中国专利奖申报书

（发明/实用新型）

专 利 号：ZL201810543449.0

专利名称：数字资产的离线支付方法、付款端、收款端及存储介质

申报单位：招商银行股份有限公司

推荐单位：中国银行业协会

二〇二二年 十 月 十七 日

国家知识产权局制

一、 申报项目基本信息

专利号	ZL201810543449.0		
专利名称	数字资产的离线支付方法、付款端、收款端及存储介质		
专利权人	招商银行股份有限公司		
发明人	张育明、潘海清、陈鹏		
IPC 主分类号	G06Q20/32		
是否在国家专利密集型产品备案认定试点平台上备案	否		
通讯地址 /邮编	广东省深圳市福田区深南大道7088号招商银行大厦 /518000		
联系人 [1]	陈鹏	**手机 [1]**	15691805618
办公电话 [1]	0755-86205685	**电子邮箱 [1]**	chenpeng9@cmbchina.com
联系人 [2]	黄凯峰	**手机 [2]**	13713938908
办公电话 [2]	0755-89271758	**电子邮箱 [2]**	kaifenghuang@cmbchina.com
推荐单位	中国银行业协会		

二、专利质量评价材料

（一）新颖性和创造性：

1. 技术背景

当前的数字资产并未充分考虑离线状态的用户支付和交易，而 在某些特定场景下，如网络环境差、无网环境，用户对于离线支付的需求是普遍存在的。基于该背景，本专利提出了一种在离线环境下可以完成数字资产支付的方案。

2. 技术方案

专利针对用户处于网络状况较差环境、甚至没有网络的情况下(比如地铁、偏远山区等)，无法进行支付的问题，提出了一种硬件钱包内置安全芯片的解决方案，硬件钱包可以存储部分UTXO作为离线数字资产，并能存储相关的离线交易。离线状态下用户只能花费这部分离线数字资产，此时交易会先在硬件钱包安全芯片中接收、执行，存储在离线交易列表中，联网状态下第一时间完成全网广播与确认，更新数字资产的全局状态，解决了当前数字资产在网络环境差、无网环境下等离线状态无法完成支付的问题。

支持离线交易的数字货币钱包客户端可临时存储部分UTXO及待处理交易，离线交易只能花费这些临时存储的UTXO，当用户钱包联网后首先处理钱包中待处理交易，更新UTXO信息，再进行其他在线交易。以用户A面对面向用户B离线转账为例介绍离线交易的过程，如下图1所示。

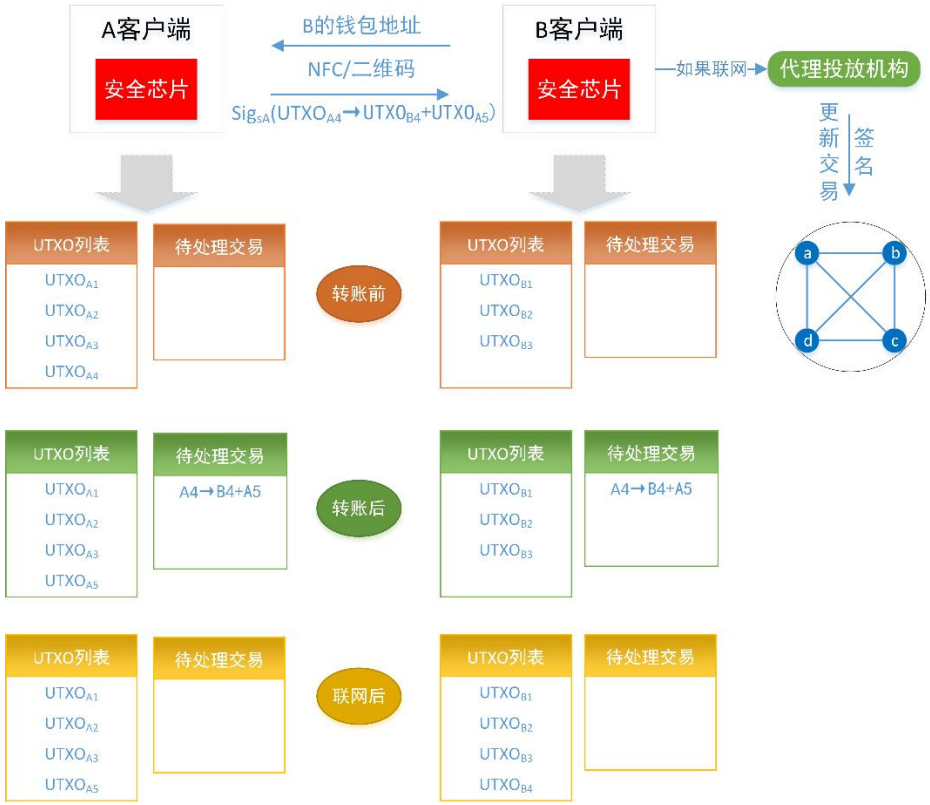

图1离线交易示意图

用户A通过NFC或二维码等方式获取用户B的钱包地址，在安全芯片中对转账交易信息做签名。签名后的交易信息加入客户端的待处理交易列表，同时通过NFC或者二维码等方式将签名后的交易信息以及用户A的证书发送给用户B。用户B验证用户A的身份以及A的交易签名是否正确，如果正确则加入待处理交易列表。当用户A或者用户B联通网络时，通过代理投放机构更新同步该离线交易到数字货币网络。如果A再用UTXOA5给C转

账UTXOC1，则交易A5→C1+A6需要等待交易A4→B4+A5确认之后才能确认。

离线支付模式中，可能存在付款方伪造的可能性，因此需要严格控制数字货币钱包客户端本地临时存储的UTXO列表及读取控制权限，限制离线支付金额大小，增加客户端之间交互的双向认证，降低数字货币钱包客户端伪造的概率，减少收款人权益受损的可能性。如果客户端软件存在漏洞，被用户A恶意更改过，则UTXOA4可能是伪造或者已花费的，联网后交易被确认是非法的，用户B可能会收不到钱。一种可能的事后解决措施是B提供用户A签名过的待处理交易记录让权威机构裁决，对用户A实行加倍罚款惩罚。由于用户只有一个客户端且一个UTXO不可能花费两次，所以用户转账资金最终会同步到数字货币网络账本。

（二）实用性：

数字人民币双离线支付场景。

（三）文本质量：

1.说明书已清楚、完整地公开发明的内容，并使所属技术领域的技术人员能够理解和实施。

说明书已清楚、完整地公开发明的内容，专业术语使用正确，其内涵和外延表述恰当，并使所属技术领域的技术人员能够理解和实施。该专利对工作原理和流程阐述清楚完整，表达方式符合专利法规要求。

2.权利要求书清楚、简要。

权利要求书共10项权利要求。

权利要求1要求保护一种数字资产的离线支付方法，包括以下步骤：

1）在接收到离线支付指令时，根据离线支付指令和UTXO生成对应的UTXO消耗记录

2）根据收款地址将UTXO消耗记录发送至收款端；

3）在接收到收款端返回的确认信息时，根据UTXO消耗记录更新UTXO，获得二次UTXO，并将UTXO消耗记录存储至待处理信息库中；

4）在与交易服务器连接成功时，将待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新付款端的个人数字资产账户。

权利要求2要求在接收到二次离线支付指令时，进一步判断所述UTXO消耗记录是否已同步至所述交易服务器。

权利要求3要求在与交易服务器连接成功时，进一步判断待处理信息库中是否存在未同步的UTXO消耗记录。

权利要求4要求在接收到在接收到离线支付指令时，判断所述离线支付指令包括的支付金额是否小于预设支付阈值，和/或判断所述付款端在预设周期内的离线支付指令接收次数是否小于预设接收阈值。

权利要求5要求在接收到付款端发送的UTXO消耗记录时，需进一步判断UTXO消耗记录包括的付款端身份信息验证所述付款端是否可信。

权利要求6要求在更新收款端的个人数字资产账户之后，还应根据已同步的UTXO消耗记录生成对应入账UTXO。

权利要求7要求付款端的本地至少存储有一个UTXO，包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的离线支付程序，离线支付程序执行时，能实现如权利要求1至4中任一项所述的数字资产的离线支付方法的步骤。

权利要求8要求收款端包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的离线支付程序，离线支付程序执行时，能实现要求5至6中任一项所述的数字资产的离线支付方法的步骤。

权利要求9要求存储介质上存储有离线支付程序，离线支付程序执行时，能实现如权利要求1至4中任一项所述的数字资产的离线支付方法的步骤。

权利要求10要求存储介质上存储有离线支付程序，离线支付程序执行时，能实现如权利要求5至6中任一项所述的数字资产的离线支付方法的步骤。

3. 权利要求以说明书为依据，保护范围合理。

权利要求1至10保护了一种数字资产的离线支付方法，通过一个实际的例子介绍离线交易的过程，对权利要求的技术方案予以充分的说明，本领域的技术人员能够从说明书中公开的内容得到或概括得出的技术方案。因此，参评专利权利要求可以得到说明书的支持。

独立权利要求1及其从属权利要求2-10均涉及适合数字资产离线支付方法，权利要求1的保护范围最大，从属权利要求2至10对独立权利要求进行了细化，进一步阐述了支付过程中的细节问题。参评专利权利要求呈现了一个层层递进、宽窄适宜的保护范围。

三、技术先进性评价材料

（一）技术原创性及重要性：

本专利属于基础型专利。

1.解决无网络环境下的支付问题

不管是实体银行卡支付，还是手机支付，都受制于网络环境，网络一旦中断，支付便不能进行下去，给用户带来不好的支付体验，本专利解决了无网络环境下的支付问题，极大的提高了便捷性，提升了用户体验。

2.支付过程引入UTXO概念，便于交易追溯和纠纷裁定

通过UTXO，可以很方便的追踪每一笔交易的来龙去脉，避免资产凭空产生、消失等情况发生，同时也为发生经济纠纷时提供了直接的证据。

（二）技术优势：

通过对公开文献进行检索，在该专利申请日之前，未发现类似专利，属首创。

（三）技术通用性：

该专利技术未来可应用于数字人民币的离线支付场景。

四、运用及保护措施和成效评价材料（一）

（一）专利运用：

无。

（二）专利保护：

1.及时取得专利申请，一旦有新的研发成果，首先想到去申请专利，申报了核心专利后立即申请了一批外围专利，同时为了防止竞争对手申请改进型专利，形成专利池实施保护。

2.及时收集与公司专利有关的特别是同行业此类技术信息，并得到求证，如果有涉嫌侵犯我公司专利的个人及单位，我们及时查证。

（三）制度建设及条件保障和执行情况：

1.知识产权管理标准化建设情况

单位内部形成严格的专利申请审批流程，保证专利质量和实质性内容的最大化公开和保护；外部聘请专业的知识产权代理公司，为单位提供专利权、著作权的代理申请服务，便于快速、有效的申请各项知识产权；聘请知识产权局专家对企业员工进行了知识产权方面的培训，增强企业内部人员知识产权保护意识；成立法律合规部，便于知识产权保护相关法律诉讼。

2.当检索到专利被侵权时，公司法务部门积极进行维权，维护本单位的权益。

运用及保护措施和成效评价材料（二）

（四）经济效益

自行实施情况[1]

时间 / 项目	实施日至 2021 年底	2020 年初至 2021 年底
产量	0	0
新增销售额（万元）	0	0
新增利润（万元）	0	0
新增出口额（万元）	0	0

经济效益说明（或列表）：（500 字以内）

无。

注：应写明经济效益计算过程，并附经济效益证明材料。可提供有资质的会计师事务所出具的参评专利经济效益专项审计报告等作为经济效益相关证明材料。

专利许可情况[2]（可加行）

被许可单位	许可金额（万元）	至 2021 年底许可收入（万元）	许可种类	是否进行许可合同备案
无				

[1] 对于主要依靠参评专利取得市场竞争优势的，应当提交参评专利涉及的产品在国家专利密集型产品备案认定试点平台上备案成功的相关证明。

[2] 填写专利许可情况的，应当提交专利实施许可合同备案证明。许可种类填写独占许可、排他许可、普通许可等。

许可合计（万元）				
专利出资情况（可加行）				
单位名称	出资金额（万元）			
无				
出资合计（万元）				
专利融资情况[3]（可加行）				
单位名称	融资金额（万元）			
无				
融资合计（万元）				

[3] 填写专利质押融资情况的，应当提交专利权质押登记通知书。

五、社会效益及发展前景评价材料

（一）社会效益状况：详细说明参评项目对促进技术进步、提高科学管理水平、保护自然资源与生态环境、消除公害污染、安全生产、改善劳动条件、医疗保健、保障国家和公共安全、提高人民物质文化生活水平、引领消费习惯等方面所起的作用。如能采取定量方法说明的，均需有具体数字。

（二）行业影响力状况：详细说明参评项目实施对行业发展及技术趋势的影响。

（三）政策适应性：详细说明参评项目属于国家政策明确鼓励、支持的，还是限制、禁止类别，或无明确导向，并具体说明原因。

（一）社会效益状况：

随着互联网的快速发展，数字资产被广泛研究并应用，给用户带来全新的资产管理和支付的体验，并且能够减少实物资产所带来的安全性问题。只需带上一部手机，就可以pay anywhere，但这是基于一个前提的，那就是你所处的支付环境必须能够连接网络，否则无法进行，像电梯、地下室、偏远山区这些地方，网络可能就没有覆盖到，用户通过电子支付就是支付不了，而这些又是非常关键的支付场景，可能影响用户的衣食住行等日常生活，这无疑给用户带来不好的体验，是很多电子支付模式的“通病”。

本专利提出了一种在离线环境也能完成支付的方法，有助于突破现有电子支付的局限性，真正实现pay anywhere，为用户带来无忧、便捷、顺畅的支付体验，同时也有利于资金的快速流通，促进社会经济的发展。

（二）行业影响力状况：

无。

（三）政策适应性：

随着数字人民币落地速度的加快，试点城市也在进一步扩大，覆盖领域越来越多，国家扎实稳妥推进数字人民币试点工作，意在推进人民币国际化进程，满足实体经济金融服务的需求。

数字人民币的亮点之一是其双离线支付的特性，即收付款双方在无网络的条件下，只需碰一碰就能完成支付。本专利也提出了一种离线环境下支付的方法，为双离线支付实现提供了一个思路，适应现有政策发展。

六、获奖情况

获奖情况：简要列出参评专利何时何地获何种等级的奖励及其颁奖单位等情况，按奖项重要程度排序（ 500 字以内）。

专利成果在2018年中国支付清算协会组织的“数字货币重点课题”活动中，获评优秀课题成果，在进入最终评比的34份作品中排名第2，被编入优秀课题成果集。