A GLIMPSE OF DIGITAL MONEY

数字货币初探

姚 前 / 著

中国金融出版社

数字货币初探

姚 前 著

中国金融出版社

责任编辑：陈　翎
责任校对：孙　蕊
责任印制：丁淮宾

图书在版编目（CIP）数据

数字货币初探（Shuzi Huobi Chutan）/姚前著. —北京：中国金融出版社，2018.5
ISBN 978-7-5049-9415-8

Ⅰ.①数…　Ⅱ.①姚…　Ⅲ.①电子货币—研究　Ⅳ.①F830.46

中国版本图书馆 CIP 数据核字（2018）第 019882 号

出版发行　中国金融出版社
社址　北京市丰台区益泽路 2 号
市场开发部　（010）63266347，63805472，63439533（传真）
网上书店　http://www.chinafph.com
（010）63286832，63365686（传真）
读者服务部　（010）66070833，62568380
邮编　100071
经销　新华书店
印刷　北京市松源印刷有限公司
尺寸　169 毫米×239 毫米
印张　25.5
字数　340 千
版次　2018 年 5 月第 1 版
印次　2018 年 5 月第 1 次印刷
定价　65.00 元
ISBN 978-7-5049-9415-8
如出现印装错误本社负责调换　联系电话（010）63263947

序　言

几年前，当我们开始做数字货币研究的时候，这一领域既冷门，又边缘，不少人都质疑此项研究的必要性。这项工作的展开不能不归功于周小川博士的敏锐洞察力和学术前瞻性。这两年，随着比特币价格的暴涨暴跌，人们开始纷纷关注这一新兴事物。作为一个研究者，尽管我认为比特币还只是一种准私人数字货币，但我对其代表的数字货币技术的未来满怀憧憬！

应该说，有很多人是因为比特币而知道的数字货币。实际上，远在比特币之前，数字货币就是密码学的一个研究分支。自20世纪70年代以来，密码学界一直有一个梦想，我们手里拿的实物现金能不能数字化以后，通过数字加密技术，像发一个邮件一样，直接从某一个数字身份人转移到另外一个数字身份人的名下？就这么一个问题，很简单但也很复杂，引起了众多学者的兴趣，开创性的人物是David Chaum。1982年，他提出了一种具备匿名性、不可追踪性的电子现金系统，作为最早能够落地的试验系统，得到了学术界的高度认可。1994年Bruce Schneier的集大成之作 *Applied Cryptography*：*Protocols*，*Algorithms*，*and Source Code in C*，就专设一节，探讨David Chaum的数字现金协议[①]。

到2008年，一位化名Nakamoto的神秘人物提出了比特币的构想。数字货币的发烧友们狂喜地发现，去中心化的数字货币梦想竟也可以大规模试验了。这就是我们目前看到的席卷全球的比特币试验。客观而言，这个试验极具争议，有人对其背后的技术啧啧称叹，有人攻击它是诈骗工具，有人认为其堪比黄金，

① Bruce Schneier. 应用密码学：协议、算法与C源程序［M］. 吴世忠等译. 北京：机械工业出版社，2000：98－104.

也有人认为它一钱不值。一些知名人士，比如许多诺贝尔经济学奖获得者，也发表了自己的观点。“天下熙熙，皆为利来；天下攘攘，皆为利往”，众说纷纭间，与传统意义上的商品、资产、支付工具、货币等均有所不同的比特币以其丰厚的回报，吸引了全球投资者的眼球。

想要评价它，我们必须回到中本聪的经典论文《比特币——一种点对点的电子现金系统》。其中有两个关键词：“点对点”和“电子现金系统”。“点对点”的特性，使我们想起了实物货币，因为它就具有“点对点”这一优越的支付特性，只是其支付功能逐步被电子支付工具所蚕食。时至今日，“无现金社会”喧嚣尘上，似乎实物现金已无容身之地。果真如此吗？事实上主要经济体的实物现金投放和使用是在增加而不是减少①。所以实物现金的未来究竟如何，恐怕现在还不能妄下结论。

也许从哲学角度分析有助于理解这个问题。按照马克思主义辩证法，一样事物从自然产生到消亡，并不是简单的消失，而是有一个推陈出新，此乃“否定之否定”。货币亦是如此。假使实物现金在长期的历史进程中要消亡的话（当然这一点还有很大争议），这个“否定之否定”应该是什么？个人认为，那就是“点对点＋电子支付系统”。也就是说，从实物现金的角度看，需要“＋电子支付系统”；而从银行存款转账、第三方支付等电子支付工具的角度看，则需要“＋点对点”。按目前电子支付系统的发展势头，无论“无现金社会”实现与否，电子支付将实物现金的特性融合进来，是显见的趋势。所以个人以为，所谓的数字货币应该是电子货币和实物现金的一体化。这个一体化如果动态地去理解可能会更好，现在数字货币的定义还是存在争议的，我理解这个事情不要把它看成一个静止的状态。数字货币一定与货币的数字化进程紧密相关，在这个进程中，货币的数字化实际上是一个非常动态的、不断演进的东西，有些属性可能我们看得很清楚，还有一些属性很可能现在还看不清，还需要完全展开，需要观察和研究。这个观察和研究，如何结合法定数字货币的设计，成为我们

① Cash is Still King in the Digital Era [EB/OL]. http://money.cnn.com/2017/11/20/news/economy/cash-circulation-payment/index.html. 2017.

现在工作的重点。

很显然，实物货币向数字货币演进的意义在于，实物货币的支付功能优化了，可以在多种交易介质和渠道上完成支付，具有良好的普适性和泛在性。电子支付工具向数字货币演进的意义则在于，它能吸收实物货币“点对点”支付和匿名性的特性，将支付权利真正地赋予用户自身。在一定程度上，第三方支付的出现破除了用户对银行账户的依赖以及被施予的约束（如需到银行物理网点和 ATM 办理业务、一层层烦琐的业务程序等），有效释放了用户的支付主动性和能动性，降低了支付交易成本。但这还远远不够，账户是否可以透明？向谁透明？透明到什么程度？数字货币是否可被追踪？这些理应都由用户自主掌控。

或许有人会说，既然数字货币是实物货币和电子支付工具的发展方向，那么是否就意味着比特币终将胜出，笑到最后？也许一些持“货币非国家化”观念的自由主义者会这么认为。但是，许多国际组织和政府部门却倾向于将比特币定位成虚拟货币。为什么叫虚拟货币？因为它背后没有资产支撑，许多人（包括多位诺贝尔经济学奖获得者）认为它是没有前景的，尽管它的暴涨掀起了一股庞大的浪潮。“比特币也许失败，问题是这里头有钱可赚”，这句话道尽了很多人对“比特币”们的真实心态。比特币价格涨到什么程度才算合理？其暴涨究竟有多少泡沫？这是仁者见仁，智者见智的问题，作为研究者而不是投机客，追问“比特币”们的真正价值所在才是问题的关键。

回顾加密货币的研究历程，如果说 David Chaum 模式的数字货币是基于“银行—个人—商家”三方模式来设计的，那么比特币模式的数字货币则由原来的三方模式，变成了点对点的两方交易模式。这当然是一个范式的飞跃，但这两个模式都没有考虑中央银行的角色。David Chaum 只是探讨了匿名化现金的实现机制，根本没有涉及中央银行。比特币所谓的挖矿发行，煞有介事，实质上是把记账权、铸币权和发行权混为一谈，央行的角色因此消解。实际上，他们更多的是在研究数字化技术本身，但货币作为一般等价物，显然不只是（数字）铸币技术的问题，其背后的价值支撑才是关键。纵观各种货币形态均有价值锚定。商品货币、金属货币的价值锚定来源于物品本身的内在价值。金本位制度

下，各国法定货币以黄金为价值锚定。布雷顿森林体系崩溃以后，各国法定货币虽不再与黄金挂钩，但是以主权信用为价值担保。全球那么多的货币，根本的区别在于背后的价值支撑而不是铸币技术。相信现有的数千种加密货币，在追求极客技术的同时，也会逐步认识到这一点：当前的经济社会是一个高度发达的信用经济，货币发行和管理功能有缺陷的“比特币”们实难担当大任，核心问题在于这类“可转让数字资产”很难构建自身的价值支撑体系。

所以，必须把目前虚拟货币缺乏价值支撑这一根本性的缺陷给矫正过来。技术固然可以向典型的虚拟货币、加密货币取经，但人类社会长期形成的货币的本质内涵，理应是数字货币发行的基石。从这个意义上说，虚拟货币的未来得有一个“去虚拟”的过程，一个可能的变化是在前述所言的“点对点 + 电子支付系统”的基础上，再加上强有力的“央行信用”，也就是“点对点 + 电子支付系统 + 央行信用”。

因为价值支撑的缺失，各国政府对于虚拟货币活动，如ICO、虚拟货币交易等，一直持审慎的态度，对其中隐含的金融风险和投资者保护问题高度警惕，但对代币或者是虚拟货币背后的技术却是态度积极。中国人民银行是最早对数字货币进行研究和试验的中央银行，其他主要国家央行也高度重视数字货币的研究。目前央行数字货币已成为国际央行会议最重要的主题词之一。数字货币可谓是数字经济发展的基石，把实物货币转为数字货币的梦想已在民间率先发力和试验，中央银行必须奋起直追。

以太坊的创始人 Vitalik Buterin 认为，数字货币这样的创新由政府部门来主导是不可能实现的。这是一个很有趣的观点，私人数字货币伴随着财富效应，趋之若鹜；法定数字货币一定程度上则是对原有知识结构和投资收益的挑战，阻力难免。两者的难易程度一望即知，问题是在推动创新方面，政府的作用怎么可能缺位呢？早在 20 世纪 20 年代，凯恩斯就写下了这样的话：

“宣称私人利益和社会利益必定会相互一致，这是没有根据的，上天并非是如此来统治世界的。说两者在实际上是一致的，这也是不真实的，在现实生活中并非是如此来管理社会的。断言开明的自利必定会促进公共利益，也不是根据经济学原理得出的正确推论。而所谓自利一般是开明的，同样也是不符合实

际情况的。”①

当下愈演愈烈的 ICO、IFO 仿佛就是这段话最好的注解，有人因此感慨：“人性是比特币生态链上最大的弱点！”所以笔者以为，对于 Vitalik 的论断，最好看看情况再下结论。无论是官方还是民间，数字货币研发进程的大幕都才刚刚拉开。两者也未必就是绝对的泾渭分明，公权与私权，宛若一枚硬币的两面，既对立又统一。任何新生事物都需要时间来检验。

实际上，老百姓对货币的基本要求也就两个：一个是不能假了，另一个是不能毛了。无论对私人数字货币，还是法定数字货币，这两个要求都概莫能外。就全局最优的角度而言，我们相信，央行数字货币理应更能满足大众对货币的需求。

实物现金“＋电子支付系统”，数字货币“＋央行信用”，电子支付工具“＋点对点”甚至“＋央行信用”，“＋可控匿名”，“＋智能便捷”……各类演变看似各异，实则脉络清晰。不仅朝着“你中有我，我中有你”的方向演进，而且“草蛇灰线”，“伏脉千里”之外的则是那若隐若现的法定数字货币。

这一历史进程正徐徐展开！

大浪淘沙，我们都在这一进程之中！

姚 前

2018 年 1 月 20 日

① 凯恩斯．预言与劝说［M］．赵波，包晓闻，译．南京：江苏人民出版社，1999：313.

目　录

第一章　数字货币概述

数字货币是指以数字形式存在的货币，在不同语境下，有着不同的内涵和外延。目前，狭义的数字货币主要指纯数字化、不需要物理载体的货币；广义的数字货币等同于电子货币，泛指一切以电子形式存在的货币。

从狭义看，最早的数字货币源于1982年David Chaum提出的一种具备匿名性、不可追踪性的电子现金系统[①]。它的两项关键技术是随机配序和盲化签名：随机配序产生的唯一序列号保证数字现金的唯一性；盲化签名确保银行对该数字现金的匿名背书。Chaum的理论及其研发的E－Cash激发了研究者们对数字货币的兴趣。经过近四十年的发展，数字货币已经在Chaum理论的基础上融合了群盲签名、公平交易、离线交易、货币的可分割性等新概念。

但Chaum当时建立的模型还是传统的“银行、个人、商家”三方模式。每个使用过的E－Cash序列号都会被存储在银行数据库中，且在每次交易中系统都要验证E－Cash序列号的唯一性，因此随着交易量的上升，数据库就会变得越来越庞大，验证过程也会越来越困难。

2008年，中本聪发表经典论文《比特币：一种点对点的电子现金系统》[②]，提出了一种全新的电子化支付思路——建立完全通过点对点技术实现的电子现金系统，将Chaum的三方交易模式转变为去中心化的点对点交

① Chaum D. Blind Signatures for Untraceable Payments [M]. Advances in Cryptology. Springer US, 1983: 199－203.

② Nakamoto S. Bitcoin: a Peer－to－peer Electronic Cash System [EB/OL]. https://bitcoin.org/bitcoin.pdf. 2008.