Financial Risk and Management: An International Journal
Volume 4, Number 2, 2025

Tokenization and New Forms of Payment Risk in the Digital Economy

Halimatus Sakdiyah[1]

[1] Universitas Airlangga, Surabaya, Indonesia

Article history:
Received: July 25, 2025
Revised: September 11, 2025
Accepted: November 5, 2025
Published: December 30, 2025

Keywords:
Digital Economy,
Payment Risk,
Systemic Risk,
Tokenisation,
Tokenised Money.

Identifier:
Zera Open
Page: 95-109
https://zeraopen.com/journal/frmij

Abstract

This article examines tokenization as both a security mechanism and a source of new payment risks in the digital economy. The study synthesises recent evidence on how tokenization supports the growth of contactless cards, mobile wallets, instant transfers, and embedded finance while reshaping risk at the user, platform, and system levels. Tokenization reduces exposure of sensitive payment credentials and helps contain card not present fraud by limiting storage and transmission of primary account data within digital wallets and online platforms. At the same time, the review shows that concentration of mappings in token vaults, reliance on specialised token service providers, and complex token lifecycle management introduce fresh operational, governance, and legal vulnerabilities. The extension of token based designs into tokenised deposits, central bank digital currencies, and programmable settlement infrastructures further links tokenization to liquidity, run, and contagion risk. Overall, the article argues that tokenization should be viewed as a structural innovation that reconfigures the architecture of payment risk rather than as a narrow technical fix and for future empirical research.

1. Introduction

The rapid expansion of the digital economy has transformed how households and firms initiate, route, and settle payments, with contactless cards, mobile wallets, instant transfers, and embedded finance platforms displacing cash and traditional card-present transactions. This transformation has been accompanied by a sharp increase in cyberattacks, fraud, and data breaches targeting payment infrastructures, prompting regulators and industry bodies to strengthen security baselines through frameworks such as the Payment Card Industry Data Security Standard and the European Union's Second Payment Services Directive. Recent empirical studies show that security perceptions, especially around data protection and fraud prevention, are now central to digital payment adoption decisions, particularly among younger users who rely heavily on mobile and platform-based services (Al-Qudah et al., 2024). Against this backdrop, tokenization has emerged as a cornerstone technology for protecting sensitive payment data while preserving the speed and convenience expected in the digital economy.

In payment systems, tokenization replaces primary account numbers or other sensitive credentials with non-sensitive tokens that can be used to authorize transactions without exposing the underlying data. Evidence from recent technical and applied studies suggests that network and gateway tokenization can materially reduce card not present fraud and narrow the attack surface of digital wallets and e-commerce platforms by limiting the storage and transit of real card data (Bhutta et al., 2022). At the same time, tokenization is increasingly embedded into broader digital payment security architectures that combine encryption, biometric

authentication, and real time anomaly detection to counter phishing, malware, account takeovers, and large scale data breaches. These developments have led many practitioners and policymakers to frame tokenization primarily as a risk mitigating innovation that enables compliance and supports trust in digital payments.

However, the growing reliance on tokenization also creates new forms and channels of payment risk that are less well understood. The concentration of sensitive mappings in token vaults, dependence on specialized token service providers, and proliferation of application programming interfaces for token lifecycle management introduce fresh operational, governance, and third-party risks into payment chains (Banerjee et al., 2022). Misconfigured tokenization architectures, weak access controls, or failures in token provisioning and detokenization processes can generate single points of failure, complex incident response paths, and hidden correlations across merchants, acquirers, and processors. In parallel, tokenization is evolving beyond traditional card-based payments into tokenized deposits, programmable wallets, and smart-contract-based settlement layers, further blurring the boundary between cybersecurity risk, operational disruption, and liquidity or settlement risk in modern payment systems (Bhutta et al., 2022).

A further source of emerging risk arises from the extension of tokenization into wholesale and policy-relevant infrastructures, including central bank digital currencies, tokenized bonds, and cross-border "currency bridges." Recent work on the centralized use of decentralized technology highlights how tokenization can enhance the efficiency and programmability of monetary and payment systems, but

also underscores that perceived risks around governance, interoperability, and privacy strongly influence adoption and trust (Zhang, 2024). As tokenized payment instruments and infrastructures become more interconnected with existing real-time gross settlement systems, card networks, and open-banking interfaces, the potential for complex contagion channels and new systemic vulnerabilities increases. This article therefore examines tokenization not only as a security enhancement, but as a driver of qualitatively new forms of payment risk in the digital economy, mapping how token architectures, governance choices, and regulatory responses reshape the risk profile of contemporary payment ecosystems.

2. Literature Review

The growing literature on digital payments shows that the diffusion of wallets, instant transfers, and contactless instruments is tightly linked to how users perceive security, privacy, and fraud risk. Studies on mobile wallet adoption consistently find that perceived security and trust are among the strongest predictors of attitudes and usage intention, alongside usefulness and ease of use. Chawla and Joshi (2020), for example, show that security concerns and perceived risk significantly shape behavioural intention, with age and gender moderating these relationships in mobile wallet adoption. Similarly, Kapoor et al. (2022) document that in the context of the COVID-19 pandemic, perceived security and privacy protection are central to mobile wallet adoption decisions, reinforcing the view that security perceptions are now part of the core value proposition of digital payment services rather than a secondary attribute.

Beyond user perceptions, recent work has begun to map the concrete information security risks embedded in digital payment architectures. Huang et al. (2024) identify detailed "security risk items" for mobile payments offered by non-bank service providers, including vulnerabilities in credential storage, transaction routing, and third-party integrations, and show how firms respond through a combination of tokenization, encryption, access control, and governance practices. At the transaction level, Cherif et al. (2023) review disruptive technologies in credit card fraud detection and highlight how card-not-present environments and e-commerce ecosystems expand the attack surface, calling for layered controls that include tokenization, behavioural analytics, and machine-learning-based anomaly detection. Complementing this perspective, Onumadu and Abroshan (2024) show that proximity payment channels based on near-field communication face specific cyber threats such as relay attacks and skimming and argue that mitigations must combine secure element design, dynamic credentials, and, increasingly, tokenization to limit the exposure of sensitive data.

At the infrastructure and policy level, the literature on central bank digital currencies (CBDCs) and tokenised forms of money underscores that tokenization can both reduce some traditional operational risks and introduce new channels of payment and liquidity risk. Ahnert et al. (2024) synthesize the economics of CBDCs, documenting how digital central bank money may improve payment efficiency and resilience but can also affect bank funding structures, run dynamics, and the allocation of liquidity across the system. Tercero-Lucas (2023) uses a modern monetary system framework to show that CBDCs can alter the transmission of

shocks through payment and funding networks, with implications for financial stability depending on design choices such as remuneration, access, and limits. Buzuriu (2024) reviews this emerging evidence and highlights that digital public money and tokenised deposits may create novel forms of competition and interconnectedness between payment instruments, raising questions about new liquidity, run, and contagion risks that extend beyond traditional card and account based payment systems.

Finally, recent legal and regulatory scholarship emphasizes that tokenization also reconfigures legal and governance risk in payment and settlement chains. Lavayssière (2024) analyses the legal structures of tokenised assets and shows that differences in how jurisdictions recognize on-chain records, custodial arrangements, and contractual rights can generate significant uncertainties around ownership, enforceability, and investor protection. When applied to payment tokens, tokenised deposits, or programmable settlement assets, these issues suggest that concentration in token service providers, ambiguity over liability in case of technical failures, and fragmentation of legal regimes can become sources of operational and systemic risk in their own right. Taken together, this body of work indicates that tokenization should be understood not only as a technical control that enhances digital payment security, but also as a structural innovation that reshapes the configuration of cyber, operational, legal, and financial stability risks across the digital payment ecosystem.

3. Methods

This study employs a systematic literature review method to synthesise existing evidence on tokenization and new forms of payment risk in the digital economy. The review focuses on peer-reviewed journal articles and high-quality conference papers that examine tokenization in relation to digital payments, fraud, cybersecurity, operational risk, liquidity and settlement risk, central bank digital currencies, tokenised deposits, and related payment innovations. The temporal scope is restricted to recent publications in order to capture the latest developments in technology, regulation, and market practice. The review seeks to answer how tokenization is conceptualised in the literature, which types of risks it is argued to mitigate, and which new payment risks and vulnerabilities it may create at the user, platform, and system levels.

Relevant studies were identified through structured searches in major academic databases such as Scopus, Web of Science, ScienceDirect, IEEE Xplore, and SpringerLink, complemented by targeted searches in Google Scholar for additional peer-reviewed sources. A combination of keywords and Boolean operators was used, including terms such as "tokenization", "digital payments", "payment risk", "card-not-present fraud", "central bank digital currency", "tokenised deposits", "programmable money", and "systemic risk", with filters set for English-language and peer-reviewed outputs. Inclusion criteria required that studies explicitly address tokenization or tokenised forms of money in the context of payment systems or financial market infrastructures and provide empirical, conceptual, legal, or technical analysis of associated risks. Exclusion criteria removed

non-peer-reviewed materials, local open-journal outlets, purely cryptographic or engineering papers without a payment-risk focus, and duplicate records.

The review process followed a structured screening protocol comprising three stages: initial identification, title and abstract screening, and full-text assessment. At each stage, studies were checked against the inclusion and exclusion criteria to ensure consistency and transparency. For all retained articles, a standardised data extraction form was used to capture publication details, research context, methodological approach, type of tokenization or tokenised instrument, payment context (retail, wholesale, cross-border), and the specific risk dimensions discussed, including cyber, fraud, operational, liquidity, legal, governance, and systemic risk. The extracted information was then synthesised using a qualitative, thematic approach that grouped findings into three analytical layers: user and transaction level risk, platform and provider-level risk, and infrastructure and system-level risk. This structure allows the review to map how token architectures, governance choices, and regulatory frameworks jointly shape the evolving risk profile of tokenized payments in the digital economy.

4. Results and Discussion

The systematic review reveals that tokenization sits at the intersection of two major strands in the digital payments literature: user-level security perceptions and infrastructure-level risk management. At the user and transaction level, studies on mobile and digital payment adoption show that perceived security, privacy, and fraud protection are decisive determinants of usage intention, alongside convenience and

usefulness (Chawla & Joshi, 2020; Kapoor et al., 2022; Al-Qudah et al., 2024). These findings help explain why tokenization, although largely invisible to end-users, is promoted by providers as a way to strengthen trust in mobile wallets, instant payments, and platform-based services. In this sense, tokenization functions as a "back-end" mechanism that supports the "front-end" trust constructs documented in the adoption literature: by reducing the exposure of sensitive credentials, tokenization underpins the perception that digital payments are safe enough to substitute for cash and card-present transactions.

At the same time, the review shows that tokenization only addresses a subset of the concrete security vulnerabilities identified in digital payment architectures. Huang et al. (2024) document that mobile payment services face risks related to credential storage, transaction routing, and third party integrations, and that firms respond through combinations of tokenization, encryption, access control, and governance mechanisms. Similarly, Cherif et al. (2023) highlight that card not present and e-commerce environments expand the attack surface for fraud, calling for layered controls that combine tokenization with behavioural analytics and machine-learning based anomaly detection. Onumadu and Abroshan (2024) further show that near field communication payments introduce specific threats such as relay attacks and skimming, which must be mitigated through secure element design and dynamic credentials alongside tokenization. Taken together, these studies indicate that tokenization is most effective when embedded in a multi layered security architecture; as a standalone measure, it cannot fully neutralise the broader spectrum of cyber and fraud risks in digital payments.

For platform and provider-level risk, the evidence suggests a more ambivalent picture. Technical studies emphasise that network and gateway tokenization can materially reduce card not present fraud and limit the storage and transit of real card data in wallets and e-commerce platforms (Bhutta et al., 2022). However, legal and governance analyses point to new vulnerabilities created by the concentration of sensitive mapping information in token vaults and the dependence on specialised token service providers. Banerjee et al. (2022) discuss how tokenisation frameworks centralise control and data within a small number of actors, raising questions about liability, accountability, and privacy when token vaults or token lifecycle management interfaces are compromised. Lavayssière (2024) shows that the legal recognition of on-chain records, custodial arrangements, and contractual rights remains uneven across jurisdictions, creating uncertainty over ownership and enforceability in tokenised environments. When these legal frictions intersect with technical dependence on third-party token service providers, tokenization can shift the locus of risk rather than eliminate it, concentrating operational and governance risk in a few critical nodes of the payment ecosystem.

The review also highlights that tokenization is increasingly deployed beyond traditional card-based retail payments into tokenised deposits, programmable wallets, and smart-contract-based settlement layers, blurring the line between cyber risk, operational disruption, and liquidity or settlement risk. Bhutta et al. (2022) underline that integrating tokenization with real-time anomaly detection and programmable workflows can enhance security and automation, but misconfigurations or failures in token provisioning and detokenization processes can

generate single points of failure and complex incident response paths. This aligns with the broader literature on central bank digital currencies and tokenised forms of money, which finds that digital public money and tokenised deposits may introduce new channels of liquidity and run risk. Ahnert et al. (2024) show that central bank digital currencies can alter bank funding structures and run dynamics, while Tercero-Lucas (2023) and Buzuriu (2024) emphasise that competition and interconnectedness between digital public money, tokenised deposits, and legacy payment instruments may amplify contagion during stress episodes. Although these studies do not always focus on tokenization in a narrow technical sense, they underscore that token based designs at the infrastructure level have systemic implications that go beyond fraud mitigation.

Finally, the findings suggest that governance and regulatory design play a critical role in determining whether tokenization functions primarily as a stabilising or destabilising force in payment systems. Zhang (2024) argues that the centralised use of decentralised technology in areas such as central bank digital currencies and cross-border currency bridges can enhance efficiency and programmability, but that adoption and trust are highly sensitive to perceptions of governance, interoperability, and privacy. When combined with the legal uncertainties documented by Lavayssière (2024) and the concentration and liability concerns raised by Banerjee et al. (2022), this implies that poorly designed tokenisation regimes risk creating opaque dependencies and fragmented legal responsibilities across payment chains. Conversely, carefully calibrated token governance anchored in clear liability rules, robust oversight of token service providers, and interoperable technical standards

can harness the security benefits documented in the transaction-level literature while containing new forms of operational, legal, and systemic risk.

Overall, the systematic review shows that tokenization should not be interpreted as a purely technical fix to fraud and data breaches. At the user level, it indirectly supports adoption by reinforcing perceived security and trust, but only as one element in a broader security and user experience bundle. At the platform level, it reduces certain data-exposure and fraud risks while simultaneously creating new operational and governance vulnerabilities linked to vaults, providers, and complex token lifecycle management. At the system level, token based designs in central bank digital currencies, tokenised deposits, and programmable payment infrastructures reshape liquidity, run, and contagion dynamics in ways that depend critically on legal, regulatory, and design choices. These layered results justify treating tokenization as a structural innovation that reconfigures the entire risk architecture of the digital payment ecosystem, rather than as an isolated security control.

5. Conclusion

This study concludes that tokenization occupies a dual role in the digital payment ecosystem: it is both a powerful security enhancer and a source of new, sometimes opaque, forms of risk. At the user level, tokenization supports the trust and perceived security that drive adoption of mobile wallets, instant payments, and other digital channels, reinforcing evidence that data protection and fraud prevention are now core components of the value proposition for payment services. At the platform level, tokenization demonstrably reduces card-not-present fraud and

limits the exposure of sensitive credentials, but it also creates new operational and governance vulnerabilities by concentrating sensitive mappings in token vaults and increasing dependence on specialised token service providers. At the system level, the extension of token-based designs into central bank digital currencies, tokenised deposits, and programmable settlement infrastructures reshapes liquidity, run, and contagion dynamics, indicating that tokenization has macro-financial implications that reach far beyond conventional cyber-risk narratives.

These findings imply that tokenization should be treated not as a self-contained technical fix, but as a structural innovation that reconfigures the entire risk architecture of modern payment systems. For regulators and policymakers, the key challenge is to design governance and supervisory frameworks that preserve the clear security and efficiency benefits of tokenization while addressing concentration, legal uncertainty, interoperability gaps, and potential systemic vulnerabilities. This calls for clear allocation of liability along payment chains, robust oversight of token service providers, harmonised standards for token lifecycle management, and careful calibration of token-based public money and settlement infrastructures. For researchers, the results highlight the need for more integrated work that links micro level security design with platform governance and system-wide stability analysis, so that future tokenization regimes can be engineered with both fraud mitigation and financial stability in view.

References

Al-Qudah, A. A., Al-Okaily, M., Shiyyab, F. S., Taha, A. A., Almajali, D. A., Masa'deh, R. E., & Warrad, L. H. (2024). Determinants of digital payment adoption among Generation Z: An empirical study. *Journal of Risk and Financial Management, 17*(11), 521.

Banerjee, S., Shukla, S., & Menon, K. S. (2022). The tokenisation framework and its privacy discontents: Issues and solutions. *NUJS Law Review, 15*, 208.

Bhutta, M. N. M., Bhattia, S., Alojail, M. A., Nisar, K., Cao, Y., Chaudhry, S. A., & Sun, Z. (2022). Towards secure IoT-based payments by extension of Payment Card Industry Data Security Standard (PCI DSS). *Wireless Communications and Mobile Computing, 2022*(1), 9942270.

Buzuriu, B. C. (2024). Central bank digital currencies and financial stability: Literature review and new questions. *Timisoara Journal of Economics and Business, 17*(1), 41–64.

Carapella, F., Swem, N., & Gerszten, J. (2023). Tokenization: Overview and financial stability implications. *Finance and Economics Discussion Series*.

Chawla, D., & Joshi, H. (2023). Role of mediator in examining the influence of antecedents of mobile wallet adoption on attitude and intention. *Global Business Review, 24*(4), 609–625.

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University–Computer and Information Sciences, 35*(1), 145–174.

Garratt, R., & Shin, H. S. (2023). Stablecoins versus tokenised deposits: Implications for the singleness of money. *BIS Bulletin, 73*.

Kapoor, A., Sindwani, R., Goel, M., & Shankar, A. (2022). Mobile wallet adoption intention amid COVID-19 pandemic outbreak: A novel conceptual framework. *Computers & Industrial Engineering, 172*, 108646.

Lavayssière, X. (2024). Legal structures of tokenised assets. *European Journal of Risk Regulation*, 1–13.

Liébana-Cabanillas, F., Kalinic, Z., Muñoz-Leiva, F., & Higueras-Castillo, E. (2024). Biometric m-payment systems: A multi-analytical approach to determining use intention. *Information & Management, 61*(2), 103907.

Onumadu, P., & Abroshan, H. (2024). Near-field communication (NFC) cyber threats and mitigation solutions in payment transactions: A review. *Sensors, 24*(23), 7423.

Ruslim, T. S., & Herwindiati, D. E. (2024). Adoption of e-wallet in the post-pandemic era: A study on Generation X's intention to use e-wallet. *Innovative Marketing, 20*(2), 267.

Zhang, Y., Gong, B., & Zhou, P. (2024). Centralized use of decentralized technology: Tokenization of currencies and assets. *Structural Change and Economic Dynamics, 71*, 15–25.