区块链用户匿名与可追踪技术

李佩丽 徐海霞*

(中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)

(中国科学院数据与通信保护研究教育中心 北京 100093)

(中国科学院大学网络空间安全学院 北京 100049)

摘 要：区块链具有透明性、数据完整性、防篡改等优点，在金融、政府、军事等领域有重要应用价值。目前有越来越多的工作研究区块链的隐私保护问题，典型的包括门罗币、Zerocash, Mixcoin等等。这些隐私保护方法可以用于保护区块链上用户的身份和交易的金额。隐私保护方案是双刃剑，一方面是对合法用户隐私的完善保护，另一方面如果完全脱离监管，则是对洗钱、勒索等违法犯罪行为的姑息和纵容。针对区块链上各种层出不穷的隐私保护方案，监管也要与时俱进。该文研究区块链用户身份的隐私保护和监管方法，提出了用户匿名和可追踪的技术，旨在推动区块链在实际中的应用。

关键词：区块链；匿名；追踪；群签名

中图分类号：TP311 **文献标识码**：A **文章编号**：1009-5896(2020)05-1061-07

DOI: 10.11999/JEIT190813

Blockchain User Anonymity and Traceability Technology

LI Peili XU Haixia

(*Institute of Information Engineering of Chinese Academy of Sciences*, *Beijing* 100093, *China*)

(*Data Assurance and Communication Security Research Center of Chinese Academy of Sciences*, *Beijing* 100093, *China*)

(*School of Cyber Security*, *University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)

Abstract: Blockchain has the advantages of transparency, data integrity, tamper resistance, etc., and has important application value to the fields of finance, government, and military. There are many work to study the privacy protection of the blockchain, typically including Monero, Zerocash, Mixcoin, and more. Their privacy protection methods can be used to protect the identity of the user and the amount of the transaction. The privacy protection scheme is a double-edged sword. On the one hand, it is the perfect protection of the privacy of legitimate users. On the other hand, if it is completely out of supervision, it is the appeasement and connivance of illegal crimes such as money laundering and extortion. In response to the various endangered privacy protection schemes on the blockchain, regulation must also keep pace with the times. In view of this, the privacy protection and supervision methods of blockchain user's identity is studied, and anonymity and traceability technology to promote the application of blockchain to practice is proposed.

Key words: Blockchain; Anonymity; Traceability; Group signature

1 引言

区块链作为比特币系统[1]的核心技术，受到企业、科研机构、政府的广泛关注和研究。2016年国务院印发了《“十三五”国家信息化规划》，首次将区块链技术列入其中并将其定为战略性前沿技术，提出加强区块链等新技术的创新及应用。目前对于区块链没有统一的定义，一般认为区块链是一种分布式的公开数据库，具有防伪、防篡改、交易可追溯、去信任化等特点。区块链的诸多优点吸引了不少企业开发基于区块链的应用。区块链技术目前主要应用在金融领域，另外在保险行业、物流、版权保护等领域已初步有一些应用[2]。

收稿日期：2019-10-22；改回日期：2020-01-20；网络出版：2020-02-25

*通信作者： 徐海霞 xuhaixia@iie.ac.cn

基金项目：国家重点研发计划(2017YFB0802500)，北京市科技计划(Z191100007119007)，山东省重大科技创新工程(2019JZZY020129)

Foundation Items: The National Key R&D Program of China (2017YFB0802500), Beijing Municipal Science and Technology Project (Z191100007119007), The Major Science and Technology Innovation Project of Shandong Province (2019JZZY020129)

到目前为止，比特币仍然是区块链最典型的应用，比特币系统中通过用户大量自由生成交易地址来实现用户真实身份的保密，即实现了匿名性。区块链上的交易内容包括用户的地址、转账金额等都是公开透明的，可以让所有参与节点对交易进行验证和记录。区块链账本公开透明的特点方便了节点对交易的验证，但同时带来了用户的隐私保护问题。近年来的研究发现，由于区块链数据的公开透明性，通过大量分析交易和网络数据，可以设计去匿名方案[3]。在实际应用中，企业或用户可能不希望自己的交易信息被公开地放在链上，包括交易双方的身份、交易金额、交易事由等内容[4]。隐私问题对于个人和企业都至关重要，尤其在很多金融系统、军事领域更是如此。那么该如何保证区块链上用户身份和数据的机密性是区块链走向实际应用面临的一项重要挑战。在此基础上的监管问题也受到大家的关注，因为隐私保护可能会助长恶意用户的行为。本文针对区块链用户身份保护和监管进行研究，提出了区块链用户(包括消息发起者和接收者)匿名与可追踪技术，在保护用户身份的同时，只有监管机构可以追踪用户的身份。

本文的结构如下，第2节介绍相关背景知识，第3节介绍目前主流的区块链隐私保护方法，第4节介绍本文的技术思路和方案构造，第5节给出总结。

2 背景知识

本节对区块链相关概念、群签名、Groth-Sahai证明系统进行介绍。

2.1 区块链

本文引用《区块链技术指南》[5]一书中对区块链的定义。区块链是基于区块链技术形成的分布式公共数据库(或称公开账本)。其中区块链技术是指多个参与方之间基于现代密码学、分布式一致性协议、点对点网络通信技术和智能合约编程语言等形成的数据交换、处理和存储的技术组合。

为了方便地理解区块链技术，本文先从介绍比特币入手。在比特币出现之前，数字货币系统需要可信的第三方机构来保证交易的安全有效，例如Ecash[6]，记账权则交给可信中心。比特币是首个去中心化的数字货币，可以解决双重支付和共识问题。比特币系统不依赖于可信的中心管理员，系统中的用户地位平等。大家共同维护账本、验证交易，并且竞争提出区块(记账)。

比特币系统的分布式记账就是通过区块链技术来实现的。在比特币系统中交易被存储在数据区块中，大约每10 min就会产生1个区块。每个区块包含区块头和区块体两部分。其中交易以Merkle tree的形式存储在区块体部分，区块头包含当前版本号、前一个区块的地址、时间戳、随机数和前一区块的哈希值以及交易Merkle tree的根。区块是通过挖矿产生的。而挖矿的过程是穷举随机数的过程。矿工(比特币用户)将10 min内的交易打包加上前一个区块的哈希值，算出一个随机数，使得这些值的哈希值满足某个条件。如果矿工算出了满足条件的随机数则获得了这个区块的记账权，随后矿工需要将其广播交给其他用户验证。挖矿的矿工竞争获得记账权，矿工需要付出大量的能源和时间，以更大的概率获得一个区块的记账权。通过这样的记账方式，大家共同验证、维护统一的账本，已经记录在区块链中的数据无法篡改。

比特币中区块链的简易结构如图1所示。

区块链上记录的每笔交易形式可抽象为(PK_A, PK_B, m,σ)。其中PK_A为交易发送者A的公钥，PK_B为交易接收者B的公钥，m为消息(在比特币中为金额及前一笔交易的哈希值)，σ为发送者对这笔交易的签名。

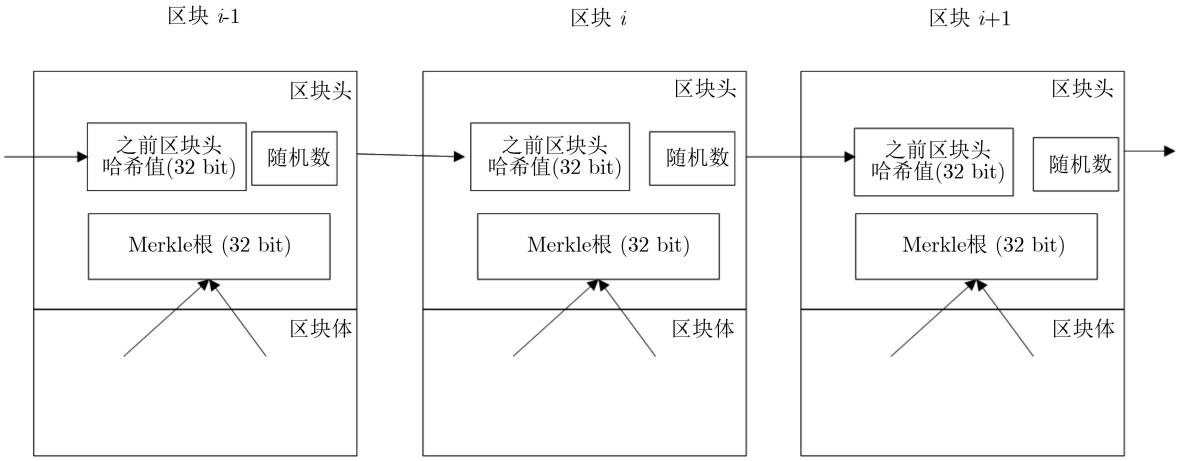

图 1 比特币中区块链的简易结构

2.2 群签名

群签名概念是由Chaum等人[7]在1991年的欧密会上提出的，其具有3个特性：(1)只有群中的成员可以进行签名；(2)接收者可以验证这是一个有效的签名，但是无法知道这个签名属于群中的哪一个成员，实现了匿名性；(3)一旦出现争议或纠纷，群管理员可以打开签名，找到此签名属于群中哪一个成员，实现可追踪性。正是由于结合了匿名性与可追踪两种特性，群签名适合用于区块链用户身份匿名和可追踪。

群签名的定义： 群签名一般包含创建(Setup)、加入(Join)、签名(Sign)、验证(Verify)、打开(Open)、撤销(Revoke) 6个多项式时间算法.

(1) 创建(Setup)：群管理员生成群公钥和群私钥，群公钥用于群签名验证，群私钥用于生成成员证书及打开签名。

(2) 加入(Join)：此时分为两种情况：

(a) 动态群签名中，用户会和群管理员进行交互，完成后群管理员获取可以打开此用户群签名相关的追踪信息，用户获得成员证书以及用于进行群签名的私钥；

(b) 静态群签名中，群管理员和用户之间没有交互，由群管理员直接生成成员的证书并秘密传送给成员。

(3) 签名(Sign)：群成员利用自己的成员证书和私钥来对消息进行签名。

(4) 验证(Verify)：验证者通过群公钥来验证群签名的合法性，但是无法获得签名的实际签名者的信息。

(5) 打开(Open)：对于合法的群签名，群管理员可以打开签名，并找出实际的签名者。

(6) 撤销(Revoke)：群管理员可以撤销某成员的签名权利，此后此用户无法再生成合法的群签名。

2.3 Groth-Sahai证明系统

Groth-Sahai针对双线性群上的一系列等式给出了简单高效的非交互式证据不可区分证明(Non-Interactive Witness Indistinguishable proof, NIWI)和非交互零知识证明(Non-Interactive Zero Knowledge proof, NIZK)的构造方法[8]。他们的证明系统适用于双线性映射上的几个等式，包括线性对乘积等式(pairing product equations), 多标量乘法等式(multi-exponentiation equations)和2次等式(quadratic equations)。他们为这3类等式提供了非交互式证据不可区分的证明。证明满足完美的完备性，完美的合理性和证据不可区分性。证明系统建立在公共参考串模型下。有两类参考串，一类是为了证明完美的合理性，另一类是为了证明证据不可区分性，这两类参考串是计算不可区分的。系统参数产生者拥有陷门，可以从证明中提取用户的证据。

3 已有隐私保护方法介绍

目前区块链隐私保护方法大致可分为3类：基于混合技术、基于环签名和基于零知识证明。下面分别对这3类进行介绍：

(1) 基于混合技术：混合技术目的是为了打乱输入和输出之间的对应关系，使得其他用户不知道一笔钱来自哪个用户，即实现了发送者的匿名性。在这方面有很多相关的工作，其中又分为带中心的混合[9–11]和去中心的混合[12–15]。混合技术适用于多个节点同时有交易任务且交易金额一样的情况下。

(2) 基于环签名：环签名是一种简化的群签名，环签名中只有环成员没有管理者,不需要环成员间的合作。其他用户只知道签名是由环中的用户所签，但不知道是具体是哪个用户[16]。CryptoNote[17]就采用环签名方案实现了发送者身份的隐藏，采用隐身地址的方法实现了接收者的身份隐藏。隐身地址的方法具体来说就是发送方通过接收方的公开信息生成一个随机地址作为接收方的地址，接收方可以通过自己的秘密信息恢复出相应的私钥。因此每次接收者的地址在变化，使得其他节点不能链接哪些交易是发向同一个接收者的，实现了交易的不可关联性。门罗币在CryptoNote基础上实现，后续提出了金额隐藏的方案，且实现了交易可链接的性质，采用了可链接的环签名技术[18]。环签名和隐身地址方法相结合能够保证发送者和接收者的匿名性，发送交易的用户只需要知道环中其他成员的公钥，不像混合技术需要其他用户同时参与交易。

(3) 基于零知识证明：为了提供更好的匿名性，Miers等人[19]基于零知识证明设计了一种扩展的比特币系统Zerocoin，使得输入的比特币地址与输出的比特币地址之间没有直接关系。Zerocoin中币值金额是固定的，无法实现金额的拆分。文献[20]在2014年提出了一种新的匿名数字货币：Zerocash。Zerocash建立在Zerocoin的基础上并对其进行了改进。它采用简洁的非交互零知识证明(zk-SNARKs)和同态承诺等密码工具[21,22]，被称为是一种完全匿名的货币。这种方法提供了很好的隐私保护，不过目前来看证明的实现比较复杂，产生证明效率较低，离实际应用还有一段距离。

上述3类技术关注隐私保护问题的研究，都没有考虑用户身份的监管问题。在实际应用中，监管是至关重要的环节。通过前面的分析，环签名技术较适用于实现用户的匿名性，在此基础的监管可以

考虑用可链接、可追踪的环签名实现特定条件下的用户身份追踪[18,23]。可链接、可追踪的环签名只有在同一个用户对相同的消息用相同的私钥做了两次签名的情况下，其身份才会被追踪到，这个技术适用场景较窄。鉴于此，本文提出了一种基于群签名的区块链用户匿名可追踪方案。本方案不仅考虑消息发起者的匿名可追踪，还涉及到接收者的匿名可追踪。

4 区块链用户匿名与可追踪方案

4.1 设计思路

在第3节已经提到，环签名的方法是目前比较实用的用户匿名技术。不过为了实现可监管特性，本文采用了群签名技术。群签名有一个群管理者，签名者公钥对其他用户保密，群管理者能够获得签名者的公钥(这里即用户身份)。群签名实现交易发送方的匿名性和可追踪。发送方对交易做了群签名后，其公钥是隐藏的，保证了匿名性；监管者通过陷门可以从群签名中获得用户的公钥，实现了追踪。

本文采用Groth[24]在2007年提出的群签名方案。其方案对Zhou等人[25]的签名方案做了一点改动用于产生群成员证书，结合Boneh等人[26]的签名方案和Groth-Sahai证明系统[8]设计了不需要随机预言机的群签名方案。因为Groth的群签名方案采用的是Groth-Sahai证明系统，群管理员拥有陷门可以从证明中提取出用户的公钥。这里本文不对群签名方案整体细节做太多介绍，只重点介绍一下群签名的创建(Group.Setup)和加入(Group.Join) 算法。因为这是产生用户公私钥和证书的过程，便于后续介绍接收者匿名可追踪。

Group.Setup(1^k):

群管理员产生双线性群$\mathrm{gk} := (p, G, G_{\mathrm{T}}, e, g) \leftarrow G\left(1^k\right)$;

随机选择$f, h, z \leftarrow G$，计算$T := e(f, z)$，返回$(\mathrm{gpk}, \mathrm{gsk}) := ((\mathrm{gk}, f, h, T), z)$；

Group.Join{$\mathrm{User}_i(\mathrm{gpk})$, $\mathrm{Issuer}(\mathrm{gpk}, \mathrm{gsk})$}:

$$
\begin{aligned}
&(\mathrm{sk}_i, \mathrm{pk}_i) \leftarrow \mathrm{User}_i(\mathrm{gk}), \mathrm{Issuer}(\mathrm{gk})\\
&r \leftarrow Z_p\\
&a := f^{-r}\\
&b := (\mathrm{pk}_i \cdot h)^r z\\
&\mathrm{cert} := (a, b)
\end{aligned}
$$

用户i的公私钥为$(\mathrm{sk}_i, \mathrm{pk}_i)$，用户$i$证书记为$(\mathrm{pk}_i, \mathrm{cert} = (a, b))$。

在Group.Join算法结束后，用户拿到了自己的公私钥对和相应的证书。证书的验证算法记为Cert.Verify：若$e(a, \mathrm{pk}_i \cdot h)e(f, b) = T$，返回1，否则返回 0。需要说明这个证书并不是不可伪造的，不过即便用户伪造新的公钥pk'的证书，其无法完成后续的群签名操作。因此整体的群签名方案是防伪造的。

群签名可以直接实现发送者的匿名可追踪。如何做到交易接收方的匿名和监管呢？这方面目前还没有相关工作。接收方的匿名性如果采用隐身地址的方法，监管较为困难。我们采用群签名的证书产生机制结合Groth- Sahai证明系统设计了可验证的匿名证书。群管理员为用户颁发证书，这个证书可以被用户随机化产生匿名证书。发送方将接收方的匿名证书而不是接收方公钥放到了交易里，从而隐藏了接收方的公钥。监管者拥有陷门可以从匿名证书提取出接收方的公钥。

证书的匿名化算法记为Cert.Anym，包括下面两步：

(1) 对Group.Join算法产生的证书$(\mathrm{pk}_i, \mathrm{cert} = (a, b))$进行随机化：随机选择$\rho \leftarrow Z_p$，计算$a' = af^{-\rho}$，$b' = b(h \cdot \mathrm{pk}_i)^{\rho}$；(注：随机化后的证书仍然满足等式$e(a', \mathrm{pk}_i \cdot h)e(f, b') = T$)；

(2) 实现可验证的匿名证书：产生非交互的证据不可区分的证明$\pi : \mathrm{NIWI}\{(b', \mathrm{pk}_i) : e(a', \mathrm{pk}_i \cdot h)$ $e(f, b') = T\}$，其中(b', pk_i)是证据，a', h, f, T均公开。这个证明可以直接采用Groth-Sahai证明系统来实现。用户匿名化之后的证书为$\mathrm{cert}' = (a', \pi)$。拥有陷门的群管理员可以从证明$\pi$中提取出用户的公钥$\mathrm{pk}_i$。

这与群签名不同的地方在于，这里只证明证书的有效性。适用于接收者的匿名和追踪，因为接收者不需要做签名操作。前面本文提到这种证书产生方式并不满足防伪造的性质，恶意的交易接收者有可能伪造新的公钥pk_i'发送给交易发送者，虽然他不知道pk_i'的私钥(这个结论基于离散对数困难问题)。为了杜绝这一行为，接收者在公布自己的公钥和证书的时候需要附上监管者的签名。另外发送者可以根据接收者的公钥和证书伪造新的公钥pk_i'的证书，使得证书验证通过。不过这会带来一个后果，那就是谁都不能再花这笔钱，因为用户无法知道新的公钥pk_i'所对应的私钥。因此通过上述证书产生方式及监管者的签名就能够保证接收者公钥的保密，而且可以被监管者追踪。

4.2 方案构造

在基于区块链的系统中，用户之间存在消息传输，这个过程本文将其称之为交易。为了方便描述和理解，本文设定的交易场景为：用户A给用户B做了一个承诺，记录在区块链上。用户A为发起者，用户B为接收者，承诺记为m(m不包括两方身份的

信息)。区块链系统用户匿名可追踪技术分为了5个阶段：(1)初始阶段；(2)用户注册；(3)发送消息；(4)消息验证；(5)用户追踪。 方案具体设计如下：

(1) 初始阶段：监管机构运行群签名的Group.Setup算法，产生群公钥gpk和群私钥gsk，监管者执行一般的签名算法产生一对公私钥对(vk, sk)；

(2) 用户注册：用户和监管机构之间执行群签名的加入(Group.Join)算法，用户获得相应的公私钥对$(\mathrm{pk}_i, \mathrm{sk}_i)$和证书$\mathrm{cert}_i$. 监管者在发送证书$\mathrm{cert}_i = (a, b)$的同时，用sk对$(\mathrm{pk}_i, \mathrm{cert}_i)$做签名$\mathrm{sig}_{\mathrm{sk}}(\mathrm{pk}_i, \mathrm{cert}_i)$，将签名也发给用户。监管者保存用户的注册列表(如图2)；

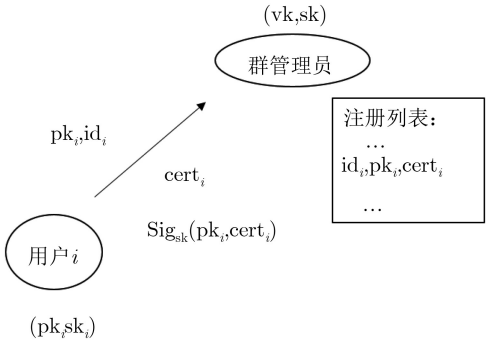

图 2 用户注册

(3) 发送消息：(a) 用户A计划给用户B发送消息m，用户A随机产生标签，记为tag，将发送请求和标签tag及A的签名发给B；

(b) 用户B将公钥$\mathrm{pk_B}$和证书$\mathrm{cert_B}$和监管者的签名$\mathrm{sig_{sk}}(\mathrm{pk_B}, \mathrm{cert_B})$发送给用户A；

(c) 用户A验证收到的证书和签名，若都验证通过，执行Cert.Anym算法对用户B的证书做匿名化：随机选择$\rho \leftarrow Z_p$，计算$a' = af^{-\rho}$, $b' = b(h \cdot \mathrm{pk}_i)^{\rho}$。产生非交互的证据不可区分的证明$\pi : \mathrm{NIWI}\{(b', \mathrm{pk_B}) : e(a', \mathrm{pk_B} \cdot h)\, e(f, b') = T$。用户B的匿名证书记为$\mathrm{cert_B}' = (a', \pi)$。

用户A用B的公钥$\mathrm{pk_B}$加密b':$\mathrm{Enc}_{\mathrm{pk_B}}(b')$。

用户A用私钥$\mathrm{sk_A}$对$(\mathrm{tag}, \mathrm{m}, \mathrm{Enc}_{\mathrm{pk_B}}(\rho), \mathrm{cert_B}')$做群签名，得到的群签名记为$\sigma$；

(d) 用户A将信息$(\mathrm{tag}, \mathrm{m}, \mathrm{Enc}_{\mathrm{pk_B}}(b'), \mathrm{cert_B}', \sigma)$公布到区块链上。(说明：通过引入随机标签tag，接收方容易查找哪条消息是发给自己的。将$\mathrm{Enc}_{\mathrm{pk_B}}(b')$发给用户B是为了后续让用户B可以后续向他人证明其有m，因为有了$(a', b', \mathrm{cert_B}')$，用户B拥有$\mathrm{pk_B}$对应的私钥$\mathrm{sk_B}$，采用关于知识的零知识证明，用户B就可以向外界证明承诺m的确是给我的。)

(4)消息验证：(a) 区块链上任意用户都可以执行群签名验证算法Group.Verify$((\mathrm{tag}, \mathrm{m}, \mathrm{cert_B}'), \sigma)$，若通过，说明发送方是群成员，即被管理员认证过的。进行下一步；

(b) 验证接收者证书：执行证书验证算法Cert.Ver$(\mathrm{gpk}, \mathrm{cert_B}')$判断$\mathrm{cert_B}'$是否是一个有效的证书，若是，则验证算法输出1。

(5) 身份追踪：监管者执行群签名的Open算法可以获得发送者的公钥。接收者匿名证书中证明π可以采用Groth-Sahai证明系统，监管者通过陷门从匿名证书中抽取出接收者的公钥。

接收者B收到用户A给他的承诺m后，当他要使用m时，他可以向外界证明其有证书相应的私钥，这就和群签名方案是一致的。

需要说明的是当应用场景为数字货币，消息m为数字货币中的交易金额时，需要考虑交易的双花问题。即用户A对同一笔钱花两次。因为群签名方案隐藏了发送者的公钥，恶意的发送者可以对同样的消息m再做一次群签名，实现双花。本文考虑可以通过增加一个标签S来防止这个问题。发送者的公私钥对为$(\mathrm{pk_A}{=}g^{\mathrm{sk_A}}, \mathrm{sk_A})$，令$S = h^{\mathrm{sk_A}}$，公开$h$和$S$，除了群签名本身，还需要证明群签名的用的私钥$\mathrm{sk_A}$与$S$以$h$为底的指数是相等的。这样当用户A再一次用$(\mathrm{pk_A}, \mathrm{sk_A})$做签名时，其标签$S$是一样的，就会被发现。

4.3 安全性说明

匿名性：发送者的匿名性直接基于群签名方案的匿名性。接收者的匿名性基于所设计的证书的匿名性。接收者的证书每次被随机化为a', b'，且采用非交互证据不可区分的证明$\pi : \mathrm{NIWI}\{(b', \mathrm{pk_B}) : e(a', \mathrm{pk_B} \cdot h)\, e(f, b') = T\}$隐藏了$b'$, $\mathrm{PK_B}$。因此接收者的匿名性基于证明的证据不可区分性。

可追踪性：发送方的可追踪特性是通过群签名可追踪性实现的。接收者可追踪性是由Groth-Sahai NIWI证明的可靠性及可抽取特性保证的。

5 结论

本文研究区块链用户隐私保护和可追踪技术，旨在解决区块链在实际应用存在的隐私保护和监管难题。本文首先介绍了目前主流的区块链隐私保护方法，并分析了这些方法存在的局限。为了达到隐私保护和监管的平衡，本文基于群签名、Groth-Sahai证明系统提出可同时保证发送方、接收方匿名可追踪的方案。

参 考 文 献

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash

system[EB/OL]. https://bitcoin.org/bitcoin.pdf, 2008.

[2] 曹素珍, 王斐, 郎晓丽, 等. 基于无证书的多方合同签署协议[J]. 电子与信息学报, 2019, 41(11): 2691–2698. doi: 10.11999/JEIT190166.
CAO Suzhen, WANG Fei, LANG Xiaoli, *et al*. Multi-party contract signing protocol based on certificateless[J]. *Journal of Electronics & Information Technology*, 2019, 41(11): 2691–2698. doi: 10.11999/JEIT190166.

[3] NARAYANAN A, BONNEAU J, FELTEN E, *et al*. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction[M]. Princeton University Press, 2016.

[4] 牛淑芬, 王金凤, 王伯彬, 等. 区块链上基于B+树索引结构的密文排序搜索方案[J]. 电子与信息学报, 2019, 41(10): 2409–2415. doi: 10.11999/JEIT190038.
NIU Shufen, WANG Jinfeng, WANG Bobin, *et al*. Ciphertext sorting search scheme based on b+ tree index structure on blockchain[J]. *Journal of Electronics & Information Technology*, 2019, 41(10): 2409–2415. doi: 10.11999/JEIT190038.

[5] 邹均, 张海宁, 唐屹, 等. 区块链技术指南[M]. 北京: 机械工业出版社, 2016: 97–99.
ZOU Jun, ZHANG Haining, TANG Yi, *et al*. Guidelines for Blockchain Technology[M]. Beijing: China Machine Press, 2016: 97–99.

[6] CHAUM D, FIAT A, and NAOR M. Untraceable Electronic Cash[M]. GOLDWASSER S. Advances in Cryptology — CRYPTO' 88. New York: Springer, 1990: 319–327. doi: 10.1007/0-387-34799-2_25.

[7] CHAUM D and VAN HEYST E. Group Signatures[M]. DAVIES D W. Advances in Cryptology — EUROCRYPT ' 91. Berlin: Springer, 1991: 257–265. doi: 10.1007/3-540-46416-6_22.

[8] GROTH J and SAHAI A. Efficient non-interactive proof systems for bilinear groups[C]. The 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, 2008: 415–432. doi: 10.1007/978-3-540-78967-3_24.

[9] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. *Communications of the ACM*, 1981, 24(2): 84–90. doi: 10.1145/358549.358563.

[10] BONNEAU J, NARAYANAN A, MILLER A, *et al*. Mixcoin: Anonymity for Bitcoin with Accountable Mixes[M]. CHRISTIN N and SAFAVI-NAINI R. Financial Cryptography and Data Security. Berlin: Springer, 2014: 486–504. doi: 10.1007/978-3-662-45472-5_31.

[11] VALENTA L and ROWAN B. BLIndcoin: Blinded, accountable mixes for bitcoin[C]. 2015 International Conference on Financial Cryptography and Data Security, San Juan, USA, 2015: 112–126. doi: 10.1007/978-3-662-48051-9_9.

[12] MAXWELL G. Coinjoin: Bitcoin privacy for the real world[EB/OL]. Post on Bitcoin Forum. https://bitcointalk.org/index.php?topic=279249.0, 2013.

[13] RUFFING T, MORENO-SANCHEZ P, and KATE A. CoinShuffle: Practical decentralized coin mixing for bitcoin[C]. The 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 2014: 345–364. doi: 10.1007/978-3-319-11212-1_20.

[14] RUFFING T, MORENO-SANCHEZ P, and KATE A. P2P mixing and unlinkable bitcoin transactions[C]. The 24th Annual Network and Distributed System Security Symposium, San Diego, USA, 2017: 824.

[15] RUFFING T and MORENO-SANCHEZ P. Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin[C]. 2017 International Conference on Financial Cryptography and Data Security, Sliema, Malta, 2017: 133–154.

[16] CHANDRAN N, GROTH J, and SAHAI A. Ring signatures of sub-linear size without random oracles[C]. The 34th International Colloquium on Automata, Languages, and Programming, Wrocław, Poland, 2007: 423–434.

[17] BERGAN T, ANDERSON O, DEVIETTI J, *et al*. CryptoNote v 2.0[J]. https://cryptonote.org/whitepaper.pdf, 2013.

[18] LIU J K, WEI V K, and WONG D S. Linkable spontaneous anonymous group signature for ad hoc groups[C]. The 9th Australasian Conference on Information Security and Privacy, Sydney, Australia, 2004: 325–335. doi: 10.1007/978-3-540-27800-9_28.

[19] MIERS I, GARMAN C, GREEN M, *et al*. Zerocoin: Anonymous distributed e-cash from bitcoin[C]. 2013 IEEE Symposium on Security and Privacy, Berkeley, USA, 2013: 397–411.

[20] BEN SASSON E, CHIESA A, GARMAN C, *et al*. Zerocash: Decentralized anonymous payments from bitcoin[C]. 2014 IEEE Symposium on Security and Privacy, San Jose, USA, 2014: 459–474.

[21] BEN-SASSON E, CHIESA A, TROMER E, *et al*. Succinct non-interactive zero knowledge for a von Neumann architecture[C]. The 23rd USENIX Conference on Security Symposium, Berkeley, USA, 2014: 781–796.

[22] PEDERSEN T P. Non-interactive and information-theoretic Secure Verifiable Secret Sharing[M]. FEIGENBAUM J. Annual International Cryptology— CRYPTO '91. Berlin: Springer, 1991: 129–140. doi: 10.1007/3-540-46766-1_9.

[23] FUJISAKI E and SUZUKI K. Traceable ring signature[C]. The 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, 2007: 181–200.

doi: 10.1007/978-3-540-71677-8_13.

[24] GROTH J. Fully anonymous group signatures without random oracles[C]. The 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2007: 164–180. doi: 10.1007/978-3-540-76900-2_10.

[25] ZHOU Sujing and LIN Dongdai. Shorter Verifier-local Revocation Group Signatures from Bilinear Maps[M]. POINTCHEVAL D, MU Yi, and CHEN Kefei. Cryptology and Network Security. Berlin: Springer, 2006: 126–143. doi: 10.1007/11935070_8.

[26] BONEH D and BOYEN X. Short Signatures without Random Oracles[M]. CACHIN C and CAMENISCH J L. Advances in Cryptology - EUROCRYPT 2004. Berlin: Springer, 2004: 56–73. doi: 10.1007/978-3-540-24676-3_4.

李佩丽：女，1988年生，助理研究员，研究方向为密码学、区块链隐私保护与监管.

徐海霞：女，1973年生，副研究员，研究方向为安全多方计算、区块链隐私保护与监管、共识机制.