数字货币或是数字凭证（上）：

到底什么是“数字货币”？

蔡维德、向伟静、胡舒风

北航数字社会与区块链实验室

2021 年 9 月 7 日

1. 前言

央行数字货币（Central Bank Digital Currency, CBDC）从 2015 年发展至今，讨论基本围绕两个主要方向展开：基于代币（Token）模型和基于账户模型。这两个方向都有支持者：

1) 基于代币的系统中，CBDC 创建为具有特定面额的代币，将代币从一方转移到另一方就像将钞票从一个人移交给另一人一样。
2) 基于账户的系统中，央行、商业银行和其他金融机构需要为 CBDC 的所有用户保留账户信息，这意味着要管理许多账户。

关于这两个方向的讨论一直在进行。例如：

- 国际清算银行（Bank for International Settlement, BIS）坚持使用账户模型[1]；
- 美国民间的数字美元（Digital Dollar）计划却坚持使用 Token 模型[2]；
- 花旗银行认为 Token 模型更好，并在数字货币 2.0 （Digital Currency 2.0）[3]中坚持数字货币只能走 Token 路线；
- 美联储认为这两个模型各有千秋。

本文以 3 篇国外学者的文章来讨论这问题：

- 第 1 篇文章是英国金融科技公司 SETL 的观点[4]，该公司长期在数字货币领域做研究，特别是在交易结算方面。文中认为一些公开的讨论存在误区（见第 2 节）。
- 第 2 篇文章作者是前美联储的学者[5]，他认为目前公开的讨论没有依据，现在数字代币系统既有 Token 属性，又有账户属性，很难说这系统是基于 Token 的还是基于账户的（见第 3 节）。
- 第 3 篇论文作者是美联储学者，他们同意第 2 篇作者的观点，但是措辞更加激烈[6]。他们认为这些讨论文章出自计算机界和央行界两个不同学术领域，存在学术壁垒，讨论时常会出现鸡同鸭讲的现象。比如，即便使用同样名词，但是其代表意义也不同。美联储学者还指出现在央行经常提及的基于账户和基于 Token 的观点出自一篇论文，而该论文发布时间早于数字货币时期且根本没有考虑到数字货币的分类。可是央行学者却反复引用该论文的分类法来区分数字货币，这不够严谨。同时计算机界常使用的专业名称在银行界却可能有不同的解释（见第 4 节）。

过去有人说数字货币不是科技问题，也不是金融问题，而是“信仰”问题。这里我们不讨论信仰问题，而是实事求是地讨论到底什么是数字货币。从上面 3 篇文章可以看出，即使现在已经爆发数字货币战争，而到底什么是“数字货币”还没有定论。数字货币的出现早已经震撼美联储等多家央行，什么是数字货币是个严肃的问题。

在这两方的观点中，一方是从保护个人隐私角度出发，另外一方是从坚持央行执行监管的职责出发。通过在学术和媒体舆论上的不断讨论，最终才能得到一个双方都可以接受的方案。虽然现在还有观点没有理清，讨论什么是数字货币还为时尚早，但是以后还会有许多新思想和理论来解释这个问题。

数字货币讨论也不会只关注在“隐私 vs 监管”的冲突。事实上，这两个模型的社会治理理念不同，数字货币系统设计、监管科技、清结算也都会不同。**这两模型的路线如果继续发展，会产生截然不同的 CBDC 模型，不同的金融市场模型，不同的合规和地下经济**。英国学者认为 CBDC 会改变整个国家经济体系，不同 CBDC 模型必然会产生不同的经济生态和生活方式，我们预测这个问题会一直讨论下去。今天热议的话题，以后可能根本不是问题；而现在不认为是问题的课题，以后可能反而是争论的热点。

我们在写《智能合约：重构社会契约》这本书时，发现英国法律协会在 2019 年研究智能合约时提出的一个观点值得大家关注。他们认为数字资产，不是真实资产，只是代表资产的所有权。例如数字房地产，不是真实房地产，而是房地产所有权的数字凭证。数字货币是数字资产的一种，如果其他数字资产都不是真实资产，那么数字货币也不是真实货币，更不是数字现金。如果从该角度出发，又会走到一个完全不同的数字货币系统设计和使用场景中。这将意味着有至少 3 种数字货币模型：

- 基于 Token 的数字货币；
- 基于账户的数字货币；
- 基于凭证的数字货币。

在基于凭证的模型中，凭证的密钥遗失只是代表需要重新开启一个流程申请资产凭证，这并不会造成资产的流失。这就根本性地解决了数字货币如今存在的一个关键问题：私钥遗失代表资产流失。基于凭证的数字货币不再是有价的“数字资产”，而是有价资产的“数字凭证”。数字货币只是凭证不是资产，这与传统数字货币思想不同。按照传统观点，不论是基于 Token 还是基于账户的数字货币都属于“数字资产”。

这样的设计也带来新的思想。除了密钥遗失问题可以一劳永逸地解决，监管方式同样也改变了。监管方可以控制存储在金融机构的资金，如果发现洗钱现象，则可以不放款，甚至可以远程取消相关数字货币的合法性，使其停止继续流通。

另外数字稳定币或是 CBDC 也不一定只能采取一种方式，同时间可能有多种方式一同出现。就像现在资金允许以现金、银行存款、支票、或是预付卡的形式同时出现。以后可能有多种数字货币方式同时间出现，与传统货币共存。

英国法律协会仅提出了凭证这个名称，却没有提出具体实施方案和系统设计方案，我们将在下篇提出我们的关于数字凭证的设计方案和理论。

2. 英国金融科技公司 SETL 的观点

SETL 是一家致力于为金融市场、资产管理和支付构建基于区块链解决方案的英国公司，其最先投身于数字货币的研究。该公司的总工程师安东尼·库利根对 Consensys 白皮书展开了批评和讨论。他提出 Consensys 白皮书《央行与数字货

币的将来》（*Central Banks and the Future of Digital Money*）[7] 问题很多。

这里先介绍 Consensys 白皮书相关的部分内容：

> 一个重要的设计决策是系统基于代币还是基于账户。
>
> 在基于代币的系统中，CBDC 创建为具有特定面额的代币。将代币从一方转移到另一方并不需要协调两个数据库，而是实时将所有权转让，就像将纸币从一人交给另一人一样。
>
> 在基于账户的系统中，央行将为 CBDC 的用户持有账户。在这种方法中，各国央行必须为货币的所有用户持有账户，这意味着要管理更多的账户。
>
> 我们基于多种原因建议基于代币的系统。它将使央行免于承担大规模账户保管和对账的职责，以及在出现问题或服务质量差的情况下随之而来的声誉风险。

SETL 总工程师对上面的思想持不同看法。首先，他指出 Consensys 公司自己使用以太坊账号系统，而以太坊不是 Token 系统。根据以太坊的白皮书，以太坊就是账户系统（下面是以太坊白皮书内容）：

> 在以太坊，状态是由称为“账户”的对象组成，每个账户都有 20 个 byte 地址，状态转换是账户之间的价值和信息的直接转移。以太坊账户包含四个部分：
>
> 1）随机数，用于确保每笔交易只能被处理一次的计数器；
>
> 2）该账户当前的以太币余额；
>
> 3）该账户的合约代码（如果有）；
>
> 4）账户的存储空间（默认为空）。

既然 Consensys 自己都使用账户系统，那么也就没有理由也没有借口批评其他团队使用账户模型。在摇旗呐喊强力支持基于 Token 的团队的同时，自己反倒使用基于账户的数字货币。根据白皮书，他还提出 5 个观点来反驳：

1）他认为所有货币包括数字货币，都有特定面额。因此 Consensys 白皮书上说“CBDC 创建为具有特定面额的代币”没有意义。 所有货币不论是 CBDC 或是传统货币，都有单位大小（例如，一美分或一美元）可以在其中进行转移。而这与货币的设计和使用代币系统或是账户系统没有一点关系。

2）基于账户的系统，例如以太坊，并没有“两个数据库”，也不需要协调。

3）他认为 Consensys 白皮书没有解释为什么基于代币的系统比基于账本的系统更快。而事实上，以太坊交易速度超过比特币交易速度。Consensys 作者的观点和事实不符。

4）白皮书所说的基于账户的 CBDC，央行需要管理大量的用户账户。但如今央行系统已然是这样运营的。

5）白皮书说如果央行使用账户系统，会导致央行有声誉风险。但现在世界上所有央行都使用基于账户的系统，如果按此逻辑，他们都存在声誉风险，包括国际清算银行。而使用 Token 系统的央行，就没有声誉风险吗？一些国家发行基于 Token 的数字货币却失败的故事是明显的反例（一些这样数字货币的币价已经归零）。

他还认为 CBDC 的优势在于人们可以以数字形式转移价值。在一些数字货币系统中可以无需证明使用人身份，或是不经过第 3 方机构（例如银行）。数字货币的价值是不需要记录使用人的身份，而是需要使用人能够操作一些手机或是计算机的作业，例如输入数字密码。

3. 加州大学前美联储学者的观点

一篇英文论文《代币或是账户系统：数字货币可以都是》（Token or Account-Based? A Digital Currency can be both）。作者是 Rod Garratt，他是加州大学讲座教授，也是前美联储学者。作者认为基于账户系统和基于代币系统的区别：

- 基于账户的系统需要验证付款人的身份；
- 而基于代币的系统则需要验证用于付款的对象的有效性。

基于代币的数字货币模型受到一些人的追捧，原因是在这种模型下的数字货币或是稳定币具有较强的匿名性，就像把纸币从一个人交给另一个人，所有权随实际占有而改变。而纸币和硬币就是这样的无记名工具，一个人能够不可逆转的将一件事物的控制权传递给另一个人，双方不需要证明自己的身份，也不需要任何第三方证明他们的信誉和身份。因此，在基于代币的数字货币模型下，用户的自由度较高，隐私性较好，但同时会给监管带来困难。

作者表示许多数字代币事实上可以算基于账户的系统，但同时也可以算做基于代币的系统，例如比特币（传统上比特币属于基于代币的系统）。

- **比特币是基于账户的系统**：该账户是“比特币地址”，私钥是从该账户交易所需的身份证明。每次比特币用户想消费比特币时，该用户必须使用私钥验证其身份。重要的是用户必须遵循系统的流程，以验证他们在系统内建立的身份。

- **比特币是基于代币的系统**：当有人想花比特币时，协议通过跟踪其历史来验证其有效性。当前事件历史记录用于验证正在传输的“对象”（例如在比特币就是 UTXO）的有效性，只有当它尚未使用时，该对象才有效。因此比特币像现金一样，一般人不能识别真假比特币，尽管真假现金有的时候也不是很容易识别。

作者得到上面 2 个完全不同的结论，是因为可以以不同观点来解释什么是账户。当定义改变的时候，解释也不同。

我们的观点：

Rod Garratt 的观点是正确的。早期比特币和以太坊白皮书都没有说清楚什么是 Token？什么是账户？连比特币这样被公认为基于 Token 的系统，也可以解释为基于账户的系统。由于比特币就是“使用一次的账户”，这么来看就是一个账户系统。

而且由于最近美国监管科技发展较快，以前认为基于 Token 的数字货币隐私性更好的观点已经被推翻。因为美国最大的暗网都不接受比特币。在美国监管科技公司眼里，绝大部分比特币交易都能被追踪，没有隐私权。反而因为使用比特币，参与者被监管单位怀疑在洗钱，于是受到了全程监管。

美国已经将一些交易所，列为 100%洗钱机构（就是每一笔交易都在洗钱）。任何用户在这些交易所买卖数字代币，都会被美国监管单位认为参与洗钱。2021 年 6 月美国 FBI 在很短时间就找到比特币赎金事件，就在传递一个重要信息：不要再幻想可以使用比特币来洗钱。

《互链网：未来连接的方式》书中提出了一个概念：**如果数字货币完全基于 Token 系统，反而有可能得到更多的监管**。美国监管单位提出 TRISA 系统，而我们又提出 STRISA 系统，这些系统都是洗钱的克星。不论是基于 token，或是基于账户系统，都可以被监管到。

4. 美联储学者的观点

美联储的学者在《数字货币环境中的代币和账户》（*Tokens and Accounts in the Context of Digital Currencies*）这篇文章中拿以太坊为实例讨论了代币和账户模型。首先，作者表示在计算机界和金融界对使用代币是有不同的看法。

4.1. 计算机界的观点

以太坊有智能合约，其早期用例是区块链上资产（或其表示）的程序化定义。以太坊社区将这些资产称为“代币”。总体思路是，智能合约可以定义自己的账户，以跟踪用户代币的余额，并允许用户以该代币进行交易。鉴于在以太坊上进行智能合约编程的灵活性，有很多方法可以实现这种系统。因此，为了保障代币操作的一致性，在以太坊启动后不久后就提出并采用了可替代代币的标准接口。

该标准以其提案号 ERC-20[8]闻名。遵循此标准的智能合约发行的代币称为 ERC-20 代币。该标准接口允许各种功能，包括在区块链上从一个地址到另一个地址发送代币，将它们作为“津贴”委派给第三方，以及为它们分配类似于股票代号的标识符。

ERC-20 标准的广泛采用可能有助于通过使用智能合约将“加密货币代币”的概念塑造为在区块链上发行的自定义资产。

以太坊一个重要的特征是电子记录。与比特币使用称为“未用交易输出”（也称为 UTXO）的格式处理记录保存不同，以太坊通过账户地址记录信息。这些账户地址在概念上类似于传统金融中的用户账户。但是，在以太坊中，任何 ERC-20 账户上的代币余额都分散在参与计算的网络节点中。

控制这些代币的用户余额的软件被称为数字钱包，但此类钱包不包含任何有价值的资产，只存储私钥。只要拥有私钥，就可以在区块链平台上授权数字代币的交易，就像在支票上签名可以激活支票的价值。有私钥，就可以查看或是控制在以太坊网络上的数字代币。但是数字代币只存在区块链网络上，并以账户余额的形式存在，并不储存在“钱包”内。

备注：

- 以太币：只存在以太坊网络上；
- 数字钱包：保存以太币的私钥的系统（可以是硬件或是软件钱包）；
- 私钥：拥有这私钥，就拥有在网络上的以太币，包括转移以太币。

一旦拥有私钥就能控制网络上的代币，也可以将这些代币的控制权转让给他人。代币的发送方和接收方不需要与代币发行方建立关系，他们只需要一个以太坊地址，并控制私钥。发件人通过加密签名向以太坊网络提交消息来发起传输，该消息将从其余额中扣除代币，并将这笔代币添加到收件人账户余额中。在发件人使用其私钥授权将一定数量的代币控制权重新分配给他人后，该收件人可以使用自己的私钥以同样的方式从其账户余额中转移代币。

4.2. 金融界的观点

2009 年，卡恩（Kahn）和罗伯兹（Roberds）撰写了一篇有关支付经济学的开创性论文，确立了“基于账户”的支付系统与“价值存储”的支付系统之间的区别。在他们的描述中，二分法的本质归结为每个系统所需的验证类型：身份验证是账户系统的核心，防伪保护是价值存储系统的核心。这表明身份验证是基于账户的支付系统（例如银行存款）和价值存储支付系统（例如现金）之间的本质区别。如此一来，传统的代币系统则可归类为价值存储系统。但是这篇文章根本没有讨论数字货币，这篇文章的结论是否符合数字货币的范畴可以进一步讨论，但现在随意地将数字货币区分为这两种形态可能早了一些。

美联储文章作者认为严格区分两种支付系统类型的意义不大：

- 并非所有账户都依赖身份验证。例如，访问某些银行账户可能涉及了解一条秘密信息，而不是对身份进行验证。
- 其次，“数字对象”（digital objects）形式的货币引发了有关技术可行性、安全性和隐私性的重大问题。
- 再有，数字代币本质上只是加密货币和央行的信息片段。历史上代币只代表价值的有形资产。然而，现在的代币化可以代表任何有价值的资产数字化，例如现金和证券。例如，通过区块链系统发行数字股票或是数字房地产。而这些数字资产，离开了其发行环境，是否还具有类似于现金的价值值得思考。（备注：例如 2021 年河南水灾，当时当地没有网络，支付宝等不能使用，而现金仍然可以使用。支付宝离开它的特定环境（互联网）就失去价值。）

他们认为许多 CBDC 研究报告都集中在概念、货币政策或是技术问题上。但是讨论货币政策需要同时考虑技术是不是可行。如果技术不可行，或是有其他科技有办法绕过政策，货币政策就没有价值。任何数字货币讨论需要同时考虑货币政策和技术可行性，避免连数字货币是什么，能做什么，不能做什么，都没有理清。

参考文献

[1]. https://coinfomania.com/imf-and-world-bank-launches-crypto-token/

[2]. https://www.nasdaq.com/articles/while-support-grows-for-fed-issued-digital-dollar-progress-is-slow-2021-06-24

[3]. https://finance.yahoo.com/news/citi-cbdcs-part-digital-money-155205790.html

[4]. https://setl.io/blog/token-or-account-based-cbdc/

[5]. http://econintersect.com/pages/contributors/contributor.php?post=202008220530

[6]. https://www.marketscreener.com/news/latest/Tokens-and-accounts-in-the-context-of-digital-currencies--32078317/

[7]. https://pages.consensys.net/central-banks-and-the-future-of-digital-money

[8]. https://ethereum.org/en/developers/docs/standards/tokens/erc-20/