基于认证中心的新型纸质货币防伪方案

作者：赵凯锋

摘要： 提出了一种基于信息技术的纸质货币防伪方案，该防伪方案通过引入数字签名和认证机制，在传统纸质货币防伪技术之外，探索了一种新型的纸质货币防伪思路。

关键词： 防伪；货币；数字签名；身份认证

引言

纸质货币的防伪向来是一项严峻的挑战。本文尝试将信息技术中经常使用到的基于数字签名的身份验证技术与纸质货币防伪的需求相结合，提出了一种有别于传统纸质货币防伪技术的新型防伪方案。该防伪方案通过引入认证服务器和认证客户端的方式对市场上流通的纸质货币进行防伪保护。该方案首先使用随机标识符对纸质货币进行唯一标识，之后通过认证客户端识别该标识符并在认证服务器上根据纸质货币持有者的需要将对应的纸质货币标识为“入库加锁”状态和“出库解锁”状态，从而实现对纸质货币的防伪以及防失窃和损毁等。经过思想实验，从理论上来看，该防伪方案具有较强的防伪效果和较好的可操作性。

1 现有纸质货币防伪技术分析

现有防伪技术主要是基于纸质货币的制造工艺实现的防伪。从制造工艺角度来看，我们可以把其中用到的防伪技术分为特殊载体、特殊颜料和特殊印制方式。现有防伪技术实现防伪效果的前提是合法的纸币与伪造的纸质货币在制造工艺上具有一定程度的差别，即只有在伪造者无法完整掌握并利用合法纸质货币的制造工艺的情况下，这些防伪技术才可能发挥作用。但是，随着信息的传播更加便捷，不法分子学习

伪造货币的成本已经极大地降低。与此同时，信息技术在我国的应用已经取得了长足的发展，因此，尝试将信息技术应用在纸质货币防伪领域不仅具有极强的现实意义，也是一种革新纸质货币防伪思路的有益尝试。

2 将信息技术应用在纸质货币防伪领域的可行性分析

2.1 计算机领域身份认证技术的发展现状

综合计算机领域目前的发展现状而言，计算机领域的身份认证技术主要由信息摘要技术和数字签名技术组成。信息摘要技术可以使用单向散列函数，针对原始信息，生成一段固定长度且不可逆的散列值。数字签名技术可以使用非对称加密算法，以私钥加密，公钥解密的方式对一段信息的散列值进行签名，从而确保信息的完整性和不可伪造性。在具体的实现上，有 PKI 公开密钥基础设施和基于 PKI 的 CA 认证中心等。

2.2 计算机领域身份认证机制的应用现状

当前计算机领域的身份认证机制在加密、通信和电子支付等领域拥有广泛的应用场景和丰富的应用实践。可以说，计算机领域的身份认证技术已经发展得十分完善，并且在实际生产环境下得到了广泛的实践验证，能够满足当前和未来较长一段时间内的身份认证需求。

2.3 在信息化时代研究纸质货币防伪技术的必要性

纵观目前世界上各个国家和地区，几乎所有的国家和地区的法定货币仍然是纸质货币。纸质货币除了具有法律赋予的法理意义之外，其所代表的一个国家或地区的文

化内涵和主权象征也是 2020 年 1 月 1 日当今任何电子支付系统都无法取代的。因此，在可预见的未来，纸质货币仍将是一个国家或地区经济生活领域的一个重要组成部分。

2.4 使用者接受新型纸质货币防伪方式的可能性

当今，信息技术已经渗透到了人们生活的各个方面。在金融支付方式上，人们日常使用的支付宝，微信支付等移动支付手段已经十分便捷并且拥有大量的用户。

不仅仅是在终端支付环节，信息技术在整个金融领域的应用都十分广泛。例如银行系统中的各种加密算法和身份认证机制以及基于区块链的加密货币等。这些都足以说明，以目前的信息技术的软件和硬件基础以及受众的接受能力，信息技术和金融的结合不仅不会降低金融领域的安全性，而且将增强其安全性并较容易被大众所接受。

3 基于认证中心的新型纸质货币防伪方案

3.1 基于认证中心的新型纸质货币防伪技术的原理

该防伪技术的核心是由具有公信力的机构主办的认证中心以及由该认证中心运行和维护的认证服务器。此外，为了发挥认证服务器的功能还需要可用于向认证服务器标记特定纸质货币状态信息的各种终端设备。最后，为了方便使用者执行相应的操作，还需要在纸质货币上印制能够标识特定纸质货币的字符。

3.1.1 纸质货币上的字符

这个字符是唯一的和随机的，而且每个纸质货币上的字符在服务器上存储时都经过了加密及签名认证，签名数据存储在认证服务器上。由于这个字符是唯一和随机

的，且字符生效的前提是字符对应的纸质货币在公开发行之前经过了认证服务器的签名认证，并且签名认证的数据还存储在认证服务器上。因此，如果有人想凭空捏造一个字符来用于制造假币是不可能通过认证服务器的认证的。

用于标识纸质货币身份的字符可以直接印制在纸质货币上，因此，已经生产出来的纸质货币也可以使用该方案进行改造，只需要在现有纸质货币上打印一串字符并向认证服务器提交一条新的认证记录即可。

此外，并不是所有的纸质货币上的字符都必须有对应的实体纸质货币。因为，通常情况下，一个国家或地区发行的纸质货币是有最小面额的，但在具体的交易过程中可能产生最小的实体货币也无法表示的数额。因此，对于一些无法表示的小数额，也可以生成对应的用于标识该数额的字符并存入相应的用户账户，而有无对应的实体货币并不影响整个系统的正常工作。

3.1.2 认证服务器

认证中心服务器由具有公信力的机构运行和维护，服务器中保存有每张纸币上的随机字符对应的签名数据以及状态信息等，是一一对应的关系。这些状态信息保存在不同用户的账户中，对应于用户的资产状况。

3.1.3 认证客户端

纸质货币上的随机字符和服务器上的签名数据能够确保凭空捏造的随机字符是不能通过验证的，但是，这样做无法确保对有人拿现有纸质货币上已有的随机字符伪造纸质货币进行有效的检测。因此，这里需要有一个认证客户端，也就是终端设备。终端设备可以是取款机，验钞机，手机应用程序，网页程序或者专用硬件设备等。用户

通过认证客户端登陆认证服务器之后，可以对特定的纸质货币进行"入库加锁"和"出库解锁"的状态切换操作，该操作由认证客户端向认证服务器发起，之后纸币的状态将被记录在服务器中。"入库加锁"状态代表此张纸质货币已暂停市场流通，停止行使支付功能。"出库解锁"状态代表此张纸质货币开始进行市场流通并开始行使支付功能。一旦纸质货币进入“入库加锁”的状态，那么该纸质货币就和特定的用户账户信息绑定在了一起，也就是说，任意一张处于入库加锁状态的纸质货币都有其唯一对应的用户。处于入库加锁状态的纸质货币不能在合法的经济活动中行使其购买力，除非该纸质货币目前的合法持有主体利用客户端对该纸质货币进行出库解锁操作。此外，根据需要，认证服务器也可以在一定条件下将相应的纸质货币标记为“空状态”，处于空状态的纸质货币既不处于“入库加锁”状态，也不处于“出库解锁”状态，从用户的角度来看，处于“空状态”的纸质货币和采用传统防伪技术的纸质货币在使用方式上没有区别。

正常情况下，出库解锁一般发生在买方将纸质货币支付给卖方的或者客户将货币存入银行的过程中，而入库加锁一般发生在卖方接收买方支付的纸质货币过程中或者银行接收客户存款等场景中。通常情况下，“入库加锁”和“出库解锁”两个操作是连续进行的，即一方将货币 A 出库解锁必然对应另一方对货币 A 的入库加锁。

由于已经出库解锁但没有入库加锁的纸质货币面临着被伪造，丢失，失窃或者损毁的可能，所以，通常情况下，任何一个想要确保自己现金安全的人都会尽可能快的对纸质货币进行入库加锁操作。 同时，在技术上也可以方便用户进行入库加锁的操作，例如当纸质货币经过卖方的验钞机时即可将该纸质货币绑定卖方的用户信息并入库加锁。

3.1.4 认证服务器和认证客户端的安全机制

假如服务器中保存的签名数据被窃取，攻击者拿到了全部签名数据，则认证中心可以通过对纸质货币上的随机字符或者对原来的签名数据进行重新加密和签名的方式生成新的签名数据并向所有认证客户端声明新的签名数据才是合法有效的数据。由于新型的防伪技术可以从客户端那里获知每一张纸币在市场上的流转过程，且每张纸币在特定时间段内都有其对应的法律主体，所以如果攻击者想通过盗取认证服务器的数据达到盗取纸质货币的目的是极难实现的。另外，认证服务器也可以是分布式的，像使用了区块链技术的加密货币一样，每个认证客户端都可以既是客户端也是认证服务器，因此，可以把每笔交易信息都保存在全网内所有的客户端上，由全网内的所有客户端共同监督每一笔交易，这样一来认证服务器的安全性就更高了。

由于本文介绍的防伪机制是和现在已有的防伪机制共存且相互独立的，即使本文所介绍的防伪机制由于某种原因完全失效，依靠传统防伪技术仍能有效确保一个国家或地区的货币系统的安全。

认证客户端的安全机制主要是为了确保两方面的安全性。一是确保操作认证客户端的是合法用户，二是确保合法用户的与认证服务器的通信是正常的和保密的。基于目前的技术，认证客户端可以通过综合使用密码，生物特征识别等方式验证用户的合法性，还可以通过设置登陆尝试次数的方式阻断暴力破解。目前的通信加密技术也已经十分完善，可以确保认证客户端与认证服务器之间的通信具有可接受的正常性和保密性。

3.2 模拟伪造攻击的思想实验

在这里，我将列举一些在纸质货币全生命周期内（即从纸质货币被制造出来到被

销毁的整个过程中）可能发生的攻击和破坏行为对本防伪技术方案造成的影响以说明本方案在应对这些针对传统货币的伪造攻击时所能发挥的独特优势。

3.2.1 假设伪造者掌握了所有纸质货币上的编码字符

由于纸质货币上的编码字符是直接印制在纸质货币上的，因此一个人获取一定数量的纸质货币上的编码字符并不是不可能的。

一般情况下，伪造者很难掌握一个区域内所有正在流通的纸质货币上的编码字符，但是，这里我们考虑极端情况，不妨假设伪造者通过某种方式掌握了一定区域内所有正在流通的纸质货币上的编码字符并且有能力从制作工艺的角度上完全伪造真实的纸质货币。也就是说，伪造者掌握了一定区域内正在流通的所有纸质货币的完整“克隆”。那么在这种情况下，伪造者就可以在该区域内的经济活动中使用这些货币了吗？答案是否定的。

我们知道，每张纸质货币都有其对应的持有者，一个区域内所有的纸质货币几乎不可能只对应一个或者少数几个持有者。无论纸质货币是处于“入库加锁”状态还是“出库解锁”状态，其都有与之对应的持有者或者与之对应的交易，纸质货币的持有者可能在任何时刻和其他人发生涉及现金的交易，从而导致相应纸质货币的状态发生变化。因此，即使伪造者掌握了市场上流通的所有纸质货币上的随机字符并伪造出了对应的纸质货币，但伪造者仍然需要准确地知道交易发生的时间，发生交易的双方和用于交易的具体的货币才可能冒充纸质货币的真实持有者参与交易并从中获利。于是，这就构成了一个分布式的防伪系统，整个区域内的每个人，每个认证客户端以至于每张纸质货币都在维护着这样一个防伪屏障。从这个角度来看，整个系统越复杂，即涉及的用户和纸质货币越多，交易发生得越频繁，则防伪效果越好。

3.2.2 假设伪造者伪造自己合法持有的纸质货币

假设伪造者伪造技术十分高超，能够制作出两张一模一样的纸质货币，于是，此时传统纸质货币防伪手段已经失效。而且，由于伪造者伪造的是自己合法持有的纸质货币，因此，伪造者可以掌握被伪造的纸质货币的交易时间，交易对象和用于交易的具体的纸质货币。但是即使是这样，伪造者仍然没有达到其伪造货币并从中获利的目的。因为，无论一张纸质货币有多少份“克隆”，在交易过程中，当该纸质货币从一个用户账户出库解锁并在另一个用户账户中入库加锁之后，该纸质货币就已经不属于原来的用户，即使原来的用户拥有多个该纸质货币的“克隆”也无法连续对同一张纸质货币执行出库解锁操作。

综上可知，即使有多张完全一样的纸质货币，但是从其实际作用的角度来看仍然只相当于一张纸质货币。如此一来，伪造自己持有的纸质货币就失去了造假的意义。

3.3 新型防伪方案与现有货币使用方式的区别与优势

在生活中，我们可以这样认为，存入银行的纸质货币和从银行取出的纸质货币都是合法的纸质货币，而且纸质货币存入银行之后也不会发生丢失或损毁。因此，银行可以被视作一种具有公信力的“实体保险柜”。当我们把纸质货币存入银行，并获取一个存款凭证之后就相当于进行了“入库加锁”。类似的，使用存款凭证将纸质货币从银行中取出就相当于“出库解锁”。只有将纸质货币从银行中取出，也就是进行“出库解锁”，我们才可以在涉及现金的交易中使用该纸质货币。

虽然将纸质货币存入银行较为安全，但由于物理上的限制，用户和实体银行之间几乎不可能实现随时随地的存取操作。这也就意味着将纸质货币存入银行以防伪和防失窃的方法并不能普及到用户的每一笔涉及现金的交易中。

不过，信息技术在提供随时随地的服务方面具有天然的优势。本防伪方案和传统的将纸质货币存入银行并获取到存储凭证的区别在于，本方案中的“入库加锁”和“出库解锁”是基于信息技术实现的，不需要实体银行的参与，用户可以通过终端设备与网络随时随地进行入库加锁与出库解锁操作。同时，标记为入库加锁状态的纸质货币就相当于存入了银行，是一种“虚拟银行”。如果这个虚拟银行由具有公信力的机构运作，则这就是一个具有公信力的“虚拟保险柜”。根据前文的分析，该虚拟保险柜在防伪和防失窃方面能产生和实体银行几乎一样的效果。因此，本方案填补了纸质货币在实体银行之外的环境中所需要的防伪，防丢失等需求的空缺，能够普及到每一笔涉及现金的交易活动中。

在目前的支付方式中，已经实现用户的身份信息与金额的绑定，而在本方案中实现的则是用户的身份信息与具体的每一张纸质货币相绑定，从而产生了防伪和防丢失等优势。

就目前而言，在经济活动中被广泛使用的交易方式有无现金交易和有现金交易两种。其中，无现金交易中的代表有移动支付和信用卡。接下来我们以移动支付为例来说明移动支付在面对涉及现金的交易时所具有的不足。

移动支付在我国已经相当普及，移动支付的安全性和便捷性也已经获得了广泛的认可。但是，一旦在移动支付的过程中混入了现金，则移动支付就无法继续确保整个交易过程中的安全。例如，当 Alice 使用移动支付的方式向 Bob 出借 100 块钱时，Bob 收到的是具有真实价值的 100 块钱，而若 Bob 使用一张伪造的纸质货币向 Alice 偿还借款时，这张伪造的货币并不具有法律上承认的真实价值。因此，混合有现金交易的移动支付仍然面对着纯现金交易所需要面对的防伪问题。而如果使用本文构建的防伪方案就可以把移动支付所具有的安全性等优势延伸到含有现金交易的场景中。例

如，当 Bob 想使用现金向 Alice 偿还借款时，必须使用凭证登陆自己在认证中心的账户，将需要给 Alice 的纸质货币出库解锁，之后 Alice 登陆自己在认证中心的账户，将该纸质货币入库加锁。这样一来，即使 Bob 给 Alice 的是一张伪造的纸质货币，而 Bob 仍然持有对应的那张真实的纸质货币，但由于在认证中心的系统中，Bob 已经将该纸质货币转交到 Alice 的账户中，于是就无法再次将该纸质货币进行出库解锁操作并继续发挥该张纸质货币的购买力。因此，虽然 Bob 持有的这张纸质货币并不是伪造的，但是对于 Bob 而言该张纸质货币已经失去了价值。除非该纸质货币再次在 Bob 的账户中进行了入库加锁操作。

综合来看，本防伪方案相较于移动支付以及信用卡支付的优势就在于，本方案中用户操作的是特定的每一张纸质货币和传统非现金支付方式中操作的仅仅相当于纸质货币的数额。因此，基于本方案可以对交易过程进行更详细的操控，从而产生防伪和防失窃的效果。

4 新型纸质货币防伪技术的扩展应用

4.1 利用新型防伪技术对货币流动的监控

传统的纸质货币在市场上流通时几乎可以认为是匿名的，但是采用新型防伪技术之后，每张纸质货币在任一时间段内都绑定了对应的用户信息，从而实现了一定程度的非匿名性，因此可以实现对一定范围内的金融市场中资金流动情况的全面监控。

4.2 保障个人货币资产安全

采用新型防伪技术的纸质货币可以在发生丢失，失窃和损毁的情况下仍然确保个人货币资产不受损失。

只要纸质货币的合法持有者对纸质货币进行了入库加锁操作，则该纸质货币在入库加锁状态下将唯一属于其合法持有者（纸质货币上的随机字符和一个合法的社会身份信息进行了绑定），那么一旦该纸质货币丢失或损毁，合法持有者可以根据丢失纸质货币上的随机字符向银行等法定机构申请作废原纸质货币（这里的“作废”是指认证服务器会将表示对应纸质货币的字符标记为不再具备购买能力），之后银行可以向被作废纸质货币的合法持有者提供和原纸质货币等额但标识字符不同的纸质货币。这样一来，人们就可以不用担心因纸质货币丢失，失窃或者因火灾，地震等造成的纸质货币损毁带来的经济损失。

另外，由于作废原纸质货币后银行另行提供的纸质货币和原来的纸质货币的随机字符不同，且换取一个新纸质货币的前提是作废原来的纸质货币，这也杜绝了有人恶意提出申诉骗取纸质货币的可能。

总结

该防伪方案可以在完全不依赖纸质货币制造工艺的情况下独立实现一定的防伪效果，而且该防伪方案可以和现有防伪方案共存。施行该方案的过程中不需要对传统纸质货币制作工艺和发行流程做较大的更改。综合来看，该防伪技术具有极强的防伪能力和可操作性。

参考文献：

[1] 龚秒,彭莉.电子防伪技术专利综述[J].科学与财富,2019,(9):144.

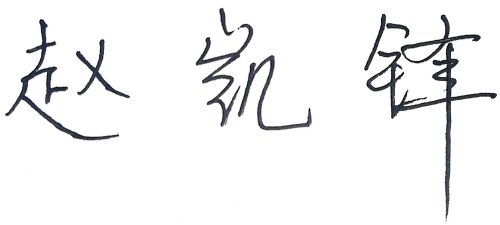
[2] 李方.基于二维码的茶产品防伪系统设计与研究[J].福建茶叶,2018,40(12):19.

[3] 秦宇,梁艳,张楠,付文强.计量检定机构证书报告防伪与防篡改技术的研究[J].中国计量,2019(04):51-52.

[4] 王文雨,孙源,孙忠道.人民币的“草稿”——实验票样[J].金融博览(财富),2019(04):91-93.

[5] 刘心来.日元纸币防伪技术研究[J].中国刑警学院学报,2019(01):98-102.

本文档所属者签名：



数字签名由 赵凯锋
DN： C=CN, OU=https://zhaokaifeng.com/, O=https://zhaokaifeng.com/, CN=赵凯锋, E=zhaokaifengcom@gmail.com
原因： 我是该文档所有者
日期： 2020-01-01 18:45:34