密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2018, 5(5): 546–555

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

区块链技术专刊

基于区块链的公平多方不可否认协议

苑博奥[1], 刘 军[2], 李 戈[1]

1. 陆军工程大学 指挥信息系统学院, 南京 210007
2. 南京审计大学金审学院, 南京 210046
通信作者: 苑博奥, E-mail: yuanboao1201@sina.com

摘 要: 多方不可否认协议有着广泛的应用场景, 诸如多方电子支付和视频会议等. 在这些应用场景中, 各参与方互不信任, 有着事后否认曾参与协议的可能, 多方不可否认协议便是为解决这一问题而产生的一类密码协议. 为实现协议的公平性, 现有的多方不可否认协议都依赖于可信第三方 TTP 的参与, 中心化的 TTP 成为了协议的性能瓶颈, 同时, 在现实中很难保证 TTP 的完全可信, 给协议带来了潜在的安全威胁. 在区块链中, 所有的节点通过共识算法共同维护一个公开链结构, 提供了类似去中心化 TTP 的功能, 有助于解决由中心化 TTP 带来的性能和安全问题. 本文基于公开链结构, 提出一个完全无 TTP 参与的多方不可否认协议, 并用形式化分析方法证明了协议满足不可否认性、公平性和时限性. 与经典协议进行对比, 所提协议在各项指标中均显示了良好的性能.

关键词: 多方不可否认协议; 区块链; 无 TTP; 不可否认性; 公平性; 时限性
中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000264

中文引用格式: 苑博奥, 刘军, 李戈. 基于区块链的公平多方不可否认协议[J]. 密码学报, 2018, 5(5): 546–555.
英文引用格式: YUAN B A, LIU J, LI G. Fair multi-party non-repudiation protocol based on block chain[J]. Journal of Cryptologic Research, 2018, 5(5): 546–555.

Fair Multi-party Non-repudiation Protocol Based on Block Chain

YUAN Bo-Ao[1], Liu Jun[2], Li Ge[1]

1. College of Command Information Systems, The Army Engineering University of PLA, Nanjing 210007, China
2. Nanjing Audit University Jinshen College, Nanjing 210046, China
Corresponding author: YUAN Bo-Ao, E-mail: yuanboao1201@sina.com

Abstract: Multi-party non-repudiation protocol has a wide range of applications, such as multi-party electronic payment and video conferencing. In these applications, the parties involved in the protocol may not trust each other and may even deny the fact of participation, thus multi-party non-repudiation protocol is one of the cryptographic protocols aiming at the problem. To achieve fairness, current multi-party non-repudiation protocols rely on a trusted third party (TTP), and the centralized TTP becomes a bottleneck in protocols' performance. In practice, it is hard to guarantee that the TTP is completely trustworthy, this brings potential security threats to the protocol. In the block chain, all nodes maintain a public chain of block by consensus algorithm, providing the function of decentralized

收稿日期: 2017-08-01 定稿日期: 2017-11-30

TTP, which helps to solve the performance and security problems caused by a centralized TTP. Based on the public chain of block, this study proposes a multi-party non-repudiation protocol without TTP's participation, and proves by formal analysis that the protocol meets the properties of non-repudiation, fairness, and timeliness. Compared with the classical protocols, the proposed protocol shows a good performance in each aspect.

Key words: multi-party non-repudiation protocol; block chain; no TTP; non-repudiation; fairness; timeliness

1 引言

计算机网络技术的发展, 提供了便捷的通信和资源共享服务, 在享受其发展带来成果的同时, 网络中传输的信息的安全问题愈加突显出来. 密码协议 (又称安全协议) 便是为解决这样的问题, 保证信息交互的安全, 综合运用密码算法和协议设计技术产生的网络交互协议. 冯登国 [1] 依据密码协议的设计目标将密码协议分为 4 类: 密钥交换协议、认证协议、认证密钥交换协议和电子商务协议. 不可否认协议是电子商务协议中的一种, 主要用于防止协议的参与方在协议执行后否认自己参与协议的事实, 损害其他参与方的利益, 多方不可否认协议是指参与方数目多于两个的不可否认协议, 协议参与方数目的增多使得协议拓扑结构更加复杂, 交互过程更富于动态性, 使得协议的设计与安全性分析更加困难.

不可否认协议的设计依据有无可信第三方 TTP (trusted third party) 可分为两种, 一种是无 TTP 的协议, 此类协议通过将不可否认证据分成若干份, 逐份相互交换的方式进行, 只能保证在一定概率下的公平性, 另一种是含有 TTP 参与的协议, 协议公平性的实现依赖于 TTP 的公平与公正, 但是中心化的 TTP 具有较低的可靠性和较高的安全风险 [2]. 对多方不可否认协议的研究大致有两条主线, 一条主线是降低可信第三方 TTP 的参与所造成的性能瓶颈和安全隐患. 2000 年, Kremer 和 Markowitch 扩展一个两方不可否认协议提出了第一个多方不可否认协议 [3], 同年, 在协议参与方大多诚实的假设下给出了协议的优化版本 [4], 相比原协议, 此协议在正常运行时不需要 TTP 的参与, 当争议发生时, 才需要 TTP 参与解决争端, 减少了 TTP 的参与. 2002 年, 邓所云等提出采用可公开验证的门限秘密共享方案 (p, n) 来把对单一 TTP 的依赖分散开来, 将单一 TTP 的功能交由 p 个 TTP 协调完成, 从而降低由于 TTP 的诚实性假设带来的安全风险 [5]. 文献 [6] 和文献 [7] 针对协议中存在的排斥性问题进行改进, 即消息的发送方在协议执行中存在优势, 可以将合法的接收者排除在外, 分别提出了一个多方不可否认协议, 将确定接收者集合的控制权交给了 TTP, 但这种设计方式显然加重了 TTP 的负担. 文献 [8] 则针对 TTP 在实际运营中存在的问题, 提出期望强公平的概念, 即从协议的执行结果无法判断 TTP 是否介入了协议的运行, 以此保护 TTP 的信誉, 这种方式无疑增加了 TTP 的优势, 协议参与方需要给予 TTP 更多的信任. 此外, Feng 等将多方不可否认协议用于解决云存储中存在的安全问题 [9]. 至此, 仍然不存在一种可以完全脱离对 TTP 依赖的多方不可否认协议.

另一条主线是对协议分析方法的研究, 验证协议是否满足所需的安全目标. 协议的形式化分析是验证协议是否满足其安全目标的重要方法. 现有的对多方不可否认协议的形式化分析方法大多是对两方协议分析方法向多方的扩展, 这种扩展涉及到密码协议的三大类形式化分析方法: 逻辑方法、模型检测方法和定理证明方法, 但是至今仍没有针对多方不可否认协议的完善的形式化分析技术. 在对逻辑方法的扩展中 [10,11], 已有的研究工作将时间因素引入 SVO 逻辑, 分析了多方不可否认协议的公平性和时限性, 成功发现了协议中存在的时限性缺陷. 在对模型检测方法的扩展中 [12], 用交替转换系统建模协议, 用交替时序逻辑刻画协议的安全属性, 分析了协议的公平性, 其局限性表现在分析过程中限定了协议实例的数量和接收者的数量, 存在着状态空间爆炸问题, 该方法可以发现协议中存在的安全问题, 却不能说明协议一定正确. 在对定理证明方法的扩展中, 文献 [13] 将签名操作引入串空间模型, 并对应修改模型中的定义, 将公平性表达为若发起者串中包含接收不可否认证据项, 则必定有接收者串中包含发送不可否认证据项, 反之亦然, 该方法可以证明协议的正确性, 但是对不能完成证明的协议不能说明其存在的安全缺陷, 协议的证明过程较为复杂.

本文延续多方不可否认协议第一条主线的研究, 尝试利用区块链中去中心化的网络结构设计多方不可

否认协议, 缓解由于 TTP 的参与而造成的协议性能瓶颈, 降低协议参与方对 TTP 诚实性的依赖, 提升协议的安全性.

本文的章节安排如下: 第 2 节介绍区块链的相关内容; 第 3 节基于区块链技术设计一个不依赖于 TTP 的高效的多方不可否认协议; 第 4 节对设计的多方不可否认协议进行安全性分析和性能对比; 第 5 节总结全文.

2 区块链

区块链 (block chain) 本意是由区块这一数据结构组成的长链, 后演变为代指使用链式区块结构作为核心技术的全新的去中心化基础架构与分布式计算范式 [14], 由 Satoshi Nakamoto 在 2008 年提出 [15], 比特币是迄今为止最为成功的区块链应用场景. 区块链由众多的网络节点组成, 节点之间是对等的关系, 以扁平式拓扑结构相互连通和交互, 不存在中心节点, 不需要相互信任, 在激励机制的作用下, 节点共同维护一个由区块这一数据结构组成的链结构. 本文以 BlockChain 代指这一由区块组成的长链, 如图1所示, 每一个区块包含了在时间戳所示范围内发生的所有货币交易, 并加入了之前区块结构的 Hash 值. 新区块由分布式节点间通过共识算法竞争获得, 首先获得新区块的节点向全网广播该区块, 每个节点在验证区块的合法性后将其加入长链 BlockChain 中, 并开始下一区块的竞争. 这一链结构保存了从区块链诞生开始全网的所有交易信息, 由各节点自行选择存储完整的或部分的链结构.

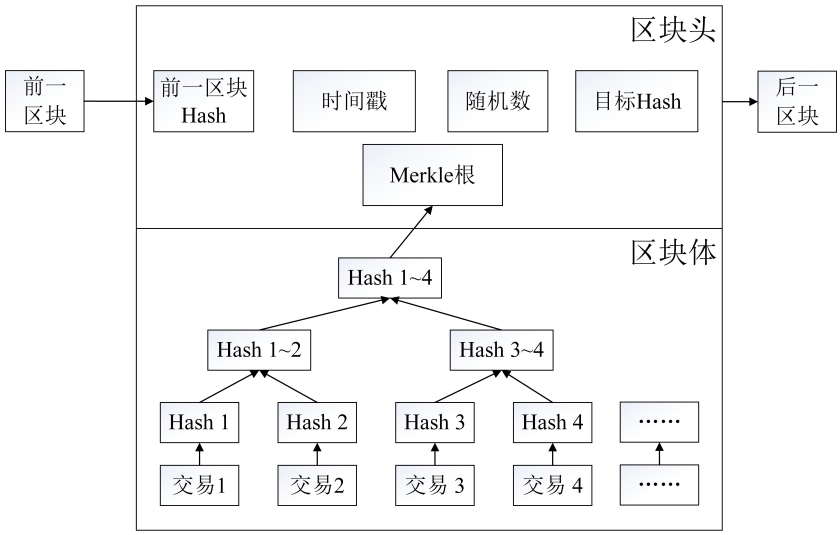

图 1 区块结构图

Figure 1 Structure of block

以比特币为例给出区块链结构中交易的存储形式, 如图2所示. 图中展示了两个交易, 即 T_A 和 T_B, 涉及到三个参与主体 A、B 和 C, 图中的箭头显示了 d 个单位的比特币的流转过程, $[T_A]$ 代表交易 T_A 除去 in-script 字段后的所有字段值, $\mathrm{sig}_A(m)$ 代表用主体 A 的私钥对消息 m 进行签名, $\mathrm{ver}_A(\mathrm{body}, \sigma)$ 代表使用主体 A 的公钥验证 σ 为消息 body 的签名. 主体 A 在交易 T_X 中获得了大于 d 个数量的比特币, A 在交易 T_A 中将 T_X 中的 d 个比特币支付给了 B, 而 B 则在交易 T_B 中将这 d 个比特币进一步支付给了 C. 交易 T_A 和 T_B 中均包含了 4 个字段, 以交易 T_B 为例, 字段 in 指明了本次交易的比特币来源于交易 T_A; 字段 val 指明了交易的比特币数量为 d; 字段 out-script 指明了输出条件 $\mathrm{ver}_C(\mathrm{body}, \sigma 2)$, 要求下一交易必须提供主体 C 的签名, 只有满足这一输出条件的交易才可以进一步使用本交易中的比特币, 私钥的保密性保证了只有主体 C 可以使用交易 T_B 中的 d 个比特币, 即实现了比特币从 B 流向了 C; 为满足输入交易 T_A 中的 out-script 要求, 字段 in-script 则提供了 B 对交易 T_B 的相应签名.

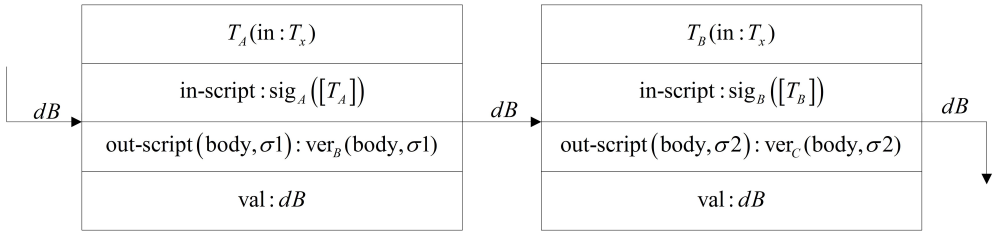

图 2 交易结构图

Figure 2 Structure of transactions

依据区块链中的网络结构及其运行方式, 给出区块链中的安全模型如下 [16,17]:

(1) 区块链中各节点之间不存在安全信道连接;

(2) 区块链中的节点均可以访问到正确的链结构 BlockChain;

(3) 节点发布的正确交易会在最大时延 $\max_{BB}$ 内被包含到正确的链结构 BlockChain 中;

(4) 区块链中的链结构 BlockChain 在诚实节点比例大于 50% 下是不可以伪造和篡改的.

3 协议设计

3.1 符号说明

对协议中涉及的符号进行说明如下:

1) 协议参与主体: 协议涉及两类参与主体, 消息发送者主体 A, 消息接收者的主体集合 B, B' 为主体 A 确定的最终可以获得消息的主体集合, B_i 为主体集合中某一特定主体;

2) 协议消息符号: $f_{\{\text{Eoo,Eor,Con}\}}$ 为消息标识, 分别预示着消息的目的为源不可否认证据、接收不可否认证据和密钥公布证据; l 是一个特殊的标识, $l = h(m,k)$, 其中 $h()$ 为单向哈希函数, 指示着本次协议运行的唯一性; t 为协议运行的时间参数, 指明了交易 OPEN 出现在链结构 BlockChain 中的最后期限; c 为用对称密钥 k 对消息 m 加密的密文, 即 $c = \{m\}_k$; $E_{R'}(k)$ 为运用组加密方式对 k 的加密密文, 只可以由主体 $R_i \in R'$ 进行解密;

3) 证据项及缩写: $\text{Eoo} = S_A(f_{\text{Eoo}}, B, l, t, c)$, $\text{Eor}_i = S_{B_i}(f_{\text{Eor}}, A, l, t, c)$ 和 $\text{Con\_}k = S_A(f_{\text{Con}}, A, B', l, E_{B'}(k))$ 均为主体对消息的签名, 分别代表了主体 A 对密文 c 的发送不可否认证据、主体 B_i 对密文 c 的接收不可否认证据和主体 A 对密钥 k 的公布不可否认证据; 为表述方便, 分别以 Eoo_p、Eor_{ip} 和 $\text{Con\_}kp$ 代表主体所签名的原消息;

4) 消息传递方式: $X \Rightarrow Y$: 主体 X 以多播或广播的形式对外发送消息, 可以是向主体集合 Y 多播消息, 也可以是向全网广播交易信息; $X \to Y$: 主体 X 向主体 Y 发送消息; $X \leftrightarrow Y$: 主体 X 通过访问网络中的公开信息, 从 Y 处获得消息, 例如向某一主体获取链结构 BlockChain.

3.2 协议流程

协议分为两个阶段, 第一个阶段是对消息密文的传送以及收集相应的不可否认证据, 第二个阶段是利用区块链中链结构 BlockChain 的公开性和可验证性公布密钥, 消息的发送方通过向区块链中广播交易 OPEN 的方式, 向接收方公布密文的解密密钥, 包含此交易的区块成为了接收双方的不可否认证据. 协议的执行流程如下:

1. $A \Rightarrow B : f_{\text{Eoo}}, B, l, t, c, \text{Eoo}$;

2. $B_i \to A : f_{\text{Eor}}, A, B_i, l, \text{Eor}_i$ where each $B_i \in B$;

3. $A \Rightarrow \text{BlockChain: OPEN(in} : T_{Ax})$;

4. $B_i \leftrightarrow \text{BlockChain: Con\_}kp, \text{Con\_}k$ where each $B_i \in B'$.

协议起始, 主体 A 拥有消息 m, 希望将此消息发送给主体集合 B 中的成员, 主体 A 随机选取一个对称密钥 k 和一个合适的时间点 t, 并计算得到 $l = h(m,k)$、$c = E_k(m)$ 和 $\text{Eoo} = S_A(f_{\text{Eoo}}, B, l, t, c)$, 随后 A 以多播的形式向主体集合 B 发送消息 (1);

主体 B_i 收到消息 (1) 后, 用 A 的公钥验证签名 Eoo 的正确性, 并检查时间 t 的合理性, 验证与检查均通过后, 主体 B_i 保存不可否认证据 Eoo 并计算 $\mathrm{Eor}_i = S_{B_i}(f_{\mathrm{Eor}}, A, l, t, c)$, 随后向主体 A 回复消息 (2), 表达愿意参与协议, 若验证签名 Eoo 错误或者主体 B_i 不能接受时间 t, 则主体 B_i 不做任何回应;

主体 A 在发送消息 (1) 后, 便开始等待集合 B 中成员的回应, 在收到消息 (2) 后, 主体 A 检查协议唯一性标签 $l \stackrel{?}{=} h(m,k)$ 以及签名 Eor_i 的正确性, 若未通过检查, 则忽略该主体的消息 (2), 若检查通过, 则主体 A 保存不可否认证据 Eor_i 并将主体 B_i 加入集合 B' 中. 主体 A 会选择一个合适的时间 $t' < t - \max_{BB}$ 对外广播交易 OPEN, 超过此时间到达的消息 (2) 将被忽略;

主体 B_i 回复消息 (2) 后, 在时刻 t 访问区块链中的公开链结构 BlockChain, 查找到交易 OPEN, 从交易 OPEN 中提取出 Con_k 和 Con_kp, 检查协议唯一性标识 l 和签名 Con_k 的正确性, 用私钥解密 $E_{R'}(k)$ 得到密钥 k, 再进一步解密密文 c 得到消息 m, 保存不可否认证据 Con_k. 若主体 B_i 未查找到交易 OPEN 或签名 Con_k 错误, 则认为主体 A 发布密钥有误, 协议终止, 此时仍然不影响协议的公平性, 在安全性分析中将进行证明.

交易 OPEN 的结构如图3所示, 假设主体 A 拥有标识其身份的唯一公私钥对, 同时拥有若干用于区块链中进行交易的临时公私钥对, 不妨设为 Ax 和 Ay, 区块链中允许用户产生用于交易的临时公私钥对, 这一假设在区块链中是可行的, 这些不同的公私钥对就像主体 A 不同的银行账户. 假设主体 A 曾在交易 T_{Ax} 中获得不少于 d 个比特币, 交易 OPEN 以交易 T_{Ax} 为输入, 并在字段 in-script 中对外公布了 Con_k 和 Con_kp, 在交易费用为零的情况下, 主体 A 并没有任何经济损失, 只是将在账户 Ax 下的 d 个比特币转移到了账户 Ay 下.

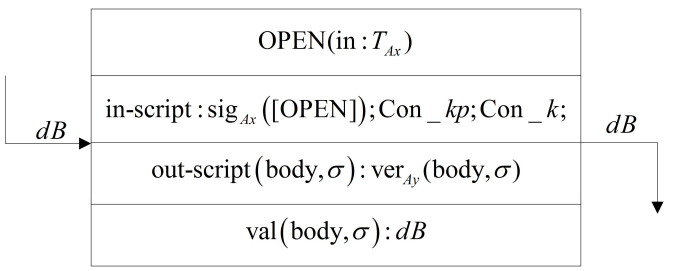

图 3 交易 OPEN 结构图
Figure 3 Structure of transaction OPEN

4 协议安全性与性能分析

4.1 安全性分析

多方不可否认协议的设计主要需要满足三个安全目标, 一是不可否认性, 这是此类协议的设计初衷, 包括消息发送方对发送行为的不可否认和接收方对消息正确接收这一事实的不可否认, 二是公平性, 协议执行结束后, 消息发送方应获得接收方的接收证据, 同时, 接收方也必须获得发送方的发送证据, 公平性是指或者协议参与方均获得自己所需的证据项, 或者协议参与方均没有获得任何有价值的信息, 三是时限性, 协议的诚实参与方应在有限时间内完成协议, 并且没有违反公平性, 协议的任意参与方都可以在任意时刻终止协议, 但前提是这种行为没有损害自身的利益, 不满足时限性的协议, 协议参与方因无法接收到所需证据项而长久等待下去, 无法正常终止协议. 很显然, 不满足时限性的协议很有可能同样不满足公平性, 但是不能将时限性分析简单归于公平性的分析, 协议设计中一些时间因素的设置不当会造成时限性问题, 但是简单对协议的公平性进行分析却容易忽略时间因素的作用, 不能发现其中存在的问题. 综合比较现有的多方不可否认协议分析方法, 文献 [10] 的方法对协议参与方的数量没有限制, 同时不存在状态空间爆炸问题, 能够比较完整的支持三大安全目标的分析. 因此, 本文采用文献 [10] 的方法对所提协议进行安全性分析.

1983 年, Dolev 和 Yao 提出了 DY 模型, 模型中抽象了攻击者所具有的攻击能力: 一是攻击者可以获取通过网络的任何消息; 二是攻击者可以以合法用户的身份, 向其他任何用户发起会话; 三是攻击者有可能成为任何用户所发送消息的接收者. 在该模型下, 攻击者对网络具有完全的控制权, 可以在协议执行中的任何环节采取多种形式的攻击. 逻辑分析方法建立在 DY 模型的基础上, 从已知的事实出发推理得到所需的安全目标或其反面. 文献 [10] 的方法是对 SVO 逻辑的扩展, 在 SVO 逻辑的基础上引入了时间表达式, 一般安全性质的分析与 SVO 逻辑相同, 时限性的分析通过时间演算进行分析. 列出安全性分析中用到的推理规则和公理如下:

分离规则 (MP): $\frac{\vdash\varphi,\vdash\varphi\rightarrow\psi}{\vdash\psi}$;

必然规则 (Nec): $\frac{\vdash\varphi}{\vdash P\ \text{believes}\varphi}$;

A1. P believes $\varphi\wedge P$ believes $(\varphi\rightarrow\psi)\rightarrow P$ believes ψ;

A4. $\mathrm{PK}_\sigma(Q,k)\wedge R$ received $S_Q(X)$ at $[T]\rightarrow Q$ said X at $[T]$;

A6. P received $(X_1,\cdots,X_n)$ at $[T]\rightarrow P$ received X_i at $[T]$;

A7. P received $\{X\}_k$ at $[T_1]\wedge P$ has $\widetilde{k}$ at $[T_2]\rightarrow P$ received X at $[\max(T_1,T_2)]$, $\widetilde{k}$ 为与 k 对应的解密密钥;

A9. P received $S_Q(X)$ at $[T]\rightarrow P$ received X at $[T]$.

在进行逻辑推理之前, 首先给出若干协议假设, 这些假设是对协议运行环境的表述, 是协议运行的基础. 关于主体密钥的假设, 任意仲裁方 J 相信主体拥有自己的私钥, 同时公钥对外公开:

P1.1 J believes $\mathrm{PK}_\sigma(A,k_A)$;

P1.2 J believes $\mathrm{PK}_\sigma(B_i,k_{B_i})$;

P1.3 $\mathrm{PK}_\sigma(A,k_A)$;

P1.4 $\mathrm{PK}_\sigma(B_i,k_{B_i})$.

主体是理智的, 不会做对自己不利的事情, 即 B_i 仅在收到 Eoo 后才会发送 Eor_i, 而 A 仅在收到 Eor_i 后, 才会对外公布 Con_k:

P2.1 B_i said Eor_{ip} at $[T_x]\rightarrow(B_i$ received Eoo at $[T_y|\{x|x\leqslant T_x\}])$;

P2.2 J believes $(B_i$ said Eor_{ip} at $[T_x]\rightarrow(B_i$ received Eoo at $[T_y|\{x|x\leqslant T_x\}]))$;

P2.3 A said Con_kp at $[T_x]\rightarrow(A$ received Eor_i at $[T_y|\{x|x\leqslant T_x\}])$.

区块链中链结构 BlockChain 是公开的, 可以被所有节点正确访问到, 并且任意仲裁方 J 均相信这一点, 此处的证据 Con_k 特指来自于链结构 BlockChain 中的交易 OPEN, 而并非通过简单的消息发送与接收:

P3.1 P received Con_k at $[T]\rightarrow Q$ received Con_k at $[T]$;

P3.2 J believes (P received Con_k at $[T]\rightarrow Q$ received Con_k at $[T]$).

关于组加密方式的假设, 协议中使用的组加密方案具有保密性, 即只有属于组内的成员才能使用自己的私钥解密组加密密文:

P4 J believes $((R_i$ received $E_R(X)$ at $[T])\wedge(R_i\in R)\rightarrow R_i$ received X at $[T])$.

定理 1 不可否认性: 协议满足不可否认性, 当某一协议参与方否认曾参与协议时, 相关参与方可以通过向仲裁方提交不可否认证据维护自身利益. 消息发送方 A 应保存的证据有 Eor_i、消息 m 和对应的解密密钥 k; 消息接收方 B_i 应保存的证据有 Eoo、消息 m 和对应的解密密钥 k.

证明: 假设协议结束后, 接收方 B_i 否认收到了消息 m, 此时发送方 A 向仲裁方 J 提交证据项 Eor_i、消息 m 和密钥 k 并申请进行仲裁, 仲裁方 J 独立计算 $l=h(m,k)$, 并据此在链结构 BlockChain 中找到对应的交易 OPEN, 从中提取出 $E_{B'}(k)$ 和证据项 Con_k, 通过组加密方式的特性, 判定 $B_i\in B'$ 是否成立, 若不成立, 通知 A 接收方 B_i 不能解密组加密密文, 未获得消息 m, 仲裁结束; 若有 $B_i\in B'$ 成立, 则有如下推理过程.

(1) J believes (J received $\{\mathrm{Eor}_i$, Con_$k\}$) 前提.

(2) J believes (P received $(X_1,\cdots,X_n)$ at $[T]\rightarrow P$ received X_i at $[T]$) A6 Nec.

(3) J believes (J received Eor_i) (1) (2) A1 MP.

(4) J believes ($\mathrm{PK}_\sigma(Q,k) \wedge R$ received $S_Q(X)$ at $[T] \rightarrow Q$ said X at $[T]$) A4 Nec.

(5) J believes (B_i said Eor_{ip}) P1.2 (3) (4) A1 MP.

(6) J believes (B_i received Eoo) (5) P2.2 A1 MP.

(7) J believes (P received $S_Q(X)$ at $[T] \rightarrow P$ received X at$[T]$) A9 Nec.

(8) J believes (B_i received Eoo_p) (6) (7) A1 MP.

(9) J believes (B_i received c) (8) (2) A1 MP.

(10) J believes (J received Con_k) (1) (2) A1 MP.

(11) J believes (B_i received Con_k) (10) P3.2 A1 MP.

(12) J believes (B_i received Con_kp) (11) (7) A1 MP.

(13) J believes (B_i received $E_{B'}(k)$) (12) (2) A1 MP.

(14) J believes ($B_i \in B'$) 前提

(15) J believes (B_i received k) (13) (14) P4 A1 MP.

(16) J believes (B_i received m) (9) (15) A7 Nec. A1 MP.

至此, 仲裁方 J 判定主体 B_i 收到了消息 m. 对于主体 A 否认发送过消息 m 的情况, 其证明过程相似, 在此不再赘述. □

定理 2 公平性: 协议满足强公平性, 协议某一参与方获得完整不可否认证据当且仅当其它利益相关方同样获得了完整的不可否认证据. 设置公平性目标如下:

G1. A received {Eor_i, Con_k} $\rightarrow$ B_i received {Eoo,Con_k}

G2. B_i received {Eoo, Con_k} $\rightarrow$ A received {Eor_i, Con_k}

证明: 首先对 G1. 进行证明, 若 A received { Eor_i, Con_k} 为假, 则目标 G1. 为真, 前提为假则结论为真. 下面仅分析 A received {Eor_i, Con_k} 为真的情况.

(17) A received {Eor_i, Con_k} 前提

(18) A received Eor_i (17) A6 MP.

(19) B_i said Eor_{ip} P1.2 (18) A4 MP.

(20) B_i received Eoo (19) P2.1 MP.

(21) A received Con_k (17) A6 MP.

(22) B_i received Con_k (21) P3.1 MP.

(23) B_i received {Eoo, Con_k} (20) (22)

G2. 的证明过程与此类似, 在此不再赘述. □

定理 3 时限性: 协议的所有参与方都可以在时刻 t 之前完成协议, 而不影响公平性.

证明: 由定理 2 可知, 协议满足公平性, 则或者参与方均获得完整的不可否认证据, 或者都没有获得完整的不可否认证据. 若参与方均未获得完整的证据, 则参与方可在 t 时刻终止协议, 而不影响公平性. 下面仅对参与方均获得完整证据的情况进行证明. 假设链结构 BlockChain 中包含交易 OPEN 的区块上时间戳为 t_{OPEN}, 由于链结构 BlockChain 的公开可访问性, 任意主体均可在 t_{OPEN} 时刻访问到 Con_k.

(24)J received Con_k at $[t_{\mathrm{OPEN}}]$ 前提

(25)A received Con_k at $[t_{\mathrm{OPEN}}]$ (24) P3.1 MP.

(26)B_i received Con_k at $[t_{\mathrm{OPEN}}]$ (24) P3.1 MP.

(27)A said Con_kp at $[t_{\mathrm{OPEN}}]$ P1.3 (26) A4 MP.

(28)A received Eor_i at $[T_x|\{x|x \leqslant t_{\mathrm{OPEN}}\}]$ (27) P2.3 MP.

(29)B_i said Eor_{ip} at $[T_x|\{x|x \leqslant t_{\mathrm{OPEN}}\}]$ P1.4 (28) A4 MP.

(30)B_i received Eoo at $[T_y|\{x|x \leqslant T_x\}]$ (29) P2.1 MP.

由以上的逻辑推理 (25) 和 (28) 可知, 主体 A 在不晚于 t_{OPEN} 时刻收到了所有的证据项, 由 (26)、(29) 和 (30) 可知, B_i 在不晚于 t_{OPEN} 时刻收到了所有证据项, 并进一步可以获得消息明文 m. 由协议要

求, 交易 OPEN 必须在 t 时刻以前出现在链结构 BlockChain 中, 则有 $t_{\mathrm{OPEN}} \leqslant t$ 成立, 即协议满足时限性. □

4.2 性能对比

分别从签名操作、非对称密码操作和对 TTP 的依赖程度等几个方面将本文协议与典型多方不可否认协议进行对比, 其中对证据项存储数的统计各文献中标准不一. 本文假设存在这样两个理想函数 f_1 和 f_2: 若存在主体 O 对消息 m_1、m_2 和 m_3 的签名 $s = S_O(m_1, m_2, m_3)$, 则有 $f_1(O, s)$ 可以判断签名的主体是否为 O, $f_2(s, m_2)$ 可以判断签名 s 中是否包含消息 m_2, 简化了协议中证据项存储数量的分析, 并且保证了数据仍然可以表征协议性能的优劣. 对 TTP 的依赖程度设置为 3 个选项: on-line 是指 TTP 会参与协议的每次运行; off-line 是指在理想情况下, 协议运行不需要 TTP 参与, 对比数据均在理想情况下进行统计; no-TTP 是指协议运行完全不需要 TTP 的参与.

假设 $|B| = n$, 即集合 B 中共有 n 个主体成员, $|B'| = m$, 集合 B' 中共有 m 个主体成员. 表1展示了消息发送方主体 A 的对比情况, 其中文献 [9] 所提协议中在消息收发双方之间存在着云提供者主体 CloudProvider, CloudProvider 在协议中承担了 m+6 次签名操作并存储了 m+1 个证据项; 文献 [7] 中 TTP 承担了 m 次非对称密码操作, 可以看到, 本文协议在各项指标上均具有良好的协议性能. 表2展示了消息接收方主体 B_i 的对比情况, 可以看到所有协议的数据均为常数项, 本文协议保持了较好的协议性能.

表 1 主体 $\boldsymbol{A}$ 性能对比

Table 1 Performance contrasts of entity $\boldsymbol{A}$

性能	文献 [3]	文献 [5]	文献 [7]	文献 [9]	本文协议
签名生成与验证	m+3	2m+3	m+n+2	4(+m+6)	m+3
非对称加密与解密	m	m+n+1	n(+m)	n	m
证据项存储数	m+5	m+2	3m+2	1(+m+1)	m+2
对 TTP 的依赖程度	on-line	off-line	on-line	off-line	no-TTP
单播消息数	2	0	n+2	1	0
广播消息数	1	2	0	0	2

表 2 主体 $\boldsymbol{B_i}$ 性能对比

Table 2 Performance contrasts of entity $\boldsymbol{B_i}$

性能	文献 [3]	文献 [5]	文献 [7]	文献 [9]	本文协议
签名生成与验证	3	5	3	5	3
非对称加密与解密	1	1	2	1	1
证据项存储数	6	4	4	1	3
对 TTP 的依赖程度	on-line	off-line	on-line	off-line	no-TTP
单播消息数	2	2	2	1	2
广播消息数	0	0	0	0	0

4.3 关于组加密方案

组加密方案提供了这样的特性, 可以由一方独立完成加密过程, 只能由组内成员解密. 文献 [18] 提出一种组加密方案, 在多方不可否认协议的设计中一直延续了对此方案的使用, 此加密方案同样适用于本文所提协议. 加密方案基于非对称密码体制和中国剩余定理, 假定 m 个组内成员均保有自己的私钥 d_i, 同时将公钥 e_i 和一个大整数 N_i 对外公开. 加密方想以组加密的方式加密密钥 k, 以 $E(k, e_i)$ 表示用公钥

e_i 加密 k 所得结果, 以 $D(x, d_i)$ 表示用私钥 d_i 解密 x 所得结果, 其独立计算 $c_i = E(k, e_i)(1 \leqslant i \leqslant m)$, 由中国剩余定理可知, 存在解 X 使得 $X \equiv c_i \bmod N_i(1 \leqslant i \leqslant m)$ 成立, 解 X 即为对 k 的组加密密文, 组内成员计算 $k = D(X, d_i)$. 本文协议中组加密以 $E_{R'}(k)$ 表示, 暗含了通过组加密密文可以判断主体是否可以正确解密密文, 即 $R_i \in R'$, 只需要计算 $E_{R'}(k) \bmod N_i = E(k, e_i)$ 是否成立即可.

5 结束语

本文基于区块链提出一种无 TTP 的多方不可否认协议, 形式化分析证明了协议满足不可否认性、强公平性和时限性, 并与经典协议在签名操作和非对称密码操作等多个方面进行了对比分析, 所提协议均显示了良好的协议性能.

References

[1] FENG D G, FAN H. Survey on theories and methods of formal analyses for security protocols[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2003, 20(4): 389–406. [DOI: 10.3969/j.issn.1002-1175.2003.04.001]
冯登国, 范红. 安全协议形式化分析理论与方法研究综述 [J]. 中国科学院研究生院学报, 2003, 20(4): 389–406. [DOI: 10.3969/j.issn.1002-1175.2003.04.001]

[2] TIAN H B, HE J J, FU L Q. A privacy preserving fair contract signing protocol based on public block chains[J]. Journal of Cryptologic Research, 2017, 4(2): 187–198. [DOI: 10.13868/j.cnki.jcr.000173]
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 [J]. 密码学报, 2017, 4(2): 187–198. [DOI: 10.13868/j.cnki.jcr.000173]

[3] KREMER S, MARKOWITCH O. A multi-party non-repudiation protocol[C]. In: Information Security for Global Information Infrastructures—SEC 2000. Springer Boston, 2000: 271–280. [DOI: 10.1007/978-0-387-35515-3_28]

[4] MARKOWITCH O, KREMER S. A multi-party optimistic non-repudiation protocol[C]. In: Information Security and Cryptology—ICISC 2000. Springer Berlin Heidelberg, 2000: 109–122. [DOI: 10.1007/3-540-45247-8_9]

[5] DENG S Y, SUI A F, HU Z M, et al. An optimistic fair multi-party non-repudiation protocol[J]. Journal of Electronics & Information Technology, 2002, 24(12): 1985–1989.
邓所云, 隋爱芬, 胡正名, 等. 一个优化的公平的多方不可否认协议 [J]. 电子与信息学报, 2002, 24(12): 1985–1989.

[6] HE B, LI X J, XIA C H, et al. A fair multi-party non-repudiation protocol[J]. Computer Engineering and Applications, 2005, 41(27): 120–122. [DOI: 10.3321/j.issn:1002-8331.2005.27.038]
何冰, 李肖坚, 夏春和, 等. 公平的多方不可否认协议 [J]. 计算机工程与应用, 2005, 41(27): 120–122. [DOI: 10.3321/j.issn:1002-8331.2005.27.038]

[7] HAN Z G, LUO J Z. A fair multi-party non-repudiation protocol[J]. Chinese Journal of Computers, 2008, 31(10): 1705–1715. [DOI: 10.3321/j.issn:0254-4164.2008.10.005]
韩志耕, 罗军舟. 一个公平的多方不可否认协议 [J]. 计算机学报, 2008, 31(10): 1705–1715. [DOI: 10.3321/j.issn:0254-4164.2008.10.005]

[8] LI Y P, SI G D, WANG Y M. A new multi-party non-repudiation protocol[J]. Computer Science, 2006, 33(8): 95–97. [DOI: 10.3969/j.issn.1002-137X.2006.08.025]
李艳平, 司光东, 王育民. 一种新的多方不可否认协议 [J]. 计算机科学, 2006, 33(8): 95–97. [DOI: 10.3969/j.issn.1002-137X.2006.08.025]

[9] FENG J, CHEN Y, SUMMERVILLE D H. A fair multi-party non-repudiation scheme for storage clouds[C]. In: International Conference on Collaboration Technologies and Systems. IEEE, 2011: 457–465. [DOI: 10.1109/CTS.2011.5928724]

[10] HAN Z G, LUO J Z. Analysis and improvement of timeliness of a multi-party non-repudiation protocol[J]. Acta Electronica Sinica, 2009, 37(2): 377–381. [DOI: 10.3321/j.issn:0372-2112.2009.02.025]
韩志耕, 罗军舟. 多方不可否认协议时限性分析与改进 [J]. 电子学报, 2009, 37(2): 377–381. [DOI: 10.3321/j.issn:0372-2112.2009.02.025]

[11] WANG X Q, WANG, X M. Formal analysis of multi-party non-repudiation protocols without TTP[C]. In: Proceedings of the International Conference on Communications and Intelligence Information Security. IEEE, 2010: 96–99. [DOI: 10.1109/ICCIIS.2010.33]

[12] WANG X M, WENG L C. Analysis and improvement of a fair multi-party non-repudiation protocol based on ATL logic[J]. Information Security and Technology, 2011, 2011(9): 21–25. [DOI: 10.3969/j.issn.1674-9456.2011.09.005]
汪学明, 翁立晨. 基于 ATL 逻辑的公平多方不可否认协议的分析与改进 [J]. 信息安全与技术, 2011, 2011(9): 21–25.

[DOI: 10.3969/j.issn.1674-9456.2011.09.005]
[13] LI L, WANG L C, CHEN J, et al. Fairness analysis for multiparty nonrepudiation protocols based on improved strand space[J]. Discrete Dynamics in Nature & Society, 2014, 2014(1): 1–7. [DOI: 10.1155/2014/904717]
[14] YUAN Y, WANG F Y. Blockchain: The state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481–494. [DOI: 10.16383/j.aas.2016.c160158]
袁勇, 王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报, 2016, 42(4): 481–494. [DOI: 10.16383/j.aas.2016.c160158]
[15] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[OL]. https://bitcoin.org/bitcoin.pdf, 2008.
[16] ANDRYCHOWICZ M, DZIEMBOWSKI S, MALINOWSKI D, et al. Fair two-party computations via bitcoin deposits[C]. In: Financial Cryptography and Data Security—FC 2014. Springer Berlin Heidelberg, 2014: 105–121. [DOI: 10.1007/978-3-662-44774-1_8]
[17] KIAYIAS A, ZHOU H S, ZIKAS V. Fair and robust multi-party computation using a global transaction ledger[C]. In: Advances in Cryptology—EUROCRYPT 2016, Part II. Springer Berlin Heidelberg, 2016: 705–734. [DOI: 10.1007/978-3-662-49896-5_25]
[18] CHIOU G H, CHEN W T. Secure broadcasting using the secure lock. IEEE Transactions on Software Engineering, 1989：15(8): 929–934. [DOI: 10.1109/32.31350]

作者信息

苑博奥 (1992–), 河北晋州人, 硕士研究生. 主要研究领域为安全协议.
yuanboao1201@sina.com

刘军 (1969–), 江苏吴县人, 教授. 主要研究领域为信息安全, 软件工程.
13914735588@139.com

李戈 (1983–), 江苏南京人, 讲师. 主要研究领域为信息安全.
lige1901@139.com