行”的批评

却缺乏耐心。这种基于知识背景和分析视角的对立显然无助于我们更为深入地探讨数字货币的本质和它在未来社会中的角色。在整个经济与社会都可能由于底层技术变革而发生范式转换的时刻，不同观念的相互交流和补充对于理解未来趋势的意义不言而喻，我们应该将数字货币对现有观念的挑战看作实现这种联合的一次机会。