数字货币或是数字凭证（下）：交子数字凭证模型

蔡维德、向伟静、胡舒风

2021 年 11 月 22 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。在《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》一文中讨论了 3 个问题：数字货币的资产到底在哪里？合规数字货币应该何时何处结算？以及遗失的数字货币应该如何处置？本文承接上一篇文章将详细介绍交子数字凭证模型。该模型不同于“传统”数字货币模型，不再是数字化的货币，而是数字化的凭证。数字凭证仍然可以交易、清结算，但是在管理和监管方面比传统数字货币强。最重要的一点是，在该模型中，私钥的遗失不再代表价值的流失。我们进一步将这一模型融合到非同质化权益（Non-Fungible Rights，NFR）中[6]，借助实质资产不在链上交易的特性，NFR 相比 NFT 在稳定性上有了更明显的优势。

2. 交子数字凭证模型

本文提出一个数字凭证模型。稳定币发行后在链上的交易中，真实货币与数字凭证一一对应。客户使用数字凭证完成交易；稳定币发行方获取链上节点共识的交易结果，生成新的数字凭证，完成稳定币所有权的转移，实现稳定币的交易。

该模型可有效提高稳定币交易的抗系统性风险的能力。模型中抽象出 3 类角色，分别为：

- 稳定币（或是其他数字资产）发行方；
- 虚拟资产服务商（Virtual Asset Service Provider, VASP）以及；
- 客户方。

其中客户方包括企业或个人；稳定币发行方通过权威单位（例如政府或是银行）获得授权发行数字凭证。持有人获得相应的数字凭证表明所有权，所有稳定币的交易通过区块链上数字凭证的验证、生成与失效等操作来实现。区块链上节点完成数字凭证的生成、验证与失效，并管理一个失效凭证 ID 列表，用于记录因为丢失或已花费而失效的数字凭证，同时用于验证数字凭证的有效性。具体涉及稳定币发行、流通、找回的步骤如下：

1) 稳定币发行方维护一个表头为币种、币值、凭证 ID、获得所有权时间的稳定币发行列表。每发行一笔稳定币，发行方都要记录对应数值，以便在稳定币丢失后找回，并向通过审核的个体发放数字凭证。每次稳定币交易也都记录在案。
2) 稳定币的交易是确保数字凭证有效的前提下，审核数字凭证中所代表的金额的有效性，将发送方的数字凭证做失效处理，同时生成新的接收方的数字凭证，以实现稳定币所有权的转移。
3) 稳定币的丢失找回流程是客户端提交找回申请后，链上节点先将凭证 ID 放入失效凭证列表，并通知发行方审核并确认该稳定币所有权的准确性，生成可获得新数字凭证的许可，节点在获得该许可后生成新的数字凭证返回给客户端。

2.1 数字凭证数据结构

稳定币发行方获得授权发行稳定币数字凭证，发行方维护一个表头为币种、

币值、凭证 ID、获得所有权时间的稳定币发行列表，用于记录虚拟资产服务商或客户的稳定币兑换历史，可用于稳定币丢失后进行找回判定。

虚拟资产服务商通过虚拟资产服务商 ID 作为金融机构标识码向发行方申请用一定数额的法币兑换一定量的稳定币。稳定币发行方验证该申请后向虚拟资产服务商发放对应数额的数字凭证。虚拟资产服务商凭借数字凭证向客户方发放储蓄或贷款。

企业或个人通过向虚拟资产服务商申请借贷或储蓄的方式获取稳定币，发生稳定币所有权的转移。虚拟资产服务商在接收到申请贷款或储蓄的申请后，根据不同角色产生不同身份的数字凭证，即对于企业和个人将分别生成企业数字凭证和个人数字凭证。

2.2 数字资产找回流程

不慎遗失的数字凭证找回流程如下：

1）企业/个人向虚拟资产服务商提交数字凭证丢失申请，在钱包或是其他地方找到凭证 ID 的备份，然后生成稳定币凭证丢失申请；

2）稳定币凭证丢失申请提交后，进行两步处理，第一步为原有凭证失效，第二步为生成新的有效的数字凭证；

3）虚拟资产服务商发布新的有效的数字凭证。

2.3 利用数字凭证实现交易

VASP 通过虚拟资产服务商 ID 作为金融机构标识码向发行方申请用一定数额的法币兑换一定量的稳定币，稳定币发行方验证该申请后向 VASP 发放对应数额的数字凭证，VASP 凭借数字凭证向客户方发放储蓄或贷款。

在这种数字凭证交易中有两种情况，即 A→B 和 A→A。A→B 是实现 A 向 B

转移一定数额的稳定币，A→A 是完成 A 丢失持有稳定币的数字凭证后申请得到新的数字凭证，对此节点也可记录为一次稳定币交易，只不过是交易双方为同一个人。在生成新的数字凭证期间，若是有其他客户获得了旧的数字凭证，将无法通过有效性验证，不能获得对应稳定币的使用权。

在数字凭证模型中，准备金与数字凭证存在一一对应关系，在链上进行交易的是数字凭证。若是交易链突发意外，几个节点同时崩溃，也可凭借发行方的稳定币发行记录生成新的数字凭证，不会发生稳定币丢失或失效的问题。

3. 监管机制

对于监管机构来说，基于比特币式的代币的模型由于只能用一次，所以需要多次计算才能追踪到个人交易历史。但是因为历史数据公开存于区块链上，追踪也不是问题。不论是基于代币的模型或是基于账户的模型，我们可以使用 STRISA 系统[4]，监管到账户的钱包，可以有效防范不法分子利用数字代币进行洗钱的风险。

同时，稳定币监管的实现可参照下图的蝴蝶模型[5]。以发行方为中心，左右两侧（翅膀）都在强监管下。这两个监管方式和机制不同，但又互相交互。左边保证稳定币的价值，右边保证稳定币的交易合规。该模型是根据美国前财政部公布的监管规则发展出来的。美国财政部规定每一天托管机构必须报告准备金的数据，以及还在流动的代币情况。一方面可以反洗钱，一方面保护数字稳定币的持有者以及参与的商家。

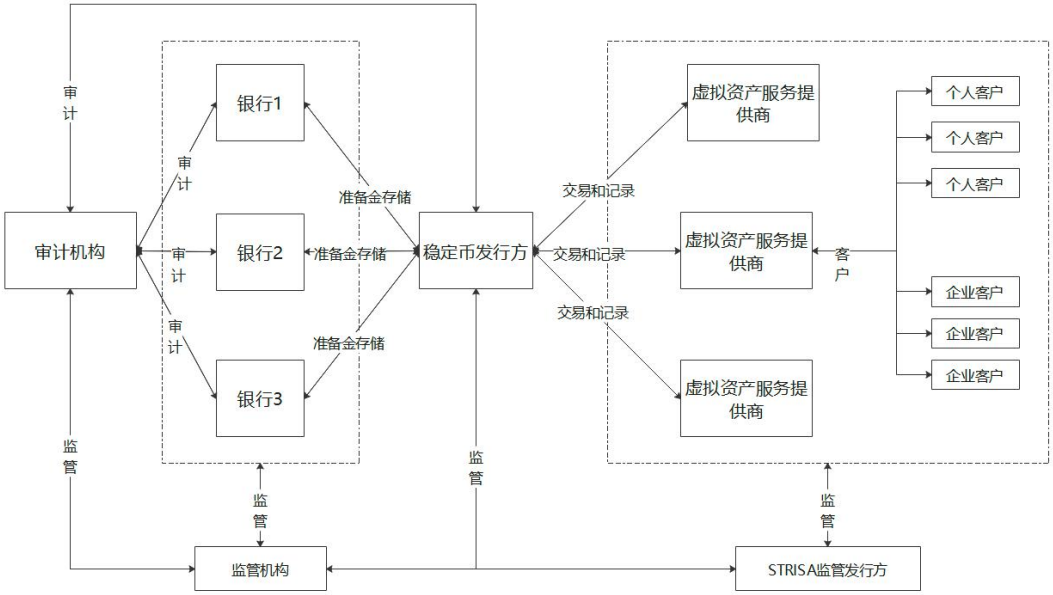

图 1 蝴蝶模型

蝴蝶模型不是美国财政部提出的规则，而是一个可以运行的计算模型。美国只提出了制度上的规则，而蝴蝶模型将这些规则打包成为一个可以执行的计算模型。美国财政部提出的模型还是使用传统的数字货币模型，即数字货币结算在网络系统上，不是结算在后面的托管银行。在《数字货币或是数字凭证（中）》中，我们提出目前的数字货币模型和现代金融市场模型是有冲突的，使用起来格格不入，风险非常大。

交子数字凭证也可以交易，而蝴蝶模型也适用，只是这里蝴蝶模型不是管理数字货币，而是管理交子数字凭证。当客户需要实际资产（例如美元、人民币、或是房地产）的时候，客户可以将数字钱包内的交子提交到托管银行兑换实际资产。

4. 交子清结算

在交子模型环境下，结算分两步，第一步在数字货币网络，第二步在银行完

成，即最终结算和清算还是在银行。由于还是在银行结算，数字货币和资产模型就会与现代金融市场的模型相匹配，代币、数字货币将不再和数字货币模型冲突。

因此交子模型需要在银行系统内使用互链网或是区块链系统。如果银行使用传统数据库，若是职员作弊，外面的系统即使使用强大的区块链系统也无济于事。同时由于结算在银行，如果银行出事，外面的系统再强大，也无法保证交易完备性。

图 2 交子模型+互链网

5. 比较

下表列举了比特币、以太坊、Token 数字货币、账户数字货币、Token 数字凭证以及账户数字凭证在设计上的不同（表 1）。下表提出的账户数字货币模型、交子数字凭证、账户数字凭证还可以有不同的实现方式，表上只列举一种方式。

表 1 不同的设计

	资产	资产私钥	账本	特性
比特币	在比特币网络上	Token（私钥）存在钱包	Token 是只能用一次的账本	失去私钥，网络上资产成为孤儿
以太坊	在以太坊网络上	Token 存在钱包	有全额账本。完整历史的账户	失去私钥，网络上资产成为孤儿
Token 数	在数字货币网	Token （私钥）	Token 只能用一	失去私钥，网络上资产

字货币	络上	存在钱包	次的账户	成为孤儿
账户数字货币	在数字货币网络上	身份证认定账户，以账户认定资产拥有者	有全额账本。完整历史的账本	失去身份证（例如生物身份证）失去资产
交子数字凭证	真实资产在托管银行；数字凭证以交子方式留在网络上	交子 （数字凭证）存在钱包	交子（数字凭证）只能用一次的账户	失去交子数字凭证，实际资产还在，审核后先将遗失的交子作废，然后重发新交子；托管银行内资产经过合规流程取出
账户数字凭证	真实资产在托管银行；数字凭证交子在网络上	数字凭证交易需要数字凭证和身份证；	有全额数字凭证账本。完整数字凭证历史的账本；托管银行维持法币的全额账本和完整历史	失去交子数字凭证，但实际资产还在托管银行，审核后先将遗失的交子作废，然后重发新交子；托管银行内资产经过合规流程取出

基于数字凭证的设计思想，资产遗失的风险大大降低，交易也多一层的保护，即在网络上的交易有第一层保护，在银行结算时有第二层保护。稳定币的价值也不再被流通环境所限，同时将稳定币的信用价值交还给托管银行或是央行（而不是在网络上），由银行或是央行保证其价值，而用户持有的是一个能证明所有权的数字凭证。因此只要保证银行内部系统稳定，稳定币可以有强大的抗系统性风险的能力。在这样的设计思路下，交易也将发生变化，具体见下表（表 2）。

表 2 不同的交易方式

	链上交易	交易所交易

比特币	认 Token 不认其他， Token 由比特币网络验证。如果通过，就可以交易，旧 Token 不再有效，产生新 Token，任何比特币资产还是存在网络上，新 Token 存在钱包上	交易所收集 Token，自己交易后，在比特币网络上一次交易后交回给客户（或是比特币，或是法币，或是其他数字代币）
以太坊	认钱包账户，钱包间转账由以太坊网络验证，如果通过，就可以交易。转出方余额下降，转入方余额上升	交易所收集 Token，在内部账户间进行若干次交易，最后在以太坊网络上进行一次交易后交回给客户
Token（私钥）数字货币	认钱包账户，钱包间转账由数字货币网络验证，如果通过，就可以交易。转出方余额下降，转入方余额上升	交易所收集 Token，在内部账户间进行若干次交易，最后在数字货币网络上进行一次交易后交回给客户
账户数字货币	使用身份证关联账户，交易需要第三方验证身份，如果通过就可以交易。转出方余额下降，转入方余额上升	交易所收集身份信息，在内部账户间进行若干次交易，定期打包向链上报告总交易结果
交子数字凭证	认钱包账户，钱包间转账由数字凭证网络验证，如果通过（包括数字凭证没有报备遗失），就可以交易	交易所收集交子，确定这些没有报备遗失过，在内部账户间进行若干次交易，在数字货币网络上进行一次交易，继续在银行结算，银行结算后将信息传给客户。
账户数字凭证	使用身份证关联账户，交易需要第三方验证身份，如果通过就可以交易。转出方余额下降，转入方余额上升	交易所收集身份信息，确定这些没有报备遗失过，在内部账户间进行若干次交易，打包向链上报告总交易结果，然后继续在银行结算，银行结算后将信息传给客户。

由于分两次结算，第一次是网络上的预结算，第二次是银行内的结算。两次结算可以实时执行，也可以通过其他方式进行。例如网络上的结算不用立即传到银行完成二次结算，而是可以等待一段时间，累积一定数量的待银行结算交易，然后一次性打包提交到银行完成二次结算。但是这会延迟单笔交易完成时间。

6. NFR 采用交子模型避开金融风险

2021 年 10 月 14 号，我们发布《非同质化权益（NFR）白皮书——数字权益建设中的区块链技术应用》[6]。我们提出一个不同于国外 NFT 模型的新型数字凭证 NFR 来保证资产的真实性，不可分割性，以及唯一性。NFT 使用的是数字代币和公链，而 NFR 使用的是互链网和交子模型，因此实际资产继续留在物理空间，而不在网络上，这和 NFT 哲学思想正好相反。

貔貅模型

国外 NFT 的数字资产留在网络上，在钱包里只是数字资产的私钥。在这种模型下，NFT 使用的人越多，就会有越多实际资产上传到网络上，并且留存在网络上，这样 NFT 网络会累积了大量实际资产。拥有 NFT 的用户，实际上拥有的是网络上资产的私钥。这像一个银行保险库，里面有许多金银珠宝等资产，但是所有资产只能进保险库而不能离开，就如传说的貔貅一样只进不出。用户拥有的是转让私钥的权力，而没有将资产从银行保险库拿出的权力。如果任由这种只进不出的模式继续发展下去，最终 NFT 网络（例如以太坊网络）将会是世界上最大的资产中心，其资产将会超过银行，甚至超过一些国家的 GDP。

在 2021 年 11 月数字代币的市值首次超过世界 GDP 排名第 5 的英国的 GDP。现在每天都有大量的艺术品上传到以太坊网络上，除非数字代币价值大跌，否则以太坊网络总市值只会不断增加。

NFT 以实养虚

这种 NFT 模型就是“以实养虚”，因为用户以实际资产（法币等）购买网络上数字资产的私钥，但不能从网络上下载实际资产。NFT 拥有者只是拥有实际资产的拷贝份和网络发行的私钥，在物理空间并没有拥有实际资产，用户出示的是拷贝份，也就是一个智能合约产生的 GIF、视频、或是其他文件。而资产事实上一直留在网络上属于网络的永久资产。

NFT 提供洗钱通道

由于 NFT 使用以太坊系统，其以太币是今天地下经济的重要“货币”，因此 NFT 成为了国际洗钱的通道，通过在国内发布数字资产（例如艺术品），再到国外交易以太币，完成国际洗钱。这样的洗钱方式可追溯到清朝乾隆年间，大臣和珅曾使用典当行来洗钱。他把不值钱的破碗放在典当行，而贿赂的人就以重金来购买这些破碗，和珅以这种看似合法的方式收到贿款。当时没有数字代币，而如今 NFT 可以代替典当行来洗钱，而把资金留在国外。

NFR 没有数字代币洗钱的风险，以虚养实

因此中国若是采取 NFT，大量的资产就会留在国外网络上，而且可能有洗钱的风险。但采用 NFR，实际资产还是在物理空间，没有留在国外网络，借助数字代币来洗钱的路就会行不通。同时数字凭证交子却可以在全世界流通，扩大了交易市场，交子也不是实际资产，降低了交易的风险。

由于在网络上的交子不是实际资产，但是可以用来交易，因此在这种模型，网络科技是助力实体经济，就是以虚养实。

元宇宙需要验证参与人员和资产

2021 年元宇宙（Metaverse）得到世界的关注。在元宇宙环境下，可以有商业活动，包括买卖、合同等。但这些都需要认证。由于国外元宇宙系统已经决定采用 NFT 作为基础科技，华夏元宇宙只能采取没有数字代币的 NFR。

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

[6]. 非同质化权益（NFR）白皮书—数字权益中的区块链技术应用 ，2021.10.14