

## 【2019.12.20】陈海波 《从实物货币视角看数字货币》

自从2009年比特币问世以来，货币研究迎来一轮新的热潮。面对比特币等数字货币市值不断攀高的形势，加上移动的迅猛发展导致现金使用量明显下降，中央银行也开始积极研究自己的数字货币，以便更好地履行自己的职责。

在研究数字货币的过程中，研究人员很少从技术的角度把实物货币和数字货币进行统一。一是把货币分为有形货币和无形货币，即实物货币是有形货币，数字货币是无形货币，两者似乎没有本质的共同技术属性。二是把货币分为商品货币和信用货币，例如纸币、硬币之前诸如金、银、贝壳等具有价值的货币，被称为商品货币；纸币、硬币及之后的电子货币等依靠信用机制的货币，被称为信用货币。三是把数字货币分为基于账户和基于价值两种形式，技术上似乎也是分开来说。

然而，按照第一性原理，不管是实物货币还是数字货币，既然都是货币，一定有其最基本的共同技术属性。本文试图从第一性原理出发，探索货币最本质的技术属性。为了更好地理解货币的本质属性，本文从易于理解的实物货币的视角出发，将数字货币与实物货币进行类比分析，从而更加深刻理解数字货币等各种货币形态的本质技术属性。

### 货币的本质是账本信息

货币是人类历史上因劳动分工之后而诞生的伟大发明，使人类社会发生了翻天覆地的变化。一直以来，许多经济学家都试图准确定义货币，但各种定义似乎都存在一定的局限性。从文献分析和现实的货币存在形式来看，不管是商品货币还是信用货币，都不能孤立地去看，将其仅当做一般等价物、一串加密数据可能不合适。因货币与所有者或持有者密不可分，并提供给一定规模的群体使用，所以我们可能需要联系地、系统地去看待货币。比如：黄金在开采出来之前不能被称为货币；纸钞在印钞厂没有从央行发行出来时只能称为发行基金，也不能称为货币。只有黄金和纸钞与所有者和持有者发生权属关系，它们才可能称为货币。

货币可能与账本记录密不可分，其三个货币基本属性从账本技术的角度可以理解为：价值存储指账本具有唯一性、信息准确、长期保存、不可恶意篡改；交易媒介指经济活动发生交易时，账本信息的更新；计价单位指人们通过共识达成一个统一的价值计量单位，可以是牛羊的只数，也可以是谷物和黄金的重量，甚至可以设定一个基本的价值单位，例如“元”，用于价值的比较和统计。

### 数字货币解析

数字货币从字面上可认为由数字和货币两部分组成。一般来说，数字可能与模拟相对应。数字信号指由离散数字的物理量所表示的信号。模拟信号是指用连续变化的物理量所表示的信号。模拟信号与数字信号的区别可根据幅度取值是否离散来确定。在计算机中，数字信号用0和1的二进制数表示，故其抵抗环境等各种干扰的能力比模拟信号强很多。如果数字货币是由离散的数字信号所表示的货币形态，那么模拟货币可以理解为连续的信号所表示的货币形态。纵观货币的各种形态，连续表示价值的可能是金、银这种称重货币，每次称重的结果都是连续的。

之后，为了便于交易，方便人们使用，能够迅速、无误差识别价值，连续信号表示的模拟货币演变成离散面额标记的数字货币。从某种程度上说，自从对货币进行离散面额标记后，货币就可以算作数字货币。不管是金属货币、纸质货币、塑料货币还是电子货币，描述货币价值的信号都是离散的数字信号，只不过记录这些数字信号的载体的介质不同而已。所以，广义的数字货币不仅包括电子货币还包括一些实物货币。

狭义的数字货币主要是指除了金、银、现金等实物货币之外的电子货币。自从人们发明电子元件记录信息之后，货币就有了新的电子化形式。早期电子货币并不需要加密，而是明文传递货币账本信息，这是因为当时支持电子货币的硬件设施门槛很高，攻击者既不能获取明文，更不能对明文进行恶意篡改。这如同现在的纸币通过防伪技术保护纸币的明文信息一样，早期处理电子信息的物理设备就是一种“防伪技术”，能够保护明文信息。然而，随着科学技术的不断普及和发展，仅依靠电子基础物理设施的高技术门槛已不能解决数字货币的安全问题。加密技术的发展对于数字货币的安全广泛使用起到了重要的推

动作用，其中也包括了为保护数字货币使用者隐私而诞生的盲签名等隐私保护技术、为减少对中心化信任而出现的分布式账本技术。

## 基于账户与基于价值的比较

当前，研究人员把数字货币分为基于账户和基于价值两种形式。基于账户的货币是指在银行等金融机构内的存款；基于价值的货币是指预存在银行卡或者移动设备的价值表示。然而，从分类学的方法来看，账户和价值似乎不是一个层面的事物。基于账户和基于非账户，或者基于价值和基于非价值可能才是一个层面的事物。非账户并不代表价值，非价值也并不就是账户。

数字货币本质是账本信息，可能分为基于空间集中账本形式和基于空间分离账本形式比较合适。空间集中账本指的是价值(存款)存储在一个空间集中的账本上，类似于一些研究人员认为的基于账户形式的货币；空间分离账本指的是价值(存款)存储在一个空间分离的账本上，账户是由所有者持有来体现，类似于一些研究人员认为的基于价值形式的货币。

基于空间集中账本形式的货币也包括以比特币为代表的“数字货币”。只不过为了减少对中心化机构的信任要求，以比特币为代表的空间集中账本不仅由一家中心化机构管理，还由多个节点分布式管理，从而防止了账本的恶意篡改和货币的双花。然而，目前以比特币为代表的“数字货币”还不具备货币的基本属性，可能称为数字资产比较合适。这如同纸张不是最开始就可作为货币的载体，而是后来加入防伪技术后才能用作货币信息的载体一样，当前基于分布式账本技术的比特币等“数字货币”，将来也可能随着科学技术的不断发展，具备货币的基本属性，从而成为真正的货币。

基于空间分离账本形式的货币也包括现金，只不过现金记录价值的载体是人们可以感知的纸张、塑料等。如果空间分离账本形式的货币记录的载体是电子设备，比如银行卡和移动设备，那么它就类似于基于价值的数字货币。

本文从第一性原理出发研究货币的本质技术属性，认为不管是实物货币还是数字货币，其技术本质都是账本信息，只不过各种货币形态体现在记录货币账本信息的载体不同，以及价值尺度和账户表现形式的方式不一样。如果从信息技术的角度看，那么离散信息表示价值的货币已经具有数字货币的属性。一般来说，数字货币是取其狭义，即指电子设备记录 and 处理的货币账本。数字货币分为基于空间集中账本和空间分离账本两种形式可能更合适。由于货币本质是账本信息，直接关系到人类社会的产品和服务的分配，与经济社会的发展密切相关，所以难以篡改、易于使用是核心，其信用至关重要。