2017-07

交易隐私保护方案

Version 1.0.0

目录

本方案旨在实现 WanChain 上交易的隐私保护，以一次性账户系统和环签名技术为基础，辅以独特设计的邮票系统，最终完成对 WANChain 上原生币以及智能合约代币交易的隐私保护。

1 一次性账户系统

1.1 一次性账户系统构成

一次性账户系统是整个隐私保护的基础，系统中每个用户拥有唯一主账户和多个子账户，子账户也可以看作智能合约中的账户，而子账户通常不是用户自己产生，而是由交易对方为用户生成，如下图所示。

Figure 1-1 用户账户系统

Alice 拥有唯一主账户(A,B)，以及若干子账户(A_1,S_1)，(A_2,S_2)，(A_3,S_3)，…。Bob 为 Alice 转账时，通过主账户(A,B)生成了(A_1,S_1)和(A_2,S_2)，Carol 为 Alice 转账时，生成了(A_3,S_3)。可以看到为 Alice 转账的每一笔交易都会给 Alice 生成一个子账户，即 Onetime-account，而只有 Alice 拥有这些子账户的管理和使用权限。

1.2 账户生成算法

$E(\mathbb{F}_p)[r]$是椭圆曲线$E/\mathbb{F}_p$的r阶子群，G是$E(\mathbb{F}_p)[r]$的生成元。$E/\mathbb{F}_p$选取比特币或以太坊的曲线$y^2 = x^3 + 7$。

1.2.1 主账户生成

Alice 在 WANChain 上原有账户为(A,a)，其中$A = [a]G$，为生成一次性账户系统主账户，则选取随机数$b \in [1, r-1]$，计算$B = [b]G$，以(a,b)作为 Alice 的私钥，以(A,B)作为 Alice 主账户公钥。最终 Alice 拥有主私钥(a,b)和扫描密钥(A,b)，而公开(A,B)作为 Alice 的主账户地址。

1.2.2 子账户生成

当 Bob 要为 Alice 转账时，需要使用 Alice 的主账户(A, B)为 Alice 生成子账号(A_1, S_1)。

Bob 产生随机数$s \in [1, r-1]$，计算

$$S_1 = [s]G$$

$$A_1 = A + [\text{Hash\_p}([s]B)]G$$

这里Hash_p 是将椭圆曲线的点映射到$[1, r-1]$的函数。

则 Alice 生成子账户为

$$(A_1, S_1)$$

(A_1, S_1)是一次性子账户，由于随机数s并没有公开，只是公开了含有s信息的S_1，而S_1并不能计算出s，由椭圆曲线离散对数问题保证。A_1是子账户的公钥分量，S_1是随机因素分量。

Alice 的每一个子账户都是基于主账户(A, B)的随机账户。

1.2.3 子账户的验证和对应私钥

Alice 扫描链中所有一次性账户，取链中的S_1分量和扫描密钥(A, b)参与计算

$$A_1' = A + [\text{Hash}([b]S_1)]G$$

若$A_1' = A_1$，则可以确定(A_1, S_1)是自己的子账户；

若$A_1' \neq A_1$，则可以确定(A_1, S_1)不是自己的子账户。

这是由于$B = [b]G$，于是

$$[s]B = [sb]G = [b][s]G = [b]S_1$$

由于仅有 Alice 知道扫描密钥(A, b)，则只有 Alice 能验证属于自己的子账号(A_1, S_1)。

Alice 需要花子账号(A_1, S_1)的资产，需要计算(A_1, S_1)对应的私钥x，

$$x = a + \text{Hash}([b]S_1)$$

于是有子账户的公钥分量$A_1 = [x]G$。对于每个子账户，Alice 都可以计算其对应的私钥x。

2 环签名方案

2.1 环签名简介

2001 年，Rivest 等人在如何匿名泄露秘密的背景下提出了一种新型签名技术，称为环签名（Ring Signature）。环签名可以被视为一种特殊的群签名（Group Signature），由于群签名需要可信中心和安全的建立过程，往往在匿名保护上存在漏洞（签名者对于可信中心是可追溯的），而环签名在群签名基础上去除了可信中心和安全建立过程，对于验证者来说，签名者是完全匿名的，所以环签名更具实用价值。

自环签名提出后，大量学者发现其重要的价值，基于椭圆曲线、门限等多种环签名被大量设计开发，总体概括可分为四类：

1. 门限环签名
2. 关联环签名
3. 可撤销匿名性环签名
4. 可否认环签名

为实现区块链上智能合约的代币交易隐私性，我们使用一种关联环签名，以实现隐私性的同时防止双花问题。

2.2 环签名方案

环签名可分为四个部分：**GEN**，**SIG**，**VER**，**LNK**。

GEN：采集公共参数，随机选取$n-1$个公钥，合同用户公钥P构成公钥集合$S=\{P_i|i=1,2\ldots,n\}$；对用户公私钥对（P,x），$x\in[1,l-1]$，l为点P的阶，生成公钥镜像I。

SIG：针对所需签名消息m，利用公钥集合$S=\{P_i|i=1,2\ldots,n\}$，其中P_s为用户真实公钥，计算输出签名$ringsig$。

VER：基于消息m，公钥集合S和签名$ringsig$，验证签名合法性，输出“True”或“False”。

LNK：利用集合$\mathcal{I}=\{I_i\}$，判断$ringsig$签名是否已使用。

具体过程介绍如下：

GEN: 签名者使用公私钥对（P,x），有$P=xG$，计算$I=xH_p(P)$，其中H_p为hash 函数，输出椭圆曲线上一个随机的点。随机选取$n-1$个公钥合同P构成公钥地址集$S=\{P_i|i=1,2\ldots,n\}$，其中$P_s=P$。

SIG：签名者选择随机数$\{q_i|i=1,2,\ldots,n\}$和$\{\omega_i|i=1,2,\ldots,n,i\neq s\}$，做如下计算：

$$L_i=\begin{cases}q_iG, & if\ \ i=s\\ q_iG+\omega_iP_i, & if\ \ i\neq s\end{cases}$$
$$R_i=\begin{cases}q_iH_p(P_i), & if\ \ i=s\\ q_iH_p(P_i)+\omega_iI, & if\ \ i\neq s\end{cases}$$

计算：

$$c=H_s(m,L_1,\ldots,L_n,R_1,\ldots,R_n)，\ H_s\text{为 hash 函数}$$

计算：

$$c_i=\begin{cases}\omega_i, & if\ \ i\neq s\\ c-\sum_{i=1,i\neq s}^{n}c_i\ \ mod\ l, & if\ \ i=s\end{cases}$$
$$r_i=\begin{cases}q_i, & if\ \ i\neq s\\ q_s-c_sx\ \ mod\ l, & if\ \ i=s\end{cases}$$

最后生成签名：

$$ringsig=(I,c_1,\ldots,c_n,r_1,\ldots,r_n)$$

VER: 验证者验证签名时，基于消息m、公共参数和$S=\{P_i|i=1,2\ldots,n\}$、$ringsig=(I,c_1,\ldots,c_n,r_1,\ldots,r_n)$，计算：

$$\begin{cases}L_i'=r_iG+c_iP_i,\\ R_i'=r_iH_p(P_i)+c_iI\end{cases}$$

然后验证等式$\sum_{i=1}^{n}c_i=H_s(m,L_1',\ldots,L_n',R_1',\ldots,R_n')\ mod\ l$是否成立，若成立，则签名有效，执行 LNK。

说明：验证过程发现等式成立即需要$L_i'=L_i$，$R_i'=R_i$，以L_i'为例说明如下：

$$L_i=\begin{cases}q_iG, & if\ \ i=s\\ q_iG+\omega_iP_i, & if\ \ i\neq s\end{cases}$$
$$L_i'=r_iG+c_iP_i,$$

$i\neq s$时，有$q_i=r_i$，$\omega_i=c_i$，显然成立，而$i=s$时：$L_s=q_sG=(r_s+c_sx)G=$

$r_s G + c_s P_s = L_s'$，综上有$L_i' = L_i$，同理$R_i' = R_i$成立，则说明 VER 过程是正确的。

LNK：对于区块链上已经出现过的所有I构建集合$\mathcal{J}$，若当前I在集合中出现，则说明该公钥已被使用，认为签名交易不合法；若没有出现过，则认为签名交易合法，并将I加入集合$\mathcal{J}$。

3 基于一次性账户的邮票系统

前文中发现，当使用环签名进行隐私保护时，交易的发起方不可追溯，那么将导致交易费不知从哪个账户收取的问题，为解决这个问题，在 WANChain 上设计并实现邮票系统。邮票系统基于一次性账户体系，在邮票系统中，每张邮票就是一个一次性账户，邮票系统中使用$Onetime-stamp$表示，实际上$Onetime-stamp$与$Onetime-account$相同。用户需要使用代币隐私交易的时候就需要预先购买邮票，将邮票“贴”在交易上才可以完成隐私交易，每张邮票只可使用一次，下面进行详细说明。

邮票系统是一个智能合约，其中设置若干面值，每种面值下存储用户购买的相应面值的邮票信息。合约中提供购买邮票和退还邮票功能：

购买邮票功能：购买邮票功能为用户提供使用万币购买邮票的服务。若用户$Account$需要购买邮票，则发起一笔交易，向邮票系统智能合约转账预购邮票面值$value$的万币并调用合约中购买函数，参数是用户为自己生成的一次性账户，而这一账户将作为邮票$Onetime-stamp$存储在智能合约面值$value$的列表之中，表示用户已经成功购买了这张邮票：

$$Tx = (Account, StampSC, value, payload, sig)$$

$$payload = (\text{"}buy\text{"}, Onetime-stamp)$$

退还邮票功能：退还邮票功能为用户提供将未使用的邮票退款的服务。若用户$Account$已购买邮票$Onetime-stamp$，且邮票未使用，则用户可调用邮票系统智能合约中的邮票退还函数将相应面值万币退还到自己的账户$Account$。退还函数所需参数为邮票$Onetime-stamp$、邮票面值$value$和邮票与自己所做环签名$ringsig$，退还交易确认后合约将在相应面值列表中删除这张邮票，表示邮票已退还：

$$Tx = (Account, StampSC, payload, sig)$$

$$payload = ("refund", Onetime - stamp, value, ringsig)$$

$$ringsig = (I, c_1, c_2, r_1, r_2)$$

在邮票退还功能中之所以使用环签名是为了要求用户提供邮票所对应的I值，以保证邮票并未使用过，不会出现邮票使用后再退还的情况。

实现邮票系统后，若用户需要发起隐私保护的代币交易，则先行在邮票系统中购买邮票，邮票面值基于调用合约消耗和用户意愿而定，然后在代币交易的Tx中不在出现用户的账户信息，而将用户使用的邮票与随机选取同面值的邮票形成集合作为交易发起方，以邮票环签名作为交易合法性的保证：

$$OTA\_Tx = (StampSet, TokenSC, payload, ringsig_{StampSet})$$

代币交易扣除的交易费就是所使用邮票的面值，所以每张邮票只能使用一次，而矿工在挖出新区块后，其挖矿奖励除了$Coinbase$原有部分外，还需扫描区块，将隐私保护的代币交易中使用的邮票价值一并给予，这样一来$Coinbase$比原有情况增加了邮票价值的量。为了保证系统万币总量不变，我们设置邮票智能合约的地址为固定的数值，如$WANChainStampSystem$的 hash 结果，以此保证任何人没有合约的私钥，也就无法将合约收到的万币转出（除用户主动申请退还邮票外），这就意味着邮票系统合约中的钱被锁死，在$Coinbase$增加的情况下保证了万币总量不变。

4 原生币交易隐私保护方案

原生币的交易隐私保护方案类似于邮票系统的实现方式，通过在 WANChain 上部署一个对应于万币智能合约实现。

4.1 万币智能合约

万币智能合约是 WANChain 上部署的一个类似于邮票系统的智能合约，其中设置若干离散面值的代币，代币以 1：1 比例对应于万币，智能合约中提供两个功能：购买代币功能和退还代币功能。购买代币功能允许用户向合约转等值万币，合约中将把用户提供的一次性账户添加到相应面值的存储列表之中；退还代币功能允许用户以一次性账户的环签名为参数进行调用，成功后将相应面值万币退还到用户的账户之中，下面根据交易场景详细说明万币交易的隐私保护过程。

4.2 交易场景

用户 1 主账户私钥为(a,b)，主账户公钥为(A,B)；用户 2 主账户私钥为(c,d)，主账户公钥为(C,D)。用户 1 希望为用户 2 转移$value$的万币。此为交易的场景。

4.3 交易流程

- 交易发起：

用户 1 首先利用用户 2 的主账户公钥(C,D)为其构造一次性账户$Onetime-account2$，然后以一次性账户为参数调用万币只能合约$WANCoinSC$的购买代币函数：

$$Tx=(Account1,WANCoinSC,value,payload,sig)$$

$$payload=("buy",Onetime-account2)$$

- 交易发起确认：

Validator 接收到这笔交易，验证sig与$Account1$对应关系，验签通过后调用万币智能合约，合约把$Onetime-account2$存储在对应于$value$面值下的列表中。

- 交易接收：

用户 2 利用其扫描密钥扫描$WANCoinSC$的存储列表，发现$Onetime-account2$属于自己，然后利用$Onetime-account2$在其对应面值列表中随机选取$n-1$个一次性账户做环签名，并把环签名作为参数调用合约中退还代币函数：

$$Tx=(Account2,WANCoinSC,payload,sig)$$

$$payload=("refund",OTASet,ringsig)$$

- 交易接收确认：

Validator 接收到这笔交易，验证sig与$Account2$对应关系，验签通过后调用万币智能合约，合约验证环签名合法性，并通过$ringsig$中I值未出现过确认该账户没有提过款，确认无误后将向$Account2$账户转入$value$面值的万币。

4.4 隐私效果分析

基于 Onetime-account 和环签名的万币隐私交易方案能够做到以下隐私效果：

1) 利用一次性账户，交易发起过程中，无法得知交易发起者将代币转给哪

个用户。

2) 利用环签名，交易接收过程中，无法得知接收者提出的是哪个一次性账户中的代币，但同时保证每个一次性账户不会重复提款。

在本方案中，交易发起方可以与购买代币的一次性账户建立联系，交易接收方无法与一次性账户建立联系，就保证了发起方与接收方之间不能对应，也就实现了隐私保护，但目前为了便于环签名的使用，万币智能合约中只能设置几个固定离散面值的存储，无法实现任意面值的交易，这也将是后续研究中的一项。

5 代币交易隐私保护方案

5.1 交易场景

用户 1 主账户私钥为(a, b)，主账户公钥为(A, B)；用户 2 主账户私钥为(c, d)，主账户公钥为(C, D)。用户 1 在代币智能合约 SC 中账户为$Onetime - account1$，想要从这个账户中为用户 2 转移$value$的代币。此为交易的场景。

5.2 交易发起

用户 1 要发起这笔交易，需先购买邮票，记为$Onetime - stamp$，然后构造一笔合法的交易，通过 P2P 网络将这笔交易传播出去。一笔交易包含四个字段：TransFrom，TransTo，Data，RingSig。构造过程如下：

1) 在邮票系统中随机选取$n - 1$个与$Onetime - stamp$同面值的邮票，合同$Onetime - stamp$构成一个含有n张邮票的集合$StampSet$，构成整笔交易字段 TransFrom。这是为环签名做准备，隐藏交易发起者身份。
2) 交易字段 TransTo 为调用的代币智能合约的地址$TokenSC$。
3) 交易字段 Data 同样包含四个字段：SC_TransFrom、SC_TransTo、SC_Value、SC_Sig。构造过程为：首先为用户 2 构造$Onetime - account2$；交易输入 SC_TransFrom 为用户 1 控制的$Onetime - account1$，交易目标地址 SC_TransTo 为刚为用户 2 构造的$Onetime - account2$，交易代币值 SC_Value 为$value$，并且用户 1 为这笔交易计算签名sig，它与$Onetime - account1$匹配。

4) 交易字段 RingSig 的构造：使用环签名方案，将 Trans From 作为公钥集合对交易的 Trans From、Trans To、Data 进行环签名，得到签名$ringsig$。

最终代币隐私交易的交易结构为：

$$OTA\_Tx = (StampSet, TokenSC, Data, ringsig)$$

$$Data = (Onetime - account1, Onetime - account2, value, sig)$$

5.3 交易验证

Validator 在拿到一笔交易后，进行如下验证以及计算：

1) 验证交易中 RingSig 是否与 Trans From 的账户集合匹配，如果验证通过，则表明交易合法，否则拒绝。
2) 以 Data 字段作为输入，执行 TransTo 中地址对应的智能合约。智能合约会验证 SC_Sig 是否与 SC_TransFrom 匹配，如果匹配则在 SC_TransFrom 账户中减掉 SC_Value 的代币，同时创建 SC_TransTo 账户，并添加金额 SC_Value。

5.4 交易确认

用户 2 在需要确认用户 1 的代币转移是否成功，过程如下：

1) 利用扫描密钥对智能合约维护的 Onetime-account 进行扫描。
2) 扫描发现$Onetime - account2$属于自己，然后利用主私钥和$Onetime - account2$计算其对应的私钥。

至此，用户 2 已经确认收到一笔代币转账，并获得新的一次性账户$Onetime - account2$的使用权限。

5.5 隐私效果分析

基于 Onetime-account 和环签名的代币隐私交易方案能够做到以下隐私效果：

1) 利用邮票系统和环签名方案保证交易发起者全网匿名。
2) 利用 Onetime-address 保证智能合约代币账户与主账户隔离。

在本方案中，为将交易发起方隐匿，使用邮票系统和环签名，邮票系统中邮票与用户的对应关系是可追溯的，但隐私交易时对邮票进行了环签名，使得每笔

隐私交易所使用的邮票是不可追溯的，也就将交易和真实发起方隔离，任何人无法追溯交易真实发起者，进而实现对发起方的隐私性保护。对于交易接收方，在智能合约中使用一次性账户系统，使得每次转账交易都为接收方创建新的一次性账户，任何人在没有接收方扫描密钥的前提下无法确认一次性账户的归属关系，进而实现了对接收方的隐私性保护。