International Journal of Safety and Security Engineering
Vol. 16, No. 9, September, 2026, pp. 2007-2016
Journal homepage: http://iieta.org/journals/ijsse

From Adoption to Security Assurance: Mapping the Knowledge Structure and Evidence Gaps in Digital Wallet Security, Privacy, Governance, and Auditability (2015–2025)

Maria Rosa Cruzado Puente[1], Edinson Nestor Mendoza Culqui[1], Carlos Daniel Gonzales Hidalgo[1*], Joel Vásquez Quintos[2], Sara Judith Terán Leiva[2], Gladys Magaly Bernal Cubas[1], Jaime Laramie Castañeda Gonzales[3]

[1] Faculty of Accounting, Economic, and Financial Sciences, Universidad San Martin de Porres-Filial Norte, Chiclayo 14012, Peru
[2] Faculty of Accounting and Business Sciences, Universidad Nacional Autónoma de Chota, Chota 06121, Peru
[3] Administración y Negocios, Universidad Tecnológica del Peru (UTP), Chiclayo 14011, Peru

Corresponding Author Email: cgonzalesh@usmp.pe

Copyright: ©2026 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.160907

Received: 25 July 2026
Revised: 31 August 2026
Accepted: 11 September 2026
Available online: 30 September 2026

Keywords:
auditability, digital wallets, governance, privacy, scientometrics, security assurance

ABSTRACT

This study maps the scientific and conceptual structure of digital-wallet security assurance and identifies evidence gaps across security, privacy, risk, governance, fraud control, and auditability. A reproducible Scopus search covering 2015–2025 retrieved 80 English-language articles. Title-and-abstract screening excluded eight peripheral records, leaving 72 documents. Performance analysis, citation analysis, author-keyword co-occurrence, spectral community detection, and dictionary-based longitudinal coding were applied. The corpus comprised 59 sources, 250 authors, 1,985 citations, and 279 distinct author keywords. Security and authentication appeared in 45 documents (62.5%), whereas adoption/continuance and trust/risk each appeared in 28 (38.9%). Recent work strengthened fraud detection, crypto-custody, offline-payment, trust, and risk themes. Auditability and accountability were absent from titles and author keywords and appeared only marginally in one abstract. Unlike broad mappings of electronic payments or wallet adoption, this study isolates digital wallets as security-control environments and reframes the literature around a transition from adoption to verifiable assurance. Future research and practice should operationalize auditable controls, tamper-evident logs, incident evidence, governance responsibilities, and comparable assurance metrics across custodial and non-custodial wallet architectures.

1. INTRODUCTION

Digital wallets have moved from peripheral payment applications to infrastructures that mediate retail payments, remittances, central-bank digital currency experiments, crypto-asset custody, and access to platform-based financial services. Their expansion has generated a mature stream of adoption research built around perceived usefulness, ease of use, trust, perceived risk, provider reputation, and behavioral intention [1-8]. Yet adoption is no longer the only relevant question. As wallets store credentials, payment tokens, private keys, transaction histories, and identity attributes, their reliability increasingly depends on security architecture, privacy safeguards, fraud controls, governance arrangements, and demonstrable accountability.

The literature has responded unevenly to this transition. Technical studies examine wallet vulnerability and exploit detection [9], cryptographic key management [10], authentication and proof-of-ownership mechanisms [11], offline payment protocols [12], forensic recovery [13], and additional cryptographic, vulnerability-analysis, and wallet-security mechanisms [14-21]. Behavioral studies continue to model trust, perceived security, privacy, and continuance intention [1-4]. A smaller governance-oriented stream addresses data-protection compliance, crypto custody, regulatory responsibility, and self-custody [22-26]. These streams are relevant to the same assurance problem but are often studied independently, which makes it difficult to determine whether the field has developed a coherent knowledge base or merely accumulated disconnected technical and behavioral solutions.

Existing bibliometric studies have generally mapped digital payments, mobile-wallet adoption, financial inclusion, or blockchain-enabled finance at a broad level. A recent study in this journal mapped personal-information security across electronic payments using Scopus, Web of Science, VOSviewer, and Bibliometrix [27]. That contribution established the importance of privacy, trust, and technology acceptance, but it did not isolate digital wallets as a distinct control environment or examine whether security claims are supported by governance, traceability, incident evidence, and independent verification. The present study therefore narrows the unit of analysis to payment, financial, and crypto-asset wallets and evaluates the field through a security-assurance

lens. This high-precision framing makes it possible to distinguish perceived security from verifiable control effectiveness and to identify auditability as a structural evidence gap rather than an established research stream.

This study treats assurance as the capacity to generate justified confidence that a wallet operates in accordance with stated security, privacy, integrity, compliance, and accountability requirements. Assurance is broader than security: it includes the governance of controls, traceability of transactions and incidents, evidence preservation, responsibility allocation, and independent verification. The proposed adoption-to-assurance transition does not imply that adoption research disappears. Instead, assurance themes increasingly intersect with adoption constructs, while new technical and regulatory streams emerge. Scientometric mapping is therefore used to assess both the structure of this convergence and the gaps that remain.

The general objective is to map the intellectual and thematic structure of Scopus-indexed research on digital-wallet assurance from 2015 to 2025 and to identify evidence gaps across security, privacy, fraud control, governance, risk, and auditability. The specific objectives are to: (1) characterize the evolution, sources, authors, countries, citation impact, and collaboration patterns of the corpus; (2) map the conceptual structure linking adoption, trust, security, privacy, crypto-wallet infrastructure, and compliance; (3) examine the temporal transition from adoption-centered research toward assurance-centered themes; and (4) identify underdeveloped constructs and propose a research agenda for trustworthy and auditable wallet ecosystems. The study focuses on financial, payment, and crypto-asset wallets; records in which the wallet was incidental or only an identity container were excluded.

2. LITERATURE REVIEW

Adoption research established the behavioral foundations of digital-wallet scholarship. Trust mediates merchant intention, while perceived usefulness, ease of use, enjoyment, convenience, privacy, and security shape initial, renewed, and continued use [1-8]. Recent evidence further connects perceived security and protective behavior with satisfaction, loyalty, usage barriers, government support, gamification, and risk responses [28-34]. This evidence demonstrates that assurance perceptions affect adoption, but a perception-based construct is not equivalent to evidence that technical controls are effective. Studies measuring perceived security can therefore coexist with unresolved vulnerabilities, opaque governance responsibilities, or weak incident-accountability mechanisms.

The technical-security stream addresses authentication, cryptographic protocols, private-key protection, wallet ownership proofs, forensic acquisition, and vulnerability testing [9-13, 14-21, 35]. Crypto-wallet studies extend the problem from payment credentials to loss-resistant key storage, custody, smart-contract interaction, and recovery. Experimental studies have demonstrated both secure outsourced verification and practical exposure of wallet secrets, while forensic work has recovered transaction, key, passphrase, and device evidence from software and hardware environments [14, 15, 17, 19]. Distributed key management, seed-phrase splitting, biometric authentication, and shared-custody designs attempt to reduce single-point-of-failure risk [16, 18, 20, 21, 36]. Reviews and application studies additionally show that blockchain integration can strengthen payment controls while creating wallet-smart-contract and protocol-specific attack surfaces [37-39]. These studies provide concrete control mechanisms, but their heterogeneous architectures and threat models limit comparability. Security is frequently demonstrated through a protocol or case implementation rather than a standardized assurance framework that can be independently evaluated.

Privacy and governance research is narrower but conceptually important. Empirical work has evaluated mobile wallet privacy policies, GDPR compliance, and country-level privacy risk [22-24]. Legal scholarship has examined data protection, crypto-custody terms, self-custody regulation, and allocation of liability [25, 26]. These studies shift the unit of analysis from user perceptions to institutional duties and observable policy properties. Nevertheless, privacy compliance, technical security, and operational governance remain weakly integrated, and auditability is rarely operationalized as a measurable construct.

3. METHODOLOGY

3.1 Research design and database

A retrospective bibliometric and thematic study was conducted using Scopus records. The design combined performance analysis with science mapping, following established guidance for transparent bibliometric research [40, 41]. Scopus was selected as the single source because it supplies standardized citation, affiliation, author-keyword, and reference metadata under persistent EIDs, which supports consistent deduplication and reproducible network construction across the interdisciplinary security, information systems, finance, and legal literature. A single normalized source also avoided cross-database differences in citation counts, source titles, and document identifiers. The resulting corpus is intentionally focused: the search required both a wallet descriptor and an assurance descriptor in prominent metadata fields. Its size therefore reflects a high-precision design rather than an attempt to represent all electronic-payment research.

3.2 Search strategy

The final search was executed on 24 July 2026. The strategy required a wallet descriptor and an assurance descriptor in the title or author keywords, as well as a financial, payment, or transaction context in the title, abstract, or keywords. The search was limited to English-language articles published from 2015 through 2025. The complete executable equation is reported in Appendix A. The query retrieved 80 records. This precision-oriented design may reduce recall compared with a broader TITLE-ABS-KEY strategy because both the wallet and assurance descriptors were restricted to the title or author keywords.

3.3 Eligibility and quality control

Eligibility screening was conducted at the title-and-abstract level. Records were included when a financial, payment, or crypto-asset wallet was a substantive object and at least one assurance dimension was central to the study: security, authentication, privacy, data protection, fraud, risk, trust,

governance, regulation, compliance, custody, or auditability. Eight records were excluded because wallets were incidental to broader work on bank-FinTech cooperation, organizational blockchain transparency, digital authentication, cryptocurrency regulation, national payment systems, self-sovereign identity/KYC, digitally facilitated economic abuse, or blockchain criminal law. The final corpus contained 72 records. Ambiguous records were re-read against the wallet-centrality and assurance-centrality criteria. No missing DOI, keyword, or reference value was imputed. All seven authors participated in title-and-abstract screening. Ambiguous records, including the eight ultimately excluded, were re-read collectively, and inclusion decisions were reached by consensus. Because screening was collective rather than independently duplicated, no inter-rater agreement statistic was calculated. Figure 1 presents a PRISMA 2020-style flow diagram summarizing this selection process [42].

3.4 Analytical procedures

The analysis was implemented in Python 3.12 using pandas, scikit-learn, and Matplotlib. Performance analysis covered annual output, source and author productivity, country participation, citation counts, and international co-authorship. Author keywords were lowercased and normalized for common singular/plural and orthographic variants. A weighted co-occurrence matrix was constructed for keywords appearing in at least two documents, and spectral clustering with a fixed random seed identified communities. Thematic evolution was compared between 2015–022 and 2023–2025. A transparent multi-label dictionary coded title and author-keyword evidence into security/authentication, privacy/data protection, trust/risk/user protection, governance/regulation/compliance, fraud/financial crime, adoption/continuance, and auditability/accountability. Documents could receive multiple labels. Country-level productivity was computed using full counting: each document was credited once to every country represented in the author affiliations, and a document with authors from k countries was counted once under each of the k countries. International collaboration (Multiple Country Publications, MCP) was defined as any document whose author affiliations spanned two or more distinct countries. The multi-label dictionary was applied only to titles and author keywords, representing a conservative, high-precision, lower-recall design consistent with the search strategy.

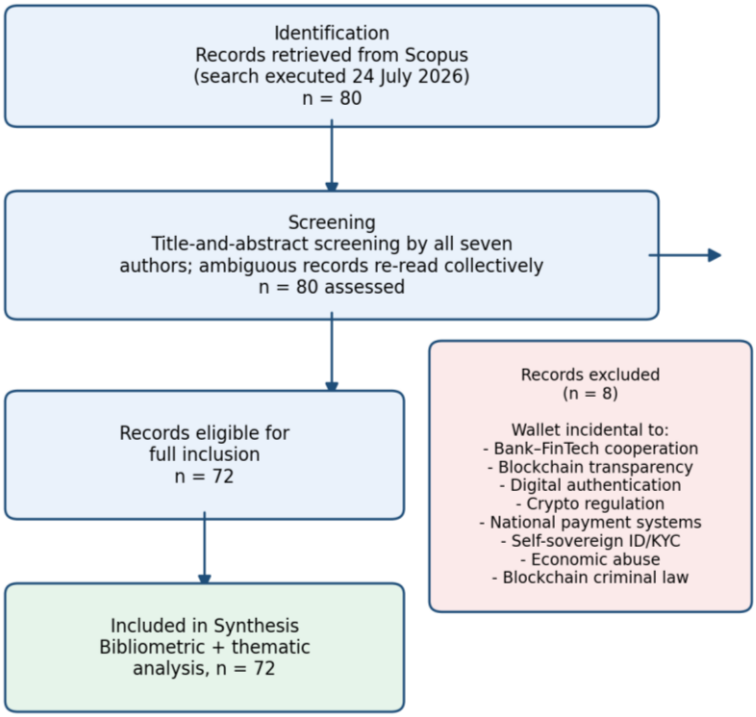


Figure 1. PRISMA 2020-style flow diagram of record identification, screening, and inclusion

4. RESULTS

4.1 Corpus profile and growth

The 72-document corpus was dispersed across 59 sources and involved 250 distinct authors. It accumulated 1,985 Scopus citations, with a mean of 27.6 and a median of 11.5 citations per document; five articles were uncited at the extraction date. Fifteen documents (20.8%) involved affiliations from more than one country. The gap between the mean and median reflects a right-skewed impact distribution dominated by a limited set of highly cited adoption and trust studies.

Table 1. Annual scientific production

Year	Documents
2015	0
2016	0
2017	1
2018	3
2019	4
2020	8
2021	4
2022	4
2023	14
2024	17
2025	17

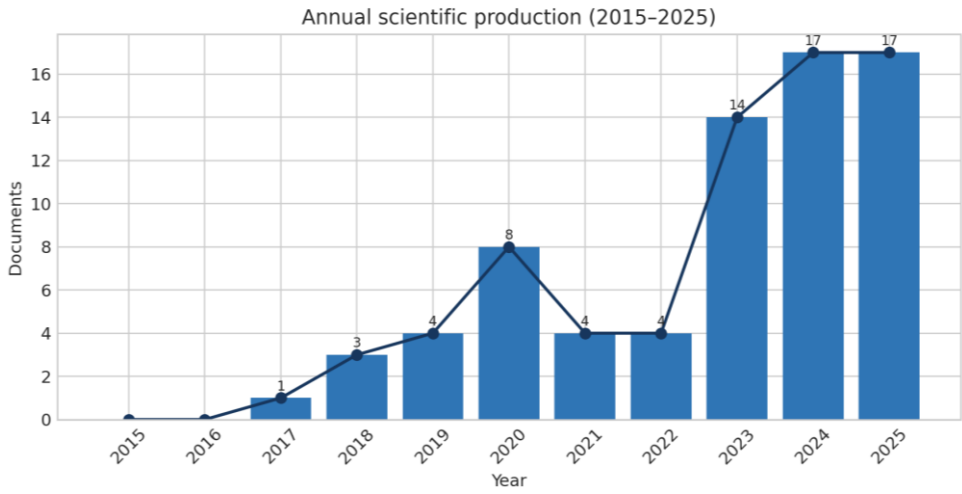


Figure 2. Annual scientific production in the final corpus

No eligible article was retained for 2015 or 2016. Output began with one article in 2017 and increased to 17 articles in both 2024 and 2025, equivalent to a 42.5% compound annual growth rate from 2017 to 2025. Two-thirds of the corpus (48 articles) were published during 2023–2025, demonstrating that assurance-oriented wallet research is recent rather than evenly distributed across the study window. The trajectory accelerated after 2022, when technical security, crypto-wallet, custody, and fraud-detection studies expanded alongside behavioral work. This annual trajectory is summarized in Table 1 and Figure 2.

4.2 Sources, authors, countries, and impact

Cogent Business & Management, IEEE Access, and Applied Sciences each published four articles, while the Journal of Retailing and Consumer Services published three (Table 2). Source influence differed from productivity: the three Journal of Retailing and Consumer Services articles accumulated 562 citations, more than any other source. The distribution shows an interdisciplinary field spanning consumer behavior, information systems, cybersecurity, engineering, data protection, and financial regulation.

Rao, H.R. was the most productive author with four documents, while Akanfe, O. and Valecha, R. each authored three. Their shared work on privacy-policy compliance and country-level privacy risk constitutes the most coherent governance-oriented program in the corpus [22-24]. India led country participation with 15 documents and 679 citations, followed by the United States with 10 documents, while Saudi Arabia and China each contributed seven documents. The 20.8% international-collaboration share indicates that most assurance research remains nationally or institutionally bounded. The 15 documents attributed to India represent country-level productivity under full counting, whereas the 15 internationally collaborative documents represent publications with author affiliations spanning more than one country (MCP); the identical values are coincidental.

Table 2. Most productive and influential sources

Source	Documents	Citations
Cogent Business & Management	4	243
IEEE Access	4	92
Applied Sciences (Switzerland)	4	56
Journal of Retailing and Consumer Services	3	562
Computers & Security	2	45
Review of Integrative Business and Economics Research	2	15
Global Business Review	1	113
Polish Journal of Management Studies	1	98

Table 3. Most cited documents

Reference	Document	Citations	Citations/Year
Singh and Sinha [1]	How perceived trust mediates merchant's intention to use a mobile wallet technology?	370	61.7
Chawla and Joshi [3]	Role of mediator in examining the influence of antecedents of mobile wallet adoption on attitude and intention.	113	37.7
To and Trinh [2]	Understanding behavioral intention to use mobile wallets in Vietnam: Extending the TAM model with trust and enjoyment.	165	33.0
Mombeuil and Uhde [4]	Relative convenience, relative advantage, perceived security, perceived privacy, and continuous use intention of China's WeChat Pay: A mixed-method two-phase design study.	108	21.6
Mombeuil [6]	An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets.	84	14.0
Alaeddin et al. [5]	From physical to digital: Investigating consumer behaviour of switching to mobile wallet; [Od fizycznego do cyfrowego: Badanie zachowania konsumenckiego przestawiania się na portfel mobilny].	98	12.3
Sarmah et al. [7]	Understanding intentions and actual use of mobile wallets by millennial: An extended TAM model perspective.	72	12.0
Garrouch [8]	Does the reputation of the provider matter? A model explaining the continuance intention of mobile wallet applications.	58	11.6

The most cited article was Singh and Sinha's study of trust and merchant intention (370 citations), followed by To and Trinh's extension of TAM with trust and enjoyment (165 citations) [1, 2]. Chawla and Joshi's mediation study recorded 113 citations, and Mombeuil and Uhde's mixed-method analysis of security, privacy, and continued use recorded 108 [3, 4]. In contrast, newer technical and governance studies have lower raw citation counts because of their shorter exposure windows. The citation hierarchy therefore confirms the historical dominance of adoption research but should not be interpreted as evidence that assurance topics are less relevant. Table 3 now also reports citations-per-year (citations divided by years elapsed since publication, reference year (2026), to correct for publication-age bias: under this normalized indicator, Chawla and Joshi [3] rose above To and Trinh [2] despite its lower raw citation count, because its shorter exposure window understates its raw total. We adopt citations-per-year as the primary indicator for interpreting document influence in this fast-growing field. Consistent with this indicator, Table 3 is now sorted in descending order of citations-per-year rather than raw citation count, and each entry is prefixed with its corresponding reference number.

4.3 Conceptual structure

The author-keyword co-occurrence network (Figure 3) contained five interpretable communities. The first linked trust, perceived usefulness, perceived ease of use, perceived risk, attitude, and behavioral intention, representing the adoption-and-value tradition. The second connected mobile wallet, security, privacy, continuance intention, digital signature, machine learning, and fraud detection, showing an emerging bridge between behavioral and technical assurance. The third grouped cryptocurrency, crypto wallet, Bitcoin, memory forensics, and cryptographic protocols. The fourth connected digital wallet, blockchain, cryptocurrency wallet, key management, offline payment, and multiparty computation. The fifth comprised GDPR, privacy policies, mobile wallet and remittance applications, and digital payment systems. This structure indicates that assurance is not one consolidated specialty; it is distributed across behavioral, technical, crypto-asset, infrastructure, and compliance communities (Table 4).

Table 4. Most frequent normalized author keywords

Keyword	Documents
mobile wallet	18
security	12
trust	11
digital wallet	10
cryptocurrency	10
perceived usefulness	8
perceived ease of use	6
blockchain	5
privacy	5
continuance intention	5
cryptocurrency wallet	5
crypto wallet	4
perceived risk	4
perceived trust	3
digital signature	3

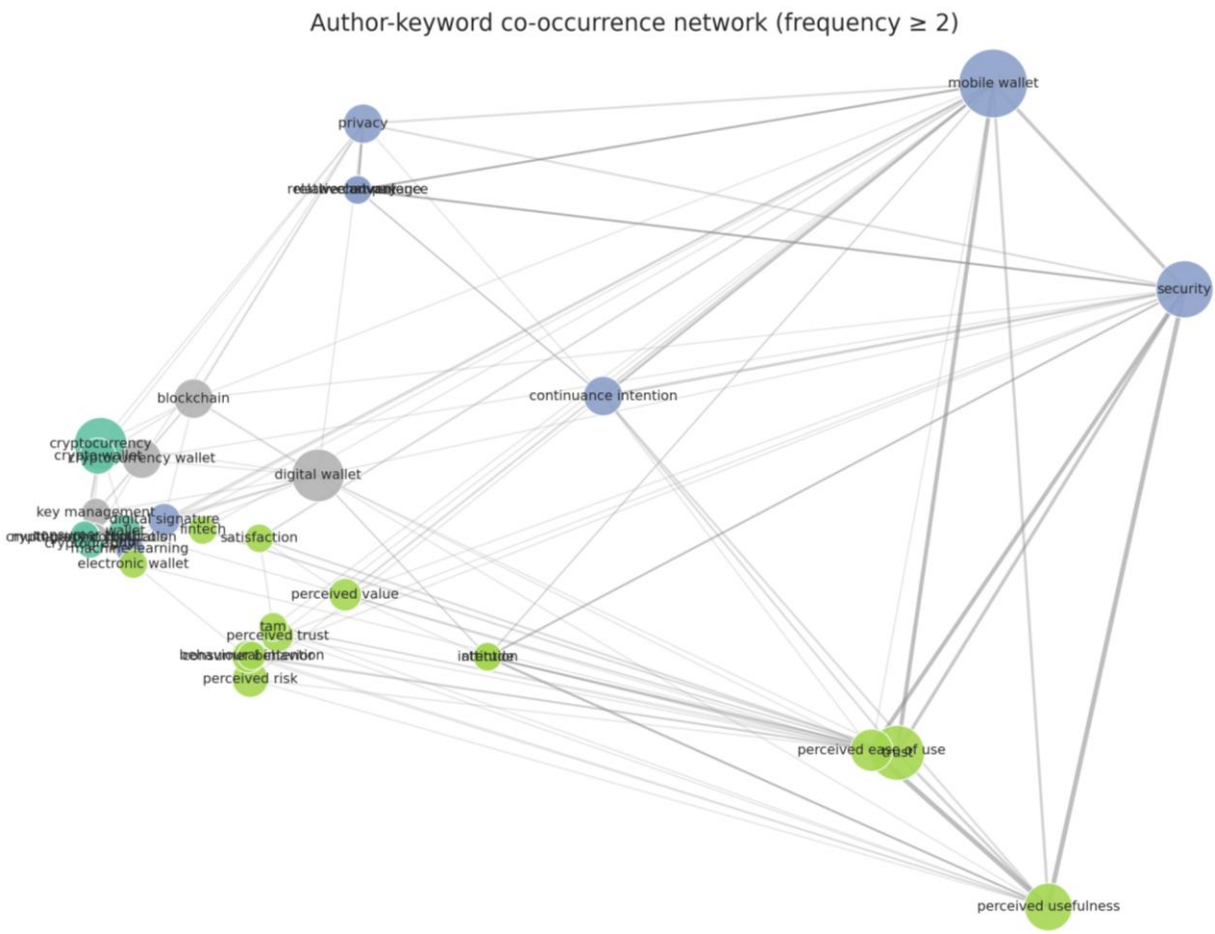


Figure 3. Author-keyword co-occurrence network (minimum frequency: two documents)

4.4 Thematic evolution and evidence gaps

Security and authentication were the largest coded theme, appearing in 45 documents (62.5%) and maintaining the same proportional presence in 2015–2022 and 2023–2025. Adoption/continuance and trust/risk each appeared in 28 documents (38.9%). Trust/risk increased from 33.3% of early documents to 41.7% of recent documents, while governance/regulation/compliance increased from 12.5% to 14.6%. Fraud and financial crime appeared only in the recent period. Privacy/data protection declined in relative share from 33.3% to 6.3%. Because the comparison uses unequal windows (eight years and 24 documents versus three years and 48 documents), these percentage shifts describe the composition of each period and should be interpreted as exploratory rather than confirmatory. A documents-per-year comparison provides additional context but does not remove the temporal asymmetry: privacy/data protection remained at 1.0 document per year (8/8 versus 3/3), whereas trust/risk increased from 1.0 to 6.7 documents per year (8/8 versus 20/3). Thus, the lower recent share of privacy research reflects rapid expansion in other themes rather than a decline in its absolute annual output. Table 5 reports the within-period shares used for the thematic comparison; the unequal period lengths remain a study limitation.

The sharpest evidence gap concerned auditability (Figure 4). None of the 72 titles or author-keyword sets used audit, auditability, accountability, traceability, or assurance as a substantive descriptor. This result derives from the multi-label dictionary applied systematically and uniformly at the title/author-keyword level. During title-and-abstract eligibility screening, the authors identified one 2025 smart-contract and wallet-interaction case study whose abstract mentioned auditability. Because the same dictionary was not systematically applied to all 72 abstracts, this observation is presented only as an illustrative instance and not as a formal abstract-level prevalence estimate. The reproducible finding is therefore the 0.0% prevalence at the title/author-keyword level. This conservative result may underestimate auditability-related discussion in the full texts, but it shows that auditability is not established as an explicit organizing construct in the corpus. Although the literature frequently discusses security, trust, privacy, and compliance, it rarely examines how claims can be independently verified, how evidence should be retained, who is accountable for control failures, or which metrics support assurance across custodial and non-custodial models.

Table 5. Thematic evolution based on multi-label coding

Theme	Early n	Recent n	Early Share	Recent Share
Adoption and continuance	10	18	41.7%	37.5%
Fraud and financial crime	0	2	0.0%	4.2%
Governance, regulation and compliance	3	7	12.5%	14.6%
Privacy and data protection	8	3	33.3%	6.3%
Security and authentication	15	30	62.5%	62.5%
Trust, risk and user protection	8	20	33.3%	41.7%
Auditability and accountability	0	0	0.0%	0.0%

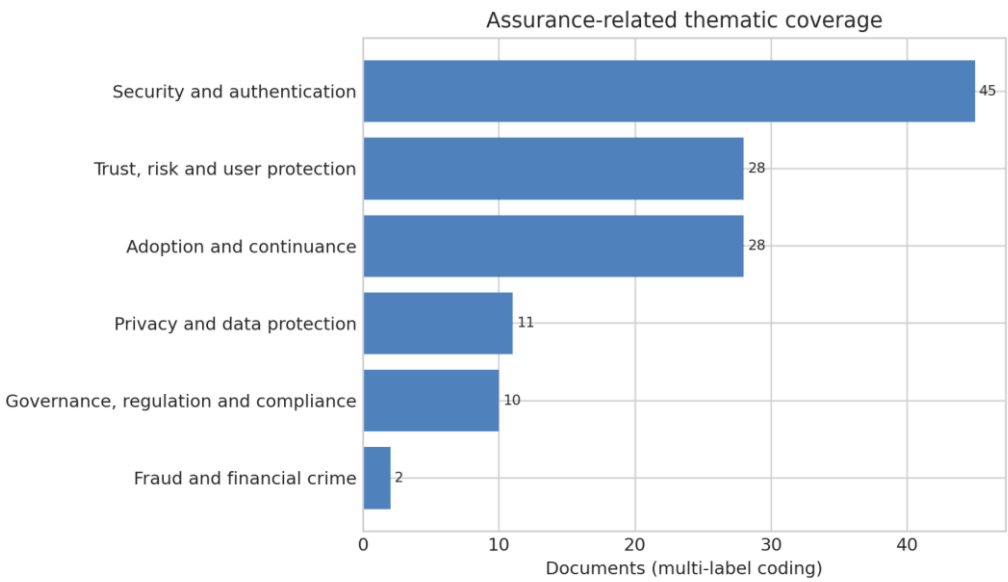


Figure 4. Assurance-related thematic coverage of the corpus

5. DISCUSSION

The results support an incomplete adoption-to-assurance transition: adoption remains dominant by citation leadership, yet two-thirds of the corpus was published after 2022 and increasingly addresses authentication, crypto-custody, vulnerability detection, fraud, offline payments, and regulatory responsibility [18-21, 36-39, 43-46]. The field is shifting from whether users will adopt a wallet to whether wallet ecosystems operate dependably under adversarial and regulatory conditions.

Security is quantitatively dominant but conceptually

fragmented: protocol-oriented papers demonstrate mechanisms such as key protection, ownership proofs, and offline payments [10-21, 35-39], while behavioral papers treat security as a perception influencing use and loyalty [3, 4, 28, 29, 33, 34]. Integrating these evidence standards requires models linking control design and incidents to user confidence and recovery outcomes.

The declining relative share of privacy-focused work suggests specialization in a small group of policy-compliance studies, not reduced privacy risk, even as wallets combine more data types and introduce new linkability concerns. Privacy research should move beyond policy-text analysis toward data-flow mapping and comparative enforcement outcomes.

Most importantly, auditability is almost absent; this is the gap that distinguishes assurance from the broader security literature. A secure protocol cannot alone demonstrate that controls operated continuously or that retained evidence supports independent review. Even recent smart-contract security work treats auditability as an application property rather than a measurable construct [39]. Wallet research therefore needs explicit control objectives, event-log integrity, and assurance reporting across custodial, mobile-payment, CBDC, and smart-contract environments.

6. RESEARCH AGENDA AND IMPLICATIONS

6.1 Research agenda

A future research agenda should prioritize: (1) validated assurance constructs distinguishing perceived security from verified control effectiveness; (2) auditable architectures with tamper-evident logging and recoverable key controls; (3) comparative governance/liability analysis across custodial, non-custodial, and CBDC wallets; and (4) longitudinal, cross-country studies linking regulation, controls, incidents, and trust.

6.2 Security assurance control-evidence framework

To translate the mapped evidence gaps into engineering and governance requirements, Table 6 links six assurance dimensions to illustrative control objectives and reviewable evidence. The framework does not claim that the controls are already standardized across wallet types. Rather, it specifies the minimum evidence categories that future empirical studies can test in custodial, non-custodial, mobile-payment, CBDC, and smart-contract environments.

Table 6. Security assurance control-evidence framework

Assurance Dimension	Illustrative Control Objective	Verifiable Evidence
Authentication	Prevent unauthorized wallet access and privileged misuse	Authentication logs, factor-enrolment records, failed-access alerts
Key custody	Protect key generation, storage, recovery, and transfer	Key-ceremony records, custody approvals, recovery-test evidence
Transaction integrity	Preserve authorization, completeness, and non-repudiation	Signed transaction records, reconciliation results, exception logs
Fraud monitoring	Detect anomalous or abusive transactions promptly	Model alerts, explainability outputs, case disposition and escalation records
Privacy	Limit data collection, linkage, retention, and disclosure	Data-flow maps, consent records, retention logs, access reviews
Incident governance	Assign responsibility and preserve reviewable incident evidence	Incident timelines, chain-of-custody records, remediation approvals

Table 7. Derivation of the security assurance control-evidence framework from the coded corpus

Assurance Dimension (Table 6)	Corresponding Coding Category (Table 5)	Supporting References
Authentication & Key custody	Security/authentication	[9-21, 35, 36]
Transaction integrity & Incident governance	Governance/regulation/compliance	[25, 26, 37-39]
Fraud monitoring	Fraud/financial crime	[43-46]
Privacy	Privacy/data protection	[22-24]

The six dimensions in Table 6 constitute a normative synthesis that translates the evidence gaps identified through the scientometric analysis—principally the near-total absence of auditability as a title or keyword construct—into engineering and governance requirements, rather than representing a direct output of the spectral clustering. Table 7 clarifies this derivation by mapping each dimension to its corresponding multi-label coding category in Table 5 and to the supporting references.

6.3 Practical and policy implications

For researchers, the findings call for interdisciplinary designs connecting behavioral trust, cybersecurity evaluation, privacy engineering, regulation, and assurance testing. Wallet providers should support trust claims with observable control evidence rather than communication alone. Regulators can use comparable assurance criteria to clarify minimum expectations for authentication, custody, privacy, fraud monitoring, recovery, interoperability, and third-party governance. For accounting and audit professionals, the relevant object is not conventional financial reporting but the wallet as a technology-enabled control environment whose transaction integrity, access management, evidence retention, and responsibility arrangements require systematic assessment.

7. CONCLUSION

This study mapped 72 Scopus-indexed articles on digital-wallet security assurance published between 2015 and 2025. The evidence shows a recent, interdisciplinary field whose historical influence remains rooted in adoption and trust, while

technical work increasingly addresses authentication, crypto-custody, vulnerability detection, fraud, offline payments, and regulatory responsibility. Security is prominent but fragmented across behavioral perceptions, protocol demonstrations, forensic investigations, and governance studies. Auditability is virtually absent as an explicit construct. The proposed control–evidence framework converts this absence into testable requirements for authentication, custody, transaction integrity, fraud monitoring, privacy, and incident governance. Digital-wallet research has therefore moved beyond adoption, but it has not yet established common evidence for demonstrating that controls operate effectively, accountably, and under independent review.

The study is limited to Scopus, English-language articles, and records published through 2025. The specialized query improves precision but may omit studies that use product names or assurance terminology not captured by the equation. Citation counts favor older publications; country extraction depends on affiliation metadata; and keyword clustering is sensitive to author terminology and the frequency threshold. Dictionary-based coding is transparent and reproducible but cannot replace independent content analysis. Future research should validate the categories through independent coders, semantic models, or embedding-based techniques and should test the proposed evidence categories against actual wallet architectures, incidents, and regulatory regimes. Title-and-abstract screening was conducted collectively by all seven authors rather than through independent duplicate screening; consequently, no inter-rater agreement statistic was calculated. Country-level findings use full rather than fractional counting, which may modestly overstate the productivity of countries whose publications disproportionately involve multinational teams. Because the recent sub-period (2023–2025) is markedly shorter than the early sub-period (2015–2022), the thematic comparison is exploratory. Within-period shares account for differences in corpus size but do not eliminate the imbalance in temporal coverage. Future studies with a longer post-2023 window should test these patterns using matched equal-length periods, rolling averages, alternative cut-off years, or trend regression of annual thematic shares. A systematic abstract-level search for auditability-related terms across all 72 abstracts, followed by manual verification, is also needed.

DATA AVAILABILITY

The complete Scopus search equation is provided in Appendix A. The eligibility criteria, screening procedure, period definition, keyword normalization, thematic coding, country-counting rule, and international-collaboration definition are described in Section 3. No separate supplementary file or external dataset is required to interpret the results reported in this article.

REFERENCES

[1] Singh, N., Sinha, N. (2020). How perceived trust mediates merchant's intention to use a mobile wallet technology. Journal of Retailing and Consumer Services, 52: 101894. https://doi.org/10.1016/j.jretconser.2019.101894

[2] To, A.T., Trinh, T.H.M. (2021). Understanding behavioral intention to use mobile wallets in Vietnam: Extending the TAM model with trust and enjoyment. Cogent Business & Management, 8(1): 1891661. https://doi.org/10.1080/23311975.2021.1891661

[3] 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. https://doi.org/10.1177/0972150920924506

[4] Mombeuil, C., Uhde, H. (2021). Relative convenience, relative advantage, perceived security, perceived privacy, and continuous use intention of China's WeChat Pay: A mixed-method two-phase design study. Journal of Retailing and Consumer Services, 59: 102384. https://doi.org/10.1016/j.jretconser.2020.102384

[5] Alaeddin, O., Rana, A., Zainudin, Z., Kamarudin, F. (2018). From physical to digital: Investigating consumer behaviour of switching to mobile wallet. Polish Journal of Management Studies, 17(2): 18-30. https://doi.org/10.17512/pjms.2018.17.2.02

[6] Mombeuil, C. (2020). An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets. Journal of Retailing and Consumer Services, 55: 102127. https://doi.org/10.1016/j.jretconser.2020.102127

[7] Sarmah, R., Dhiman, N., Kanojia, H. (2021). Understanding intentions and actual use of mobile wallets by millennial: An extended TAM model perspective. Journal of Indian Business Research, 13(3): 361-381. https://doi.org/10.1108/JIBR-06-2020-0214

[8] Garrouch, K. (2021). Does the reputation of the provider matter? A model explaining the continuance intention of mobile wallet applications. Journal of Decision Systems, 30(2-3): 150-171. https://doi.org/10.1080/12460125.2020.1870261

[9] Biryukov, A., Tikhomirov, S. (2019). Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. Pervasive and Mobile Computing, 59: 101030. https://doi.org/10.1016/j.pmcj.2019.101030

[10] Cambou, B.F., Alam, M. (2025). Challenge-response pair mechanisms and multi-factor authentication schemes to protect private keys. Applied Sciences, 15(6): 3089. https://doi.org/10.3390/app15063089

[11] Wang, C., Liu, Z.Y., Mambo, M. (2024). On the proof of ownership of digital wallets. Cryptography, 8(4): 57. https://doi.org/10.3390/cryptography8040057

[12] Yoon, J., Kim, Y. (2025). Offline payment of central bank digital currency based on a trusted platform module. Journal of Cybersecurity and Privacy, 5(2): 14. https://doi.org/10.3390/jcp5020014

[13] Mirza, M.M., Ozer, A., Karabiyik, U. (2022). Mobile cyber forensic investigations of Web3 wallets on Android and iOS. Applied Sciences, 12(21): 11180. https://doi.org/10.3390/app122111180

[14] Qin, Z., Sun, J.F., Wahaballa, A., Zheng, W.T., Xiong, H., Qin, Z.G. (2017). A secure and privacy-preserving mobile wallet with outsourced verification in cloud computing. Computer Standards & Interfaces, 54: 55-60. https://doi.org/10.1016/j.csi.2016.11.012

[15] Volety, T., Saini, S., McGhin, T., Liu, C.Z., Choo, K.K.R. (2019). Cracking Bitcoin wallets: I want what you have in the wallets. Future Generation Computer Systems, 91: 136-143. https://doi.org/10.1016/j.future.2018.08.029

[16] He, S.Y., Wu, Q.H., Luo, X.Z., et al. (2018). A social-network-based cryptocurrency wallet-management scheme. IEEE Access, 6: 7654-7663. https://doi.org/10.1109/ACCESS.2018.2799385
[17] Thomas, T., Piscitelli, M., Shavrov, I., Baggili, I. (2020). Memory FORESHADOW: Memory forensics of hardware cryptocurrency wallets—A tool and visualization framework. Forensic Science International: Digital Investigation, 33: 301002. https://doi.org/10.1016/j.fsidi.2020.301002
[18] He, X.J., Lin, J.F., Li, K.Z., Chen, X.M. (2019). A novel cryptocurrency wallet management scheme based on decentralized multi-constrained derangement. IEEE Access, 7: 185250-185263. https://doi.org/10.1109/ACCESS.2019.2961183
[19] Park, A.H., Ryu, H., Park, W., Jeong, D. (2023). Forensic investigation framework for cryptocurrency wallet in the end device. Computers & Security, 133: 103392. https://doi.org/10.1016/j.cose.2023.103392
[20] Bukhari, S.T., Janjua, M.U., Qadir, J. (2024). Secure storage of crypto wallet seed phrase using ECC and splitting technique. IEEE Open Journal of the Computer Society, 5: 278-289. https://doi.org/10.1109/OJCS.2024.3398794
[21] Erinle, Y., Feng, Y., Xu, J., Vadgama, N., Tasca, P. (2025). Shared-custodial wallet for multi-party crypto-asset management. Future Internet, 17(1): 7. https://doi.org/10.3390/fi17010007
[22] Akanfe, O., Valecha, R., Rao, H.R. (2021). Design of an inclusive financial privacy index (INF-PIE): A financial privacy and digital financial inclusion perspective. ACM Transactions on Management Information Systems, 12(1): 1-33. https://doi.org/10.1145/3403949
[23] Akanfe, O., Valecha, R., Rao, H.R. (2020). Assessing country-level privacy risk for digital payment systems. Computers & Security, 99: 102065. https://doi.org/10.1016/j.cose.2020.102065
[24] Akanfe, O., Valecha, R., Rao, H.R. (2023). Design of a compliance index for privacy policies: A study of mobile wallet and remittance services. IEEE Transactions on Engineering Management, 70(3): 864-876. https://doi.org/10.1109/TEM.2020.3015222
[25] Peeters, J. (2020). Data protection in mobile wallets. European Data Protection Law Review, 6(1): 56-65. https://doi.org/10.21552/edpl/2020/1/8
[26] Zetzsche, D., Nikolakopoulou, A. (2025). Crypto custody: An empirical assessment. Journal of Financial Regulation, 11(1): 73-97. https://doi.org/10.1093/jfr/fjaf004
[27] Guan, Y., Tick, A. (2025). Security of personal information in electronic payments: A bibliometric analysis and model extension. International Journal of Safety and Security Engineering, 15(4): 631-641. https://doi.org/10.18280/ijsse.150401
[28] Muhtasim, D.A., Tan, S.Y., Hassan, M.A., Pavel, M.I., Susmit, S. (2022). Customer satisfaction with digital wallet services: An analysis of security factors. International Journal of Advanced Computer Science and Applications, 13(1): 195-206. https://doi.org/10.14569/IJACSA.2022.0130124
[29] Chauhan, V. (2024). Understanding users' protective behavior and its suppressor effect on perceived risk in M-wallet/banking use: An Indian urban-rural comparison. Technological Forecasting and Social Change, 201: 123255. https://doi.org/10.1016/j.techfore.2024.123255
[30] Ajina, A.S., Joudeh, J.M.M., Ali, N.N., Zamil, A.M., Hashem, T.N. (2023). The effect of mobile-wallet service dimensions on customer satisfaction and loyalty: An empirical study. Cogent Business & Management, 10(2): 2229544. https://doi.org/10.1080/23311975.2023.2229544
[31] Rana, N.P., Luthra, S., Rao, H.R. (2023). Assessing challenges to mobile wallet usage in India: An interpretive structural modelling approach. Information Technology & People, 36(4): 1533-1554. https://doi.org/10.1108/ITP-07-2021-0535
[32] Rahman, S., Nguyen-Viet, B., Nguyen, Y.T.H., Kamran, S. (2024). Promoting fintech: Driving developing-country consumers' mobile-wallet use through gamification and trust. International Journal of Bank Marketing, 42(5): 841-869. https://doi.org/10.1108/IJBM-01-2023-0033
[33] Ojo, A.O., Fawehinmi, O., Ojo, O.T., Arasanmi, C., Tan, C.N.L. (2022). Consumer usage intention of electronic wallets during the COVID-19 pandemic in Malaysia. Cogent Business & Management, 9(1): 2056964. https://doi.org/10.1080/23311975.2022.2056964
[34] Chand, K., Tiwari, R., Gupta, A., Taneja, S., Özen, E. (2025). How does perceived security influence mobile wallet users' behavior? A SEM investigation. Managerial Finance, 51(1): 146-165. https://doi.org/10.1108/MF-05-2024-0414
[35] Houy, S., Schmid, P., Bartel, A. (2024). Security aspects of cryptocurrency wallets: A systematic literature review. ACM Computing Surveys, 56(1): 1-31. https://doi.org/10.1145/3596906
[36] Iqbal, S., Irfan, M., Ahsan, K., et al. (2020). A novel mobile wallet model for elderly using fingerprint as authentication factor. IEEE Access, 8: 177405-177423. https://doi.org/10.1109/ACCESS.2020.3025429
[37] Al-Zubaidie, M., Jebbar, W.A. (2024). Providing security for flash loan system using cryptocurrency wallets supported by XSalsa20 in a blockchain environment. Applied Sciences, 14(14): 6361. https://doi.org/10.3390/app14146361
[38] Rattanawiboonsom, V., Khan, N. (2024). Blockchain technology in mobile payments: A systematic review of security enhancements in mobile commerce. International Journal of Interactive Mobile Technologies, 18(21): 134-148. https://doi.org/10.3991/ijim.v18i21.52099
[39] Wilczyński, A., Jasnosz, G. (2025). Security assessment of smart contract integration and wallet interaction in decentralized applications: A case study of BlockScribe. Applied Sciences, 15(15): 8473. https://doi.org/10.3390/app15158473
[40] Aria, M., Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4): 959-975. https://doi.org/10.1016/j.joi.2017.08.007
[41] Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., Lim, W.M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, 133: 285-296. https://doi.org/10.1016/j.jbusres.2021.04.070
[42] Page, M.J., McKenzie, J.E., Bossuyt, P.M., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372: n71.

https://doi.org/10.1136/bmj.n71
[43] Abdirahman, A.A., Hashi, A.O., Dahir, U.M., Elmi, M.A., Rodriguez, O.E.R. (2024). Enhancing security in mobile wallet payments: Machine learning-based fraud detection across prominent wallet platforms. International Journal of Electronics and Communication Engineering, 11(3): 96-105. https://doi.org/10.14445/23488549/IJECE-V11I3P110
[44] Janbhasha, S., Kumar, C.H.N.S., Sitharamulu, V., Madhu Babu, B.N.V., Battu, H.R., Venkataramana, K. (2025). A hybrid approach for fraud detection in digital wallet transactions using adversarial autoencoders and gated recurrent units. Engineering, Technology & Applied Science Research, 15(4): 25532-25537. https://doi.org/10.48084/etasr.10898
[45] Lim, H.J., Lee, S., Kim, M., Lee, W. (2025). Comparative analysis of security features and risks in digital asset wallets. Electronics, 14(12): 2436. https://doi.org/10.3390/electronics14122436
[46] Gao, B.R., Zhang, R., Tao, Y., Qin, S.H. (2025). Cocoon: Certificateless blockchain wallet supporting both stealth address and revocation. Cybersecurity, 8(1): 100. https://doi.org/10.1186/s42400-025-00380-7

APPENDIX

Complete Scopus search equation

```
(
 TITLE("digital wallet*" OR "mobile wallet*" OR "electronic wallet*" OR "e-wallet*" OR "m-wallet*" OR "payment wallet*" OR "cryptocurrency wallet*" OR "crypto wallet*" OR "Web3 wallet*" OR "digital asset wallet*" OR "self-custody wallet*")
 OR
 AUTHKEY("digital wallet*" OR "mobile wallet*" OR "electronic wallet*" OR "e-wallet*" OR "m-wallet*" OR "payment wallet*" OR "cryptocurrency wallet*" OR "crypto wallet*" OR "Web3 wallet*" OR "digital asset wallet*" OR "self-custody wallet*")
)
AND
(
 TITLE(secur* OR cybersecurity OR authentication OR cryptograph* OR encryption OR privac* OR "data protection" OR fraud* OR "money laundering" OR AML OR governance OR regulation OR regulatory OR compliance OR audit* OR accountability OR transparency OR "consumer protection" OR KYC OR risk* OR trust* OR safety OR forensic* OR resilience OR recovery OR "proof of ownership" OR "seed phrase")
 OR
 AUTHKEY(secur* OR cybersecurity OR authentication OR cryptograph* OR encryption OR privac* OR "data protection" OR fraud* OR "money laundering" OR AML OR governance OR regulation OR regulatory OR compliance OR audit* OR accountability OR transparency OR "consumer protection" OR KYC OR risk* OR trust* OR safety OR forensic* OR resilience OR recovery OR "proof of ownership" OR "seed phrase")
)
AND TITLE-ABS-KEY(payment* OR transaction* OR financ* OR fintech OR banking OR "electronic money" OR "digital money" OR "mobile commerce" OR "financial service*")
AND PUBYEAR > 2014 AND PUBYEAR < 2026
AND (DOCTYPE(ar) OR DOCTYPE(re))
AND LANGUAGE(english)
```