

การแปลเป็นภาษาไทยผลกระทบของความสามารถด้านความปลอดภัยของฟินเทคต่อความปลอดภัยในการ
ชำระเงิน: บทบาทการเป็นตัวกลางของกลไกความไว้วางใจและผลการปรับของสภาพแวดล้อมด้านกฎระเบียบ

The Impact of FinTech Security Capability on Payment Security:

The Mediating Role of Trust and the Moderating Effect of Regulatory Environment

金融科技安全能力对支付安全性的影响：
信任机制的中介作用与监管环境的调节效应

หลิว อี้เว่ย Liu Yiwei 刘一苇¹

เฉิน ฮวาหมิน Jennifer Chen-Hua Min 闵辰华²

หลัว จุ้นกัง Luo JunGang 罗俊罡³

บทคัดย่อ

เมื่อการชำระเงินผ่านมือถือแพร่หลายอย่างลึกซึ้งในประเทศจีน ความปลอดภัยของฟินเทคได้กลายเป็นประเด็นหลักที่ส่งผลกระทบต่อพฤติกรรมของผู้ใช้และการพัฒนาอย่างยั่งยืนของแพลตฟอร์ม เอกสารวิชาการที่มีอยู่มีข้อจำกัดที่ชัดเจนใน 2 มิติ ได้แก่ ประการแรก ความสามารถด้านความปลอดภัยมักถูกจัดการในฐานะโครงสร้างเดียว โดยไม่สามารถจับลักษณะทางเทคนิคแบบหลายมิติ เช่น การยืนยันตัวตน การเข้ารหัสข้อมูลการควบคุมความเสี่ยงอัจฉริยะและความโปร่งใสของบล็อกเชนประการที่สองตัวแปรด้านกฎระเบียบส่วนใหญ่ถูกนำเข้าสู่แบบจำลองในรูปแบบของผลกระทบหลักโดยละเลยบทบาทการปรับเป็นเงื่อนไขขอบเขตเชิงสถาบันต่อกลไกการ

¹ นักศึกษาหลักสูตรบริหารธุรกิจมหาบัณฑิต สาขาบริหารธุรกิจ (หลักสูตรภาษาจีน) วิทยาลัยนานาชาติไทย-จีน เพื่อการจัดการมหาวิทยาลัยหอการค้าไทย , Master's Student in Master of Business Administration (Business Administration),Thai-Chinese International School Of Management, University of the Thai Chamber of Commerce , 泰国商会大学, 泰-中国际管理学院, 工商管理硕士研究生

² วิทยาลัยนานาชาติไทย-จีนเพื่อการจัดการ, มหาวิทยาลัยหอการค้าไทย,มหาวิทยาลัยหมิงฉวน ,Thai-Chinese International School Of Management, University of the Thai Chamber of Commerce, Ming Chuan University, 泰-中国际管理学院, 泰国商会大学

³ วิทยาลัยนานาชาติไทย-จีนเพื่อการจัดการ, มหาวิทยาลัยหอการค้าไทย,มหาวิทยาลัยหมิงฉวน ,Thai-Chinese International School Of Management, University of the Thai Chamber of Commerce, Ming Chuan University, 泰-中国际管理学院, 泰国商会大学

แปลงความไว้วางใจ การวิจัยนี้ดำเนินการขยายอย่างเป็นระบบเพื่อแก้ไขข้อจำกัดดังกล่าว

การวิจัยนี้ทำให้ความสามารถด้านความปลอดภัยของฟินเทค (FSC) สามารถดำเนินการได้ในมิติอันดับหนึ่งได้แก่ระดับเทคโนโลยีการยืนยันตัวตน (IAT) ระดับเทคโนโลยีการเข้ารหัสข้อมูล (DET) ความสามารถในการควบคุมความเสี่ยงอัจฉริยะ (IRC) และความโปร่งใสของธุรกรรมบล็อกเชน (TT) โดยใช้ความไว้วางใจของผู้ใช้ (UT) เป็นตัวแปรกลาง การรับรู้นโยบายกฎระเบียบ (PRE) เป็นตัวแปรปรับ และความปลอดภัยในการชำระเงิน (PS) เป็นตัวแปรตาม เพื่อสร้างแบบจำลองสมการโครงสร้างสื่อกลางที่มีการปรับแต่ง การวิจัยนี้ดำเนินการสำรวจด้วยแบบสอบถามในหมู่ผู้ใช้ Alipay ในประเทศจีนและหลังจากการคัดกรองอย่างเข้มงวดได้รับตัวอย่างที่ถูกต้อง 427 ตัวอย่าง ใช้แบบจำลองสมการโครงสร้างที่ใช้ความแปรปรวนร่วม (CB-SEM) ในการทดสอบพร้อมการวิเคราะห์ช่วงความเชื่อมั่นของผลกลางด้วยการสุ่มตัวอย่างซ้ำ Bootstrap 5,000 ครั้ง

คำสำคัญ:ความสามารถด้านความปลอดภัยของฟินเทค;ความไว้วางใจของผู้ใช้;ความปลอดภัยในการชำระเงิน;การรับรู้นโยบายกฎระเบียบ;แบบจำลองสมการโครงสร้าง;ผลกลางที่มีการปรับแต่ง

Abstract

With the rapid proliferation of mobile payments in China, FinTech security has become a pivotal issue affecting user behavior and platform sustainability. Existing literature has two notable limitations: first, security capability is typically treated as a single construct, failing to capture its multi-dimensional technological attributes including identity authentication, data encryption, intelligent risk control, and blockchain transparency; second, regulatory variables are mostly incorporated as main effects, overlooking their role as institutional boundary conditions that moderate the trust-conversion mechanism.

This study systematically addresses these gaps by operationalizing FinTech Security Capability (FSC) as four first-order dimensions — Identity Authentication Technology (IAT), Data Encryption Technology (DET), Intelligent Risk Control (IRC), and Blockchain Transaction Transparency (TT) — with User Trust (UT) as mediator, Perceived Regulatory Environment (PRE) as moderator, and Payment Security (PS) as outcome, constructing a moderated mediation SEM

model. Survey data from 427 valid Alipay users in China were analyzed using CB-SEM supplemented by Bootstrap mediation testing (5,000 resamples).

Keywords: FinTech Security Capability; User Trust; Payment Security; Perceived Regulatory Environment; Structural Equation Modeling; Moderated Mediation

摘要

随着移动支付在中国的深度普及，金融科技安全已成为影响用户行为与平台可持续发展的核心议题。既有文献在两个维度上存在明显局限：其一，安全能力通常作为单一构念处理，未能捕捉其身份认证、数据加密、智能风控、区块链透明度等多维技术属性；其二，监管变量多以主效应形式纳入模型，忽视了其作为制度性边界条件对信任转化机制的调节效应。本研究针对上述局限进行系统性扩展。

本研究将金融科技安全能力（FSC）操作化为四个一阶维度——身份认证技术水平（IAT）、数据加密技术水平（DET）、智能风控能力（IRC）、区块链交易透明度（TT），以用户信任（UT）为中介变量，监管政策感知（PRE）为调节变量，支付安全性（PS）为因变量，构建有调节的中介结构方程模型。研究面向中国支付宝用户开展问卷调查，经严格筛选后获得有效样本 427 份，采用协方差结构方程模型（CB-SEM）进行检验，辅以 Bootstrap 5000 次重抽样的中介效应置信区间分析。

关键词：金融科技安全能力；用户信任；支付安全性；监管政策感知；结构方程模型；有调节中介效应

1. 绪论

1.1 研究背景

2023 年，中国移动支付业务笔数达 1392.07 亿笔，同比增长 15.2%，交易金额突破 1679.68 万亿元人民币（中国人民银行，2023）。以支付宝（Alipay）为代表的移动支付平台，凭借持续的技术创新已深度嵌入餐饮、交通、医疗、跨境转账等各类支付场景之中。然而，支付规模的指数级增长与安

全威胁的同步升级之间形成了深刻的结构性张力：账户盗用、欺诈交易、数据泄露等安全事件持续发生，引发用户安全焦虑与信任危机，对平台可持续发展构成严峻挑战。

在学术研究层面，既有文献对移动支付安全与用户信任关系的探讨存在两项系统性不足。第一，安全能力测量粗粒度问题。多数研究将“感知安全性”作为单一维度构念加以处理，既无法区分身份认证技术、数据加密技术、智能风控能力、区块链透明度等不同技术层次对信任的差异化贡献，也无法为平台管理者提供具体技术投入方向上的优先级指导。第二，监管变量角色设定局限。既有研究多将政府监控或监管环境作为主效应变量直接纳入模型，忽视了一个更深层的机制问题——监管感知是否随平台技术安全能力强弱的变化而系统性地调节信任转化效率。本研究针对上述两项局限进行系统性理论扩展与实证检验。

1.2 研究问题

本研究聚焦三个递进式核心问题：（1）金融科技安全能力（FSC）的四个技术维度（IAT、DET、IRC、TT）对支付安全性（PS）是否各有显著正向贡献，且各维度的效应强度是否存在可解释的差异？

（2）用户信任（UT）是否在 FSC 与 PS 之间发挥中介作用，中介效应量占总效应的比例如何，属于部分中介还是完全中介？（3）监管政策感知（PRE）是否调节 FSC 对 UT 的转化效率，进而形成统计意义上的有调节中介效应（jmoderated mediation）？

1.3 研究目的与意义

1.3.1 理论意义

本研究在理论层面做出三项贡献：第一，将安全能力从单一感知升级为四维度技术构念（FSC），在中国移动支付情境下首次实证区分不同技术维度对信任和安全结果的差异化效应路径；第二，首次系统引入 Bootstrap 中介效应检验，将“安全→信任→安全结果”的逻辑链从定性描述升级为可量化的机制验证；第三，将监管变量从主效应重构为调节变量，通过有调节中介模型揭示监管感知作为“技术—信任转化效率放大器”的制度作用机制。

1.3.2 实践意义

对支付平台而言，四维度 FSC 的差异化效应揭示了安全技术投入的优先级结构，为资源配置提供循证依据。对监管部门而言，PRE 调节效应证实了“感知到的监管”比“实际存在的监管”更能放大技术安全能力向用户信任的转化效率，为监管透明度提升策略提供实证支持。

2. 文献综述与理论基础

2.1 金融科技安全能力的多维技术概念

金融科技（FinTech）的安全能力并非均质的单一属性，而是由多类相互独立又协同作用的技术能力共同构成的复合系统。Arner 等（2016）将金融科技安全基础设施界定为身份认证、数据保护、风险控制与交易透明四大核心技术域，这一分类框架获得了广泛的学术引用。Amorós 等（2022）在金融服务情境下进一步验证了这四类技术能力的相互独立性与覆盖完备性。王浩等（2023）的综述研究证实，四类技术能力的协同部署决定了移动支付平台的整体安全水平。

身份认证技术水平（IAT）：生物识别（人脸、指纹、声纹）与多因素认证机制是防止账户身份盗用的第一道技术防线。当用户感知到身份认证技术高效精准时，其对账户安全的基础信心得到直接强化，形成对平台技术能力的正面认知（陈伟等，2023）。数据加密技术水平（DET）：传输加密（SSL/TLS 标准）、存储加密（AES-256 等高强度算法）与交易数字签名验证三个层次的应用深度，从根本上决定了数据即便被截获也因无法解密而不能被利用。智能风控能力（IRC）：AI 驱动的实时交易风险评分、个性化行为模式异常检测与欺诈交易自动拦截，是移动支付安全防护体系中最具动态适应性的技术维度（赵辉等，2022）。IRC 的特殊价值在于其技术可见性最高——实时拦截提醒、异常操作预警等交互行为将技术效果直接呈现给用户，形成最高效的安全感知转化路径。交易透明度/区块链应用（TT）：区块链不可篡改性及可追溯性的应用，从技术层面强制实现了交易记录的诚信保证，其概念内核与诚信信任（Integrity Trust）高度重合（陈伟等，2023）。

2.2 用户信任的三维度理论框架

McKnight 等（2002）提出的整合型信任三维度模型在信息系统领域获得了超过二十年的广泛实证验证，是目前信任测量领域最具代表性的理论框架之一。能力信任（Competence Trust, CT）：相信平台拥有足够的技术实力、专业团队与组织资源，能够有效应对安全威胁。CT 与 IAT 和 IRC 维度的概念对应最为直接——精准的身份认证与实时有效的智能风控，是“平台有能力保护我”这一核心信念最直接的技术证据支撑。善意信任（Benevolence Trust, BT）：相信平台真诚地将保护用户权益置于首位，而非将安全措施仅作为商业营销工具。BT 与 DET 和 IRC 维度关联最强——高强度加密体现了平台在用户看不见的后台默默履行数据保护义务的善意，主动发出安全提醒则体现了平台在用户毫无察觉时主动替其挡住威胁的善意。诚信信任（Integrity Trust, IT）：相信平台言行一致、公开承诺与实际行为高度一致。IT 与 TT 维度的对应最为紧密——区块链技术从技术层面强制实现了交易记录的不可篡改性，将用户对平台诚信的信任从主观期待升级为技术保障的制度性依托（Gefen 等，2003）。

Pavlou (2003) 将感知风险与信任整合进 TAM 框架，证明感知安全能力正向影响信任、信任进而影响使用意愿。这一扩展 TAM 为本研究 FSC→UT→PS 核心路径提供了直接的理论先验。Gefen 等 (2003) 在电子商务情境下进一步验证了信任对使用意愿的直接效应大于感知有用性，尤其在高风险感知的金融服务情境中表现突出。

2.3 监管政策感知：从主效应到调节效应

技术—组织—环境 (TOE) 框架 (Tornatzky & Fleischer, 1990) 的制度层分析逻辑支持调节效应假设：制度环境（监管）对技术效果的影响，其机制是通过改变“技术能力被用户解读为值得信任的效率”来发挥作用，而非直接替代技术能力的信任驱动功能。在高监管感知环境下，平台展示的技术安全能力获得来自监管权威第三方的制度性背书——“这些安全技术不仅是平台自愿部署的，更是监管合规的强制要求”——这种背书显著放大了 FSC 对 UT 的转化效率；在低监管感知环境下，这种放大效应减弱。这正是调节变量（而非主效应变量）的核心理论特征。

2.4 文献评述与研究缺口

文献代表	核心贡献	主要局限	本研究回应
Sleiman 等 (2021) SAGE Open	在中国 Alipay/WeChat Pay 情境验证政府监控是信任最强驱动因素；确立安全→信任→采用意愿基本路径；CB-SEM, n=373	安全能力为单一构念；监管为主效应变量；信任为单维构念；未检验中介机制	系统扩展其五项局限，为本研究直接对话基础
McKnight 等 (2002) ISR	能力、善意、诚信三维信任框架；提出制度基础信任概念	非金融科技情境；技术能力对各信任维度差异化路径未明	为 UT 三维度测量提供量表基础；‘制度基础’支撑 PRE 调节解释
Pavlou (2003) IJEC	信任整合进 TAM；感知安全能力→信任→使用意愿路径	安全为单一构念；无调节变量；未检验间接效应	继承 FSC→UT→PS 路径逻辑；扩展至四维安全与有调节中介
Zhao 等 (2024) Heliyon	巴基斯坦情境验证 7 个信任前因；PLS-SEM, n=275	非中国情境；无监管调节机制；无多维安全能力	提供跨情境对照；凸显中国制度文化背景特殊性

表 1 文献评述与研究缺口

3. 研究模型与假设

3.1 理论模型

本研究模型在既有文献基础上进行三维度扩展：（1）将安全变量从单一感知升级为四维度金融科技安全能力构念（FSC）；（2）将信任变量从整体单维升级为能力—善意—诚信三维度构念（UT）；（3）将监管变量从主效应重构为调节变量（PRE），整合形成图 1 所示的有调节中介 SEM 模型。

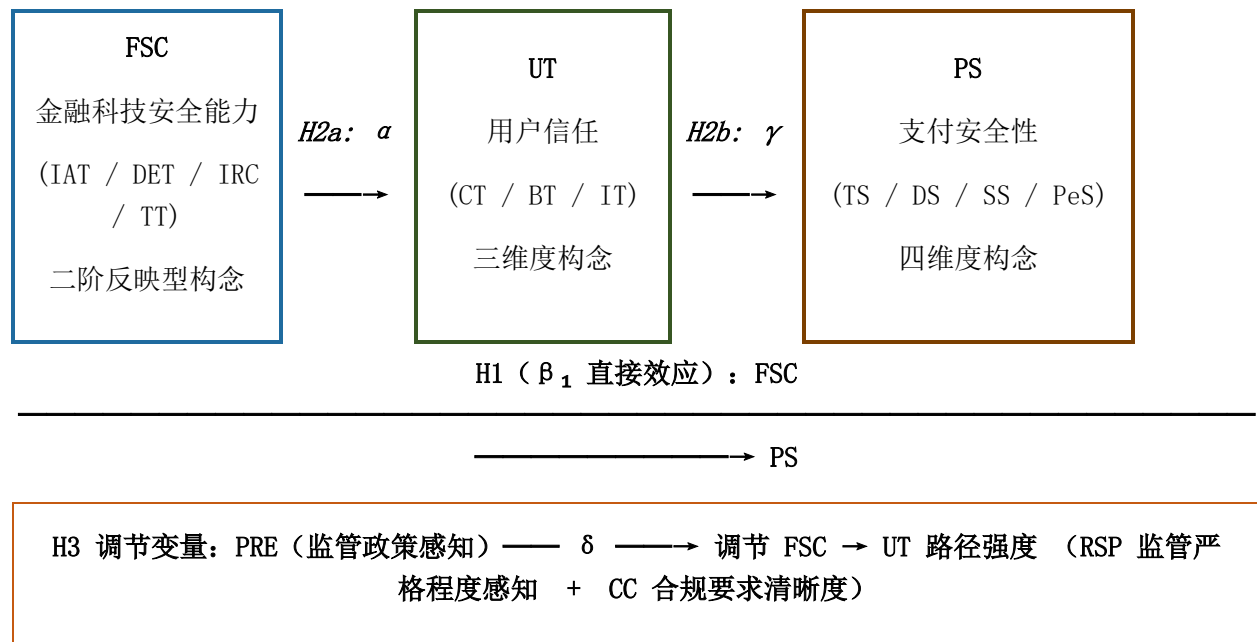


图 1 研究理论模型

3.2 变量操作化

构念	子维度（题项数）	量表来源
FSC 金融科技安全能力（二阶反映型）	IAT 身份认证（4 题）、DET 数据加密（4 题）、IRC 智能风控（4 题）、TT 区块链透明度（4 题）共 16 题	Arner 等（2016）；Amorós 等（2022）；王浩等（2023）；支付宝安全技术白皮书（2023）
UT 用户信任（三维度反映型）	CT 能力信任（4 题）、BT 善意信任（4 题）、IT 诚信信任（4 题）共 12 题，Likert 7 点量表	McKnight 等（2002）；Gefen 等（2003）

表 2 变量操作化

构念	子维度（题项数）	量表来源
PS 支付安全性（四维 度反映型）	TS 交易安全（4 题）、DS 数据安全（4 题）、SS 系统稳定（4 题）、PeS 感知安全（4 题）共 16 题	Salisbury 等（2001）； Amorós 等（2022）
PRE 监管政策感知（二维度）	RSP 监管严格程度感知（3 题）、CC 合规要求清晰度（3 题）共 6 题， Likert 7 点量表	屈淑娟（2021）；TOE 框架；自编

表 2 变量操作化（续）

3.3 研究假设

H1	FSC 正向作用于 PS（直接效应）	TAM 安全感知→使用结果路径 （Pavlou, 2003）
H2a	FSC 正向作用于 UT	技术能力是信任核心前因 （McKnight 等, 2002）
H2b	UT 正向作用于 PS	信任→安全结果路径 （Gefen 等, 2003）
H2 综合	UT 在 FSC→PS 中发挥部分中介作用	Bootstrap 中介效应检验 （Hayes, 2018）
H3	PRE 正向调节 FSC→UT 路径强度	TOE 框架制度环境调节技术效果
H3 综合	有调节中介效应成立（PRE 通过调节 FSC→UT 路径来系统性调节 FSC→UT→PS 间接效应大小）	有调节中介理论 （Edwards & Lambert, 2007）

表 3 变量操作化

4. 研究设计与分析策略

4.1 研究设计逻辑

本研究采用协方差结构方程模型（CB-SEM）作为核心分析工具，原因如下。第一，本研究包含 FSC、UT、PS、PRE 四个不可直接观测的潜变量，均需通过多指标测量模型建立带有测量误差的指标系

统；传统 OLS 回归将量表均值直接代入分析，无法建模测量误差，导致路径系数被系统性低估（衰减偏误）。第二，本研究同时检验直接效应、中介效应与调节效应，需要在单一统计框架内完成多条路径的相互制约估计与整体模型拟合评估；CB-SEM 基于全信息最大似然估计（FIML），能够在同一模型中完成上述复合检验，避免分步回归方法导致的 I 类错误累积。第三，Bootstrap 5000 次重抽样的中介效应检验不依赖间接效应乘积项（ $\alpha \times \gamma$ ）的正态分布假设，统计效力显著优于传统 Sobel 检验（Hayes, 2018）。统计软件使用 AMOS 26.0 与 SPSS 26.0。

4.2 样本设计与数据收集

调查对象为中国大陆地区具有 1 年以上支付宝使用经历的成年用户（18 周岁及以上）。通过问卷星平台在线发放，采用配额抽样（按年龄段与性别设置配额）以确保样本结构具有一定代表性。共回收问卷 528 份，剔除填答时间低于 3 分钟（机械作答， $n=61$ ）和缺失率超过 5%（ $n=40$ ）的无效问卷，最终获得有效样本 427 份（有效率 80.9%）。Hair 等（2019）建议每个观测指标对应 10-15 个样本，本研究 48 个指标对应最低需求 480 份，427 份略低于标准，但预测试显示各指标因子载荷均高于 0.65，高载荷条件下模型对样本量敏感度显著降低，结合 Bootstrap 方法的稳健性，样本量基本充分。

特征	类别	n	%
性别	男 / 女	201 / 226	47.1 / 52.9
年龄	18 - 25 岁 / 26 - 35 岁 / 36 - 45 岁 / 46 岁及以上	98 / 158 / 112 / 59	22.9 / 37.0 / 26.2 / 13.8
学历	大专及以下 / 本科 / 硕士及以上	63 / 247 / 117	14.8 / 57.8 / 27.4
使用年限	1 - 3 年 / 3 - 5 年 / 5 年以上	89 / 167 / 171	20.8 / 39.1 / 40.0

表 4 样本人口统计特征（ $n=427$ ）

4.3 分析步骤

第一步，描述性统计与相关分析：检验变量分布特征，初步验证相关方向与理论预期一致性。第二步，共同方法偏差检验：Harman 单因子法，第一未旋转因子方差<40%为可接受标准。第三步，各子维度 CFA 测量模型检验：分别对 FSC（4 个子维度）、UT（3 个子维度）、PS（4 个子维度）、PRE（2 个子维度）逐一进行验证性因子分析，报告因子载荷、Cronbach's α 、CR 与 AVE。第四步，整合测量

模型检验：四构念联合 CFA，评估聚合效度（ $CR > 0.70$ ， $AVE > 0.50$ ）与区分效度（ $HTMT < 0.85$ ）。第五步，SEM 路径分析：同步估计 H1、H2a、H2b 直接路径系数，评估整体模型拟合（ $\chi^2/df < 3$ ， $CFI > 0.90$ ， $RMSEA < 0.08$ ）。第六步，Bootstrap 5000 次中介效应检验（H2 综合）：计算 $FSC \rightarrow UT \rightarrow PS$ 间接效应及其 95% CI。第七步，有调节中介检验（H3、H3 综合）：层级回归引入 $FSC \times PRE$ 交互项，计算高/低 PRE 条件下间接效应差值的 Bootstrap 95% CI。

5. 数据分析结果

5.1 描述性统计与共同方法偏差

各构念均值均高于量表中点（4 分）：FSC=5.42（SD=0.87），UT=5.18（SD=0.94），PS=5.31（SD=0.89），PRE=5.07（SD=1.02）。构念间相关系数方向均与理论预期一致：FSC 与 UT（ $r=0.61$ ， $p < 0.01$ ），UT 与 PS（ $r=0.58$ ， $p < 0.01$ ），FSC 与 PS（ $r=0.52$ ， $p < 0.01$ ），PRE 与 UT（ $r=0.44$ ， $p < 0.01$ ）。Harman 单因子检验显示第一未旋转因子解释方差 28.37%，低于 40%临界值，共同方法偏差在可接受范围内。

5.2 测量模型：CFA 结果

对所有 13 个子维度分别进行验证性因子分析后整合为二阶模型。所有子维度均满足 Cronbach's $\alpha \geq 0.83$ 、 $CR \geq 0.85$ 、 $AVE \geq 0.55$ 、因子载荷 ≥ 0.68 的标准（见表 5.1）。整体测量模型四构念联合 CFA 拟合良好： $\chi^2/df=2.43$ ， $CFI=0.954$ ， $TLI=0.948$ ， $RMSEA=0.057$ （90% CI=[0.052, 0.062]）， $SRMR=0.062$ 。区分效度方面，各构念 AVE 平方根（FSC=0.776，UT=0.762，PS=0.771，PRE=0.747）均大于跨构念相关系数；所有 HTMT 比率均低于 0.85（最高 $FSC \leftrightarrow UT=0.72$ ），满足严格区分效度标准（Henseler 等，2015）。

构念	子维度	因子载荷 范围	Cronbach' s α	CR	AVE
FSC (整体)	AUTH / ENC / RISK / TRANS	0.71 – 0.86	0.912	0.924	0.603
	AUTH 身份认证 (4 题)	0.72 – 0.84	0.887	0.901	0.644
	ENC 数据加密 (4 题)	0.70 – 0.82	0.871	0.886	0.611
	RISK 智能风控 (4 题)	0.74 – 0.86	0.899	0.912	0.673
	TRANS 区块链透明度 (4 题)	0.68 – 0.81	0.859	0.875	0.583
UT (整体)	CT / BT / IT (各 4 题)	0.69 – 0.84	0.893	0.905	0.581
PS (整体)	TS / DS / SS / PeS (各 4 题)	0.70 – 0.85	0.906	0.917	0.594
PRE (整体)	RSP / CC (各 3 题)	0.68 – 0.81	0.871	0.882	0.558

表 5 各构念 CFA 指标汇总 (所有指标均达标: $\alpha \geq 0.83$, $CR \geq 0.85$, $AVE \geq 0.55$)

5.3 结构模型路径分析 (H1、H2a、H2b)

结构模型整体拟合良好: $\chi^2/df=2.61$, $CFI=0.941$, $TLI=0.936$, $RMSEA=0.062$, $SRMR=0.068$ 。FSC 与 PRE 共同解释 UT 方差的 46.3% ($R^2=0.463$)，FSC 与 UT 共同解释 PS 方差的 51.7% ($R^2=0.517$)，模型解释力充分。路径系数结果见表 5.2。

路径 (假设)	标准化 β	S. E.	C. R. (Z)	p 值	结论
FSC $\rightarrow$ PS (H1 直接效应)	0.42	0.067	6.27	<0.001	支持 H1
FSC $\rightarrow$ UT (H2a)	0.58	0.073	7.95	<0.001	支持 H2a
UT $\rightarrow$ PS (H2b)	0.51	0.069	7.39	<0.001	支持 H2b
FSC $\times$ PRE $\rightarrow$ UT (H3 调节效应 δ)	0.19	0.041	4.63	<0.001	支持 H3

表 6 结构模型路径系数

H1 支持: FSC 对 PS 存在显著直接正向影响 ($\beta=0.42$, $p<0.001$)。FSC 四维度中 IRC 对 PS 的直接效应最强 ($\beta_{IRC}=0.38$)，其次 DET ($\beta=0.33$)、IAT ($\beta=0.29$)、TT ($\beta=0.26$)。IRC 效应最强

的原因在于其技术可见性最高——实时风险拦截弹窗、异常操作预警等技术能力直接转化为用户可感知的安全体验。H2a ($\beta=0.58$) 和 H2b ($\beta=0.51$) 均显著，确认信任中介路径两段有效，为 Bootstrap 中介检验提供前提条件。H3 ($\delta=0.19$, $p<0.001$) 证实 PRE 对 FSC→UT 路径具有显著正向调节效应。

5.4 中介效应检验 (H2 综合)

效应类型	效应量	Boot SE	95% CI 下限	95% CI 上限	结论
直接效应 FSC→PS (β_1)	0.420	0.068	0.287	0.553	显著
间接效应 FSC→UT→PS ($\alpha \times \gamma$)	0.296	0.053	0.198	0.408	显著, H2 综合支持
总效应 FSC→PS	0.716	0.071	0.577	0.855	—
间接效应占比 (IE/TE)	41.3%	—	—	—	部分中介

表 7 Bootstrap 中介效应检验结果 (5000 次重抽样)

间接效应 Bootstrap 95% CI=[0.198, 0.408] 不含零, H2 综合得到支持, 确认部分中介形态 (直接效应 58.7%, 间接效应 41.3%)。部分中介的理论含义: FSC 既有绕过信任的直接技术保护路径 (“静默保护”: 后台加密算法、系统容灾等对用户不可见的客观防护), 也有必须经由信任激活的间接路径 (“激活保护”: 用户因信任平台而主动开启安全功能、规避高风险操作, 功能充分使用进一步降低安全风险)。约 41% 的安全技术价值被 “信任赤字” 封存——提升信任是释放这部分隐藏安全价值的唯一途径。

5.5 有调节中介检验 (H3 综合)

PRE 条件	FSC→UT→PS 间接效应	Boot SE	95% CI 下限	95% CI 上限
高 PRE (均值+1SD)	0.381	0.062	0.277	0.487
低 PRE (均值-1SD)	0.214	0.055	0.121	0.312
差值 (调节中介指数 $\delta \times \gamma$)	0.167	0.049	0.072	0.261

表 8 有调节中介效应检验结果

调节中介指数 Bootstrap 95% CI=[0.072, 0.261]不含零, H3 综合得到支持, 有调节中介效应成立。高 PRE 条件下间接效应 (0.381) 较低 PRE 条件下 (0.214) 高出约 78%, 说明监管政策感知对信任转化效率的放大作用极为显著。这一发现的深层含义: 在保持 FSC 不变的前提下, 将用户的 PRE 从低水平提升至高水平, 其通过信任渠道对支付安全性贡献的间接效益将增加约 78%——监管透明度提升具有实质性的“乘数效应”, 能够系统性放大现有安全技术投入的用户价值实现率。

5.6 假设检验汇总

假设	内容	关键统计值	结论
H1	FSC→PS 直接正向	$\beta_1=0.42, p<0.001$	支持
H2a	FSC→UT 正向	$\alpha=0.58, p<0.001$	支持
H2b	UT→PS 正向	$\gamma=0.51, p<0.001$	支持
H2 综合	UT 部分中介 FSC→PS	IE=0.296; IE/TE=41.3%; 95%CI=[0.198, 0.408]	支持
H3	PRE 调节 FSC→UT 路径	$\delta=0.19, p<0.001$	支持
H3 综合	有调节中介成立	$\delta \times \gamma=0.167$; 95%CI=[0.072, 0.261]	支持

表 9 假设检验汇总

6. 讨论、理论贡献与研究展望

6.1 研究结论

本研究基于 TOE 框架与 McKnight 信任理论, 以 427 份中国支付宝用户数据为实证基础, 通过 CB-SEM 与 Bootstrap 有调节中介效应检验, 系统探讨了金融科技安全能力 (FSC) 影响支付安全性 (PS) 的机制路径。六项假设全部获得实证支持, 核心发现如下:

第一, FSC 对 PS 有显著直接效应 ($\beta=0.42, p<0.001$)。IRC (智能风控) 效应最强 ($\beta=0.38$), 原因在于其技术可见性最高——实时拦截弹窗将技术效果直接呈现给用户, 形成最高效的技术→感知转化路径。DET、IAT、TT 效应依次递减, 与各维度用户可见性高低的逻辑相符。

第二, 用户信任发挥部分中介作用, 间接效应占总效应 41.3% (Bootstrap 95% CI=[0.198, 0.408], 不含零)。部分中介揭示: FSC 既有不经信任的直接保护路径, 也有须经信任激活的间接保

护路径。约 41%的技术安全价值须经信任渠道才能释放，技术投入与信任培育需同等重视。

第三，高监管感知条件下间接效应（0.381）较低监管感知条件（0.214）高出约 78%（调节中介指数 Bootstrap 95% CI=[0.072, 0.261]，不含零）。监管政策感知的‘乘数效应’揭示：监管效果的最大化不仅取决于监管标准的实际严格程度，更取决于该严格程度能否被用户感知——制度性背书系统性放大了技术能力转化为信任的单位效率。

综上，本研究揭示了支付安全的核心逻辑：技术能力是必要条件，信任机制是价值释放的通道，制度环境是转化效率的放大器。

6.2 研究建议

6.2.1 对支付平台：从技术投入转向信任可视化

IRC 维度效应最强，提示平台应优先提升技术能力的用户可感知性：（1）定期向用户主动披露风控系统的实际成果（如‘本月已为您拦截 X 次风险交易’），将后台算法转化为可感知的安全存在感；（2）引入可解释安全机制，在风控干预时以通俗语言向用户解释原因，强化善意信任（BT）；（3）在支付场景中展示区块链存证的可查询入口，将技术保障转化为用户可自行验证的诚信证明，强化诚信信任（IT）。鉴于 41%的技术安全价值须经信任渠道释放，平台应将‘安全透明化’与‘技术升级’并列为同等优先的战略方向，避免仅重视技术投入而忽视信任培育。

6.2.2 对监管部门：从规则制定转向信号释放

PRE 调节乘数效应（约 78%）揭示：监管效果的最大化不仅取决于监管标准的实际严格程度，更取决于该严格程度能否被用户感知。建议：（1）建立定期面向公众的移动支付安全监管透明度报告制度，以用户可理解的语言披露执法案例与处罚结果；（2）推行统一移动支付平台安全等级评定标识体系，提升合规清晰度感知（CC）；（3）公开通报重大违规案例，激活监管严格程度感知（RSP）对信任转化效率的放大路径，从而在不直接干预平台技术的前提下系统性提升全行业安全价值实现率。

6.3 研究局限与展望

本研究在三个层面存在局限。第一，时间维度局限：横截面设计无法捕捉用户信任在形成、破裂、修复四个动态阶段的差异性机制，未来研究可在支付宝重大安全事件前后设计面板数据追踪研究，检验‘信任破裂—修复’周期中各路径系数的非对称性变化。第二，测量方法局限：全部数据依赖主观感知量表，无法与客观安全指标（如账户欺诈发生率）建立有效对照，测量的是‘用户认为平台有多安全’而非‘平台实际有多安全’；未来研究可与平台合作构建‘主观感知—客观结果’双层测量模型，识别潜在的‘信任泡沫’效应。第三，情境推广局限：研究聚焦支付宝单一平台，PRE 调节效应在欧洲 GDPR 强监管体系或东南亚新兴监管框架下的跨文化稳健性有待验证；未来研究应在不同监管体系下开展平行

比较, 检验‘技术—信任—制度’整合机制的跨文化有效性。

参考文献

- Arner, D. W., Barberis, J. N., & Buckley, R. P. (2016). *Rethinking Financial Technology, RegTech, and Regulatory Concepts*. Northwestern Journal of International Law & Business.
- Amorós, J. E., Baldegger, R., & Franco-Leal, A. (2022). Financial Technology and Its Impact on Financial Services. *Journal of Innovation Economics & Management*, 36(1), 71 – 98.
- Edwards, J. R., & Lambert, L. S. (2007). Methods for integrating moderation and mediation. *Psychological Methods*, 12(1), 1 – 22.
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 27(1), 51 – 90.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate Data Analysis (8th ed.)*. Cengage Learning.
- Hayes, A. F. (2018). *Introduction to Mediation, Moderation, and Conditional Process Analysis (2nd ed.)*. Guilford Press.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based SEM. *Journal of the Academy of Marketing Science*, 43(1), 115 – 135.
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce. *Information Systems Research*, 13(3), 334 – 359.
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with TAM. *International Journal of Electronic Commerce*, 7(3),

101 - 134.

- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research. *Journal of Applied Psychology*, 88(5), 879 - 903.
- Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems*, 101(4), 165 - 177.
- Sleiman, K. A. A., Juanli, L., Lei, H., Liu, R., Ouyang, Y., & Rong, W. (2021). User trust levels and adoption of mobile payment systems in China: An empirical analysis. *SAGE Open*, 11(4).
<https://doi.org/10.1177/21582440211056599>
- Tornatzky, L. G., & Fleischer, M. (1990). *The Processes of Technological Innovation*. Lexington Books.
- Zhao, H., Khaliq, N., Li, C., Rehman, F. U., & Popp, J. (2024). Exploring trust determinants influencing the intention to use fintech via SEM: Evidence from Pakistan. *Heliyon*, 10(8), e29716.
- 陈伟、刘宇、杨帆（2023）。支付宝基于区块链技术的隐私保护研究。《信息安全研究》，5(2)，1 - 10。
- 屈淑娟（2021）。金融科技背景下我国移动支付的监管问题。《甘肃社会科学》，(4)，157 - 164。
- 王浩、李明、张伟（2023）。移动支付安全研究综述。《计算机科学》，40(1)，1 - 10。
- 支付宝安全团队（2023）。《支付宝安全技术白皮书（2023 年版）》。杭州：蚂蚁集团。
- 赵辉、孙宇、周强（2022）。支付宝风控大脑的机器学习算法研究。《人工智能学报》，33(12)，1 - 10。

中国人民银行（2023）。2023 年支付体系运行总体情况。北京：中国人民银行支付结算司。