

数字货币或是数字凭证（中）： 传统数字货币模型与国家货币体系的冲突

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 17 日

1. 前言

我们在《数字货币或是数字凭证（上）：到底什么是“数字货币”》一文中讨论了 3 个国外学者的观点，探讨数字货币是基于代币（Token）模型还是基于账户模型，或是两种模型均可。其中美联储的一个重要结论是数字货币的关键在于应考察该数字货币是如何实现的，而不是将传统经济学论文内对货币的分析引申到数字货币上。究其原因是实际数字货币系统的特性决定数字货币经济理论的真实性。

本文继续讨论什么是“数字货币”。在 2020 年 10 月国际货币基金组织 (International Monetary Fund, IMF) 的报告《跨境数字货币对宏观经济的影响》(Digital Money Across Borders: Macro-Financial Implications) 中提到数字货币对世界储备货币、金融稳定性、外汇管理、外币取代本币、融资和贷款、监管政策、央行货币政策都会产生影响。由于篇幅限制，本文只讨论 3 个问题：

- 1) 数字货币的资产到底在哪里？
- 2) 合规数字货币应该何时何处结算？
- 3) 遗失的数字货币应该如何处理？

以往基于 token 的数字货币和基于账户的数字货币最大的争论在于隐私保护和监管强度。本文从这两大路线出发探讨其所代表的更大的意义，即这两大路线如果继续发展，产生截然不同的 CBDC 模型、不同的金融市场模型以及不同的合规和地下经济。

由于数字凭证和传统数字货币的设计差距大，许多新思想将冲击传统数字货币思想。例如：什么是数字货币的“央行”？一个国家如果采用比特币当作法定货币意味着什么？一个央行为什么发行 CBDC 却采取比特币发币的模式？我们同意美联储的观点，真实货币理论是从现实系统的特性上推导出的货币理论，需要对数字货币系统有全面地了解，并对于该系统每一个特性都有深刻的分析。不然得出数字货币理论可能与实际结果相左。

我们一直在提的一个概念：区块链系统的细微变动会引发数字货币的巨大改变；而数字货币的小小变革又会给金融市场带来结构性的转变。过去以共识机制、交易流程、监管性来解释这种“蝴蝶效应”，在本文将会看到数字货币结算机制上的改变，会对重要数字货币理论产生结构性的改革。

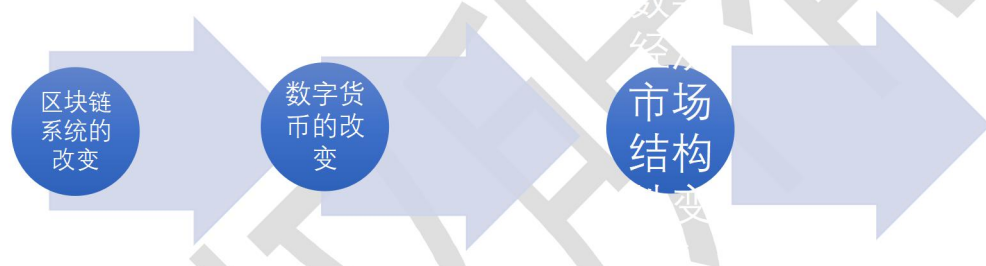


图 1：系统上小改变，对应的数字货币大改动，市场发生结构性的改革

普林斯顿大学的“数字货币区”（Digital Currency Areas, DCS）理论影响了世界许多重要组织，包括美联储、国际货币基金组织、英国央行、欧洲央行、美国财政部以及多家学术机构例如哈佛大学、麻省理工学院、伯克利大学等。过去两年这些单位纷纷根据数字货币区理论出台国际或是国家货币政策，例如美国财政部在 2021 年允许美国银行参与区块链网络和发行稳定币。

事实上，普林斯顿大学的数字货币区理论部分是根据脸书稳定币项目衍生而来。由于脸书稳定币系统在 2020 年 11 月在系统设计出现改革，并因此影响到稳定币作业流程，导致市场产生结构性的改变。故而数字货币区理论需要进行相应的更新。

上篇的观点主要出于国外学者，本篇的观点主要阐述我们的研究。

2. 什么是数字货币的资产？资产存在哪里？

无论是传统数字代币、数字稳定币、或是央行数字货币（Central Bank Digital Currency, CBDC），现在大部分数字货币是指“货币”或“钱”。例如有一美元数字货币就代表一美元钱¹。但是这种设计存在明显缺陷，即数字货币若是等于“现金”，那么遗失了数字货币，价值也随之遗失。比如曾经就出现过多次比特币遗失的事件。数字化的结果应该使得货币更安全才对，反观上述设计可能会导致货币更不安全。

英国法律协会认为数字资产不是实际资产。例如数字房产，在市区的房子，不会因为 Token 遗失而导致房子消失。房子除非因自然灾害等不可抗力而消失，不然房产一直都存在。同理，区块链系统消失不应该导致数字资产消失，这些和实际资产没有关系。英国法律协会讨论的是数字资产，而不是讨论数字货币。但是我们认为数字货币其实是数字资产的一种，因此数字货币也只能是货币的数字凭证，而不是货币本身。

本节先讨论比特币（2.1 节）和以太坊系统（2.2 节）的“资产”，2.3 节讨论传统数字代币的资产存储位置，2.4 节讨论这些数字代币和现在金融货币体系的冲突，2.5 节讨论合规数字货币应该采取和数字代币不同的路线，2.6 节讨论数字稳定币和 CBDC 应该采取的数字凭证路线。

2.1. 比特币系统

比特币系统使用的是 UTXO 模型，即账户跟随着交易。系统只有交易记录，没有账户信息，这被称为“半账本模型”。某一个“账户”中的余额并不是由一个数字表示的，而是由当前区块链网络中所有数据跟当前“账户”有关的 UTXO 组成。当需要计算某个地址中的余额时，需要遍历整个网络中的全部相关区块。所以，如果系统只有交易记录而没有账户信息，会存在透明度问题，且难以管理。

2.2. 以太坊系统

以太坊系统是全账本模型，一个地址对应一个余额。当每次查询账户余额时，不需要计算 UTXO 的复杂过程，只需取出地址对应的余额即可。虽然以太坊系统查找账户信息方便，块中也有交易信息可以找到账户，不存在透明度问题，但由于既要进行交易又要维持账户，其存在扩展性问题。事实上，以太坊这种系统也比较难以管理，币链不分离，交易共识不分离，系统要囊括以太坊代币，以及使用 ERC-20 产生的其他代币，可见系统体量之大。

¹有的数字货币还有其他问题，例如 USDT 长期被批评没有足够的准备金。但是这是另外的一个问题，就是准备金不足的问题。美国财政部在 2021 年 1 月提出的规则就是处理这问题。

2.3. 数字代币的价值在于网络系统

比特币和以太坊的数字代币资产只存储在网络上，例如比特币资产在比特币网络上，以太坊资产在以太坊网络上²。这和数字资产的观点不同，例如数字房地产，资产是物理上的房子，不是在网络上；再如数字股票，资产是公司股权，包括分红权和管理权。如果比特币网络消失，比特币资产将完全丧失价值；同理如果以太坊网络消失，以太坊资产也会完全消失。但是数字房产遗失，房产还在；数字股票遗失，股权还在，公司也还在运作。由此可见数字代币的价值不在物理世界，而是存在于虚拟的网络环境中。比特币和以太坊都使用 P2P 网络协议来保证他们的价值永存，因为 P2P 协议使比特币和以太坊网络难移除。

2.4. 数字代币价值体系和现在货币体系冲突

数字货币两条路线：1) 基于 token 的数字货币系统以及 2) 基于账户的数字货币系统，大部分学者认为这两条路线是隐私保护和强监管的意识形态的竞争。但我们认为还有其他更深的含义，数字代币和合规数字货币代表两个不同的货币体系：

- 基于网络的货币体系：价值只存在网络上，货币只是数字符号，价值来自支持地下经济的活动；
- 基于传统货币体系：价值存在央行、银行、托管机构。价值来自国家信用，可以支持任何经济活动，包括合规经济和地下经济活动。

	数字代币	合规数字稳定币/CBDC
实际资产	数字符号	国家法币
存储地方	数字代币的网络上	央行、银行、托管机构
价值来源	地下经济	国家信用
主要支持	地下经济活动	任何经济活动包括合规和地下经济活动

这两个明显不同甚至是对立的货币体系。如果坚持国家货币体系，却采取 token 模型并且将资产存在网络上，这表示数字货币的实现可能已经违反了国家货币体系的原则。由于 CBDC 是国家法币的数字化，而合规数字货币是银行存款

² 一些使用以太坊 ERC-20 的数字代币资产也是建立在以太坊上。由于这原因许多其他的代币系统也是拷贝了以太坊系统的部分代码。他们宁愿自己重建一个与以太坊类似的系统，也不愿使用以太坊网络来建立数字代币。因为如果使用 ERC-20，等于依赖于以太坊系统。^[1,2]也因为这原因，国外分析师认为以太坊市值以后会大于比特币市值。这里有个重要信息，即使在数字代币世界，一些代币不愿意附属于其他代币。何况世界各国央行，他们的 CBDC 愿意附属在一个现成代币的网络系统上？

的数字化，他们不只是存在网络上的符号。因此这里的冲突已经不只是不同的实现方式，也不只是隐私保护和监管的竞争，而是两种不同货币体系之间的冲突。

按照这样逻辑，一些坚持使用 token 方式的数字稳定币项目，最后可能就只有两个选择：

1) 数字货币只可以是现金的数字化，即数字货币就是数字化的现金，而现金是同时间可以在合规市场和地下市场上使用；

2) 如果不是现金数字化，这些项目代表的货币体系就和现在国家货币体制无法兼容。一旦部署就会出现混乱，最终必须停止执行。

2.5. 合规数字稳定币以及 CBDC 和数字代币的货币体系不同

因此，数字稳定币和 CBDC 都不应该学习比特币或以太坊的模型，因为他们的价值只存储在网络上。数字稳定币的价值存储在托管中心，与 CBDC 存储在央行同理。

像比特币、以太坊这样的公链系统，其区块链网络就是数字货币的央行，比特币、以太币脱离其区块链系统将失去实际价值。但是数字凭证的设计，则很有可能采用区块链联盟方式（不是联盟链，而是多链合作的联盟），存在多个链，包括银行内和银行外，覆盖多方交易。同时在一个链上可以处理多币种，存储多条记录，最终的结算交还给托管中心或是银行来实现。

如果任何数字稳定币或是 CBDC 选择了将 token 当成唯一凭证（token 的遗失代表资产的遗失）的模型，这代表央行或是银行不再是唯一背书机构。这里已经不再是“隐私 vs 监管”的冲突，而是数字稳定币或 CBDC 价值的背书应由谁来承担的问题。如果 token 是唯一的凭证，代表区块链网络是央行的一部分，而且两者不能分割，这与世界央行的想法背道而驰。

CBDC（直接）和数字稳定币（间接）的价值在于国家信用和体制，而不是网络的信用。但是当 token 成为唯一的凭证，间接意味着央行放弃了国家的部分铸币权。近期萨尔瓦多接受比特币为国家法定货币，代表该国央行愿意放弃部分铸币权，而且全盘接受比特币的“货币政策”，其中包括经常性的暴涨和暴跌。这也代表很大部分萨尔瓦多国际资产存在比特币网络上，而不是存在央行或是银行内，且交易并不关心持有 token 的人是谁。

2.6. 合规数字货币应该是数字凭证

传统币链分离概念是指多个币种可以在同一区块链系统上使用。现在有一个全新的币链分离的思想出现：**即使相关的区块链系统消失了，数字货币的价值仍然存在。**

CBDC 应该具有类似于纸币所代表的价值和功能。法币依靠政府的信用保证货币价值，CBDC 也应该具有等价的信用价值。相反，现有的一些数字代币可看作是持有者对发行者的一种债权，若 CBDC 以此为设计思路，会对流通媒介存在极强的依赖性，CBDC 的信用价值将大打折扣。

那么 CBDC 是不是一种货币？事实上 CBDC 不被当作货币可能更加合理。CBDC 应该仅仅是一个等值凭证，即拥有同等法币的数字证明。故而，CBDC 的系统设计关键是不能将其价值依托在某个区块链系统中。也就是说，真实的 CBDC 应在央行，而链上实现交易的是 CBDC 的数字凭证，用户手中持有的也是 CBDC 的数字凭证。CBDC 和数字凭证存在一对一关系。

	合规稳定币/CBDC 是价值	合规稳定币/CBDC 是数字凭证
价值	数字货币就是法币	数字货币是法币的数字凭证
存储	数字货币必须保存好，因为这些就是实际价值	数字货币只是数字凭证，真实货币在央行、银行、托管中心
遗失数字货币	遗失所有相关的资金	所有相关的资金还存留在央行、银行、托管中心
使用	类似现金	类似现金
交易	交易即是结算	交易即是记录，需要第二次在央行或是银行结算
信用风险	只要 CBDC 存在，而且真实，没有信用风险；合规数字稳定币的风险在于发行和运营机构	如果是 CBDC，资金存在央行，没有信用风险；合规数字稳定币的风险来自发行和运营机构
流动性风险	只要 CBDC 存在，而且真实，没有流动性风险；合规数字稳定币的风险在于发行和运营机构	如果是 CBDC，资金存在央行，没有流动性风险；合规数字稳定币的风险来自发行和运营机构。发行方有没有使用准备金是重要关键
孤儿数字货币	会出现，资金一去不返	私钥遗失资金还在，所有孤儿数字货币可以追回

同理，数字稳定币只是价值的凭证，实际价值在托管中心，例如银行。用户拥有托管中心的货币及其凭证。数字股票也不代表真实的股份，只是股份的凭证。如果数字股票遗失，股权还在。股民可以通过一个流程将股权取回来。

在这样的设计思路下，即使交易的区块链出现系统性风险，在大量节点崩溃的情况下，用户也可通过保留的数字凭证找回丢失的资金。同样，如果用户不慎丢失了持有的 CBDC，可在限定时间内用新产生的数字凭证找回丢失的 CBDC，而旧的数字凭证将失效。这样即使之前的数字凭证被别人拿到了，也无法获取到相应的 CBDC。

传统数字代币存放在公链上，但是如果私钥丢失，该用户所持有的币将成为链上的“孤儿”（orphan）。这些孤儿币无人认领也无法使用。

比特币、以太坊系统上的代币依附于区块链系统，用户拥有私钥仅意味着拥有这些币的使用权，这些币依旧存在于区块链网络中。相反，基于数字凭证的区块链网络中运行的不是真实的数字货币，网络上仅保留交易记录，链上的结算仅代表交易记录的更新与整合。实际的结算是由链上产生交易后提交到托管银行完成。

在传统的数字货币系统中“交易即是结算”，在数字凭证模型却改为“交易即是记录”。由于币链分离，数字凭证模型下，币的流通将不受特定网络系统的限制。即使特定网络消失，只要身份被证实，就可以在联盟中的其他链上继续流通，或是到托管中心换回准备金。

3. 实时结算：数字凭证需要交易后结算

在结算方面，代币不论是基于 token 还是基于账户的系统都可实现结算一步到位。包括美国前财政部在内的许多机构表示这是数字货币的一个显著优势，是改变世界金融系统的重要创新。由于交易即是结算，交易可以飞快完成。2019 年 7 月由英国央行行长公开说明代币交易速度快，2021 年 6 月英国央行再度肯定代币的这一优势，这也直接促成了 2015 年英国央行开启数字英镑。在 2020 年年底，国际货币基金组织提供数据证实数字货币的速度的确高于传统银行货币。

但在金融市场基础设施原则（Principles of Financial Market Infrastructure, PFMI）中提到^[3]，交易和结算应该分开而不是一步到位，因为监管需要更多的时间来防止洗钱。这两种观点都有支持者。

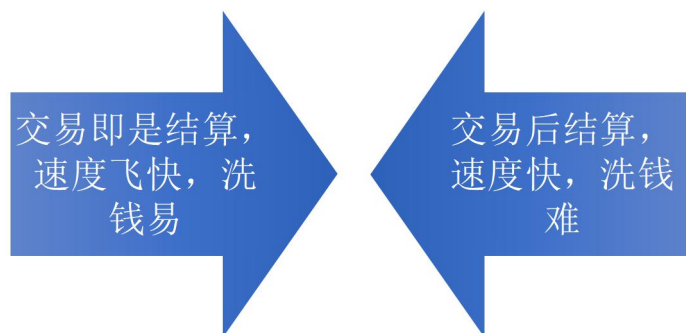


图 2: 交易即是结算 vs 交易后结算

英国央行的最终决策是交易后的 2 小时内完成结算，即“实时结算”，而英国央行选择了“骑墙观望”（sit on the fence），表示中立：认为数字英镑是实时结算（交易和结算一次到位），但只要在 2 小时内完成结算也算是实时结算。英国央行本质上还是将交易和结算机制分离，以现代计算机的性能来说，2 小时所产生的计算数量级已经十分巨大了，亿万次计算步骤都可以完成。

3.1. 脸书稳定币交易和结算机制分开

脸书 Diem 稳定币支付系统还开发了 FastPay 结算系统，详见于论文“FastPay: High-Performance Byzantine Fault-Tolerant Settlement”（发布于 2020 年 11 月），结算和交易系统分开，并且在区块链系统内有嵌入式监管机制。所以脸书将交易和结算分离，接受政府的监管。

FastPay: High-Performance Byzantine Fault Tolerant Settlement

Mathieu Baudet*
mathieubaudet@fb.com
Facebook Novi

George Danezis
gdanezis@fb.com
Facebook Novi

Alberto Sonnino
asonnino@fb.com
Facebook Novi

ABSTRACT

FastPay allows a set of distributed authorities, some of which are Byzantine, to maintain a high-integrity and availability settlement system for pre-funded payments. It can be used to settle payments in a native unit of value (crypto-currency), or as a financial side-infrastructure to support retail payments in fiat currencies. FastPay is based on Byzantine Consistent Broadcast as its core primitive, foregoing the expenses of full atomic commit channels (consensus). The resulting system has low-latency for both confirmation and payment finality. Remarkably, each authority can be sharded across many machines to allow unbounded horizontal scalability.

FastPay is a Byzantine Fault Tolerant (BFT) real-time gross settlement (RTGS) system. It enables authorities to jointly maintain account balances and settle pre-funded retail payments between accounts. It supports extremely low-latency confirmation (sub-second) of eventual transaction finality, appropriate for physical point-of-sale payments. It also provides extremely high capacity, comparable with peak retail card network volumes, while ensuring gross settlement in real-time. FastPay eliminates counterparty and credit risks of net settlement and removes the need for intermediate banks, and complex financial contracts between them, to absorb these risks. FastPay can accommodate arbitrary capacities through efficient sharding architectures at each authority. Unlike any tradi-

图 3: 脸书稳定币发布其结算系统的设计

事实上，脸书的区块链交易和链上结算系统也是一步到位，只是后面多加了一个结算机制，表示前面区块链系统内的“结算”只是“预结算”，后面添加的结算才是资金的转移。

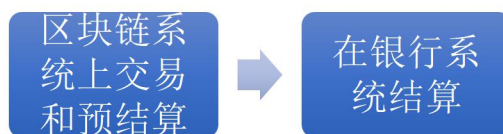


图 4：在区块链系统预结算后，在银行系统结算

在金融市场中，结算后资产才会转移。后期如若出现问题，交易很难回滚。因此在数字货币上，交易和结算一步到位风险高。

3.2. 数字凭证需要交易后结算

数字凭证由于资金实际存在于托管银行，结算还需要在银行体系内完成，因此数字凭证的模型类似脸书的数字稳定币结算模型，最终在银行机构结算。

这样数字凭证不能一步到位，交易不能立即结算，只能是预结算，结算流程多一道手续，也给监管机构多一些时间实现监管。

3.3. 数字货币交易的回滚机制

由于交易和结算分离，数字货币交易可以实现回滚，而传统的区块链系统不能回滚。可回滚的区块链交易可以解决区块链领域的一个重大难题，如果不能回滚，交易即时结算具有巨大金融风险，支付、清算、结算、监管都会遇到困难。

4. 数字货币区“平台为中心”理论更新

2019 年 7 月普林斯顿大学发布数字货币区理论（Digital Currency Areas, DCA）很快就得到了包括英国央行在内的许多机构的重视。在 2019 年 8 月 23 日英国央行在美国演讲中根据这理论提出了以后数字货币取代美元成为世界储备货币。后来这理论连续在欧洲央行、美联储内一再讨论且长达 2 年之久。国际货币基金组织 2020 年 10 月的报告也是根据这理论进行广泛的讨论，认为数字货币改变世界金融市场。原来数字货币区理论包含下面重要结果：

- 1) 数字货币是跨国界跨领域的，不要认为数字货币是国家货币或者地区货币，数字货币产生时就是跨国界的货币，跨领域的货币。
- 2) 货币的功能有交易媒体、价值存储和计量，在数字货币出来时，交易的媒体是最重要的。
- 3) 数字货币（digital dollarization）会取代法币，市场现状会发生改变。

- 4) 数字货币最终会影响到世界储备货币，形成世界储备货币的竞争。
- 5) 数字经济以平台为中心，而不是以银行为中心，市场结构改变。
- 6) 数字货币因为网络连接而产生，但是却因为竞争而使金融市场更加分裂。

其他学者包括我们对数字货币区理论进行延伸，例如：

- 1) 细分数字货币区为合规市场和地下市场，以及其他分类；
- 2) 二元竞争增加为三元货币竞争（数字代币、法币、稳定币）；
- 3) 更新数字货币区分方法，原来是以平台区分，现在更新为地缘政治区分，原因是各国提出监管政策阻止脸书平台进入。

但是第 5 项“平台为中心”的思想需要更新。根据美联储的观点，任何数字货币需要根据实际系统来分析。2019 年 6 月，只有数字代币在世界横冲直闯，没有大型合规数字货币出现，同时大部分数字“资产”都是存在于区块链网络中，结算也在网络上，不是在银行。后来脸书提出数字稳定币，明显数字稳定币的资产比银行的资产还大。在 2020 年 5 月欧洲央行预计脸书稳定币会有 3 万亿欧元的资产，将成为欧洲最大的货币基金。这也间接证实了普林斯顿大学的理论是正确的，即在数字货币时代是以平台为中心。美国前财政部也同意这种观点，并于 2021 年 1 月积极鼓励美国银行加入区块链网络系统，一起推“大网络，小银行”的数字货币区。

2020 年 4 月脸书发布稳定币 2.0 版本，增加了数字货币监管以及准备金的机制。如果一个国家要发展自己的数字货币，脸书就自动放弃进入该市场，并且愿意协助这些国家建立他们的数字货币科技，放弃公链思想，但是整体区块链系统的架构没有改变。按照脸书发布稳定币 2.0 白皮书，普林斯顿大学的数字货币区不需要更新。

但在 2020 年 11 月，脸书稳定币团队发布 FastPay 结算系统。这结算系统并非在区块链网络上结算，而是在机构内结算（见 3.1 节）。根据 FastPay 系统，普林斯顿大学的数字货币区的“平台为中心”理论也就不再成立了（见下表）。

	资产存储在	结算	中心
传统区块链网络	网络	在网络	区块链网络
脸书稳定币 1.0 和 2.0	网络	在网络	区块链网络
脸书 FastPay 结算系统	托管银行，网络只是记账	在托管银行，网络只是预结算	银行
数字凭证	银行，网络只是记账	在银行，网络只是预结算	银行

本文提出数字凭证思想比 FastPay 走得更远。脸书 FastPay 的文章主要在讨论系统的架构和协议，但其对于数字货币理论的冲击却没有讨论。因此当时学者在讨论数字稳定币时还是基于原来脸书稳定币的系统架构。没有想到，在美国财政部鼓励美国银行进军区块链网络的时候，脸书稳定币系统架构却暗中改变了。

FastPay 系统并没有使用区块链系统，而是使用简化的拜占庭将军协议（不是完整版的拜占庭将军协议），脸书工程师认为简化结算流程可加快结算速度。FastPay 系统和稳定币区块链系统分开，而且是在金融机构内结算，不是在区块链系统上结算。

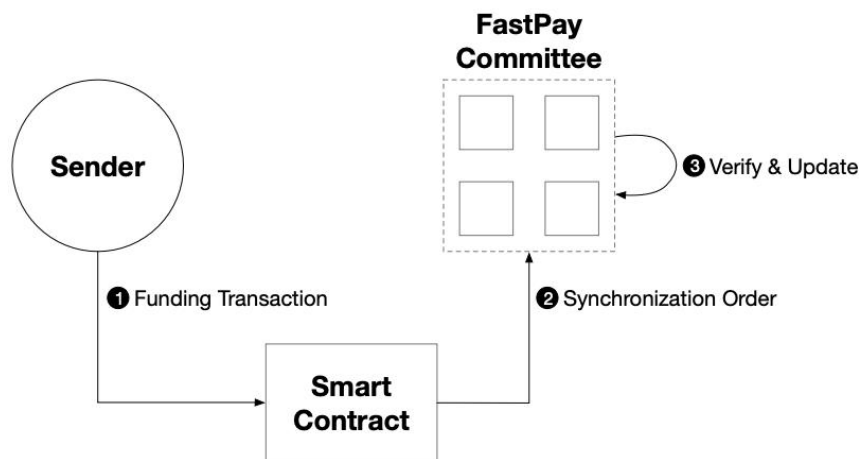


Figure 3: Transfer of funds from the Primary to FastPay.

图 5: FastPay 结算系统没有使用区块链系统，而且和稳定币主链分开

下图显示发展的历史:



图 6：由于数字货币系统改变，“平台为中心”理论更新到“银行为中心”

如果以后数字货币的世界还是以银行为中心，这代表改变的规模比原本想象的要小，更容易进行，监管上也更容易。

如果上面推论正确，那么许多理论需要更新：

- 美国前财政部在 2020-2021 年公布的数字经济计划蓝图（包括美国银行参与区块链网络以及美联储建立新型国家支付网络）需要更新规划，因为该政策是以区块链网络为中心；
- 整个合规数字货币市场结构改变，国际货币基金组织在 2020 年提出的未来数字经济架构需要更新；
- 地下市场的作业也会改变。地下市场会采取更加隐蔽的数字货币，避开央行、银行、国际和国家监管单位；
- CBDC 的设计也会改变，不能采取资金存在网络的模式。
- 国际和国家监管策略也会改变，金融机构会是监管的重点，这会减轻监管科技的压力；
- 地下数字经济会和合规数字经济分道扬镳，由于数字稳定币和 CBDC 的监管重点会在银行，地下经济活动不会到合规银行从事商业活动，也需要重新建立自己的数字货币体系。因为以前地下经济的支柱（比特币和以太坊）已经被西方国家收编，接受监管。这会产生两级的影响：部分地下经济合法化，而另一部分地下经济只能更加隐蔽继续在地下活动，地下经济成为隐私计算的先锋。

如果未来脸书宣布不采用 FastPay 系统结算，而采取另外一个新结算机制，数字货币理论可能还会继续跟随改变。

5. 总结

数字货币应该如何设计还是一个研究课题。由于数字货币带来的金融市场改革，会影响到整个国家的经济体系，以及国家法币在世界市场的地位，所以需要谨慎考量。考虑因素也不应该只是关注在“隐私 vs 监管”的顾虑。由于数字货币只是数字资产的一种，现在国际的趋势是数字货币科技先行，数字资产科技跟随，因此如何设计一套安全、可靠、合理、隐私而又可监管的数字货币和数字资产是重要目标。

本文分析了传统数字货币结算机制，脸书 FastPay 结算系统以及数字凭证，可以清楚看出不同价值存储、不同结算会导致不同的金融市场结构。这种结构的改变不只会改变合规市场，地下市场也会改变。

“交子”是中国最早的纸币，也是世界上最早使用的纸币，第一次出现是在中国四川省。宋仁宗天圣元年（1023 年）由监官主持银票（官交子）发行的政府设益州银票务，这是中国最早由政府发行的银票。交子是银票，不是银子，开始的时候只是银子的存折或是凭证，由于有信誉，后来才被当成货币使用。我们的数字凭证就以“交子”为名，借助交子的含义，将新数字货币模型命名为“交子数字凭证”模型。



图 7：1023 年中国发行的交子

参考文献

- [1]. 蔡维德、姜晓芳、王康明, 银行和支付体系的改革: 新型货币战争进入第 2 阶段 (一) 2021. 01. 12
- [2]. 蔡维德, 姜晓芳, 王康明. “美国合规稳定币管理模型: 新型货币战争进入第二阶段 (二)”, 2021. 02. 22
- [3]. 蔡维德等, “PFMI 指导下的全新区块链设计: 下一代区块链系统 (二)”, 2021. 04. 01
- [4]. Wei-Tek Tsai, Dong Yang, Kangmin Wang, Weijing Xiang and Enyan Deng, Srisa: A New Architecture to Enforce Travel Rule//FICC 2020
- [5]. 蔡维德等, 美国合规稳定币管理模型: 新型货币战争进入第二阶段 (二)
<http://m.xinhua08.com/share.php?url=http://fintech.xinhua08.com/a/20210222/1976264.shtml>