计 算 机 研 究 与 发 展
Journal of Computer Research and Development

https://crad.ict.ac.cn
63(10): 2543−2556, 2026

本期推荐

面向智能终端的状态通道离线代理与容错恢复框架

王 晨[1] 赫丽勤[1] 马昊玉[2] 沈 剑[1] 贾春福[3]

[1](浙江理工大学信息科学与工程学院(网络空间安全学院) 杭州 310018)

[2](北京交通大学网络空间安全学院(国家保密学院) 北京 100044)

[3](南开大学密码与网络空间安全学院 天津 300350)

(wangchen@zstu.edu.cn)

A State Channel Framework with Offline Proxy and Fault-Tolerant Recovery for Intelligent Terminals

Wang Chen[1], He Liqin[1], Ma Haoyu[2], Shen Jian[1], and Jia Chunfu[3]

[1](*School of Information Science and Engineering* (*School of Cyber Science and Technology*), *Zhejiang Sci-Tech University*, *Hangzhou* 310018)

[2](*School of Cyberspace Science and Technology* (*School of State Secrets Protection*), *Beijing Jiaotong University*, *Beijing* 100044)

[3](*College of Cryptology and Cyber Science*, *Nankai University*, *Tianjin* 300350)

Abstract State channels provide an effective solution for blockchain scalability by migrating transaction execution off-chain. However, existing approaches typically rely on strong assumptions, such as a static set of participants, continuously online nodes, and extremely low failure rates. These assumptions are difficult to satisfy in intelligent terminal environments and significantly hinder practical deployment. To address these challenges, we propose a state channel framework with offline proxy and fault-tolerant recovery for intelligent terminals. The main contributions are summarized as follows: 1) To mitigate channel reconstruction overhead caused by frequent joining and leaving of intelligent terminals, a dynamic membership management mechanism is proposed. Based on joint group signatures and symmetric credential verification, it enables members to complete permission changes without exposing real identities, achieving privacy-preserving and secure admission in dynamic environments. 2) To address transaction interruption caused by intermittent connectivity of intelligent terminals, a trusted execution environment (TEE)-assisted offline proxy mechanism is designed. Participants delegate transaction signing and state updates to a locally deployed TEE array, where offline proxy execution is performed in an isolated environment, ensuring continuity of blockchain operations in asynchronous and dynamic scenarios. 3) To cope with node failures or state loss risks, a fault-tolerant state recovery mechanism based on low-density parity-check (LDPC) codes is proposed. Participant states are encoded into sparse fragments and distributed across the TEE array, and sparse parity-check decoding is exploited to achieve high-probability and efficient fault-tolerant recovery. Experimental results demonstrate that, compared with existing methods, the proposed framework improves transaction success rates by 1.36–1.51 times, reduces latency by 20%–30%, and maintains system availability above 95% even with 20% state data loss, exhibiting significant

收稿日期: 2026-06-04; **修回日期**: 2026-07-09

基金项目: 国家重点研发计划(2023YFB2703700); 国家自然科学基金项目(62302457, 62441228); 浙江省自然科学基金项目(LQ24F020008); 浙江省领军型创新团队(2023R01001); 京津冀自然科学基金合作专项(25JJJC0005)

This work was supported by the National Key Research and Development Program of China (2023YFB2703700), the National Natural Science Foundation of China (62302457, 62441228), the Zhejiang Provincial Natural Science Foundation of China (LQ24F020008), the Program for Leading Innovative Research Team of Zhejiang Province (2023R01001), and the Foundation Items: Beijing-Tianjin-Hebei Natural Science Cooperation Project (25JJJJC0005).

通信作者: 沈剑(shenjian@zstu.edu.cn)

performance advantages in dynamic intelligent terminal environments and partial failure scenarios.

Key words blockchain; state channel; intelligent terminals; offline proxy; fault-tolerant recovery

摘 要 状态通道通过将交易迁移至链外执行,为区块链扩展性提供了一种有效的解决方案。然而,现有方案通常假设参与者集合静态不变、节点持续在线且故障率极低,这些强假设难以适配智能终端场景,严重制约了其实际部署。为应对上述挑战,提出一种面向智能终端的状态通道离线代理与容错恢复框架,核心贡献包括3个方面:1)针对智能终端频繁加入或离开导致的通道重构开销,提出一种动态成员管理机制,基于联合组签名与对称凭证验证等技术,支持成员在不暴露真实身份的前提下完成权限变更,实现动态环境下的隐私保护与安全准入;2)针对智能终端间歇性连接导致的事务中断问题,设计一种可信执行环境(trusted execution environment, TEE)辅助的离线代理机制,参与者将交易签名和状态更新委托至本地部署的TEE阵列,在隔离环境中完成离线代理执行,保障异步动态场景下的区块链操作连续性;3)针对节点故障或状态丢失风险,提出一种基于低密度奇偶校验(low-density parity-check, LDPC)码的容错状态恢复机制,将参与方状态编码为稀疏分片并分散存储至TEE阵列,并利用稀疏奇偶校验解码实现高概率高效容错恢复。实验结果表明,与现有方法相比,所提出框架的交易成功率达到现有方法的1.36~1.51倍,延迟降低20%~30%,在20%状态数据丢失的情况下,系统的可用性仍保持在95%以上,在智能终端动态环境与部分故障场景下展现出显著的性能优势。

关键词 区块链;状态通道;智能终端;离线代理;容错恢复

中图法分类号 TP311.13; TP309

DOI: 10.7544/issn1000-1239.202660403 **CSTR:** 32373.14.issn1000-1239.202660403

区块链是一种去中心化、防篡改的分布式账本技术,能够在不可信参与方之间实现安全、透明的数据记录[1]。凭借其无需预设信任的运行机制与强数据完整性保障,区块链已在数据共享[2]、联邦学习[3],以及元宇宙[4]等领域获得广泛应用。然而,链上交易吞吐量的固有限制构成了区块链可扩展性[5]的核心瓶颈,从而推动了第2层(Layer-2)扩展方案的发展。

Layer-2是部署于底层区块链之上的扩展技术,通过将大量交易执行、状态更新或计算过程迁移至链下,仅在必要时将关键状态或最终结果提交至链上,从而在保证底层区块链安全性的同时显著提升系统吞吐量、降低交易确认延迟和链上存储开销。目前,Layer-2技术主要包括状态通道、侧链、Rollup以及Plasma等方案。其中,状态通道由于能够实现低延迟、低成本的链下交互,并保持链上最终一致性,已成为区块链Layer-2扩展的重要技术路线之一,尤其适用于高频交互和资源受限的智能终端应用场景。

状态通道作为一类成熟的第2层扩展技术[6-8],允许参与方在链下完成快速、低成本的交易交互,仅在通道开启和最终结算阶段将关键状态提交至链上。状态通道的生命周期可分为3个阶段:在初始化阶段,参与方将资金或状态提交至链上的智能合约,该合约可作为系统的加密锚点;在链下交互阶段,参与方通过交换签名消息来共同实现状态转移;在交互结算阶段,双方最近一次达成一致的状态提交至链上进行验证和最终结算。以闪电网络[9-10]、虚拟通道[11-12]及Celer Network[13]为代表的实际系统已验证了该范式在提升系统吞吐量与降低链上开销方面的显著优势。尽管如此,现有状态通道设计仍面临静态参与者集合、持续在线要求及有限容错能力等关键约束,难以适配智能终端所处的动态、异步及资源受限环境,严重制约其实际部署。

具体而言,首先,大多数现有方案假设参与方集合固定不变,缺乏安全高效的成员加入或退出机制,通道重构成本高昂。其次,状态通道协议通常要求参与方持续在线以完成交易签名和状态同步,这一持续在线的需求限制了其在资源受限的智能终端上的部署,临时断连或设备故障可能导致交易中断,可用性保障不足。此外,现有状态通道设计的容错能力有限,当参与方崩溃或丢失本地状态时,恢复通常依赖链上仲裁、中心化备份或人工干预,削弱了区块链自治原则。上述3类缺陷在智能终端场景中尤为突出。

针对上述挑战,可信执行环境(trusted execution environment, TEE)[14]与纠删码技术为状态通道的优

化提供了新思路。TEE 通过硬件隔离实现安全计算，已广泛应用于隐私保护的链下执行场景[15]。然而，TEE 辅助方案往往存在中心化信任假设、回滚攻击以及硬件漏洞等风险[16]。纠删码作为高性价比的数据冗余手段，能够在部分数据丢失时重建原始信息[17]，而传统纠删码在区块链状态恢复中的计算开销与去中心化适配问题尚待解决。低密度奇偶校验（low-density parity-check, LDPC）码[18]因其稀疏校验矩阵带来的近最优恢复性能与低计算开销，为资源受限场景下的高效容错恢复提供了潜在路径。

针对现有状态通道在静态参与者集合、持续在线要求及有限容错能力等方面的局限，提出一种面向智能终端的状态通道离线代理与容错恢复框架，旨在全面提升动态环境下的灵活性、可用性和鲁棒性。核心贡献包括：

1）提出一种动态成员管理机制，基于联合群签名与对称凭证验证构建安全准入协议，使参与方能够在不暴露真实身份的前提下完成权限变更，实现不中断通道运行的成员动态加入与退出，解决智能终端频繁成员变化导致的通道重构开销问题。

2）设计一种 TEE 辅助的离线代理机制，采用本地部署的 TEE 阵列作为代理执行载体，参与方在受限策略下自主处理委托交易，支持安全的链下状态更新和交易签，保障异步动态场景下的区块链操作连续性，缓解智能终端间歇性连接导致的交易中断问题。

3）提出一种基于 LDPC 码的容错状态恢复机制，参与方状态被编码为稀疏分片并分布到 TEE 阵列中，节点故障或数据丢失时通过解码存活分片的子集高概率恢复原始状态，实现无需中心化备份的容错恢复。

上述机制形成面向智能终端场景的协同框架：动态成员管理输出的权限更新情况实时同步到 TEE 阵列；TEE 阵列承担离线执行与状态分片存储；LDPC 编码的稀疏状态分片结构适配成员动态变更的增量状态重构。三者协同实现了动态环境下状态通道运行，避免了传统方案中成员变动导致的通道频繁重构、离线导致的交易中断以及故障导致的状态丢失等问题。

1 相关工作

本节主要介绍区块链扩展、TEE 辅助的链下执行以及基于纠删码的状态恢复等技术的研究现状，并总结它们在动态成员管理、安全链下执行以及容错状态恢复方面的能力与局限性。

为提升区块链系统的可扩展性[19]，近年来 Layer-2 技术得到了广泛研究。Kalodner 等人[20]提出了 Arbitrum 链下扩展方案，通过链下执行智能合约、链上欺诈挑战验证机制完成交易确认，在保证底层区块链安全性的同时有效提升了系统吞吐量，并兼顾了智能合约执行效率与隐私保护能力。Han 等人[21]针对 Rollup 中心化排序器存在的单点故障、审查攻击及性能瓶颈问题，提出了一种基于共享排序器的多槽位加权领导者选举算法，通过引入提议者–构建者分离机制，有效降低了恶意节点当选概率，并提升了 Layer-2 网络的交易处理性能与鲁棒性。TrustPay[22]提出了一种双层区块链服务交易框架，采用父链–子链协同架构及 REFEREE 共识协议，实现了 Web 服务交易记录、自动结算和可信支付，提高了系统的可扩展性和交易处理效率。然而，上述 Layer-2 方案主要面向通用链下扩展或 Rollup 场景，对参与节点频繁离线、动态成员管理以及状态恢复等问题关注较少。相比之下，状态通道通过将交易执行与状态更新限制在固定参与方之间，具有低时延、低链上开销等优势，更适用于智能终端等高频交互场景。

状态通道作为解决公有区块链可扩展性瓶颈的典型第二层方案，能够显著提升吞吐量并降低交易延迟。代表性工作包括闪电网络[9-10,23]和 Raiden 网络[24]，它们通过构建链下支付通道网络，实现了低成本、高效率的微支付机制。针对支付通道中的隐私泄露问题，Gai 等人[25]提出一种基于承诺的匿名支付通道，以实现无限制的链下双向支付，并保证参与者的隐私。在此基础上，研究者进一步针对通道网络的可扩展性与灵活性问题提出改进方案，Aumayr 等人[11]提出虚拟通道概念，使中间节点仅在创建阶段参与，建立后交易双方可独立执行任意多次链下交易，无需中间节点后续介入，显著提升了支付通道网络的可靠性与效率。Wei 等人[12]在此基础上提出 Thor 协议，引入容量与中间节点数量比率指标，为多个用户配对高效构建虚拟支付通道网络，优化了资金利用效率。随着应用需求的拓展，状态通道逐渐从专用支付向通用计算模型演进。后续的改进方案，如 Perun[26]、Counterfactual[27]、一般支付通道等，将状态通道推广至支持任意链下状态更新和智能合约执行，突破了传统支付场景的限制，成为一种通用的链下扩展框架。Celer Network[13]作为运行于现有区块链之上的网络化链下扩展系统，通过通用状态通道与侧链套件支持快速链下状态转换，推动状态通道向

互联网规模落地。然而，这些系统通常假设参与方为固定集合，并要求所有参与方在通道生命周期内保持持续在线。由于实际应用中参与方可能频繁变动且网络连接不稳定，这些假设限制了其在动态或资源受限环境下的实际可用性。

TEE 在链下区块链架构中得到广泛关注，用于实现可验证机密计算。代表性系统如 DeCloak[16]、Ekiden[28] 以及近期的一些方案[29-30] 利用 TEE 在链下安全执行智能合约，并通过远程证明确保完整性和可审计性。Teechain[31] 提出了一种高性能第二层支付网络，通过 TEE 支持异步链下交易。对于状态通道，TEE 提供了安全委托、私密状态转移和低延迟争议解决等关键能力。然而，现有许多 TEE 辅助方案仍存在固有局限，如依赖中心化信任锚点，以及在节点故障或数据丢失时缺乏稳健的状态持久化与恢复机制。

为了降低区块链存储开销并提升数据可用性，纠删码技术被广泛探索。早期工作[32-33] 将纠删码引入区块链存储层，以支持低成本冗余和容错数据检索。LDPC 由于稀疏校验矩阵、接近最优的解码性能及低计算开销而受到关注。相关研究[34-36] 展示了将 LDPC 码整合至去中心化存储和云-边协作系统的可行性。然而，LDPC 码在区块链环境，尤其是在需要实时恢复、低延迟和最小冗余开销的动态链下环境的应用仍相对有限。

表 1 对所提出的方案与现有代表性状态通道方案进行了综合比较。传统方案如闪电网络[10] 和 Perun[26] 虽然支持链下交易，但基本不具备动态成员管理和健壮的状态恢复机制。Ekiden[28] 和 Teechain[31] 虽然通过硬件隔离增强了安全性，但它们要么依赖静态信任假设，要么无法在通道关闭过程中应对网络级攻击。SharHSC[37] 通过引入基于分片的监督委员会，实现了部分离线执行和拜占庭容错状态恢复。

Table 1 Functions Compared with the Existing Schemes

表 1 与现有方案的功能比较

方案	动态性	离线性	可恢复性	TEE	韧性	通道类型
Lightning[10]	×	×	×	×	×	HTLC
DeCloak[16]	√	√	△	√	△	Hybrid
Perun[26]	×	×	×	×	×	Virtual
Ekiden[28]	×	×	×	√	×	Hybrid
Teechain[31]	×	√	×	√	×	Ledger
SharHSC[37]	×	△	△	×	×	Hybrid
本文	√	√	√	√	√	Hybrid

注：√表示全部支持，△表示部分支持，×表示不支持。

与 DeCloak[16] 使用分布式 TEE 进行有限恢复不同，SharHSC 通过其所设计架构实现去中心化共识，同时保持与现有区块链系统的兼容性。

2 系统概述

2.1 系统模型

本文提出了一种支持动态多方参与、离线场景下高可用的区块链状态通道系统模型。该模型将 TEE[14] 与基于编码的冗余技术相结合，以提升系统的安全性与韧性。系统由 3 类核心组件协同构成：动态参与节点、TEE 代理网络与底层区块链。这些组件协同工作，以实现动态成员管理、离线状态维护以及故障后的快速恢复。

动态参与节点是系统的基本实体，负责交易签名、状态更新与执行。每个节点集成轻量级身份认证模块、本地 TEE 实例以及状态分片编码器，分别支撑成员准入、离线代理与容错恢复功能。

TEE 代理网络构成分布式执行层，由各节点上的本地 TEE 实例组成，承担离线交易处理、群签名验证及状态分片管理任务。该网络在节点间歇断连期间维持操作连续性，并在故障发生时提供状态重建所需的分片数据。

底层区块链作为最终争议仲裁层，仅负责记录通道初始化参数、成员变更承诺及最终结算状态。正常运行时最小化链上交互以降低开销，仅在争议裁决或通道生命周期关键节点介入。

2.2 系统架构

本文设计了一种基于 TEE 代理的动态状态通道架构。如图 1 所示，该架构包括区块链争议仲裁层、动态参与实体层及分布式执行层。

区块链争议仲裁层通过智能合约验证成员变更与状态承诺，作为最终的争议仲裁与状态锚定层。该层仅在通道开启、关闭及异常争议时介入，正常运行期间最小化链上交互以降低系统开销。

动态参与实体层负责本地状态管理与成员生命周期操作。各参与实体通过轻量级身份认证模块完成安全加入与退出，并将交易签名及状态更新委托至本地 TEE 实例执行。

TEE 代理网络层通过在 TEE 阵列中引入基于 LDPC 码的冗余编码机制，实现离线运行支撑与分布式状态恢复，在节点发生故障时保证系统的高效容错恢复能力。

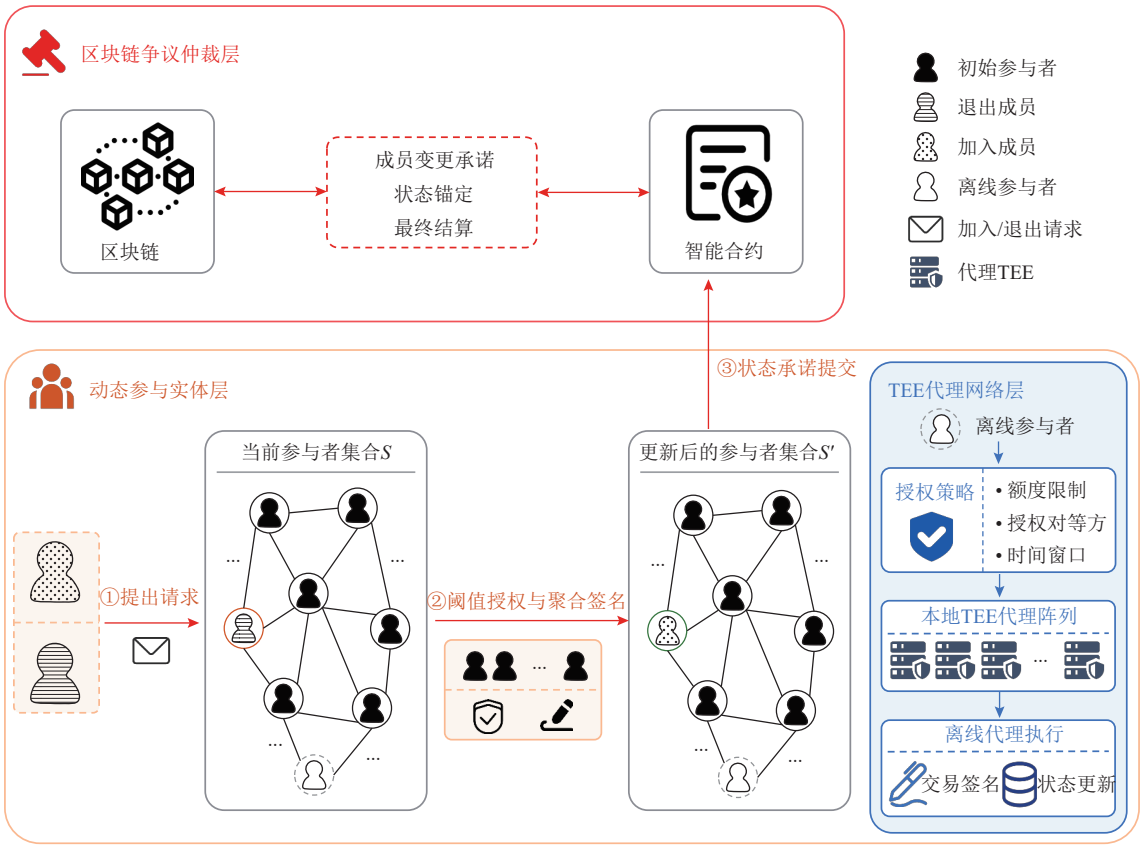


Fig. 1 Architecture of TEE agent-based dynamic state channels

图 1 基于 TEE 代理的动态状态通道架构

3 状态通道离线代理与容错恢复框架

本文设计了一种基于 LDPC 编码的分布式状态恢复机制。该机制通过对状态数据进行分片与低密度奇偶校验编码，在保证较低存储开销的同时，为系统提供冗余容错能力；同时结合 TEE 辅助存储与恢复策略，实现状态数据的安全分布式存储与快速重构。当部分节点失效或状态片段丢失时，系统能够利用剩余有效数据片段完成原始状态恢复，从而增强链下状态通道的鲁棒性与连续运行能力。其整体架构如图 2 所示。方案的核心由动态成员管理、

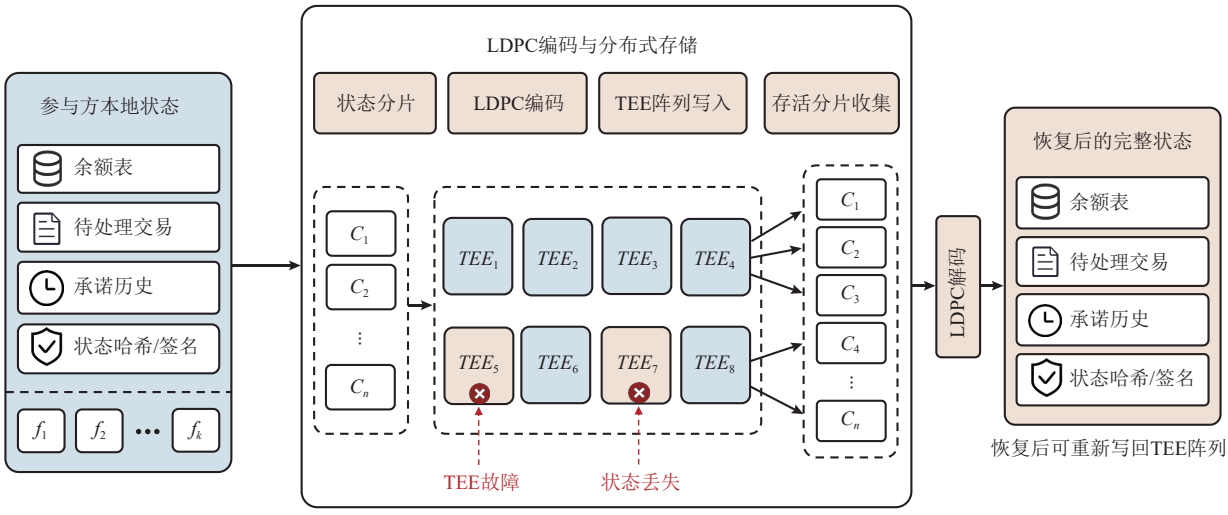


Fig. 2 Architecture of distributed state recovery based on LDPC coding

图 2 基于 LDPC 编码的分布式状态恢复架构

TEE 辅助的离线代理及基于 LDPC 码的容错状态恢复 3 个机制从准入、执行、容错 3 个层面形成完整框架: 动态成员管理为 TEE 代理网络提供可信的参与者集合与权限基线; TEE 代理网络在隔离环境中执行离线委托与状态分片管理; 容错恢复机制则为 TEE 阵列中的状态分片提供冗余保障, 确保节点故障时的状态可重建。以下对框架的整体工作流程及 3 个核心机制进行详细阐述。

3.1 动态成员管理机制

动态成员管理机制负责维护状态通道参与者集合的生命周期, 支持参与者在不暴露真实身份的前提下完成安全准入与权限变更, 避免因成员变动导致的通道频繁重构。

1)系统初始化。设 $\mathbb{G}_1$、$\mathbb{G}_2$和$\mathbb{G}_T$为阶为大素数 p 的乘法循环群, 并定义双线性映射 e: $\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$。设 $g_1\in\mathbb{G}_1$和 $g_2\in\mathbb{G}_2$分别为 $\mathbb{G}_1$与 $\mathbb{G}_2$的生成元。定义哈希函数 H_1: $\{0,1\}^*\to\mathbb{G}_1$, 用于将任意长度的二进制字符串映射到群 $\mathbb{G}_1$中的元素。在状态通道初始化阶段, 可信密钥生成中心(key generation center, KGC)为每个参与者 P_i生成唯一的密钥对: 随机选择私钥 $sk_i\in\mathbb{Z}_p$, 并计算其对应的公钥。私钥 sk_i通过安全信道分发给参与者 P_i, 公钥 pk_i则公开发布并维护于系统公钥列表$\{pk_i\}$中。

$$pk_i=g_2^{sk_i}\in\mathbb{G}_2\ 。\tag{1}$$

2)新成员加入。设状态通道的初始参与者集合为 $\mathcal{P}=\{P_1,P_2,\cdots,P_n\}$, 各参与者 P_i对应唯一标识符 ID_i。当新参与者 P_{new}请求加入状态通道时, 其构造加入请求消息 $M_{\text{new}}=(PK_{\text{new}}\|ID_{\text{new}}\|T)$, 其中 T为时间戳, 并通过认证 P2P 网络向当前所有参与者 $\mathcal{P}$广播该请求。

系统采用动态阈值实现成员变更授权, 成员变更所需的最小授权阈值定义为 $t=\lceil 2n/3\rceil$, 其中 n表示当前状态通道中的参与者数量。该阈值兼顾系统安全性与容错能力。现有成员 $P_i\in\mathcal{P}$($|\mathcal{P}|=n\geqslant t$)收到加入请求后, 首先验证请求者身份信息; 若验证通过, 使用其私钥 sk_i对加入请求消息 M_{new}计算签名 $\sigma_i=H(M_{\text{new}})^{sk_i}\in\mathbb{G}_1$。$P_{\text{new}}$从当前成员中收集至少 t个有效签名, 记为$\{\sigma_{i_1},\sigma_{i_2},\cdots,\sigma_{i_t}\}$。构造聚合签名:

$$\sigma=\prod_{j=1}^{t}\sigma_{i_j}=H(M_{\text{new}})^{\sum_{j=1}^{t}sk_{i_j}}\ 。\tag{2}$$

对应地, 签名者的公钥聚合为:

$$pk=\prod_{j=1}^{t}pk_{i_j}=g_2^{\sum_{j=1}^{t}sk_{i_j}}\ 。\tag{3}$$

状态通道的链上智能合约作为验证方, 通过计算双线性对等式来验证聚合签名 σ的有效性:

$$e(\sigma,g_2)=e(H(M_{\text{new}}),pk)\ 。\tag{4}$$

若等式成立, 智能合约批准该加入请求, 并将 P_{new}加入状态通道参与者集合并更新公钥列表; 否则, 拒绝请求。该机制保证新成员仅在获得诚实多数授权后方可加入, 维持动态环境下的安全性与一致性。

3)现有成员退出。当现有成员 P_{leave}发起退出状态通道的请求时, 其提交的请求中需包含该参与者最近一次的本地状态 H_{S}以及当前交易承诺。链上智能合约执行以下验证: 验证所提交状态是否与通道的最新确认状态保持同步, 并检查是否存在涉及该参与者的待处理或未确认交易。若验证通过且所有相关交易均已完成结算, 则更新成员集合为 $\mathcal{P}_{\text{new}}\leftarrow\mathcal{P}\backslash\{P_{\text{leave}}\}$, 此后, 在后续状态签名过程中将不再包含参与者 P_{leave}的公钥。验证通过后, 进入强制宽限期, 允许其他成员对提交状态提出争议, 防止恶意退出或伪造状态。

算法 1 形式化描述了成员退出的链上处理逻辑。该过程首先验证成员当前提交的状态, 并确保其与通道最近一次确认的状态承诺保持一致; 随后检查是否存在涉及该参与者的待处理或未确认交易, 以防止在仍存在未履行义务的情况下提前退出。当所有检查均通过后, 退出请求将进入一个强制宽限期, 在此期间其他成员可以对提交状态提出争议。该争议窗口可有效防止恶意退出或伪造状态声明的行为。

算法 1. 状态通道成员退出流程。

输入: 退出请求参与者 P_{leave}, 状态哈希值 H_{S};

输出: 退出请求批准或拒绝。

① if $P_{\text{leave}}\notin\mathcal{P}$ then

② return 拒绝(参与者未激活);

③ end if

④ if H_{S}不包含 P_{leave}状态分量 then

⑤ return 拒绝(状态不匹配);

⑥ end if

⑦ if 存在涉及 P_{leave}的未确认交易 then

⑧ return 拒绝(存在待处理交易);

⑨ end if

⑩ 标记 P_{leave}退出请求为待处理;

⑪ 将退出记录的区块编号记录为当前区块;

⑫ while 宽限期未过期 do

⑬ if 检测到提交状态争议 then

⑭ 取消退出请求;

⑮ return 拒绝(状态存在争议)；

⑯ end if

⑰ end while

⑱ 更新集合：$\mathcal{P}' \leftarrow \mathcal{P}\backslash\{P_{\text{leave}}\}$ 共识阈值：$t' = \lceil 2|P'|/3 \rceil$；

⑲ 将P_{leave}公钥从后续状态签名中移除；

⑳ return 批准。

如果在规定时间内未出现有效争议，则该参与者将被正式从成员集合$\mathcal{P}$中移除，从当前轮次之后的下一轮起，其公钥将不再参与状态生成与验证过程。同时，由于状态转换通过哈希链相互关联，并将关键承诺锚定在链上，因此历史签名仍然可以被正常验证，从而保证系统的向后安全性。在成员成功退出后，其余参与者需要更新本地维护的成员集合$P' \leftarrow P\backslash\{P_{\text{leave}}\}$，重新计算系统的共识阈值$t' = \lceil 2|P'|/3 \rceil$，将用户$P_{\text{leave}}$的公钥从后续状态签名中移除。该机制确保了在参与者集合发生变化的情况下，状态通道仍能够保持安全、稳定地运行。

当状态通道中的当前成员就最新状态达成一致后，每个参与者对该新状态进行签名，从而形成一个由全体成员共同认证的状态承诺。随后，该状态承诺被提交至区块链进行验证与记录。链上智能合约负责验证所提交的聚合签名的有效性；若验证通过，则更新链上存储的状态信息，从而保证系统状态的一致性与可审计性。

3.2 TEE 辅助的离线代理机制

TEE 辅助的离线代理机制利用参与者本地部署的 TEE 阵列，在成员授权范围内代理执行交易签名与状态更新，解决智能终端间歇性连接导致的交易中断问题。同时，TEE 阵列作为状态分片的物理载体，为后续 LDPC 编码与分布式存储提供 TEE。

1)TEE 实例部署。状态通道中的每个参与者P_i在本地部署一个专用的 TEE 阵列，表示为：

$$\left\{TEE_i^{(1)}, TEE_i^{(2)}, \cdots, TEE_i^{(k)}\right\}, \tag{5}$$

其中每个TEE为独立的安全 Enclave 实例。阵列化部署方式在参与者节点内部提升系统的容错能力，并支持并行执行，从而提高整体处理效率。

2)委托授权策略配置。每个参与者P_i定义形式化代理授权策略集合$\theta_i = (L_{\max}, \mathcal{A}_i, \mathcal{T}_i)$，规定在其离线期间允许代表其执行交易的约束条件。具体而言，θ_i包含以下内容。

① 最大交易限制$L_{\max}$：设定代理执行操作的累计交易金额或交易次数上限，防止滥用或意外的过度交易。

② 授权对等节点列表$\mathcal{A}_i \subseteq \mathcal{P}$：限定被信任的交易对手节点，仅允许这些节点发起或转发涉及P_i的代理交易。

③ 时间有效窗口$\mathcal{T}_i = [T_{\text{start}}, T_{\text{end}}]$：限定代理策略的有效时间范围，防止离线授权被无限期利用。

3)委托交易处理与状态更新。当参与方P_i暂时离线时，其 TEE 阵列在预先配置的代理策略θ_i约束下自主处理交易。该设计支持并行委托执行，并能够在单个 TEE 出现故障时提升系统的鲁棒性。其他参与方(例如$P_j \in \mathcal{P}$)可以发起一笔面向P_i的交易$Tx_{j\to i} = (amount, receiver, nonce, timestamp, context)$，该交易被发送至$P_j$的 TEE 阵列中一个可用的安全执行环境。该 TEE 的选择通过负载均衡或轮询调度策略实现。在接收到交易后，依据代理策略θ_i执行如下验证：

① $amount \leqslant L_{\max}$，交易金额不得超过预先设定的最大交易额度；

② $P_j \in \mathcal{A}_i$，交易发送方必须存在于授权的参与方列表中；

③ $timestamp \in \mathcal{T}_i$，交易时间戳必须位于允许的时间有效窗口内。

若上述条件均满足则验证通过，选定的执行环境使用其绑定的私钥$SK_i^{(r)}$对该交易进行签名：

$$\sigma_i^{TEE^{(r)}} = H(Tx_{j\to i})^{SK_i^{(r)}} \in \mathbb{G}_1 。 \tag{6}$$

随后更新本地状态S为S'，包括余额调整、*nonce*递增及其他与应用相关的状态变化。更新后的状态哈希值计算为$h(S') = H(S')$，并生成状态承诺元组：

$$C_i^{(r)} = \left(\sigma_i^{TEE^{(r)}}, S', h(S')\right) 。 \tag{7}$$

该签名后的状态承诺会被广播至其他参与方进行验证共识。一旦被法定数量的参与方接受，该更新状态将被纳入系统的链下全局状态承诺中。

3.3 基于 LDPC 码的容错状态恢复机制

基于 LDPC 码的容错状态恢复机制为 TEE 阵列中的状态数据提供冗余保障。当 TEE 实例故障或节点状态丢失时，该机制利用稀疏校验矩阵的近最优解码性能，从存活分片中高概率恢复原始状态，无需依赖中心化备份或链上仲裁。

1)状态分片与 LDPC 编码。参与方P_i的本地通道状态划分为k个等长的数据片段，构成原始状态向量：$\boldsymbol{S}_{P_i} = (s_1, s_2, \cdots, s_k) \in \mathbb{F}_2^{K\times a}$。各片段表示具有语义意义的状态单元，如余额表、待处理交易或承诺历史等。随后，利用稀疏生成矩阵$\boldsymbol{G} \in \mathbb{F}_2^{k\times\alpha}$对状态数据片段进行编码，其中$\alpha = k(1+\epsilon)$，$\epsilon \in (0,1)$为冗余因子。通过

编码生成总计α个编码片段$\boldsymbol{F}_i=(f_1,f_2,\cdots,f_\alpha)\in\mathbb{F}_2^{1\times k}$，其生成方式为$\boldsymbol{F}_i=\boldsymbol{S}_{P_i}\cdot\boldsymbol{G},\alpha>k$。前$k$个片段对应原始状态数据，剩余的$\alpha-k$个片段为由生成矩阵计算得到的校验片段。各编码片段$f_{i,j}$在存储前都会进行加密签名处理，并被安全地存放于独立且经过远程验证的 TEE 实例中，形成分布式的状态存储结构。该设计通过状态冗余与 TEE 代理网络协同，TEE 承担离线代理计算并作为编码分片的可信存储节点。

2)分布式恢复算法。LDPC 码凭借稀疏校验矩阵结构，在冗余条件满足时以高概率实现接近最优的数据恢复。设可用片段索引集合为Λ，当其数量满足$|\Lambda|\geqslant k(1+\delta)$时（$\delta$>0 表示解码裕度），即可完成原始状态重构，用于描述系统引入的冗余开销。例如，当$\delta=0.1$时，意味着系统具有约 10% 的冗余度，此时大约需要$1.1k$个片段即可恢复原始状态。

假设部分 TEE 发生故障，可用的编码片段集合为Λ_i，且满足$|\Lambda|\geqslant k$。此时系统按照如下步骤执行恢复过程：

首先，从存活的 TEE 中请求对应的编码片段，并构造收集到的片段向量$\boldsymbol{D}=(d_{i_1},d_{i_2},\cdots,d_{i_\ell})^{\mathrm{T}}$，$\ell=|\Lambda|\geqslant k$，$j_1,j_2,\cdots j_\ell\in\Lambda_i$为可用片段的原始索引。

随后，根据索引集合Λ_i，从生成矩阵$\boldsymbol{G}$中提取相应的子矩阵$\boldsymbol{G}'\in\mathbb{F}_2^{\ell\times k}$，建立线性关系$\boldsymbol{D}=\boldsymbol{G}'\cdot\boldsymbol{S}$，其中$\boldsymbol{S}\in\mathbb{F}_{2^m}^k$表示待恢复的状态向量。

接着，采用解码策略进行求解，具体的解码策略根据$\boldsymbol{G}'$的结构进行选择：当$\boldsymbol{G}'$具有稀疏结构时，采用基于置信传播的 LDPC 解码算法。恢复出各状态片段$S_{i,1},S_{i,2},\cdots,S_{i,k}$。当$\boldsymbol{G}'$较为稠密且为满秩矩阵时，则通过高斯消元法求解恢复向量$\boldsymbol{S}=(\boldsymbol{G}')^{-1}\cdot\boldsymbol{D}$，将解码得到的状态片段重新组合，得到完整的状态数据$\boldsymbol{S}=(S_{i,1},S_{i,2},\cdots,S_{i,k})$。恢复后的状态可重新分发至各 TEE 中进行存储，或直接用于后续的交易处理与状态更新。

3)解码成功概率分析。假设各 TEE 节点以概率p_f独立发生故障，则在总计α个节点中至少$k(1+\delta)$个节点存活的概率可表示为：

$$P_{\mathrm{succ}}=\sum_{\ell=k}^{\alpha}\binom{\alpha}{\ell}(1-p_f)^{\ell}(p_f)^{\alpha-\ell},\tag{8}$$

其中，$\binom{\alpha}{\ell}$表示从α个节点中选择ℓ个正常节点的组合数，$(1-p_f)^{\ell}$表示这ℓ个节点正常工作的概率，$(p_f)^{\alpha-\ell}$表示其余$\alpha-\ell$个节点发生故障的概率。通过增大编码片段数量α或降低节点故障概率，可有效提升系统的状态恢复成功率。

4 安全性分析

本节对所提框架进行全面的安全性分析。在形式化安全模型的基础上，结合密码学安全假设与概率分析方法，系统评估该方案抵御签名伪造攻击的能力、离线委托机制的安全性，以及在节点发生故障情况下状态恢复机制的鲁棒性。

4.1 动态成员管理的不可伪造性

定义 1. 动态成员管理不可伪造性。动态成员管理协议允许参与方在状态通道的生命周期内加入或退出该通道。该协议满足不可伪造性，当且仅当任何概率多项式时间攻击者$\mathcal{A}$无法在未获得不少于t个诚实节点授权的情况下，伪造一个可通过验证的新成员加入通道的聚合签名。

定理 1. 成员加入的签名不可伪造性。假设 BLS 签名方案在适应性选择消息攻击下满足存在性不可伪造性（EUF-CMA），则本方案中的动态成员管理协议能够抵御签名伪造攻击，并保证新成员的加入必须获得诚实多数节点的批准。

证明. 将攻击者与挑战者之间的交互建模为标准的密码学安全博弈。设存在一个概率多项式时间攻击者$\mathcal{A}$，其目标是在未获得足够数量诚实节点签名的情况下伪造一个有效的聚合签名。

① 初始化。挑战者为所有参与方生成密钥对$\{sk_i,pk_i\}_{i=1}^n$，并将所有公钥提供给攻击者$\mathcal{A}$。攻击者最多可以腐化$q=\lfloor(n-1)/3\rfloor$个参与方，并获得这些节点的私钥。

② 签名查询。攻击者$\mathcal{A}$可以对消息集合$\{M_j\}$向签名预言机发起适应性签名查询，但仅限于已被腐化的参与方。

③ 伪造尝试。攻击者输出一个针对新消息$M^*\notin\{M_j\}$的伪造聚合签名σ^*，并声称该消息已被至少t个参与方签名。

伪造成功当且仅当

$$Verify(pk,\sigma^*,M^*)=1,$$

其中，pk表示声称签名者对应的聚合公钥，且其中来自诚实参与方的有效签名数量少于t。若攻击者能够完成上述伪造，则可利用该伪造结果破解 BLS 签名方案的 EUF-CMA 安全性：以σ^*和pk作为输入，通过双线性映射的线性性质分解出至少 1 个诚实参与方的有效签名，从而构造出对 BLS 签名方案的伪造攻击。因此，攻击者成功的概率满足：

$$P_r[Verify(pk,\sigma^*,M^*)=1]\leqslant Adv_{\mathrm{BLS}}^{\mathrm{EUF-CMA}}(\lambda)\ 。$$

该概率在安全参数λ下为可忽略函数。因此，所设计的动态成员管理机制能够保持签名不可伪造性，有效抵御未经授权的成员更新操作。 证毕.

推论 1. 成员退出的状态一致性。成员退出过程中，宽限期与状态哈希验证机制确保：若P_{leave}所提交状态与通道最新确认状态不一致，或存在未确认交易，则退出请求将被拒绝。结合定理 1 的签名不可伪造性，恶意节点无法伪造其他成员对争议状态的签名，从而保障退出过程的公平性与状态一致性。

4.2 TEE 离线委托的安全性

定义 2. TEE 离线委托安全性。每个参与者P_i将交易执行权限委托给本地 TEE 阵列，该委托受形式化定义的代理策略θ_i约束。在 Intel SGX enclave 强制执行代码完整性且支持可验证的远程认证的前提下，TEE 代理仅签署严格符合授权策略θ_i的交易。

定理 2. 策略约束下委托不可绕过性。假设 SGX 远程认证是安全的，且 TEE enclave 代码是经过认证且不可篡改的，则任何概率多项式时间攻击者$\mathcal{A}$无法使 TEE 实例对不满足θ_i约束的交易$Tr\notin ValidT(\theta_i)$生成可通过验证的签名：

$$Pr[Verify(pk_i^{(j)},\sigma_i^{TEE^{(j)}},Tr)=1,Tr\notin ValidT(\theta_i)]\leqslant Adv_{\mathrm{SGX}}^{\mathrm{forge}}(\lambda)\ 。$$

证明. 假设存在攻击者$\mathcal{A}$能够诱导 enclave 实例$TEE_i^{(j)}$对$Tr\notin ValidT(\theta_i)$生成有效签名$\sigma_i^{TEE^{(j)}}$，即攻击者$\mathcal{A}$试图输出一个有效的元组$(Tr,\sigma_i^{TEE^{(j)}})$，使得：

$$Verify(pk_i^{(j)},\sigma_i^{TEE^{(j)}},Tr)=1,\ Tr\notin ValidT(\theta_i)\ 。$$

由于 enclave 逻辑通过 SGX 远程认证安全封闭且代码完整性受硬件保护，攻击者的任何成功都意味着以下至少 1 种情况成立。

1）代码完整性破坏。攻击者修改了 enclave 内部的交易验证逻辑，使其绕过签名约束的检查。但这与 SGX 的代码完整性保护假设矛盾，enclave 代码在加载时经度量哈希验证，任何篡改将导致远程认证失败。

2）私钥提取。攻击者从 enclave 中提取私钥并在 enclave 外生成签名，但这与 SGX 的机密性保护假设矛盾，私钥存储于 enclave 安全内存，受硬件内存加密保护，即使物理攻击者亦难以提取。

因此，2 种情况均违反 SGX 基本安全假设，故攻击成功的概率被界定为：

$$Pr[Verify(pk_i^{(j)},\sigma_i^{TEE^{(j)}},Tr)=1,Tr\notin ValidT(\theta_i)]\leqslant \mathrm{Adv}_{\mathrm{SGX}}^{\mathrm{forge}}(\lambda)\ ,$$

在安全参数λ下可忽略。 证毕.

推论 2. 离线期间的权限边界。定理 2 表明，即使成员长期不在线，TEE 代理的执行权限严格受限于预定义策略。攻击者无法通过劫持离线节点或伪造交易指令扩大代理权限，从而将离线期间的风险控制在可量化范围内。

定义 3. 状态恢复成功。状态S被编码为α个片段，分布在α个 TEE 实例中。当至少有$k(1+\delta)$个有效片段可用且可通过 LDPC 解码正确恢复原始状态S时，称恢复成功。

定理 3. LDPC 恢复的概率下界。假设 TEE 节点独立故障的概率为p_f，系统以冗余因子$\delta>0$分发$\alpha=k(1+\delta)$个片段。令满足二项分布的随机变量$X\sim Binomial(\alpha,1-p_f)$表示存活片段数，则恢复成功概率满足：

$$P_{\mathrm{succ}}=Pr[X\geqslant k]\geqslant 1-\varepsilon(k,\delta)\ 。$$

在$p_f<\dfrac{\delta}{1+\delta}$的条件下，$\varepsilon(k,\delta)=\exp(-\delta^2k/2)$。

证明. 由$X\sim Binomial(\alpha,1-p_f)$，其中$\alpha=k(1+\delta)$。LDPC 码的解码特性允许从任意不少于$k$个存活片段中恢复原始状态。设均值$\mu=\mathbb{E}[X]=\alpha(1-p_f)=k(1+\delta)(1-p_f)$，将恢复失败概率表示为：

$$Pr[X<k]=Pr[X<(1-\zeta)\mu]\ ,$$

其中$(1-\zeta)\mu=k$，解得：

$$\zeta=1-\frac{k}{\mu}=1-\frac{1}{(1+\delta)\left(1-p_f\right)}>0\ 。$$

满足切尔诺夫下界的应用条件。应用该界：

$$Pr[X<(1-\zeta)\mu]\leqslant\exp(-\zeta^2\mu/2)\ 。$$

在节点故障率远低于冗余率时，$\zeta^2\mu\approx\delta^2k/(1+\delta)$，因此：

$$Pr[X<k]\leqslant\exp(-\delta^2k/2)\ 。$$

从而恢复成功概率满足：

$$P_{\mathrm{succ}}=1-Pr[X<k]\geqslant 1-\exp\left(-\delta^2k/2(1+\delta)\right)\ ,$$

$$P_{\mathrm{succ}}\geqslant 1-\exp\left(-\delta^2k/2\right)\ 。$$

该界限表明，方案在最小冗余开销的情况下实现了强大的容错性，使其非常适合在现实的 TEE 故障假设下进行大规模部署。 证毕.

5 性能分析

搭建所提出框架的原型系统，对所提框架在动态成员管理效率、消息延迟、交易成功率、TEE 故障恢复能力及链上开销等维度的性能进行评估。实验

设计遵循对照原则，选取 Lightning[9]、Perun[26] 以及 SharHSC[37] 作为基准方案，在相同网络规模与交易负载条件下进行横向对比，以验证框架在智能终端动态环境下的综合优势。所选方案分别代表了当前状态通道领域中不同类型的典型技术路线：Lightning 代表经典支付型状态通道，Perun 代表通用虚拟状态通道，而 SharHSC 代表融合分片与容错机制的混合状态通道方案。通过与上述具有代表性的方案进行对比，能够从消息处理效率、动态环境适应能力以及系统鲁棒性等多个维度，全面验证本文方案的有效性与先进性。

尽管各基准方案的设计目标和应用场景存在一定差异，但均属于区块链链下扩展领域的代表性方案。为保证实验比较的公平性、可靠性与可重复性，本文在统一的实验平台、网络规模、交易负载及故障模型下开展所有对比实验，各方案均采用一致的实验配置进行测试，并以交易成功率、消息延迟和容错恢复能力等核心性能指标作为统一评价标准。每组实验在相同配置下独立重复运行 10 次，统计 10 次实验结果的平均值作为最终实验结果，以减小随机因素对实验结果的影响。在此基础上，对各方案的综合性能进行客观评价。

5.1 实验环境

1)硬件与平台配置。搭建原型系统，并部署于多个虚拟机节点。每个虚拟节点均配备支持 Intel SGX 的 Intel Core i5-7300HQ 处理器，运行 Ubuntu 22.04 LTS 操作系统。利用 Intel SGX SDK 在本地实例化 TEE，实现委托交易的安全执行及状态分片的硬件级可靠管理。

2)区块链基础设施。底层区块链通过 Ganache 搭建私有以太坊网络模拟。智能合约采用 Solidity 语言编写并经编译器优化。链上操作 Gas 消耗通过 Web3.py 接口实时采集，确保成本评估的准确性。

3)动态环境模拟。为模拟智能终端的动态特性，实验支持参与节点在运行时动态加入和退出系统。交易流程、成员管理操作以及故障注入过程均通过基于 Web3.py 接口的自动化 Python 脚本进行调度与控制。脚本协调多方交易执行、施加时间约束并收集详细日志用于后续分析。

4)关键参数设置。初始通道成员数为 10，测试 1~5 个成员动态加入与退出的操作延迟，统计从请求发起至链上更新完成的端到端时延；交易性能测试分别设置 10、100、200、300、400、500 笔交易梯度与 10、50、100、150、20 个节点网络规模，设置冗余因子 $\epsilon = 0.1, 0.2, 0.5$，链上开销测试针对通道开启、成员添加、成员移除、通道关闭 4 类操作，在固定 Gas 价格的私有链环境下统计总消耗、执行成本与存储成本。

为保证实验结果的公平性与可比性，本文所有对比方案均部署于统一的实验环境，包括相同的硬件平台、软件版本、网络配置及底层区块链环境。所有方案均运行于同一区块链，采用一致的节点规模、交易负载、区块生成参数及网络通信条件；在容错实验中，各方案均采用相同的节点故障注入方式和状态丢失比例进行测试，保证实验结果能够客观反映不同方案的性能差异。

5.2 动态成员管理延迟分析

为评估动态成员管理的效率，在初始 10 个成员的状态通道基础上，分别动态增加或移除 1~5 个参与者，测试从请求发起到链上更新完成的端到端时延。

如图 3 所示，加入与退出操作延迟随着新增或移除参与者数量的增加呈近似线性增长。当同时加入 5 个成员时，加入操作的耗时约为 5.8 s；而在相同规模下，退出操作的耗时约为 3.6 s。退出延迟低于加入延迟，原因在于退出无需执行新成员的密钥分发与 TEE 远程认证流程，仅需状态验证与集合更新。

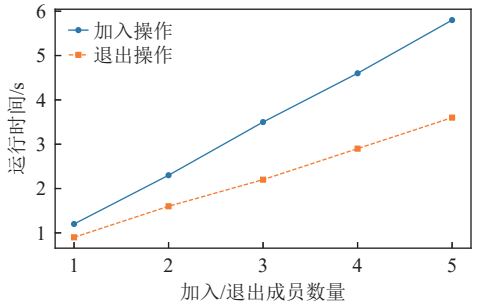


Fig. 3 The relationship between the delay of member joining or leaving and the number of members

图 3 成员加入/退出延迟与成员数量的关系

DeCloak[16] 虽提供了较强的动态成员管理安全保障，但其在实际应用中引入了较大的性能开销。每次成员变更都需要与 TEE 网络进行多轮交互，包括远程认证、组密钥更新以及安全状态重分发，随后还需将新的状态提案提交至链上并进行验证。该过程通常会引入 5~8 个区块确认延迟，通信复杂度随参与者数量呈线性增长 $O(n)$，在频繁成员变动的场景下会带来持续的协调开销。

实验结果表明，本方案通过门限签名聚合与轻量级凭证验证，将成员变更的链上交互压缩为单次聚合签名验证，显著降低了协调开销，能够支持低延迟且具备良好扩展性的成员更新机制，适用于动态

的链下环境部署。

5.3 不同交易规模下的消息延迟对比

在交易规模逐步增加条件下，对比本方案与Lightning[9]、SharHSC[37]的平均消息延迟结果如图 4所示。

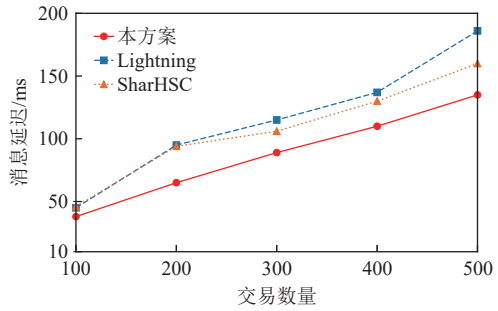


Fig. 4 Analysis of message delay performance for different schemes

图 4 不同方案的消息延迟性能分析

实验结果表明，在较低交易规模下，3 种方案的延迟表现基本相近。随着交易负载的增加，本方案展现出明显的性能优势。Lightning 的延迟的增长主要来源于串行化的支付路径协商过程以及链上仲裁带来的额外开销；SharHSC 受限于跨分片状态同步的验证成本；本方案通过并行化交易处理、本地化验证和异步容错有效缓解了上述问题，在交易规模增加时能够突破串行路径协商限制、减少链上仲裁频率，同时避免了由于节点故障引入的额外同步时延。

随着交易规模由 100 增加至 500，本方案平均消息延迟由约 38 ms 增至 135 ms，始终低于 Lightning（约 180 ms）和 SharHSC（约 160 ms）。在 500 笔交易规模下，本方案平均消息延迟较 Lightning 和 SharHSC 分别降低约 25.0% 和 15.6%。综合不同交易规模下的实验结果，本方案平均消息延迟较对比方案降低约 20%～30%，表明该方案在高负载条件下具有较好的通信效率和可扩展性。

5.4 交易成功率分析

在不同网络规模下（节点数 $n \in \{10,50,\cdots,200\}$），评估各方案的交易成功率，结果如图 5 所示。

随着节点数量的增加，由于通信复杂度上升、协调开销增大以及网络动态变化引发的交易失败概率提高，所有方案的成功率均呈现下降趋势。在所评估的方案中，本方案表现出最为稳定的性能，随着网络规模扩大仅出现轻微下降。这一结果主要得益于本方案的门限共识、离线代理、分布式状态恢复等机制的设计。门限共识无需全体在线即可达成状态承诺，降低对单个节点可用性的依赖；TEE 代理在节点断连期间维持交易执行，减少因间歇性连接导致的失败；节点临时故障时，LDPC 编码保障状态可从其他 TEE 实例快速重建，避免交易中断。

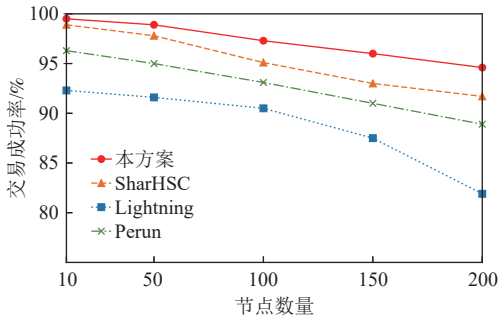


Fig. 5 Analysis of transaction success rates for different schemes

图 5 不同方案的交易成功率分析

相比之下，Lightning[9]的成功率下降较为明显，这主要是由于其依赖串行化的支付路径协商过程，并且对网络拓扑变化较为敏感。Perun[26]和 SharHSC[37]的性能处于中等水平，但在大规模部署场景下仍受到验证开销和状态同步延迟的影响。当网络规模增加至 200 个节点时，本方案的交易成功率仍达到约 95%，较 SharHSC、Perun 和 Lightning 分别提高 2.7、5.7 和 12.5 个百分点，交易成功率提升约 1.36~1.51 倍，表明所提出机制能够有效缓解网络规模扩展带来的性能退化，在大规模部署场景下仍保持较高的交易可靠性。

由于 Perun 主要面向虚拟通道构建与通用状态抽象，其核心优化目标并非高并发消息处理与离线代理执行，因此在图 4 的消息延迟实验中，重点选取了与本文方案在交易处理机制上更具可比性的 Lightning 与 SharHSC 进行对比；而在图 5 中，则进一步引入 Perun，对不同网络规模下的交易成功率与系统稳定性进行综合分析。

5.5 TEE 故障下的恢复成功率

在不同冗余参数ϵ配置下，评估 TEE 节点失效率与状态恢复成功率的关系，结果如图 6 所示。

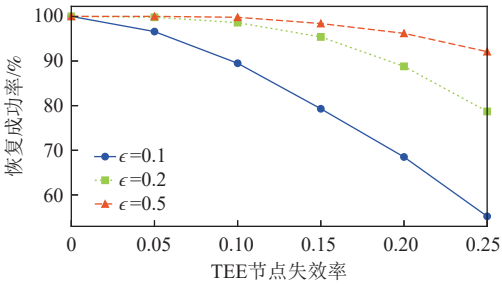


Fig. 6 Analysis of recovery success rate

图 6 恢复成功率分析

随着 TEE 失效率的增加,恢复成功率呈现出持续下降的趋势,这与系统预期的容错特性相一致。值得注意的是,较高的冗余水平($\epsilon = 0.3$)能够显著提升系统鲁棒性,即使在节点失效率达到 25% 时,恢复成功率仍可保持在 90% 以上。相比之下,较低的冗余配置($\epsilon = 0.1$)会导致性能明显下降,在相同失效率下恢复成功率降至 55.2%。

实验结果表明,当 TEE 节点失效率达到 20% 时,$\epsilon = 0.3$ 配置下系统恢复成功率达到 96.5%,较 $\epsilon = 0.2$ 和 $\epsilon = 0.1$ 分别提高 11.7 百分点和 32.2 个百分点,相对提升约 13.8% 和 50.1%。较高的冗余配置能够提供更多可用于恢复的编码数据块,即使部分 TEE 节点失效,系统仍能够完成状态重构,从而有效降低节点故障对恢复过程的影响,保证系统的可用性和可靠性。从而,提高冗余度能够有效增强系统对节点故障的抵抗能力,从而实现更加可靠的状态恢复。总体而言,实验结果验证了所提出的容错恢复机制在多 TEE 部署环境中保障系统稳定性与容错性的有效性。

5.6 链上 Gas 开销分析

在以太坊环境下分析各主要智能合约操作的 Gas 消耗,结果如图 7 所示。每类操作成本划分为执行成本(门限签名验证、内部校验等密码学计算)与交易成本(链上存储写入、事件触发)。

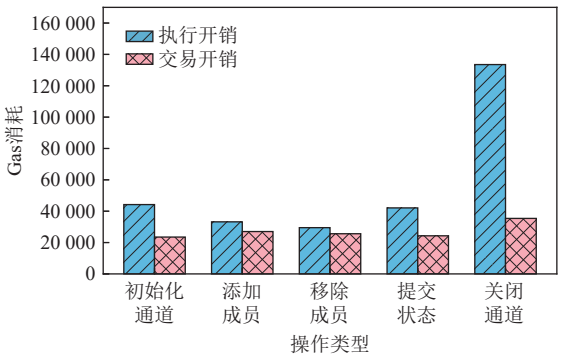


Fig. 7 Gas consumption for each operation of our scheme

图 7 本方案各个操作的 Gas 消耗

在所有操作中,关闭通道的 Gas 消耗最高,其中执行成本约占总成本的 79%。这主要反映了通道关闭过程中涉及的复杂密码学验证与结算逻辑所带来的计算开销。其他操作的执行成本也占据了总 Gas 消耗的 60% 以上。相比之下,添加成员和移除成员等轻量级操作约消耗 60 000 gas,其执行成本与交易成本分布相对均衡。各类合约操作中执行成本占主导的分布特征与以太坊的 Gas 定价机制相一致。

本方案在支持动态成员管理和分布式状态恢复的同时,通过在 TEE 中执行链下计算以及引入基于 LDPC 的容错状态恢复机制,显著提升了成本效率,因此,适用于同时要求高吞吐量与强容错性的区块链应用场景。在实际部署中,建议对高频操作进行批处理,并根据系统吞吐能力与故障特性对 LDPC 编码参数(如码率和码长)进行优化,以进一步降低提交交易的 Gas 开销。

6 结 论

本文围绕面向智能终端的区块链状态通道动态管理与分布式恢复问题,提出了一种高弹性、可扩展的状态通道框架。针对智能终端环境中节点动态加入/退出频繁、设备间歇性离线及资源受限等核心挑战,构建了支持动态参与、离线交易执行与分布式状态恢复的链下协同机制。具体来说,提出了动态成员管理机制,实现了状态通道参与者的灵活重构;设计了 TEE 辅助的离线代理机制,保障了离线场景下交易执行的安全性;提出了基于 LDPC 码的容错状态恢复机制,有效提升了系统在状态丢失情况下的容错与恢复能力。实验结果表明,所提出方案在交易成功率、系统延迟及可用性方面均优于现有方法:交易成功率提升 1.36~1.51 倍,在高负载条件下延迟降低 20%~30%,且在 20% 状态丢失情况下仍能保持超过 95% 的系统可用性。本方案在保证强一致性与高可用性的同时,显著降低了链上交互开销,能够有效适应动态、异构且资源受限的智能终端应用场景,为区块链在智能物联网环境中的高效应用提供了一种可行的技术路径。未来工作将进一步探索跨链状态通道的互操作机制,并在支持 Intel SGX v2、Intel TDX 以及 AMD SEV 等新一代 TEE 平台上完成系统部署与实验验证,进一步评估所提框架在不同硬件平台下的性能、可扩展性和工程适用性,从而提升系统的通用性与安全性。

作者贡献声明: 王晨、赫丽勤负责方案整体设计并撰写论文;王晨、赫丽勤、马昊玉负责部分算法思路和实验方法;沈剑、贾春福提出指导意见并修改论文。

参 考 文 献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. (2008-10-31)[2026-04-23]. https://bitcoin.org/bitcoin.pdf

[2] Li Zhecheng, Zhang Bo. A lightweight blockchain-based cross-domain authentication and data sharing scheme for the industrial Internet of things[J]. Journal of Computer Research and

Development, 2025, 62(10): 2416−2427 (in Chinese)
(李哲成, 张波. 基于区块链的轻量级工业物联网跨域认证与数据共享方案[J]. 计算机研究与发展, 2025, 62(10): 2416−2427)

[3] Chen Ruonan, Dong Ye, Liu Yizhong, et al. Flock: Robust and privacy-preserving federated learning based on practical blockchain state channels[C]//Proc of the ACM on Web Conf 2025. New York: ACM, 2025: 884−895

[4] Wang Yuntao, Su Zhou, Zhang Ning, et al. A survey on metaverse: Fundamentals, security, and privacy[J]. IEEE Communications Surveys & Tutorials, 2022, 25(1): 319−352

[5] Pan Chen, Liu Zhiqiang, Liu Zhen, et al. Research on scalability of blockchain technology: Problems and methods[J]. Journal of Computer Research and Development, 2018, 55(10): 2099−2110 (in Chinese)
(潘晨, 刘志强, 刘振, 等. 区块链可扩展性研究: 问题与方法[J]. 计算机研究与发展, 2018, 55(10): 2099−2110)

[6] Xu Zihuan, Chen Lei. L2chain: Towards high-performance, confidential and secure layer-2 blockchain solution for decentralized applications[J]. Proceedings of the VLDB Endowment, 2022, 16(4): 986−999

[7] Negka L D, Spathoulas G P. Blockchain state channels: A state of the art[J]. IEEE Access, 2021, 9: 160277−160298

[8] Frassetto T, Jauernig P, Koisser D, et al. POSE: Practical off-chain smart contract execution[J]. arXiv preprint, arXiv: 2210.07110, 2022

[9] Poon J, Dryja T. The bitcoin Lightning network: Scalable off-chain instant payments[EB/OL]. (2016-01-14)[2026-07-09]. https://www.bitcoinlight-ning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf.

[10] Qiao Yan, Wu Kui, Khabbazian M. Non-intrusive balance tomography using reinforcement learning in the Lightning network[J]. ACM Transactions on Privacy and Security, 2024, 27(1): 1−32

[11] Aumayr L, Maffei M, Ersoy O, et al. Bitcoin-compatible virtual channels[C]//Proc of 2021 IEEE Symp on Security and Privacy (SP). Los Alamitos, CA: IEEE, 2021: 901−918

[12] Wei Qiushi, Yang Dejun, Yu Ruozhou, et al. Thor: A virtual payment channel network construction protocol over cryptocurrencies[C]//Proc of IEEE Conf on Computer Communications (IEEE INFOCOM 2024). Piscataway, NJ: IEEE, 2024: 771−780

[13] Dong Mo, Liang Qingkai, Li Xiaozhou, et al. Celer Network: Bring internet scale to every blockchain[J]. arXiv preprint, arXiv: 1810.00037, 2018

[14] Costan V, Devadas S. Intel SGX explained[R]. Cryptology ePrint Archive, 2016: 86

[15] Das P, Eckey L, Frassetto T, et al. FastKitten: Practical smart contracts on bitcoin[C]//Proc of 28th USENIX Security Symp (USENIX Security 19). Berkeley, CA: USENIX Association, 2019: 801−818

[16] Ren Qian, Li Yue, Wu Yingjun, et al. DeCloak: Enable secure and cheap multi-party transactions on legacy blockchains by a minimally trusted TEE network[J]. IEEE Transactions on Information Forensics and Security, 2023, 19: 88−103

[17] Qi Xiaodong, Zhang Zhao, Jin Cheqing, et al. BFT-Store: Storage partition for permissioned blockchain via erasure coding[C]//Proc of the 36th Int Conf on Data Engineering (ICDE). Piscataway, NJ: IEEE, 2020: 1926−1929

[18] Gallager R. Low-density parity-check codes[J]. IRE Transactions on Information Theory, 2003, 8(1): 21−28

[19] Xu Minghui, Guo Hechuan, Cheng Ye, et al. EC-chain: Cost-effective storage solution for permissionless blockchains[C]//Proc of IEEE Conf on Computer Communications (IEEE INFOCOM 2025). Piscataway, NJ: IEEE, 2025: 1−10

[20] Kalodner H, Goldfeder S, Chen Xiaoqi, et al. Arbitrum: Scalable, private smart contracts[C]//Proc of the 27th USENIX Security Symp (USENIX Security 18). Berkeley, CA: USENIX Association, 2018: 1353−1370

[21] Han Huijian, Wang Mingwei, Yang Feng, et al. A Layer-2 expansion shared sequencer model for blockchain scalability[J]. Blockchain: Research and Applications, 2025, 6(3): 100292

[22] Pang Shengye, Zhao Xinkui, Yu Shuyi, et al. TrustPay: A dual-layer blockchain-based framework for trusted service transaction[J]. IEEE Transactions on Services Computing, 2025, 18(2): 1068−1080

[23] Weintraub B, Kumble S P, Nita-Rotaru C, et al. Payout races and congested channels: A formal analysis of security in the lightning network[C]//Proc of the 2024 on ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2024: 2562−2576

[24] Network R. What is the Raiden network[EB/OL]. 2018[2026-07-09]. https://raiden.network/101.html

[25] Gai Keke, Guo Yunwei, Yu Jing, et al. Cape: Commitment-based privacy-preserving payment channel scheme in blockchain[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22: 3977−3992

[26] Dziembowski S, Eckey L, Faust S, et al. Perun: Virtual payment hubs over cryptocurrencies[C]//Proc of 2019 IEEE Symp on Security and Privacy (SP). Los Alamitos, CA: IEEE, 2019: 106−123

[27] Coleman J, Horne L, Xuanji L. Counterfactual: Generalized state channels[R/OL]. 2018[2026-07-09]. https://l4.ventures/papers/statecha-nnels.pdf

[28] Cheng R, Zhang Fan, Kos J, et al. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts[C]//Proc of 2019 IEEE European Symp on Security and Privacy (EuroS&P). Piscataway, NJ: IEEE, 2019: 185−200

[29] Liu Chunchi, Guo Hechuan, Xu Minghui, et al. Extending on-chain trust to off-chain–trustworthy blockchain data collection using trusted execution environment (TEE)[J]. IEEE Transactions on Computers, 2022, 71(12): 3268−3280

[30] Zhang Fan, Cecchetti E, Croman K, et al. Town crier: An authenticated data feed for smart contracts[C]//Proc of the 2016 ACM SIGSAC Conf on Computer and Communications Security. New York: ACM, 2016: 270−282

[31] Lind J, Naor O, Eyal I, et al. Teechain: A secure payment network with asynchronous blockchain access[C]//Proc of the 27th ACM Symp on Operating Systems Principles. New York: ACM, 2019: 63−79

[32] Zhang Mizhipeng, Wu Chentao, Li Jie, et al. Dynamic-EC: An efficient dynamic erasure coding method for permissioned blockchain systems[J]. Frontiers of Computer Science, 2025, 19(1): 191101

[33] Wang Yan, Wang Hao, Cao Yanghuang. Comprehensive review of storage optimization techniques in blockchain systems[J]. Applied Sciences, 2024, 15(1): 243

[34] Qi Xiaodong, Zhang Zhao, Jin Cheqing, et al. A reliable storage partition for permissioned blockchain[J]. IEEE Transactions on

Knowledge and Data Engineering, 2020, 33(1): 14−27

[35] Li Chunlin, Zhang Jing, Yang Xianmin, et al. Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices[J]. Information Processing & Management, 2021, 58(4): 102602

[36] Mitra D, Tauz L, Dolecek L. Overcoming data availability attacks in blockchain systems: Short code-length LDPC code design for coded Merkle tree[J]. IEEE Transactions on Communications, 2022, 70(9): 5742−5759

[37] Liu Yizhong, Li Peiyuan, Li Dongyu, et al. SharHSC: A sharding-based hybrid state channel to realize blockchain scalability and security[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 22(3): 2705−2722



Wang Chen, born in 1994. PhD, associate professor, master supervisor. Member of CCF. His main research interests include secure data aggregation, edge computing security, and AI security.

王 晨, 1994 年生。博士, 副教授, 硕士生导师。CCF 会员。主要研究方向为安全数据聚合、边缘计算安全、人工智能安全。



He Liqin, born in 2000. Master candidate. Her main research interests include information security and blockchain technology.

赫丽勤, 2000 年生。硕士研究生。主要研究方向为信息安全、区块链技术。



Ma Haoyu, born in 1986. PhD, associate professor, master supervisor. Member of CCF. His main research interests include software security, operating system security, blockchain, and side-channel attack and defense.

马昊玉, 1986 年生。博士, 副教授, 硕士生导师。CCF 会员。主要研究方向为软件安全、操作系统安全、区块链、侧信道攻防。



Shen Jian, born in 1985. PhD, professor, PhD supervisor. Member of CCF. His main research interests include data security, security systems, mobile computing and networking, ad-hoc networks, and ubiquitous sensor networks.

沈 剑, 1985 年生。博士, 教授, 博士生导师。CCF 会员。主要研究方向为数据安全、安全系统、移动计算与网络、自组织网络、泛在传感网络。



Jia Chunfu, born in 1967. PhD, professor, PhD supervisor. Member of CCF. His main research interests include network and system security, cryptography application, and malware analysis.

贾春福, 1967 年生。博士, 教授、博士生导师。CCF 会员。主要研究方向为网络与系统安全、密码应用、恶意代码分析。