面向去中心化环境的数据所有权安全转移协议

禹 勇[1)] 姚宇超[1)] 史隽彬[2)] 阳昊辰[1)]

[1)](陕西师范大学计算机科学学院 西安 710119)

[2)](西安邮电大学网络空间安全学院 西安 710121)

摘 要 在去中心化市场中,大量数据资产通常需要长时间锁定在智能合约中,直至交易完成。尽管这种锁定机制对交易安全非常重要,却严重限制了数据资产的流动性与灵活性,导致市场参与者交易效率降低、机会成本增加,阻碍了去中心化应用的推广与规模化发展。为解决上述问题,本文提出了一种面向去中心化环境的数据所有权安全转移协议。本协议在不额外增加区块链网络计算或存储负担的前提下,实现了锁定数据资产所有权的安全转移。首先,构建了包含数据出质人(最初拥有并质押数据资产)、第三方受让人(欲获得数据资产所有权)和数据质权人(质押期间控制数据资产)的系统模型,明确了各方角色、交互方式和安全需求。其次,采用零知识证明技术对链下参与者进行身份认证,通过不暴露敏感身份信息和数据资产细节的方式,确保身份与交易的合法性,有效保护参与者隐私和数据资产机密性。此外,为安全、公平地实现数据资产控制权转移,设计了链下两方秘密交换协议,用于安全交换智能合约升级密钥,以完成数据所有权的变更,显著缓解了区块链网络的拥堵问题,降低了交易成本与延迟。同时,引入可升级智能合约机制,实现对锁定数据所有权的安全修改和上链,且不会增加额外开销。最后,在最常见的数据资产抵押交易场景中,对提出的协议与现有协议进行了比较。实验结果表明,与现有协议相比,本协议在提高资产流动性、增强交易效率和保护参与者隐私方面均具有明显优势,具体表现为本协议响应延迟低,可有效提升数据资产交易频率,从而显著提升了去中心化市场的数据资产流动性。

关键词 数据所有权;公平秘密交换;智能合约;零知识证明

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2025.01356

Secure Data Ownership Transfer Protocol for Decentralized Environments

YU Yong[1)] YAO Yu-Chao[1)] SHI Jun-Bin[2)] YANG Hao-Chen[1)]

[1)](School of Computer Science, Shaanxi Normal University, Xi'an 710119)

[2)](School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121)

Abstract In decentralized markets, the liquidity of data assets presents a critical challenge due to the inherent characteristics of blockchain systems. Specifically, significant amounts of data assets are typically required to remain locked within smart contracts until transactions reach completion. This obligatory locking mechanism, while vital for security, severely restricts the liquidity and flexibility of data assets. Consequently, data owners and other market participants face reduced efficiency and increased opportunity costs, hindering the broader adoption and scalability of blockchain-based decentralized applications. To overcome this prevalent limitation, this paper introduces a novel hybrid protocol for the secure transfer of data ownership, operating through a

收稿日期:2024-12-01;在线发布日期:2025-03-31。本文得到国家密码科学基金(2025NCSF02025)、国家自然科学基金联合基金重点项目(U24B20149, U23A20302)、国家自然科学基金面上项目(62272385)、国家自然科学基金国际合作交流项目(62311540156)、陕西省重点研发计划重点产业创新链项目(2024GX-ZDCYL-01-09)、陕西省杰出青年科学基金(2022JC-47)资助。**禹 勇**(通信作者),博士,教授,主要研究领域为公钥密码理论及应用、区块链与密码货币以及云计算安全。E-mail: yuyong@snnu.edu.cn。**姚宇超**,博士研究生,主要研究领域为区块链与密码货币。**史隽彬**,博士,讲师,主要研究领域为可搜索加密与云计算安全。**阳昊辰**,博士研究生,主要研究领域为区块链与去中心化身份。

combination of on-chain and off-chain methodologies. The principal innovation is facilitating the safe transfer of ownership rights over locked data assets without placing additional computational or storage demands on the underlying blockchain network. By integrating off-chain operations, our approach mitigates the scalability concerns commonly associated with purely on-chain solutions. Firstly, we define a comprehensive system model consisting of three essential stakeholders: the data pawner, who initially owns and pledges the data asset; the third-party transferee, who aims to acquire ownership rights to the locked data; and the data pledgee, who holds custody of the data asset during the pledge period. This structured model lays the groundwork for identifying precise interaction patterns, role definitions, and security requirements essential for robust implementation. Subsequently, the proposed protocol leverages zero-knowledge proof techniques to authenticate the identities of off-chain participants. Zero-knowledge proofs enable verification of identities and transaction legitimacy without exposing sensitive identity-related information or details of the underlying data assets. Thus, participant privacy and asset confidentiality are robustly preserved throughout the transaction lifecycle. To realize the secure and fair transfer of control, we incorporate a two-party fair secret exchange protocol executed entirely off-chain. This exchange allows involved parties to securely trade contract upgrade keys, enabling the modification of ownership rights associated with the locked data. Such off-chain execution significantly alleviates blockchain congestion and reduces transaction-related costs and latency. Moreover, utilizing an upgradable smart contract infrastructure further ensures that modifications to ownership rights are securely and reliably reflected on-chain without unnecessary complexity. Finally, we rigorously evaluate the proposed hybrid protocol through comparative analyses against existing methodologies in prevalent real-world scenarios of data asset collateral loans. Through comprehensive assessment, it is demonstrated that our proposed protocol consistently achieves superior outcomes, particularly in terms of improving liquidity, enhancing transaction efficiency, and ensuring participant privacy. Specifically, empirical results indicate that the adoption of our protocol substantially reduces the latency associated with ownership transfers, facilitates increased frequency of data asset transactions, and significantly improves overall asset liquidity within decentralized markets. Overall, the hybrid on-chain and off-chain data ownership secure transfer protocol presented herein effectively addresses the critical liquidity issue inherent in existing blockchain-based decentralized market designs. Through a strategic combination of zero-knowledge proofs, off-chain secret exchanges, and upgradable smart contract mechanisms, our solution delivers notable improvements in liquidity and usability without compromising security, privacy, or scalability, thus holding significant potential to advance the practical utility and widespread adoption of blockchain-based data markets.

Keywords　data ownership; fair secret exchange; smart contract; zero knowledge proof

1　引　言

区块链通过智能合约实现了去中心环境下的自动化交易，实现了点对点的数据价值转移。在去中心化市场中，数据的抵押交易业务是其核心组成部分[1]，但现有的交易需要将数据资产锁定在智能合约中，这虽确保了交易的安全性，却大幅限制了资产的流动性，降低了市场的活力，制约了数据的再利用效率。具体来说，在去中心化数据抵押交易中，一方需要先将等价的数据资产转移到智能合约中锁定抵押，另一方再根据抵押的数据价值转出相应的资金，最后等待前者偿还资金并取回抵押完成交易。在该过程中，为了保证交易

的原子性，规避违约风险，合约会锁定双方的数据资产直至交易完成。但是，这导致了数据资产在交易完成前无法流通，严重限制了数据抵押交易业务的应用和推广。目前存在三个问题需要解决：

（1）如何实现合约中业务逻辑的修改，以支持数据所有权的转移。

（2）如何保证权限的安全性[2]，防止合约被非法修改或盗取。

（3）如何在不增加计算开销的情况下，实现对现有协议功能上的扩展。

为解决上述问题，本文在Black等[3]提出的方案基础上，考虑了去中心化市场中最常见的现实场景：当抵押资产价值迅速上涨时，数据所有者会希望不提前偿还资金的前提下将抵押的数据资产变现，以获取额外的资金；而投资者由于抵押资产价值大幅高于债务余额，会主动寻求投资机会并继承资金偿还责任。因此，本文研究如何在保证交易安全性的前提下，对现有去中心化场景中的数据抵押交易业务进行功能扩展，并以上述场景为基础实现安全的数据所有权转移，以解决链上数据资产锁定的问题，提高数据的流动性。本文的主要工作包括：

（1）定义了数据所有权安全转移的系统模型。与现有的数据抵押交易协议不同，模型通过引入第三方受让人接收数据资产，支持抵押数据的所有权转移，从而有效解决数据资产的流动性问题。

（2）通过引入可升级的智能合约，实现对协议中各参与方权限的动态管理。该设计使协议参与方拥有对各自身份信息进行修改的密钥，从而实现锁定资产所有权的转移，解决资产流动性低的问题。

（3）在使用零知识证明技术保护隐私的前提下验证链下参与者的身份，并通过两方公平秘密交换实现链上合约升级密钥交换，最终利用可升级智能合约修改锁定数据的所有权。

（4）将提出的协议与已有的数据资产抵押交易协议进行比较，证明了其在计算成本可控的同时实现了功能扩展。

2 相关工作

去中心化数据抵押交易协议的构造依赖基于哈希时间锁定的跨链原子交换技术[4-7]，安全高效的跨链原子交换协议[8]可以极大提升数据抵押交易协议的鲁棒性。Herlihy等[4]在BitcoinTalk论坛上提出了原子交换，它是指构成一笔完整跨链交易的子交易仅可处于未执行或已完成状态，不存在任何中间状态[9]。该方案基于哈希时间锁实现，经过改进后成为一种主要的跨链模式。但由于不同链的交易确认速度和规则存在差异，可能导致交易失败或被攻击，因此需要进一步探索如何构建安全的交换。Dalton等[10]提出了一种去中心化的公平秘密交换协议，在无需可信第三方的前提下实现信息交换，拓展了新的研究思路。刘等[11]提出了改进哈希时间锁的跨链资产交互协议NCASP，通过中间账户进行资产托管和转移的方式改进哈希时间锁，使得在原有跨链交易的速率保持不变的同时，提高了交易的安全性。Zakhary等[12]提出了AC3WN，这是一种去中心化的公证人网络，通过侧链上的智能合约对跨链资产交换的交易状态进行控制，实现了去中心化原子跨链交换，确保了原子交换的原子性和最终承诺性。而Lys等[13]则在前者的基础上移除AC3WN中使用的公证人网络侧链，改为使用基于哈希时间锁定机制的原子交换技术。Tian等[14]提出了一种去中心化的资产交易协议，实现了不同类型资产之间的交换，并基于智能合约支持了多对用户并行处理跨链资产交换，提高了跨链资产交换的性能。Herlihy等[7]则提出了一种基于哈希时间锁的三方交易方案，该方案可以在没有可信中介的前提下完成三方货币互换，Malavolta等[15]则在前者的基础上进一步扩展了交易方数量。张等[16]提出了一种多方跨链协议，基于哈希时间锁定实现了多方多链资产交换结算。葛等[17]则进一步提出了多人链下支付方案，将交易清算从链上的全网矿工认证转移到链下通道内的支付双方认证，从而实现了支付近乎即时确认，极大地提升了区块链的可扩展性。

目前对去中心化数据抵押交易协议的研究大都集中在智能合约和哈希时间锁定机制上，其实现思路是在无需可信公证人的前提下，通过哈希时间锁定机制构造的交易合约完成交易，使其在满足安全性的前提下实现尽可能多的金融属性[4,7,18-19]。因此，如何选择合适的密码学工具，保护交易双方在博弈过程中的利益不受损害，也成为当前对去中心化数据抵押交易协议研究的一个热点[20-22]。Jain等[23]提出了多种拍卖模型，为数据抵押交易协议的清算过程提供了多种选择。Black等[3]则提出了一种基于哈希时间锁的交易协议，该协议支持在没有可信第三方的情况下完成数据抵押和取回操作，而

Khajehpour等[24]进一步改进了基于哈希时间锁的交易协议，该协议支持数据抵押交易的参与者在不可信的环境下进行可靠的交易。Belotti等[25]提出了一个可以达成“纳什均衡”的原子交换方案，使得参与交换的每个交易方在知道其他参与者的均衡策略的前提下，没有参与者可以透过改变策略使自身受益。Nadahalli等[26]借鉴了美式看涨期权来补偿在原子交换中处于劣势地位的交易方，使其免受资产锁定期间其价值波动可能造成的潜在损失，但协议过高的耦合性导致其丧失了一部分可移植性和兼容性。随着对去中心化数据抵押交易协议的深入研究，原子交换的公平性[18,21,27-28]、高效性[29-31]、隐私性[32-33]、扩展性[34]、互操作性[35]、扩展合约的安全性[2,36]以及交易数据资产的弹性[37-38]也逐渐被考虑进来。此外，当前对数据抵押交易协议的研究并不局限于抵押业务本身，针对其改进的协议已经可以适用于其他业务中[39]，这些研究为实现更加灵活的贷款业务提供了新思路和新方法。Tefagh等[40]提出了跨链债务，基于哈希时间锁定合约实现了对锁定数据资产的担保。Han等[18]基于原始的原子交换协议提出了溢价机制，并实现了期权交易，Engel等人[37]则在前者的基础上进一步实现了期权转让协议，并支持权利转让，完善了期权交易的功能。目前，针对数据抵押交易协议的相关研究成果丰硕，方案不断得到完善，但是针对交易中锁定数据的弹性机制的研究却十分匮乏，缺少锁定数据资产的再流通方法。尤其是在交易完成前，无论锁定的数据价值如何波动，交易双方都无法将其合理地利用起来，这极大地限制了交易资产的弹性。

3　预备知识

本文提出的数据所有权转移协议基于零知识证明、不经意传输、对称认证加密和两方公平秘密交换等密码工具，下面对相关知识进行简单介绍。

3.1　零知识证明

零知识证明是一种确保秘密所有者在不泄露秘密任何信息的前提下，对所持秘密进行证明的机制[41]。该证明机制的核心算法如下：

（1）初始化算法 $crs \leftarrow \mathrm{Setup}(1^{\lambda})$：输入安全参 λ，生成公共参考串 crs。

（2）证明算法 $\pi \leftarrow \mathrm{Prove}(crs, w, x)$：输入公共参考串 crs、陈述 x 以及证据 w，生成证明 π。

（3）验证算法 $1/0 \leftarrow \mathrm{Verify}(crs, x, \pi)$：输入公共参考串 crs、陈述 x 以及证明 π 进行验证。若证明是真实的，则输出1；否则，输出0。

非交互式零知识证明系统需要满足以下三个性质：

（1）完备性：如果证明者知道证据，则一定能通过有效算法让验证者通过验证。

（2）可靠性：恶意的证明者无法用错误的证据让验证者通过验证。

（3）零知识性：恶意的验证者不能获取除了证明者是否拥有陈述以外的任何信息。

3.2　不经意传输

不经意传输协议OT[42]是一种保证通信双方信息隐私性的通信协议，已被广泛应用于隐私计算等领域。在OT协议中，涉及信息发送方和信息接收方两个主体。其中，接收方只能从发送方的消息集合中获取一个私有信息，而发送方则不会知晓接收方查询了哪一个私有信息。n-选-1 OT协议的理想函数如下：

（1）参数：长度为 t 的消息。

（2）输入：随机选择 $x_1, x_2, \cdots, x_n \leftarrow \{0,1\}^t$，并随机选择 $i \leftarrow \{1, 2, \cdots, n\}$。

（3）输出：输出 $x_i \xleftarrow{OT} \{x_1, x_2, \cdots, x_n\}$。

3.3　IND-CPA安全的对称认证加密方案

定义1.　一个IND-CPA安全的对称认证加密方案 $\varepsilon = \{KeyGen, Enc, Dec\}$ 由三个多项式时间算法组成[43-44]：

（1）$KeyGen(\lambda)$：输入安全参数 λ，输出认证加密密钥 $k = (k_e, k_m)$，其中 k_e 为加密密钥，k_m 为认证密钥。

（2）$Enc_k(m)$：输入明文 m，使用先加密后认证的方式用密钥 k 对 m 进行处理，明文 m 首先被密钥 k_e 加密成密文 c_c，然后通过密文 c_c 和密钥 k_m 计算标签 c_t，输出包含有标签的密文 $c = (c_c, c_t)$。

（3）$Dec_k(c)$：输入密文 c，用密钥 k 对 c 进行处理，输出相应的明文 m 或者错误符号 $\perp$。

对称认证加密方案 ε 需满足正确性要求。对于任意认证密钥 k 以及明文 m，若 $Enc_k(m) = c$，则 $Dec_k(c) = m$。如果密文被篡改，或者不是由发送方发出的，则 $Dec_k(c) = \perp$。一个对称认证加密方案除了需要满足正确性外，还应当满足选择明文攻击下的密文不可区分性（IND-CPA），其形式化定义如下。

定义2. 对于任意一个概率多项式时间敌手A，在下述游戏中的优势$Adv_A^{IND-CPA}(\lambda)$是可忽略的，则方案$\varepsilon=\{KeyGen, Enc, Dec\}$是一个满足IND-CPA的对称认证加密方案。敌手$A$与挑战者$C$以如下交互流程执行游戏$Game_{IND-CPA}$：

(1) 挑战者C执行$KeyGen(\lambda)$算法随机选取认证加密密钥k。

(2) 敌手A可以访问加密预言机A^{OEnc_k}以获得任意明文m_i对应的密文c_i。

(3) 敌手A选择两个明文m_0, m_1作为挑战，并将其发送给挑战者C。

(4) 挑战者C获得挑战明文后，随机选择$b\leftarrow\{0,1\}$，并计算$Enc_k(m_b)$生成挑战密文c，将c发送给敌手A。

(5) 敌手输出$b'\leftarrow A^{OEnc_k}(c)$作为其对$b$的猜测。若$b'\neq\perp$且$b'=b$，则输出1，敌手赢得游戏；否则输出0。

敌手A成功赢得游戏的优势定义为安全参数λ的函数：

$$Adv_A^{IND-CPA}(\lambda)=|2\Pr[Game_{IND-CPA}(\lambda)=1]-1|$$

对于概率多项式时间敌手A，一个对称认证加密方案ε仅在以下情况下是安全的：

$$Adv_A^{IND-CPA}(\lambda)\leqslant negl(\lambda)$$

3.4 两方公平秘密交换

Alex等[10]基于不经意传输协议和IND-CPA安全的对称认证加密方案，提出了一种两方公平秘密交换协议。该协议中，参与交换的两个秘密须同时交换，要么双方秘密都交换成功，要么均无法获取对方秘密。与传统方法不同，该协议不需要任何第三方仲裁，具体过程如下：

(1) 对于参与交换的两方X和Y，双方各自通过安全参数λ生成一对密钥$\{k_{x0}, k_{x1}\}$，$\{k_{y0}, k_{y1}\}$。

(2) 双方分别随机选择一个密钥，并对各自需要交换的秘密dx和dy加密。假设双方都随机选择了k_{x0}和k_{y0}，并计算出c_x和c_y然后交换。

(3) 双方随机选择m_x和m_y，且$0\leqslant m_x, m_y\leqslant M$，并商定执行$M$次协议所需时间$T$作为协议规定时间。

(4) Y通过安全参数λ'生成密钥b，并计算$k_{y0}'\leftarrow k_{y0}\oplus b$，确保X先进行不经意传输获得$k_{y0}'$，并且在协议规定时间$T$内无法破解$k_{y0}$，但可以在协议规定时间$T$之外破解$k_{y0}$。

(5) 双方构造大小为M的向量：M_x:$[k_{x1}, \cdots, k_{x0}, \cdots, k_{x1}]$，$M_y$:$[k_{y1}, \cdots, k_{y0'}, \cdots, k_{y1}]$，其中$k_{x0}$位于向量的$m_x$位置，$k_{y0'}$位于向量的$m_y$位置。

(6) X通过不经意传输协议从M_y中学习$k_y'\xleftarrow{OT}M_y$，但此时无法解出k_y。

(7) Y从M_x中学习$k_{x'}\xleftarrow{OT}M_x$，若$k_{x'}=k_{x0}$且$k_y'=k_{y0}'$，则Y将b发送给X，否则重新进行步骤(6)-(7)。

通过以上步骤，实现了X和Y之间的秘密公平交换，在此过程中无需任何第三方介入。但是该协议的错误率为$(M-1)/M$，并且需要最多运行M次。如果在智能合约中执行该协议，则会造成较大的计算开销。

4 系统模型

本节介绍本文所设计的系统模型和数据所有权安全转移协议中的参与角色，以及其中可能存在的威胁，并介绍安全模型。

4.1 系统模型

在对基于区块链和智能合约的协议进行功能扩展时，本文在Black等人[3]和Khajehpour等人[24]所述方案的基础上，提出了数据所有权安全转移协议需要满足的设计原则，如图1所示：

(1) 低耦合性：数据所有权安全转移协议以模块化的方式增加，不应对原有协议的执行逻辑和流程产生强耦合依赖。这可以确保原有功能不受影响，同时方便后续的修改和移除。

(2) 低链上开销：数据所有权安全转移协议应避免引入过多的额外链上计算和存储开销，以降低参与各方的交易成本。

(3) 高可扩展性：数据所有权安全转移协议以可选的方式增加，如果某些参与方不需要使用这些功能，不会增加额外的执行成本。

(4) 高容错性：数据所有权安全转移协议具备容错机制，即使新增功能执行失败，也不应影响协议原有功能的正常执行。这确保了协议的整体稳定性。

根据上述原则，以及去中心化数据交易中最常见的抵押交易场景，本文设计了如图2所示的系统模型。系统包含3个实体：数据出质人、第三方受让人和数据质权人。各个实体的具体介绍如下：

(1) 数据出质人：指将数据作为抵押物提供给他人以换取报酬的主体。该主体对数据拥有所有权

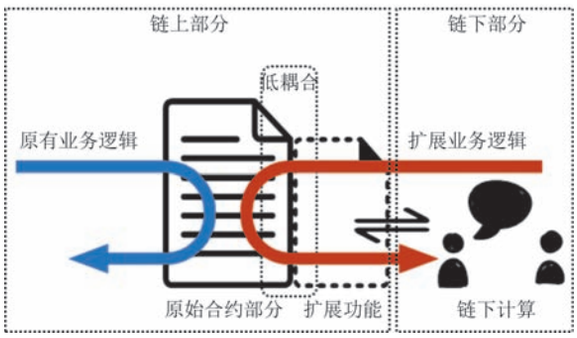

图1　数据所有权安全转移协议的设计原则

或处分权，通过抵押数据来获得资金或其他形式的报酬，并且需确保按时偿还所获得的资金。在交易开始时，出质人与质权人签订智能合约，并在智能合约中存入一定数量的数据资产，以确保资金按时偿还。当抵押数据的价值上升时，出质人可以在不提前偿还资金的前提下将抵押的数据资产变现，以获取额外的资金。在数据所有权安全转移协议中，出质人的主要责任是保证在规定时间内完成资金的偿还，否则可能会丧失抵押数据资产的所有权。此外，出质人可以与第三方受让人进行交易，将抵押数据的所有权和偿还责任转移给受让人，通过这种方式来复用出质人的锁定资产，在不终止现有交易的情况下实现锁定资产的去抵押。

（2）数据质权人：指接收数据并给付报酬的主体。该主体通过支付一定的报酬来获得数据的抵押权，以便在一定条件下对数据进行管理和使用，在该数据所有权安全转移协议中扮演关键角色，通过评估出质人抵押的数据资产价值，提供需要按时归还的资金。作为交易的主体，质权人通常期望出质人或受让人在规定的时间内偿还资金。在数据所有权安全转移协议中，质权人扮演的角色不仅是资金提供者，还是合约的管理者，他们有权限更新合约的实现，设置哈希锁，以及决定是否与受让人进行交易。

（3）第三方受让人：指最终接受抵押和数据所有权的第三方主体。该主体在数据抵押人履行完相关义务后，按照约定从数据出质人处获得数据的所有权，同时承担相应的资金偿还责任，并利用数据价值和偿还责任的差获利。通过与出质人达成协议，受让人接受抵押数据的所有权转移，并同意继承偿还资金的责任。在交易过程中，受让人使用哈希锁技术来锁定手续费，并与出质人进行秘密交换。一旦交易确认，受让人将替代原本交易中的出质人，同时获得数据资产的所有权并负责偿还资金。

协议的具体执行流程如下：

（1）出质人和质权人正常缔约交易。交易中包含了约定的资金金额和抵押数据，并确定了费用以及偿还的期限。出质人接受这些条件，完成交易的缔约。

（2）受让人加入交易，设置一个手续费提取密

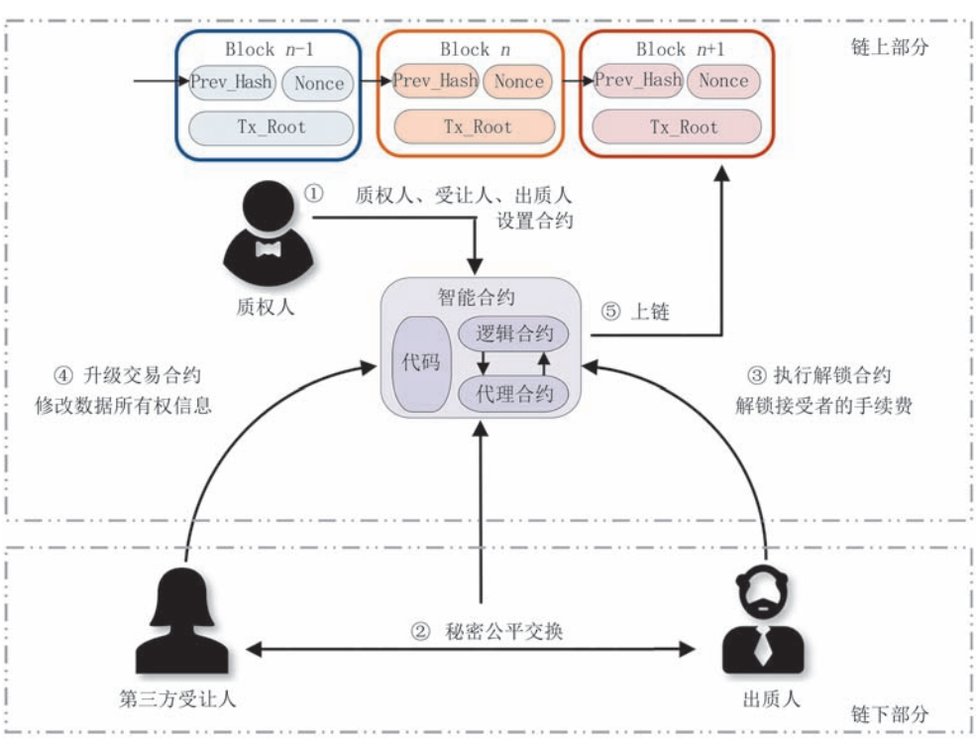

图2　数据所有权转移协议系统模型图

钥，并锁定一定数量的手续费。随后质权人在合约中配置一个升级密钥，并共享给出质人，从而完成第一步对合约的数据所有权转让设置。

（3）出质人和受让人在链下通过两方秘密交换协议完成第二步交换各自密钥。出质人使用手续费提取密钥完成第三步解锁受让人锁定的手续费作为报酬。

（4）受让人使用升级密钥完成第四步更新交易合约，修改原有交易协议中的抵押偿还信息。

（5）将合约数据上链完成第五步，从而实现抵押数据资产的所有权转移和资金偿还义务的继承。

4.2 威胁模型

威胁模型是指在系统模型中，参与方可能存在因追求自身最大利益而不诚实或损害他方权益的动机。本文假设参与方均以自己的利益优先，并可能为了更高的利益做出恶意行为。对参与该协议的任意一方而言，在链上质押任何资产都存在一定风险。如果没有对这部分风险进行合理补偿，则视为遭受了损失。具体来说，质押在链上的资产可能由于各种原因导致其价格产生波动，这对于质押该资产的一方来说需要承担相应成本。同时，参与方在诚实遵守和违反两种情况下，所面临的风险程度也不相同。如果诚实遵守，参与方只需承担与正常质押风险相关的开销。而如果违反规定，将导致其质押资产时间延长，其承担的风险成本将会上升。因此遵守时的风险总额要低于违反协议时的风险总额，该差异将促使所有参与方选择诚实遵守。本文充分考虑了质权人、出质人和受让人可能存在的威胁模型。

（1）质权人威胁模型：质权人为了最大化自己的经济利益，试图声称出质人没有按时偿还资金，以便没收更多的抵押数据资产，或者在获得受让人的手续费后尝试将受让人排除在交易合约之外。

（2）出质人威胁模型：出质人在与受让人的交易中，会尝试获得受让人的手续费而不转移抵押数据的所有权和偿还责任。此外在链下交换密钥时，会存在诚实且好奇的敌手尝试在己方密钥不泄露的情况下获取对方密钥的攻击行为。

（3）受让人威胁模型：受让人希望从交易中获得尽可能多的利益，他会尝试接受出质人抵押数据资产所有权但不接受偿还责任，或者接受出质人的抵押数据资产所有权以及偿还责任后收回手续费。此外，在链下交换密钥时，会存在诚实且好奇的敌手尝试在己方密钥不泄露的情况下获取对方密钥的攻击行为。

4.3 安全模型

本节将进一步对链下部分的两方秘密交换协议的安全模型进行描述。本文借鉴了Alex等人[10]提出的非标准假设：假设存在安全的参数λ，以及可在一段时间内破解的相对安全参数λ'，同时假设存在一个因子M，它与λ'无关，并满足：

$$MAdv_A^{IND-CPA}(\lambda)=Adv_A^{IND-CPA}(\lambda')$$

其中，$Adv_A^{IND-CPA}(\cdot)$表示在IND-CPA意义下，攻击者的成功概率或优势。

在这一假设下，因子M用于衡量攻击安全参数λ与λ'各自所需的时间之比。它并不直接依赖λ或λ'本身，而是取决于两者之间的相对变化。如果λ与λ'一直保持同步增长，则M的取值将保持不变。

接下来，将这一假设应用到对称认证加密方案ε上：若破解$\varepsilon(\lambda)$的时间至少为t_1，破解$\varepsilon(\lambda')$至少为t_3，那么必然有$t_3<t_1$，并且$M=t_3/t_1$。在链上的合约部分，还设定了一个手续费提取截止时间t_2。为了确保受让人只能在出质人提取手续费之后再进行交易信息升级，需要满足$t_2<t_3<t_1$。如此一来，出质人会先完成手续费提取，而受让人只能等到此过程结束后，才有足够时间与条件来更新交易信息，从而保证整个流程的安全性和可执行性。

基于对称认证加密方案以及不经意传输协议构造的两方秘密交换协议，需要满足计算完备性和计算公平性[10]。计算完备性确保了在链下两方秘密交换协议中，参与交换的受让人和出质人只能同时按照预期完成交易，即受让人能够升级交易信息的同时出质人能够获得数据所有权转移手续费。计算公平性则确保了在链下两方秘密交换协议中，任意一方不能在多项式时间内破解对方的密钥信息，也不能从协议执行历史中恢复出对方的密钥。具体定义如下：

定义3. 计算完备性. 对于参与交换的受让人和出质人，以及相互交换的密钥C_1和C_2，在协议执行成功后，受让人成功提交C_2且出质人成功提交C_1的概率为1，即：

$$\Pr[thirdParty(C2updated)\wedge borrower(C1updated)]=1$$

则称链下两方秘密交换协议满足计算完备性。

定义4. 计算公平性. 对于任意一个概率多项式时间敌手A，A在下述游戏中的优势$Adv_A^{Fairness}(\lambda)$是可忽略的，则链下密钥公平秘密交换方案Π满足计算公平性。敌手A与挑战者C执行游戏$Game_{Fairness}$如下：

（1）挑战者C从协议执行历史log中随机选择一条包含其密钥信息k的加密记录δ。

（2）敌手A计算$k' \leftarrow A(\delta)$。

（3）若$k=k'$则输出1，否则输出0。

敌手A成功计算$k=k'$的优势定义为安全参数λ的函数：

$$Adv_A^{Fairness}(\lambda)=\Pr[Game_{Fairness}(\lambda)=1]$$

对于概率多项式时间敌手A，链下两方秘密交换方案Π仅在以下条件下是满足计算公平性的：

$$Adv_A^{Fairness}(\lambda)\leqslant negl(\lambda)$$

5　数据所有权安全转移协议

本节将对数据所有权安全转移协议的交互逻辑和工作流程进行描述。表1列举了协议中常用的符号及其含义。

本文所提出的数据所有权安全转移协议由以下两部分构成：第一，链上智能合约，包含数据抵押交易合约和数据所有权转移合约。其设计具有低耦合性，实现了对各类数据抵押交易协议的最大兼容。只要合约满足含有出质人、质权人、抵押数据等必要字段，就可与数据所有权转移合约配合使用。第二，链下两方秘密交换协议。该协议与数据所有权转移合约高度耦合，确保出质人与受让人在链下交换密钥的过程中权益不受损害。通过上述设计，本协议框架在提供高效数据流通的同时，也充分保障各参与方的安全性，为跨链数据所有权转移场景提供了一个行之有效的解决方案。

表1　协议中部分符号定义

符号	描述
$lender$	质权人角色
$borrower$	出质人角色
$thirdParty$	第三方受让人角色
t_0	还款时间
t_1	数据所有权转移失效时间
t_2	交易信息更新时间
t_3	交易信息更新延期时间
$set(\cdot)$	初始化信息设置
$address(\cdot)$	获取地址
C_1	数据所有权转移手续费解锁密钥
C_2	交易信息升级密钥
$Hash(\cdot)$	哈希锁
$k \xleftarrow[i]{OT} \boldsymbol{m}$	使用不经意传输协议获取向量$\boldsymbol{m}$中第i个位置的元素
λ,λ'	安全参数
k_{B0},k_{B1}	出质人设置的加密密钥
k_{T0},k_{T1}	受让人设置的加密密钥
b	出质人设置的延迟解密密钥
X_1	对C_1加密后的密文
X_2	对C_2加密后的密文
$k_{T_{i_B}}$	在向量$\boldsymbol{m}_T$中位置为i_B的元素
$k_{B_{i_T}'}$	在向量$\boldsymbol{m}_B$中位置为i_T的元素
v	验证结果
$k_B \xleftarrow{b} k_{B'}$	出质人获取$k_{B'}$后通过b求k_B
$Hash(C)$	哈希函数

5.1　链上智能合约

质权人、出质人和受让人都参与了链上智能合约的交互。如果受让人不参与数据所有权转移，则链上合约只执行原有数据抵押交易协议，此时数据所有权转移部分不会产生额外的开销。如果受让人参与数据所有权转移，则在数据所有权转移完成后，原本存在于出质人与质权人之间的数据抵押交易将转变为受让人与质权人之间的新的数据抵押交易。在数据所有权转移后，出质人不再参与后续的交易流程。

5.1.1　合约设计

本文参考了Black等人[3]设计的数据抵押交易协议，并基于可升级智能合约设计了数据所有权安全转移协议。协议包含三个合约，具体如下：

（1）代理合约$ProxyContract$：该合约由质权人部署，用于代理交易合约中的所有算法并提供合约升级功能。

（2）交易合约$LoanContract$：该合约由质权人部署，通过代理合约来控制该合约实现交易部署、数据所有权转移信息确认等功能。合约中有以下算法：

① 交易初始化算法，$initializeLoan(borrower, set(L_L), set(B_C), set(L_F), t_0)$：质权人初始化设置借款人信息、交易本金、抵押数据、费用和资金偿还时间，并部署合约。

② 抵押算法，$depositCollateral(B_C)$：出质人将抵押数据抵押至合约中。

③ 资金转让算法，$lend(L_L)$：质权人将资金发送给出质人。

④ 交易信息升级算法，$setThirdPartyHashlock(Hash(C_2), t_2, t_3, address(HashlockContract))$：质权人将交易信息升级密钥的哈希锁、交易信息更新时间、延长时间、数据所有权转移合约的地址存入本合约中。

⑤ 数据所有权转移算法，$transferDebt(C_2)$：受

让人在获得C_2后执行该算法升级交易信息，替代出质人，同时释放数据所有权转移合约中的手续费给出质人和质权人。

⑥ 资金偿还算法，*repayLoan*(L_L+L_F)：出质人提交交易本金以及手续费，进行还款。

⑦ 抵押数据扣押算法，*claimCollateral*(B_C)：质权人可在资金偿还截止日期后执行该算法取回出质人的抵押数据资产。

(3) 数据所有权转移合约*HashlockContract*：该合约由受让人部署，用于启动数据所有权转移流程，具体包含以下算法：

① 手续费锁定算法，*depositFee*(T_F)：受让人将手续费存入本合约中。

② 交易信息升级确认算法，*releaseFunds*(C_1)：出质人在获取C_1后，在t_1前执行该算法修改合约状态。

③ 数据所有权转移撤销算法，*reFund*()：协议执行失败受让人可以取回质押在合约中的手续费。

链上合约运行过程分为4个阶段，具体如图3所示，分别是交易设置阶段、数据所有权转移设置阶段、数据所有权转移完成阶段、交易完成阶段。各阶段详细描述如下：

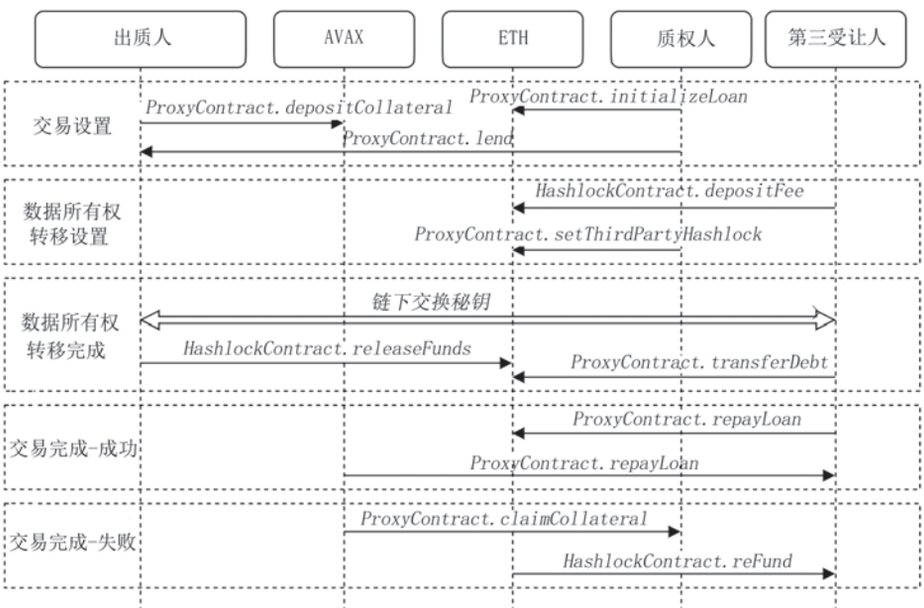

图3 链上合约执行流程

(1) 交易设置阶段：质权人通过代理合约部署交易合约，并调用交易初始化算法初始化设置交易信息、交易资金、抵押金额、费用和交易到期时间t_0，随后发送交易合约地址给出质人进行确认。出质人随后执行抵押算法将数据资产抵押至合约中。质权人在确认数据抵押情况后执行资金转让算法将交易本金发送给出质人，完成交易设置阶段。

(2) 数据所有权转移设置阶段：受让人部署数据所有权转移合约，并初始化质权人信息、交易信息、数据所有权转移手续费解锁密钥哈希锁、交易合约的地址，并让质权人进行确认后执行交易信息升级算法，将交易信息升级密钥的哈希锁、交易信息更新时间t_2、延长时间t_3、协议失效时间t_1、数据所有权转移合约的地址存入交易合约中，然后将C_2发送给出质人。其中$t_2<t_3<t_1<t_0$。受让人确认合约后执行手续费锁定算法将数据所有权转移手续费存入数据所有权转移合约中。

(3) 数据所有权转移完成阶段：出质人和受让人在链下通过两方秘密交换协议进行交换，在出质人先获取C_1后，在t_2前执行交易信息升级确认算法。此时合约将状态置为*C*1*updated*，并等待交易合约状态变为*C*2*updated*后，将锁定在合约中的T_F平分发送给出质人和质权人，同时合约将交易合约中的t_2延长至t_3以确保受让人可以及时更新交易信息。受让人在获得C_2并且数据所有权转移合约状态变为*C*1*updated*后，在t_3前执行数据所有权转移算法，此时合约会将状态置为*C*2*updated*并更新交易信息，从而完成数据所有权转移。该阶段出质人和受让人将同时进行链上和链下的交互，具体协商过程将在5.2节进行详细说明。

（4）交易完成阶段：上一阶段完成后，数据抵押交易协议中的抵押数据所有权和资金偿还义务继承将由受让人继承，受让人需要在t_0前执行资金偿还算法还款并取回抵押数据。如果未能在t_0前还清交易本金，则质权人可在t_0后执行抵押数据扣押算法扣押数据资产。

5.1.2　抵御威胁

针对4.2节所述的威胁模型，本节将对质权人、出质人、受让人可能进行的攻击行为进行分析，确保链上合约在执行过程中的安全性。分析如下：

（1）质权人：对于质权人可能会在数据抵押交易协议到期前，强制结束协议并扣押数据的攻击行为，交易合约可以避免，在交易合约的作用下，质权人无法在初始化时设置的还款时间到达之前执行抵押数据扣押算法强制扣押数据资产。

（2）出质人：对于出质人可能在受让人获得密钥C_2之前，尝试提取执行数据所有权转移算法的攻击行为，数据所有权转移合约可以避免，在该合约中设置了状态监测以及状态同步两组安全参数，出质人虽然会优先获得C_1，但是在上传C_1到合约后合约会先修改合约状态至$C1updated$，同时检测交易合约的状态是否同步为$C2updated$，只有在C_2上传之后才能进一步执行手续费提取操作，因此出质人无法发起该攻击。

对于出质人在获取C_1后拒绝发送b或使用假密钥给受让人的攻击行为，数据所有权转移合约以及交易合约可避免。在出质人提交C_1后数据所有权转移合约会通过同步锁将交易合约中的交易信息升级截止时间由t_2升级为t_3。而受让人在链下的两方秘密交换协议中，受让人在获取$k_{B'}$后立即尝试破解k_B，如果$k_{B'}$中包含了正确的k_B，则交换协议中的安全参数λ'决定受让人可以在t_3时间前恢复出k_B并获得C_2提交，从而完成交易信息升级。如果$k_{B'}$中未包含正确的k_B，则受让人将无法恢复出C_2，交易合约无法修改状态至$C2updated$，而数据所有权转移合约会因为无法解锁手续费导致数据所有权转移完成阶段失败。此时交易合约会清除数据所有权转移信息，受让人仅需在时间t_3前（相较于时间t_1会缩短）承担手续费价格波动的风险。在此时受让人、出质人、质权人将重新开始数据所有权转移设置阶段，或出质人和质权人继续交易完成阶段。故出质人也无法进行此攻击。

对于出质人尝试在己方密钥不泄露的情况下与受让人交易以骗取C_1的攻击行为，交易合约在出质人提交$Hash(C_2)$后将哈希值公开在合约中。在链下进行密钥交换之前，任何自称出质人的交易方都需要生成证明$\pi_2 \leftarrow Prove(Hash(C_2), C_2)$，然后由受让人执行验证$v_2 \leftarrow Verify(Hash(C_2), \pi_2)$. 若通过验证，则确保交易方拥有$C_2$并验证出质人身份，进而避免此类攻击。对链下交易时出质人通过分析密文来获取受让人密钥的攻击行为的安全性证明，将在5.2.2节中进行详细介绍。

（3）受让人：对于受让人可能会在出质人获得C_1之前尝试升级合约执行交易信息升级的攻击行为，交易合约可以避免。链下的两方秘密交换协议中受让人在执行向量构造算法中获取$k_{B'}$后立即尝试破解k_B，破解时间将大于出质人获取C_1的时间，故受让人无法执行此类攻击行为。

对于受让人可能会使用假密钥给出质人的攻击行为，交易合约中设置了只有在数据所有权转移合约状态变为$C1updated$后才能提交C_2，此时受让人将在时间t_1前（大于出质人攻击时所需承担风险的时间t_3）承担手续费被锁定无法交易所造成的价值波动风险，则通过事件监测的方式避免此类攻击行为。

对于受让人尝试在己方密钥不泄露的情况下与出质人交易骗取C_2的攻击行为，数据所有权转移合约可以确保在受让人提交$Hash(C_1)$后，将哈希值公开在合约中。在链下进行密钥交换之前，任何自称受让人的交易方都需要生成证明$\pi_1 \leftarrow Prove(Hash(C_1), C_1)$，并且由出质人执行验证$v_1 \leftarrow Verify(Hash(C_1), \pi_1)$。若通过验证则确保交易方拥有$C_1$并验证受让人身份，进而避免此类攻击。对链下交易时受让人通过分析密文来获取出质人密钥的攻击行为的安全性证明，将在5.2.2节中进行详细介绍。

5.2　链下两方秘密交换协议

本文将参考于等人[45]提出的链上公平交换方案思路，在Alex等人[10]方案的基础上构造链下部分的合约密钥交换方案，以实现在不显著增加链上开销的情况下对已有数据抵押交易协议的扩展。链下部分参与方包括出质人和受让人，目的是交换合约中的数据所有权转移手续费解锁密钥C_1和交易信息升级密钥C_2。链下部分的意义在于将数据所有权安全转移协议中计算开销较大的部分转移到链下，以实现在不增加链上开销的前提下对原有数据抵押

交易协议进行扩展。由于传统金融工具种类繁多、交互复杂，扩展部分与原有协议之间需要保持较低的耦合度，实现模块化。这样各方才能以最小的开销实现预期功能。Dalton等[10]提出的秘密公平交换协议支持两方链下秘密交换，相较于其他公平交换协议，该协议具有无需第三方或可信中介的特点，交换双方除了链下交换的计算开销外没有任何其他成本。本文在该协议的基础上进行了修改，引入零知识证明以防止恶意用户干扰交易过程，确保只有拥有正确密钥的交易地址才可以参与交换。同时在数据所有权转移合约中限制出质人和受让人提交的截止时间，从而确保密钥交换的安全性。

5.2.1 算法定义

一个公平秘密交换协议Π能够使参与秘密交换的两方安全交换各自的秘密，在交换过程中不会出现秘密泄露或者某一方提前获取秘密的情况。方案流程如图4所示，其中包含7个算法，即$\Pi=(IdentityAuth, SetParams, KeyGen, Enc_k, VectorGen, Study, Update)$，其中*IdentityAuth*算法包含了零知识证明的*Setup*, *Prove*, *Verify*算法；*KeyGen*算法则使用Alex等人[10]方案中的*KeyGen*算法；*Update*算法描述了两方执行链上合约的过程，该步骤包含了链上操作。具体算法定义如下：

(1) 安全参数协商算法(*SetParams*)：

① 计算$\lambda, \lambda' \leftarrow SetParams()$，设攻击加密方案$\varepsilon(\lambda)$的时间为$t_1$，攻击加密方案$\varepsilon(\lambda')$的时间为$t_3$，则$t_2 < t_3 < t_1$。

② 计算$M' = 1/M = t_1/t_3$。

(2) 身份验证算法(*IdentityAuth*)：

① 输入λ计算$crs1, crs2 \leftarrow Setup(\lambda)$

② 输入$C_1, Hash(C_1), C_2, Hash(C_2)$，计算$\pi_1 \leftarrow Prove(crs1, C_1, Hash(C_1))$，$\pi_2 \leftarrow Prove(crs2, C_2, Hash(C_2))$

③ 计算$v_1 \leftarrow Verify(crs1, Hash(C_1), \pi_1)$，$v_2 \leftarrow Verify(crs2, Hash(C_2), \pi_2)$。

④ 判断$v_1 = true$且$v_2 = true$，若是，则通过验证；否则终止协议。

(3) 密钥生成算法(*KeyGen*)：

① 输入λ，计算$k_{B0}, k_{B1} \leftarrow KeyGen(\lambda)$，$k_{T0}, k_{T1} \leftarrow KeyGen(\lambda)$。

② 输入λ'，计算$b \leftarrow KeyGen(\lambda')$，$k_{B0'} \leftarrow k_{B0} \oplus b$。

(4) 加密算法(Enc_k)：

① 随机选取$k_{B0} \leftarrow \{k_{B0}, k_{B1}\}$，假设这里选取的是$k_{B0}$，并计算$X_2 \leftarrow Enc_{k_{B0}}(C_2)$。

② 随机选取$k_{T0} \leftarrow \{k_{T0}, k_{T1}\}$，假设这里选取的是$k_{T0}$，并计算$X_1 \leftarrow Enc_{k_{T0}}(C_1)$。

(5) 向量构造算法(*VectorGen*)：

① 构造大小为M'的向量$\boldsymbol{V}_{M'} = \{1, 2, \cdots, M'\}$，并随机选取$i_B \in \boldsymbol{V}_{M'}$。

② 构造$m_B \leftarrow \{k_{B1}, \cdots, k_{B1}, k_{B0'}, k_{B1}, \cdots, k_{B1}\}$，其中$k_{B0'}$位于向量的$i_B$位置。

③ 随机选取$i_T \in \boldsymbol{V}_{M'}$，并构造$m_T \leftarrow \{k_{T1}, \cdots, k_{T1}, k_{T0}, k_{T1}, \cdots, k_{T1}\}$，其中$k_{T0}$位于向量的$i_T$位置。

(6) 学习算法(*Study*)：

① 计算$k_{B_{T'}} \xleftarrow[i_T]{OT} m_B$，$k_{T_{B'}} \xleftarrow[i_B]{OT} m_T$。

② 计算$Hash(C_1)$是否等于$Hash(Dec_{k_{T_B}}(X_1))$，若不等则令$\boldsymbol{V}_{M'} = \{1, \cdots, i_B - 1, i_B + 1, \cdots, M'\}$，重新执行向量构造算法，若相等则$i_B = i_T$。

③ 计算$k_{B_T} \xleftarrow{b} k_{B_{T'}}$。

(7) 合约升级算法(*Update*)：

① 执行$C1updated \leftarrow releaseFunds(C_1)$，并等待同步$C2updated$。

② 执行$C2updated \leftarrow transferDebt(C_2)$。

5.2.2 安全性分析

定理1. 计算完备性. 对于参与交换的第三方受让人*thirdParty*和出质人*borrower*，在协议执行成功后双方成功提交C_2和C_1概率为1，即

$$\Pr[thirdParty(C2updated) \wedge borrower(C1updated)] = 1$$

证明. 若$i_B = i_T$，则受让人*thirdParty*和出质人*borrower*在第一次即可成功交换C_1和C_2，并由4.1节合约设计所述的状态监测、状态同步两组安全参数确保协议执行成功后C_1和C_2只提交成功一个的概率为0，即：

$$\Pr[(C2updated \wedge \overline{C1update}) \vee (\overline{C2updated} \wedge C1update)] = 0$$

若$i_B \neq i_T$，由于$0 \leqslant m \leqslant M$，则单次执行学习算法后受让人*thirdParty*和出质人*borrower*成功交换C_1和C_2的概率$\Pr[thirdParty(C2) \wedge borrower(C1)] \models 1/M$，由于假设中$M$在双方协商后即为定值，故双方在有限次执行向量构造算法和学习算法后当$i_B = i_T$时即可成功完成交换；若交换过程中任何一方中断退出，则由4.1节中的数据所有权转移合约中断数据所有权转移过程。

综上所述，协议执行成功后受让人提交C_2并且出质人提交C_1的概率1，协议满足计算完备性。

定理2. 计算公平性. 在随机预言机模型下，如果对称认证加密算法是满足选择明文攻击下密文不可区分的，则链下两方秘密交换协议满足计算公平性。

证明. 若存在一个多项式时间敌手A，在随机预言机模型中能在$Game_{Fairness}$中以不可忽略的优势$Adv_A^{Fairness}(\lambda)$从加密的历史记录中输出一个有效信息，则一定存在一个模拟者S能够攻破满足IND-CPA的对称认证加密方案并从加密信息中恢复出明文信息。具体证明如下：

敌手A收到加密记录δ，并尝试通过以下步骤提输出包含在加密记录δ中的密钥信息：

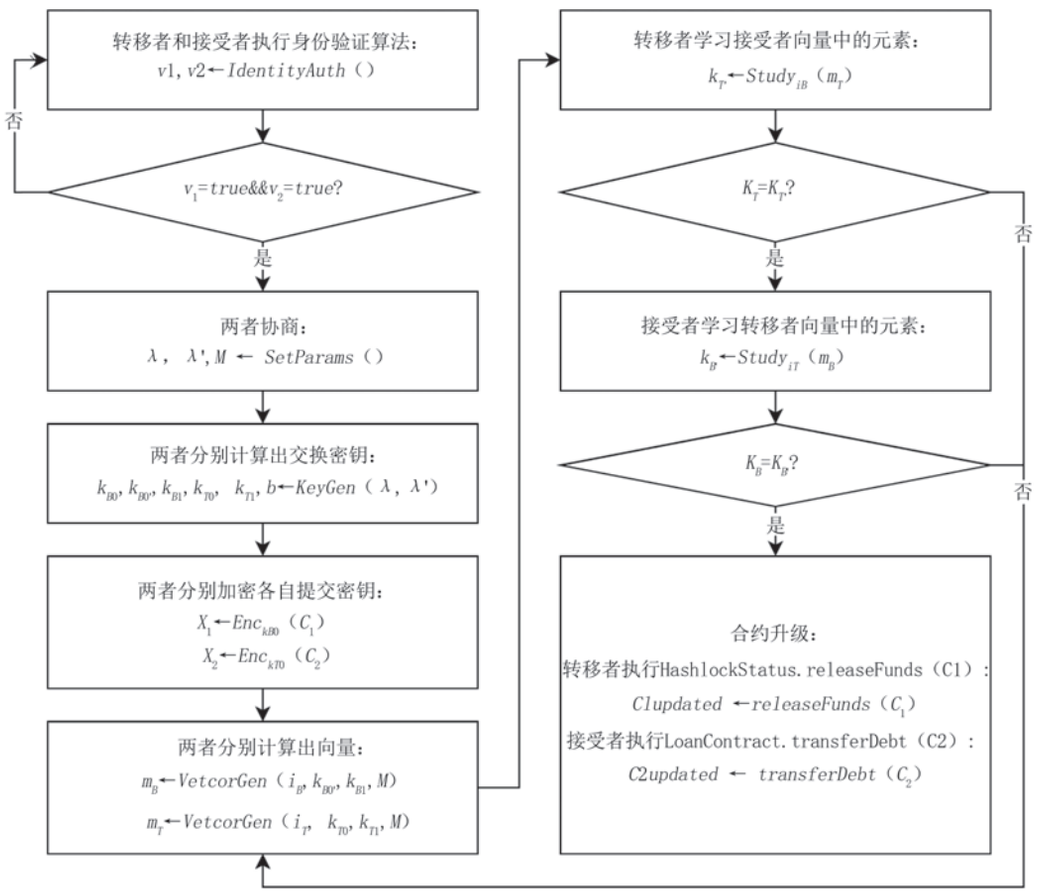

图4　链下两方秘密交换协议执行流程

（1）构造$k_0 \leftarrow \{0,1\}^n$，$k_1 \leftarrow \{0,1\}^n$，并随机选择$b \leftarrow \{0,1\}$计算$log \leftarrow \delta \leftarrow k_b$。

（2）随机选取$\delta' \leftarrow log$。

（3）计算$k_b' \leftarrow A(\delta')$。

（4）若$k_b' = k_b$，则输出1，否则输出0。

若敌手A在游戏$Game_{Fairness}$中拥有不可忽略的优势$Adv_A^{Fairness}(\lambda)$，并成功执行$k_b' \leftarrow A(\delta')$，而$\delta'$又由满足IND-CPA的对称加密算法$Enc_k()$加密得到，则此时模拟者$S$必定可利用敌手$A$的能力在游戏$Game_{IND-CPA}$中成功猜测$b' \leftarrow S^{OEnc_k}(c)$，从而获得不可忽略的优势$Adv_S^{IND-CPA}(\lambda)$。对于加密记录$\delta'$中可能包含的不同信息，$Adv_A^{Fairness}(\lambda)$与$Adv_S^{IND-CPA}(\lambda)$关系如下：

当$\delta' = \{X_2\}$，此时记敌手A为受让人$thirdParty$，则有$Adv_A^{Fairness}(\lambda) \leqslant Adv_S^{IND-CPA}(\lambda)$，即模拟者$S$此时可以利用其能力恢复出$X_2$，并进一步恢复出$C_2$。

当$\delta' = \{X_2, X_1\}$，此时记敌手A为出质人$borrower$，则有$Adv_A^{Fairness}(\lambda) \leqslant Adv_S^{IND-CPA}(\lambda)$，即模拟者$S$此时可以利用其能力恢复出$X_1$，并进一步恢复出$C_1$。

当$\delta' = \{X_2, X_1, k_{B_T'}\}$，此时记敌手$A$为受让人$thirdParty$，若$k_{B_T'} \neq k_{B0'}$，则与上一情况相同；若$k_{B_T'} = k_{B0'}$，由于$k_{B0'} \leftarrow k_{B0} \oplus b$，且$b \leftarrow KeyGen(\lambda')$，根据安全模型有$Adv_A^{Fairness}(\lambda) = (1/M) Adv_S^{IND-CPA}(\lambda')$，即此时敌手$A$解出$k_{B0'}$至少为$t_3$是合理的。同

时根据安全模型，存在 $MAdv_S^{IND-CPA}(\lambda)=Adv_S^{IND-CPA}(\lambda')$，故此时模拟者 S 的优势 $Adv_S^{IND-CPA}(\lambda)=(1/M)Adv_S^{IND-CPA}(\lambda')=Adv_A^{Fairness}(\lambda)$

当 $\delta'=\{X_2,X_1,k_{B_T}',k_{T_B}\}$，此时记敌手 A 为出质人 *borrower*，若 $k_{T_B}\neq k_{T0}$，则与第二种情况相同；若 $k_{T_B}=k_{T0}$，则有 $Adv_A^{Fairness}(\lambda)\leqslant Adv_S^{IND-CPA}(\lambda)$，即模拟者 S 此时可利用其能力恢复出 k_{T_B}。

综上所述，若存在一个多项式时间敌手 A 可以从加密的历史记录中输出一个有效信息，则一定存在一个模拟者 S 能够攻破满足 IND-CPA 的对称认证加密方案，证毕。而一个满足 IND-CPA 的对称认证加密方案有 $Adv_A^{IND-CPA}(\lambda)\leqslant negl(\lambda)$，故 $Adv_A^{Fairness}(\lambda)\leqslant negl(\lambda)$，执行链下两方秘密交换协议的参与方都无法以不可忽略的优势从历史纪录中恢复出任何与交换密钥有关的信息，即 $Adv_{borrower}^{Fairness}(\lambda)\leqslant negl(\lambda)$ 且 $Adv_{thirdParty}^{Fairness}(\lambda)\leqslant negl(\lambda)$，协议满足计算公平性。

6 实验分析

我们对协议链上部分的合约开销与链下部分的两方秘密交换协议的计算开销进行了测试。首先对协议的链上部分中交易合约与数据所有权转移合约进行测试，并与Black等[3]提出的去中心化数据抵押交易协议中所涉及的数据抵押和资金偿还部分进行对比；随后将对链下两方秘密交换协议的计算开销进行效率测试，计算链下密钥交换协议中各算法的执行效率。本文的测试环境为 Intel(R) Core(TM) i7-12700F CPU@2.10 GHz，16 GB，Windows 11 22H2。

6.1 链上智能合约测试

对链上智能合约进行测试内容包括测试合约运行的Gas消耗。影响Gas开销的因素有合约代码复杂度、存储量、循环和递归、外部调用等。因此，合约的Gas开销将作为智能合约运行效率的评判标准，本文使用以太坊测试链在remixIDE环境中编写了以下合约：

(1) 原始交易合约：该合约是根据Black等人[3]提出的去中心化数据抵押交易协议里数据抵押和资金偿还部分流程重写的原始合约，用于和本协议中的链上部分进行对比测试。合约中去除了清算和拍卖过程，以便在后续的测试中准确反映出数据抵押交易部分的Gas消耗。

(2) 支持数据所有权转移的交易合约：该合约在原始交易合约基础上进行修改，在不干扰数据抵押交易执行流程的基础上增加了数据所有权转移函数，以支持数据所有权转移功能。

(3) 数据所有权转移扩展合约：该合约是受让人用于接入数据所有权转移的启动合约，出质人和质权人通过该合约提取受让人抵押的手续费。

(4) 代理合约：该合约是用于控制支持数据所有权转移的交易合约的代理合约，实现业务逻辑和数据的分离，以支持交易信息修改功能。

本文的测试日期是2024年11月8日11:00，当前时段Gas价格为18 GWei。四种合约及执行对应函数的Gas消耗如表2所示。合约的部署消耗的Gas是最多的，原始的交易合约部署需要Gas为579885，需要花费0.01 eth。而修改后支持数据所有权转移功能的交易合约及其代理合约部署需要的Gas值总计2215122，需要花费0.03 eth。在协议的整个链上流程中，Gas花费最大的部分为合约的部署过程，这是因为部署合约需要执行初始化存储，复制代码等操作。

与原始数据抵押交易协议相比，本协议在部署时需要额外部署代理合约和逻辑合约，其Gas消耗的增量主要集中在逻辑合约中新增的数据所有权转移函数。完整执行数据所有权转移流程涉及交易信息升级算法、数据所有权转移算法、手续费锁定算法、交易信息升级确认算法四个函数，总计需要消耗的Gas为240939，总花费为0.0043 eth。与Black等人[3]提出的协议相比，本文设计的数据所有权转移功能消耗的Gas较少，在不显著增加额外链上开销的情况下可以实现对已有协议的升级，符合对原子贷款协议功能扩展的设计原则，具有较高的实用性。

6.2 链下两方秘密交换协议测试

本文使用Pycharm IDE编译Python程序，实现协议Π中的7个算法。*IdentityAuth* 算法借鉴了Giacomelli等[46]提出的ZKBoo协议，对参与交换的密钥进行零知识证明来确认身份；*SetParams* 算法通过密钥长度来实现对安全参数 λ 和 λ' 的协商；*KeyGen* 算法和 Enc_k 算法使用基于AES算法的EtM组合方案进行仿真；*VectorGen* 算法和 *Study* 算法则利用RSA通过n-选-1 OT协议实现。其中 *IdentityAuth*、*SetParams*、*KeyGen*、Enc_k 算法的运行效率如图5所示。

在链下两方秘密交换的过程中，*IdentityAuth*、

表2　链上智能合约及执行函数的运行开销

合约名称	函数名称	Gas消耗	Gas花费/eth
原始交易合约	部署合约	579 885	0.010 4379 30
	贷款初始化算法	158 761	0.002 857 698
	抵押算法	255 63	0.000 460 134
	贷款算法	397 77	0.000 715 986
	贷款偿还算法	538 75	0.000 969 750
	抵押数据扣押算法	444 96	0.000 800 928
代理合约	部署合约	115 365 4	0.020 765 772
支持数据所有权转移的交易合约	部署合约	106 146 8	0.019 106 424
	贷款初始化算法	141 926	0.002 554 668
	抵押算法	277 95	0.000 500 310
	贷款算法	431 56	0.000 776 808
	交易信息升级算法	969 34	0.001 744 812
	数据所有权转移算法	447 86	0.000 806 148
	贷款偿还算法	564 42	0.001 015 956
	抵押数据扣押算法	237 64	0.000 427 752
数据所有权转移扩展合约	部署合约	716 424	0.012 895 632
	手续费锁定算法	256 77	0.000 462 186
	交易信息升级确认算法	735 42	0.001 323 756

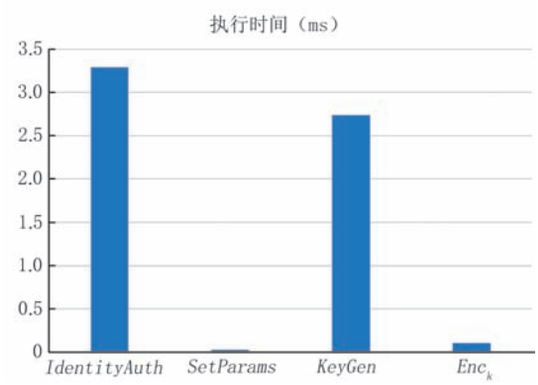

图5　*IdentityAuth*、*SetParams*、*KeyGen*、Enc_k算法执行效率

SetParams、*KeyGen*、Enc_k四个算法只运行一次，其中*IdentityAuth*算法需要3.2901 ms，*SetParams*算法需要0.0233 ms，*KeyGen*算法需要3.7339 ms，Enc_k算法需要0.1046 ms。算法整体消耗时间很少，可以在资源受限的平台中部署运行。而*VectorGen*，*Study*两个算法的运行时间取决于交换双方随机选择的i_B与i_T，当$i_B=i_T$时交换完成，交换次数的上限不超过M。本节对两个算法从执行1次到执行100次进行测试，具体结果如图6和图7所示。

*VectorGen*算法在执行10次时需要0.0264 ms，在执行50次时需要0.1383 ms，在执行100次时需要0.2777 ms。而*Study*算法在执行10次时需要2747 ms，在执行50次时需要14090 ms，在执行100次时需要28125 ms。两个算法的执行成本均随执行次数的增长呈线性增加，而成功执行链下两方秘密交换协议平均仅需执行60次*VectorGen*算法和*Study*算法，链下协议的整体开销可控。综上所述，链下两方秘密交换协议的整体开销较低，易于部署。

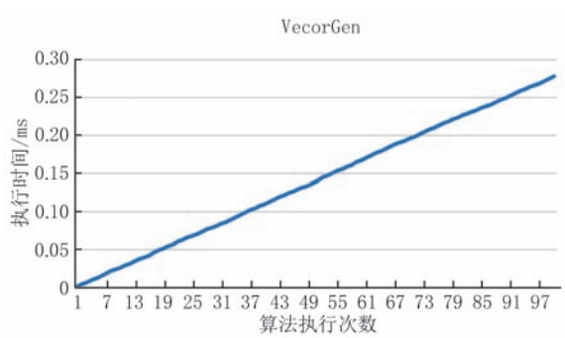

图6　*VectorGen*算法执行效率

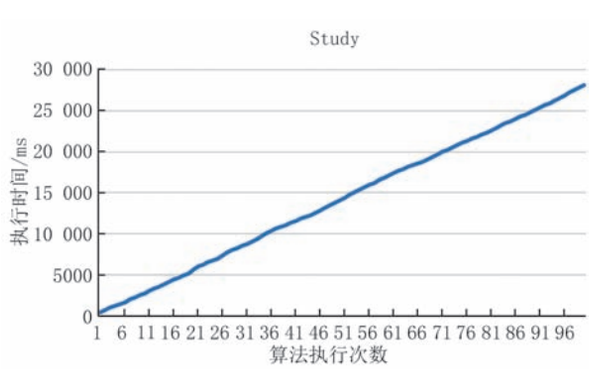

图7　*Study*算法执行效率

7 总 结

针对现有数据抵押交易协议无法满足数据所有权转移的问题，本文设计了面向去中心化环境的数据所有权安全转移系统模型，提出了一种安全高效的数据所有权转移协议。基于可升级的智能合约以及两方公平交换协议，对原有功能进行了扩展，结合链上链下交互的方式，将大部分计算转移到链下，并通过测试实验进行比较，验证了所提出的数据所有权安全转移协议的实用性，为未来开展数字货币相关的金融业务、促进数据要素流通提供了新思路。

参 考 文 献

[1] Schär F. Decentralized finance: On blockchain-and smart contract-based financial markets. FRB of St. Louis Review, 2021: 153-174

[2] Hu Tianyuan, Li Zecheng, Li Bixin, et al. Contractual security and privacy security of smart contract:A system mapping study. Chinese Journal of Computers, 2021, 44(12): 2485-2514 (ih Chinese)
(胡甜媛，李泽成，李必信等. 智能合约的合约安全和隐私安全研究综述. 计算机学报，2021,44(12): 2485-2514)

[3] Black M, Liu T, Cai T. Atomic loans: Cryptocurrency debt instruments. arXiv, 2019

[4] Herlihy M. Atomic cross-chain swaps//Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing. Egham, United Kingdom. 2018: 245-254

[5] Cai Xiaoqing, Deng Yao, Zhang Liang, et al. The principle and core technology of blockchain. Chinese Journal of Computers, 2021, 44(1): 84-131 (ih Chinese)
(蔡晓晴，邓尧，张亮等. 区块链原理及其核心技术 .计算机学报，2021, 44 (1): 84-131)

[6] Liu Aodi, Du Xuehui, Wang Na, et al. Research progress on blockchain system security technology. Chinese Journal of Computers, 2024, 47(3): 608-646 (ih Chinese)
(刘敖迪，杜学绘，王娜等. 区块链系统安全防护技术研究进展 .计算机学报，2024, 47 (3): 608-646)

[7] Herlihy M, Liskov B, Shrira L. Cross-chain deals and adversarial commerce. Proceedings. of the VLDB endowment, 2019, 13(2): 100-113

[8] Xuan H, Yong Y, Feiyue W. Security problems on blockchain: The state of the art and future trends. Acta Automatica Sinica, 2019, 45(1): 206-225 (ih Chinese)
(韩璇，袁勇，王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报，2019,45(1):206-225)

[9] Yie A, Casallas R, Deridder D, et al. Realizing model transformation chain interoperability. Software & Systems Modeling, 2012, 11(1): 55-75

[10] Dalton A, Thomas D, Cheung P. Secret swapping: Two party fair exchange. IACR Cryptol. ePrint Arch. 2023 (2023): 585

[11] Feng L, Jiahao Z, Junjie Z, et al. Novel hash-time-lock-contract based cross-chain token swap mechanism of blockchain. Computer Science, 2022, 49(1): 336-344 (ih Chinese)
(刘峰，张嘉昊，周俊杰等. 基于改进哈希时间锁的区块链跨链资产交互协议. 计算机科学，2022,49(1): 336-344)

[12] Zakhary V, Agrawal D, El Abbadi A. Atomic commitment across blockchains. Proceedings of the VLDB Endowment, 2020,32(11): 1319-1331

[13] Lys L, Micoulet A, Potop-Butucaru M. Atomic cross chain swaps via relays and adapters//Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems. London, UK. 2020: 59-64

[14] Tian H, Xue K, Luo X, et al. Enabling cross-chain transactions: A decentralized cryptocurrency exchange Protocol. IEEE Transactions on Information Forensics and Security, 2021, 16: 3928-3941

[15] Malavolta G, Moreno-Sanchez P, Schneidewind C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability//Proceedings of the 2019 Network and Distributed System Security Symposium. San Diego, USA. 2019: 1-8

[16] Shitong Z, Bo Q, Haibin Z. Research on the protocol of multiple cross-chains based on the hash lock. Cyberspace Security, 2018, 9(11): 57-62+67 (ih Chinese)
(张诗童，秦波，郑海彬. 基于哈希锁定的多方跨链协议研究. 网络空间安全，2018,9(11): 57-62+67)

[17] Ge Zhonghui, Zhang Yi, Long Yu, et al. A high-concurrency multi-party off-chain payment scheme. Chinese Journal of Computers, 2021, 44(1): 132-146 (ih Chinese)
(葛钟慧，张奕，龙宇 等. 一种支持高并发的多人链下支付方案. 计算机学报，2021,44(1): 132-146)

[18] Han R, Lin H, Yu J. On the optionality and fairness of Atomic Swaps//Proceedings of the 1st ACM Conference on Advances in Financial Technologies. Zurich, Switzerland. 2019: 62-75

[19] Heilman E, Lipmann S, Goldberg S. The arwen trading protocols//Proceedings of the International Conference on Financial Cryptography and Data Security. Kota Kinabalu, Malaysia,2020: 156-173

[20] Tefagh M, Bagheriesfandabadi F, Khajehpour A, et al. Capital-free futures arbitrage. Researchgate, 2020. https://www.researchgate. net/publication/344886866_Capital-free_Futures_Arbitrage

[21] Xu J, Ackerer D, Dubovitskaya A. A game-theoretic analysis of cross-chain atomic swaps with HTLCs//Proceedings of the IEEE 41st International Conference on Distributed Computing Systems. Washington, USA. 2021: 584-594

[22] Xue Y, Herlihy M. Hedging against sore loser attacks in cross-chain transactions//Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing. Virtual, Italy. 2021: 155-164

[23] Jain A, Sikora R. A classification of auction mechanism:

Potentiality for Multi-Agent System (MAS) based modeling. SWDS 2006: 473-483

[24] Khajehpour A, Bagheri F, Abdi M. Demo paper: Atomic bonded cross-chain debt//Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency. Sydney, Australia. 2021: 1-3

[25] Belotti M, Moretti S, Potop-Butucaru M, et al. Game theoretical analysis of cross-chain swaps//Proceedings of the IEEE 40th International Conference on Distributed Computing Systems. Singapore, 2020: 485-495

[26] Nadahalli T, Khabbazian M, Wattenhofer R. Grief-free atomic swaps//Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency. Shanghai, China. 2022: 1-9

[27] Janin S, Qin K, Mamageishvili A, et al. FileBounty: Fair data exchange//Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops. Genoa, Italy. 2020: 357-366

[28] Ladóczki B, Bíró J, Tapolcai J. Stochastic analysis of the success rate in atomic swaps between blockchains//Proceedings of the 2022 4 th International Conference on Blockchain Computing and Applications. San Antonio, USA. 2022: 41-46

[29] Zhu Yan, Qin Bohan, Chen E, et al. An advanced smart contract conversion and its design and implementation for auction contract. Chinese Journal of Computers, 2021, 44(3): 652-668 (ih Chinese)
(朱岩，秦博涵，陈娥 等. 一种高级智能合约转化方法及竞买合约设计与实现. 计算机学报，2021,44(3): 652-668)

[30] Eckey L, Faust S, Schlosser B. OptiSwap: Fast optimistic fair exchange//Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. Taipei, China. 2020: 543-557

[31] Mazumdar S. Towards faster settlement in HTLC-based cross-chain atomic swaps//Proceedings of the IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications. Atlanta, USA. 2022: 295-304

[32] Deshpande A, Herlihy M. Privacy-preserving cross-chain atomic swaps//Proceedings of the Financial Cryptography and Data Security. Kota Kinabalu, Malaysia. 2020: 540-549

[33] Shen Meng, Che Zheng, Zhu Liehuang, et al. Anonymity in blockchain digital currency transactions: Protection and confrontation. Chinese Journal of Computers, 2023, 46(1): 125-146 (ih Chinese)
(沈蒙，车征，祝烈煌 等. 区块链数字货币交易的匿名性:保护与对抗. 计算机学报，2023,46(1): 125-146)

[34] Chung H, Masserova E, Shi E, et al. Ponyta: Foundations of side-contract-resilient fair exchange. Cryptology ePrint Archive, 2022

[35] Wang G, Wang Q, Chen S. Exploring blockchains interoperability: A systematic survey. ACM Computing Surveys, 2023, 55(13s): 1-38

[36] Jian W, Hang Y, Zhen H, et al. Access control methods of data sharing in cloud storage based on smart contract. Netinfo Security, 2021, 21(11): 40-47 (ih Chinese)
(王健，于航，韩臻 等. 基于智能合约的云存储共享数据访问控制方法. 信息网络安全，2021,21(11):40-47)

[37] Engel D, Xue Y. Transferable cross-chain options//Proceedings of the 4th ACM Conference on Advances in Financial Technologies. Cambridge, USA. 2022: 161-179

[38] Kechen Y, Li G, Hongwei Y, et al. The high-value data sharing model based on blockchain and game theory for data centers. Netinfo Security, 2022, 22(6): 73-85 (ih Chinese)
(于克辰，郭莉，阴宏伟 等. 面向数据中心场景的基于区块链与博弈论的高价值数据共享模型. 信息网络安全，2022,22(6):73-85)

[39] Zamyatin A, Harz D, Lind J, et al. XCLAIM: Trustless, interoperable, cryptocurrency-backed assets//Proceedings of the 2019 IEEE Symposium on Security and Privacy. San Francisco, USA. 2019:193-210

[40] Tefagh M, Bagheri F, Khajehpour A, et al. Atomic bonded cross-chain debt//Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications. Xi′an , China. 2020: 50-54

[41] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems//Proceedings of the 17 th annual ACM symposium on Theory of computing. Providence Rhode Island, USA. 1985: 291-304

[42] Rabin M O. How To Exchange Secrets with Oblivious Transfer. IACR Cryptol. ePrint Arch. 2005 (2005): 187

[43] Ping Z. Information and communication engineering[Ph. D. Thesis]. Hefei:University of Science and Technology of China, 2018
(张平. 认证加密方案的设计与分析[博士学位论文]. 合肥:中国科学技术大学，2018)

[44] Xiaomei L. The research and design of authenticated encryption scheme based on improved merkle-damgård construction[Ph.D. Thesis]. Lanzhou:Lanzhou Jiaotong University, 2017
(雷晓妹. 基于改进 Merkle-Damgård 结构的认证加密方案的研究与设计 [博士学位论文]. 兰州:兰州交通大学，2017)

[45] Lei Y, Xiaofang Z, Yi S, et al. Implementation of fair contract signing protocol based on blockchain technology. Journal of Software, 2020, 31(12): 3867-3879 (ih Chinese)
(于雷，赵晓芳，孙毅 等. 基于区块链技术的公平合约交换协议的实现. 软件学报，2020,31(12):3867-3879)

[46] Giacomelli I, Madsen J, Orlandi C. ZKBoo: Faster zero-knowledge for boolean circuits//Proceedings of the 25th USENIX Conference on Security Symposium. Austin, USA. 2016: 1069-1083

YU Yong, Ph. D, professor. His research interests include public key cryptography theory and applications, blockchain and cryptocurrencies, and cloud computing security.

YAO Yu-Chao, Ph. D. candidate. His research interests include blockchain and cryptocurrencies.

SHI Jun-Bin, Ph. D. His research interests include searchable encryption and cloud computing security.

YANG Hao Chen, Ph. D. candidate. His research interests include blockchain and decentralized identity.

Background

This research addresses the significant and timely issue of secure data ownership transfer within decentralized environments, an essential topic in blockchain security and data transfer protocols. The rising prominence of decentralized markets globally, especially those heavily reliant on smart contracts, has revealed critical challenges related to data asset liquidity. One prominent issue is the locking of assets within smart contracts until transactions are conclusively finalized, significantly reducing the fluidity and availability of data assets for immediate reuse or further transactions.

Internationally, extensive efforts have been invested in developing cryptographic protocols such as atomic swaps and fair secret exchange mechanisms. These protocols aim to facilitate secure and trustless transactions, enabling parties to exchange data assets without intermediary involvement. Despite these advancements, existing methods frequently encounter limitations concerning adaptability and flexibility. This is particularly evident in high-stakes scenarios involving data as collateral, where the rigidity of current protocols negatively impacts transaction fluidity and asset usability.

In response to these shortcomings, this paper proposes a novel integrated protocol that synergistically combines on-chain and off-chain processes to enhance data liquidity significantly. The proposed system innovatively facilitates data ownership transfer without imposing additional computational burdens on blockchain networks. The key to achieving this balance lies in the strategic application of zero-knowledge proofs, which verify participant identities securely and privately, alongside a robust two-party fair secret exchange mechanism. These tools collaboratively augment the functionality of smart contracts, making it possible to effectively manage ownership transitions for data assets even while they remain locked within contractual obligations.

Belonging to the broader field of decentralized finance research, this study represents an essential step forward in developing adaptable, secure transaction frameworks. By addressing core liquidity challenges, the proposed approach has substantial implications for the management of data assets in decentralized markets. Improved liquidity and efficient transaction processing facilitated by this protocol promise to enhance market dynamism and usability significantly.

Furthermore, this work builds upon previous research conducted by the team, notably in fair data exchange and privacy-preserving protocols. Prior studies laid critical groundwork in understanding and addressing fundamental barriers to efficient, secure data transactions. This current research expands on these foundations, introducing advanced mechanisms explicitly designed to mitigate issues related to data lock-in, thereby substantially improving transaction efficiency in decentralized financial systems. Overall, this protocol has the potential to transform data asset management in decentralized environments, unlocking unprecedented opportunities for asset reuse and market efficiency.

This work was supported by the National Cryptologic Science Fund of China(2025NCSF02025), the National Natural Science Foundation of China (Grant No. U24B20149, 62272385, U23A20302, 62311540156), the Key Industrial Innovation Chain Project of Shaanxi Province Key R&D Program (2024GX-ZDCYL-01-09), and the Distinguished Youth Science Foundation of Shaanxi Province(2022JC-47).