Hans Journal of Data Mining 数据挖掘, 2026, 16(3), 90-104
Published Online July 2026 in Hans. https://www.hanspub.org/journal/hjdm
https://doi.org/10.12677/hjdm.2026.163009

Hans汉斯

基于混合区块链架构的可验证数据隐私保护方案

齐钰娇*，刘雪艳，贾博龙，罗田田

西北师范大学人工智能与计算机学院(软件学院)，甘肃 兰州

收稿日期：2026年6月6日；录用日期：2026年6月30日；发布日期：2026年7月6日

摘 要

作为日常公益活动之一，物资捐赠有助于改善受赠者(包括个人、机构或团体)的条件与环境。然而，捐赠过程中身份隐私保护不足、资源分配的公平性及有效性难以保证，难以兼顾资源共享与物资信息隐私保护之间的平衡等问题，制约了其有效实施。为应对这些挑战，本文提出了一种基于混合区块链架构的可验证数据隐私保护方案。该方案利用可随机化证书确保交易行为与身份之间的不可链接性，通过智能合约自动生成捐赠请求的优先级列表并记录交易状态，保证物资分配的公平性及有效性；同时引入佩德森承诺机制，确保资产与捐赠行为的可验证。通过结合私有链与联盟链，实现慈善组织内部数据的隐私保护，以及跨组织的资源共享与捐赠交易监督。安全性分析表明，该方案满足匿名性、可验证性、机密性与完整性要求。仿真实验结果显示，该方案具有良好的可行性、执行效率与性能。

关键词

隐私保护，可随机化证书，区块链，智能合约，物资捐赠

A Verifiable Data Privacy Protection Scheme Based on a Hybrid Blockchain Architecture

Yujiao Qi*, Xueyan Liu, Bolong Jia, Tiantian Luo

School of Artificial Intelligence and Computer Science (School of Software), Northwest Normal University, Lanzhou Gansu

Received: June 6, 2026; accepted: June 30, 2026; published: July 6, 2026

Abstract

As one of the everyday public welfare activities, material donations help improve the conditions

*通讯作者。

文章引用: 齐钰娇, 刘雪艳, 贾博龙, 罗田田. 基于混合区块链架构的可验证数据隐私保护方案[J]. 数据挖掘, 2026, 16(3): 90-104. DOI: 10.12677/hjdm.2026.163009

and environments of donees, including individuals, institutions, or groups. However, issues such as privacy protection, fairness in resource allocation, and the balance between resource sharing and privacy protection hinder its effective implementation. To address these challenges, this paper proposes a verifiable data privacy protection scheme based on a hybrid blockchain architecture. The scheme utilizes randomizable credentials to ensure unlinkability between transactions and identities, employs smart contracts to automatically generate priority lists for donation requests and record transaction status, thereby ensuring the fair distribution of materials, and introduces the Pedersen commitment mechanism to guarantee the verifiability of assets and donations. By incorporating both private and consortium blockchains, the scheme protects internal data security within charitable organizations and enables cross-organizational resource sharing and transaction supervision, respectively. Security analysis demonstrates that the scheme satisfies the requirements of anonymity, verifiability, confidentiality, and integrity. The simulation results show that the scheme has good feasibility, execution efficiency and performance.

Keywords

Privacy Protection, Randomized Anonymous Certificate, Blockchain, Smart Contract, Material Donation

1. 引言

随着经济全球化与社会现代化的持续推进，公众的社会责任意识显著增强。在基本生活需求得到满足的基础上，越来越多的个人和企业开始主动关注社会问题，并通过多种形式支持弱势群体，积极参与公益行动[1]。在数字化时代，捐赠管理平台为公益事业带来了前所未有的便捷与效率。目前，主流捐赠平台 Eleo [2]，DonorSnap [3]，easyTithe [4]主要依托云计算技术构建，采用集中式架构提供服务。但该架构存在明显单点故障风险，如果中心服务器或者数据库出现故障，将会使整个系统无法正常运行，进而使捐赠流程中断。这不仅影响捐赠者的使用体验，也可能延误对受助群体的及时支持。此外，透明度不足是当前捐赠系统的另一关键问题。由于捐赠者和受赠者难以实时了解捐赠物资的流向与使用情况，信息不对称直接导致了公众信任的缺失。为应对上述挑战，近年来学术界相继提出了基于区块链技术的慈善捐赠方案，利用去中心化、不可篡改和可追溯等特性，为解决慈善捐赠中的系统可靠性及透明度问题提供了新的技术路径。

近年来，基于区块链的捐赠方案被提出，为解决上述挑战提供了新的路径。J. Sung 等人[5]将区块链技术的三个核心特征－透明性、不可篡改性和高效性，应用于非营利组织的捐赠系统。通过实证分析，验证了区块链技术在提升非营利组织可信度方面的有效性，为 NPO 采用区块链提供了理论和实践基础。Hasan 等人[6]基于区块链的物理物品交付证明解决方案，该方案利用区块链技术和智能合约解决了交付过程中的信任缺失和追踪难题，在增强交易透明度、追踪性和安全性方面具有一定优势。Li 等人[7]设计了一个基于区块链和智能合约的物资捐赠系统，该系统通过智能合约实现需求发布、物资捐赠、物资分配等功能，并使用零知识证明技术保护物资在物流过程中的隐私安全。然而，在保护参与用户的身份隐私方面尚有不足，每次交易使用相同的匿名，容易导致身份与交易行为关联泄露身份隐私。Badarudi 等人[8]提出了一种基于区块链的数字援助模型，旨在解决灾难响应与恢复中的资源分配与协调挑战。该模型利用区块

链实现资源的透明管理和快速分配，同时通过区块链代币化功能，将物理资产转化为数字资产促进快速流通与互操作性，并保障资产的安全性和可信度。然而，该模型不支持物资捐赠，这在一定程度上限制了其应用范围。Zhou 等人[9]提出了一种高效且安全的基于区块链的捐赠方案，具有隐私保护和可审计性，但未能实现跨组织资源共享。为此，D. Zhang 等人[10]提出了一种基于联盟区块链的医疗数据安全共享方案，通过结合链上智能合约的细粒度属性访问控制与链下加密存储，解决了医疗数据在跨机构共享中的隐私泄露、信息孤岛及密钥管理难题。此外，利用私有链和联盟链的特性，Zhuji 等人[11]提出了一种结合私有链与联盟链的医疗数据共享方案，该方案通过私有链分布式加密存储患者医疗数据，防止数据丢失、泄露和篡改。同时，构建联盟链存储医院间的交易数据及各私有链中的医疗信息摘要，实现跨机构数据共享促进医疗资源有效利用。Li 等人[12]提出了一种基于双链结构与国家密码算法的疫苗溯源方案，有效解决了传统方案中数据易篡改、可信度低、责任追踪难及信息孤岛等问题。

针对上述问题，本文提出了一种结合私有区块链和联盟链技术的物资捐赠方案。该方案不仅确保了隐私性、可追溯性、可审计性和公平性，还在整个捐赠过程中保持了匿名性。本文的主要贡献如下：

(1) 提出了一种基于混合区块链架构的可验证数据隐私保护方案。该方案能有效实现定向与非定向两种捐赠模式，同时支持随机匿名捐赠，确保物资(如食品、衣物等实物)的公平分配，并保持捐赠交易的可追溯性和可审计性。其中，定向捐赠允许捐赠者自主选择符合其意愿的捐赠请求；非定向捐赠则指捐赠者不指定受赠方，直接进行物资捐赠。

(2) 将私有区块链与联盟链相结合，旨在保护隐私的同时实现跨组织资源共享。可随机化证书实现了匿名交易。利用智能合约确保物资的公平分配并记录捐赠交易状态。Pedersen 承诺保证了捐赠交易的可验证性。

(3) 对该方案进行了全面的安全性分析和实验验证。结果表明，该方案在满足捐赠交易的隐私性、公平性、可追溯性和可审计性的同时，能有效实现跨组织的资源共享。同时，该方案在性能和开销方面也展现出一定优势。

2. 方案模型

2.1. 系统模型

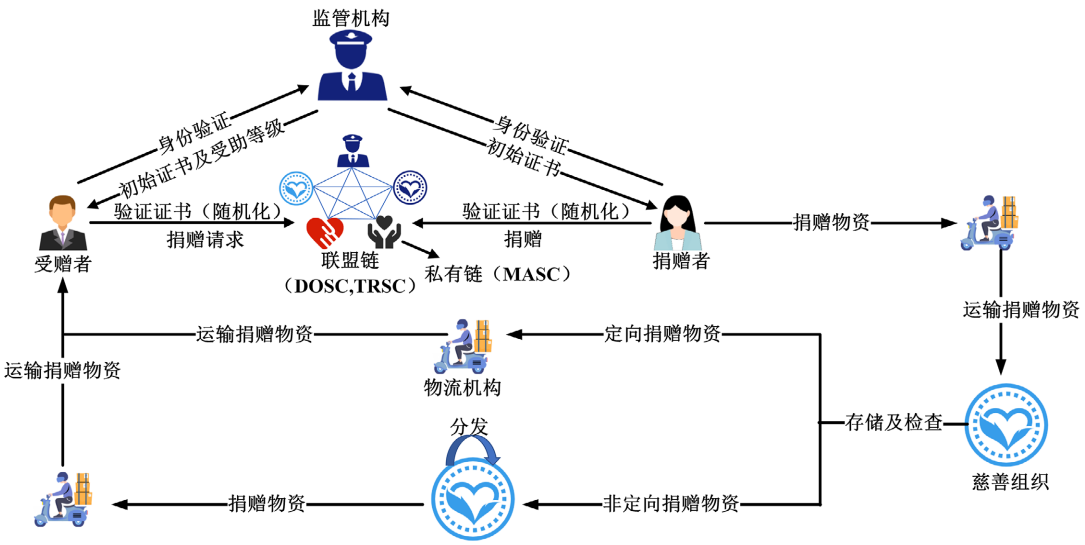

Figure 1. System model
图 1. 系统模型

方案系统模型，由捐赠者(Donor, Don)，受赠者(Donee, Doe)，监管机构(Regulatory Authority, RA)，物流机构(Logistics, L)，慈善组织(Charity Organization, C)，私有区块链(Private Blockchain, PBC)，联盟区块链(Consortium Blockchain, CBC)组成，如图 1 所示。

2.2. 混合区块链架构设计

混合区块链架构由私有链和联盟链构成，为确保两条区块链之间的可靠协同，该架构采用链间服务调用机制，避免了引入复杂的跨链协议。图 2 展示了混合区块链架构的主要结构。

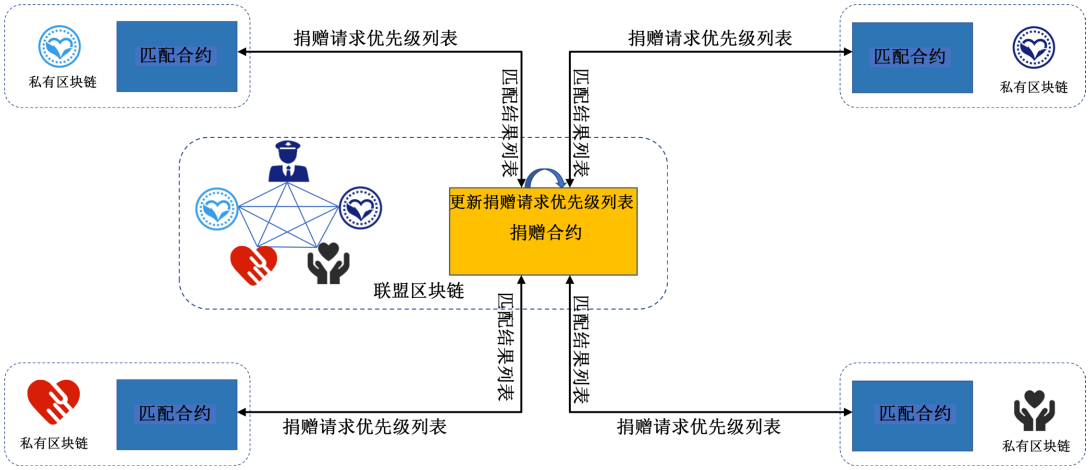

Figure 2. Hybrid blockchain architecture
图 2. 混合区块链架构

联盟链由多个慈善组织节点与监管机构节点共同维护，并运行两个核心智能合约，DOSC 与 TRSC。DOSC 根据受赠者的捐赠请求受助紧急程度等级生成捐赠请求优先级列表，并将其发布至联盟链，用于跨组织资源共享，慈善组织通过联盟链调用 DOSC 获取可信的捐赠请求优先级列表。

私有链由各慈善组织独立部署和管理，用于存储组织内部物资信息，同时在私有链上部署 MASC。MASC 可根据联盟链发布的捐赠请求优先级列表，在非定向捐赠场景下实现物资与捐赠请求的自动匹配，实现高效的资源调度。

3. 方案详细设计

3.1. 系统初始化

设 $\mathbb{G}_1$， $\mathbb{G}_2$， $\mathbb{G}_T$ 是阶为素数 p 的循环群， g_1 是 $\mathbb{G}_1$ 的生成元， g_2， q_2 是 $\mathbb{G}_2$ 的生成元。其中，双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$，定义哈希函数 $Hash$ 为 SHA-256，其映射关系为： $Hash:\{0,1\}^*\to\mathbb{Z}_p^*$。该系统的公共参数为 $pp=\left(p,g_1,g_2,q_2,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,\mathbb{Z}_p^*,e,Hash\right)$。

每个 C_i 都有各自的公私钥对 $\left(PK_{C_i},SK_{C_i}\right)$，其中 $PK_{C_i}=g_2^{-SK_{C_i}}$。RA 充当证书授权中心的角色，Don，Doe 根据公共参数生成各自的公私钥对。在交易过程中，为保护个人隐私， Don， Doe 可以对其公钥及初始证书进行随机化处理。以 Doe 为例，具体步骤如下：

(1) RA 选择两个随机数 $x,y\in\mathbb{Z}_p^*$ 作为其私钥，并计算 $X=g_2^x$， $Y=g_2^y$。RA 的公私钥对为 $PK_{RA}=\left(X,Y\right)$， $SK_{RA}=\left(x,y\right)$。

(2) Doe 选择一个随机数 $\alpha\in\mathbb{Z}_p^*$ 作为其私钥，并计算 g_1^{α}。Doe 的公私钥对为 $SK_{Doe}=\alpha$，$PK_{Doe}=g_1^{\alpha}$，追踪参数为 $Trk=g_2^{\alpha}$，该参数用于追溯恶意 Doe 的真实身份。

(3) *Doe* 将自己的公钥 PK_{Doe}，追踪参数 Trk，及个人属性 $Attr=\{attr_1,attr_2,\cdots,attr_n\}$ 提交给 *RA*。随后，*RA* 为 *Doe* 生成初始证书 *Cert*。*RA* 收到 *Doe* 发送的 PK_{Doe}，Trk，$Attr$ 后，对于每一个属性 $attr_i$ $(i=1,2,\cdots,n)$ 进行验证并逐一签名。*RA* 执行以下操作：

① 选择随机数 $z_i\in\mathbb{Z}_p^*$。

② 计算 $\widetilde{X}_i=g_1^{z_i}$，$\widetilde{Y}_i=PK_{Doe}^{Hash(attr_i)\cdot z_i}=g_1^{\alpha\cdot Hash(attr_i)\cdot z_i}$。

③ 每一个属性生成签名 $\delta_i=(\delta_{i1},\delta_{i2})=\left(\widetilde{X}_i,\widetilde{X}_i^{x}\cdot\widetilde{Y}_i^{y}\right)$，得到 $\delta=(\delta_1,\delta_2,\cdots,\delta_n)$。

④ 生成初始证书 $Cert=(\delta,attr)$，并将发送给用户 *Doe*。

⑤ 将对应记录保存在追踪列表 $\tilde{T}=(Trk_i,PK_{Doe},Cert)$。

(4) 在交易过程中，*Doe* 使用个人私钥，对公钥及初始证书中属性签名进行随机化处理，并生成零知识证明。*Doe* 执行以下操作：

① 公钥随机化处理。*Doe* 选择一个随机数 $\eta\in\mathbb{Z}_p^*$，计算 $\lambda=g_1^{\eta}$，随后计算 $\mu=PK_{Doe}^{\eta}=\left(g_1^{\alpha}\right)^{\eta}$，得到随机化处理后的公钥 $PK_{Dem}'=(\lambda,\mu)$。

② 初始证书随机化处理。假设只需公开属性下标为 $m(m\le n)$ 的属性，隐藏其余属性，则对需要被隐藏的属性的签名先进行聚合，得到聚合签名 δ'：

$$\delta'=(\delta_1',\delta_2')=\left(\prod_{i\ne m}^{n}\widetilde{X}_i\ ,\prod_{i\ne m}^{n}\widetilde{X}_i^{x}\cdot\widetilde{Y}_i^{y}\right)=\left(g_1^{\sum_{i\ne m}^{n}z_i}\ ,g_1^{x\sum_{i\ne m}^{n}z_i+\alpha\cdot y\sum_{i\ne m}^{n}Hash(attr_i)\cdot z_i}\right)$$

③ 对聚合后的签名 δ' 进行随机化。*Doe* 选择一个随机数 $w\in\mathbb{Z}_p^*$，并使用私钥 $SK_{Doe}=\alpha$ 计算：

$$\widetilde{\delta_1'}=\delta_1'^{w},\widetilde{\delta_2'}=\delta_2'^{w},\widetilde{\delta_3'}=\prod_{i\ne m}^{n}\left(\delta_{i1}^{Hash(attr_i)\cdot\alpha}\right)^{w}=g_1^{\alpha\cdot w\sum_{i\ne m}^{n}Hash(attr_i)\cdot z_i}$$

④ 生成零知识证明：

$$\pi=NIZK\left\{\left(\sum Hash(attr_i),\alpha\right)\mid\widetilde{\delta_3'}=\prod_{i\ne m}^{n}\left(\delta_{i1}^{Hash(attr_i)\cdot\alpha}\right)^{w}\wedge\mu=\lambda^{\alpha}\right\}$$

⑤ 随机化后签名为 $\widetilde{\delta'}=\left(\widetilde{\delta_1'},\widetilde{\delta_2'},\widetilde{\delta_3'},\pi\right)$。其中，零知识证明 π 用于证明属性 $attr_i$ 的正确性，私钥的证明过程也类似，过程如下：

a. *Doe* 选择一个随机数 $R\in\mathbb{Z}_p^*$。

b. *Doe* 计算 $H=Hash\left(\prod_{i\ne m}^{n}\left(\delta_{i1}^{R}\right)^{w},\delta_{i1}^{w},\widetilde{\delta_3'},\lambda,\mu\right)$。

c. *Doe* 计算 $S=R+H\cdot\alpha\cdot Hash(attr_i)$，$\pi=S$。

d. *Doe* 计算 $r_j=Hash(attr_j)\cdot\alpha \bmod p$。

e. *Doe* 生成随机化证书 $Cert'=\left(\widetilde{\delta'},\pi,\delta_j,attr_j\right)$，其中 $j=m$，$j\le n$。

⑥ *C* 在 PBC 上部署 MASC；*RA* 在 CBC 上部署 DOSC 与 TRSC。

3.2. 捐赠请求上传

Doe 选择 C_i，上传捐赠请求并提交身份匿名证书。C_i 首先对该匿名证书的合法性与有效性进行验证，验证通过后受理其捐赠请求。

(1) 匿名证书验证。在交易过程中，*Doe* 选择的 C_i 收到 $\left(Cert',PK_{Doe}',r_j,\delta_{i1}^{w}\right)$，并进行验证：

$$e\left(\widetilde{\delta_1'},X\right)\cdot e\left(\widetilde{\delta_3'},Y\right)=\ e\left(\widetilde{\delta_2'},g_2\right)$$

$$\prod_{i\neq m}^{n}\left(\delta_{i1}{}^{S}\right)^{w}=\prod_{i\neq m}^{n}\left(\delta_{i1}{}^{R}\right)^{w}\cdot\widetilde{\delta_{3}'}^{H}$$

$$e\left(\delta_{j1},X\cdot Y^{r_j}\right)=e\left(\delta_{j2},g_2\right)$$

若上述等式均成立，则 *Doe* 提供的证书有效，随后在 CBC 完成注册。

(2) 捐赠请求上传。 *Doe* 向 C_i 平台上传捐赠请求：

$$Demand_i=\left(PK_{Doe}',C_i,M_{inf}\right)$$

其中， M_{inf} 则是所需物资的具体信息清单：

$$M_{inf}=(type,quality,number,urgency)$$

随后， C_i 为 *Doe* 生成一个受赠编号 $Recv_{id}$ ，并将 $Demand_i$ 和 $Recv_{id}$ 上传至 DOSC，DOSC 根据受助紧急程度等级对捐赠请求进行排序，若受助紧急程度等级相同，则按提交时间排序，生成捐赠请求的优先级列表 *PriorityList* ：

$$PriorityList=\left(Recv_{id},PK_{Doe}',urgency,type,quality,number,isMatched,time\right)$$

3.3. 捐赠

捐赠分为定向捐赠与非定向捐赠。定向捐赠指捐赠者可以选择符合其捐赠意向的捐赠项目进行捐赠；非定向捐赠指捐赠者无需选择具体捐赠项目，直接进行捐赠。

(1) 定向捐赠

① *Don* 访问 C_i 的网站，查看捐赠请求优先级列表，选择与其捐赠意愿相符的捐赠请求，并进行定向捐赠。 *Don* 计算物资信息 M_{inf} 的哈希值，得到 $H_1=Hash\left(M_{inf}\right)$ 。

② *Don* 生成物流信息：

$$L_{Don_i}=\left(PK_{Doe}',H_1,C_i,\sigma_{Don}\right)$$

其中 PK_{Doe}' 是受赠者的公钥，C_i 作为收件方。随后，*Don* 将 L_{Don_i} 和捐赠物资交给物流 L ，L 向 *Don* 提供物流订单号 L_{id} 。

③ *Don* 生成捐赠响应：

$$Don_i=\left(L_{id},Don_{id},PK_{Doe}',M_{inf},Demand_i,time\right)$$

其中，Don_{id} 为捐赠编号，*time* 为当前时间戳。随后，*Don* 使用 C_i 的公钥 PK_{C_i} 进行加密，生成 $Enc\left(Don_i\right)$，并将 $Enc\left(Don_i\right)$ 发送给 C_i 。

④ *Don* 选择一个随机数 $v\in\mathbb{Z}_p{}^{*}$，计算用于资产证明 VoA 的 $Asset=PK_{C_i}{}^{v}$，以及用于捐赠证明 VoD 的承诺。随后， *Don* 生成捐赠交易：

$$Tr_{Don_i}=\left(Asset,Comm,H_1,Hash\left(Don_i\right),time,\sigma_{Don}\right)$$

将 Tr_{Don_i} 上传至 TRSC 和 CBC。$Hash\left(Don_i\right)$ 是捐赠的数字证明。后续每个阶段交易状态的转换通过 TRSC 实现。

⑤ L 将捐赠物资的运输交易 $Tr_L=\left(PK_{Doe}',H_1,time,\sigma_{Don},\sigma_L\right)$ 上传至 TRSC。

(2) 非定向捐赠

① *Don* 选择 C_i 进行非定向捐赠。 *Don* 计算物资信息 M_{inf} 哈希值 $H_1=Hash\left(M_{inf}\right)$ 。

② *Don* 生成物流信息：

$$L_{Don_i}=\left(H_1,C_i,\sigma_{Don}\right)$$

其中 C_i 是收件人。随后，将 L_{Don_i} 及捐赠物资交给 L。L 为 Don 提供一个物流订单 L_{id}。

③ Don 生成捐赠响应：

$$Don_i=\left(L_{id},Don_{id},M_{inf},time\right)$$

Don 使用 C_i 的公钥 PK_{C_i} 加密 Don_i 生成 $Enc\left(Don_i\right)$，并将 $Enc\left(Don_i\right)$ 发送给 C_i。

④ Don 选择一个随机数 $v\in\mathbb{Z}_p^*$，计算用于资产证明 VoA 的 $Asset=PK_{C_i}{}^{v}$，以及捐赠证明 VoD 的承诺 $Comm=g_2{}^{v}q_2{}^{Hash(Don_i)}$。随后，$Don$ 生成捐赠交易：

$$Tr_{Don_i}=\left(Asset,Comm,H_1,Hash\left(Don_i\right),time,\sigma_{Don}\right)$$

将 Tr_{Don_i} 上传至 TRSC 和 CBC。$Hash\left(Don_i\right)$ 是捐赠的数字证明。

⑤ L 将捐赠物资的运输交易 $Tr_L=\left(H_1,time,\sigma_{Don},\sigma_L\right)$ 上传至 TRSC。

3.4. 物资分发

当 C_i 接收到捐赠物资后，C_i 判断其为定向捐赠或非定向捐赠，并据此进行物资分发。

(1) 定向分发

① C_i 在收到捐赠物资包裹后，首先检查物资以防出现以次充好的情况，随后将接收交易：

② C_i 重新计算物资信息的哈希值 $H_2=Hash\left(M_{inf}\right)$，若 $H_1=H_2$，C_i 选择一个随机数 $v'\in\mathbb{Z}_p^*$，并计算新的 $Asset'=PK_{C_i}{}^{v'}$ 和 $Comm'=g_2{}^{v'}\cdot q_2{}^{Hash(Don_i)}$，然后使用捐赠者的公钥 PK_{Don} 加密 v' 生成 $Enc\left(v'\right)$。

$$Tr_{rec}=\left(PK_{Doe}',H_1,time,\sigma_{Don},\sigma_{C_i}\right)$$

上传至 TRSC。同时，C_i 使用 SK_{C_i} 对 $Enc\left(Don_i\right)$ 进行解密。

③ C_i 生成物流信息：

$$L_{C_i}'=\left(H_2,PK_{Doe}',\sigma_{Don}\right)。$$

随后，C_i 将 L_{C_i}' 及捐赠物资移交给物流方 L'，Doe 为收件人，L' 为 C_i 提供一个物流订单号 L_{id}'。

④ C_i 生成分发事务：

$$Tx_{dis}=\left(PK_{Doe}',H_2,Asset',Comm',Enc\left(v'\right),time,\sigma_{Don},\sigma_{C_i}\right)$$

上传至 CBC。随后，C_i 将分发结果上传至 DOSC，将分发结果与优先级列表进行匹配，并更新优先级列表。对于已完成匹配的捐赠请求，将其匹配状态改为 $ture$。同时，将分发信息：

$$Tr_{dis}=\left(PK_{Doe}',H_2,time,\sigma_{Don},\sigma_{C_i}\right)$$

上传至 TRSC。在当日结束时，C_i 计算捐赠总数 $\sum Hash\left(Don_i\right)$，并将 $Int=q_2{}^{\sum Hash(Don_i)}$ 上传至 CBC。

⑤ L' 将 Tr_{dis} 的运输交易 $Tr_{L'}=\left(PK_{Doe}',H_2,time,\sigma_{Don},\sigma_{L'}\right)$ 上传至 TRSC。

(2) 非定向分发

① C_i 在收到捐赠物资包裹后，首先检查物资以防出现以次充好的情况，随后将接收交易：

$$Tr_{rec}=\left(PK_{Doe}',H_1,time,\sigma_{Don},\sigma_{C_i}\right)$$

上传至 TRSC。同时，C_i 使用 SK_{C_i} 对 $Enc\left(Don_i\right)$ 进行解密。

② C_i 重新计算物资信息的哈希值 $H_2=Hash\left(M_{inf}\right)$，若 $H_1=H_2$，则 C_i 上传物资信息：

$$DonationInfo=\left\{type,quality,number\right\}$$

上传至 MASC，并基于 DOSC 生成的 *PriorityList* 进行物资匹配，生成匹配结果：

$$ResultList = \left(Recv_{id}, type, quality, number\right)$$

其中，*type* 指物资类别，*quality* 指物资质量。随后，将生成的 *ResultList* 上传至 DOSC，并与 *PriorityList* 进行匹配，同时更新 *PriorityList*。对于已成功匹配的捐赠请求，将其匹配状态更改为 *true*。

③ 匹配成功，C_i 选择一个随机数 $v' \in \mathbb{Z}_p^*$，并计算新的 $Asset' = PK_{C_i}{}^{v'}$ 和 $Comm' = g_2{}^{v'} \cdot q_2{}^{Hash(Don_i)}$，然后使用捐赠者的公钥 PK_{Don} 加密 v' 生成 $Enc\left(v'\right)$。

④ C_i 生成物流信息：

$$L'_{C_i} = \left(H_2, PK_{Doe}', \sigma_{Don}\right)$$

随后，C_i 将 L'_{C_i} 及捐赠物资交给 L'，*Doe* 为收件人，L' 为 C_i 提供一个物流订单号 L'_{id}。

⑤ C_i 生成分发事务：

$$Tx_{dis} = \left(PK_{Doe}', H_2, Asset', Comm', time, \sigma_{Don}, \sigma_{C_i}\right)$$

上传至 CBC。同时，将分发信息：

$$Tr_{dis} = \left(PK_{Doe}', H_2, time, \sigma_{Don}, \sigma_{C_i}\right)$$

上传至 TRSC。在当日结束时，C_i 计算捐赠总数 $\sum Hash\left(Don_i\right)$，并将 $Int = q_2{}^{\sum Hash(Don_i)}$ 上传至 CBC。

⑥ L' 将 Tr_{dis} 的运输交易 $Tr_{L'} = \left(PK_{Doe}', H_2, time, \sigma_{Don}, \sigma_{L'}\right)$ 上传至 TRSC。

3.5. 物资接收

(1) *Doe* 接收到物资后，对物资进行检查，并重新计算接收到的物资信息 M_{inf} 的哈希值，得到 $H_3 = Hash\left(M_{inf}\right)$。

(2) *Doe* 生成受赠响应：

$$Gft_i = \left(PK_{Doe}', Don_{id}, M_{inf}, time\right)。$$

随后，*Doe* 使用 C_i 的公钥 PK_{C_i} 对 Gft_i 进行加密生成 $Enc\left(Gft_i\right)$，并将 $Enc\left(Gft_i\right)$ 发送给 C_i，及时向 C_i 反馈受赠情况。

(3) *Doe* 将受赠事务：

$$Tx_{Gft_i} = \left(PK_{Doe}', H_3, Hash\left(Gft_i\right), time, \sigma_{Don}, \sigma_{Doe}\right)$$

上传至 TRSC 和 CBC 上。其中，$Hash\left(Gft_i\right)$ 是物资已接收的数字凭证。

3.6. 审计与验证

在审计阶段重点关注以下三个方面：

(1) ***RA* 对一天内的捐赠交易进行验证。** *RA* 筛选上传到 CBC 中且满足条件 $H_1 = H_2$ 的分发事务 Tx_{dis} 及捐赠交易 Tr_{Don}。随后，对筛选出的交易中的 *Asset*，*Comm*，*Int* 进行聚合，进行 VoA 验证。验证过程如下：

$$IntAsset_{Don} = PK_{C_i}{}^{\sum v}, IntComm_{Don} = q_2{}^{\sum v} g_2{}^{\sum Hash(Don_i)}$$

$$IntAsset_{C_i} = PK_{C_i}{}^{\sum v'}, IntComm_{C_i} = q_2{}^{\sum v'} g_2{}^{\sum Hash(Don_i)}$$

验证：

$$\log_{IntComm_{Don}/Int}{}^{IntAsset_{Don}} = \log_{IntComm_{C_i}/Int}{}^{IntAsset_{C_i}}$$

若等式成立，则证明捐赠交易是真实且合理的。

(2) *Don* **验证个人捐赠记录。***Don* 筛选出上传到 CBC 上的分发交易中满足 $H_1 = H_2$ 且有 *Don* 签名的分发事务 Tx_{dis}。随后，获取 $Comm'$，使用私钥 SK_{Don} 解密 $Enc(v')$ 获得 v'，并计算：

$$Comm' \cdot g_2^{v-v'} = Comm$$

若等式成立，则证明个人捐赠记录是准确完整地。

(3) *RA* **追踪恶意参与者的真实身份。**若存在恶意的 *Doe*，C_i 向 *RA* 发送其公钥 PK_{Doe}'，*RA* 通过其公钥及追踪列表 $\tilde{T}$ 中的 $\{Trk_1, Trk_2, \cdots, Trk_k\}$ 追踪参数，其中，$Trk_i\ (i = 1, 2, \cdots, k)$ 是 k 个不同用户的追踪参数，计算等式：

$$e(\mu, g_2) = e(\lambda, Trk_i)$$

验证：

$$e(\mu, g_2) = e(PK_{Doe}^{\eta}, g_2) = e\left(\left(g_1^{\alpha}\right)^{\eta}, g_2\right) = e\left(g_1^{\eta}, g_2^{\alpha}\right) = e(\lambda, Trk_i)$$

若等式成立，则 *RA* 找到对应的 Trk_i，即可在追踪列表 $\tilde{T}$ 中追踪其真实身份。

4. 理论分析

(1) 正确性

① **初始化阶段。**C_i 需要对参与交易的 $Doe(Don)$ 进行证书验证，以确保交易的合法性与安全性。

隐藏属性签名验证：

$$\begin{aligned} e(\widetilde{\delta_1}', X) \cdot e(\widetilde{\delta_3}', Y) &= e(\delta_1'^{w}, g_2^{x}) \cdot e\left(\prod_{i\neq m}^{n}\left(\delta_{i1}^{Hash(attr_i)\cdot\alpha\cdot w}\right), g_2^{y}\right) \\ &= e\left(g_1^{\sum_{i\neq m}^{n} z_i \cdot w}, g_2^{x}\right) \cdot e\left(g_1^{\alpha\cdot w\sum_{i\neq m}^{n} Hash(attr_i)\cdot z_i}, g_2^{y}\right) \\ &= e(g_1, g_2)^{x\cdot w\cdot\sum_{i\neq m}^{n} z_i + y\cdot\alpha\cdot w\cdot\sum_{i\neq m}^{n} Hash(attr_i)\cdot z_i} \\ &= e(g_1, g_2)^{\left(x\cdot\sum_{i\neq m}^{n} z_i + y\cdot\alpha\cdot\sum_{i\neq m}^{n} Hash(attr_i)\cdot z_i\right)w} = e(\widetilde{\delta_2}', g_2) \end{aligned}$$

零知识证明验证：

$$\begin{aligned} \prod_{i\neq m}^{n}\left(\delta_{i1}^{R}\right)^{w} \cdot \widetilde{\delta_3}'^{H} &= \prod_{i\neq m}^{n}\left(g_1^{z_i}\right)^{R\cdot w} \cdot \prod_{i\neq m}^{n} g_1^{H\cdot\alpha\cdot w\cdot\sum_{i\neq m}^{n} Hash(attr_i)\cdot z_i} \\ &= g_1^{R\cdot w\cdot\sum_{i\neq m}^{n} z_i} \cdot g_1^{H\cdot\alpha\cdot w\cdot\sum_{i\neq m}^{n} Hash(attr_i)\cdot z_i} \\ &= g_1^{R\cdot w\cdot\sum_{i\neq m}^{n} z_i + H\cdot\alpha\cdot w\cdot\sum_{i\neq m}^{n} Hash(attr_i)\cdot z_i} = \prod_{i\neq m}^{n}\left(\delta_{i1}^{S}\right)^{w} \end{aligned}$$

公开属性签名验证：

$$\begin{aligned} e(\delta_{j1}, X \cdot Y^{r_j}) &= e\left(g_1^{z_j}, g_2^{x} \cdot g_2^{y\cdot Hash(attr_j)\cdot\alpha \bmod p}\right) \\ &= e\left(g_1^{z_j}, g_2^{x+y\cdot(Hash(attr_j)\cdot\alpha)\bmod p}\right) \\ &= e(g_1, g_2)^{z_j(x+y\cdot(Hash(attr_j)\cdot\alpha)\bmod p)} = e(\delta_{j2}, g_2) \end{aligned}$$

② **审计阶段。** *Don* 完成个人捐赠记录验证， *RA* 验证一天时间内捐赠交易，两部分验证工作。

捐赠记录验证： *Don* 执行捐赠验证(*VoD*)，以评估个人捐赠记录的准确性与完整性。

$$Comm' \cdot g_2^{v-v'} = g_2^{v'} \cdot q_2^{Hash(Don_i)} \cdot g_2^{v-v'} = g_2^{v} \cdot q_2^{Hash(Don_i)} = Comm$$

捐赠交易验证： *RA* 执行资产验证(*VoA*)，以审查捐赠全过程的合规性。

$$\begin{aligned} \text{左边} &= \log_{IntComm_{Don}/Int}^{IntAsset_{Don}} \qquad \text{右边} = \log_{IntComm_{C_i}/Int}^{IntAsset_{C_i}} \\ &= \log_{IntComm_{Don}/q_2^{\sum Hash(Don_i)}}^{IntAsset_{Don}} \qquad = \log_{IntComm_{C_i}/q_2^{\sum Hash(Don_i)}}^{IntAsset_{C_i}} \\ &= \log_{g_2^{\sum v}}^{PK_{C_i}^{\sum v}} = \log_{g_2^{\sum v}}^{g_2^{(-SK_{C_i})\sum v}} \qquad = \log_{g_2^{\sum v'}}^{PK_{C_i}^{\sum v'}} = \log_{g_2^{\sum v'}}^{g_2^{(-SK_{C_i})\sum v'}} \\ &= -SK_{C_i} \qquad = -SK_{C_i} \end{aligned}$$

左边 = 右边，等式成立，证毕。

(2) 匿名性

本方案中的匿名性是指， $Don(Doe)$ 使用个人私钥对初始证书中需要隐藏的属性的签名进行随机化处理，同时随机化初始公钥，以生成不同的匿名证书和公钥。

定理 3-1：在 DLIN 假设[13]下，随机化证书能够满足匿名性。

证明：假设存在攻击者 A，对可随机化证书的匿名性具有一定的攻击优势。下面将构造一个算法 D 来解决 DLIN 问题，过程如下。

初始化：给定群参数 $x, y, z \in G_1$ $a, b, c \in \mathbb{Z}_p^*$ 及两组元素 $\left(x^a, y^b, z^{a+b}\right)$，$\left(x^a, y^b, z^c\right)$。随后，算法 D 生成公共参数 pp。最后，将算法 D 生成的公共参数 pp 发送给攻击者 A。

查询阶段：攻击者 A 通过随机预言机进行查询，与算法 D 进行交互。在密钥生成阶段，攻击者 A 向算法 D 请求获取公私钥对。算法 D 选择一个随机数 $\alpha \in \mathbb{Z}_p^*$，计算 z^α，并生成 $\left(z^\alpha, \alpha\right)$，其中 z^α 作为公钥 PK，α 作为私钥 SK。随后，算法 D 将生成的公钥发送给攻击者 A。在追踪阶段，算法 D 根据攻击者 A 的查询请求，返回公钥 PK 并模拟系统的追踪功能。

请求阶段：攻击者 A 向算法 D 请求证书。此时，攻击者 A 需要选择一个挑战比特 $b \leftarrow (0,1)$，算法 D 将基于该比特生成不同的证书。在签发阶段，攻击者 A 根据先前选择的挑战比特 b 向算法 D 发起请求，生成与 b 相关的证书。当 $b=1$ 时，算法 D 生成一个有效证书 $Cert = \left(z, z^{a+b}\right)$；当 $b=0$ 时，算法 D 生成一个随机证书 $Cert = \left(z, z^c\right)$。在随机化阶段，算法 D 随机选取 $r \in \mathbb{Z}_p^*$，生成随机化证书 $Cert^r$ 并将其返回给攻击者 A。

猜测阶段：攻击者 A 输出 $b' \leftarrow (0,1)$ 作为对证书 $cert^r$ 的猜测结果。对于攻击者 A 而言，$Cert = \left(z, z^{a+b}\right)$ 和 $Cert = \left(z, z^c\right)$ 均为有效证书，其中一个是原始证书，另一个是随机化后的证书。若攻击者 A 能够以超过 1/2 的不可忽略概率成功区分这两种证书，则表明算法 D 能够区分有效证书 $Cert = \left(z, z^{a+b}\right)$ 与随机证书 $Cert = \left(z, z^c\right)$，进而解决 DLIN 问题。根据 DLIN 假设，在一般双线性群模型中，对于一个最多可进行 l 次查询的群预言机，任何攻击者成功解决 DLIN 问题的概率均不会超过 $8(l+9)^2/p$ [13]，其中 l 是攻击者 A 进行群运算查询的次数， p 是群的素数阶。

分析表明，即使在面对能够访问多个预言机的潜在攻击者时，短期内也难以成功区分有效证书与随机化证书，证明可随机化证书能够有效实现匿名安全性。

(3) 安全性

本节将围绕本方案的机密性、可追溯性与可审计性以及公平性展开深入探讨，以全面评估本方案的可靠性与有效性。

① **机密性**

本方案的机密性旨在确保 *C* 在跨组织物资共享过程中，其内部物资详细信息的保密性。因此，本文采用 PBC 与 CBC 协同运作的架构。各 *C* 通过建立独立的 PBC，存储并管理其组织内部的物资信息。仅在特定物资需要进行跨组织共享时，直接进行捐赠。有效避免了组织内部物资信息直接暴露于联盟链，降低了因信息泄露而引发针对性攻击的安全风险。

此外，为保障捐赠过程中物资信息的机密性，本方案采用哈希函数对物资信息进行加密处理。在身份隐私保护方面，设计可随机化证书，每次捐赠交易参与者可根据需求随机化属性签名并生成零知识证明隐藏特定身份属性，同时随机化公钥，确保交易过程中身份信息与捐赠交易行为不可关联，有效防止交易记录被追溯或被用于关联分析，进一步增强了隐私保护能力。

② **可追踪性和可审计性**

本方案的可追溯性涵盖以下两方面：a. *RA* 具备追溯恶意参与者真实身份的能力；b. 确保捐赠交易过程中每个环节的交易状态均可被查询与追踪。可审计性则体现在：a. *RA* 能够对一段时间内的捐赠交易进行审计；b. *Don* 可验证其个人捐赠信息是否被完整、准确地记录。

考虑潜在对手可能采用的三种攻击手段。攻击 1，部分 *Don* 可能故意虚报所捐赠资产，甚至以次充好进行捐赠；攻击 2，恶意 *Doe* 可能谎称未收到已送达的捐赠物资；攻击 3，*C* 可能存在虚报捐赠交易行为，声称已完成捐赠，却私下截留物资或未如实记录所接收物资的全部信息。

针对攻击 1，*C* 在接收到捐赠物资后，首先对物资质量进行检查，防止以次充好的恶意行为，并将接收交易 Tr_{rec} 上传至 CBC。同时，*C* 重新计算接收物资的哈希值 H_2，并判断 H_2 是否与捐赠时提供的哈希值 H_1 一致。若两者不一致，则表明 *Don* 可能存在虚报捐赠资产的行为。此外，若 *C* 与 *Don* 涉嫌串通，*RA* 也可通过对比分发事务 Tx_{dis} 与接收事务 Tx_{Gft_i} 中哈希值的一致性，准确判断捐赠方是否虚报捐赠资产，进而有效筛选并识别潜在的恶意捐赠者。

针对攻击 2，*Doe* 在收到物资后需及时向 C_i 慈善组织反馈确认接收，并将本次捐赠交易的相关记录上传至 TRSC 与 CBC。在此过程中，TRSC 记录上传的每一笔捐赠交易的状态。*RA* 通过查询 TRSC，可验证并确认最终捐赠交易的真实性与有效性，有效防止 *Doe* 以未收到捐赠物资为由实施恶意欺诈。

针对攻击 3，*RA* 对一段时间内完成的捐赠交易执行严格的审计。在此过程中，*RA* 通过 VoA 验证 $\log_{IntComm_{Don}/Int}{}^{IntAsset_{Don}} = \log_{IntComm_{C_i}/Int}{}^{IntAsset_{C_i}}$，验证 *C* 在该时间段内执行的捐赠资产是否与接收的捐赠资产完全一致。同时，为防止篡改，每笔捐赠的交易状态均通过 TRSC 记录，使 *RA* 能够进一步确认最终捐赠交易的真实性与有效性。此外，*Don* 也可通过 VoD 验证 $Comm' \cdot g_2{}^{v-v'} = Comm$，验证其个人捐赠信息是否已被完整、准确地记录。

最后，针对任何恶意参与者，*RA* 可通过计算 $e(\mu, g_2) = e(\lambda, Trk_i)$ 追踪并确认其真实身份。

③ **公平性**

Doe 在发布捐赠请求前，*RA* 将根据 *Doe* 的具体属性确定其受助紧急程度等级，而非仅依据捐赠请求而忽略受助紧急程度。在后续捐赠过程中，捐赠智能合约 DOSC 根据捐赠请求的受助紧急程度等级生成捐赠请求优先级列表 *PriorityList*，并按照该列表逐一进行物资匹配。然而，部分恶意慈善组织可能通过收受贿赂以改变捐赠请求优先级列表，并按其意愿进行分配。但是，由于受助紧急程度等级由监管机构生成，一旦捐赠请求提交，DOSC 将基于受助紧急程度等级对捐赠请求进行排序，并将排序结果上传至 CBC，供 *RA* 实时监测与评估，消除了捐赠请求优先级被随意篡改的可能性。

同时，MASC 能够自动完成捐赠请求与物资的匹配，其执行过程不受人为因素干扰。*C* 根据结果列表 *Resultlist* 分配物资，并接受 *RA* 与 *Don* 的双重监督，进一步确保了捐赠物资的公平且有效分配。

④ **女巫攻击与重识别攻击**

本方案通过引入可随机化证书，有效抵御女巫攻击[14]。参与者须经由监管机构完成实名注册以获取初始证书($Cert$)，这显著增加了攻击者创建多重身份的成本；随机化证书($Cert'$)由参与者使用其个人私钥自主生成，即使监管机构遭入侵，也无法伪造或批量生成有效证书；通过 Trk ，监管机构能够快速追溯所有女巫节点背后的真实身份，这极大地增加了实施女巫攻击的风险。

同时，可随机化证书基于随机化签名和零知识证明，为抵抗重识别攻击[15]提供了密码学层面的保证。用户可以自主生成多个不可关联的匿名证书，确保其身份在不同交易中不被关联。在证书有效性验证过程中，用户为其私钥及隐藏属性信息生成零知识证明，在不泄露任何信息的前提下完成验证。DLIN假设证明了本方案的匿名性，攻击者无法以不可忽略的优势区分或关联用户身份。此外，RA 仅在检测到异常行为时通过 Trk 追溯用户的真实身份，保障隐私的同时，消除了重识别攻击的可能性。

5. 性能分析

5.1. 功能比较

表 1 展示了本方案与现有方案在功能上的对比分析。文献[16]-[19]中，多次交易使用同一匿名身份提高了身份与交易行为被关联的风险，导致隐私泄露，使参与者受到针对性攻击。其次，文献[9] [16] [18] [19]存在明显的功能局限，均不能支持跨组织资源共享。同时，这些方案未考虑内部物资信息隐私保护，使得同样面临隐私泄露而导致的针对性安全威胁。此外，在物资匹配过程中，现有文献[9] [16]-[19]往往忽略捐赠请求的受助紧急程度，仅根据捐赠请求进行匹配，可能导致物资分配延误，对捐赠的公平性和有效性产生负面影响。相较之下，本方案采用可随机化证书，确保每次交易使用唯一的匿名身份，保证交易的匿名性与不可关联性。同时，可追踪恶意参与者的真实身份。通过 PBC 与 CBC 协同，在实现跨组织共享物资的同时，能够有效保护内部物资信息的隐私，并对每笔捐赠交易进行有效监督。此外，为设定受助紧急程度等级，DOSC 依据该等级自动生成捐赠请求优先级列表，MASC 依据优先级列表依次进行匹配，兼顾了捐赠请求的紧急程度的同时杜绝了人为因素的干扰。

Table 1. Functional comparative analysis
表 1. 功能对比分析

	文献[16]	文献[17]	文献[18]	文献[19]	文献[9]	本方案
匿名性与不可链接性	×	×	×	×	√	√
物资信息隐私	×	√	×	√	×	√
捐赠请求紧急性	×	×	×	×	×	√
可追溯性与可审计性	√	√	√	√	√	√
跨组织共享	×	√	×	×	×	√

5.2. 计算开销

在计算开销方面，将本方案与 Fabric 区块链中的 Idemix 机制[11]进行了对比分析，结果如表 2。其中 T_P, T_H, T_E 分别表示幂运算、哈希运算及双线性对运算的时间。 n 表示属性的数量， m 表示公开属性的数量，且满足 $m < n$ 。

(1) 实验仿真

为进一步验证本方案的性能，在运行 64 位 Windows 10 操作系统、Intel Core i5-8250U CPU (@ 1.60 GHz~1.80 GHz)和 8 GB RAM 的计算机上进行实验。开发工具为 IntelliJ IDEA，加密算法采用 JPBC 库提供的 D224 曲线，该曲线可提供 1344 位安全级别。数据均通过 100 次平均计算获得，时间单位为毫秒。

此外，使用 Solidity 语言在 Remix 平台上编译智能合约，并将合约部署至基于 Geth 客户端构建的联盟链与私有链本地测试环境中进行测试。

Table 2. Computational cost at each stage
表 2. 各阶段计算开销

	文献[20]	本方案
密钥生成	$(n+11)T_P+2T_H$	$5T_P$
初始证书生成	$(n+2)T_P$	$n(4T_P+T_H)$
随机化公钥	NULL	$2T_P$
随机化匿名证书	$(n-m+14)T_P+2T_H$	$(n-m+2)T_P+T_H$
验证匿名证书	$(n+10)T_P+2T_H+2T_E$	$(m+6)T_P+(3+2m)T_E$

① **Gas 消耗**

为评估合约部署与关键函数调用所产生的 *Gas* 消耗，分别进行了 1 至 5 次重复实验，并记录每次交易的 *GasUsed* 值，实验结果如图 3(a)所示。显著的开销集中出现在合约部署阶段。这主要是因为 DOSC 和 MASC 需要分别上传捐赠请求与物资信息，而 TRSC 则需记录捐赠物资在交易全流程各阶段的状态变化，均涉及大量数据的链上存储。相比之下，合约部署完成后，后续调用操作所需的 *Gas* 消耗则显著降低。此外，在上传捐赠请求阶段，需上传包含请求参数与物资详细信息在内的完整信息；在匹配阶段，*C* 需获取捐赠请求优先级列表副本并上传至 MASC 进行匹配，二者均会产生较高的 *Gas* 消耗。因此，在合约部署之后，系统的 *Gas* 开销主要集中于上述两个阶段。

② **初始证书生成**

本方案中，可随机化证书的生成与验证过程均在链下执行，减轻链上操作的计算压力。在初始证书生成阶段，对生成不同属性数量及属性数量动态变化的初始证书所需时间开销进行了测试，结果如图 3(b)所示。在属性数量固定(Attr = 5、10、15)的情况下，初始证书生成时间随属性数量增加而增加。文献[20]在固定属性数量下的时间开销较低。然而，当属性数量发生动态变化(例如每次增加 5 个属性，即 Attr +5)时，本方案仅需验证变更属性的合法性并签名，无需对所有属性进行验证，提生了灵活性也降低了时间开销。相比之下，在属性数量固定时，文献[20]的时间开销较低，这是因为 *CA* 需要对所有属性进行验证，然后统一签名。然而，当属性发生变动时，文献[20]中的 *CA* 需要对所有属性重新进行验证和签名，这不仅牺牲了灵活性，也增加了时间成本。因此，在属性数量动态变化的场景下，本方案展现出更高的效率与灵活性。

① **随机化和验证**

在进行捐赠之前，$Don(Doe)$ 会根据其个人意愿或具体的捐赠要求，公开或隐藏证书中的特定属性。属性的隐藏是通过对该属性的签名进行随机化，并生成相应的零知识证明，同时对原始公钥进行随机化来实现的，为每笔交易生成唯一的匿名证书和公钥。在交易时，C_i 需要验证参与者所提交的匿名证书的有效性。以包含 10 个属性的证书为例，分别探讨了不同隐藏属性数量与公开属性数量对时间开销的影响，结果如图 3(c)所示。

本方案在证书和公钥的随机化阶段以及证书的验证阶段均呈现出较低的时间开销。在证书随机化过程中，采用了先聚合签名再进行随机化；在证书验证过程中，验证隐藏属性聚合签名和零知识证明，以及公开属性签名，验证时间开销主要取决于公开属性的数量，且已验证的公开属性无需重复计算，实现高效验证。文献[20]中，每生成一个匿名证书，都必须由 *CA* 执行一次验证和重新签名，这意味着用户需要与 *CA* 进行多次交互才能生成不同的匿名证书，这无疑增加了操作的复杂性。此外，*CA* 会对证书中的所有属性进行统一签名，这虽然保证了信息的完整性，却牺牲了灵活性。频繁的交互及签名机制共同导

致了时间开销的增加。

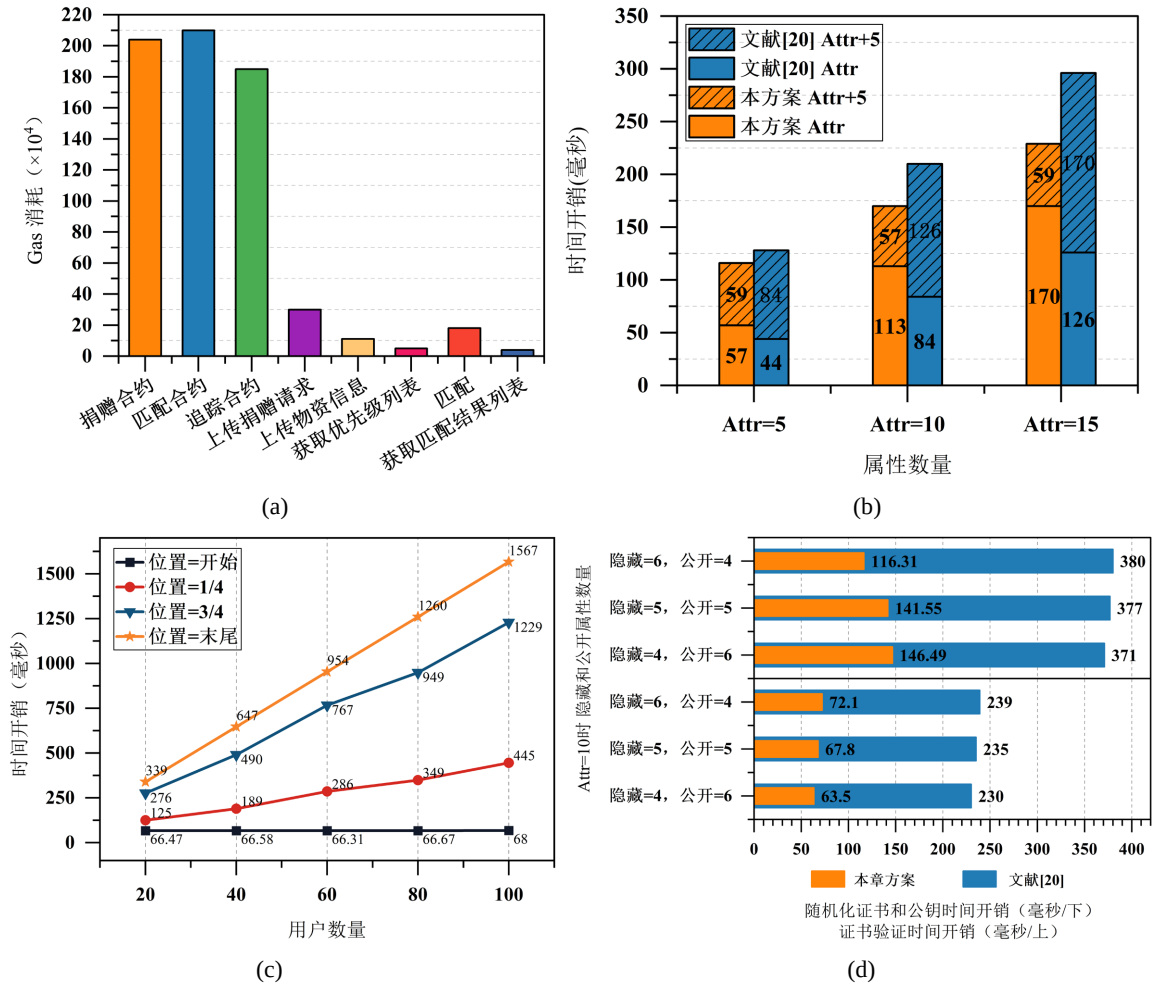

Figure 3. Experimental simulation. (a) Gas consumption; (b) Initial certification generation; (c) Randomization and Verification; (d) Identity tracing

图 3. 实验仿真。(a) Gas 消耗；(b) 初始化证书生成；(c) 随机化及验证；(d) 身份追踪

② **可追踪性**

通过随机化后的匿名证书与公钥追踪恶意参与者是本方案具备而 Idemix [11]所不具备的一项独特特性。追踪恶意参与者所需的时间开销如图 3(d)所示。可以看出，追踪所需时间随用户总数增加而呈线性增长。这是因为时间开销与参与者数量及恶意参与者在追踪序列中的具体位置密切相关。在实验设计中，将恶意参与者分别置于追踪列表的起始处、1/4 处、3/4 处及末尾处，模拟测试在不同位置的追踪效率。可以看出在 100 名用户的场景下，当恶意参与者位于追踪列表末尾时，追踪过程仅需 1.5 秒，该耗时处于可接受范围内。

6. 结论

本文提出了基于混合区块链架构的可验证数据隐私保护方案。该方案通过可随机化证书及零知识证明实现身份隐私保护、身份与交易行为不可关联，并充分考虑捐赠请求及其受助紧急程度。智能合约自动生成捐赠请求的优先级列表，完成需求与物资的匹配，并全程记录捐赠交易状态。混合区块链架构设

计兼顾了跨组织资源共享与保护慈善组织内部物资信息隐私。此外，该方案支持定向与非定向的多元化捐赠模式，同时 Pedersen 承诺支持捐赠者与监管机构对捐赠资产及捐赠交易进行验证。理论分析与实验评估表明，该方案在隐私保护与计算开销方面表现出色，综合性能突出。

参考文献

[1] 推动中国互联网慈善事业高质量发展 2022 年中国互联网慈善峰会专家观点摘要[J]. 中国民政, 2022(10): 50-51.

[2] Eleo (2025) Eleo Online Donor Management Software. https://eleoonline.com/

[3] DonorSnap (2025) DonorSnap Donor Management Software. https://donorsnap.com/

[4] easyTithe (2025) easyTithe Online Giving Platform. https://www.easytithe.com/

[5] Sung, J., Bock, G.W. and Kim, H.M. (2023) Effect of Blockchain-Based Donation System on Trustworthiness of Npos. *Information & Management*, **60**, Article 103812. https://doi.org/10.1016/j.im.2023.103812

[6] Hasan, H.R. and Salah, K. (2018) Blockchain-based Solution for Proof of Delivery of Physical Assets. In: *Lecture Notes in Computer Science*, Springer, 139-152. https://doi.org/10.1007/978-3-319-94478-4_10

[7] Li, T., Hu, D., Li, M., Li, Y. and Zheng, S. (2022) A Blockchain-Based Material Donation Platform. 2022 *International Conference on Blockchain Technology and Information Security* (*ICBCTIS*), Huaihua, 15-17 July 2022, 246-254. https://doi.org/10.1109/icbctis55569.2022.00061

[8] Badarudin, P.H.A.P., Wan, A.T. and Phon-Amnuaisuk, S. (2020) A Blockchain-Based Assistance Digital Model for First Responders and Emergency Volunteers in Disaster Response and Recovery. 2020 8*th International Conference on Information and Communication Technology* (*ICoICT*), Yogyakarta, 24-26 June 2020, 1-5. https://doi.org/10.1109/icoict49345.2020.9166389

[9] Zhou, Y., Lei, H. and Bao, Z. (2024) Eisdspa: An Efficient and Secure Blockchain-Based Donation Scheme with Privacy Protection and Auditability. *IEEE Open Journal of the Communications Society*, **5**, 7498-7510. https://doi.org/10.1109/ojcoms.2024.3504403

[10] Zhang, D., Wang, S., Zhang, Y., Zhang, Q. and Zhang, Y. (2022) A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain. *Security and Communication Networks*, **2022**, 1-15. https://doi.org/10.1155/2022/2759787

[11] Zhuji, X., Wang, J., Ding, W. and Wu, W. (2023) Blockchain-Based System for Vaccine Traceability. 2023 *IEEE International Conference on Data Mining Workshops* (*ICDMW*), Shanghai, 1-4 December 2023, 706-715. https://doi.org/10.1109/icdmw60847.2023.00097

[12] Li, C., Liu, J., Qian, G., Wang, Z. and Han, J. (2022) Double Chain System for Online and Offline Medical Data Sharing Viaprivate and Consortium Blockchain: A System Design Study. *Frontiers in Public Health*, **10**, Article 1012202. https://doi.org/10.3389/fpubh.2022.1012202

[13] Boneh, D., Boyen, X. and Shacham, H. (2004) Short Group Signatures. In: *Lecture Notes in Computer Science*, Springer, 41-55. https://doi.org/10.1007/978-3-540-28628-8_3

[14] Douceur, J.R. (2002) The Sybil Attack. In: *Lecture Notes in Computer Science*, Springer, 251-260. https://doi.org/10.1007/3-540-45748-8_24

[15] Henriksen-Bulmer, J. and Jeary, S. (2016) Re-Identification Attacks—A Systematic Literature Review. *International Journal of Information Management*, **36**, 1184-1192. https://doi.org/10.1016/j.ijinfomgt.2016.08.002

[16] Li, Z., Zhang, W., Qin, H. and Zhou, H. (2021) Charitable Donation System Based on Blockchain Technology. *Proceedings of the* 2021 1*st International Conference on Control and Intelligent Robotics*, Guangzhou, 18-20 June 2021, 92-96. https://doi.org/10.1145/3473714.3473730

[17] Demir, M., Turetken, O., Ferworn, A., *et al*. (2023) A Blockchain-Based System for Aid Delivery: Concept Development, Data Modeling, and Validation. *Journal of Database Management*, **34**, 1-35. https://doi.org/10.4018/jdm.321757

[18] Datta, S. and Namasudra, S. (2024) Blockchain-Based Secure and Scalable Supply Chain Management System to Prevent Drug Counterfeiting. *Cluster Computing*, **27**, 9243-9260. https://doi.org/10.1007/s10586-024-04417-3

[19] Duan, J., Wang, L., Wang, W. and Gu, L. (2023) TRCT: A Traceable Anonymous Transaction Protocol for Blockchain. *IEEE Transactions on Information Forensics and Security*, **18**, 4391-4405. https://doi.org/10.1109/tifs.2023.3296286

[20] Camenisch, J. and Van Herreweghen, E. (2002) Design and Implementation of the Idemix Anonymous Credential System. *Proceedings of the* 9*th ACM conference on Computer and Communications Security*, Washington, DC, 18-22 November 2002, 21-30. https://doi.org/10.1145/586110.586114