基于区块链的多方隐私保护公平合同签署协议*

吴进喜[1], 高 莹[2], 张宗洋[2], 殷大鹏[1]

[1] 北京航空航天大学 数学与系统科学学院, 北京 中国 100191

[2] 北京航空航天大学 网络空间安全学院, 北京 中国 100191

摘要 传统的公平合同签署协议通过引入中心化的可信第三方来保证协议的公平性。当第三方不诚实且和签署一方进行合谋, 就会对另一方产生不公平。同时, 第三方可能会泄露参与方的敏感信息, 这将极大地威胁参与方的隐私。故合同签署的公平性和隐私性均依赖于第三方的可靠性。基于区块链的公平合同签署协议可去中心化从而避免依赖第三方来解决公平性, 但区块链可被公开访问和验证, 这为参与方的隐私问题又带来新的挑战。已有的基于公开区块链的隐私保护公平合同签署协议利用参与方共享的秘密因子对合同信息及公钥进行加密从而隐藏了参与方数字证书中的真实身份信息; 但在协议的承诺阶段, 由于区块链的假名性, 执行两笔保证金交易时可能会泄露正在签署合同的参与方信息。为最大限度保护参与方的身份隐私, 本文基于混币技术, 通过引入半诚实可信第三方来提供参与者身份的混淆服务, 并结合盲的可验证加密签名方案, 设计出新的隐私保护公平合同签署协议。该协议可支持多个合同签署人通过区块链完成公平的合同签署, 不仅可以保护与合同相关的隐私内容, 还可以保护参与方的身份隐私。

关键词 区块链; 假名性; 公平合同签署协议; 隐私保护; 混淆服务

中图法分类号 TP309 **DOI 号** 10.19363/j.cnki.cn10-1380/tn.2018.05.02

A Multi-Party Privacy Preserving Fair Contract Signing Protocol based on Blockchains

WU Jinxi[1], GAO Ying[2], ZHANG Zongyang[2], YIN Dapeng[1]

[1] School of Mathematics and Systems Sciences, Beihang University, Beijing 100191, China

[2] School of Cyber Science and Technology, Beihang University, Beijing 100191, China

Abstract Traditional fair contract signing protocols need a centralized trusted third party (TTP) to ensure the fairness of the protocols. When the third party becomes dishonest and colludes with one participant, it is unfair for the other participant. Meanwhile, the third party may reveal sensitive information from the participants, which is a great threat to the privacy of the participants. Therefore, the fairness and privacy are dependent on the reliability of the third party. Using blockchain technology, fair contract signing protocols can be decentralized to achieve fairness. It poses new challenges to the privacy issues since anyone can access and verify a public blockchain. In the existing privacy preserving fair contract signing protocol based on public blockchain, the secret information shared by the participants is used to encrypt the contract information and the public keys so as to conceal the true identity information in the participants' digital certificates. However, in the commit phase of the protocol, two deposits would probably reveal the identity information of the participants because of the pseudonymity in the blockchain. For maximum protection of participants' privacy, this paper uses the coin mixing technique, which introduces a semi-honest third party to provide the mixing service, and designs a new fair contract signing protocol based on blind verifiably encryption signature scheme. The new protocol allows multi-party contract signers to fulfill the task of fair contract signing on blockchain, and protects not only the privacy contents related to the contract but also the privacy of identities of contract signers.

Key words blockchain; pseudonymity; fair contract signing protocol; privacy preserving; mixing service

1 引言

随着电子商务的发展, 互联网上的公平合同签署日益普遍。公平合同签署协议本质上是参与方公平地交换对合同的数字签名, 这是基于公平交换协议的实际应用。按照是否有第三方参与, 公平交换协议可分为两类: 一类是不需要第三方参与的。比如基于逐步交换协议的思想[1], 参与双方一步一步地释

通讯作者: 高莹, 博士, 副教授, Email: gaoying@buaa.edu.cn。

本课题得到国家重点研发计划“现代服务业共性关键技术研发及应用示范”重点专项（NO. 2017YFB1400700）资助; 北京市自然科学基金（NO.4182033）资助; 信息安全国家重点实验室开放课题（NO.2017-MS-02）; 北航金华北斗应用研究院开放基金项目（NO.BARI1702）资助。

收稿日期: 2018-01-30; 修改日期: 2018-04-28; 定稿日期: 2018-05-02

放所交换的信息。由于网络的异步性, 该类协议总是存在“一比特的不公平性”, 从而不能满足真正的公平性。另外一类依赖于可信第三方, 比如半可信第三方的公平交换协议[2]。大部分(半)可信第三方是高度中心化的, 掌握着一些敏感信息, 例如合同信息、签署合同方的身份信息以及合同签名信息等。如果第三方不诚实, 将敏感信息泄露给他人, 那么这显然对参与方是不利的, 并且对参与方的隐私造成极大的威胁。因此, 在设计公平合同签署协议时, 不仅需要考虑第三方的中心化问题, 还要考虑用户的隐私保护需求。

近年来, 由于区块链具有无中心化、公开透明等特点, 受到人们的广泛关注[3,4]。直观来看, 它是一个无中心化的可信第三方, 可以消除中心化可信第三方的不可靠性。不仅如此, 比特币采用一次性公钥作为用户的假名身份, 在一定程度上保护了用户的身份隐私。因此, 在公平合同签署协议中引入区块链技术是一个值得尝试的方法[5-8]。

但是因为区块链的无中心化特点, 当争端发生时, 又产生了新的隐私泄露问题[6]。普通的公平合同签署协议, 可信第三方可以提取合同的数字签名, 然后转交给签署方。基于区块链的公平合同签署协议, 区块链上的每个节点上都可以提取合同的数字签名。这违背了用户隐私保护的原则。文献[5]基于时间戳服务器, 提出了一个无可信第三方的公平合同签署协议, 该协议可以通过区块链技术实现。文献[9-12]主要研究的是基于区块链的公平交换协议, 可用于公平合同签署协议的技术实现。但这些公平合同签署协议都没有考虑用户的隐私保护需求。因此, 文献[6]提出了盲的可验证加密签名(Blind verifiably encrypted signature, BVES), 并将它应用于公平合同签署协议的设计当中。该协议保护了所签署的合同信息、数字签名以及身份信息, 同时基于保证金来达到协议的公平性。

而区块链是公开透明的, 每个节点都可以查看区块上的交易信息。文献[13,14]中说明了在区块链上可以通过追溯比特币的资金流动分析出资金的拥有者, 即用户身份。例如, 买家去商店利用比特币购买商品时, 商家可以同时记录买家所使用的比特币公钥信息和真实身份, 并且可以持续追踪买家的比特币零钱去向, 所以买家的身份信息已经泄露[14]。因此, 区块链并非真正地具有匿名性, 而是假名性。文献[6]设计了基于区块链技术的满足隐私保护的公平合同签署协议。但由于区块链自身存在的假名性问题, 当合同签署双方达成一个 Commit 交易时, 指定的两笔保证金交易会泄露出他们的身份信息。因此, 设计出既满足公平性又达到隐私保护需求的合同签署协议仍然是一个难点。

1.1 本文工作

本文基于混币思想[15], 改进基于公开区块链的隐私保护公平合同签署协议[6], 并提出一个新的基于区块链的公平合同签署协议, 满足以下性质:

(1) 公平性：利用区块链技术实现公平性。签署方在交换签名前需要交纳保证金, 诚实方可以通过释放签名来赎回保证金, 而不诚实方将会受到惩罚, 失去交纳的保证金。

(2) 隐私保护：结合 BVES 方案和混币思想实现隐私保护需求。BVES 方案盲化合同消息和身份信息, 并且只有签署方才能提取出普通签名; 引入半诚实可信第三方来提供混淆服务, 切断签署方之间的直接联系。让签署方与第三方公平地签署合同, 最后签署方能够在区块链上得到 BVES 签名, 并计算出其他签署方的普通签名。

(3) 多方合同签署：不同于只满足两方的合同签署协议, 本协议可以满足多方合同签署。只要签署方通过第三方进行合同签署, 其他签署方就可以提取该方的普通签名, 直到所有签署方诚实地释放 BVES 签名, 该协议完成, 否则终止。

1.2 相关工作

已有大量工作致力于解决合同签署的公平交换问题。首先是无可信第三方的逐步交换协议[16], 虽然无可信第三方, 但是仍存在不公平性, 且通信代价高。随后, 部分工作引入可信第三方, 可分为在线可信第三方[17]和离线可信第三方[18]。在线可信第三方协议需要第三方可信且在线工作, 在多用户的系统中, 这会成为一个瓶颈。相比之下, 离线可信第三方协议更具实用性, 只需要在签署方有争端时才参与进来。但协议的公平性和隐私性均依赖于可信第三方。近期有一些工作基于区块链技术来设计公平合同签署协议。针对于隐私保护需求, 文献[6]构造一种盲的可验证加密签名算法, 并提出基于区块链的隐私保护公平合同签署协议。签署方首先在链下进行协商秘密因子, 用来盲化合同信息和身份信息来实现隐私保护; 在链上实现公平交换 BVES 签名, 从而实现双方公平合同签署。随后, 文献[8]基于实用性考虑, 提出一种专门签署合同的数字货币 Contract Coin。文献[7]提出一种基于区块链的三方公平合同签署协议。该协议在链下验证签名; 在链上只公平交换秘密因子, 从而保障签署方隐私。

但是由于比特币交易的可追踪性、可链接性以及交易金额公开, 导致其存在隐私泄露问题[13,14]。因此, 研究人员相继提出各种隐私保护方案。Maxwell

提出 Coinjoin[19]混币技术, 把不同用户的多个交易合并成一个交易, 从而隐藏交易输入方和输出方的对应关系。Mixcoin[20]利用可信的第三方来混淆比特币地址, 但这个第三方可能侵犯用户的隐私并窃取用户的比特币。门罗币[21]利用环签名和隐蔽地址技术来达到隐私保护需求。为了提供更高的匿名性, Ben-Sasson 等在 Zerocoin[22]方案上进一步提出了 Zerocash[23]方案, 利用非交互式零知识证明协议实现匿名性更强的电子现金系统, 保护用户信息和交易额的隐私。

现有公开工作没有考虑区块链系统自身存在的隐私泄露问题, 所以本文基于混币思想, 引入半诚实可信第三方提供混淆服务, 避免让区块链上的公开节点直接判断出签署方正在签署合同, 从而保护签署方隐私。

1.3 本文框架

本文的框架如下: 第 2 节介绍比特币脚本和 BVES 方案; 第 3 节分析文献[6]中公平合同签署协议的不足之处, 并给出改进协议的目标; 第 4 节中给出改进的公平合同签署协议; 最后第 5 节给出了协议的安全性分析并讨论其不足之处。

2 预备知识

本节介绍预备知识。在 2.1 节介绍比特币脚本知识, 在 2.2 节介绍 BVES 方案。

2.1 比特币脚本

比特币在交易中使用脚本系统, 其交易的灵活性依赖于输入和输出脚本, 可以通过设置合理的输出脚本来限定比特币花费的条件。在比特币交易中, 最普遍的交易方式是标准交易(standard transactions)。该交易的输入脚本表示若用户提供的公钥和数字签名能通过上一笔交易的输出脚本的验证, 那么该用户是该比特币的拥有者, 可以花费该比特币。输出脚本则是限定了下一个比特币拥有者若要花费比特币就必须提供一个公钥以及一个数字签名。

例如, 图 1 中 T_A 表示交易, 资金来源于交易 T_1; $in\text{-}script:\mathrm{Sig}_A([T_A])$ 表示输入脚本的参数信息为 A 对交易 T_A 的签名, 若通过 T_1 的输出脚本验证, 则能花费该比特币; $out\text{-}script(body,\sigma_M):ver(body,\sigma_M)$ 表示输出脚本验证函数的参数信息, 若签名 σ_M 验证通过, 则交易 T_A 是将比特币支付给 M; val: d B: 表示该交易的金额为 d B。因此, 该图表示 A 支付给 M 价值为 d B 的比特币, 然后 M 支付给 C 价值为 d B 的比特币。

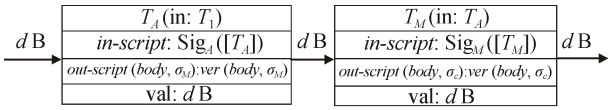

图 1 标准交易

Figure 1 Standard transactions

为了设计合适的公平合同签署协议, 可以合理地设置输入脚本和输出脚本的参数并且加入交易时间锁。例如, 图 2 中交易 *Fuse* 的 tclock: t 表示该交易在时间 t 内被锁定。该图表示 A 将 T_A 交易作为输入生成 *Put* 交易, 支付给 M 价值为 d B 的比特币, 并且生成一个 *Fuse* 交易。限定条件为: 若时间 t 后, M 还没有接收该比特币, 则 A 可以对 *Fuse* 交易签名, 拿回比特币。

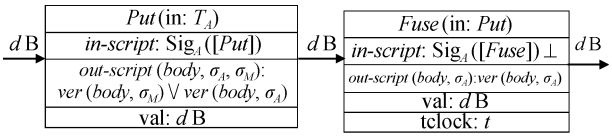

图 2 特殊交易

Figure 2 Special transactions

因此, 在设计公平合同签署协议时, 可以利用脚本系统选取合适参数来强迫参与方诚实地执行协议。

2.2 BVES 方案

这部分简要介绍文献[6]中的 BVES 方案, 该方案里有三个参与者, 即签名者 Alice, 签名提取者 Bob 以及验证者 Minter。假设 Alice 和 Bob 都知道所签署的合同消息为 m, 其索引消息为 m_{index}。Alice 有一个有效证书, 而 Bob 只需要一个临时的密钥对。Minter 帮助 Bob 验证 Alice 的签名。该方案由以下八个算法组成:

Setup: 设 G_1 是一个循环加法群, P 为生成元。G_2 是一个循环乘法群且 $|G_1|=|G_2|=q$, 其中 q 为素数。定义 $e:G_1\times G_1\to G_2$ 为一个双线性对, 并定义两个密码哈希函数 $H:\{0,1\}^*\to Z_q^*$ 以及 $H_1:G_2\to Z_q^*$。

KeyGen: 随机选择 $x\in_R Z_q^*$, 并计算 $y=xP$。将 y 作为公钥, x 则作为私钥。此时 Alice 的密钥对为 (x_A,y_A), Bob 的密钥对为 (x_B,y_B)。

Sign: 对于一个消息 m, Alice 计算生成一个普通签名:

$$\delta_{\text{Alice}}=\frac{1}{H(m)+x_A}P. \tag{1}$$

Verify: 对于一个消息签名对 $(m,\delta_{\text{Alice}})$, 验证签

名的方程如下:

$$e\left(H\left(m\right)P+y_A,\delta_{\text{Alice}}\right)=e\left(P,P\right). \tag{2}$$

PreSignAgree: Alice签署消息 m，并发给Bob。

1. Alice随机选取 $\alpha\in_R Z_q^*$，然后计算 αP 以及 $s=H_1\left(e\left(y_A,y_B\right)^{\alpha}\right)$，最后计算 sy_A 和 $sH\left(m\right)$。随后Alice把以下四元组发给Bob:

$$\left(\alpha P,sy_A,m_{index},sH\left(m\right)\right). \tag{3}$$

2. Bob计算 $s'=H_1\left(e\left(y_A,\alpha P\right)^{x_B}\right)$。然后验证 $s'y_A$=sy_A 和 $s'H\left(m\right)$=$sH\left(m\right)$。若所有的验证都能通过, Bob返回true, 否则返回false。

BVESSign: Alice生成一个BVES签名:

$$\delta_{\text{BVES}}=\frac{1}{\left(H\left(m\right)+x_A\right)s}y_B. \tag{4}$$

BVESVer: 利用以下四元组作为输入:

$$\left(\delta_{\text{BVES}},sH\left(m\right),sy_A,y_B\right). \tag{5}$$

Minter验证下面的等式:

$$e\left(sH\left(m\right)P+sy_A,\delta_{\text{BVES}}\right)=e\left(P,y_B\right). \tag{6}$$

BVESExt: Bob计算 $\frac{s'}{x_B}\delta_{\text{BVES}}$，提取普通签名。

3 对公平合同签署协议的分析

文献[6]构造出 BVES 方案, 并设计了基于公开区块链的隐私保护公平合同签署协议。该协议在链下验证对方的数字证书的长期 BVES 公钥, 并交换临时 BVES 密钥和比特币公钥。然后利用参与方共享的秘密因子 s 对合同信息 m 以及长期密钥对应的公钥进行加密, 隐藏了参与方的数字证书中的真实身份信息和合同信息。由于 BVES 方案是可验证加密签名方案, 所以区块链上的每个节点都能验证BVES签名, 但只有参与方才能计算出普通的数字签名, 从而也保护了参与方的真实数字签名。

但是, 由于区块链本身的假名性, 在协议承诺部分, T_A 和 T_B 两笔保证金交易可能分别泄露出 Alice 和 Bob 的身份信息。这显然侵犯了参与方的隐私。为最大限度保护参与方隐私, 可以对该协议进行改进。

首先, 引入一个半诚实可信第三方 Minter 作为中间服务方, 提供混淆服务, 让参与方分别跟 Minter 签署合同。这样, 区块链上的节点无法直接看出 Alice 和 Bob 要签署合同。为了隐藏参与方的身份信息和合同信息, 需要利用秘密因子对相关信息进行加密, 而且只有参与方知道秘密因子。由于参与方要分别与 Minter 签署合同, 所以参与方需要共享两个秘密因子, 并各自选取一个秘密因子进行加密处理。

其次, 若直接应用文献[6]的公平合同签署协议, 只有 Minter 能够计算得出参与方的普通签名, 并且知道合同信息。此时 Minter 成为高度中心化的可信第三方, 变成系统的瓶颈。注意到, 公平合同签署协议本质上是交换参与方的数字签名, 所以只需要交换参与方的 BVES 签名, 并不需要 Minter 的 BVES 签名。但是计算普通签名时, 参与方不仅需要知道秘密因子, 还需要知道 Minter 的临时私钥。由于参与方的秘密因子是共享的, 所以只需要知道 Minter 的临时私钥即可。因此, 设计协议时, 要限定 Miner 公布其临时私钥。

再次, 为了抵御 DoS 等攻击, 参照文献[24]的做法, 在接收服务之前, 参与方需要支付少量的服务费 w B 给第三方 Minter。另外, 针对每笔成功的合同, Minter 需要收取额外的服务费 f B。此处要求 w 远小于 f。这样一定程度上可以避免 Minter 偷盗服务费 w B。

最后, 在文献[6]的基础上, 对于我们的协议增加以下假设:

1) 假定每一份合同的保证金都相同, 均为 d B (为了防止攻击者通过比较保证金等额与否, 判断参与方签署同一份合同);

2) 第三方 Minter 不能拒绝提供服务 (防止第三方拒绝服务而导致合同签署失败);

3) 合同具有时效性, 由参与方协定 (参与方在协定的任意时间内与第三方签署合同即可)。

综合以上分析, 协议目标如下:

1) 如果 Alice 和 Bob 成功地签署合同, 双方都只需要支付给 Minter 服务费 $f+w$ B。

2) 如果 Alice 和 Bob 都拒绝签署合同, 双方都失去保证金 $d+f$ B, 均需支付给 Minter 服务费 $w+d+f$ B。

3) 如果仅仅是一方成功签署合同, 该方需支付给 Minter 服务费 $f+w$ B。另一方需支付给 Minter 服务费 $w+d+f$ B。

4) 协议满足隐私保护需求。

4 改进的公平合同签署协议

本节基于第 3 节的分析给出改进的公平合同签署协议。在 4.1 节中简要介绍记号, 在 4.2 节中介绍协议的具体步骤。

4.1 记号介绍

假设参与方 A 和 M, 其中 A 的密钥对为(x_A, y_A), M 的密钥对为(x_M, y_M)。为了便于理解协议的具体流程图, 在介绍协议之前先在表 1 解释相关记号。

表 1 记号

Table 1 Notations

记号	意义
$Commit(in: T_A, T_M)$	A 和 M 分别将 T_A 和 T_M 交易作为输入构成 Commit 交易
$[T_A]$	交易 T_A 中除输入脚本以外的全部内容
$\mathrm{Sig}_A([T_A])$	A 利用私钥 x_A 对 $[T_A]$ 的签名
$in\text{-}script: \perp, \mathrm{Sig}_A([T_A])$	输入脚本的参数信息. 其第一个参数省略, 用 $\perp$ 表示; 第二个参数是 A 对 $[T_A]$ 的签名
$ver_A(body, \sigma_A)$	利用 A 的公钥 y_A 来验证数字签名 σ_A 是否正确
$out\text{-}script(body, \sigma_A)$	输出脚本的参数信息
δ^M_{BVES}	针对消息 M 的 BEVS 签名
$BV(\delta^A_{\mathrm{BVES}}, s_1H(m), s_1y_A, y'_M)$	按照公式(6)验证 A 的 BVES 签名是否正确
val: d B	交易的金额为 *d* B
Tclock: t	交易在时间 *t* 内被锁定, 时间 *t* 后才能解锁

4.2 协议

该协议的签署方可以是多方, 并且每个签署方选择的第三方也可以不同。协议成功当且仅当所有签署方成功与各自选定的第三方进行合同签署。为了方便介绍, 本节采用同一个第三方 Minter, 签署方只有两方 Alice 和 Bob。因此, 该协议包括 Alice 以及 Bob 和 Minter 两个签署合同过程。因为两个过程类似, 所以只着重介绍 Alice 和 Minter 的签署合同过程, 并在图 3 中展示签署合同的主要步骤。

Pre-condition: 签署方和第三方生成协议所需的公私钥对; 签署方共享两个秘密因子, 并将盲化的合同信息和身份信息发给第三方, 第三方返回其临时公钥。

1. Alice、Bob以及第三方Minter分别有三组密钥对: 一对是比特币密钥, 一对是通过KeyGen算法产生的临时BVES密钥, 最后一对是包含在公钥证书中的长期BVES密钥。Alice的长期密钥对是(x_A, y_A), 临时密钥对是(x'_A, y'_A); Bob的长期密钥对是(x_B, y_B), 临时密钥对是(x'_B, y'_B); Minter的长期密钥对是(x_M, y_M), 临时密钥对是(x'_M, y'_M)、(x''_M, y''_M)等。

2. Alice和Bob对合同 *m* 达成一致, 并产生了一个合同索引 m_{index}。他们交换各自的长期以及临时两组密钥对。若公钥证书无效, 协议终止。否则, Alice和Bob分别运行PreSignAgree算法, 共享两个秘密因子 s_1 和 s_2。然后分别计算 $s_iH(m)$, s_iy_A 以及 s_iy_B, 其中 $i \in \{1,2\}$。

3. Alice将包含合同信息的 $s_1H(m)$ 和包含身份信息的 s_1y_A 都发送给第三方Minter, 并预交给他价值为 *w* B的服务费。然后Minter生成BVES临时公钥 y'_M, 最后返回给Alice。同样, Bob将包含合同信息的 $s_2H(m)$ 和包含身份信息的 s_2y_B 都发送给第三方Minter, 并预交给他价值为 *w* B的服务费。然后Minter生成BVES临时公钥 y''_M, 最后返回给Bob。

4. Alice和Bob分别指定交易 T_A 和 T_B, 价值均为 $d+f$ B。Minter指定两个交易 T_{M1} 和 T_{M2}, 价值均为 *d* B。

Commit: 签署方和第三方交纳保证金, 生成对应的Commit交易。此过程分为两个阶段, 第一阶段是Commit_1, 实现Alice和Minter交纳保证金; 第二阶段是Commit_2, 实现Bob和Minter交纳保证金。

Commit_1:

1. Alice和Minter将 T_A 和 T_{M1} 交易作为输入, 构成Commit_1 交易。

2. Alice对Commit_1 交易签名, 并发送给Minter。

3. Minter利用Alice的比特币公钥来验证这个签名, 并且核对Commit_1 交易中脚本的参数信息。若正确, Minter对这个Commit_1 交易签名, 然后广播出去。否则, 协议终止。

4. 双方等待这个交易被记录在区块链上。

Commit_2:

1. Bob和Minter将 T_B 和 T_{M2} 交易作为输入, 构成Commit_2 交易。

2. Bob对交易Commit_2 签名, 并发送给Minter。

3. Minter利用Bob的比特币公钥来验证这个签名, 并且核对Commit_2 交易中脚本的参数信息。若正确, Minter对这个Commit_2 交易签名, 然后广播出去。否则, 协议终止。

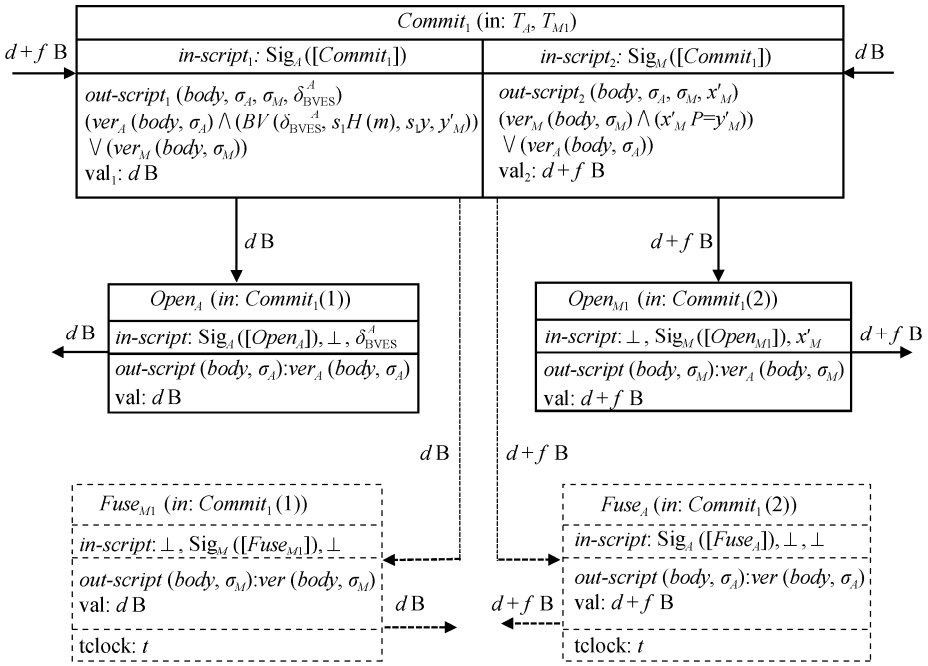

图 3　公平合同签署协议

Figure 3　A fair contract signing protocol

4. 双方等待这个交易被记录在区块链上。

Open: 签署方诚实地公布其BVES签名生成 $Open_A$ 交易，赎回保证金;同样第三方诚实地公布其临时私钥生成 $Open_{M1}$ 交易，赎回保证金。此过程分为两个阶段，第一阶段是Open$_1$，实现Alice和Minter签署合同并赎回保证金；第二阶段是Open$_2$，实现Bob和Minter签署合同并赎回保证金。

Open$_1$：若Commit$_1$ 出现在区块链上，则Alice生成一个BVES签名

$$\delta_{BVES}^{A}=\frac{1}{\left(H\left(m\right)+x_{A}\right)s_{1}}y'_{M}\,, \tag{7}$$

然后生成 $Open_A$ 交易，最后广播出去；Minter则是公布他BVES的临时私钥 x'_M，然后生成 $Open_{M1}$ 交易，最后广播出去。否则，协议终止。

Open$_2$：若Commit$_2$ 出现在区块链上，则Bob生成一个BVES签名

$$\delta_{BVES}^{B}=\frac{1}{\left(H\left(m\right)+x_{B}\right)s_{2}}y''_{M}\,, \tag{8}$$

然后生成 $Open_B$ 交易，最后广播出去；Minter则是公布他BVES的临时私钥 x''_M，然后生成 $Open_{M2}$ 交易，最后广播出去。否则，协议终止。

Fuse: 协议的任一方不诚实，另一方都可以在时间 t 后生成 *Fuse* 交易，得到对方的保证金作为奖励。此过程分为两个阶段，第一阶段是Fuse$_1$，实现若Alice或Minter不诚实，则将其保证金奖励给对方；第二阶段是Fuse$_2$，实现若Bob或Minter不诚实，则将其交纳保证金奖励给对方。

Fuse$_1$：若在约定的时间 t 后，$Open_A$ 交易没有出现在区块链上，此时Minter广播 $Fuse_{M1}$ 交易，拿回保证金 d B；同样，如果在约定的时间 t 后，$Open_{M1}$ 交易没有出现在区块链上，此时Alice广播 $Fuse_A$ 交易，拿回保证金 $d+f$ B。

Fuse$_2$：若在约定的时间 t 后，$Open_B$ 交易没有出现在区块链上，此时Minter广播 $Fuse_{M2}$ 交易，拿回保证金 d B；同样，如果在约定的时间 t 后，$Open_{M2}$ 交易没有出现在区块链上，此时Bob广播 $Fuse_A$ 交易，拿回保证金 $d+f$ B。

Recover: 签署方在区块链上得到对方的BVES签名以及第三方的临时私钥，结合共享的秘密因子计算出对方的普通签名。

若在时间 t 内，$Open_A$ 交易出现在区块链上，此时Bob计算出Alice的普通签名:

$$\frac{s_1}{x'_M}\delta_{\mathrm{BVES}}^{A}\,; \tag{9}$$

同样，若在时间 t 内，$Open_B$ 出现在区块链上，此时Alice计算Bob的普通签名:

$$\frac{s_2}{x''_M}\delta^{B}_{\mathrm{BVES}}。 \tag{10}$$

Reward: 第三方提供混淆服务所获得的奖励。

Alice和Bob均交纳保证金 $d+f$ B, 但是只能拿回Minter交纳的保证金 d B。剩余的 f B当作第三方Minter的服务费。因此, Minter提供一次服务能够获得总服务费 $f+w$ B。

5 协议安全性分析

本节对协议的安全性进行分析。在 5.1 节证明了协议满足公平性和安全性, 在 5.2 节说明了协议还存在的不足之处。

5.1 安全性分析

定理 1 协议满足公平性。

证明. 由于 Minter 不能拒绝服务, 执行协议时需要交纳保证金 d B。假设 Minter 不诚实, 此时他既拿不到服务费, 还损失保证金。所以有理由认为他是半诚实可信的, 即 Minter 会诚实地执行协议。因此, 证明只需要考虑参与方的情况, 分为以下三种:

(1) 有一方诚实。

假设 Alice 诚实而 Bob 不诚实。这种情况意味着 Alice 跟 Minter 成功地签署合同, 只需要支付给 Minter 服务费 $f+w$ B。而 Bob 因为没有公布自己的 BVES 签名, 既无法拿到 Minter 交纳的保证金 d B, 也失去了自己交纳的保证金 $d+f$ B。Bob 因为不诚实而受到了惩罚, 总共损失 $d+f+w$ B。

(2) 双方都诚实。

这种情况意味着 Alice 和 Bob 跟 Minter 都成功地签署合同, 他们分别可以在区块链上得到对方的 BVES 数字签名以及 Minter 的 BVES 临时私钥, 最后可以通过计算得到对方对合同的普通数字签名。

(3) 双方都不诚实。

这种情况意味着 Alice 和 Bob 都没有跟 Minter 成功地签署合同, 都损失了 $d+f+w$ B。这个惩罚机制也符合实际意义, 因为双方是在谈好合同的前提下毁约, 理应受到惩罚。不仅如此, 正因为存在着双方会毁约的概率, 促使第三方不想拒绝提供服务, 并且诚实地执行协议。

根据上面的讨论得知, 双方要么都能获得对方的签名, 要么需要付出代价获得对方的签名, 要么什么都得不到, 所以该协议满足公平性。

定理 2 协议满足安全性。

证明. 从以下三个方面来证:

(1) 该协议同样基于 BVES 方案。而田海博[6]等证明了该方案在基于可验证加密签名[25,26]安全模型下具有不可提取性且是不可伪造的。并且只有参与方知道秘密因子, 所以只有参与方才能得到合同的数字签名。

(2) 在同一时期里, 假设 Minter 分别与 N 个人成功地进行签署合同。因为攻击者不知道谁跟谁在签署合同, 所以他最好的策略就是瞎猜。若 Alice 和 Bob 都在这个集合中, 那么他成功的概率为 $1/(N-1)$。若有一方不在这个集合中, 也就是说 Alice 跟 Minter 签署了合同, 但是 Bob 没有签署合同。此时, 这个隐私保护程度就相当强了, 攻击者成功的概率为 0。因此, 此时攻击者成功的最大概率为 $1/(N-1)$。当互联网中的 N 很大时, 这个概率是很小的。

(3) 更为一般的情况, Alice 和 Bob 可能跟不同的第三方在不同时期执行公平合同签署协议。但只要他们以及各自的第三方能诚实地执行协议, Alice 和 Bob 就能计算得到对方对合同的数字签名。此时, 攻击者成功的概率几乎为 0。

根据上面的分析可知, 只有参与方能够得到对方对合同的数字签名, 且不会泄露出敏感信息。因此, 协议满足安全性。

5.2 不足

本文引入第三方来提供混淆服务, 增强协议的隐私性。由于存在签署合同异步的情况, 即当 Alice 先和 Minter 签署合同, 此时 Bob 免费拿到 Alice 的普通签名, 损失一定的公平性。但是考虑在实际应用场景中, 存在签署一方为了表示签署的强烈意愿, 可能先将普通签名发给对方。因此, 在执行协议之前, 签署方可以随机协定签署的顺序, 并且规定合同签署的时效性, 若在规定时间内签署方没有签署成功就当做签署失败。

6 结论

本文利用盲的可验证加密签名方案以及区块链技术, 并且引入半诚实可信第三方来提供混淆服务, 设计出新的公平合同签署协议。该协议满足公平性和安全性, 不仅能支持多方合同签署, 还能克服区块链的假名性问题, 从而达到真正的隐私保护需求。

参考文献

[1] Blum M, “How to exchange (secret) keys,” Acm Transactions on Computer Systems, vol. 1, no. 2, pp. 175-193, 1983.

[2] Franklin M K and Reiter M K, “Fair Exchange with a Semi-Trusted Third Party,” in Acm Conference on Computer & Communications Security(CCS’99), pp. 1-5, 1999.

[3] Nakamoto, S, “Bitcoin: A Peer-to-Peer Electronic Cash System,” http://bitcoin.org/bitcoin.pdf, 2008.

[4] Wallace B, “The Rise and Fall of Bitcoin,” http://www.wired.com/agazine/2011/11/mf bitcoin/all/, 2011.

[5] Wan Z, Deng R H and Lee D, “Electronic Contract Signing Without Using Trusted Third Party,” in International Conference on Network and System Security(NSS’15), pp. 386-394, 2015.

[6] TIAN H B, HE J J and FU L Q, “A privacy preserving fair contract signing protocol based on public block chains,” Journal of Cryptologic Research, vol. 4, no. 2, pp. 187-198, 2017.
(田海博, 何杰杰, 付利青, “基于公开区块链的隐私保护公平合同签署协议”, *密码学报*, 2017, 4(2): 187–198。)

[7] Huang H, Li K C and Chen X, “A Fair Three-Party Contract Singing Protocol Based on Blockchain,” in International Symposium on Cyberspace Safety and Security(CSS’17), pp. 72-85, 2017.

[8] Tian H, He J and Fu L, “Contract Coin: Toward Practical Contract Signing on Blockchain,” in International Conference on Information Security Practice and Experience(ISPEC’17), pp. 43-61, 2017.

[9] Andrychowicz M, Dziembowski S, Malinowski D and Mazurek Łukasz, “Fair Two-Party Computations via Bitcoin Deposits,” in Financial Cryptography and Data Security(FC’14), pp. 105-121, 2014.

[10] Kumaresan R and Bentov I, “How to Use Bitcoin to Incentivize Correct Computations,” in ACM Sigsac Conference on Computer and Communications Security(CCS’14), pp. 30-41,2014.

[11] Bentov I and Kumaresan R, “How to Use Bitcoin to Design Fair Protocols,” in International Cryptology Conference(Crypto’14), pp. 421-439,2014.

[12] Liu J, Li W, Karame G O, and Asokan N, “Towards Fairness of Cryptocurrency Payments,” https://arxiv.org/pdf/1609.07256.pdf, 2016.

[13] Pomarole M, Pomarole M, Jordan G, et al, “A fistful of Bitcoins: characterizing payments among men with no names,” Communications of the Acm, vol. 59, no. 4, pp. 86-93, 2016.

[14] Ron D and Shamir A, “Quantitative Analysis of the Full Bitcoin Transaction Graph,” in Financial Cryptography and Data Security(FC’13), pp. 6-24, 2013.

[15] Chaum D L, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Communications of the Acm, vol. 24, no. 2, 1981.

[16] Goldreich O, “A Simple Protocol for Signing Contracts,” in Advances in Cryptology(Crypto’83), pp. 133-136, 1983.

[17] Benor M, Goldreich O, Micali S and R L, “A fair protocol for signing contracts,” in IEEE Transactions on Information Theory, vol. 36, no. 1, pp. 40-46, 1990.

[18] Asokan N, Schunter M and Waidner M, “Optimistic protocols for fair exchange,” in ACM Conference on Computer and Communications Security(CCS’97), pp. 7-17, 1997.

[19] G. Maxwell, “CoinJoin: Bitcoin privacy for the real world,” https://bitcointalk.org/index. php?topic=279249.0, 2013.

[20] Bonneau J, Narayanan A, Miller A, et al, “Mixcoin: Anonymity for Bitcoin with Accountable Mixes,” in International Conference on Financial Cryptography and Data Security(FC’14), pp. 486-504, 2014.

[21] Bergan T, Anderson O, Devietti J, et al, “CryptoNote v 2.0,” https://cryptonote. org/whitepaper. pdf, 2013.

[22] Miers I, Garman C, Green M, et al, “Zerocoin: Anonymous Distributed E-Cash from Bitcoin,” in Security and Privacy(S&P’13), pp. 397-411, 2013.

[23] Sasson E B, Chiesa A, Garman C, et al, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” in Security and Privacy(S&P’14), pp. 459-474, 2014.

[24] Heilman E, Baldimtsi F and Goldberg S, “Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions,” in International Conference on Financial Cryptography and Data Security(FC’16), pp. 43-60, 2016.

[25] Zhang F, Safavi-Naini R and Susilo W, “Efficient verifiably encrypted signature and partially blind signature from bilinear pairings,” in International Conference on Cryptology in India(Indocrypt’03), pp. 191-204, 2003.

[26] Zhang F, Safavi-Naini R and Susilo W, “An efficient signature scheme from bilinear pairings and its applications,” in International Workshop on Theory and Practice in Public Key Cryptography(PKC’04), pp. 277-290, 2004.

吴进喜 于 2016 年在中国矿业大学(北京)数学与应用数学专业获得学士学位。现在北京航空航天大学数学专业攻读硕士。研究领域为区块链技术及其应用。研究兴趣包括: 密码学, 区块链等。Email: mathwjx@163.com

高莹 于 2003 年在武汉大学基础数学专业获得博士学位。现任北京航空航天大学网络空间安全学院副教授。研究领域为密码学及其应用。研究兴趣包括: 公钥密码学, 区块链等。Email: gaoying@buaa.edu.cn

张宗洋 于 2012 年在上海交通大学计算机软件与理论专业获得博士学位。现任北京航空航天大学网络空间安全学院讲师。研究领域为密码学及密码货币。研究兴趣包括: 公钥密码学、区块链。Email: zongyangzhang@buaa.edu.cn

殷大鹏 于 2009 年在北京大学信息与计算科学专业获得学士学位。现在北京航空航天大学数学专业攻读硕士。研究领域为分组密码算法设计分析。研究兴趣包括: 布尔函数, 线性层等。Email: jimkate1@163.com