

基于可追责断言的支付通道网络性能优化研究

李雯琪¹, 应作斌¹, 臧嘉威¹, 熊金波^{2,3}, 刘西蒙⁴

(1. 澳门城市大学数据科学学院, 澳门 999078; 2. 福建师范大学计算机与网络空间安全学院, 福建 福州 350117;

3. 福建师范大学福建省网络安全与密码技术重点实验室, 福建 福州 350007;

4. 福州大学计算机与大数据学院, 福建 福州 350108)

摘要: 针对区块链技术在区块大小和生成速率上的固有限制导致的可扩展性问题, 支付通道网络 (payment channel network, PCN) 提供了链下扩容的有效方案。然而, 传统的使用可锁定结构的 PCN 存在以下两个缺点: 存在作恶方时该结构只能结束交易过程, 却无法对恶意行为者实施识别与惩罚; 某一笔交易需要复盘时, PCN 中出现的所有交易都需要恢复, 导致巨大的计算开销。鉴于此, 提出了一种基于可追责断言性能优化的支付通道网络方案——AAPO-PCN (accountable assertions performance optimization-payment channel network)。AAPO-PCN 通过引进可追责断言算法, 构建了一种可编辑的 Merkle 树结构。不同于传统 Merkle 树, 该方案采用变色龙哈希函数替换原有哈希算法, 并整合可追责断言机制, 旨在有效识别恶意用户。通过这种方式, 不仅令相关交易的恢复更加高效, 同时也大幅减少了计算开销。最后提供了全面的安全性分析与实验, 结果表明, AAPO-PCN 在不牺牲安全性的情况下, 具有更优的计算效率与通信开销。

关键词: 支付通道网络; 可追责断言; Merkle 树; 变色龙哈希函数

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025007

Performance optimization research of payment channel network based on accountable assertions

LI Wenqi¹, YING Zuobin¹, ZANG Jiawei¹, XIONG Jinbo^{2,3}, LIU Ximeng⁴

1. Faculty of Data Science, City University of Macau, Macau 999078, China

2. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China

3. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China

4. College of Computer and Data Science, Fuzhou University, Fuzhou 350108, China

Abstract: Restricted by block size and the block generation rate, cryptocurrencies like Bitcoin were unable to significantly improve their scalability through on-chain approaches. Payment channel networks (PCN) were recognized as one of the most important methods to achieve scalability through off-chain modes. However, traditional

收稿日期: 2024-05-27; 修回日期: 2025-01-20

通信作者: 应作斌, zbying@cityu.edu.mo

基金项目: 国家自然科学基金 (NSFC)-澳门科学技术发展基金 (FDCT) 联合科研项目 (0051/2022/AFJ)

Foundation Item: NSFC-FDCT under its Joint Scientific Research Project (0051/2022/AFJ)

引用格式: 李雯琪, 应作斌, 臧嘉威, 等. 基于可追责断言的支付通道网络性能优化研究[J]. 网络与信息安全学报, 2025, 11(1): 66-78.

Citation Format: LI W Q, YING Z B, ZANG J W, et al. Performance optimization research of payment channel network based on accountable assertions[J]. Chinese Journal of Network and Information Security, 2025, 11(1): 66-78.

PCN utilizing a lockable structure were found to have two major drawbacks. First, in the presence of malicious parties, this structure could only terminate the transaction process but could not identify or punish the malicious actors. Second, when a specific transaction needed to be reviewed, all transactions within the PCN had to be recovered, resulting in significant computational overhead. To address these issues, a scheme called accountable assertions performance optimization-payment channel network (AAPO-PCN) was proposed. In this scheme, an accountable assertion algorithm was introduced to construct an editable Merkle tree. Unlike the standard Merkle tree, the chameleon hash function was used to replace the original hash function, and accountable assertions were integrated to identify malicious users. This approach ensured that only the related transactions needed to be recovered, thereby improving efficiency. Finally, a comprehensive security analysis and experimental evaluation were conducted, demonstrating that AAPO-PCN achieved superior computational efficiency and reduced communication overhead without compromising security.

Keywords: payment channel network, accountable assertion, merkle tree, chameleon hash function

0 引言

近年来,随着互联网技术与金融领域的持续融合,基于区块链的“加密货币”日益受到关注。比特币等“加密货币”利用区块链在不信任方之间实现安全支付,其安全性依赖于一系列复杂的安全协议^[1-4]。然而,安全协议的复杂性限制了整体吞吐量^[5,6]。例如,比特币的交易速度不超过每秒6-7笔,远低于Visa的每秒最高47 000笔交易能力^[7]。同时,出于对安全和去中心化的考虑,比特币的区块大小最初被设定为1 MB,这限制了每10 min内可打包的交易数量通常约为4 000笔。这一限制使得比特币网络在链上扩展性方面受到约束^[8,9]。为缓解去中心化“加密货币”的可扩展性问题,已有的尝试包括优化共识机制和支付通道(payment channel, PC)/支付通道网络(PCN, payment channel network),后者在提升比特币的可扩展性方面已证明能达到95%的改进^[10-13]。

支付通道使交易双方能够在不公开区块链的私密环境下进行小额支付,这极大提升了“加密货币”系统的可扩展性^[14,15]。为了启动支付通道,双方需在区块链上公布其资金交易及存款信息。此后,支付通道开启,允许双方在链下执行通道内交易。交易中的支付通道资金上限等同于双方存款的总和。链外交易可以在不涉及上链的情况下调整交易双方间的资金配置。任一方均可通过将资金再次上链并将余额退回至各自账户的方式关闭PC。支付通道和支付通道网络有效提高了区块链的交易处理能力

并降低了交易确认的时延,因而被广泛应用于多方交易的支付^[16,17]。

对于支付通道而言,设想有两个用户Alice与Bob,他们通过向区块链提交首笔交易、设定交易期限,并在通道中锁定一定数额的资金,从而建立支付通道。在该模式下,Alice与Bob可通过调整链上硬币的数量来实现多次本地支付,而无须记录任何单一支付至链上。最终,Bob需在交易期限结束前,提交最后一笔交易至区块链以完成交易过程^[18]。

支付通道网络由众多支付通道组成,通过支付通道间多次跳跃(涉及多用户)实现资金的最终转移,解决了用户间直接共享支付通道的难题。此外,PCN还有望解决不同货币间潜在的跨境支付问题^[19,20]。

尽管支付通道网络拥有诸多优势,但在安全性方面仍存在一些挑战,如在多方处理中责任界定不明确^[21,22]。特别是在基于离线交易的PCN模型中,攻击者有机会利用这些场景进行洗钱等犯罪活动^[23]。例如,一个由4个用户Alice、Bob、Carol和Dave组成的PCN,其中Carol和Dave作为中介,帮助Alice向Bob支付款项。如果Alice、Carol和Dave中有恶意参与者,Bob可能无法收到Alice的支付。在这种情况下,难以确定PCN中的恶意参与者。

传统的PCN方案存在以下缺点。

1) 在传统PCN中,难以识别恶意参与者,导致无法对其进行惩罚^[24]。其问题在于系统无法确定是哪一方(发送方、中介方或接收方)行

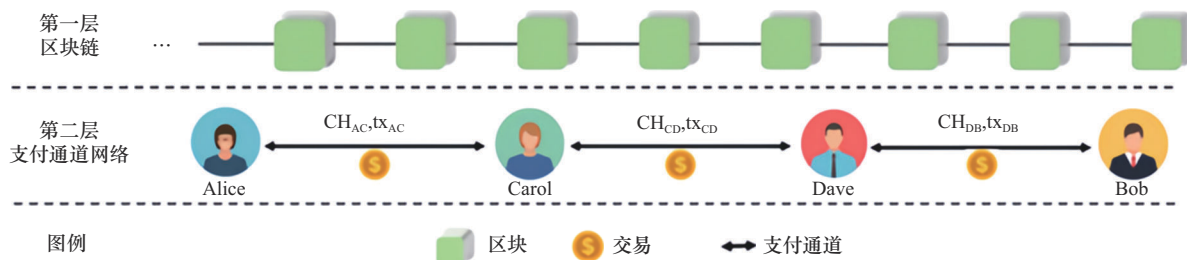


图1 传统PCN模型

Figure 1 Traditional PCN model

为不端。

2) 多数最新解决方案依赖于线性可锁定结构。PCN的安全性通过这些可锁定结构和签名来确保。虽然这种方法可以阻止可疑交易，但系统依旧无法识别恶意参与者。

3) 可锁定结构不可避免地降低了模型的计算效率。此外，它们也无法帮助识别恶意参与者^[25]。

为了解决这些问题，本文提出了基于可追责断言性能优化的支付通道网络方案——AAPO-PCN (accountable assertions performance optimization-payment channel network)，主要贡献如下。

1) 构建了一个高效且能识别与惩罚恶意行为用户的安全PCN。

2) 针对接收方在使用可锁定结构获取付款时面临的计算开销问题，AAPO-PCN通过使用变色龙哈希技术实现对相关交易的唯一恢复。

3) 实验评估显示，AAPO-PCN在不牺牲安全性的情况下，具有更优的计算效率。此外，采用AAPO-PCN不会增加区块链的计算或存储负担，且AAPO-PCN能够有效抵御多项式时间攻击。

1 相关工作

尽管区块链技术为“加密货币”交易提供了安全的基础，但其原生结构在处理大规模小额交易时表现出显著的性能瓶颈。为了解决这一核心问题，学者提出了状态通道的概念，这种技术允许在参与者间建立一个双向通道，通过在链下处理交易来显著提高系统的可扩展性^[26-30]。Plasma技术作为状态通道的一种拓展，通过创建子链在链下执行交易，进一步提高了交易处理的效率，子链的区块生成者会定期向主链提交区块状态证明，以确保所有的交易都能在必要时恢复到主链上的正确状态，提供了

一个有效的欺诈防御机制^[31]。

在比特币网络中，Poon等^[32]提出的闪电网络 (lightning network, LN) 利用状态通道和智能合约在链下执行大量交易，极大地提高了比特币的可扩展性。通过这种机制，只有初始和最终交易需要在区块链上记录，实现了高效的支付处理。然而，闪电网络未能提供支付匿名性^[15]，Green和Miers^[33]随后提出了Bolt协议，利用非交互式零知识证明和承诺方案，保护了交易的匿名性和金额的保密性。

近年来，研究人员进一步提出了跨区块链的资产交换协议^[34, 35]。例如，Thyagarajan等^[36]提出“通用原子互换”协议，该协议支持所有“加密货币”之间的安全交易，包括多资产的单次原子交换。这种技术通过适配器签名和时间锁谜题显著提高了交易的效率和安全性，使得跨不同区块链的资产交换成为可能，无须依赖于第三方。Guo等^[37]针对跨链操作提出了Cross-Channel，这是一个支持跨链服务的创新的分层通道结构。该结构支持公平和原子性操作，显著提高了跨链交易的效率和安全性，有效地减少了异步网络中的高延迟。Qin等^[38]开发的BlindHub则是一个支持变动金额的比特币兼容隐私保护支付通道枢纽，通过盲适配器签名和灵活的盲条件签名，确保交易双方关系和交易金额的匿名性，增强了支付通道的隐私保护能力。

尽管现有的支付通道和支付通道网络协议在阻止恶意交易以保护资金方面取得了进展，但这些方案往往难以有效追踪和惩罚作恶者^[39]。为解决此问题，Ruffing等^[40]提出了一种基于可解释断言的解决方案，利用保证金和密钥泄露机制，有效惩罚恶意用户。具体实现为付款人在交易开始之初放入一定数量的保证金以证实

其诚实可信。假设付款人模棱两可，即作出冲突的声明，那么付款人的密钥会被泄露，没收其保证金用以惩罚作恶。基于 Ruffing 等的方案，Tian 等^[41]在此基础上进行改进，提出了一种新的可解释断言结构，该结构允许一个断言被解释多次。此外，Avarikioti 等^[14]提出的 Cerberus 通道通过激励机制保护比特币网络中的交易安全。

在支付通道网络中，交易复盘通常需要回顾整个网络中的所有交易，导致计算开销过大。Smith 等^[42]提出了一种结合分片技术和动态 Merkle 树的方案，有效减少了复盘操作的计算负担。此外，Castellon 等^[43]提出了一种能量高效的 Merkle 树结构，进一步优化了链下支付通道的复盘效率。

然而，尽管现有研究在支付通道网络的隐私保护和安全性上做出了重要贡献，但它们在恶意行为者的追踪与惩罚方面仍然存在诸多不足，特别是在高效的追责机制和计算效率方面缺乏有效的解决方案。针对现有问题，本文提出了一种新型的 PCN 方案，通过引入责任断言的概念，不仅进一步保障了交易的安全性和隐私性，同时显著提高了计算效率，并为有效追踪和惩罚链中的作恶方提供了新的思路。

2 预备知识

2.1 可编辑的 Merkle 树

由 Ruffing 等^[40]提出的 Merkle 树可以有效处理具有指数规模节点数的数据集，而不需要对每个节点进行详尽的计算^[43]，其核心思想是运用变色龙哈希函数的特性来加速计算过程。在变色龙哈希函数中，给定随机选择的 x^* 和 r^* ，若已知公钥是声明方案的一部分，如 $\text{CH_Hash}(x^*; r^*)$ ，那么可以使用一个陷门来对某个语句 st 进行断言，即有

$$\text{CH_Hash}(x^*; r^*) = \text{CH_Hash}(x; r).$$

在 Merkle 树中计算节点 A_{ij} 时，最初的计算方法如下。

$$A_{ij} \leftarrow \text{CH_Hash}((A_{i+1}, S, B_{i+1}, S, C_{i+1}, S); r_{ij}).$$

通过将所有元素替换为虚拟元素的方法，可以将 A_{ij} 表达为 $\text{CH_Hash}(x_{ij}; r_{ij})$ 。这些元素是

通过带有密钥 k 的伪随机函数 F 导出的，即 $x_{ij} \leftarrow F_{k(i,j)}$ ^[43-45]。

2.2 变色龙哈希函数

变色龙哈希函数需满足的安全要求包括抗碰撞性、陷门碰撞性和语义安全性^[46, 47]。这些要求按以下方式分别定义。

1) 抗碰撞性：在没有陷门密钥 sk_{CH} 的情况下，对任何输入消息 m_1 ，随机数 r_1 以及消息 m_2 ，其中 $m_1 \neq m_2$ ，找不到一个整数 r_2 满足：

$$\text{CH_Hash}(m_1, r_1) = \text{CH_Hash}(m_2, r_2)$$

2) 陷门碰撞：在输入陷门密钥 sk_{CH} 之后，对任何消息 m_1 ，随机数 r_1 以及消息 m_2 ，其中 $m_1 \neq m_2$ ，能够计算出一个整数 r_2 满足：

$$\text{CH_Hash}(m_1, r_1) = \text{CH_Hash}(m_2, r_2)$$

3) 语义安全性：对任何消息 m_1, m_2 ，它们的变色龙哈希函数 $\text{CH_Hash}(m_1, r_1)$ 和 $\text{CH_Hash}(m_2, r_2)$ 的概率分布在计算上是无法区分的。

对于具有唯一密钥的变色龙哈希函数 $\text{CH} = (\text{CH_Gen}, \text{CH_Hash}, \text{CH_Col})$ ，如果存在一个确定性多项式时间算法满足以下条件，则可认为是安全的。

对所有由 CH_Gen 输出的密钥对 $(\text{pk}_{\text{CH}}, \text{sk}_{\text{CH}})$ 以及所有输入对 (m_1, r_1) 和 (m_2, r_2) ，如果满足 $\text{CH_Hash}(m_1, r_1) = \text{CH_Hash}(m_2, r_2)$ （其中 $m_1 \neq m_2$ ），则可以提取陷门密钥，并表达为 $\text{Extract_skCH}(\text{pk}_{\text{CH}}, m_1, r_1, m_2, r_2) = \text{sk}_{\text{CH}}$ 。

2.3 责任断言

责任断言用于判断用户在分布式协议中是否通过提出相互矛盾的断言来表明自己的诚实性。如果断言不一致，则认为该用户有不当行为，其他用户可提取其私钥并没收押金。如果断言一致，用户则被视为诚实，私钥将继续保密，并在交易结束后返还押金。责任断言涉及4个核心算法：密钥生成算法、断言算法、验证算法、提取算法。

1) 密钥生成算法：以安全性常数 λ 为输入，并生成公钥 pk 、私钥 sk 及辅助信息 sk_{aux} ，其中公钥 pk 与私钥 sk 是一一对应的。

$$\text{Gen}(1^\lambda) \rightarrow (\text{pk}, \text{sk}, \text{sk}_{\text{aux}}) \quad (1)$$

2) 断言算法: 输入私钥 sk 、辅助信息 sk_{aux} 、上下文 ct 以及声明 st , 输出责任断言 τ 或表示失败的符号 $\perp$ 。

$$\text{Assert}(sk, sk_{aux}, ct, st) \rightarrow \tau / \perp \quad (2)$$

3) 验证算法: 输入疑似不诚实用户的公钥 pk_S 、上下文 ct 、声明 st 以及责任断言 τ , 进行验证操作。如果验证过程中识别出了可疑用户, 算法输出 0; 反之, 输出 1。

$$\text{Verify}(pk_S, ct, st, \tau) \rightarrow \beta \quad (3)$$

4) 提取算法: 输入可疑用户的公钥 pk_S , 上下文 ct , 两个声明 st_0 、 st_1 和相应的两个责任断言 τ_0 、 τ_1 , 若存在责任, 则输出私钥 sk_S ; 否则输出 null。

$$\text{Extract}(pk_S, ct, st_0, st_1, \tau_0, \tau_1) \rightarrow sk_S / \text{null} \quad (4)$$

3 系统模型与定义

3.1 系统模型

在本文提出的多方交易系统中, 有 4 个实体: 交易发起者、交易接收者、第三方监管者和交易连接者。它们的特点如下:

1) 交易发起者是 PCN 中交易链的第一个用户, 负责初始化交易。交易发起者可能诚实或不诚实。如果他是诚实的, 首笔交易将按计划开始; 否则, 他将因为押金扣除受到惩罚。

2) 交易接收者是 PCN 中的最后一个用户和最终支付者。同样地, 他可以是诚实的或不诚实的, 并由第三方监管者进行规范。

3) 第三方监管者监督管理交易链中其他每个实体之间的交易。第三方监管者是可信的, 不能成为交易连接者。当在交易中检测到欺诈时, 第三方监管者在接收者的协助下惩罚恶意方。

4) 交易连接者连接整条交易链。一个交易的连接者是前一笔交易中的接收者以及下一笔交易中的发起者。它由构建交易链的不同用户组成, 并通过他们的个人多个支付通道实现。这些个体的诚实性与交易成功密切相关。然而, 交易连接者的数量庞大, 认为所有连接者都是诚实的是不切实际的。

通过第三方监管者可以在系统层面保证用户的诚实性。这意味着, 如果交易连接者不诚实, 他们会受到惩罚。

AAPO-PCN 系统模型如图 2 所示。

在 AAPO-PCN 中, 将区块链视为信息传输的媒介, 其交易验证信息被编入链上。近期的研究推进了链下支付的概念, 以提升区块链的可扩展性, 包括支付通道和支付通道网络。本文采用 PCN 协议来提高计算效率, 同时确保链下支付的安全性。在 AAPO-PCN 方案中使用的符号与表述如表 1 所示。

表 1 符号与表述

Table 1 Symbols and expressions

符号	描述
T	交易截止时间
$nLockTime$	押金锁定的当前持续时间
pk	用户的公钥
sk	用户的私钥
pk_{CH}	变色龙哈希函数的公钥
sk_{CH}	变色龙哈希函数的私钥
pk_S	可疑用户的公钥
sk_S	可疑用户的私钥
λ	安全参数
τ	断言
τ_0	对应用户生成的断言
τ_1	可疑用户生成的断言
ct	上下文
st	声明
st_0	变色龙哈希的私钥生成的声明
st_1	用户私钥生成的声明
sk_{aux}	辅助的秘密信息
β	布尔值

3.2 定义

AAPO-PCN 包含以下 5 种算法。

1) 密钥生成算法

$$\text{KeyGen}(1^\lambda) \rightarrow (pk, sk, pk_{CH}, sk_{CH}, sk_{aux})$$

该算法输入安全参数 λ , 输出用户在 AAPO-PCN 中的公/私钥对、变色龙哈希函数的公/私钥对, 以及辅助信息 sk_{aux} 。

2) 断言生成算法

$$\text{AssertGen}(ct, sk, sk_{CH}) \rightarrow (st_0, st_1)$$

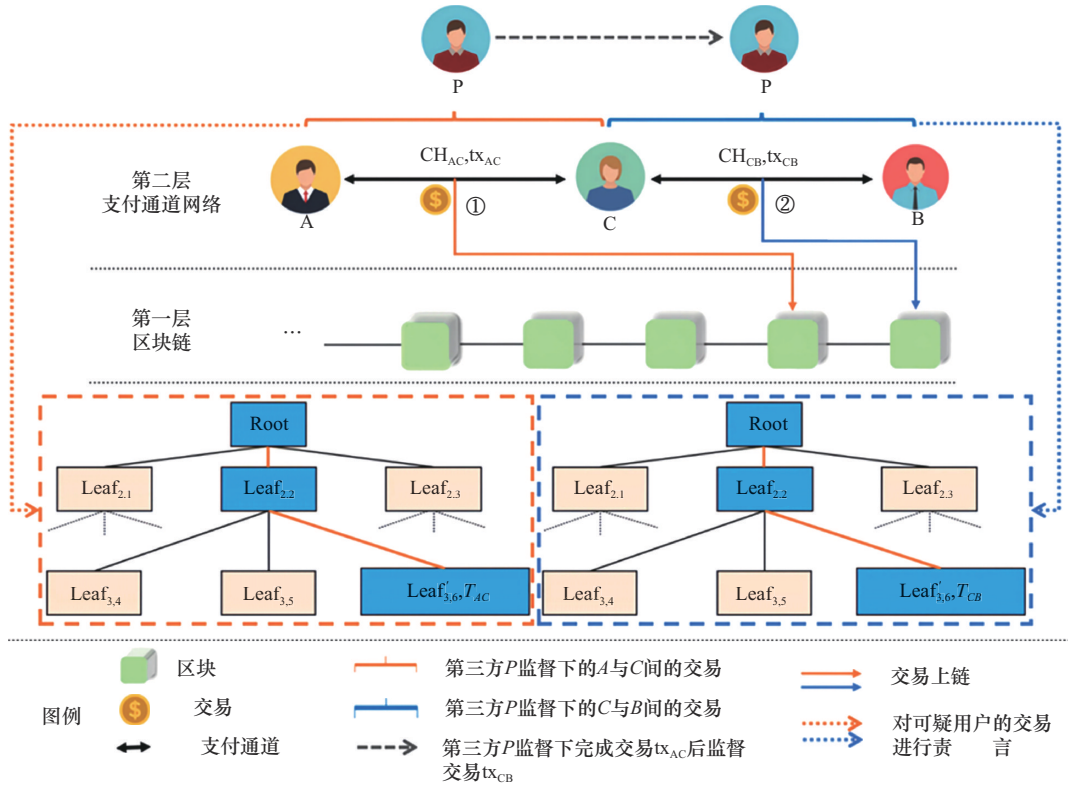


图2 AAPO-PCN 系统模型

Figure 2 AAPO-PCN system model

此算法以上下文 ct 、用户的私钥 sk 和变色龙哈希的私钥 sk_{CH} 为输入，生成两个声明 st_0 和 st_1 ，分别通过变色龙哈希的私钥和用户的私钥产生。

3) 断言算法

$$\text{Assert}(sk, sk_{aux}, ct, st) \rightarrow \tau / \perp$$

算法输入包括用户的私钥 sk 、辅助信息 sk_{aux} 、上下文 ct 和声明 st ，输出断言 τ 或失败标志 $\perp$ 。

4) 验证算法

$$\text{Verify}(pk_S, ct, st, \tau) \rightarrow \beta$$

验证算法取可疑用户的公钥 pk_S 、上下文 ct 、声明 st 和断言 τ 为输入，如果确认用户可疑，则输出 0；否则，输出 1。

5) 提取算法

$$\text{Extract}(pk_S, ct, st_0, st_1, \tau_0, \tau_1) \rightarrow sk_S / \text{null}$$

该算法以可疑用户的公钥 pk_S 、上下文 ct 、相应声明 st_0 及断言 τ_0 为输入，同时输入代表可疑用户的声明 st_1 和由其生成的断言 τ_1 ，如果确认用户可疑，则提取私钥 sk_S ；否则，返回空值 null 。

3.3 威胁模型

在本文的模型中，攻击者可能是 PCN 中扮演交易发送方角色的任一用户。对于攻击者而言，目标是在不失去押金的情况下不支付给接收方。对所有概率多项式时间 (ppt) 攻击者，他们将忽视本文设立的协议，以达到他们的作恶目的。然而，如果预期的损失大于预期的收益，他们不会冒着失去押金的风险。假设比特币的基本安全性，如比特币网络自身的限制计算能力，足以防范攻击者。

4 系统方案构造

4.1 AAPO-PCN 概述

AAPO-PCN 优先考虑提供一个安全且受监管的交易流程。设想一个交易发起方 A 和一个交易接收方 B，他们希望在公共环境中发起一个直接支付通道无法建立的交易。给定一个安全参数 λ ，满足：对应于 A 和 B 的支付通道的某些共同规范；可能是随机求和的结果，为 A 和 B 建立支付通道网络。在本文的模型中，可能有任意数量的

交易连接实体, 用 $\{\eta_1, \dots, \eta_n\} \in \Psi$ 来表示本节其余部分的所有交易连接者。

为了简化模型, 本文只包含一个交易连接者 C。正式地, 新交易过程包括以下 3 个阶段。

阶段 0: 选择 C, C 是集合 Ψ 中的一个元素。C 满足随机找到并同时存在与 A 和 B 建立支付通道的特性。

阶段 1: A 发起一个交易 T_1 并通过 PCN 与交易连接者 C 在第三方监管者 P 的监管下进行。

阶段 2: C 发起一个交易 T_2 并通过 PCN 与 B 在 P 的监管下进行。

为了消除潜在的安全威胁, 如双花攻击, 本文通过押金来保证每个参与方的诚实性。具体而言, 在交易开始前, 支付方 (如阶段 1 中的 A 和阶段 2 中的 C) 先将押金 d 转入公共资金池。除非交易被 P 确认无作恶行为, 否则这笔押金将不能回收。如果没有发现作恶, 押金将完整无损地退还给支付方。例如, 交易发起方 A 作恶, A 的押金 d_A 将被 P、B 和 C 得到; 或者交易连接者 C 在第 2 阶段作恶, 那么 C 的押金 d_C 将被 P、B 和 A 接管。

为了达到快速追责作恶方的目的, 本文运用责任断言。在交易由 A 向 C 转移的第一阶段, A 被授权使用公钥 pk_A 在上下文 ct_A 中为声明 st_A 生成断言 τ_A (其中, st 和 ct 可以是任意位串)。同理, 在交易由 C 到 B 的后续阶段, C 可使用公钥 pk_C 为声明 st_C 生成断言 τ_C 。

责任断言的设计是为了确认用户的诚实性, 并对不诚实的用户进行惩罚。若 A 诚实, 在 T 时间过后 A 可以使用其私钥 sk_A 取出他的押金; 若 A 作恶, 即 A 对于同一个上下文 ct_A 发表了两种不一致的声明 ($st_{A0} \neq st_{A1}$), 此时 C 与 P 能够利用 st_{A0} 、 st_{A1} 、 ct_A 、 τ_{A0} 、 τ_{A1} 提取 A 的私钥 sk_A , 并没收其押金。这笔押金之后会分配给涉及交易的 P、B 及 C, 作为对 A 作恶行为的惩罚。类似地, 若 C 在交易的第二阶段对 B 保持诚实, 则押金将由 C 保留; 反之, 若 C 行为不端, 则 B 和 P 将通过 st_{C0} 、 st_{C1} 、 ct_C 、 τ_{C0} 、 τ_{C1} 提取出 C 的私钥并没收 C 的押金。之后, 这笔押金将被分配给 A、B 和 P, 作为对 C 不当行为的惩罚。

4.2 AAPO-PCN 关键算法

本文方案涉及的关键算法如下。

1) 密钥生成算法

$$\text{KeyGen}(1^\lambda) \rightarrow (pk, sk, pk_{CH}, sk_{CH}, sk_{aux})$$

在 AAPO-PCN 中的密钥生成算法由两部分组成, 包括: 变色龙哈希函数的生成算法 $\text{CH_Gen}(1^\lambda) \rightarrow (pk_{CH}, sk_{CH})$, 责任断言的密钥生成算法 $\text{Gen}(1^\lambda) \rightarrow (pk, sk, sk_{aux})$ 。

定义 Merkle 树的高度为 h 、分支为 s , h 和 s 由树的性质决定。对于两笔交易 $A \rightarrow C$ 和 $C \rightarrow B$, 相应的值分别为 h_1 、 m_1 、 h_2 、 m_2 。设 F_k 为伪随机函数, H 为抗碰撞性变色龙哈希函数, S 和 L 为两个不同的哈希函数, 其中 L 定义为任意字符串到 $\{1, \dots, n^h\}$ 的映射。密钥由伪随机函数 $k \leftarrow \{0, 1\}^\lambda$ 得出。定义 q 为 Merkle 树根节点的标识。该标识用于定位并且是唯一的。Merkle 树根节点的计算应为 $x_i^1 \leftarrow F_k(p, i, 0)$ 及 $r_i^1 \leftarrow F_k(p, i, 1)$ 。责任断言的密钥设定为 $pk := pk_{CH}$ 、 $sk := sk_{CH}$ 、 $sk_{aux} := k$ 。

2) 断言生成算法

$$\text{AssertGen}(ct, sk, sk_{CH}) \rightarrow (st_0, st_1)$$

此算法上下文 ct 和声明 st 都是任意的位串。该算法根据用户私钥生成 st_1 , 根据变色龙哈希函数生成 st_0 。

3) 断言算法

$$\text{Assert}(sk, sk_{aux}, ct, st) \rightarrow \tau / \perp$$

此算法的主要思想是利用变色龙哈希的特性以快速计算。对于随机选择的 x^* 和 r^* , 如果公钥负责声明方案 $\text{CH_Hash}(x^*; r^*)$, 则可利用陷门计算 r 使其作为声明 st 的断言, 即

$$\text{CH_Hash}(x^*; r^*) = \text{CH_Hash}(x; r)$$

状态断言算法维护已用叶子节点位置的初始空集合 L 。断言算法中的 Merkle 树将其初始集合 L 设为空集合, 用于叶子节点的后续使用。断言算法的本质在于确认 ct 中的 st 是否一致。当 $L(ct)$ 不属于集合 L 时, 将其添加到集合 L 中。该算法通过断言快速计算从叶子节点 V_h 到根节点 V_1 的路径, 即

$(V_h, a_h) \rightarrow (V_{h-1}, a_{h-1} \rightarrow \dots \rightarrow (V_1, a_1))$ (其中, $v_i^1 = \text{CH_Hash}(x_i^1; r_i^1), i \in \{1, \dots, m\}$)。

$a_j \in \{1, \dots, n\}$ 定义了叶节点中不同交易的具体位置。节点 $V_j = (v_1^j, \dots, v_n^j)$ 存储了 n 个交易。 $V_j = (v_1^j, \dots, v_n^j)$ 对于包含上下文 ct 的叶节点 V_h , 其值存储为 $L(ct)$ 。对应不同交换的哈希值将按从左到右、从低到高的顺序排列在底部叶节点中。设 $x_i^j = F_k(q_j, i, 0)$ 和 $r_i^j = F_k(q_j, i, 1)$, 其中 q_j 是节点 V_j 位置的唯一标识符。

断言计算可分为两部分。首先, 在叶子节点 V_h 中计算与 st 对应的值。

$$x_{a_h}^h \leftarrow \text{CH_Col}(\text{sk}_{\text{CH}}, x_{a_h}^h; r_{a_h}^h, S(st))$$

通过利用变色龙哈希函数的陷门碰撞特性, 有 $\text{CH_Hash}(x_{a_h}^h; r_{a_h}^h) = x_{a_h}^h = \text{CH_Hash}(S(st); r_{a_h}^h)$ 。

对于该叶子节点 V_h 中的其余计算

$$v_i^h = \text{CH_Hash}(x_i^h; r_i^h), i \in \{1, \dots, m\}$$

叶子节点 V_h 存储条目 $(v_1^h, \dots, v_n^h)$ 。设 $f_h = (y_1^h, \dots, y_{a_h-1}^h, y_{a_h+1}^h, \dots, y_n^h)$ 。

利用变色龙哈希陷门的特性, 可以得出断言 $\tau := (r_{a_h}^h, f_h, a_h, \dots, r_1^1, f_1, a_1)$ 。

4) 验证算法

$$\text{Verify}(\text{pk}_S, \text{ct}, \text{st}, \tau) \rightarrow \beta$$

该算法验证由变色龙哈希函数生成的公钥 pk_{CH} 是否有效。如果有效, 算法输出 1; 否则, 输出 0。验证算法通过解析断言算法生成的 $\tau := (r_{a_h}^h, f_h, a_h, \dots, r_1^1, f_1, a_1)$ 重建 Merkle 树, 并通过快速计算变色龙哈希特性, 使交易中涉及的节点 $(V_h, V_{h-1}, \dots, V_1)$ 从叶节点 V_h 顺序恢复到根节点 V_1 。验证算法将检查其有效性。

5) 提取算法

$$\text{Extract}(\text{pk}_S, \text{ct}, \text{st}_0, \text{st}_1, \tau_0, \tau_1) \rightarrow \text{sk}_S / \text{null}$$

该算法首先恢复断言路径。提取算法通过找到 $\text{CH_Hash}(x_0; r_0) = \text{CH_Hash}(x_1; r_1)$ 在 Merkle 树中形成哈希碰撞的位置。提取算法通过使用变色龙哈希函数的陷门 sk_{CH} 提取恶意用户的私钥 sk_S ,

计算式如下。

$$\text{sk}_S = \text{sk}_{\text{CH}} \leftarrow \text{Extract}(\text{pk}_a, \text{ct}, \text{st}_0, \text{st}_1, \tau_0, \tau_1)$$

如果在 Merkle 树中无法找到形成哈希碰撞的位置, 提取算法将输出 null。

算法 1: AAPO-PCN 方案全局算法

Set: $\lambda, C_{C0}, C_{C1}, C_{B0}, C_{B1}, \text{sk}_A, \text{sk}_C$

Input: λ

Output: $\text{sk}_A, \text{sk}_C, \text{null}$

if $C_{C0} = C_{C1}$ **then**

do (KeyGen, AssertGen, Assert, Verify)

if $\text{Verify}(\text{pk}_A, \text{ct}, \text{st}, \tau_A) = 0$ **then**

$\text{sk}_A = \text{Extract}(\text{pk}_A, \text{ct}_A, \text{st}_{A0}, \text{st}_{A1}, \tau_{A0}, \tau_{A1})$

return sk_A

else $\text{Verify}(\text{pk}_A, \text{ct}, \text{st}, \tau_A) = 1$ **then**

return null

end

else if $C_{B0} = C_{B1}$ **then**

do (Gen, Assert, Verify)

if $\text{Verify}(\text{pk}_C, \text{ct}, \text{st}, \tau_C) = 0$ **then**

$\text{sk}_C = \text{Extract}(\text{pk}_C, \text{ct}_C, \text{st}_{C0}, \text{st}_{C1}, \tau_{C0}, \tau_{C1})$

return sk_C

else $\text{Verify}(\text{pk}_C, \text{ct}, \text{st}, \tau_C) = 1$ **then**

return null

end

end

AAPO-PCN 算法流程如图 3 所示。

5 分析与评估

5.1 安全性分析

在 AAPO-PCN 中, 假设攻击者是交易中的恶意发送者或中间接收者, 通过模棱两可的方式拒绝支付交易费用, 并且不损失押金。PCN 中的攻击者可以使用任何形式的拒绝原方案的方法来实现这一目标, 但如果预期损失大于预期收益, 则没有失去押金的危险。在本文中, 假设攻击者无法破坏比特币的基本安全性, 如攻击者不拥有比特币网络中的大部分计算能力。

本文重点关注操作的初始发起者和中间接收者为恶意的情况。特别地, 假设恶意交易的初始发起者和中间接收者可以积极地进行模棱两可的

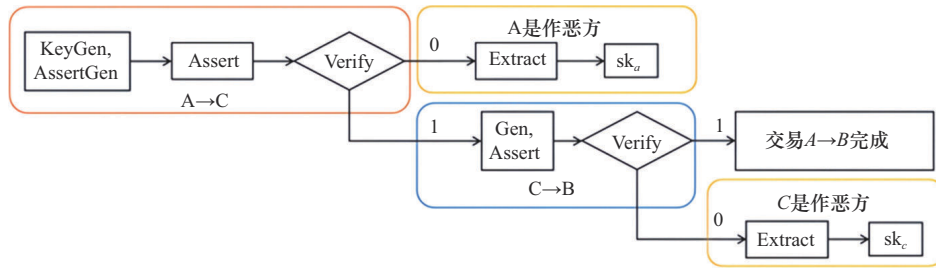


图3 AAPO-PCN算法流程

Figure3 AAPO-PCN algorithm flow

操作，而第三方监管者保持可信。恶意的初始发起者和恶意的中间接收者可以采用各种已知的模棱两可的方法。

AAPO-PCN中的可追责断言具有两个安全特性：可提取性和保密性。第一个可提取性规则指出，只要在相同上下文中声明了两个不同的声明，就可以提取密钥。对于概率多项式时间算法攻击者A或者C，定义了以下条件。

$$\Pr [\text{Extract}(\text{pk}_A, \text{ct}, \text{st}_0, \text{st}_1, \tau_0, \tau_1) \neq \text{sk}_A \wedge \forall b \in \{0, 1\}, \text{Verify}(\text{pk}_A, \text{ct}, \text{st}_B, \tau_B) = 1 \wedge \text{st}_0 \neq \text{st}_1 : (\text{pk}_A, \text{ct}, \text{st}_0, \text{st}_1, \tau_0, \tau_1) \leftarrow A(1^\lambda)]$$

保密性防止攻击者提取密钥，攻击者可以要求挑战者在选定的上下文中断言选定的声明。由于可追责断言具有可提取性，因此攻击者在要求从相同上下文中的两个不同声明中提取断言后将被排除。

5.2 实验设置

本节详细介绍实验的环境、参数以及测试场景，旨在通过并行计算时间和资源消耗来评估AAPO-PCN的性能。

以三方交易为例，本文模拟了多个三方PCN，并测试了不同参与者在计算效率提升和通信复杂性降低方面的时间和存储成本，以评估AAPO-PCN的有效性。

实验的第一步是创建一个由3个支付通道组成的网络，并建立一个第三方监管者，以监控整个交易过程中恶意行为的发生。然后，各个发送者的押金被锁定在公共资金池中。为了在交易过程中快速找到中止交易的路径，本文基于Merkle树的责任断言进行快速计算。

实验中，快速识别并惩罚交易中的恶意用户是关键。本文使用了“libsecp256k1”库，该

库由标准比特流客户端演变而来。为了与比特币密钥兼容，在一阶椭圆曲线上设计了128位安全级别。实验运行在2.40 GHz Intel Xeon E5-2680 v4处理器和64GB DDR4-1866 RAM的机器上，操作系统为Ubuntu 20.04 LTS。在此平台上，变色龙哈希评估使用私钥的计算时间需求为66 μs，而仅使用公钥时，则计算时间增加到85 μs。NVMe固态硬盘的高效存储进一步提升了数据读写效率，确保了整个实验过程的流畅。

5.3 实验结果

本文对AAPO-PCN方案的各个步骤进行了详细的计算时间分析，并与Ruffing等^[40]方案进行对比，结果如图4所示。

图4(a)展示了AAPO-PCN方案在断言阶段的计算时间。AAPO-PCN方案在不同周期数下表现出高效的计算性能，尤其是在10 000个周期的实验中，其平均计算时间为5.903 ms。实验结果表明，AAPO-PCN在保证安全性的同时，实现了对责任断言的高效处理。

图4(b)展示了AAPO-PCN方案在验证阶段的运行时间。AAPO-PCN方案在多个周期内均保持较低的计算开销，10 000个周期下的运行时间为2.701 ms，证明了该方案在多跳支付场景中的验证操作具有较高的效率。

图4(c)展示了AAPO-PCN方案在提取阶段的运行时间。实验数据显示，AAPO-PCN方案在提取操作中具备稳定的性能优化。在10 000个周期下，运行时间为5.988 ms，体现了方案在复杂多方支付场景中对提取操作的有效加速。这说明AAPO-PCN不仅能够处理大规模的交易场景，还能在确保安全性的前提下，进一步提升整体计算效率。

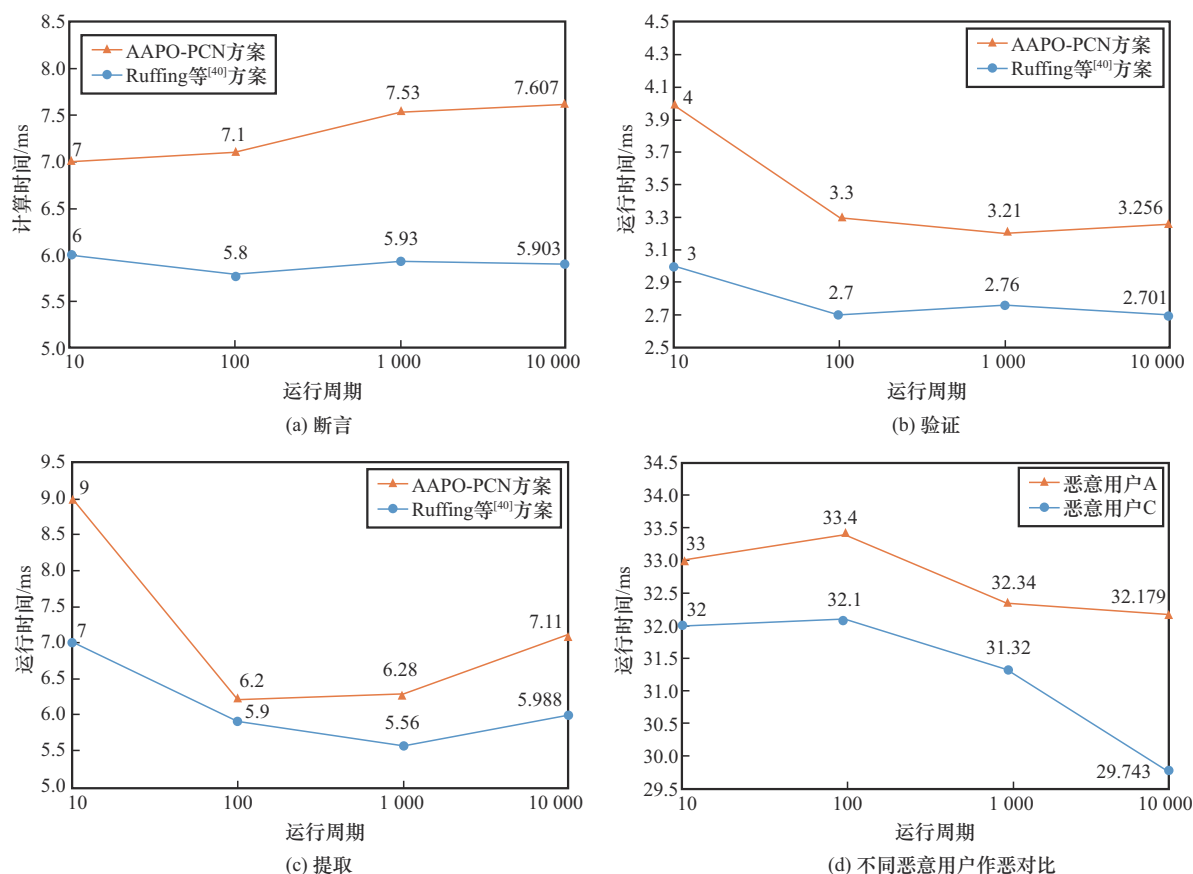


图4 AAPO-PCN实验对比

Figure 4 AAPO-PCN experimental comparison

图4(d)展示了在存在恶意用户的情况下，AAPO-PCN方案的运行时间。实验结果表明，在应对恶意行为的多方支付场景中，AAPO-PCN能够有效减少计算时间。在10 000个周期的实验中，运行时间为29.743 ms，表现出在恶意用户存在下的良好处理能力。

通过图4的实验结果可以看出，AAPO-PCN方案在各个阶段的计算性能均保持较高效率，特别是在多方交易和复杂场景中，其计算时间和系统开销表现出优异的优化效果。

目前大多数的研究中，PCN中的安全性是通过锁结构签名的方式提供的。图5展示了AAPO-PCN方案与锁结构的BLS签名PCN方案和锁结构的ECDSA签名PCN方案在运行时间上的对比。实验结果显示，AAPO-PCN方案的平均运行时间为33.4 ms，相较于其他方案，AAPO-PCN降低了运行时间，体现出其在计算效率上的优势。

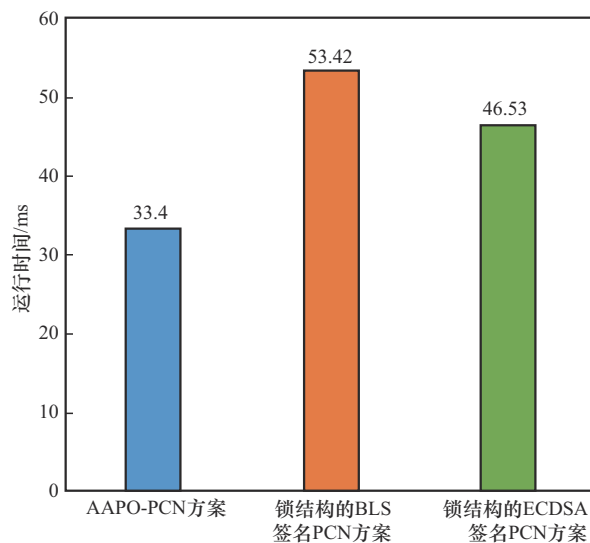


图5 不同PCN运行时间比较

Figure 5 Comparison of running time of different PCN

图6展示了关键算法与不同系统的通信开销对比。在不同的周期测试中，AAPO-PCN方案的通信开销明显低于文献[48]方案。特别是在多跳支付

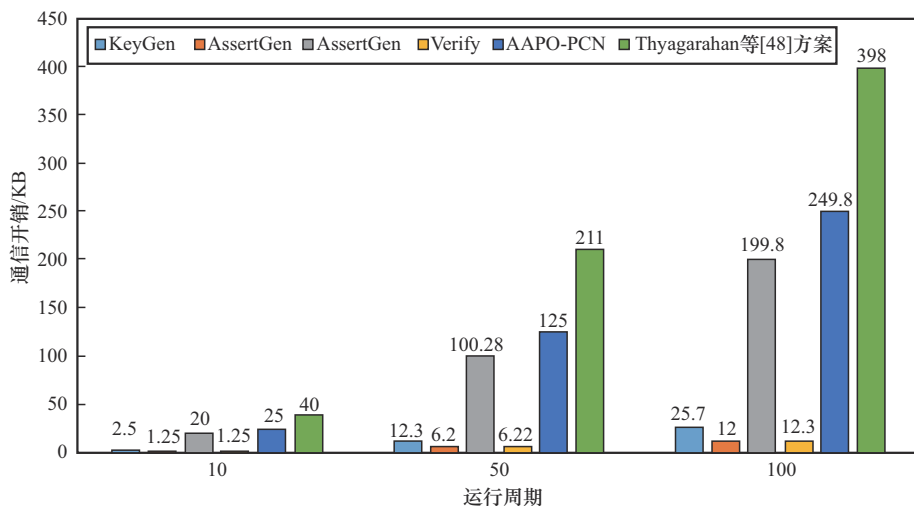


图6 关键算法与不同系统的通信开销对比

Figure 6 Comparison of communication overhead of key algorithms and different systems

场景中, AAPO-PCN通过减少签名验证的复杂度,有效降低了网络通信负担,减少了通信开销。

AAPO-PCN方案的优化主要体现在对签名验证过程的简化以及多方交易中的高效性。通过减少复杂的签名计算开销, AAPO-PCN能够在大规模、多方交易场景中保持较低的系统负载,同时确保安全性。此外, AAPO-PCN的设计进一步增强了应对恶意行为的能力,从而提高了方案的整体安全性。

从实验结果可以看出, AAPO-PCN方案不仅在运行时间上表现出明显优势,而且在应对不同规模的交易时均表现出稳定的性能。这表明AAPO-PCN适合在实际应用中部署,能够有效提升PCN的整体效率。

6 结束语

PCN解决了“加密货币”扩展性差的问题。然而,传统的PCN容易受到恶意方的攻击,从而危及交易的安全性。大多数现有的具有安全保证的PCN使用签名和锁结构。这些方法虽然确保了PCN的安全性,但会导致巨大的计算开销。本文提出了一种基于可追责断言的支付通道网络方案,分析了该方案的安全性。同时实验结果表明, AAPO-PCN在不牺牲安全性的情况下,具有更优的计算效率与通信开销。

未来的研究将着重于结合零知识证明技术,进一步提升AAPO-PCN在隐私保护与责任追踪

方面的平衡性。在保障交易双方隐私的同时,确保责任追踪机制的有效性,以应对复杂交易场景中可能出现的隐私泄露风险。通过引入更高效的隐私增强技术, AAPO-PCN有望在保持高效计算性能的基础上,提供更为全面的隐私保护能力。

参考文献:

- [1] KHAN N, STATE R. Lightning network: A comparative review of transaction fees and data analysis[C]//International Congress on Blockchain and Applications. 2019: 11-18.
- [2] AUMAYR L, MAFFEI M, ERSOY O, et al. Bitcoin-compatible virtual channels[C]//2021 IEEE Symposium on Security and Privacy (SP). 2021: 901-18.
- [3] FLORIAN M, HENNINGSSEN S, BEAUCAMP S, et al. Erasing data from blockchain nodes[C]//2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 2019: 367-376.
- [4] WOOD G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151: 1-32.
- [5] AVARIKIOTI Z, KOKORIS-KOGIAS E, WATTENHOFFER R, et al. B rick: Asynchronous incentive-compatible payment channels[C]//Financial Cryptography and Data Security: 25th International Conference, 2021: 209-230.
- [6] ZYSKIND G, NATHAN O. Decentralizing privacy: Using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops. 2015: 180-184.
- [7] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in bitcoin[C]//Financial Cryptography and Data Security: 19th International Conference, 2015: 507-527.
- [8] MIAO Y, DENG R H, CHOO K-K R, et al. Optimized verifiable fine-grained keyword search in dynamic multi-owner settings[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 18(4): 1804-1820.

- [9] MIAO Y, DENG R H, LIU X, et al. Multi-authority attribute-based keyword search over encrypted cloud data[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 18(4): 1667-1680.
- [10] ZHANG Z, ZHU D, FAN W. Qpbf: Practical byzantine fault tolerance consensus algorithm based on quantified-role[C]//2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2020: 991-997.
- [11] AVARIKIOTI Z, PIETRZAK K, SALEM I, et al. Hide & seek: Privacy-preserving rebalancing on payment channel networks[C]//International Conference on Financial Cryptography and Data Security. 2022: 358-373.
- [12] TIKHOMIROV S, MORENO-SANCHEZ P, MAFFEI M. A quantitative analysis of security, anonymity and scalability for the lightning network[C]//2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 2020: 387-396.
- [13] PAPADIS N, TASSIULAS L. State-dependent processing in payment channel networks for throughput optimization[J]. arXiv Preprint arXiv:210317207, 2021.
- [14] AVARIKIOTI Z, THYFRONITIS LITOS O S, WATTENHOFER R. Cerberus channels: Incentivizing watchtowers for bitcoin[C]//Financial Cryptography and Data Security: 24th International Conference, 2020: 346-366.
- [15] 刘懿中, 姜楠, 陈若楠, 等. 区块链链下通道研究综述[J]. 密码学报, 2024, 11(1): 45-66.
- LIU Y Z, JIANG N, CHEN R N, LIU J W. Overview on blockchain off-chain channels[J]. Journal of Cryptologic Research, 2024, 11(1): 45-66.
- [16] BAGARIA V, NEU J, TSE D. Boomerang: Redundancy improves latency and throughput in payment-channel networks[C]//International Conference on Financial Cryptography and Data Security. 2020: 304-324.
- [17] VAN DAM G, KADIR R A, NOHUDDIN P N, et al. Improvements of the balance discovery attack on lightning network payment channels[C]//IFIP International Conference on ICT Systems Security and Privacy Protection. 2020: 313-323.
- [18] MALAVOLTA G, MORENO-SANCHEZ P, KATE A, et al. Concurrency and privacy with payment-channel networks[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 455-471.
- [19] DZIEMBOWSKI S, ECKEY L, FAUST S, et al. Perun: Virtual payment hubs over cryptocurrencies[C]//2019 IEEE Symposium on Security and Privacy (SP). 2019: 106-123.
- [20] MILLER A, BENTOV I, BAKSHI S, et al. Sprites and state channels: Payment networks that go faster than lightning[C]//International Conference on Financial Cryptography and Data Security. 2019: 508-526.
- [21] YU X, THANG M S, LI Y, et al. Collusion attacks and fair time-locked deposits for fast-payment transactions in Bitcoin[J]. Journal of Computer Security, 2019, 27(3): 375-403.
- [22] MIZRAHI A, ZOHAR A. Congestion attacks in payment channel networks[C]//International Conference on Financial Cryptography and Data Security. 2021: 170-188.
- [23] ROHRER E, TSCHORSCH F. Counting down thunder: Timing attacks on privacy in payment channel networks[C]//Proceedings of the 2nd ACM Conference on Advances in Financial Technologies. 2020: 214-227.
- [24] KHALIL R, GERVAIS A. Revive: Rebalancing off-blockchain payment networks[C]//Proceedings of the 2017 ACM Sigsac Conference on Computer and Communications Security. 2017: 439-453.
- [25] GENNARO R, GENTRY C, PARNO B, et al. Quadratic span programs and succinct NIZKs without PCPs[C]//Advances in Cryptology - EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2013: 626-645.
- [26] YU B, LI X, ZHAO H. Virtual block group: A scalable blockchain model with partial node storage and distributed hash table[J]. The Computer Journal, 2020, 63(10): 1524-1536.
- [27] YUB, KERMANSHAHISK, SAKZADA, et al. Chameleon hash time-lock contract for privacy preserving payment channel networks[C]//Provable Security: 13th International Conference, 2019, 303-318.
- [28] FAN S, CHEN Y. Editable blockchain scheme based on shamir chameleon hash secret sharing[C]//2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC). 2022: 1125-1128.
- [29] TRIPATHY S, MOHANTY S K. Mappcn: Multi-hop anonymous and privacy-preserving payment channel network[C]//International Conference on Financial Cryptography and Data Security. 2020: 481-495.
- [30] 解岩凯, 魏凌波, 张驰. 面向区块链轻节点的支付通道瞭望塔技术研究[J]. 密码学报, 2021, 8(5): 778-794.
- XIE Y K, WEI L B, ZHANG C, WANG Q T, SUN Q B. On watchtower of payment channel for blockchain light nodes[J]. Journal of Cryptologic Research, 2021, 8(5): 778-794.
- [31] POON J, BUTERIN V. Plasma: Scalable autonomous smart contracts[M]. White paper, 2017: 1-47.
- [32] POON J, DRYJA T. The bitcoin lightning network: Scalable off-chain instant payments[EB]. 2016.
- [33] GREEN M, MIERS I. Bolt: Anonymous payment channels for decentralized currencies[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 473-489.
- [34] 郭朝, 郭帅印, 张胜利, 等. 区块链跨链技术分析[J]. 物联网学报, 2020, 4(2): 35-48.
- GUO Z, GUO S Y, ZHANG S L, SONG L Y, WANG H. Analysis of cross-chain technology of blockchain[J]. Chinese Journal on Internet of Things, 2020, 4(2): 35-48.
- [35] 康博涵, 章宁, 朱建明. 基于区块链的智能服务交易跨链服务框架与通信机制[J]. 网络与信息安全学报, 2021, 7(3): 105-114.
- KANG B H, ZHANG N, ZHU J N. Research on inter-blockchain service framework and communication mechanism based on smart service transaction[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 105-114.
- [36] THYAGARAJAN S A, MALAVOLTA G, MORENO-SANCHEZ P. Universal atomic swaps: Secure exchange of coins across all blockchains[C]//2022 IEEE Symposium on Security and Privacy (SP). 2022: 1299-1316.
- [37] GUO Y, XU M, YU D, et al. Cross-channel: Scalable off-chain

channels supporting fair and atomic cross-chain operations[J]. IEEE Transactions on Computers, 2023.

- [38] QIN X, PAN S, MIRZAEI A, et al. Blindhub: Bitcoin-compatible privacy-preserving payment channel hubs supporting variable amounts[C]//2023 IEEE Symposium on Security and Privacy (SP). 2023: 2462-2480.
- [39] 刘峰, 张嘉溟, 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[J]. 计算机科学, 2022, 49(1): 336-344.
LIU F, ZHANG J H, ZHOU J J, et al. Novel Hash-time-lock-contract based cross-chain token swap mechanism of blockchain[J]. Computer Science, 2022, 49(1): 336-344.
- [40] RUFFING T, KATE A, SCHRÖDER D. Liar, liar, coins on fire! Penalizing equivocation by loss of bitcoins[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. 2015: 219-230.
- [41] TIAN Y, LI Y, SENGUPTA B, et al. Anonymous asynchronous payment channel from k-time accountable assertion[C]//Cryptology and Network Security: 18th International Conference (CANS 2019). 2019: 512-524.
- [42] SMITH C, RUSNAK A. Dynamic Merkle B-tree with efficient proofs[J]. arXiv preprint arXiv:200601994, 2020.
- [43] CASTELLON C, ROY S, KREIDL P, et al. Energy efficient merkle trees for blockchains[C]//2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2021: 1093-1099.
- [44] JOURENKO M, LARANGEIRA M, TANAKA K. Payment trees: Low collateral payments for payment channel networks[C]//Financial Cryptography and Data Security: 25th International Conference, 2021: 189-208.
- [45] LEE D, PARK N. Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree[J]. Multimedia Tools and Applications, 2021, 80(26): 34517-34534.
- [46] ALFAIDI A, SEMWAL S. The right to be forgotten: Privacy and security in blockchain with multi-authority based chameleon hash function map-abch solution[C]//Future of Information and Communication Conference. 2022: 861-876.
- [47] ZHANG Y, YANG D, XUE G. Cheapay: An optimal algorithm for fee minimization in blockchain-based payment channel networks[C]//ICC 2019-2019 IEEE international conference on communications 2019: 1-6.
- [48] THYAGARAJAN S A K, MALAVOLTA G. Lockable signatures for blockchains: Scriptless scripts for all signatures[C]//2021 IEEE Symposium on Security and Privacy. 2021: 937-954.

[作者简介]



李雯琪 (1999-), 女, 山东枣庄人, 澳门城市大学博士生, 主要研究方向为区块链理论及应用。



应作斌 (1982-), 男, 安徽芜湖人, 澳门城市大学副教授, 主要研究方向为区块链理论及应用、隐私计算、云边缘协同安全。



臧嘉威 (1998-), 男, 山东平度人, 主要研究方向为中等规模轻工业物联网。



熊金波 (1981-), 男, 湖南益阳人, 博士, 福建师范大学教授, 主要研究方向为安全深度学习、移动群智感知、隐私保护技术。



刘西蒙 (1988-), 男, 陕西西安人, 博士, 福州大学教授、博士生导师, 主要研究方向为密码学与人工智能安全。