doi:10.11959/j.issn.1000-436x.2017121

基于代理的密码货币支付系统

傅晓彤，陈思，张宁
（西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘 要：利用区块链技术实现的去中心化的密码货币被誉为有史以来最成功的密码货币。用户以公钥作为账户地址，使交易具备匿名性，即隐私的可保护性。然而区块链上记录的交易信息，会给用户隐私带来潜在的泄露威胁；此外，为了防止重复花费，系统约定只有在目标区块之后又有 k 个后续区块产生才能确认该目标区块上的交易是有效的，这段等待后续区块生成的时间较长，大大降低了交易效率。针对以上问题，提出一种基于代理的密码货币支付系统模型，并给出了基于盲签名算法的实现方案，通过在支付阶段引入代理，缩短了交易确认时间，提高了交易效率，同时，更好地实现了用户的匿名性即隐私保护功能。
关键词：密码货币；区块链；盲签名；匿名性
中图分类号：TP391 **文献标识码**：A

Proxy-cryptocurrency payment system

FU Xiao-tong, CHEN Si, ZHANG Ning
(Institute of Network and Information Security, Xidian University, Xi'an 710071, China)

Abstract: The decentralized cryptocurrency which was based on block chain has been thought the most successful one in history. In the system, public keys were used as the users' accounts which guaranteed the anonymity in real transactions. However, all the transaction information was recorded in the block chain, it was a potential threat for users' privacy which might leak the payment information. Moreover, to avoid double-spending, it was agreed that the transaction on the target block was valid only if another k blocks were generated after the target one. The long waiting time reduced the efficiency of the payment system. A model of payment system based on a proxy-cryptocurrency was proposed, and a solution based on blind signature techniques was proposed. The scheme introduced a proxy in the payment phase, by which transaction confirmation time could be reduced and the transaction efficiency could be improved. Meanwhile, the system implements better anonymity, namely as the privacy protection function.
Key words: cryptocurrency, block chain, blind signature, anonymity

1 引言

密码货币是现代计算机通信技术高速发展的产物，是货币作为支付手段不断进化的表现。密码货币应用密码学技术来实现数字货币的安全性和高效性，给人们的生产和生活带来了极大的便利。在现有的密码货币中，利用区块链技术实现的密码货币是目前最流行的，占用资源较少的 SPV 客户端的实现[1,2]使这种去中心化的密码货币更加实用。去中心化的密码货币于 2008 年被提出[3]，并且在 2010 年 5 月实现了第一笔交易[2]。去中心性是指密码货币的发行和交易不依赖于任何金融中心，具有点对点性质。去中心化的密码货币使用一个公共总账，即区块链来记录交易，从而避免了重复花费，并且通过网络节点的计算来发行货币。这使密码货币具有类似黄金的良好货币性能，从根源上解决了

收稿日期：2016-10-31；修回日期：2017-03-09
基金项目：国家自然科学基金资助项目（No.61402351）；教育部留学回国人员科研启动基金资助项目（No.BK16015010002）；“111 计划”基金资助项目（No.B16037）
Foundation Items: The National Natural Science Foundation of China (No.61402351), Scientific Research Foundation for the Returned Overseas Chinese Scholars, Ministry of Education (No.BK16015010002), China 111 Project (No.B16037)

通货膨胀问题。

区块链由被称为矿工的匿名参与者维持，矿工们通过执行所谓的共识协议来维持和扩展区块链。执行协议的过程就是生成新的区块的过程。为了生成新的区块，矿工需要对一定难度的数学难题进行求解，即“工作量证明”(POW)。矿工每生成一个区块，就会获得相应的报酬，这意味着每生成一个块，就有新的货币生成。区块链系统会自动调整数学难题的难度，平均每 10 min 能够生成一个新的区块，区块上记录已经被矿工验证过的合法的交易信息。交易一旦被发布在区块链上，并且其后又有 k 个区块生成，则认为该交易确实是有效的[4]，这样做是为了避免攻击者进行重复花费，即“双花”[5]。具体地说，假设攻击者想要篡改自己的交易记录，他需要重新计算该区块对应的数学难题的解，不仅如此，该区块散列值的改变将导致其后所有区块对应难题的解都改变，也就是说，攻击者需要计算当前交易所在区块以及其之后所有区块对应的解。由于诚实的矿工总是在最长的链生成新的区块，因此，攻击者要使篡改后的链长度至少与正常链长度相等才能被大多数矿工接受。这就要求攻击者至少拥有整个网络 51%的计算能力[6]。假设在记录有交易信息的区块之后又新生成了 k 个区块，则随着 k 的增大，攻击者能够成功“双花”的概率将以 k 的指数级降低。一般来说，$k=6$ 就可以认为交易是有效的[3]。

由此看来，区块链的固有属性导致了交易延迟。为了安全起见，要等待至少 6 个区块才能确认付款有效，一个区块的生成大约需 10 min，那么确认付款时间至少为 1 h。除此之外，使用区块链这个公共总账来记录交易信息带来了潜在的隐私泄露问题。公钥账户与用户真实身份没有关联，这种通过“假名”来实现的匿名性并不完善。攻击者可以通过追踪 IP 地址[7]以及分析区块链上交易的拓扑结构来暴露用户的隐私即去匿名性[8,9]，随着区块链的增长，公布的交易信息越多，去匿名性就越容易。

本文通过引入一个代理作为实际的付款方，解决了交易延迟的问题，同时达到了更好的匿名性。通过引入具有可信公钥地址的代理，减少了交易确认时间，使用部分盲签名算法和一次性公钥地址，更好地保护了用户的隐私。代理的引入并没有改变底层的协议，因此，与原有的区块链系统完全兼容。

2 背景知识

2.1 基本原理

以区块链为基础实现的密码货币主要涉及三大核心技术：交易构造、共识协议和通信网络。

交易构造利用了 ECDSA、SHA-256 等密码学算法，每个交易由输入、输出和相关参数构成。交易的输入为付款方的公钥地址，输出为收款方的公钥地址（实际为公钥地址的散列值）。输入的货币数量必须大于或等于输出的货币数量，二者之差将作为交易费用奖励给矿工。交易中的签名是付款方用自己的私钥生成的对整个交易的签名，该签名是验证本次交易合法性的依据之一。图 1 可以简单地描述交易的结构，在左边的交易中，A 为付款地址，B 和 C 为收款地址，σ_{A} 为 A 的所有者的签名。在右边的交易中，B 又作为付款地址和收款地址，D 为收款地址，σ_{B} 为 B 的所有者的签名。

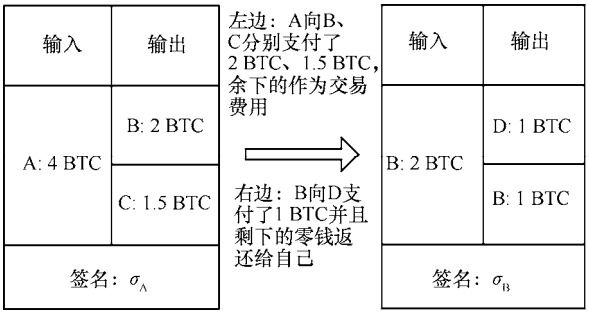

图 1 交易结构

共识协议是矿工维持和扩展区块链的协议。共识协议可以简单描述为：节点创建交易并广播，矿工首先验证交易的合法性，包括签名的正确性、交易输入地址的合法性以及货币数量的合法性等。其次，矿工将所有合法的交易集合成一个数据块作为候选区块，并进行大量的散列计算，从而找到该数据块对应数学难题的解（即 *Nonce* 值）。最后，一旦找到解则将该数据块向网络中广播。其他矿工验证该数据块的 *Nonce* 值和交易信息等其他数据信息的合法性，若合法，其他矿工将该区块作为父区块，继续挖矿。至此，该区块就作为一个新生的区块被添加到区块链末端。

交易和区块正是依赖于区块链系统的无中心的、点对点的通信网络进行广播，网络中的所有节点都是平等的，网络的拓扑结构也是随机的。网络使用了泛洪算法，只需要几秒，网络里的所有节点

都能收到消息。

2.2　椭圆曲线数字签名算法

椭圆曲线数字签名算法（ECDSA）由参数生成、密钥生成、签名生成和签名验证 4 个算法构成[10,11]。区块链上的交易使用的 ECDSA 是基于曲线 secp256k1 的，各参数如文献[12]所示。椭圆曲线数字签名算法各步骤及符号表示如下。

Setup ：系统参数生成算法。输出公共参数 $pp=(F_q,a,b,G,n)$，其中，a、b 为椭圆曲线的参数，F_q 为选定的有限域，G 为基点，n 为 G 的阶。

$KeyGen(d,pp)$ ：密钥生成算法。随机选择整数 $d\in[1,n-1]$ 计算 $Q=dG$，其中，Q 为公钥，d 为私钥。即输入参数 pp 和随机整数 d，输出公私钥对。

$Sig(d,m)$ ：签名算法。输入私钥 d 和待签名消息 m，输出关于消息 m 的签名。

$Verify(Q,Sig(d,m))$ ：验证算法。输入公钥 Q 和消息 m 的签名。若签名合法，则输出 1；否则，输出 0。

2.3　部分盲签名算法

部分盲签名算法[13]主要包括系统生成、密钥生成、签名发布和签名验证 4 个算法。其中，签名发布算法由消息盲化、共识消息生成、签名和去盲这 4 个步骤构成，是消息拥有者与签名者的交互协议。签名发布算法各步骤以及签名验证算法各符号表示如下。

$Blind(m)$ ：消息盲化算法。输入待签名消息 m，输出盲化后的消息 m^*。

$\tau(c)$ ：共识消息生成算法。输入参数 c，输出关于 c 的共识消息。

$BldSig(sk,\tau(c),m^*)$ ：签名算法。输入私钥 sk，共识消息 $\tau(c)$，盲化后的消息 m^*，输出部分盲签名 σ^*。

$Blind^{-1}(\sigma^*)$ ：去盲因子算法。输入部分盲签名 σ^*，输出 m 的签名 σ。

$Rl(m,\tau(c))$ ：关系函数。输入消息 m，共识消息 $\tau(c)$，输出签名 σ，表示 σ 是 m 的签名，且共识消息为 $\tau(c)$。

$BldVer(pk,\sigma)$ ：签名验证算法。输入公钥 pk 和签名 σ，若签名合法，则输出为 1；否则，输出 0。

2.4　匿名性技术

区块链作为一个公共总账，任何人都可以访问，为了解决由此带来的隐私问题，目前主要有 2 种思路提高匿名性：一种是通过使用替换币即 Altcoin 的方式达到更强的匿名性；另一种则是使用混币技术实现公钥地址的混淆。

Altcoin 是通过将密码货币兑换为替换币之后再换回的方式来实现混淆从而提高匿名性。文献[14]中的 Zerocoin 协议以及文献[15]中的 Zerocash 协议就是利用这种思路来实现更强的匿名性，然而，替换币的引入改变了底层协议，与原有系统不兼容。

对于无混币中心的混币技术，由参与用户共同生成混币交易。交易的输入是各用户混币前的地址，交易的输出是各用户的目的输出地址，混币交易必须含有所有参与用户的签名才是合法的。其中，最典型的协议是 CoinJoin[4]，CoinJoin 在保证匿名性的同时确保用户资金不会被窃取，然而该协议容易受到恶意用户的 DoS 攻击。CoinShuffle[16]在 CoinJoin 的基础上增加了排序协议达到了匿名混币效果，并且增加了问责协议，从而削弱了恶意用户的 DoS 攻击。

有混币中心的混币技术通过混币中心为用户混币。混币中心的引入提高了系统的可靠性，能实现较大规模的混币以达到更好的混币效果，并且能够抵抗 DoS 攻击。其中，MixCoin 协议[17]为了避免混币中心泄露用户输入输出账户地址，利用多个混币网络实现多级混币。BlindCoin 协议[18]则是在 MixCoin 的基础上引入了一个公共账簿，用该公共账簿来保证混币中心的可靠性，利用盲签名算法使用户的输出账户对混币中心不可见，不再需要多级混币。

3　有混币中心的混币系统

有混币中心的混币系统的代理参考了 MixCoin 协议中混币中心的模型，MixCoin 协议的目标是实现混币以提高匿名性，而系统的主要目的是利用不会进行“双花”的代理作为支付中介以提高交易效率，故本文将略去 MixCoin 协议中的无关细节，仅介绍相关核心协议。

3.1　MixCoin 系统模型

该系统拥有 2 个对象：混币中心 S 和用户 Alice。

混币中心：假设混币中心 S 拥有一对长期使用的签名公私钥对，如果混币中心的信誉不好，将会减少用户量。

用户：假设用户 Alice 在某个账户拥有一定数量的密码货币（该账户可能与用户 Alice 的真实身份关联）并且希望将该账户的所有货币转移到新的

账户，而任何攻击者都无法窥探新旧账户的关联。

3.2 MixCoin 协议

现将 MixCoin 协议的关键步骤描述如下。

1) Alice 将 $\langle m, t_1, K_{\text{in}}, K_{\text{out}}, D\rangle$ 发送给 S。

2) 如果 S 接受 Alice 的混币请求，则将 $\{w, t_1, t_2, K_{\text{in}}, K_{\text{out}}, K_{\text{esc}}, D'\}_{K_S}$ 发送给 Alice，其中，w 为货币数量，t_1 为 Alice 承诺支付给 S 相应量货币的截止时间，t_2 为 S 将同样多的货币返回给 Alice 的截止时间，K_{in} 为 Alice 混币前的账户，K_{out} 为 Alice 混币后的账户，K_{esc} 为 S 的收款地址，D 和 D' 为系统参数，K_S 为 S 的签名私钥。由于某些原因，S 可能会拒绝 Alice 的混币请求，则双方退出协议。

3) Alice 在截止时间前将一定数量的货币支付给 S，则区块链上会显示 Alice 的支付信息；否则，S 退出协议。

4) S 在截止时间前将对应量的货币返回给 Alice，则区块链上会显示 S 的支付信息；否则，如果 Alice 没有收到付款，则 Alice 公开步骤 2)中获得的 S 的签名，并且区块链上显示了 Alice 的付款信息，可证明 Alice 诚实地执行了协议，S 的信誉将受到损害。

基于代理的密码货币支付系统中的代理模型参考了 MixCoin 协议中混币中心 S 的模型。

4 系统描述

基于代理的密码货币支付系统有 3 个对象，分别为代理（M）、用户（User）和商家（Vender）。系统结构如图 2 所示。

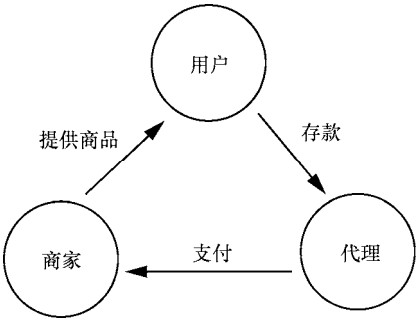

图 2 系统结构

4.1 系统模型

M：假设代理 M 拥有一对长期使用的签名公私钥对，如果 M 的信誉不好，将会减少用户量。此外，假设代理不会有“双花”行为。

User：假设用户 User 在某个公钥地址拥有一定数量的密码货币（该公钥地址可能与 User 的真实身份关联，也可能无关），用户 User 想使用该账户的货币付款且希望交易能够快速完成，同时，不想让任何攻击者获取自己的购物信息。

Vender：假设与 M 签有相关协议，M 是商家 Vender 的担保人，商家 Vender 接收 M 账户的付款。假设 Vender 拥有 2 对长期使用的签名公私钥对，如果信誉不好，会减少客户量。

4.2 相关符号说明

σ_{C}：存款承诺，代理生成的签名。

σ_{M}：账户余额信息的签名。

T：时间戳。

w：密码货币的数量。

t_1：存款时用户向 M 支付的截止时间。

v_{upk}：用户存款时的公钥地址。

v_{tpk}：M 长期的可信任公钥地址。

M_{prv}：M 长期的签名私钥。

P：每次交易的一次性公钥地址。

P^*：盲化后的一次性公钥地址。

σ_{Vender}：商家生成的交易承诺，问责步骤中使用。

σ^*_{User}：盲化的支付信息。

σ^*_{Pay}：含有盲因子的支付承诺。

σ_{Pay}：支付承诺，凭此向 M 请求支付。

σ_{receive}：收货凭证，由用户生成的签名。

$H_s(\cdot)$：将椭圆曲线上的点序列化的函数。

4.3 具体过程

本文系统可以描述为初始化、交易开始和交易完成这 3 个阶段，如图 3 所示。系统整个流程由 7 个步骤组成，其中，初始化阶段为步骤 1)和步骤 2)，交易开始阶段为步骤 3)~步骤 5)，交易完成阶段为步骤 6)和步骤 7)，具体描述如下。

1) 系统建立

各方生成相应的公私钥对。

2) 存款协议

① 用户将 (m, t_1, v_{upk}) 发送给代理，申请存款。

② 如果代理接受申请，则将 σ_{C} 发送给用户；否则，退出协议。

③ 用户在截止时间 t_1 前将公钥地址 v_{upk} 的货币支付给代理。

④ 代理收到用户的货币后，生成签名 σ_{M} 并发送给用户，σ_{M} 是用户的付款凭证；否则，退出协议。

⑤ 如果用户没有收到 σ_{M}，则公开步骤②中的签

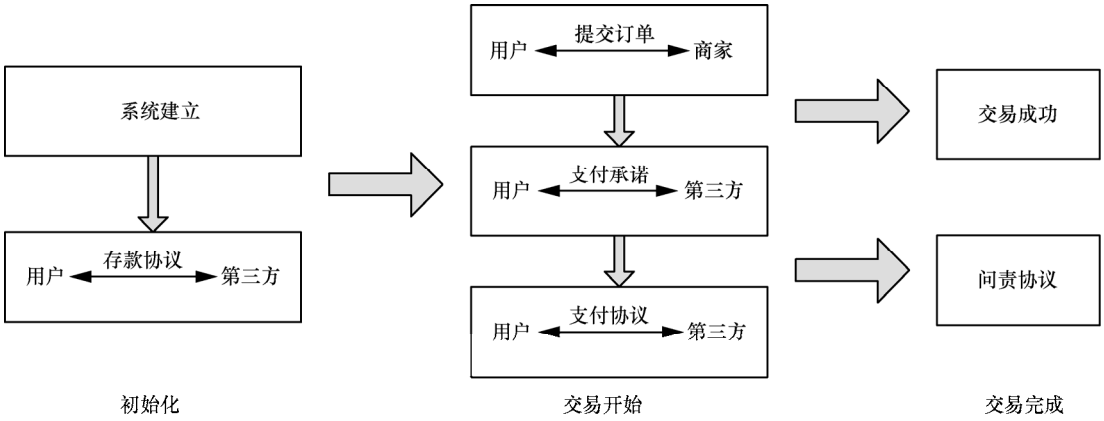

图 3　系统流程

名。区块链可以证明用户已向代理的公钥地址付款。

3) 提交订单

① 用户为本次交易生成一次性公钥地址 P，并将相关参数发送给商家。该地址是用户在本次交易中向商家付款的地址。

② 商家收到参数后计算得到步骤①中的一次性公钥地址。

③ 商家生成签名 σ_{Vender} 作为交易承诺并将其发送给用户。当商家出现恶意行为时, 用户公开该签名。

4) 支付承诺

① 用户将 σ_{M} 及盲化后的含有付款地址的支付信息 σ^{*}_{User} 发送给代理。

② 若签名合法，代理调用部分盲签名算法, 生成嵌入有共识信息的盲签名 σ^{*}_{Pay}。

③ 代理对用户的最新余额等信息进行签名得到 σ'_{M}，连同 σ^{*}_{Pay} 一起发送给用户。

5) 支付协议

① 用户将 σ^{*}_{Pay} 去盲后得到含有付款地址的支付承诺 σ_{Pay}, 并使用匿名身份(如 Tor 技术[19])将 σ_{Pay} 发送给代理。

② 代理验证 σ_{Pay} 的合法性，若合法则向 σ_{Pay} 中的一次性公钥地址 P 支付相应数量的货币。

6) 交易成功

①商家一旦在区块链上看到代理向一次性公钥地址 P 付款。则不用等到此区块之后出现 k 个区块，就立即履行交易承诺，例如给用户发货。

② 用户收到商品时，生成签名 σ_{receive} 作为收货凭证发送给商家，协议结束。

7) 问责协议

① 恶意商家没有履行交易承诺：用户将 σ_{Vender} 发送给代理并公开，如果代理在区块链中找到对应的支付交易，则认为商家作弊。

② 恶意用户诽谤商家没有履行交易承诺：商家公开 σ_{receive} 证明用户已经确认收货。

本文系统的 M 与 MixCoin 协议中的 S，都是基于信誉的，如果 M 或 S 存在恶意行为，用户可以提供证明。MixCoin 中 S 实现的是在某段时间内完成混币, 本文系统中的 M 实现的是根据用户的需要进行付款。在 MixCoin 协议中，利用区块链上用户和混币中心的支付信息是公开的，一旦混币中心未将相应的货币支付给用户，那么区块链上无对应交易，然而用户可在区块链上找到自己向混币中心付款的交易，从而证明混币中心的恶意行为。在基于代理的密码货币支付系统中，用户也是通过区块链上的交易证明自己向 M 付款，与 MixCoin 协议不同的是，一旦 M 不给用户付款，用户公开的是代理的签名，存款协议中的数字签名就是用户的付款凭证。

5　具体方案

下面，给出各步骤的具体实现方案。

1) 系统建立

① M 选择一个长期使用的公钥地址。

② M 调用部分盲签名算法的密钥生成算法生成公私钥对 (pk, sk)。

③ M 选择一对长期使用的密钥 $(M_{\text{pub}}, M_{\text{prv}})$ 作为签名密钥。

④ Vender 选择 2 对长期使用的公私钥对 $(v_{\text{pka}}, v_{\text{a}})$ 和 $(v_{\text{pkb}}, v_{\text{b}})$，使用 2 对密钥是为了生成一次性公钥地址，作为用户的付款地址。一次性公钥地址既在一定程度上保证了匿名性，又能作为 User

的支付凭证。

⑤ User 选择公钥地址 v_{upk} 向 M 存款。

2) 存款协议

① User 将 (w,t_1,v_{upk}) 发送给 M，申请存款。

② 如果 M 接受 User 的存款申请, 计算存款承诺 $\sigma_{\text{C}}=Sig\left(M_{\text{prv}},(w,t_1,v_{\text{upk}},v_{\text{tpk}})\right)$ 并发送给 User。否则，退出协议。

③ User 收到签名后, 以自己的公钥地址 v_{upk} 作为交易输入，M 的公钥地址 v_{tpk} 作为交易输出，创建交易。

④ 如果在时间 t_1 前 M 收到了 User 的付款，M 调用签名算法生成签名 $\sigma_{\text{M}}=Sig(M_{\text{prv}},(v_{\text{upk}},m,T))$ 并发送给 User。否则，退出协议。

⑤如果 User 没有收到 σ_{M}，公开 σ_C，所有人都可以验证 σ_{C} 的有效性并且能够在区块链上找到 User 的付款交易，从而证明 User 诚实地履行了协议。

3) 提交订单

① User 随机选择 $r\in[1,n-1]$，计算 $R=rG$，计算一次性公钥地址 $P=H_{\text{s}}(rv_{\text{pka}})G+v_{\text{pkb}}$。User 将 $R\|msg$ 发送给商家，其中，msg 为订单信息。

② Vender 计算本次交易的收款地址，即一次性公钥地址 $P=H_{\text{s}}(v_{\text{a}}R)G+v_{\text{pkb}}$，同时，计算该公钥对应的私钥 $P_{\text{s}}=H_{\text{s}}(v_{\text{a}}R)+v_{\text{b}}$。

③ Vender 计算 $\sigma_{\text{Vender}}=Sig(v_{\text{b}},(R,msg))$，将 σ_{Vender} 作为交易承诺发送给 User。

4) 支付承诺

① User 首先对一次性公钥地址 P 进行盲化，即计算 $P^*=Blind(P)$，计算盲化的支付信息 $\sigma^*_{\text{User}}=Sig(v_{\text{Usk}},(P^*,w))$ 并将 $\sigma^*_{\text{User}}\|\sigma_{\text{M}}$ 发送给 M，其中，v_{Usk} 为用户的签名私钥。

② M 收到 User 的消息后，调用签名验证算法验证 σ^*_{User} 的合法性, 若合法, 则证明公钥地址 v_{upk} 确实为 User 所有。继续调用验证算法，若 $Verify(v_{\text{tpk}},\sigma_{\text{M}})=1$ 成立，则根据时间戳检查 σ_{M} 是否被使用过，若 M 的数据库中没有出现过该签名且账户余额充足，则 M 计算共识参数 $s=\tau(w)$，M 调用部分盲签名算法的签名生成算法计算 $\sigma^*_{\text{Pay}}=BldSig(sk,\ s,P^*)$，得到嵌入有共识参数 s 的支付承诺。

③ M 更新余额：计算最新的账户余额信息签名 $\sigma'_{\text{M}}=Sig(v_{\text{tsk}},(v_{\text{upk}},w',T'))$，将 $(\sigma^*_{\text{Pay}},\sigma'_{\text{M}})$ 发送给 User。

5) 支付协议

① User 调用部分盲签名算法中的去盲算法计算得到签名 $\sigma_{\text{Pay}}=Blind^{-1}(\sigma^*_{\text{Pay}})=Rl(P,s)$，使用匿名身份 User* 将 σ_{Pay} 发送给 M。

② M 执行验证算法，若 $BldVer(pk,\sigma_{\text{Pay}})=1$ 成立，且该签名是第一次使用，M 向一次性公钥地址 P 付款：创建交易，以 v_{tpk} 作为交易输入，以 P 作为交易输出，交易密码货币的数量为 w。

6) 交易成功

① 商家一旦在区块链上看到 M 的公钥 v_{tpk} 向一次性公钥地址 P 付款。就不用等到此区块之后出现 k 个区块, 立即履行交易承诺, 例如为 User 发货。

② User 收到商品时，用生成一次性公钥地址的随机数 r 作为私钥，计算 $\sigma_{\text{receiver}}=Sig(r,msg)$，签名确认收货。

7) 问责协议

① 恶意的商家没有发货：用户 User 将 $(\sigma_{\text{Vender}},r,(v_{\text{pka}},v_{\text{pkb}}))$ 发送给 M，调用签名验证算法，如果 $Verify(v_{\text{pkb}},\sigma_{\text{Vender}})=1$ 成立，则证明该交易承诺确实为商家所签，计算 $P=H_{\text{s}}(rv_{\text{pka}})G+v_{\text{pkb}}$ 和 $R'=rG$，若满足 $R=R'$，则 P 确实为约定的一次性公钥。在区块链上可以找到以该公钥地址为输入的对应交易，从而证明用户确实已经向商家付款。

② 恶意用户诽谤商家：Vender 公开签名 σ_{receive} 调用签名验证算法，若 $Verify(R,\sigma_{\text{receive}})=1$ 成立，则证明 User 已经收货。

6 系统分析

6.1 一次性公钥地址的有效性

随机选择 $r\in[1,n-1]$，有

$$P=H_{\text{s}}(rv_{\text{pka}})G+v_{\text{pkb}}=(H_{\text{s}}(rv_{\text{a}}G)+v_{\text{b}})G$$

$$P'=H_{\text{s}}(Rv_{\text{a}})G+v_{\text{pkb}}=(H_{\text{s}}(rv_{\text{a}}G)+v_{\text{b}})G$$

所以 $P=P'$，即用户和商家计算得到的为同一个公钥地址 P，对应私钥为 $H_{\text{s}}(rv_{\text{a}}G)+v_{\text{b}}$，并且由于只有商家拥有私钥 v_{b}，因此，只有商家拥有一次性公钥对应的私钥。

6.2 可靠性

1) M 的可靠性

对 M 的可靠性定义为一旦 M 作弊，用户能证

明 M 的不诚实行为，则 M 是可靠的。在本文系统中，如果 M 作弊，用户通过公开 M 的签名以及区块链上的交易信息来证明 M 作弊。

2) 不可伪造性

签名算法的不可伪造性保证了用户不能篡改账户余额，并且只有拥有私钥的用户才能生成包含支付信息的签名。

即使攻击者偷取了合法的包含支付信息的签名并将签名提交给 M, M 也只是将相应量的密码货币转入签名中的公钥地址，由于攻击者没有对应的私钥，依然无法使用对应的密码货币。

6.3 匿名性

被动攻击：能抵御被动攻击。与文献[17]类似，本文系统中所有的被动攻击者都无法将用户的存款账户与一次性公钥地址相关联，即该系统不会额外泄露用户的支付隐私。匿名程度与使用 M 支付的诚实用户的数量正相关。参与用户的数量没有限制，与 M 的资源大小正相关。

主动攻击：无法抵御主动攻击。参与到系统中的主动攻击者能够利用网络攻击[20]使用户认为的匿名集比实际的小很多。关于这个问题，可以通过增加费用等方式提高网络攻击的代价。

M 为攻击者：能够抵御 M 的攻击。利用了部分盲签名算法, 使 M 无法关联用户的存款地址与一次性公钥地址。并且 M 不知道一次性公钥地址属于哪个商家。需要注意的是, M 可能会进行时间攻击，假如 M 对 User 的盲化支付信息进行签名时用户量非常少, 而 User 很快又将去盲后的支付信息发送给 M，则此时 M 将 User 与一次性公钥地址相关联的可能性就很大。

总之，本文系统能达到这样的匿名性：与直接支付相比，在交易正常进行的情况下，通过代理支付，不会向商家泄露关于用户的账户信息，商家仅能知道用户本次交易的购物信息，而不能窥探用户其他任何购物隐私。此外，代理对用户来说起到了混币中心的作用：通过 M，任何人无法将用户存款时的公钥地址 v_{upk} 与用户希望 M 支付的一次性公钥地址 P 相联系。

6.4 有效性

1) 公平性

本文系统能够实现公平交易。从商家的角度，只有确认收到付款，才会向用户发货，保证了商家的利益；从用户的角度，一旦付款，商家就无法否认。

2) 时效性

初始化阶段：主要时间消耗为一次签名算法的时间、创建交易以及确认交易的时间。然而该步骤只需初始化执行一次，不影响以后用户的支付时间。

交易开始阶段：主要时间消耗为 2 次签名算法的时间以及交易创建的时间。

交易完成阶段：主要时间消耗在生成确认收货的签名。

每次交易过程中，本文系统调用了 3 次签名算法。在实际操作中，运用能够高效实现的短签名算法，与至少需要 60 min 确认时间的原有系统相比，短签名的计算和生成效率更高。

3) 兼容性

本文系统未改变底层协议，因此，与原有的区块链系统兼容。

7 结束语

区块链的去中心化性质带来了支付时间延迟以及潜在的隐私泄露等问题，这使实际中以基于区块链的密码货币为支付方式的应用受到了限制。本文在原有的区块链协议的基础上，引入了代理作为支付中介，解决了支付时间延迟的问题并且更好地保护了用户的隐私。引入代理后，货币的生成依然是去中心化的，仍然具有通货紧缩的特性。在支付阶段引入代理，既能够保证用户匿名性，又减少了交易确认时间，从而提高了支付效率。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2008, 1(2012): 28.

[2] GERVAIS A, CAPKUN S, KARAME G O, et al. On the privacy provisions of Bloom filters in lightweight bitcoin clients[C]//Computer Security Applications Conference. 2014:326-335.

[3] BONNEAU J, MILLER A, CLARK J, et al. SoK: research perspectives and challenges for bitcoin and cryptocurrencies[C]//2015 IEEE Symposiumon Security and Privacy.2015:104-121.

[4] NARAYANAN A, BONNEAU J, FELTEN E, et al. Bitcoin and cryptocurrency technologies[M]. America:Princeton University Press, 2016.

[5] KARAME G O, ANDROULAKI E, CAPKUN S. Double-spending fast payments in bitcoin[C]//ACM Conference on Computer and Communications Security. 2012:906-917.

[6] EYAL I, SIRER E G. Majority is not enough: bitcoin mining is vulnerable[M]//Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2014.

[7] KOSHY P, KOSHY P, MCDANIEL P. An analysis of anonymity in bitcoin using P2P network traffic[C]// Finanical Cryptography and Data Security. 2014: 469-485.

[8] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of bitcoins: charaterizing payments among men with no names[C]// The 2013 Conference on Internet Measurement Conference. 2013: 127-140.

[9] REID F, HARRIGAN M. An analysis of anonymity in the bitcoin system[C]//In Security and Privacy in Social Networks. 2012: 197-223.

[10] 张方国, 王常杰, 王育民. 基于椭圆曲线的数字签名与盲签名[J]. 通信学报, 2001, 22(8): 22-28.
ZHANG F G, WANG C J, WANG Y M. Digital signature and blind signature based on elliptic curve[J]. Journal on Communications, 2001, 22(8): 22-28.

[11] JOHNSON D, MENEZES A, VANSTONE S. The elliptic digital signature algorithm(ECDSA)[J].International Journal of Information Security, 2010, 1(1):36-63.

[12] ANDREAS M A. Mastering bitcoin[M]. O'Reilly Media, 2014.

[13] ABE M, FUJISAKI E. How to date blind signatures[M]. Berlin: Springer, 1996:244-251.

[14] MIERS I, GAMAN C, GREEN M, et al. Zerocoin: anonymous distributed e-cash from bitcoin[C]//2013 IEEE Symposium on Security and Privacy, 2013:97-411.

[15] BENSASSON E, CHIESA A, GAMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy (SP). 2014:459-474.

[16] RUFFING T, MORENO P, KATE A. Coin shuffle: practical decentralized coin mixing for bitcoin[M]//Computer Security-ESORICS: Springer, 2014: 345-364.

[17] BONNEAU J, NARAYANAN, MILLER A, et al. Mixcoin: anonymity for bitcoin with accountable mixes[C]//Financial Cryptography and Data Security. 2014: 486-504.

[18] VLENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for bitcoin[C]//Financial Cryptography and Data Security. 2015:112-126.

[19] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[J].Journal of the Franklin Institute, 2004, 239(2):135-139.

[20] DOUCEUR J R. The sybil attack[C]//First International Workshop on Peer-to-Peer Systems. 2002: 251-260.

作者简介：

傅晓彤（1977-），女，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为公钥密码学及其应用。

陈思（1993-），女，河南商丘人，西安电子科技大学硕士生，主要研究方向为公钥密码学及其在密码货币中的应用。

张宁（1979-），女，陕西宝鸡人，博士，西安电子科技大学副教授，主要研究方向为椭圆曲线公钥密码学、密码货币。