编辑导读：离线支付并不罕见，微信和支付宝早已实现，在手机网络不顺畅的时候，可以享受“先享后付”。但这实质上是一种单离线支付，而数字人民币的“双离线支付”是怎么实现的？有哪些应用场景和面临的安全问题呢？

虎年新气象，开年第一篇，愿新的一年各位小伙伴诸事 666！2022 年将通过 5 篇系列文章对数字人民币实现原理和基础功能进行一一阐述。

在了解数字人民币双离线支付之前，再次科普一次数字人民币钱包是什么。数字人民币钱包分软件和硬件两种钱包形态，软件钱包即此前体验的“数字人民币”钱包，主要以手机 App 形式为主；硬件钱包则是指基于“芯片”存在的钱包，比如智能卡、手机 eSE 等。

其实，离线支付功能并不新鲜，微信和支付宝早已经实现了，这样使得我们在一些场景实现了“先享后付”功能。这种离线支付付款方可以离线，而收款方必须在线，实现原理是将离线的付款信息传到平台服务器端进行校验后完成交易，实质是一种单离线支付。

那么，数字人民币的“双离线支付”是怎么实现的？有哪些应用场景和面临的安全问题呢？

一、实现原理

1. 普通双离线支付

普通双离线支付，即在收付双方都离线的场景下先进行记账，等能做安全验证时再完成扣款。对支付业务来说，它通过交易完成之后的延期请款来完成闭环交易的过程，核心是实现快速的核身和支付的一种技术方案。

2. 数字人民币双离线支付

数字人民币双离线支付采用 NFC 技术来实现，需要收付双方设备具备内置安全芯片的硬件钱包功能，最典型的是数字人民币碰一碰功能，主要满足地下室、停车场、山区甚至是地理灾害等特殊环境下的支付需求。

NFC 是一种近距离高频无线通信技术，传输距离小于 10 厘米，采用点对点通信，无需第三方设备中转传输信号。NFC 手机支持芯片硬件加密和软件加密，不到 0.1 秒就可以完成点对点的加密通信，保证了支付安全。

双离线支付是数字人民币创新场景的一个重要方向，彻底脱离了网络对移动支付行为的约束。

二、应用场景

双离线支付是数字人民币创新场景的一个重要方向，彻底脱离了网络对移动支付行为的约束。

双离线主要支付形式是通过“碰一碰”来达到的。具体而言，包括手机与 NFC 标签的碰一碰、手机与手机的碰一碰、手机与 POS 机的碰一碰。而只有具备硬件钱包功能的手机与手机、手机与 POS 机之间才可以实现双离线支付功能。

双离线支付一般用于公交等小额支付场景，以此来降低“双花”风险。

下面主要针对公交双离线支付应用场景对双离线支付进行拆解：

公交乘车-双离线支付流程：

1.在网络条件好的情况下，乘客先把金额充值到载体中，乘车二维码、IC 卡（公交卡）或者手机钱包（华为、小米钱包）中；

2.基于 IC 技术或者 NFC 技术实现离线刷卡。在线刷卡都比较好理解，离线刷卡无非就是先记账，等网络通了以后通过延期请款来完成闭环交易，业务系统进一步跟数字人民币中心进行结算；

3. 乘客钱包余额充足，即可正常完成扣款。因在完成扣款前乘车业务系统无法获知乘客钱包余额，因此会存在钱包余额不足导致扣款失败的情况；

4.乘车业务系统与公交公司完成车票款项结算，交易完成。

垫付和追缴的机制：

如乘客钱包余额一直不足抵扣车票款项，乘车业务系统就会存在坏账的情况。此时，业务系统就需要拥有垫付和追缴的机制。追缴机制一般通过限制乘客最多可欠款的乘车次数来控制，达到一定的欠款次数乘客无法再次使用乘车服务，直到补齐欠款；垫付一般由业务系统合作方来承担坏账金额。以上垫付和追缴机制同样适用于地铁乘车等小额高频场景，主要应用城市有北京亿通行、青岛琴岛通、深圳通和天府通等城市。

三、安全问题及应对措施

1. 面临的安全问题

通过了解，数字人民币的碰一碰支付背后的技术其实是 NFC 技术，它比二维码扫码要安全得多。不过“双离线支付”也面临较高的安全风险，有人可能利用当中的时间差作恶，比如将同一笔数字货币重复花几次，在现实中这是克隆的假币，而在线上世界只要复制数字货币的核心数据，这就行业中所说的“双花问题”（DoubleSpending）。这就也是我们最担心的安全问题。为了防止“双花”，第三方支付平台需要对每一笔交易进行验证，而“双离线支付”却无法在第一时间进行验证，因此双离线支付”一般只用于公交等小额支付的场景，以此来降低风险。

2. 安全应对措施

一是基于风控制度，在交易安全机制方面主要对双离线支付的交易时间和次数加以限制。

双离线支付在“交易时间”和“交易次数”方面均有限制。双离线支付的交易时限是为 4 小时，次数为 10 次。无论是卡式还是手机的双离线支付，都有一定的“离线可用次数”，即在双离线支付的情况下，付款方仅可以使用有限次数的双离线支付。当“离线可用次

数”消耗尽时即需要通过某种通讯手段与数字人民币的钱包后台进行同步，使硬件钱包里的钱与数字人民币钱包后台的钱保持一致。

对于双离线使用次数的限制，一方面是由于硬件钱包的储存容量问题，硬件钱包的容量目前比较小，而双离线交易下需要将币串和信息存储在本地，这导致可存储的币串有限，间接地影响了交易笔数上限。另一方面，目前由于低功耗下硬件钱包芯片的算力有限，离线交易次数过多，会造成交易时间过长，从而影响交易时间和效率。

第二个是垫付和追缴的机制。

前文公交场景中已作了描述，这里不再赘述。

四、数字人民币碰一碰

数字人民币的碰一碰支付安全吗？会不会随便什么人拿个手机碰一碰我的手机就把我的钱偷走了呢？答案是，肯定不会。手机碰一碰不会直接付款。碰一碰之后，还要输入支付金额，以及输入支付密码或者指纹才能完成转账，步骤跟现在的扫码支付类似。

数字人民币碰一碰要比扫码支付方便，扫码支付遇到网络不好或者光线不好，是无法完成支付的。数字人民币碰一碰只要在 10 厘米范围以内，碰一碰，就可以完成支付，支付体验和安全要优于扫码支付。

五、结束语

硬件钱包的双离线支付功能更好地体现了数字人民币支付即结算的天然属性。数字人民币将会采取事后追责机制，以对不良交易记录进行惩戒（在征信系统中实现），也就是说，如果联网后在验币处理时，系统判断硬件钱包出现伪币或者双花现象，该钱包将被列入黑名单，钱包也将处于停用状态。且用且珍惜！！

作者：沐沐，公众号“沐沐讲数币”运营号主，“数字人民币支付产品”专家、特邀讲师。曾任职于某上市支付公司，N 年支付产品汪一枚（支付界老油条）。做过几年聚合支付系统建设，经历过数字人民币支付场景从 0 到 1 的搭建的过程。