内部资料　注意保存

中国社会科学院金融研究所支付清算研究中心
Research Center of Payment & Settlement, IFB

支付清算评论

2023 年第 7 期(总第 110 期)　　2023 年 7 月

目 录

数字货币概念辨析及典型数字货币简介

许多学者在研究数字货币时，都试图对电子货币、虚拟货币和数字货币的概念范畴进行辨析，甚至是对三者的概念界定进行较为严格的划分。不过，本文更希望通过细致的梳理，使人们能够认识到这三个概念在中文语义下涵盖范围之间的交叉，以及其在现实的使用中概念自身的不断演化。

一、对数字货币概念的辨析

（一）电子货币

在早期的文献中，电子货币的概念指的是储存在电子计算机里的并能通过电子计算机系统进行转账和划拨的存款，主要形式是由电子计算机系统操作的各种塑制银行卡，包括信用卡、支票卡、自动出纳机卡、记账卡、灵光卡等（童频，1992）。可以说，电子货币的概念是伴随着银行电子化而产生，是19世纪60年代以来美、日等国的金融机构为其银行电子化的目标投入巨款并已取得的成效之一，以结算简便、调拨迅速、节约纸张、方便用户、加快商品流通速度的显著优点而受到国际金融界的瞩目（刘勤和钱淑萍，1991）。目前从知网上可以查询到的最早使用电子货币这一概念的国内文献是曾子敬1986年发表在《广东金融》上的一篇文章，介绍的也正是香港地区银行业中业已存在的信用卡、自动出纳机（ATM）等。

此后，随着现实中金融业的电子化以及数字化程度不断向前

推进，学界对于电子货币的概念界定也在不断演变。根据巴塞尔银行监管委员会（BCBS）（1998）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。王鲁滨（1999）则进一步指出，作为一种储值或预付产品，电子货币又可分为智能卡和网络货币，其是伴随着电子商务的发展而发展起来的，当时较为代表性的产品包括 CAFÉ、Cybercash、Digicash、Mondex 等。不过鉴于现实中快速的演进速度，更多学者则试图从更广义的也更功能化的角度来界定电子货币。例如岩崎和雄和左藤元则（1999）曾从数字化角度对电子货币进行了较宽泛的定义：“电子货币是指‘数字化的货币’，举凡付款、取款、通货的使用、融资存款等与通货有关的信息，全部经过数字化者，便叫电子货币。”周光友（2009）则认为电子货币“应该是指计算机网络为基础，以各种卡片或数据存储设备为介质，借助各种与电子货币发行者相连接的终端设备，在进行支付和清偿债务时，使预先存放在计算机系统中的电子数据以电子信息流的形式在债权债务人之间进行转移的，具有某种货币职能的货币。”董昀和辛超（2013）提出，电子货币是指以计算机或其他存储设备为存在介质、以数据或卡片形式履行货币支付流通职能的“货币符号”，其具体形式包括卡基、数基存款货币，电子票据等等。

从上述对电子货币概念界定的演变中不难看出，理解电子货币的更重要的视角应落在更为现实的金融基础设施以及支付工具

的发展演变上。某种程度上讲，电子货币本身并非是一种孤立的货币形态的转变，而是在金融业电子化数字化发展过程中支付清算体系以及支付工具演变的附带品。我们从一些早期的文献中也不难发现这一点。例如李遵法、许桂琴 1993 年的一篇文章就是着眼于电子货币流通系统而不是电子货币本身。按照其定义，所谓电子货币流通系统就是以电子计算机网络通讯、数据库、电子化自动金融机具和商业机具为基础的，把自动化银行、自动化消费场所和单位工资代发系统等联结起来，以电子信息转账的形式来取代传统的货币流通方式的贷币流通系统（李遵法和许桂琴，1993）。金卡工程建设更是被人们普遍认为是我国进入电子货币时代的标志（程静，1995；王华庆，1995；等）。此外，许多探讨电子货币发展的文章，其着眼点和内容实际上就是针对各国支付清算系统（祁英，1998）或者电子支付工具（王鲁滨，1999）的研究，包括其对货币供需、对金融体系尤其是银行业影响等。

最后，有两点有意思的地方特别值得注意。第一，1997 年一篇名为《新型交易媒介——电子货币》的文章发表于《国际金融研究》杂志“金融科技”版块中，可见金融科技一词即便在当时或许也并不是一个生僻概念，这也提示我们研究金融科技以及与之相关的数字货币或电子货币时，可能需要具备一定的历史视角。第二，和后来学界对虚拟货币以及目前对数字货币的探讨一样，早期针对电子货币的一个重要研究方向也在于其可能存在的风险和问题，甚至巴塞尔支付清算系统委员会在 1996 年也曾发表了有

关电子货币安全性的报告，同年国际清算银行也发表了题为《电子货币的发展带给中央银行的问题》的报告。这充分说明由技术进步带来的支付形式和货币形式的重大转变在任何时候都有可能会对现存金融体系形成较大的冲击。

（二）虚拟货币

与电子货币概念沿着支付工具变迁的主脉络不断演变相比，虚拟货币的概念则从一开始就比较泛化。虚拟货币是与虚拟经济相对应的，而虚拟经济在我国学界的话语体系中存在两种意思。一种是沿着马克思的虚拟资本理论创造出的概念，与之相对应的虚拟货币则指代的就是信用货币（梁坚和陈国华，2004）。不过“虚拟货币”概念在这种语境中的使用比较少见，并且与本书研究主题关系不大，故这里不再多谈。另一种对“虚拟经济”概念的使用则是用其指代互联网经济，这与本文探讨的主题关系就比较密切了，故需详述。

在互联网经济的语境下，人们在使用虚拟货币概念时仍然有着不同的指代对象。从国内研究文献来看，虚拟货币的指代对象经历了几次较大的改变。早期期刊中提及的虚拟货币通常指的就是当时的电子货币。例如，目前从知网上可查询到的最早使用虚拟货币概念出现在 1997 年《珠江经济》杂志“环球博览”栏目中的一条资讯中，其指代的就是上文中提及的电子货币的一种，就是王鲁滨（1999）文章中提及的网络货币。费宇东（1998）在探讨当时网上购物的付款方式时，同样使用虚拟货币一词来指代这

种电子货币，即 Cybercash 这种以信用卡付款方式运作的网络支付工具。与上述文献将虚拟货币局限于网络货币不同，还有部分学者对于虚拟货币的概念界定则相对更宽泛，但却仍包含在电子货币的范畴之中。例如周湘仕（1998）将英国西敏寺银行开发的早期的电子钱包 Mondex 也包含在虚拟货币的概念范围内;而在李翀(2003)的文章中则基本上将虚拟货币完全与当时包括信用卡、ATM 等在内的电子货币划上了等号。

随着互联网经济的快速发展以及网络生态的完善，人们对虚拟货币这一概念的使用方式也逐渐进入了一个新的阶段。早在 1999 年,《Internet 信息世界》杂志中一篇名为《网络社群营销新路》的文章中就使用虚拟货币一词指代一些仅存在于网络社区中的“货币”。大约在 2005 年后，绝大部分文章中所谈到的虚拟货币便都由电子货币转化为了这种网络社区虚拟货币。在当时最主要的代表是游戏币，这类虚拟货币由互联网运营商发行，在某一特定范围内充当一般等价物，具备有限的流通和支付功能。曹红辉（2008）曾描绘虚拟货币是“一般通过购买、赠送、奖励等方式获得，对发行人提供的物品或服务不依赖于现实货币而独立地充当价值尺度的计量单位”,这大体上就是指这类虚拟货币。包括腾讯的 Q 币、魔兽世界 G 币、亚马逊 coins、Facebook Credits 等等，这些虚拟货币在网络社区中被用于与应用程序、虚拟商品及相关服务有关的交易，形成了复杂的运行机制。尽管早期这种网络虚拟货币更多被用来购买虚拟产品和服务，但仍有不少学者

关注其对于现实中的货币流通以及金融秩序带来的冲击(陈东海，2007；钟孝生，2007)，更有人已注意到网络虚拟货币的支付领域正在向实体经济领域不断的扩展（张磊，2007)。

随着比特币等新一代的互联网货币或者说数字货币的兴起，虚拟货币一词的概念和内涵进一步发生改变，上面提及的虚拟货币的两种截然不同的语义从此开始逐渐融合，这恰恰因为这些新的虚拟货币既有网络虚拟社区币的特点，同时又具备电子货币的现实支付功能。根据谢平等（2014）的定义，以虚拟货币为蓝本发展起来的互联网货币是由某个网络社区发行和管理，不受或少受央行监管的，以数字形式存在的，被网络社区成员普遍接受和使用的货币。ECB（2012）也指出，“虚拟货币是一种不受监管的电子货币，它们通常由开发者发行，在一个特定的虚拟社区内被成员们使用和接受”。从中可见，虚拟货币和互联网货币在此阶段似乎已经能够包含在电子货币的概念范畴之内了。尽管我们可以简单的将其分为两类，第一类是诸如Q币等在网络虚拟社区中使用的“货币”,第二类则是比特币、莱特币这些全新的互联网货币，然而仔细剖析上面提及的关于虚拟货币的定义的话，我们不难发现二者的共性，也即是其之所以被并称的原因。

如果说电子货币一词侧重的是支付工具以及与之相关的“货币”电子化和数字化进程，那么虚拟货币一词则侧重于强调货币发行的主体。游戏币等网络虚拟社区币是由特定网络虚拟社区的运营者发行，而互联网货币则是“去中心化”发行，注意这二者

的发行主体均不是传统的中央银行-商业银行体系。贝多广等（2013）曾指出，在电子货币中，银行电子货币（包括电子支票）受到政府监管，属于法定货币范畴；而以互联网货币为主体的虚拟货币不受政府监管,属于补充性货币范畴;补充性货币的出现，不再简单是法定货币内部纸币与电子货币的替代，而是法币被补充性货币替代，而中央银行难以监控补充性货币的发行。按照这个分类法，我们便不难理解为何称之为“虚拟”。目前文献中提到的虚拟货币更多指代的就是上面提及的第二类，即互联网货币，恰恰这也是后文我们会详细探讨的数字货币中的一种。

（三）数字货币

早在 2000 年以前，国内期刊中就已屡屡出现“数字货币”的概念。1996 年《个人电脑》杂志上转载的一篇译文名字就叫做《数字货币之现状》，其指代的就是上文反复提及的 Cybercash、Digicash 等网络电子货币或虚拟货币(Rupley, 1996)。1998 年，国内有数本杂志都曾转载了美国两位学者在《未来学家》杂志上撰写的有关数字货币前景的文章，认为其“前景诱人”，而这里提及的数字货币指代的依然是网络电子货币。可见，如果仅从概念范畴来看，电子货币、虚拟货币以及数字货币在当时基本上是一致的，因此随着概念逐渐统一，进入 2000 年后有关数字货币的研究就很少了。

直到比特币的出现，才令数字货币再次受到各界的关注。一方面电子货币的概念已逐渐清晰，另一方面人们对比特币等加密

数字货币的使用已明显不再局限于网络虚拟社区内，因此尽管虚拟货币的概念仍然可以被用来指代这一类“货币”，但人们更希望用一个更加贴切的专有名词来指代这种数字化发行和流通的新型“货币”。因此可以看到，此后相当长一段时间，国内文献中数字货币基本上就是与比特币等加密数字货币等价，而国外文献谈论的焦点也转化为加密数字货币（Crypto Currency），即便偶尔有人使用数字货币（Digital Currency）一词，基本上指代的也是加密数字货币。关于此有大量的国内外文献可以佐证，在此不再一一列举。

事实上，对于电子货币、虚拟货币以及数字货币概念之间的纠结并非仅存在于国内，自比特币横空出世后，各国学者以及官方都在围绕这种新生事物进行概念上的辨析。Wagner（2014）就将数字货币定义为以电子形式储存和转移的货币。这一定义较为笼统，不仅包含了数字货币，还包含了电子货币在里面。欧央行2015年2月发布了一份关于虚拟货币的报告将数字货币定义为一种价值的数据表现形式,它并非由货币当局发行,在某种情况下,它可被当作货币的替代品（ECB, 2015）。同年11月国际清算银行发布了一个题目为《数字货币》的报告，其中认为数字货币是一种电子形态的货币，可以纳入广义电子货币的范畴。

然而实践的进展总是跑在理论的前面。比特币在现实中引起了各界的极大兴趣，并直接导致各国央行开启了央行数字货币（Central Bank Digital Currency, CBDC）研发竞赛，而在商业

领域针对比特币价值不稳定的问题，许多机构也开始探讨所谓的稳定币，2019 全球最大社交平台 Facebook 发布 Libra 项目白皮书，更是将人们对数字货币的关注度提高到一个新的水平。央行数字货币、稳定币等形态的数字货币陆续出现，使得人们开始重新思考数字货币的定义。目前来看，各国接受度最高的是 CPMI 在 2018 年提出的“货币之花”。CPMI 从四个关键属性对各类“货币”进行分划：发行人（中央银行或非中央银行）、货币形态（数字或实物）、可获取性（广泛或受限制）、实现技术（基于账户或基于代币）（CPMI，2018）。

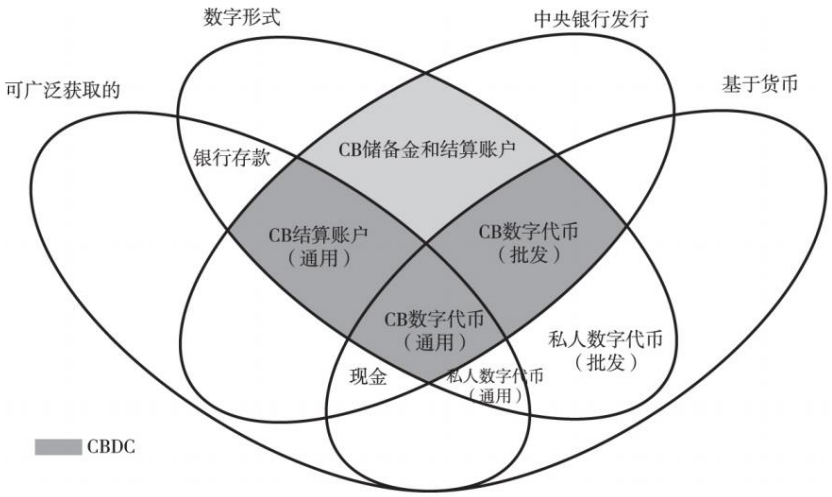

图 1 货币之花

资料来源：CPMI. Central Bank Digital Currencies. CPMI Papers, No.174, 2018.

纵观现实中对数字货币以及与之相关的电子货币、虚拟货币等词汇应用的演化历程，我们不难发现这些概念本身可能都不是严格意义上的学术概念，并且随着时间向前推移，这几个概念的范畴又在不断的分开或融合。例如中本聪自身也是将比特币称为电子现金（Electronic Cash）而非数字现金（Nakamoto，2008）；

而英国央行副行长 Broadbent 在谈论数字货币时也曾指出各国银行账户上流通的货币绝大部分本身就是数字化的（Broadbent，2016）。因此，可能更值得我们关注的并不是每个概念的具体范畴，而是其试图强调的侧重点。电子货币强调的是支付结算以及附着于其上的更多金融业态的电子化和数字化趋势，虚拟货币则强调的是“货币”发行或经营的主体向央行-银行体系外的拓展。而当前所谓的数字货币以及由此带来的各种经济金融现象，既是这种电子化和数字化趋势的延续，又存在发行主体向非官方体系的拓展，故在概念上出现混淆自然情有可原。对于数字货币这种现实中正在快速发展演变中的新事物，我们更倾向于在探究现实中人们关心的实际问题上下功夫，因此本文并不试图对数字货币做一个权威的概念界定，而是将研究对象聚焦于几种现实中人们更多提及的“数字货币”上，一是以比特币为代表的私人发行加密数字货币（非稳定币），二是以 Libra 为代表的稳定币，三是以数字人民币为代表的央行数字货币。

二、几种代表性数字货币

这里我们将详细探讨上述几个典型的数字货币案例，第一个就是私人发行加密数字货币的代表比特币，第二个是 2019 年以来备受争议的 Libra，第三个是数字人民币。其中，以 Libra 为代表的稳定币的最主要用途在于跨境支付。

（一）比特币

1、比特币的兴起

比特币发明者中本聪于2008年写下了题为《比特币：一种点对点的电子现金系统》的文章，开启了一种新的货币体系，也是去中心化的虚拟电子货币研究的开山之作。根据中本聪的设计，比特币本质上是一套通过开源的算法产生的密码编码体系，所有感兴趣的人都可以自行发掘。该系统以不属于任何一个国家，没有中央服务器或者托管方，完全去中心化，所有一切都是基于参与者的自愿参与。比特币正式创建于2009年1月，是迄今为止最成功的加密数字货币，它采用开源的区块链技术，将交易信息存储在分布式账本中，这使得破解网络几乎成为了不可能的。

可以说，比特币的诞生具有跨时代的意义，正是由其开启了人们探索数字货币的时代。比特币的普及不仅推动了数百种其他的私人发行加密数字货币的出现，也令诸多金融机构加入到探索区块链应用的行列之中并进而催生出各种稳定币，同时还对各国央行具有极大的启发作用，令其纷纷开始探索法定的数字货币。

2011年6月，比特比中国网站正式成立，这是中国最早的比特币交易平台。比特币中国的建立标志着比特币正式进入中国。从那以后，越来越多的中国网民通过网站、微博、QQ群参与制造比特币和从事比特币交易，比特币在中国的影响力逐渐增大，中国比特币活跃节点[①]数目快速飙升。除了交易领域，在挖矿技术和矿场投资方面，中国在全球范围内也一直处于前列，最有代表性

[①] 所谓“节点”，是指处于活跃状况的比特币客户端，但真正的用户数量远多于这些节点数。

的证明就是NGzhang（网名）率先生产出世界上第一台ASIC比特币挖矿机阿瓦隆（Avalon），并且按期迭代更新，挖矿效率一度领先全球。此外，挖矿行业优秀企业还有蚂蚁矿机等等。中国买家的狂热不仅带动了国际上比较主流的互联网货币（例如比特币）的价格暴涨，并且国内自行模仿而生的各种山寨币也是层出不穷。有国内权威媒体在2014年6月曾调查发现，国内交易的互联网货币已超百种，年发行总额动辄近亿元人民币，无外乎其感慨称现在在国内“开个网站就能发币”。

从2013年底开始，国内相关部委就已开始对比特币等加密数字货币进行整顿，后来随着互联网金融专项整治的深入推进，到目前为止，混乱狂热的投机局面在国内基本上已经平抑了，不过从国际上看，比特币的价格仍然在大幅波动中。

2、对于发行机制的探讨

针对当前货币发行机制中的币值不稳定问题，当前无论是官方法定货币还是私人虚拟货币，其货币发行机制均是以中心化的账户模式进行，这种中心化的货币发行模式需要存在某种机制来约束发行主体的超发冲动，哈耶克（2019）提出应实施自由银行业务（free banking）和货币自由发行（free issue of money），取消政府垄断发行货币的权力以构建竞争性货币制度，因为货币发行是极为有利可图的生意，私人企业会更加倾向于执行严格的纪律约束，以此来保证公众对其发行货币的信赖与使用，而政府显然缺乏相关纪律约束。因此，可寄希望的货币竞争机制就是基

于官方和私人中心化的货币发行的竞争关系,如账户支付机制下,私人机构发行的非法定货币称为虚拟货币（Vitrual Currency),这时期的虚拟货币具有真实货币的支付结算等相应功能，并没有任何主权货币或机构为其信用背书，但其发行和流通机制仍是中心化的。

然而，以比特币为代表的加密数字货币虽然也是以“自下而上”的方式与国家公权背书的信用货币进行竞争，但其竞争的思路与账户交易机制中的虚拟货币不同，即将集中式的发行与流通的账户模式改变为分布式的账本模式，并实施去中心化的管理机制。具体来说，此种加密数字货币可分为以算法为信用基础的比特币等算法货币，以特定合约价值为信用基础的以太币等众筹货币，以及通过锚定区块链资产为信用基础的数字代币。由于众筹货币机制主要应用于证券资产的筹集与收益分配，对信用货币发行和流通环节影响最大的是算法货币和数字代币。

在货币发行机制角度来看，作为一种私有货币，算法货币与公有货币最大的区别和差距就在于“可信性”,公有货币是通过国家权威来保证其“可信性”,而私有货币是通过在网络环境内对算法的“社区互信”来实现，二者的竞争关系在于可信性的共识范围与共识强度的乘积比较，即主权国家信用货币的使用范围取决于该国主权疆域范围的大小以及在非主权范围内的可接受领域，而共识强度则在于承认该国主权货币使用性的可信程度。在全球范围内看，不能简单地比较主权国家信用货币的可信性强还是比

特币等算法货币可信性强，因为很多主权国家的信用货币仅在本国政府管辖范围内具有法偿性，而比特币等算法货币在国际网络环境下具有一定的通兑性。尤其是比特币更像是数字货币世界中的“硬通货”，在很多数字货币交易所，可以用比特币来购买其他竞争币或是数字资产。另一方面，包括美元在内的主权国家信用货币频繁进行类似“量化宽松”的货币政策，在当前的多重博弈环境下，不断损失货币持有人的共识基础，以比特币为代表的加密数字货币没有一个明确的集中发行方，货币的发行数量是以一个预先设定的透明性货币增长政策的计算机算法得出，其设计初衷是通过对货币发行规模进行技术化的“自然约束”，使货币发行的控制权回归市场，以实施总量控制的规则来替代货币当局相机抉择的货币政策。

3、对账户支付机制的改造

由于在账户支付机制下，账户的身份数据便于主权国家政府识别和管理，因此，以比特币为代表的加密数字货币是通过非中心化的“去账户”方式来规避主权国家政府的干预控制。以比特币为代表的加密数字货币，在货币流通环节中，又尽力避免将交易人身份等数据信息归集在账户之中，使货币的运行更加“匿名化”。具体来说，当前加密数字货币的通用结构分为三层：首先是以区块链分布式账本为代表的底层技术，在加密数字货币的网络环境内部，由所有网络节点共享并共同维护更新的交易记录总账本，账本以数据库的形式向全网节点公开透明，每个节点均具有

账本副本并可随时监督；第二层是共识协议，基于区块链协议中的共识性算法，以软件系统形式自动进行链上的货币资产的确权转移与公证记录，以实现资金转账功能；第三层则是货币本身，也就是资金转移的标签化传输。

而加密数字货币对账户支付模式的改造体现在对账户记账格式和账户数据属性的改变。首先，区块链创新了交易数据记录格式，区块链是将产生的交易数据按照一定的时间间隔分成不同的区块进行保存，就如同会计的月度或季度账本，将所有一定时间段内的交易消息整理和汇总，而后又将链用不同的区块相链接，这个链接的关联点是匹配各区块相对应的哈希值，而哈希值只能验证真伪，但无法回溯区块内的交易信息，这样就可以形成一个更整体和安全的账本记录。如同复式记账法对传统流水式记账的改变，记账格式在区块链机制下实现了同一时间区间内的数据整合，即在账户间贷记、借记关系的双向调整基础上，进一步增加了记账维度。其次，区块链将账户的数据属性改变为加密数字货币状态集合，去除了账户数据对身份属性特征的要求。在交易过程中，以比特币为代表的加密数字货币可凭借其内部的脚本程序安排，自行发送到任意“地址”，地址的公开性全网播报与密钥的权益性解压使在任何一个区块内，并根据状态记录自动归集为一个权益集合，这样就将账户与账户间的信息网络体系内置于加密数字货币代码程序之中，在某种程度上，这种由货币和账本共同组成的支付系统替代了原有账户体系的支付功能特征，账户的贷

记、借记关系转变为对货币在账本间运动轨迹的时间性记录。因此，账户功能退化为金属货币时代的货币存储功能，如在比特币的设计中,账户的物理形态退化为与网络环境相隔离的存储介质，而以太坊、Libra 等其他加密数字货币则试图保留账户的原有外在形式。但无论对账户外在形式如何改造，原账户支付机制下将资金存储、身份验证以及交易信息交互等三大功能属性集合于账户一身的枢纽性作用发生了巨大改变。通过对上述支付机制的结构性变化，加密数字货币创造出替代账户交易体系的价值传导网络，即只需要通过加密数字货币所有权标签或以货币链接资产的所有权标签进行确权登记和转移，即可快速完成自由、免费、零延时的国际汇兑业务。由于改变账户对于交易者身份属性的管理，使比特币等加密数字货币的运行脱离原有金融体系，使其货币发行和流通体系更加独立，而且还从根本上免除了在账户货币机制中发行中介、支付中介的相应功能，使货币交易重回“现金支付”的即时性结算特征，大幅削减货币发行和运行的中介成本。

（二）Libra

1、从稳定币到 Libra

鉴于比特币等加密数字货币币值不稳定的问题，不少机构开始探索更适合充当价值尺度的稳定币，将其与法币币值进行锚定。从稳定机制来看，目前市场上影响较大的稳定币主要包括两种[①]：第一种是由法币为抵押的稳定币，最有代表性的是 USDT，是由

[①] 也有一些对无低押的稳定币的探索，如 Basis，不过市场影响力不大。

Tether 公司承诺严格遵守 1:1 的准备金保证,即每发行 1 个 USDT 代币，其银行账户都会有 1 美元的资金保障；第二种是以加密数字货币作为抵押的稳定币，典型的例子是 BitCNY，是以 BTS（比特股）作为抵押发行的，如果 BTS 的价格大跌，抵押给系统的 BTS 币总价值跌到接近系统贷出的 BitCNY 总价值,系统就会强制将抵押物卖出以偿还“贷款”。

一些企业巨头也纷纷加入到稳定币的探索和发行中来。例如，摩根大通发起的一种与金融机构合作伙伴进行清算使用的稳定币 JPM Coin（摩根币），沃尔玛正在策划中的用于超市积分替代和消费等用途的沃尔玛币等。不过其中引起人们最大关注的当属 Facebook 组织牵头发起的联盟链稳定币 Libra[①]。

2019 年 6 月 18 日，全球最大社交平台 Facebook 上线加密货币项目 Libra，并发布项目白皮书，引发全球关注。Libra 功能定位是支付和普惠金融，致力于建立一套简单的、无国界的货币和为全球数十亿用户服务的金融基础设施。

Libra 加密货币具有如下三个主要特点：一是基于区块链技术。Libra 项目的开发建立在开源、可扩展的“Libra 区块链”基础上。二是以资产储备为后盾。Libra 币由一篮子波动相对较小的资产作为价值储备，包括稳定且信誉良好的中央银行现金及政府证券等，且严格对照真实储备资产价值进行制造和销毁。三是

[①] 有一些人认为 Libra 并非典型的稳定币，因为其并不与单一币种挂钩，不过我们倾向于认为其从发行机制上看与稳定币是高度相似的，只不过更像是一种数字化的“SDR”。

由独立协会管理。由 Facebook 发起建立独立的非营利性会员制组织 Calibra 协会对 Libra 币进行管理，协会目前共有 28 家会员，包括 Mastercard、Visa、Paypal 等支付巨头，eBay、Uber 等电商和移动互联网公司，以及 Vodafone 等电讯运营商。

2、Libra 对账户支付机制的改造路径及特征

Facebook 在其 Libra 白皮书中明确指出,传统银行所提供的金融服务不均衡、不平等的问题。如当今“互联网和移动宽带的出现”使全球绝大多数人口实现了低成本的信息连接,“这种连通性使更多人能够进入金融生态系统，从而推动了经济赋权”，然而当前的金融体系所提供的服务人群覆盖率和业务渗透率低于新网络技术提供的信息联通性，如“全球仍有 17 亿成年人不在金融体系之内，无法使用传统银行，即使 10 亿人拥有移动通信设备，近 5 亿人可以享受互联网的接入服务”。与此同时，这种金融服务供给的不均衡，还造成了“无银行账户”人员在金融成本上遭遇到不平等对待，如“财富较少的人却为获得金融服务而付出更多。从汇款和电汇费用到透支以及 ATM 费用，来之不易的收入受到侵蚀。发薪日贷款可以收取 400%或更高的年化利率，虽然仅借入 100 美元，但财务费用甚至可以高达 30 美元。”

表 1　非银支付体系与脸书 Libra 加密货币支付体系运行机制的比较

运行机制特征	非银支付机构支付体系	脸书 Libra 加密货币的支付体系相似点	脸书 Libra 加密货币的支付体系创新点

支付代币（IOU）的发行与价值基础	终端客户可用法定货币购买支付代币，所售代币的资金存入托管银行，以此资产作为代币的价值基础	终端客户可用本地法定货币购买支付代币，所售代币价值由“Libra 储备”资产池作为支撑	该资产池由投资性和地理分散性的资产作为支撑，承认各币种对应的资产价值存在波动性，但在Libra储备中设定相对应价值的一篮子合成货币的银行存款和短期政府债券，这种锚定组合货币的设计尽可能保证低波动性
代币兑换的双向性	通常实现与法定货币一对一的兑换关系，客户既可以将资金换做代币，也可以即时将兑出资金返回银行存款账户	可将当地法定货币以一定的比率兑换成Libra稳定币，也可以按相应比率兑回原法定货币或其他法定货币	区块链内以Token特征的代币既可以兑换资产，也可以兑换货币，且资产既可以分为所有权交换，也可以拆分出使用权交换
支付功能的应用流程	在体系内的网币账户间支付条件下，第三方支付机构进行交易信息的数据库更新，并由托管银行进行每日净额结算，而在非网币账户模式下的银行账户间的“通道支付”条件下，完全由银行进行结算与交易数据库的管理	区块链内的Token交易在地址间转换，而涉及区块链外的Token交易，则通过在链外进行代币兑换	以账本记录代替账户记录，记账逻辑发生转化，是不同地址间Token的总和，而非账户间货币余额的总和。
交易信息的信任基础	依托于银行体系构建信息信任基础。	由Libra协会在初期进行储备资产管理，同时计划后期转移至自动化储备管理	一是基于技术的信任，以POW为代表；二是基于制度的信任，以POS为代表。根据Libra协议，存在客户终端和验证者两种实体类型，对数据库进行更新与维护。
定位	支付服务机构	支付服务合作联盟	支付基础设施

（三）数字人民币及其他

加密货币的兴起也引发了各国央行开始纷纷探索央行数字货币，其中中国是较早对央行数字货币展开研究的国家之一。2014

年，人民银行成立数字货币研究团队，对其发行、业务运行框架、关键技术、发行流通环境、法律问题等进行深入研究。2017 年，人民银行在深圳正式成立数字货币研究所。2018 年，数字货币研究所搭建贸易金融区块链平台。2020 年 4 月起，数字人民币研发工作稳妥推进，先行在中国深圳、苏州、“雄安新区”、成都及未来的冬奥场景进行内部封闭试点测试，以不断优化和完善数字人民币支付功能。2020 年 10 月份新增上海、海南、长沙、西安、青岛、大连作为试点城市。至此初步形成“10+1”试点格局。截至 2021 年底，数字人民币试点场景超过 808.51 万个，开通的个人钱包 2.61 亿个，交易额突破 875.65 亿元。2022 年，数字人民币作为北京冬奥会金融服务的一大创新举措，成为继 Visa 和现金支付后奥运场馆支付的第三种方式，实现了 40 多万个冬奥场景的覆盖，涵盖了餐饮、住宿、出行、游玩、购物、娱乐等七个重点领域需求。2022 年 4 月，数字人民币三期试点扩容。

表 2　数字人民币的发展历程

时间	事件
2014 年	央行成立法定数字货币专门研究小组，开始论证央行发行法定数字货币的可行性。
2015 年	央行发布央行发行数字货币的系列研究报告，央行发行数字货币的原型方案的完成两轮修订。
2016 年 1 月 20 日	央行召开数字货币研讨会，进一步明确了央行发行数字货币的战略目标，指出 DC/EP 研究团队将积极攻关数字货币的关键技术，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。
2016 年 11 月	央行确定使用数字票据交易平台作为央行数字货币的试点应用场景，并启动了数字票据交易平台的封闭开发工作。
2016 年 11 月 9 日	央行在官网发布 2017 年度人员招聘岗位需求，其中将招录 6 名相关专业人才从事数字货币及相关底层平台的软硬件系统

	的架构设计和开发工作。
2017 年 2 月 4 日	中国人民银行推动的基于区块链的数字票据交易平台测试成功，将开展基于区块链技术的数字票据平台建设相关工作。
2017 年 3 月 30 日	央行科技工作会议强调构建以数字货币探索为龙头的央行创新平台。
2017 年 7 月 3 日	DC/EP 研究所正式挂牌成立。依据招聘信息，数字货币研究所主要的研究内容包括数字货币法律事务、软件开发等。
2018 年 1 月 25 日	数字票据交易平台实验性生产系统成功上线试运行，并结合区块链技术前沿河票据业务实际情况对前期数字票据交易平台原型系统进行了全方位的改造和完善。
2018 年 3 月 22 日	全国金融标准化技术委员会成立了法定数字货币专项工作组。
2018 年 3 月 28 日	人民银行召开 2018 年全国货币金融工作电视电话会议，会议指出稳步推进 DC/EP 研发。
2018 年 9 月 4 日	深圳人行联合中国人民银行总行数字货币研究所推出的湾区贸易金融区块链平台上线试运行，初步构建了数字化贸易金融生态圈。
2018 年 9 月 5 日	中国人民银行数字货币研究所已在深圳成立“深圳金融科技有限公司”，该公司参与了贸易金融区块链等项目的开发。
2018 年 9 月 12 日	DC/EP 研究所《法定数字货币模型与参考架构设计》项目在银行科技发展奖评审领导小组会议上获得一等奖。
2019 年 2 月 21 日	人民银行 2019 年全国货币金融工作会议，强调“稳步、深入”推进央行数字研发。
2019 年 5 月	5 月底，在贵阳举办的 2019 中国国际大数据产业博览会上，DC/EP 研究所开发的 PBCTFT 贸易融资的区块链平台亮相，其服务于粤港澳大湾区贸易金融，并已落地。
2019 年 8 月 2 日	央行召开的 2019 年下半年工作电视会议，会议要求加快推进我国央行数字货币（DC/EP）研发步伐，跟踪研究国内外虚拟货币发展趋势，继续加强互联网金融风险整治。
2019 年 8 月 10 日	在第三届中国金融四十人论坛上，穆长春首度公布 DC/EP 采用“双层运营体系”，同时宣称 DC/EP 已经“呼之欲出”。
2019 年 9 月 5 日	《中国日报》英文版报道，DC/EP 的“闭环测试”开始，测试中会摸你某些支付方案并涉及一些商业和非政府机构。
2019 年 9 月 6 日	原央行支付司司长穆长春担任中国人民银行数字货币研究所所长。
2019 年 9 月 24 日	中国人民银行行长易纲明确表示，央行对于央行数字货币的推出“没有时间表”，并称“还会有一系列的研究、测试、试点、情蛊和风险防范”。
2019 年 11 月	DC/EP 研究所前所长姚前向记者表示，央行加密货币（CBCC）是 DC/EP 研发的重要方向之一。我国央行的研究起点也就是 CBCC。数字货币原型系统探所了区块链的应用，但并不完全依赖该技术。
2020 年 2 月	《金融分布式账本技术安全规范》（JR/T 0184-2020）金融行业标准由中国人民银行正式发布。标准规定了金融分布式账

	本技术的安全体系，包括基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、运维要求和治理机制等方面，标准适用于在金融领域从事分布式账本系统建设或服务运营的机构。
2020 年 4 月	4 月 16 日，数位银行业内人士表示，数字货币由央行牵头进行，各家银行内部正在就落地场景等进行测试，有的已经在内部员工中用于缴纳党费等支付场景，央行人士表示，数字货币不会取代微信支付或支付宝。据人民银行数字货币研究所相关负责人介绍，数字人民币体系基本完成顶层设计、标准制定、功能研发、联调测试等工作，先行在深圳、苏州、雄安新区、成都及未来的冬奥场景进行内部封闭试点测试。
2020 年 10 月	新增上海、海南、长沙、西安、青岛、大连作为第二批试点城市。
2022 年 1 月 4 日	数字人民币（试点版）App 在各大安卓应用商店和苹果 App Store 上架。
2022 年 1 月 6 日	微信支持数字人民币，意味着数字人民币开始逐渐展现在大众的视野，数字人民币的购买力进一步提升。
2022 年 1 月 18 日	央行发布数字人民币最新数据，截至 2021 年 12 月 31 日，数字人民币试点场景已超过 808.51 万个，累计开立个人钱包 2.61 亿个，交易金额 875.65 亿元，试点有效验证了数字人民币业务技术设计及系统稳定性、产品易用性和场景适用性，增进了社会公众对数字人民币设计理念的理解。
2022 年 4 月	中国人民银行召开数字人民币研发试点工作座谈会，发布第三批数字人民币试点地区。其中，浙江省杭州市、宁波市、温州市、绍兴市、金华市及湖州市 6 个承办 2022 年亚运会的城市成功入围。

资料来源：中国人民银行，中信建投证券研究发展部，第一财经，上海票据交易所，中国电子银行网等。

中国现阶段的央行数字货币（DC/EP，Digital Currency Electronic Payment）设计应注重 M0 替代，而不是 M1、M2 替代。同时，电子支付工具的资金转移必须通过账户完成，采用的是账户紧耦合方式，而央行数字货币则应基于账户松耦合形式。时任人民银行数字货币研究所所长姚前（2018a）提出，虽然央行数字货币的当前目标是替代 M0 的实物现金形态，但事实上，央行数字货币势必会融入更多新特性，而不仅仅是替代现金。这就说明，

央行数字货币预留其对 M1 和 M2 的替代可能。在技术路线方面，央行数字货币可分为基于账户形式（account-based）和基于价值形式（value-based），姚前（2018b）认为可考虑在商业银行传统账户体系下，引入数字货币钱包属性，实现一个账户下对不同属性货币的多重管理。而央行数字货币研究所所长穆长春在其 2019 年 9 月的公开讲座中，提出数字货币可在双离线环境下进行支付且无需绑定账户，可以与比特币等加密数字货币一样，具有摆脱银行账户体系的特有优势。因此，研究现有双层零售支付账户的运行特征,有助于理解央行数字货币发行和流通的机制设计趋势，同时，当前电子支付环境下高度重视账户资源的共识机制，与数字货币及其分布式账本技术的“去账户”理念将如何协调，这些问题都具有较强的现实意义。2019 年 Libra 项目的推出使得各国普遍意识到央行数字货币的重要性。

（四）讨论：谁会成为真正的货币？

诚如前文所言，现实中人们提及的“数字货币”主要包括私人发行加密数字货币(非稳定币)、稳定币以及央行数字货币三种。央行数字货币能够成为真正的通货，这一点无需论证，问题则在于另外两种是否也能成为真正的货币，而本文则倾向于得出否定的答案。

首先来看私人发行的加密数字货币，其中最具代表性的也是发展最好的当属比特币。由于这种货币是去中心化的，因此社会上很多人似乎由此看到了哈耶克、弗里德曼等老一辈经济学家提

出的非国家化货币理念实现的影子。然而与早先几年相比，近年来大多数学者对其认识开始回归理性。比如，Evans（2014）便指出即使比特币之类的私人发行加密数字货币能够借助分布式账本来便利金融交易以及进一步推动分布式创新，但其在激励和治理方面的明显缺陷也使得其整体上逊色于现有的货币体系。而Walch（2015）则对照《金融市场基础设施原则》（PFMI），从操作风险的角度论证了比特币式加密数字货币的种种不适用于金融市场基础设施的弊端。此外，诸如能源消耗等技术问题，以及洗钱和恐怖融资等监管问题也常常被人提及。不过我们认为，比特币之所以不能成为真正的货币,根本原因还是在于其投资品属性上。并非投资品本身不能充当货币。从货币的发展历史来看，货币的职责起初是由实物来担当，并且人们在不断摸索过程中会寻找价值最具稳定性的实物来充当一般等价物，比如金银[①]。实物货币的优点在于其本身具有价值和使用价值，因此，价值稳定的实物便天然的具有用来衡量其他商品价值的价值尺度功能。但是到了符号货币时代，由于纸币或更为虚拟的电子货币本身是没有实际的使用价值和价值，而完全是充当交易媒介，因此其价格稳定性便会与投资品属性发生矛盾，因为人们的投资（或投机）一定会带来其价格的波动，这种不稳定使得投资品天然的就不具备衡量其他商品价格的职能。因此在现实中能够成为广义货币的金融资产，其存在的主要目的绝不是被大众用来投资，并且由于其期限短、

[①] 实际上马克思认为货币天然是金银，还有其他方面的考虑，如体积小、易分割等。

收益较为固定或是其他种种原因，其本身被用于炒买炒卖的价值不大。实际上，相比于股票等其他金融资产，比特币还有其更为特殊的属性，其投资价值基于其能否被认可为货币，而若要成为货币则需要价格的稳定，而这又使其丧失了投资价值。实际上对于一种虚拟的符号来说，在现实中我们无法设想市场会自发的调和这种矛盾，或按经济学的术语讲，或许存在一个均衡，但这个均衡一定是不稳定的。因此除非有某种外在于市场的力量去硬性规定其为货币，并且限制其与其他商品交换的相对价格，否则其根本不可能成为被人们普遍视为价值尺度和交易媒介的货币，但是一旦这种情况发生，那同时便意味着其失去了非主权货币的初衷。因此，无论怎样看，比特币都是一个悖论。此外，即便是比特币号称能够控制发行总量的这个优点，我们也需理性看待，正如马丁·沃尔夫所指,“虽然单一加密货币的供应有限，但总供应量是无限的”。IMF 曾披露，只是截至 2018 年 4 月加密数字货币就已有 1500 种。“这个数字很容易达到 150 万。处理加密数字货币的最佳方法是将其视为没有内在价值的投机符号”（沃尔夫，2019）。

再来看稳定币，市场上比较成功的稳定币，要么更多局限于虚拟社区之中使用，要么只是一些机构借其完成支付结算业务的中介工具。目前来看对于现实世界冲击最大的当属 Libra。然而由于存在诸多问题,Libra 项目能否落地存较大不确定性。第一，金融监管与合规将是最大挑战。满足各国金融监管与合规要求对

于加密货币来说是项艰难的考验，尤其在反洗钱和反恐怖融资方面。白皮书发布后不久，各国监管部门就已高度关注 Libra 项目的进展:法国财政部长警告称 Facebook 的加密货币不具备成为主权货币的能力;英国央行行长呼吁 G7 集团严格审查监管 Libra 项目;国际政府间合作机构反洗钱金融行动特别工作组(FATF)2019 年 6 月 22 日公布最终版反洗钱和恐怖主义融资监管指引，明确要求包括加密货币交易所在内的虚拟资产服务供应商必须与政府分享转移资金的客户信息。此外，鉴于 Libra 币的发行机制可能扰乱一些国家的法币地位和金融体系，预计其在部分国际收支较脆弱的国家也难获得官方认可。第二，存在较大汇率风险和流动性风险。尽管 Libra 币试图将币值锚定一篮子货币，但实际操作中人们更可能使用各自的货币分别与之进行兑换，这会带来 Libra 项目运作过程中的币种错配和汇率风险。同时由于 Libra 储备资产需要追求一定的回报用以支付系统成本、交易费用以及投资者分红，因此也要承担期限错配和流动性风险，如遭遇大规模挤兑甚至可能引发系统性金融风险。因此，如何处理汇率风险和流动性风险也将是 Libra 项目能否被监管机构及大众认可的关键点之一。第三，如何满足数据监管规则是另一难题。对于大型互联网公司来说,满足数据监管规则本身就是其面临的一大挑战，Facebook 就曾因其在欧洲的业务违反了 GDPR 的规定而受到处罚。而目前 Libra 白皮书仍未回答如何在技术上实现数据隐私的保护。对此,欧洲数据保护主管 Giovanni Buttarelli 公开表示了担忧，

认为 Libra 项目将使 Facbook 进一步整合个人数据和金融信息，对用户隐私构成额外风险。第四，区块链技术支持 Libra 项目仍存瓶颈。目前区块链技术的发展水平大致可支持千万级到亿级的用户规模，而截至 2022 年 1 月 Facebook 月活跃用户达 29 亿，要支持如此大规模用户的支付需求仍存技术障碍；且一味追求交易规模和速度，又会在开放性、安全性、隐私性等方面难以满足用户需求和监管要求。综上所述，Libra 项目落地困难重重，并且即便最终能够落地，也必然会在满足各国监管要求的情况下将其功能局限在服务 Facebook 自身的支付生态圈上，对于各国法币以及国际货币体系很难直接构成冲击。事实上，2022 年 1 月更名为 Meta 的 Facebook 已决定出售稳定币项目 Diem（即原 Libra）。

因此，我们倾向于认为，未来可能只有央行数字货币能够笑到最后，即成为真正的数字货币。不过，我们却并不排除互联网的发展具有改造传统货币体系的可能性。货币的本质或许只是信息（姜奇平，2013），因此随着互联网的发展可以提供更好的信息服务时，必然给人们带来无限的遐想。即便今天的比特币更多执行的并不是交易媒介的功能，而是沦为一种投机工具，但是这种尝试或许为将来探索出一种个人交易层面的“超主权货币”提供了经验。此外，即便私人发行的加密数字货币或稳定币可能无法成为真正的货币，也不能忽视其未来在经济金融领域可能发挥的重要作用。

参考文献（略）。

从账户货币到数字货币：历史演化视角（下）

（接）另一方面，信用货币通过中央银行与商业银行的二元账户机制发行，使货币价值的信用担保部分转移至银行体系，政府对主权货币的运行机制是通过中央银行向商业银行体系批发“负债”,并通过商业银行的信用创造来传导货币的流动性的金融机构，金融中介理论提供了诸多以银行为代表的金融中介机构在中心化货币体系中的积极作用和特殊意义。但事实上，金融中介机构作为维系法定货币政策以及执行支付功能的中介机构，必然会要求相应的成本补偿和经济增长的利益分成，这就进一步增加了支付的摩擦成本。

基于该二元账户体系的货币发行模式，商业银行通过账户货币的发行中介功能实现了货币的信用创造，从而间接性地分享了中央政府发行货币的权力，这可以被认为是账户货币信用属性的分化。因为对于账户货币的持有人而言，其所持有的信用货币并非中央银行的债券，而是相当于持有某家商业银行的某种抵押债券，并因此享受相应的债券收益，但在某种程度上来说，央行对账户货币的信用担保方式是间接性的，账户货币的直接信用担保由其账户所属的商业银行提供。虽然中央银行通过货币准备金制度和货币市场回购等公开操作，具有对货币市场的调节作用，但是这种制度红利的边际效应变得不再明显：一方面，商业银行在经济周期上升过程中，存在过度释放信用创造的动机，使得货币

流通信用在短时间内泛滥，这使得中央银行将被迫采取相应手段进行调控，而当经济下行趋势下，商业银行又不愿释放流动性，货币政策的传导效应不佳。

为此，中央银行以及整个金融监管体系，不断设计和强化对商业银行的监管制度，如对银行资本的严格监管，以及保护中小储户的存款保险制度等等。但有时这种金融行业监管以及体系内的信用互助增信既不能彻底解决货币间接发行所导致的金融空转问题，商业银行体系凭借在货币发行与流通的政府授权权力，在整个经济利益的划分中出现了风险和收益的不对称性，也无法在严重的金融危机面前有效应对，以至于对于系统性金融机构存在“大而不倒”的护身符，只能最后由政府和全体社会来为损失买单，进而影响到整个社会的公平性。从理论上来说，商业银行对中央银行的货币信用权力存在“委托-代理”问题，信用货币的二元账户发行机制存在变革的需求。

此外，账户货币的流通运行格局也在影响着信用货币的发行机制。首先，假定拥有全社会规模的账户体系是执行货币发行中介职能的前提条件，那么具有现代账户支付体系管理能力的并不局限于银行系统，部分非银支付机构账户体系同样可以承接中央银行的货币发行中介功能。事实上，账户体系及其网络内部支付功能的建立已经使账户体系构建方拥有了账户货币的发行条件。如对于某些非银行运营的商业平台账户体系中，其充值账户的购买能力已经不再局限于其平台体系内部，这样其平台账户内的余

额货币成为更一般意义上的交易媒介。

根据巴塞尔银行监管委员会的定义，广义的电子货币是指通过硬件设备或者电脑网络完成支付的存储价值或预先支付机制，也就是依靠电子设备网络实现存储和支付功能的货币。狭义的电子货币可以视为法币的电子化形态，与之相应的虚拟货币则是非法币的电子化，法定电子货币与虚拟货币虽然在货币发行的合法性或者法偿性存在差异，但在支付网络环境内具有相似的货币流通功能，都是一种价值的数据表达形式。虚拟货币在其支付网络的封闭环境下已经拥有了与法币相似的支付功能，部分非银支付机构为了使其支付网络转为开放环境，将其账户内代币与法币的兑换比率固定为 1:1，并将客户备付金全额上缴至中央银行以保证支付和取现承诺，虽然这种中心化发行机制和与商业银行的保值安排使非银账户体系丧失一定的独立性，但这仍可以说明非银行账户体系构建方已然具备了某种发行货币的权利和基础性条件。

在数字货币时代，从中央银行的角度来说，若要变革原有的二元账户货币发行机制，或许存在两个路径选择：一个是将二元账户发行机制扩展至具有全民账户体系能力的机构，而不是以商业银行或非银行支付机构进行划线，因为代理发行数字货币均需要实行 100%存款准备金制度，同时改变原有商业银行基于账户货币的信用创造机制，或可引入竞争性的信用创造机制以刺激金融体系更好地为实体经济服务。另一个是数字货币发行无需中介机构的账户体系介入，账户货币发行机制改为“中央银行-公众”的

直接账户模式，居民存款直接存于央行账户，形成央行与民众之间直接的资产负债关系，这样货币发行及信用属性又完全回归至中央银行。

对于普通民众而言，其可以在将货币资产存入银行账户以获得相应利息并承担银行可能发生破产而带来的损失，或者将货币资产存入更加安全的央行数字钱包中进行选择。而对于中央银行而言，这种货币发行机制可以使其拥有更大的利率政策空间，当然这种转换的代价是增加了金融运行机制的不确定性，如英格兰银行副行长本·布劳德本特认为，“中央银行的资产负债表可以对每个市场参与者（包括个人）开放，但可能会导致商业银行存款转移至中央银行，由此将产生多方影响”（Ben Broadbent，2016）。

（二）账户货币的中介性支付成本问题

在货币流通阶段，账户货币的支付是将货币由实物形态交换转为记账单元的增减，这个转变过程虽然规避了交易空间和时间的束缚，但整个支付信息流程需要大量的支付中介机构及金融基础设施参与运行，这本质上是增加了社会支付的运行成本。反过来，虽然现金交易存在交换媒介自身条件及交易场所和时间的限制，但现金交易本身仅是货币的实物交割，其交易的即时性是真正实现了“支付即结算”，也无需交易身份识别、交易者付款能力或信用额度确认、交易信息及单据报送等各种支付中介服务。随着技术的革新与支付市场的发展，这种中介机构的支付性成本需要一个进一步“脱媒”的演化过程。

首先，账户支付的身份认定需要第三方的中介机构进行认定。这种认定成本产生于账户开立环节的身份认证、账户使用环节中的身份验证，还产生于账户身份数据的更新维护及防范账户盗用的安全工作。数字货币依靠密码编写来使得每一个单位货币都具有独立的识别机制，就如同数字货币拥有了一个自身的“身份证号码”，可以自带“公钥与私钥”的身份识别验证工作，并通过诸如拜占庭容错机制等实现在公共网络条件下的“指令辩伪”，包括支付信息指令发出方的身份识别、指令发出方是否拥有交易数字货币的所有权，以及该数字货币是否被多次使用等，这些验证工作在传统的账户支付机制下，是需要一个或多个支付中介进行验证确认与信息交互才能完成，而在数字货币的支付机制则可通过其网络节点对新增交易信息的共识算法进行确认，从而实现了建立在数字化信任基础上不依赖特定中介的价值交换，并由此节省了支付中介的相应工作与成本。

其次，账户支付的账本交易需要中央化的中介机构进行数据库的数据登记和保存。在传统信息系统的安全方案中，数据库的安全防护依靠专用机房、专有网络和专业安全软件进行层层设防的访问控制，只有通过 API 等专用访问通道，并经身份认证、鉴权等安全流程验证后方能进行核心数据的访问与修正，虽然这些机制保证账户数据和交易记录的可信性，但相关维护成本均作为社会交易成本的一部分。而可作为数字货币底层技术的“区块链”可以分布式账本代替中心化账本。

根据英国金融行为监管局的定义，分布式账户可以视为一种技术模式方案，即实现对网络交易者活动的即时记载[①]。在提高账本数据更新效率方面，依靠点对点网络传输、加密技术以及共享数据库等技术发展，分布式账本技术实现交易活动与账户薄记的即时同步，这意味着数字货币的每次支付流转即同步发生全网记账和点对点的实时结算，也意味着传统的支付、清算和结算将同步完成，深刻改变了以账户为运行基础的传统支付清算运行机制。

而在交易数据安全方面，不同于传统的“中心报送”模式，网络节点（Nodes）相互之间就分布式账户中的交易记录进行全网比对验证，将验证后的区块信息并加注“时间戳”并入主区块链的共识账本之中，同时又会将数据信息反馈回每个网络节点的分布式账户之中，形成“区块+链”的记录模式，通过区块链中的“点对点通信交互”和“共识算法”使共识账本中交易信息不可篡改。在该模式下，账户功能演变为货币存储和权属的认证功能，其转账和支付以及账目登记等功能被转移至数字货币本身，从而降低账户中介在支付体系中的重要性作用。

再次，货币流通的线上与线下交互中介成本。当前网络支付的实质是将线下交易线上化，即在货币发行阶段仍需要大量的印刷纸币以适应线下交易的现金需求，而网络支付又将大量的线下货币现金兑换为电子形态的账户货币（无论是电子货币还是虚拟货币），并由账户在交易网络中以支付或转账方式完成交易，同时

[①] FCA. Discussion Paper on Distributed Ledger Technology. April, 2017, page 2.

网络支付账户剩余资金可以随时兑回线下货币。这样就形成了一种账户的功能分离，即网络账户强化了支付功能，银行账户保留了资金保管和结算功能，这种功能分离在一定程度上促进了支付效率的提升，但是从另一方面来说，将线下支付工具转换为线上支付工具本身也是一种效率损失。而在码基及生物特征为代表的端口型账户形态下,还需要因各支付机构账户形态不能直接识读，而出现的聚合服务中介，这种俗称“第四方支付”的聚合支付业态进一步丰富了支付中介的服务种类和商业形态，但在某种程度上增加了社会支付成本，或者说进一步增加了支付产业在交易规模的量级要求。

由上可见，当前信用货币的账户性支付机制需要各种类型的支付中介，围绕着账户支付机制的中介功能，支付中介可分为交易身份验证中介、交易数据登记与账本数据维护中介乃至网络线下货币线上化中介和不同账户形态聚合服务中介，这些支付中介相应地增加了货币流通的成本,限制了实际可行的最小交易规模。而人们对数字货币的诉求点之一就是希望借助其实现中介性支付成本的降低。

（三）货币账户化的价值数据安全与使用问题

在账户支付机制下，账户间交易需要信息流和资金流的体系内传输，因此价值数据与身份信息均需要存储于账户体系之中，但随之而来的是数据集中和数据隐私保护之间的矛盾已经成为社会关注的焦点。

2018 年 3 月，英国媒体“第四频道”曝光了英国商业运营的政治数据分析公司“剑桥分析（Cambridge Analytica)”的暗访视频。该公司声称该公司利用包括利用一款嵌入 Facebook 的软件获取用户数据，此事件反映出社交媒体可以通过设定人工智能推荐算法，制造恶意聊天机器人等 AI 技术，误导受众群体观点。同年，支付宝面在向其用户推出个性化的“2017 支付宝年账单”，但由于其在年度账单的首页设置了“我同意《芝麻服务协议》”这一选项，遭到社会公众对其滥用默认同意规则的批评，并引发就互联网金融数据获取，以及个人数据隐私保护等问题的广泛讨论。2020 年 5 月，脱口秀演员池子在其个人微博中声称，中信银行上海虹口支行在未经其本人授权允许，且无任何司法机关进行合法调查的情况下，擅自将其账户交易明细直接打印并交给原雇佣公司上海笑果文化传媒有限公司，并导致其本人银行账户冻结。按照银行规定程序，个人银行账户交易明细需要本人持有银行卡或有效证件到银行网点查询，但事实上，银行账户本身集中储存着账户人卡号、身份证等个人身份信息，在银行内部管理机制或信息数据系统存在缺陷的情况下，依然可以出现个人价值数据被恶意侵入的风险。

与此同时，账户对价值数据及个人信息的集中化管理，某种程度上模糊了账户数据资源究竟应归属于账户持有人还是账户管理机构。实质上，金融业界涉及到“开放共享”也好，“互联互通”也罢，纷繁多样的概念都离不开两个关键问题：第一，开放谁的

数据？第二，向谁开放？这两个问题本质上都是涉及数据资源的所属权和交易的问题，若与之相对应的就是个人数据信息的保护问题，这就需要进行客户的授权、技术上的脱媒处理以及监管政策的配套规范等支持；若与之相对应的是机构所属数据，那么就要涉及机构之间数据共享的平等性，或者说是数据交易的合理性，在市场环境下，没有任何机构会将自己所属的资源共享他人，而不求索取，这是违背市场规律的，也无法实现政策的可持续。

以银行间账户合作机制为例，账户分类政策允许银行II类和III类账户可在绑定其他银行的Ⅰ类账户基础上开立，这原本将有助于中小银行的账户开立，更加便利低线城市及偏远地区的普惠金融服务，但从具体实践来看，大型商业银行并不情愿将账户资源“无偿共享”至中小银行，对于五要素中的Ⅰ类账户回执采取消极态度，银行间相互认证机制逐渐演绎成“分级认证”：由工、农、中、建、交、邮储六大行签订账户管理合作协议，允许协议内银行账户相互认证，中信、招商等 12 家股份制银行成立“商业银行网络金融联盟”，建立同类银行相互认证机制，这种大型银行与中小型银行的对立，与此前银行间通兑通存难以推行的情形如出一辙。由此，若围绕数据所有权及共享机制的利益分配问题不能得到有效解决，包括“开放银行”的数据价值共享理念很可能无法实现其设计的初衷。

在这种情况下，人们对数字货币的期许很大程度上也与追求数据和隐私安全密不可分。例如，比特币被中本聪构造出来，就

是为了用它在互联网上模拟一种类似现金的支付系统，其匿名性是支付宝、微信等支付工具提供不了的。而由一个可信任的央行发行的数字货币尽管不能达到比特币这样的匿名性，但也可在很大程度上避免数据泄露的问题。

四、供给端的变革动力

尽管我们认为在需求端弥补账户货币存在的缺陷或不足是推动数字货币产生和发展的主要变革动力，但是供给端的变革动力也是需详加剖析的。从供给侧角度来看，促进数字货币产生和发展的因素大体可分为三类：即以网络信息技术和加密技术为代表的技术创新、以打破原有格局和追求秩序变革为动机的各类行为主体和以变革性技术创新与风险投资为特征的商业及金融环境。

首先，从底层技术的创新应用来看，加密技术的重大突破成为数字货币发展的主要因素。一般来说，对价值信息的传输存在两种思路。

第一种思路是对价值信息的传输路径进行安全防护，即在信息指令发出、接收以及传输网络等节点采用专用设备和专属网络，如银行网点的柜台交易、ATM 机交易、银行卡交易等属于基于该理念的支付行为，但是这种支付方式投入大、交易覆盖率有限，社会支付的成本较高；

第二种思路是对价值信息自身进行加密保护，该理念的价值意义在于加密价值信息可以在通用设备及公共网络中进行传输，省去了大量的硬件投入和维护工作，也减少对交易双方的身份认

定、交易信息真实性的账户 管理及维护工作，然而其也面临信息加密安全性和开放性的两难问题。

所谓安全性，就是指要有足够的安全强度，信息不能被窃取和篡改。所谓开放性，就是要求被最广泛的大众所接受和日常使用。在传统对称密码体系中，由于加密解密共用一把钥匙，因此很难在大规模分发密钥的同时保持足够的安全强度。

1976 年，怀特福德·迪菲（Whitefield Diffie）和马丁·赫尔曼（Martin Hellman）发表了一篇题为“密码学的新方向”（New Direction in Cryptography）的论文，提出建立非对称密码体系设想，即将原来对称密码体系下的一把钥匙一分为二，一个是加密密钥，被用来加密信息，加密密钥可以公开，也称为公钥；另一个是解密密钥，被用来从密文中恢复明文，由个人维持其机密性，也称为私钥。从私钥可以推导出公钥，但从公钥很难逆推出私钥。1978 年，罗纳德·李维斯特（Ronald Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）基于该设想首次提出非对称加密算法（由三位发明人的姓氏字母合称 RSA 算法），由于公钥可在服务器进行全网公开，价值信息发出方可用接收方的公钥加密，并用其私钥签名，而接收方可以用发出方的公钥验证其身份信息，并用自身的私钥解密阅读报文信息，这样既保证了价值信息传递的安全性，也解决了价值信息发出方的身份认证问题。

另一个技术突破在于区块链为代表的分布式账本技术，其解

决的是在公共网络系统中，价值信息传输后登记与存储问题，反映为货币流通中的双重花费问题（简称“双花问题”）。密码学者发现哈希函数（也称“安全散列函数”）具有将给定输入信息迅速收敛为固定输出字符信息，且一旦给定输入信息发生变化，输出字符即可变更，且不可回溯至原输入信息，因此可以凭借哈希函数的特性快速生成随机数对信息包进行序列标注，以防止信息的复制滥用。而对于哈希函数的验证模式，则存在集中式和分布式两种路径。

1983 年，戴维·乔姆（David Chaum）发表题为《用于不可追踪的支付系统的盲签名》,提出了一种基于 RSA 算法的新密码协议——盲签名，即利用盲签名构建一个具备匿名性和不可追踪性的电子现金系统，同时将随机配序产生的唯一序列号保证数字现金的唯一性。但乔姆对随机配序的序列号作为 E-Cash，并以银行的数据库进行验证和比对，这样势必影响加密货币的开放性，因为随着交易量的上升，数据库的储存容量与比对验证都显得十分困难。

基于这个难题，2008 年，中本聪发表其经典论文《比特币：一种点对点的电子现金系统》,将中心化的验证方式改变为去中心化的点对点交易模式，即将集中性的薄记方式改为分布式薄记方式，即在账户支付信息交互的结构化设计中，推出分布式账户（Distributed Ledger Technology）技术对原有中心化账户结构进行替代。通过这种互相验证的公开记账系统，解决了数字货币

的开放性问题（Nakamoto，2008）。

其次，推进数字货币创新及应用的行为主体可分为创新个体精英行为和意图打破原有金融秩序的国家行为。从创新个体及团队层面来看，以乔布斯、扎克伯格、埃隆·马斯克等人为代表的美国硅谷精英赋予了当前金融科技特殊的创新理念。他们大多在经历了“硅谷劫难”和“华尔街危机”后，对美国的科技创新和金融投资进行了深刻的反思与批判，其崇尚从“从 0 到 1”的技术变革，强调技术的“颠覆性”特征。

如彼得·蒂尔在其著作《从 0 到 1—开启商业与未来的秘密》，认为照搬已取得成就的经验，只是一种水平进步（可理解为延续性技术），这种进步很容易想象，并可以通过全球化推广至世界各地，探索新的道路则被视为垂直进步（可理解为变革性技术），这种从 0 到 1 的进步用科技的发展来代表，相比于全球化为全球带来的水平性进步而言，科技创新所带来的垂直性进步更具有影响力。

此外，在技术价值观方面，部分数字货币及金融科技创新者常自诩为社会现行规则中“逆行者”，强调“科技赋权”，认为解决公共物品的问题可以通过社区性的互助而非依靠中央集权制度的权威体系，因此，部分技术创新者有意将其自身理念融于到创新技术之中，希望体现对现行运行体制的“颠覆性”。如发源于 70 年代标榜个人意识的朋克（Punk）运动影响了当时的密码学年轻学者，其希望设计不受垄断性机构控制的自由代码，结束国家对

货币和金融资源的绝对垄断，再如 Paypal 支付产品在设立初期，声称其产品开发的目的就在于要“颠覆世界金融体系”，即为除美国外的其他国家居民开设离岸账户，以使其能够绕开国家的资本管控机制，“把手中的货币换成像美元这样稳定的货币”，并为此设置了“统治世界指数（World Domination Index)”，而脸书公司的“Libra”项目依然招募了 Paypal 创始人彼得·蒂尔，原总裁大卫·马库斯以及网景创始人马克·安德森等人，由此可以看出数字货币与第三方支付在其人员精神理念上的延续性。

除部分科技精英及创新型企业致力于推动包括数字货币在内创新性产品之外，部分主权国家也纷纷开展数字货币的研发工作。一类是以欧美国家中央银行为代表，其逐渐意识到只有提前评估数字货币对货币及政策金融体系影响，提前布局官方数字货币发行，才能保障法定货币的市场地位。

如英格兰银行于 2016 年 8 月发表工作论文《中央银行发行数字货币的宏观经济学》，首次从理论上探讨了数字货币与宏观经济间的影响关系，随后其他欧美发达国家央行也纷纷启动数字货币的研究，乃至其发行与流通的设计与测试工作。

总体来讲，欧美国家央行期望数字货币的发行可以结合现金货币和账户货币两种货币形态的优点，有效降低支付体系交易成本，规避账户体系“大而不倒”、“密而不倒”的系统性金融风险，同时又尽可能地保证其对货币市场的干预能力以及对金融体系的监控与监管手段。

另一类国家则是受到或面临美国制裁的主权国家。近年来，美国越来越多的实施针对非国家实体的清单制裁方式（包括特别制定国民和人员封锁清单，即 SDN 清单、行业制裁识别清单、海外逃避制裁者清单、外国金融机构第 561 条款清单等），如根据外国金融机构第 561 条款第 203 款规定，美国财政部一旦发现外国金融机构蓄意地与伊朗中央银行或特定金融机构的任何金融交易或提供相关便利，即可对该金融机构进行制裁，这种针对非美国主体实施的二级制裁（Secondary Sanction）是典型的长臂管辖行为[①]，为而制裁的主要方式为禁止美国金融机构为特定外国金融机构开立或维持代理账户或通汇账户，或对其已在美国开立的代理行账户或通汇账户进行限制。

由于这种所谓智慧制裁（Smart Sanction）的实施抓手正是通过美元结算账户体系或与美国金融机构相关联的账户体系进行，因此，诸如伊朗、委内瑞拉、俄罗斯等国因受制于美国的金融霸权，希望开发并利用数字货币中“去账户”的管理模式，以及“点对点”的跨境支付功能，绕开美元结算账户系统对特定账户资产和相关汇路通道的冻结制裁。

第三，创新型企业或行业外企业在战略经营理念与商业运行模式与行业内成熟型企业不同。创新型企业在发展理念上对传统西方经济学者追求的“市场均衡”不屑一顾，认为供需双方在价

[①] 按照是否对被制裁对象具备管辖权，美国财政部以美国实体和非美国实体将制裁分为两种形式，针对美国实体采取一级制裁（Primary Sanctions），针对非美国实体实施二级制裁（Secondary Sanctions）。

格上的均衡意味着产品的同质化，产品价格由市场决定而非企业则失去定价权，这并不是自由市场竞争所追求的目标，自由竞争就是应鼓励企业技术创新，使其能够依托自身独特的技术优势从而在若干利基市场上获得超额的利润。

因此，创新型企业并不像行业内成熟企业一样紧盯竞争对手的市场策略，而是倾向采用变革性技术，率先在边缘市场及长尾客户中寻求响应，如谷歌公司虽然在美国搜索引擎市场上占据主导性地位，但不惜降低发展效率将业务扩展至自动驾驶汽车、安卓手机等多个领域，脸书公司致力于将关注点放在自身产品技术的先进性以及是否能够响应甚至是引领市场的客户需求。

创新型企业的另一个运行特征是其经营模式能够在全球范围内迅速扩散，一旦金融科技创新产品及其商业模式被一国市场确认，随即被迅速推广至其他国家。如德国的扎姆韦尔兄弟就在美国市场分析互联网创意公司，并在欧洲市场成功山寨对标企业，如德国版 YouTube（My Video）、推特（Frazr）、脸书（StudiVZ）以及爱彼迎(Wimdu)。由于金融科技创新及相关产品存在快速“周期迭代”特征与“网络效应”，创新企业的技术扩散追求“市场优先”原则，而非“利润优先”原则，如领英创始人里德·霍夫曼在《闪电式扩张》中指出，科技创新企业应如同二战德军实施的“闪电战”一样，即便在不确定环境下，也应优先考虑市场占有速度，而相对放弃实施效率与利润率等其他规模化企业的传统目标。与此同时，创新型企业当前深受科技风险投资的青睐，可以

充分利用资本市场募集资金，研发技术上更加的复杂交易产品和交易系统。

据毕马威统计，2021 年，全球金融科技投资交易再创新高，总交易数量达到 5684 宗，投资总额也达到 2100 亿美元，打破了 2018 年以来的记录。支付科技、保险科技、监管科技、网络安全技术、财富科技、区块链、加密货币等金融科技细分领域的企业成为资本扶持的重点。在这种新型商业创新理念及投资环境下，对变革性技术的狂热偏好促进了包括数字货币技术在内的金融科技迅速发展，并即时向全世界各国扩展相关创新模式，以期获得超额利润回报。

研究团队主要成员

杨涛	支付清算研究中心	主任	研究员
程炼	支付清算研究中心	副主任	研究员
周莉萍	支付清算研究中心	秘书长	研究员
董昀	支付清算研究中心	副秘书长	副研究员
李鑫	支付清算研究中心	特约研究员	
经邦	支付清算研究中心	特约研究员	
宗涛	支付清算研究中心	特约研究员	
赵鹞	支付清算研究中心	特约研究员	

主 办： 中国社会科学院金融研究所支付清算研究中心

主 编： 杨 涛 （ytifb@cass.org.cn）

副主编：程 炼 （clifb@cass.org.cn）

周莉萍（zlpifb@cass.org.cn）

声 明

《支付清算评论》为内部交流刊物，其中的文章除非经特别注明，均由中国社科院金融所支付清算研究中心（以下简称“研究中心”）的研究团队完成，研究报告中的观点、内容、结论仅供参考，研究中心不承担任何单位或个人因使用本信息材料而产生的任何责任。本刊物的文字内容归研究中心所有，任何单位及个人未经许可，不得擅自转载使用。

研究中心是由中国社会科学院批准设立的所级非实体性研究单位，由中国社会科学院金融研究所作为主管单位，专门从事支付清算理论、政策、行业、技术等方面的重大问题研究。2015 年 5 月 27 日，“国家金融与发展实验室”经中国社会科学院院务会批准设立。同年 11 月 10 日，中共中央全面深化改革领导小组第十八次会议批准国家金融与发展实验室为国家首批高端智库。根据中央与中国社会科学院的安排，研究中心同时被整合成为实验室的下属研究机构。

研究中心的名誉理事长、学术委员会主席为中国社科院原副院长、国家金融与发展实验室理事长李扬研究员，理事长为中国社科院金融所原所长王国刚研究员，主任为中国社科院金融所杨涛研究员。

地址：北京市东城区王府井大街 27 号综合楼 5-7 层 中国社会科学院金融研究所
邮编：100710
网址：www.rcps.org.cn

联系人：齐孟华
电话: 010-65265139
手机：13466582048
E-mail: qmhifb@cass.org.cn