Co-organised by THE HONG KONG POLYTECHNIC UNIVERSITY 香港理工大學 SCHOOL OF HOTEL AND TOURISM MANAGEMENT

CAU | CENTRAL ASIAN UNIVERSITY

Supported by HTMi Hotel and Tourism Management Institute Switzerland

Conference Proceedings of the 3rd One Belt • One Road • One Tourism

International Conference

Tashkent, Uzbekistan
24-27 June 2025

ISBN: 978-988-7884637

Foreword from Conference Chair

Responding to China's Belt & Road Initiative, the School of Hotel and Tourism Management at The Hong Kong Polytechnic University pioneered the "One Belt One Road One Tourism" International Conference. This conference serves as a dynamic platform for fostering a global tourism academic community with a shared future among Belt & Road countries and regions. The inaugural conference took place in Indonesia in 2018, followed by the second conference in mainland China in 2019. The third "One Belt One Road One Tourism" International Conference is co-organized by the School of Hotel and Tourism Management at The Hong Kong Polytechnic University and the Hospitality Management and Tourism School at Central Asian University in Tashkent, Uzbekistan, from June 24-27, 2025.

The conference brings together scholars and professionals in hospitality and tourism to engage in meaningful interactions and share research findings and best practices under the theme "Development, Marketing, Sustainability." This year, the conference has accepted 95 abstracts and 8 full papers, which are published in the Conference Proceedings, showcasing the latest advancements and insights in the field.

As the conference continues to grow, it strengthens the bonds between participating countries and regions, fostering collaboration and innovation in tourism. By addressing key challenges and opportunities, the "One Belt One Road One Tourism" International Conference plays a crucial role in shaping the future of global tourism, promoting sustainable development, and enhancing cultural exchange. We look forward to the impactful discussions and partnerships that will emerge from this year's event, paving the way for a more connected and prosperous tourism landscape.

Prof. Kaye Chon
Dean and Chair Professor,
Walter & Wendy Kwok Family Foundation Professor in
International Hospitality Management
School of Hotel and Tourism Management
The Hong Kong Polytechnic University

Prof. Dr. Erdogan Ekiz
Founding Dean of Tourism and Hospitality Management School
Central Asian University

Contents

Blockchain-Based Solutions for Enhancing Customer Data Security in Hospitality

Yeldar NURULY[1], Aisulu SEMBAYEVA[2,] Aliya AKTYMBAYEVA[3]

[1]Ph.D. candidate; Senior Research Fellow, Senior Lecturer, Department of Recreational Geography & Tourism, Faculty of Geography & Environmental Sciences, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

Centre for Sustainable Development in Central Asia, Al-Farabi Kazakh National University, in partnership with The Hong Kong Polytechnic University, Almaty, Kazakhstan.

yeldar.nuruly@kaznu.edu.kz

ORCID: https://orcid.org/0000-0002-9321-2285

[2]4th-year student majoring in "Restaurant and Hotel Business", Department of Recreational Geography & Tourism, Faculty of Geography & Environmental Sciences, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

sembayeva_aisulu@live.kaznu.kz

ORCID: https://orcid.org/0009-0008-2392-7390

[3]Candidate of Sciences in Geography, Associate Professor, Leading Research Fellow, Department of Recreational Geography & Tourism, Faculty of Geography & Environmental Sciences, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

Centre for Sustainable Development in Central Asia, Al-Farabi Kazakh National University, in partnership with The Hong Kong Polytechnic University, Almaty, Kazakhstan.

aliya.aktymbayeva@kaznu.edu.kz

ORCID: https://orcid.org/0000-0003-1269-4356

Abstract

1. Background

The hospitality industry is undergoing rapid digital transformation, driven by the increasing integration of cloud-based systems, Internet of Things (IoT) devices, biometric check-in solutions,

and customer-facing mobile platforms [1], [2]. However, this technological progress has also expanded the industry's cyber-attack surface, exposing hotels to threats such as identity theft, payment fraud, loyalty program abuse, and unauthorized data access. Traditional centralized IT architectures used in Property Management Systems (PMS), Customer Relationship Management (CRM), and point-of-sale networks are proving insufficient in preventing modern attacks that target data integrity, confidentiality, and availability [3], [4]. Recent incidents–such as the Marriott, Hyatt, and Romantik Seehotel Jagerwirt breaches–highlight the urgency for system-wide innovations in data protection, compliance, and forensic accountability [5], [6]. Blockchain technology, with its inherent features of decentralization, immutability, cryptographic integrity, and programmable automation via smart contracts, has emerged as a promising architecture for rethinking cybersecurity in hospitality environments.

2. Aim and research questions

This study investigates the role of blockchain-based solutions in enhancing customer data security within the hospitality sector. Specifically, it addresses three core research questions (RQs):

- *RQ1: How can blockchain technology improve the security of customer data in the hospitality sector?*
- *RQ2: What specific cybersecurity weaknesses in hospitality can blockchain help with?*
- *RQ3: What are the challenges to adopting blockchain in hospitality, and how can these be resolved?*

The goal is to produce a robust conceptual framework that links blockchain mechanisms to specific cybersecurity functions and hospitality applications, and to develop a threat classification matrix that serves as a strategic decision-support tool for industry practitioners.

3. Methodology

This research follows an integrative approach, combining:

- A systematic literature review of 85 peer-reviewed articles and industry reports published between 2014 and 2024, sourced from Scopus, IEEE Xplore, Springer, and Web of Science. The review focused on blockchain applications in cybersecurity, data protection in hospitality, and verified blockchain implementations. Non-empirical or outdated sources were excluded.
- Thematic synthesis of cybersecurity threat categories, mapped to blockchain-based countermeasures.
- Construction of a conceptual framework linking blockchain mechanisms (e.g., decentralization, immutability, encryption) to security functions, cybersecurity outcomes, and hospitality system applications.

- Design of a Cybersecurity Threat-Mitigation Matrix classifying eight common threat types (e.g., payment fraud, insider access, IoT vulnerabilities) and aligning each with specific blockchain tools such as smart contracts, verifiable credentials, and permissioned ledgers.

Framework development was informed by system design principles from Hyperledger Fabric, Ethereum, IPFS, federated learning protocols, and Zero-Knowledge Proofs, combined with behavioral theories such as the Privacy Calculus Model and Antecedent–Privacy Concern–Outcome (APCO) framework.

4. Findings

The analysis produced a layered Blockchain–Security–Application Framework (BSAF), which demonstrates how blockchain's structural mechanisms map onto security functions and, in turn, enable secure hospitality use cases.

Conceptual Framework Summary:

Blockchain Mechanism	**Security Function Enabled**	**Hospitality Outcome**
Decentralization	Availability	System uptime for PMS/IoT
Immutability	Integrity	Tamper-proof logs and guest trust
Encryption (ZKP/FHE)	Confidentiality	Biometric ID and payment data protection
Smart Contracts	Access Control	Staff role separation, IoT access limits
Self-Sovereign Identity (SSI/DID)	Auditability	Consent tracking, regulatory compliance

Additionally, the study presents a Cybersecurity Threat-Mitigation Matrix, classifying eight critical attack surfaces and pairing each with corresponding blockchain defenses:

Threat Category	**Vulnerability**	**Blockchain-Based Mitigation**
Centralized Data Risks	Single point of failure in PMS	Distributed ledger, off-chain IPFS backups
Weak Access Control	Staff login reuse, insider attacks	Smart contract-based RBAC, SSI/DID auth
Payment Fraud	POS data breach, card theft	Tokenized payments, on-chain audit trails
Identity Theft	Loyalty scams, fake profiles	Verifiable credentials, decentralized ID
IoT Device Exploits	Hijacked smart locks/devices	Blockchain-based IoT auth (IoTChain, OSCAR)

Insider Threats	Log tampering, unauthorized escalation	Immutable logs, threshold key access
Regulatory Non-Compliance	No audit trail for consent/logs	ZKP compliance trails, Fabric PDCs
Loyalty Program Abuse	Double spending, unauthorized transfers	Smart contract tokens, public verification

Performance benchmarks from deployments in adjacent domains show that blockchain-backed cybersecurity solutions can:

- Lower average response latency by up to 40% [7], [8].
- Increase trust and data-sharing willingness among consumers when privacy-preserving mechanisms are present [9], [10].

Behavioral findings also support these technical results. Studies show that:

- Loyalty members experience greater trust loss after a breach than non-members [11].
- Customers expect visible security assurances, such as certifications and privacy dashboards [12].
- Technologically inclined guests are more receptive to blockchain-driven features, especially when presented with data-sharing incentives and control over privacy settings [9].

5. Contributions

This study offers three primary contributions:

First, it develops a novel, layered conceptual framework that connects blockchain's architectural features to security functions and sector-specific use cases in hospitality.

Second, the study introduces a Cybersecurity Threat Classification and Mitigation Matrix that serves as a practical reference for hospitality IT managers and cybersecurity teams. It links known vulnerabilities (e.g., weak access control, loyalty fraud) with blockchain-based remedies (e.g., smart contracts, SSI) in an actionable format.

By articulating these conceptual and applied contributions, the study provides a strategic roadmap for hospitality firms aiming to future-proof their cybersecurity architecture through blockchain. It also positions blockchain not as a silver bullet, but as a modular infrastructure component–one that, when integrated with smart access policies, privacy-enhancing technologies, and regulatory compliance protocols, can significantly raise the resilience and trustworthiness of guest data systems.

References

Aleksandar Erceg, Jovanka Damoska Sekuloska, and Ivan Kelić, *Hospitality and Tourism Information Technology*. USF M3 Publishing, LLC, 2021. doi: 10.5038/9781732127593.

P. Thaichon, P. K. Dutta, P. Raj Chelliah, and S. Gupta, *Technology and Luxury Hospitality*. London: Routledge, 2024. doi: 10.4324/9781003488248.

M. C. Arcuri, L. Gai, F. Ielasi, and E. Ventisette, "Cyber attacks on hospitality sector: stock market reaction," *Journal of Hospitality and Tourism Technology*, vol. 11, no. 2, pp. 277–290, Jun. 2020, doi: 10.1108/JHTT-05-2019-0080.

N. Shabani and A. Munir, "A Review of Cyber Security Issues in Hospitality Industry," 2020, pp. 482–493. doi: 10.1007/978-3-030-52243-8_35.

"How Hilton Enhances Customer Experience (CX) with Digital Innovations in Hospitality." Accessed: Mar. 15, 2025. [Online]. Available: https://www.renascence.io/journal/how-hilton-enhances-customer-experience-cx-with-digital-innovations-in-hospitality

M. Manglani, "Compromised Systems, Compromised Data: A Technical Analysis of the Marriott Data Breach," *International Journal of Science and Research (IJSR)*, vol. 13, no. 4, pp. 176–180, Apr. 2024, doi: 10.21275/SR24402124923.

Z. Ullah, A. Waheed, M. Ismail Mohmand, S. Basar, M. Zareei, and F. Granda, "AICyber-Chain: Combining AI and Blockchain for Improved Cybersecurity," *IEEE Access*, vol. 12, pp. 142194–142214, 2024, doi: 10.1109/ACCESS.2024.3463976.

D. Ngabo, D. Wang, C. Iwendi, J. H. Anajemba, L. A. Ajao, and C. Biamba, "Blockchain-Based Security Mechanism for the Medical Data at Fog Computing Architecture of Internet of Things," *Electronics (Basel)*, vol. 10, no. 17, p. 2110, Aug. 2021, doi: 10.3390/electronics10172110.

R. M. Frey, P. Buhler, A. Gerdes, T. Hardjono, K. L. Fuchs, and A. Ilic, "The effect of a blockchain-supported, privacy-preserving system on disclosure of personal data," in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, IEEE, Oct. 2017, pp. 1–5. doi: 10.1109/NCA.2017.8171385.

P. Fakfare, N. Manosuthi, J.-S. Lee, M. Jin, H. Han, and J. J. Kim, "Data vulnerability and privacy risk among hotel guests who share personal data," *Journal of Vacation Marketing*, Sep. 2024, doi: 10.1177/13567667241276213.

H. S. Chen and T.-M. (Catherine) Jai, “Trust fall: data breach perceptions from loyalty and non-loyalty customers,” *The Service Industries Journal*, vol. 41, no. 13–14, pp. 947–963, Oct. 2021, doi: 10.1080/02642069.2019.1603296.

K. Berezina, C. Cobanoglu, B. L. Miller, and F. A. Kwansa, “The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth,” *International Journal of Contemporary Hospitality Management*, vol. 24, no. 7, pp. 991–1010, Sep. 2012, doi: 10.1108/09596111211258883.