Introduction
周子衡
阿里巴巴研究院顾问、中国社科院金融研究所副研究员

数字货币的属性与供需分析

文/周子衡　本文编辑/丁开艳

网络数字世界为现实的经济社会提供了一个纯粹数理环境，数字货币诞生于此。如今，伴随网络经济快速发展，数字货币受到越来越多的关注。本文探究了数字货币的身份属性、账户属性，并思考数字货币未来存在的各种可能性。

打个比方，在数字网络环境中，每一数字货币好比是一辆机动车，牌号唯一，相互独立，无牌或冒牌的网络数字机动车造不出来，进不了系统，上不了“路”，这就不会出现假钞、伪钞。

网络数字世界为现实的经济社会提供了这样一个纯粹数理环境，数字货币恰恰于此诞生了，货币自身演变的规律提供了探究数字货币独特的视角。

解读数字货币的视角

现代货币体系的稳健运行须有三项基本保障：控制货币供给、反洗钱、打击伪钞。完成三大保障耗费了巨大的资源，付出了巨额成本或代价。然而，这一货币体系并不完美：货币运行中的隐患始终存在，货币犯罪依然猖獗，货币危机乃至金融危机亦时有发生。那么，“完美”的、理想的货币图景又是什么样子呢？

这里列举但不限于以下四项标准：每一货币、任一账户都不会出现纰漏，任何违规自始不会发生；由此没有监管活动与监管者，也没有欺诈与隐瞒的发生；货币总量是确定而充分的，不需要、也不存在“货币创造”；由此不需要总量调控，更不存在调控者。如此“完美”，简直是痴人说梦。然而，这个“完美”的货币图景，存在着数学意义上的解决方案，换言之，在纯粹的数理环境下，这一理想能够实现。问题是，经济社会的现实环境与所谓的“纯粹数理环境”又相距有多远呢？

网络数字世界为现实的经济社会提供了这样一个纯粹数理环境，并且，数字货币恰恰于此诞生了，且完备了前述四项标准。解读数字货币的途径有很多，从货币自身演进的视角来，笔者认为主要有四方面：数字货币具有不可变更的身份属性；数字货币不能脱离账户而存在；数字货币的支付与记账完成；数字货币的供给基于货币共识，亦即所谓“基础协议”；货币数字的需求与政府部门。

数字货币的身份属性：每一数字货币都永久绑定一组“身份编码”

数字货币依靠密码编写来给予每一货币独立而唯一的身份标识，以牢固确定其身份属性。形象地说，数字货币一诞生就有了一组终生不变的身份证号码。

众所周知，每一张纸钞是有编码的，印刷发行当局应用该编码来管理与规划货币发行，有关当局通过监察纸钞编码来查证伪钞或其他犯罪线索。可以说，纸钞是有明确的身份标识的，一钞一号，这就是其“身份性”。现实中通过号码防伪的成本太高，更难以杜绝盗号、冒号，因此，发行当局被迫求助于身份之外的一系列防伪技术识别手段，来确保真实性。可以说，运行中的纸钞的“真实性”与“身份性”分离了，且“真实性”超过了“身份性”，出现了身份的混同。

通过密码编写，任一数字货币获得了一组编码，这组编码即是此一数字货币。换言之，在数字网络环境中，数字货币本身就是其身份识别编码。密码编写依循其规律，大体而

言，密码编写完成意味着，一定数量组的编码就发生了。

数字货币重拾每一货币的身份性，将身份识别作为唯一准则。从这一点看，数字货币与纸钞并无本质的不同，都是一组编码，且数字货币的存在与流转完全依靠其身份编码，始终不会发生身份混同。打个比方，在数字网络环境中，每一数字货币好比是一辆机动车，牌号唯一，相互独立，无牌或冒牌的网络数字机动车造不出来，进不了系统，上不了“路”。这就不会出现假钞、伪钞。

数字货币的账户属性：数字货币总是绑定在某一账户内

密码编写完成了，就好比造就了一个密码锁。这个密码锁有确定数量的若干个解，每个解就是一个数字货币。这就需要按照一定的程式去寻找出这些解。有如，比特币的“挖矿”，就是在求解开锁，每找到一个解（即比特币），就存放入挖矿者的账户内；同时，向所有的账户“宣告”，并得到确认，该比特币已属于该账户所有。这就是说，数字货币的身份属性与账户属性自始就是绑定在一起的。打个比方说，每一数字一诞生就有了终生不变的“身份证”，且成了永久的“有房户”。

账户所有人通过秘钥来开启该账户，如果忘记了，也就丢了钥匙，那么，就打不开账户，无法动用账户内的数字货币了，但这并不意味着账户内的数字货币消失。只有同一数字货币系统内的账户才能接收本系统发行的数字货币，数字货币无法脱离数字货币自身系统的账户体系而存在。这就是说，数字货币不会自行消失，一经拥有便永不会丢失。简言之，任一数字货币总是归属于特定的账户，它只“活”在账户中。这也就是其账户属性。

数字货币的使用：支付与记账同步

各类电子货币支付被确认，有一个时间上的延迟，这个延迟体现的是支付地点与记账地点之间的空间距离。虽然伴随着技术进步，这个距离在大多数情况下已经不重要，延迟的时间甚或可以忽略不计，但是，程序上而言，电子货币并非是在支付的同时发生记账的。事实上，电子货币支付只是发出了记账指令，支付确认只是收到记账指令的确认，记账还是发生在后台系统中。这表明，所谓的电子货币并不是同步记账货币，它也不是账户本身，而只是开启账户进而发出记账指令的“钥匙”而已。严格说，电子货币的账簿与其本身是脱离的，其账簿归属于银行后台系统。可见，电子货币支付活动是通过“分步记账”完成的。

数字货币的每一流转，都是被加盖了时间戳，且被全网记录。它不具备、不需要，以致根本排斥记账中心，更不存在后台记账的情况，支付的同时即发生与完成记账。数字货币的身份属性和账户属性是紧密绑定在一起的，任一支付，即同步发生账户变更，亦即同步发生记账。这是数字货币系统本身所设定的。可见，与电子货币不同，数字货币的支付活动是通过“同步记账”完成的。

“同步记账”是相对于电子货币的“分步记账”而言的，事实上，同步记账不仅是通过记账而发生支付，而且这一记账亦是通过整个数字货币系统完成的，之所谓全网记账。正是

数字货币是在一个网络设施与数字技术支持下近乎纯粹的数理环境中发生与运行的，它与银行货币本质不同的是，数字货币没有假币，也没有货币创造，数字货币是一块网上运行、数字化生存的“净土”。

基于此，在所有货币种类或形态中，数字货币不仅支付效率最高，而且也是最为安全的支付工具。

数字货币的供给：作为货币共识的“基础协议”

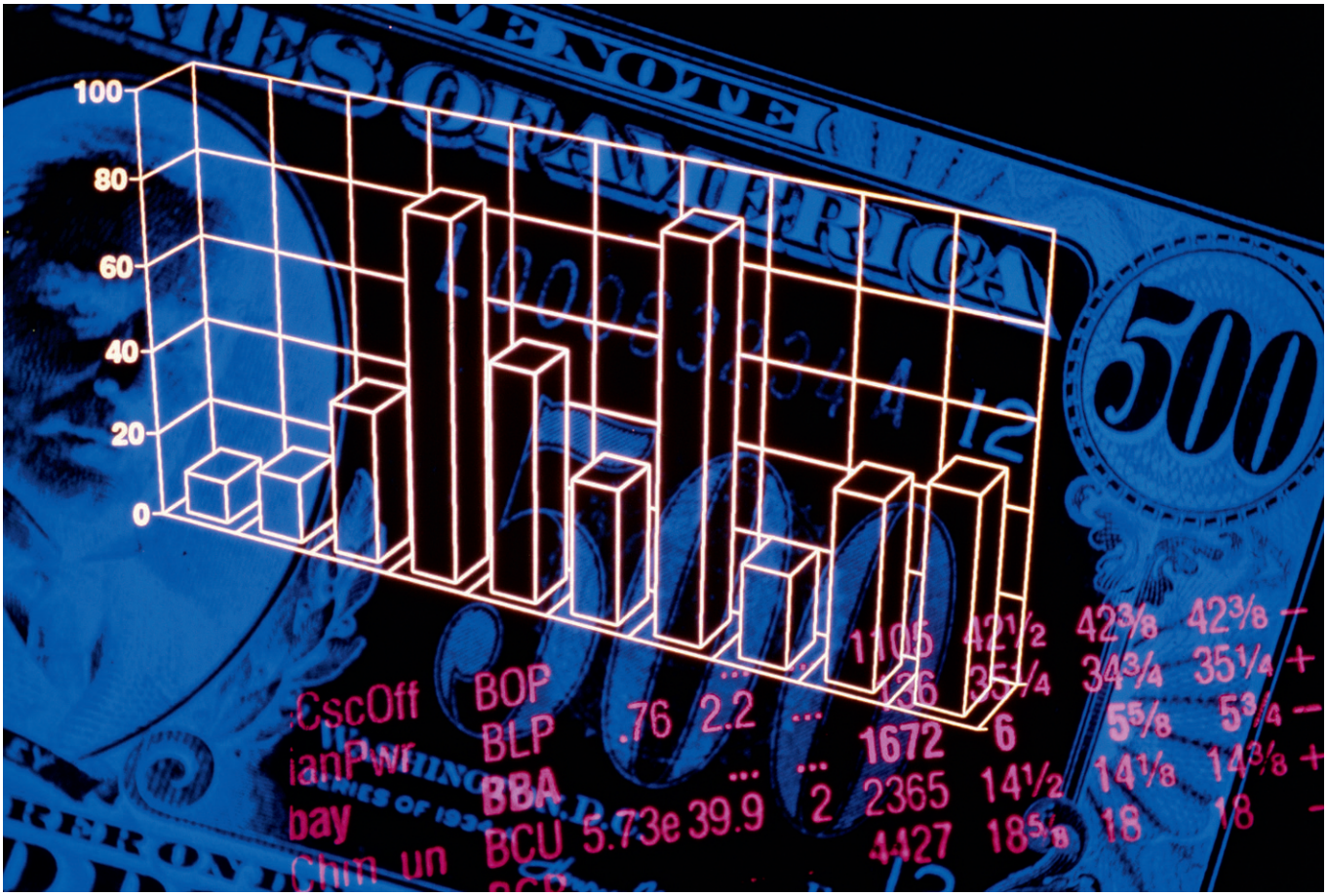
货币历史表明，没有货币共识，就不会有货币，也无所谓货币供给。数字货币的货币供给，是一个纯粹的数学解决方案，在数理环境中，货币共识作为基础协议，得到完全的遵守，没有例外。这就决定了数字货币的效率性和安全性。网络数字世界，使数字货币供给成为现实。

数字货币有许多种类，大同而小异。在技术上，数字货币各有其数学解决方案，借助于密码技术及区块链技术；在逻辑上，数字货币基于“共识”。这个共识，也可被称为基础协议，亦即数学上的解决方案。认可这一数学解决方案或“基础协议”，就成为数字货币“共识”的一分子，亦即加入该数字货币系统。

货币学派大师弗里德曼在其所著《货币的祸害》一书中开篇讲到耶普岛的石头币：在太平洋的耶普岛上，人们使用巨大的石块作为货币，并在各岛间用船来运送石币。一次发

生了沉船，石币坠入海底，无法打捞出海。岛上的长老们聚议决定，石币依然有效，这便有一个新的“基础协议”。这个事件意义十分重大，表明石币转化为记账货币，而记账货币基于一种货币共识。时至今日，美国纽约美联储地下金库中的金块分属世界各地不同的所有人，金块变换主人并不需要搬运，只要完成记账即可。这就说明，货币与账户的密切关系，货币的身份属性和账户属性，决定了记账活动，而这个体系是参与人的“共识”决定的。货币“共识”是一个潜在的协议形态，它并不是以强制力为保障的。在津巴布韦和朝鲜所发生的货币失败，并不表明两个货币当局缺乏足够的强制力。失败的中心事实是，货币发行者没有能够与接受者形成必要的货币共识。在20世纪初叶，作为大英帝国的殖民地的非洲埃塞俄比亚，依然流通着哈布斯堡王朝的特雷莎银币，殖民者想转变为英镑不成功，进而用更高质量的银币来替代特雷莎银币，同样归于失败。于是，英国人只有按照当地意愿来发行仿制的特雷莎银币，问题才最终缓解。要知道，哈布斯堡王朝早已不在，特雷莎皇后也早已作古，可是要替换特雷莎银币，仍然需要殖民者与当地达成货币共识，即便这个共识是颜面扫地的妥协。同样的故事发生在英殖民地香港，1866年英国人在港开厂铸币，仅仅两年，铸币厂倒闭，殖民者也难以改变香港人白银硬币的共识。

数字货币（digital currency）是将货币的身份属性与账户属性绑定在一起，为每一货币的每次流转加盖时间戳，并在全网记录。是的，数字货币存在于网络数字环境中，它无需实物，也不是实物，它只是一套记账系统。可以说，数字货币是在一个网络设施与数字技术支持下近乎纯粹的数理环境中发生与运行的，它与银行货币本质不同的是，数字货币没有假币，也没有货币创造。数字货币是一



块网上运行、数字化生存的“净土”，它的发端自有其货币共识——基础协议。不同种类的数字货币更像是一个个俱乐部，诸如，比特币（Bitcoin）、莱特币（Litecoin）、狗币（Dogecoin）、瑞波币（Ripple）、未来币（NXT）和点点币（Peercoin）等等。任何人如认可俱乐部的章程——基础协议——便可加入成为会员，就拥有相应的账户，基础协议也保证了数字货币的身份属性、账户规范和记账规则。未来势将涌现出更多的数字货币（俱乐部），拥有更多更为广泛的数字货币持有者（会员）。

对于数字货币的基础协议，一旦加入，便无从违反，或可退出。一个不被违反的基础协议或货币共识，效率最高，也最安全。现实的社会经济体系复杂动荡，即便有一系列的外部保障也完全无法达成并遵守如此的货币共识。正如前文所言，这就是在一个纯粹的数理环境下实现的，是一个标准的数学解决方案。可以说，数字货币的“共识”或“基础协议”，反映出数字货币供给的基本特征。

数字货币的需求：关注政府部门的角色

数字货币原本是“小众货币”，伴随网络经济快速发展，数字货币开始受到关注，并引发更多人的兴趣，开始为整个经济社会所发现与重视，也引发了许多争论乃至对立。放弃对于数字货币的立场或态度不谈，数字货币的需求究竟来自何方？需求将有多大？这些问题是非常值得进一步观察与深入思考的。

现而今，数字货币的使用范围不断拓展，应用场景日趋多样化。然而，在进入一般商品流通和服务贸易中的问题上，数字货币往往受到强力的排斥。一种颇为强势的意见认为，数字货币作为商品没有问题，但是不能作为货币。其含义是，可以用一系列的主权货币来购买数字货币，但是不能用数字货币来直接购买商品与服务。全球几乎每周都有关于数字货币的应用与认可获得新进展的消息，但是，数字货币的应用仍然受到限制。这就决定了，数字货币的需求势能难以释放出来，也便难以转化为对先行货币体系形成冲击的动能。

拥有完美的机制和无限可能的未来，现实却步步受阻。这就决定了，对于数字货币的投资或投机需求猛增，数字货币发行的特征更加剧了这一态势。因此，先行多数数字货币的需求来源是投资或投机需求，甚或一些数字货币的拓展主要依靠投资或投机需求。这一方面为数字货币发展提供了动能，但是另一方面也使数字货币价格虚高，阻碍数字货币的推广。

相对私人需求绝对性主导，企业部门、政府部门对于数字货币的开放度严重不足。不过，事情正在其变化。在比特币问题上，各主权国家的货币当局表态花样百出，立场左右互现。切开数字货币的肌肉，很容易发现里面的技术支撑骨架——区块链技术和加密技术。近一年多来，各方对于数字货币的立场或态度可谓是全面回暖。其中，最为醒目的是，区块链技术普遍受到关注甚或追捧。无论就企业与市场方面，还是监管当局而言，区块链技术均能大幅提高效率与安全，降低风险与资源成本。更为重要的是，这一革命性的技术的普遍应用，将极大地提升与拉平不同金融市场间的效率差距，亦将极大地提升监管效能、水平，特别是使落后者迎头赶上。

对于政府部门而言，数字货币像一柄双刃剑：一方面任其发展、渗透，乃至蔓延，终将对主权货币或法币造成过大压力，足以掣肘中央银行的货币权能，有力杯葛政策当局的经济意志，并对金融体系的稳定产生压力；另一方面激励其发展有助于全面提升监管效能与水平，革新金融市场的效率，提升整体金融安全水平，减少金融监管与运行的巨大成本代价和效率损失，从而也有助于最终维系与确保金融稳定。不过，利弊得失的精算正在逐步让位于政策取舍与时机的把握。

货币演进的历史表明，政府部门往往是新货币共识的最后妥协者与加入者，但往往也是货币变革的最终决定性力量。