基于博弈论和可验证共识的防合谋跨链交易方案

贾雪丹[1,2]，王良民[3]，黄龙霞[4]

（1.海南师范大学信息科学技术学院，海南 海口 571158；2.海南师范大学扩展现实与数智教育海南省工程研究中心，海南 海口 571158；3.东南大学区块链应用监管教育部工程研究中心，江苏 南京 211189；4.江苏大学计算机科学与通信工程学院，江苏 镇江 212013）

摘　要：现有的跨链交易方案缺乏对跨链合谋问题的考虑。为此，提出防合谋跨链通道，实现可扩展的防合谋跨链交易。首先，提出跨多中继链通道建立方法，为任意业务链用户创建包含跨链交易双方和中继链观察者的链下通道，实现隐私保护的可扩展跨链交易。其次，设计基于博弈激励的防合谋跨链交易协议，刺激合谋者之间的不信任以防止跨链通道用户合谋，保障跨链交易的安全性。最后，提出基于通道状态证明的分层可验证跨链共识方法，实现安全跨链结算。对引发的参与方博弈进行了形式化分析，证明在合理假设下，所提方案保证不合谋是通道用户的主导策略。通过实验表明，所提方案在防范跨链用户合谋的同时实现了高跨链吞吐率，与传统中继跨链方案相比具备可扩展性。

关键词：区块链；跨链交易；安全协议；防合谋

中图分类号：TP393

文献标志码：A

DOI：10.11959/j.issn.1000–436x.2024202

Collusion-resistant cross-chain transaction scheme based on game theory and verifiable consensus

JIA Xuedan[1,2], WANG Liangmin[3], HUANG Longxia[4]

1. School of Information Science and Technology, Hainan Normal University, Haikou 571158, China
2. Hainan Engineering Research Center for Extended Reality and Digital Intelligent Education, Hainan Normal University, Haikou 571158, China
3. Blockchain Application Supervision Engineering Research Center of the Ministry of Education, Southeast University, Nanjing 211189, China
4. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China

Abstract: Existing cross-chain transaction solutions often overlook the issue of cross-chain collusion. In response, the counter-collusion cross-channel was proposed to facilitate scalable and collusion-resistant cross-chain transactions. Firstly, a strategy for establishing multiple-relay channels was introduced, including relay chain observers. These channels serve as off-chain pathways connecting users from different business chains, thereby facilitating private and scalable cross-chain transactions. Secondly, a collusion-resistant cross-chain transaction protocol based on game-theoretic incentives was designed, stimulating distrust among colluders to deter cross-chain collusion and uphold transaction security. Thirdly, a layered verifiable cross-chain consensus method was proposed, relying on channel state proofs to ensure secure cross-chain settlement. Formal analyses of participant game dynamics demonstrate that non-collusion emerges as the dominant strategy for channel users under reasonable assumptions. Experimental results indicate that the proposed scheme effectively prevents cross-chain collusion while achieving high cross-chain throughput and scalability compared to traditional relay-based cross-chain solutions.

Keywords: blockchain, cross-chain transaction, secure protocol, collusion resistance

---

收稿日期：2024–06–05；**修回日期：**2024–11–07

通信作者：贾雪丹，laura_j@163.com

基金项目：国家自然科学基金资助项目（No.62372105）；江苏省前沿引领技术基础研究基金资助项目（No.BK20202001）；海南师范大学博士科研启动经费基金资助项目（No.HSZK-KYQD-202440）

Foundation Items: The National Natural Science Foundation of China (No.62372105), The Leading-edge Technology Program of Jiangsu Natural Science Foundation (No.BK20202001), The Doctoral Research Funding of Hainan Normal University (No.HSZK-KYQD-202440)

0　引言

跨链技术实现区块链间代币或信息的转移，突破了底层单区块链性能和功能瓶颈[1-5]。目前主要有公证人、侧链与中继链、哈希时间锁定合约（HTLC, hash time lock contract）和分布式私钥控制 4 种跨链技术[6]。公证人机制通过单个或多个可靠团体原子性地执行跨链交易；侧链机制允许侧链读取和验证主链事务；中继链不仅作为应用链的侧链，还负责跨链消息验证和转发；HTLC 的核心是在规定时间内提供与哈希值对应的原内容来解冻资产；分布式私钥控制实现用户私钥去中心化管理，跨链时锁定原链资产并在目的链创建新的资产。但上述跨链技术仍存在一定局限，公证人机制对可信中介的依赖降低了安全性，HTLC 难以证明资产锁定的有效性，分布式私钥控制面临技术可行性难题[7]。虽然多数跨链项目采用中继模式，如 Cosmos[8] 与 Polkadot[9]，但中继链验证者节点对应用链的状态更新有重要影响，尽管有钓鱼者监控，仍存在安全风险。

跨链交易过程还面临合谋攻击威胁[10-12]，多个跨链节点秘密生成协作协议进行恶意行为，影响跨链交易安全性和跨链结算公平性。上述 4 种跨链技术中，侧链和 HTLC 依赖于哈希时间锁技术，更容易受到合谋攻击[5,13]。而且在跨链交易过程中，恶意用户间可以通过合谋实现双花攻击[14]。此外，随着跨链交易需求增长，跨链吞吐率可扩展性成为除了跨链安全外另一个亟待解决的问题[15]。以中继跨链为例，跨链交易需要在中继链等待交易数据上链、共识并同步公开，跨链效率低且缺乏对跨链内容的隐私保护，随着接入链数量增加，中继链性能和安全问题愈加严重。链下通道技术能够有效提升区块链系统性能[16]，仅通道开通和关闭过程需要链上确认，用户可以通过通道进行多次链下交易而无须链上操作，大大降低了区块链负载。但当前的通道方案，如支付通道[17]、状态通道[18]、虚拟通道[19-20]和支付通道网络[21-22]等，仅支持单链交易，无法直接用于提升跨链性能。已有研究者通过构建跨链通道[2-4]，允许不同区块链中的任意 2 个用户通过多跳路径进行交易，实现跨链互操作扩展性。但是，这些跨链通道方案依赖的哈希时间锁技术容易受到合谋攻击和双花攻击威胁[5,13-14]。

要实现可扩展的防合谋跨链交易，面临 2 个重要挑战。一方面，跨链交易面临隐私泄露和合谋威胁，区块链间跨链交互需要保证安全性和可靠性，避免跨链过程中交易隐私泄露及合谋导致不公平问题；另一方面，跨链的共识算法比单链具有更多的不透明机制，如果中继者和跨链一方合谋作弊，会使得共识对另一方不利，需要可验证跨链共识方案实现安全跨链结算。针对上述问题，本文提出防合谋跨链通道，设计基于博弈激励的防合谋跨链交易协议和基于通道状态证明的安全跨链结算方法，并通过博弈分析证明不合谋才是所有跨链参与者的主导策略；所设计方案避免繁重的密码运算和大量额外质押，通过防合谋跨链通道实现可扩展跨链交易。

本文的主要贡献总结如下。

1) 提出防合谋跨链通道模型，建立跨多中继链的链下通道，保障任意业务链用户间安全和高效跨链交易处理实现可扩展跨链交易，且通道内跨链交易信息对外不可见，保证跨链隐私。

2) 为了防止通道参与者合谋，提出基于博弈激励的跨链交易协议，在合谋者之间刺激产生背叛和不信任并通过合约实现，保证不合谋是参与者最优策略；为了避免复杂的跨链通道争议，通过基于哈希的加密可验证跨链通道状态证明实现可验证跨链共识，保证安全和隐私的跨链结算。

3) 通过博弈分析证明防合谋的有效性；实验结果表明，所提方案以较小开销实现防合谋跨链交易，且与其他中继跨链方案相比，所提方案实现高跨链吞吐率，具有可扩展性。

1　相关研究

针对区块链跨链交易和合谋攻击问题，研究者已提出相应解决方案。

1.1　跨链交易

相对于公证人、HTLC 和分布式私钥控制技术，基于中继链的跨链交易方案在安全性、互操作性和可行性方面具有一定优势，但在面临大量接入链跨链交易请求时，中继链仍面临性能瓶颈。链下通道是广泛使用的链下扩展技术[23]，旨在降低链上验证和存储成本，实现高效加密货币原子交换。针对单链环境，已提出支付通道[17]、状态通道[18]、虚拟通道[19-20]和支付通道网络[21-22]，实现交易吞吐率扩展，并针对通道瞭望塔[24]和通道路由[16]提出解决方案。为了实现可扩展跨链交易，研究者尝

试将链下通道技术应用于跨链服务。跨链通道[2]针对跨链协议在处理链上事务时可扩展性差的问题，提出支持跨链服务的分层链下通道，设计分层交互协议、分层结算协议和通用公平交换协议，实现跨链通道中未结算金额的支付，并保证了跨链交互的可扩展性、公平性和原子性。跨链通道要求跨链交易双方在两条区块链上都有账户。为此提出基于中间节点辅助的链下扩展方法[3,25-26]。跨账本协议Interledger[25]依赖HTLC，通过结合哈希锁和支付通道来实现链下跨货币多跳支付，并确保不同跳的支付原子性。但HTLC易遭受虫洞攻击和合谋攻击，且InterLedger协议要求所有加密货币都实现HTLC。Malavolta等[26]提出防止虫洞攻击的匿名多跳锁（AMHL, anonymous multi-hop lock），并给出3种构造方法：通用AMHL、基于椭圆曲线数字签名（ECDSA）的AMHL和基于Schnorr签名的AMHL。文献[3]提出跨链支付通道网络XHub，设计审计员通信协议、集线器注册协议、交易协议和集线器管理协议，且有关跨链集线器的可靠信息以分散的方式进行管理，保证正确遵守协议的用户能够成功付款或从服务中获利，实现了跨链服务可用、原子性和可审计跨链交易。为了避免中间节点全程参与跨链交易，文献[4]提出跨链虚拟支付通道，允许不同区块链系统中的2个用户在中间节点的帮助下进行无限的链外交易，中间节点只参与通道的开通和关闭操作，进一步提高跨链交易效率，并在一定程度上增强跨链交易隐私性。为了使支付通道网络适用于隐私加密货币，Wang等[27]提出匿名增强多跳锁，结合可链接环适配器签名和匿名多跳锁支付通道网络架构，实现支持Monero的支付通道网络。

1.2　合谋攻击

区块链中的合谋问题包括基于区块链的应用中的合谋[28-30]和区块链底层技术中的合谋[31]，研究者已分别提出解决方案。文献[28]针对委托计算中的合谋问题提出基于博弈论和智能合约的解决方案，并实现三方贝叶斯纳什均衡。文献[29-30]针对区块链拍卖系统中的合谋问题提出解决方案，实现了防止单向拍卖中的买家合谋和双向拍卖中的拍卖方与竞拍者合谋。

共识技术作为区块链的基石，其性能直接影响区块链系统的安全性和事务处理能力[32]。针对容错类共识算法面临的节点合谋攻击，文献[33]提出抗合谋攻击的全局随机化共识算法，利用映射函数和加权随机函数实现发起者和验证者节点的全局随机化，并利用精炼贝叶斯博弈构造合谋合约，分析求得合谋者之间的纳什均衡点，解决超过$\frac{1}{3}$节点的合谋攻击问题。针对委托权益证明机制（DPoS）中恶意节点合谋操纵选举导致的安全威胁，文献[34]提出基于权力指数的DPoS合谋攻击检测与预防方法，基于博弈理论中权力指数的思想构建DPoS的加权投票博弈模型，分析恶意节点的行为动机，通过异常的权力指数变化幅度进行攻击检测，加入Softsign激活函数抑制恶意节点的权力指数，利用激活函数的饱和性预防DPoS合谋攻击。

支付通道作为实现区块链可扩展性的主流技术，也面临合谋威胁。为了缓解通道参与者必须保持在线问题，支付通道网络引入通道瞭望塔，通过瞭望塔监控通道内的欺诈行为。然而，瞭望塔与通道参与者并非完全可信，瞭望塔可能与作弊对手勾结并从中获利，威胁通道安全。Pisa[35]提供可公开验证的加密证据，以惩罚作弊瞭望塔。文献[36-37]利用合谋的核心困难——秘密偏离串通协议通常是有利可图的，带来合谋者之间的不信任，使理性的参与者不会串通，实现单瞭望塔和分布式瞭望塔下的安全通道。

跨链交易过程也面临合谋威胁[11-12]，侧链和HTLC机制更容易遭受合谋攻击[5,13]。文献[14]针对跨链交易中恶意用户通过合谋实现双花攻击提出解决方案。文献[3,10]基于多数安全假设防止恶意用户跨链合谋。本文方案无须多数安全假设，实现可扩展的防合谋跨链交易。表1给出了本文方案和当前主流跨链交易方案的比较。

表1　　方案比较

方案	隐私保护	防合谋	可验证	可扩展
文献[14]	×	√	×	×
文献[10]	×	×	√	×
文献[2]	×	×	√	√
文献[4]	√	×	√	√
文献[3]	×	×	√	√
文献[1]	√	×	√	×
本文方案	√	√	√	√

2　系统模型和问题描述

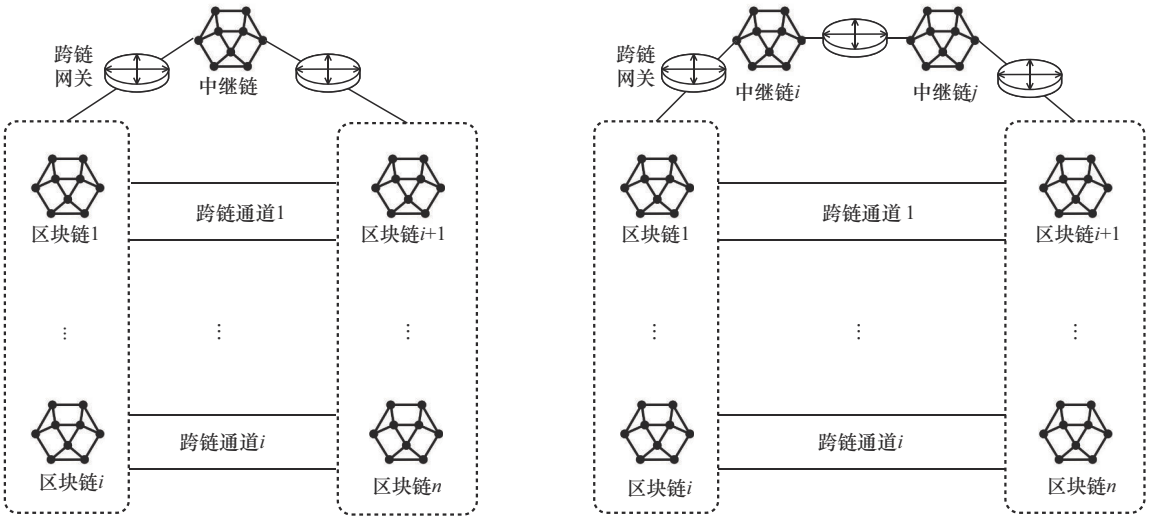
本节首先介绍提出的基于跨链通道的跨链模型，然后对跨链过程中存在的合谋问题进行分析，最后给出设计目标。

2.1　跨链模型

针对中继跨链机制面临的跨链交易处理性能问题，提出基于中继链跨链通道的跨链模型，解决面临大量跨链交易请求时由于中继链处理瓶颈导致的跨链时延增加或跨链失败问题，实现可扩展性。如图1所示，所提跨链模型中存在2个模式的跨链通道：单中继链跨链通道和多中继链跨链通道。

在单中继链跨链通道中，跨链交易双方通过其业务链网关连接到同一中继链，由该中继链对跨链交易请求和业务链代币锁定证明进行验证，然后选择中继链节点作为跨链通道的观察者并为跨链参与者建立跨链通道。观察者负责监控跨链通道内交易方的行为并辅助提交跨链通道状态证明（CSP, channel state proof）。如图2所示，业务链B_1用户H_1和业务链B_2用户C通过中继链R_1构建跨链通道，通道参与者包括H_1、C和观察者W_3。

当跨链交易的业务链双方没有通过跨链网关直接连接到同一个中继链时，则需要通过跨链路由网络建立跨多个中继链的连接，即需要建立多中继链跨链通道。多中继链跨链通道可以由路由中间的任一中继链负责建立通道，其他中继链选择观察者节点锁定质押加入该跨链通道。业务链跨链请求和质押锁定以及中继链观察节点质押锁定，通过路由通道上的网关进行传递并由负责建立通道的中继链进行验证，质押锁定安全性和跨链通道可靠性由区块链安全性保证。如图2所示，业务链B_1用户H_1和业务链B_3用户D通过中继链R_1、R_2及跨链路由网络中的其他中继链建立跨链路径，并由其中中继链R_0对跨链交易用户和观察者质押进行验证并构建多中继链跨链通道，跨链通道参与者包括H_1、D、W_4、W_5和其他中继链观察者。



(a) 单中继链　　(b) 多中继链

图1　基于中继链跨链通道的跨链模型

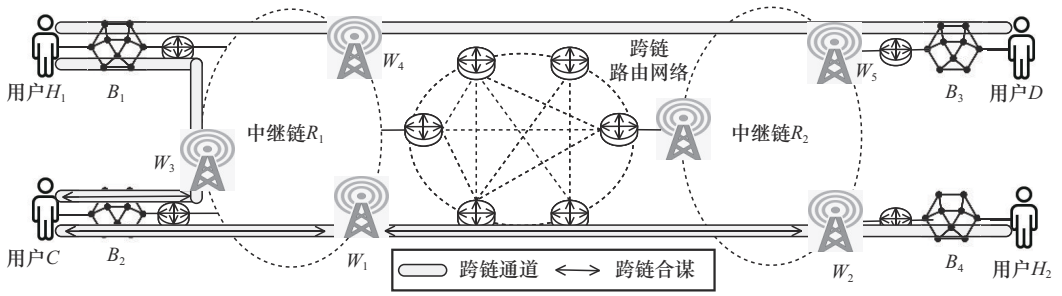


图2　跨链合谋

2.2　跨链合谋

本文假设中继链和业务链是安全的，但并不假设中继链节点和业务链用户可信。跨链通道观察者可能与跨链交易对手合谋作弊并从中获利，损害另一跨链交易方利益。如果根据合谋情况下的欺诈跨链通道状态证明进行跨链结算，将破坏跨链交易公平性和安全性。

如图2所示，所提跨链模型中的跨链通道观察者可以监控跨链交易双方行为，接受跨链交易方委托辅助提交最终状态证明，在跨链交易方离线情况下保证跨链交易安全，由此实现无须跨链交易者实时在线情况下的高效跨链交易。然而，跨链交易双方和通道观察者作为自私且理性的节点，可能通过作弊增加自身收益。恶意跨链交易者可以贿赂观察者进行合谋欺骗另一跨链交易方，进而增加自身收益[35,37]，损害非合谋节点利益。在合谋情况下，无法保证跨链交易方离线时的通道安全，且可能出现合谋观察者和理性观察者提交不一致的通道状态证明，触发烦琐耗时的通道争议处理过程，降低跨链结算效率。

本文考虑2种形式的合谋：业务链用户与观察者合谋、观察者节点间合谋，如图2所示。单中继链跨链通道中存在业务链用户和观察者合谋，如用户C和观察者W_3合谋，多中继链跨链通道中还可能存在观察者节点间合谋，如W_1和W_2合谋。无论哪种合谋方式，都可能损害跨链交易中其他参与方的利益，如业务链B_1用户H_1和业务链B_4用户H_2。

针对恶意跨链用户C发起与观察者W_1和W_2合谋，间接实现观察者W_1和W_2合谋。如图3所示，跨链交易者H雇佣通道观察者W_1和W_2监控通道安全暂时离线；恶意跨链交易对手C通过贿赂观察者W_1和W_2组成合谋团体，并试图通过发布欺诈状态证明来关闭跨链通道，造成跨链用户H损失并增加合谋团体收入。如果跨链合谋成功并根据合谋结果进行跨链结算，将破坏跨链交易安全和交易公平。为此，提出防合谋跨链交易和结算方法，防止恶意跨链交易者和通道观察者合谋提交错误状态证明，保障跨链交易安全和公平。

2.3　设计目标

针对跨链交易合谋问题，提出检测和防范方法，首先设计跨链交易协议，基于博弈激励设计一系列通道合约，促使理性参与者提交真实的跨链通道状态证明，防止通道参与者合谋，如图3所示；然后根据最终通道状态证明进行分层验证，并在中继链和业务链之间达成共识，实现安全跨链结算。方案设计目标包括隐私保护、防合谋、可验证和可扩展。

1) 隐私保护：保护跨链通道用户H和C之间的交易隐私，防止跨链交易信息泄露。

2) 防合谋：防止跨链通道参与者合谋作弊，破坏跨链交易原子性和公平性。

3) 可验证：跨链结算结果可验证，跨链交易过程中的合规或作弊行为可被检测和验证。

4) 可扩展：防止跨链交易拥堵，提高跨链交易处理性能，实现可扩展跨链交易。

3　防合谋跨链交易方案

为了实现可扩展的防合谋跨链交易，在所提跨链通道模型下，设计防合谋跨链交易协议和跨链结算协议，基于博弈激励的跨链交易协议通过破坏合谋者之间的信任来实现防合谋；基于哈希的加密可验证通道状态证明进行分层验证的跨链结算协议，在中继链和业务链之间达成共识避免通道争议，实现安全和隐私的跨链结算。首先对所提方案进行概述，然后阐述具体的跨链通道合

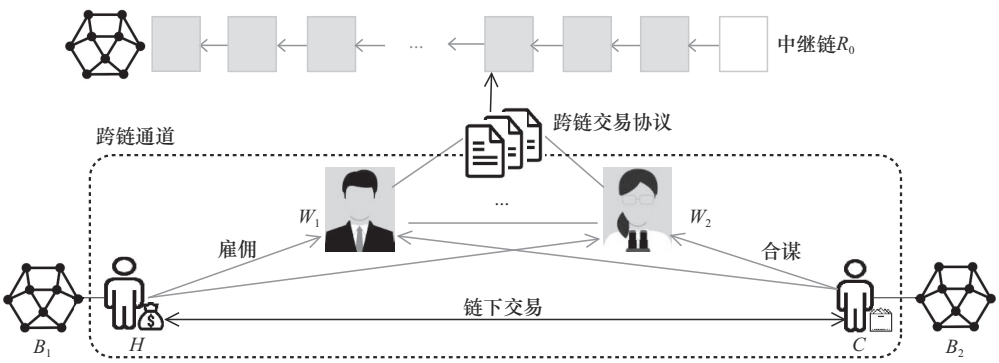


图3　防合谋跨链通道

约设计和跨链结算方法。表2给出了所提方案使用的符号及其含义。

表2　　符号及含义

符号	含义
H,C,W	跨链交易方、跨链交易对手、中继链观察者
B_i,R_i,R_0	业务链、中继链、负责建立跨链通道的中继链
p	基于哈希的加密可验证跨链通道状态证明
b	合谋合约中C和W约定支付的贿赂
c	观察者W监控跨链通道的费用
v_f	支付给R_0矿工解决跨链通道纠纷的验证费
d_w	观察者W为参与跨链通道存入的质押金
d_c	跨链交易对手C在跨链通道上拥有的代币金额
d_t	跨链交易对手C和中继链观察者W在合谋合约中的质押金
w_h	跨链交易方H支付给中继链观察者W的监控通道的报酬
w_c	跨链交易对手C发布欺诈状态证明获得的收益

3.1　方案概述

跨链协议如图4所示，业务链B_1用户H作为跨链交易发起方，通过中继链R_0和跨链路由网络，与业务链B_2用户C建立跨链通道进行跨链交易。首先，跨链交易方H和交易对手C分别在业务链B_1和B_2提交跨链交易请求并锁定质押金，通过跨链网关进行路由确定中继链R_0和路径中其他中继链R_i、R_j。然后由中继链R_0对跨链交易方和观察者在其所在区块链锁定质押交易的有效性进行验证。通过验证之后，中继链R_0选择中继链节点W_0作为通道观察者监控跨链通道安全，并为跨链交易方H、C和观察者W_0、W_i、W_j建立跨链通道。

如果业务链B_1和B_2通过跨链网关直接连接到同一个中继链，则无须多条中继链进行路由，该中继链即R_0。跨多中继链的跨链路径中，不同中继链间通过跨链网关互联并转发跨链消息，路径中任一支持图灵完备合约的中继链都可以负责建立跨链通道，即作为R_0，取路径中间的中继链作

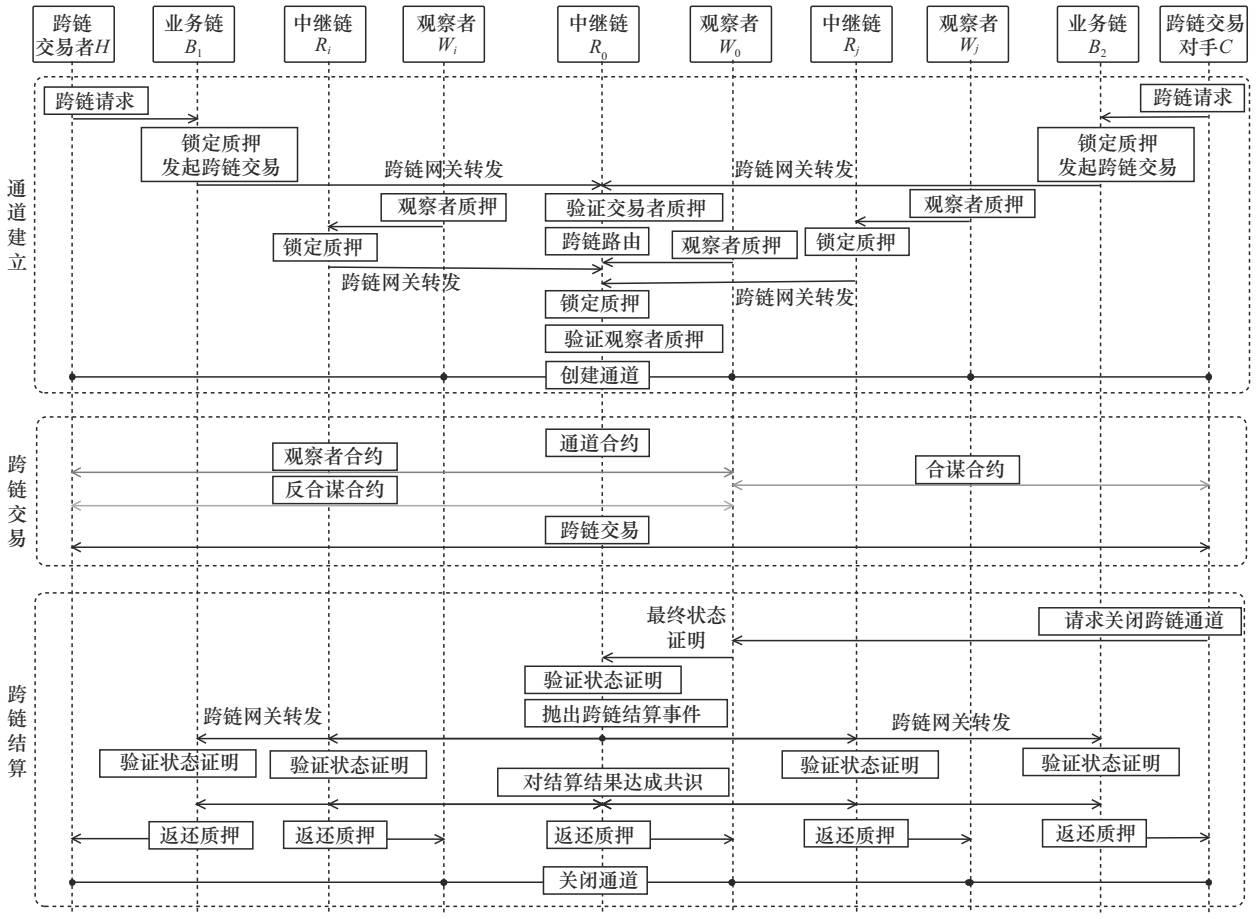


图4　跨链协议

为R_0有利于提高分层验证效率。具体的跨链路由方法不在本文讨论范围内。针对通道观察者与某一跨链交易方勾结作弊损害另一跨链交易方利益问题，基于博弈激励设计防合谋跨链交易协议，保障通道内交易安全；然后基于跨链通道状态证明进行分层验证，在业务链和中继链间就跨链结算结果达成共识，避免烦琐耗时的通道争议处理过程，在保障安全跨链结算同时，提高跨链效率实现可扩展性。

跨链交易方H可以雇佣一个或多个观察者W并签订雇佣合同，即观察者合约Contract_W，然后暂时离线。观察者W可以从检测到的欺诈中获得回报，也可以通过诚实地监控跨链通道获得收益。雇佣方H在每次交易后向所雇佣的观察者W发送最新的通道状态证明。恶意跨链交易对手C则希望通过贿赂观察者W并签订合谋合约Contract_C，共同发送欺诈CSP关闭通道来增加收益。为了打破合谋者之间的信任和平衡，利用博弈论机制激励观察者报告合谋，通过签订跨链交易者H和观察者W之间的反合谋合约Contract_A破坏合谋者间信任，实现防合谋激励。一旦恶意交易对手C的作弊行为被观察者W监控举报，交易对手将受到惩罚，观察者W将获得相应的收益，未及时做出诚实回应的观察者W也将受到惩罚。

在跨链结算过程中，基于通道状态证明设计分层验证的跨链共识方法，由中继链R_0抛出跨链结算事务，并通过其他中继链和业务链分层验证，实现所有业务链与中继链之间关于跨链结算结果的防合谋共识。

所提方案包括6个步骤，具体如下。

1) 跨链交易请求：由业务链B_1的应用节点H发起跨链交易请求，在业务链B_1锁定质押金后抛出跨链事件$(\mathrm{ID}_H,\mathrm{ID}_C,\mathrm{Inx},\mathrm{Time},\mathrm{comm}_{v_H},p_0)$，其中包含跨链交易方和交易对手身份$\mathrm{ID}_H$、$\mathrm{ID}_C$，交易索引Inx，时间戳Time，质押承诺$\mathrm{comm}_{v_H}$和初始状态证明$p_0$，然后通过跨链网关把跨链消息转发给中继链$R_0$。同时，跨链交易对手$C$，在其所在的业务链$B_2$锁定质押金，并把跨链消息$(\mathrm{ID}_C,\mathrm{ID}_H,\mathrm{Inx},\mathrm{Time},\mathrm{comm}_{v_C},p_0)$通过跨链网关转发到中继链$R_0$。

2) 中继链验证：中继链R_0通过跨链网关收到跨链交易请求$(\mathrm{ID}_H,\mathrm{ID}_C,\mathrm{Inx},\mathrm{Time},\mathrm{comm}_{v_H},p_0)$、$(\mathrm{ID}_C,\mathrm{ID}_H,\mathrm{Inx},\mathrm{Time},\mathrm{comm}_{v_C},p_0)$后，对业务链跨链事务进行验证，确认业务链节点$H$和$C$已经在所在业务链锁定质押。

3)跨链通道建立：中继链R_0通过跨链网关路由为跨链交易请求双方ID_H,ID_C建立跨链通道，跨链通道参与者除了ID_H,ID_C之外，还包括中继链观察者ID_{W_0},ID_{W_1},ID_{W_2},…，观察者所在的中继链负责观察者质押锁定，中继链R_0负责对观察者质押锁定进行验证。

4)跨链交易：跨链交易双方ID_H,ID_C在跨链通道内进行跨链交易$\mathrm{state}_{i+1} \leftarrow \mathrm{Tx}(\mathrm{state}_i,\mathrm{tx}_{i+1})$，即执行通道内交易Tx，具体交易信息为$\mathrm{tx}_{i+1}$，通道状态由$\mathrm{state}_i$更新为$\mathrm{state}_{i+1}$。同时由跨链通道观察者$W$监控跨链通道，辅助维护跨链通道状态证明$p_{i+1}=H(\mathrm{state}_{i+1},r_{i+1})$，即使用哈希函数$H$计算加密通道状态证明$p_{i+1}$，当需要时公布盲化随机数$r_{i+1}$以进行验证。

5)跨链结算：当跨链交易双方完成跨链交易后，跨链交易对手C提出跨链通道关闭请求$(\mathrm{close},\mathrm{ID}_C,\mathrm{ID}_H,\mathrm{Inx},p)$，中继链$R_0$对跨链通道状态进行验证，并发起跨链结算Xstl。

6)跨链通道关闭：通过跨链共识完成跨链结算后，中继链R_0关闭跨链通道，业务链B_1、B_2和中继链R_i按照结算结果返还用户质押。

3.2 合约设计

为了实现防合谋跨链交易，设计跨链交易协议，其中包括3个合约：观察者合约、合谋合约和反合谋合约。跨链通道合约关系如图5所示。

3.2.1 观察者合约

观察者合约Contract_W是由跨链交易方H和跨链观察者W约定的雇佣关系。观察者合约允许H离线并雇佣W来监控通道，如果跨链交易对手C单方面要求关闭跨链通道，W监控通道状态，确保提供最新状态证明p。观察者合约要求W质押d_w来激励其诚实行为。如果观察者W在约定时间$[t_1,t_3]$内诚实监控通道，押金d_w将退还；如果观察者W作弊被发现，其押金d_w将支付给H。

观察者合约内容如下。

1) 跨链交易方H和观察者W在时间t_1前签署雇佣关系，跨链交易方H将押金w_h存入观察者合约并向观察者W提供最新CSP，雇佣W监控跨链通

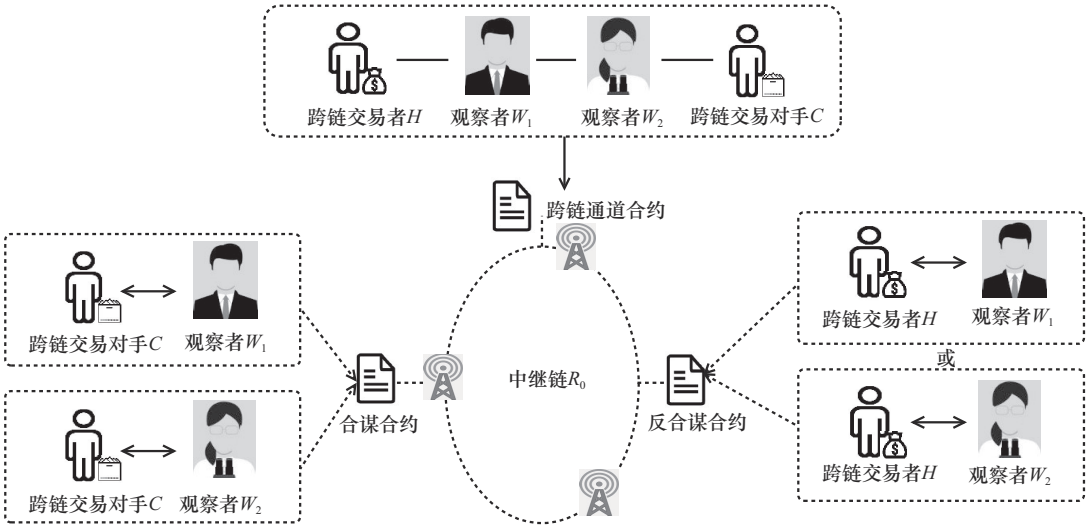


图5　跨链通道合约关系

道；观察者 W 存入押金 d_w 并承诺诚实监控跨链通道。如果超过时间 t_1 未确定雇佣关系，退还押金 w_h、d_w。

2) 如果跨链交易对手 C 在时间 $t_2 \leqslant t_3$ 请求关闭跨链通道，则根据观察者 W 行为执行算法1。

算法1　观察者辅助关闭通道

输入　观察者 W 状态证明

输出　报酬和赔偿支付结果

① if $t \leqslant \Delta \wedge p^* = p$

②　$\mathrm{Trans}(\mathrm{Addr}_W, w_h + d_w)$;

③　返回“观察者 W 诚实工作”;

④ else

⑤　$\mathrm{Trans}(\mathrm{Addr}_H, w_h + d_w)$;

⑥　返回“观察者 W 作弊”

3) 如果跨链交易对手 C 在时间 t_3 内没有请求关闭跨链通道，则根据观察者 W 行为执行算法2。

算法2　观察者完成监控

输入　观察者 W 状态证明

输出　报酬和赔偿支付结果

① if $p^* = p$

②　$\mathrm{Trans}(\mathrm{Addr}_W, w_h + d_w)$;

③　返回“观察者 W 诚实工作”;

④ else

⑤　$\mathrm{Trans}(\mathrm{Addr}_H, w_h + d_w)$;

⑥　返回“观察者 W 作弊”

如果跨链交易方 H 需要雇佣多个观察者 W，则 H 分别与通道观察者 $W_1, W_2, \cdots$ 签订上述观察者合约Contract_W。

3.2.2　合谋合约

合谋合约Contract_C由恶意跨链交易对手 C 和观察者 W 签署，允许 C 贿赂 W 合谋，即当 C 在时间 t_2 单方面要求关闭跨链通道时，W 与 C 合谋作弊提供欺诈跨链通道状态证明 p' 获取不公平利润。合谋者 C 和 W 通过在合谋合约中存入质押金来建立信任。合谋合约在 C 和 W 之间重新分配利润并惩罚偏离合谋的参与者来激励他们发送欺诈状态证明。如果合谋者 C 或 W 偏离合谋，将损失Contract_C中的质押作为惩罚。

合谋合约内容如下。

1)恶意跨链交易对手 C 和观察者 W 在时间 t_2 前签署合谋合约，C 在合谋合约中存入 $d_t + b$ 并同意提供欺诈状态证明 p'；观察者 W 同意与 C 合谋并存入锁定存款 d_t。如果在 C 关闭通道前，即时间 t_2 之前，未签署合谋合约，则合约终止并退还 d_t 和贿赂 b、d_t。

2)如果 C 在时间 t_2 发送欺诈证明 p' 请求关闭跨链通道，则根据观察者 W 行为执行算法3。

算法3　合谋关闭通道

输入　观察者 W 状态证明

输出　报酬和赔偿支付结果

① if $p^* = p'$

②　$\mathrm{Trans}(\mathrm{Addr}_C, d_t)$;

③　$\mathrm{Trans}(\mathrm{Addr}_W, b + d_t)$;

④　返回“观察者 W 和 C 合谋”;

⑤ else

⑥　$\mathrm{Trans}(\mathrm{Addr}_C, b + 2d_t)$;

⑦ 返回“观察者W未履行合谋合约”

3) 如果C在时间t_2发送非约定的状态证明，即$p \neq p'$，则根据观察者W行为执行算法4。

算法4 虚假状态关闭通道

输入 观察者W状态证明

输出 报酬和赔偿支付结果

① if $p^* = p'$

② $\text{Trans}(\text{Addr}_W, b + 2d_t)$;

③ 返回“观察者W遵循合谋合约，C背离合谋合约”;

④ else

⑤ $\text{Trans}(\text{Addr}_W, d_t)$;

⑥ $\text{Trans}(\text{Addr}_C, b + d_t)$;

⑦ 返回“观察者W和C都未遵循合谋合约”

4) 如果C在时间t_3前没有请求关闭跨链通道，则把$d_t + b$退还给C，d_t退还给W。

在合谋合约中，C向W行贿b激励W串通。C和W都锁定存款d_t，以确保偏离合谋的参与者总是获得比不偏离更低的报酬；遵循合谋的参与者总是比不遵循合谋获得更高的收益。合谋合约必须在t_2之前签署，如此C和W才可以建立信任进行合谋，且恶意交易对手C需在t_2前提供p'给合谋观察者W。如果合谋者C和W同时偏离合谋，即算法4中步骤④，则都不会受到惩罚。

合谋合约打破了观察者合约Contract_W的平衡，但仅限于单个观察者的情形，因为其他观察者可以发现并报告作弊情况。故完整的合谋可能包含C和其他观察者W之间的贿赂合谋。即发起合谋的C分别与观察者W_1、W_2签订合谋合约，并由此建立W_1和W_2之间的间接合谋关系，保证W_1和W_2不会互相举报对方与C的合谋。

3.2.3 反合谋合约

为了防止跨链通道参与者合谋破坏跨链交易公平和安全，设计反合谋合约Contract_A，旨在打破合谋合约构建的信任和平衡，使合谋成为理性参与者不恰当的选择。

反合谋合约允许报告合谋的观察者W在假装遵从合谋合约的同时秘密背叛对方C。如果没有这一豁免，观察者W不会自愿报告合谋，因为，①如果观察者W报告并遵守合谋合约，它将失去在观察者合约中的存款d_w；②如果观察者W向雇佣方H报告并背叛合谋，它将失去在合谋合约中的保证金d_t。在这2种情况下，对观察者W而言不报告合谋更加有利可图。所设计的反合谋合约破坏合谋者之间的信任，激励观察者W报告合谋，允许观察者W假装继续遵循合谋，使得观察者W报告合谋不仅没有风险，而且有利可图。

反合谋合约的具体设计如下。

1) 跨链交易方H和观察者W在时间t_2前签署反合谋合约，H在反合谋合约中存入质押d_c；观察者W同意报告合谋行为并存入验证费v_f。如果在t_2前未签署反合谋合约，则合约终止并退还d_c、v_f。

2) 如果观察者W在时间t_2前报告合谋，执行算法5。

算法5 观察者报告合谋

输入 观察者W和跨链交易对手C状态证明

输出 报酬和赔偿支付结果

① if $t = t_2 \wedge p = p'$

② if $p^* = p$

③ $\text{Trans}(\text{Addr}_W, v_f + d_c)$;

④ 返回“观察者W报告合谋并背离合谋合约”;

⑤ else

⑥ $\text{Trans}(\text{Addr}_H, d_c)$;

⑦ 返回“W报告并遵循合谋”;

⑧ else

⑨ $\text{Trans}(\text{Addr}_H, v_f)$;

⑩ 返回“C未发送欺诈状态证明”

3) 如果观察者W在时间t_2前没有报告合谋，退还d_c给H，退还v_f给W。

在合谋合约设计中提到，恶意跨链交易对手C要成功实现合谋，需要分别与跨链交易方H雇佣的观察者W_1、W_2签订合谋合约。但H不必与雇佣的观察者一一签订反合谋合约，只要有观察者W报告合谋，即可破坏所有合谋者之间的信任。

根据实际区块链系统运行情况，各合约中涉及的代币金额间有以下关系成立：①观察者收到的报酬大于其监控通道的开销$w_h > c$，即观察者W不接受低薪工作；②$w_c > b$，即跨链交易对手C支付的贿赂b不会超过其从合谋中获得的收益w_c。

3.3 跨链结算

交易双方完成跨链交易后，申请关闭跨链通道，中继链R_0根据最新状态证明进行跨链结算，并就结算结果与业务链和其他中继链达成跨链共识，

实现安全跨链结算。本节首先给出跨链结算流程，然后提出分层验证的跨链共识方法，如图6所示，提高跨链结算效率的同时保证跨链结算正确性。

3.3.1　跨链结算流程

首先由跨链交易方H或C提交最新跨链通道状态证明p，申请关闭跨链通道。观察者W_0把通道关闭信息提交给中继链R_0，中继链R_0验证后发起跨链结算并把结算信息通过跨链网关依次传递给H和C跨链路由中的其他中继链R_i、R_j，以及H和C所在的业务链B_1和B_2。如果跨链通道中有观察者W报告合谋，则所有中继链和业务链对跨链结算信息进行验证；否则，每个中继链R_i负责验证本链观察者W_i的相关行为和结算信息，业务链B_1和B_2分别对H和C的行为和结算信息进行验证。跨链结算包括5个步骤。

1) 发起通道关闭请求：跨链交易者H和C结束跨链交易，申请关闭跨链通道，发起关闭跨链通道请求(close,ID_C,ID_H,Inx,p)，由观察者W_0提交给中继链R_0。

2) 抛出跨链结算事件：中继链R_0接收到跨链通道关闭请求(close,ID_C,ID_H,Inx,p)后，对通道状态证明p进行验证，通过验证后，抛出跨链结算事件Xstl。

3) 结算信息分层验证：跨链结算事件Xstl通过跨链网关进行转发，跨链交易方H和C跨链路由中的中继链R_i通过跨链网关接收到跨链结算事件后，对跨链结算事件Xstl进行验证并转发；跨链交易方H和C所在的业务链B_1和B_2收到跨链结算事件和中继链验证结果后，进行验证。

4) 达成跨链结算共识：跨链交易方H和C所在业务链和跨链路径上中继链完成验证后，验证结果信息由通过跨链网关依次传递到中继链R_0；中继链R_0接收并检查业务链和其他中继链的验证结果，所有中继链和业务链都通过验证后，业务链和中继链就当前结算结果达成共识。

5) 关闭通道并返还质押：中继链R_0关闭跨链通道，并根据共识结果返还本链观察者W_0质押；其他中继链R_i和业务链B_1、B_2按照跨链结算结果，返还本链观察者W_i或跨链交易用户H、C质押。

3.3.2　分层跨链共识

基于通道状态证明提出分层跨链共识方法，如图6所示，实现安全跨链结算。在跨链交易方H或C提出关闭通道请求后，观察者W_0提交最终通道状态证明p到建立通道的中继区块链R_0，由中继链R_0对跨链通道参与者行为进行验证，即图6中步骤①。

然后R_0根据验证结果抛出跨链结算事件Xstl，根据通道中有无报告合谋，跨链结算事件Xstl分为两类，分别标记为XSettle_1、XSettle_0。以中继链R_0为起点，通过跨链网关分别向业务链B_1和业务链B_2方向的其他中继链R_i和R_j传递跨链结算信息Xstl，中继链和业务链分别执行步骤②进行分层验证，验证方法如算法6所示。

算法6　分层验证

输入　跨链结算信息XSettle_1或XSettle_0

输出　跨链共识结果

① 收到跨链结算信息的中继链R_i根据本链观察者W_i提供的跨链通道状态证明和跨链结算信息中的相应内容，在本链进行验证并转发：

② if Xstl =XSettle_1

③　　R_i验证跨链结算信息中所有参与者行为和结算结果；

④ else

⑤　　R_i对本链观察者W_i的相关结算信息和行为进行验证；

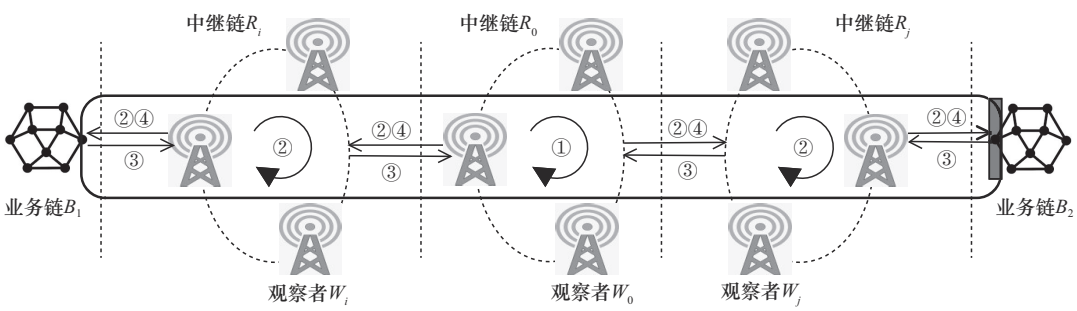


图6　分层跨链共识

⑥ 对业务链B_i，根据跨链交易方提供的跨链通道状态证明和跨链结算信息中的相应内容，进行验证并就验证结果达成链内共识：

⑦ if Xstl =XSettle_1

⑧ B_i对跨链结算信息和中继链验证结果进行验证；

⑨ else

⑩ B_i对本链用户H或C和跨链交易对手C或H的结算信息和行为进行验证

在跨链共识过程中，业务链B_i和中继链R_i自身的共识过程不受影响，即中继链和业务链基于链内共识对收到的结算信息进行验证。

路由路径上的中继链和业务链都对结算结果验证并达成链内共识后，执行步骤③，通过跨链网关发送验证结果到建立跨链通道的中继链R_0。中继链R_0接收并检查业务链和其他中继链的验证结果，如果中继链和业务链都对当前结算结果无异议，业务链和中继链就当前结算结果达成共识。

达成跨链共识后，中继链R_0关闭跨链通道，执行步骤④通知其他中继链和业务链。确认跨链通道关闭后，中继链R_0、R_i及业务链B_1、B_2根据共识结果进行链内结算，返还本链观察者W_0、W_i或跨链交易用户H、C质押。

注意，因为3.2节的防合谋跨链交易协议设计，不合谋是所有跨链通道参与者的最优策略，故中继链R_0根据跨链通道状态抛出的跨链结算事件Xstl大概率为XSettle_0。另外，在跨链共识过程中，还可以根据通道状态和结算结果增加对中继链观察者W的信誉维护和更新，进一步激励观察者W的诚实行为。而且，在构建新的跨链通道选择中继链观察者时，可以优先选择信誉值更高更加诚实可靠的中继链节点作为跨链通道观察者W。

4 安全性分析

本节首先对方案中各参与者之间引发的博弈进行分析，证明不合谋才是参与用户的最优选择，然后对方案的隐私保护性能和可验证性进行分析。

4.1 防合谋

本节采用不完全信息博弈对所设计的通道合约引发的博弈进行分析。不完全信息表示某一跨链通道参与者对其他跨链通道参与者所采取的行动一无所知。跨链通道中的交易是匿名的，通道参与者无法获得完整的信息，将博弈建模为不完全信息博弈，更符合真实情况。

对观察者合约Contract_W，只要$w_h > c$成立，跨链交易对手C和观察者W的最优策略都是诚实提交状态证明p。签署合谋合约Contract_C后，打破了观察者合约建立的平衡，只要$w_h > c$和$w_c > b > w_h - c + d_w$成立，根据此时的序贯均衡，跨链交易对手C会发起合谋，观察者W同意合谋，C在时间t_2发送欺诈状态证明p'且W提交p'。反合谋合约Contract_A破坏了合谋合约建立的合谋者间信任，此时由3个合约共同引发的博弈过程存在唯一序贯均衡。

定理1 如果$w_c > b > w_h - c + d_w$和$w_h > c$成立，所有合约引发的博弈具有唯一的序贯均衡(s_C, s_W)。根据均衡，跨链交易对手C不发起合谋，跨链通道观察者W不报告合谋，且C和W诚实提交状态证明p。

定理1证明过程详见附录1。

4.2 隐私保护

本文通过设计跨链通道，实现跨链交易可扩展性的同时，通过建立不同跨链通道从网络层面实现跨链交易信息的隔离，保证跨链交易数据只对跨链通道内用户H和C可见。

定理2 所提跨链交易方案实现跨链交易方H和C之间隐私保护的跨链交易。

定理2证明过程详见附录1。

该跨链交易方案只支持两方之间隐私保护的跨链交易，暂不支持多方隐私保护的跨链交易。

4.3 可验证性

本文通过跨链通道合约和分层可验证共识设计，实现跨链行为可验证。

定理3 所提跨链交易方案实现跨链结算结果可验证，且跨链交易过程中的合规或作弊行为可被检测和验证。

定理3证明过程详见附录1。

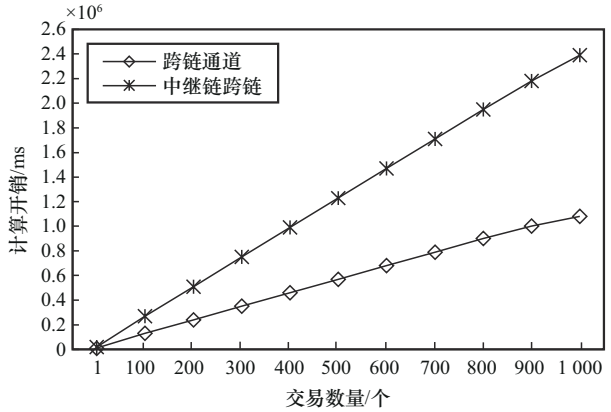
5 性能评估

本文通过实验部署测试所提跨链交易方案的性能，基于Fabric实例化了1条中继链和2条业务链，分别部署在AMD Ryzen 7 5800H 16 GB、Intel i512500H16 GB和Intel i512500H 8 GB服务器上，每条链设置2个组织和3个共识节点。所有机器运行Ubuntu 22.04 LTS操作系统。并基于Solidity实

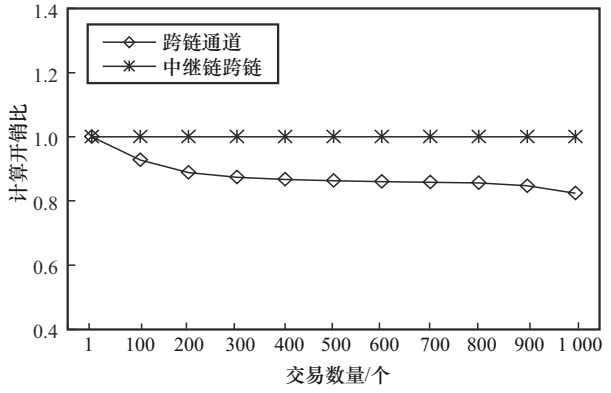
现观察者合约、合谋合约和反合谋合约主要功能，使用以太坊集成开发环境Remix进行测试，然后部署在本地模拟网络Ganache上，对所提方案有效性和可扩展性进行验证。

5.1　计算开销

图7给出了所提基于中继链通道的跨链交易方案和基于中继链的跨链交易方案的计算开销比较，主要包括签名和验证所需的时间开销。图7(a)给出了2类方案的计算开销与交易数量的关系；图7(b)给出了2类方案的计算开销比与交易数量的关系。



(a) 计算开销与交易数量的关系



(b) 计算开销比与交易数量的关系

图7　计算开销比较

由图7可以看出，相比于基于中继链的跨链交易方案，所提方案具有较低的计算成本。这主要是由两方面原因导致的计算开销降低。一方面，跨链通道减少了频繁跨链交易带来的中继链链上处理开销，链上交易的数量是恒定的，与跨链通道中跨链交易双方的交易数量无关；另一方面，所提方案的防合谋性能不依赖于复杂的高级密码原语，如非交互式零知识证明或同态加密等，而是通过适量质押和博弈激励，打破合谋者之间的信任，进而保障安全跨链交易。

而且，随着跨链交易数量的增多，跨链交易开销降低得更加明显。产生这一结果的原因主要是，跨链通道的建立过程和关闭通道时需要执行的跨链结算过程，所需的计算量基本固定，随着跨链交易数量增加，额外的计算开销主要是跨链交易过程中交易双方的签名和验证开销，从而使得跨链通道中的平均交易开销逐渐降低。跨链交易计算开销的降低可以提高跨链交易处理效率，增加跨链吞吐率，进而提高跨链扩展性。

5.2　合约开销

本节测试了在以太坊模拟网络上部署和执行跨链通道合约的成本，如表3所示，将合约开销成本量化为执行智能合约的每个功能所消耗的开销总量。观察者合约Contract_W、合谋合约Contract_C和反合谋合约Contract_A的总成本分别约为230万、210万和270万以太坊燃料。

表3　　合约开销

合约	功能	开销/Gas
Contract_W	Init	1 908 573
	Create	252 753
	Hire	73 128
	Distributed	71 594
Contract_C	Init	1 649 663
	Create	310 927
	Collude	82 069
	Distributed	109 361
Contract_A	Init	1 983 365
	Create	353 079
	Betryal	80 782
	Distributed	302 843

运行智能合约的成本开销主要与合约功能的计算复杂性和存储开销相关。由于区块链上的数据存储成本非常高，对跨链通道中的观察者合约Contract_W、合谋合约Contract_C和反合谋合约Contract_A来说，合约初始化操作Init的成本明显高于雇佣观察者、与其他通道用户合谋及背叛合谋等操作，原因是需要在观察者合约Contract_W、合谋合约Contract_C和反合谋合约Contract_A初始化时提

前支付所有数据结构的初始化成本。随着关闭跨链通道的请求数量增加，存储成本会逐渐降低，但由于所提方案仅支持跨链双方交易，而非多方跨链交易，如果每对跨链交易方都需要建立新的合约，仍存在较大开销。可以通过相同业务链的不同用户复用合约来降低总体合约执行成本，这是完全可行的，且节约了每次建立跨链通道前的跨链路由成本。

5.3　跨链吞吐率

本节测试了观察者吞吐率，并将跨链通道吞吐率与基于中继链的跨链交易方案[7-9]进行了比较。首先在参与者之间创建10^i个链下交易（$0\leqslant i\leqslant 6$），每个交易都至少与一个跨链通道观察者交换一次跨链通道状态证明。然后，计算交换状态证明所需的时间、处理每个事务以量化吞吐率所需的平均时间。如图8所示，当跨链交易请求数量大于10^3时，基于中继链的跨链交易方案的吞吐率趋于稳定，而当跨链交易请求数量大于10^5时，中继链跨链吞吐率明显下降，即基于中继链的跨链交易方案受性能瓶颈限制导致跨链交易处理不及时。但对于所提方案，当跨链交易请求数量达到10^6时，跨链交易请求仍然可以正常得到处理，因为诚实通道观察者帮助实现跨链交易方离线时的跨链交易处理和安全保障；博弈激励防止通道观察者和跨链交易方的不诚实行为；跨链结算验证过程可发现并防止跨链通道中的作弊行为，且无须触发烦琐的争议处理。这表明跨链通道可以更高效地批量处理大量跨链交易事务，具备跨链可扩展性。

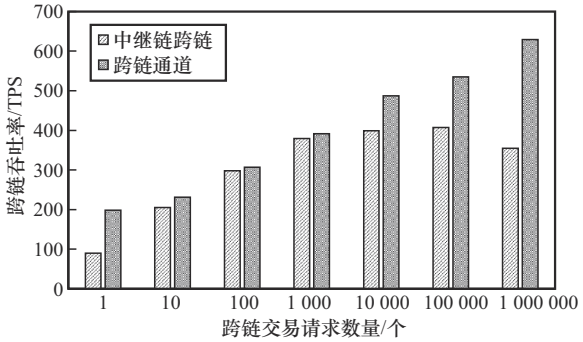


图8　跨链吞吐率对比

6　结束语

本文提出防合谋跨链通道，通过多中继链为任意业务链用户建立链下通道，实现隐私保护的跨链交易扩展，并针对其中存在的合谋问题给出解决方案。设计防合谋跨链交易协议，通过观察者合约、合谋合约和反合谋合约并结合基于博弈论的激励机制，防止通道参与者合谋。针对跨链结算，提出基于哈希加密可验证状态证明的跨链共识方法，保证跨链结算安全。采用不完全信息博弈型对合约进行分析，通过数学推导和证明获得唯一序贯均衡，证明所提方案防合谋的有效性。最后，实验结果验证了方案以较低开销实现可扩展的防合谋跨链交易。

附录1　定理证明

定理1证明　反合谋合约Contract_A破坏了合谋合约建立的合谋者间信任，此时由3个合约共同引发的博弈过程如图9所示，博弈参与者包括C、W_1和W_2，虚线框或单独非终端节点表示信息集，实线表示参与者动作，加粗实线表

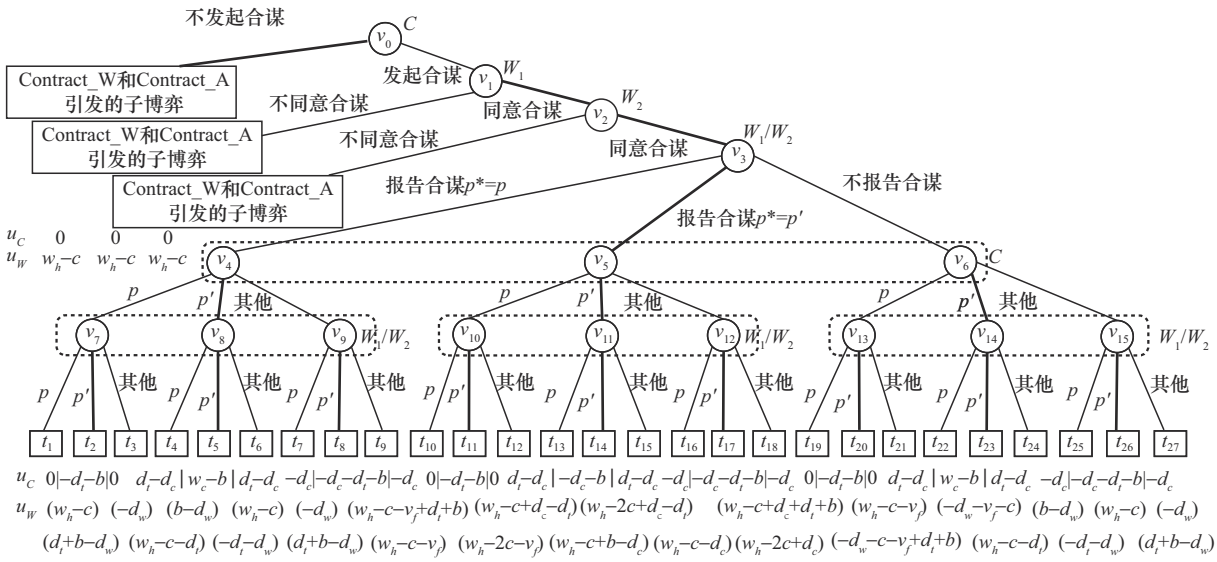


图9　所有合约引发的博弈

示唯一序贯均衡中的动作，u表示参与者收益。

如果跨链交易对手C没有发起合谋，或者C发起合谋但是观察者W_1或W_2没有同意合谋，则合谋不成功，博弈过程进入由观察者合约Contract_W和反合谋合约Contract_A引发的子博弈过程，如图10所示。

如果跨链交易对手C发起与观察者W_1和W_2的合谋，且观察者W_1和W_2都同意与C串通，另外，观察者W_1或W_2和跨链交易方H签署反合谋合约Contract_A并将向H报告合谋情况，即进入图9中以节点v_3为根的子博弈树。

首先观察图9中观察者W的收益，在信息集$I_{W,3}=\{v_3\}$处，观察者W在终端节点t_2处的收益为d_t+b-d_w，高于终端节点t_1和t_3处的收益w_h-c和$-d_w$。因为$b>w_h-c+d_w$成立，有$b-d_w>w_h-c$，又d_t、$d_w>0$，所以$d_t+b-d_w>-d_w$和$d_t+b-d_w>w_h-c$成立。观察者W在节点v_7将发送欺诈状态证明p'。同理，观察者W在节点v_8、v_9也将发送欺诈状态证明p'，即，观察者W在信息集$I_{W,4}=\{v_7,v_8,v_9\}$发送欺诈状态证明p'。同理，观察者W在信息集$I_{W,5}=\{v_{10},v_{11},v_{12}\}$和$I_{W,6}=\{v_{13},v_{14},v_{15}\}$发送欺诈状态证明$p'$。总之，无论跨链交易对手$C$的策略是什么，观察者$W$都会发送欺诈状态证明$p'$以使自身收益最大化。

接下来，观察跨链交易对手C的收益。在$I_{C,2}=\{v_4,v_5,v_6\}$处，由于观察者W会发送欺诈状态证明p'，跨链交易对手C在非终端节点(v_4,v_5,v_6)处的可到达的终端节点分别是(t_2,t_5,t_8)、(t_{11},t_{14},t_{17})和(t_{20},t_{23},t_{26})。在终端节点(t_2,t_5,t_8)，跨链交易对手C的收益分别为$-d_t-b$、w_c-b和$-d_c-d_t-b$，其中w_c-b最大，跨链交易对手C在v_4会发送欺诈状态证明p'以实现收益最大化。同理，跨链交易对手C在节点v_5、v_6也将发送欺诈状态证明p'，即跨链交易对手C在信息集$I_{C,2}=\{v_4,v_5,v_6\}$发送欺诈状态证明p'。

最后，观察者W在信息集$I_{W,3}=\{v_3\}$处，由于跨链交易对手C会发送欺诈状态证明p'，观察者W可到达的终端节点为(t_5,t_{14},t_{23})，收益分别为$b-d_w$、$w_h-c+b+d_c$和$b-d_w$。因为$w_h-c+d_c>-d_w$，故$w_h-c+b+d_c$最大，观察者W在信息集$I_{W,3}=\{v_3\}$处报告合谋并提交欺诈状态证明$p^*=p'$，即子博弈v_3在t_{14}结束。跨链交易对手C和观察者W收益分别为$-d_c-b$、$w_h-c+b+d_c$。此时跨链交易对手C的收益$-d_c-b$小于其不发起跨链合谋时的收益0，即观察者合约和反合谋合约引发的子博弈的序贯均衡中获得的收益，如图10所示。所以理性的跨链交易对手C不会选择发起合谋。即跨链交易对手C不会在子树中与观察者W恶意串通，以欺诈另一跨链交易方和其他观察者的存款，而且理性的观察者W也不会在诚实监控跨链通道并发送真实状态证明p的同时同意合谋。

根据博弈分析，存在唯一的序贯均衡，要求理性的参与者不会为了自身利益最大化而发起或同意合谋，否则他们不仅无法获得正常的利益，还会因此支付更多罚款。

证毕。

定理2证明　通道隔离是实现区块链隐私保护的重要机制。本文所提方案的隐私保护性能来自2方面，其一，通道外用户无法窥见跨链交易双方的跨链交易，这是由通道隔离和基于哈希的加密可验证CSP共同保证的；其二，通道内跨链交易双方交易明细对通道观察者保密，这是由H和C加密通信和观察者维护基于哈希的加密可验证CSP$p_{i+1}=H(\text{state}_{i+1},r_{i+1})$保障的。

跨链用户H和C通过在各自所在的源区块链上锁定质押，由中继链R_0辅助建立跨链通道并记录初始通道状态，随后H和C在链下进行跨链交易，非通道参与者的其他区块链节点和外部攻击者无法获得H和C链下交易信息。

跨链通道观察者W负责监控通道安全，只负责维护和提交基于哈希的加密可验证$p_i=H(\text{state}_i,r_i)$，并不直接参与$H$和$C$之间的加密跨链交易，也不直接获取通道状态$\text{state}_i$和盲化随机数$r_i$，无法获取具体的跨链交易信息。

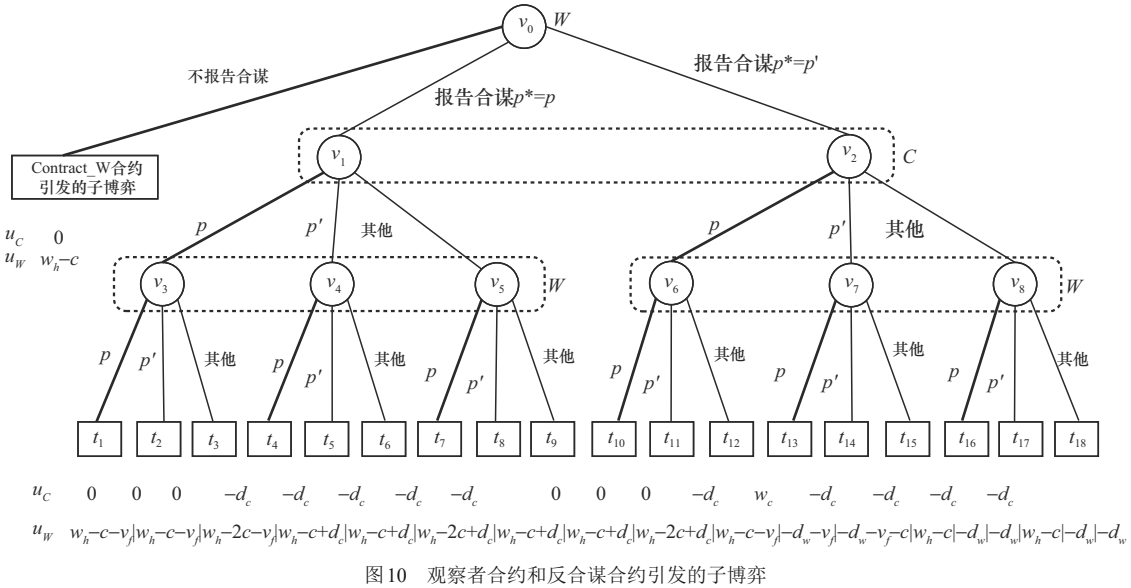


图10　观察者合约和反合谋合约引发的子博弈

跨链结算验证信息只包含经过哈希加密的最终通道状态 $p_{\text{sett}} = H(\text{state}_{\text{sett}}, r_{\text{sett}})$，而非 $\text{state}_{\text{sett}}$。关闭跨链通道时，只需要验证最新的通道状态 $H(\text{state}_{\text{sett}}, r_{\text{sett}})$ 并达成跨链共识，然后将通道最终状态 $H(\text{state}_{\text{sett}}, r_{\text{sett}})$ 公布并记录在中继链上，以在中继链和业务链之间实现安全结算。

当发现合谋时，盲化随机数 r_i、r_{sett} 会被披露，以完成存在合谋情况下针对合谋者的验证过程，此时会揭露部分隐私。但定理 1 证明了不合谋是通道用户的最优策略。

证毕。

定理 3 证明 在跨链通道建立前，所有跨链通道参与者 H、C 和 W 都需要提前在其所在的源区块链上进行质押，并作为跨链通道的初始状态 p_0。

根据定理 1，不合谋是所有跨链通道参与者的最优选择，最终跨链通道结束时，跨链通道参与方均提供正确的最终通道状态证明 $H(\text{state}_{\text{sett}}, r_{\text{sett}})$ 并签名 σ_i^{state}。在跨链结算过程中，各中继链和业务链只需首先对各方签名 σ_i^{state} 进行验证，然后对加密的最终通道状态证明 $H(\text{state}_{\text{sett}}, r_{\text{sett}})$ 进行验证，即可达成跨链共识，并关闭跨链通道。

虽然所提方案保证了不合谋是所有用户的主导策略，接下来，本文仍给出了一个合谋情况下可验证性的例子。考虑一个恶意用户 C 与观察者 W_C 合谋，期望以虚假状态证明 $p'_{\text{sett}} = H(\text{state}'_{\text{sett}}, r'_{\text{sett}})$ 而非真实的状态证明 $p_{\text{sett}} = H(\text{state}_{\text{sett}}, r_{\text{sett}})$ 进行跨链结算，其中 $\text{state}'_{\text{sett}} = (v'_H, v'_C, v'_{W_C})$，$\text{state}_{\text{sett}} = (v_H, v_C, v_{W_C})$，且 $v'_H < v_H, v'_C > v_C, v'_{W_C} > v_{W_C}$。因为用户 H 提供的最终通道状态证明为 $p_{\text{sett}} = H(\text{state}_{\text{sett}}, r_{\text{sett}})$，即通道用户提供的最终加密通道状态不同，则需要用户 H 和 C 揭示盲化随机数 r_{sett} 和 r'_{sett}，并获得原始的通道状态证明 $\text{state}_{\text{sett}}$ 和 $\text{state}'_{\text{sett}}$ 进行验证，以确定最新的通道状态，并进行跨链结算。

在跨链结算过程中，各中继链和业务链根据算法 6 对结算信息中的证明 p_{sett} 进行验证，通过跨链共识之后，完成跨链交易并关闭跨链通道。如果跨链通道参与者 H、C 和 W 诚实，则在跨链通道关闭结束后，通道参与者可以拿回跨链通道建立前所有的质押。否则，可以由 p_{sett} 揭示 r_{sett} 获得 $\text{state}_{\text{sett}}$，并根据 $\text{state}_{\text{sett}}$ 验证结果进行结算，即最终跨链结算过程中会对合谋者的违规行为进行跨链验证并达成跨链共识。

综上，虽然跨链通道内的详细跨链交易信息不可见，跨链交易过程中跨链通道参与者的诚实或作弊行为是可以验证的。

证毕。

参考文献：

[1] TAO Y C, LI B, LI B C. On atomicity and confidentiality across blockchains under failures[J]. IEEE Transactions on Knowledge and Data Engineering, 2024, 36(2): 766-780.

[2] GUO Y H, XU M H, YU D X, et al. Cross-channel: scalable off-chain channels supporting fair and atomic cross-chain operations[J]. IEEE Transactions on Computers, 2023, 72(11): 3231-3244.

[3] ZHANG X X, QIAN C. A cross-chain payment channel network[C]// Proceedings of the 2023 IEEE 31st International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2023: 1-11.

[4] JIA X F, YU Z, SHAO J, et al. Cross-chain virtual payment channels[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 3401-3413.

[5] HAUGUM T, HOFF B, ALSADI M, et al. Security and privacy challenges in blockchain interoperability - A multivocal literature review[C]// Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering. New York: ACM Press, 2022: 347-356.

[6] BUTERIN V. Chain interoperability[R]. 2016.

[7] 叶少杰, 汪小益, 徐才巢, 等. BitXHub: 基于侧链中继的异构区块链互操作平台[J]. 计算机科学, 2020, 47(6): 294-302.
YE S J, WANG X Y, XU C C, et al. BitXHub: side-relay chain based heterogeneous blockchain interoperable platform[J]. Computer Science, 2020, 47(6): 294-302.

[8] KWON J, BUCHMAN E. Cosmos white paper[R]. 2019.

[9] WOOD D G. Polkadot: vision for a heterogeneous multi-chain framework[R]. 2016.

[10] TIAN H Y, XUE K P, LUO X Y, et al. Enabling cross-chain transactions: a decentralized cryptocurrency exchange protocol[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3928-3941.

[11] 马宇航, 张亮, 吴星雨, 等. 基于分布式密钥生成和属性基密码的多方跨链交易方案[J]. 计算机研究与发展, 2023, 60(11): 2534-2544.
MA Y H, ZHANG L, WU X Y, et al. Multi-party cross-chain transaction scheme based on distributed key generation and attribute-based encryption[J]. Journal of Computer Research and Development, 2023, 60 (11): 2534-2544.

[12] 李芳, 李卓然, 赵赫. 区块链跨链技术进展研究[J]. 软件学报, 2019, 30(6): 1649-1660.
LI F, LI Z R, ZHAO H. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software, 2019, 30(6): 1649-1660.

[13] KHOSLA A, SARAN V, ZOGHB N. Techniques for privacy over the interledger[R]. 2018.

[14] SAI K, TIPPER D. Disincentivizing double spend attacks across interoperable blockchains[C]//Proceedings of the 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). Piscataway: IEEE Press, 2019: 36-45.

[15] XIE J F, YU F R, HUANG T, et al. A survey on the scalability of blockchain systems[J]. IEEE Network, 2019, 33(5): 166-173.

[16] 贾林鹏, 裴奇, 王鑫, 等. 链下通道路由算法综述[J]. 软件学报, 2022, 33(1): 233-253.
JIA L P, PEI Q, WANG X, et al. Survey on offchain channel routing algorithm[J]. Journal of Software, 2022, 33(1): 233-253.

[17] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[R]. 2016.

[18] DZIEMBOWSKI S, FAUST S, HOSTÁKOVÁ K. General state channel networks[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 949-966.

[19] DZIEMBOWSKI S, ECKEY L, FAUST S, et al. Perun: virtual payment hubs over cryptocurrencies[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2019: 106-123.

[20] DZIEMBOWSKI S, ECKEY L, FAUST S, et al. Multi-party virtual state channels[C]//Proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Berlin: Springer, 2019: 625-656.

[21] PAPADIS N, TASSIULAS L. Payment channel networks: single-hop scheduling for throughput maximization[C]//Proceedings of the IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2022: 900-909.

[22] ZHANG X X, QIAN C. Towards aggregated payment channel networks[C]//Proceedings of the 2022 IEEE 30th International Conference on Network Protocols (ICNP). Piscataway: IEEE Press, 2022: 1-11.

[23] 陈晶, 杨浩, 何琨, 等. 区块链扩展技术现状与展望[J]. 软件学报, 2024, 35(2): 828-851.
CHEN J, YANG H, HE K, et al. Current situation and prospect of blockchain scaling technology[J]. Journal of Software, 2024, 35(2): 828-851.

[24] 解岩凯, 魏凌波, 张驰, 等. 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, et al. On watchtower of payment channel for blockchain light nodes[J]. Journal of Cryptologic Research, 2021, 8(5): 778-794.

[25] THOMAS S, SCHWARTZ E. A protocol for interledger payments[R]. 2016.

[26] MALAVOLTA G, MORENO-SANCHEZ P, SCHNEIDEWIND C, et al. Anonymous multi-hop locks for blockchain scalability and interoperability[C]//Proceedings of the 2019 Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2019: 1-15.

[27] WANG X H, LIN C, HUANG X Y, et al. Anonymity-enhancing multi-hop locks for monero-enabled payment channel networks[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 2438-2453.

[28] DONG C Y, WANG Y L, ALDWEESH A, et al. Betrayal, distrust, and rationality: smart counter-collusion contracts for verifiable cloud computing[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 211-227.

[29] WU S K, CHEN Y J, WANG Q, et al. CReam: a smart contract enabled collusion-resistant e-auction[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(7): 1687-1701.

[30] JIA X D, WANG L M, CHENG K, et al. A blockchain-based privacy-preserving and collusion-resistant scheme (PPCR) for double auctions [J]. Digital Communications and Networks, 2023: doi. org/10.1016/j. dcan.2023.05.002.

[31] 刘敖迪, 杜学绘, 王娜, 等. 区块链系统安全防护技术研究进展[J]. 计算机学报, 2024, 47(3): 608-646.
LIU A D, DU X H, WANG N, et al. Research progress on blockchain system security technology[J]. Chinese Journal of Computers, 2024, 47 (3): 608-646.

[32] 周子钰, 张宗洋, 刘建伟. 中本聪共识安全性质研究方法[J]. 中国科学: 信息科学, 2022, 52(5): 837-855.
ZHOU Z Y, ZHANG Z Y, LIU J W. Methods of security analysis for Nakamoto consensus[J]. Scientia Sinica (Informationis), 2022, 52(5): 837-855.

[33] 张宝, 田有亮, 高胜. 基于博弈论抗合谋攻击的全局随机化共识算法[J]. 网络与信息安全学报, 2022, 8(4): 98-109.
ZHANG B, TIAN Y L, GAO S. Global randomized consensus algorithm resist collusion attack based on game theory[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 98-109.

[34] 付晓东, 漆鑫鑫, 刘骊, 等. 基于权力指数的DPoS合谋攻击检测与预防[J]. 通信学报, 2022, 43(12): 123-133.
FU X D, QI X X, LIU L, et al. Detecting and preventing collusion attack in DPoS based on power index[J]. Journal on Communications, 2022, 43(12): 123-133.

[35] MCCORRY P, BAKSHI S, BENTOV I, et al. Pisa: arbitration outsourcing for state channels[C]//Proceedings of the 1st ACM Conference on Advances in Financial Technologies. New York: ACM Press, 2019: 16-30.

[36] ZHANG Y H, YANG D J, XUE G L, et al. Counter-collusion smart contracts for watchtowers in payment channel networks[C]//Proceedings of the IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2021: 1-10.

[37] DU M, YANG P, TIAN W, et al. Anti-collusion multiparty smart contracts for distributed watchtowers in payment channel networks[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3600-3614.

[作者简介]

贾雪丹（1988– ），女，山东德州人，海南师范大学讲师，主要研究方向为区块链安全、隐私保护技术。

王良民（1977– ），男，安徽潜山人，博士，东南大学教授、博士生导师，主要研究方向为密码学与安全协议、物联网安全、大数据安全及区块链技术。

黄龙霞（1991– ），女，江苏泰州人，博士，江苏大学副教授，主要研究方向为信息安全、云存储安全、区块链安全。